ALGEBRAI NYELV- ÉS KÓDELMÉLET

Babcsányi István

2013

Tartalomjegyzék

ELŐSZÓ

A jegyzetet az *Algebrai Automaelmélet* elektronikus jegyzet szerves folytatásának szánjuk. A jegyzet elérhető az alábbi címen:

`http://tankonyvtar.ttk.bme.hu/pdf/18.pdf`

Mind a két jegyzetben sok évi oktatási tapasztalat összegződik. Tartalmazzák a Budapesti Műszaki és Gazdaságtudományi Egyetem Természettudományi Karának alkalmazott matematikus szakán tartott *Formális rendszerek* négyféléves témacsoport utolsó három félévének anyagát, de ennél jóval bővebb terjedelműek. A kötetek egyfajta bevezetést adnak az automaták, a formális nyelvek és a változó hosszúságú kódok algebrai elméletébe. Az elméletbe további kiváló bevezetést nyújt a [10] elektronikus jegyzet, amely igen sok példával és feladattal segíti a terület tökéletes megértését. A terület egy rövid világos áttekintését adja a [14] elektronikus jegyzet. A jegyzethez csatlakozik a sok feladatot tartalmazó [15] elektronikus példatár. Minthogy a [10] és a [15] jegyzetek már mindenki számára hozzáférhetők, ezért szükségtelennek tartottuk, hogy a jelen jegyzet nagyon sok feladatot tartalmazzon. A fejezetek többsége végén azonban mégis vannak feladatok, amelyek remélhetőleg teljesebbé teszik az előbb említett két jegyzet, valamint a [2] jegyzetünk feladatgyűjteményét. A jegyzet alig tartalmaz automatákkal kapcsolatos feladatot, mivel ilyen jellegű feladatok sokasága található a [2] jegyzetünkben is. A feladatokhoz általában megoldási útmutatót adunk. Sok esetben közöljük a teljes megoldást.

A jegyzetünkben is felhasznált halmazelméleti és algebrai fogalmakat és tételeket Az *Algebrai Automataelmélet* elektronikus jegyzetünk *Függelék*ében foglaltuk össze. A Tárgymutató ezeket az adatokat nem tartalmazza. A lineáris algebra, a számelmélet és a kombinatorika alapfogalmait és alapvető eredményeit azonban most is ismertnek tételezzük fel.

Megemlítjük, hogy algoritmikusan megoldható és megoldhatatlan problémákkal is foglalkozunk. Az algoritmus matematikai fogalmára nincs egységes, mindenki számára elfogadott definíció. A számunkra megfelelő algoritmus fogalmának kialakításához közelítsük meg először a matematikai eljárás fogalmát Révész György segítségével. A [37] alapműnek is tekinthető munkájában a következőket írja:

Az olyan módszert nevezzük matematikai értelemben eljárásnak, amelynek minden részlete teljes pontossággal előre ki van dolgozva, tehát menet közben további gondolkodást nem igényel. Ez végeredményben azt jelenti, hogy minden eljárást elvileg egy számítógépbe be lehet programozni.

*Eljárás*on általában valamely nyelven véges hosszúságú kifejezéssel leírt, diszkrét lépésekben végrehajtható utasítások egy rendszerét értik, amelyek végrehajtásának sorrendje is meg van adva. Ez természetesen nem matematikai

meghatározás. A számítógépek elterjedésével azonban sok eljárás programozható, azaz átírható (kódolható) a számítógépek nyelvére. A.M.Turing nyomán képzeljünk el egy ideális számítógépet (Turing automatát), amely diszkrét időskálában dolgozik, soha nem hibázik, akármennyi ideig képes dolgozni, anélkül, hogy elromolna, s kapacitása korlátlanul bővíthető. A Turing automata tehát a számítógépek egy elméleti modelljének tekinthető. (A Turing automata fogalmát a 11.1. alfejezetben pontosan megadjuk.) *Matematikai algoritmus*nak vagy röviden *algoritmus*nak olyan (matematikai) eljárást nevezünk, amely véges számú lépésben befejeződik. A *Church–Turing tézis* azt mondja ki, hogy minden formalizálható probléma, amely algoritmussal megoldható, az megoldható Turing automatával is. Eddig nem találtak olyan matematikai algoritmust, amelyhez nem lehet a megfelelő Turing automatát megkonstruálni. A vizsgálatainkban igaznak fogadjuk el a *Church–Turing tézis*t.

Fontosak lesznek számunkra az *eldöntési eljárások*, amelyek állítások igazságának eldöntésére szolgálnak. A *kiszámítási* vagy *megadási* eljárások egy adott eredmény vagy objektum megadására vagy megkonstruálására szolgálnak. A *felsorolási eljárások* eredmények, objektumok felsorolását adják. Az algoritmusok elméletébe jó bevezetést nyújt a [38] felsőoktatási tankönyv.

A lektorálás hálátlan munkáját most is, mint az előző jegyzetem esetében, kedves barátom Dömösi Pál egyetemi tanár végezte el. Lelkiismeretes munkáját hálásan köszönöm. Köszönettel tartozom most is Sági Gábor egyetemi docensnek a rajzok precíz elkészítéséért. Köszönöm a téma iránt érdeklődő halgatóimnak, hogy a jegyzet részletes áttanulmányozása során sok hibát kijavítottak benne. Nem utolsósorban megköszönöm Tóth Lászlónak a jegyzet végső formájának gondos kialakítását.

I. rész

NYELVEK

A formális nyelvek algebrai elmélete ma már a számítástudománynak fontos önálló területe, amelynek megalapozásában a döntő lépést Noam Chomsky tette meg a generatív grammatikák fogalmának bevezetésével. Chomsky a generatív grammatika fogalmát a természetes nyelvek szintaktikai (nyelvtani) elemzése céljából vezette be. Egy természetes nyelv tekinthető az ábécéje (beleértve az írásjeleket és a szóközt is) feletti szabad félcsoport szintaktikailag és szemantikailag (jelentéstanilag) helyes mondatokból álló részhalmazának. A generatív grammatikák a programozási nyelvek, mint speciális formális nyelvek, esetén is alapvető fontosságúak. Egy programozási nyelvhez meg kell adni azon szabályok összeségét, amelyek segítségével definiálható, hogy egy ezen nyelven írott programot mikor tekintünk formailag helyesnek. Ezeknek a szabályoknak az összeségét a programozási nyelv *szintaxis*ának nevezzük. A legelterjedtebb módszer egy programozási nyelv szintaxisának megadására a generatív grammatikával való megadás. Ezzel a kérdéssel nem foglalkozunk, de a formális nyelvek és az automaták szoros kapcsolata miatt a következőkben formális nyelvek algebrai elméletének egy rövid megalapozását adjuk, különös tekintettel az automatákkal való kapcsolatukra. Érdemes tanulmányozni Révész György kitűnően megírt [37] munkáját, valamint Arto Salomaa átfogó [40] monográfiáját.

Az általunk is ismertetett klasszikus formális nyelvek elméletében egy nyelvet egy grammatika generál, vagy mint majd a későbbiekben látjuk egy automata ismer fel. A modern szamítástudományban a számítások (levezetések) megosztása is fontos szerepet játszik. Ez a formális nyelvek elméletében a *grammatikai rendszerek* megjelenését jelentette. A grammatikai rendszerek vizsgálatára nem térhetünk ki, de rövid bevezetést találunk a [10] egyetemi jegyzetben. A részletesebb tanulmányozás céljából ajánljuk a [8] monográfiát is.

1. fejezet

Nyelvek algebrája

Legyen U tetszőleges nemüres halmaz. Összhangban a természetes nyelvek nyelvtani fogalmaival, a formális nyelvek elméletében U-t *ábécé*nek is mondjuk. Az U elemeit betűknek vagy jeleknek is nevezzük. Az U^* szabad monoid bármely L részhalmazát *(U feletti) formális nyelv*nek vagy röviden *nyelv*nek nevezzük. Ha $L' \subseteq L$, akkor azt mondjuk, hogy L' az L nyelv *részny*elve. Az L nyelv elemeit *mondatok*nak is nevezzük. Ha L véges halmaz, akkor *véges nyelv*nek, ha pedig végtelen halmaz, akkor *végtelen nyelv*nek mondjuk. Az $\emptyset$ üres halmazt *üres nyelv*nek, az U^*-ot pedig *univerzális nyelv*nek nevezzük U felett.

Megjegyezzük, hogy ha az U ábécé véges, akkor U^* megszámlálhatóan végtelen és az U feletti nyelvek halmaza, azaz az U^* halmaz $P(U^*)$ hatványhalmaza kontinuum számosságú.

A természetes nyelvek valamilyen véges ábécé feletti formális nyelvek. Legyen például U a magyar ábécé betűit, az írásjeleket és az elválasztó üres jelet tartalmazó halmaz. (Az elválasztó üres jel nem az üres szó!) A magyar nyelv az az $L(\subset U^*)$ nyelv, amelynek elemei az értelmes magyar szavak és mondatok halmaza, beleértve a betűket, az írásjeleket és az elválasztó üres jelet is.(Természetesen ez a halmaz időben változó.)

1.1. Műveletek nyelvekkel

Nyelvek egyesítésén, metszetén, különbségén halmazelméleti egyesítésüket, metszetüket, különbségüket értjük. Egy U halmaz feletti nyelvek halmaza, azaz U^* halmaz $P(U^*)$ hatványhalmaza a halmazelméleti egyesítés metszet és komplementerképzés műveletekre Boole algebra. Az üres szót továbbra is e-vel jelöljük. Az egyesítés, a metszet és komplementerképzés műveleteket *Boole műveletek*nek nevezzük. A nyelvek egyesítésének műveletét a nyelvek *összeadás*ának

is nevezzük és a + műveleti jelet is használjuk a formális nyelvek algebrai elméletében. Megállapodunk az egyszerűbb írásmód kedvéért abban is, hogy az $\{u\}$ $(u \in U \cup \{e\})$ egyelemű nyelveket azonositjuk u elemükkel, azaz $\{u\} = u$. Az U halmaz elemeit *elemi nyelvek*nek is hívjuk.

A nyelvek között további műveleteket vezetünk be. Az L_1 és L_2 nyelv *szorzatá*n vagy *konkatenációjá*n az

$$L_1 L_2 = \{uv; u \in L_1, v \in L_2\}$$

nyelvet értjük. Egy U halmaz feletti nyelvek $\mathcal{L}(U)$ halmaza az összeadás $(+)$ és a konkatenáció $(\cdot)$ műveletére félgyűrűt alkot, amelynek $\emptyset$ a zéruseleme és e az egységeleme. Továbbá

$$(L_1 \cap L_2)L_3 \subseteq L_1 L_3 \cap L_2 L_3, \quad L_3(L_1 \cap L_2) \subseteq L_3 L_1 \cap L_3 L_2.$$

Definiáljuk egy L nyelv nemnegatív egész kitevős hatványait, mégpedig az

$$L^0 = e, \quad L^{k+1} = L^k L \quad (k \in N)$$

összefüggésekkel. Egy L nyelv *Kleene iteráltjá*n vagy röviden *iteráltjá*n azt az L^* nyelvet értjük, amely azokból és csak azokból szavakból áll, amelyek előállíthatók véges sok L-beli szó szorzataként, beleértve az L elemeit, mint egytényezős és az üres szót, mint nullatényezős L-beli elemek szorzatát, azaz

$$L^* = \sum_{k=0}^{\infty} L^k.$$

A $*$ (egyváltozós) műveletet *Kleene iteráció*nak vagy *iteráció*nak nevezzük. Nem nehéz belátni, hogy bármely L nyelvre $(L^*)^* = L^*$, valamint $\emptyset^* = e^* = e$. Egy L nyelv *e-mentes iteráltjá*n értjük az $L^+ = \sum_{k=1}^{\infty} L^k$ nyelvet. Ez azt jelenti, hogy ha $e \in L$, akkor $L^+ = L^*$, ha pedig $e \notin L$, akkor $L^+ = L^* - e$. Az összeadás, a konkatenáció és a iteráció műveletét *reguláris műveletek*nek nevezzük. Az $\mathcal{L}(U) = (P(U^*), +, ., *)$ algebrai struktúrát (*az U halmaz feletti*) *nyelvalgebrá*nak nevezzük. $\mathcal{L}(U)$ nyelvalgebra tetszőleges L_1 és L_2 elemére

$$(L_1 \cap L_2)^* \subseteq L_1^* \cap L_2^*, \quad L_1^* + L_2^* \subseteq (L_1 + L_2)^*.$$

Egyszerűen bizonyítható a

1.1. Lemma. *Ha L, L_1 és L_2 tetszőleges nyelvek, akkor teljesülnek az*

$$L^* = e + LL^*, \quad LL^* = L^*L, \quad (L_1 + L_2)^* = (L_1^* L_2^*)^*,$$

$$L^* = (e + L + \cdots + L^{k-1})(L^k)^* \ (k \in N_+)$$

azonosságok.

Egy U halmaz feletti nyelvet *reguláris nyelv*nek nevezünk, ha előállítható az U elemeiből és az $\emptyset$ üres nyelvből a reguláris műveletek véges számú alkalmazásával. Ezek szerint minden véges nyelv, így minden elemi nyelv is reguláris. Az $\emptyset$ üres nyelvet is regulárisnak tekintjük. Mivel $e = \emptyset^*$, ezért az e nyelv is reguláris.

Ha $U = \{u_1, u_2, \ldots, u_n\}$, azaz U véges ábécé, akkor U^* és U^+ is reguláris nyelv , ugyanis

$$U^* = (u_1 + u_2 + \cdots + u_n)^*,$$

$$U^+ = (u_1 + u_2 + \cdots + u_n)(u_1 + u_2 + \cdots + u_n)^*.$$

Minden reguláris nyelvhez hozzárendelhetünk egy ún. (*U feletti*) *reguláris kifejezés*t az alábbi módon: Egy L nyelv reguláris kifejezésén értsünk olyan kifejezést, amely azt mutatja meg, hogyan állítható elő az L nyelv az U elemeiből és az $\emptyset$ üres nyelvből a reguláris műveletek véges számú alkalmazásával. Egy reguláris kifejezés tehát véges sok $u \in U$ és az $\emptyset$ szimbólumokból, a reguláris műveletek műveleti jeleiből és a műveletek elvégzésének sorrendjét meghatározó zárójelpárokból épül fel, azaz maga is egy szó az $U \cup \{\emptyset, +, ., *, (,)\}$ ábécé felett. Így az üres nyelv reguláris kifejezése az $\emptyset$ szimbólum, az $u \in U$ elemi nyelv reguláris kifejezése pedig az u szimbólum. A definícióból látható, hogy nyelvekből reguláris műveletek véges számú alkalmazásával kapott nyelvek egy reguláris kifejezését megkapjuk, ha a nyelvek reguláris kifejezéseit ugyanúgy kapcsoljuk össze reguláris műveletekkel, mint a nyelveket.

Ha a műveletek sorrendjét zárójelekkel nem adjuk meg egy kifejezésben, akkor megállapodás szerint először az iterációt, majd a szorzást, s végül az összeadást végezzük el. A definícióból látható, hogy minden reguláris kifejezés egyértelműen meghatároz egy reguláris nyelvet, ezért a reguláris nyelveket megadhatjuk reguláris kifejezésükkel is. A reguláris nyelvek nem határozzák meg egyértelműen reguláris kifejezésüket. Ha $U = \{u_1, u_2, \ldots, u_n\}$, akkor például az U^* univerzális nyelv az $(u_1 + u_2 + \cdots + u_n)^*$ és a

$$(u_1 + u_2 + \cdots + u_n)(u_1 + u_2 + \cdots + u_n)^* + \emptyset^*$$

reguláris kifejezéssel is megadható. Amikor egy reguláris nyelvet reguláris kifejezéssel adunk meg, a nyelv és a reguláris kifejezés közé egyenlőség jelet teszünk. Ekkor tulajdonképpen helytelenül járunk el, mivel az egyenlőség egyik oldalán szavaknak egy halmaza, a másik oldalon pedig egy formális kifejezés áll. Ebből azonban nem származik ellentmondás, a tárgyalásmódot viszont egyszerűbbé teszi.

Az U^*-beli $p^{-1} = u_{i_k} \ldots u_{i_2} x_{i_1}$ szót az U^*-beli $p = u_{i_1} u_{i_2} \ldots u_{i_k}$ szó *tükörképé*nek nevezzük. Ha $p_1, p_2, \ldots, p_k \in U^*$, akkor

$$(p_1 p_2 \ldots p_k)^{-1} = p_k^{-1} \ldots p_2^{-1} p_1^{-1}.$$

Egy L nyelv *tükörképe* pedig az pedig az $L^{-1} = \{p^{-1}; p \in L\}$ nyelv. Természetesen $(L^{-1})^{-1} = L$. Egy nyelvet (speciálisan egy szót) *palindrom*nak mondunk, ha megegyezik tükörképével. Egyszerű példák a palindromokra az $\emptyset$, e, U^*, U^+ nyelvek. Az összes (U^*-beli) palindromot tartalmazó nyelvet az (U *feletti*) *palindromok nyelvé*nek hívjuk. A palindromok nyelvének résznyelvei is palindromok. Azt az egyváltozós műveletet, amely minden szóhoz ill. nyelvhez a tükörképét rendeli, *tükrözés*nek hívjuk.

Jelölje $R(U)$ az U halmaz feletti reguláris nyelvek halmazát. $R(U)$ az U feletti nyelvek halmazának az a legszűkebb részhalmaza, amely tartalmazza az U feletti véges nyelveket, zárt véges sok nyelv egyesítésére és szorzására, továbbá a nyelvek iterációjára. Ez azt is jelenti, hogy az $\mathcal{R}(U) = (R(U), +, ., *)$ algebrai struktúra az U feletti $\mathcal{L}(U)$ nyelvalgebra részalgebrája, amelyet *reguláris nyelvalgebrá*nak nevezünk. A definícióból az is látható, hogy minden reguláris nyelv tükörképe is reguláris, azaz $\mathcal{R}(U)$ zárt a tükrözésre. A 8.6 Tétel szerint a véges ábécé feletti reguláris nyelvek Boole algebrát alkotnak az egyesítés, a metszet és a komplementerképzés műveletére.

Legyen L egy U halmaz feletti nyelv és $p \in U^*$ tetszőleges szó. Az L nyelv *p szerinti bal oldali deriváltjá*n az

$$L_p^{(b)} = \{q \in U^*; pq \in L\} \tag{1.1}$$

nyelvet értjük. Hasonló módon, L *p szerinti jobb oldali deriváltja* az

$$L_p^{(j)} = \{q \in U^*; qp \in L\} \tag{1.2}$$

nyelv. Nyilvánvaló, hogy $L_e^{(b)} = L_e^{(j)} = L$. Azokat az egyváltozós műveleteket, amelyek minden nyelvhez a $p \in U^*$ szerinti bal [jobb] oldali deriváltját rendeli, *p szerinti bal* [*jobb*] *oldali deriválás*nak nevezzük.

Tetszőleges U feletti L, L_1, L_2 nyelvekre és $u \in U$ betűre érvényesek az

$$(L^*)_u^{(b)} = L_u^{(b)} L^*, \quad (L^*)_u^{(j)} = L^* L_u^{(j)}, \tag{1.3}$$

$$(L_1 + L_2)_u^{(b)} = (L_1)_u^{(b)} + (L_2)_u^{(b)}, \quad (L_1 + L_2)_u^{(j)} = (L_1)_x^{(j)} + (L_2)_u^{(j)}, \tag{1.4}$$

$$(L_1 L_2)_u^{(b)} = (L_1)_u^{(b)} L_2 + \varepsilon(L_1)(L_2)_u^{(b)}, \tag{1.5}$$

$$(L_1 L_2)_u^{(j)} = L_1 (L_2)_u^{(j)} + (L_1)_u^{(j)} \varepsilon(L_2), \tag{1.6}$$

$$L = \sum_{u \in U} u L_u^{(b)} + \varepsilon(L) = \sum_{u \in U} L_u^{(j)} u + \varepsilon(L) \tag{1.7}$$

azonosságok, ahol

$$\varepsilon(L) = \begin{cases} e, & \text{ha } e \in L, \\ \emptyset, & \text{ha } e \notin L. \end{cases}$$

Tetszőleges U feletti L, L_1, L_2 nyelvekre és $p \in U^*$ szóra fennállnak a következő azonosságok is:

$$(L_1 + L_2)^{-1} = L_1^{-1} + L_2^{-1},\ (L_1L_2)^{-1} = L_2^{-1}L_1^{-1},\ (L^*)^{-1} = (L^{-1})^*, \tag{1.8}$$

$$(L_p^{(b)})^{-1} = (L^{-1})_{p^{-1}}^{(j)}, \quad (L_p^{(j)})^{-1} = (L^{-1})_{p^{-1}}^{(b)}. \tag{1.9}$$

Véges ábécé feletti reguláris nyelv bal [jobb] oldali deriváltjai is regulárisak. (Ezt a 8.6 Tétel bizonyításában mutatjuk meg.) Ez azt jelenti, hog az U véges ábécé feletti reguláris nyelvek $\mathcal{R}_U$ halmaza zárt bármely $p \in U^*$ szó szerinti bal [jobb] oldali deriválás műveletére.

Legyenek U_k $(k \in I)$ tetszőleges ($U = \{u_k;\ k \in I\}$-től nem feltétlenül különböző) halmazok, legyen továbbá $V = \cup_{k\in I} U_k$. Definiáljunk egy $h : U \to P(V^*)$ leképezést úgy, hogy minden $u_k \in U$ elemre $h(u_k) \in P(U_k^*)$ teljesüljön, azaz minden U_k elemhez egy U_k feletti nyelvet rendeljen. A h leképezés értelmezését terjesszük ki az U^* szabad monoidra úgy, hogy (a kiterjesztés után is megtartva a h jelölést) legyen $h : U^* \to P(V^*)$, amelyre teljesüljenek a

$$h(e) = e, \quad h(pq) = h(p)h(q) \quad (p, q \in U^*)$$

feltételek. A h leképezést *helyettesítés*nek nevezzük. A helyettesítés fogalmát szavakról nyelvekre is kiterjesztjük úgy, hogy minden $L \subseteq U^*$ nyelvre legyen

$$h(L) = \sum_{p\in L} h(p).$$

Azt mondjuk, hogy a h helyettesítés *reguláris*, ha minden $h(u_k)$ $(k \in I)$ nyelv reguláris. Továbbá, h *e-mentes helyettesítés*, ha az e üres szót egyik $h(u_k)$ nyelv sem tartalmazza. Végül a h helyettesítést *homomorfizmus*nak nevezzük, ha minden $h(u_k)$ nyelv egyelemű. Látható, hogy ebben az esetben h az U^* szabad monoidnak az V^* szabad monoidba való monoid-homomorfizmusa. Ebben az esetben a $h(L)$ nyelvet az $L \subseteq U^*$ nyelv *homomorf képé*nek nevezzük. A reguláris kifejezés és a helyettesítés definíciójából közvetlenül adódik a következő tétel.

1.2. Tétel. *A reguláris nyelvek halmaza zárt a reguláris helyettesítésre. Speciálisan, reguláris nyelv homomorf képe is reguláris.*

1.2. Végtelen szavak

Rövid bevezetést adunk a végtelen hosszúságú szavakat is tartalmazó nyelvek, egyszerűen mondva a *végtelen szavak* elméletébe. Legtöbb fogalom az előzőekben definiált bizonyos fogalmak általánosításai. A végtelen szavak elméletét

Dominique Perrin és Jean-Éric Pin részletesen tárgyalják a [36] monográfiában.

Legyen U tetszőleges ábécé. Az U ábécé elemeiből képezett

$$p = (u_1, u_2, \dots, u_k, \dots)$$

végtelen sorozatokat az U *ábécé feletti végtelen szavak*nak fogjuk nevezni és rájuk a

$$p = u_1 u_2 \dots u_k \dots$$

írásmódot használjuk. Az U feletti végtelen szavak halmazát jelöljük U^ω-val. Ebben a részben az U^* szabad monoid elemeit U *feletti véges szavak*nak is mondjuk. Legyen

$$U^\infty = U^* \cup U^\omega,$$

azaz az U *feletti szavak* halmaza. Az U^∞ halmaz részhalmazait is U *feletti nyelvek*nek fogjuk nevezni.

Tetszőleges $L \subseteq U^*$ és $M \subseteq U^\infty$ nyelv *szorzat*án vagy *konkatenáció*ján az

$$LM = \{pq : p \in L, q \in M\}. \tag{1.10}$$

nyelvet értjük. Nyilvánvaló, hogy minden $L, K \subseteq U^*$ és $M \subseteq U^\infty$ nyelvre

$$(LK)M = L(KM), \quad (L+K)M = LM + KM. \tag{1.11}$$

Az $L \subseteq U^*$ nyelvekre bevezetjük az ω *végtelen iteráció* műveletet az

$$L^\omega = \{p_1 p_2 \dots p_k \dots ;\ p_k \in L - e, k = 1, 2, \dots\} \tag{1.12}$$

definícióval. A definíció alapján

$$\emptyset^\omega = \{e\}^\omega = \emptyset$$

és minden $p \in U^+$ szóra

$$\{p\}^\omega = pp \dots p \dots,$$

azaz p egymásutánírása végtelen sokszor. Az előző részben bevezetett reguláris műveleteket és a végtelen iterációt együtt ω*-reguláris műveletek*nek nevezzük. Könnyen belátható az alábbi

1.3. Lemma. *Tetszőleges $L, K \in U^*$ nyelvekre*
(1) $(L+K)^\omega = (L^*K)^\omega + (L+K)^* L^\omega$;
(2) $(LK)^\omega = L(KL)^\omega$;
(3) $(\forall n \in N_+)((L^n)^\omega = (L^+)^\omega = L^\omega$;
(4) $LL^\omega = L^+ L^\omega = L^\omega$.

Most megadjuk az U feletti ω-reguláris nyelvek fogalmát. Ez a fogalom a véges szavakra értelmezett reguláris nyelvfogalom egy általánosítása. Az U feletti reguláris nyelvek halmaza legyen $\mathcal{R}(U)$. Az *U feletti ω-reguláris nyelvek osztálya* az U^∞ halmaz hatványhalmazának az a legszűkebb $\mathcal{R}$ részhalmaza, amely teljesíti az alábbi négy feltételt.
(1) $\emptyset \in \mathcal{R}$ és ha $u \in U$, akkor $\{u\} \in \mathcal{R}$;
(2) $\mathcal{R}$ zárt a nyelvek összeadására;
(3) Minden $L \subseteq U^*$ és $K \subseteq U^\infty$ nyelvre, ha $L, K \in \mathcal{R}$, akkor $LK \in \mathcal{R}$;
(4) Minden $L \subseteq U^*$ nyelvre, ha $L \in \mathcal{R}$, akkor $L^* \in \mathcal{R}$ és $L^\omega \in \mathcal{R}$.

Használjuk erre az $\mathcal{R}$ részhalmazra a $\mathcal{R}_\infty(U)$ jelölést. Összegezve, $\mathcal{R}_\infty(U)$ az U feletti nyelveknek az a legszűkebb halmaza, amely tartalmazza U^∞ véges részhalmazait, zárt véges sok nyelv egyesítésére és (1.10)-ben definiált szorzására, továbbá az iteráció és a (1.12)-ben definiált végtelen iteráció műveletére.

Legyen $\mathcal{R}_\omega(U)$ az U feletti végtelen szavak U^ω halmazának ω-reguláris részhalmaza, azaz

$$\mathcal{R}_\omega(U) = U^\omega \cap \mathcal{R}_\infty(U). \tag{1.13}$$

A $\mathcal{R}_\omega(U)$ halmaz elemeinek egy egyszerű jellemzését adja a következő tétel. Ezt jellemzést szokás definícióként is használni.

1.4. Tétel. *A $K \subseteq U^\omega$ nyelv akkor és csak akkor ω-reguláris U felett, ha véges sok LM^ω alakú nyelv összege, amelyekben $L \subseteq U^*$ és $M \in U^+$ reguláris nyelvek U felett.*

Bizonyítás Az nyilvánvaló, hogy ha $K \subseteq U^\omega$ nyelv ω-reguláris U felett véges sok LM^ω alakú nyelv összege, amelyekben $L \subseteq U^*$ és $M \in U^+$ reguláris nyelvek U felett, akkor K ω-reguláris U felett.

Megfordítva, azt látjuk be, hogy az (1.13)-ban megadott halmaz minden eleme a tételben megadott alakú. Az U feletti reguláris nyelvek $\mathcal{R}(U)$ halmazát az elemi nyelvekből a reguláris műveletek véges számú alkalmazásával kapjuk. Nyilvánvaló, hogy

$$\mathcal{R}(U) \cap \mathcal{R}_\omega(U) = \emptyset \tag{1.14}$$

Az $\mathcal{R}_\omega(U)$ ω-reguláris halmaz elemei $\mathcal{R}(U)$ elemeiből kaphatók az ω-reguláris műveletek véges számú alkalmazásával. Vagyis $\mathcal{R}_\omega(U)$ elemeit a következő módon kaphatjuk meg. Tekintjük $\mathcal{R}(U)$ elemei végtelen iteráltjainak halmazát, ehhez hozzáadjuk a végtelen iteráltak $\mathcal{R}(U)$ elemeivel balról való szorzatainak halmazát, és végül hozzáadjuk az igy kapott halmaz véges részhalmazainak egyesítéseit. Vagyis egy $K \subseteq U^\omega$ ω-reguláris nyelv U felett valóban véges sok LM^ω alakú nyelv összege, amelyekben $L \subseteq U^*$ és $M \in U^+$ reguláris nyelvek U felett. □

Egy nyelv akkor és csak akkor ω-reguláris nyelv, ha megadható *ω-reguláris kifejezés*sel. Az ω-reguláris kifejezés definíciója csak annyiban különbözik az előző részben megadott reguláris kifejezés definíciójától, hogy a reguláris műveleteket kiegészítjük az ω végtelen iterációval.

Megmutatható, hogy $\mathcal{R}_\omega(U)$ zárt a Boole műveletekre, azaz Boole algebra (Dominique Perrin és Jean-Éric Pin [36]). Ezt szemlélteti a következő egyszerű példa.

1.5. Példa. *Legyen $U = \{u, v\}$ és $L \subset U^\omega$ az a nyelv, amelynek a szavaiban v véges sokszor fordul elő. Az L nyelv megadható az $L = (u + v)^* u^\omega$ ω-reguláris kifejezéssel. azaz L ω-reguláris nyelv. Az L komplementere U^ω-ban azoknak a végtelen szavaknak a halmaza, amelyekben v végtelen sokszor fordul elő. Az L komplementere megadható az $\overline{L} = (u^* v)^\omega$ ω-reguláris kifejezéssel, ezért szintén ω-reguláris nyelv.*

Feladatok

1.1. Ha $K \subseteq U^+$, $L, M \subseteq U^*$ és $M = KM + L$, akkor $M = K^* L$.
1.2. Legyen $K \subseteq U^+$ és $L \subseteq U^*$. Igazoljuk, hogy az $X = KX + L$ $(X \subseteq U^*)$ egyenlet egyetlen megoldása $X = K^* L$.

2. fejezet

Generatív grammatikák

Egy véges nyelvet megadhatunk elemei felsorolásával is. Végtelen nyelv megadása általában bonyolultabb feladat. Ezért szeretnénk, olyan algoritmust találni, amely alkalmazásával a nyelv minden eleme származtatható és segítségével eldönthető, hogy egy szó az adott nyelvnek eleme vagy nem. A nyelvek ilyen algoritmikus megadására szolgálnak a generatív grammatikák. A generatív grammatika fogalmának megközelítéséhez tekintsük példaként a "Süt a nap." egyszerű magyar mondatot. A mondat szintaktikai elemzéséhez különböző nyelvtani kategóriák szükségesek. Vegyük például a "főnév" nyelvtani kategóriát. A "főnév" szó szerepel a magyar nyelv szókészletében is. Jelölje ezért a "főnév" nyelvtani kategóriát <főnév>, megkülönböztetve a "főnév" szótól. Induljunk ki a <mondat> nyelvtani kategóriából. Írjuk helyébe az

<ige><szóköz><névelő><szóköz><főnév><írásjel>

mondatformát, amelyre

$$\text{<mondat>} \longrightarrow \text{<ige><szóköz><névelő><szóköz><főnév> <írásjel>}$$

jelölést használhatjuk. Ha elvégezzük valamilyen sorrendben a

$$\text{<főnév>} \longrightarrow \text{nap}, \quad \text{<ige>} \longrightarrow \text{Süt}, \quad \text{<névelő>} \longrightarrow \text{a},$$

$$\text{<szóköz>} \longrightarrow \text{␣}, \quad \text{<írásjel>} \longrightarrow .$$

átírásokat, akkor megkapjuk a "Süt a nap." mondatot.

A "Süt a nap." mondat egy levezetése a <mondat> nyelvtani kategóriából:

$$\text{<mondat>} \Longrightarrow \text{<ige><szóköz><névelő><szóköz><főnév><írásjel>} \Longrightarrow$$

$$\Longrightarrow \text{<ige><szóköz><névelő><szóköz>nap<írásjel>} \Longrightarrow$$

$$\Longrightarrow \text{<ige><szóköz><névelő> nap<írásjel>} \Longrightarrow$$

$$\Longrightarrow \text{Süt<szóköz><névelő> nap<írásjel>} \Longrightarrow$$
$$\Longrightarrow \text{Süt<szóköz>a nap<írásjel>} \Longrightarrow$$
$$\Longrightarrow \text{Süt<szóköz>a nap.} \Longrightarrow \text{Süt a nap.}$$

Ez a mondat a <mondat> nyelvtani kategóriából a következő szabályokkal is levezethető:

$$\text{<mondat>} \longrightarrow \text{<ige><szóköz>a<szóköz>nap.},$$

$$\text{<szóköz>} \longrightarrow \text{<szóköz>a<szóköz>}, \quad \text{<ige>} \longrightarrow \text{Süt}, \quad \text{<szóköz>} \longrightarrow \text{␣}$$

(Ezekkel a szabályokkal a <mondat> nyelvtani kategóriából levezethető például a "Süt a a nap." hibás mondat is.)

Az előbb vázolt motiváció késztette CHOMSKYt arra, hogy egy nyelvet véges ábécé feletti jelsorozatok halmazának, a nyelvtant pedig nyelvtani kategóriák (változók) és formális átírási szabályok véges halmazának tekintse, s ezzel megalkossa a formális nyelv és a generatív grammatika fogalmát.

Generatív grammatikán (*generatív nyelvtan*on) vagy röviden *grammatikán* (*nyelvtan*on) olyan $G = (V_N, V_T, S, H)$ rendszert értünk, ahol $V_N \neq \emptyset$ és $V_T \neq \emptyset$ diszjunkt véges ábécék, S tetszőleges V_N-beli betű, H pedig olyan (P, Q) rendezett párok véges halmaza, amelyekre $P, Q \in (V_N \cup V_T)^*$ és P tartalmaz V_N-beli betűt.

A V_N halmazt *nemterminális ábécé*nek, az elemeit *nemterminális betűk*nek, *nemterminális szimbólumok*nak, *nemterminálisok*nak vagy *változók*nak nevezzük. A V_T halmaz pedig a *terminális ábécé*, elemei pedig *terminális betűk*, *terminális szimbólumok* vagy *terminálisok*. Az $S \in V_N$ elem a *kezdőszimbólum* vagy *mondatszimbólum*. A H halmaz a *grammatika szabályainak halmaza*. Végül a H-beli (P, Q) párok az ún. *helyettesítési szabályok* vagy *átírási szabályok* vagy röviden *szabályok*. A (P, Q) A (P, Q) helyettesítési szabályra leginkább a $P \longrightarrow Q$ jelölést használjuk, ahol P-t a szabály *bal oldalá*nak, Q-t pedig a szabály *jobb oldalá*nak nevezzük. A $P \longrightarrow Q$ alakú szabályokat *P-re vonatkozó szabályok*nak is mondjuk. A V_T^* halmaz elemeit, amelyeket *terminális szavak*nak is nevezünk, általában kis latin betűkkel, $(V_N \cup V_T)^*$ elemeit pedig nagy latin betűkkel írjuk. (Bár a jegyzetben általában a halmazokat is nagy latin betűkkel jelöljük, ez nem vezet soha félreértéshez.)

Legyen $P, Q \in (V_N \cup V_T)^*$. Azt mondjuk, hogy Q *közvetlenül levezethető* a P szóból a G grammatikában, ha vannak olyan R, T, P', Q' szavak a $(V_N \cup V_T)^*$ halmazban, hogy $P = RP'T$ és $Q = RQ'T$, ahol $P' \longrightarrow Q'$ H-beli helyettesítési szabály. Erre a $P \Longrightarrow_G Q$ jelölést használjuk. A $\Longrightarrow_G$ egy binér reláció a $(V_N \cup V_T)^*$ halmazon. Ezt *közvetlen derivációnak* is szokás nevezni. Legyen $\Longrightarrow_G$ reflexív és tranzitív lezártja $\Longrightarrow_G^*$. Azt mondjuk, hogy a Q szó (*a* G

grammatikában) *levezethető* vagy *elérhető* a P szóból, ha $P \Longrightarrow_G^* Q$ teljesül, amit G-beli *derivációnak* is nevezünk. Ez azt jelenti, hogy léteznek olyan $P_0, P_1, \ldots, P_k \in (V_N \cup V_T)^*$ szavak, amelyekre

$$P = P_0, \quad P_{i-1} \Longrightarrow_G P_i \quad (i = 1, 2, \ldots, k), \quad P_k = Q. \tag{2.1}$$

Ekkor a

$$P \Longrightarrow_G P_1 \Longrightarrow_G \cdots \Longrightarrow_G P_{k-1} \Longrightarrow_G Q \tag{2.2}$$

sorozatot a Q *szó* P*-ból való* k *hosszúságú* G*-beli levezetésének* nevezzük. Erre használjuk a $P \Longrightarrow_G^k Q$ jelölést is. A Q szót az adott *levezetés eredményének* is nevezzük. Úgy is mondjuk, hogy Q *a* P*-ből* k *lépésben levezethető.* Ha $k = 0$, akkor $P = P_0 = Q$, és $\Longrightarrow_G^1 = \Longrightarrow_G$. Ha $k \geq 1$, akkor használjuk a $P \Longrightarrow_G^+ Q$ jelölést is. A $P_{i-1} \Longrightarrow_G P_i$ levezetést a $P \Longrightarrow_G^* Q$ levezetés i*-edik lépésének* is mondjuk. Speciálisan, ha $S \Longrightarrow_G^* Q$, akkor azt mondjuk, hogy Q *levezethető* G*-ben.* Amennyiben világos, hogy melyik grammatikáról van szó, $\Longrightarrow_G$ és $\Longrightarrow_G^*$ helyett egyszerűen $\Longrightarrow$-t ill. $\Longrightarrow^*$-ot írunk.

A $G = (V_N, V_T, S, H)$ *grammatika által generált nyelven* értjük a V_T felett

$$L(G) = \{p; \quad S \Longrightarrow_G^* p,\ p \in V_T^*\} \tag{2.3}$$

nyelvet. Ha $L = L(G)$, akkor azt is mondjuk, hogy a G grammatika *generálja* az L nyelvet.

Minden grammatika egyetlen nyelvet generál, egy nyelvet azonban több grammatika is generálhat. A G_1 és G_2 grammatikákat *ekvivalensek*nek nevezzük, ha ugyanazt a nyelvet generálják, azaz $L(G_1) = L(G_2)$. Azt is mondjuk, hogy az egyik grammatika a másik *ekvivalens átalakítása.*

Az $L(G)$ nyelv azokból a terminális szimbólumokat tartalmazó szavakból (mondatokból) áll, amelyek a G grammatikában (az S kezdőszimbólumból levezethetők). A természetes nyelvekre gondolva, a G grammatika azt mutatja meg, hogy az S mondatszimbólumból kiindulva, hogyan lehet a H-beli "nyelvtani szabályok" sorozatos alkalmazásával az $L(G)$ nyelv mondatait megszerkeszteni. Ez azt jelenti, hogy a G grammatika az $L(G)$ formális nyelv esetén ugyanazt a szerepet tölti be, mint a természetes nyelveknél a nyelvtanuk. Egy $L(G)$-beli szó (mondat) S-ből való levezetése $(V_N \cup V_T)^*$ szavain keresztül történik. Ha egy ilyen szó nemterminális szimbólumot is tartalmaz, akkor természetesen nem lehet eleme $L(G)$-nek. Az ilyen szavakat *mondatformák*nak is nevezzük. A V_T ábécé feletti szavakról azt is mondhatjuk, hogy olyan mondatformák, amelyek változókat nem tartalmaznak.

Ha bevezetjük az S = <mondat>, A = <ige>, B = <névelő>, C = <főnév>, D = <szóköz>, E = <írásjel>, x = a, y = nap, z = Süt jelöléseket, akkor a fejezet elején vett példákban $V_N = \{S, A, B, C, D, E\}$ ill. $V_N = \{S, A, D\}$, $V_T = \{x, y, z, ., \_\}$. A H-beli szabályok pedig a következők:

$$S \longrightarrow ADBDCE, \quad A \longrightarrow z, \quad B \longrightarrow x,$$

$$C \longrightarrow y, \quad D \longrightarrow \text{␣}, \quad E \longrightarrow .$$

ill.

$$S \longrightarrow ADxDy., \quad D \longrightarrow DxD, \quad A \longrightarrow z, \quad D \longrightarrow \text{␣}$$

A $G = (V_N, V_T, S, H)$ grammatika által generált nyelv:

$$L(G) = \{z\text{␣}x\text{␣}y.\} = \{\text{Süt a nap.}\}$$

ill.

$$L(G) = \{z\text{␣}x\text{␣}y., z\text{␣}x\text{␣}x\text{␣}y., z\text{␣}x\text{␣}x\text{␣}x\text{␣}y., ...\} =$$

$$= \{\text{Süt a nap., Süt a a nap., Süt a a a nap.,...}\}$$

Meg kell azonban jegyeznünk, hogy véges ábécé feletti nyelvek megadásának nem egyedüli eszköze a generatív grammatika. Vannak olyan véges ábécé feletti nyelvek amelyek generatív grammatikával meg sem adhatók.

A generatív grammatikák az ún. formális rendszerek speciális esetei. *Formális rendszer*nek nevezünk minden olyan $W = (V, H)$ párt, amelyben V tetszőleges ábécé, H pedig egy binér reláció a V^* szabad monoidon. A H elemeit tetszőleges formális rendszer esetén is (*helyettesítési*, *átírási*) *szabályok*nak hívjuk. Ha V és H véges halmazok, akkor W-t *véges formális rendszer*nek mondjuk. A (*közvetlen*) *levezetés*t is ugyanúgy definiáljuk, mint a generatív grammatikák esetében, s ugyanazokat a jelöléseket használjuk. Egy formális rendszert *asszociatív*nak hívunk, ha $P \longrightarrow Q \in H$ akkor és csak akkor, ha $Q \longrightarrow P \in H$. Ha tetszőleges $P', Q' \in U^*$ szavakra $P' \Longrightarrow_W^* Q'$ és $Q' \Longrightarrow_W^* P'$, akkor azt mondjuk, hogy P' és Q' egymással *ekvivalens*, szokásos jelöléssel $P' \Longleftrightarrow_W^* Q'$. Asszociatív formális rendszerekre az ún. *szóprobléma* a következő módon fogalmazható meg: Adott asszociatív formális rendszerhez létezik-e olyan algoritmus, amelynek segítségével U^* tetszőleges két szavára eldönthető, hogy egymással ekvivalensek.

Egy $W = (V, H)$ formális rendszert *generatív rendszer*nek nevezünk, ha ki van tüntetve az V^* szabad monoidnak egy $A \neq \emptyset$ részhalmaza, amelyet W *axiómarendszer*ének mondunk. Egy generatív rendszert tehát $W = (V, A, H)$ alakban adhatunk meg. A W *generatív rendszer által generált nyelv*nek nevezzük az

$$L(W) = \{P \in V^*; (\exists S \in A)(S \Longrightarrow_W^* P)\}$$

nyelvet. Nyilvánvaló, hogy a $W = (V, A, H)$ generatív rendszer tekinthető annak a (V, H') asszociatív formális rendszernek, amelyben $H' = L(W)^2$. A *szóprobléma* ebben az esetben azt jelenti, hogy létezik-e olyan algoritmus, amely bármely $p \in V^*$ szó esetén eldönti, hogy $p \in L(W)$ vagy $p \notin L(W)$.

Látható, hogy a generatív rendszer a generatív grammatika fogalmának általánosítása. Valóban egy $G = (V_N, V_T, S, H)$ grammatika olyan $W_G = (V, A, H)$ véges generatív rendszernek tekinthető, amelyre $V = V_N \cup V_T$, az A axiómarendszer az egyetlen S mondatszimbólumból áll, az $L(G)$ nyelvre pedig $L(G) = L(W_G) \cap V_T^*$ teljesül. Mi ebben a részben generatív grammatikákkal foglalkozunk, bár az automaták algebrai elméletében már találkoztunk más formális rendszerekkel is. Például egy $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automata (l. 6.1. alfejezet) olyan $W = (V, H)$ formális rendszerként is megadható, amelyben $V = A \cup X \cup Y$, és H azokból az $ax \longrightarrow yb$ alakú szabályokból áll, amelyekre

$$ax \longrightarrow yb \quad \Longleftrightarrow \quad (\delta(a,x) = b,\ \lambda(a,x) = y)\ (a, b \in A,\ x \in X,\ y \in Y).$$

Egy iniciális $\mathbf{A} = (A, A_0, X, \delta)$ automata tekinthető olyan $W = (V, A_0, H)$ generatív rendszernek, amelyben $V = A \cup X$, az iniciális állapotok A_0 halmaza az axiómarendszer, továbbá bármely $a, b \in A$ állapotra és $x \in X$ bemenő jelre $a \longrightarrow xb \in H$ akkor és csak akkor, ha $\delta(a, x) = b$. (`http://tankonyvtar.ttk.bme.hu/pdf/18.pdf`)

2.1. Chomsky nyelvosztályok

A generatív grammatika definíciója azt mutatja, hogy egy generatív grammatikát a helyettesítési szabályaival jellemezhetjük. Chomsky a generatív grammatikák négy típusát különböztette meg a helyettesítési szabályaikra előírt feltételek segítségével.

Legyen $i \in \{0, 1, 2, 3\}$. Azt mondjuk, hogy a $G = (V_N, V_T, S, H)$ grammatika i *típusú*, ha az alábbi feltételek közül az (i)-ediket teljesíti:
(0) A H-beli helyettesítési szabályok tetszőlegesek, azaz $P_1XP_2 \to Q$ alakúak, ahol $P_1, P_2, Q \in (V_N \cup V_T)^*$ és $X \in V_N$.
(1) A H-beli helyettesítési szabályok $P_1XP_2 \longrightarrow P_1PP_2$ alakúak, ahol $X \in V_N$, $P_1, P_2, P \in (V_N \cup V_T)^*$ és $P \neq e$, kivéve esetleg az $S \longrightarrow e$ szabályt, amely azonban csak úgy szerepelhet H-ban, ha S nem fordul elő egyetlen szabály jobb oldalán sem.
(2) A H-beli helyettesítési szabályok $X \longrightarrow P$ alakúak, ahol $X \in V_N$ és $P \in (V_N \cup V_T)^*$.
(3) A H-beli helyettesítési szabályok $X \longrightarrow pY$ vagy $X \longrightarrow p$ alakúak, ahol $X, Y \in V_N$ és $p \in V_T^*$.

Egy L nyelvet i *típusú*nak nevezünk, ha van olyan i típusú G grammatika, hogy $L = L(G)$. Az i típusú nyelvek halmazát $\mathcal{L}_i$-vel jelöljük. Az $\mathcal{L}_i$ $(i = 0, 1, 2, 3)$ halmazokat *Chomsky nyelvosztályok*nak nevezzük. A Chomsky nyelvosztályok alapvető fontosságúak a formális nyelvek elméletében. Érvényesek az

$$\mathcal{L}_3 \subseteq \mathcal{L}_2 \subseteq \mathcal{L}_1 \subseteq \mathcal{L}_0$$

tartalmazások, amelyek közül az első és a harmadik nyilvánvalóan következik a definíciókból, a másodikat azonban bizonyítani kell (3.6 Tétel). Sőt megmutatható, hogy

$$\mathcal{L}_3 \subset \mathcal{L}_2 \subset \mathcal{L}_1 \subset \mathcal{L}_0. \tag{2.4}$$

A valódi tartalmazásoknak ezt a sorozatát *Chomsky hierarchiá*nak hívjuk. A Chomsky hierarchia egyik valódi tartalmazása sem nyilvánvaló, sőt a harmadik igazolása igen nehéz. Az i típusú grammatikákra ilyen hierarchia nem érvényes. Minden 3 típusú nyelvtan 2 típusú és minden 1 nyelvtan 0 típusú. Nem igaz azonban, hogy minden 2 típusú nyelvtan 1 típusú, mert még az sem igaz, hogy minden 3 típusú nyelvtan egyben 1 típusú is. Valóban a 2 és 3 típusú nyelvtanoknál az $X \longrightarrow e$ $(X \in V_N)$ szabályok megengedettek, míg az 1 típusú nyelvtanoknál legfeljebb az $S \longrightarrow e$ szabály.

Megjegyezzük, hogy ha a grammatika definíciójában végtelen sok szabályt is megengednénk, akkor a Chomsky hierarchia nem teljesülne. Ebben az esetben minden U ábécé feletti L nyelv 3 típusú lenne, mert generálná az a 3 típusú $G = \{S, U, S, H\}$ grammatika, amelyben $H = \{S \longrightarrow p; p \in L\}$. A H végességéből pedig következik, hogy elegendő véges sok változóra és terminálisra szorítkozni. Az $L(G)$ nyelv szavai ugyanis csak azokból terminálisokból képezhetők, amelyek szerepelnek a szabályokban. Továbbá ezeknek a szavaknak a levezetéséhez csak a szabályokban szereplő véges sok változót használhatjuk.

A 0 típusú nyelvek az összes, generatív grammatikával megadható nyelvek. Ezeket *kifejezés struktúrájú*, ill. *mondatszerkezetű nyelvek*nek is nevezzük.

Az 1 típusú grammatikák esetén egy X nemterminális szimbólum adott $P_1, P_2 \in (V_N \cup V_T)^*$ szavak esetén helyettesíthető egy P_1XP_2 alakú mondatformában egy $P \in (V_N \cup V_T)^+$ szóval. Ezt úgy is mondhatjuk, hogy a $P_1 = P_2 = e$ eset kivételével X helyettesítése P-vel függ X környezetétől. Ezért ezeket a grammatikákat és az általuk generált nyelveket *környezetfüggő grammatikák*nak és *környezetfüggő nyelvek*nek hívjuk. A környezetfüggő grammatikákban az $S \longrightarrow e$ szabály kivételével minden szabály jobb oldalának hossza nagyobb vagy egyenlő mint a bal oldal hossza. Emlékeztetünk arra, hogy szavak hosszán a benne előforduló betűk számát értjük.(l. [2] jegyzetünk függelékét!) A G környezetfüggő grammatika akkor és csak akkor tartalmazza az $S \to e$ szabályt, ha $e \in L(G)$. Ebben az esetben egyetlen szabály jobb oldalán sem szerepel az S mondatszimbólum, s így e az S-ből csak egy lépésben

(közvetlenül) vezethető le.

A 2 típusú grammatikákat és nyelveket az előbbi elnevezéssel összhangban *környezetfüggetlen grammatikák*nak ill. *környezetfüggetlen nyelvek*nek is mondjuk.

Ha egy terminális nem szerepel egy $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika egyetlen szabályának jobb oldalán sem, akkor nem szerepel az adott grammatikával generált nyelv egyetlen szavában sem. Ezért az egyszerűség kedvéért a környezetfüggetlen grammatikák V_T terminális ábécéit legtöbbször úgy adjuk meg, hogy ilyen felesleges terminálisokat ne tartalmazzanak. Mivel csak az $L(G) = \emptyset$ ill. az $L(G) = e$ esetekben felesleges minden terminális, ezért környezetfüggetlen grammatikákra csak ekkor lehetséges a $V_T = \emptyset$ választás.

A 3 típusú grammatikákat ill. nyelveket *jobb lineáris*aknak is nevezzük, mivel minden szabály jobb oldalán legfeljebb egy nemterminális állhat, s az is csak a jobb oldal végén. A 8.2. alfejezetben megmutatjuk, hogy a 3 típusú nyelvek pontosan a a véges ábécék feletti reguláris nyelvek. Ezért a 3 típusú grammatikákat *reguláris grammatikák*nak is mondjuk.

Értelemszerűen tetszőleges grammatika egy-egy szabályáról is mondhatjuk, hogy *jobb lineáris (reguláris)*, *környezetfüggetlen* vagy *környezetfüggő szabály.*

A jobb lineáris (3 típusú) grammatika definíciójának általánosításaként bevezethető a lineáris grammatika fogalma:

A $G = (V_N, V_T, S, H)$ grammatikát *lineáris*nak nevezzük, ha a H-beli helyettesítési szabályok $X \longrightarrow pYq$ vagy $X \longrightarrow r$ alakúak, ahol $X, Y \in V_N$ és $p, q, r \in V_T^*$.

A definícióból következik, hogy minden lineáris grammatika 2 típusú. A G lineáris grammatika jobb lineáris, ha a H-beli helyettesítési szabályokban $q = e$. A G lineáris grammatikát *bal lineáris*nak mondjuk, ha a H-beli helyettesítési szabályokban $p = e$ teljesül. A lineáris grammatikák által generált nyelveket *lineáris nyelvek*nek nevezzük. A 8.9 Tétel bizonyításában megmutatjuk, hogy nem minden lineáris nyelv 3 típusú. A lineáris nyelvekkel részletesebben megismerkedhetünk a [10] elektronikus jegyzetben.

2.1. Tétel. *Minden bal [jobb] lineáris grammatikához van vele ekvivalens jobb [bal] lineáris grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ tetszőleges bal lineáris grammatika. Az általánosság megszorítás nélkül feltehetjük, hogy S nem szerepel egyetlen H-beli szabály jobb oldalán sem. (Ellenkező esetben ugyanis egy új S_0 mondatszimbólum bevezetésével és H-nak az $S_0 \longrightarrow S$ szabállyal való kibővítésével ez mindig elérhető. Nyilvánvaló, hogy a kapott grammatika ugyanazt a nyelvet generálja, mint az eredeti.)

Szerkesszük meg a $G' = (V_N, V_T, S, H')$ grammatikát a következő módon: Legyenek $X, Y \in V_N - S$ és $p \in X_T^*$. Minden H-beli $S \longrightarrow p$ szabály legyen H'-ben is. A H-beli $X \longrightarrow p$, $X \longrightarrow Yp$ és $S \longrightarrow Xp$ szabályok helyett vegyük fel H'-be rendre az $S \longrightarrow pX$, $Y \longrightarrow pX$ és $X \longrightarrow p$ szabályokat. A G' grammatika nyilvánvalóan jobb lineáris.

Ilyen módon minden $G = (V_N, V_T, S, H)$ bal lineáris grammatikához kölcsönösen egyértelmű módon hozzárendeltük a $G' = (V_N, V_T, S, H')$ jobb lineáris grammatikát. Megmutatjuk, hogy G és G' ekvivalens, azaz $L(G) = L(G')$.

Ha $S \longrightarrow p$ ($p \in V_T^*$), akkor $p \in L(G) \cap L(G')$. A H' halmaz definíciója szerint, hogy bármely pozitív egész k esetén akkor és csak akkor létezik G-ben az

$$S \Longrightarrow_G X_1 p_1 \Longrightarrow_G X_2 p_2 p_1 \Longrightarrow_G \cdots \Longrightarrow_G$$

$$\Longrightarrow_G X_k p_k \dots p_2 p_1 \Longrightarrow p_{k+1} p_k \dots p_2 p_1 = p$$

alakú levezetés, ahol $X_1, X_2, \dots X_k \in V_N$ és $p_1, p_2, \dots, p_{k+1} \in V_T^*$, ha G'-ben létezik az

$$S \Longrightarrow_{G'} p_{k+1} X_k \Longrightarrow_{G'} p_{k+1} p_k X_{k-1} \Longrightarrow_{G'} \cdots \Longrightarrow_{G'}$$

$$\Longrightarrow_{G'} p_{k+1} p_k \dots p_2 X_1 \Longrightarrow_{G'} p_{k+1} p_k \dots p_2 p_1 = p$$

alakú levezetés. Ez azt jelenti, hogy ebben az esetben is $p \in L(G) \cap L(G')$, s így $L(G) = L(G')$. □

2.2. Standard grammatikák

A $G = (V_N, V_T, S, H)$ grammatikát *standard grammatika*nak nevezzük, ha minden olyan H-beli átírási szabály, amelyben legalább egy terminális betű is fellép, $X \longrightarrow x$ alakú, ahol $X \in V_N$ és $x \in V_T$.

2.2. Lemma. *Minden grammatika ekvivalens egy standard grammatikával.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ tetszőleges grammatika, továbbá V olyan halmaz, amelyre $V \cap (V_N \cup V_T) = \emptyset$ és $|V| = |V_T|$ teljesül. Jelölje φ a V_T halmaz egy bijektív leképezését a V halmazra. A $V_N' = V \cup V_N$ halmaz és φ leképezés segítségével megkonstruálunk egy G-vel ekvivalens G' standard grammatikát. Legyen G' nemterminális ábécéje V_N', terminális ábécéje V_T, mondatszimbóluma pedig S. A G' grammatika H' helyettesítési szabályainak halmazát a következőképpen adjuk meg: Minden terminálist nem tartalmazó H-beli szabály legyen benne H'-ben is. Ha egy H-beli $P \longrightarrow Q$ szabály legalább egy terminálist tartalmaz, akkor minden P-ben ill. Q-ban előforduló x terminálist cseréljük ki a $\varphi(x)$ szimbólummal, s az így kapott $P' \longrightarrow Q'$ szabályt vegyük fel H'-be. Végül vegyük fel H'-be az összes $\varphi(x) \longrightarrow x$ ($x \in V_T$)

szabályt is. A konstrukcióból világos, hogy $G' = (V'_N, V_T, S, H')$ standard grammatika.

Megmutatjuk, hogy G' ekvivalens G-vel, azaz $L(G') = L(G)$ fennáll. Legyen $p = x_1x_2 \dots x_k$ tetszőleges $L(G)$-beli nemüres szó, azaz $S \Longrightarrow^*_G p$ és $p \neq e$. Akkor

$$S \Longrightarrow^*_{G'} \varphi(x_1)\varphi(x_2) \dots \varphi(x_k),$$

ahonnan a H'-beli $\varphi(x_i) \longrightarrow x_i$ $(i = 1, 2, \dots k)$ szabályok alkalmazásával kapjuk, hogy $S \Longrightarrow^*_{G'} p$, vagyis $p \in L(G')$. Ha $e \in L(G)$, akkor $S \Longrightarrow^*_G e$. Ha $S \Longrightarrow^*_G e$ levezetésben minden olyan P_i mondatforma helyett, amely legalább egy terminálist tartalmaz, azt a P'_i mondatformát vesszük, amely P_i-ből a benne szereplő x terminálisoknak $\varphi(x)$ szimbólumokkal való kicserélésével jön létre, akkor $S \Longrightarrow^*_{G'} e$. Tehát $e \in L(G')$. Ezzel megmutattuk, hogy $L(G) \subseteq L(G')$.

Megfordítva, megmutatjuk, hogy az $L(G') \subseteq L(G)$ tartalmazás is fennáll, ami azt jelenti, hogy $L(G') = L(G)$. Definiáljuk a $V \cup V_N \cup V_T$ halmaznak a $V_N \cup V_T$ halmazra való η leképezését úgy, hogy minden $x \in V_T$ terminálisra $\eta(\varphi(x)) = \eta(x) = x$, s minden $X \in V_N$ változóra $\eta(X) = X$ teljesüljön. Jelölje η_h az η leképezés homomorf kiterjesztését az $(V \cup V_N \cup V_T)^*$ szabad monoidra. Legyenek $P, Q \in (V \cup V_N \cup V_T)^*$, amelyekre $P \Longrightarrow^*_{G'} Q$ fennáll. Ha Q-nak P-ből való levezetése során csak $\varphi(x) \longrightarrow x$ alakú H'-beli szabályokat kell alkalmaznunk, akkor $\eta_h(P) = \eta_h(Q)$. Ellenkező esetben pedig nyilván $\eta_h(P) \Longrightarrow^*_G \eta_h(Q)$. Ezért a $P \Longrightarrow^*_{G'} Q$ relációból mindenképpen a $\eta_h(P) \Longrightarrow^*_G \eta_h(Q)$ reláció következik. Ha tehát $p \in L(G')$, azaz $S \Longrightarrow^*_{G'} p$, akkor

$$S = \eta_h(S) \Longrightarrow^*_G \eta_h(p) = p,$$

vagyis $p \in L(G)$. Ezzel megmutattuk, hogy az $L(G') \subseteq L(G)$ tartalmazás is igaz. □

A definíciók alapján nyilvánvaló, hogy bármely $i = 0, 1, 2$ esetén a 2.2 Lemma bizonyításában szereplő G' grammatika akkor és csak akkor i típusú,ha G is i típusú. A 3 típusú grammatikákra azonban ez nem igaz. Ha ugyanis G 3 típusú grammatika tartalmaz legalább egy $X \longrightarrow pY$ $(p \neq e)$ vagy $X \longrightarrow p$ $(|p| > 1)$ helyettesítési szabályt, akkor a G' grammatika 2 típusú lesz. Ezek alapján kimondhatjuk a következő eredményt.

2.3. Lemma. *Ha $i = 0, 1, 2$, akkor minden i típusú grammatikához létezik egy vele ekvivalens standard i típusú grammatika.*

A 2 és 3 típusú grammatikákra azok definíciójából, ill. a 0 és 1 típusú grammatikákra az előző lemmából adódik a következő állítás.

2.4. Következmény. *Minden grammatikához megadható egy ugyanolyan típusú és vele ekvivalens grammatika úgy, hogy a helyettesítési szabályainak bal oldalán terminális nem fordul elő.*

2.5. Példa. *Legyenek a* $G = (\{S, X\}, \{a, b\}, S, H)$ *környezetfüggő grammatika szabályai a következők:*

$$S \longrightarrow a,\ S \longrightarrow XS,\ S \longrightarrow aaXb,\ X \longrightarrow b,\ aXb \longrightarrow aXbb.$$

Megadunk vele ekvivalens standard környezetfüggő grammatikát.

A 2.1. Lemma bizonyításában leírt módon járunk el. Az a

$$G' = (\{S, X, A, B\}, \{a, b\}, S, H')$$

standard környezetfüggő grammatika ekvivalens G-vel, amelynek szabályai:

$$S \longrightarrow A,\ S \longrightarrow XS,\ S \longrightarrow AAXB,$$

$$X \longrightarrow B,\ AXB \longrightarrow AXBB,\ A \longrightarrow a,\ B \longrightarrow b.$$

($L(G) = L(G') = \{b^k a,\ b^k a^2 b^l,\ k = 0, 1, 2, \ldots,\ l = 2, 3, 4, \ldots\}$*.)*

2.6. Példa. *Tekintsük a*

$$S \longrightarrow abX,\ X \longrightarrow aY,\ X \longrightarrow bb,\ Y \longrightarrow b$$

szabályokkal megadott $G = (\{S, X, Y\}, \{a, b\}, S, H)$ *jobb lineáris grammatikát.*

A $G' = (\{S, X, Y, A, B\}, \{a, b\}, S, H')$ *környezetfüggetlen grammatika ekvivalens G-vel, ha a* H'*-beli szabályok a következők:*

$$S \longrightarrow ABX,\ X \longrightarrow AY,\ X \longrightarrow BB,\ Y \longrightarrow B, A \longrightarrow a,\ B \longrightarrow b.$$

($L(G) = L(G') = \{abbb, abab\}$*.)*

A két példában szereplő $S \longrightarrow A$, $X \longrightarrow B$ ill. $Y \longrightarrow B$ szabály helyettesíthető az $S \longrightarrow a$, az $X \longrightarrow b$ ill. az $Y \longrightarrow b$ szabállyal. Az ilyen típusú ún. láncszabályokról a későbbiekben lesz még szó.

2.3. Zártsági tulajdonságok

Legyen U tetszőleges véges ábécé. Az előző fejezetben definiáltuk az $\mathcal{L}(U)$ nyelvalgebrát, amelynek $\mathcal{R}(U)$ reguláris nyelvalgebra az U halmaz elemei által generált részalgebrája. Most megmutatjuk, hogy a környezetfüggetlen nyelvek $\mathcal{L}_2$, a környezetfüggő nyelvek $\mathcal{L}_1$, és a mondatszerkezetű nyelvek $\mathcal{L}_0$ halmaza

zárt a reguláris műveletekre. Ebből következik, hogy egy adott U ábécé feletti környezetfüggetlen nyelvek $CF(U)$, környezetfüggő nyelvek $CS(U)$ és a mondatszerkezetű nyelvek $PS(U)$ halmaza is zárt a reguláris műveletekre, azaz a $\mathcal{CF}(U)$, $\mathcal{CS}(U)$és $\mathcal{PS}(U)$ az $\mathcal{L}(U)$ nyelvalgebra részalgebrái. Nyilvánvaló, hogy

$$R(U) \subset CF(U) \subset CS(U) \subset PS(U). \tag{2.5}$$

2.7. Tétel. *A Chomsky nyelvosztályok zártak a reguláris műveletekre.*

Bizonyítás A 3 típusú, azaz reguláris nyelvekre nyelvekre, amint azt már megjegyeztük, a definícióból közvetlenül következik az állítás. A többi nyelvosztályra a bizonyítást műveletenként végezzük el.

Tetszőleges $i = 0, 1, 2$ esetén legyenek L_1 és L_2 a $G_1 = (V_{1,N}, V_{1,T}, S_1, H_1)$ és $G = (V_{2,N}, V_{2,T}, S_2, H_2)$ i tipusú grammatikák által generált nyelvek, azaz $L_1 = L(G_1)$ és $L_2 = L(G_2)$. A 2.3 Lemma szerint feltehető, hogy G_1 és G_2 standard grammatika. Tegyük fel azt is, hogy $V_{1,N} \cap V_{2,_N} = \emptyset$. (Ezt a változók átjelölésével mindig elérhetjük.) Először megmutatjuk, hogy a nyelvosztályok zártak az összeadásra. Legyen $S \notin V_{1,N} \cup V_{2,N}$ tetszőleges szimbólum. Ha

$$V_N = V_{1,N} \cup V_{2,N} \cup S, \quad V_T = V_{1,T} \cup V_{2,T},$$

$$H = H_1 \cup H_2 \cup \{S \longrightarrow S_1, S \longrightarrow S_2\},$$

akkor $i = 0, 2$ esetekben a $G = (V_N, V_T, S, H)$ i típusú grammatika generálja az $L_1 + L_2$ nyelvet.

Ha $i = 1$ és $e \notin L_1 + L_2$, akkor G szintén generálja az $L_1 + L_2$ nyelvet. Ha $i = 1$ és $e \in L_1 + L_2$, akkor vagy H_1 tartalmazza a $S_1 \longrightarrow e$ szabályt, vagy H_2 az $S_2 \longrightarrow e$ szabályt. Elhagyva ezeket a szabályokat, szintén 1 típusú grammatikákat kapunk. Ezekkel a G_1'-vel és G_2'-vel jelölt grammatikákkal konstruáljuk meg a fenti módon G-t. Mivel $L(G_1') = L_1 - e$ és $L(G_2') = L_2 - e$, ezért $L(G) = (L_1 + L_2) - e$. Ezután a G grammatikához új mondatszimbólumként vegyük fel az $S_0 \notin V_N$ jelet, valamint az $S_0 \longrightarrow S$ és $S_0 \longrightarrow e$ szabályokat. Nem nehéz belátni, hogy az így kapott 1 típusú grammatika éppen az $L_1 + L_2$ nyelvet generálja.

Most megmutatjuk, hogy a nyelvosztályok zártak a konkatenációra. Ha V_N, V_T halmazokat ugyanúgy definiáljuk, mint az előbb és

$$H = H_1 \cup H_2 \cup \{S \longrightarrow S_1 S_2\},$$

akkor $i = 0, 2$ esetekben ill. $i = 1$ esetben, ha $e \notin L_1 + L_2$, a G i típusú grammatika generálja az $L_1 L_2$ nyelvet.

Legyen $i = 1$ és $e \in L_1 + L_2$. Ha a fentebb definiált G_1' és G_2' grammatikákkal megkonstruáljuk az előbbi módon G-t, akkor $L(G) = (L_1 - e)(L_2 - e)$ 1 típusú

nyelv. Ha $e \notin L_1$ és $e \in L_2$, akkor $L_1L_2 = L(G) + L_1$. Ha $e \in L_1$ és $e \notin L_2$, akkor $L_1L_2 = L(G)+L_2$. Ha pedig $e \in L_1 \cap L_2$, akkor $L_1L_2 = L(G)+L_1+L_2+e$. Mivel a nyelvosztályok zártak az összeadásra, ezért mindhárom esetben azt kapjuk, hogy az L_1L_2 nyelv 1 típusú.

Végül megmutatjuk, hogy a nyelvosztályok zártak az iterációra. Ha $i = 2$ és

$$S \notin V_{1,N}, \quad V_N = V_{1,N} \cup S, \quad V_T = V_{1,T}, \quad H = H_1 \cup \{S \longrightarrow e, S \longrightarrow SS_1\},$$

akkor a $G = (V_N, V_T, S, H)$ 2 típusú grammatika nyilván az L_1^* nyelvet generálja. Legyen $i = 0, 1$ és $e \notin L_1$. Megmutatjuk, hogy ha

$$S, S' \notin V_{1,N}, \quad V_N = V_{1,N} \cup \{S, S'\}, \quad V_T = V_{1,T},$$

$$H = H_1 \cup \{S \longrightarrow e,\ S \longrightarrow S_1,\ S \longrightarrow S'S_1,$$

$$S'x \longrightarrow S'S_1x,\ S'x \longrightarrow S_1x; x \in V_T\},$$

akkor a $G = (V_N, V_T, S, H)$ i típusú grammatika az L_1^* nyelvet generálja. Először azt mutatjuk meg, hogy L_1^* minden eleme levezethető G-ben. Az e üres szó nyilván az $S \longrightarrow e$ szabállyal közvetlenül levezethető. Tekintsünk ezután egy $p \neq e$ szót L_1^*-ból, azaz legyen $p = p_1p_2 \dots p_k$, ahol $p_j \in L_1$ $(j = 1, 2, \dots, k)$. Mivel $e \notin L_1$, feltehetjük, hogy $p_j = x_jq_j$ $(x_j \in V_T, q_j \in V_T^*)$. Az

$$S \Longrightarrow_G S'S_1 \Longrightarrow_G^* S'p_k = S'x_kq_k \Longrightarrow_G S'S_1x_kq_k = S'S_1p_k$$

$$\Longrightarrow_G^* S'p_{k-1}p_k \Longrightarrow_G^* \dots \Longrightarrow_G^* S'p_2 \dots p_{k-1}p_k = S'x_2q_2 \dots p_{k-1}p_k$$

$$\Longrightarrow_G S_1x_2q_2 \dots p_{k-1}p_k = S_1p_2 \dots p_{k-1}p_k \Longrightarrow_G^* p_1p_2 \dots p_{k-1}p_k = p$$

levezetéssel kaptuk, hogy $S \Longrightarrow_G^* p$. Ezzel megmutattuk, hogy $L_1^* \subseteq L(G)$. A forditott irányú tartalmazás megmutatása céljából tekintsünk egy

$$S \Longrightarrow_G P_1 \Longrightarrow_G \dots \Longrightarrow_G P_n \Longrightarrow_G p \in V_T^*$$

levezetést. Ha ebben a levezetésben $P_1 = e$, akkor $P_1 = p = e \in L_1^*$. Ha pedig $P_1 = S_1$, akkor ez a levezetés olyan szóhoz vezet, amely szintén benne van L_1^*-ban. Egyébként P_1 csak $S'S_1$ alakú lehet, és ekkor teljes indukcióval megmutatható, hogy minden P_j $(j = 1, 2, \dots, n)$ vagy
(1) $S'Q_1 \dots Q_l$ alakú, ahol $l \geq 1$ és a $Q_2, \dots Q_l$ szavak első betűje terminális, továbbá $S_1 \Longrightarrow_{G_1}^* Q_m$ $(m = 1, \dots, l)$; vagy
(2) $Q_0Q_1 \dots Q_l$ alakú, ahol $l \geq 1$ és $Q_1, \dots Q_l$ szavak első betűje terminális, és $S_1 \Longrightarrow_{G_1}^* Q_m$ $(m = 0, 1, \dots, l)$.

Nyilván $P_1 = S'S_1$ alakja (1)-nek megfelelő. Ha P_j megfelel vagy az (1) vagy a (2) kikötésnek, akkor G minden szabályát megvizsgálva és természetesen figyelembe véve, hogy a G_1 standard grammatika, megállapítható, hogy P_{j+1} is eleget tesz az (1) vagy (2) feltételnek. Ebből viszont következik, hogy G-ben csak L_1^*-beli szavak vezethetők le, vagyis $L(G) \subseteq L_1^*$.

Abban az esetben, ha $i = 0, 1$ és $e \in L_1$, először olyan i típusú G_1' grammatikát konstruálunk, amelyre $L(G_1') = L_1 - e$. Ezt az $i = 1$ esetben egyszerűen úgy kapjuk, hogy az $S_1 \longrightarrow e$ szabályt elhagyjuk. Az $i = 0$ esetben pedig a $P \longrightarrow e$ alakú szabályokat helyettesítjük az összes $XP \longrightarrow X$ és $PX \longrightarrow X$ ($X \in V_{1,N} \cup V_{1,T}$) alakú szabállyal. Nyilvánvaló, hogy $L_1^* = (L_1 - e)^*$. Ez azt jelenti, hogy elegendő olyan nyelveket tekinteni, amelyek nem tartalmazzák az üres szót. Így visszavezettük a problémát az előző esetre. □

Már láttuk, hogy a reguláris nyelvek osztálya zárt a tükrözés műveletére. Ezt az állítást most minden nyelvosztályra igazoljuk.

2.8. Tétel. *A Chomsky nyelvosztályok zártak a tükrözésre.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ i típusú grammatika ($i = 0, 1, 2, 3$). Definiáljuk a $G' = (V_N, V_T, S, H')$ grammatikát úgy, hogy $P^{-1} \longrightarrow Q^{-1}$ akkor és csak akkor legyen H'-beli szabály, ha $P \longrightarrow Q$ H-beli szabály. A definíciókat és $i = 3$ esetben a 2.1 Tételt is használva kapjuk, hogy G' is i típusú grammatika. Látható, hogy a

$$P_1PP_2 \implies_G P_1QP_2$$

közvetlen levezetés pontosan akkor létezik, ha a

$$(P_1PP_2)^{-1} = P_2^{-1}P^{-1}P_1^{-1} \implies_{G'} P_2^{-1}Q^{-1}P_1^{-1} = (P_1QP_2)^{-1}$$

közvetlen levezetés is létezik. Ennek alapján nem nehéz belátni, hogy $L = L(G)$ akkor és csak akkor, ha $L^{-1} = L(G')$. □

2.4. Láncszabálymentes grammatikák

Tetszőleges $G = (V_N, V_T, S, H)$ grammatika esetén az $A \longrightarrow B$ ($A, B \in V_N$) alakú szabályt *láncszabály*nak vagy *átnevezés*nek nevezzük. Ha H-ban nincsenek láncszabályok, akkor azt mondjuk, hogy G *láncszabálymentes*. .

2.9. Lemma. *Minden $G = (V_N, V_T, S, H)$ környezetfüggetlen [jobb lineáris, bal lineáris, lineáris] grammatikához megadható olyan $G' = (V_N, V_T, S, H')$ láncszabálymentes környezetfüggetlen [jobb lineáris, bal lineáris, lineáris] grammatika, amelyre $L(G') = L(G)$.*

Bizonyítás Megkonstruáljuk a H' halmazt. Legyen minden $X \in V_N$ változóra N_X azon $Y \in V_N$ változók halmaza, amelyekre az $X \Longrightarrow_G^* Y$ levezetés közben csak láncszabályokat alkalmazunk. (Mivel $X \Longrightarrow_G^* X$, ezért $X \in N_X$.) Ezután minden $X \in V_N$, $Y \in N_X$ és H-beli $Y \longrightarrow P$ ($P \notin N_X$) szabály esetén tekintsük az $X \longrightarrow P$ szabályt, s legyen H' ezeknek a szabályoknak a halmaza. H'-ben nincsenek láncszabályok és tartalmaz minden olyan H-beli szabályt, amelyik nem láncszabály. Ha G jobb lineáris [bal lineáris, lineáris], akkor G' is az.

Legyen $p \in L(G)$, azaz $p \in V_T^*$ és $S \longrightarrow_G^* p$. Ha a levezetés közben nem alkalmazunk láncszabályt, akkor $p \in L(G')$. Ha a levezetés közben alkalmazunk láncszabályt, akkor, a levezetés definíciója miatt, egymás után csak véges számú lépésben tehetjük meg. Ilyenkor, ha az X változóból indulunk ki, s elérjük az Y változót, akkor utána egy $Y \longrightarrow Q$ nem láncszabályt kell alkalmazni, mert különben nem érhetnénk el egy terminális szót. Ekkor viszont teljesül, hogy $Y \in N_X$, ezért $X \longrightarrow Q$ H'-beli szabály. Minden X-ből induló és Q-ban végződő H-beli levezetés helyettesíthető azzal a H'-beli levezetéssel, amelyben csak az $X \longrightarrow Q$ szabályt alkalmazzuk. Megfordítva, minden G'-beli levezetésben alkalmazott szabály H-ban van, vagy helyettesíthető H-beli láncszabályok sorozatának és egy nem láncszabálynak az alkalmazásával. Ez azt jelenti, hogy $L(G') = L(G)$. □

A bizonyításban szereplő N_X ($X \in V_N$) halmaz egyszerűen megkonstruálható a következő iterációval:

$$N_0 = \{X\}, \quad N_{k+1} = N_k \cup \{C \in V_N; \exists (B \in N_k)(B \longrightarrow C \in H)\}.$$

Ha a k-adik lépésben $N_{k+1} = N_k$, akkor $N_X = N_k$.

2.10. Tétel. *Bármely $G = (V_N, V_T, S, H)$ láncszabálymentes 3 típusú grammatikához van olyan $G' = (V_N', V_T, S, H')$ 3 típusú grammatika, hogy $L(G') = L(G)$ és minden H'-beli szabály $X \longrightarrow xY$ vagy $X \longrightarrow e$ alakú, ahol $X, Y \in V_N$ és $x \in V_T$.*

Bizonyítás Az $X \longrightarrow xY$ vagy $X \longrightarrow e$ ($X, Y \in V_N, x \in V_T$) alakú H-beli szabályok halmazát jelölje H_1. (H_1 lehet az üres halmaz is.) Jelölje V_T' azon terminális betűk halmazát, amelyek előfordulnak a $H - H_1$ halmazban lévő szabályok jobb oldalán. Ha $H - H_1 = \emptyset$, akkor G maga is egy kívánt tulajdonságú grammatika. Legyen $H - H_1 \neq \emptyset$ és φ a V_T' halmaznak bijektív leképezése egy olyan V halmazra, amelyre $V \cap (V_N \cup V_T) = \emptyset$. Az egyszerűség kedvéért, ha $z \in V_T'$, akkor legyen $\varphi(z) = Z$. Minden H-beli

$$X \longrightarrow x_1 x_2 \ldots x_k Y \quad (X, Y \in V_N, x_1, x_2, \ldots, x_k \in V_T', k > 1)$$

szabály esetén alkossuk meg az

$$X \longrightarrow x_1X_1, X_1 \longrightarrow x_2X_2, \ldots, X_{k-1} \longrightarrow x_kY \tag{2.6}$$

szabályokat. Minden H-beli

$$X \longrightarrow x_1x_2 \ldots x_k, \quad (x_1, x_2, \ldots, x_k \in V_T', \ k \geq 1)$$

szabály esetén pedig az

$$X \longrightarrow x_1X_1, X_1 \longrightarrow x_2X_2, \ldots, X_{k-1} \longrightarrow x_kX_k, X_k \longrightarrow e \tag{2.7}$$

szabályokat. Jelöljük a (2.6) és a (2.7) alakú szabályok halmazát H_2-vel. Legyen $V_N' = V_N \cup V$ és $H' = H_1 \cup H_2$. A $G' = (V_N', V_T, S, H')$ kívánt tulajdonságú grammatika. Nem nehéz belátni, hogy $L(G') = L(G)$. □

A 2.1 Tétel bizonyítása szerint az is igaz, hogy láncszabálymentes jobb lineáris $G = (V_N, V_T, S, H)$ grammatikához van olyan $G' = (V_N', V_T, S, H')$ bal lineáris grammatika, hogy $L(G') = L(G)$ és minden H'-beli szabály $X \longrightarrow Yx$ vagy $X \longrightarrow e$ alakú, ahol $X, Y \in V_N$ és $x \in V_T$.

Feladatok

2.1. Minden véges nyelv 3 típusú.
2.2. Bármely U véges ábécé esetén az $\emptyset$ üres nyelv és az U^* univerzális nyelv 3 típusú.
2.3. Adjunk meg olyan grammatikát, amely az $\{x, y\}$ ábécé feletti $L = \{x^k y^k; k \in N\}$ nyelvet generálja.
2.4. Az $\{x, y\}$ ábécé feletti $L = \{x^k yxy^l; k, l \geq 0\}$ nyelv lineáris.

3. fejezet

Környezetfüggetlen nyelvek

Mint már említettük a programozási nyelvek szintaxisának pontos matematikai megadására alkalmasak a generatív grammatikák. Ehhez azonban általában elegendőek a környezetfüggetlen (speciálisan a reguláris) grammatikák. Ezért ebben a fejezetben a környezetfüggetlen grammatikákat és nyelveket vizsgáljuk egy kissé részletesebben.

A 2. fejezetben már beszéltünk arról, hogy a definíciókból nem következik nyilvánvalóan, hogy környezetfüggetlen nyelvek $\mathcal{L}_2$ halmaza részhalmaza a környezetfüggő nyelvek $\mathcal{L}_1$ halmazának. Ennek az az oka, hogy nem minden környezetfüggetlen (2 típusú) grammatika környezetfüggő (1 típusú). Most megmutatjuk, hogy ennek ellenére $\mathcal{L}_2 \subseteq \mathcal{L}_1$. Ehhez bevezetjük a következő fogalmat:

A $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikát *e-mentes*nek nevezzük, nevezzük, ha H nem tartalmaz $X \longrightarrow e$ $(X \in V_N)$ alakú szabályokat, kivéve esetleg az $S \longrightarrow e$ szabályt. Ha azonban H tartalmazza az $S \longrightarrow e$ szabályt, akkor S nem szerepel egyetlen H-beli szabály jobb oldalán sem. Ez azt jelenti, hogy minden e-mentes környezetfüggetlen grammatika környezetfüggő. Az e-mentes környezetfüggetlen grammatikát *szigorúan e-mentes*nek mondjuk, ha nem tartalmazza az $S \longrightarrow e$ szabályt. (Ebben az esetben természetesen lehetnek olyan szabályok, amelyek jobb oldalán S szerepel.)

Az e-mentes környezetfüggetlen grammatikákban az $S \longrightarrow e$ szabály szerepeltetése nem játszik lényeges szerepet. Ez csupán azt jelenti, hogy a grammatika által generált nyelv tartalmazza az e üres szót.

3.1. Lemma. *Bármely $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikához van olyan $G' = (V'_N, V_T, S', H')$ e-mentes környezetfüggetlen grammatika, amelyre $L(G') = L(G)$.*

Bizonyítás A G környezetfüggetlen grammatikához konstruálunk egy szigorúan e-mentes $G_1 = (V_N, V_T, S, H_1)$ környezetfüggetlen grammatikát a következő

módon. Definiáljuk először a

$$V_1 = \{X \in V_N; X \longrightarrow e \in H\},$$

és minden i pozitív egész számra

$$V_{i+1} = V_i \cup \{X \in V_N; X \longrightarrow P \in H, P \in V_i^*\}$$

halmazokat. A definícióból látható, hogy

$$V_1 \subseteq \ldots V_i \subseteq V_{i+1} \cdots \subseteq V_N.$$

Mivel V_N véges, ezért van olyan k pozitív egész szám, hogy $V_k = V_{k+j}$ minden j pozitív egész számra. Jelöljük V_k-t röviden V-vel. Az $X \Longrightarrow_G^* e$ levezetés akkor és csak akkor teljesül, ha $X \in V$. (Tehát $e \in L(G)$ akkor és csak akkor, ha $S \in V$.)

Szerkesszük meg H_1-et a következő módon: Minden $X \longrightarrow P$ $(P \neq e)$ H-beli szabály legyen H_1-ben is. Ezenkívül vegyük be H_1-be az összes olyan $X \longrightarrow Q$ $(Q \neq e)$ szabályt, amelyet az előbbi $X \longrightarrow P$ $(P \neq e)$ szabályokból kaphatók úgy, hogy P-ből elhagyunk V-beli elemeket.

Ekkor egyrészt $L(G_1) \subseteq L(G) - e$. Ha ugyanis veszünk egy G_1-beli levezetést, akkor abban minden olyan $X \longrightarrow Q$ szabály alkalmazása, amely nincs H-ban, helyettesíthető azon $X \longrightarrow P$ H-beli szabály alkalmazásával, amelyből $X \longrightarrow Q$ keletkezett és azon változók e-re való levezetésével, amelyeket P-ből elhagytunk.

A fordított tartalmazás pedig azért igaz, mert, ha alkalmazunk egy $X \longrightarrow P$ H-beli szabályt, majd P-ből egy e-től különböző szót vezetünk le úgy, hogy ugyanakkor a P-ben szereplő bizonyos változókból az e-t vezetjük le, akkor $X \longrightarrow P$ szabály helyettesíthető egy olyan $X \longrightarrow Q$ H_1-beli szabállyal, amelyben Q-t P-ből az előbbi változók elhagyásával kapjuk.

Eszerint $L(G_1) = L(G) - e$. Ha tehát $e \notin L(G)$, akkor $G' = G_1$. Ha $e \in L(G)$, akkor legyen $G' = (V'_N, V_T, S', H')$, ahol $S' \notin V_N$ egy új mondatszimbólum, $V'_N = V_N \cup S'$ és $H' = H_1 \cup \{S' \longrightarrow e, S' \longrightarrow S\}$. □

A 3.1 Lemmából nyilvánvalóan adódik, hogy $\mathcal{L}_2 \subseteq \mathcal{L}_1$. Ezt a lemmát szokás *üresszó lemmá*nak is nevezni.

A Lemma bizonyításából egyszerű eljárást kapunk környezetfüggetlen grammatikával ekvivalens e-mentes környezetfüggetlen grammatika megkonstruálására. Lássunk erre egy példát!

3.2. Példa. *Legyenek* $V_N = \{S, X, Y, Z\}, V_T = \{x, y\}$ *és a* H*-beli szabályok:*

$$S \longrightarrow XYZ,\ X \longrightarrow YY,\ X \longrightarrow e,$$

$$Y \longrightarrow ZZ,\ Y \longrightarrow x,\ Z \longrightarrow XX,\ Z \longrightarrow y.$$

Megadunk a $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikával ekvivalens e-mentes környezetfüggetlen grammatikát.

A 3.1 Lemma bizonyításában leírt módon először meghatározzuk azon nemterminálisok V halmazát, amelyekből levezethető e :

$$V_1 = \{X\},\ V_2 = \{X, Z\},\ V_3 = \{X, Y, Z\},\ V = V_4 = \{S, X, Y, Z\}.$$

(Mellesleg $e \in L(G)$, mivel $S \in V$.) A H_1-beli szabályok:

$$S \longrightarrow XYZ, \quad S \longrightarrow XY, \quad S \longrightarrow YZ, \quad S \longrightarrow XZ, \quad S \longrightarrow X,$$
$$S \longrightarrow Y, \quad S \longrightarrow Z, \quad X \longrightarrow YY, \quad X \longrightarrow Y, \quad Y \longrightarrow ZZ,$$
$$Y \longrightarrow Z, \quad Y \longrightarrow x, \quad Z \longrightarrow XX, \quad Z \longrightarrow X, \quad Z \longrightarrow y.$$

A $G_1 = (V_N, V_T, S, H_1)$ grammatikára $L(G_1) = L(G) - e$. A G-vel ekvivalens e-mentes környezetfüggetlen grammatikát úgy kapjuk, hogy G_1 szabályaihoz hozzávesszük még az S' új mondatszimbólumot és az $S' \longrightarrow S$, $S' \longrightarrow e$ szabályokat.

A környezetfüggetlen grammatikák esetén minden levezetés megadható egy irányított fa, az ún. *levezetési fa* vagy *derivációs fa* segítségével. Szokás ezt a *levezetés fájá*nak is nevezni. A levezetési fa csúcspontjai a levezetésben szereplő jeleknek felelnek meg. A csúcsokat ezekkel a jelekkel címkézzük (jelöljük) meg. A gráf élei úgy vannak irányítva, hogy a terminális jeleknek megfelelő csúcspontok végpontok, azaz nem indul ki belölüki él, míg a változóknak megfelelő csúcspontokból legalább egy él indul ki. Az egy csúcspontból kiinduló élek annak a helyettesítési szabálynak az alkalmazását jelzik, amelynek bal oldalán élek közös kiindulási pontjában található változó áll, a jobb oldalán pedig az élek végpontjaiban található jelek sorozata, az egyes éleket balról jobbra véve sorra.

Tegyük fel például, hogy a $G = (\{S, X, Y\}, \{x, y, z\}, S, H)$ grammatika az

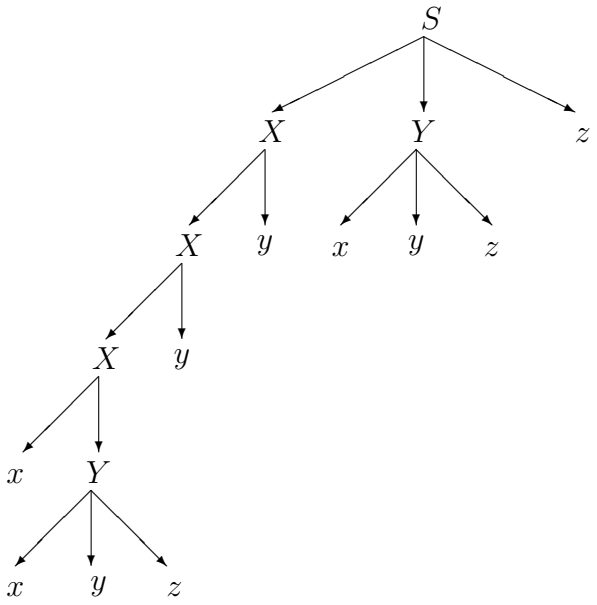
$$S \longrightarrow XYz, \quad X \longrightarrow Xy, \quad X \longrightarrow xY, \quad Y \longrightarrow xyz$$

szabályokat tartalmazza. Ebben a grammatikában megadható az

$$S \Longrightarrow XYz \Longrightarrow XyYz \Longrightarrow Xy^2Yz \Longrightarrow$$
$$\Longrightarrow xYy^2Yz \Longrightarrow x^2yzy^2Yz \Longrightarrow x^2yzy^2xyz^2$$

levezetés, amelynek levezetési fája az 3.1. ábrán látható irányított gráf.

Az $x^2yzy^2xyz^2$ szót a levezetési fa végpontjaiban lévő terminálisok balról jobbra való leolvasásával kapjuk.



3.1. ábra.

3.1. Chomsky normálforma

Egy $G = (V_N, V_T, S, H)$ grammatikáról azt mondjuk, hogy *Chomsky normálformá*ban van megadva, ha minden H-beli szabály $X \longrightarrow x$ vagy $X \longrightarrow YZ$ alakú, ahol $X, Y, Z \in V_N$ és $x \in V_T$.

Minden Chomsky normálformában megadott grammatika szigorúan e-mentes környezetfüggetlen grammatika.

3.3. Tétel. *Bármely $G = (V_N, V_T, S, H)$ szigorúan e-mentes környezetfüggetlen grammatikához van vele ekvivalens Chomsky normálformában megadott $G' = (V'_N, V_T, S, H')$ grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ szigorúan e-mentes környezetfüggetlen grammatika. A 2.3 Lemma szerint feltehető, hogy G standard, azaz a terminálisok csak $X \longrightarrow x$ $(X \in V_N, x \in V_T)$ alakú szabályokban fordulnak elő. A 2.9 Lemma szerint még az is elérhető, hogy ez a standard grammatika láncszabálymentes legyen, azaz nem tartalmaz $X \longrightarrow Y$ $(X, Y \in V_N)$ szabályokat. Ez azt jelenti, hogy H csak következő alakú szabályokat tartalmazhat:

$$X \longrightarrow x, \quad Y \longrightarrow Y_1 Y_2 \dots Y_k \quad (k \geq 2),$$

ahol $X, Y, Y_1, Y_2, \ldots Y_k \in V_N, x \in V_T$. Megszerkesztjük H'-t. Tartalmazza H' az $Y \longrightarrow Y_1 Y_2 \ldots Y_k$ $(k \geq 3)$ H-beli szabályok kivételével a többi H-beli szabályt. Tekintsük most azokat az $Y \longrightarrow Y_1 Y_2 \ldots Y_k$ szabályokat (ha vannak ilyenek), amelyekre $k \geq 3$. Egy ilyen szabályt helyettesíthetjük az

$$Y \longrightarrow Y_1 Z_1, \quad Z_1 \longrightarrow Y_2 Z_2, \quad \ldots, \quad Z_{k-2} \longrightarrow Y_{k-1} Y_k$$

szabályok halmazával, ahol $Z_1, Z_2, \ldots, Z_{k-2} \notin V_N \cup V_T$ újonnan bevezetett nemterminálisok. Ezeket az utóbbi szabályokat is vegyük be H'-be, s legyen V'_N a V_N és az előbbi módon bevezetett új nemterminálisok halmazának egyesítése. Ilyen módon valóban olyan Chomsky normálformában megadott $G' = (V'_N, V_T, S, H')$ grammatikát kapunk, amely ekvivalens G-vel. □

A 3.2 Példa megoldásában szereplő $G_1 = (V_N, V_T, S, H_1)$ szigorúan e-mentes környezetfüggetlen grammatikához, a 3.3 Tétel bizonyítása alapján, úgy kapunk vele ekvivalens Chomsky normálformában megadott grammatikát, hogy bevezetünk még egy új Z_1 nemterminálist és az $S \longrightarrow XYZ$ szabályt kicseréljük az $S \longrightarrow XZ_1,\ Z_1 \longrightarrow YZ$ szabályokra.

Ha az e-mentes környezetfüggetlen $G = (V_N, V_T, S, H)$ grammatika tartalmazza az $S \longrightarrow e$ szabályt, akkor az $S \longrightarrow e$ szabály törlésével belőle kapott szigorúan e-mentes grammatika környezetfüggetlen. (Ebből a 3.1 Lemma bizonyítása szerint az is következik, hogy ha egy L nyelv környezetfüggetlen, akkor az $L - e$ nyelv is az.) A 3.3 Tétel szerint, ez a szigorúan e-mentes grammatika vele ekvivalens Chomsky normálformára hozható. Ezután újra visszaírva az $S \longrightarrow e$ szabályt, G-vel ekvivalens e-mentes környezetfüggetlen grammatikát kapunk, amelyben a helyettesítési szabályok az $S \longrightarrow e$ szabályon kívül $X \longrightarrow x$ vagy $X \longrightarrow YZ$ alakú, ahol $X, Y, Z \in V_N - S$ és $x \in V_T$.

Már említettük, hogy egy programozási nyelv szintaxisának leírására alkalmasak a generatív grammatikák. A gyakorlatban fontos feladat annak eldöntése, hogy a felhasználó által megírt $p \in V_T^*$ program megfelel-e a G grammatikával megadott szintaktikai előírásoknak, azaz a grammatika szabályainak, hiszen csak ebben az esetben fogadja el és hajtja végre a programot a számítógép. Ez éppen annak eldöntését jelenti, hogy $p \in L(G)$ teljesül-e. Ezek után nem kell hangsúllyoznunk a következő definíció fontosságát.

Egy U ábécé feletti L nyelvet *rekurzív*nak nevezünk U felett, ha bármely $p \in U^*$ szórol algoritmikusan eldönthető, hogy benne van-e L-ben, azaz megoldható az L nyelvre vonatkozó szóprobléma. Az U ábécé feletti rekurzív nyelvek összege, szorzata és komplementere is rekurzív. Nyelvek egy osztályát *rekurzív*nak nevezzük, ha minden eleme rekurzív. Megmutatjuk, hogy a környezetfüggetlen nyelvek osztálya rekurzív.

A generatív grammatikák ún. *szintaktikus elemzésének alapfeladata* olyan algoritmusok keresesése, amelyek ezt a kérdést eldöntik. A következő tétel bizo-

nyításából egy ilyen (nem túl hatékony) eljárás adódik. A későbbiekben azt is megmutatjuk, hogy a tétel környezetfüggő nyelvekre is igaz, mondatszerkezetű nyelvekre általában azonban nem. FÜLÖP ZOLTÁN [18] egyetemi jegyzete nagyon jó bevezetést nyújt a grammatikák szintaktikus elemzésébe. Mi azonban a szintaktikus elemzéssel nem foglalkozunk.

3.4. Tétel. *Minden környezetfüggetlen nyelv rekurzív.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika és $p \in V_T^*$. A 3.1 Lemma szerint feltehetjük, hogy G e-mentes. Ha $p = e$, akkor legfeljebb $|H|$ lépésben eldönthető, hogy $e \in L(G)$ vagy $e \notin L(G)$. (Azt kell megnézni, hogy $S \longrightarrow e$ H-beli szabály-e vagy nem.) Ezért a továbbiakban feltehetjük, hogy $p \neq e$. A 3.3 Tétel szerint feltehetjük, hogy G Chomsky normálformában megadott szigorúan e-mentes környezetfüggetlen grammatika. Ha $p \in L(G)$, akkor létezik egy $S \Longrightarrow_G^* p$ levezetés. Tegyük fel, hogy a levezetés $k(\geq 1)$ lépésből áll. Pontosan $|p|$ lépésben kell alkalmazni $X \longrightarrow x$ ($X \in V_N, x \in V_T$) alakú szabályt és $k - |p|$ lépésben $X \longrightarrow YZ$ ($X, Y, Z \in V_N$) alakú szabályt. Az utóbbi lépésekkel mindig eggyel növekszik a nemterminálisok száma, ezért $|p| = k - |p| + 1$, azaz $k = 2|p| - 1$. Ebből következik, hogy adott $p \in V_T^+$ esetén elegendő az $2|p|-1$ hosszúságú $S \Longrightarrow_G^* P$ levezetéseket megadni, beleértve azokat is amelyek nem vezetnek terminális szavakhoz, s megvizsgálni, hogy van-e olyan P, hogy $P = p$. Mivel véges számú ilyen levezetés van, ezért $p \neq e$ esetben is algoritmikusan eldönthető, hogy $p \in L(G)$ vagy $p \notin L(G)$. □

A bizonyítás egy érdekes adaléka, hogy Chomsky normálformában megadott grammatikában az általa generált nyelv minden szava páratlan számú lépéssel vezethető le.

3.2. Bar-Hillel lemma

A következő lemma alapvető jelentőségű a környezetfüggetlen nyelvek elméletében. A lemmát (*a környezetfüggetlen nyelvekre vonatkozó*) *pumpáló lemmá*nak is szokták nevezni.

3.5. Lemma. *(Bar-Hillel lemma) Ha L környezetfüggetlen nyelv U felett, akkor van olyan (L-től függő) n pozitív egész szám, hogy ha $p \in L$ és $|p| > n$, akkor p előállítható $p = ruvwt$ $(r, t, u, v, w \in U^*)$ alakban, ahol $|uvw| \leq n$, $uw \neq e$ és minden m nemnegatív egész számra $ru^m vw^m t \in L$.*

Bizonyítás Tegyük fel, hogy a $G = (V_N, V_T, S, H)$ 2 típusú grammatika generálja az L környezetfüggetlen nyelvet, azaz $L = L(G)$. A 3.1 Lemma szerint

feltehetjük, hogy G e-mentes. Sőt azt is feltehetjük, hogy G szigorúan e-mentes, mert L pontosan akkor környezetfüggetlen, ha $L - e$ is az, s mindkét nyelvhez választhatók ugyanazok a lemmában szereplő k és n pozitív egész számok. A 3.3 Tétel szerint G-t megadhatjuk Chomsky normálformában.

Ha egy $p \in L$ szónak a levezetése olyan levezetési fával ábrázolható, amelyben a leghosszabb út j hosszúságú, akkor a Chomsky normálforma miatt $|p| \leq 2^j$. Tegyük fel, hogy $|V_N| = l$. Ha $|p| > 2^l$, akkor az $S \Longrightarrow^* p$ levezetés fájában a leghosszabb útnak l-nél hosszabbnak kell lenni. Vegyük ennek az útnak az utolsó $l+1$ hosszúságú szakaszát. Van olyan $X \in V_N$ változó, amely ezen a szakaszon legalább kétszer előfordul. Vegyük ennek a nemterminálisnak két ilyen előfordulását. Ezek közül az S mondatszimbólumhoz közelebb eső X-hez tartozó részfa végpontjainak megfelelő szó legyen $q(\in V_T^*)$, a másik X-hez tartozó részfa végpontjainak megfelelő szó pedig legyen $v(\in V_T^*)$. Ezekre nyilván $X \Longrightarrow^* q$ és $X \Longrightarrow^* v$ teljesül, továbbá q tartalmazza részszóként v-t, azaz $q = uvw(u, w \in V_T^*)$.

Megmutatjuk, hogy $uw \neq e$. Mivel G-t Chomsky normálformában adtuk meg és X-nek az $S \Longrightarrow^* p$ levezetésben lévő két előfordulásáról van szó, ezért az $X \Longrightarrow^* uXw$ levezetés első lépése csak $X \Longrightarrow YZ$ $(Y, Z \in V_N)$ lehet. De G szigorúan e-mentes, ezért $uw \neq e$.

Emellett természetesen $p = rqt$ is teljesül valamilyen $r, t(\in V_T^*)$ szavakra. Az X változó megválasztása miatt $|q| \leq 2^{l+1}$. Másrészt $S \Longrightarrow^* rXt$ és $X \Longrightarrow^* uXw$ is fennáll, ezért tetszőleges $m \geq 0$ egész számra $S \Longrightarrow^* ru^m vw^m t$. Ez azt jelenti, hogy a lemma állítása $n = 2^{l+1}$ pozitív egész számmal teljesül. □

A Bar-Hillel lemma azt mondja ki, hogy egy végtelen környezetfüggetlen nyelvben minden elég hosszú szóhoz végtelen sok "hasonló szerkezetű szó" van. A lemma bizonyításából az is következik, hogy ha egy véges L nyelvet a Chomsky normálformában megadott $G = (V_N, V_T, S, H)$ grammatika generálja és $|V_N| = l$, akkor az L-beli szavak hossza legfeljebb 2^l. Ugyanis, ha $p \in L$ és $|p| > 2^l$, akkor a pumpáló lemma szerint L végtelen. A lemma segítségével megmutatjuk a (2.4) Chomsky hierarchiában a második valódi tartalmazás helyességét.

3.6. Tétel. $\mathcal{L}_2 \subset \mathcal{L}_1$.

Bizonyítás A tétel igazolásához megadunk egy olyan környezetfüggő nyelvet, amelyik nem környezetfüggetlen.

Megmutatjuk, hogy az $U = \{a, b, c\}$ ábécé feletti $L = \{a^j b^j c^j; j \in N\}$ nyelv nem környezetfüggetlen. Indirekt bizonyítást végzünk. Tegyük fel, hogy L környezetfüggetlen. Akkor vannak olyan k, n pozitív egész számok, hogy minden k-nál hosszabb L-beli p szóra, így a $p = a^k b^k c^k$ szóra is, teljesülnek a Bar-Hillel lemma feltételei. Azaz a $p = a^k b^k c^k$ szó felírható $p = ruvwt$ $(r, t, u, v, w \in U^*)$

alakban, ahol $|uvw| \leq n$, $uw \neq e$ és minden m nemnegatív egész számra $ru^m vw^m t \in L$. Vizsgáljuk meg, hogyan helyezkednek el a u és w szavak p-ben. Megállapíthatjuk, hogy u és hasonlóan w sem tartalmazhat különböző betűket, mert akkor az $ru^m vw^m t \in L$ $(m \geq 2)$ szó nem írható $a^j b^j c^j$ alakban. Tehát mind u mind w legfeljebb egy fajta betűt tartalmaz. Ez viszont ellentmondáshoz vezet, mert akkor m-et növelve $ru^m vw^m t \in L$ szavakban legalább egy fajta betű száma nem növekszik.

Most azt mutatjuk meg, hogy az L nyelvet generálja az az 1 típusú $G = (V_N, U, S, H)$ grammatika, amelyben $V_N = \{S, X, Y, Z_1, Z_2\}$ és a H-beli szabályok a következők:

$$S \longrightarrow abc, \quad S \longrightarrow aXbc,$$

$$Xb \longrightarrow XZ_1, \quad XZ_1 \longrightarrow Z_1Z_1, \quad Z_1Z_1 \longrightarrow Z_1X, \quad Z_1X \longrightarrow bX,$$

$$bY \longrightarrow Z_2Y, \quad Z_2Y \longrightarrow Z_2Z_2, \quad Z_2Z_2 \longrightarrow YZ_2, \quad YZ_2 \longrightarrow Yb,$$

$$Xc \longrightarrow Ybcc, \quad aY \longrightarrow aaX, \quad aY \longrightarrow aa.$$

Mivel $S \longrightarrow abc$, ezért $abc \in L(G)$. Ezután azt látjuk be, hogy minden j pozitív egész számra

$$S \Longrightarrow_G^* a^j X b^j c^j.$$

Minthogy $S \longrightarrow aXbc$, ezért $j = 1$ esetben az állítás igaz. Ha valamilyen pozitív egész j-re $S \Longrightarrow_G^* a^j X b^j c^j$, akkor csak az

$$Xb \longrightarrow XZ_1, \quad XZ_1 \longrightarrow Z_1Z_1, \quad Z_1Z_1 \longrightarrow Z_1X, \quad Z_1X \longrightarrow bX$$

szabályokat alkalmazhatjuk ebben a sorrendben j-szer. Utána csak $Xc \longrightarrow Ybcc$ helyettesítést végezhetjük el, majd a

$$bY \longrightarrow Z_2Y, \quad Z_2Y \longrightarrow Z_2Z_2, \quad Z_2Z_2 \longrightarrow YZ_2, \quad YZ_2 \longrightarrow Yb$$

helyettesítéseket ebben a sorrendben j-szer. Így

$$S \Longrightarrow_G^* a^j Y b^{j+1} c^{j+1}$$

levezetést kapjuk. Ezután két lehetőség között választhatunk. Vagy befejezzük a levezetést az $aY \longrightarrow aa$ helyettesítéssel:

$$S \Longrightarrow_G^* a^{j+1} b^{j+1} c^{j+1}.$$

Vagy pedig folytatjuk az $aY \longrightarrow aaX$ helyettesítéssel:

$$S \Longrightarrow_G^* a^{j+1} X b^{j+1} c^{j+1}.$$

Az S-ből csakis ezek a mondatformák vezethetők le. Ebből már könnyen belátható, hogy $L = L(G)$, azaz környezetfüggő, s így $\mathcal{L}_2 \subset \mathcal{L}_1$. □

Az előbbi bizonyításban szereplő L nyelvet generálja az egyszerűbb 0 típusú $G' = (V'_N, U, S, H')$ is, amelyben $V'_N = \{S, X, Y\}$ és a H'-beli szabályok:

$$S \longrightarrow abc, \quad S \longrightarrow aXbc, \quad Xb \longrightarrow bX, \quad bY \longrightarrow Yb,$$

$$Xc \longrightarrow Ybcc, \quad aY \longrightarrow aaX, \quad aY \longrightarrow aa.$$

Ez a grammatika azonban nem környezetfüggő. A 4.1. alfejezetben kapunk majd választ arra, hogy milyen 0 típusú grammatikákhoz van ekvivalens 1 típusú grammatika.

3.7. Következmény. *Egyelemű ábécé feletti környezetfüggetlen nyelvek regulárisak.*

Bizonyítás Legyen az $\{x\}$ ábécé feletti L nyelv környezetfüggetlen. Feltehetjük ,hogy $e \notin L$. Ha ugyanis az L nyelv reguláris, akkor az $L + e = L + \emptyset^*$ nyelv is az, hiszen reguláris nyelvek összege is reguláris. Mivel minden véges nyelv reguláris, ezért azt is feltehetjük, hogy az L nyelv végtelen.

Legyenek k és n a környezetfüggetlen nyelvekre vonatkozó pumpáló lemmában szereplő L-től függő pozitív egész számok. A pumpáló lemma szerint minden $j > k$ esetén, ha $x^j \in L$, akkor van olyan $1 \leq m \leq n$, hogy minden $l \geq 0$ egész számra $x^{j+lm} \in L$ is teljesül. Legyen $1 \leq m_1 < m_2 < \cdots < m_t \leq n$ az összes ilyen m. Ebből adódik, hogy $t \leq n$. Mivel L végtelen, ezért $1 \leq t$. Legyenek továbbá

$$L_0 = \{x^j \in L; 0 < j \leq k\},$$

$$L_s = \{x^j \in L; j > k, x^{j+lm_s} \in L, l \geq 0\}, \quad s = 1, 2, \ldots, t.$$

Nyilvánvaló, hogy $L = \sum_{s=0}^{t} L_s$. Tehát elegendő megmutatni, hogy minden $0 \leq s \leq t$ esetén az L_s nyelv reguláris. Az L_0 nyelv véges, ezért reguláris. Minden $x^j \in L_s$ $(s \geq 1)$ esetén van olyan $l \geq 0$ és $0 \leq d_s \leq m_s - 1$, hogy $j = lm_s + d_s$. Adott d_s-hez jelöljük j_s-sel a legkisebb ilyen j kitevőt. Ha

$$0 \leq d_{s,1} < d_{s,2} < \cdots < d_{s,r} \leq m_s - 1, \quad \text{és} \quad j_{s,1}, \quad j_{s,2}, \quad \ldots, \quad j_{s,r}$$

az összes előbbi módon definiált d_s ill. j_s, akkor

$$L_s = \sum_{v=1}^{r} \{x^{j_{s,v}+lm_s}; l \geq 0\} = \sum_{v=1}^{r} x^{j_{s,v}} (x^{m_s})^*,$$

azaz reguláris, amiből adódik, hogy L is reguláris. □

A későbbiekben megmutatjuk, hogy legalább kételemű véges ábécékre a 3.7 Következmény már nem igaz.

A 2.7 Tétel szerint a környezetfüggetlen nyelvek osztálya zárt a reguláris műveletekre. Ez azonban nem igaz a Boole műveletekre.

3.8. Tétel. *A környezetfüggetlen nyelvek osztálya nem zárt a metszetre és a komplementerképzésre.*

Bizonyítás Legyenek $L_1 = \{a^k b^k c^n; k, n \in N\}$ és $L_2 = \{a^k b^n c^n; k, n \in N\}$ $U = \{a, b, c\}$ feletti nyelvek. Megmutatjuk, hogy L_1 és L_2 környezetfüggetlen. Legyen $V_N = \{S, X, Y\}$ és

$$H_1 = \{S \longrightarrow XY,\ X \longrightarrow aXb,\ X \longrightarrow e,\ Y \longrightarrow cY,\ Y \longrightarrow e\},$$

$$H_2 = \{S \longrightarrow XY,\ Y \longrightarrow bYc,\ Y \longrightarrow e,\ X \longrightarrow Xa,\ X \longrightarrow e\}.$$

Nyilvánvaló, hogy a $G_i = (V_N, U, S, H_j)$ $(i = 1, 2)$ környezetfüggetlen grammatika generálja az L_i nyelvet. Azonban, mint azt a 3.6 Tétel bizonyításában láttuk, az

$$L_1 \cap L_2 = \{a^j b^j c^j; j \in N\}$$

nyelv nem környezetfüggetlen.

Ebből már az is következik, hogy a környezetfüggetlen nyelvek osztálya a komplementerképzésre sem zárt. A De Morgan azonosságok szerint ugyanis

$$L_1 \cap L_2 = \overline{\overline{L}_1 \cup \overline{L}_2}$$

írható bármely két nyelvre. Amiből látható, hogy ha a környezetfüggetlen nyelvek osztálya zárt volna komplementerképzésre, akkor a metszetre is zárt lenne, ami az előbbiek miatt lehetetlen. □

3.9. Tétel. *Bármely környezetfüggetlen grammatikáról algoritmikusan eldönthető, hogy az általa generált nyelv üres, véges vagy végtelen.*

Bizonyítás A 3.1 Lemma szerint elegendő e-mentes környezetfüggetlen grammatikákat vizsgálni.

Először megmutatjuk, hogyan dönthető el algoritmikusan, hogy egy $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika által generált $L = L(G)$ nyelv üres vagy nem. Ha H tartalmazza az $S \longrightarrow e$ szabályt, akkor $e \in L$, s így a nyelv nemüres. Ezért a továbbiakban feltehetjük, hogy G szigorúan e-mentes. A 3.3 Tétel szerint G megadható Chomsky normálformában. Legyen $|V_N| = l$. Ha egy levezetés fájában van olyan S-ből kiinduló út, amely hossza nagyobb, mint l, akkor ennek az útnak a mentén nem szerepelhet csupa különböző nemterminális, mint azt a Bar-Hillel lemma bizonyításában már láttuk. Vagyis van olyan $X \in V_N$ nemterminális, amely legalább kétszer előfordul ennek az útnak a mentén. Tekintsük most X-nek ezen az úton az S-től legtávolabbra eső előfordulását. Vegyük a levezetés fájának azt a részfáját, amelynek ez az X gyökere. Ha ezzel a részfával helyettesítjük azt a részfát, amelynek gyökere

egy S-hez ezen az úton közelebb eső X, akkor az előbbi út hossza az adott két előfordulás közötti távolsággal lerövidül. Másrészt nyilvánvaló, hogy az így nyert fa is egy, az adott grammatikában lehetséges levezetés fája. Tehát a G grammatikában bármely $S \Longrightarrow^* p$ ($p \in V_T^*$) levezetéshez található olyan $S \Longrightarrow^* q$ ($q \in V_T^*$) levezetés, amelynek fája nem tartalmaz l-nél hosszabb utat. Ezért annak eldöntéséhez, hogy üres-e az L nyelv, elegendő olyan levezetéseket megvizsgálni, amelynek fájában a leghosszabb út legfeljebb l hosszúságú. Mindazon fák T halmazát, amelyek eleget tesznek ennek a korlátozásnak a például következő algoritmussal kaphatjuk meg:
Az egyetlen S csúcspontból álló fát felvesszük T-be.
Minden olyan fát felveszünk T-be, amely egyetlen H-beli szabály alkalmazásával nyerhető egy már előzőleg a T-be felvett fából, kivéve, ha a leghosszabb útja l-nél hosszabb.

Bármely grammatikához csak véges sok ilyen fa van, így az eljárás véges sok lépésben befejeződik. Most már csak azt kell megvizsgálnunk, hogy van-e T-ben olyan fa, amelynek minden végpontjában terminális jel szerepel. Ha nincs ilyen, akkor az adott grammatikában egyetlen terminális szó sem vezethető le, azaz $L = \emptyset$.

A Bar-Hillel lemma segítségével el tudjuk dönteni, hogy az L nyelv véges vagy végtelen. A lemmában szereplő k és n pozitív egész számok megadása után csak azt kell eldöntenünk, hogy van-e az L nyelvben k-nál hosszabb, de legfeljebb $k+n$ hosszúságú szó, amilyen szó nyilvánvalóan csak véges sok lehet. Tegyük fel ugyanis, hogy az L végtelen, de csak k-nál nem hosszabb vagy $k+n$-nél hosszabb szavak vannak L-ben. Mivel L végtelen, van olyan $p \in L$, hogy $|p| > k+n$. Legyen p a $(k+n)$-nél hosszabb L-beli szavak közül egy legkisebb hosszúságú szó. A Bar-Hillel lemma szerint $p = ruvwt, |uvw| \leq n,\ uw \neq e$ és minden m nemnegatív egész számra $ru^m vw^m t \in L$. Ha $m = 0$, akkor $k < |rvt| < |p|$ és $rvt \in L$. Ez azonban ellentmondás, mivel feltevésünk miatt $|rvt| \leq k$. □

3.3. Redukált grammatikák

A környezetfüggetlen grammatika definíciója megenged olyan szimbólumokat is, amely a grammatika által generálható nyelv meghatározásához feleslegesek. Ezeket a szimbólumokat célszerű kiküszöbölni. Először foglalkozzunk a nemterminális szimbólumokkal. Legyen $G = (V_N, V_T, S, H)$ egy környezetfüggetlen grammatika. Az X változóról azt mondjuk, hogy *terminál*ó, ha van olyan $p \in V_T^*$, amelyre $X \Longrightarrow^* p$. A definícióból következik, hogy $L(G) = \emptyset$ akkor és csak akkor, ha S nem terminál*ó*.

3.10. Lemma. *Legyen $G = (V_N, V_T, S, H)$ egy környezetfüggetlen [jobb lineáris] grammatika. Ha $L(G) \neq \emptyset$, akkor megadható olyan G-vel ekvivalens $G_1 = (V, V_T, S, H_1)$ környezetfüggetlen grammatika [jobb lineáris], amelyben V a V_N-beli terminálló változók halmaza.*

Bizonyítás Először meghatározzuk a V_N-beli terminálló változók V halmazát. Legyen

$$V_1 = \{X \in V_N; \exists (p \in V_T^*)(X \longrightarrow p \in H)\},$$

és minden i pozitív egész számra

$$V_{i+1} = V_i \cup \{X \in V_N; \exists (P \in (V_i \cup V_T)^*)(X \longrightarrow P \in H)\}.$$

A definícióból belátható, hogy

$$V_1 \subseteq \ldots V_i \subseteq V_{i+1} \cdots \subseteq V_N.$$

Mivel V_N véges, ezért van olyan k pozitív egész szám, hogy $V_k = V_{k+j}$ minden j pozitív egész számra. Jelöljük ezt a V_k-t V-vel. Az $X \Longrightarrow_G^* p$ levezetés akkor és csak akkor teljesül, ha $X \in V$. (Tehát $p \in L(G)$ akkor és csak akkor, ha $S \in V$.) A konstrukcióból világos, hogy $X \in V_N$ akkor és csak akkor terminálló, ha $X \in V$. (Mivel $L(G) \neq \emptyset$, ezért $S \in V$.)

Álljon H_1 azon H-beli szabályokból, amelyek nem tartalmaznak $(V_N - V)$-beli változókat. Azt kell még igazolni, hogy $L(G) = L(G_1)$. Mivel $H_1 \subseteq H$, ezért $L(G_1) \subseteq L(G)$. Megfordítva, ha $p \in L(G)$, azaz $S \Longrightarrow_G^* p$, akkor a levezetés valamennyi lépésében szereplő változó terminálló, tehát valamennyi lépésben szereplő H-beli szabály benne van H_1-ben is. Így $p \in L(G_1)$, azaz $L(G) \subseteq L(G_1)$. □

A következőkben a nem elérhető változókat szűrjük ki. Az $X \in V_N$ változót *elérhető*nek nevezzük, ha vannak olyan $P, Q \in (V_N \cup V_T)^*$ szavak, amelyekre $S \Longrightarrow^* PXQ$, azaz ha X előfordul valamelyik mondatformában. A definícióból következik, hogy S mindig elérhető.

3.11. Lemma. *Bármely $G = (V_N, V_T, S, H)$ egy környezetfüggetlen [jobb lineáris] grammatikához megadható olyan vele ekvivalens $G' = (W, V_T, S, H')$ környezetfüggetlen [jobb lineáris] grammatika, amelyben W a (V_N-beli) elérhető változók halmaza.*

Bizonyítás Először megadjuk a (V_N-beli) elérhető szimbólumok W halmazát. Legyen $W_0 = \{S\}$ és minden i nemnegatív egész számra

$$W_{i+1} = W_i \cup \{X \in V_N; \exists (Y \in W_i, P, Q \in (V_N \cup V_T)^*)(Y \longrightarrow PXQ \in H)\}.$$

Nyilvánvaló, hogy

$$W_0 \subseteq \ldots W_i \subseteq W_{i+1} \cdots \subseteq V_N.$$

Mivel V_N véges, ezért van olyan k nemnegatív egész szám, hogy $W_k = W_{k+j}$ minden j pozitív egész számra. Jelöljük ezt a W_k-t W-vel. Az A konstrukcióból következik, hogy $X \in V_N$ akkor és csak akkor elérhető, ha $X \in W$.

Most megadjuk a G' grammatikát. Álljon H' azon H-beli szabályokból, amelyek nem tartalmaznak $(V_N - W)$-beli szimbólumokat. Mivel $S \in W$, ezért $W \neq \emptyset$.

Meg kell még mutatni, hogy $L(G) = L(G')$. Mivel $H' \subseteq H$, ezért szükségképpen $L(G') \subseteq L(G)$. Megmutatjuk, hogy $L(G) \subseteq L(G')$. Ha $L(G) = \emptyset$, akkor ez nyilvánvalóan teljesül. Tegyük fel, hogy $L(G) \neq \emptyset$. Ha $p \in L(G)$, azaz $S \Longrightarrow_G^* p$, akkor a levezetés valamennyi lépésében szereplő változó elérhető, tehát valamennyi lépésben szereplő H-beli szabály H'-beli szabály is. Tehát $p \in L(G')$, vagyis $L(G) \subseteq L(G')$. □

Legyen $G = \{V_N, V_T, S, H\}$ környezetfüggetlen grammatika és $L(G) \neq \emptyset$. A G grammatikát *redukált*nak nevezzük, ha minden változója szerepel legalább egy $S \Longrightarrow_G^* p$ $(p \in V_T^*)$ levezetésben. Nyilvánvaló, hogy G pontosan akkor redukált, ha minden változója termináló és elérhető. Egy változóról azt mondjuk, hogy *felesleges*, ha nem szerepel legalább egy $S \Longrightarrow_G^* p$ $(p \in V_T^*)$ levezetésben sem, vagyis ha nem termináló vagy nem elérhető.

Ha $G = \{V_N, V_T, S, H\}$ környezetfüggetlen grammatika és $L(G) = \emptyset$, vagyis S nem termináló, akkor a $G = \{\{S\}, V_T, S, \emptyset\}$ grammatikát nevezzük *redukált*nak.

A 3.10 és a 3.11 Lemmákat alkalmazva a következő tétel bizonyításában egy algoritmust adunk meg a felesleges változók törlésére. Ezt két lépésben érjük el. Először a nem termináló változókat hagyjuk el.

3.12. Tétel. *Bármely $G = (V_N, V_T, S, H)$ környezetfüggetlen [jobb lineáris] grammatikához megadható ekvivalens redukált $G' = (V_N', V_T, S, H')$ környezetfüggetlen [jobb lineáris] grammatika.*

Bizonyítás Ha $L(G) = \emptyset$, akkor $G' = \{\{S\}, V_T, S, \emptyset\}$. Ha $L(G) \neq \emptyset$, akkor megadjuk a 3.10 Lemma alapján a $G_1 = (V, V_T, S, H_1)$ grammatikát, majd alkalmazzuk G helyett G_1-re a 3.11 Lemmát, akkor $L(G) = L(G_1) = L(G')$.

Nem nehéz megmutatni, hogy G' redukált. Legyen ugyanis $X \in W$. Ez azt jelenti, hogy X elérhető változó, azaz vannak olyan $P, Q \in (W \cup V_T)^*$, amelyekre $S \Longrightarrow_G^* PXQ$ teljesül. Ebből következik, hogy a levezetésben minden változó elérhető, vagyis a levezetésben alkalmazott minden H-beli szabály benne van H'-ben is. Tehát $S \Longrightarrow_{G'}^* PXQ$. Továbbá G_1-ben, ezért G'-ben is minden változó termináló, azaz van olyan $p \in V_T^*$, hogy $PXQ \Longrightarrow_{G'}^* p$. Kaptuk, hogy $S \Longrightarrow_{G'}^* PXQ \Longrightarrow_{G'}^* p$, vagyis X nem felesleges. □

Legyen tetszőleges $G = (V_N, V_T, S, H)$ grammatika és $L(G) \neq \emptyset$. A G grammatika x terminálisát *felesleges*nek nevezzük, ha $V_T^* x V_T^* \cap L(G) = \emptyset$, vagyis nem szerepel $L(G)$ egyetlen szavában sem. Már az előző fejezetben említettük, hogy ha egy terminális nem szerepel egy G grammatika egyetlen szabályában sem, akkor az $L(G)$ nyelv egyetlen szavában sem fordul elő. Ha G redukált környezetfüggetlen grammatika és egy terminális szerepel G legalább egy szabályában, akkor előfordul $L(G)$ legalább egy szavában. Ezért ezek a felesleges terminálisok könnyen kiküszöbölhetők.

Ha $L(G) = \emptyset$, akkor természetesen minden terminális felesleges. Ebben az esetben azonban legalább egy terminálist meg kell hagynunk, mert különben ellentmondásba kerülünk a grammatika definíciójával.

3.13. Példa. *Legyenek* $G = (V_N, V_T, S, H)$, $V_N = \{S, X, Y, Z\}$, $V_T = \{x, y\}$ *és a* H*-beli szabályok:*

$$S \longrightarrow X, \quad S \longrightarrow Y, \quad X \longrightarrow xY, \quad X \longrightarrow yS, \quad X \longrightarrow y,$$

$$Y \longrightarrow XY, \quad Y \longrightarrow Yx, \quad Z \longrightarrow XS, \quad Z \longrightarrow y.$$

Konstruáljunk G*-vel ekvivalens redukált* G' *környezetfüggetlen grammatikát.*

A 3.12 Tétel bizonyításában szereplő algoritmust követve, először meghatározzuk G termináló változóit a 3.10 Lemma bizonyításában megadott módon. Kapjuk, hogy

$$V_1 = \{X, Z\}, \quad V_2 = \{S, X, Z\} = V_3 = V,$$

azaz G-ben csak Y nem termináló változó. Azokat a szabályokat hagyjuk meg, amelyekben Y nem szerepel. Így kapjuk a $G_1 = (V, V_T, S, H_1)$ grammatikát, ahol $V = \{S, X, Z\}$, a H_1-beli szabályok pedig:

$$S \longrightarrow X, \quad X \longrightarrow yS, \quad X \longrightarrow y, \quad Z \longrightarrow XS, \quad Z \longrightarrow y.$$

Most a 3.11 Lemma bizonyítását követve kiszámoljuk G_1 elérhető változóit:

$$W_0 = \{S\}, \quad W_1 = \{S, X\} = W_2 = W.$$

Azokat a szabályokat tartjuk meg, amelyekben Z nem szerepel, azaz $G' = (\{S, X\}, \{x, y\}, S, H')$, ahol a H'-beli szabályok:

$$S \longrightarrow X, \quad X \longrightarrow yS, \quad X \longrightarrow y.$$

Mivel x nem szerepel egyetlen szabályban sem, ezért törölhető a terminális ábécéből.

3.4. Bal oldali levezetések

Az alábbiakban olyan levezetési eljárást ismertetünk, amely az egyes lépésekben a mondatformák elején [végén] álló terminális részszó hosszát nem csökkenti. Ez a nyelvek és automaták kapcsolatát vizsgálva is fontos lesz számunkra. Kérdés, lehet-e ezt úgy megvalósítani, hogy a mondatformák elején [végén] lévő terminális részszó hossza növekedjen. Ehhez már általában a környezetfüggetlen grammatikát is módosítani kell, hiszen egy

$$X \longrightarrow YP \quad (X, Y \in V_N,\ P \in (V_N \cup V_T)^*)$$

alakú szabály alkalmazása a mondatforma elején álló terminális jelek számát nem növeli. Megmutatjuk, hogy szigorúan e-mentes környezetfüggetlen nyelvekre a módosítás megoldható úgy, hogy a kapott grammatika ekvivalens marad az eredeti grammatikával. Környezetfüggetlen nyelvek egy újabb normálformáját is bevezetjük, ami az eljárást megkönnyíti.

Legyen $G = (V_N, V_T, S, H)$ tetszőleges környezetfüggetlen grammatika. A $P \Longrightarrow_G^* Q$ levezetést *bal* [*jobb*] *oldali levezetés*nek nevezzük, s rá a

$$P \Longrightarrow_{G,b}^* Q \quad [P \Longrightarrow_{G,j}^* Q]$$

jelölést használjuk, ha a levezetés minden lépésében a bal [jobb] oldalról az első nemterminálist helyettesítjük egy rá vonatkozó szabály jobb oldalával. Ebben az esetben azt is mondjuk, hogy Q *balról* [*jobbról*] *levezethető* P*-ből* (*a* G *grammatikában*). Ha

$$S \Longrightarrow_{G,b}^* Q \quad [S \Longrightarrow_{G,j}^* Q],$$

akkor Q-t (*a* G *grammatikában*) *balról* [*jobbról*] *levezethetőnek* vagy *bal* [*jobb*] *mondatformá*nak hívjuk.

3.14. Lemma. *Legyen* $G = (V_N, V_T, S, H)$ *tetszőleges környezetfüggetlen grammatika. Ha* $p \in V_T^*$ *levezethető az* $X \in V_N$ *nemterminálisból, akkor balról [jobbról] is levezethető* X*-ből.*

Bizonyítás A levezetés hossza szerinti teljes indukcióval bizonyítunk. Az 1 hosszúságú levezetésekre az állítás nyilvánvaló. Tegyük fel, hogy az n-nél nem hosszabb

$$Y \Longrightarrow_G^* q \quad (Y \in V_N, q \in V_T^*)$$

levezetésekhez létezik $Y \Longrightarrow_{G,b}^* q$ bal oldali levezetés. Tegyük fel, hogy az

$$X \Longrightarrow_G^* p \quad (X \in V_N, p \in V_T^*)$$

levezetés $n+1$ hosszúságú. Mivel G 2 típusú grammatika, ezért az $X \Longrightarrow_G^* p$ levezetés első lépése

$$X \Longrightarrow p_1 X_1 p_2 \dots p_k X_k p_{k+1}$$

alakú, ahol

$$p_1, p_2, \dots, p_{k+1} \in V_T^*,\ X_1, X_2, \dots, X_k \in V_N, \quad (k \geq 1).$$

Ez azt jelenti, hogy léteznek olyan legfeljebb n hosszúságú

$$X_i \Longrightarrow_G^* q_i \quad (q_i \in V_T^*, \quad i = 1, 2, \dots, k)$$

levezetések, hogy

$$p = p_1 q_1 p_2 q_2 \dots p_k q_k p_{k+1}.$$

Az indukciós feltevés miatt léteznek az

$$X_i \Longrightarrow_{G,b}^* q_i \quad (i = 1, 2, \dots, k)$$

bal oldali levezetések is. Ezeket a levezetéseket sorra alkalmazva az

$$X \Longrightarrow p_1 X_1 p_2 \dots p_k X_k p_{k+1} \Longrightarrow_G^* p_1 q_1 p_2 X_2 \dots p_k X_k p_{k+1} \Longrightarrow_G^*$$

$$\Longrightarrow_G^* \dots \Longrightarrow_G^* p_1 q_1 p_2 q_2 \dots p_k X_k p_{k+1} \Longrightarrow_G^* p_1 q_1 p_2 q_2 \dots p_k q_k p_{k+1}$$

levezetésben p-nek X-ből való bal oldali levezetését kapjuk. Hasonlóan bizonyítható, hogy p jobbról is levezethető X-ből. □

A 3.14 Lemmából következik, hogy ha egy terminális szó levezethető egy környezetfüggetlen grammatikában, akkor balról [jobbról] is levezethető.

3.5. Rekurzív változók

A $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika $X \in V_N$ változóját (G-*ben*) *rekurzív*nak nevezzük, ha vannak olyan $P, Q \in (V_N \cup V_T)^*$ $(PQ \neq e)$ szavak, amelyekre $X \Longrightarrow_G^* PXQ$ levezetés teljesül. Ha $P = e$ $[Q = e]$, akkor azt mondjuk, hogy X (G-*ben*) *balrekurzív* [*jobbrekurzív*]. Ha G-ben van

$$X \longrightarrow PXQ \quad P, Q \in (V_N \cup V_T)^*, \quad PQ \neq e$$

alakú szabály, akkor azt mondjuk, hogy X *közvetlenül rekurzív*. Hasonlóan beszélünk *közvetlenül balrekurzív* [*jobbrekurzív*] változóról. A fenti definícióból következik, hogy minden közvetlenül [bal, jobb] rekurzív változó [bal, jobb] rekurzív.

3.15. Tétel. *A szigorúan e-mentes és redukált $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikára $L(G)$ akkor és csak akkor végtelen, ha G-nek van rekurzív változója.*

Bizonyítás Legyen X a G grammatika egy rekurzív változója. Akkor vannak olyan $P, Q \in (V_N \cup V_T)^*$ $(PQ \neq e)$ szavak, amelyekre $X \Longrightarrow_G^* PXQ$. A G grammatika redukált, ezért vannak olyan $P', Q' \in (V_N \cup V_T)^*$, hogy

$$S \Longrightarrow_G^* P'XQ' \Longrightarrow_G^* p'vq',$$

ahol

$$P' \Longrightarrow_G^* p', \quad X \Longrightarrow_G^* v \quad Q' \Longrightarrow_G^* q' \quad (p', v, q' \in V_T^*).$$

S így

$$S \Longrightarrow_G^* P'P^kXQ^kQ' \Longrightarrow_G^* p'p^kvq^kq', \quad (k \in N_+)$$

ahol

$$P \Longrightarrow_G^* p, \quad Q \Longrightarrow_G^* q, \quad (p, q \in V_T^*).$$

De G szigorúan e-mentes, így $pq \neq e$. Ez azt jelenti, hogy $p'p^kvq^kq' \in L(G)$ minden pozitív egész k számra, vagyis $L(G)$ végtelen.

Tegyük fel most, hogy G-nek nincs rekurzív változója. Akkor egy levezetés során minden szabály legfeljebb egyszer alkalmazható. Ha $|H| = n$, akkor az első lépést S-ből legfeljebb n féleképpen tehető meg. Minden első lépés után legfeljebb $(n-1)$ féleképpen tehető meg a második lépés. Ezt folytatva, nem nehéz belátni, hogy S-ből legfeljebb $n!$ terminális szó vezethető le, azaz $L(G)$ véges. □

A tételből következik, hogy rekurzív változóval rendelkező redukált grammatikával ekvivalens grammatikák is rendelkeznek rekurzív változóval. Ezt úgy is mondjuk, hogy grammatikák ekvivalens átalakítása nem szünteti meg a rekurziót. Olyan algoritmus azonban van, amely kiküszöböli a balrekurziót [jobbrekurziót]. Ezt az eljárást használják környezetfüggetlen grammatikák szintaktikus elemzésénél is. Természetesen az átalakított grammatikában nem szűnik meg a rekurzió. Mi most csak olyan algoritmust ismertetünk, amely a közvetlen balrekurziót szünteti meg. Ennek segítségével megadjuk a 2 típusú grammatikák egy újabb normálformáját. A balrekurzió megszüntetésére vonatkozó algoritmust találhatunk például Fülöp Zoltán már említett [18] egyetemi jegyzetében.

3.16. Lemma. *Legyen X a $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika közvetlenül balrekurzív változója, és legyenek az X baloldalú szabályok*

$$X \longrightarrow XP_1, \quad X \longrightarrow XP_2, \ldots, X \longrightarrow XP_k,$$

$$X \longrightarrow Q_1, \quad X \longrightarrow Q_2, \ldots, X \longrightarrow Q_l,$$

ahol $Q_1, Q_2, \ldots, Q_l$ *egyike sem kezdődik az* X *változóval. Legyen továbbá* $X' \notin V_N \cup V_T$ *és* $V'_N = V_N \cup \{X'\}$. *Az*

$$X \longrightarrow XP_1, \quad X \longrightarrow XP_1, \ldots, X \longrightarrow XP_k$$

szabályokat cseréljük ki a H*-ban az*

$$X' \longrightarrow P_1X', \quad X' \longrightarrow P_2X', \ldots, X' \longrightarrow P_kX',$$

$$X \longrightarrow Q_1X', \quad X \longrightarrow Q_2X', \ldots, X \longrightarrow Q_lX',$$

$$X' \longrightarrow P_1, \quad X' \longrightarrow P_2, \ldots, X' \longrightarrow P_k$$

szabályokkal. Ha az így kapott szabályok halmaza H' *és* $G' = (V'_N, V_T, S, H')$, *akkor* $L(G) = L(G')$ *és* X *nem közvetlenül balrekurzív* G'*-ben.*

Bizonyítás Az új szabályok definíciójából nyilvánvaló, hogy G'-ben X nem közvetlenül balrekurzív. Megmutatjuk, hogy $L(G) = L(G')$.

Először azt mutatjuk meg, hogy $L(G) \subseteq L(G')$. Azok a G-beli levezetések, amelyek nem tartalmazzák X-et G'-ben is elvégezhetők, ezért elegendő olyan levezetéseket tekinteni, amelyekben előfordul az X változó. Ha egy ilyen levezetés tartalmazza a lépések

$$PXQ \Longrightarrow_G PXP_{i_1}Q \Longrightarrow_G \ldots \Longrightarrow_G PXP_{i_m} \ldots P_{i_1}Q \Longrightarrow_G PQ_jP_{i_m} \ldots P_{i_1}Q$$

sorozatát, ahol

$$P, Q \in (V_N \cup V_T)^*, \quad 1 \leq i_1, \ldots, i_m \leq k, \quad 1 \leq j \leq l,$$

akkor az újonnan bevezetett szabályok segítségével megadható helyette a lépések

$$PXQ \Longrightarrow_{G'} PQ_jX'Q \Longrightarrow_{G'} PQ_jP_{i_m}X'Q \Longrightarrow_{G'} \ldots \Longrightarrow_{G'}$$
$$\Longrightarrow_{G'} PQ_jP_{i_m} \ldots P_{i_2}X'Q \Longrightarrow_{G'} PQ_jP_{i_m} \ldots P_{i_1}Q$$

sorozata. Ha a levezetésben mindenütt elvégezzük ezeket a helyettesítéseket, akkor egy G'-beli levezetést kapunk, ami azt jelenti, hogy $L(G) \subseteq L(G')$.

Most megmutatjuk, hogy $L(G') \subseteq L(G)$. Ekkor is elegendő azokat a levezetéseket megvizsgálni, amelyekben X' előfordul. Az X' változót tartalmazó szabályok definíciója miatt X' csak úgy lehet egy G'-beli levezetésben, ha X is szerepel ebben a levezetésben. Pontosabban, ha egy G'-beli levezetés tartalmazza az X' változót, akkor tartalmaz egy

$$PXQ \Longrightarrow_{G'} PQ_jX'Q \Longrightarrow_{G'} PQ_jP_{i_1}X'Q \Longrightarrow_{G'} \ldots \Longrightarrow_{G'}$$

$$\Longrightarrow_{G'} PQ_jP_{i_1}\dots P_{i_{m-1}}X'Q \Longrightarrow_{G'} PQ_jP_{i_1}\dots P_{i_m}Q,$$
$$P,Q \in (V'_N \cup V_T)^*, \quad 1 \le j \le l, \quad 1 \le i_1,\dots,i_m \le k, \quad 1 \le m$$

lépéssorozatot is. Ez helyettesíthető a G-beli

$$PXQ \Longrightarrow_G PXP_{i_m}Q \Longrightarrow_G \dots \Longrightarrow_G PXP_{i_1}\dots P_{i_m}Q \Longrightarrow_G PQ_jP_{i_1}\dots P_{i_m}Q$$

lépéssorozattal. Ha a levezetésben mindenütt elvégezzük ezeket a helyettesítéseket, akkor egy G-beli levezetéshez jutunk, azaz $L(G') \subseteq L(G)$. □

A 3.16 Lemma egy algoritmust ad a redukált 2 típusú grammatikák közvetlen balrekurziójának megszüntetésére. Alkalmazzuk sorra a balrekurzív változókra a lemmában szereplő helyettesítéseket. Ez annyi új változó bevezetését jelenti, amennyi a balrekurzív változók száma. Az új szabályok definíciójából látható, hogy az új változók közvetlenül jobbrekurzív változók az új grammatikában.

3.6. Greibach normálforma

A $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikáról azt mondjuk, hogy *Greibach normálformá*ban van megadva, ha minden szabálya

$$X \longrightarrow xP \quad (X \in V_N, \quad x \in V_T, \quad P \in V_N^*)$$

alakú.

Ez a normálforma bizonyos analógiát mutat a 3 típusú grammatikákkal. Lényeges különbség azonban, hogy P egynél több változóból is állhat. Ha ugyanis a Greibach normálforma további finomításával elérhető lenne, hogy a szabályok jobb oldalán mindig legfeljebb egy változó szerepeljen, akkor ez azt jelentené, hogy az $\mathcal{L}_3$ reguláris nyelvosztály megegyezne az $\mathcal{L}_2$ környezetfüggetlen nyelvosztállyal. Ezt azonban később kimutatjuk, hogy nem igaz. A definíció alapján könnyen belátható, hogy a Greibach normálformájú grammatikában nincs balrekurzív változó. Egy Greibach normálformában megadott G grammatikában egy $p \in L(G)$ szó levezetése pontosan $|p|$ lépésből áll.

3.17. Példa. *Tekintsük a Greibach normálformában megadott*

$$G = (\{S, X, Y\}, \{a, b\}, S, H)$$

grammatikát, amelynek a szabályai:

$$S \longrightarrow aYX,\ X \longrightarrow aY,\ X \longrightarrow b,\ Y \longrightarrow b.$$

A 3.14 Lemma szerint az

$$S \Longrightarrow aYX \Longrightarrow abX \Longrightarrow abb,$$

$$S \Longrightarrow aYX \Longrightarrow abX \Longrightarrow abaY \Longrightarrow abab$$

bal oldali levezetések mutatják, hogy $L(G) = \{abb, abab\}$. *Az abb szó levezetése* 3 *lépésből, az abab szó levezetése pedig* 4 *lépésből áll.*

3.18. Tétel. *Szigorúan e-mentes környezetfüggetlen grammatikához van vele ekvivalens Greibach normálformában megadott grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ szigorúan e-mentes környezetfüggetlen grammatika. A 3.3 Tétel szerint G megadható Chomsky normálformában. Vezessünk be a V_N halmazon egy tetszőleges $\leq$ rendezést. Legyen

$$X_1 < X_2 < \cdots < X_n \quad (n = |V_N|).$$

Először olyan átalakításokat végzünk, amellyel elérjük, hogy a szabályok jobb oldala terminálissal vagy a bal oldalon lévő változónál nagyobb változóval kezdődjön. Induljunk ki azokból a szabályokból, amelyek bal oldala X_1. Ha X_1 nem közvetlenül balrekurzív, akkor ezek a szabályok megfelelnek a követelményeknek.

Ha X_1 közvetlenül balrekurzív, akkor a végezzük el a szabályokban a 3.16 Lemma szerinti átalakításokat. A bevezetett új változót jelölje X_1', és legyen $X_1' < X_1$. Így az X_1' és az X_1 bal oldalú szabályok jobb oldala nem kezdődik X_2-nél kisebb változóval.

Térjünk át az X_2 bal oldalú szabályokra. Az $X_2 \longrightarrow X_1X_j$ alakú szabályokat cseréljük ki az összes $X_2 \longrightarrow PX_j$ alakú szabályra, ahol $X_1 \longrightarrow P$ alakú szabályok az előző lépések során kapott X_1 bal oldalú szabályok. Ezzel elérjük, hogy a kapott szabályok jobb oldala terminálissal vagy X_2-nél nem kisebb változóval kezdődik. Ha így azt kapjuk, hogy X_2 közvetlenül balrekurzív, akkor a végezzük el a szabályokban ismét a 3.16 Lemma szerinti átalakításokat. Legyen az új változó X_2'. Ha X_1'-t definiáltuk, akkor legyen $X_2' < X_1'$, ha pedig nem, akkor legyen $X_2' < X_1$. Így az X_2' és az X_2 bal oldalú szabályok jobb oldala nem kezdődik X_3-nél kisebb változóval.

Legyen $1 \leq k \leq n$. Tegyük fel, hogy minden X_k-nál kisebb változóra már teljesül, hogy ha egy szabály bal oldala X_k-nál kisebb változó, akkor a szabály jobb oldala terminálissal vagy ennél a változónál nagyobb változóval kezdődik. Az $X_k \longrightarrow X_lX_j$ $(1 \leq l < k)$ alakú szabályokat cseréljük ki az összes $X_k \longrightarrow PX_j$ alakú szabályra, ahol $X_l \longrightarrow P$ alakú szabályok az előző lépések során kapott X_l bal oldalú szabályok. Ezzel elérjük, hogy a kapott szabályok jobb oldala terminálissal vagy X_k-nál nem kisebb változóval kezdődik.

Ha X_k közvetlenül balrekurzív, akkor a végezzük el a szabályokban ismét a 3.16 Lemma szerinti átalakításokat. Legyen az új változó X'_k és X'_k legyen a legkisebb a változók között. Így az X'_k és az X_k bal oldalú szabályok jobb oldala nem kezdődik X_{k+1}-nél kisebb változóval.

Ha $k < n$, akkor ebben az esetben is folytatjuk az eljárást X_{k+1}-gyel. Ha $k = n$, akkor ebben az esetben is a kapott szabályok jobb oldala terminálissal kezdődik. Az eljárás $k = n$ esetben befejeződik. Átalakítottuk a grammatika szabályait úgy, hogy a szabályok jobb oldala terminálissal vagy a bal oldalon lévő változónál nagyobb változóval kezdődik.

Ezután visszafelé haladunk. Jelöljük az eljárás során kapott új változók halmazát V-vel. Az X_{n-1} baloldalú szabályok $X_{n-1} \longrightarrow xP$ vagy $X_{n-1} \longrightarrow X_nQ$ alakúak, ahol $x \in V_T$ és $P, Q \in (V_N \cup V)^*$. Az $X_{n-1} \longrightarrow X_nQ$ szabályokat cseréljük ki az $X_{n-1} \longrightarrow xRQ$ alakú szabályok összességével, ahol xRQ-t egy

$$X_n \longrightarrow xR \quad (x \in V_T, R \in (V_N \cup V)^*)$$

helyettesítéssel kaptuk.

Ha már minden $n-k < l$ $(1 \leq k \leq n-1)$ esetén az X_l bal oldalú szabályok

$$X_l \longrightarrow xP \quad (x \in V_T, R \in (V_N \cup V)^*)$$

alakúak, akkor vegyük az X_{n-k} bal oldalú szabályokat. Ezek $X_{n-k} \longrightarrow yP$ vagy $X_{n-k} \longrightarrow X_lQ$ alakúak, ahol $n-k < l$, $y \in V_T$ és $P, Q \in (V_N \cup V)^*$. Az $X_{n-k} \longrightarrow X_lQ$ alakú szabályokat cseréljük ki az $X_{n-k} \longrightarrow xPQ$ szabályok összességére.

Legyen az így kapott szabályok halmaza H'. A $G' = (V_N \cup V, V_T, S, H')$ grammatika Greibach normálformájú. A 3.16 Lemmát is felhasználva, nem nehéz meggyőződni arról, hogy minden lépésben ekvivalens átalakításokat hajtottunk végre. Ez azt jelenti, hogy $L(G) = L(G')$. □

A Greibach normálforma segítségével egy eljárást kapunk a balrekurzió megszüntetésére. A 3.1 Lemma bizonyításában látott módon tetszőleges környezetfüggetlen grammatikához megszerkeszthetünk egy ekvivalens e-mentes környezetfüggetlen grammatikát. A 3.12 Tétel alapján ez redukálttá tehető. Ha a kapott grammatika tartalmazza az $S \longrightarrow e$ szabályt, akkor ezt a szabályt törölve egy szigorúan e-mentes és redukált környezetfüggetlen grammatikát kapunk. A 3.18 Tétel bizonyításában látott módon ez Greibach normálformára hozható. Az esetleg törölt $S \longrightarrow e$ szabályt visszaírva az eredeti grammatikával ekvivalens grammatikát kapunk, amely nem tartalmaz balrekurzív változót.

3.19. Példa. *Tekintsük a Chomsky normálformában megadott*

$$G = (\{S, X, Y\}, \{a, b\}, S, H)$$

grammatikát, amelynek a szabályai:

$$S \longrightarrow XY,\ X \longrightarrow SY,\ Y \longrightarrow YY,\ X \longrightarrow a,\ Y \longrightarrow b.$$

A 3.18 Tétel bizonyításában közölt algoritmussal megadunk egy vele ekvivalens Greibach normálformájú garmmatikát. (Nem nehéz belátni, hogy $L(G) = ab^+$.)

Vezessük be az $S < X < Y$ rendezést. (A rendezés megadása tetszőleges. Más rendezés esetén általában más, de ekvivalens Greibach normálformát kapunk.) Az

$$S \longrightarrow XY$$

szabály S-nél nagyobb változóval kezdődik, ezért áttérhetünk az

$$X \longrightarrow SY, \quad X \longrightarrow a$$

szabályokra. Az $X \longrightarrow SY$ szabály helyett tekintsük az $X \longrightarrow XYY$ szabályt. Az X változó balrekurzív, ezért elvégezzük a 3.16 Lemma szerinti átalakításokat, vagyis az $X \longrightarrow XYY$ szabály helyett az

$$X' \longrightarrow YYX', \quad X' \longrightarrow YY, \quad X \longrightarrow aX'$$

szabályokat tekintjük, ahol X' egy új változó. Tegyük fel, hogy $X' < S$.

Most áttérhetünk az

$$Y \longrightarrow YY,\ Y \longrightarrow b$$

szabályokra. Az Y változó is balrekurzív, így a 3.16 Lemma alapján a $Y \longrightarrow YY$ szabály helyett tekintsük az

$$Y' \longrightarrow YY', \quad Y' \longrightarrow Y, \quad Y \longrightarrow bY'$$

szabályokat, ahol Y' ismét egy új változó. Legyen $Y' < X'$.

Az eljárás eddigi alkalmazásával a következő szabályokhoz jutottunk a változók megadott rendezésével fordított sorrendben:

$$Y \longrightarrow bY', \quad Y \longrightarrow b,$$

$$X \longrightarrow aX', \quad X \longrightarrow a,$$

$$S \longrightarrow XY,$$

$$X' \longrightarrow YYX', \quad X' \longrightarrow YY,$$

$$Y' \longrightarrow YY', \quad Y' \longrightarrow Y.$$

Az eljárás szerint az Y és az X baloldalú szabályok megfelelnek a követelményeknek. Az $S \longrightarrow XY$ szabály helyett tekintsük az

$$S \longrightarrow aX'Y, \quad S \longrightarrow aY$$

szabályokat. (Végezzük el a szabály jobb oldalán az első változóban az X bal oldalú szabályokkal a helyettesítést.) Ha az X' és Y' bal oldalú szabályok jobb oldalán is elvégezzük az első változóban a lehetséges helyettesítéseket, akkor a G-vel ekvivalens $G' = (\{S, X, Y, X', Y'\}, \{a, b\}, S, H')$ Greibach normálformában megadott grammatikához jutunk, amelynek H'-beli szabályai:

$$Y \longrightarrow bY', \quad Y \longrightarrow b,$$

$$X \longrightarrow aX', \quad X \longrightarrow a,$$

$$S \longrightarrow aX'Y, \quad S \longrightarrow aY,$$

$$X' \longrightarrow bY'YX', \quad X' \longrightarrow bY'Y, \quad X' \longrightarrow bYX', \quad X' \longrightarrow bY,$$

$$Y' \longrightarrow bY'Y', \quad Y' \longrightarrow bY', \quad Y' \longrightarrow b.$$

3.7. Reguláris környezetfüggetlen nyelvek

A 3.19 Példában szereplő ab^+ nyelv reguláris. A nyelv generálható az egyszerűbb Greibach normálformában megadott $G = (\{S, X\}, \{a, b\}, S, H)$ reguláris grammatikával is, amelynek a szabályai:

$$S \longrightarrow aX, \quad X \longrightarrow bX, \quad X \longrightarrow b.$$

Most egy szükséges és elegendő feltételt adunk arra, hogy egy környezetfüggetlen nyelv mikor reguláris.

Egy $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatikát *önbeágyazó*nak nevezünk, ha van olyan $X \in V_N$ rekurzív nemterminálisa, amely nem balrekurzív és nem jobbrekurzív, azaz

$$X \Longrightarrow_G^* PXQ$$

teljesül valamilyen $P, Q \in (V_N \cup V_T)^+$ nemüres szavakra. Az L környezetfüggetlen nyelvet *önbeágyazó*nak mondjuk, ha minden olyan környezetfüggetlen grammatika, amely L-et generálja önbeágyazó.

3.20. Tétel. *Egy környezetfüggetlen nyelv akkor és csak akkor reguláris, ha nem önbeágyazó.*

Bizonyítás A reguláris grammatikák definícójából következik, hogy nincsen önbeágyazó reguláris grammatika. Ezért minden reguláris nyelv generálható nem önbeágyazó környezetfüggetlen grammatikával.

Megfordítva, legyen a $G = (V_N, V_T, S, H)$ környezetfüggetlen grammatika nem önbeágyazó. Ha $L(G) = \emptyset$ vagy $L(G) = e$, akkor van G-vel ekvivalens reguláris grammatika. (Például tetszőleges $V_T \neq \emptyset$ teminális ábécé esetén a $G = (\{S\}, V_T, S, \{S \longrightarrow S\})$ reguláris grammatika $\emptyset$-t, a $G = (\{S\}, V_T, S, \{S \longrightarrow e\})$ reguláris grammatika pedig e-t generálja.) Ezért feltehetjük, hogy $L(G) \neq \emptyset, e$ A 3.12 Tétel szerint azt is feltehetjük, hogy G redukált. Így minden $X \in V_N$ változó elérhető, azaz létezik egy

$$S \Longrightarrow_G^* VXW, \quad V, W \in (V_N \cup V_T)^*$$

alakú levezetés. Először tegyük fel, hogy minden $Y \in V_N$ változóhoz van

$$Y \Longrightarrow_G^* RST \quad R, T \in (V_N \cup V_T)^*$$

alakú levezetés. Nevezzük el ezeket a grammatikákat *elsőfajúak*nak. Megmutatjuk, hogy minden elsőfajú grammatika reguláris. Azok a szabályok, amelyek jobb oldala nem csupán terminális jeleket tartalmaz,

$$X \longrightarrow PYQ \quad X, Y \in V_N, \quad P, Q \in (V_N \cup V_T)^*$$

alakúak. Ha $P \neq e$ és $Q \neq e$, akkor

$$X \Longrightarrow_G PYQ \Longrightarrow_G^* PRSTQ \Longrightarrow_G^* PRVXWTQ,$$

ami ellentétben áll azzal, hogy G nem önbeágyazó. Ha H-ban vannak

$$X_1 \longrightarrow PY_1, \quad X_2 \longrightarrow Y_2Q, \quad X_1, X_2, Y_1, Y_2 \in V_N, \quad P, Q \in (V_N \cup V_T)^+$$

alakú szabályok, akkor

$$X_1 \Longrightarrow_G PY_1 \Longrightarrow_G^* PR_1ST_1 \Longrightarrow_G^* PR_1V_2X_2W_2T_1 \Longrightarrow_G^*$$

$$\Longrightarrow_G^* PR_1V_2Y_2QW_2T_1 \Longrightarrow_G^* PR_1V_2R_2ST_2QW_2T_1 \Longrightarrow_G^*$$

$$\Longrightarrow_G^* PR_1V_2R_2V_1X_1W_1T_2QW_2T_1,$$

ami szintén ellentétes azzal, hogy G nem önbeágyazó.

Tegyük fel, hogy minden H-beli szabály, amely jobb oldalán nem csupán terminálist tartalmaz,

$$X \longrightarrow PY \quad X, Y \in V_N, \ P \in (V_N \cup V_T)^*$$

alakú. Tartalmazzon P legalább egy $Z \in V_N$ nemterminálist. A P szó

$$P = P_1 Z P_2, \quad P_1, P_2 \in (V_N \cup V_T)^*, \quad P_1 \neq e$$

alakú nem lehet, mert akkor a szabály $X \longrightarrow PY = P_1 Z P_2 Y$ alakú, ahol $P_1 \neq e$ és $P_2 Y \neq e$, és már bebizonyítottuk, hogy H ilyen alakú szabályt nem tartalmazhat. Ha $P = ZQ$ $(Q \in (V_N \cup V_T)^*)$, akkor

$$X \Longrightarrow_G PY = ZQY \Longrightarrow_G^* ASBQRST \Longrightarrow_G^*$$

$$\Longrightarrow_G^* AVXWBQRVXWT \Longrightarrow_G^* AVPYWBQRVPYWT \Longrightarrow_G^*$$
$$\Longrightarrow_G^* AVPRSTWBQRPYWT \Longrightarrow_G^* AVPRVXWTWBQRPYWT,$$

ami ismét lehetetlen. azaz $P \in V_T^*$. Hasonlóan látható be, hogy ha minden a H-beli szabály, amely jobb oldalán nem csupán terminálist tartalmaz,

$$X \longrightarrow YQ \quad X, Y \in V_N,\ Q \in (V_N \cup V_T)^*$$

alakú, akkor $Q \in V_T^*$. Tehát G jobb vagy bal lineáris grammatika, ami a 2.7 Tétel szerint azt jelenti, hogy reguláris.

Ezek után, az elsőfajú grammatikák felhasználásával a nemterminálisok $|V_N| = n$ száma szerinti teljes indukcióval bebizonyítjuk, hogy minden nem önbeágyazó környezetfüggetlen $G = (V_N, V_T, S, H)$ grammatikához van vele ekvivalens reguláris grammatika. Ha $n = 1$, akkor $V_N = \{S\}$. Definíció szerint $S \Longrightarrow_G^* S$, ezért a G elsőfajú, s így reguláris. Tegyük fel, hogy n nemterminálist tartalmazó grammatikákra az állítás igaz. Legyen $|V_N| = n + 1$. Ha G elsőfajú, akkor nyilván reguláris. Tegyük fel, hogy G nem elsőfajú. Akkor tartalmaz olyan $A \in V_N$ nemterminálist, amelyre $A \Longrightarrow_G^* PSQ$ levezetés semmilyen $P, Q \in (V_N \cup V_T)^*$ mellett sem teljesül. ($A = S$ nem lehetséges, hiszen definíció szerint $S \Longrightarrow_G^* S$.) Tekintsük a

$$G_1 = (V_N - S, V_T, A, H_1)$$

grammatikát, amelyben H_1-et úgy kapjuk H-ból, hogy elhagyjuk belőle azokat a szabályokat, amelyekben S előfordul. Vegyük továbbá a

$$G_2 = (V_N - A, V_T \cup A, S, H_2)$$

grammatikát, amelyben H_2-t úgy kapjuk H-ból, hogy elhagyjuk belőle azokat a szabályokat, amelyek bal oldalán A szerepel. (Tehát ebben az esetben A-t terminálisnak tekintjük.) Mivel $H_1, H_2 \subset H$, ezért G_1 és G_2 egyike sem önbeágyazó. Az indukciós feltevés szerint mind a két grammatika reguláris.

Léteznek tehát olyan $G' = (V'_N, V_T, S', H')$ és $G'' = (V''_N, V_T \cup A, S'', H'')$ reguláris grammatikák, amelyekre $L(G_1) = L(G')$ ill. $L(G_2) = L(G'')$. Feltehetjük továbbá, hogy $V'_N \cap V''_N = \emptyset$. Vegyük most a

$$\tilde{G} = (V'_N \cup V''_N \cup A, V_T, S'', H' \cup H'' \cup \{A \longrightarrow S'\})$$

grammatikát. Nyilvánvalóan $\tilde{G}$ is reguláris. Megmutatjuk, hogy $L(G) = L(\tilde{G})$. Ha ugyanis $p \in L(G)$, akkor vagy $p \in L(G_2) = L(G'')$, vagy az $S \Longrightarrow^*_G p$ levezetésben valahol előfordul A. Mindkét esetben $p \in L(\tilde{G})$. Megfordítva, ha $p \in L(\tilde{G})$, akkor az $S'' \Longrightarrow^*_{\tilde{G}} p$ levezetésben vagy csak H''-beli szabályokat alkalmazunk, vagy legalább egyszer alkalmazzuk az $A \longrightarrow S'$ szabályt. Az első esetben $p \in L(G'') \cap V_T^* \subset L(G)$, a második esetben a szabályok alkalmazásának sorrendjét mindig megválaszthatjuk úgy, minden H''-beli szabály alkalmazása megelőzze minden H'-beli szabály alkalmazását. Eszerint a kérdéses levezetés

$$S'' \Longrightarrow^*_{\tilde{G}} p_1 A p_2 A \dots p_{k-1} A p_k \Longrightarrow^*_{\tilde{G}} p_1 q_1 p_2 q_2 \dots p_{k-1} q_{k-1} p_k = p$$

alakban írható, ahol $p_j, q_j \in V_T^*$. Amellett nyilván

$$p_1 A p_2 A \dots p_{k-1} A p_k \in L(G_2), \quad q_j \in L(G_1),$$

amiből $p \in L(G)$ következik. □

3.8. Homomorf jellemzés

A továbbiakban megmutatjuk, hogy minden környezetfüggetlen nyelv előállítható egy reguláris nyelv és egy speciális környezetfüggetlen nyelv közös részének homomorf képeként. Ezt úgy is mondjuk, hogy minden 2 típusú nyelv *homomorfan jellemezhető* (*karakterizálható*) egy reguláris nyelv és egy speciális 2 típusú nyelv közös részével.

Tekintsük a $G = (\{S\}, V_n, S, H)$ környezetfüggetlen grammatikát, ahol

$$V_n = \{a_1, a'_1, a_2, a'_2, \dots, a_n, a'_n\} \quad (n \geq 1)$$

és a H-beli szabályok

$$S \longrightarrow e, \quad S \longrightarrow SS, \quad S \longrightarrow a_i S a'_i \quad (i = 1, 2, \dots n).$$

A $D_n = L(G)$ nyelvet a (V_n *ábécé feletti*) *Dyck nyelv*nek nevezzük. D_n azokból a szavakból áll, amelyekben sorra törölve az $a_i a'_i$ alakú részszavakat, végül az üres szót kapjuk. Ha $p, q \in D_n$, akkor $pq \in D_n$, vagyis D_n a V_n^* szabad monoid részmonoidja. Nem nehéz belátni, hogy ha $p \in D_n$, akkor minden

$a, a' \in V$ esetén $apa' \in V_n$. Továbbá minden D_n-beli $p \neq e$ szó felírható $p = ap_1a'p_2$ $(a, a' \in V,\ p_1, p_2 \in D_n)$ alakban. Ha $aa'q \in D_n$ $(a, a' \in V)$, akkor $q \in D_n$. Ha a_i és a'_i $(i = 1, 2, \ldots, n)$ az egymásnak megfelelő különböző bal és jobb oldali zárójeleket jelöli, akkor azt is mondhatjuk, hogy D_n a *zárójelek nyelve.*

3.21. Tétel. *Minden környezetfüggetlen nyelv homomorf képe egy reguláris nyelv és egy Dyck nyelv közös részének.*

Bizonyítás Legyen L egy környezetfüggetlen nyelv. Ha $e \in L$ és $L - e = \varphi(D \cap R)$, ahol R egy reguláris nyelv, D egy Dyck nyelv, φ egy homomorfizmus, akkor $L = \varphi(D \cap (R \cup e))$ Következésképpen feltehetjük, hogy $e \notin L$. A 3.1 Lemma és a 3.3 Tétel szerint így azt is feltehetjük, hogy ha $L = L(G)$, akkor a $G = (V_N, V_T, S, H)$ grammatika Chomsky normálformában van megadva.

Legyen $V_T = \{a_1, a_2, \ldots, a_n\}$, s legyenek a terminálisokat nem tartalmazó szabályok az

$$X_i \longrightarrow Y_iZ_i \quad (i = 1, 2, \ldots, k)$$

szabályok. (Természetesen az X_i, Y_i, Z_i változók között lehetnek egyenlők is.) Vezessük be az

$$a_{n+1}, \ldots, a_{n+k}, a'_1, \ldots, a'_n, a'_{n+1}, \ldots, a'_{n+k} \notin V_N \cup V_T$$

új terminálisokat és tekintsük a

$$V_{n+k} = \{a_1, a'_1, a_2, a'_2, \ldots, a_{n+k}, a'_{n+k}\}$$

ábécét. (Az a_{n+i} jeleket *bal zárójelek*nek, az a'_{n+i} jeleket pedig *jobb zárójelek*nek is nevezzük.) Legyen D_{n+k} a V_{n+k} ábécé feletti Dyck nyelv. Definiáljuk a $\varphi : V_{n+k} \to V_T$ leképezést a következő módon:

$$\varphi(a_i) = a_i \quad (i = 1, 2, \ldots, n),$$

$$\varphi(a_i) = \varphi(a'_j) = e \quad (i = n + 1, \ldots, n + k,\ j = 1, 2, \ldots, n + k).$$

Terjesszük ki φ-t V^*_{n+k}-nak V^*_T-ra való monoid-homomorfizmusává. Jelölje a kiterjesztést ugyancsak φ.

Végül tekintsük a $G_1 = (V_N, V_{n+k}, S, H_1)$ grammatika által generált R nyelvet, ahol

$$H_1 = \{X \longrightarrow aa'; X \longrightarrow a \in H\} \cup$$
$$\cup \{X \longrightarrow aa'a'_{n+i}Z_i; X \longrightarrow a \in H,\ i = 1, 2, \ldots, k\} \cup$$
$$\cup \{X_i \longrightarrow a_{n+i}Y_i; X_i \longrightarrow Y_iZ_i \in H,\ i = 1, 2, \ldots, k\}.$$

Az $R = L(G_1)$ nyelv nyilvánvalóan reguláris.

Megmutatjuk, hogy $L = \varphi(D_{n+k} \cap R)$. Először belátjuk, hogy $L \subseteq \varphi(D_{n+k} \cap R)$. Ehhez elegendő megmutatni, hogy ha $p \in L$ és valamely $X \in V_N$ változóra $X \Longrightarrow_G^* p$, akkor van olyan $q \in D_{n+k} \cap R$, amelyre $\varphi(q) = p$ és $X \Longrightarrow_{G_1}^* q$. Ezt a levezetés t hossza szerinti teljes indukcióval mutatjuk meg. A 3.14 Lemma szerint feltehetjük, hogy a levezetések bal oldali levezetések.

Ha $t = 1$, akkor $X \longrightarrow p \in H$ és $p \in V_T$. Következésképpen $X \longrightarrow pp' \in H_1$. Így $pp' \in D_{n+k} \cap R$ és

$$\varphi(pp') = \varphi(p)\varphi(p') = pe = p.$$

Tegyük fel, hogy minden t-nél nem hosszabb levezetésre igaz az állítás. Legyen az $X \Longrightarrow_{G,b}^* p$ levezetés $t+1$ hosszúságú. Mivel G Chomsky normálformában van megadva, ezért a levezetés első lépése egy $X_i \longrightarrow Y_i Z_i$ $(1 \leq i \leq k)$ szabály alkalmazása, ahol $X_i = X$. Ebből következik, hogy $p = p_1 p_2$ és

$$Y_i \Longrightarrow_{G,b}^* p_1, \quad Z_i \Longrightarrow_{G,b}^* p_2$$

t-nél nem hosszabb levezetések. Az indukciós feltevés miatt vannak olyan $q_1, q_2 \in D_{n+k} \cap R$, amelyekre

$$\varphi(q_1) = p_1, \quad Y_i \Longrightarrow_{G_1,b}^* q_1, \quad \varphi(q_2) = p_2, \quad Z_i \Longrightarrow_{G_1,b}^* q_2.$$

Mivel $X \longrightarrow Y_i Z_i \in H$, ezért $X \longrightarrow a_{m+i} Y_i \in H_1$. Következésképpen

$$X \Longrightarrow_{G_1,b} a_{n+i} Y_i \Longrightarrow_{G_1,b}^* a_{n+i} q_1 a'_{n+i} Z_i \Longrightarrow_{G_1,b}^* a_{n+i} q_1 a'_{n+i} q_2.$$

(Az $Y_i \Longrightarrow_{G_1,b}^* q_1$ bal oldali levezetés utolsó lépésében egy $Y \longrightarrow aa'$ típusú szabályt kell alkalmazni. Az előbbi levezetésben ehelyett az $Y \longrightarrow aa'Z_i$ szabályt alkalmaztuk.) Minthogy $q_1, q_2 \in D_{n+k} \cap R$, így $a_{n+i} q_1 a'_{n+i} q_2 \in D_{n+k} \cap R$ és

$$\varphi(a_{n+i} q_1 a'_{n+i} q_2) = \varphi(a_{n+i})\varphi(q_1)\varphi(a'_{n+i})\varphi(q_2) = e p_1 e p_2 = p_1 p_2 = p.$$

Az $\varphi(D_{n+k} \cap R) \subseteq L$ fordított tartalmazás bizonyításához elegendő megmutatni, hogy ha $q \in D_{n+k} \cap R$ és valamely $X \in V_N$ változóra $X \Longrightarrow_{G_1,b}^* q$, akkor $X \Longrightarrow_{G,b}^* \varphi(q)$. Ezt is a levezetés t hossza szerinti teljes indukcióval mutatjuk meg.

Ha $t = 1$, akkor $q = aa'$ $(a \in V_T)$. Ebből $X \longrightarrow a = \varphi(q) \in H$, s így $X \Longrightarrow_G \varphi(q)$.

Tegyük fel, hogy minden t-nél nem hosszabb levezetésre igaz az állítás. Legyen $q \in D_{n+k} \cap R$ és az $X \Longrightarrow_{G_1,b}^* q$ levezetés $t+1$ hosszúságú. Mivel $t + 1 \geq 2$, ezért a levezetés első lépése nem lehet egy $X \longrightarrow aa'$ szabály alkalmazása. Megmutatjuk, hogy az első lépésként egy $X \longrightarrow aa'a'_{n+i}Z_i$ szabályt sem alkalmazhatunk. Ha ugyanis ilyen szabályt alkalmazunk, akkor

$$X \Longrightarrow_{G_1,b} aa'a'_{n+i}Z_i \Longrightarrow_{G_1,b}^* aa'a'_{n+i}r = q,$$

ahol $r \in V_{n+k}^*$ és $Z_i \Longrightarrow_{G_1,b}^* r$ egy t hosszúságú levezetés. A feltevés miatt $q = aa'a'_{n+i}r \in D_{n+k}$, amiből $a'_{n+i}r \in D_{n+k}$. Ez azonban lehetetlen. (A tétel előtti Dyck nyelvekre vonatkozó megjegyzések szerint.) Tehát

$$X \Longrightarrow_{G_1,b} a_{n+i}Y_i \Longrightarrow_{G_1,b}^* a_{n+i}r = q,$$

ahol $r \in V_{n+k}^*$ és $Y_i \Longrightarrow_{G_1,b} r$ egy t hosszúságú levezetés. (Az első lépésből következik, hogy $X \longrightarrow Y_iZ_i$ egy H-beli szabály.) Mivel $q = a_{n+i}r \in D_{n+k}$, ezért felírható $q = a_{n+i}q_1a'_{n+i}q_2$ $(q_1, q_2 \in D_{n+k})$ alakban. Ebből $r = q_1a'_{n+i}q_2$. Így

$$Y_i \Longrightarrow_{G_1,b}^* sY \Longrightarrow_{G_1,b} saa'a'_{n+i}Z_i \Longrightarrow_{G_1,b}^* q_1a'_{n+i}q_2 = r,$$

ahol $Y \longrightarrow aa'a_{n+i}Z_i$ H_1-beli szabályban a és a' ugyanaz, mint az

$$Y_i \Longrightarrow_{G_1,b}^* sY \Longrightarrow_{G_1,b} saa' = q_1$$

levezetésben szereplő $Y \longrightarrow aa'$ H_1-beli szabályban. Továbbá $Z_i \Longrightarrow_{G_1,b}^* q_2$. Mivel az $Y_i \Longrightarrow_{G_1,b}^* q_1$ és a $Z_i \Longrightarrow_{G_1,b}^* q_2$ levezetések hossza legfeljebb t, ezért az indukciós feltevés szerint

$$Y_i \Longrightarrow_{G,b}^* \varphi(q_1), \quad Z_i \Longrightarrow_{G,b}^* \varphi(q_2).$$

Innen

$$X \Longrightarrow_{G,b} Y_iZ_i \Longrightarrow_{G,b}^* \varphi(q_1)\varphi(q_2) = \varphi(a_{n+i}q_1a'_{n+i}q_2) = \varphi(q). \qquad \square$$

A 3.21 Tétel bizonyításában megadott V_{n+k} ábécé és így a D_{n+k} Dyck nyelv függ a G grammatikától, s ezért az L nyelvtől is. Azonban könnyen módosítható úgy a bizonyítás, hogy a Dyck nyelv csak egyedül a V_T terminális ábécétől függjön. Ehhez elegendő a

$$V'_T = \{a_1, a'_1, \ldots, a_n, a'_n, b, b', c, c'\}$$

ábécét tekinteni V_{n+k} helyett. Az a_{n+i} "bal zárójelet" helyettesítsük bc^ib-vel, az a_{n+i} "jobb zárójelet" pedig $b'(c')^ib'$-vel. Ebből megkapjuk a 3.21 Tétel egy erősebb változatát:

3.22. Tétel. *Minden V_T ábécéhez és a $2|V_T|+4$ elemű V'_T ábécé feletti D Dyck nyelvhez létezik a $(V'_T)^*$-nek egy φ monoid-homomorf leképezése V_T^*-ra, amelyre minden V_T feletti L környezetfüggetlen nyelvhez megadható olyan V'_T feletti R reguláris nyelv, hogy $L = \varphi(D \cap R)$.*

3.9. Környezetfüggetlen kifejezések

Az 1.1. alfejezetben megmutattuk, hogy a reguláris nyelvek reguláris kifejezésekkel is megadhatók. Az iteráció műveletéhez hasonló tulajdonságú egyváltozós műveletek bevezetésével elérhető, hogy a környezetfüggetlen nyelvek is megadhatók legyenek a reguláris kifejezésekhez hasonló ún. *környezetfüggetlen kifejezések*kel.

Legyen $u \in U$, valamint L és M tetszőleges nyelvek az U ábécé felett. Az *M nyelvnek az L nyelvbe való u-helyettesítés*én azt az U feletti nyelvet értjük, amely azokból és csak azokból a

$$q = p_1 q_1 p_2 q_2 \dots p_k q_k p_{k+1} \quad p_j, q_l \in U^*$$

szavakból áll, amelyekre

$$p = p_1 u p_2 u \dots p_k u p_{k+1} \in L, \quad q_1, q_2, \dots, q_k \in M,$$

és az u betű nem fordul elő a $p_1, p_2, \dots, p_{k+1}$ szavak egyikében sem. Az u-helyettesítés egy kétváltozós művelet a $P(U^*)$ halmazon. Jelöljük ezt a műveletet $\circ_u$-val, s az M nyelvnek az L nyelvbe való helyettesítését $L \circ_u M$-mel. A definícióból látható, hogy minden $u \in U$ betűre a $\circ_u$ művelet asszociatív.

A $\circ_u$ művelet segítségével bevezetjük egy tetszőleges U feletti L nyelv $\circ_u^n(L)$ *u-hatványá*t minden n pozitív egész kitevőre az

$$\circ_u^1(L) = L, \quad \circ_u^{n+1}(L) = (\circ_u^n(L)) \circ_u L$$

összefüggésekkel.

Végül az L nyelv *u-iteráltjá*n a nyelvek iteráltja fogalmának analógiájára azt az L^u nyelvet értjük, amely a

$$\sum_{n=1}^{\infty} \circ_u^n(L)$$

nyelvnek azokat a szavait tartalmazza, amelyekben u nem fordul elő. Ez egy egyváltozós műveletet definiál $P(U^*)$-on, amelyet *u-iteráció*nak nevezzük.

A nyelvek összeadásának, szorzásának és u-iterációjának segítségével bevezetjük az (*U feletti*) *környezetfüggetlen kifejezés* fogalmát a következő rekurzív definícióval:

1. Az U ábécé elemei, továbbá az $\emptyset$ és e legyenek környezetfüggetlen kifejezések.
2. Ha L és M környezetfüggetlen kifejezések, akkor $L + M$, LM, L^u $(u \in U)$ is környezetfüggetlen kifejezések.
3. Minden U feletti környezetfüggetlen kifejezés előáll az 1. alatti kifejezésekből a 2. lépés véges számú alkalmazásával.

A reguláris kifejezésekhez hasonlóan minden környezetfüggetlen kifejezés egyértelműen előállít egy U feletti nyelvet. Igaz a következő állítás.

3.23. Tétel. *Egy V ábécé feletti nyelv akkor és csak akkor környezetfüggetlen, ha előállítható valamilyen $U(\supseteq V)$ ábécé feletti környezetfüggetlen kifejezéssel.*

Bizonyítás Először a környezefüggetlen nyelveket generáló 2 típusú grammatikák nemterminális szimbólumainak n száma szerinti teljes indukcióval megmutatjuk, hogy minden V feletti környezetfüggetlen nyelv előállítható valamilyen $U(\supseteq V)$ feletti környezetfüggetlen kifejezéssel. Mivel definíció szerint $\emptyset$ és e környezetfüggetlen kifejezések, ezért a 3.12 Tétel szerint elegendő megmutatni, hogy ha a V feletti L környezetfüggetlen nyelv generálható a 2 típusú redukált grammatikával, akkor L előállítható egy $V_N \cup V$ ábécé feletti környezetfüggetlen kifejezéssel.

Legyen L olyan V feletti környezetfüggetlen nyelv, amely generálható az egyetlen nemterminálist tartalmazó $G = (\{S\}, V, S, H)$ 2 típusú redukált grammatikával. Legyenek

$$p_1, p_2, \ldots, p_k \in (V \cup \{S\})^* \tag{3.1}$$

azok a szavak halmaza, amelyek a H-beli szabályok jobb oldalain fellépnek. Nyilvánvaló, hogy a

$$(\sum_{j=1}^{k} p_j)^S \tag{3.2}$$

környezetfüggetlen kifejezés az L nyelvet állítja elő. Ezzel az állítást $n = 1$ esetre bebizonyítottuk.

Tegyük fel ezután, hogy minden legfeljebb n nemterminálist tartalmazó 2 típusú grammatikára igaz az állítás.

Legyen L olyan környezetfüggetlen nyelv, amely generálható egy $n+1$ nemterminálist tartalmazó 2 típusú $G = (V_N, V, S, H)$ grammatikával, ahol $V_N = \{S, A_1, \ldots, A_n\}$. Minden $1 \leq j \leq n$ esetén vegyük azt a

$$G_j = (V_N - S, V \cup \{S\}, A_j, H') \tag{3.3}$$

grammatikát, amelyben H'-t úgy kapjuk H-ból, hogy minden olyan szabályt elhagyunk belőle, amelynek a bal oldalán S van. Nyilvánvaló, hogy a G_j grammatikák is 2 típusúak. Az indukciós feltevés miatt az $L_j = L(G_j)$ $(j = 1, 2, \ldots n)$ nyelvek előállíthatók a $(V_N - \{S\}) \cup V$ ábécé feletti környezetfüggetlen kifejezésekkel.

Tekintsük a $G = (V_N, V, S, H)$ grammatikát és legyen

$$S \longrightarrow P_1, S \longrightarrow P_2, \ldots, S \longrightarrow P_r \tag{3.4}$$

az összes olyan H-beli szabály, amelynek a bal oldalán S áll. Minden $1 \leq s \leq r$ indexre definiálunk egy $V \cup \{S\}$ feletti L'_s nyelvet úgy, hogy legyen

$$L'_s = \{P_s\} \tag{3.5}$$

abban az esetben, ha $P_s \in (V \cup \{S\})^*$ és legyen

$$L'_s = Q_0 L_{j_1} Q_1 L_{j_2} \dots Q_{m-1} L_{j_m} Q_m \tag{3.6}$$

abban az esetben, ha

$$P_s = Q_0 A_{j_1} Q_1 A_{j_2} \dots Q_{m-1} A_{j_m} Q_m, \quad Q_0, Q_1, \dots, Q_m \in (V \cup \{S\})^*.$$

Akkor a G grammatika által generált $L = L(G)$ nyelvre kapjuk, hogy

$$L = L(G) = (\sum_{s=1}^{r} L'_s)^S. \tag{3.7}$$

Az indukciós feltevést és az L'_s nyelvek definícióját figyelembe véve az utóbbi összefüggésből azt kapjuk, hogy az L nyelv előállítható az $U = V_N \cup V$ ábécé feletti környezetfüggetlen kifejezéssel.

Ezután azt mutatjuk meg, hogy megfordítva, ha egy V feletti L nyelv előállítható valamely $U(\supseteq V)$ ábécé feletti környezetfüggetlen kifejezéssel, akkor L környezetfüggetlen, azaz generálható 2 típusú grammatikával. A bizonyítás céljából jelölje $L(U)$ az U feletti nyelveknek azt a legszűkebb halmazát, amely az $\emptyset, e, u \in U$ nyelveket tartalmazza és amely zárt az összeadásra, a szorzásra és az U-beli u elemekkel végzett u-iterációkra. Eszerint $\mathcal{L}(U)$ elemei pontosan azok az U feletti nyelvek, amelyek U feletti környezetfüggetlen kifejezéssel előállíthatók. Ezért elegendő megmutatni, hogy $L(U)$ minden eleme környezetfüggetlen. Az $\emptyset$, az e és az $u \in U$ nyelvek regulárisak, ezért környezetfüggetlenek is. S így, mivel 2.7 Tétel szerint a környezetfüggetlen nyelvek osztálya zárt az összeadásra és a szorzásra, elegendő azt igazolni, hogy az U feletti környezetfüggetlen nyelvek halmaza zárt az u-iterációra bármely $u \in U$ esetén.

Ez utóbbi igazolásához legyen L tetszőleges U feletti környezetfüggetlen nyelv, s legyen $G = (V_N, V_T, S, H)$ $(V_T \subseteq U)$ olyan 2 típusú grammatika, amelyre $L = L(G)$. A 2.3 Lemma szerint feltehető, hogy G standard. A 2.2 Lemma bizonyításban láttuk, hogy G megadható úgy, hogy létezik V_T-nek V_N-be való olyan kölcsönösen egyértelmű φ leképezése, amelyre a terminálist is tartalmazó H-beli szabályok pontosan $\varphi(x) \longrightarrow x$ $(x \in V_T)$ alakúak. Ha $u \in U$ olyan, hogy $u \notin V_T$, akkor nyilvánvalóan $L^u = L$. Ha pedig $u \in V_T$, akkor L^u generálható azzal a $G' = (V'_N, V_T - u, S, H')$ 2 típusú grammatikával, amelyben H'-t úgy kapjuk H-ból, hogy a H-beli $\varphi(u) \longrightarrow u$ szabályt a $\varphi(u) \longrightarrow S$ szabállyal cseréljük ki. Így mindenképpen azt nyerjük, hogy L^u környezetfüggetlen, azaz az U feletti környezetfüggetlen nyelvek halmaza zárt az u-iterációra bármely $u \in U$ esetén. □

A 3.23 Tétel bizonyításának első része egy eljárást ad környezetfüggetlen nyelvnek környezetfüggetlen kifejezéssel való megadására. Ezt az eljárást a következő példával mutatjuk be. A reguláris kifejezésekhez hasonlóan, egy környezetfüggetlen nyelv nem csak egy környezetfüggetlen kifejezéssel adható meg.

3.24. Példa. *A 3.8 Tétel bizonyítása során már láttuk, hogy az* $V = \{x, y, z\}$ *ábécé feletti* $L = \{x^k y^n z^n; k, n \geq 0\}$ *nyelvet generálja* $G = (V_N, V, S, H)$ *redukált környezetfüggetlen grammatika, ahol* $V_N = \{S, A, B\}$ *és*

$$H = \{S \longrightarrow AB, B \longrightarrow yBz, B \longrightarrow e, A \longrightarrow Ax, A \longrightarrow e\}.$$

Megadjuk az L *egy környezetfüggetlen kifejezését.*

Legyenek,(3.3) szerint,

$$G_1 = (\{A, B\}, V \cup \{S\}, A, H'), \quad G_2 = (\{A, B\}, V \cup \{S\}, B, H')$$

azok környezetfüggetlen grammatikákat, amelyekre

$$H' = \{A \longrightarrow Ax, \quad A \longrightarrow e, \quad B \longrightarrow yBz, \quad B \longrightarrow e\}$$

azaz H-ból elhagytuk az $S \longrightarrow AB$ szabályt. Az indukciós feltevés szerint $L_j = L(G_j)$ $(j = 1, 2)$ nyelvek legyenek megadva $\{A, B\} \cup V$ feletti környezetfüggetlen kifejezéssel. Az $S \longrightarrow AB$ az egyetlen (3.4)-ben definiált szabály. Így (3.6) szerint $L'_1 = L_1 L_2$. Amiből (3.7) szerint kapjuk, hogy

$$L = (L'_1)^S = (L_1 L_2)^S.$$

az L nyelv egy $V_N \cup V$ feletti környezetfüggetlen kifejezése. Most meghatározzuk L_1 egy környezetfüggetlen kifejezését $\{A, B\} \cup V$ felett:

H'-ből hagyjuk el, (3.3) alapján, az $A \longrightarrow Ax$ és $A \longrightarrow e$ szabályokat:

$$H'' = \{B \longrightarrow yBz, \quad B \longrightarrow e\}.$$

Legyen $G_{11} = (B, V \cup \{S, A\}, B, H'')$. ezért (3.1) és (3.2) szerint

$$L_{11} = L(G_{11}) = (e + yBz)^B.$$

A (3.4)-ben definiált szabályok

$$A \longrightarrow Ax, \quad A \longrightarrow e,$$

ezért (3.5) szerint

$$L'_{11} = e, \quad L'_{12} = Ax,$$

így (3.7) alapján

$$L_1 = (L'_{11} + L'_{12})^A = (e + Ax)^A.$$

Hasonló módon:

$$L_2 = (e + yBz)^B,$$

s így

$$L = (L_1 L_2)^S = ((e + Ax)^A (e + yBz)^B)^S.$$

Egyszerűbben jutunk célhoz azonban, ha az L nyelvet azzal a redukált környezetfüggetlen $G = (\{S, A\}, V, S, H)$grammatikával generáljuk, amelynek szabályai:

$$S \longrightarrow e, \quad S \longrightarrow xS, \quad S \longrightarrow xA, \quad A \longrightarrow yAz, \quad A \longrightarrow yz.$$

Ebben az esetben (3.3) szerint $G_1 = (A, V \cup \{S\}, A, H')$, ahol

$$H' = \{A \longrightarrow yAz, \quad A \longrightarrow yz\}.$$

(3.1) és (3.2) alapján $L(G_1)$ megadható az $L_1 = (yz + yAz)^A$ környezetfüggetlen kifejezéssel. (3.4), (3.5) és (3.6) segítségével kapjuk, hogy

$$L'_1 = e, \quad L'_2 = xS, \quad L'_3 = xL_1$$

Ezért (3.7) miatt

$$L = (L'_1 + L'_2 + L'_3)^S = (e + xS + x(yz + yAz)^A)^S$$

környezetfüggetlen kifejezéssel.

3.10. Parikh függvények

Az alfejezetben a környezetfüggetlen nyelveket a bennük szereplő különböző betűk számának eloszlása szerint jellemezzük. Megmutatjuk, hogy minden környezetfüggetlen nyelvhez van olyan reguláris nyelv, amelyben a különböző betűk számának eloszlása ugyanaz.

A vizsgálatainkban alapvető szerepet játszanak az olyan n dimenziós vektorok, amelyek komponensei nemnegatív egész számok. Az alfejezetben vektorokon mindig ilyen vektorokat fogunk érteni. Jelölje ezeknek a vektoroknak a halmazát $N^{(n)}$.

Az $M \subseteq N^{(n)}$ halmazt *lineáris*nak nevezzük, ha van olyan $k \in N$ és vannak olyan $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_k$ vektorok, hogy

$$M = \{\mathbf{t}_0 + \sum_{i=1}^{k} n_i \mathbf{t}_i; \quad n_1, \ldots, n_k \in N\} \tag{3.8}$$

Az M halmazt *féllineáris*nak mondjuk, ha véges sok lineáris halmaz egyesítése.

Legyen $U = \{u_1, \ldots, u_n\}$ tetszőleges ábécé. Jelölje $|p|_{u_i}$ a $p \in U^*$ szóban az $u_i \in U$ betű előfordulásainak számát. A $\varphi : U^* \to N^{(n)}$ leképezést *Parikh függvény*nek nevezzük, ha minden $p \in U^*$ szóra

$$\varphi(p) = (|p|_{u_1}, \ldots, |p|_{u_n}), \tag{3.9}$$

teljesül. Legyen továbbá tetszőleges $L \subseteq U^*$ nyelv esetén

$$\varphi(L) = \{\varphi(p); \quad p \in L\} \tag{3.10}$$

3.25. Példa. *Az*

$$M = \{(r,s,t);\ r = s \quad vagy \quad s = t, \quad (r,s,t) \in N^(3)\}$$

halmaz féllineáris, mert egyesítése annak a két lineáris halmaznak, amelyekre a (3.8) definíció jelölései szerint $\mathbf{t}_0, \mathbf{t}_1, \mathbf{t}_2$

$$(0,0,0),\ (1,1,0),\ (0,0,1) \quad ill. \quad (0,0,0),\ (1,0,0),\ (0,1,1).$$

Könnyen látható, hogy $M = \varphi(L)$, ahol például L az $U = \{u,v,w\}$ ábécé feletti $(uv)^*w^* + u^*(vw)^*$ reguláris kifejezéssel megadott nyelv. De $M = \varphi(L_1 + L_2)$ is, ahol

$$L_1 = \{u^i v^i w^j;\ i,j \in N\} \quad és \quad L_2 = \{u^l v^k w^k;\ l,k \in N\}.$$

Megmutatható, hogy L_1 és L_2, s így a 2.7 Tétel szerint $L_1 + L_2$ is környezetfüggetlen nyelvek (l. 3.10 feladat).

A következő két tétel mutatja, hogy az előző példa eredményei nem véletlenek.

3.26. Tétel. *(Parikh tétel) Ha az $L \subseteq U^*$ nyelv környezetfüggetlen, akkor $\varphi(L)$ féllineáris.*

Bizonyítás Az e nyelv nyilvánvalóan lineáris, ezért elegendő megmutatni, hogy az $e \notin L$ környezetfüggetlen nyelvek féllineárisak. Ebből ugyanis következik, hogy az $L + e$ nyelvek is féllineárisaik. A 3.1 Lemma alapján az is feltehető, hogy L szigorúan e-mentes. A 3.3 Tétel szerint L-et megadhatjuk Chomsky normálformában. (Ez a feltétel csak amiatt kell, hogy ne szerepeljenek $X \longrightarrow X$ vagy $Y \longrightarrow e$ alakú szabályok.) Legyen $L = L(G)$, ahol $G = (V_N, U, S, H)$ környezetfüggetlen grammatika. Tekintsük a változóknak egy olyan $V \subseteq V_N$ részhalmazát, amelyre $S \in V$. Jelölje L_V azt a U feletti

nyelvet, amely azokból a $p \in U^+$ szavakból áll, amelyek levezethetők S-ből úgy, hogy a levezetésben szereplő változók V-beliek, s minden V-beli változó szerepel a levezetésben. Mivel V_N véges halmaz, ezért véges sok ilyen V részhalmaz van. Továbbá minden $p \in U^+$ szóhoz van ilyen tulajdonságú $V \neq \emptyset$ részhalmaz, amelyre $p \in L_V$. Tekintsünk ugyanis egy $S \Longrightarrow_G^* p$ levezetést, s legyen V a levezetésben szereplő változók halmaza. Ez azt jelenti, hogy L véges sok ilyen L_V egyesítése. Ezért a bizonyításhoz elegendő megmutatni azt, hogy $\varphi(L_V)$ féllineáris.

Tegyük fel, hogy $|V| = m$. Jelölje $L_{V,m} \subseteq L_V$ azoknak a $p \in L_V$ szavaknak a halmazát, amelyek megadhatók olyan $S \Longrightarrow_G^* p$ levezetéssel, amelyekben L_V definíciója szerint csak V-bel változók szerepelnek, továbbá minden ilyen változó a levezetés fájának útjain legfeljebb $(m+1)$-szer. Nyilvánvaló, hogy $L_{V,m}$ véges.

Most minden $X \in V$ esetén legyen V_X azoknak az $P \in U^*XU^*$ mondatformáknak a halmaza, amelyekre van olyan $X \Longrightarrow_G^* P$ levezetés, amelyekben csak V-beli változók szerepelnek, s a levezetés fájának útjain minden változó legfeljebb $(m+1)$-szer. Világos, hogy a minden $X \in V$ változóra a V_X halmaz is véges. (Megjegyezzük, hogy V_X lehet $\emptyset$ is.)

Legyen $\alpha : V_X \to U^*$ az a leképezés, amely a V_X-beli szavakból törli az X változót, azaz

$$\alpha(pXq) = pq \quad (p, q \in U^*). \tag{3.11}$$

Továbbá legyen

$$\varphi(L_{V,m}) = \{\mathbf{s}_1, \ldots, \mathbf{s}_l\}, \tag{3.12}$$

és

$$\{\varphi(\alpha(P)); \quad P \in V_X, X \in V\} = \{\mathbf{t}_1, \ldots, \mathbf{t}_k\}. \tag{3.13}$$

Tetszőleges $1 \leq j \leq l$ esetén vegyük a

$$K_j = \{\mathbf{s}_j + \sum_{i=1}^{k} n_i \mathbf{t}_i; \quad n_1, \ldots, n_k \in k \in N\}, \tag{3.14}$$

és a

$$K = \cup_{j=1}^{l} K_j \tag{3.15}$$

halmazokat. A (3.8) definíció szerint K féllineáris.

Megmutatjuk, hogy $\varphi(L_V) = K$. Először a $K \subseteq \varphi(L_V)$ tartalmazást igazoljuk. Legyen $\mathbf{t} \in K$ tetszőleges vektor. Ha $\mathbf{t} = \mathbf{s}_j$ valamely $1 \leq j \leq l$ esetén, akkor (3.12) szerint van olyan $p \in L_{V,m}$, hogy $\varphi(p) = \mathbf{t}$. Így a $K \subseteq \varphi(L_V)$ tartalmazás bizonyításához (3.14) és (3.15) szerint elegendő megmutatni azt, hogy ha tetszőleges $\mathbf{t} \in K$ vektorra $\mathbf{t} \in \varphi(L_V)$, akkor $\mathbf{t} + \mathbf{t}_i \in \varphi(L_V)$ $(1 \leq i \leq k)$. Ha $\mathbf{t} \in K \cap \varphi(L_V)$, akkor van olyan $p \in L_V$, amelyre $\varphi(p) = \mathbf{t}$ és olyan $S \longrightarrow_G^* p$

levezetés, amelyben csak V-beli változók vannak. Így (3.13) szerint léteznek olyan $X \in V$ és $P \in U^*XU^*$, amelyekre van olyan $X \Longrightarrow_G^* P$ levezetés, amelyben csak V-beli változók szerepelnek, s a levezetés fájának minden útján legfeljebb $(m+1)$-szer, valamint $\varphi(\alpha(P)) = \mathbf{t}_i$. Tekintsük azt a levezetést, amelynek levezetési fáját úgy kapjuk, hogy az $S \Longrightarrow_G^* p$ levezetés fájában egy X-szel jelölt csúcsa helyére az $X \Longrightarrow_G^* P$ levezetés fáját tesszük. Ha az így kapott levezetéssel a $w \in U^+$ szót kapjuk, akkor $w \in L_V$ és

$$\mathbf{t} + \mathbf{t}_i = \varphi(p) + \varphi(\alpha(P)) = \varphi(w) \in \varphi(L_V),$$

azaz $K \subseteq \varphi(L_V)$.

Most igazoljuk $\varphi(L_V) \subseteq K$ tartalmazást. Ha $\mathbf{t} \in \varphi(L_V)$, akkor van olyan $p \in L_V$, hogy $\varphi(p) = \mathbf{t}$. Legyen $S \Longrightarrow_G^* p$ olyan levezetés, amelynek F levezetési fájában minden változó V-beli, s a levezetési fának nincs olyan útja, amelyben valamely változó $(m+1)$-nél többször szerepelne. Ebben az esetben $p \in L_{V,m}$, ezért van olyan $\mathbf{s}_j \in \varphi(L_{V,m})$ $(1 \leq j \leq l)$, hogy $\mathbf{t} = \mathbf{s}_j$, azaz $\mathbf{t} \in K$.

Tegyük fel, hogy az F levezetési fa valamely útjának legalább $m+2$ csúcsa van ugyanazzal a változóval jelölve. Legyenek ennek az útnak $c_0, c_1, \ldots, c_{m+1}$ csúcsai ugyanazzal az $X \in V$ változóval jelölve. Az F levezetési fa c_h gyökerű részfája legyen F_h $(h = 0, 1, \ldots, m+1)$. F_0-ban minden úton legfeljebb $m+1$ alkalommal szerepel ugyanaz a változó. Mivel F_{h+1} az F_h fa részfája, ezért minden F_h-ban minden úton legfeljebb $m+1$ csúcs van ugyanazzal a változóval megjelölve. Nyilvánvalóan van olyan $1 \leq h \leq m$, amelyre F_h-ban és F_{h+1}-ben ugyanazok a változók szerepelnek. Jelölje F' azt a levezetési fát, amelyet úgy kapunk F-ből, hogy a c_h csúcsot F_{h+1} részfával helyettesítjük. Másrészt legyen F" az a levezetési fa, amelyet úgy származtatunk F_h-ból, hogy töröljük a F_{h+1} részfát a gyökere kivételével, azaz F_h-ban az F_{h+1} részfát az X változóval megjelölt egyetlen csúcsból álló részfával helyettesítjük. Akkor van olyan $P \in U^*XU^*$ és olyan $X \Longrightarrow_G^* P$ levezetés, amelynek levezetési fája F". Így $\varphi(\alpha(P)) = \mathbf{t}_i$ valamely $1 \leq i \leq k$ esetén. Ha F' az $S \Longrightarrow_G^* q$ levezetés fája, akkor

$$\varphi(p) = \varphi(q) + \mathbf{t}_i.$$

Nyilvánvaló, hogy $q \in L_V$. Továbbá F'-nek kevesebb csúcsa van mint F-nek. Ha F'-ben nincs olyan út, amelyben V-beli változó $(m+1)$-nél többször szerepelne, akkor $q \in L_{V,m}$. Ekkor van olyan $\mathbf{s}_j \in \varphi(L_{V,m})$ $(1 \leq j \leq l)$, hogy $\varphi(q) = \mathbf{s}_j$, azaz

$$\varphi(p) = \mathbf{s}_j + \mathbf{t}_j \in K.$$

Ellenkező esetben ismételjük meg p helyett q-val a fenti eljárást. Véges számú lépésben kapjuk, hogy

$$\varphi(p) = \mathbf{s}_j + \sum_{j=1}^{k} n_i \mathbf{t}_i \in K.$$

Ezzel megmutattuk, hogy $\varphi(L_V) = K$. □

Legyen L_1 és L_2 két $U = \{u_1, \ldots, u_n\}$ ábécé feletti nyelv. Azt mondjuk, hogy L_1 és L_2 *betűekvivalens*ek, ha $\varphi(L_1) = \varphi(L_2)$, ahol φ a Parikh függvény. Minthogy minden véges nyelv reguláris, ezért a következő tétel a végtelen (nem reguláris) környezetfüggetlen nyelvek esetében érdekes.

3.27. Tétel. *Bármely környezetfüggetlen nyelvhez van vele betűekvivalens reguláris nyelv.*

Bizonyítás Legyen L környezetfüggetlen nyelv az $U = \{u_1, \ldots, u_n\}$ ábécé felett. A 3.26 Tétel szerint $\varphi(L)$ féllineáris. Így $\varphi(L)$ véges sok $K_1, \ldots, K_l$ lineáris halmaz egyesítése. Tegyük fel, hogy

$$K_j = \{\mathbf{t}_{j_0} + \sum_{i=1}^{k_j} n_i \mathbf{t}_{j_i} \quad n_i \in N,\ i = 1, \ldots, k_j\}, \quad (j = 1, \ldots, l).$$

Minden j_i-re $(j = 1, \ldots, l,\ i = 1, \ldots, k_j)$ legyen

$$\mathbf{t}_{j_i} = (m_{j_i,1}, \ldots, m_{j_i,n})$$

Ha L_j $(j = 1, \ldots, l)$ az

$$u_1^{m_{j_0,1}} \ldots u_n^{m_{j_0,n}} (u_1^{m_{j_1,1}} \ldots u_n^{m_{j_1,n}})^* \ldots (u_1^{m_{j_{k_j},1}} \ldots u_n^{m_{j_{k_j},n}})^*$$

reguláris nyelv, akkor $\varphi(L_j) = K_j$ $(j = 1, \ldots, l)$. Amiből következik, hogy az $L' = L_1 \cup \cdots \cup L_k$ reguláris nyelv betűekvivalens L-lel. □

A 3.27 Tétel szerint egy $U = \{u_1, \ldots, u_n\}$ ábécé feletti (nem reguláris) környezetfüggetlen nyelv szavaiban a betűket lehet úgy permutálni, hogy a permutálásokkal kapott nyelv reguláris. Megjegyezzük, hogy a 3.27 Tételből azonnal adódik a 3.7 Következmény, vagyis, hogy egyelemű ábécé feletti nyelv akkor és csak akkor környezetfüggetlen, ha reguláris.

3.28. Példa. *Az $U = \{x, y\}$ ábécé feletti*

$$L = \{x^k y^k;\ k \in N\} \cup \{xyx^l y^{2l};\ l \in N\} \cup \{yx^{2m} y^{2m};\ m \in N\}$$

nyelv környezetfüggetlen, de nem reguláris. Az L nyelv betűekvivalens az $L' = (xy)^* + xy(xy^2)^* + xy(x^2y^2)^*$ reguláris nyelvvel.

Az L nyelv környezetfüggetlen, mert generálja a $G = (\{S, A, B\}, \{x, y\}, S, H)$ 2 típusó grammatika, amelyben a H-beli szabályok:

$$S \longrightarrow e, \quad S \longrightarrow xSy, \quad S \longrightarrow xyA, \quad S \longrightarrow xyB$$

$$A \longrightarrow xAy^2, \quad A \longrightarrow e, \quad B \longrightarrow x^2By^2, \quad B \longrightarrow e.$$

A 8.8 Lemma segítségével megmutatható, hogy L nem reguláris. Továbbá

$$\varphi(L) = \varphi(L') = \{\mathbf{t}_0 + k\mathbf{t}_1;\ k \in N\} \cup \{\mathbf{t}_1 + l\mathbf{t}_2 + m\mathbf{t}_3;\ l, m \in N\},$$

ahol

$$\mathbf{t}_0 = (0, 0), \quad \mathbf{t}_1 = (1, 1), \quad \mathbf{t}_2 = (1, 2),$$

azaz a két nyelv betűekvivalens. A 3.26 Tétel szerint $\varphi(L)$ féllineáris.

A következő példa mutatja, hogy a arikh tétel) nem fordítható meg.

3.29. Példa. *A 3.6 Tétel bizonyításában megmutattuk, hogy az $\{x, y, z\}$ ábécé feletti $L = \{x^k y^k z^k; k \in N\}$ nyelv környezetfüggő, de nem környezetfüggetlen. Az előző példához hasonlóan a $\varphi(L) = \{(k, k, k); k \in N\}$ halmaz lineáris, s így féllineáris, mert a*

$$\mathbf{t}_0 = (0, 0, 0),\ \mathbf{t}_1 = (1, 1, 1)$$

vektorok megfelelnek a (3.8) feltételnek. Megjegyezzük, hogy az L nyelv betűekvivalens az $\{(xyz)^k; k \in N\}$ reguláris nyelvvel.

Feladatok

3.1. Adjunk meg olyan környezetfüggetlen grammatikákat, amelyek generálják az

$$L_1 = \{a^{3n} b^n;\ n = 1, 2, \dots\}, \quad L_2 = \{a^m b^k;\ m \geq k \geq 0\}$$

és az $(L_1 L_2 + L_2)^*$ nyelveket.

3.2. Jelölje $|p|_a$ és $|p|_b$ a $p \in \{a, b\}^*$ szóban a ill. b előfordulásainak számát. Adjunk meg olyan környezetfüggetlen grammatikát, amely tetszőleges k pozitív egész számra az

$$L_k = \{p \in \{a, b\}^*;\ |p|_a = k|p|_b\}$$

nyelvet generálja.

3.3. Az $U = \{u, v, w\}$ ábécé feletti

$$L = \{u^i v^i w^j;\ i, j \in N\} \cup \{u^l v^k w^k;\ l, k \in N\}$$

nyelv környezetfüggetlen.

3.4. A véges V ábécé feletti palindromok $P(V)$ nyelve lineáris, s így környezetfüggetlen. Adjuk meg a nyelvet környezetfüggetlen kifejezéssel.
3.5. Az egyelemű $\{x\}$ ábécé feletti $L = \{x^{j^2}; j \geq 1\}$ nyelv nem környezetfüggetlen.
3.6. Jelölje P a prímszámok halmazát. Az egyelemű $\{x\}$ ábécé feletti $L = \{x^i;\ i \in P\}$ nyelv nem környezetfüggetlen.
3.7. A $p \in X^*$ szót *négyzetmentes*nek nevezzűk, ha nincs q^2 $(q \in X^+)$ alakú részszava. A négyzetmentes szavak nyelvének egy résznyelve akkor és csak akkor környezetfüggetlen, ha véges (s így reguláris). Ha $|X| \leq 2$, akkor a négyzetmentes szavak nyelve véges.

4. fejezet

Környezetfüggő nyelvek

A 3.6 Tétel szerint a környezetfüggő nyelvek osztálya bővebb, mint a környezetfüggetlen nyelvek osztálya. Mint már említettük ez az állítás a megfelelő grammatikákra nem igaz. Azonban bizonyos környezetfüggetlen nyelvek generálását egyszerűbbé tehetjük környezetfüggő grammatikák felhasználásával. Ebben a fejezetben a környezetfüggő nyelvek néhány alapvető tulajdonságát tárgyaljuk.

4.1. Hosszúságot nem csökkentő grammatikák

Egy $G = (V_N, V_T, S, H)$ grammatika $P \longrightarrow Q$ H-beli szabályát *hosszúságot csökkentő*nek nevezzük, ha $|P| > |Q|$ és *hosszúságot nem csökkentő*nek nevezzük, ha $|P| \leq |Q|$. Hasonlóan beszélhetünk *hosszúságot növelő* ill. *nem növelő* szabályról is. A $G = (V_N, V_T, S, H)$ grammatikát *hosszúságot nem csökkentő*nek hívjuk, ha minden H-beli szabály jobb oldala legalább olyan hosszú, mint a bal oldala, azaz minden H-beli $P \longrightarrow Q$ szabályra $|P| \leq |Q|$.

A környezetfüggő grammatikák szabályai, az $S \longrightarrow e$ szabály kivételével, hosszúságot nem csökkentők. Másrészt igaz a következő lemma.

4.1. Lemma. *Minden hosszúságot nem csökkentő grammatikához megadható egy vele ekvivalens környezetfüggő grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ hosszúságot nem csökkentő grammatika. A 2.2 Lemma szerint feltehető, hogy G standard. (A standard grammatika konstrukciója során hosszúságot nem csökkentő grammatikából hosszúságot nem csökkentő grammatikát kapunk.) Tekintsük azt a $G' = (V'_N, V_T, S, H')$ grammatikát, amelyben H'-t H-ból a következőképpen kapjuk. Minden H-beli $X \longrightarrow x$ $(X \in V_N, x \in V_T)$ alakú szabály legyen H'-beli szabály is. (Mivel G standard, ezért a terminálisokat csak ilyen alakú szabályok tartalmazzák.)

Továbbá minden H-beli $X \longrightarrow P$ $(X \in V_N, P \in V_N^+)$ alakú szabály is legyen H'-beli szabály. Legyen $P \longrightarrow Q$ egy tetszőleges terminálist nem tartalmazó H-beli szabály, amelyre $|P| \geq 2$. Akkor $P = X_1X_2 \dots X_k$ és $Q = Y_1Y_2 \dots Y_n$ alakban adható meg, ahol $X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_n \in V_N$, $(2 \leq k \leq n)$. Vezessük be a $Z_1, Z_2, \dots Z_k \notin V_N \cup V_T$ új változókat és vegyük a következő szabályokat:

$$X_1X_2 \dots X_k \longrightarrow Z_1X_2 \dots X_k, \quad Z_1X_2 \dots X_k \longrightarrow Z_1Z_2X_3 \dots X_k,$$

$$Z_1Z_2 \dots Z_{k-1}X_k \longrightarrow Z_1Z_2 \dots Z_{k-1}Z_kY_{k+1} \dots Y_n,$$

$$Z_1Z_2 \dots Z_kY_{k+1} \dots Y_n \longrightarrow Y_1Z_2 \dots Z_kY_{k+1} \dots Y_n, \dots$$

$$Y_1 \dots Y_{k-1}Z_kY_{k+1} \dots Y_n \longrightarrow Y_1 \dots Y_{k-1}Y_kY_{k+1} \dots Y_n.$$

Vegyük be H'-be minden ilyen $P \longrightarrow Q$ H-beli szabály helyett az előbbi típusú szabályokat. Továbbá V_N' tartalmazza ezeket az új nemterminálisokat és V_N elemeit. Belátható, hogy olyan G' (standard) környezetfüggő grammatika, amely ekvivalens G-vel. □

Az előző lemma azt jelenti, hogy a hosszúság nem csökkentése a környezetfüggőséggel egyenértékű tulajdonság. Kivételt csupán az üres szó generálását biztosító $S \longrightarrow e$ szabály képez. Megmutatható, hogy (2.4) utolsó

$$\mathcal{L}_1 \subset \mathcal{L}_0$$

valódi tartalmazása igaz. Ez az jelenti, hogy a hosszúság nem csökkentése lényeges megszorítást jelent a mondatszerkezetű grammatikákhoz képest. A környezetfüggő grammatikákkal kapcsolatos problémákat általában jóval nehezebb eldönteni, mint környezetfüggetlen grammatikák esetében, mivel a levezetések szerkezete sokkal bonyolultabb lehet. A hosszúság nem csökkentése azon kevés jó tulajdonságok egyike, amit mindig használhatunk.

4.2. Rekurzív nyelvek

A 3.4 Tétel környezetfüggő nyelvekre is igaz, azaz ezekre a nyelvekre is megoldható a szóprobléma.

4.2. Tétel. *Minden környezetfüggő nyelv rekurzív.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ környezetfüggő grammatika és $p \in V_T^*$. A $p = e$ esetben $e \in L(G)$ akkor és csak akkor, ha $S \longrightarrow e \in H$, ami nyilván eldönthető. Feltehetjük tehát, hogy $|p| = n \geq 1$. Tekintsük az olyan

$$S = P_0, P_1, \dots, P_{k-1}, P_k = p$$

szósorozatokat $(V_N \cup V_T)^+$-ból, amelyekre

$$1 = |P_0| \leq |P_1| \leq \cdots \leq |P_{k-1}| \leq |P_k| = n.$$

Mivel $V_N \cup V_T$ véges halmaz, ezért az összes ilyen sorozat csak véges sok különböző szót tartalmaz. Ez azt jelenti, hogy az összes olyan sorozatnak száma, amelyekben ismétlés nem fordul elő, véges. E véges sok sorozat mindegyikében megvizsgálható, hogy

$$P_j \Longrightarrow_G P_{j+1}, \quad 0 \leq j < n$$

teljesül-e. (Az ismétléseket tartalmazó sorozatokat nem kell figyelembe venni, mert minden ismétlést tartalmazó levezetéshez található ismétlést nem tartalmazó levezetés is.) □

A bizonyításban szereplő eldöntési eljárás természetesen gyakorlati célra nem nagyon alkalmas. Mindenesetre látható belőle a probléma nehézsége, ha a sorozatokra $|P_j| \leq |P_{j+1}|$ nem teljesül. Tetszőleges 0 típusú grammatika esetén bizonyítható, hogy ez a tartalmazási probléma ténylegesen eldönthethetetlen.

A következő tétel szerint a 4.2 Tétel megfordítása nem igaz. Ez azt jelenti, hogy a rekurzív nyelvek osztálya bővebb a környezetfüggő nyelvek osztályánál.

4.3. Tétel. *Létezik olyan rekurzív nyelv, amelyik nem környezetfüggő.*

Bizonyítás Azt mutatjuk meg, hogy kételemű ábécé felett is van olyan rekurzív nyelv, amelyik nem környezetfüggő. Legyen a kételemű ábécé $\{a, b\}$. Tekintsük azokat a környezetfüggő grammatikákat, amelyek mindegyikének terminális ábécéje $\{a, b\}$ és mondatszimbóluma S. Ezen grammatikák nemterminális ábécéit tekinthetjük ugyanazon megszámlálhatóan végtelen

$$V = \{S, X_1, X_2, \dots\}$$

halmaz véges részhalmazaiként. (A változók átjelölésével ez mindig elérhető.) Nyilvánvalóan minden $\{a, b\}$ feletti környezetfüggő nyelv generálható ilyen grammatikával. Egy ilyen grammatikát a szabályok egy

$$P_1 \longrightarrow Q_1, \quad P_2 \longrightarrow Q_2, \quad \dots, \quad P_n \longrightarrow Q_n$$

sorozatával is megadhatunk. A szabályokból ugyanis meg tudjuk határozni a nemterminális ábécét. (Természetesen, ha a szabályokat más sorrendben adjuk meg, akkor is ugyanazt a grammatikát kapjuk.) Minden ilyen G grammatikához megadunk egy $\{a, b\}$ feletti p_G szót a következő módon:

Legyen

$$V' = \{a, b, \longrightarrow, \#, S, X_1, X_2, \dots\}.$$

Definiáljuk a $\varphi : V' \to a^+b$ leképezést a

$$\varphi(a) = ab, \quad \varphi(b) = a^2b, \quad \varphi(\longrightarrow) = a^3b, \quad \varphi(\#) = a^4b,$$

$$\varphi(S) = a^5b, \quad \varphi(X_i) = a^{5+i}b, \quad i = 1, 2, \ldots$$

feltételekkel. A φ leképezés V' bijektív leképezése a^+b-re. Jelöljük szintén φ-vel a φ monoid-homomorf kiterjesztését a V'^* szabad félcsoportra.

Legyen

$$p_G = \varphi(P_1 \longrightarrow Q_1 \# P_2 \longrightarrow Q_2 \# \ldots \# P_n \longrightarrow Q_n).$$

Ha $p_G = p_{G'}$, akkor nem nehéz belátni, hogy G-t és G'-t szabályoknak ugyanazzal a sorozatával adtuk meg, azaz $G = G'$. Ebből következik, hogy a G grammatikákat a p_G szavakkal is megadhatjuk.

Legyen az $\{a, b\}$ feletti L nyelv azoknak a p_G szavaknak a halmaza, amelyekre $p_G \notin L(G)$. Megmutatjuk, hogy az L nyelv rekurzív, de nem környezetfüggő.

A 4.2 Tétel szerint algoritmikusan eldönthető, hogy p_G eleme-e az $L(G)$ környezetfüggő nyelvnek. Így az is eldönthető algoritmikusan, hogy p_G eleme-e L-nek. Ez azt jelenti, hogy L rekurzív.

Tegyük fel, hogy L környezetfüggő. Akkor van olyan p_G-vel megadott G grammatika, amelyre $L = L(G)$. Az L definíciója miatt, ha $p_G \in L(G) = L$, akkor $p_G \notin L$. Ha pedig $p_G \notin L(G) = L$, akkor $p_G \in L$. Mindkét esetben ellentmondásra jutottunk. Vagyis L nem környezetfüggő. □

Az U ábécé feletti L nyelvet (U *felett*) *rekurzíve felsorolható*nak nevezzük, ha van olyan eljárás, amely az összes $p \in L$ szót valamilyen sorrendben (esetleg ismétlésekkel) előállítja, azaz felsorolja.

Könnyű belátni, hogy minden 0 típusú nyelv rekurzíve felsorolható. Ehhez nem kell mást csinálnunk, mint rendre előállítanunk a mondatszimbólumból $1, 2, \ldots$ lépésben levezethető összes mondatformát, s ezek közül kiválasztani a terminális szavakat. A 11.3 Következmény szerint a 0 típusú nyelvek osztálya és a véges ábécék feletti rekurzíve felsorolható nyelvek osztálya megegyezik.

Továbbá minden véges ábécé feletti rekurzív nyelv rekurzíve felsorolható. Nem kell ugyanis mást tennünk, mint rendre előállítani az összes $p \in U^*$ szót, miközben minden egyes új szó előállítása után alkalmazzuk rá az eldöntési algoritmust, és belevesszük a felsorolásba, ha igen választ kapunk, egyébként elhagyjuk. Ezáltal megadtunk egy felsorolási eljárást, ahol még az ismétléseket is kizártuk.

Megfordítva viszont abból, hogy egy véges ábécé feletti nyelv rekurzíve felsorolható, még nem következik, hogy rekurzív is. Megmutatjuk, hogy a véges ábécé feletti rekurzíve felsorolható nyelvek osztálya bővebb a rekurzív nyelvek osztályánál. Ehhez először bebizonyítjuk a következő állítást.

4.4. Lemma. *A véges ábécé feletti L nyelv akkor és csak akkor rekurzív, ha L és $\overline{L}$ rekurzíve felsorolható.*

Bizonyítás Legyen L tetszőleges U véges ábécé feletti nyelv. Ha az L nyelv rekurzív, akkor $\overline{L}$ is rekurzív, s ezért mind a kettő rekurzíve felsorolható.

Megfordítva, tegyük fel, hogy L és $\overline{L}$ rekurzíve felsorolhatók. Legyen $p \in U^*$. Kombináljuk az L és $\overline{L}$ elemeinek felsorására szolgáló eljárásokat úgy, hogy váltakozva hol az egyikkel, hol a másikkal állítunk elő egy szót, miáltal az U^*-beli szavaknak egy olyan

$$p_1, p_2, \ldots, p_{2n-1}, p_{2n}, \ldots \quad (n = 1, 2, \ldots)$$

felsorolását kapjuk, ahol $p_{2n-1} \in L$ és $p_{2n} \in \overline{L}$. Mivel $L + \overline{L} = U^*$, ezért a felsorolásban valahol előfordul p. Most már csak azt kell eldönteni, hogy p páratlan vagy páros helyen szerepel-e a sorozatban, s így végeredményben egy eldöntési algoritmust adtunk meg, vagyis L rekurzív. □

A 4.4 Lemma szerint annak megmutatásához, hogy a véges ábécé feletti rekurzíve felsorolható nyelvek osztálya bővebb a véges ábécé feletti rekurzív nyelvek osztályánál, elegendő egy véges ábécé felett olyan rekurzíve felsorolható nyelvet találni, amelynek komplementere nem rekurzíve felsorolható.

4.5. Tétel. *Létezik véges ábécé feletti rekurzíve felsorolható nyelv, amely nem rekurzív.*

Bizonyítás Azt mutatjuk meg, hogy az $\{a\}$ egyelemű ábécé felett van olyan rekurzíve felsorolható nyelv, amelyenek komplementere nem rekurzíve felsorolható. A 4.4 Lemma szerint ebből már következik az állítás.

Tegyük fel, hogy minden rekurzíve felsorolható $L \subseteq a^*$ nyelvhez a felsorolási eljárás le van írva valamilyen nyelven. Pontosabban feltételezhetjük, hogy van olyan V véges ábécé, hogy az előbbi eljárások mindegyikét valamely $E \in V^*$ szóval jellemezhetjük. Miután V^* megszámlálhatóan végtelen, az E szavakat valamilyen

$$E_0, E_1, E_2, \ldots$$

sorozatba rendezhetjük. Definiáljuk a következő $L \subseteq a^*$ nyelvet: $a^k \in L$ akkor és csak akkor, ha az E_k eljárás felsorolja az a^k szót.

Először is nyilvánvaló, hogy $\overline{L}$ nem lehet rekurzíve felsorolható. Ha ugyanis az lenne, akkor volna olyan E_i eljárás a fenti sorozatban, amely pontosan $\overline{L}$ elemeit sorolja fel. De akkor akár $a^i \in L$, akár $a^i \notin L$, ellentmondásba kerülünk L definíciójával.

Végül megmutatjuk, hogy L rekurzíve felsorolható. Minden eljárás diszkrét lépésekre bontható, vagyis beszélhetünk az E_k (k-adik eljárás) l-edik lépéséről.

Jelöljük ezt a lépést a (k, l) rendezett párral. Amennyiben a k-adik eljárás az l-edik lépésben befejeződik, akkor ennek az eljárásnak a m-edik lépését $l < m$ esetben úgy értelmezzük, hogy nem csinálunk semmit. Kombináljuk az eljárásokat úgy, hogy a

$$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2), (0,3), \ldots$$

lépéseket ilyen sorrendben hajtjuk végre egymás után. Ha most a (k, l)-edik lépés éppen az a^k szónak E_k által felsorolt nyelvhez való hozzávételét eredményezi, akkor a^k-t felvesszük L-be. Ezzel megadtunk egy eljárást, amely felsorolja L elemeit, tehát L valóban rekurzíve felsorolható. □

4.3. Kuroda normálforma

Most megadjuk a grammatikák Chomsky normálformájának egy általánosítását. A $G = (V_N, V_T, S, H)$ grammatikáról azt mondjuk, hogy *Kuroda normálformá*ban van megadva, ha minden H-beli szabály $X \longrightarrow x$, $X \longrightarrow Y$, $X \longrightarrow YZ$, vagy $XY \longrightarrow WZ$ alakú, ahol $X, Y, W, Z \in V_N$ és $x \in V_T$.

Látható, hogy minden Kuroda normálformában megadott grammatika hosszúságot nem csökkentő grammatika. Igaz a Chomsky normálformára vonatkozó 3.3 Tétel hasonló eredmény.

4.6. Tétel. *A $G = (V_N, V_T, S, H)$ hosszúságot nem csökkentő grammatikához van ekvivalens Kuroda normálformában megadott $G' = (V'_N, V_T, S, H')$ grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ hosszúságot nem csökkentő grammatika. A 2.3 Lemma miatt feltehető, hogy G standard, azaz a terminálisok csak $X \longrightarrow x$ $(X \in V_N, x \in V_T)$ alakú szabályokban fordulnak elő. Megszerkesztjük V_N-ből és H-ból V'_N-t és H'-t. Az

$$X \longrightarrow x, \quad X \longrightarrow Y, \quad X \longrightarrow YZ,$$

$$XY \longrightarrow WZ, \quad X, Y, W, Z \in V_N,\ x \in V_T$$

alakú szabályok legyenek H'-beli szabályok is. Ha $|Q| \geq 3$, akkor az

$$X \longrightarrow Q \quad (X \in V_N,\ Q \in V_N^+)$$

alakú H-beli szabályokat, mint azt a 3.3 Tétel bizonyításában a Chomsky normálformára való átalakításnál tettük, $X \longrightarrow YZ$ alakú szabályokkal helyettesíthetjük, miközben V_N-t is kibővítjük új változókkal.

Tekintsük végül az olyan $P \longrightarrow Q$ $(P, Q \in V_N^+)$ H-beli szabályokat, amelyekre $|P| \geq 2$ és $|Q| \geq 3$. Legyen

$$P = X_1 X_2 \dots X_k, \quad Q = Y_1 Y_2 \dots Y_n,$$

ahol $X_1, X_2, \dots X_k, Y_1, Y_2, \dots, Y_n \in V_N$, $(k \leq n)$. Vegyük fel a nemterminálisok közé az új $Z_2, Z_3, \dots, Z_{n-1}$ változókat és cseréljük ki a $P \longrightarrow Q$ alakú szabályokat a következő szabályokkal:

$$X_1 X_2 \longrightarrow Y_1 Z_2, \quad Z_2 X_3 \longrightarrow Y_2 Z_3, \quad \dots, \; Z_{k-1} X_k \longrightarrow Y_{k-1} Z_k,$$

$$Z_k \longrightarrow Y_k Z_{k+1}, \quad Z_{k+1} \longrightarrow Y_{k+1} Z_{k+2}, \; \dots, \quad Z_{n-1} \longrightarrow Y_{n-1} Y_n.$$

Könnyen belátható, hogy így kapott $G' = (V'_N, V_T, S, H')$ grammatika G-vel ekvivalens. □

4.7. Következmény. *Ha egy környezetfüggő grammatika nem tartalmazza az $S \longrightarrow e$ szabályt, akkor létezik vele ekvivalens Kuroda normálformában megadott grammatika.*

A Kuroda normálformában megadott grammatika nem környezetfüggő, ha tartalmaz $XY \longrightarrow WZ$ $(X, Y, W, Z \in V_N)$ alakú szabályokat. Ezek a szabályok azonban helyettesíthetők a következő környezetfüggő szabályokkal:

$$XY \longrightarrow XY', \quad XY' \longrightarrow X'Y', \quad X'Y' \longrightarrow X'Z, \quad X'Z \longrightarrow WZ,$$

ahol X' és Y' új változók. Ezt *finomított Kuroda normálformá*nak is mondjuk. Kaptuk a 4.7 Következmény alapján az alábbi eredményt.

4.8. Következmény. *Ha a G környezetfüggő grammatika nem tartalmazza az $S \longrightarrow e$ szabályt, akkor van L-lel vele ekvivalens finomított Kuroda normálformában megadott grammatika.*

Az $XY \longrightarrow WZ$ szabályt nem lehet egyszerűen az

$$XY \longrightarrow X'Y, \quad X'Y \longrightarrow X'Z, X'Z \longrightarrow WZ$$

szabályokkal helyettesíteni. Ugyanis, ha az eredeti grammatika szabályai például a következőek:

$$S \longrightarrow XY, \; Y \longrightarrow ZA, \; XY \longrightarrow WZ,$$

akkor a fenti helyettesítéssel egy olyan grammatikát kapunk, amelyben megadható az

$$S \Longrightarrow XY \Longrightarrow X'Y \Longrightarrow X'ZA \Longrightarrow WZA$$

levezetés, amely az eredeti grammatikában nem teljesül.

Figyeljük meg, hogy a Kuroda normálforma finomításakor az $XY \longrightarrow WZ$ alakú szabályt olyan környezetfüggő szabályokkal helyettesítjük, amelyeknél vagy csak bal oldali vagy csak jobb oldali környezet fordul elő, de mindkét változat szerepel. Ezeket *bal [jobb] oldali környezetfüggő szabályok*nak nevezzük.

Megmutatható, hogy lehet csak bal [jobb] oldali környezetfüggő szabályokkal, azaz *bal [jobb] oldali környezetfüggő grammatiká*val tetszőleges környezetfüggő nyelvet generálni, azonban egy környezetfüggő grammatikának egyoldalú környezetfüggő grammatikává való átalakítása általában túlságosan bonyolult ahhoz, hogy gyakorlati célra felhasználjuk.

Az egyoldalú környezetfüggő grammatikák viszont használhatók bizonyos környezetfüggetlen nyelvek megadására, ami előnyös lehet ezek gépi feldolgozásának meggyorsítására. Az egyoldalú környezetfüggő grammatikákat is normálformára hozhatjuk.

4.9. Tétel. *Minden bal oldali környezetfüggő grammatikához megadható olyan ekvivalens grammatika, amelynek szabályai a következő alakúak lehetnek:*

$$X \longrightarrow x, \quad X \longrightarrow Y, \quad X \longrightarrow YZ, \quad XY \longrightarrow XZ,$$

ahol x terminális jel, X, Y, Z pedig nemterminálisok.

Bizonyítás Hasonlóan járunk el, mint a 4.1 Lemma bizonyításában, ezért a bizonyítást nem részletezzük. Csak annyit jegyzünk meg, hogy egy bal oldali környezetfüggő szabály:

$$X_1X_2 \ldots X_kX \longrightarrow X_1X_2 \ldots X_kY_1Y_2 \ldots Y_n$$

alakú, amelyben csak változók szerepelnek. Az ilyen szabályt helyettesíthetjük az

$$X_1X_2 \longrightarrow X_1Z_2, \quad Z_2X_3 \longrightarrow Z_2Z_3, \quad \ldots, \quad Z_{k-1}X_k \longrightarrow Z_{k-1}Z_k,$$
$$Z_kX \longrightarrow Z_kW_1, \quad W_1 \longrightarrow Y_1W_2, \quad \ldots, \quad W_{n-1} \longrightarrow Y_{n-1}Y_n,$$
$$Z_2 \longrightarrow X_2, \quad Z_{k-1} \longrightarrow X_{k-1}, \quad Z_k \longrightarrow X_k$$

szabályokkal, ahol $Z_2, \ldots, Z_k, W_1, \ldots W_{n-1}$ újonnan bevezetett változók. □

Természetesen analóg tétel érvényes jobb oldali környezetfüggő grammatikákra.

4.10. Példa. *Megmutatjuk, hogy a $V_T = \{x, y\}$ ábécé feletti*

$$L = \{x^k y^k x^k; k \geq 1\}$$

nyelv környezetfüggő és nem környezetfüggetlen. Megadunk egy L-t generáló Kuroda normálformában adott grammatikát.

A Bar-Hillel lemma segítségével megmutatható, hogy L nem környezetfüggetlen. Az L generálható azzal a $G = (V_N, V_T, S, H)$ hosszúságot nem csökkentő grammatikával, amelyre $V_N = \{S, A\}$ és

$$H = \{S \longrightarrow xSAx,\ S \longrightarrow xyx,\ xA \longrightarrow Ax,\ yA \longrightarrow yy\}.$$

A 4.1 Lemma szerint L környezetfüggő. A 4.6 Tétel szerint van G-vel ekvivalens Kuroda normálformában adott grammatika. Az alábbiakban megszerkesztjük ezt a grammatikát.

Először átalakítjuk a 2.2 Lemma bizonyításában megadott módon standard 1 típusú $G' = (V_N, V_T, S, H')$ g rammatikává. Felvesszük az $X, Y \notin V_N \cup V_T$ új változókat, azaz $V'_N = V_N \cup \{X, Y\}$ és H' legyen az

$$S \longrightarrow XSAX, \quad S \longrightarrow XYX, \quad XA \longrightarrow AX,$$

$$YA \longrightarrow YY, \quad X \longrightarrow x, \quad Y \longrightarrow y$$

szabályok halmaza. Utána a 4.6 Tétel bizonyítása szerint járunk el. A 3.3 Tétel bizonyításában alkalmazott eljárással az $S \longrightarrow XSAX$ és $S \longrightarrow XYX$ szabályokat kicseréljük H'-ben az

$$S \longrightarrow XX_1, X_1 \longrightarrow SX_2, \quad X_2 \longrightarrow AX,$$

ill. az

$$S \longrightarrow XY_1, \quad Y_1 \longrightarrow YX$$

szabályokkal és kiegészítjük V'_N-t az $X_1, X_2, Y_1 \notin V'_N \cup V_T$ új változókkal. Ilyen módon eljutunk a változók V''_N és a szabályok H'' halmazához. A $G'' = (V''_N, V_T, S, H'')$ grammatika ekvivalens G'-vel, így G-vel is, és Kuroda normálformában van megadva. (Ha lenne olyan szabály is, amelynek bal oldala kettőnél nagyobb hosszúságú, akkor ezekre a 4.6 Tétel bizonyításában megadott eljárást alkalmaznánk.)

Az $L = \{x^k y^k x^k; k \geq 0\}$ környezetfüggő nyelv generálható azzal a grammatikával, amelyet G-ből úgy kapunk, hogy felvesszük a szabályok közé az $S \longrightarrow e$ szabályt. Ez azt jelenti, hogy generálható azzal a grammatikával is, amelyet G''-ből kapunk az $S \longrightarrow e$ szabály felvételével.

Feladatok

4.1. Tetszőleges U ábécé feletti rekurzív nyelvek Boole algebrát alkotnak a szokásos halmazelméleti műveletekre.
4.2. Tetszőleges U ábécé feletti rekurzív nyelvek nyelvalgebrát alkotnak, azaz zártak a reguláris műveletekre.

5. fejezet

Mondatszerkezetű nyelvek

A 11.3 Következményben megmutatjuk, hogy a mondatszerkezetű nyelvek osztálya megegyezik a rekurzíve felsorolható nyelvek osztályával. Jelölje $\mathcal{L}_r$ a rekurzív nyelvek osztályát. A 4.3 és a 4.5 Tételek szerint

$$\mathcal{L}_1 \subset \mathcal{L}_r \subset \mathcal{L}_0.$$

A 4.5 Tétel bizonyítása szerint van olyan rekurzíve felsorolható nyelv, amelynek komplementere nem rekurzíve felsorolható. Ebből következik, hogy a mondatszerkezetű nyelvek osztálya nem zárt a komplementerképzésre.

5.1. Révész normálforma

A mondatszerkezetű grammatikákhoz megadható a finomított Kuroda normálforma egy általánosítása. A $G = (V_N, V_T, S, H)$ grammatikáról azt mondjuk, hogy *Révész normálformá*jú, ha a H-beli szabályok

$$S \longrightarrow e,\ X \longrightarrow x,\ X \longrightarrow Y, X \longrightarrow YZ, XY \longrightarrow XZ,\ XY \longrightarrow ZY, XY \longrightarrow Y \tag{5.1}$$

alakúak lehetnek, ahol az S mondatszimbólum csak a szabályok bal oldalán fordulhat elő.

5.1. Tétel. *Minden* 0 *típusú grammatikához van ekvivalens Révész normálformájú grammatika.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ tetszőleges 0 típusú grammatika. Először a $P \longrightarrow e$ alakú szabályokat helyettesítjük az $xP \longrightarrow x$ és $Px \longrightarrow x$ szabályokkal, ahol x befutja a teljes $V_N \cup V_T$ ábécét. Ezáltal olyan grammatikát kapunk, amely az $L(G) - e$ nyelvet generálja. Ha $e \in L(G)$, akkor a szabályok közé felvesszük az $S \longrightarrow e$ szabályt, így egy a G-vel ekvivalens

G' grammatikát kapunk. Ez a 2.3 Lemma szerint átalakítható standard 0 típusú grammatikává, azaz amelyben minden terminálist is tartalmazó szabály $X \longrightarrow x$ ($X \in V_n, x \in V_T$) alakú. Az így kapott szabályokon és az esetlegesen szereplő $S \longrightarrow e$ szabályon kívül az összes többi szabály ekkor $P \longrightarrow Q$ alakú lesz, ahol $P, Q \in V_N^+$. Ezek közül a hosszúságot nem csökkentő szabályokat helyettesítjük a finomított Kuroda normálforma megszerkesztésének előző fejezetben megismert eljárásával.

Ezért csak a hosszúságot csökkentő szabályokkal kell foglalkoznunk. Egy ilyen szabály

$$X_1X_2 \dots X_k \longrightarrow Y_1Y_2 \longrightarrow Y_n, \quad X_1, \dots, X_k, Y_1, \dots Y_n \in V_N,\ k > n \geq 1$$

alakú. Ezt helyettesítjük az

$$X_{k-1}X_k \longrightarrow Z_kW_k,\ Z_kW_k \longrightarrow W_k,$$

$$X_{k-2}W_k \longrightarrow Z_{k-1}W_{k-1},\ Z_{k-1}W_{k-1} \longrightarrow W_{k-1},\ \dots,$$
$$X_nW_{n+2} \longrightarrow Z_{n+1}W_{n+1},\ Z_{n+1}W_{n+1} \longrightarrow W_nY_n,$$
$$X_{n-1}W_n \longrightarrow W_{n-1}Y_{n-1},\ \dots,\ X_1W_2 \longrightarrow W_1Y_1,\ W_1Y_1 \longrightarrow Y_1$$

szabályokkal, ahol $W_1, \dots W_k, Z_{n+1}, \dots Z_k$ újonnan bevezetett változók. Itt az $AB \longrightarrow CD$ alakú szabályok mindegyikét helyettesíthetjük, a Kuroda normálforma finomításánál megismert módon, négy-négy környezetfüggő szabállyal.

Belátható, hogy ezekkel a helyettesítésekkel az erdetivel ekvivalens 0 típusú grammatikát kapunk, amelynek szabályai (5.1) alakúak. □

A fenti bizonyítás csak akkor ad egy algoritmust a normálforma megszerkesztésére, ha el tudjuk dönteni, hogy $e \in L(G)$ vagy $e \notin L(G)$ teljesül. Ha a G grammatikban nincsenek $P \longrightarrow e$ alakú szabályok, akkor természetesen $e \notin L(G)$. Ilyen szabályok létezéséből, kivéve az $S \longrightarrow e$ szabályt, nem feltétlenül következik, hogy $e \in L(G)$. Egy olyan grammatikát mindig el tudunk készíteni a bizonyításban szereplő eljárással, amelyre az $L(G) - e$ nyelvet generálja. Ahhoz viszont, hogy az $S \longrightarrow e$ szabály felvegyük-e vagy sem, tudnunk kell, hogy $e \in L(G)$ vagy $e \notin L(G)$. A 5.1 Tétel természetesen igaz, mert $e \in L(G)$ vagy $e \notin L(G)$, azaz nincs harmadik lehetőség, még akkor sem ha nem tudjuk eldönteni, hogy melyik eset áll fenn. A 4.2 Tétel szerint az 1 típusú grammatikáknál ez a kérdés mindig eldönthető. Ott ugyanis bármely szó levezetésénél mindig csak véges sok különböző szó fordulhat elő. A 0 típusú grammatikáknál éppen ezt a végességet nem lehet garantálni, mivel hosszúságot növelő és csökkentő szabályok egyaránt lehetnek. Ezért, mint már említettük, általában a 0 típusú nyelvekre a 4.2 Tétel nem terjeszthető ki.

5.2. Balról rendezett levezetések

Bizonyos fokig csökkenthetjük a megvizsgálandó levezetések számát az alábbiakban definiált speciális levezetésekkel, bár ez nem sokat segít a tartalmazási probléma eldöntésében.

Legyen $G = (V_N, V_T, S, H)$ tetszőleges generatív grammatika. A

$$W_0 \Longrightarrow_G W_1 \Longrightarrow_G \cdots \Longrightarrow_G W_n \tag{5.2}$$

levezetést *balról rendezett*nek mondjuk, ha vannak olyan

$$R_j, P_j, Q_j, T_j \in (V_N \cup V_T)^*, \quad j = 0, 1, \ldots, n$$

szavak, amelyekre

$$W_j = R_j P_j T_j, \quad W_{j+1} = R_j Q_j T_j,$$

ahol $P_j \longrightarrow Q_j$ H-beli szabályok és

$$|R_j| \leq |R_{j+1} P_{j+1}|, \quad j = 0, 1, \ldots, n-1. \tag{5.3}$$

A *jobbról rendezett levezetés*t hasonlóan definiáljuk. (A (5.3) feltételek helyett a

$$|T_j| \leq |Q_{j+1} T_{j+1}|, \quad j = 0, 1, \ldots, n-1. \tag{5.4}$$

feltételek szerepelnek.)

Ay (5.2) és az 5.3) [(5.4)] definíciókból nyilvánvalóan következik, hogy a környezetfüggetlen grammatikákra definiált bal [jobb] oldali levezetések balról [jobbról] rendezett levezetések.

5.2. Tétel. *Bármely $G = (V_N, V_T, S, H)$ generatív grammatikában egy tetszőleges $P \Longrightarrow_G^* Q$ levezetéshez megadható egy ugyanolyan hosszú P-vel kezdődő és Q-val végződő balról [jobbról] rendezett levezetés.*

Bizonyítás A bizonyítást csak a balról rendezett esetre végezzük el. A bizonyítás jobbról rendezett esetben nyilván hasonlóan végezhető el. Tegyük fel, hogy (5.2)-ben definiált $P \Longrightarrow_G^* Q$ levezetés nem balról rendezett. Legyen $0 \leq k < n$ a legkisebb olyan index, amelyre a balról rendezettség (5.3) feltétele nem teljesül, vagyis vannak olyan $P_k \longrightarrow Q_k$ és $P_{k+1} \longrightarrow Q_{k+1}$ szabályok, amelyekre $W_k = R_k P_k T_k$, $W_{k+1} = R_k Q_k T_k$ és

$$|R_k| > |R_{k+1} P_{k+1}|.$$

Eszerint $R_k = R_{k+1} P_{k+1} U_{k+1}$, valamely $U_{k+1} \in (V_N \cup V_T)^+$ szóra. Ez azt jelenti, hogy a levezetésben a k-adik és $(k+1)$-edik lépést felcserélhetjük, azaz

$$R_kP_kT_k \implies_G R_kQ_kT_k = R_{k+1}P_{k+1}U_{k+1}Q_kT_k \implies_G R_{k+1}Q_{k+1}U_{k+1}Q_kT_k$$

lépések helyett vehetjük az

$$R_kP_kT_k = R_{k+1}P_{k+1}U_{k+1}P_kT_k \implies_G$$

$$\implies_G R_{k+1}Q_{k+1}U_{k+1}P_kT_k \implies_G R_{k+1}Q_{k+1}U_{k+1}Q_kT_k$$

lépéseket. Így a balról rendezettség a k és $(k+1)$-edik lépésekre teljesülni fog. Az eljárást mindaddig megismételjük, amig a teljes levezetés balról rendezett nem lesz. □

Már láttuk, hogy környezetfüggetlen grammatikákban a levezetések megadhatók egy irányított gráf, a levezetési fa segítségével, ahol a végpontokhoz terminális jelek, egyéb csúcspontokhoz változók vannak rendelve. Ezt a megadási módot minden további nélkül nem lehet átvinni környezetfüggő és mondatszerkezetű grammatikákra, mivel itt a szabályok bal oldalán egynél több jelből álló sorozatok is állhatnak. Ezt a nehézséget könnyen áthidalhatjuk az alábbi módon. A $G = (V_N, V_T, S, H)$ grammatika minden egyes szabályát címkézzük meg. Ez azt jelenti, hogy vegyünk egy F halmazt, amely annyi elemet tartalmaz, mint ahány H-beli szabály van. Tegyük fel, hogy $F \cap (V_n \cup V_T) = \emptyset$. Minden szabályhoz rendeljük hozzá kölcsönösen egyértelmű módon F egy elemét, másképpen mondva, címkézzük meg a szabályokat F elemeivel. A *levezetési fá*t ezek után úgy adunk meg egy levezetéshez, hogy minden szabály alkalmazásához beiktatunk még egy-egy új csúcspontot, amelyhez a szóban forgó szabály címkéjét rendeljük hozzá. A szabály bal oldalán álló jelsorozat egyes betűinek megfelelő csúcspontokból irányított élet húzunk ebbe az új csúcspontba, majd ez utóbbiból kimenő éleket húzunk a szabály jobb oldalán álló jelsorozat egyes betűinek megfelelő csúcspontokba.

Legyenek például $V_N = \{S, A, B\}$, $V_T = \{a, b\}$, a H-beli szabályok pedig:

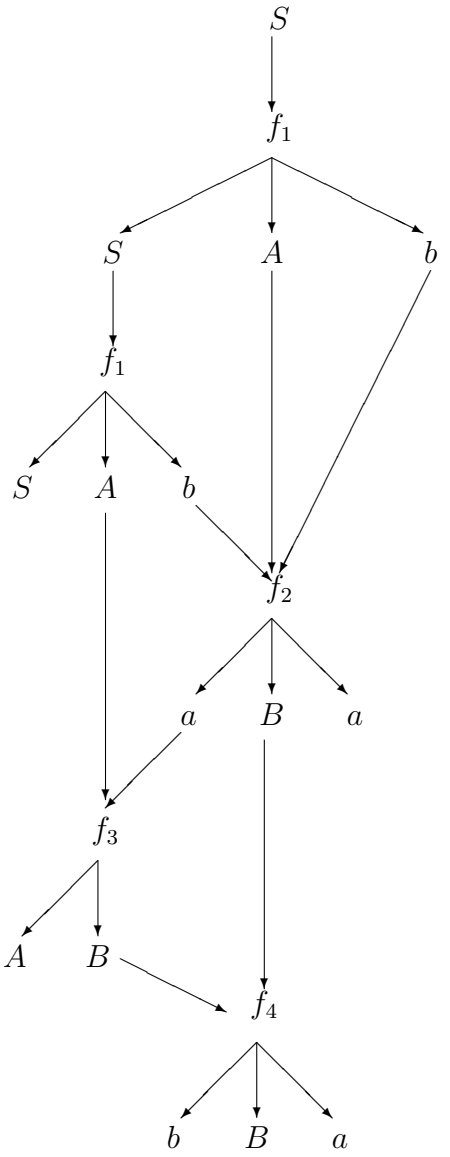
$$f_1 : S \longrightarrow SAb,\ f_2 : bAb \longrightarrow aBa,\ f_3 : Aa \longrightarrow AB,\ f_4 : BB \longrightarrow aBb.$$

(A szabályokat az $F = \{f_1, f_2, f_3, f_4\}$ halmaz elemeivel címkéztük meg.)

Az

$$S \implies SAb \implies SAbAb \implies SAaBa \implies SABBa \implies SAaBba$$

levezetés fáját a 5.1. ábra mutatja. A levezetés $SAaBba$ eredményét most is a végpontokat megjelölő betűk balról jobbra való leolvasásával kapjuk meg. A levezetés fája most is lényegében egyértelműen ábrázolja az adott levezetést, vagyis a gráfról leolvasható levezetések között legfeljebb egyes szabályok



5.1. ábra.

végrehajtásának sorrendjében lehet különbség. (A mi példánkban a szabályok sorrendje nem változtatható.) Belátható, hogy minden ilyen gráfhoz egyegyértelműen hozzárendelhető egy balról rendezett levezetés.

Megjegyezzük, hogy minden mondatszerkezetű nyelv homomorfan karak-

terizálható két környezetfüggetlen nyelv közös részével. Az érdeklődő olvasó az ezzel kapcsolatos vizsgálatokat megtalálhatja például Arto Salomaa [40] könyvében.

5.3. Algoritmikusan eldönthetetlen problémák

Az előző alfejezet alapján látjuk, hogy a mondatszerkezetű nyelvek osztálya nem rekurzív, azaz nem minden U ábécé feletti L mondatszerkezetű nyelvre dönthető el a szóprobléma, azaz nem minden mondatszerkezetű nyelv esetén dönthető el algoritmikusan az, hogy egy $p \in U^*$ szó benne van-e L-ben vagy nem. Ebből további algoritmikusan eldönthetetlen problémák következnek, amelyek közül vannak olyanok, amelyek szűkebb nyelvosztályokra sem dönthető el. Ebben az alfejezetben ezekre adunk néhány példát.

A 3.9 Tétel szerint bármely környezetfüggetlen grammatikáról algoritmikusan eldönthető, hogy az általa generált nyelv üres, véges vagy végtelen. Ez azonban környezetfüggő grammatikákra már nem igaz.

5.3. Tétel. *Nem minden környezetfüggő grammatikáról dönthető el algoritmikusan, hogy az általa generált nyelv üres, véges vagy végtelen.*

Bizonyítás Legyen $G = (V_N, V_T, S, H)$ tetszőleges 0 típusú grammatika és $p \in V_T^*$ tetszőleges szó. Legyenek $S_0, S_1, S_2, S_3, a \notin V_N \cup V_T$ and $G' = (V'_N, V'_T, S_0, H')$ az a 1 típusú grammatika, amelyre

$$V'_N = V_N \cup V_T \cup \{S_0, S_1, S_2, S_3\}, \quad V'_T = \{a\}.$$

A H'-beli szabályokat pedig a következőképpen definiáljuk:

$$P \longrightarrow Q \in H', \text{ha} \quad P \longrightarrow Q \in H \quad \text{és} \quad |P| \leq |Q|;$$
$$P \longrightarrow QS_1^k \in H', \text{ha} \quad P \longrightarrow Q \in H \quad \text{és} \quad |P| = |Q| + k,\ k > 0;$$
$$S_1 A \longrightarrow AS_1 \in H', \quad \text{ha} \quad A \in V_N \cup V_T.$$

Továbbá az

$$S_0 \longrightarrow SS_1S_2,\ pS_1 \longrightarrow a^{|p|}S_1,\ S_3S_1 \longrightarrow aS_3,\ S_3S_2 \longrightarrow aa$$

szabályok is H'-beliek. Megmutatható, hogy $L(G') \neq \emptyset$ akkor és csak akkor, ha $p \in L(G)$. Mivel a mondatszerkezetű nyelvek osztálya nem rekurzív, ezért az 1 típusú nyelvek osztálya esetén az üresség problémája algoritmikusan nem dönthető el.

Ha a H'-beli szabályokat kiegészítjük az $S_1 \longrightarrow S_1S_1$ szabállyal, akkor $L(G')$ akkor és csak akkor végtelen, ha $p \in L(G)$. Ez azt jelenti, hogy a végtelenség problémája az 1 típusú nyelvek osztálya esetén algoritmikusan szintén nem dönthető el. □

Algoritmikusan eldönthetetlen még például, hogy adott ábécé feletti két környezetfüggetlen nyelv metszete vagy egy környezetfüggetlen nyelv komplementere üres, véges (végtelen), reguláris, környezetfüggetlen. Algoritmikusan eldönthetetlen az is, hogy egy környezetfüggetlen nyelv reguláris. Továbbá adott ábécé feletti két környezetfüggetlen nyelv egyenlő vagy az egyik tartalmazza a másikat. Ezek a vizsgálatok is megtalálhatja Arto Salomaa [40] már az előző alfejezetben említett monográfiájában.

5.4. Geffert normálformák

Végül bizonyítás nélkül említünk néhány Viliam Gefferttől származó további normálformát mondatszerkezetű nyelvekre. A bizonyítás a 0 típusú nyelvek és a Turing automaták 11.3 Következmény szerinti kapcsolatán alapul.

A $G = (V_N, V_T, S, H)$ grammatikáról azt mondjuk, hogy *Geffert normálformá*jú, ha $3 \leq |V_N| \leq 5$, a H-beli szabályok $S \longrightarrow P$ ($P \in (V_N \cup V_T)^*$) típusú környezetfüggetlen szabályok és az alábbiakban felsorolt öt szabálycsoport közül valamelyik:

$$AB \longrightarrow e, \quad CD \longrightarrow e \quad (V_N = \{S, A, B, C, D\});$$

$$AB \longrightarrow e, \quad CC \longrightarrow e \quad (V_N = \{S, A, B, C\});$$

$$ABC \longrightarrow e \quad (V_N = \{S, A, B, C\});$$

$$AA \longrightarrow e, \quad BBB \longrightarrow e \quad (V_N = \{S, A, B\});$$

$$ABBBA \longrightarrow e, \quad (V_N = \{S, A, B\}).$$

Nyilvánvaló, hogy a Geffert normálformájú grammatikák mondatszerkezetű grammatikák.

5.4. Tétel. *Minden* 0 *típusú grammatikához van ekvivalens bármilyen Geffert normálformájú grammatika.*

Az érdeklődő olvasók kedvéért közöljük, hogy a tétel bizonyítása megtalálható például a *V. Geffert, Normal forms for phrase-structure grammars, Informatique théorique et applications, 25/5 (1991), 473-496* cikkben.

Feladat

5.1. Tetszőleges U ábécé feletti rekurzíve felsorolható nyelvek nyelvalgebrát alkotnak, azaz zártak a reguláris műveletekre.

II. rész

NYELVEK ÉS AUTOMATÁK

Ebben a részben a formális nyelveket automaták segítségével adjuk meg. A téma szép feldolgozása található Gécseg Ferenc [19] egyetemi jegyzetében. A [2] jegyzetünkben részletesen foglalkozunk az automaták algebrai elméletével. Itt most először röviden felelevenítjük az algebrai automataelmélet számunkra szükséges fogalmait és eredményeit. Majd részletesen tárgyaljuk a különböző Chomsky nyelvosztályokhoz tartozó nyelveket felismerő automaták típusait. Foglalkozunk a végtelen szavakat felismerő automatákkal is. Részletesebben vizsgáljuk a reguláris nyelvek nevezetesebb speciális típusait is. Megemlítünk azonban olyan nyelveket is, amelyek nem tartoznak a Chomsky nyelvosztályokhoz, de szorosan kapcsolódnak a kódok algebrai elméletéhez.

6. fejezet

Automaták

6.1. Az automata fogalma

*Mealy automatá*nak vagy röviden *automatá*nak nevezzük azt az

$$\mathbf{A} = (A, X, Y, \delta, \lambda)$$

rendszert, amely áll az $A \neq \emptyset$, $X \neq \emptyset$ és Y halmazokból, valamint a

$$\delta : A \times X \to A \quad \text{és} \quad \lambda : A \times X \to Y$$

függvényekből. Az A, X és Y halmaz elemeit rendre az $\mathbf{A}$ automata *állapotai*nak, *bemenő jelei*nek és *kimenő jelei*nek mondjuk, a halmazokat pedig értelemszerűen $\mathbf{A}$ *állapothalmazá*nak, *bemenő halmazá*nak és *kimenő halmazá*nak, a δ és λ függvényeket pedig $\mathbf{A}$ *átmenetfüggvény*ének ill. *kimenetfüggvény*ének nevezzük.

Egy Mealy automata működését úgy gondoljuk el, hogy ha az automata valamely t időpillanatban az $a \in A$ állapotban van és ebben az időpillanatban az $x \in X$ bemenő jelet kapja, akkor kiadja a $\lambda(a, x) \in Y$ jelet és a $t + 1$ időpillanatban átmegy a $\delta(a, x) \in A$ állapotba. Vagyis feltételezzük, hogy az automata diszkrét időskálával dolgozik, azaz meghatározott, egymástól elkülöníthető időpontokban kaphat bemenő jelet.

Ha az átmenet- és kimenetfüggvénye minden (a, x) $(a \in A, x \in X)$ párra értelmezve van, akkor az automatát *teljesen definiált*nak, ellenkező esetben pedig *parciális*nak mondjuk. A továbbiakban automatán mindig teljesen definiált automatát értünk. Ha parciális automatáról lesz szó, akkor azt külön jelezzük.

Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automatát *Moore automatá*nak nevezzük, ha létezik olyan $\mu : A \to Y$ függvény, hogy bármely $a \in A$ állapotra és $x \in X$ bemenő jelre

$$\lambda(a, x) = \mu(\delta((a, x)).$$

A μ függvényt a Moore automata *jelfüggvény*ének nevezzük és Moore automatákra az $\mathbf{A} = (A, X, Y, \delta, \mu)$ jelölést használjuk.

Moore automata működését is diszkrét időskálával képzeljük el, azaz ha az automata valamely t időpillanatban az $a \in A$ állapotban van, és az $x \in X$ bemenő jelet kapja, akkor a $t+1$ időpillanatban átmegy a $\delta(a, x) \in A$ állapotba és kiadja a $\mu(\delta(a, x))$ jelet.

Ha az Y kimenő halmaz üres, s így a λ kimenetfüggvény nincs értelmezve, akkor az automatát *kimenő jel nélküli automatá*nak nevezzük, amelynek a jelölése $\mathbf{A} = (A, X, \delta)$. Természetesen a kimenő jel nélküli automata felfogható olyan automataként is, amely mindig az üres jelet bocsátja ki. Ezért, ha egy automatának egyetlen kimenő jele van, akkor kimenő jel nélküli automatának is tekinthető. Így a kimenő jeles automaták esetében a kimenő halmazról feltesszük, hogy legalább kételemű halmaz. Az $\mathbf{A} = (A, X, \delta)$ kimenő jel nélküli automata tekinthető olyan $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automatának is, amelyre $\lambda = \delta$ teljesül. Ebben a esetben $Y = A$. A kimenő jel nélküli automata felfogható $\mathbf{A} = (A, X, Y, \delta, \mu)$ Moore automataként is, ahol $\mu = \iota_A$. Ebből következik, hogy $Y = A$.

Megjegyezzük, hogy ebben az alfejezetben a definíciókat és tételeket Mealy [Moore] automatákra mondjuk ki. Értelemszerűen ezek a kimenetfüggvényre [jelfüggvényre] vonatkozó feltételek nélkül kimenő jel nélküli automatákra is érvényesek.

Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automatát *redukált bemenetű*nek nek nevezzük, ha nincsenek un. *felesleges bemenő jelek*, vagyis minden $a \in A$ állapotra, ha $\delta(a, x_1) = \delta(a, x_2)$ és $\lambda(a, x_1) = \lambda(a, x_2)$, akkor $x_1 = x_2$.

Sokszor az $\mathbf{A}$ Mealy automata kimeneti viselkedése nem fontos számunkra, ezért az Y kimenő halmazt és a λ kimenetfüggvényt elhagyhatjuk. Az így kapott $\mathbf{A}_v = (A, X, \delta)$ kimenő jel nélküli automatát az $\mathbf{A}$ Mealy automata *vetület*ének vagy vagy *projekciójá*nak nevezzük.

Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automatához egy másik kimenő jel nélküli automatát is rendelünk, amely leírja az automata kimeneti viselkedését is. Az $\mathbf{A}$ Mealy automata *vázá*n azt az $\mathbf{A}_Y = (A \times Y, X, \delta_Y)$ kimenő jel nélküli automatát értjük, amelyre δ_Y-t minden $(a, y) \in A \times Y,\ x \in X$ esetén

$$\delta_Y((a, y), x) = (\delta(a, x), \lambda(a, x)). \tag{6.1}$$

Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ automatát *iniciális automatá*nak nevezzük, ha az A állapothalmazának valamely a_0 állapotát kijelöljük. Ekkor az

$$\mathbf{A} = (A, a_0, X, Y, \delta, \lambda)$$

vagy a $(\mathbf{A}, a_0)$ jelölést használjuk. Az a_0 állapotot az $\mathbf{A}$ automata *kezdőállapotá*nak vagy *iniciális állapotá*nak mondjuk és megállapodunk abban, hogy az automata működése kezdetén ebben az állapotban van.

Az $\mathbf{A}' = (A', X, Y, \delta', \lambda'[\mu'])$ automatát az $\mathbf{A} = (A, X, Y, \delta, \lambda]\mu])$ automata *részautomatá*jának, nevezzük, ha $A' \subseteq A$, a δ' és $\lambda'[\mu']$ függvények pedig a δ ill. λ függvények szűkítései a $A' \times X$ halmazra. Ha nem vezet ellentmondásra, akkor δ'-t és λ'-t [μ'-t] is egyszerűen δ-val ill. λ-val [μ]-vel] jelöljük.

A $c \in A$ állapotot $\mathbf{A}$ *csapdájá*nak nevezzük, ha minden $x \in X$ bemenő jelre $\delta(c, x) = c$. Ez pontosan azt jelenti, hogy $(\{c\}, X, Y, \delta, \lambda)$ az $\mathbf{A}$ automata egyállapotú részautomatája.

6.2. Véges automaták

Az automatát *véges*nek, nevezzük, ha az A, X halmazok, s így az Y halmaz is tekinthető végesnek. Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ véges Mealy automata *átmenet-kimenettáblázat*án olyan téglalap alakú táblázatot értünk, amelynek sorait $\mathbf{A}$ bemenő jeleivel, oszlopait pedig $\mathbf{A}$ állapotaival jelöljük meg. Az $x \in X$ bemenő jellel megjelölt sor és az $a \in A$ állapottal megjelölt oszlop metszetébe a $(\delta(a, x), \lambda(a, x))$ rendezett párt írjuk:

A	a
	$\vdots$
x	$\cdots \quad (\delta(a, x), \lambda(a, x)) \quad \cdots$
	$\vdots$

Megállapodunk abban, hogy ha az automata iniciális, akkor az oszlopok megjelölését a kezdőállapottal kezdjük. Az $\mathbf{A} = (A, X, Y, \delta, \mu)$ Moore automata átmenet-kimenettáblázata (bal oldali táblázat) abban különbözik az előző táblázattól, hogy az x-szel jelölt sor és az a-val jelölt oszlop metszetében csak a $\delta(a, x)$ állapot áll és az a állapot fölé a $\mu(a)$ kimenő jel kerül.

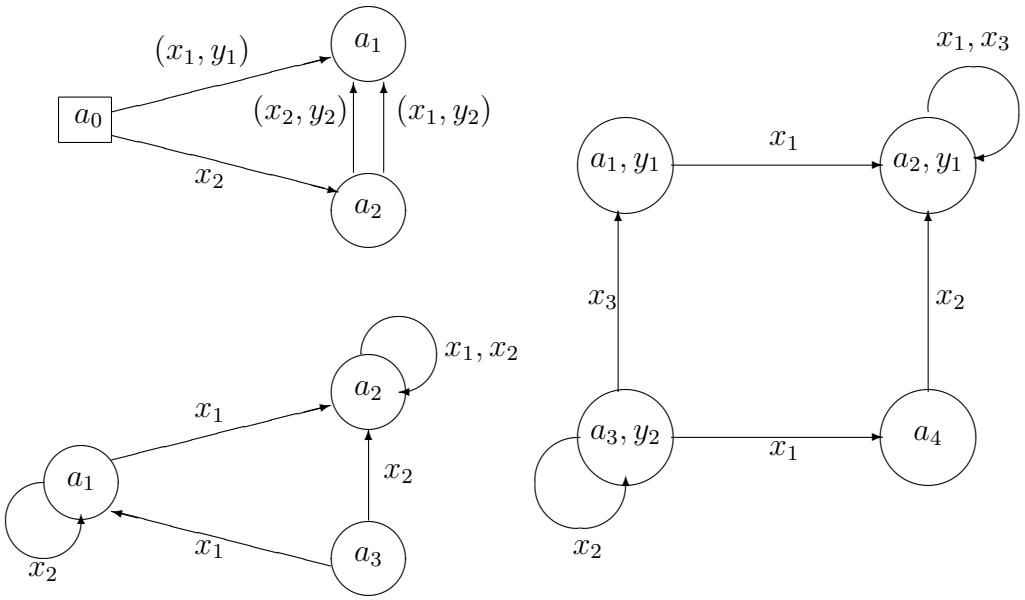
	$\mu(a)$
$\mathbf{A}$	a
	$\vdots$
x	$\cdots \quad \delta(a, x) \quad \cdots$
	$\vdots$

$\mathbf{A}$	a
	$\vdots$
x	$\cdots \quad \delta(a, x) \quad \cdots$
	$\vdots$

Parciális automaták esetén a táblázatokban azokat a helyeket nem töltjük ki, ahol az egyes függvények nincsenek értelmezve.

A véges automaták működését megadhatjuk irányított gráffal is. Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ véges Mealy automata *átmenet-kimenetgráfjá*n azt az irányított gráfot értjük, amelynek kis körökkel ábrázolt csúcsait megjelöljük az automata állapotaival. Az $a \in A$ állapottal megjelölt csúcsból akkor és csak akkor vezet a

$b \in A$ állapottal megjelölt csúcsba az (x, y) rendezett párral megjelölt irányított él, ha az $x \in X$ bemenő jel hatására az automata az a állapotból átmegy a b állapotba, miközben kiadja az y jelet, azaz $\delta(a, x) = b$ és $\lambda(a, x) = y$. Parciális automata esetén előfordulhat, hogy nem minden x bemenő jelre vezet az a állapottal megjelölt csúcsból valamilyen (x, y) rendezett párral megjelölt irányított él egy másik csúcsba. Az is lehet, hogy az irányított él csak az x bemenő jellel van megjelölve. Ez azt jelenti, hogy az automata nem ad ki jelet ennél az átmenetnél. Megállapodunk abban, hogy iniciális automata kezdő állapotát kör helyett egy kis négyzet ábrázolja. Az $\mathbf{A} = (A, X, Y, \delta, \mu)$ Moore automata átmenet-kimenetgráfja az előbbi gráftól annyiban tér el, hogy az $a \in A$ állapot $\mu(a)$ jelét az a-val megjelölt csúcshoz írjuk. Az a-val megjelölt csúcsból, röviden a-ból, akkor és csak akkor vezet $x \in X$ bemenő jellel megjelölt irányított él b-be, ha $\delta(a, x) = b$. Ezek alapján nyilvánvalóan adódik egy kimenő jel nélküli automata *átmenetgráfja*. Az 6.1. ábrában egy Mealy, Moore ill. kimenő jel nélküli automata gráfja látható.



6.1. ábra.

6.3. Az automaták szekvenciális működése

Legyen $\mathbf{A} = (A, X, Y, \delta, \lambda)$ tetszőleges Mealy automata. Az X^* és Y^* szabad monoidokat $\mathbf{A}$ *bemenő félcsoport*jának ill. *kimenő félcsoport*jának, elemeiket

pedig **A** *bemenő szavai*nak ill. ill. *kimenő szavai*nak fogjuk mondani.

A δ és λ függvények értelmezését kiterjesztjük a következő módon. Az egyszerűség kedvéért a függvényeket a kiterjesztés után is δ ill. λ jelöli. Legyenek

$$\delta : A \times X^* \to A^+ \quad \text{és} \quad \lambda : A \times X^* \to Y^* \tag{6.2}$$

olyanok, hogy tetszőleges $a \in A$ állapotra és az e üres szóra teljesüljenek

$$\delta(a, e) = a \quad \text{és} \quad \lambda(a, e) = e, \tag{6.3}$$

feltételek, továbbá bármely $p = x_1 x_2 \dots x_k \in X^+$ bemenő szó esetén legyen

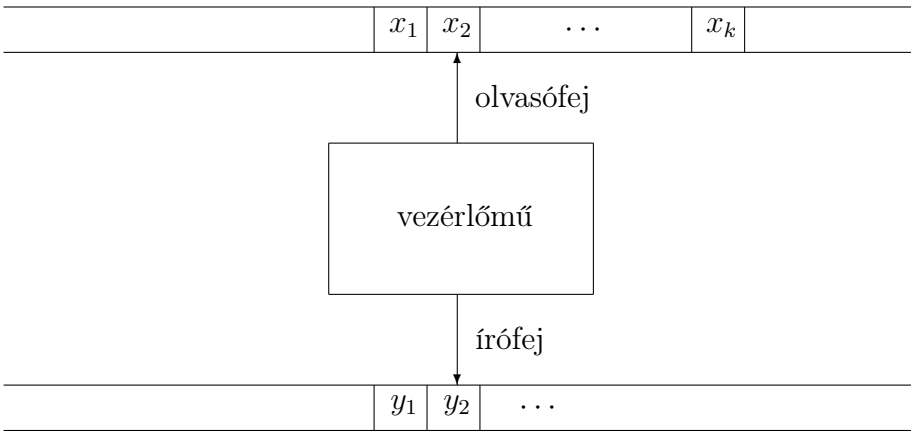
$$\delta(a, p) = a_1 a_2 \dots a_k \quad \text{és} \quad \lambda(a, p) = y_1 y_2 \dots y_k, \tag{6.4}$$

ahol

$$a_1 = \delta(a, x_1),\ a_2 = \delta(a_1, x_2),\ \dots,\ a_k = \delta(a_{k-1}, x_k),$$
$$y_1 = \lambda(a, x_1),\ y_2 = \lambda(a_1, x_2),\ \dots,\ y_k = \lambda(a_{k-1}, x_k).$$

A Mealy automata átmenetfüggvényének és kimenetfüggvényének ez a kiterjesztése azt mutatja, hogy ha az automata nem kap bemenő jelet, vagyis az üres szót kapja, akkor állapotát nem változtatja meg és nem ad ki jelet. Ha pedig egy k jelből álló jelsorozatot kap, akkor ennek hatására ugyancsak k jelből álló jelsorozatot bocsát ki. Az automata úgy működik, hogy a bemenő szó jeleit balról jobbra egymásután "olvassa el", állapotok egy sorozatán megy keresztül és közben a kimenő jeleket is egymásután adja ki. E tulajdonság alapján azt mondjuk, hogy az automata *szekvenciális működésű gép*. Ezt a 6.2. ábra alapján szemléletesen például úgy képzelhetjük el, hogy az automatának (vezérlőműnek) van egy olvasófeje és egy írófeje. Az olvasófej előtt egy rekeszekre osztott szalag (bemenő szalag) mozog. A bemenő szalag egyes rekeszeibe legfeljebb egy betű írható. A szalagra sorra rá vannak írva a bemenő szó betűi. Az automata az olvasófej segítségével egymás után beolvassa a szó betűit, a leolvasás ütemében állapotok sorozatán megy át, s ebben az ütemben az állapotátmenetekkel vezérli az írófejet, az írófej az előtte mozgó másik szalagra (kimenő szalag) kiírja a megfelelő szót.

A definícióban szereplő $a_1, a_2, \dots, a_{k-1}$ állapotokat az $a, a_1, a_2, \dots a_{k-1}, a_k$ állapotsorozat *közbülső állapotai*nak is nevezzük, az a_k állapotra pedig az $(ap)_{\mathbf{A}}$ jelölést is használjuk. Ha nem vezet ellentmondásra, azaz csak egy automatát vizsgálunk, akkor $(ap)_{\mathbf{A}}$-t helyett a rövidebben ap jelölést használjuk. Ha az $a, b \in A$ állapotokhoz van olyan $p \in X^*$ bemenő szó, amelyre $b = ap$ teljesül, akkor azt mondjuk, hogy *a b állapot* (*a p szóval*) *elérhető az a állapotból*. Iniciális automatát *iniciálisan összefüggő*nek nevezzük, ha a kezdőállapotból bármely állapota elérhető. Ha pedig $a \in A$ állapotra és a $p \in X^*$ bemenő szóra



6.2. ábra.

az *ap* állapot létezik, akkor azt mondjuk, hogy *az automata az a állapotban elfogadja vagy felismeri az p bemenő szót.*

Ha az $\mathbf{A} = (A, X, Y, \delta, \mu)$ Moore automata esetében a δ átmenetfüggvény kiterjesztését a Mealy automatákra megismert módon végezzük el, μ jelfüggvény értelmezését pedig homomorf módon terjesztjük ki az A^+ szabad félcsoportra, vagyis úgy, hogy minden $a_1 \dots a_k \in A^+$ állapotsorozatra

$$\mu(a_1 \dots a_k) = \mu(a_1) \dots \mu(a_k). \tag{6.5}$$

6.4. Nemdeterminisztikus automaták

Az eddigi automaták mind olyanok, hogy ha egy adott állapotban egy adott bemenő jelet elfogadnak, akkor egyértelműen megmondható, hogy melyik állapotba mennek át, s ha adnak ki kimenő jelet, akkor melyiket. Az ilyen automatákat *determinisztikus automaták*nak nevezzük. Szükségünk lesz azonban a nemdeterminisztikus automaták fogalmára is.

Az $\mathbf{A} = (A, X, Y, \delta, \lambda)$ *nemdeterminisztikus Mealy automata* fogalmát a determinisztikus Mealy automata fogalmából úgy kapjuk, hogy a δ átmenetfüggvény és a λ kimenetfüggvény értelmezését módosítjuk, mégpedig legyenek

$$\delta : A \times X \to P(A), \quad \lambda : A \times X \to P(Y) \tag{6.6}$$

alakúak, ahol $P(A)$ és $P(Y)$ az A ill. Y hatványhalmazát jelöli. Megjegyezzük, hogy a definíció szerint a nemdeterminisztikus Mealy automata akkor is

adhat kimenő jelet, ha nem kap bemenő jelet. Látható, hogy egy determinisztikus $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automata olyan nemdeterminisztikus Mealy automatának tekinthető, amelyben minden $a \in A$ és $x \in X$ esetén

$$\delta(a, x)| \leq 1, \quad |\lambda(a, x)| \leq 1. \tag{6.7}$$

Az $\mathbf{A} = (A, X, Y, \delta, \mu)$ *nemdeterminisztikus Moore automata* annyiban különbözik egy nemdeterminisztikus Mealy automatától, hogy a $\lambda : A \times X \to P(Y)$ kimenetfüggvény helyett az

$$\mu : A \to P(Y) \tag{6.8}$$

jelfüggvény szerepel.

A nemdeterminisztikus automatákat is inicializálhatjuk, azaz kijelölhetünk kezdőállapotoknak egy halmazát, és úgy tekintjük, hogy az automata működése kezdetén valamelyik kezdőállapotban van.

Mivel alapvetően a determinisztikus automatákat tanulmányozzuk, ezért a továbbiakban automatán mindig determinisztikus automatát értünk, és jelezük, ha nemdeterminisztikus automatáról lesz szó.

A teljesen definiált nemdeterminisztikus automata működése annyiban különbözik a teljesen definiált determinisztikus automata működésétől, hogy ha az automata az $a \in A$ állapotban az $x \in X$ bemenő jelet kapja, akkor valamelyik $\delta(a, x)$-beli állapotba megy át és kiad egy $\lambda(a, x)$-beli jelet. A parciális nemdeterminisztikus automata pedig lehet olyan a állapotban, amelyben nem fogad el minden bemenő jelet, vagy ha minden bemenő jelet el is fogad, előfordulhat olyan x bemenő jel, hogy miközben az automata átmegy a $\delta(a, x)$ állapotok egyikébe, nem ad kimenő jelet. Természetesen az is lehetséges, hogy az automata úgy kimnenő jelet, hogy nem kap bemenő jelet.

Nemdeterminisztikus automata átmenet-kimenetgráfja olyan, hogy egy csúcsból több olyan irányított él is vezethet csúcsokba, amelyeket megjelölő rendezett párok első vagy második tagja megegyezik.

6.5. Homomorfizmus, izomorfizmus

Legyenek $\mathbf{A} = (A, X, Y, \delta, \lambda[\mu])$ és $\mathbf{A}' = (A', X, Y, \delta', \lambda'[\mu'])$ tetszőleges Mealy [Moore] automaták. Azt mondjuk, hogy az $\alpha : A \to A'$ leképezés az $\mathbf{A}$ *automatának az* $\mathbf{A}'$ *automatába való homomorfizmusa* vagy *homomorf leképezése*, ha minden $a \in A,\ x \in X$ párra

$$\alpha(\delta(a, x)) = \delta'(\alpha(a), x), \tag{6.9}$$

$$\lambda(a, x) = \lambda'(\alpha(a), x) \quad [\mu(a) = \mu'(\alpha(a))]. \tag{6.10}$$

Ha még α szürjektív is, akkor azt mondjuk, hogy az $\mathbf{A}'$ automata az $\mathbf{A}$ automata *homomorf képe*, aminek a jelölése: $\mathbf{A} \sim \mathbf{A}'$. Használjuk az $\mathbf{A}' = \alpha(\mathbf{A})$ jelölést is. Ha α bijektív, akkor azt mondjuk, hogy az $\mathbf{A}'$ automata az $\mathbf{A}$ automata *izomorf képe*, aminek a jelölése: $\mathbf{A} \simeq \mathbf{A}'$.

Automaták valamely homomorfizmusát *iniciális homomorfizmus*nak nevezzük, ha kezdőállapot homomorf képe is kezdőállapot.

6.6. Automaták kongruenciái

Legyen $\mathbf{A} = (A, X, Y, \delta, \lambda[\mu])$ tetszőleges Mealy [Moore] automata. A $\rho \subseteq A^2$ ekvivalenciát $\mathbf{A}$ *kongruenciájá*nak nevezzük, ha minden $a, b \in A$ állapotpárra és $x \in X$ bemenő jelre teljesülnek az

$$(a,b) \in \rho \implies (\delta(a,x), \delta(b,x)) \in \rho \quad \text{és } \lambda(a,x) = \lambda(b,x)\ [\mu(a) = \mu(b)] \tag{6.11}$$

feltételek. Ez parciális automata esetén jelentse azt is, hogy $\delta(a,x)$ $[\lambda(a,x)$, $\mu(a)]$ akkor és csak akkor van értelmezve, ha $\delta(b,x)$ $[\lambda(b,x)$, $\mu(b)]$ is értelmezve van. Nem nehéz belátni, hogy a ρ ekvivalencia akkor és csak akkor kongruencia, ha az $(a,b) \in \rho$ feltételből minden $p \in X^*$ bemenő szóra következik, hogy

$$(ap, bp) \in \rho \quad \text{és} \quad \lambda(a,p) = \lambda(b,p) \quad [\mu(\delta(a,p)) = \mu(\delta(b,p))]. \tag{6.12}$$

Legyen ρ az $\mathbf{A} = (A, X, Y, \delta, \lambda[\mu])$ Mealy [Moore] automata egy kongruenciája és A/ρ az A állapothalmaz ρ szerinti faktorhalmaza. Definiáljuk az $\mathbf{A}/\rho = (A/\rho, X, Y, \delta_\rho, \lambda_\rho[\mu_\rho])$ Mealy [Moore] automatát, amelyre a δ_ρ átmenetfüggvényt és a λ_ρ kimenetfüggvényt [μ_ρ jelfüggvényt] minden $a \in A$ állapotra és $x \in X$ bemenő jelre a

$$\delta_\rho(\rho[a], x) = \rho[\delta(a,x)], \tag{6.13}$$

$$\lambda_\rho(\rho[a], x) = \lambda(a,x) \quad [\mu_\rho(\rho[a]) = \mu(a)] \tag{6.14}$$

összefüggésekkel értelmezzük. Könnyen belátható, hogy az $\mathbf{A}/\rho$ automata jól definiált. $\mathbf{A}/\rho$-t az $\mathbf{A}$ automata ρ *szerinti faktorautomatá*jának nevezzük.

Az $\alpha_\rho : a \to \rho[a]$ leképezés az $\mathbf{A}$ automatának az $\mathbf{A}/\rho$ faktorautomatára való homomorfizmusa. Ezt az $\mathbf{A}$ automatának az $\mathbf{A}/\rho$ faktorautomatára való *természetes* (vagy *kanonikus*) *homomorfizmus*ának nevezzük. Érvényes az alábbi . algebrákra vonatkozó ún. *homomorfiatétel.*

6.1. Tétel. *Ha* α *az* $\mathbf{A} = (A, X, Y, \delta, \lambda[\mu])$ *automatának az* $\mathbf{A}' = (A', X, Y, \delta', \lambda'[\mu'])$ *automatára való homomorfizmusa, akkor* $\ker\alpha$ *kongruencia* $\mathbf{A}$*-n és* $\mathbf{A}' \cong \mathbf{A}/\ker\alpha$.

6.7. Karakterisztikus félcsoport

Legyen $\mathbf{A} = (A, X, \delta)$ tetszőleges kimenő jel nélküli automata. Definiáljuk az X^* szabad monoidon a $\rho_{\mathbf{A},a}$ $(a \in A)$ relációkat a

$$(p, q) \in \rho_{\mathbf{A},a} \quad \Longleftrightarrow \quad ap = aq \quad (p, q \in X^*) \tag{6.15}$$

feltétellel. Legyen továbbá $\rho_{\mathbf{A}} = \cap\{\rho_{\mathbf{A},a}; a \in A\}$, azaz

$$(p, q) \in \rho_{\mathbf{A}} \quad \Longleftrightarrow \quad (\forall a \in A)\ (ap = aq) \quad (p, q \in X^*). \tag{6.16}$$

6.2. Lemma. *Bármely $a \in A$ állapot esetén $\rho_{\mathbf{A},a}$ az X^* szabad monoid jobb kongruenciája, $\rho_{\mathbf{A}}$ pedig X^* kongruenciája.*

Bizonyítás Nyilvánvaló, hogy $\rho_{\mathbf{A}}$ és minden $a \in A$ állapotra $\rho_{\mathbf{A},a}$ ekvivalencia. Ha az $a \in A$ állapotra és a $p, q \in X^*$ bemenő szavakra $ap = aq$ teljesül, akkor (6.3) és (6.4) alapján bármely $r \in X^+$ bemenő szóra

$$a(pr) = (ap)r = (aq)r = a(qr),$$

azaz $(pr, qr) \in \rho_{\mathbf{A},a}$. Ez azt jelenti, hogy $\rho_{\mathbf{A},a}$ jobb kongruencia.

Ha $(p, q) \in \rho_{\mathbf{A}}$, akkor minden $a \in A$ állapotra és $r \in X^+$ bemenő szóra $(p, q) \in \rho_{\mathbf{A},ar}$, azaz

$$a(rp) = (ar)p = (ar)q = a(rq),$$

vagyis $\rho_{\mathbf{A}}$ kongruencia. □

A (6.16) feltétellel definiált $\rho_{\mathbf{A}}$ kongruenciát az $\mathbf{A} = (A, X, \delta)$ automata *Myhill–Nerode kongruenciá*jának nevezzük. Az $X^*/\rho_{\mathbf{A}}$ faktorfélcsoportot pedig $\mathbf{A}$ *karakterisztikus félcsoport*jának hívjuk.

A karakterisztikus félcsoport Mealy automatákra is definiálható ([2]). Mealy automata karakterisztikus félcsoportján a Mealy automata vázának karakterisztikus félcsoportját értjük. A vizsgálatainkban azonban erre a fogalomra nem lesz szükségünk.

6.8. Automataleképezések

Legyen X^* a nemüres X halmaz feletti szabad monoid. Az X halmaz elemeivel megfogalmazott *információk*on az X^*-beli szavakat értjük. Ha a p és q olyan X^*-beli szavak, amelyekhez vannak olyan r és t X^*-beli szavak, hogy $p = rqt$, akkor a q szót a p szó *részszavá*nak nevezzük. Ha $q \neq p$, akkor q-t p *valódi részszavá*nak hívjuk. Ha $r = e$, akkor azt mondjuk, hogy a q részszó a p *kezdőszelet*e vagy *prefix*e. Ha pedig $t = e$, akkor q a p *zárószelet*e vagy *szuffix*e.

Így az üres szó bármely szó részszava (prefixe, szuffixe). Ha $q \neq p$, akkor q-t a p *valódi kezdő* [*záró*] *szeleté*nek hívjuk.

*Alfabetikus leképezések*nek nevezzük az $\alpha : X^* \to Y^*$ alakú leképezéseket, azaz az X^* szabad félcsoportnak az Y^* szabad félcsoportba való leképezéseit. *Információátalakítás*on egy alfabetikus leképezés megadását értjük. Az α alfabetikus leképezést *szóhossztartó*nak hívjuk, ha minden $p \in X^*$ szóra $|\alpha(p)| = |p|$ teljesül. Azt mondjuk, hogy az α alfabetikus leképezés *prefixtartó*, ha tetszőleges szó minden kezdőszeletét a képszó egy kezdőszeletébe viszi át. Ezt úgy is megfogalmazhatjuk, hogy bármely $p(\in X^*)$ szóhoz van olyan $\alpha_p : X^* \to Y^*$ alfabetikus leképezés, amely minden $q \in X^*$ szóra teljesíti a

$$\alpha(pq) = \alpha(p)\alpha_p(q) \tag{6.17}$$

feltételt. Megmutatható, hogy az α_p leképezések is szóhossz- és prefixtartóak.

Egy $\mathbf{A} = (A, X, Y', \delta, \lambda)$ $(\emptyset \subset Y' \subseteq Y)$ Mealy automata tetszőleges $a \in A$ állapotára definiáljuk azt az $\alpha_{\mathbf{A},a} : X^* \to Y^*$ alfabetikus leképezést, amelyre

$$\alpha_{\mathbf{A},a}(p) = \lambda(a, p) \quad (p \in X^*). \tag{6.18}$$

Az $\alpha_{\mathbf{A},a}$ leképezést az $\mathbf{A}$ *automata* (a *állapota*) *által indukált leképezés*ének nevezzük. Azt is mondjuk, hogy $\alpha_{\mathbf{A},a}$-t az $\mathbf{A}$ automata (az a állapotával) indukálja. Ha nem vezet félreértésre, akkor $\alpha_{\mathbf{A},a}$ helyett a rövidebb α_a jelölést is használjuk.

Az $\alpha : X^* \to Y^*$ alfabetikus leképezést *automataleképezés*nek nevezzük, ha létezik olyan $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automata és olyan $a \in A$ állapot, hogy $\alpha = \alpha_{\mathbf{A},a}$. Ha az $\mathbf{A}$ Mealy automata iniciális az a_0 kezdő állapottal, akkor az α_{a_0} leképezést az $\mathbf{A}$ *iniciális automata által indukált leképezés*nek mondjuk és rá az $\alpha_{\mathbf{A}}$ jelölést is használjuk.

6.3. Tétel. *Egy $\alpha : X^* \to Y^*$ alfabetikus leképezés akkor és csak akkor automataleképezés, ha szóhossz- és prefixtartó leképezés.*

A tétel bizonyítása megtalálható például a [2] elektronikus jegyzetünkben. Az $\mathbf{A} = (A, X, Y, \delta, \mu)$ Moore automata $a \in A$ állapota által indukált $\alpha_a : X^* \to Y^*$ automataleképezésen értjük az

$$\alpha_a(e) = e, \quad \alpha_a(p) = \mu(\delta(a, p)) \quad (p \in X^+) \tag{6.19}$$

feltételekkel definiált függvényt.

Tetszőleges $\mathbf{A} = (A, X, Y, \delta, \lambda)$ Mealy automatára legyen

$$\Phi(\mathbf{A}) = \{\alpha_{\mathbf{A},a}; a \in A\}.$$

A közös X bemenő és Y kimenő halmazzal rendelkező $\mathbf{A}$ és $\mathbf{B}$ Mealy (Moore) automatát *ekvivalens*nek nevezzük, ha $\Phi(\mathbf{A}) = \Phi(\mathbf{B})$. Legyen $\mathbf{A}$ iniciális automata a_0 kezdőállapottal és $\mathbf{B}$ iniciális automata b_0 kezdőállapottal. Az $\mathbf{A}$ és $\mathbf{B}$ automatát *iniciálisan ekvivalens*nek mondjuk, ha $\alpha_{\mathbf{A},a_0} = \alpha_{\mathbf{B},b_0}$. Mint azt majd a 7.4 alfejezetben látjuk, számunkra elegendő a felismerő automaták ekvivalenciájával foglalkozni.

6.4. Tétel. *(Gill tétele) Bármely [iniciális] Mealy automatához létezik vele [iniciálisan] ekvivalens [iniciális] Moore automata. Ha a Mealy automata véges, akkor a vele [iniciálisan] ekvivalens Moore automata is választható végesnek.*

Az automaták ekvivalenciájával részletesen foglalkozunk a [2] jegyzetünk II. részében.

A 6.1. alfejezetben említettük, hogy egy $\mathbf{A} = (A, X, \delta)$ kimenő jel nélküli automata tekinthető olyan Mealy automatának is, amelynek δ átmenetfüggvénye egyúttal kimenetfüggvény is. Ez alapján az $\mathbf{A}$ *kimenő jel nélküli automata által indukált automataleképezések*en értjük azokat az $\alpha_a : X^* \to A^*$ $(a \in A)$ lekepezéseket, amelyekre $\alpha_a(p) = \delta(a, p)$ $(p \in X^+)$ és $\alpha(e) = e$ teljesülnek.

Legyenek X és Y nemüres halmazok, továbbá $\alpha : X^* \to Y^*$ tetszőleges olyan automataleképezés, hogy minden $y \in Y$ szerepel valamely $\alpha(p)$ $(p \in X^*)$ szóban. Ez az utóbbi feltétel az α leképezésre nem jelent megszorítást, hiszen azok a jelek, amelyek nem szerepelnek egyetlen képszóban sem, az Y halmazból nyilvánvalóan elhagyhatók. Ebben az alfejezetben végig feltesszük, hogy Y ilyen felesleges jeleket nem tartalmaz.

Ezt felhasználva, a következő lemmában azt mutatjuk meg, hogy az automataleképezések megadhatók szabad félcsoportok osztályozásai segítségével.

6.5. Lemma. *Bármely $\alpha : X^* \to Y^*$ automataleképezéshez hozzárendelhető az X^+ szabad félcsoportnak egy $|Y|$ számosságú $\mathcal{C}_\alpha$ osztályozása. Megfordítva, ha $\mathcal{C}$ az X^+ egy osztályozása és Y tetszőleges $|\mathcal{C}|$ számosságú halmaz, akkor Y elemeinek jelölésétől eltekintve egyértelműen megadható az az $\alpha : X^* \to Y^*$ automataleképezés, amelyre $\mathcal{C} = \mathcal{C}_\alpha$ teljesül.*

Bizonyítás Legyen $\alpha : X^* \to Y^*$ tetszőleges automataleképezés. Bármely $y \in Y$ jelre legyen L_y azoknak a $p \in X^+$ szavaknak a halmaza, amelyekre az $\alpha(p)$ szó az y jelre végződik. A

$$\mathcal{C}_\alpha = \{L_y; y \in Y\} \tag{6.20}$$

halmaz nyilvánvalóan X^+ egy osztályozása és $|\mathcal{C}_\alpha| = |Y|$.

Megfordítva, legyen $\mathcal{C} = \{L_i; i \in I\}$ az X^+ szabad félcsoport egy osztályozása. Tekintsük azt az $\alpha : X^* \to I^*$ alfabetikus leképezést, amelyre $\alpha(e) = e$ és tetszőleges $p = x_1x_2 \dots x_n \in X^+$ szó esetén $\alpha(p) = i_1i_2 \dots i_n$ teljesül, ahol

$$x_1 \in L_{i_1}, x_1x_2 \in L_{i_2}, \dots, x_1x_2 \dots x_n \in L_{i_n}.$$

Az α konstrukciójából következik, hogy α automataleképezés és $\mathcal{C} = \mathcal{C}_\alpha$. □

A (6.20) osztályozást az α *automataleképezés által indukált osztályozás*nak nevezzük.

Az automataleképezésekkel kapcsolatosan megfogalmazunk két természetes problémát. Az egyik az, hogy tetszőleges automatához hogyan lehet meghatározni azokat az automataleképezéseket, amelyeket az automata állapotai indukálnak. A problémának a megoldása tulajdonképpen egy adott automata viselkedésének, információátalakító képességének kivizsgálását jelenti. Ez a probléma *az automaták analízisiének problémája.* Ehhez természetesen valamilyen módon meg kell adni az automatát. Ez véges esetben nem okoz gondot, mert az automatát megadhatjuk például átmenet-kimenettáblázatával vagy gráfjával, s ebből véges számú lépésben leolvasható, hogy az általa indukált automataleképezések a vizsgált bemenő szót melyik kimenő szóba viszik át. Végtelen esetben azonban általában még az is probléma, hogy az automatát milyen módon adjuk meg. Egyszerűbb esetekben ez megtehető végtelen átmenet-kimenettáblázat vagy gráf vagy az átmenet- és kimenetfüggvények képlettel vagy valamilyen utasítással való megadásával.

A másik probléma az, hogy egy alfabetikus leképezésről hogyan lehet eldönteni, hogy automataleképezés-e, s ha igen, hogyan lehet megkonstruálni olyan iniciális automatát, amely ezt a leképezést indukálja. Ez *az automaták szintézisének problémája.* Ez a probléma még véges automaták esetén is nehezebb, mert egy alfabetikus leképezés értelmezési tartománya mindig végtelen halmaz, ezért már az alfabetikus leképezés megadása is kérdéses. Egyszerűbb esetekben megadhatjuk formulával, irányított fával vagy valamilyen utasítással. A szintézis problémáját véges automatákra a 8.5. alfejezetben megoldjuk.

7. fejezet

Nyelvek felismerése automatákban

7.1. Kimenő jel nélküli automatákban felismerhető nyelvek

Ha az $\mathbf{A} = (A, a_0, X, \delta)$ iniciális kimenő jel nélküli automata A állapothalmazának egy F részhalmazát kijelöljük, akkor a *felismerő automata* vagy *akceptor* fogalmához jutunk. Az F halmazt a *végállapotok halmazá*nak nevezzük, az automatára pedig az $\mathbf{A}_F = (A, a_0, X, \delta, F)$ jelölést is használjuk. Azt mondjuk, hogy az X feletti L nyelv *felismerhető* az $\mathbf{A} = (A, a_0, X, \delta; F)$ automatában, vagy más szóval az $\mathbf{A}$ automata *előállítja* vagy *elfogadja* az L nyelvet, ha

$$L = \{p \in X^*; a_0 p \in F\}. \tag{7.1}$$

Ebben az esetben használjuk az $L = L(\mathbf{A}, a_0, F)$ vagy az $L = L(\mathbf{A}, F)$ jelölést. Úgy is mondjuk, hogy az L nyelvet az $\mathbf{A} = (A, a_0, X, \delta)$ automata (az $F(\subseteq A)$ halmazzal) *felismeri* vagy *előállítja* vagy *elfogadja*. Az $\emptyset$ üres nyelvet bármely iniciális kimenő jel nélküli automata felismeri, mégpedig az $\emptyset$ üres halmazzal. Ha $F = \{a\}$, akkor az $F = a$ jelölést is használjuk és úgy mondjuk, hogy $\mathbf{A}$ felismeri az L nyelvet az a állapottal. Az e nyelvet bármely olyan $\mathbf{A} = (A, a_0, X, \delta)$ automata felismeri az a_0 állapottal, amelyben nincs olyan $p \in X^+$, hogy $a_0 p = a_0$.

Az $\mathbf{A} = (A, X, a_0, \delta)$ iniciális automata *iniciálisan összefüggő részautomatájá*nak nevezzük az $\mathbf{A}' = (A', X, a_0, \delta)$ iniciális automatát, amelyre $A' = \{a_0 p;\ p \in X^*\}$. Nyilvánvaló, hogy $\mathbf{A}$ pontosan azt a nyelvet ismeri fel az $F(\subseteq A)$ halmazzal, amelyet $\mathbf{A}'$ az $F \cap A'$ halmazzal. Ez azt jelenti, hogy elegendő iniciálisan összefüggő felismerő automatákra szorítkozni.

Bármely X feletti L nyelv felismerhető valamely iniciálisan összefüggő automatában. Ha ugyanis $\mathbf{X}^* = (X^*, e, X, \delta)$ a $\delta(p, x) = px \quad (p \in X^*, x \in X)$

átmenetfüggvénnyel definiált iniciálisan összefüggő úgynevezett X *feletti szabad automata*, akkor az ${\mathbf{X}^*}_L = (X^*, e, X, \delta, L)$ automata pontosan az L nyelvet ismeri fel.

Megállapodunk abban is, hogy felismerő automata homomorf képe is felismerő automata legyen, mégpedig úgy, hogy a homomorfizmus iniciális homomorfizmus legyen. Továbbá egy állapot képe akkor és csak akkor legyen végállapot, ha az állapot maga is végállapot. Vagyis α legyen az $\mathbf{A} = (A, a_0, X, \delta_A, F)$ automata olyan homomorf leképezése a $\mathbf{B} = (B, b_0, X, \delta_B, K)$ automatára, amelyre

$$\alpha(a_0) = b_0 \quad \text{és} \quad F = \alpha^{-1}(K). \tag{7.2}$$

Az $\mathbf{A}_F = (A, a_0, X, \delta, F)$ felismerő automatát tekinthetjük az

$$\mathbf{A}_{F,\mu} = (A, a_0, X, Y, \delta, \mu)$$

Moore automatának is, ahol $Y = \{0, 1\}$, továbbá bármely $a \in A$ állapot esetén $\mu(a) = 1$, ha $a \in F$ és $\mu(a) = 0$, ha $a \notin F$. Az $\mathbf{A}_{F,\mu}$ automatát az $\mathbf{A}_F$ *felismerő automatához rendelt Moore automatá*nak nevezzük. A felismerő automatához rendelt Moore automata működését úgy képzelhetjük el, hogy "igen"-t mond akkor, ha $p \in L$ ($\mu(a_0 p) = 1$) ill. "nem"-et mond, ha $p \notin L$ ($\mu(a_0 p) = 0$). Vagyis, ha $\alpha_{a_0} : X^* \to \{0, 1\}^*$ az $\mathbf{A}_{F,\mu}$ Moore automata által indukált, (6.19)-ben definiált automataleképezés, akkor

$$L = \{p \in X^*; \alpha_{a_0}(p) \in \{0, 1\}^* 1\}. \tag{7.3}$$

7.2. Félcsoportelméleti jellemzés

7.1. Tétel. *(Myhill–Nerode tétel) Az X véges ábécé feletti L nyelv akkor és csak akkor ismerhető fel véges kimenő jel nélküli automatában, ha előáll valamely X^*-on értelmezett véges indexű ρ jobb kongruencia bizonyos osztályainak egyesítéseként.*

Bizonyítás Legyen $L = L(\mathbf{A}, a_0, F)$, ahol $\mathbf{A} = (A, a_0, X, \delta, F)$. Legyen továbbá $\rho_{\mathbf{A},a_0}$ (6.15) feltétellel értelmezett jobb kongruencia. Tegyük fel, hogy $(p, q) \in \rho_{\mathbf{A},a_0}$ ($p, q \in X^*$) és $p \in L$. Minthogy $a_0 p = a_0 q$, ezért $q \in L$. Ezzel megmutattuk, hogy L $\rho_{\mathbf{A},a_0}$-osztályok egyesítése. Ha $\mathbf{A}$ véges automata, akkor $\rho_{\mathbf{A},a_0}$ nyilvánvalóan véges indexű.

Megfordítva, tegyük fel, hogy X^*-nak van olyan ρ jobb kongruenciája, hogy

$$L = \cup(\rho[p]; p \in L).$$

Tekintsük az

$$\mathbf{A} = (X^*/\rho, \rho[e], X, \delta_\rho, L/\rho)$$

automatát, amelyre minden $p \in X^*$ és $x \in X$ esetén

$$\delta_\rho(\rho[p], x) = \rho[px].$$

(Könnyen látható, hogy $\mathbf{A}$ jól definiált.) A (6.3) és a (6.4) kiterjesztések alapján kapjuk, hogy

$$p \in L(\mathbf{A}, \rho[e], L/\rho) \Longleftrightarrow \rho[p] = \rho[e]p \in L/\rho \Longleftrightarrow p \in L,$$

azaz $L = L(\mathbf{A}, \rho[e], L/\rho)$. Ha X véges ábécé és ρ véges indexű, akkor $\mathbf{A}$ véges automata. □

Minthogy (6.16) szerint $\rho_{\mathbf{A}} \subseteq \rho_{\mathbf{A},a_0}$, ezért a következő tétel is igaz.

7.2. Tétel. *Az X véges ábécé feletti L nyelv akkor és csak akkor ismerhető fel véges kimenő jel nélküli automatában, ha előáll valamely X^*-on értelmezett véges indexű ρ kongruencia bizonyos osztályainak egyesítéseként.*

Legyen L tetszőleges X ábécé feletti nyelv. Definiáljuk az X^* szabad félcsoporton a τ_L és a ϑ_L relációkat a

$$(p, q) \in \tau_L \quad \Longleftrightarrow \quad (\forall r \in X^*)(pr \in L \iff qr \in L), \tag{7.4}$$

illetve a

$$(p, q) \in \vartheta_L \quad \Longleftrightarrow \quad (\forall r, s \in X^*)(spr \in L \iff sqr \in L) \tag{7.5}$$

feltételekkel. Nem nehéz belátni, hogy τ_L jobb kongruencia, ϑ_L pedig kongruencia X^*-on, továbbá $\vartheta_L \subseteq \tau_L$. Ha $L = \emptyset$, akkor $\vartheta_L = \tau_L$ az univerzális reláció X^*-on. Az is látható, hogy L τ_L-osztályok, s így ϑ_L-osztályok egyesítése is.

7.3. Lemma. *Legyen ρ tetszőleges jobb kongruencia [kongruencia] X^*-on és $L \neq \emptyset$ tetszőleges nyelv X felett. Az L nyelv akkor és csak akkor ρ-osztályok egyesítése, ha $\rho \subseteq \tau_L$ [$\tau \subseteq \vartheta_L$].*

Bizonyítás Legyen ρ egy jobb kongruencia X^*-on és az $L \neq \emptyset$ egy X feletti nyelv. Tegyük fel, hogy $(p, q) \in \rho$ ($p, q \in X^*$). Akkor minden $r \in X^*$ szóra $(pr, qr) \in \rho$. Ha L ρ-osztályok egyesítése, úgy $pr \in L$ akkor és csak akkor, ha $qr \in L$, azaz $(p, q) \in \tau_L$, vagyis $\rho \subseteq \tau_L$. Hasonlóan látható be, hogy ha ρ kongruencia és L ρ-osztályok egyesítése, akkor $\rho \subseteq \vartheta_L$. Az állítás megfordítása nyilvánvalóan igaz. □

7.3. Szintaktikus félcsoport

A (7.5) feltétellel definiált ϑ_L kongruenciát *szintaktikus kongruenciá*nak nevezzük, az X^*/ϑ_L faktorfélcsoportot pedig L *szintaktikus félcsoport*jának nevezzük. Hasonlóan a (7.4) τ_L jobb kongruenciát *szintaktikus jobb kongruenciá*nak hívjuk,

Legyen D az $\mathbf{A} = (A, X, \delta)$ kimenő jel nélküli automata A állapothalmazának tetszőleges részhalmaza. A D részhalmaz segítségével definiáljuk az A állapothalmazon $\tau(D)$ relációt úgy, hogy minden $b, c \in A$ és $p \in X^*$ esetén

$$(b, c) \in \tau(D) \quad \Longleftrightarrow \quad (bp \in D \iff cp \in D) \tag{7.6}$$

Nem nehéz belátni, hogy $\tau(D)$ az $\mathbf{A}$ automata legnagyobb olyan τ kongruenciája, amelyre D bizonyos τ-osztályok egyesítése. Jelölje továbbiakban ι_A és ω_A az identikus illetve az univerzális relációt A-n. Nyilvánvaló, hogy $\tau(D) = \tau(A - D)$, továbbá $\tau(D) = \omega_A$ akkor és csak akkor, ha $D = \emptyset$ vagy $D = A$. Ha $\tau(D) = \iota_A$, akkor D-t az $\mathbf{A}$ *diszjunktív részhalmaz*ának nevezzük, ha pedig $D = \{a\}$, akkor a-t egyszerűen $\mathbf{A}$ *diszjunktív állapot*ának.

Az $\mathbf{A} = (A, X, \delta)$ kimenő jel nélküli automata ρ kongruenciáját az $\mathbf{A}_F = (A, a_0, X, \delta, F)$ *felismerő automata kongruenciájá*nak nevezzük, ha $\rho \subseteq \tau(F)$. Ez alapján felismerő automatákra a homomorfiatétel a következőképpen mondható ki:

7.4. Tétel. *Ha* α *az* $\mathbf{A} = (A, a_0, X, \delta, F)$ *felismerő automata homomorf leképezése az* $\mathbf{A}' = (A', b_0, X, \delta', K$ *felismerő automatára, akkor* $\ker\alpha$ *az* $\mathbf{A}$ *automata olyan kongruenciája, amelyre* $\ker\alpha \subseteq \tau(F)$ *és* $\mathbf{A}' \cong \mathbf{A}/\ker\alpha$.

Egy $\mathbf{A} = (A, a_0, X, \delta, F)$ felismerő automatát *egyszerű*nek nevezünk, ha az $\tau(F) = \iota_A$. (Ez az egyszerűség pontosan ugyanazt jelenti, mint a felismerő automatához rendelt Moore automata egyszerűsége (l. [2])).

Tetszőleges $\mathbf{A} = (A, a_0, X, \delta, F)$ felismerő automata esetén az $\mathbf{A}/\tau(F)$ faktorautomata nyilvánvalóan egyszerű. A 7.4 homomorfiatételből az is következik, hogy $\mathbf{A}/\tau(F)$ minden olyan $\mathbf{B}$ felismerő automatának homomorf képe, amely $\mathbf{A}$-nak homomorf képe.

7.5. Tétel. *Ha az* X *feletti* $L \neq \emptyset$ *nyelv felismerhető az* $\mathbf{A} = (A, a_0, X, \delta, F)$ *automatában az állapothalmaz valamely részhalmazával, akkor az* X^*/ϑ_L *szintaktikus félcsoport az* $X^*/\rho_{\mathbf{A}}$ *karakterisztikus félcsoport homomorf képe. Ha* $\mathbf{A}$ *egyszerű iniciálisan összefüggő automata, akkor a szintaktikus félcsoport egyenlő a karakterisztikus félcsoporttal.*

Bizonyítás Könnyen látható, hogy $\rho_{\mathbf{A}} \subseteq \vartheta_L$, amiből következik a tétel első állítása.

Legyen a $\mathbf{A} = (A, a_0, X, \delta, F)$ automata iniciálisan összefüggő és egyszerű. Megmutatjuk, hogy $\vartheta_L \subseteq \rho_{\mathbf{A}}$. Legyen $(p, q) \in \vartheta_L$ $(p, q \in X^*)$, azaz minden $s, r \in X^*$ párra $spr \in L$ akkor és csak akkor, ha $sqr \in L$. Ha az $\mathbf{A}$ automata az L nyelvet az F halmazzal ismeri fel, akkor ebből következik, hogy minden $s, r \in X^*$ párra $a_0spr \in F$ akkor és csak akkor, ha $a_0sqr \in F$. Mivel $\mathbf{A}$ iniciálisan összefüggő, azaz $A = \{a_0s; s \in X^*\}$, ezért minden $a \in A$ állapotra és $r \in X^*$ bemenő szóra $apr \in F$ akkor és csak akkor, ha $aqr \in F$, azaz $(ap, aq) \in \tau(F)$, ahol $\tau(F)$ a (7.6) feltétellel definiált kongruencia. Minthogy $\mathbf{A}$ egyszerű, ezért $ap = aq$, azaz $(p, q) \in \rho_{\mathbf{A}}$. Ezzel megmutattuk, hogy $\vartheta_L \subseteq \rho_{\mathbf{A}}$, s így $\vartheta_L = \rho_{\mathbf{A}}$. □

7.4. Felismerő automaták ekvivalenciája

Az $\mathbf{A} = (A, a_0, X, \delta_A), F$ és a $\mathbf{B} = (B, b_0, X, \delta_B, K)$ felismerő automatákat *ekvivalens*nek mondjuk, ha $L(\mathbf{A}, F) = L(\mathbf{B}, K)$.

7.6. Lemma. *Ha α az $\mathbf{A} = (A, a_0, X, \delta, F)$ automata egy homomorfizmusa, akkor*

$$L(\mathbf{A}, a_0, F) = L(\alpha(\mathbf{A}), \alpha(a_0), \alpha(F)).$$

Bizonyítás A (6.3) és a (6.4) kiterjesztések alapján könnyen belátható, hogy minden $a \in A$ állapotra és $p \in X^*$ bemenő szóra $\alpha(ap) = \alpha(a)p$. Így (7.2)-t is felhasználva

$$p \in L(\mathbf{A}, a_0, F) \iff a_0p \in F \iff \alpha(a_0)p = \alpha(a_0p) \in \alpha(F) \iff$$

$$\iff p \in L(\alpha(\mathbf{A}, \alpha(a_0), \alpha(F). \qquad \square$$

Már említettük, hogy elegendő iniciálisan összefüggő felismerő automatákra szorítkozni. Ekvivalens iniciálisan összefüggő automatákra érvényes a következő tétel:

7.7. Tétel. *Ekvivalens iniciálisan összefüggő felismerő automaták között izomorfiától eltekintve egyetlen olyan automata van, amely a többi homomorf képe. Ez az automata választható bármelyik automatához tartozó egyszerű felismerő automatának.*

Bizonyítás Legyen L tetszőleges X feletti nyelv. Vegyük a (7.4) szintaktikus jobb kongruenciát. Tekintsük az

$$\mathbf{X}^*/\tau_L = (X^*/\tau_L, \tau_L[e], X, \delta)$$

iniciálisan összefüggő automatát úgy, hogy minden $p \in X^*$ és $x \in X$ esetén $\delta(\tau_L[p], x) = \tau_L[px]$ teljesüljön. Mivel τ_L jobb kongruencia, ezért az automata jól definiált. A (6.3) és a (6.4) kiterjesztések alapján könnyű belátni, hogy L-et az automata felismeri az $F = \{\tau_L[p]; p \in L\}$ halmazzal.

Tegyük fel most, hogy L-et felismeri az $\mathbf{A} = (A, a_0, X, \delta', K)$ automata is. Legyen $\tau(K)$ a (7.6)-ben definiált kongruencia. Akkor bármely $p, q \in X^*$ esetén

$$(a_0p, a_0q) \in \tau(K) \iff (\forall r \in X^*)(a_0pr \in K \iff a_0qr \in K) \iff$$

$$\iff (\forall r \in X^*)(pr \in L \iff qr \in L) \iff (p, q) \in \tau_L.$$

Ebből következik, hogy az $\alpha(\tau(K)[a_0p]) = \tau_L[p]$ $(p \in X^*)$ leképezés $A/\tau(K)$ bijektív leképezése X^*/τ_L-re. Nem nehéz megmutatni, hogy α az $\mathbf{A}/\tau(K)$ egyszerű felismerő automata izomorf leképezése az $\mathbf{X}^*/\tau_L$ egyszerű felismerő automatára. □

A 7.7 Tétel érvényes általában Moore automatákra, sőt Mealy automatákra is. Ezzel részletesen foglalkozunk a [2] jegyzetünk 9. fejezetében.

A 7.7 Tétel szerint az $\mathbf{X}^*/\tau_L$ automata minimális abban az értelemben, hogy $|X^*/\tau_L| \leq |A|$. Ha $\mathbf{A}$ véges automata, akkor a τ_L szintaktikus jobb kongruencia, s így a $vartheta_L$ szintaktikus kongruencia véges indexű. A következő fejezetben megmutatjuk, hogy véges ábécé feletti nyelv akkor és csak akkor ismerhető fel véges automatában, ha reguláris (8.1 Tétel). Ezek alapján kimondhatjuk a következő állítást:

7.8. Következmény. *Az X véges ábécé feletti L nyelv akkor és csak akkor reguláris, ha ϑ_L szintaktikus kongruenciája véges indexű.*

Tegyük fel, hogy az X ábécé feletti L nyelv felismerhető véges automatában. Az L *nyelv súlyá*n azt az $s(L)$ nemnegatív egész számot értjük, amelyre L felismerhető $s(L)$ állapotú automatában, és ha L felismerhető valamely $\mathbf{A} = (A, a_0, X, \delta, F)$ automatában, akkor $s(L) \leq |A|$. A 7.7 Tétel szerint $s(L) = |A^*/\tau(F)|$.

A [2] elektronikus jegyzetünk *Automaták és nyelvek* részében megmutatjuk, hogy bármely véges $\mathbf{A} = (A, a_0, X, \delta, F)$ automata esetén létezik algoritmus $\tau(F)$ meghatározására. Ha a véges iniciálisan összefüggő felismerő automatát (7.3) szerint Moore automatának tekintjük, akkor ez az algoritmus a Moore automatákra vonatkozó *Aufenkamp–Hohn algoritmus*. Megjegyezzük, hogy az Aufenkamp-Hohn algoritmust eredetileg Mealy automatákra adták meg. A [2] jegyzetünkben azonban az algoritmust megfogalmazzuk speciálisan Moore automatákra is. A [2] jegyetünk említett részében egy példát adunk erre az algoritmusra. Szokás ezt az algoritmust a *véges automaták minimalizálásá*nak is nevezni. A véges automatákban felismerhető nyelveket minimális állapotszámmal felismerő automata algoritmikus megadásának gondos leírása Gécseg Ferenc [19] egyetemi jegyzetében is megtalálható.

7.5. Nemdeterminisztikus automatákban felismerhető nyelvek

Azt mondjuk, hogy az X feletti L nyelvet az $\mathbf{A} = (A, A_0, X, \delta)$ nemdeterminisztikus kimenő jel nélküli iniciális automata az $F(\subseteq A)$ halmazzal *felismeri* vagy *előállítja* vagy *elfogadja*, ha

$$L = \{p \in X^*; A_0 p \cap F \neq \emptyset\} \tag{7.7}$$

ahol $A_0 p$ a kezdőállapotok A_0 halmazából p szóval elérhető állapotok halmazát jelöli. Determinisztikus esetben ez a definíció megegyezik a (7.1) definícióval.

Mivel minden X feletti nyelv felismerhető determinisztikus automatával, sőt speciálisan iniciálisan összefüggő automatával is, ezért a nemdeterminisztikus automatákkal felismert X feletti nyelvek megyegyeznek a determinisztikus automatákkal felismert X feletti nyelvekkel, azaz az X feletti nyelvekkel. A 6.1. alfejezetben megállapodtunk abban, hogy egy automata, ha mást nem mondunk, akkor teljesen definiált és determinisztikus, s így a nemdeterminisztikus automaták osztályának valódi részosztálya. Ezért azt várnánk, hogy a véges nemdeterminisztikus automatákkal felismerhető nyelvek osztálya bővebb a véges automatákkal felismerhető nyelvek osztályánál. Az alábbiakban megmutatjuk, hogy ez nincs így. Ennek ellenére azért foglalkozunk a nemdeterminisztikus automatákkal, mert ezek és több analogonjuk későbbi konstrukciókban fontos szerepet játszanak. A bizonyításhoz szükségünk lesz a hatványautomata fogalmára.

Az $\mathbf{A} = (A, X, \delta)$ automata *hatványautomatájá*nak nevezzük a $\mathbf{P}(\mathbf{A})^+ = (P(A)^+, X, \delta)$ automatát, ha $P(A)$ az A hatványhalmaza, $P(A)^+ = P(A) - \emptyset$ és minden $A' \in P(A)^+$ és $x \in X$ esetén

$$\delta(A', x) = \{\delta(a, x); a \in A'\}. \tag{7.8}$$

(Az egyszerűség kedvéért a hatványautomata átmenetfüggvényét is δ-val jelöltük) Ha az automata parciális, akkor előfordulhat, hogy $\delta(A', x)$ $A' \neq \emptyset$ esetben is üres. Ezért *parciális automata hatványautomatájá*nak a $\mathbf{P}(\mathbf{A}) = (P(A), X, \delta)$ automatát tekintjük, ahol minden $x \in X$ bemenő jelre

$$\delta(\emptyset, x) = \emptyset. \tag{7.9}$$

Sok esetben $P(A)$ egyelemű részhalmazait azonosítjuk az elemükkel. Ha a δ függvény értelmezését (6.3) és (6.4) szerint kiterjesztjük a $P(A) \times X^*$ szorzathalmazra, akkor nem nehéz belátni, hogy minden $A' \in P(A)$ és $p \in X^*$ esetén

$$\delta(A', p) = \{\delta(a, p); a \in A'\} \quad \text{és} \quad A'p = \{ap; a \in A'\} \tag{7.10}$$

7.9. Tétel. *A véges nemdeterminisztikus automatákban felismerhető nyelvek megegyeznek a véges automatákban felismerhető nyelvekkel.*

Bizonyítás Mivel minden véges automata megállapodásunk szerint teljesen definiált és determinisztikus, így definíció szerint nem determinisztikus is. Ezért, ha egy nyelv felismerhető véges automatával, akkor felismerhető véges nemdeterminisztikus automatával is.

Megfordítva, tegyük fel, hogy az X feletti L nyelv felismerhető az $\mathbf{A} = (A, A_0, X, \delta)$ ($A_0 \subseteq A$) véges iniciális nemdeterminisztikus automatában az $F(\subseteq A)$ halmazzal. Inicializáljuk az $\mathbf{P}(\mathbf{A})$ hatványautomatát az A_0 állapottal, azaz legyen $\mathbf{P}(\mathbf{A}) = (P(A), A_0, X, \delta)$. Akkor az $\mathbf{P}(A)$ véges automata felismeri L-t a $T = \{B \in P(A); B \cap F \neq \emptyset\}$ halmazzal. □

A teljesség kedvéért megjegyezzük, hogy a nemdeterminisztikus automatáknak egy másik típusát is be szokták vezetni, mégpedig úgy, hogy (6.6) definícióban X helyett $X \cup e$ legyen. Ez azt jelenti, hogy az automata egyik állapotból bemenő jel nélkül is átmehet egy másik állapotba. Ezt *e átmenetes* vagy *spontán átmenetes nemdeterminisztikus automatá*nak nevezik. A 7.9 Tétel akkor is igaz, ha a tételben szereplő nemdeterminisztikus automaták e átmenetesek. (A bizónyítás megtalálható például Ésik Zoltán [14] egyetemijegyzetében.)

7.6. Zártsági tulajdonságok

Megmutatjuk, hogy egy X ábécé feletti véges (kimenő jel nélküli) automatákban felismerhető nyelvek halmaza zárt a reguláris és a Boole műveletekre.

Szükségünk lesz a kimenő jel nélküli automaták direkt szozatának fogalmára. Az $\mathbf{A} = (A, X, \delta_A)$ és az $\mathbf{B} = (B, X, \delta_B)$ automaták *direkt szorzatá*n értjük azt az $\mathbf{A} \times \mathbf{B} = (A \times B, X, \delta)$ automatát, amelyre

$$\delta((a, b), x) = (\delta_A(a, x), \delta_B(b, x)) \quad (a \in A,\ b \in B, x \in X). \tag{7.11}$$

Ha az automaták iniciálisak, akkor legyen direkt szorzatuk is iniciális. Mégpedig, ha a_0 az $\mathbf{A}$ és b_0 a $\mathbf{B}$ automata kezdőállapota, akkor az $\mathbf{A} \times \mathbf{B}$ direkt szorzat kezdőállapota legyen (a_0, b_0). Nyilvánvalóan a $\times$ művelet asszociatív.

A következő tétel azt jelenti, hogy egy véges ábécé feletti véges automatákban felismerhető nyelvek halmaza Boole algebra a halmazelméleti egyesítés, metszet és komplementerképzés műveletekre.

7.10. Tétel. *Az X véges ábécé feletti véges automatákban felismerhető nyelvek halmaza zárt a Boole műveletekre.*

Bizonyítás Legyenek $L, K \in R(X)$ $(L \neq K)$ tetszőlegesek. Megmutatjuk, hogy ha L és K felismerhető az $\mathbf{A} = (A, a_0, X, \delta_A)$ ill. a $\mathbf{B} = (B, b_0, X, \delta_B)$ véges automatákban az F illetve H halmazokkal, akkor $L \cup K$ felismerhető az $\mathbf{A} \times \mathbf{B}$ direkt szorzatban $M = (F \times B) \cup (A \times H)$ halmazzal. (A kezdőállapot természetesen (a_0, b_0).)

Legyen először $p \in L + K$. Akkor $p \in L$ vagy $p \in K$. Szimmetria okok miatt elegendő a $p \in L$ esettel foglalkozni. Ekkor $a_0 p \in F$,

$$(a_0, b_0)p = (a_0 p, b_0 p) \in F \times B.$$

(l. (6.3) és (6.4).) Ezzel megmutattuk, hogy $L \cup K \subseteq L(\mathbf{A} \times \mathbf{B}, M)$.

Megfordítva, legyen $p \in L(\mathbf{A} \times \mathbf{B}, M)$. Ekkor

$$(a_0 p, b_0 p) = (a_0, b_0)p \in M.$$

Ezért $a_0 p \in F$ vagy $b_0 p \in H$, azaz $p \in L$ vagy $p \in K$, vagyis $p \in L + K$, amivel beláttuk az $L(\mathbf{A} \times \mathbf{B}, M) \subseteq L \cup K$ tartalmazást, s így $L \cup K = L(\mathbf{A} \times \mathbf{B}, M)$. Tehát a véges automatákban felismerhető X feletti nyelvek halmaza zárt az egyesítés műveletére.

Nem nehéz belátni, hogy $L \cap K$ is felismerhető az $\mathbf{A} \times \mathbf{B}$ automatában az $F \times H$ halmazzal. Továbbá, ha L felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges iniciálisan összefüggő automatában az állapothalmaz F részhalmazával, akkor az L nyelv $\overline{L} = X^* - L$ komplementere felismerhető ugyanebben az automatában az $\overline{F} = A - F$ halmazzal. □

A 7.7 Tételből azonnal adódik, hogy az X ábécé feletti véges kimenő jel nélküli automatákban felismerhető nyelvek halmaza zárt a kivonásra. ($L - K = L \cap \overline{K}$ miatt $L - K$ is felismerhető a bizonyításban szereplő $\mathbf{A} \times \mathbf{B}$ automatában az $F \times (B - H)$ halmazzal.)

A következő tétel bizonyításához definiáljuk az $\mathbf{A} = (A, X, \delta)$ nemdeterminisztikus automata $\mathbf{P}(\mathbf{A}) = (P(A), X, P(Y), \delta)$ hatványautomatáját is. A δ átmenetfüggvényt minden $A' \in P(A)$ és $x \in X$ esetén a

$$\delta(A', x) = \cup_{a \in A'} \delta(a, x) \tag{7.12}$$

összefüggéssel adjuk meg. Sokszor egy nemdeterminisztikus automatát a hatványautomatájával adunk meg, amely teljesen definiált és determinisztikus. Ha $\mathbf{A}$ iniciális és kezdőállapotainak halmaza A_0, akkor $\mathbf{P}(\mathbf{A})$-t is iniciálisnak tekintjük, mégpedig A_0 kezdőállapottal. A δ' átmenetfüggvény értelmezését, ha nem mondunk mást, akkor a következő módon terjesztjük ki a $P(A) \times X^*$ halmaz azon részhalmazára, ahol ez lehetséges: Legyen minden $a \in A$ állapotra

$$\delta(a, e) = a, \tag{7.13}$$

ahol e az üres szó. Tetszőleges $a \in A, x \in X$ és $p \in X^*$ esetén pedig

$$\delta(a, px) = \delta(a, p) \cup_{b \in ap} \delta(b, x). \tag{7.14}$$

Végül, ha $A' \in P(A)$ és $p \in X^*$, akkor legyen

$$\delta(A', p) = \cup_{a \in A'} \delta(a, p). \tag{7.15}$$

Nem nehéz belátni, hogy determinisztikus esetben ez a kiterjesztés a szokásos (6.3) és (6.4) kiterjesztéseket adja. Megmutatható, hogy ez a kiterjesztés nemdeterminisztikus esetben is ezt jelenti. Ha az **A** nemdeterminisztikus automata az $a \in A$ állapotban van és a $p \in X^*$ bemenő szót elfogadja, akkor ap az a állapotból a p szóval elérhető állapotok halmaza.

7.11. Tétel. *Az X véges ábécé feletti véges automatákban felismerhető nyelvek halmaza zárt a reguláris műveletekre.*

Bizonyítás Azt már az előző tételben megmutattuk, hogy az X véges ábécé feletti véges automatákban felismerhető nyelvek halmaza zárt az összeadás (egyesítés) műveletére.

Legyenek most L és K olyan X feletti nyelvek, amelyek felismerhetők az $\mathbf{A} = (A, a_0, X, \delta_A)$ ill. a $\mathbf{B} = (B, b_0, X, \delta_B)$ véges automatákban az F ill. H halmazokkal. Feltehetjük, hogy $L \neq \emptyset$ és $K \neq \emptyset$. (Ha $L = \emptyset$ vagy $K = \emptyset$, akkor $LK = \emptyset$.) Vegyük fel az **B** automata $\mathbf{P}(\mathbf{B}) = (P(B), X, \delta_B)$ hatványautomatáját (l. (7.8), (7.9) és (7.10)). Definiáljuk a

$$\mathbf{C} = (A \times P(B), (a_0, \emptyset), X, \delta$$

véges iniciális automatát úgy, hogy minden $a \in A,\ D \in P(B)$ és $x \in X$ esetén

$$\delta((a, D), x) = \begin{cases} (\delta_A(a, x), \delta_B(D, x)) & \text{ha } \delta_A(a, x) \notin F, \\ (\delta_A(a, x), \delta_B(D, x) \cup b_0), & \text{ha } \delta_A(a, x) \in F \end{cases}$$

teljesüljön. Terjesszük ki a δ átmenetfüggvény értelmezését az $(A \times P(B)) \times X^*$ halmazra (6.3) és (6.4) szerint a szokásos módon, felhasználva azt, hogy minden $x \in X$ bemenő jelre $\delta_B(\emptyset, x) = \emptyset$.

Bármely $a \in A$ állapotra és $p \in X^*$ bemenő szóra definiáljuk az

$$R_B(p) = \{b_0 r; p = qr,\ aq \in F\}$$

halmazt. A δ átmenetfüggvény definíciójából következik, hogy

$$(a_0, \emptyset)p = (a_0 p, R_B(p)).$$

Azt állítjuk, hogy a $\mathbf{C}$ automata felismeri az LK nyelvet az $A \times T_B$ halmazzal, ahol $T_B = \{D \in P(B); D \cap K \neq \emptyset\}$. Ha ugyanis $p \in LK$, akkor $p = qr$, ahol $q \in L$ és $r \in K$. Ezért $R_B(p) \neq \emptyset$ és

$$(a_0, \emptyset)p = (a_0 p, R_B(p)) \in A \times T_B.$$

Kaptuk, hogy $LK \subseteq L(\mathbf{C}, A \times T_B)$. Legyen $p \in L(\mathbf{C}, A \times T_B)$, azaz

$$(a_0 p, R_B(p)) = (a_0, \emptyset)p \in A \times T_B.$$

Ha p minden q kezdőszeletére $a_0 q \notin F$, akkor $R_B(p) = \emptyset$, ami T_B definíciója miatt lehetetlen. Ezért vannak olyan $q, r \in X^*$, hogy $p = qr$ és $a_0 q \in F$. Ez azt jelenti, hogy $R_B(p) \cap H \neq \emptyset$. Így vannak olyan $q, r \in X^*$, hogy $p = qr$, $a_0 q \in F$ és $b_0 r \in K$, vagyis $p \in LK$. Ami az $L(\mathbf{B}, A \times T_B) \subseteq LK$ tartalmazást bizonyítja. Tehát $LK = L(\mathbf{B}, A \times T_B)$. Ezzel megmutattuk, hogy a véges automatákban felismerhető X feletti nyelvek halmaza zárt a konkatenáció műveletére.

Legyen végül az X feletti L nyelv olyan, amely felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában az állapothalmaz F részhalmazával. Feltehetjük, hogy $L \neq \emptyset$ és $L \neq e$. (Ha $L = \emptyset$ vagy $L = e$, akkor $L^* = e$.) Definiáljuk a $\tilde{\mathbf{A}} = (P(A), a_0, X, \tilde{\delta})$ nemdeterminisztikus automata $\tilde{\delta}$ átmenetfüggvényét úgy, hogy minden $a \in A$ állapotra és $x \in X$ bemenő jelre teljesüljön a

$$\tilde{\delta}(a, x) = \begin{cases} \delta(a, x), & \text{ha } \delta(a, x) \notin F, \\ \{\delta(a, x), a_0\}, & \text{ha } \delta(a, x) \in F \end{cases}$$

összefüggés. A (7.12) feltétel alapján adjuk meg az $\tilde{\mathbf{A}}$ automata

$$\mathbf{P}(\mathbf{A}) = (P(A), X, a_0, \tilde{\delta})$$

hatványautomatáját.

Az egyértelműség kedvéért a bizonyítás során az $\tilde{\mathbf{A}}$ automatában az $A' \in P(A)$ részhalmaz állapotaiból a $p \in X^*$ bemenő szóval elérhető állapotok halmazát jelöljük $\delta'(A', p)$-vel.

Legyen $T = \{B \in P(A); B \cap F \neq \emptyset\}$. Megmutatjuk, hogy az L nyelv L^+ e-mentes iteráltja felismerhető a $\mathbf{P}(\mathbf{A})$ automatában a T halmazzal. Először azt látjuk be a kitevő szerinti teljes indukcióval, hogy L minden pozitiv egész kitevős hatványa részhalmaza az $L(\mathbf{P}(A), T)$ halmaznak. Legyen $p \in L$, azaz $a_0 p \in F$. Az (7.13)-(7.15) feltételeket felhasználva kapjuk, hogy $a_0 p \in \delta'(a_0, p)$. (Ha $p = e$, akkor $a_0 p = a_0 = \delta'(a_0, p)$.) Ezért $\delta'(a_0, p) \in T$. Ezzel megmutattuk, hogy $L \subseteq L(\mathbf{P}(\mathbf{A}), T)$. Tegyük fel minden $1 \leq i < n$ egész számra, hogy $L^i \subseteq L(\mathbf{P}(\mathbf{A}), T)$, és legyen $p \in L^n$. Akkor van olyan $q \in L$ és $r \in L^{n-1}$,

hogy $p = qr$. Definíció szerint $a_0q \in F$, az indukciós feltevés szerint pedig $\delta'(a_0, r) \in T$. Mivel $a_0q \in F$, ezért $\tilde{\delta}$ függvény definíciója miatt $a_0 \in \delta'(a_0, q)$. Így $\delta'(a_0, r) \subseteq \delta'(a_0, p)$, ezért $\delta'(a_0, p) \in T$. Ami azt jelenti, hogy minden pozitiv egész n-re $L^n \subseteq L(\mathbf{P}(\mathbf{A}), T)$, azaz $L^+ \subseteq L(\mathbf{P}(\mathbf{A}), T)$.

Legyen most $p \in L(\mathbf{P}(\mathbf{A}), T)$, vagyis $\delta'(a_0, p) \in T$, amiből következik, hogy $\delta'(a_0, p) \cap F \neq \emptyset$. Ha $p = e$, akkor $a_0 \in F$, s ezért $p \in L$. Tegyük fel, hogy $p \neq e$. A p szónak van olyan $q \in X^+$ prefixe, amelyre $a_0q \in F$. (Ellenkező esetben $\delta'(a_0, p) = a_0p$, s így $a_0p \in F$, ami lehetetlen.) Legyen $q_1 \in X^+$ a p szó legrövidebb prefixe, amelyre $a_0q_1 \in F$. Ha $q_1 = p$, akkor $p \in L$. Ha $p = q_1p_1$ ($p_1 \in X^+$), akkor, (7.16)-ot is felhasználva, kapjuk, hogy

$$\delta'(a_0, p) = \delta'(\{a_0q_1, a_0\}, p_1) = \delta'(a_0q_1, p_1) \cup \delta'(a_0, p_1).$$

A p_1 szónak van olyan $q' \in X^+$ prefixe, hogy $a_0q_1q' \in F$ vagy $a_0q' \in F$. (Ellenkező esetben $\delta'(a_0q_1, p_1) = a_0q_1p_1$ vagy $\delta'(a_0, p_1) = a_0p_1$, de $\delta'(a_0, p) \cap F \neq \emptyset$ miatt $a_0q_1p_1 \in F$ vagy $a_0p_1 \in F$, ami lehetetlen.) Legyen $q_2 \in X^+$ a p_1 szó legrövidebb prefixe, amelyre $a_0q_1q_2 \in F$ vagy $a_0q_2 \in F$. Ha $q_1q_2 = p$, akkor $p \in L + L^2$. Ha $p = q_1q_2p_2$ ($p_2 \in X^+$), akkor

$$\delta'(a_0, p) = \delta'(a_0q_1, p_1) \cup \delta'(a_0, p_1) = \delta'(a_0q_1q_2, p_2) \cup \delta'(a_0q_2, p_2) \cup \delta'(a_0, p_2).$$

Az eljárást véges sokszor megismételve azt kapjuk, hogy van olyan n pozitív egész szám, hogy $p \in L + L^2 + \cdots + L^n$. Ebből következik, hogy $L(\mathbf{P}(\mathbf{A}), T) \subseteq L^+$, s így $L(\mathbf{P}(\mathbf{A}), T) = L^+$. Mivel a véges automatákban felismerhető X feletti nyelvek halmaza zárt az összeadás műveletére és $L^* = L^+ + e$, ezért L^* is felismerhető véges automatában. Ezzel beláttuk azt is, hogy a véges automatákban felismerhető X feletti nyelvek halmaza zárt az iteráció műveletére. □

7.7. Mealy automatákban felismerhető nyelvek

A nyelvek felismerhetőségének fogalma kiterjeszthetjük Mealy automatákra is úgy, hogy az automata kimeneti viselkedését is figyelembe vesszük. Azt mondjuk, hogy az X ábécé feletti L nyelv *felismerhető* vagy *előállítható* az $\mathbf{A} = (A, a_0, X, Y, \delta, \lambda)$ Mealy automatában az $A' \times Y'$ ($A' \subseteq A$, $Y' \subseteq Y \cup e$) halmazzal, ha

$$L = \{p \in X^*;\ (a_0p, \overline{\lambda(a_0, p)}) \in A' \times Y'\}. \tag{7.16}$$

Az $A' \times Y'$ halmazt Mealy automaták esetében nevezzük *végállapotok halmazá*nak Az $(a, y) \in A' \times Y'$ végállapotban a-t *állapotkoordináta*nak, y-t pedig *kimenő koordináta*nak nevezzük. Ebben az esetben L-re az $L(\mathbf{A}, a_0, A' \times Y')$ vagy az $L(\mathbf{A}, A' \times Y')$ jelölést használjuk. Nyilvánvaló, hogy $e \in L$ akkor és csak akkor, ha $(a_0, e) \in A' \times Y'$.

7.12. Lemma. *Mealy automatákban felismerhető nyelvek megegyeznek a kimenő jel nélküli automatákban felismerhető nyelvekkel.*

Bizonyítás A 7.1. alfejezetben az $\mathbf{A} = (A, a_0, X, \delta, F)$ kimenő jel nélküli felismerő automatához hozzárendeltük azt az $\mathbf{A}_{F,\mu} = (A, a_0, X, \{0,1\}, \delta, \mu)$ Moore automatát, amelyre minden $a \in A$ állapotra $\mu(a) = 1$, ha $a \in F$ és $\mu(a) = 0$, ha $a \notin F$. Nem nehéz belátni, hogy $\mathbf{A}$ az F halmazzal pontosan azt a nyelvet ismeri fel, amelyet $\mathbf{A}_{F,\mu}$ Moore automata (így Mealy automata is) az $(F, 1)$ halmazzal.

Megfordítva, az $\mathbf{A} = (A, a_0, X, Y, \delta, \lambda)$ Mealy automatában az $A' \times Y'$ $(A' \subseteq A, Y' \subseteq Y)$ halmazzal felismert nyelv nem más, mint az $\mathbf{A}$ automata (6.1)-ben definiált $\mathbf{A}_Y = (A \times Y, X, \delta_Y)$ vázában az $A' \times Y'$ halmazzal felismert nyelv, ha $\mathbf{A}_Y$-t az $A_0 = \{(a_0, y;\ (y \in Y\}$ halmazzal inicializáljuk. Könnyen belátható ugyanis, hogy minden $p \in X^*$ bemenő szóra és y kimenő jelre $(a_0, y)p = (a_0 p, \overline{\lambda(a_0, p)})$. (Természetesen $\overline{\lambda(a_0, p)}$ a $\lambda(a_0, p)$ kimenő szó utolsó betűjét jelenti az $\overline{e} = e$ megállapodással.) □

A 7.12 Lemma bizonyításából kapjuk az alábbi következményt.

7.13. Következmény. *Mealy automatákban felismerhető nyelv felismerhető olyan Mealy automatában is, amelyben a végállapotok kimenő koordinátája megegyezik.*

Feladatok

7.1. Az $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában az állapothalmaz F részhalmazával felismerhető L nyelv akkor és csak akkor véges, ha a $\delta(a_0, p)$ $(a_0 p \in F)$ sorozatok különböző állapotokból állnak.

7.2. Ha X legalább kételemű véges ábécé, akkor az X feletti palindromok $P(X)$ nyelve nem reguláris.

8. fejezet

Reguláris nyelvek

Már a 3. fejezet bevezetőjében mondtuk, hogy a programozási nyelvek szintaxisának matematikai megadására nagyon jól használhatók környezetfüggetlen, s ezen belül a reguláris grammatikák. Ezért a 3. fejezetben elég részletesen tárgyaltuk a környezetfüggetlen grammatikákat és nyelveket. Ebben a fejezetben a reguláris nyelvekről további fontos és érdekes részleteket közlünk. Többek között az automaták analízisének és szintézisének problémájához (l. 6.8. alfejezetet) hasonlóan megfogalmazzuk és megoldjuk a véges kimenő jel nélküli automaták analízisének és szintézisének problémáját. A *véges kimenő jel nélküli automaták analízisé*n olyan algoritmust értünk, amely tetszőleges véges iniciális kimenő jel nélküli automatában felismert nyelvnek megadja egy reguláris kifejezését. A *véges kimenő jel nélküli automaták szintézise* pedig olyan algoritmust jelent, amely egy reguláris kifejezéssel megadott nyelvhez megad egy iniciális véges kimenő jel nélküli automatát, amely állapothalmazának valamely részhalmazával felismeri a nyelvet.

A 7.6. alfejezetben, valamint 7.1 és a 7.5 Tételekben a véges automatákkal felismerhető nyelvekkel foglalkoztunk. Ilyen irányú vizsgálatainkat az alapvető jelentőségű Kleene tétellel folytatjuk, amely szerint a reguláris nyelvek $\mathcal{R}$ osztálya éppen a véges automatákkal felismerhető nyelvek osztálya. Pontosabban, ha X egy véges ábécé, akkor az X felettit reguláris nyelvek $R(X)$ halmaza pontosan az X feletti véges kimenő jel nélküli automatákkal felismerhető nyelvek halmaza. Megjegyezzük, hogy sok eredményt a [2] elektronikus jegyetünk *Automaták és nyelvek* részében közöltünk, de a teljesség kedvéért ezeket megismételjük.

8.1. Kleene tétele

8.1. Tétel. *(Kleene tétele) Véges ábécé feletti nyelv akkor és csak akkor reguláris, ha felismerhető véges automatában.*

Bizonyítás Először megmutatjuk azt, hogy bármely $X = \{x_1, x_2, \ldots, x_m\}$ ábécé feletti reguláris nyelv felismerhető X feletti véges automatában. Az 1.1. alfejezetben megadtuk a reguláris nyelv fogalmát. Ez alapján A 7.10 Tétel szerint csak azt kell megmutatni, hogy az $\emptyset$ üres nyelv, az e nyelv és az x_j $(j = 1, 2, \ldots m)$ elemi nyelvek felismerhetők X feletti véges automatákban.

Az $\emptyset$ üres nyelv tetszőleges véges automatában felismerhető az állapothalmaz üres részhalmazával.

Az e üres szóból álló egyelemű nyelv felismerhető például abban az

$$\mathbf{A} = (\{a_0, a\}, a_0, X, \delta)$$

kétállapotú automatában az a_0 állapottal, amelyben minden $x \in X$ bemenő jelre

$$\delta(a_0, x) = \delta(a, x) = a.$$

Bármely $x_i \in X$ egyelemű nyelv felismerhető az

$$\mathbf{A}_i = (\{a_0, a_1, a_2\}, a_0, X, \delta_i)$$

automatában az a_1 állapottal, amelynek állapotfüggvényét minden $x_j \in X$ bemenő jelre a

$$\delta_i(a_k, x_j) = \begin{cases} a_1, & \text{ha } k = 0,\ j = i, \\ a_2, & \text{ha } k = 0,\ j \neq i, \\ a_2, & \text{ha } k = 1, 2 \end{cases}$$

összefüggéssel definiáljuk.

Ezek után bebizonyítjuk az állítás megfordítását, azaz azt, hogy minden véges automatában felismerhető nyelv reguláris. Tegyük fel, hogy az X feletti L nyelv felismerhető az $\mathbf{A}_F = (A, a_0, X, \delta)$ véges automatában az F halmazzal, azaz $L = L(\mathbf{A}, F)$. Ha $L = \emptyset$, akkor definíció szerint reguláris. Tegyük fel, hogy $L \neq \emptyset$. Az egyszerűbb írásmód kedvéért legyen $A = \{1, 2, \ldots, n\}$ és $a_0 = 1$. Ha $F = \{i_1, i_2, \ldots i_k\}$, akkor nyilvánvalóan érvényes az

$$L(\mathbf{A}_F) = L(\mathbf{A}, i_1) + L(\mathbf{A}, i_2) + \cdots + L(\mathbf{A}, i_k) \tag{8.1}$$

összefüggés. Ez azt jelenti, hogy ha az $L(\mathbf{A}, i_j)$ $(j = 1, 2, \ldots, k)$ nyelvek regulárisak, akkor $L = L(\mathbf{A}, F)$ is az. Ezért elegendő bebizonyítani, hogy az

automata állapothalmazának egyelemű részhalmazaival felismerhető nyelvek regulárisak.

Tetszőleges $i, j = 1, 2, \ldots, n$ és $k = 0, 1 \ldots, n$ egész számokra jelölje $L_{i,j}^{(k)}$ azt az X feletti nyelvet, amelyek azokból és csak azokból X^*-beli szavakból áll, amelyek hatására az $\mathbf{A}$ automata az i állapotából a j állapotába megy át úgy, hogy az átmenet során közbülső állapotként legfeljebb az $1, 2, \ldots, k$ állapotok léphetnek fel. Speciálisan $L_{i,j}^{(0)}$ pontosan azokat a bemenő szavakat tartalmazza, amelyek az $\mathbf{A}$ automatát az i állapotból közbülső állapot nélkül viszi át a j állapotba. Ilyen jelölés mellett

$$L(\mathbf{A}, i) = L_{1,i}^{(n)}, \tag{8.2}$$

ezért elegendő megmutatni, hogy az $L_{1,i}^{(n)}$ nyelv reguláris. Ennél többet mutatunk meg, mégpedig k szerinti teljes indukcióval megmutatjuk ezt minden $L_{i,j}^{(k)}$ $(1 \leq i, j \leq n,\ 0 \leq k \leq n)$ nyelvre.

Legyen $k = 0$. Nyilvánvaló, hogy ebben az esetben

$$L_{i,j}^{(0)} = \{x \in X; \delta(i, x) = j\}. \tag{8.3}$$

Mivel X véges halmaz, ezért $L_{i,j}^{(0)}$ is véges. ($L_{i,j}^{(0)} = \emptyset$ is lehetséges.) De minden véges nyelv reguláris, így $k = 0$ esetre igaz az állítás. Legyen $k \geq 1$. Tegyük fel, hogy az

$$L_{i,j}^{(k-1)} \quad (1 \leq i, j \leq n)$$

nyelvek mind regulárisak. Megmutatjuk, hogy

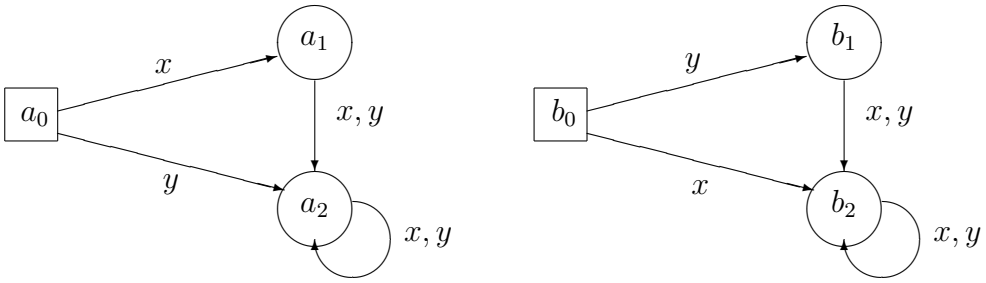
$$L_{i,j}^{(k)} = L_{i,j}^{(k-1)} + L_{i,k}^{(k-1)} \left(L_{k,k}^{(k-1)}\right)^* L_{k,j}^{(k-1)} \tag{8.4}$$

igaz, ami azt jelenti, hogy $L_{i,j}^{(k)}$ is reguláris. A definíció alapján világos, hogy az egyenlőség jobb oldalán lévő halmaz része a bal oldalinak. Annak megmutatásához, hogy a bal oldali halmaz is része a jobb oldalinak, tekintsünk egy tetszőleges $p \in L_{i,j}^{(k)}$ szót. Ha nincs ilyen p szó, akkor ez triviális, mivel $L_{i,j}^{(k)} = \emptyset$. Ha van ilyen p szó, akkor különböztessünk meg két esetet. Ha p úgy viszi át az $\mathbf{A}$ automatát az i állapotból a j állapotba, hogy a közbülső állapotok között nem fordul elő a k állapot, akkor $p \in L_{i,j}^{(k-1)}$. Ha pedig p úgy viszi át az $\mathbf{A}$ automatát az i állapotból a j állapotba, hogy közbülső állapotként a k állapot is fellép, akkor $p \in L_{i,k}^{(k-1)} \left(L_{k,k}^{(k-1)}\right)^* L_{k,j}^{(k-1)}$. Ebből már látható, hogy, a bal oldali halmaz része a jobb oldalinak. Ezzel megmutattuk, hogy minden $k = 0, 1, \ldots, n$ számra minden $L_{i,j}^{(k)}$ $(1 \leq i, j \leq n)$ nyelv reguláris. Ami azt jelenti, hogy minden véges automatában felismerhető nyelv reguláris. □

Megjegyezzük, hogy a Kleene tétel második részének bizonyítása McNaughtontól és Yamadától származik. Kleene erre egy nagyon bonyolult, nehezen követhető bizonyítást adott. A Kleene tétel bizonyításából látható, hogy a véges kimenő jel nélküli automaták analízisének és szintézisének problémája megoldható. Az analízis probléma egy algoritmikus megoldását a (8.1)-(8.4) összefüggések alkalmazásával kapjuk. A szintézis problémájának egy algoritmikus megoldása is leolvasható a Kleene tétel és a 7.10 Tétel bizonyításból. A bizonyításból az algoritmus lépéseinek sorrendje is megkapható. Ez az algoritmus azonban meglehetősen nehézkes, és még egyszerűbb szerkezetű reguláris kifejezéssel megadott nyelv esetén is nagy állapotszámú automatát eredményezhet. Az algoritmus nagymértékben egyszerűsíthető, ha a konstrukciókban csak iniciálisan összefüggő automatákkal dolgozunk, vagyis csak a kezdő állapotból elérhető állapotokat írjuk fel. Nézzük meg ezt az egyszerűsített eljárást a következő példában.

8.2. Példa. *Megadunk olyan automatát, amelyben az $X = \{x, y\}$ halmaz feletti xy reguláris kifejezéssel megadott nyelv felismerhető.*

A Kleene tétel bizonyításában használt algoritmus szerint először is meg kell konstruálni az $\mathbf{A}_x$ és $\mathbf{A}_y$ háromállapotú automatákat az x ill. y elemi nyelvek felismeréséhez. Adjuk meg ezeket az automatákat a 8.1. ábrán átmenetgráfjukkal:



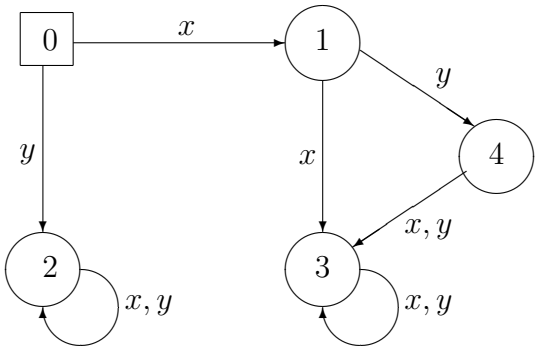
8.1. ábra.

Azután a bizonyításból leolvasott algoritmus szerint venni kell az $\mathbf{A}_x$ automata és a $\mathbf{P}(\mathbf{A_y})$ hatványautomata direkt szorzatát az $(a_0, \emptyset)$ kezdőállapottal. Könnyen belátható, hogy ennek az automatának 24 állapota van. Nekünk azonban csak az $(a_0, \emptyset)$ állapotból elérhető állapotokra van szükségünk, ezért elegendő a direkt szorzat $0 = (a_0, \emptyset)$ kezdőállapotú iniciálisan összefüggő $\mathbf{C} = (C, 0, X, \delta)$ részautomatáját megkonstruálni. Ehhez meghatározzuk az 0 állapotból elérhető állapotokat:

$$\delta(0, x) = (a_1, b_0) = 1, \quad \delta(0, y) = (a_2, \emptyset) = 2,$$

$$\delta(1,x) = (a_2, b_2) = 3, \quad \delta(1,y) = (a_2, b_1) = 4,$$
$$\delta(2,x) = \delta(2,y) = 2,$$
$$\delta(3,x) = \delta(3,y) = \delta(4,x) = \delta(4,y) = 3.$$

A **C** automata átmenetgráfját a 8.2. ábrán láthatjuk.



8.2. ábra.

A **C** automata felismeri az xy nyelvet a 4 állapottal.

Még ez az egyszerűsített eljárás sem biztosítja azt, hogy a legkisebb állapotszámú automatát kapjuk meg a nyelvet felismerő automaták közül.

Nem nehéz belátni, hogy az xy nyelv felismerhető az $\mathbf{D} = (D, d_0, X, \delta')$ négyállapotú automatában is a d_2 állapottal, ahol az automata átmenettáblázata:

D	d_0	d_1	d_2	d_3
x	d_1	d_3	d_3	d_3
y	d_3	d_2	d_3	d_3,

A **D** automata a **C** automata homomorf képe. (A $\varphi : C \to D$ leképezés, amelyre $\varphi(0) = d_0,\ \varphi(1) = d_1,\ \varphi(2) = \varphi(3) = d_3, \varphi(4) = d_2$, homomorfizmus.) Az olvasóra bízzuk annak átgondolását, hogy az xy nyelv négynél kevesebb állapotú automatában nem állítható elő.

A véges iniciális automaták szintézisproblémájának megoldására egy Gluskovtól származó, az előzőnél sokkal hatékonyabb algoritmust ismertetünk a [2]

elektronikus jegyzetünk *Automaták és nyelvek* részében. Ráadásul ez az algoritmus alkalmas arra is, hogy véges sok, reguláris kifejezéssel megadott nyelvhez egyszerre szerkesszünk meg olyan véges iniciálisan összefüggő automatát, amelyben az adott nyelvek mindegyike felismerhető az állapothalmaz alkalmas részhalmazaival. Ez az algoritmus alkalmas a véges automatákkal indukálható automataleképezések meghatározására is.

Mint említettük, a véges kimenő jel nélküli automaták analízis problémájának egy algoritmikus megoldását a (8.1)-(8.4) összefüggések alkalmazásával kapjuk. A következő példában ezt mutatjuk be.

8.3. Példa. *Felírjuk annak az L nyelvnek egy reguláris kifejezését, amely felismerhető az*

A	1	2	3
x	1	3	3
y	2	1	1

átmenettáblázattal megadott $\mathbf{A} = (\{1,2,3\}, 1, \{x,y\}, \delta)$ *iniciális automatában a* 3 *állapottal.*

A (8.1) és a (8.2) összefüggések jelölései szerint $L = L(\mathbf{A}, 3) = L_{1,3}^{(3)}$. A (8.4) rekurziós formula és az 1.1 Lemma felhasználásával kapjuk, hogy

$$L = L_{1,3}^{(2)} + L_{1,3}^{(2)} \left(L_{3,3}^{(2)}\right)^* L_{3,3}^{(2)} = L_{1,3}^{(2)} \left(e + \left(L_{3,3}^{(2)}\right)^* L_{3,3}^{(2)}\right) = L_{1,3}^{(2)} \left(L_{3,3}^{(2)}\right)^*.$$

De

$$L_{1,3}^{(2)} = L_{1,3}^{(1)} + L_{1,2}^{(1)} \left(L_{2,2}^{(1)}\right)^* L_{2,3}^{(1)}.$$

Megrajzolva $\mathbf{A}$ átmenetgráfját, a (8.3) összefüggés felhasználásával az átmenetgráfról könnyen leolvasható, hogy

$$L_{1,3}^{(1)} = L_{1,3}^{(0)} + L_{1,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,3}^{(0)} = \emptyset + xx^*\emptyset = \emptyset,$$

$$L_{1,2}^{(1)} = L_{1,2}^{(0)} + L_{1,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,2}^{(0)} = y + xx^*y = (e + xx^*)y = x^*y,$$

$$L_{2,2}^{(1)} = L_{2,2}^{(0)} + L_{2,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,2}^{(0)} = \emptyset + yx^*y = yx^*y,$$

$$L_{2,3}^{(1)} = L_{2,3}^{(0)} + L_{2,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,3}^{(0)} = x + yx^*\emptyset = x,$$

ezért

$$L_{1,3}^{(2)} = \emptyset + x^*y(yx^*y)^*x = x^*y(yx^*y)^*x.$$

Továbbá

$$L_{3,3}^{(2)} = L_{3,3}^{(1)} + L_{3,2}^{(1)} \left(L_{2,2}^{(1)}\right)^* L_{2,3}^{(1)},$$

és

$$L_{3,3}^{(1)} = L_{3,3}^{(0)} + L_{3,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,3}^{(0)} = x + yx^*\emptyset = x,$$

$$L_{3,2}^{(1)} = L_{3,2}^{(0)} + L_{3,1}^{(0)} \left(L_{1,1}^{(0)}\right)^* L_{1,2}^{(0)} = \emptyset + yx^*y = yx^*y,$$

ezért

$$L_{3,3}^{(2)} = x + yx^*y(yx^*y)^*x.$$

Következésképpen

$$L = L_{1,3}^{(2)} \left(L_{3,3}^{(2)}\right)^* = x^*y(yx^*y)^*x(x + yx^*y(yx^*y)^*x)^*$$

a keresett nyelv egy reguláris kifejezése.

A 3.4 Tétel szerint bármely szóról algoritmikusan eldönthető, hogy benne van-e egy adott környezetfüggetlen nyelvben, s így speciálisan egy reguláris nyelvben. A formális nyelvek elméletének ezen jellegzetes problémájának eldöntésére reguláris nyelvek esetén Kleene tétele segítségével is adhatunk egy algoritmust. Ehhez valamilyen módon, például az említett Gluskov algoritmus alkalmazásával ([2]), konstruálunk egy véges $\mathbf{A} = (A, a_0, X, \delta)$ automatát, amelyben L felismerhető az állapothalmaz valamely F részhalmazával. Utána legfeljebb $|p| + |F|$ számú lépéssel eldönthető, hogy $a_0p \in F$, azaz $p \in L$, vagy nem.

Kleene tétele alapján a következő tételben szükséges és elégséges feltételt adunk egyelemű ábéc'e feletti nyelv regularitására.

8.4. Tétel. *Az $\{x\}$ ábécé feletti L nyelv, akkor és csak akkor reguláris, ha vannak olyan L_1, L_2 $\{x\}$ feletti véges nyelvek és $0 \leq n$ egész szám, amelyekre $L = L_1 + L_2(x^n)^*$.*

Bizonyítás Ha az L_1, L_2 $\{x\}$ feletti véges nyelvekre és $0 \leq n$ egész számra $L = L_1 + L_2(x^n)^*$, akkor L definíció szerint nyilvánvalóan reguláris.

Megfordítva, legyen az $\{x\}$ ábécé feletti L nyelv reguláris, akkor Kleene tétele szerint van olyan $\mathbf{A}_F = (A, \{x\}, a_0, \delta, F)$ véges automata, amelyre $L = L(\mathbf{A}, F)$. Tudjuk, hogy elegendő iniciálisan összefüggő automatára szorítkozni. Az $\mathbf{A}$ automata végessége miatt vannak olyan $0 \leq k$ és $1 \leq n$ egész számok, hogy $a_0x^k = a_0x^{k+n}$. Legyenek k és n a legkisebb ilyen tulajdonságúak, azaz

$$A = \{a_0, a_0x, \ldots, a_0x^k, \ldots, a_0x^{k+n-1}\}.$$

Legyen továbbá

$$F = \{a_0x^{i_1}, \ldots, a_0x^{i_j},$$

ahol $0 \leq i_1 < \cdots < i_j \leq k + n - 1$. Ha $k = 0$, akkor $L_1 = \emptyset$ és $L_2 = \{x^{i_1}, \ldots, x^{i_j}\}$. Ha $0 < k$, akkor $L_1 = \emptyset$ és $L_2 = \{x^{i_1}, \ldots, x_{i_j}\}$ $(k \leq i_1)$, vagy $L_1 = \{i_1, \ldots i_l\}$ és $L_2 = \{x^{i_{l+1}}, \ldots, x^{i_j}\}$ $(i_l \leq k - 1$ és $k \leq i_{l+1})$, vagy $L_1 = \{x^{i_1}, \ldots, x^{i_j}\}$ $(i_j \leq k - 1$ és $L_2 = \emptyset$. □

8.2. $\mathcal{L}_3 = \mathcal{R}$

A Chomsky nyelvosztályok definíciójánál bizonyítás nélkül említettük meg, hogy a 3 típusú vagy más néven jobb lineáris nyelvek pontosan a reguláris nyelvek. Ezt az állítást most bebizonyítjuk. Megmutatjuk, ugyanis hogy a véges automatákban felismerhető nyelvek megegyeznek a 3 típusú nyelvekkel. Kleene tétele szerint ez azt jelenti, hogy a 3 típusú és a reguláris nyelvek ugyanazok.

8.5. Tétel. *Véges ábécé feletti nyelv akkor és csak akkor ismerhető fel véges automatában, ha 3 típusú.*

Bizonyítás Tegyük fel, hogy az L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában az állapothalmaz F részhalmazával. Definiáljuk a $G = (A, X, a_0, H)$ grammatikát úgy, hogy a nemterminálisok az automata állapotai, a terminálisok a bemenő jelei legyenek. A mondatszimbólum legyen az automata kezdőállapota és a szabályainak H halmaza a következő szabályokat tartalmazza:

$$a \longrightarrow x\delta(a,x)\ (a \in A, x \in X), \quad b \longrightarrow e\ (b \in F).$$

Látható, hogy a G grammatika 3 típusú. Az $a \longrightarrow x\delta(a,x)$ szabályt írhatjuk röviden az $a \longrightarrow x(ax)$ alakban is. Megmutatjuk, hogy a G grammatika generálja az L nyelvet, azaz $L = L(G)$. Ehhez, (2.3) és (7.1) szerint, azt kell belátni, hogy minden $p \in X^*$ bemenő szóra $a_0 \Longrightarrow_G^* p$ akkor és csak akkor, ha $a_0 p \in F$. Ha $p = e$, akkor az H-beli átírási szabályok miatt, $a_0 \Longrightarrow_G^* e$ akkor és csak akkor, ha $a_0 e = a_0 \in F$. Ha $p = x_1 x_2 \dots x_k$ $(x_i \in X, i = 1, 2, \dots, k)$, akkor (2.2) alapján

$$a_0 \Longrightarrow_G x_1(a_0 x_1) \Longrightarrow_G x_1 x_2(a_0 x_1 x_2) \Longrightarrow_G \cdots \Longrightarrow_G$$

$$\Longrightarrow_G x_1 x_2 \dots x_k(a_0 x_1 x_2 \dots x_k).$$

Így $a_0 \Longrightarrow_G^* p$ akkor és csak akkor, ha $a_0 p \in F$. Ezzel megmutattuk, hogy minden véges automatában felismerhető nyelv 3 típusú.

Megfordítva, tegyük fel, hogy a V_T véges ábécé feletti L nyelv 3 típusú, azaz van olyan $G = (V_N, V_T, S, H)$ jobb lineáris grammatika, hogy $L = L(G)$. A 2.9 Lemma és a 2.10 Tétel szerint feltehető, hogy G láncszabálymentes és minden H-beli szabály $X \to xY$ vagy $X \to e$ $(X, Y \in V_N, x \in V_T)$ alakú. Legyen $\mathbf{A} = (V_N, S, V_T, \delta)$ az a nemdeterminisztikus automata, amelyre minden $X \in V_N$ és $x \in V_T$ esetén

$$\delta(X,x) = \{Y \in V_N; X \longrightarrow xY \in H\}.$$

Megmutatjuk, hogy az L nyelv felismerhető a $\mathbf{A}$ automatában az $F = \{X \in V_N; X \to e \in H\}$ halmazzal.

Legyen $p \in L(G)$, akkor van olyan $X \in V_N$, hogy $X \to e$ H-beli szabály és

$$S \Longrightarrow^* pX \Longrightarrow p.$$

Ebből (7.15) felhasználásával következik, hogy $X \in Sp$. De $X \in F$, s így $Sp \cap F \neq \emptyset$. Ez (7.7) szerint azt jelenti, hogy $p \in L(\mathbf{A}, F)$.

Megfordítva, legyen $p \in L(\mathbf{A}, F)$. Akkor $Sp \cap F \neq \emptyset$. Ha $p = e$, akkor $Sp = S \in F$, azaz $S \to e$ H-beli szabály, ezért $e \in L(G)$. Ha $p \neq e$, akkor legyen $p = x_1 x_2 \dots x_k$ $(x_1, x_2, \dots, x_k \in V_T)$. A $Sp \cap F \neq \emptyset$ feltételből következik, hogy vannak olyan $X_1, X_2, \dots, X_k \in V_N$, hogy

$$X_1 \in \delta(S, x_1), X_2 \in \delta(X_1, x_2), \dots, X_k \in \delta(X_{k-1}, x_k), X_k \in F.$$

Ebből következik, hogy

$$S \to x_1 X_1, X_1 \to x_2 X_2, \dots, X_{k-1} \to x_k X_k, X_k \to e$$

H-beli szabályok. Ezért $S \Longrightarrow^* p$, azaz $p \in L(G)$. Ezzel megmutattuk, hogy $L(G) = L(\mathbf{A}, F)$. □

A 8.1 Tétel (Kleene tétele) és a 8.5 Tétel alapján a 7.10 Tétel következőképpen is kimondható:

8.6. Tétel. *Véges ábécé feletti reguláris nyelvek halmaza zárt a Boole műveletekre.*

Már az 1.1. alfejezetben említettük, hogy reguláris nyelv tükörképe,és minden $p \in X^*$ szó szerinti bal [jobb] oldali deriváltja is reguláris. A következő tétel egy újabb szükséges és elégséges feltétel a nyelvek regularitására.

8.7. Tétel. *Egy véges ábécé feletti nyelv akkor és csak akkor reguláris, ha véges sok egymástól különböző bal [jobb] oldali deriváltja van.*

Bizonyítás Legyen L reguláris nyelv X felett. Akkor Kleene tétele szerint létezik olyan $\mathbf{A} = (A, a_0, X, \delta)$ véges iniciális automata, amelyben felismerhető az állapothalmaz valamely F részhalmazával. Akkor bármely $p \in X^*$ szóra az L nyelv (1.1)-ben definiált p szerinti bal oldali $L_p^{(b)}$ deriváltja felismerhető az

$$F_p^{(b)} = \{a_0 pq; pq \in L\}$$

halmazzal abban a véges iniciális automatában, amelyet $\mathbf{A}$-ból úgy kapunk, hogy benne kezdőállapotként a_0 helyett $a_0 p$-t választjuk. Nyilvánvaló, hogy

$F_p^{(b)}$ az F halmaz egy részhalmaza. Mivel F véges, ezért véges sok különböző részhalmaza van. Amiből következik, hogy L-nek véges sok egymástól különböző bal oldali deriváltja van.

Tekintsük most az L nyelv (1.2)-ben definiált p szerinti $L_p^{(j)}$ jobb oldali deriváltját. Az (1.9) azonosságot is felhasználva, az

$$L_p^{(j)} = \left((L_p^{(j)})^{-1}\right)^{-1} = \left((L^{-1})_{p^{-1}}^{(b)}\right)^{-1}$$

összefüggéshez jutunk. Ez azt jelenti, hogy L-nek pontosan annyi egymástól különböző jobb oldali deriváltja van, mint amennyi egymástól különböző bal oldali deriváltja L^{-1}-nek. Mivel L reguláris nyelv, ezért L^{-1} is reguláris nyelv X felett. Így L^{-1}-nek is véges sok egymástól különböző bal oldali deriváltja van. Amiből következik, hogy L-nek véges sok egymástól különböző jobb oldali deriváltja van.

Megfordítva, tegyük fel, hogy az X feletti L nyelvnek összes különböző bal oldali deriváltja

$$L_{p_1}^{(b)}, L_{p_2}^{(b)}, \ldots, L_{p_n}^{(b)}.$$

Legyen τ_L (7.4)-ben definiált jobb kongruencia. Bármely p és q X^*-beli szóra

$$L_p^{(b)} = L_q^{(b)} \quad \Longleftrightarrow \quad (p,q) \in \tau_L.$$

Ez azt jelenti, hogy τ_L véges indexű. Amiből a 7.1 és 7.3 Lemmák, valamint Kleene tétele szerint következik, hogy L reguláris.

Tegyük fel most, hogy L-nek véges sok egymástól különböző jobb oldali deriváltja van. Akkor (1.9) szerint az L^{-1} nyelvnek véges sok egymástól különböző bal oldali deriváltja van. Ami az előbbiek szerint azt jelenti, hogy L^{-1} reguláris nyelv. Ebből következik, hogy L is reguláris nyelv. □

8.3. Pumpáló lemma

A következő lemma egy szükséges feltételt ad arra, hogy egy nyelv reguláris legyen. Tudjuk, hogy minden véges nyelv reguláris, ezért a lemma véges nyelvekre nyilvánvalóan teljesül. A segítségével azonban bizonyos végtelen nyelvekről meg tudjuk mutatni, hogy nem regulárisak. A lemmát *reguláris nyelvekre vonatkozó pumpáló lemmá*nak nevezik, megkülönböztetve a környezetfüggetlen nyelvekre vonatkozó pumpáló lemmától (l. 3.5 Lemma).

8.8. Lemma. *Ha L reguláris nyelv a véges X ábécé felett, akkor van olyan (L-től függő) n pozitív egész szám, hogy ha $p \in L$ és $|p| \geq n$, akkor p előállítható $p = uvw$ $(u, v, w \in X^*)$ alakban, ahol $0 < |v| \leq |uv| \leq n$, és minden m nemnegatív egész számra $uv^m w \in L$.*

Bizonyítás Kleene tétele értelmében van olyan

$$\mathbf{A}_F = (A, a_0, X, \delta; F)$$

véges felismerő automata, amelyre $L = L(\mathbf{A}, F)$. Legyen $|A| = n$. Megmutatjuk, hogy n eleget tesz a tétel állításának.

Legyen $p \in L$ olyan, hogy $|p| \geq n$, vagyis

$$p = x_1 x_2 \dots x_k \ (x_1, x_2, \dots, x_k \in X, n \leq k).$$

Az (6.4) definíció szerint

$$\delta(a_0, p) = a_1 a_2 \dots a_k, \quad \text{ahol} \quad \delta(a_{l-1}, x_l) = a_l, l = 1, 2, \dots, k.$$

Mivel $k \geq n$, ezért az állapotok $a_0, a_1, \dots, a_k$ sorozatában van legalább két megegyező állapot, vagyis vannak olyan $0 \leq i < j \leq k$ számok, hogy $a_i = a_j$. Továbbá, i és j választhatók úgy, hogy az $a_0, \dots, a_{j-1}$ sorozatban már nincsenek megegyező állapotok. Legyenek $u = x_1 \dots x_i$, $v = x_{i+1} \dots x_j$ és $w = x_{j+1} \dots x_k$. (Ha $i = 0$, akkor $u = e$, ha pedig $j = k$, akkor $w = e$.) Belátjuk, hogy u, v és w kielégítik a tétel feltételeit. Az, hogy $p = uvw$ és $v \neq e$, nyilvánvaló. Tegyük fel, hogy $|uv| = j > n$, azaz $j - 1 \geq n$. Ez azt jelenti, hogy az $a_0, \dots, a_{j-1}$ sorozatban van legalább két megegyező állapot. Ez azonban lehetetlen, ezért $|uv| \leq n$. Mivel $a_i = a_j$, ezért minden $m \geq 0$ egész számra $a_i v^m = a_j$. (A v^0 az e üres szót jelenti.) Így minden $m \geq 0$ egész számra

$$a_k = a_0 p = a_0 uvw = a_0 uv^m w.$$

Mivel $p \in L$, ezért $a_0 p \in F$. Ebből következik, hogy $a_0 uv^m w \in F$. Ami azt jelenti, hogy $uv^m w \in L$. □

A reguláris nyelvekre vonatkozó pumpáló lemma segítségével megmutatjuk a (2.4) Chomsky hierarchiában az első valódi tartalmazás helyességét.

8.9. Tétel. $\mathcal{L}_3 \subset \mathcal{L}_2$.

Bizonyítás A valódi tartalmazás igazolásához elegendő megadni egy olyan környezetfüggetlen nyelvet, amelyik nem reguláris. Könnyű igazolni (l. 2.4 feladat), hogy az $X = \{x, y\}$ ábécé feletti $L = \{x^k y^k; k \geq 0\}$ nyelvet generálja az a 2 típusú (speciálisan lineáris) $G = (S, X, S, H)$ grammatika, amelyben $H = \{S \to xSy, S \to e\}$. Megmutatjuk, hogy L nem reguláris. Indirekt bizonyítást adunk. Tegyük fel, hogy L reguláris. Akkor van olyan n pozitív egész szám, hogy minden legalább n hosszúságú L-beli p szóra, így a $p = x^n y^n$ szóra is, teljesülnek a pumpáló lemma feltételei. Azaz a $p = x^n y^n$ szó

felírható $p = uvw$ $(u, v, w \in X^*)$ alakban, ahol $|uv| \leq n$, $v \neq e$ és minden m nemnegatív egész számra $uv^m w \in L$. Vizsgáljuk meg a v szóban az x és y betűk előfordulását. Ha v-ben csak x betű szerepel, akkor például az uv^2w szóban az x-ek száma nagyobb, mint az y-ok száma. Ez azonban lehetetlen, mivel $uv^2w \in L$. Ugyanúgy mutatható meg, hogy v nem állhat csupa y betűből. Ezek szerint v-ben mind a két betűnek szerepelnie kell. Ez azonban azt jelenti, hogy az uv^2w szóban van olyan y, amely megelőz egy x betűt, ami $uv^2w \in L$ miatt szintén lehetetlen. Tehát az L nyelv nem teljesíti a pumpáló lemma követelményeit, ezért nem reguláris. □

A 3.7 Következmény szerint egyelemű ábécé esetén minden környezetfüggetlen nyelv reguláris. Megmutatjuk, hogy legalább kételemű ábécé esetén (2.5)-ben az első tartalmazás valódi.

8.10. Következmény. *Ha $|U| > 1$, akkor $R(U) \subset CF(U)$.*

Bizonyítás Legyen $x, y \in U$ és $x \neq y$. Akkor a 8.9 Tétel bizonyítása szerint $\{x^k y^k; k \geq 0\} \in CF(U)$, de $\{x^k y^k; k \geq 0\} \notin R(U)$. □

8.4. Eldöntési algoritmusok

A 3.9 Tétel szerint algoritmikusan eldönthető, hogy egy reguláris nyelv üres, véges vagy végtelen. Az alábbiakban ennek eldöntésére reguláris grammatikák helyett véges automaták segítségével adunk algoritmust.

8.11. Lemma. *Ha az $L \neq \emptyset$ nyelv felismerhető egy n állapotú automatában, akkor van L-ben legfeljebb $n-1$ hosszúságú szó.*

Bizonyítás Tegyük fel, hogy az L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ n állapotú automatában az állapothalmaz F részhalmazával. Válasszuk ki L egy tetszőleges p elemét. Ha $|p| \leq n-1$, akkor készen vagyunk a bizonyítással. Ha $|p| \geq n$, akkor $|A| = n$ miatt létezik p-nek olyan q kezdőszelete, hogy $|q| \leq n-1$ és $a_0 q = a_0 p$. Mivel $p \in L$, ezért $a_0 q = a_0 p \in F$, s így $q \in L$. □

8.12. Lemma. *Egy n állapotú automatában felismerhető L nyelv akkor és csak akkor végtelen, ha van L-ben olyan p szó, amelyre $n \leq |p| < 2n$.*

Bizonyítás Ha van ilyen p szó L-ben, akkor a pumpáló lemma alapján L végtelen.

Megfordítva, tegyük fel, hogy az X feletti végtelen L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ n állapotú automatában az állapothalmaz F részhalmazával. Mivel L végtelen, van olyan $p \in L$, hogy $n \leq |p|$. Ha $|p| < 2n$, akkor készen

vagyunk a bizonyítással. Legyen $|p| \geq 2n$. Akkor a pumpáló lemmában szereplő jelöléseket alkalmazva, vannak olyan $u, v, w \in X^*$ szavak, hogy $p = uvw$, $0 < |v| \leq |uv| \leq n$, és $q = uw \in L$, vagyis $n \leq |q| = |p| - |v| < |p|$. Ha $|q| < 2n$, akkor a bizonyítást befejeztük. Ha $|q| \geq 2n$, akkor alkalmazzuk a pumpáló lemmát q-ra. Ezt folytatva, véges számú lépés után kapunk olyan $r \in L$ szót, amelyre $n \leq |r| < 2n$. □

A 3.9 Tételnek reguláris nyelvekre egy másik bizonyítását adjuk. A bizonyítás reguláris nyelvekre automaták segítségével ad egy eldöntési algoritmust.

8.13. Tétel. *Létezik olyan algoritmus, amelynek alkalmazásával eldönthető, hogy egy véges automatában felismerhető nyelv üres, véges vagy végtelen.*

Bizonyítás Tegyük fel, hogy az L nyelv felismerhető $\mathbf{A} = (A, a_0, X, \delta)$ n állapotú automatában az állapothalmaz F részhalmazával. Jelölje $X(k)$ az X^* legfeljebb k hosszúságú szavainak részhalmazát, és legyen

$$A(k) = \{a_0 p;\ p \in X(k)\}.$$

A 8.11 Lemma szerint, $L \neq \emptyset$ akkor és csak akkor, ha $A(n-1) \cap F \neq \emptyset$. Mivel bármely nemnegatív egész számra $X(k)$ véges halmaz, ezért véges számú lépésben eldönthető, hogy L üres vagy nem. Legyen $L \neq \emptyset$. A 8.12 Lemma szerint, L akkor és csak akkor végtelen, ha

$$(A(2n-1) - A(n-1)) \cap F \neq \emptyset.$$

Ez szintén eldönthető véges számú lépésben. □

8.14. Tétel. *Létezik véges automatákban felismerhető nyelvek egyenlőségét eldöntő algoritmus.*

Bizonyítás Ha az L és K nyelvek regulárisak, akkor a 8.6 Tétel szerint az

$$L' = (L \cap \overline{K}) + (K \cap \overline{L})$$

nyelv is reguláris. Világos, hogy

$$L = K \Longleftrightarrow L' = \emptyset.$$

A 8.13 Tétel szerint az algoritmikusan eldönthető, hogy $L' = \emptyset$. □

8.15. Tétel. *Létezik olyan algoritmus, amellyel eldönthető, hogy két véges automatában felismerhető nyelv közül valamelyik tartalmazza-e a másikat.*

Bizonyítás Ha az L és K nyelvek regulárisak, akkor a 8.6 Tétel szerint az $L \cap \overline{K}$ nyelv is az. Továbbá

$$L \subseteq K \Longleftrightarrow L \cap \overline{K} = \emptyset.$$

Az utóbbi állítás pedig a 8.13 Tétel szerint algoritmikusan eldönthető. □

8.5. Véges automaták alaptétele

Az automaták szintézisének 6.8. alfejezetben megfogalmazott problémájához visszatérve, ebben az alfejezetben a reguláris nyelvek segítségével ezt a problémát megoldjuk véges automatákra.

Tekintsük a (6.20)-ban definiált $\alpha : X^* \to Y^*$ automataleképezés által indukált osztályozás. A 6.5 Lemmából nyilvánvalóan következik az alábbi lemma:

8.16. Lemma. *Ha $X \neq \emptyset$ és $Y \neq \emptyset$ véges halmazok, akkor bármely $\alpha : X^* \to Y^*$ automataleképezés által indukált $\mathcal{C}_\alpha$ osztályozás véges. Megfordítva, a véges $X \neq \emptyset$ feletti X^+ szabad félcsoport tetszőleges $\mathcal{C}$ véges osztályozása a véges Y halmaz elemeinek jelölésétől eltekintve egyértelműen meghatározza azt az $\alpha : X^* \to Y^*$ automataleképezés, amelyre $\mathcal{C} = \mathcal{C}_\alpha$ teljesül.*

Az $X \neq \emptyset$ véges ábécé feletti nyelvek $\{L_1, L_2, \ldots, L_n\}$ rendszerét *X feletti reguláris teljes rendszer*nek nevezzük, ha a rendszer az X^+ szabad félcsoport osztályozása és minden eleme reguláris nyelv. A következő tételt fontossága miatt *a véges automaták alaptételé*nek is nevezzük:

8.17. Tétel. *A véges $X \neq \emptyset$ és $Y \neq \emptyset$ halmazok esetén egy $\alpha : X^* \to Y^*$ automataleképezés akkor és csak akkor indukálható véges iniciális automatával, ha az α által indukált $\mathcal{C}_\alpha$ osztályozás X feletti reguláris teljes rendszer.*

Bizonyítás A 8.16 Lemma szerint az $\alpha : X^* \to Y^*$ automataleképezés és a $\mathcal{C}_\alpha$ osztályozás az Y halmaz elemeinek jelölésétől eltekintve kölcsönösen egyértelműen meghatározzák egymást.

A szükségesség kimutatása céljából tegyük fel, hogy az $\alpha : X^* \to Y^*$ automataleképezés indukálható az $\mathbf{A} = (A, a_0, X, Y, \delta, \lambda)$ véges iniciális Mealy automatával. Feltehetjük, hogy $\mathbf{A}$ iniciálisan összefüggő. Legyen minden $y \in Y$ kimenő jelre (6.20)-ban definiált L_y halmaz és

$$A_y = \{a_0 p; p \in L_y\}.$$

A (7.16) definíció szerint L_y felismerhető az $\mathbf{A}$ Mealy automatában az $A_y \times y$ halmazzal. Minthogy $\mathbf{A}$ véges automata, ezért Kleene tétele miatt $\mathcal{C}_\alpha$ reguláris teljes rendszer X felett.

Megfordítva, az elegendőség bizonyításához tegyük fel, hogy az α automataleképezés által indukált $\mathcal{C}_\alpha = \{L_y; y \in Y\}$ véges osztályozás reguláris teljes rendszer X felett. Legyen $Y = \{y_1, \ldots, y_n\}$. Tegyük fel, hogy az L_{y_i} $(i = 1, \ldots, n)$ reguláris nyelvet felismeri az $\mathbf{A}_i = (A_i, a_{i0}, X, \delta_i)$ iniciálisan összefüggő automata az F_i halmazzal. Feltehető az is, hogy ha $i \neq j$, akkor $A_i \cap A_j = \emptyset$. Legyen $\mathbf{A} = (A, \mathbf{a}_0, X, \delta)$ az $\mathbf{A}_i$ iniciális automaták direkt szorzata, azaz $A = A_1 \times \cdots \times A_n$, $\mathbf{a}_0 = (a_{10}, \ldots, a_{n0})$, továbbá minden

$\mathbf{a} = (a_1, \ldots, a_n) \in A$ és $x \in X$ esetén

$$\delta(\mathbf{a}, x) = (\delta_1(a_1, x), \ldots, \delta_n(a_n, x).$$

Egészítsük ki ezt az automatát az $\mathbf{A}' = (A, \mathbf{a}_0, X, Y, \delta, \lambda)$ Mealy automatává úgy, hogy minden $\mathbf{a} = (a_1, \ldots, a_i, \ldots, a_n) \in A$ és $x \in X$ esetén

$$\lambda(\mathbf{a}, x) = y_i \quad \Longleftrightarrow \quad (\delta_i(a_i, x) \in F_i \text{ és } \delta_j(a_j, x) \notin F_j \ (j \neq i)). \tag{8.5}$$

Minden más esetben $\lambda(\mathbf{a}, x)$ legyen Y egy tetszőleges rögzített eleme.

A bemenő szavak hossza szerinti teljes indukcióval megmutatjuk, hogy $\mathbf{A}$ iniciális automata indukálja az α automataleképezést, azaz $\alpha = \alpha_{\mathbf{A}}$. A (6.3) és a (6.4) kiterjesztéseket is felhasználva kapjuk, hogy

$$\alpha(e) = \lambda(\mathbf{a}_0, e) = \alpha_{\mathbf{A}}.$$

Az $x \in X$ bemenő jelre legyen $\alpha(x) = y_i$. Mivel $\mathcal{C}_\alpha = \{L_{y_i} \ i = 1, \ldots, n\}$ az X^+ szabad félcsoport osztályozása, ezért (8.5) szerint $\delta_i(a_i, x) in F_i$, s ha $j \neq i$, akkor $\delta_j(a_j, x) \neq F_j$. Ez azt jelenti, hogy

$$\alpha(x) = y_i = \lambda(\mathbf{a}_0, x) = \alpha_{\mathbf{A}}(x).$$

Tegyük fel, hogy $p \in X^+$ bemenő szóra $\alpha(p) = \alpha_{\mathbf{A}}(p)$. Ha $x \in X$ bemenő jelre $px \in L_{y_i}$, akkor (6.17)-et és a 6.3 Tételt is felhasználva $\alpha(px) = \alpha(p)\alpha_p(x)$, s így $\alpha_p(x) = y_i$. De $px \in L_{y_i}$ miatt $\delta_i(a_{i0}p, x) \in F_i$. Így a (8.5) feltételből következik, hogy $\lambda(\mathbf{a}_0, x) = y_i$. Amiből

$$\alpha_{\mathbf{A}}(px) = \lambda(\mathbf{a}_0, px) = \lambda(\mathbf{a}_0, p)\lambda(\mathbf{a}_0 p, x) =$$

$$= \alpha_{\mathbf{A}}(p)y_i = \alpha(p)\alpha_p(x) = \alpha(px),$$

vagyis $\alpha = \alpha_{\mathbf{A}}$. □

Megjegyezzük, hogy a bizonyításban szereplő $\mathbf{A}'$ Mealy automata tekinthető olyan Moore automatának is, amelynek μ jelfüggvénye definálható úgy, hogy minden $\mathbf{a} = (a_1, \ldots, a_i, \ldots, a_n) \in A$ és $x \in X$ esetén

$$\mu(\mathbf{a}) = y_i \quad \Longleftrightarrow \quad (a_i \in F_i \text{ és } a_j \notin F_j \ (j \neq i)). \tag{8.6}$$

Minden más esetben $\mu(\mathbf{a})$ legyen Y egy tetszőleges rögzített eleme.

A 8.16 Lemma és a véges automaták alaptétele bizonyításában a *véges automaták szintézisproblémájának egy algoritmikus megoldásá*t kapjuk. A reguláris teljes rendszerben szereplő nyelveket felismerő kimenő jel nélküli automatákat megkonstruálhatjuk például a Kleene tétel bizonyítása alapján.

A következő tételben azt mutatjuk meg, hogy a véges Mealy és Moore automatákkal megvalósítható információátalakítások, azaz az általuk indukált automataleképezések reguláris nyelveket reguláris nyelvekké alakítanak át.

8.18. Tétel. *Ha az X véges ábécé feletti L nyelv reguláris és $\alpha : X^* \to Y^*$ automataleképezés, akkor az Y ábécé feletti $\alpha(L) = \{\alpha(p);\ p \in L\}$ nyelv is reguláris.*

Bizonyítás Kleene tétele szerint van olyan véges $\mathbf{A} = (A, a_0, X, \delta_A)$ automata, amely felismeri az L nyelvet az állapothalmaz valamely F részhalmazával. Legyen $\mathbf{B} = (B, b_0, X, Y, \delta_B, \lambda_B)$ egy olyan véges Mealy automata, amely indukálja az $\alpha : X^* \to Y^*$ automataleképezést, azaz $\alpha = \alpha_{\mathbf{B}}$ (l. a 6.8. alfejezetet). Vegyük a következő nemdeterminisztikus véges automatát:

$$\mathbf{C} = (A \times B, (a_0, b_0), Y, \delta_C),$$

ahol

$$(a', b') \in \delta_C((a, b), y) \iff \delta_A(a, x) = a',\ \delta_B(b, x) = b',\ \lambda_B(b, x) = y \quad (8.7)$$

valamilyen $x \in X$ bemenő jel esetén. Megmutatjuk, hogy $\mathbf{C}$ állapothalmazának $F \times B$ részhalmazával felismeri az $\alpha(L)$ nyelvet.

Legyen $p \in L$. Ha $p = e$, akkor $\alpha(p) = e \in \alpha(L)$. De $(a_0, b_0) \in F \times B$, ezért $e \in L(\mathbf{C}, F \times B)$. Ha pedig $p = x_1 x_2 \dots x_k$ és $\alpha(p) = y_1 y_2 \dots y_k$, ahol $x_j \in X$, $y_j \in Y$ $(j = 1, 2 \dots, k)$, akkor (6.4) és (7.1) szerint vannak olyan $a_i \in A$ és $b_i \in B$ állapotok, hogy minden $i \in \{0, 1, 2, \dots, k-1\}$ esetén

$$\delta_A(a_i, x_{i+1}) = a_{i+1}, \quad \delta_B(b_i, x_{i+1}) = b_{i+1}, \quad \lambda_B(b_i, x_{i+1}) = y_{i+1}$$

teljesülnek. Az (7.14) definíciót is felhasználva, ezekből adódik, hogy

$$(a_{i+1}, b_{i+1}) \in \delta_C((a_i, b_i), y_{i+1}), \quad i = 0, 1, \dots, k-1,$$

azaz

$$(a_k, b_k) \in \delta_C((a_0, b_0), \alpha(p)) \cap F \times B.$$

Ez a (7.7) definíció szerint azt jelenti, hogy $\alpha(p) \in L(\mathbf{C}, F \times B)$.

Megfordítva, tegyük fel, hogy $q \in L(\mathbf{C}, F \times B)$, azaz

$$(a_0, b_0)q \cap (F \times B) \neq \emptyset.$$

Ha $q = e$, akkor $(a_0, b_0) \in F \times B$, azaz $a_0 \in F$, ezért $e \in L$, s így $e = \alpha(e) \in \alpha(L)$. Ha $q = y_1 y_2 \dots y_k$ $(y_1, y_2, \dots, y_k \in Y)$, akkor vannak olyan $(a_i, b_i) \in A \times B$ $(i = 1, 2, \dots k)$ állapotok, hogy $(a_k, b_k) \in F \times B$ és

$$(a_{i+1}, b_{i+1}) \in \delta_C((a_i, b_i), y_{i+1}), \quad i = 0, 1, \dots, k-1,$$

s így (8.7) szerint vannak olyan $x_{i+1} \in X$ bemenő jelek, hogy

$$\delta_A(a_i, x_{i+1}) = a_{i+1}, \quad \delta_B(b_i, x_{i+1}) = b_{i+1}, \quad \lambda_B(b_i, x_{i+1}) = y_{i+1}.$$

Ez azt jelenti, hogy $q = \alpha(p)$, ahol $p = x_1 x_2 \dots x_k \in L$, amiből következik, hogy $q \in \alpha(L)$.

Ezzel megmutattuk, hogy $\alpha(L) = L(\mathbf{C}, F \times B)$. □

Feladatok

8.1. Konstruáljunk meg olyan véges (teljesen definiált determinisztikus) automatát, amely felismeri az $x(x+y)((x+y)^3)^*y-(x+y)^*x^3(x+y)^*$ nyelvet.
8.2. Tegyük fel, hogy az L nyelv felismerhető egy n állapotú véges automatában az állapothalmaz valamely részhalmazával. Az L nyelv akkor és csak akkor véges, ha minden $p \in L$ szó legfeljebb $n-1$ hosszúságú.
8.3. Adjunk felső korlátot arra, hány lépésben dönthető el, hogy egy n állapotú és k bemenő jelű automata állapothalmazának valamely l elemű részhalmazával felismerhető nyelv üres, véges vagy végtelen.
8.4. Legalább kételemű X ábécé esetén az $L = \{pp^{-1}; p \in X^*\}$ nyelv nem reguláris.

9. fejezet

Büchi automaták

Azt mondjuk, hogy a $p \in X^\omega$ végtelen szó egy *kezdőszelete* vagy *prefixe* az $r \in X^*$ szó, ha van olyan $q \in X^\omega$, amelyre $p = rq$. Ha $r \neq e$, akkor r a p szó *valódi kezdőszelete* vagy *valódi prefixe*. Ez a fogalom a véges szavakra definiált fogalom természetes általánosítása.

A $p \in X^\omega$ szó *Büchi szerint előállítható* a nemdeterminisztikus

$$\mathbf{A}_F = (A, A_0, X, \delta; F)$$

automatában, vagy más szóval az $\mathbf{A}_F$ nemdeterminisztikus automata *Büchi szerint felismeri* vagy *elfogadja* a p szót, ha van a p szó prefixeinek olyan $r_1, r_2, \ldots, r_k, \ldots$ sorozata és olyan $a_0 \in A_0$ kezdőállapot, amelyekre

$$0 \leq |r_1| < |r_2| < \cdots < |r_k| < \ldots,$$

$$\{a_0 r_1, a_0 r_2, \ldots, a_0 r_k, \ldots\} \subseteq F,$$

azaz automata a p szó hatására egy kezdőállapotból végtelen sokszor eljut egy végállapotba. Az $\mathbf{A}_F = (A, A_0, X, \delta; F)$ nemdeterminisztikus automatát *Büchi automatá*nak is nevezzük. Az $\mathbf{A}_F$ automatát akkor nevezzük *determinisztikus Büchi automatá*nak, ha determinisztikus és egy kezdőállapota van. Jelölje az $\mathbf{A}_F$ nemdeterminisztikus automatában Büchi szerint felismerhető szavak halmazát, a 7. fejezet jelölésével összhangban, $L_\omega(\mathbf{A}, A_0, F)$ vagy röviden $L_\omega(\mathbf{A})$. Továbbá azt mondjuk, hogy az $L \subseteq X^\omega$ nyelv *Büchi szerint felismerhető* az $\mathbf{A}_F = (A, A_0, X, \delta; F)$ nemdeterminisztikus automatában, vagy az $\mathbf{A}_F$ nem determinisztikus automata *Büchi szerint előállítja* vagy *elfogadja* az L nyelvet, ha $L = L_\omega(\mathbf{A}, A_0, F)$ vagy röviden $L = L_\omega(\mathbf{A})$. Úgy is beszélünk, hogy az L nyelvet az $\mathbf{A} = (A, A_0, X, \delta)$ automata Büchi szerint felismeri (az $F(\subseteq A)$ halmazzal.

A $p \in X^\omega$ végtelen szót *periodikus*nak nevezünk, ha

$$p = rqq \ldots q \ldots \quad (r \in X^*,\ q \in X^+). \tag{9.1}$$

Ha r és q a legkisebb hosszúságú szavak, amelyekre (9.1) teljesül, akkor q hosszát p *periódus*ának nevezzük. Ha $r = e$, akkor p-t *teljesen periodikus*nak mondjuk. Végtelen szavak esetében is beszélhetnénk *primitív végtelen szavak*ról a 12.6. alfejezetben bevezetett fogalom általánosításaként, de erre a fogalomra nem lesz szükségünk.

9.1. Lemma. *Ha a nemüres $K \subseteq X^\omega$ nyelv véges Büchi automatában felismerhető, akkor tartalmaz periodikus szót.*

Bizonyítás Tegyük fel, hogy a nemüres $K \subseteq X^\omega$ nyelv felismerhető a véges $\mathbf{A} = (A, A_0, X, \delta; F)$ Büchi automatában. Ha $p \in K$, akkor van olyan $a_0 \in A_0$, $r \in X^*$ és F végessége miatt vannak olyan $q_i \in X^+$ szavak, amelyekre

$$p = rq_1q_2 \dots q_k \dots, \quad a = a_0r \in F,\ aq_i = a\ (i = 1, 2, \dots, k, \dots).$$

Ebből következik, hogy a $p' = rq_1q_1 \dots q_1 \dots$ szó is eleme K-nak. □

9.2. Példa. *Az*

A	1	2
x	$\{1,2\}$	$\emptyset$
y	$\emptyset$	$\{1,2\}$

Büchi automata az 1 *kezdőállapottal és a* 2 *végállapottal az $L = x(x^*y)^\omega$ nyelvet ismeri fel. Az 1.4 Tétel szerint L ω-reguláris. Az L nyelv végtelen sok periodikus szót tartalmaz. Például*

$$x(xy)(xy) \dots (xy) \dots$$

2 *periódusú szó. (De például az $x(y)(xy)(x^2y) \dots (x^ky) \dots$ nem periodikus.)*

A 7. fejezetben láttuk, hogy a véges szavak felismerésére elegendő teljesen definiált automatákat használni. A következő lemma szerint ez végtelen szavak esetén is így van.

9.3. Lemma. *Ha $K \subseteq X^\omega$ felismerhető egy [véges, determinisztikus] Büchi automatában, akkor felismerhető egy teljesen definiált [véges, determinisztikus] Büchi automatában is.*

Bizonyítás Tegyük fel, hogy a $K \subseteq X^\omega$ nyelv felismerhető az

$$\mathbf{A} = (A, A_0, X, \delta; F)$$

Büchi automatában. Ha $\mathbf{A}$ nem teljesen definiált, akkor vegyünk fel egy $d \notin A$ új állapotot. Terjesszük ki a δ átmenetfüggvény értelmezését az $(A \cup d) \times X$ halmazra a következőképpen. Legyen Minden $x \in X$ bemenő jelre $\delta(d, x) = d$. Ha valamely $a \in A$ és $x \in X$ párra δ nincs értelmezve, akkor legyen $\delta(a, x) = d$. Nyilvánvaló, hogy K felismerhető az $\mathbf{B} = (A \cup d, A_0, X, \delta; F)$ Büchi automatában is. Ha $\mathbf{A}$ véges [determinisztikus], akkor $\mathbf{B}$ is véges [determinisztikus]. □

Megmutatjuk, hogy a végtelen szavakat tartalmazó nyelvekre érvényes Kleene tételének megfelelője. Ehhez azonban szükséges a következő fogalom és lemma. Az $\mathbf{A} = (A, A_0, X, \delta; F)$ automatát *normalizált automatá*nak nevezzük, ha $A_0 = \{a_0\}$, $F = \{d\}$, továbbá nincsenek olyan $a, b \in A$ állapotok és $x, y \in X$ bemenő jelek, amelyekre $\delta(a, x) = a_0$ és $\delta(d, y) = b$ teljesülne.

9.4. Lemma. *Bármely* $\mathbf{A} = (A, A_0, X, \delta; F)$ *véges automatához van olyan* $\mathbf{B} = (B, b, X, \delta'; d)$ *normalizált véges automata, amelyre* $L(\mathbf{A}, F) = L(\mathbf{B}, d)$.

Bizonyítás Tekintsük az $\mathbf{A} = (A, A_0, X, \delta; F)$ véges automatát. Legyenek $b, d \notin A$ új állapotok és $B = A \cup \{b, d\}$. Legyen δ' a δ átmenetfüggvény következő kiterjesztése. Az $A \times X$ halmazon legyen $\delta' = \delta$. Ha $a \in A_0$ és $x \in X$ párra $\delta(a, x) \in F$, akkor legyen $\delta'(b, x) = d$. Ha $a' \in A$ állapothoz van olyan $a \in A_0$ és $x \in X$, hogy $\delta(a, x) = a'$, akkor legyen $\delta'(b, x) = a'$. Végül, ha $a' \in A$ állapotra és $x \in X$ bemenő jelre $\delta(a', x) \in F$, akkor legyen $\delta'(a', x) = d$.

Nyilvánvaló, hogy az így definiált $\mathbf{B} = (B, b, X, \delta'; d)$ automata normalizált. Ezenkívül,

$$ax_1x_2 \dots x_k \in F \quad (a \in A_0, x_1, x_2, \dots, x_k \in X, k \geq 1)$$

akkor és csak akkor, ha $bx_1x_2 \dots x_k = d$, azaz $L(\mathbf{A}, F) = L(\mathbf{B}, d)$. □

Most megmutatjuk Kleene tételének analogonját végtelen szavakból álló nyelvekre.

9.5. Tétel. *Egy* $L \subseteq X^\omega$ *nyelv akkor és csak akkor* ω*-reguláris, ha felismerhető egy véges* $\mathbf{A} = (A, A_0, X, \delta; F)$ *Büchi automatában.*

Bizonyítás Ha $L \subseteq X^\omega$ nyelv felismerhető a véges $\mathbf{A} = (A, A_0, X, \delta; F)$ Büchi automatában, akkor

$$L = \sum_{a \in A_0} \sum_{d \in F} L(\mathbf{A}, a, d)(L(\mathbf{A}, d, d) - e)^\omega.$$

Kleene tétele szerint $L(\mathbf{A}, a, d)$ és $L(\mathbf{A}, d, d) - e$ $(a \in A_0, d \in F)$ reguláris nyelvek X felett, ezért az 1.4 Tétel szerint L ω-reguláris.

A tétel megfordításának bizonyításához először tekintsük a KM^ω alakú ω-reguláris nyelveket, amelyekben $K \subseteq X^*$ és $M \subseteq X^+$ reguláris nyelvek X felett. Ha $K = \emptyset$ vagy $M = \emptyset$, akkor $KM^\omega = \emptyset$ nyilvánvalán felismerhető olyan Büchi automatában, amelyben a végállapotok halmaza üres.

Legyen $K = \{e\}$, $\emptyset \subset M \subseteq X^+$ és $\mathbf{A} = (A, b, X, \delta; d)$ normalizált véges automata, amely felismeri az M nyelvet. Ha azonosítjuk b-t a d állapottal,

akkor olyan Büchi automatát kapunk, amely felismeri az M^ω nyelvet az $b = d$ kezdő és végállapottal.

Legyenek most $\emptyset \subset K, M \subset X^+$, továbbá $\mathbf{A} = (A, b, X, \delta; d)$ és $\mathbf{A}' = (A', b', X, \delta'; d')$ olyan normalizált véges automaták, amelyek felismerik a K ill. M nyelvet. Ha azonosítjuk a b' és d' állapotokat a d állapottal, akkor olyan Büchi automatát kapunk, amely felismeri a KM^ω nyelvet a b kezdőállapottal és a $b' = d' = d$ végállapottal. Ha $\emptyset \subset K', M \subset X^+$és $K = K' + e$, akkor $KM^\omega = K'M^\omega + M^\omega$. Ezt az esetet is magába foglalja a bizonyítás utolsó lépese.

A bizonyítás befejezéséhez ugyanis, az 1.4 Tétel szerint, elegendő megmutatni, hogy két $L, L' \subseteq X^\omega$ ω-reguláris nyelv $L + L'$ összege is ω-reguláris X felett. Tegyük fel, hogy $\mathbf{A} = (A, A_0, X, \delta; F)$ és $\mathbf{A}' = (A', A'_0, X, \delta'; F')$ véges Büchi automaták felismerik az L ill. L' nyelvet. Azt is feltehetjük, hogy $A \cap A' = \emptyset$. Nyilvánvaló, hogy az $L + L'$ nyelvet gaz $\mathbf{A}$ és $\mathbf{A}'$ Büchi automaták direkt összege felismeri a kezdőállapotok $A_0 \cup A'_0$ és végállapotok $F \cup F'$ halmazával. □

A 7.9 Tétel szerint a véges nemdeterminisztikus automatákkal felismerhető nyelvek megegyeznek a véges determinisztikus automatákkal felismerhető nyelvekkel. A véges Büchi automatákkal felismerhető nyelvekre ez azonban nem igaz. A fejezetet a véges determinisztikus Büchi automatákkal felismerhető nyelvek jellemzésével fejezzük be. Ehhez a bevezetünk a véges szavakat tartalmazó nyelvekre egy újabb egyváltozós műveletet.

Tetszőleges $L \subseteq X^*$ esetén legyen $\overrightarrow{L}$ azoknak X^ω-beli végtelen szavaknak a halmaza, amelyeknek végtelen sok L-beli prefixe van.

9.6. Példa. *Legyen $X = \{x, y\}$. Ha $L = x^*y$, akkor $\overrightarrow{L} = \emptyset$. Ha $L = (xy)^+$, akkor $\overrightarrow{L} = (xy)^\omega$. Ha pedig $L = (x^*y)^+ = (x + y)^*y$, azaz L azoknak az X feletti véges szavaknak a halmaza, amelyek y-ra végződnek, akkor $\overrightarrow{L} = (x^*y)^\omega$, vagyis azoknak a végtelen szavaknak a halmaza, amelyek (megszámlálhatóan) végtelen sokszor tartalmazzák y-t.*

9.7. Lemma. *Az $\mathbf{A} = (A, a_0, X, \delta; F)$ Büchi automatára*

$$L_\omega(\mathbf{A}, F) = \overrightarrow{L(\mathbf{A}, F)} - e.$$

Bizonyítás Ha $p \in L_\omega(\mathbf{A}, F)$, akkor van a p szó prefixeinek olyan

$$r_1, r_2, \ldots, r_k, \ldots$$

sorozata, hogy

$$0 \leq |r_1| < |r_2| < \cdots < |r_k| < \ldots,$$

$$\{a_0r_1,\ a_0r_2, \dots, a_0r_k, \dots\} \subseteq F,$$

azaz $r_k \in F$ $(k = 1, 2, \dots)$, vagyis $L_\omega(\mathbf{A}, F) \subseteq \overrightarrow{L(\mathbf{A}, F)} - e$.

Megfordítva, ha $p \in \overrightarrow{L(\mathbf{A}, F)} - e$, akkor p-nek végtelen sok prefixe van a $L(\mathbf{A}, F) - e$ halmazban. Mivel $\mathbf{A}$ determinisztikus, $p \in L_\omega(\mathbf{A}, F)$. □

9.8. Tétel. *Egy $K \subseteq X^\omega$ nyelvre a következő két állítás ekvivalens:*
(1) K felismerhető egy determinisztikus Büchi automatában;
(2) Van olyan $L \subseteq X^+$ nyelv, amelyre $K = \overrightarrow{L}$.
Továbbá, ha X megszámlálható, akkor ezek a feltételek ekvivalensek az alábbi feltétellel:
(3) K felismerhető megszámlálható állapothalmazú determinisztikus Büchi automatában.

Bizonyítás A 9.7 Lemma szerint az (1) feltételből következik (2).

Legyen most $L \subseteq X^+$, amelyre $K = \overrightarrow{L}$. A 7. fejezet elején beszéltünk arról, hogy bármely X feletti L nyelv felismerhető a (3.13) feltétellel definiált (iniciálisan összefüggő) $\mathbf{X}^* = (X^*, e, X, \delta)$ szabad automatában a végállapotok L halmazával, azaz $L = L(X^*)$. A 9.7 Lemma szerint

$$K = \overrightarrow{L} = \overrightarrow{L(X^*)} = L_\omega(X^*).$$

Így a (2) feltételből következik (1).

Ha X megszámlálható, akkor a $\mathbf{X}^*$ szabad automata megszámlálható állapothalmazú. Ebben az esetben a (2) feltételből következik (3). Mivel a (3) feltételből nyilvánvalóan következik (1), ezért ekkor a három feltétel ekvivalens. □

9.9. Következmény. *Egy $K \subseteq X^\omega$ nyelv akkor és csak akkor ismerhető fel egy véges determinisztikus Büchi automatával, ha van olyan $L \subseteq X^+$ reguláris nyelv, amelyre $K = \overrightarrow{L}$.*

Bizonyítás A 9.7 Lemma bizonyítása szerint, ha K felismerhető véges determinisztikus Büchi automatával, akkor L reguláris X felett. Megfordítva, ha van olyan $L \subseteq X^+$ reguláris nyelv, amelyre $K = \overrightarrow{L}$, akkor L felismerésére választható egy véges determinisztikus automata. A 9.8 Tétel bizonyításában a szabad automata helyett ezt az automatát használva, kapjuk, hogy K felismerhető véges determinisztikus Büchi automatával. □

Most példát adunk arra, hogy nem minden $K \subseteq X^\omega$ nyelvhez van olyan $L \subseteq X^+$ nyelv, amelyre $K = \overrightarrow{L}$. A 9.8 Tétel szerint ez azt jelenti, hogy a véges determinisztikus Büchi automatákkal felismerhető nyelvek halmaza valódi része véges Büchi automatákkal felismerhető nyelvek halmazának.

9.10. Példa. *Legyen K azoknak az $X = \{x, y\}$ ábécé feletti végtelen szavaknak a halmaza, amelyekben y véges sokszor fordul elő, azaz $K = (x + y)^* x^\omega$.*

Az

A	1	2
x	1	2
y	$\{1, 2\}$	$\emptyset$

Büchi automata az 1 és 2 kezdőállapotokkal és a 2 végállapottal a K nyelvet ismeri fel.

Tegyük fel, hogy K megadható $K = \overrightarrow{L}$ alakban, ahol $L \subseteq X^+$. Akkor például az $yx^\omega \in K$ végtelen szónak van yx^{k_1} alakú L-beli prefixe. Az $yx^{k_1}yx^\omega$ K-beli szónak van $yx^{k_1}yx^{k_2}$ alakú L-beli prefixe. Ezt folytatva kapjuk, hogy K-ban van olyan szó, amelyben végtelen sokszor előfordul y. Ez azonban lehetetlen, ezért K nem adható meg $K = \overrightarrow{L}$ alakban, ahol $L \subseteq X^+$.

Determinisztikus Büchi automatában felismerhető nyelveket *determinisztikus nyelvek*nek is nevezzük. A 9.8 Tétel alapján a 9.6 és a 9.10 Példákból látható, hogy determinisztikus nyelv komplementere nem mindig determinisztikus. Ha $L_1, L_2 \subseteq X^+$, akkor

$$\overrightarrow{L_1 + L_2} = \overrightarrow{L_1} + \overrightarrow{L_2}.$$

A 9.8 Tétel szerint ez azt jelenti, hogy determinisztikus nyelvek összege determinisztikus. Megmutatható az is, hogy determinisztikus nyelvek metszete szintén determinisztikus. (Ezzel kapcsolatban ismét Dominique Perrin és Jean-Éric Pin [36] munkájára utalunk.)

10. fejezet

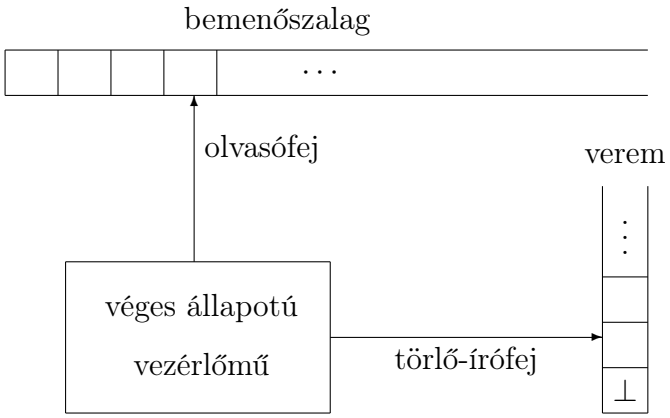
Veremautomaták

Kleene tétele szerint a reguláris nyelvek megegyeznek a véges automatákban felismerhető nyelvekkel. Ebben a fejezetben megadjuk azokat az automatákat, az ún. *veremautomaták*at, amelyek a környezetfüggetlen nyelveket ismerik fel.

10.1. A veremautomata fogalma

A veremautomaták működését szemléletesen például a következőképpen képzelhetjük el. Egy veremautomata egy cellákra osztott (potenciálisan jobbról végtelen) bemenő szalagból, egy véges vezérlő egységből (belső memóriából) és egy *verem*ből (végtelen külső memóriából) áll, amely lehet egyik irányból potenciálisan végtelen szalag, amely cellákra van felosztva és minden cellában a veremábécé egy betűje állhat. A bemenő szalagra a véges számú bemenő jelből álló bemenő szó van írva, az első cellától kezdve cellánként egy betű, amelyet egy balról jobbra mozgó olvasófej segítségével olvas el a vezérlő egység. A verem végtelen irányából első nemüres celláját a *verem tetejé*nek, az utolsó celláját pedig a *verem aljá*nak nevezzük. Ebben a memóriában a beérkező információk érkezésük sorrendjében őrződnek meg, és az automata bármely pillanatban csak a verem tetejéhez tud hozzáférni. Ezt az elemet egy törlő-írófejjel törölhetjük a memóriából, és a helyébe új megőrzendő információ írhatunk. Ezek után az új információnak is csak a legfelső eleméhez férhetünk hozzá. A memória ilyen elrendezését *veremszerű elrendezés*nek nevezzük. Ez egy olyan tárolási módot jelent, hogy az adatok törlése a bevitelükhöz sorrendjéhez képest fordítva történik.

A veremautomata bekapcsoláskor egy rögzített belső állapotba (kezdőállapotba) kerül. A verem üres, ami azt jelenti, hogy az aljára egy rögzített jel (*kezdő jel*) van felírva a veremábécéből. (Ez jelzi a verem alját.) A kezdő jel nem törölhető. A veremautomata is diszkrét lépésekben, ütemekben dolgozik.



10.1. ábra.

A vezérlő egység egy-egy lépésben az alábbi lehetőségek között választhat:
1. Leolvassa a veremmemória legfelső elemét, valamint a bemenő szó soron következő betűjét, és ezektől, valamint a saját belső állapotától függően kiválasztja a következő állapotot, s dönt arról, hogy milyen szót írjon, esetleg az üres szót is, a veremmemóriába, a beolvasott (törölt) legfelső jel helyébe. Ezután a vezérlő egység felkészül a következő bemenő jel leolvasására.
2. A belső állapotától és a veremmemória legfelső jelétől függően a vezérlő egység kiválasztja a következő állapotot, valamint a veremmemóriából beolvasott jel helyébe írandó szót. Eközben a vezérlő egység nem olvas bemenő jelet, s nem lép tovább a bemenő szalagon. Az ilyen lépéseket az automata a bemenő szó utolsó betűjének beolvasása után is megteheti. Ez a lépés azt teszi lehetővé, hogy az automata az aktuális bemenő jeltől függetlenül, mintegy autonóm üzemmódban megváltoztassa működését.

A veremautomata megáll a működésével, ha a vezérlő egységnek nincs utasítása arra, hogy mit lépjen, vagy ha a verem teljesen kiürül. Abban az esetben, ha a veremautomatának minden helyzetben van előírt lépése, csak akkor áll le a működésével, amikor beolvasta az utolsó bemenő jelet is, és ezután megtette összes lehetséges lépését.

Látható, hogy veremautomaták is, mint a kimenő jel nélküli automaták szekvenciális működésű gépek. A veremautomatának egy adott szó hatására történő müködésékor kétféle dologra figyelhetünk. Egyrészt arra, hogy van-e olyan sorozata a lehetséges átmeneteknek, amelynek során az automata valamilyen előre rögzített végállapotba kerül. Másrészt arra, hogy van-e olyan működése, amely során a bemenő szó hatására a verem kiürül. Az első esetben

azt mondjuk, hogy a veremautomata végállapotával ismerte fel az adott bemenő szót, a második esetben pedig üres veremmel. Most az előbbi szemléletes fogalmak absztrakciójaként megadjuk a veremautomaták és a veremautomaták által felismerhető nyelvek fogalmát.

Az $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \perp)$ rendszert *veremautomatá*nak vagy *pushdown automatá*nak nevezzük, ahol az $A \neq \emptyset$ véges halmaz az *állapothalmaz*, $a_0 (\in A)$ a *kezdőállapot* , az $X (\neq \emptyset)$ véges halmaz a *bemenő halmaz* vagy *bemenő ábécé*, $\Gamma (\neq \emptyset)$ a *veremábécé*, a $\perp (\in \Gamma)$ a *kezdő jel*, a

$$\delta : A \times (X \cup e) \times \Gamma \to P(A \times \Gamma^*)$$

(parciális) függvény az *átmenet-* vagy *mozgásfüggvény* a következő feltételeket kielégítő függvény:

$$(b, P) \in \delta(a, x, \perp) \quad \Longrightarrow \quad P \in (\Gamma - \perp)^* \perp, \tag{10.1}$$

$$((b, P) \in \delta(a, x, Z), \quad Z \neq \perp) \quad \Longrightarrow \quad P \in (\Gamma - \perp)^*. \tag{10.2}$$

Az $\mathbf{A}$ veremautomatát *determinisztikus*nak mondjuk, ha minden $a \in A, Z \in \Gamma$ és $x \in X \cup e$ esetén

$$|\delta(a, x, Z)| \leq 1$$

Egy $\mathbf{A} = (A, a_0, X, \delta)$ véges automatát tekinthetünk egy

$$\mathbf{A}' = (A, a_0, X, \delta', \{\perp\}, \perp)$$

veremautomataként, ahol minden $a \in A$ és $x \in X \cup e$ esetén $\delta'(a, x, \perp) = \delta(a, x)$.

A veremautomatáknál is kijelölhetjük a *végállapotok* $F (\subseteq A)$ halmazát. Ebben az esetben a véges automatákhoz hasonlóan az

$$\mathbf{A}_F = (A, a_0, X, \delta, \Gamma, \perp; F)$$

jelölést is használjuk.

A veremautomata definíciójából látható, hogy az $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \perp)$ veremautomata (6.6) szerint felfogható egy (parciális) nemdeterminisztikus

$$(A \times \Gamma^*, (a_0, \perp), X, \delta)$$

kimenő jel nélküli automataként, azzal a kiegészítéssel, hogy akkor is megváltozhat az automata állapota, ha nem kap bemenő jelet. Mivel $\Gamma \neq \emptyset$, ezért ez a kimenő jel nélküli automata végtelen.

Mint azt már mondtuk, az $\mathbf{A}$ veremautomata működésének kezdetén az a_0 kezdő állapotban van, és a verem alján a $\perp$ kezdőjel áll, többi cella pedig

üres, azaz a verem üres. Ha pedig **A** működésének valamelyik időpillanatában (lépésében) az automata az $a \in A$ állapotban van, az olvasófej a bemenő szalag olyan cellájára mutat, amelyben az $x \in X \cup e$ jel áll és a verem tetején a Z jel található, akkor **A** működése a következő lehetőségek valamelyike szerint folytatódhat:
1. Ha $\delta(a, x, Z) = \emptyset$, akkor **A** nem működik tovább.
2. Ha $\delta(a, x, Z) \neq \emptyset$ és $x \neq e$, akkor olvasófej eggyel jobbra lép, az automata átmegy egy b állapotba, a törlő-írófej pedig törli a verem tetején álló Z jelet és helyébe egy P szót ír, amelyekre $(b, P) \in \delta(a, x, Z)$.
3. Ha $\delta(a, e, Z) \neq \emptyset$, akkor az olvasófej nem mozdul el, **A** egy b állapotba kerül, ugyanakkor a törlő-írófej a verem tetején lévő Z jel helyébe egy P szót ír, amelyekre $(b, P) \in \delta(a, e, Z)$.

10.2. Nyelvek felismerése veremautomatákban

Ha az **A** veremautomata az $a \in A$ állapotban van, a bemenő szalagon az rp $(r, p \in X^*)$ szó, az olvasófej r utolsó betűjét tartalmazó cella után következő cellára mutat, a veremben pedig a $P \in (\Gamma - \perp)^* \perp$ szó áll, akkor azt mondjuk, hogy **A** a $[a, p, P]$ *konfiguráció*ban van. Az $[a, e, P]$ konfiguráció ezek szerint azt jelenti, hogy az automata az a állapotban van, a bemenő szalagon az r szó áll, az olvasófej r utolsó betűjét tartalmazó cella utáni első üres cellára mutat, a veremben pedig a $P \in (\Gamma - \perp)^* \perp$ szó áll.

Akkor mondjuk, hogy a $[b, p, QP]$ konfiguráció *közvetlenül levezethető* az $[a, xp, ZP]$ konfigurációból, jelekben

$$[a, xp, ZP] \quad \Longrightarrow_{\mathbf{A}} \quad [b, p, QP], \tag{10.3}$$

ahol $a, b \in A, x \in X \cup e,\ p \in X^*,\ Z \in \Gamma,\ P, Q \in \Gamma^*$, ha

$$(b, Q) \in \delta(a, x, Z),$$

ahol Z a verem tetején áll. az $[a, xp, ZP]$ konfigurációból, jelekben Ez azt jelenti, hogy ha $Z \in \Gamma$ a verem tetején áll és $(b, Q) \in \delta(a, e, Z)$, akkor

$$[a, p, ZP] \quad \Longrightarrow_{\mathbf{A}} [b, p, QP]. \tag{10.4}$$

A (10.3) közvetlen levezetés $x \neq e$ esetben azt jelenti, hogy **A** az a állapotban van, az olvasófej az x bemenő jelre mutat és a verem tetején a Z jel áll. Egy időpillanat elteltével az automata átmegy a b állapotba, az olvasófej a p szó első betűjét tartalmazó cellára ugrik, a törlő-írófej törli a veremből Z-t és a P szó fölé a Q szót irja. (Ha $p = e$, akkor természetesen az olvasófej az x bemenő jel utáni első üres cellára ugrik.)

Az $x = e$ eset, azaz a (10.4) közvetlen levezetés, csak annyiban különbözik az előző esettől, hogy az olvasófej nem mozdul el az üres celláról.

Egy $[b, q, Q]$ konfigurációt *levezethető*nek nevezünk az $\mathbf{A}$ veremautomatában az $[a, p, P]$ konfigurációból, jelekben

$$[a, p, P] \quad \Longrightarrow_{\mathbf{A}}^{+} \quad [b, q, Q], \quad a, b \in A,\ p, q \in X^*,\ P, Q \in \Gamma^*, \tag{10.5}$$

ha létezik $\mathbf{A}$ konfigurációinak olyan $\Psi_0, \Psi_1, \ldots, \Psi_k$ sorozata, hogy

$$\Psi_0 = [a, p, P], \quad \Psi_k = [b, q, Q], \quad \Psi_j \quad \Longrightarrow_{\mathbf{A}} \quad \Psi_{j+1},\ j = 0, 1, \ldots, k-1,$$

és legyen $\Longrightarrow_{\mathbf{A}}^{*}$ a $\Longrightarrow_{\mathbf{A}}$ binér reláció reflexív és tranzitív lezártja. Ezen relációk jelölésére, ha nem vezet félreértésre, röviden a $\Longrightarrow$ ill. $\Longrightarrow^*$ jeleket használjuk. Jelölje $\Longrightarrow^+$ a $\Longrightarrow$ reláció tranzitív lezártját, azaz $1 \leq k$.

Azt mondjuk, hogy az X feletti L nyelv *felismerhető az*

$$\mathbf{A} = (A, a_0, X, \delta, \Gamma, \bot)$$

veremautomatában az állapotok F halmazával, vagy más szóval az $\mathbf{A}$ automata *előállítja* vagy *elfogadja* az L nyelvet az F halmazzal, ha

$$L = \{p \in X^*; \quad [a_0, p, \bot] \ \Longrightarrow_{\mathbf{A}}^{+} \ [b, e, Q],\ b \in F,\ Q \in (\Gamma - \bot)^* \bot\} \tag{10.6}$$

Ebben az esetben is az $L = L(\mathbf{A}, F)$ jelölést használjuk. Az F halmaz elemeit veremautomaták esetében is *végállapotok*nak hívjuk. Továbbá azt mondjuk, hogy L $\mathbf{A}$-ban *üres veremmel ismerhető fel* vagy *állítható elő*, más szóval $\mathbf{A}$ *üres veremmel felismeri*, *előállítja* vagy *elfogadja* az L nyelvet, ha

$$L = \{p \in X^*; \quad [a_0, p, \bot] \ \Longrightarrow_{\mathbf{A}}^{+} \ [a, e, \bot],\ a \in A\} \tag{10.7}$$

Erre az $L = L(\mathbf{A})$ jelölést fogjuk használni. A definícióból nyilvánvalóan következik, hogy $e \in L$ akkor és csak akkor, ha $\delta(a_0, e, \bot) \neq \emptyset$.

10.1. Példa. *Az $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \bot)$ veremautomatát, amelyre*

$$A = \{a_0, a\},\ X = \{x, y, z\},\ \Gamma = \{\bot, V, W\},$$

az alábbi három átmenettáblázattal adjuk meg:

		a_0	a
$\bot$	e	$\emptyset$	$\emptyset$
	x	$(a_0, V\,\bot)$	$\emptyset$
	y	$(a_0, W\,\bot)$	$\emptyset$
	z	$(a, \bot)$	$\emptyset$

		a_0	a
V	e	$\emptyset$	$\emptyset$
	x	(a_0, VV)	$(a, \bot)$
	y	(a_0, WV)	$\emptyset$
	z	(a, V)	$\emptyset$

		a_0	a
W	e	$\emptyset$	$\emptyset$
	x	(a_0, VW)	$\emptyset$
	y	(a_0, WW)	$(a, \bot)$
	z	(a, W)	$\emptyset$

A táblázatok első oszlopában a verem tetején lévő jelet tüntettük fel. Eszerint a második táblázatból leolvasható például, hogy ha $\mathbf{A}$ *az* a_0 *kezdő állapotban van, a verem tetején a* V *jel áll és az olvasófej a bemenő szó egy* y *betűjére mutat, akkor az automata a kezdő állapotban marad, de a verem tetején lévő* V *jel helyére a* WV *szó kerül úgy, hogy a verem tetején a* W *jel áll. Megmutatjuk, hogy* $L(\mathbf{A}) = \{pzp^{-1}; p \in \{x, y\}^*\}$*, ahol* p^{-1} *a* p *tükörképe.*

Mivel $\delta(a_0, e, \bot) = \emptyset$, ezért az $[a_0, e, \bot]$ konfigurációból nem vezethető le egyetlen $[a, e, \bot]$ konfiguráció sem, így $e \notin L(\mathbf{A})$. A táblázatokból látható, hogy ha egy $p \in X^+$ szó nem tartalmaz z betűt, akkor p leolvasásakor az automata az a_0 kezdő állapotban marad és a verem tartalma $|p|$ számú jellel megnövekszik, ezért nem ürül ki a verem, azaz az ilyen szavak nem lehetnek $L(\mathbf{A})$ elemei. Ha p tartalmaz z betűt, akkor az $\mathbf{A}$ automata p leolvasásakor, ha az olvasófej eléri az első z betűt, átkerül az a állapotba és a leolvasás végéig ott is marad. Ha még egy z betű volna p-ben, akkor az automata leállna, s így ebben az esetben sem ürülne ki a verem, vagyis az ilyen p szavak sem lehetnek $L(\mathbf{A})$ elemei. Legyenek $p, q \in \{x, y\}^*$, akkor (10.3) és (10.5) szerint

$$[a_0, pzq, \bot] \quad \Longrightarrow_{\mathbf{A}}^* \quad [a_0, zq, P\ \bot] \quad \Longrightarrow_{\mathbf{A}} \quad (a, q, P\ \bot),$$

ahol $P \in (\Gamma - \bot)^*$ a p szóból úgy kapható meg, hogy mindenütt x-et V-vel, y-t pedig W-vel helyettesítjük. (Természetesen, ha $p = e$, akkor $P = \bot$.) Ha $q \neq p^{-1}$, akkor a q szó leolvasása közben $\mathbf{A}$ leállna, azaz nem ürülne ki a verem, vagyis $pzq \notin L(\mathbf{A})$. Ha $q = p^{-1}$, akkor (10.4)-et is felhasználva kapjuk, hogy

$$[a, q, P\ \bot] \quad \Longrightarrow^* \quad [a, e, \bot].$$

Ezzel megmutattuk, hogy $L(\mathbf{A})$ pontosan a pzp^{-1} ($p \in \{x, y\}^*$) szavakat tartalmazza.

Gyakorlásképpen nézzük meg az z és x^2yzyx^2 szavak levezetését:

$$[a_0, z, \bot] \Longrightarrow_{\mathbf{A}} [a, e, \bot].$$

$$[a_0, x^2yzyx^2, \bot] \Longrightarrow [a_0, xyzyx^2, V\ \bot] \Longrightarrow [a_0, yzyx^2, VV\ \bot] \Longrightarrow$$
$$\Longrightarrow [a_0, zyx^2, WVV\ \bot] \Longrightarrow [a, yx^2, WVV\ \bot] \Longrightarrow$$
$$\Longrightarrow [a, x^2, VV\ \bot] \Longrightarrow [a, x, V\ \bot] \Longrightarrow [a, e, \bot].$$

10.3. Nyelvek felismerése üres veremmel

10.2. Tétel. *Egy nyelv akkor és csak akkor ismerhető fel veremautomatában az állapothalmaz valamely részhalmazával, ha felismerhető veremautomatában üres veremmel.*

Bizonyítás Először tegyük fel, hogy egy X ábécé feletti L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \perp)$ veremautomatában üres veremmel, azaz $L = L(\mathbf{A})$. Legyenek $a_0', a_v \notin A$ $(a_0' \neq a_v), \perp' \notin \Gamma$, továbbá $A' = A \cup \{a_0', a_v\}$ és $\Gamma' = \Gamma \cup \perp'$. Definiáljuk az $\mathbf{A}' = (A', a_0', X, \delta', \Gamma', \perp')$ veremautomatát úgy, hogy a δ' teljesítse a következő feltételeket:

$$\delta'(a_0', e, \perp') = (a_0, \perp\perp'); \tag{10.8}$$

$$\delta'(a, x, Z) = \delta(a, x, Z), \quad a \in A, Z \in \Gamma, x \in X \cup e; \tag{10.9}$$

$$\delta'(a, e, \perp') = (a_v, \perp'), \quad a \in A. \tag{10.10}$$

Megmutatjuk, hogy az $\mathbf{A}'$ veremautomata az a_v állapottal felismeri L-et. Ha $p \in L$, akkor (10.7) szerint van olyan $c \in A$, hogy

$$[a_0, p, \perp] \implies_{\mathbf{A}}^{+} [c, e, \perp]. \tag{10.11}$$

A következő levezetésben először (10.8)-at, majd (10.9) alapján a (10.11) levezetés lépéseit, végül (10.10)-et alkalmazzuk:

$$[a_0', p, \perp'] \implies_{\mathbf{A}'} [a_0, p, \perp\perp'] \implies_{\mathbf{A}'}^{*} [c, e, \perp'] \implies_{\mathbf{A}'} [a_v, e, \perp'].$$

Ezért (10.4) szerint $p \in L(\mathbf{A}', a_v)$. Ezzel megmutattuk, hogy $L \subseteq L(\mathbf{A}', a_v)$

Legyen most $p \in L(\mathbf{A}', a_v)$, azaz (10.6) szerint van olyan $Q \in (\Gamma' - \perp')^* \perp'$

$$[a_0', p, \perp'] \implies_{\mathbf{A}'}^{*} [a_v, e, Q]. \tag{10.12}$$

Nyilvánvaló, hogy a (10.12) levezetésben az első lépés (10.8) miatt csak

$$[a_0', p, \perp'] \implies_{\mathbf{A}'} [a_0, p, \perp\perp']$$

lehet. Másrészt, $\perp'$ csak a verem alján állhat. Az a_v állapot azonban csak olyankor léphet fel, ha előzőleg a verem tetején $\perp'$ állt. Ezért $Q = \perp'$, ami éppen azt jelenti, hogy létezik egy $b \in A$, amelyre

$$[a_0, p, \perp] \implies_{\mathbf{A}}^{*} [b, e, \perp].$$

Kaptuk, hogy $p \in L$, vagyis $L(\mathbf{A}', a_v) \subseteq L$, s így $L = L(\mathbf{A}', a_v)$.

Másodszor tegyük fel, hogy egy X ábécé feletti L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \bot)$ veremautomatában az A állapothalmaz F részhalmazával, azaz $L = L(\mathbf{A}, F)$. A bizonyítás első részében tekintett $\mathbf{A}'$ veremautomata δ' átmenetfüggvényét adjuk meg most a következő módon. A (10.8) feltétel teljesüljön most is. A (10.9) feltételt módosítsuk úgy, hogy akkor és csak akkor teljesüljön, ha $a \notin F$ vagy $x \neq e$. Legyen továbbá

$$\delta'(a, e, Z) = \delta(a, e, Z) \cup (a_v, \bot'), \quad a \in F, Z \in \Gamma; \tag{10.13}$$

$$\delta'(a_v, e, Z) = (a_v, \bot'), \quad Z \in \Gamma \cup \bot' \,. \tag{10.14}$$

Megmutatjuk, hogy az $\mathbf{A}'$ veremautomata üres veremmel felismeri L-et. Ha $p \in L$, akkor (43.6) szerint van olyan $b \in F$ és $Q \in (\Gamma - \bot)^* \bot$, amelyekre

$$[a_0, p, \bot] \implies^*_{\mathbf{A}} [b, e, Q] \tag{10.15}$$

teljesül. Ha $Q = Z_1 Z_2 \dots Z_k \bot \;\; (Z_j \in \Gamma - \bot, j = 1, 2, \dots, k)$, akkor először (10.8)-at, majd (10.13) alapján a (10.15) levezetés lépéseit, azután (10.14)-et alkalmazva kapjuk az alábbi levezetést:

$$[a_0', p, \bot'] \implies_{\mathbf{A}'} [a_0, p, \bot\bot'] \implies^*_{\mathbf{A}'} [b, e, Q\,\bot'] \implies_{\mathbf{A}'}$$

$$\implies_{\mathbf{A}'} [a_v, e, Z_2 \dots Z_k\,\bot'] \implies^*_{\mathbf{A}'} [a_v, e, \bot'],$$

azaz $p \in L(\mathbf{A}')$. Ezzel megmutattuk, hogy $L \subseteq L(\mathbf{A}')$.

Megfordítva, ha $p \in L(\mathbf{A}')$, akkor (10.7) és (10.13) szerint létezik a

$$[a_0', p, \bot'] \implies^*_{\mathbf{A}'} [a, e, \bot'] \implies_{\mathbf{A}'} [a_v, e, \bot'] \; (a \in A')$$

levezetés. az első lépés (10.8) miatt most is csak

$$[a_0', p, \bot'] \implies_{\mathbf{A}'} [a_0, p, \bot\bot']$$

lehet, azaz a

$$[a_0, p, \bot\bot'] \implies^*_{\mathbf{A}'} [a_v, e, \bot']$$

levezetés létezik. Az a_v állapotba, (10.13) és (10.14) szerint, viszont egy $b \in F$ állapotból juthatunk. Tehát

$$[a_0, p, \bot\bot'] \implies^*_{\mathbf{A}'} [b, e, Q\,\bot']$$

fennáll valamely $b \in F$ és $Q \in (\Gamma - \bot)^* \bot$ elemre. Ez viszont úgy lehetséges, hogy

$$[a_0, p, \bot] \implies^*_{\mathbf{A}} [b, e, Q]$$

is fennáll. Kaptuk, hogy $p \in L$, azaz $L(\mathbf{A}') \subseteq L$, s így $L = L(\mathbf{A}')$. □

10.4. A veremautomaták és a környezetfüggetlen nyelvek

A 10.2 Tétel értelmében a továbbiakban beszélhetünk egyszerűen a *veremautomatákkal felismerhető* vagy *előállítható nyelvek*ről, függetlenül attól, hogy végállapotok halmazával vagy üres veremmel ismerjük fel a nyelvet az automatában. Megmutatjuk, hogy a veremautomatákkal felismerhető nyelvek pontosan a környezetfüggetlen nyelvek.

10.3. Tétel. *Egy nyelv akkor és csak akkor környezetfüggetlen, ha felismerhető veremautomatában.*

Bizonyítás A szükségesség kimutatása céljából legyen L olyan környezetfüggetlen nyelv, amely generálható a $G = (V_N, V_T, S, H)$ 2 típusú grammatikával. A 2.3 és a 2.9 Lemma, valamint a 3.12 Tétel szerint feltehető, hogy G standard alakú, láncszabálymentes és redukált. Tekintsük azt az $\mathbf{A} = (\{a\}, a, V_T, \delta, V_N \cup V_T, S)$ veremautomatát, amelynek δ mozgásfüggvényét definiáljuk úgy, hogy legyen tetszőleges $X \in V_N$ változó esetén

$$\delta(a, e, X) = \{(a, Q^{-1}S); X \longrightarrow Q \in H\}, \tag{10.16}$$

és tetszőleges $x \in V_T$ terminális esetén pedig

$$\delta(a, x, x) = (a, S). \tag{10.17}$$

Minden más esetben legyen a δ értéke $\emptyset$. Megmutatjuk, hogy L felismerhető üres veremmel az $\mathbf{A}$ verem automatában. Ehhez elegendő azt igazolni, hogy minden $X \in V_N$ és $p \in V_T^*$ esetén

$$(X \Longrightarrow_G^* p) \quad \Longleftrightarrow \quad ([a, p, X] \Longrightarrow_{\mathbf{A}}^* [a, e, S]), \tag{10.18}$$

ugyanis ez $X = S$ esetben éppen állításunkat igazolja. Az $X \Longrightarrow_G^* p$ levezetések n hossza szerinti teljes indukcióval igazoljuk, hogy

$$(X \Longrightarrow_G^* p) \quad \Longrightarrow \quad ([a, p, X] \Longrightarrow_{\mathbf{A}}^* [a, e, S]). \tag{10.19}$$

A 3.14 Lemma szerint elegendő bal oldali levezetésekre szorítkozni. Legyen $p \in V_T^*$. Ha $n = 1$, akkor $X \longrightarrow p$ H-beli szabály. De G standard alakú, ezért $p \in V_T \cup e$. Így (10.16)-ot és $p \neq e$ esetben (10.17)-et alkalmazva kapjuk, hogy

$$[a, p, X] \Longrightarrow_{\mathbf{A}} [a, p, p] \Longrightarrow_{\mathbf{A}} [a, e, S].$$

Tegyük fel, hogy minden legfeljebb $n \geq 1$ hosszúságú $X \Longrightarrow_G^* p$ bal oldali levezetésre igaz (10.18). Legyen $X \Longrightarrow_G^* p$ $n+1$ hosszúságú bal oldali levezetés.

Akkor vannak olyan $X_j \in V_N$, $p_j \in V_T^*$ és legfeljebb n hosszúságú $X_j \Longrightarrow_G^* p_j$ $(j = 1, 2, \dots k)$ bal oldali levezetések, amelyekre

$$X \Longrightarrow_G X_1X_2 \dots X_k \Longrightarrow_G^* p_1p_2 \dots p_k = p.$$

Az indukciós feltevés miatt minden $X_j \Longrightarrow_G^* p_j$ levezetésre teljesül (10.18). Innen kapjuk, hogy

$$[a, p, X] = [a, p_1p_2 \dots p_k, X] \Longrightarrow_{\mathbf{A}} [a, p_1p_2 \dots p_k, X_k \dots X_2X_1] \Longrightarrow_{\mathbf{A}}$$

$$\Longrightarrow_{\mathbf{A}} [a, p_1p_2 \dots p_k, X_k \dots X_2p_1^{-1}] \Longrightarrow_{\mathbf{A}}^* [a, p_2 \dots p_k, X_k \dots X_2] \Longrightarrow_{\mathbf{A}}^* \cdots$$

$$\Longrightarrow_{\mathbf{A}}^* [a, p_k, X_k] \Longrightarrow_{\mathbf{A}} [a, p_k, p_k^{-1}] \Longrightarrow_{\mathbf{A}}^* [a, e, e].$$

Megfordítva, a (10.15) típusú átmenet száma szerinti teljes indukcióval megmutatjuk, hogy

$$([a, p, X] \Longrightarrow_{\mathbf{A}}^* [a, e, e]) \quad \Longrightarrow \quad (X \Longrightarrow_G^* p). \tag{10.20}$$

Legyen $p \in V_T^*$. Ha $n = 1$

$$[a, p, X] \Longrightarrow_{\mathbf{A}} [a, p, p^{-1}] \Longrightarrow_{\mathbf{A}}^* [a, e, e],$$

amiből következik, hogy $X \to p \in H$, azaz $X \Longrightarrow_G^* p$. (Természetesen ebből az is adódik, hogy $p \in X \cup e$.)

Tegyük fel, hogy, ha legfeljebb $n \geq 1$ (10.15) típusú átmenet segítségével hajtható végre az $[a, p, X] \Longrightarrow_{\mathbf{A}}^* [a, e, e]$ levezetés, akkor (10.19) igaz. Legyen $[a, p, X] \Longrightarrow_{\mathbf{A}}^* [a, e, e]$ levezetés $n + 1$ (10.15) típusú átmenet segítségével végrehajtható. Akkor

$$\delta(a, X, e) = \{(a, Q^{-1}); X \to Q \in H\} \neq \emptyset,$$

mert különben nem létezne ez a levezetés. Ezért van $X \to Q$ alakú H-beli szabály. Mivel G standard alakú, ezért $Q \in V_T \cup e$ vagy $Q \in V_N^*$. Ha $Q \in V_T \cup e$, akkor

$$[a, p, X] \Longrightarrow_{\mathbf{A}} [a, p, Q] \Longrightarrow_{\mathbf{A}}^* [a, e, e],$$

ami azonban csak úgy lehetséges, ha $Q = p^{-1} = p$. Ez azonban lehetetlen, mivel a levezetés $n + 1 \geq 2$ (10.15) típusú átmenet segítségével hajtható végre. Minthogy G láncszabálymentes, ezért $Q = X_1X_2 \dots X_k$, ahol $X_j \in V_N$ $(j = 1, 2, \dots, k)$ és $1 < k \leq n + 1$.

$$[a, p, X] = [a, p, X_k \dots X_2X_1] \Longrightarrow_{\mathbf{A}} [a, e, e].$$

Ez azt jelenti, hogy p felírható $p = p_1p_2 \dots p_k$ $(p_j \in V_T^*)$ alakban, ahol

$$[a, p_j, X_j] \Longrightarrow_{\mathbf{A}}^* [a, e, e], \quad j = 1, 2, \dots, k$$

levezetések legfeljebb n (10.15) típusú átmenet segítségével hajthatók végre. Az indukciós feltevés miatt léteznek az

$$X_j \Longrightarrow_G^* p_j, \quad j = 1, 2, \ldots, k$$

levezetések. Ebből kapjuk, hogy

$$X \Longrightarrow_G X_1X_2 \ldots X_k \Longrightarrow_G^* p_1X_2 \ldots X_k \Longrightarrow_G^* \cdots \Longrightarrow_G^* p_1p_2 \ldots p_k = p,$$

azaz $X \Longrightarrow_G^* p$. Ezzel megmutattuk, hogy minden környezetfüggetlen nyelv felismerhető egyállapotú veremautomatában üres veremmel.

Most megmutatjuk, hogy minden veremautomatában felismerhető nyelv környezetfüggetlen. Legyen $\mathbf{A} = (A, a_0, X, \delta, \Gamma, \perp)$ tetszőleges veremautomata. A 10.2 Tétel szerint feltehető, hogy az L nyelvet az automata az üres veremmel ismeri fel, azaz $L = L(\mathbf{A})$. Legyen továbbá $S \notin A \cup X \cup \Gamma$ és $V_N = (A \times \Gamma \times A) \cup S$. Definiáljuk a $G = (V_N, X, S, H)$ 2 típusú grammatikát úgy, hogy a H-beli szabályok a következő alakúak:

$$S \to (a, \perp, a_0), \quad a \in A; \tag{10.21}$$

$$(b_0, Z, b) \to (b_0, Z_1, b_1)(b_1, Z_2, b_2) \ldots (b_{k-1}, Z_k, b_k)x, \quad b \in A,\ Z \in \Gamma, \tag{10.22}$$

ahol $b_0, b_1, \ldots b_k \in A,\ Z_1, \ldots Z_k \in \Gamma, k \geq 1, x \in X \cup e$ és $(b_k, Z_1Z_2 \ldots Z_k) \in \delta(b, Z, x)$;

$$(b_0, Z, b) \to x, \quad b \in A,\ Z \in \Gamma, \tag{10.23}$$

ha $b_0 \in A,\ x \in X \cup e$ és $(b_0, e) \in \delta(b, Z, x)$ Megmutatjuk, hogy $L^{-1} = L(G)$, azaz L^{-1} nyelv környezetfüggetlen. A 2.8 Tétel szerint ebből már következik, hogy L is környezetfüggetlen. Elegendő megmutatni, hogy minden $b, c \in A$ és $Z \in \Gamma$ esetén

$$([b, p^{-1}, Z] \Longrightarrow_{\mathbf{A}}^* [c, e, e]) \quad \Longleftrightarrow \quad ((c, Z, b) \Longrightarrow_G^* p), \tag{10.24}$$

ugyanis ez az ekvivalencia (10.7) és (10.20) szerint $b = a_0$ és $Z = \perp$ esetben éppen az $L^{-1} = L(G)$ jelenti.

Először a $(c, Z, b) \Longrightarrow_G^* p$ levezetés n hossza szerinti teljes indukcióval megmutatjuk, hogy

$$((c, Z, b) \Longrightarrow_G^* p) \quad \Longrightarrow \quad [b, p^{-1}, Z] \Longrightarrow_{\mathbf{A}}^* [c, e, e], \tag{10.25}$$

Ha $n = 1$, akkor $(c, Z, b) \Longrightarrow_G p$. Ez azonban (10.22) miatt csak úgy lehet, ha $p \in X \cup e$ és $(c, e) \in \delta(b, Z, p)$. Következésképpen $[b, p^{-1}, Z] \Longrightarrow_{\mathbf{A}} [c, e, e]$.

Tegyük fel, hogy minden legfeljebb $n \geq 1$ hosszúságú $(c, Z, b) \Longrightarrow_G^* p$ levezetésre teljesül (10.24). Legyen $(c, Z, b) \Longrightarrow_G^* p$ egy $n+1$ hosszúságú levezetés.

Figyelembe véve a H-beli szabályok definícióját ez a levezetés az alábbi alakban írható:

$$(c,Z,b) \Longrightarrow_G (c,Z_1,b_1)(b_1,Z_2,b_2)\dots(b_{k-1},Z_k,b_k)x \Longrightarrow_G^* p_1p_2\dots p_kx = p,$$

ahol egyrészt $(b_k, Z_1Z_2\dots Z_k) \in \delta(b,Z,x)$ $k \geq 1$, másrészt az indukciós feltevés miatt a

$$(b_{j-1},Z_j,b_j) \Longrightarrow_G^* p_j, \quad ,b_0 = c,\ j = 1,2,\dots,k$$

levezetések legfeljebb n hosszúságúak. Ezért

$$[b_j, p_j^{-1}, Z_j] \Longrightarrow_{\mathbf{A}}^* [b_{j-1}, e, e]). \tag{10.26}$$

A (10.21), (10.22) definíciók és a (10.26) levezetések felhasználásával kapjuk, hogy

$$\begin{gathered}[b,p^{-1},Z] = [b, xp_k^{-1}p_{k-1}^{-1}\dots p_1^{-1}, Z] \Longrightarrow_{\mathbf{A}} \\ \Longrightarrow_{\mathbf{A}} [b_k, p_k^{-1}p_{k-1}^{-1}\dots p_1^{-1}, Z_1\dots Z_{k-1}Z_k] \Longrightarrow_{\mathbf{A}}^* \\ \Longrightarrow_{\mathbf{A}}^* [b_{k-1}, p_{k-1}^{-1}\dots p_1^{-1}, Z_1\dots Z_{k-1}] \Longrightarrow_{\mathbf{A}}^* \cdots \\ \Longrightarrow_{\mathbf{A}}^* [b_1, p_1^{-1}, Z_1] \Longrightarrow_{\mathbf{A}}^* [c,e,e].\end{gathered}$$

azaz (10.25) implikáció igaz.

A $[b,p^{-1},Z] \Longrightarrow_{\mathbf{A}}^* [c,e,e]$ levezetés n hossza szerinti teljes indukcióval mutathatjuk meg, hogy

$$([b,p^{-1},Z] \Longrightarrow_{\mathbf{A}}^* [c,e,e]) \quad \Longrightarrow \quad ((c,Z,b) \Longrightarrow_G^* p) \tag{10.27}$$

Ha $n = 1$, akkor $[b,p^{-1},Z] \Longrightarrow_{\mathbf{A}} [c,e,e]$. Ez azonban csak úgy lehet, ha $p \in X \cup e$ és $(c,e) \in \delta(b,Z,p)$. Ezért (10.22) szerint $(c,Z,b) \Longrightarrow_G p$.

Tegyük fel, hogy minden legfeljebb $n \geq 1$ hosszúságú $[b,p^{-1},Z] \Longrightarrow_{\mathbf{A}}^* [c,e,e]$ levezetésre teljesül (10.27). Legyen $[b,p^{-1},Z] \Longrightarrow_{\mathbf{A}}^* [c,e,e]$ egy $n+1$ hosszúságú levezetés. Akkor (10.3) és (10.5) szerint

$$[b,p^{-1},Z] = [b,xq^{-1},Z] \Longrightarrow_{\mathbf{A}} [b_k,q^{-1},Z_1\dots Z_{k-1}Z_k] \Longrightarrow_{\mathbf{A}}^* [c,e,e], \tag{10.28}$$

ahol $p = qx$ $(q \in X^*, x \in X \cup e), b_k \in A$ és $Z_1, Z_2, \dots Z_k \in \Gamma,\ k \geq 1$, olyanok, amelyekre $(b_k, Z_1Z_2\dots Z_k) \in \delta(b,Z,x)$. Az indukciós feltevés szerint a

$$[b_k, q^{-1}, Z_1\dots Z_{k-1}Z_k] \Longrightarrow_{\mathbf{A}}^* [c,e,e] \tag{10.29}$$

levezetés n hosszúságú. A (10.29) levezetésből kapjuk, hogy a q szó felírható olyan $q = p_1p_2\dots p_k$ $(p_j \in X^*, j = 1,2,\dots,k)$ alakban, amelyre a

$p_k^{-1}, p_{k-1}^{-1}, \ldots, p_1^{-1}$ szavak ilyen sorrendben történő elolvasása után rendre törlődnek a veremből a $Z_k, Z_{k-1}, \ldots, Z_1$ jelek. Ez azt jelenti, hogy vannak olyan $b_{k-1}, \ldots, b_1, b_0 = c$ állapotok, amelyekre

$$([b_j, p_j^{-1}, Z_j] \Longrightarrow_{\mathbf{A}}^{*} [b_{j-1}, e, e]), \quad j = k, \ldots, 2, 1.$$

Mivel ezeket levezetéseket a (10.29) levezetésben sorra alkalmazzuk, ezért legfeljebb n hosszúságúak lehetnek. Az indukciós feltevés szerint

$$(b_{j-1}, Z_j, b_j) \Longrightarrow_G^{*} p_j, \quad j = 1, 2, \ldots, k. \tag{10.30}$$

A (10.19) definícióból és (10.28) levezetés első lépéséből kapjuk, hogy

$$(c, Z, b) \to (b_0, Z_1, b_1)(b_1, Z_2, b_2) \ldots (b_{k-1}, Z_k, b_k)x. \tag{10.31}$$

A (10.31) szabályban végrehajtva sorra a (10.30) levezetéseket, kapjuk, hogy

$$(c, Z, b) \Longrightarrow_G^{*} p_1 p_2 \ldots p_k x = p,$$

vagyis (10.27) fennáll. Ezzel megmutattuk, hogy (10.24) is igaz. □

A tétel bizonyításából nyilvánvalóan adódik azonban az alábbi eredmény.

10.4. Következmény. *Egy nyelv akkor és csak akkor ismerhető fel veremautomatában, ha felismerhető egyállapotú veremautomatában üres veremmel.*

Megmutatható, hogy veremautomatákra nem igaz a 7.9 Tétel megfelelője, azaz nem minden környezetfüggetlen nyelv ismerhető fel determinisztikus veremautomatával.

10.5. Tétel. *A determinisztikus veremautomatákkal felismerhető nyelvek osztálya valódi részosztálya a veremautomatákkal felismerhető nyelvek osztályának.*

A bizonyítás megtalálható például Gécseg Ferenc [19] jegyzetében.

A determinisztikus automatákkal felismerhető nyelveket *determinisztikus környezetfüggetlen nyelvek*nek nevezzük. Mint arról már az I. rész bevezetőjében is beszéltünk a programozási nyelvek szintaxisának megadására a legalkalmasabb módszer generatív G grammatikákkal való megadás. Erre különösen alkalmasak a determinisztikus környezetfüggetlen nyelveket generáló környezetfüggetlen garmmatikák. Gyakorlatban ez annak az un. *szintaktikai elemzés*ét jelenti, hogy a felhasználó által írt $p(\in X^*)$ program megfelel-e a szintaktikai előírásoknak, azaz $p \in L(G)$ teljesül-e. Mint az I. rész bevezetőjében azt is említettük, hogy a jegyzet terjedelme miatt ezzel nem foglalkozhatunk. A szintaktikai elemzésről azonban részletes bevezetőt olvashatunk például a [18] és a [19] jegyzetekben is.

11. fejezet

Turing automaták

A fejezetben bevezetjük a (nemdeterminisztikus) Turing automata fogalmát. Megmutatjuk, hogy az ilyen automatákban felismerhető nyelvek osztálya megegyezik a 0 típusú nyelvek osztályával.

11.1. A Turing automata fogalma

Legyenek $A \neq \emptyset$ és $X \neq \emptyset$ tetszőleges véges halmazok, $a_0 \in A$ és $\# \in X$ egy-egy kitüntetett elem, δ pedig

$$\delta : A \times X \to P(A \times X \times V)$$

típusú függvény, ahol $V = \{\leftarrow, \rightarrow, \downarrow\}$. Az $\mathbf{A} = (A, a_0, X, \delta, \#)$ rendszert (*nemdeterminisztikus*) *Turing automatá*nak nevezzük, ha tetszőleges $a \in A$ és $x \in X$ esetén teljesülnek a

$$((b, z, v) \in \delta(a, \#),\ z \neq \#) \quad \Longrightarrow \quad v \neq \downarrow, \tag{11.1}$$

$$(b, \#, v) \in \delta(a, x) \quad \Longrightarrow \quad x = \#. \tag{11.2}$$

feltételek. Az A és X halmazokat $\mathbf{A}$ *állapothalmaz*ának ill. *bemenő halmaz*ának, $\#$ szimbólumot $\mathbf{A}$ *korlátozó jel*ének, a δ függvényt pedig $\mathbf{A}$ *mozgásfüggvény*ének nevezzük.

Az $\mathbf{A} = (A, a_0, X, \delta, \#)$ Turing automatát *determinisztikus*nak mondjuk, ha minden $a \in A$ és $x \in X$ párra $|\delta(a, x)| \leq 1$ teljesül.

Az $\mathbf{A} = (A, a_0, X, \delta, \#)$ Turing automatában is kijelölhetünk végállapotok egy $F \subseteq A$ halmazát. Ebben az esetben használjuk az

$$\mathbf{A}_F = (A, a_0, X, \delta, \#; F)$$

jelölést is.

A Turing automata működését a következő módon képzelhetjük el. A Turing automata diszkrét időskálában dolgozik. Úgy tekintjük, hogy az $\mathbf{A} = (A, a_0, X, \delta, \#)$ Turing automata író-olvasófejjel van ellátva, amely $\mathbf{A}$ működésének minden időpillanatában egy cellákra osztott mindkét irányban végtelen bemenő szalag valamely cellájára mutat. A bemenő szalag celláiba egy $(X - \#)^*$-beli p bemenő szó betűi vannak folytatólagosan beírva, a többi cellában pedig mindenütt a # korlátozó jel áll. (A p szó egy program kezdő feltételének tekinthető.) Emellett működésének minden időpillanatában $\mathbf{A}$ valamilyen A-beli állapotban van. Feltételezzük, hogy működése kezdetén $\mathbf{A}$ az a_0 kezdőállapotban van és az író-olvasófej a szalagon lévő $p \in (X - \#)^*$ szó első betűje előtt álló, hozzá legközelebb lévő # jelet tartalmazó cellára mutat.

Ha működésének valamely időpillanatában az automata az $a \in A$ állapotban van és az író-olvasófej a bemenő szalag olyan cellájára mutat, amelyben az $x \in X$ jel áll, akkor az automata működése az alábbi lehetőségek valamelyike szerint folytatódhat:

1. Ha $\delta(a, x) = \emptyset$, akkor $\mathbf{A}$ nem működik tovább.
2. Ha $(b, z, \downarrow) \in \delta(a, x)$, akkor az író-olvasófej kitörli a cellából az x jelet, helyébe a z jelet írhatja, az író-olvasófej helyben marad és az automata átmegy a b állapotba.
3. Ha $(b, z, \leftarrow) \in \delta(a, x)$, akkor az író-olvasófej kitörli a cellából az x jelet, helyébe a z jelet írhatja, majd az író-olvasófej egy cellával balra lép és közben az automata átmegy a b állapotba.
4. Ha $(b, z, \rightarrow) \in \delta(a, x)$, akkor az író-olvasófej kitörli a cellából az x jelet, helyébe a z jelet írhatja, majd az író-olvasófej egy cellával jobbra lép és közben $\mathbf{A}$ átmegy a b állapotba.

Ha $x = \#$ és $z \neq \#$, akkor a 3. [4.] lépés után a bemenő szalagon lévő $p \in (X - \#)^*$ szó helyett a zp $[pz] \in (X - \#)^*$ szó kerülhet. A Turing automata e tulajdonságát úgy is kifejezhetjük, hogy a Turing automata képes munkaterének kibővítésére. Azonban (11.2) miatt az író-olvasófej korlátozó jelre csak korlátozó jelet cserélhet.

Ha $|X| \geq 2$, akkor a definíció alapján egy Turing automata olyan végtelen (parciális és nemdeterminisztikus) kimenő jel nélküli automatának tekinthető, amelynek állapothalmaza $A \times \#(X - \#)^*\#$ és bemenő halmaza X.

A Turing automata működésének leírására is bevezetjük a konfiguráció fogalmát. Azt mondjuk, hogy az $\mathbf{A} = (A, a_0, X, \delta, \#)$ Turing automata a

$$[p, a, q] \quad (p, q \in X^*,\ a \in A)$$

*konfiguráció*ban van, ha $\mathbf{A}$ az a állapotban van, a bemenő szalagon a pq szó áll, az író-olvasófej pedig a q szó első betűjét tartalmazó cellára, ill. ha q az üres szó, akkor közvetlenül a p szó után álló # jelet tartalmazó cellára mutat.

(Ha $p = q = e$, akkor az író-olvasófej akkor a bemenő szalag minden cellája a korlátozó jelet tartalmazza.)

Az $\mathbf{A}$ Turing automatában a K_2 konfigurációt a K_1 konfigurációból *közvetlenül levezethető*nek nevezzük, jelekben

$$K_1 \Longrightarrow_{\mathbf{A}} K_2,$$

ha tetszőleges $a, b \in A$, $x, y, z \in X$, $u \in X - \#$ és $p, q \in X^*$ esetén a következő feltételek valamelyike teljesül:

$$K_1 = [p, a, xq], \quad K_2 = [p, b, yq], \quad (b, y, \downarrow) \in \delta(a, x); \tag{11.3}$$

$$K_1 = [p, a, xq], \quad K_2 = [py, b, q], \quad (b, y, \rightarrow) \in \delta(a, x); \tag{11.4}$$

$$K_1 = [pz, a, xq], \quad K_2 = [p, b, zyq], \quad (b, y, \leftarrow) \in \delta(a, x); \tag{11.5}$$

$$K_1 = [e, a, \#q], \quad K_2 = [e, b, \#uq], \quad (b, u, \leftarrow) \in \delta(a, \#); \tag{11.6}$$

$$K_1 = [p\#, a, e], \quad K_2 = [pu\#, b, e], \quad (b, u, \rightarrow) \in \delta(a, \#). \tag{11.7}$$

Akkor mondjuk, hogy a K konfigurációból (n *lépésben*) *levezethető* vagy (n *lépésben kiszámítható* a K' konfiguráció, jelekben:

$$K \Longrightarrow_{\mathbf{A}}^* K',$$

ha megadható konfigurációk olyan $K_0, K_1, \ldots, K_n$ sorozata, hogy

$$K = K_0, \quad K_{i-1} \Longrightarrow_{\mathbf{A}} K_i \ (i = 1, 2, \ldots, n), \quad K_n = K'. \tag{11.8}$$

A (11.8) sorozatot $\mathbf{A}$-beli *levezetés*nek, vagy *számítás*nak nevezzük. Ha nem vezet félreértésre, akkor $\Longrightarrow_{\mathbf{A}}$ és $\Longrightarrow_{\mathbf{A}}^*$ helyett a $\Longrightarrow$ ill. $\Longrightarrow^*$ kifejezést is használjuk.

11.2. Nyelvek felismerése Turing automatákban

Azt mondjuk, hogy az $X - \#$ ábécé feletti L nyelv *felismerhető* az $\mathbf{A} = (A, a_0, X, \delta, \#)$ (nemdeterminisztikus) Turing automatában az A állapothalmaz egy F részhalmazával vagy *előállítható* az $\mathbf{A}_F = (A, a_0, X, \delta; F)$ automatában, röviden, L felismerhető az $\mathbf{A}$ Turing automatában, ha L pontosan azokból a $p \in (X - \#)^*$ szavakból áll, amelyekhez létezik olyan $q \in (X - \#)^*$ szó és olyan $a \in F$ állapot, hogy

$$[e, a_0, \#p\#] \Longrightarrow_{\mathbf{A}}^* [\#q\#, a, e]. \tag{11.9}$$

(Ezt úgy is elképzelhetjük, hogy az $\mathbf{A}$ Turing automata az a_0 kezdőállapotból indulva, a p kezdeti feltételből a (11.9) program végrehajtásával kiszámítja q-t

és az a végállapotba kerül, azaz megáll.) Ugyanúgy, mint más automatatípusok esetén, azt is mondjuk, hogy $\mathbf{A}$ Turing automata *felismeri* vagy *előállítja* vagy *elfogadja* az L nyelvet (az F halmazzal). Most is használjuk az $L = L(\mathbf{A}, F)$ jelölést.

11.1. Példa. *Tekintsük az*

A	a_0	a_1	a_2	a_3
$\#$	$(a_1, y, \leftarrow)$	$(a_2, \#, \rightarrow)$	$(a_3, \#, \rightarrow)$	$\emptyset$
x	$(a_1, y, \downarrow)$	$(a_2, y, \rightarrow)$	$\emptyset$	$\emptyset$
z	$\emptyset$	$(a_1, z, \rightarrow)$	$\{(a_1, z, \downarrow)\}$	$\emptyset$
u	$\emptyset$	$(a_0, x, \downarrow)$	$\emptyset$	$\emptyset$

determinisztikus Turing automatát. Megmutatjuk, hogy $zzx \in L(\mathbf{A}, a_3)$ *és* $zxz, xzz \notin L(\mathbf{A}, a_3)$.

Az zzx szóra vonatkozó

$$[e, a_0, \#zzx\#] \Longrightarrow [e, a_1, \#zzzx\#] \Longrightarrow [\#, a_2, zzzx\#] \Longrightarrow$$
$$\Longrightarrow [\#, a_1, uzzx\#] \Longrightarrow [\#, a_0, xzzx\#] \Longrightarrow [\#, a_1, zzzx\#] \Longrightarrow$$
$$\Longrightarrow [\#u, a_1, zzx\#] \Longrightarrow [\#uu, a_1, zx\#] \Longrightarrow [\#uuu, a_1, x\#] \Longrightarrow$$
$$\Longrightarrow [\#uuuz, a_2, \#] \Longrightarrow [\#uuuz\#, a_3, e]$$

levezetés szerint $zzx \in L(\mathbf{A}, a_3)$. Az zxz szóra vonatkozó

$$[e, a_0, \#zxz\#] \Longrightarrow [e, a_1, \#zzxz\#] \Longrightarrow [\#, a_2, zzxz\#] \Longrightarrow$$
$$\Longrightarrow [\#, a_1, uzxz\#] \Longrightarrow [\#, a_0, xzxz\#] \Longrightarrow [\#, a_1, zzxz\#] \Longrightarrow$$
$$\Longrightarrow [\#u, a_1, zxz\#] \Longrightarrow [\#uu, a_1, xz\#] \Longrightarrow [\#uuz, a_2, z\#] \Longrightarrow$$
$$\Longrightarrow [\#uuz, a_1, u\#] \Longrightarrow [\#uuz, a_0, x\#] \Longrightarrow [\#uuz, a_1, z\#] \Longrightarrow$$
$$\Longrightarrow [\#uuzu, a_1, \#] \Longrightarrow [\#uuzu\#, a_2, e]$$

számítás szerint $zxz \notin L(\mathbf{A}, a_3)$. Mivel

$$[e, a_0, \#xzz\#] \Longrightarrow [e, a_1, \#zxzz\#] \Longrightarrow [\#, a_2, zxzz\#] \Longrightarrow$$
$$\Longrightarrow [\#, a_1, uxzz\#] \Longrightarrow [\#, a_0, xxzz\#] \Longrightarrow [\#, a_1, zxzz\#] \Longrightarrow$$
$$\Longrightarrow [\#u, a_1, xzz\#] \Longrightarrow [\#uz, a_2, zz\#] \Longrightarrow [\#uz, a_1, uz\#] \Longrightarrow$$
$$\Longrightarrow [\#uz, a_0, xz\#] \Longrightarrow [\#uz, a_0, zz\#]$$

számítás tovább nem folytatható, mert $\delta(a_0, z) = \emptyset$ miatt a $\mathbf{A}$ Turing automata leáll, ezért $xzz \notin L(\mathbf{A}, a_3)$.

11.3. A Turing automaták és a mondatszerkezetű nyelvek

11.2. Tétel. *Minden Turing automatában felismerhető nyelv* 0 *típusú.*

Bizonyítás Tegyük fel, hogy az X véges ábécé feletti L nyelv felismerhető az $\mathbf{A} = (A, a_0, U \cup \#, \delta, \#)$ $(\# \notin U)$ Turing automatában az állapotok $F \subseteq A$ részhalmazával, azaz $L = L(\mathbf{A}, F)$. Konstruáljuk meg a $G = (V_N, U, S, H)$ 0 típusú grammatikát a következőképpen:

Legyen U' egy olyan ábécé, amelyre $|U'| = |U|$, $U' \cap (A \cup U) = \emptyset$ és $\# \notin U'$. Legyen továbbá φ az X ábécé bijektív leképezése U'-re és $V_N = A \cup U' \cup \{\#, S, R, T\}$, ahol $S, R, T \notin A \cup U \cup U' \cup \{\#\}$. Jelöljük szintén φ-vel φ homomorf kiterjesztését U^*-ra.

Ezek után megadjuk a H-beli helyettesítési szabályok definícióját:
Minden $a \in A$, $x \in U \cup \#$ párra

$$b\varphi(y) \longrightarrow a\varphi(x), \quad \text{ha} \quad (b, y, \downarrow) \in \delta(a, x), \tag{11.10}$$

$$\varphi(y)b \longrightarrow a\varphi(x), \quad \text{ha} \quad (b, y, \rightarrow) \in \delta(a, x). \tag{11.11}$$

Minden $a \in A$, $x \in U$, $z \in U \cup \#$ hármasra

$$b\varphi(z)\varphi(y) \longrightarrow \varphi(z)a\varphi(x), \quad \text{ha} \quad (b, y, \leftarrow) \in \delta(a, x). \tag{11.12}$$

Minden $a \in A$, $u \in U$ párra

$$b\#\varphi(u) \longrightarrow a\#, \quad \text{ha} \quad (b, u, \leftarrow) \in \delta(a, \#), \tag{11.13}$$

$$\varphi(u)b\# \longrightarrow a\#, \quad \text{ha} \quad (b, u, \rightarrow) \in \delta(a, \#). \tag{11.14}$$

Továbbá

$$S \longrightarrow R\#a \ (a \in A), \quad R \longrightarrow R\varphi(x) \ (x \in U), \quad R \longrightarrow \#, \tag{11.15}$$

$$T\varphi(x) \longrightarrow \varphi(x)T \ (x \in U), \quad a_0\# \longrightarrow T, \quad T\# \longrightarrow e. \tag{11.16}$$

Végül

$$\varphi(x) \longrightarrow x \ (x \in U). \tag{11.17}$$

Megmutatjuk, hogy az így definiált 0 típusú grammatika generálja az L nyelvet. Legyen e célból $p \in L$ tetszőleges szó. Akkor létezik olyan $q \in U^*$ és $a \in F$, hogy

$$[e, a_0, \#p\#] \Longrightarrow_{\mathbf{A}}^* [\#q\#, a, e].$$

A (11.10) - (11.14) szabályok figyelembevételével kapjuk, hogy

$$\#\varphi(q)\#a \Longrightarrow_G^* a_0\#\varphi(p)\#.$$

A (11.15) szabályok miatt

$$S \Longrightarrow_G^* \#\varphi(q)\#a,$$

és (11.16) miatt

$$a_0\#\varphi(p)\#a \Longrightarrow_G^* \varphi(p).$$

Ezért, (11.17)-et is felhasználva,

$$S \Longrightarrow_G^* \#\varphi(q)\#a \Longrightarrow_G^* a_0\#\varphi(p)\# \Longrightarrow_G^* \varphi(p) \Longrightarrow_G^* p,$$

tehát $p \in L(G)$, s így $L \subseteq L(G)$.

Megfordítva, legyen $p \in L(G)$, azaz $S \Longrightarrow_G^* p$. Ekkor van olyan $q \in U^*$ bemenő szó és $a \in F$ állapot, hogy a (11.15) szabályok felhasználásával

$$S \Longrightarrow_G^* \#\varphi(q)\#a,$$

s a (11.10) - (11.14) szabályok felhasználásával

$$\#\varphi(q)\#a \Longrightarrow_G^* a_0\#\varphi(p)\#.$$

Innen a (11.10) - (11.14) szabályok definícióját figyelembe véve

$$[e, a_0, \#p\#] \Longrightarrow_{\mathbf{A}}^* [\#q\#, a, e],$$

azaz $p \in L$. Ezzel megmutattuk, hogy az $L(G) \subseteq L$ tartalmazás is fennáll, vagyis $L = L(G)$. □

A *Church–Turing tézis* szerint minden rekurzíve felsorolható nyelvhez létezik felsorolási algoritmus Turing automata segítségével, azaz felismerhető Turing automatában. (A *Church–Turng tézis* számunkra elegendő megfogalmazása megtalálható az Előszóban.)

Másrészt a 4.2. alfejezetben megmutattuk, hogy minden 0 típusú nyelv rekurzíve felsorolható. Így, ha igaz a *Church–Turing tézis*, akkor a következők is igazak.

11.3. Következmény. *Bármely véges ábécé feletti L nyelvre ekvivalensek az alábbi állítások:*
(1) L 0 típusú nyelv;
(2) L rekurzíve felsorolható nyelv
(3) L felismerhető Turing automatában.

A következő eredményt bizonyítás nélkül közöljük. A bizonyítás megtalálható többek között RÉVÉSZ GYÖRGY [37] munkájában.

11.4. Tétel. *A determinisztikus Turing automatákkal felismerhető nyelvek megegyeznek a nemdeterminisztikus Turing automatákkal felismerhető nyelvekkel.*

Végül definiáljuk a Turing automaták egy speciális osztályát , az ún. *lineárisan korlátolt automatá*kat. Megmutatható, hogy az általuk felismert nyelvek az 1 típusú nyelvek. A bizonyítást, annak hosszadalmassága miatt nem végezzük el. Az olvasó a bizonyítást megtalálhatja például PEÁK ISTVÁN [34] egyetemi jegyzetében.

Az $\mathbf{A} = (A, X, a_0, \delta, \#)$ Turing automatát (*nemdeterminisztikus*) *lineárisan korlátolt automatá*nak nevezzük, ha tetszőleges $a \in A$ és $x \in X$ esetén

$$(b, z, v) \in \delta(a, \#) \quad \Longrightarrow \quad z = \#. \tag{11.18}$$

Tehát egy lineárisan korlátolt automata olyan Turing automata, amelynek nincs olyan $z \neq \#$ bemenő jele, amelyre teljesülne a (11.1) feltétel. Így a lineárisan korlátolt Turing automata működése közben a bemenő szalagon az író-olvasófej korlátozó jelet csak korlátozó jelre cserélhet, vagyis nem képes munkaterének kibővítésére. Ez azt jelenti, hogy egy lineárisan korlátolt Turing automatában a levezetésekben a (11.6) és a (11.7) közvetlen levezetések nem szerepelnek.

11.5. Tétel. *Egy nyelv akkor és csak akkor* 1 *típusú, ha felismerhető lineárisan korlátolt Turing automatában.*

Megoldatlan az a probléma, hogy a 11.4 Tétel állítása igaz-e lineárisan korlátolt determinisztikus Turing automatákra. Ez az ismert *LBA probléma* (LBA a *linear bounded automaton* szavak kezdőbetűit jelenti.) A lineárisan korlátolt determinisztikus Turing automatákkal felismert nyelveket *determinisztikus környezetfüggő nyelvek*nek nevezzük. Az LBA probléma úgy is megfogalmazható, hogy a determinisztikus környezetfüggő nyelvek osztálya egyenlő-e a nemdeterminisztikus környezetfüggő nyelvek osztályával.

11.4. Turing automaták bonyolultsága

Amint azt a 3.1. alfejezetben definiáltuk, egy X ábécé feletti L nyelvet *rekurzív*nak neveztünk X felett, ha bármely $p \in U^*$ szórol algoritmikusan eldönthető, hogy benne van-e L-ben, azaz megoldható az L nyelvre vonatkozó szóprobléma. Az nyilvánvaló, hogy egy adott ábécé feletti rekurzív nyelv komplementere is rekurzív az adott ábécé felett. Nyelvek egy osztályát *rekurzív*nak

neveztük, ha minden eleme rekurzív. A 4.2 Tétel szerint a környezetfüggő nyelvek osztálya rekurzív. A 4.3 Tétel azt mutatja, hogy létezik olyan rekurzív nyelv, amelyik nem környezetfüggő. A 4.2. alfejezetben megadtuk a rekurzívan felsorolható nyelvek fogalmát. Az X ábécé feletti L nyelvet (X *felett*) *rekurzíve felsorolható*nak hívtunk, ha van olyan eljárás, amely az összes $p \in L$ szót valamilyen sorrendben (esetleg ismétlésekkel) előállítja, azaz felsorolja. A 4.4 Lemma szerint egy véges ábécé feletti nyelv akkor és csak akkor rekurzív, ha a nyelv és komplementere is rekurzíve felsorolható az ábécé felett. A 4.5 Tétel szerint véges ábécé felett van olyan rekurzíve felsorolható nyelv, amely nem rekurzív az ábécé felett. Ezek szerint, mint már azt az 5. fejezet elején is említettük, 11.3 Következmény alapján

$$\mathcal{L}_1 \subset \mathcal{L}_r \subset \mathcal{L}_0, \tag{11.19}$$

ahol $\mathcal{L}_1$, $\mathcal{L}_r$ $\mathcal{L}_0$ rendre a környezetfüggő, a rekurzív és a mondatszerkezetű nyelvek osztálya. Ez azt jelenti, hogy nem minden mondatszerkezetű nyelvre oldható meg a szóprobléma. A 11.2. alfejezetben tárgyaltuk, hogy egy X bemenő halmaz feletti Turing automata által felismerhető L nyelv esetén egy $p \in X^*$ szóra $p \in L$ azt jelenti, hogy a Turing automata a kezdőállapotából indulva, a p kezdeti feltételből a (11.9) program (algoritmus) végrehajtásával kiszámítja a $q \in X^*$ eredményt és egy végállapotba kerül, azaz megáll. Azt is mondhatjuk, hogy a (11.19) második valódi tartalmazása határt szab a kiszámíthatóságnak.

Mint már említettük, a Turing automata, mint az általunk definiált minden automata diszkrét időskálában dolgozik. Az Előszóban beszéltünk arról, hogy egy *matematikai algoritmus* olyan matematikai eljárás, amely Turing automatával véges számú lépésben végrehajtható. Ezt úgy is mondhatjuk, hogy a matematikai eljárás véges idő alatt befejeződik. Mint ezt már 11.3 Következmény előtt is megjegyeztük, az algoritmusnak ez a fogalma A *Church–Turing tézis* alapján kellően megalapozottnak tűnik. Mint azt az Előszóban megfogalmaztuk, a *Church–Turing tézis* lényegében azt mondja ki, hogy minden pontosan definiált matematikai algoritmushoz megadható egy Turing automata, amely ezt az algoritmust végrehajtja.

Mivel a rekurzív nyelvek osztálya meghatározza a kiszámíthatóság határát, a nemrekurzív mondatszerkezetű nyelvekre nem garantált, hogy egy eljárás befejeződik, azaz a Turing automata véges sok lépés után megáll, vagyis az adott probléma megoldható. Ez pedig egy adott probléma esetén lehetséges, mivel a *Gödel tétel* értelmében vannak olyan problémák, amelyek nem oldhatók meg, azaz az eljárás soha nem fejeződik be.

A gazdaságosság szempontjából persze nem mindegy, hogy ha egy eljárás befejeződik, akkor mennyi idő alatt. Megjegyezzük, hogy azonosítjuk a lépések számát az eljárás végrehajtásának idejével, ami diszkrét eljárások esetén

megtehető. De az sem lényegtelen, hogy a számítás során a bemenő szalagon hány cellát használunk fel. Nyilvánvalóan a bonyolultabb eljárások több időt vagy több cellát használnak fel a számítás során. Természetesen a idő és a szalag (cellák) felhasználása függ a Turing automata felépítésétől, például a belső állapotok számától is. Ezek a számok a Turing automaták (rekurzív nyelvek, algoritmusok) bonyolultságát különböző szempontok szerint mérhetik. Ez vezetett a Turing automaták (algoritmusok) illetve a rekurzív nyelvek bonyolultságelméletének kialakulásához. Többféle bonyolultsági fogalom található a [9] és a [10] munkákban. Például a Turing automata un. *tárbonyolultság függvény*ét az eljárás során a bemenő szalagon legalább egyszer felhasznált cellák számával jellemezhetjük a kezdeti feltétel hosszának függvényében. Mi csupán az időtartam szerinti bonyolultsággal foglalkozunk röviden a kezdeti feltétel (bemenő szó) hosszának függvényében.

Jelölje $\mathbf{A}$ egy X véges ábécé (bemenő halmaz) feletti Turing automatát. Ha az $\mathbf{A}$ Turing automata a $p \in X^*$ kezdeti feltétellel a kezdőállapotból egy végállapotba kerül, akkor jelölje $l_{\mathbf{A}}(p)$ a számítás lépéseinek számát. Ha ez nem teljesül, akkor legyen $l_{\mathbf{A}}(p) = \infty$. Legyen továbbá minden n pozitív egész számra

$$t_{\mathbf{A}}(n) = \sup\{l_{\mathbf{A}}(p);\ p \in X^n\}.$$

A $t_{\mathbf{A}}$ függvényt $\mathbf{A}$ *időbonyolultság függvény*ének nevezzük, és azt mutatja meg, hogy az eljárás n hosszúságú kezdeti feltétel esetén hány lépésben, azaz mennyi idő alatt fejeződik be.

Gyakorlati szempontból jól kezelhetők azok a Turing automaták amelyekre $t_{\mathbf{A}}(n)$ az n változó polinomja. Ezt úgy is mondjuk, hogy a problémákat *polinomiális idő* alatt oldja meg a Turing automata. Ha ezek a Turing automaták determinisztikusak, akkor P *bonyolultságú Turing automaták*nak, az általuk felismert (rekurzív) nyelveket pedig P *bonyolultságú nyelvek*nek nevezzük. Ha pedig ezek a Turing automaták nemdeterminisztikusak, akkor NP *bonyolultságú Turing automaták*nak, az általuk felismert (rekurzív) nyelveket pedig NP *bonyolultságú nyelvek*nek mondjuk.

Mivel minden determinisztikus Turing automata nemdeterminisztikus is, ezért a P bonyolultságú nyelvek osztálya részosztálya az NP bonyolultságú nyelvek osztályának, röviden mondva $P \subseteq NP$. Bár a 11.4 Tétel szerint a determinisztikus Turing automatákkal felismerhető nyelvek osztálya megegyezik a nemdeterminisztikus Turing automatákkal felismerhető nyelvek osztályával, ebből nem következik, hogy $P = NP$. A $P = NP$ vagy $P \subset NP$ régóta megoldatlan problémája a formális nyelvek elméletének, ez az un. *P-NP probléma*. Általában elfogadott az a nézet, hogy $P \subset NP$.

12. fejezet

Speciális nyelvek

A fejezetben a reguláris nyelvek néhány nevezetes részosztályáról lesz szó. Reguláris nyelvek mellett azonban bemutatunk nem reguláris nyelveket is. Először tekintsük a legegyszerűbb esetet, a véges nyelvek osztályát.

12.1. Véges nyelvek

A fő cél annak a kérdésnek a vizsgálata, hogy egy véges nyelv felismeréséhez minimálisan hány állapotú automata ill. hány végállapot szükséges. Nyilvánvalóan minden véges nyelv tekinthető véges ábécé feletti reguláris nyelvként.

A 7.4. alfejezetben definiáltuk a véges automatákban felismerhető, azaz Kleene tétele szerint a reguláris nyelvek súlyát. Vagyis egy X ábécé feletti L *reguláris nyelv súlyá*n azt az $s(L)$ nemnegatív egész számot értjük, amelyre L felismerhető $s(L)$ állapotú automatában és ha L felismerhető valamely $\mathbf{A} = (A, X, \delta)$ automatában, akkor $s(L) \leq |A|$. A 7.7 Tétel bizonyítása szerint egy L reguláris nyelv súlya megegyezik a (7.4)-ben definiált τ_L jobb kongruencia indexével. Az L reguláris nyelv *felismerési* vagy *reprezentációs számá*n pedig azt az $r(L)$ nemnegatív egész számot értjük, amelyre L felismerhető egy automata $r(L)$ számú állapotával és ha L felismerhető valamely $\mathbf{A}_F = (A, a_0, X, \delta; F)$ automatában, akkor $r(L) \leq |F|$. Nyilvánvaló, hogy minden L véges nyelvre $r(L) \leq |L|$. Az L véges nyelvet *irreducibilis*nek nevezzük, ha $r(L) = |L|$ és *reducibilis*nek, ha $r(L) < |L|$. Az üres nyelv és az egyelemű nyelvek természetesen irreducibilisek.

12.1. Példa. *Legyen* $A = \{0, 1, 2, \ldots, n, n+1, n+2\}$, $X = \{x, y\}$,

$$\delta(j, x) = j + 1 \quad (j = 0, 1, \ldots, n-1),$$

$$\delta(n, x) = \delta(n+1, x) = \delta(n+2, x) = n + 2,$$

$$\delta(k, y) = n + 1 \quad (k = 1, 2, \ldots, n),$$
$$\delta(0, y = \delta(n + 1, y) = \delta(n + 2, y) = n + 2.$$

Az $L = xy + x^2y + \cdots + x^ny$ *nyelv felismerhető a* 0 *kezdő állapottal és az egyetlen* $n + 1$ *végállapottal. Vagyis* $r(L) = 1$*, így* L *minden* $2 \leq n$ *esetén reducibilis.*

12.2. Lemma. *Ha az* X *véges ábécé feletti* L *véges nyelv reducibilis, akkor bármely* $p \in X^+$ *szóra az* $L + p$ *nyelv is reducibilis.*

Bizonyítás Legyen L reducibilis nyelv X véges ábécé felett. Ez azt jelenti, hogy van olyan $\mathbf{A} = (A, a_0, X, \delta_A)$ iniciális véges automata és $F \subseteq A$, amelyre $L = L(\mathbf{A}, a_0, F)$ és $|F| = r(L) < |L|$. Egy ilyen automata megadható úgy is, hogy bármely L-beli $q = q_1q_2$ $(q_2 \neq e)$ szó esetén minden $r \in X^*$ szóra $a_0q_1 = a_0r$ akkor és csak akkor, ha $q_1 = r$. Ha ez az $\mathbf{A}$ automatára nem teljesül, akkor ilyen automatát a következő módon szerkeszthetünk meg. Minden $p \in L$ szó esetén a $\delta_A(a_0, p)$ út közbülső állapotainak feleltessünk meg új (egymástól és A elemeitől is különböző) állapotokat. Legyen ezen állapotok halmaza A'. Továbbá vegyünk fel meg egy $c \notin A \cup A'$ állapotot. Értelmezzük a $\mathbf{B} = (B, a_0, X, \delta_B)$ iniciális automatát az alábbi módon. Legyen $B = A \cup A' \cup c$. Ha $p \in L$, akkor $\delta_B(a_0, p)$ legyen az az út, amelyet a $\delta_A(a_0, p)$ útból úgy kapunk, hogy a közbülső állapotokat sorra kicseréljük a nekik megfeleltetett új állapotokkal. Ezek után, ha valamely $b \in B$ és $x \in X$ esetén $\delta_B(b, x)$ nincs definiálva, akkor legyen $\delta_B(b, x) = c$. Az így kapott automata jól definiált és $L = L(\mathbf{B}, a_0, F)$. (Megjegyezzük, hogy c az automata egy csapdája.)

Legyen $p \in X^+$ tetszőleges bemenő szó. Ha $p \in L$, akkor a tétel állítása nyilvánvalóan igaz. Ezért feltehetjük, hogy $p \notin L$. A $\mathbf{B}$ automatából szerkesszük meg a következő $\mathbf{D} = (D, a_0, X, \delta_D)$ iniciális automatát.

Legyen $a_1 = a_0p_1$, ha p_1 a p szó L-beli maximális hosszúságú prefixe. (Ha p-nek nincs L-beli $q \neq e$ prefixe, akkor pedig legyen $p_1 = e$.) Ha $p_2 = x_1x_2 \ldots x_m$ $(x_1, x_2, \ldots, x_m \in X)$, akkor vegyük fel a $d_1, d_2, \ldots, d_m \notin B$ új állapotokat és legyen $D = B \cup \{d_1, d_2, \ldots, d_m\}$, továbbá

$$\delta_D(a_1, x_1) = d_1, \ \delta_D(d_1, x_2) = d_2, \ldots, \delta_D(d_{m-1}, x_m) = d_m.$$

Tegyük fel először, hogy $p_1 \neq e$ p-nek L-beli maximális hosszúságú prefixe. Ha $\mathbf{B}$-ben valamely p_1-től különböző rx $(r \in X^*, x \in X)$ szóra $a_0rx = a_1$, akkor az $a_0r \in B$ állapotra legyen $\delta_D(a_0r, x) = d_m$. Minden más $b \in B$, $x \in X$ párra legyen $\delta_D(a, x) = \delta_B(a, x)$. Végül, ha egy $d \in D$, $x \in X$ párra $\delta_D(b, x)$ még nincs definiálva, akkor legyen $\delta_D(d, x) = c$.

Ha p-nek nincs L-beli $q \neq e$ prefixe, akkor az előbbiek szerint $\delta_D(a_0, x_1) = d_1$. Minden más $b \in B$, $x \in X$ párra legyen $\delta_D(b, x) = \delta_B(b, x)$. Továbbá minden $x \in X - x_{i+1}$ esetén $\delta_D(d_i, x) = \delta_B(a_0x_1 \ldots x_i, x)$ $(i = 1, 2, \ldots, m - 1)$.

Ha valamely $d \in D$, $x \in X$ párra $\delta_D(d,x)$ még nincs definiálva, akkor most is legyen $\delta_D(d,x) = c$. Világos, hogy a $\mathbf{D}$ automata jól definiált és $L+p$ felismerhető $\mathbf{D}$-ben az $F + d_m$ halmazzal. Ezért

$$r(L+p) \leq |F| + 1 < |L| + 1 = |L+p|$$

miatt $L+p$ reducibilis. □

12.3. Következmény. *Ha az X véges ábécé feletti L véges nyelv irreducibilis, akkor minden résznyelve is irreducibilis. Ha pedig L reducibilis és K tetszőleges X feletti véges nyelv, akkor az $L+K$ nyelv is reducibilis.*

12.4. Tétel. *Egy X véges ábécé feletti $L \neq \emptyset$ véges nyelv akkor és csak akkor irreducibilis, ha felismerhető*

$$L = p_1 + p_1p_2 + \cdots + p_1p_2 \ldots p_k \quad (1 \leq k) \tag{12.1}$$

alakban, ahol $p_1 \in X^*,\ p_2, \ldots, p_k \in X^+$.

Bizonyítás Ha a (12.1) alakú L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ automatában az F halmazzal, akkor

$$F = \{a_0p_1, a_0p_1p_2, \ldots, a_0p_1p_2 \ldots p_k\},$$

vagyis $r(L) = |F| = |L|$, azaz L irreducibilis.

Megfordítva, tegyük fel, hogy L véges irreducibilis nyelv X felett. Ha $|L| = 1$, akkor L nyilvánvalóan (12.1) alakú. Legyen $2 \leq |L|$. A 12.3 Következmény szerint L tetszőleges két különböző p és q szavára a $\{p,q\}$ nyelv is irreducibilis. Megmutatjuk, hogy p és q közül egyik prefixe a másiknak. Ha valamelyik szó az üres szó, akkor nyilvánvalóan igaz az állítás. Tegyük fel, hogy $p \neq e$ és $q \neq e$. Legyen $p = x_1x_2 \ldots x_m$ és $q = y_1y_2 \ldots y_n$, ahol $x_i, y_j \in X$, $(i = 1,2,\ldots,m, j = 1,2,\ldots,n, m \geq n)$.

Tegyük fel először, hogy q-nak van olyan $q_1 = y_1y_2 \ldots y_k$ $(1 \leq k < n)$ prefixe, amely p-nek is prefixe. Szerkesszük meg az $\mathbf{A} = (A, a_0, X, \delta)$ automatát a következő módon. Vegyük fel az $a_0, a_1, \ldots, a_m$ állapotokat úgy, hogy

$$\delta(a_0, x_1) = a_1,\ \delta(a_1, x_2) = a_2,\ \ldots,\ \delta(a_{m-1}, x_m) = a_m$$

teljesüljön. Ezek után vegyünk fel további $b_{k+1}, b_{k+2}, \ldots, b_{n-1}$ állapotokat és definiáljuk a

$$\delta(b_k,\ y_{k+1}) = b_{k+1},\ \delta(b_{k+1}, y_{k+2}) = b_{k+2},\ \ldots,\ \delta(b_{n-1}, y_n = a_m$$

átmeneteket. Végül legyen c az eddigiektől különböző állapot és

$$A = \{a_0, a_1, \ldots, a_m, b_{k+1}, b_{k+2}, \ldots, b_{n-1}, c\}.$$

Ha valamely $b \in A$, $x \in X$ párra $\delta(b, x)$ még nincs definiálva, akkor legyen $\delta(b, x) = c$. Világos, hogy **A** olyan iniciális automata, amelyben a $\{p, q\}$ nyelv felismerhető az $\{a_m\}$ egyelemű halmazzal. Ez azonban lehetetlen, mivel $\{p, q\}$ irreducibilis.

Tegyük fel most, hogy a p és q szavaknak nincs az üres szótól különböző közös prefixe. Az előbbi konstrukciót módosítsuk úgy, hogy az $a_0, a_1, \ldots, a_m$ állapotokban az automata működjön az előbb definiált módon. A

$$b_{k+1},\ b_{k+2},\ \ldots,\ b_{n-1}$$

állapotok helyett pedig vegyük fel a $d_1, d_2, \ldots, d_{n-1}$ állapotokat, amelyekre és a q szó betűire definiáljuk a

$$\delta(a_0, y_1) = d_1,\ \delta(d_1, y_2) = d_2,\ \ldots,\ \delta(d_{n-2}, y_{n-1}) = d_{n-1}, \delta(d_{n-1}, y_n) = a_m$$

átmeneteket. Az **A** automata ilyen módosításával olyan iniciális automatához jutunk, amelyben a $\{p, q\}$ nyelv felismerhető az egyelemű $\{a_m\}$ halmazzal. Ez szintén lehetetlen. Következésképpen, L tetszőleges két különböző szava közül az egyik a másiknak valódi prefixe, ahonnan már következik, hogy L (12.1) alakú. □

A következőkben azzal foglalkozunk, hogy egy véges L nyelv egy reguláris kifejezésének ismeretében hogyan határozhatjuk meg az $s(L)$ és $r(L)$ számokat. Világos, hogy $s(\emptyset) = 1$, $r(\emptyset) = 0$, s(e)=2 és $r(e) = 1$. Ezért a továbbiakban csak olyan véges nyelvekkel foglalkozunk, amelyek legalább egy nemüres szót tartalmaznak.

Mivel a véges nyelvek reguláris nyelvek, ezért megadhatók reguláris kifejezéssel is. Ha az X feletti L véges nyelv nem tartalmazza az üres szót, akkor megadható olyan α reguláris kifejezéssel, amelyben nincs iteráció. Ha pedig $e \in L$, akkor megadható egy $\alpha + \emptyset^*$ reguláris kifejezéssel, amelyben az α reguláris kifejezés nem tartalmaz iterációt. (Emlékeztetünk arra, hogy $\emptyset^* = e$.) Ha α-ra alkalmazzuk a reguláris kifejezésekre is érvényes

$$\beta\gamma + \beta\gamma' = \beta(\gamma + \gamma') \tag{12.2}$$

disztributív szabályt ameddig csak lehetséges, akkor a véges nyelvek un. *normál alakú reguláris kifejezés*ehez jutunk. Pontosabban a következőket mondhatjuk: (1) Minden $p \in X^*$ szó normál alakú reguláris kifejezés.

(2) Ha $p \in X^+$ és α normál alakú reguláris kifejezés, akkor $p(\alpha)$ is normál alakú reguláris kifejezés.
(3) Ha α és β normál alakú reguláris kifejezések és nincsenek olyan $\gamma, \gamma_1, \gamma_2$ reguláris kifejezések, amelyekre $\alpha = \gamma\gamma_1$, $\beta = \gamma\gamma_2$, akkor $\alpha + \beta$ is normál alakú reguláris kifejezés.
(4) Minden normál alakú reguláris kifejezés előáll (1)-(3) alatt megadott módon.

Felhívjuk a figyelmet arra, hogy egy α normál alakú reguláris kifejezésre $e\alpha$ nem normál alakú reguláris kifejezés.

12.5. Lemma. *Minden véges nyelvnek létezik normál alakú reguláris kifejezése, amely az összeadandók sorrendjétől eltekintve egyértelműen meghatározott.*

Bizonyítás Már említettük, hogy ha (12.2) disztributív szabályt addig alkalmazzuk, ameddig csak lehetséges, akkor bármely véges nyelv normál alakú reguláris kifejezéséhez jutunk.

Az egyértelműség bizonyítását a véges nyelv elemszáma szerint teljes indukcióval végezzük el. Az egyértelműség igaz minden egyelemű nyelvre. Tegyük fel, hogy a normál alakú reguláris kifejezés egyértelműsége (az összeadandók sorrendjétől eltekintve) minden X feletti $1 \leq n$ elemű nyelvre igaz. Legyen L tetszőleges $n+1$ elemű nyelv X felett. Akkor L előállítható $L = L' + p$ ($p \in X^+$) alakban, ahol L' X feletti n elemű nyelv. Legyen α' az L' nyelv normál alakú reguláris kifejezése. Az indukciós feltevés szerint α' az összeadandók sorrendjétől eltekintve egyértelműen meghatározott. Legyen $r \in X^*$ a leghosszabb olyan szó, amelyre valamilyen $q \in L'$ szóval $p = rp_1$ és $q = rq_1$. Akkor α'-ből L normál alakú reguláris kifejezéséhez jutunk p-nek α'-höz való hozzávételével. A p szó pozíciója ebben a normál alakban az r szó által az összeadandók sorrendjétől eltekintve egyértelműen meghatározott. □

12.6. Példa. *Az $X = \{x, y, z\}$ ábécé feletti*

$$L = x^2 + xy + xyz + yx^2 + y^2 + y^2z^2 + yz + yz^2 + zx^2 + zxy + zxyz$$

véges nyelv esetén (12.2) segítségével kapjuk L

$$L = x(x + y(e + z)) + y((x^2 + y(e + z^2) + z(e + z)) + zx(x + y(e + z))$$

normál alakú reguláris kifejezését.

Egy α normál alakú reguláris kifejezés valamely α' reguláris részkifejezését α *elágazásá*nak nevezzük, ha létezik olyan, legalább egy nemüres szót tartalmazó β kifejezés, hogy $\beta\alpha'$ összeadandó α-ban.

12.7. Példa. *A 12.6 Példában szereplő normál alakú reguláris kifejezés elágazásai:*

$$(x + y(e + z), e + z, x^2 + y(e + z^2) + z(e + z), x, e + z^2, x(x + y(e + z)).$$

Minden L véges nyelvhez hozzárendelhetünk egy γ reguláris kifejezést úgy, hogy vesszük az L nyelv α normál alakú reguláris kifejezésését és α-ból elhagyunk bizonyos elágazásokat úgy, hogy minden α-beli elágazásból pontosan egyet tartunk meg. Az α-ból így előálló γ kifejezést az L *nyelvhez tartozó reprezentációs alak*nak nevezzük. Megjegyezzük, hogy egy nyelvhez tartozó reprezentációs alak a nyelv által nincs egyértelműen meghatározva és nem feltétlenül az illető nyelvet állítja elő.

12.8. Példa. *Az*

$$x(x + y) + y(x^2 + y(e + z^2) + z(e + z)) + zx,$$

$$x(x + y(e + z)) + y(x^2 + y(e + z^2) + z) + zx,$$

$$x + y(x^2 + y(e + z^2) + z(e + z)) + zx(x + y),$$

$$x + y(x^2 + y(e + z^2) + z) + zx(x + y(e + z)),$$

reguláris kifejezések mindegyike 12.6 Példában szereplő normál alakú reguláris kifejezés egy reprezentációs alakja.

Definiáljuk ezután egy X ábécé feletti *véges nyelvet előállító reguláris kifejezés karakterisztikus szám*át:
(1) Az X ábécé betűinek és az e üres szónak a karakterisztikus száma 1.
(2) Ha $x \in X$ és $\alpha \neq e$ olyan reguláris kifejezés, amelynek karakterisztikus száma n, akkor az $x(\alpha)$ kifejezés karakterisztikus száma $n + 1$.
(3) Reguláris kifejezések összegének karakterisztikus száma megegyezik az összeadandók karakterisztikus számainak összegével.

Nem nehéz megmutatni, hogy egy L véges nyelvhez tartozó bármely két reprezentációs alak karakterisztikus száma megegyezik. Ezt a közös számot az L *nyelv karakterisztikus szám*ának nevezzük és rá a $c(L)$ jelölést használjuk. Ugyancsak egyszerűen látható, hogy az e üres szó az L-hez tartozó minden reprezentációs alakban ugyanannyiszor fordul elő. Jelölje ezt a közös számot $\epsilon(L)$.

12.9. Tétel. *Ha L X feletti (legalább egy nemüres szót tartalmazó) véges nyelv, akkor*

$$s(L) = c(L) + 3, \quad r(L) = \epsilon(L) + 1.$$

Bizonyítás A tétel nyilvánvalóan igaz abban az esetben, ha L egyetlen $p \in X^+$ szóból áll. Ekkor ugyanis L egyetlen reprezentációs alakja p, s így $c(L) = |p|-1$, $\epsilon(L) = 0$. Továbbá, mivel a p-hez tartozó utat leíró $a_1, a_2, \ldots, a_{|p|}$ állapotokhoz még egy kezdőállapotra és egy csapdára van szükség, amelybe minden nem p-hez tartozó út vezet, ezért $s(L) = |p| + 2$ és $r(L) = 1$.

Tegyük fel ezután, hogy a tétel igaz a (legalább egy nemüres szót tartalmazó) L véges nyelvre. Legyen $p \in X^+$ és tekintsük a pL nyelvet. Könnyen belátható, hogy

$$s(pL) = s(L) + |p|, \quad r(pL) = r(L), \quad c(pL) = c(L) + |p|, \quad \epsilon(pL) = \epsilon(L).$$

Ha ugyanis az L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ automatában az $F \subseteq A$ halmazzal, akkor a pL nyelv felismerhető abban $\mathbf{B} = (B, a_1, X, \delta')$ automatában az F halmazzal, amelyet úgy kapunk $\mathbf{A}$-ból, hogy még felvesszünk új $a_1, a_2, \ldots, a_{|p|-1}$ állapotokat és a p szóval az a_1 állapotból az a_0 állapotba vezető utat. Továbbá felveszünk meg egy c csapdát is. Természetesen $B = A \cup \{a_1, a_2, \ldots, a_{|p|-1}, c\}$. A δ' átmenetfüggvény az $A \times X$ halmazon egyezzen meg δ-val, minden más út vezessen a csapdába.

Tegyük fel végül, hogy a tételt már bebizonyítottuk olyan L és K (legalább egy nemüres szót tartalmazó) véges nyelvekre, amelyek olyan normál alakú α és β reguláris kifejezésekkel vannak megadva, hogy egyetlen α-beli α' és β-beli β' összeadandóhoz sincsenek olyan $\gamma, \gamma_1, \gamma_2$ reguláris kifejezések, amelyekre $\alpha' = \gamma\gamma_1$, $\beta' = \gamma\gamma_2$. Továbbá α-nak és β-nak nincs közös elágazása és $\alpha + \beta$ is normál alakú reguláris kifejezés. Ilyen feltételek mellett fennállnak az

$$r(L + K) = r(L) + r(K) - 1, \tag{12.3}$$

$$s(L + K) = s(L) + s(K) - 3 \tag{12.4}$$

összefüggések. Valóban (12.3) következik, abból, hogy ugyanaz a végállapot választható az olyan $p \in L+K$ szavakhoz, amelyek nem valódi prefixei egyetlen $L + K$-beli szónak sem. (A reprezentációs szám definíciója miatt az L és a K nyelveket legkisebb számú végállapottal felismerhető automatákban pontosan egy-egy ilyen végállapot van, s ezeket "egybeolvaszthatjuk".) Ebből következik a (12.4) egyenlőség is, felhasználva azt, hogy az L és K nyelveket legkisebb állapotszámmal felismerő automaták kezdő állapotait és csapdáit külön-külön "egybeolvaszthatjuk". Másrészt a definíciók alapján nyilvánvaló, hogy

$$c(L + K) = c(L) + c(K), \tag{12.5}$$

$$\epsilon(L + K) = \epsilon(L) + \epsilon(K) \tag{12.6}$$

A (12.3)-(12.6) egyenlőségekből már közvetlenül adódik, hogy a tétel az $L + K$ nyelvre is igaz.

Ha a tétel igaz valamilyen L véges nyelvre, nyilván igaz az $L + e$ nyelvre is. Ezzel igazoltuk a tételt minden olyan véges nyelvre, amely reprezentációs alakkal van megadva. Így, minthogy egy nyelv súlya és reprezentációs száma nem változik a normál alakról reprezentációs alakra való áttérés során, a tétel bizonyítását befejeztük. □

12.10. Példa. *A 12.6 Példában szereplő L véges nyelv 12.8 Példában megadott reprezentációs alakjaiból leolvasható, hogy $c(L) = 7$ és $\epsilon(L) = 2$. Így az előbbi tétel szerint $s(L) = 10$ és $r(L) = 3$. Ha felrajzoljuk az*

A	0	1	2	3	4	5	6	7	8	9
x	5	8	9	9	9	4	5	9	4	9
y	1	2	9	9	9	7	9	9	9	9
z	6	7	3	4	9	9	9	4	9	9.

automata átmenetgráfját, abból könnyen leolvasható, hogy L felismerhető a 0 *kezdőállapotból a* $\{2, 4, 7\}$ *halmazzal.*

12.2. Definit nyelvek

Azt mondjuk, hogy az X ábécé feletti L nyelv *k definit*, ha bármely legalább k hosszúságú $p \in X^*$ szó akkor és csak akkor eleme L-nek, ha a k hosszúságú szuffixe is eleme L-nek. Egy $L \subseteq X^*$ nyelvet *definit*nek nevezünk, ha k definit valamilyen k nemnegatív egész számra. Ha $k > 0$, akkor L-et *k-adfokban definit*nek nevezzük, ha k definit, de nem $(k-1)$ definit. Ezt a k számot az L nyelv *definitségi fokán*ak nevezzük és rá a $df(L)$ jelölést használjuk. Csak két X feletti 0-adfokban definit nyelv van, mégpedig $\emptyset$ és X^*. A definícióból adódik, hogy egy nyelv legfeljebb egy $k \in N$ számra k-adfokban definit.

Mivel a véges nyelvek mindig tekinthetők véges ábécé felett, ezért minden L véges nyelv definit nyelv. Ha $L \neq \emptyset$, akkor

$$df(L) = 1 + \max\{|p|; p \in L\}. \tag{12.7}$$

(Arról már beszéltünk, hogy $df(\emptyset) = 0$.) Könnyen belátható a

12.11. Lemma. *Egy $L \subseteq X^*$ nyelv akkor és csak akkor k definit, ha bármely olyan $p, q \in X^*$ szóra, amelyeknek megegyezik a k hosszúságú szuffixe, $p \in L$ akkor és csak akkor, ha $q \in L$.*

12.12. Következmény. *Ha $L \subseteq X^*$ k definit, akkor minden k-nál nagyobb l pozitív egész számra l definit is.*

12.13. Tétel. *Minden X véges ábécé feletti L definit nyelv előállítható*

$$L = L_1 + X^*L_2 \tag{12.8}$$

alakban, ahol L_1 és L_2 véges nyelvek és

$$\max\{|p|; p \in L_1 + L_2\} \leq df(L). \tag{12.9}$$

Megfordítva, minden (12.8) alakú nyelv definit és

$$df(L) \leq 1 + \max\{|p|; p \in L_1 + L_2\}. \tag{12.10}$$

Bizonyítás Legyen az $L \subseteq X^*$ nyelv k-adfokban definit. Ha $k = 0$, akkor $L = \emptyset$ vagy $L = X^*$. Mindkét esetben L (12.8) alakú, mégpedig az első esetben $L = \emptyset + X^*\emptyset$, a második esetben pedig $L = \emptyset + X^*e$. Mindkét esetben (12.9) is igaz.

Legyen ezután $k > 0$. Ha L véges, akkor $L = L + X^*\emptyset$ és (12.7) miatt (12.9) is igaz.

Tegyük fel, hogy L végtelen és legyenek

$$L_1 = \{p \in L; |p| < k\}, \quad L_2 = \{p \in L; |p| = k\}.$$

Mivel $df(L) = k$, ezért $X^*L_2 \subseteq L$ és így $L_1 + X^*L_2 \subseteq L$. A fordított irányú tartalmazás nyilvánvalóan fennáll, ezért $L = L_1 + X^*L_2$, ahol L_1 és L_2 véges nyelvek. Emellett világos, hogy a kapott felbontásra (12.9) is teljesül.

Megfordítva, tegyük fel, hogy az L nyelvre és a véges L_1, L_2 nyelvekre érvényes a (12.8) felbontás. Ha $L_i \neq \emptyset$, akkor legyen

$$k_i = \max\{|p|; p \in L_i\},$$

ha pedig $L_i = \emptyset$, akkor $k_i = 0$ $(i = 1, 2)$. Legyen továbbá

$$k = \max\{k_1 + 1, k_2\}.$$

Megmutatjuk, hogy L k definit. Tekintsünk e célból egy legalább k hosszúságú $p \in X^*$ szót és legyen $r \in X^*$ a p szó k hosszúságú szuffixe. Ha $p \in L$, akkor $k_1 < k$ miatt $p \notin L_1$. Így p előállítható $p = p_1p_2$ alakban, ahol $p_1 \in X^*$, $p_2 \in L_2$ és $|p_2| \leq k$. Ezért $r = p'p_2$ $(p' \in X^*)$, azaz $r \in X^*L_2 \subseteq L$. Tegyük most fel, hogy $r \in L$. Minthogy $|r| = k > k_1$, ezért $r \in X^*L_2$, s így előállítható $r = p'p_2$ $(p' \in X^*)$ alakban. Következésképpen

$$p = qr = qp'p_2 \in X^*L_2 \subseteq L.$$

A fentiek éppen azt jelentik, hogy L k definit, azaz definíció szerint L definit. Emellett a (12.10) egyenlőtlenség is teljesül. □

12.14. Következmény. *Az X véges ábécé feletti definit nyelvek halmaza zárt a halmazelméleti egyesítés, metszet és komplementerképzés műveletekre és ilyen L és K nyelvekre*

$$df(L+K) \leq \max\{df(L), df(K)\},$$
$$df(L \cap K) \leq \max\{df(L), df(K)\},$$
$$df(L) = df(\overline{L}).$$

Bizonyítás Legyen L az X véges ábécé feletti k-adfokban definit nyelv. Megmutatjuk, hogy $\overline{L}$ is k-adfokban definit. Mivel $\emptyset$ és X^* definit nyelvek egymás komplementerei és $df(\emptyset) = df(X^*) = 0$, ezért a továbbiakban feltehetjük, hogy $k > 0$. Ha L véges, akkor legyen $L_1 = L$ és $L_2 = \emptyset$. Ha pedig L végtelen, akkor legyen

$$L_1 = \{p \in L; |p| < k\}, \quad L_2 = \{p \in L; |p| = k\}.$$

A 12.13 Tétel bizonyításában láttuk, hogy $L = L_1 + X^*L_2$. Nem nehéz meggyőződni arról, hogy

$$\overline{L} = (\sum_{n=0}^{k-1} X^n - L_1) + X^*(X^k - L_2),$$

azaz $\overline{L}$ is definit. A definit nyelv definíciója szerint világos, hogy $df(L) = df(\overline{L})$.

Ha L és K az X véges ábécék feletti definit nyelvek, akkor a 12.13 Tétel szerint vannak olyan X feletti L_1, L_2, K_1, K_2 véges nyelvek, amelyekre $L = L_1 + X^*L_2$ és $K = K_1 + X^*K_2$. Így

$$L + K = (L_1 + X^*L_2) + (K_1 + X^*K_2) = (L_1 + K_1) + X^*(L_2 + K_2),$$

azaz a 12.13 Tétel alapján $L + K$ is definit és

$$df(L+K) \leq \max\{df(L), df(K)\}.$$

Mivel $L \cap K = \overline{\overline{L} + \overline{K}}$, ezért $L \cap K$ is definit és

$$df(L \cap K) \leq \max\{df(L), df(K)\}. \qquad \square$$

Véges ábécét feltételezve, (12.8)-ból következik, hogy a definit nyelvek reguláris nyelvek Boole algebrájának rész Boole algebrája. Kleene tétele szerint felismerhetők véges automatákban. A véges ábécé feletti definit nyelveket speciális véges automaták ismerik fel. Most azt vizsgáljuk meg, hogy ezek az automaták milyen típusúak.

Az $\mathbf{A} = (A, X, \delta)$ automatát k *definit*nek nevezzük, ha van olyan $k \in N$, hogy

$$\forall(p \in X^k)\ (|Ap| = 1). \tag{12.11}$$

Nem nehéz belátni, hogy ha $\mathbf{A}$ k definit, akkor $(k+1)$ definit is. Az $\mathbf{A}$ automatát *definit*nek mondjuk, ha k definit valamilyen $k \in N$ számra. A legkisebb ilyen k számot $\mathbf{A}$ *definitségi fok*ának nevezzük és $df(\mathbf{A})$-val jelöljük. Azt is mondjuk, hogy az $\mathbf{A}$ automata *k-adfokban definit*. Egy $\mathbf{A}$ automata tehát pontosan akkor k-adfokban definit, ha tetszőleges legalább k hosszúságú bemenő szó hatására $\mathbf{A}$ minden állapotból egy csak ettől a szótól függő állapotba megy át és van olyan $k-1$ hosszúságú bemenő szó, valamint $\mathbf{A}$-nak legalább két olyan állapota, hogy e két állapotból e szó hatására egymástól különböző állapotokba megy át.

Szemléletesen azt mondhatjuk, hogy ha egy $\mathbf{A} = (A, X, \delta)$ automata k-adfokban definit, akkor egy legalább k hosszúságú $p \in X^*$ szó hatására eljutva az ap állapotba, "nem emlékszik" a kiindulási $a \in A$ állapotra. Ezért a definit automatákat *véges memóriájú automaták*nak is nevezzük.

12.15. Tétel. *Ha az L nyelv felismerhető egy $\mathbf{A} = (A, a_0, X, \delta)$ véges definit automatában, akkor L definit nyelv és $df(L) \leq df(\mathbf{A})$. Megfordítva, ha egy L definit nyelv felismerhető egy $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában, amelyre $|A| = s(L)$ teljesül, akkor $\mathbf{A}$ definit automata és $df(\mathbf{A}) = df(L)$.*

Bizonyítás Tegyük fel, hogy az L nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges k-adfokban definit automatában az $F(\subseteq A)$ halmazzal. Legyen $|p| \geq k$, $p = p'q$ és $|q| = k$ $(p', q \in X^*)$. Mivel $\mathbf{A}$ k-adfokban definit, ezért $a_0p = (a_0p')q = a_0q$. Tehát $a_0p \in F$ akkor és csak akkor, ha $a_0q \in F$, azaz $p \in L$ akkor és csak akkor, ha $q \in L$. Ezzel megmutattuk, hogy L k definit. Amiből már következik, hogy $df(L) \leq df(\mathbf{A})$.

Megfordítva, tegyük fel, hogy az L k-adfokban definit nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában az $F(\subseteq A)$ halmazzal. Továbbá, tegyük fel, hogy $|A| = s(L)$, azaz az $\mathbf{A}$ automata állapotainak száma megegyezik az L nyelv súlyával. Ez azt jelenti, hogy $\mathbf{A}$ a legkevesebb állapottal rendelkező olyan automata, amelyben L felismerhető az állapothalmaz egy alkalmas F részhalmazával. Legyenek $a, b \in A$ tetszőleges állapotok. Mivel $|A| = s(L)$ miatt $\mathbf{A}$ nyilván iniciálisan összefüggő, ezért vannak olyan $p, q \in X^*$ bemenő szavak, amelyekre $a_0p = a$ és $a_0q = b$. Legyenek tetszőleges r legalább k hosszúságú szóra $a_1 = ar$ és $b_1 = br$. Mivel L k-adfokban definit, ezért bármely $r' \in X^*$ szóra $prr' \in L$ akkor és csak akkor, ha $qrr' \in L$, azaz $a_0prr' \in F$ akkor és csak akkor, ha $a_0qrr' \in F$, vagyis minden $r' \in X^*$ szóra $a_1r' \in F$ akkor és csak akkor, ha $b_1r' \in F$. De $|A| = s(L)$ miatt az $\mathbf{A}_F$ egyszerű, ezért $ar = a_1 = b_1 = br$. Ezzel megmutattuk, hogy az $\mathbf{A}$ automata k definit.

Megmutatjuk, hogy $\mathbf{A}$ k-adfokban definit. Ha $k = 0$, akkor készen vagyunk. Legyen a továbbiakban $k > 0$. Mivel L nem $(k-1)$ definit, ezért vannak olyan $p_1, p_2 \in X^*$ és $q \in X^{k-1}$ szavak, hogy $p_1q \in L$, de $p_2q \notin L$. Ez azt jelenti, hogy

$a_0p_1q \in F$ és $a_0p_2q \notin F$. Tehát az a_0p_1 és az a_0p_2 állapotokra $(a_0p_1)q \neq (a_0p_2)q$. Ezzel megmutattuk, hogy $\mathbf{A}$ nem $(k-1)$ definit, vagyis $df(\mathbf{A}) = df(L)$. □

12.16. Következmény. *Egy véges X ábécé feletti L nyelv akkor és csak akkor definit, ha az őt felismerő $\mathbf{A}_F$ egyszerű automata véges definit automata és $df(L) = df(\mathbf{A}_F)$.*

12.17. Tétel. *Ha egy k-adfokban definit nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges automatában, akkor $|A| \geq k+1$.*

Bizonyítás Tegyük fel, hogy az L k-adfokban definit nyelv felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ n állapotú véges automatában az $F(\subseteq A)$ halmazzal. Ha $k = 0$, akkor a tétel nyilván igaz.

Legyen ezért a továbbiakban $k > 0$, továbbá $X(i) = \{p \in X^*;\ |p| \leq i\}$. Tekintsük minden $i \in N$ számra A-n azt a ρ_i ekvivalenciát, amelyre tetszőleges $a, b \in A$ állapotpár esetén

$$(a,b) \in \rho_i \quad \Longleftrightarrow \quad (\forall p \in X(i))(ap \in F \iff bp \in F).$$

Nyilvánvaló, hogy $\rho_{i+1} \subseteq \rho_i$ $(i \in N)$. Ha m_i jelöli a ρ_i-osztályok számát, akkor $1 \leq m_i \leq m_{i+1} \leq n$. Megmutatjuk, hogy az $i = 0, 1, \ldots, k-1$ indexekre $m_i < m_{i+1}$.

Minthogy L nem $(k-1)$ definit, ezért vannak olyan $p_1, p_2 \in X^*$ szavak és olyan $q = x_1x_2\ldots x_{k-1} \in X^{k-1}$ szó, hogy $p_1q \in L$, de $p_2q \notin L$. Legyen $i \in \{0, 1, \ldots, k-1\}$ tetszőleges és q_i a q i hosszúságú prefixe, továbbá $q = q_ir$ $(r \in X^*)$. Akkor

$$(a_0p_1q_i)r = a_0p_1q \in L, \quad (a_0p_2q_i)r = a_0p_2q \notin L$$

adódik és így $|r| = k - i - 1$ miatt

$$\rho_{k-i-1}[a_0p_1q_i] \neq \rho_{k-i-1}[a_0p_2q_i].$$

Legyen most p' tetszőleges olyan bemenő szó, amelyre $|p'| \geq k - i$ fennáll. Akkor, mivel L k-adfokban definit,

$$p_1q_ip' \in L \quad \Longleftrightarrow \quad p_2q_ip' \in L$$

és így

$$(a_0p_1q_i)p' \in F \quad \Longleftrightarrow \quad (a_0p_2q_i)p' \in F,$$

azaz

$$\rho_{k-i}[a_0p_1q_i] = \rho_{k-i}[a_0p_2q_i].$$

De i tetszőleges 0 és $k-1$ közé eső egész szám volt, következésképpen

$$1 \leq m_1 < m_2 < \cdots < m_k \leq n,$$

ahonnan már $|A| = n \geq k+1$ adódik. □

12.18. Tétel. *Létezik olyan algoritmus, amely segítségével eldönthető, hogy egy véges ábécé feletti reguláris nyelv definit vagy nem definit.*

Bizonyítás Legyen L reguláris nyelv az X véges ábécé felett. Feltehető, hogy $L \neq \emptyset, X^*$, mivel $\emptyset$ és X^* definit nyelvek X felett. Például a Kleene tétel bizonyításából kapható algoritmus alkalmazásával megszerkeszthető olyan $\mathbf{A} = (A, a_0, X, \delta)$ iniciálisan összefüggő véges automata, amelyben L felismerhető valamely $\emptyset \subset F \subset A$) halmazzal. Legyen $|A| = n$ és tetszőleges $i \in N$ számra κ_i az az ekvivalencia A-n, amelyet tetszőleges $a, b \in A$ állapotpárra

$$(a, b) \in \kappa_i \iff (\forall p \in X^i)(ap \in F \iff bp \in F) \tag{12.12}$$

által definiálunk. Eszerint a κ_0-osztályok F és $A - F$. A definícióból világos, hogy

$$(a, b) \in \kappa_{i+1} \iff (\forall x \in X)(\delta(a, x), \delta(b, x)) \in \kappa_i), \tag{12.13}$$

ami $\mathbf{A}$ végessége miatt lehetővé teszi a κ_i-osztályok meghatározását. Nem nehéz belátni, hogy L akkor és csak akkor k definit, ha $\kappa_k = \omega_A$, azaz az univerzális reláció és

$$df(L) = \min\{k; \kappa_k = \omega_A\}.$$

Ha pedig $\kappa_{n-1} \neq \omega_A$, akkor a 12.17 Tétel alapján azt kapjuk, hogy L nem definit. □

12.19. Példa. *Tekintsük $X = \{x, y\}$ ábécé feletti*

$$L = xyx + (x + y)^*(x^2 + y)$$

negyedfokban definit nyelvet. Ha az L nyelvre a Kleene tétel bizonyításából kapható algoritmust alkalmazzuk, akkor az

$\mathbf{A}$	a_0	a_1	a_2	a_3	a_4	a_5	a_6
x	a_1	a_3	a_5	a_3	a_6	a_3	a_3
y	a_2	a_4	a_2	a_2	a_2	a_2	a_2

átmenettáblázattal megadott automatához jutunk, amelyben L felismerhető az a_0 kezdőállapotból az

$$F = \{a_2, a_3, a_4, a_6\}$$

halmazzal. (Ez könnyen belátható, ha például felrajzoljuk az automata átmenet gráfját.)

A 12.18 Tétel bizonyítása során megadott algoritmus felhasználásával megmutatjuk, hogy $\mathbf{A} = (A, a_0, X, \delta)$ *definit automata. Adjuk meg a (12.12) feltétellel definiált* κ_i*-osztályokat a (12.13) öszefüggést is felhasználva:*

$$\kappa_0 - \textit{osztályok}: \quad \{a_0, a_1, a_5\},\ \{a_2, a_3, a_4, a_6\},$$

$$\kappa_1 - \textit{osztályok}: \quad \{a_0, a_2\},\ \{a_1, a_3, a_4, a_5, a_6\},$$

$$\kappa_2 - \textit{osztályok}: \quad \{a_0, a_2, a_3, a_4, a_5, a_6\},\ \{a_1\},$$

$$\kappa_3 - \textit{osztályok}: \quad \{a_0\},\ \{a_1, a_2, a_3, a_4, a_5, a_6\},$$

$$\kappa_4 - \textit{osztály}: \quad \{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}.$$

Ez azt jelenti, hogy az $\mathbf{A}$ *automata negyedfokban definit.*

Ha most az $\mathbf{A}_F$ *felismerő automatát minimalizáljuk az Aufenkamp–Hohn algoritmussal, akkor négy lépés után a*

$$b_0 = \{a_0\},\ b_1 = \{a_1\},\ b_2 = \{a_2\},\ b_3 = \{a_5\},\ b_4 = \{a_3, a_4, a_6\}$$

jelölések mellett a

$\mathbf{B}$	b_0	b_1	b_2	b_3	b_4
x	b_1	b_4	b_3	b_4	b_4
y	b_2	b_4	b_2	b_2	b_2

egyszerű automatához jutunk, amely az L *nyelvet a* b_0 *kezdőállapotból a* $\{b_2, b_4\}$ *halmazzal állítja elő.*

12.3. Nilpotens nyelvek

Az alfejezetben a véges nyelvek egy természetes általánosításával foglalkozunk. Egy X ábécé feletti L nyelvet *nilpotens*nek nevezünk, ha vagy maga, vagy komplementere véges. Kleene tétele szerint a nilpotens nyelvek felismerhetők véges automatákban. A véges nyelvek definit nyelvek, ezért a 12.14 Következményből adódik a

12.20. Következmény. *Az* X *véges ábécé feletti nilpotens nyelvek az* X *feletti nyelvek Boole algebrájának valódi rész Boole algebrája a halmazelméleti egyesítés, metszet és komplementerképzés műveletekre.*

Bizonyítás A véges nyelvek definit nyelvek, ezért a 12.14 Következményből közvetlenül kapjuk, hogy az X véges ábécé feletti nilpotens nyelvek az X feletti definit nyelvek Boole algebrájának rész Boole algebrája.

Legyen most $X = \{x, y\}$ és $L = x + X^*y$. Az L nyelv másodfokban definit, de L-lel együtt

$$\overline{L} = e + X^*(xx + yx)$$

is végtelen, ezért nem nilpotens. □

Az $\mathbf{A} = (A, X, \delta)$ automatát k *nilpotens*nek nevezzük, ha van olyan $k \in N$ és $c \in A$, hogy

$$\forall(a \in A, p \in X^k)\ (ap = c). \tag{12.14}$$

Ha az $\mathbf{A}$ automata k nilpotens, akkor nyilvánvalóan $(k+1)$ nilpotens is. Az $\mathbf{A}$ automatát *nilpotens*nek mondjuk, ha k nilpotens valamilyen $k \in N$ számra. A legkisebb ilyen k számot $\mathbf{A}$ *nilpotenciafokán*ak nevezzük. Azt is mondjuk, hogy az $\mathbf{A}$ automata *k-adfokban nilpotens*. Nem nehéz belátni, hogy c az automata egyetlen csapdája. A definícióból látható, hogy minden nilpotens automata definit.

12.21. Tétel. *Egy X véges ábécé feletti L nyelv akkor és csak akkor nilpotens, ha felismerhető véges nilpotens automatában.*

Bizonyítás Legyen L olyan nyelv, amely felismerhető az $\mathbf{A} = (A, a_0, X, \delta)$ véges k-adfokban nilpotens automatában az $F(\subseteq A)$ halmazzal. Legyen c az $\mathbf{A}$ automata csapdája. Ha $c \in F$, akkor tetszőleges p legalább k hosszúságú szóra $a_0p \in F$. Ebből következik, hogy ha $p \notin L$, akkor $|p| < k$. Ez azt jelenti, hogy L komplementere véges, azaz L nilpotens. Ha $c \notin F$, akkor $p \in X^*$ szóra $a_0p \in F$ esetén $|p| < k$, amiből következik, hogy L véges és így nilpotens.

Megfordítva, legyen L nilpotens nyelv a véges X ábécé felett. Tegyük fel először, hogy L véges és legyen $k = 1 + \max\{|p|; p \in L\}$. Tekintsük az $\mathbf{A} = (A, a_0, X, \delta)$ automatát, ahol a_0 tetszőleges szimbólum.

$$A' = \{a_0p; |p| < k, p \in X^+\},$$

c egy további szimbólum és $A = A' \cup \{a_0, c\}$. A δ átmenetfüggvényt definiáljuk a következőképpen. Tetszőleges $a \in A$, $x \in X$ párra $a = a_0p$, $|p| < k-1$ esetekben legyen $\delta(a_0p, x) = a_0px$, $|p| = k-1$ esetekben pedig $\delta(a_0p, x) = c$, s végül $a = c$ esetben $\delta(a, x) = c$. Világos, hogy $\mathbf{A}$ olyan véges nilpotens automata, amelyben L felismerhető az $F = \{a_0p; p \in L\}$ halmazzal.

Legyen most L komplementere véges. Szerkesszük meg az előbbi automatát L helyett L komplementerével. Az így kapott $\mathbf{A}$ véges nilpotens automatában L felismerhető az $A - F$ halmazzal. □

12.4. Iterációmentes nyelvek

Egy X ábécé feletti nyelvet *iterációmentes nyelv*nek vagy *csillagmentes nyelv*nek nevezünk, ha előállítható az X elemeiből, az e üres szóból és az $\emptyset$ üres nyelvből a Boole műveletek és a konkatenáció véges (nem nulla) számú alkalmazásával. Az $\emptyset$ üres nyelvet és az e üres szót is iterációmentesnek tekintjük. Ezek szerint minden véges nyelv és így minden elemi nyelv iterációmentes. Ha az X ábécé feletti L és K nyelv iterációmentes, akkor $L + K$, $L \cap K$, LK és $\overline{L}$ is iterációmentes. Tetszőleges X ábécé esetén X^* is iterációmentes, minthogy $X^* = \overline{\emptyset}$.

Ha X véges ábécé, akkor X is iterációmentes, ezért e kifejezhető X elemeibő és az $\emptyset$ üres nyelvből a Boole műveletek és a konkatenáció véges (nem nulla) számú alkalmazásával:

$$e = \overline{X^+} = \overline{X^*X} = \overline{\overline{\emptyset}X}.$$

Így véges X ábécé esetén az iterációmentes nyelveket elegendő az $\emptyset$ üres nyelv és az $x \in X$ elemi nyelvek segítségével definiálni. A 8.6 Tételt is felhasználva kapjuk, hogy az X véges ábécé feletti iterációmentes nyelvek halmaza az X feletti reguláris nyelveknek az a legszűkebb részhalmaza, amely zárt a Boole műveletekre és a konkatenációra, de nem zárt az iterációra.

Az 1.1. alfejezetben a reguláris nyelvekre bevezettük a a reguláris kifejezés fogalmát. Hasonlóan minden X ábécé feletti iterációmentes nyelvhez hozzárendelhetünk egy ún. (X *feletti*) *iterációmentes kifejezés*t az alábbi módon: Egy L nyelv iterációmentes kifejezésén értsünk olyan kifejezést, amely azt mutatja meg, hogyan állítható elő az L nyelv az X elemeiből, az e üres szóból és az $\emptyset$ üres nyelvből a Boole műveletek és a konkatenáció véges (nem nulla) számú alkalmazásával. Az $\emptyset$ üres nyelv, az e üres szó és az $x \in X$ elemi nyelv iterációmentes kifejezése legyen az $\emptyset$, az e ill. az x szimbólum.

Mivel nem vezet ellentmondásra, a reguláris nyelvekhez és reguláris kifejezésekhez hasonlóan, az iterációmentes nyelv és egy iterációmentes kifejezése közé egyenlőség jelet teszünk.

12.22. Példa. *Az* $\{a, b\}$ *ábécé feletti* $(ab)^*$ *nyelv iterációmentes.*

Nem nehéz ugyanis belátni, hogy

$$(ab)^* = \overline{b\overline{\emptyset} + \overline{\emptyset}a + \overline{\emptyset}aa\overline{\emptyset} + \overline{\emptyset}bb\overline{\emptyset}}.$$

A 12.13 Tételből következik, hogy véges ábécé felett minden definit, s így minden nilpotens nyelv is iterációmentes.

Szükségünk lesz néhány félcsoportelméleti fogalomra és tételre. Egy félcsoport *részmonoidján* [*részcsoportján*] a félcsoport olyan részfélcsoportját értjük,

amelyik monoid [csoport]. Így nyilvánvaló, hogy félcsoport egy részmonoidjának egységeleme a félcsoport egy idempotens eleme. A következő jól ismert félcsoportelméleti tételt nem bizonyítjuk.

12.23. Tétel. *Az S véges félcsoport bármely $s \in S$ eleméhez vannak olyan k és n pozitív egész számok, amelyekre $s, \ldots, s^k, \ldots, s^{k+n-1}$ különböző elemek és $s^{k+n} = s^k$. Továbbá $\{s^k, \ldots, s^{k+n-1}\}$ az S félcsoport n-edrendű ciklikus részcsoportja.*

A k számot, az $s \in S$ elem *index*ének, n-et pedig s *periódus*ának nevezzük.

Az S véges félcsoportot *aperiodikus*nak nevezzük, ha minden részcsoportja egyelemű. Nem nehéz meggondolni, hogy ez pontosan azt jelenti, hogy a félcsoport minden elemének periódusa 1.

12.24. Lemma. *Az S véges félcsoport akkor és csak akkor aperiodikus, ha van olyan k_S pozitív egész szám, hogy minden $s \in S$ elemre $s^{k_S+1} = s^{k_S}$.*

Bizonyítás Ha S aperiodikus és $s \in S$, akkor 12.23 Tétel szerint s periódusa 1. Ha k_S legalább akkora, mint S elemei indexének szuprémuma, akkor minden $s \in S$ elemre $s^{k_S+1} = s^{k_S}$.

Megfordítva, legyen a k_S pozitív egész szám olyan, hogy minden $s \in S$ elemre $s^{k_S+1} = s^{k_S}$. Legyen G az S véges félcsoport egy részcsoportja és e_G G egységeleme. Ha s a G részcsoport tetszőleges eleme, akkor

$$s^{k_S} s = s^{k_S+1} = s^{k_S} = s^{k_S} e_G \in G,$$

amiből $s = e_G$, azaz $G = \{e_G\}$. □

12.25. Lemma. *Minden véges ábécé feletti iterációmentes nyelv szintaktikus félcsoportja aperiodikus.*

Bizonyítás Emlékeztetünk arra, hogy egy X ábécé feletti L nyelvre (7.5)-ben definiáltuk a ϑ_L *szintaktikus kongruenciát*. Az X^*/ϑ_L faktorfélcsoportot pedig az L nyelv *szintaktikus félcsoport*jának neveztük.

Nem nehéx belátni, hogy az $\emptyset$, az e és az $x \in X$ nyelvek szintaktikus félcsopotja aperiodikus.

Így elegendő megmutatni, hogy az X ábécé feletti K és L nyelvek szintaktikus félcsoportja aperiodikus, akkor a $K + L$, a KL, a $K \cap L$ és a $\overline{K}$ nyelvek szintaktikus félcsoportja is aperiodikus. Ehhez legyenek n_K, n_L pozitív egész számok olyanok, amelyekre minden $p \in X^*$ szó esetén $(p^{n_K}, p^{n_K+1}) \in \vartheta_K$ és $(p^{n_L}, p^{n_L+1}) \in \vartheta_L$. Ha $m = \sup\{n_k, n_L\}$, akkor minden $p \in X^*$ szóra

$$(p^m, p^{m+1}) \in \vartheta_{K+L} \quad \text{és} \quad (p^{n_K+n_L}, p^{n_K+n_L+1}) \in \vartheta_{KL},$$

amiből következik, hogy $K + L$ és KL szintaktikus félcsoportja aperiodikus.

Minthogy $\vartheta_K = \vartheta_{\overline{K}}$, ezért $\overline{K}$ szintaktikus félcsoportja egyenlő K szintaktikus félcsoportjával, amely a feltétel miatt aperiodikus.

Továbbá $K \cap L = \overline{\overline{K} + \overline{L}}$ miatt $L \cap L$ szintaktikus félcsoportja is aperiodikus. □

Véges ábécé feletti reguláris nyelvekre a 12.25 Lemma megfordítása is igaz. Ennek bizonyításához azonban lényegesen több félcsoportelméleti előkészítés szükséges.

12.26. Lemma. *Az M aperiodikus monoid bármely s, r és t elemére*

$$srt = r \quad \Longrightarrow \quad sr = r = rt. \tag{12.15}$$

Bizonyítás Ha $srt = r$, akkor minden k pozitív egész számra $s^k r t^k = r$. Ha k legalább akkora, mint r indexe, akkor $s^{k+1} r t^k = r$. Innen $r = s(s^k r t^k) = sr$. Hasonlóan mutatható meg, hogy $r = rt$. □

Az aperiodikus monoidok (12.15) tulajdonságát *kancellatív tulajdonság*nak nevezzük.

12.27. Lemma. *Az M monoid tetszőleges s elemére*

$$W(s) = \{r \in M;\ s \notin MrM\} \tag{12.16}$$

(a halmazelméti tartalmazásra) az M monoid legnagyobb olyan ideálja, amelynek nem eleme s.

Bizonyítás Tegyük fel, hogy $W(s) = \emptyset$. Megmutatjuk, hogy s M bármely $I \neq \emptyset$ ideáljának eleme. Ha $r \in I$, akkor $MrM \subseteq I$, s így ha $s \notin MrM$, akkor $r \in W(s)$. Ellentmondás. Tehát $s \in MrM \subseteq I$.

Tegyük fel most, hogy $W(s) \neq \emptyset$. Megmutatjuk, hogy $W(s)$ M ideálja. Legyen $r \in W(s)$ és $t \in M$. Ha $s \in MrtM$, akkor $s \in MrtM \subseteq MrM$, ami ellentmond $W(s)$ definíciójának. Így $s \notin MrtM$, azaz $rt \in W(s)$. Hasonlóan látható be, hogy $tr \in W(s)$. Ez azt jelenti, hogy $W(s)$ M ideálja.

Legyen végül I M olyan ideálja, amelynek s nem eleme. Ha $r \in I$, akkor $MrM \subseteq I$. Mivel $s \notin I$, ezért $s \notin MrM$, azaz $r \in W(s)$, vagyis $I \subseteq W(s)$. kaptuk, hogy $W(s)$ M legnagyobb s-et nem tartalmazó ideálja. □

12.28. Lemma. *Az M aperiodikus monoid bármely s elemére*

$$s = (sM \cap Ms) - W(s). \tag{12.17}$$

Bizonyítás A (12.16) definíció szerint $s \notin W(s)$. Mivel $s \in sM \cap Ms$, ezért $s \in (sM \cap Ms) - W(s)$.

Tegyük fel, hogy $r \in (sM \cap Ms) - W(s)$. Akkor $r = sp = qs$ és $s = urv$ valamilyen $p, q, u, v \in M$ elemekre. Ebből $s = urv = (uq)sv$. A (12.15) kancellatív tulajdonság miatt $s = uqs = sv$. Így $s = ur = usp$. Ismét a kancellatív tulajdonság szerint $s = us = sp$, azaz $s = r$. □

12.29. Lemma. *Legyen az M aperiodikus monoid egységeleme e_M. Az M monoid s elemére $|MsM| = |M|$ akkor és csak akkor, ha $s = e_M$.*

Bizonyítás Ha $s = e_M$, akkor nyilvánvalóan $M = M^2 = Me_MM$. Tegyük fel, hogy valamely $s \in M$ elemre $|MsM| = |M|$. Az M monoid végessége miatt $MsM = M$. Így vannak olyan $p, q \in M$ elemek, hogy $e_M = psq = (ps)e_Mq$. A (12.15)kancellatív tulajdonság szerint $e_M = (ps)e_M = e_Mq$. Amiből $e_M = ps = q$. De $e_M = pe_Ms$, s így szintén a kancellatív tulajdonság alapján $e_M = p = s$□

12.30. Lemma. *Ha φ a véges X ábécé feletti X^* szabad monoid monoid-homomorfizmusa az M aperiodikus monoidra, akkor $\varphi^{-1}(e_M)$ iterációmentes nyelv X felett.*

Bizonyítás Legyen $W = \{x \in X;\ \varphi(x) \neq e_M\}$. Megmutatjuk, hogy

$$\varphi^{-1}(e_M) = X^* - X^*WX^*,$$

amiből nyilvánvalóan adódik, hogy $\varphi^{-1}(e_M)$ iterációmentes.

Legyen $x \in W$ és $u, v \in X^*$. Tegyük fel, hogy $\varphi(uxv) = e_M$, s így

$$e_M = \varphi(u)\varphi(x)e_M\varphi(v),$$

amiből a 12.26 Lemma szerint

$$e_M = \varphi(u)\varphi(x) = \varphi(v).$$

Most a 12.26 Lemmát az $e_M = \varphi(u)e_M\varphi(x)$ egyenletre alkalmazva, $e_M = \varphi(x)$ adódik, ami ellentmond W definíciójának. Vagyis $e_M \notin \varphi(X^*WX^*)$.

Legyen most $p \in X^* - X^*WX^*$. Tegyük fel, hogy $\varphi(p) \neq e_M$. Akkor $p \in X^+$, azaz vannak olyan $x_1, \ldots, x_j \in X$ betűk, amelyekre $p = x_1 \ldots x_j$. Mivel $\varphi(p) \neq e_M$, ezért van olyan x_i $(1 \leq i \leq j)$, hogy $\varphi(x_i) \neq e_M$. Ez azt jelenti, hogy $x_i \in W$ és így $p \in X^*WX^*$, ami szintén ellentmondás. Ezzel megmutattuk, hogy $X^* - X^*WX^* = \varphi^{-1}(e_M)$. □

A célunk eléréséhez szükségünk van a következő technikai jellegű lemmára.

12.31. Lemma. *Ha X véges ábécé és φ X^* monoid-homomorfizmusa az M aperiodikus monoidra és $m \in M - e_M$, akkor az alábbi három feltétel mindegyikéből $|MnM| > |MnM|$ következik.*

$$n\varphi(x)M = Mm, \quad n \notin mM \quad (x \in X,\ n \in M); \tag{12.18}$$

$$M\varphi(x)n = mM, \quad n \notin Mm \quad (x \in X,\ n \in M); \tag{12.19}$$

$$m \in M\varphi(x)nM \cap Mn\varphi(y)M, \quad m \notin M\varphi(x)n\varphi(y)M), \tag{12.20}$$

ahol $x, y \in X$ és $n \in M$.

Bizonyítás Megmutatjuk, hogy a (12.18) feltételből $|MnM| > |MnM|$ következik. $MmM = M\varphi(x)nM \subseteq MnM$, azaz $|MmM| \leq |MnM|$. Tegyük fel, hogy $MmM = MnM$. Ebből az következik, hogy $n = umv$ valamilyen $u, v \in M$ elemekre. Mivel $m \in n\varphi(x)M$, így olyan $p \in M$ is van, hogy $m = np$, azaz $n = umv = un(pv)$. A 12.26 Lemma szerint $n = un = npv$, amiből $n = npv = mv \in mM$. Ez azonban lehetetlen. Akkor $MmM \subset MnM$, azaz M végessége miatt $|MmM| < |MnM|$.

Hasonlóan mutatható meg, hogy a (12.19) feltételből $|MnM| > |MnM|$ következik.

Végül megmutathatjuk, hogy a (12.20) feltételből is $|MnM| > |MnM|$ következik. Ebben az esetben is nyilvánvaló, hogy $|MmM| \leq |MnM|$. Tegyük fel most is, hogy $MmM = MnM$. Így most is vannak olyan $u, v \in M$ elemek, hogy $n = umv$. A feltételekből az is következik, hogy

$$m = r\varphi(x)ns = pn\varphi(y)t \quad (p, r, s, t \in M),$$

amiből

$$n = umv = u(r\varphi(x)ns)v = (ur\varphi(x))n(sv).$$

A 12.26 Lemmát felhasználva kapjuk, hogy $n = ur\varphi(x)n$. De

$$m = pn\varphi(y)t = p(ur\varphi(x)n)\varphi(y)t = (pur)\varphi(x)n\varphi(y)t,$$

ami ellentétes a feltételeinkkel. Ebből itt is azt kapjuk, hogy $|MmM| < |MnM|$. □

A (12.18), a (12.19) és a (12.20) feltételek alapján definiáljuk X^* következő részhalmazait.

Legyen V_1 $[V_2]$ a $\varphi^{-1}(n)x$ $[x\varphi^{-1}(n)]$ halmazok egyesítése, ahol

$$n \in M, x \in X\ n\varphi(x)M = mM, n \notin mM\ [M\varphi(x)n = Mm, n \notin Mm]$$

Valamint legyen W az $\{x \in X;\ m \notin M\varphi(x)M\}$ halmaz és azon $x\varphi^{-1}(n)y$ halmazok egyesítése, amelyekre

$$n \in M,\ x, y \in X,\ m \in M\varphi(x)nM \cap Mn\varphi(y)M,\ m \notin M\varphi(x)n\varphi(y)M.$$

12.32. Lemma. *Legyen X tetszőleges véges ábécé. Ha φ az X^* szabad monoid monoid-homomorfizmusa az M aperiodikus monoidra és $m \in M - e_M$, akkor*

$$\varphi^{-1}(m) = (V_1X^* \cap X^*V_2) - X^*WX^*.$$

Bizonyítás Először megmutatjuk, hogy

$$\varphi^{-1}(m) \subseteq (V_1X^* \cap X^*V_2) - X^*WX^*.$$

Legyen $w \in \varphi^{-1}(m)$, azaz $\varphi(w) = m$.

Tegyük fel, hogy u a legrövidebb prefixe w-nek, amelyre $\varphi(u)M = mM$. Ha $u = e$, akkor $M = mM$, azaz van olyan $p \in M$, hogy $mp = e_M$. Akkor a (12.15) kancellatív tulajdonság szerint $m = e_M$. Ez azonban lehetetlen, így $u \notin e$. Ha $u = rx$ $n = \varphi(r)$, ahol $r \in X^*$ és $X \in U$, akkor

$$mM = \varphi(u)M = \varphi(r)\varphi(x)M = n\varphi(x)M.$$

Tegyük fel, hogy $n \in mM$. Akkor $n = mp$ valamely $p \in M$ elemre. Így

$$\varphi(r)M = mpM \subseteq mM$$

és

$$mM = \varphi(u)M = \varphi(r)\varphi(x)M \subseteq \varphi(r)M,$$

amiből $\varphi(r)M = mM$. Ez ellentmond u választásának, ezért $n \notin mM$. Ebből következik, hogy $w \in V_1X^*$. Hasonlóan látható be, hogy $w \in X^*V_2$.

Megmutatjuk, hogy $w \notin X^*WX^*$. Ha $q \in W$, akkor $q = x,\ m \notin M\varphi(x)M$ vagy $\varphi(q) = \varphi(x)n\varphi(y),\ m \notin M\varphi(x)n\varphi(y)M$. Mindkét esetben $m \notin M\varphi(p)M$. Ha $w \in X^*WX^*$, akkor $w = uqv$ valamilyen $q \in W$ és $u, v \in X^*$ szavakra, amiből

$$m = \varphi(w) = \varphi(u)\varphi(q)\varphi(v) \in M\varphi(q)M,$$

ami ellentmondás, így $w \notin X^*WX^*$.

Ezzel megmutattuk, hogy

$$\varphi^{-1}(m) \subseteq (V_1X^* \cap X^*V_2) - X^*WX^*.$$

Másodszor megmutatjuk, hogy

$$(V_1X^* \cap X^*V_2) - X^*WX^* \subseteq \varphi^{-1}(m).$$

Ehhez legyen $w \in V_1X^*V_2) - X^*WX^*$ és $n = \varphi(w)$.

A 12.28 Lemma segítségével megmutatjuk, hogy $n = m$, azaz $w \in \varphi^{-1}(m)$, ami az állításunkat igazolja.

Minthogy $w \in V_1X^*$, ezért $w = uv \quad (u \in V_1, v \in X^*)$. Így $\varphi(u) = n\varphi(x)$, ahol $n\varphi(x)M = mM$, ezért

$$n = \varphi(w) = \varphi(u)\varphi(v) = n]\varphi(x)\varphi(v) \in mM.$$

Mivel $w \in X^*V_2$ is teljesül, hasonló módon kapjuk, hogy $n \in Mm$. Ezért $n \in mM \cap Mm$.

A 12.28 Lemma szerint csak azt kell még igazolnunk, hogy $m \in MnM$. Indirekt bizonyítást végzünk. Tegyük fel, hogy $m \notin MnM = M\varphi(w)M$. Legyen $w = uzv$ $(u, z, v \in X^*)$, ahol z a legkisebb hoszúságú olyan szó, hogy $m \notin M\varphi(z)M$. Mivel, $M = M^2$, ezért nyilvánvalóan $z \neq e$. Tegyük fel, hogy $z \in X$. De $m \notin M\varphi(z)M$, ezért $z \in W$, amiből következik, hogy $w \in X^*WX^*$. Ez azonban lehetetlen, így $2 \leq |z|$. Legyen $z = xry$, ahol $x, y \in X$ és $r \in X^*$. A z választása miatt $m \in M\varphi(x)\varphi(r)M$. Hasonlóan $m \in M\varphi(r)\varphi(y)M$. Ebből következik, hogy $z \in W$, ami lehetetlen, vagyis $m \in MnM$. Ez viszont azt jelenti, hogy $n \notin W(m)$. A 12.28 Lemma szerint $n = m$. □

A fentebb ismertetett félcsoportelméleti eredmények segítségével bizonyítjuk be a 12.25 Lemma megfordítását:

12.33. Lemma. *Ha az X véges ábécé feletti L reguláris nyelv szintaktikus félcsoportja aperiodikus, akkor L iterációmentes.*

Bizonyítás Legyen φ az X^* szabad monoid természetes homomorfizmusa az $M(L) = X^*/\vartheta_L$ szintaktikus monoidra. A 7.3 Lemma szerint L ϑ_L osztályok egyesítése, azaz van olyan $P \subseteq M(L)$, amelyre

$$L = \sum_{m \in P} \varphi^{-1}(m).$$

Ezért elegendő megmutatni, hogy minden $m \in P$ esetén $\varphi^{-1}(m)$ iterációmentes. A 12.30 Lemma szerint $\varphi^{-1}(e_{M(L)})$ iterációmentes. Legyen $m \in P$. Tegyük fel, hogy minden olyan $n \in P$ esetén, amelyre $|MnM| > |MmM|$, $\varphi^{-1}(n)$ iterációmentes. Akkor a 12.31 és a 12.32 Lemmákból következik, hogy $\varphi^{-1}(m)$ iterációmentes. □

A 12.25 és a 12.33 Lemmák alapján kimondjuk a reguláris nyelvek elméletének egyik legszebb tételét:

12.34. Tétel. *(Schützenberger tétele) Véges ábécé feletti reguláris nyelv akkor és csak akkor iterációmentes, ha szintaktikus félcsoportja aperiodikus.*

Az alfejezetben MARK V. LAWSON [31] munkájára is támaszkodtunk. Schützenberger tételének egy másik, a Krohn–Rhodes tétel felhasználásával történő bizonyítása megtalálható például FÜLÖP ZOLTÁN [18] elektronikus egyetemi jegyzetében. A Krohn–Rhodes tétellel részletesen foglalkozunk a [2] elektronikus egyetemi jegyzetünkben.

12.35. Példa. *Az $\{a, b\}$ ábécé feletti a^*b^* reguláris nyelv iterációmentes.*

Ha ugyanis $2 \leq n$, akkor minden $u, v, t \in \{a, b\}^*$ szóra

$$u, v \in a^* \text{ és } t \in a^*b^* \quad \Longrightarrow \quad uv^n t \in a^*b^*;$$

$$u \in a^* \; v \in a^*b^* \text{ és } t \in b^* \quad \Longrightarrow \quad uv^n t \notin a^*b^*;$$

$$u \in a^*b^* \text{ és } v, t \in b^* \quad \Longrightarrow \quad uv^n t \in a^*b^*,$$

ezért a 12.24 Lemma szerint a^*b^* szintaktikus félcsoportja aperiodikus, azaz Schützenberger tétele szerint a^*b^* iterációmentes. (A $2 \leq n$ feltétel szükséges, mert $n = 1$ esetben például $a(ab)b = a^2b^2 \in a^*b^*$, de $a((ab)^2)b = a^2bab^2 \notin a^*b^*$.)

12.5. Kommutatív nyelvek

Egy X ábécé feletti L nyelvet *kommutatív nyelv*nek nevezünk, ha valahányszor

$$x_1x_2 \ldots x_n \in L \quad (x_1, x_2, \ldots, x_n \in X),$$

mindannyisszor

$$x_{\pi(1)}x_{\pi(2)} \ldots x_{\pi(n)} \in L$$

az $\{1, 2, \ldots, n\}$ halmaz bármely π permutációjára. Eszerint $\emptyset, e, x$ $(x \in X)$, X^+ és X^* kommutatív nyelvek.

Az $\mathbf{A} = (A, X, \delta)$ automatát *kommutatív*nak nevezzük, ha bármely $a \in A$ állapotra és $x, z \in X$ bemenő jelekre

$$\delta(\delta(a, x), z) = \delta(\delta(a, z), x) \tag{12.21}$$

teljesül. A (12.21) egyenletet $axz = azx$ alakban is írhatjuk. Kommutatív automata homomorf képei is kommutatívak. Nem nehéz belátni a következő lemmát.

12.36. Lemma. *Ha az $\mathbf{A}$ automata kommutatív, $x_1, \ldots, x_k$ pedig az X bemenő halmaz tetszőleges elemei, akkor bármely $a \in A$ állapotra és az $1, \ldots, k$ indexek bármely π permutációjára*

$$ax_1 \ldots x_k = ax_{\pi(1)} \ldots x_{\pi(k)}.$$

12.37. Következmény. *Az* **A** *automata akkor és csak akkor kommutatív, ha karakterisztikus félcsoportja kommutatív.*

12.38. Tétel. *Egy nyelv akkor és csak akkor kommutatív, ha felismerhető kommutatív automatában.*

Bizonyítás A 12.36 Lemma alapján nyilvánvaló, hogy minden kommutatív automatában felismerhető nyelv kommutatív.

Megfordítva, legyen L kommutatív nyelv X felett. Tekintsük X^*-on azt a ρ_c relációt, amelyre $(p, q) \in \rho_c$ akkor és csak akkor, ha q előállítható a p szó betűinek valamilyen permutációjaként. Világos, hogy ρ_c kongruencia X^*-on és L bizonyos ρ_c-osztályok egyesítése. Tekintsük azt az

$$\mathbf{X}^*/\rho_c = (X^*/\rho_c, \rho_c[e], X, \delta_{\rho_c})$$

iniciálisan összefüggő kommutatív automatát, amelyre minden $p \in X^*$ és $x \in X$ esetén $\delta_{\rho_c}(\rho_c[p], x) = \rho_c[px]$. Nyilvánvaló, hogy az automata a $F = \{\rho_c[p];\ p \in L\}$ halmazzal felismeri L-et. □

A 12.38 Tétel és Kleene tétele szerint pontosan a kommutatív reguláris nyelvek állíthatók elő a véges kommutatív automatákban.

Egy X ábécé feletti L *nyelv kommutatív lezártján* vagy *kommutatív burkán* azt az $\hat{L}$ nyelvet értjük, amely azokból és csak azokból a szavakból áll, amelyek előállíthatók valamely L-beli szó betűinek permutálásával. Világos, hogy $L \subseteq \hat{L}$ és $\hat{L}$ a legszűkebb olyan kommutatív nyelv, amely L-et tartalmazza. Nyilvánvaló továbbá, hogy L akkor és csak akkor kommutatív, ha $L = \hat{L}$.

A következő példa mutatja, hogy egy véges X ábécé feletti reguláris nyelv kommutatív lezártja nem szükségképpen reguláris.

12.39. Példa. *Az $X = \{x, y\}$ ábécé feletti $L = (xy)^*$ reguláris nyelv $\hat{L}$ kommutatív lezártja pontosan azokat a szavakat tartalmazza, amelyekben egyenlő számú x és y van. A 8.9 Tétel bizonyításából következik, hogy $\hat{L}$ nem reguláris.*

A következőkben szükséges és elégséges feltételt adunk arra, hogy egy nyelv kommutatív lezártja mikor reguláris.

Legyen X véges ábécé és tekintsük az X^* szabad monoidon a 12.38 Tétel bizonyításában definiált ρ_c kongruenciát. Az X^*/ρ_c faktorfélcsoportot az (X *által generált*) *kommutatív szabad monoid*nak nevezzük. Legyen $\mathcal{C}(X)$ az X^*/ρ_c kommutatív szabad monoid részhalmazainak halmaza, azaz X^*/ρ_c mint ábécé feletti nyelvek halmaza. $\mathcal{C}(X)$ halmazt a reguláris műveletekkel együtt

(X *feletti*) *kommutatív nyelvalgebrá*nak nevezzük. Jelölje $\mathcal{CR}(X)$ a $\mathcal{C}(X)$ kommutatív nyelvalgebra reguláris nyelveinek halmazát. Legyen $\mathcal{L}(X)$ az X feletti nyelvek halmaza és tekintsük azt a $\varphi : \mathcal{C}(X) \to \mathcal{L}(X)$ leképezést, amelyre

$$\varphi(K) = \sum_{\rho_c[p] \in K} \rho_c[p].$$

(Ebből következik, hogy $\varphi(\emptyset) = \emptyset$.) Világos, hogy egy X feletti L nyelv akkor és csak akkor kommutatív, ha van olyan $K \in \mathcal{C}(X)$, hogy $L = \varphi(K)$.

Tetszőleges $L \in \mathcal{L}(X)$ nyelvre legyen

$$L_c = \{\rho_c[p]; p \in L\}. \tag{12.22}$$

Világos, hogy tetszőleges $K \in \mathcal{C}(X)$ nyelvre $(\varphi^{-1}(K)_c = K$ és tetszőleges $L, L' \in \mathcal{L}(X)$ nyelvekre

$$\hat{L} = \hat{L'} \quad \Longleftrightarrow \quad L_c = {L'}_c. \tag{12.23}$$

Legyen $X = \{x_1, x_2, \ldots, x_n\}$. Egy $K \in \mathcal{C}(X)$ nyelvet *normális*nak mondunk, ha megadható a $\mathcal{C}(X)$-beli

$$\rho_c[e], \rho_c[x_1], \rho_c[x_2], \ldots, \rho_c[x_n]$$

egyelemű nyelvekből és e nyelvek hatványainak iteráltjaiból a $\mathcal{C}(\mathcal{X})$-ben definiált összeadás és szorzás véges számú alkalmazásával. Minden ilyen előállítást a K *normális nyelv egy normális kifejezés*ének nevezünk.

12.40. Tétel. *Egy véges X ábécé feletti L nyelv $\hat{L}$ kommutatív lezártja akkor és csak akkor reguláris, ha az L_c nyelv normális.*

Bizonyítás Tegyük fel, hogy az $X = \{x_1, x_2, \ldots, x_n\}$ ábécé feletti L nyelv $\hat{L}$ kommutatív lezártja reguláris. Kleene tétele szerint van olyan $\mathbf{A} = (A, a_0, X, \delta)$ véges automata, amely valamely $F(\subseteq A)$ halmazzal felismeri az $\hat{L}$ nyelvet. Jelölje L' azt az X feletti nyelvet, amely azokból és csak azokból az

$$x_1{}^{k_1} x_2{}^{k_2} \ldots x_n{}^{k_n} \quad (k_1, k_2, \ldots, k_n \in N)$$

alakú szavakból áll, amelyek hatására $\mathbf{A}$ az a_0 kezdőállapotból F-beli állapotba megy át. (Bármely $x \in X$ esetén $x^0 = e$.) Könnyen látható, hogy $\hat{L} = \hat{L'}$ és így (12.17) miatt $L_c = {L'}_c$. Minthogy ${L'}_c$ normális, ezért L_c ugyancsak normális $\mathcal{C}(X)$-beli nyelv.

Megfordítva, tegyük fel, hogy az L nyelvre L_c normális. Akkor a normalitás definíciója szerint L_c előállítható $L_c = \sum_{i=1}^{r} K_r$ véges összeg alakjában, ahol

$$K_i = ((\rho_c[x_1])^{k_1})^* (\rho_c[x_1])^{m_1} ((\rho_c[x_2])^{k_2})^* (\rho_c[x_2])^{m_2} \ldots ((\rho_c[x_n])^{k_n})^* (\rho_c[x_n])^{m_n}$$

és

$$k_1, k_2, \ldots, k_n, m_1, m_2, \ldots, m_n \in N.$$

Mivel $\hat{L} = \sum_{i=1}^{k} \varphi^{-1}(K_i)$, ezért $L_1 \hat{+} L_2 = \hat{L_1} + \hat{L_2}$ $(L_1, L_2 \in \mathcal{L}(X))$ miatt elegendő megmutatni, hogy az

$$((x_1)^{k_1})^*(x_1)^{m_1}((x_2)^{k_2})^*(x_2)^{m_2} \ldots ((x_n)^{k_n})^*(x_n)^{m_n} \tag{12.24}$$

nyelv kommutatív lezártja reguláris, vagyis Kleene tétele szerint felismerhető véges automatában.

Legyen e célból minden $i \in \{1, 2, \ldots, n\}$ esetén

$$A_i = \{0, 1, \ldots, k_i + m_i - l_i\},$$

ahol $l_i = 0$, ha $k_i = 0$ és $l_i = 1$, ha $k_i > 0$.

Szerkesszük meg az $\mathbf{A} = (A, a_0, X, \delta)$ automatát úgy, hogy legyen

$$A = (A_1 \times A_2 \times \cdots \times A_n) \cup \{d\},$$

ahol d egy új szimbólum, legyen $a_0 = (0, 0, \ldots, 0)$. A δ átmenetfüggvényt definiáljuk oly módon, hogy minden $x_i \in X$ esetén $\delta(d, x_i) = d$ teljesüljön. Tetszőleges

$$a = (a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$$

esetén pedig legyen

$$\delta(a, x_i) = (a_1, \ldots, a_{i-1}, a_i + 1, a_{i+1}, \ldots, a_n),$$

ha $a_i < k_i + m_i - l_i$,

$$\delta(a, x_i) = (a_1, \ldots, a_{i-1}, m_i, a_{i+1}, \ldots, a_n),$$

ha $a_i = k_i + m_i - l_i$ és $k_i > 0$, valamint

$$\delta(a, x_i) = d,$$

ha $a_i = m_i$ és $k_i = 0$.

Nem nehéz belátni, hogy a (12.18) alatti nyelv kommutatív lezártja felismerhető az $\mathbf{A}$ automatában az egyelemű $\{(m_1, m_2, \ldots, m_n)\}$ halmazzal. □

12.6. A primitív szavak nyelve

Röviden foglalkozunk a nyelvek és kódok algebrai elméletének egy, a jelenlegi kutatások előterében lévő területéről. (A kódok algebrai elméletével a következő részben foglalkozunk.)

Legyen X tetszőleges ábécé. Egy $p \in X^+$ szót *primitív*nek nevezünk, ha a $p = q^n$ $(q \in X^+)$ feltételből $n = 1$ és így $p = q$ következik. A primitív szavak elméletét részletesen tárgyalja DÖMÖSI PÁL, HORVÁTH SÁNDOR és MASAMI ITO [11] monográfiája.

Jelölje $Q(X)$ az X^+ szabad félcsoport primitív szavainak halmazát. A *nemprimitív szavak* halmaza $\overline{Q}(X) = X^* - Q(X)$. Nyilvánvaló, hogy minden $p \in X^*$ szóhoz van olyan $q \in Q(X)$ primitív szó, amelyre $p = q^n$. Megmutatjuk, hogy minden $p \in X^*$ szóhoz egyetlen ilyen q primitív szó tartozik. Ehhez először néhány lemmát bizonyítunk be. Ezt a primitív szót p *gyök*ének nevezzük, és $\sqrt{p}$-vel jelöljük. Nyilvánvaló, hogy $Q(X)$ megegyezik a $Q^{-1}(X)$ tükörképével, azaz (az 1.1. alfejezetben definiált) palindrom.

12.41. Lemma. *Ha $p \in X^+$ és $q, r \in X^*$ szavakra $pq = qr$, akkor vannak olyan $u, v \in X^*$ szavak, amelyekre $p = uv$, $q = (uv)^k u$ $(k \in N)$ és $r = vu$.*

Bizonyítás Ha $|q| \leq |p|$, akkor $p = qw$ és $r = wq$ valamilyen $w \in X^*$ szóra, és így az állítás igaz $u = q$, $v = w$ és $k = 0$ esetre.

Ha $|q| = |p| + 1$, akkor van olyan $u \in X$, hogy $q = pu$, így

$$pq = qr \quad \Longrightarrow \quad p^2u = pur \quad \Longrightarrow \quad pu = ur,$$

amiből következik, hogy van olyan $v \in X^*$, amelyre $p = uv$, ezért $r = vu$ és $q = uvu$. Ha $|p| < |q|$, akkor $q = pw$ $(w \in X^+)$, ezért $pw = wr$. Mivel $p \neq e$ és $|w| < |q|$, ebből $|q|$ szerinti teljes indukcióval adódik az állítás. □

12.42. Lemma. *Ha a $p, q \in X^+$ szavakra $pq = qp$, akkor van olyan $r \in X^+$ és vannak olyan i, j pozitív egész számok, amelyekre $p = r^i$ és $q = r^j$.*

Bizonyítás A bizonyítást pq hossza szerinti teljes indukcióval végezzük el. Az állítás nyilvánvalóan igaz $|pq| = 2$ esetben. Tegyük fel, hogy az állítás igaz $2 \leq |pq| \leq n$ esetekben. Legyen $|pq| = n + 1$. Akkor az előző lemma szerint vannak olyan $u, v \in X^*$ szavak, és van olyan $k \in N$, hogy $p = uv = vu$ és $q = (uv)^k u$. Ha $u = e$ vagy $v = e$, akkor az állítás triviálisan teljesül. Ezért feltehető, hogy $u \neq e$ és $v \neq e$. (A $p \neq e$ feltétel miatt $u = v = e$ nem lehetséges.) Mivel $|uv| \leq n$, az indukciós feltevés szerint van olyan $r \in X^+$, amelyre $u = r^i$ és $v = r^j$ $(i, j \in N)$. Amiből $p = r^{i+j}$ és $q = r^{(k+1)i+kj}$. □

12.43. Lemma. *Ha a $p, q \in X^+$ szavaknak vannak olyan p^i és q^j pozitív egész kitevős hatványai, amelyeknek van $|p| + |q|$ hosszúságú közös prefixe, akkor van olyan $r \in X^+$, hogy $p = r^m$ és $q = r^n$ $(m, n \in N_+)$.*

Bizonyítás A feltételből következik, hogy a qp^m és a q^{n+1} szavaknak van $|p| + 2|q|$ hosszúságú közös prefixe, amiből kapjuk, hogy a qp^m és a q^n szavaknak van $|p| + |q|$ hosszúságú közös prefixe. Hasonlóan kapjuk, hogy a pq^n és a p^m szavaknak van $|p| + |q|$ hosszúságú közös prefixe. Így a qp^m és a pq^n szavaknak van $|p| + |q|$ hosszúságú közös prefixe, azaz $pq = qp$. Ezek után az állítás következik az előző lemmából. □

12.44. Lemma. *Ha a $p, q \in X^+$ szavakra $p^i = q^j$ valamilyen i, j pozitív egész számra, akkor van olyan $r \in X^+$, hogy $p = r^m$ és $q = r^n$ $(m, n \in N_+)$.*

Bizonyítás Ha $i = 1$ vagy $j = 1$, akkor az állítás nyilvánvaló. Ha $1 < i, j$, akkor $|p| + |q| < |p^i| + |q^j|$, s így az állítás az előző lemmából következik. □

12.45. Tétel. *Bármely $p \in X^+$ szóhoz egyetlen olyan $q \in Q(X)$ primitív szó és egyetlen olyan n pozitív egész szám létezik, amelyre $p = q^n$.*

Bizonyítás A bizonyítást p hossza szerinti teljes indukcióval végezzük el. Az állítás $|p| = 1$ esetben nyilvánvalóan igaz.

Tegyük fel, hogy az állítás $1 \leq |p| \leq n$ esetekben igaz. Legyen $|p| = n + 1$. Ha p primitív, akkor definíció szerint igaz az állítás. Tegyük fel, hogy p nem primitiv, akkor van olyan $q \in X^+$ szó és olyan $2 \leq n$ egész szám, hogy $|q| < |p|$ és $p = q^n$. Az indukciós feltevés miatt létezik olyan $r \in Q(X)$ és olyan $1 \leq m$ egész szám, hogy $q = r^m$, azaz $p = r^{mn}$.

Az egyértelműség az előző lemmából következik. □

Mint már az alfejezet elején említettük, bármely $p \in X^+$ esetén azt a 12.45 Tétel szerint egyetlen $q \in Q(X)$ primitív szót, amelyre $p = q^n$ teljesül *p gyökének* nevezzük és $\sqrt{p}$-vel jelöljük, n-et pedig, ami a tétel szerint szintén egyértelmű, *p fokának* nevezzük és $\deg p$-vel jelöljük. A következő tétel fontos szerepet játszik a primitív szavak elméletében.

12.46. Tétel. *Az $uv \in X^+$ szó esetén $uv = p^i$ valamely $p \in Q(X)$ primitív szóra akkor és csak akkor, ha $vu = q^i$ valamely $q \in Q(X)$ primitív szóra. Speciálisan, uv akkor és csak akkor primitív, ha vu is primitív.*

Bizonyítás A szimmetria miatt elegendő a tételt egyik irányban bizonyítani. Először tegyük fel, hogy $i = 1$, azaz $uv = p$ primitív szó. Ha vu nem primitív,

akkor a 12.45 Tétel szerint $vu = q^j$ valamely $q \in Q(X)$ primitív szóra és $2 \leq j$. Van olyan $r \in X^+$ és $t \in X^*$, hogy $v = (rt)^n r,\ u = t(rt)^m$. Innen

$$uv = (tr)^{n+m+1} = (tr)^j,$$

azaz uv nem primitív. Ellentmondás. Tehát, ha uv primitív, akkor vu is primitív.

Most legyen $uv = p^i \quad (2 \leq i)$. Akkor van olyan $r \in X^+$ és $t \in X^*$, hogy $u = (rt)^m r,\ v = t(rt)^n$, ahol $m + n = i - 1$ és $rt = p$. Mivel $p = rt$ primitív, ezért az előzőek szerint $q = tr$ is primitív és

$$vu = (tr)^i = q^i. \qquad \square$$

Egy $L \subseteq X^*$ *nyelv gyökén* ill. *fokán* a következő halmazokat értjük:

$$\sqrt{L} = \{\sqrt{p};\ p \in L - e\}, \quad \deg L = \{\deg p;\ p \in L - e\}.$$

Nyilvánvaló, hogy $\sqrt{X^*} = \sqrt{X^+} = Q(X)$ és $\deg X^* = \deg X^+ = N_+$.

Mint beszéltünk arról, hogy a legegyszerűbben kezelhető nyelvek a reguláris nyelvek. A következő tétel segítségével megmutatjuk, hogy a véges X ábécé feletti primitív szavak $Q(X)$ nyelve sajnos nem reguláris. Azt nem nehéz belátni, hogy $Q(X)$ rekurzív nyelv, s ezért mondatszerkezetű nyelv. Az is belátható, hogy $Q(X)$ környezetfüggő, de nincs eldöntve az a kérdés, hogy környezetfüggetlen-e? Dömösi Pál, Horváth Sándor és Masami Ito azt sejtik, hogy nem környezetfüggetlen. Nevezzük ezt az 1991-ben közölt sejtést *DHI sejtés*nek. (L. pl. [11] monográfiában.)

Annak bizonyítására, hogy $Q(X)$ nem reguláris szükségünk van az alábbi eredményekre, amelyek közül a következőt bizonyítás nélkül mondjuk ki, a bizonyítás hosszadalmassága miatt. A bizonyítás megtalálható például a [41] munkában.

12.47. Tétel. *Ha $p, q, r \in X^* \quad (r \neq e)$ szavakra $p^k q^m = r^n \quad (2 \leq k, m, n)$, akkor van olyan $u \in X^+$, amelynek mind a három szó hatványa.*

A tételből nyilvánvalóan adódik a

12.48. Következmény. *Ha $p, q \in Q(X)$ $(p \neq q)$, akkor $p^i q^j \in Q(X)$ minden $2 \leq i, j$ egész szám esetén.*

A $i = 1$ vagy $j = 1$ esetekre a 12.48 Következmény nem teljesül. Például, ha $p = xyx$ és $q = yxxy \quad (x, y \in X)$, akkor $p^2 q = (xyxxy)^2 \notin Q(X)$.

12.49. Következmény. *Ha $p, q \in Q(X)$ $(p \neq q)$, akkor minden i pozitív egész számra a $p^i q^*$ és a $p^* q^i$ nyelvek mindegyike legfeljebb két nemprimitív szót tartalmaz.*

Bizonyítás Tegyük fel, hogy a p^iq^* nyelvben vannak nemprimitív szavak. Legyen p^iq^j ezek közül a legrövidebb hosszúságú. Akkor $p^iq^j = r^k$, ahol $r \in Q(X)$ és $k \geq 2$. Legyen szintén $p^iq^l = s^m$, $s \in Q(X)$ és $m \geq 2$. Ezért $s^m = r^kq^{l-j}$. A 12.47 Tételből következik, hogy $l - l = 1$. Ami azt jelenti, hogy a p^iq^* nyelvben legfeljebb p^iq^j és p^iq^{j+1} nemprimitív. A p^*q^i nyelv esetén a bizonyítás hasonlóan történik. □

12.50. Tétel. *Ha az X véges ábécé feletti L nyelv véges sok primitív szót (esetleg egyet sem) tartalmaz és $\sqrt{L}$ végtelen, akkor L nem reguláris.*

Bizonyítás Tegyük fel, hogy a feltételek teljesülése mellett L mégis reguláris. Legyen m az L-ben lévő primitív szavak hosszának a maximuma.(Ha L-ben nincs primitív szó, akkor $m = 0$.)

A 8.8 (pumpáló) Lemma szerint van olyan (L-től függő) n pozitív egész szám, hogy ha $p \in L$ és $|p| \geq n$, akkor p előállítható $p = uvw$ $(u, v, w \in X^*)$ alakban, ahol $0 < |v| \leq |uv| \leq n$, és minden k nemnegatív egész számra $uv^kw \in L$. Legyen $p \in L$ olyan, hogy $|\sqrt{p}| > n$ és $|p| > m$. Akkor $p = uvw$, amelyre

$$1 \leq |v| \leq |uv| \leq n, \quad w \neq e$$

és $uv^kw \in L$ minden k nemnegatív egész számra. A 12.46 Tétel szerint wuv^k minden k pozitív egész számra nemprimitiv, mivel $|uv^kw| \geq |p| > m$. Legyen $q = \sqrt{wu}$, $i = \deg wu$ és $r = \sqrt{v}$. A 12.46 Tétel szerint $q \neq r$, mert különben

$$|\sqrt{p}| = |\sqrt{wuv}| = |\sqrt{v}| \leq |v| \leq n,$$

ami ellentmond a $|\sqrt{p}| > n$ feltételnek. Így végtelen sok nemprimitív szót kapunk a q^ir^* nyelvben, ami ellentmond 12.49 Következménynek. Kaptuk, hogy L nem lehet reguláris. □

A 12.50 Lemma második feltétele egyelemű $X = \{x\}$ ábécére nyilvánvalóan nem teljesül, mivel bármely X feletti L nyelvre $\sqrt{L} = x$.

12.51. Következmény. *Az X legalább kételemű véges ábécé feletti primitív szavak $Q(X)$ nyelve nem reguláris.*

Bizonyítás A $Q(X)$ nyelv $\overline{Q}(X)$ komplementerében nincs primitív szó és $\sqrt{\overline{Q}(X)} = Q(X)$ végtelen, ezért a 12.50 Tétel szerint $\overline{Q}(X)$ nem reguláris, s így $Q(X)$ sem reguláris. □

Megmutatjuk, hogy véges X ábécé feletti $Q^n(X)$ nyelvek minden $2 \leq n$ egész számra viszont regulárisak. Ehhez először bebizonyítunk két lemmát. Ez az eredmény legalább kételemű véges ábécé esetén érdekes. Ha ugyanis $X = \{x\}$, akkor minden n nemnegatív egész számra $Q^n(X) = x^n$ nyilvánvalóan reguláris.

12.52. Lemma. *Ha $p \in X^+$ és $p \notin x^+$ $(x \in X)$, akkor a xp [px] és a p szavak közül egyik szükségképpen primitív.*

Bizonyítás Tegyük fel, hogy

$$xp = q^n \ [px = q^n] \quad \text{és} \quad p = r^m \ (q, r \in Q(X), 2 \leq m, n).$$

Akkor a q^n és az r^m szavaknak van közös prefixe, továbbá

$$|q| + |r| = \frac{|p|+1}{n} + \frac{|p|}{m} = |p| \left(\frac{1}{n} + \frac{1}{m} \right) + \frac{1}{n} < |p| + 1,$$

ezért $|q| + |r| \leq |p|$. A 12.43 Lemma szerint q és r egy közös szó hatványai. Mivel primitívek, ezért $q = r$, azaz $xp = q^n$ [$px = q^n$] és $p = q^m$, ami lehetetlen. Így px [xp] és p közül az egyik szükségképpen primitív. □

12.53. Lemma. *Ha $p \in X^+$ és minden $x \in X$ esetén $p \notin x^+$, akkor $p \in Q^2(X)$.*

Bizonyítás Ha $p \in X^+$ és $p \notin x^+$ minden $x \in X$ betűre, akkor vannak olyan $y, z \in X$ $(y \neq z)$, hogy $p = y^i z^j q$ valamilyen i, j pozitív egész számokra és olyan $q \in X^*$ szóra, amelynek első betűje nem egyenlő z-vel. Ha $q = e$, akkor nem nehéz belátni, hogy a lemma állítása igaz.

Ha $q \neq e$, akkor két esetet különböztetünk meg. Először legyen $j \geq 2$. Mivel $q \neq z^+$, ezért a 12.52 Lemma szerint q vagy zq primitív. De

$$p = (y^i z^j)q = (y^i z^{j-1})(zq),$$

ahol $y^i z^j$ és q vagy $y^i z^{j-1}$ és zq primitívek.

Másodszor legyen $j = 1$, továbbá $q = xr$ $(x \in X, \ r \in X^*)$. Ha $r = e$, akkor $p = (y^i z)x$ és $y^i z, x \in Q(X)$. Ha $r \neq e$, akkor $r = x^m$ $(1 \leq m)$ vagy $r \notin x^+$. Ha $r = x^m$ $(1 \leq m)$, akkor

$$p = y^i zq = y^i zxr = (y^i zx^m)x,$$

ahol $y^i zx^m$ és x primitívek. Ha $r \neq x^+$, akkor ismét a 12.52 Lemma szerint r vagy xr primitív és

$$p = y^i zq = y^i zxr = (y^i zx) = (y^i z)(xr).$$

Mivel $y^i z, y^i zx \in Q(X)$, ezért ebben az esetben is igaz a tétel állítása. □

12.54. Tétel. *Ha $X = \{x_1, x_2, \ldots, x_k\}$ $(2 \leq k)$, akkor minden $2 \leq n$ egész számra $Q^n(X)$ reguláris.*

Bizonyítás A 12.53 Lemma szerint

$$Q^2(X) = [(\sum_i x_i)^+ - \sum_i x_i^+] + \sum_i x_i^2.$$

A 8.6 Tétel szerint ebből következik, hogy $Q^2(X)$ reguláris.

A 12.53 Lemma alapján nem nehéz belátni, hogy

$$Q^3(X) = \overline{\sum_{i,j} x_i^* x_j^*} + \sum_{i \neq j} (x_i^+ x_j^+ - x_i x_j) + \sum_i x_i^3.$$

Szintén a 8.6 Tételből következik, hogy $Q^3(X)$ is reguláris.

Bármely $4 \leq n$ egész számra $Q^n(X)$ a $Q^2(X)$ és a $Q^3(X)$ nyelvek valamilyen véges sok tényezős szorzata, ezért $Q^n(X)$ $(4 \leq n)$ is reguláris. □

A 12.51 Következmény szerint a legalább kételemű X véges ábécé feletti primitív szavak $Q(X)$ nyelve nem reguláris. A formális nyelvek, speciálisan a III. részben tárgyalt kódok szempontjából érdekes azonban az a kérdés, hogy egy reguláris nyelv mennyi primitív szót tartalmaz. Az alfejezet végén automaták segítségével ezt a kérdést vizsgáljuk.

Tegyük fel, hogy a legalább kételemű X véges ábécé feletti L reguláris nyelvet felismeri az $\mathbf{A} = (A, X, a_0, \delta, F)$ véges automata. Feltehetjük, hogy $2 \leq |A|$. (Az $|A| = 1$ eset érdektelen, mert ebben az esetben $L(\mathbf{A}) = X^*$ és $Q(X) \subset X^*$.) A 7.1. alfejezetben megbeszéltük, hogy elegendő iniciálisan összefüggő felismerő automatákat tekinteni.

Az $\mathbf{A} = (A, a_0, X, \delta, F$ (nem szükségképpen véges) automatát *terminálisan összefüggő*nek nevezzük, ha minden $a \in A$ állapotához van olyan $p \in X^*$ bemenő szó, amelyre $ap \in F$, azaz végállapot.

12.55. Tétel. *Legyen az* $\mathbf{A} = (A, X, a_0, \delta, F)$ *iniciálisan összefüggő automata véges,* $2 \leq |X|$ *és* $2 \leq n = |A|$. *Ha* $\mathbf{A}$ *terminálisan összefüggő, akkor*

$$|L(\mathbf{A}) \cap Q(X)| = \infty$$

és létezik olyan $q \in L(\mathbf{A}) \cap Q(X)$, *amelyre* $n \leq |q| \leq 2n - 1$.

Bizonyítás Legyenek $x, y \in X$ és $x \neq y$. Nem nehéz belátni, hogy minden i pozitív egész szám esetén van olyan $p_i \in X^*$, hogy $|p_i| \leq n - 1$ és $a_0 x^i y p_i \in F$. Ha $n - 1 \leq i$, akkor $x^i y p_i \in Q(X)$. Valamint, ha $i \neq j$, akkor $x^i y p_i \neq x^j y p_j$. Ez azt jelenti, hogy $|L(\mathbf{A}) \cap Q(X)| = \infty$. Továbbá $x^{n-1} y p_{n-1} \in L(\mathbf{A}) \cap Q(X)$ és $n \leq |x^{n-1} y p_{n-1}| \leq 2n - 1$. □

12.56. Lemma. *Ha $u, v \in X^+$ nem hatványai ugyanannak a szónak, akkor bármely különböző m és n nemnegatív egész számra $u^m v \in Q(X)$ vagy $u^n v \in Q(X)$.*

Bizonyítás Tegyük fel, hogy $u^m v \notin Q(X)$ és $u^n v \notin Q(X)$. Az általánosság megszorítás nélkül azt is feltehetjük, hogy $m < n$.

Legyen először $n = m + 1$. A12.45 Tétel szerint vannak olyan $p, q \in Q(X)$ primitív szavak és $2 \leq i, j$ egész számok, amelyekre $u^m v = p^i$ és $u^n v = q^j$. A 12.46 Tételből következik, hogy van olyan $r \in Q(X)$, amelyre $u^m vu = r^j$. Innen, $p^{2i} = u^m v y^m v$ és $r^j = u^m vu$ szavaknak $u^m v$ közös prefixe. Mivel

$$|p| + |r| \leq \frac{1}{2}|u^m v| + \frac{1}{2}|u^m vu| < |u^m v|,$$

ezért a 12.43 Lemma szerint $p = r$. Ebből következik, hogy u és v a p szó hatványai. Ellentmondás.

Legyen most $n \geq m + 2$, továbbá $u^m v = p^i$ és $u = q^j$, ahol $p, q \in Q(X)$ és $2 \leq i$, $1 \leq j$. Mivel $q^{j(n-m)} p^i = u^n v \notin Q(X)$ és $j(n - m) \geq 2$, a 12.48 Következmény miatt $p = q$. Ami ismét azt jelenti, hogy u és v a p szó hatványai. Ellentmondás. □

12.57. Tétel. *Legyen az $\mathbf{A} = (A, X, a_0, \delta, F)$ iniciálisan összefüggő automata véges, $2 \leq |X|$ és $2 \leq n = |A|$. Ha van olyan $p \in L(\mathbf{A}) \cap Q(X)$ szó amelyre $n \leq |p|$, akkor $|L(\mathbf{A}) \cap Q(X)| = \infty$.*

Bizonyítás Legyen $p \in L(\mathbf{A} \cap Q(X)$ és $n \leq |p|$. Ha $\mathbf{A}$ terminálisan összefüggő, akkor az állítás a 12.55 Tételből következik.

Ha $\mathbf{A}$ nem terminálisan összefüggő, akkor van olyan $a \in A$, hogy minden $r \in X^*$ bemenő szóra $ar \notin F$. Legyenek $p = x_1 x_2 \dots x_k$ és $a_i = a_{i-1} x_i$, ahol $x_i \in X$ $(i = 1, 2, \dots, k)$ és $n \leq k$. Mivel $a_i \in A - a$ és $n \leq k$, ezért vannak olyan $1 \leq l < m \leq k$ egész számok, amelyekre $a_l = a_m$. Ha $q = x_1 \dots x_l$, $s = x_{l+1} \dots x_m$ és $t = x_{m+1} \dots x_k$ ($m = k$ esetben $t = e$), akkor $p = qst$, $tq \neq e$ $s \neq e$ és $qs^*t \subseteq L(\mathbf{A})$. A 12.46 Tétel szerint $stq \in Q(X)$, ezért s és tq nem hatványa ugyanannak a szónak. A 12.56 Lemma szerint $|s^*tq \cap Q(X)| = \infty$. Innen $|qs^*t \cap Q(X)| = \infty$, azaz $|L(\mathbf{A}) \cap Q(X)| = \infty$. □

12.58. Tétel. *Ha $\mathbf{A}_F = (A, X, a_0, \delta, F)$ iniciálisan összefüggő automata véges, $2 \leq |X|$ és $2 \leq n = |A|$, akkor a következő állítások igazak:*

(1) $|L(\mathbf{A}) \cap Q(X)| = \infty$ akkor és csak akkor ha van olyan $p \in L(\mathbf{A}) \cap Q(X)$, amelyre $n \leq |p| \leq 3n - 3$.

(2) Ha $L(\mathbf{A}) \cap Q(X) \neq \emptyset$, akkor van olyan $p \in L(\mathbf{A}) \cap Q(X)$, amelyre $|p| \leq 3n - 3$.

Bizonyítás Ha az **A** automata terminálisan összefüggő, akkor a tétel állítása a 12.55 Tétel miatt nyilvánvalóan igaz. Ezért a továbbiakban tegyük fel, hogy **A** nem terminálisan összefüggő.

Először az (1) állítást igazoljuk. Ha van olyan $p \in L(\mathbf{A}) \cap Q(X)$, amelyre $n \leq |p| \leq 3n-3$, akkor a 12.57 Tétel szerint $|L(\mathbf{A}) \cap Q(X)| = \infty$.

Megfordítva, tegyük fel, hogy $|L(\mathbf{A}) \cap Q(X)| = \infty$. Akkor létezik olyan $p \in L(\mathbf{A}) \cap Q(X)$ szó, hogy $n \leq |p|$. Megmutatjuk, hogy olyan $p \in L(\mathbf{A}) \cap Q(X)$ szó is van, amelyre $n \leq |p| \leq 3n-3$. Mivel **A** nem terminálisan összefüggő, van olyan $a \in A$, hogy minden $r \in X^*$ bemenő szóra $ar \notin F$. Legyen $q \in L(\mathbf{A}) \cap Q(X)$ legkisebb olyan hosszúságú szó, amelyre $n \leq |q|$. Ha $|q| \leq 3n-3$, akkor készen vagyunk a bizonyítással. Tegyük fel, hogy $3n-2 \leq |q|$. Legyenek $q = x_1 x_2 \dots x_k$ és $a_i = a_{i-1} x_i$, ahol $x_i \in X,\ i = 1, 2, \dots, k$ és $3n-2 \leq k$. Mivel $a_i \in A - a \quad i = 1, 2, \dots, k$ és $3|A-a| + 1 = 3n-2 \leq k$, ezért vannak olyan $1 \leq k_1 < k_2 < k_3 < k_4 \leq k$ egész számok, amelyekre $a_{k_1} = a_{k_2} = a_{k_3} = a_{k_4}$. Legyenek

$$u = x_1 \dots x_{k_1},\ v_1 = x_{k_1+1} \dots x_{k_2},\ v_2 = x_{k_2+1} \dots x_{k_3},$$

$$v_3 = x_{k_3+1} \dots x_{k_4}, w = x_{k_4+1} \dots x_k.$$

(Ha $k_4 = k$, akkor $w = e$.) Nyilvánvalóan wu, v_1, v_2 és v_3 nem egyenlő az e üres szóval, továbbá $uv_1^* v_2^* v_3^* w \in L(\mathbf{A})$. Legyen $wu = t^i \quad t \in Q(X)$ és $1 \leq i$. Könnyen belátható, hogy elegendő a következő három esetet megvizsgálni:

Ha $v_1, v_2, v_3 \in t^+$, akkor $wuv_1v_2v_3 \notin Q(X)$, s így a 12.46 Tétel szerint $q \notin Q(X)$. Ellentmondás.

Másodszor tegyük fel például, hogy $v_1, v_2 \notin t^+$. Feltehetjük azt is az általánosság megszorítása nélkül, hogy $|v_1| \leq |v_2|$. Ha $|uv_1w| \leq n$, akkor $|v_1| \leq n-1$. Van olyan j pozitív egész szám, amelyre

$$n \leq |uv_1^j w| < |uv_1^{j+1} w| \leq 3n-3.$$

A 12.56 Lemmal szerint $v_1^j wu \in Q(X)$ vagy $v_1^{j+1} wu \in Q(X)$. A 12.46 Tétel miatt $uv_1^j w \in Q(X)$ vagy $uv_1^{j+1} w \in Q(X)$, ami ellentmond a q-ra szabott feltételeknek. Ha $|uv_1w| > n$, akkor

$$n < |uv_1w| < |uv_1^2 w| < |q|.$$

A 12.56 Lemma és a 12.46 Tétel szerint $uv_1w \in Q(X)$ vagy $uv_1^2 w \in Q(X)$, ami szintén ellentmondás.

Harmadszor legyen mondjuk $v_1 \notin t^+$ és $v_2, v_3 \in t^+$. Az előző eset bizonyításához hasonlóan, ha $|uv_1w| \leq n$, akkor $|v_1| \leq n-1$. Van olyan j pozitív egész szám, amelyre

$$n \leq |uv_1^j w| < |uv_1^{j+1} w| \leq 3n-3.$$

A 12.56 Lemma és a 12.46 Tétel szerint $uv_1w \in Q(X)$ vagy $uv_1^2w \in Q(X)$, ami ellentmondás. Ha $|uv_1w| > n$, akkor

$$n < |uv_1w| < |uv_1v_2w| < |q|.$$

A 12.56 Lemmal szerint $wuv_1 \in Q(X)$ vagy $v_2wuv_1 \in Q(X)$. A 12.46 Tétel miatt $uv_1w \in Q(X)$ vagy $uv_1v_2w \in Q(X)$, ami ellentmondás.

Most megmutatjuk, hogy a (2) állítás is igaz. Legyen $L(\mathbf{A}) \cap Q(X) \neq \emptyset$. Ha minden $p \in L(\mathbf{A}) \cap Q(X)$ szóra $|p| \leq n-1$, akkor nyilvánvalóan igaz az állítás. Ha van olyan van olyan $p \in L(\mathbf{A}) \cap Q(X)$ szó, amelyre $n \leq |p|$, akkor a 12.57 Tétel szerint $|L(\mathbf{A}) \cap Q(X)| = \infty$. Az (1) állítás miatt van olyan $q \in L(\mathbf{A}) \cap Q(X)$, amelyre $n \leq 3n-3$. □

Megemlítjük, hogy a tételben szereplő $3n-3$ nem a legkisebb felső korlát. Az irodalomban ismert, hogy ez $\frac{1}{2}(5n-9)$. Ennek bizonyításához azonban további vizsgálatok szükségesek, amit a jegyzet terjedelme nem tesz lehetővé. A 12.58 Tétel alapján kimondhatjuk a reguláris nyelvekre vonatkozó 8.13 Tétel analogonját a reguláris nyelvek és a primitív szavak közös részére.

12.59. Következmény. *Bármely iniciálisan összefüggő* $\mathbf{A} = (A, X, a_0, \delta, F)$ *véges automata esetén algoritmikusan eldönthető, hogy a* $L(\mathbf{A}) \cap Q(X)$ *halmaz üres, véges vagy végtelen.*

12.7. Diszjunktív nyelvek

Az X ábécé feletti L nyelvet *diszjunktív*nak nevezzük, ha a (7.5)-ben definiált ϑ_L szintaktikus kongruencia identikus, azaz $\vartheta_L = \iota_{X^*}$. A diszjunktív nyelvekkel kapcsolatos vizsgálatok találhatók például H.J. Shyr [41] jegyzetében. A 7.8 Következmény alapján nyilvánvaló, hogy a véges ábécé feletti diszjunktív nyelvek nem regulárisak. (Ez azt is jelenti, hogy a diszjunktív nyelvek nem lehetnek végesek.) Egyelemű ábécé esetén igaz a fordított állítás is.

12.60. Tétel. *Egyelemű ábécé feletti nyelv akkor és csak akkor diszjunktív, ha nem reguláris.*

Bizonyítás A tétel előtti megjegyzést felhasználva elegendő megmutatni, hogy ha az $\{a\}$ ábécé feletti L nyelv nem diszjunktív, akkor reguláris.

Ha L nem diszjunktív, akkor vannak olyan $0 \leq k$ és $1 \leq m$ egész számok, amelyekre $(a^k, a^{k+m}) \in \vartheta_L$. Mivel ϑ_L kongruencia, ezért minden $0 \leq t$ egész számra $(a^{k+t}, a^{k+m+t}) \in \vartheta_L$. Ez azt jelenti, hogy ϑ_L indexe legfeljebb $k+m$. Kleene tétele és 7.2 Tétel szerint L reguláris. □

Legalább kételemű véges ábécé esetén ez az állítás már nem igaz.

12.61. Lemma. *A legalább kételemű X véges ábécé feletti L nyelv akkor és csak akkor diszjunktív, ha minden $p, q \in X^*$ szóra*

$$(|p| = |q| \quad \text{és} \quad (p, q) \in \vartheta_L) \quad \Longrightarrow \quad p = q. \tag{12.25}$$

Bizonyítás Ha L diszjunktív akkor nyilvánvalóan teljesül (12.25).

Megfordítva tegyük fel, hogy (12.25) igaz. Legyen $(p, q) \in \vartheta_L \ \ (p, q \in X^*)$ és $m = \sup\{|p|, |q|\}$. Ha $w = ab^m \ \ (a, b \in X, \ a \neq b)$, akkor pw és qw primitív szavak. Minthogy ϑ_L kongruencia, így $(pw, qw) \in \vartheta_L$. Ebből következik, hogy $((pwqw, qwpw) \in \vartheta_L$. De $|pwqw| = |qwpw|$, és (12.25) miatt $pwqw = qwpw$. A 12.42 Lemma szerint pw és qw valamely $r \in X^+$ szónak pozitív egész kitevős hatványai. Azonban pw és qw primitív szavak, ezért $pw = qw$, azaz $p = q$. Ez azt jelenti, hogy ϑ_L identikus, vagyis L diszjunktív. □

Az X ábécé feletti K és L nyelveket *diszjunktív pár*nak nevezzük, ha $L \cap K = \emptyset$ és minden $p, q \in X^* \ \ (p \neq q)$ párhoz vannak olyan $u, v \in X^*$ szavak, amelyekre $upv \in K$ és $uqv \in L$ vagy $uqv \in K$ és $upv \in L$. Ha K diszjunktív nyelv, akkor nyilvánvalóan K és $\overline{K}$ diszjuntív pár. Továbbá, ha K és L diszjunktív pár, akkor mindkettő diszjunktív. Ezenkívül, ha K' és L' olyan X feletti nyelvek, amelyekre $K \subseteq K', \ \ L \subseteq L', \ \ K' \cap L' = \emptyset$, akkor K' és L' is diszjunktív pár.

A 12.6. alfejezetben az X ábécé feletti primitív szavak nyelvére a $Q(X)$ jelölést használtuk. A 12.51 Következményben megmutattuk, hogy véges ábécé esetén $Q(X)$ nem reguláris. A következőkben megmutatjuk, hogy $Q(X)$ diszjunktív. Ezzel egy másik bizonyítását is kapjuk a 12.51 Következménynek. Legyen tetszőleges $2 \leq n$ egész számra

$$Q^{(n)}(X) = \{p^n; \ p \in Q(X)\}.$$

A 12.54 Tételben megmutattuk, hogy véges X ábécé esetén bármely $2 \leq n$ egész számra $Q^n(X)$ reguláris. Nyilvánvaló, hogy $Q^{(n)}(X) \subset Q^n(X)$. A 12.45 Tételből kapjuk, hogy

$$X^* = \sum_{n=0}^{\infty} Q^{(n)}(X),$$

ahol $Q^{(0)}(X) = e$ és $Q^{(1)}(X) = Q(X)$. Ha $i \neq j$, akkor $Q^i(X) \cap Q^j(X) = \emptyset$.

12.62. Tétel. *Legalább kételemű X ábécé esetén minden $2 \leq n$ egész számra $Q(X)$ és $Q^{(n)}(X)$ diszjunktív pár.*

Bizonyítás Legyenek $p, q \in X^*$ és $p \neq q$. Feltehetjük, hogy $p \in X^+$, azaz $p = xr$, ahol $x \in X$ és $r \in X^*$. Legyen továbbá $y \in X$ és $y \neq x$. Ezenkívül $m = 2\sup\{|p|, |q|\}$, $u = y^m p$, $v = (y^m pp)^{n-1}$ $(2 \leq n)$. Mivel $y^m pp \in Q(X)$, ezért $upv = (y^m pp)^n \in Q^{(n)}(X)$.

Megmutatjuk, hogy $uqv = y^m pq(y^m pp)^{n-1} \in Q(X)$. Tegyük fel, hogy ez nem igaz, azaz $w^j = y^m pq(y^m pp)^{n-1}$, ahol $w \in Q(X)$ és $2 \leq j$. Akkor nem nehéz belátni, hogy $w = y^m xw'$ $(w' \in X^+)$. Mivel w pontosan m számu y betűvel kezdődik, ezért

$$w = (y^m pq)(y^m pp)^i = (y^m pp)^{i+1}$$

valamilyen $0 \leq i$ egész számra. Ez azonban lehetetlen, mivel $p \neq q$. Kaptuk, hogy $j = 1$, azaz $uqv \in Q(X)$. □

12.63. Következmény. *Legalább kételemű X ábécé esetén $Q^{(n)}(X)$ $(1 \leq n)$ diszjunktív. Ha X véges, akkor $Q^{(n)}(X)$ nem reguláris.*

Egy L nyelvet *diszkrét*nek nevezünk, ha minden $p, q \in L$ szóra $|p| = |q|$ akkor és csak akkor, ha $p = q$.

12.64. Lemma. *Ha a legalább kételemű X ábécé feletti L nyelv diszkrét és minden $p \in X^*$ szóra $L \cap X^*pX^* \neq \emptyset$, akkor L diszjunktív.*

Bizonyítás Legyen $|p| = |q|$ és $(p, q) \in \vartheta_L$. A feltétel szerint vannak $u, v \in X^*$ szavak, amelyekre $upv \in \vartheta_L$. Akkor $uqv \in \vartheta_L$ is teljesül. De $|upv| = |uqv|$ és L diszkrét, ezért $upv = uqv$, azaz $p = q$. Az előző feladat szerint L diszjunktív.□

12.65. Tétel. *A legalább kételemű véges X ábécé feletti L nyelvre az alábbi három állítás ekvivalens:*
(i) L tartalmaz diszjunktív résznyelvet;
(ii) Minden $p \in X^*$ szóra $L \cap X^*pX^* \neq \emptyset$;
(iii) Minden $p \in X^*$ szóra $|L \cap X^*pX^*| = \infty$.

Bizonyítás Az $(i) \Longrightarrow (ii)$ implikáció helyességét indirekt módon mutatjuk meg. Ha van olyan $p \in X^*$, amelyre $L \cap X^*pX^* = \emptyset$, akkor L bármely K résznyelvére $(p, p^2) \in \vartheta_K$, azaz K nem diszjunktív. Ellentmondás.

Az $(ii) \Longrightarrow (iii)$ implikáció helyességét szintén indirekt módon mutatjuk meg. Tegyük fel, hogy $p \in X^*$ szóra $L \cap X^*pX^*$ véges halmaz. Ha $u \in X^+$ olyan szó, amely minden $q \in L \cap X^*pX^*$ szónál hosszabb, akkor $L \cap X^*puX^* = \emptyset$. Elentmondás.

Az $(iii) \Longrightarrow (i)$ bizonyításához tegyük rendezetté az X véges ábécét. Ennek segítségével vezessük be a $\leq$ *lexikografikus rendezés*t X^*-on. (Ez a fogalom

megtalálható például a [2] jegyzetünk Függelékében.) A lexikografikus rendezés felhasználásával definiáljuk L egy K diszjunktív résznyelvét. Legyen $X^* = \{p_k; k = 1, 2, \dots\}$, ahol p_k közvetlenül megelőzi p_{k+1}-et. A feltevés miatt választhatók olyan $u_k, v_k \in X^*$ $(k = 1, 2, \dots)$ szavak, amelyekre $u_k p_k v_k \in L$ és

$$|u_k p_k v_k| < |u_{k+1} p_{k+1} v_{k+1}|.$$

Legyen $K = \{u_k p_k v_k;\ k = 1, 2, \dots\}$. A K nyelv diszkrét, $K \subseteq L$ és minden $p \in X^*$ szóra $K \cap X^* p X^* \neq \emptyset$, ezért a 12.64 Lemma szerint diszjunktív. □

12.66. Következmény. *A legalább kételemű véges X ábécé feletti L vagy $\overline{L}$ nyelv tartalmaz diszjunktív résznyelvet.*

Bizonyítás Ha $|L \cap X^* p X^*| = \infty$, akkor az előző tétel szerint L-nek van diszjunktív résznyelve.

Tegyük fel, hogy van olyan $p \in X^*$, amelyre $L \cap X^* p X^*$ véges. Akkor minden $u \in X^*$ szóra $L \cap X^* p u X^* \subseteq X^* p X^*$ miatt $L \cap X^* p u X^*$ is véges. De

$$X^* p u X^* = (L \cup \overline{L}) \cap (X^* p u X^*) = (L \cap X^* p u X^*) \cup (\overline{L} \cap X^* p u X^*).$$

Ebből kapjuk, hogy $|\overline{L} \cap X^* p u X^*| = \infty$. De $\overline{L} \cap X^* p u X^* \subseteq \overline{L} \cap X^* u X^*$. Vagyis minden $u \in X^*$ szóra $|\overline{L} \cap X^* u X^*| = \infty$. Szintén az előző tétel miatt $\overline{L}$-nek van diszjunktív résznyelve. □

12.67. Tétel. *Legyen L diszjunktív nyelv a legalább kételemű véges X ábécé felett. Ha $L = L_1 \cup L_2$ és $L_1 \cap L_2 = \emptyset$, akkor L_1 vagy L_2 diszjunktív vagy mindkét nyelv tartalmaz diszjunktív résznyelvet.*

Bizonyítás Tegyük fel, hogy L_1 és L_2 egyike sem diszjunktív, továbbá L_2 nem tartalmaz diszjunktív résznyelvet. Akkor a 12.65 Tétel szerint van olyan $w \in X^+$, hogy $L_2 \cap X^* w X^*$ véges. Mivel L_1 sem diszjunktív, ezért a 12.61 Lemma szerint vannak olyan $u, v \in X^*$, amelyekre $u \neq v$, $|u| = |v|$ és $(u, v) \in \vartheta_{L_1}$. Feltehetjük azt is, hogy $|u| > \sup\{|pwq|;\ pwq \in L_2\}$. De $(uw, vw) \in \vartheta_{L_1}$. A 12.65 Tétel alapján, ha $ruwt \in L$, akkor $rvwt \in L_1 \subseteq L$. Hasonlóan, ha $rvwt \in L$, akkor $ruwt \in L$, azaz $(uw, vw) \in \vartheta_L$. Mivel L diszjunktív, ezért $uw = vw$. Ez azonban lehetetlen, mert $u \neq v$. A 12.65 Tételből következik, hogy L_1 és L_2 tartalmaz diszjunktív résznyelvet. □

Mivel diszjunktív nyelv komplementere is diszjunktív, ezért az alábbi következmény azt jelenti, hogy nincs minimális [maximális] diszjunktív nyelv.

12.68. Következmény. *Legyen L diszjunktív nyelv a legalább kételemű véges X ábécé felett. Ha F véges részhalmaza L-nek, akkor $L - F$ is diszjunktív.*

Bizonyítás Mivel $L = (L - F) \cup F$, $(L - F) \cap F = \emptyset$ és F nem tartalmaz diszjunktív résznyelvet, ezért a 12.67 Tétel szerint $L - F$ diszjunktív. □

Érvényes a 12.67 Tétel következő élesítése diszkrét diszjunktív nyelvekre.

12.69. Tétel. *Legyen L diszkrét diszjunktív nyelv a legalább kételemű véges X ábécé felett. Ha $L = L_1 \cup L_2$ és $L_1 \cap L_2 = \emptyset$, akkor L_1 vagy L_2 diszjunktív.*

Bizonyítás Tegyük fel, hogy L_1 és L_2 egyike sem diszjunktív. Akkor a 12.61 Lemma szerint vannak olyan $p, q, r, t \in X^+$ szavak, amelyekre $p \neq q$, $r \neq t$, $|p| = |q|$, $|r| = |t|$, $(p, q) \in \vartheta_{L_1}$, $(r, t) \in \vartheta_{L_2}$. Ebből következik, hogy $(pr, qr) \in \vartheta_{L_1}$ és $(pr, pt) \in \vartheta_{L_2}$. Mivel L diszjunktív, a 12.65 Tétel szerint vannak olyan $u, v \in X^*$ szavak, amelyekre $uprv \in L$. Ha $uprv \in L_1$, akkor $uqrv \in L_1$, mert $(pr, qr) \in \vartheta_{L_1}$. De L diszkrét, ezért $uprv = uqrv$, ami ellentmond annak, hogy $p \neq q$. Hasonlóan, az $uprv \in L_2$ feltételből is ellentmondásra jutunk. Vagyis L_1 vagy L_2 diszjunktív. □

12.70. Tétel. *A legalább kételemű véges X ábécé feletti L nyelvre az alábbi három állítás ekvivalens:*
(i) L diszjunktív;
(ii) Minden $p \in X^*$ szóra $L \cap X^*pX^*$ diszjunktív;
(iii) Van olyan $p \in X^*$ szó, amelyre $L \cap X^*pX^*$ diszjunktív.

Bizonyítás Az $(i) \Longrightarrow (ii)$ implikáció következik a 12.65 és a 12.67 Tételekből, mivel

$$L = (L \cap X^*wX^*) \cup (L \cap \overline{X^*wX^*}), \quad (L \cap \overline{X^*wX^*}) \cap X^*wX^* = \emptyset.$$

Az $(ii) \Longrightarrow (iii)$ implikáció nyilvánvalóan igaz.

Az $(iii) \Longrightarrow (i)$ implikáció helyességének igazolásához tegyük fel, hogy a $w \in X^*$ szóra $L \cap X^*wX^*$ diszjunktív. Tegyük fel, hogy L nem diszjunktív. Akkor vannak olyan $u, v \in X^+$, amelyekre $u \neq v$ és $(u, v) \in \vartheta_L$. De ϑ_L kongruencia, ezért $(wu, wv) \in \vartheta_L$, s nyilván $wu \neq wv$. Ebből következik, hogy minden $p, q \in X^*$ esetén $pwuq \in L$ akkor és csak akkor, ha $pwvq \in L$, azaz $pwuq \in L \cap X^wX^*$ akkor és csak akkor, ha $pwvq \in L \cap X^*wX^*$, vagyis $L \cap X^*wX^*$ nem diszjunktív. Ellentmondás. □

12.8. Sűrű és ritka nyelvek

Az alfejezetben vizsgált nyelvek fontos szerepet játszanak a kódok algebrai elméletében. Így azt is mondhatjuk, hogy ez az alfejezet köti össze a II. és a III. részt.

Az X feletti L nyelvet *sűrű*nek nevezzük X felett, ha

$$(\forall p \in X^*)(L \cap X^* p X^* \neq \emptyset) \tag{12.26}$$

Például a 3.8. alfejezetben definiált környezetfüggetlen *Dyck nyelv* sűrű az adott ábécé felett. A nemsűrű nyelveket *ritka nyelvek*nek is hívjuk. Ritka nyelv minden résznyelve is ritka. Sűrű nyelvet tartalmazó nyelv szintén sűrű egy adott ábécé felett. Ha $|X| = 1$, akkor az X feletti véges nyelvek a ritka, a végtelen nyelvek pedig a sűrű nyelvek.

A 12.65 Tétel alapján nem nehéz belátni az alábbi tételt:

12.71. Tétel. *A legalább kételemű véges X ábécé feletti L nyelv akkor és csak akkor sűrű, ha tartalmaz diszjunktív résznyelvet.*

12.72. Lemma. *Ha L az X ábécé feletti sűrű nyelv, akor a $K \subseteq X^*$ nyelvre*

$$(\forall p \in X^*)\ (K \cap X^* p X^* \neq \emptyset)$$

feltételből következik, hogy K is sűrű nyelv X felett.

Bizonyítás Ha L sűrű nyelv X felett, akkor minden $p \in X^*$ szóhoz vannak olyan $u, v \in X^*$ szavak, hogy $upv \in L$. A feltétel szerint $L \cap X^* upv X^* \neq \emptyset$. Így

$$\emptyset \neq K \cap X^* upv X^* \subseteq K \cap X^* p X^*,$$

azaz K sűrű nyelv X felett. □

A 12.65 Tétel $(i) \Longrightarrow (ii)$ implikációjának bizonyításából következik az alábbi lemma. A bizonyítás során ugyanis nem használjuk ki az ábécé végességét.

12.73. Lemma. *Tetszőleges legalább kételemű X ábécé feletti diszjunktív nyelv sűrű X felett.*

Az állítás megfordítása nem igaz. Például $Q(X)$ prímszám hossúságú szavainak résznyelve sűrű nyelv X felett, de nem diszjunktív. A 12.63 Következmény és a 12.73 Lemma szerint nyilvánvalóan igaz a következő állítás:

12.74. Következmény. *A legalább kételemű X ábécé feletti primitív szavak $Q(X)$ nyelve X felett sűrű nyelv.*

A következő tételben az L nyelv $\sqrt{L}$ gyöke szerepel, amelynek fogalmát a 12.6. alfejezetben vezettük be.

12.75. Tétel. *A legalább kételemű X ábécé feletti L nyelv akkor és csak akkor sűrű X felett, ha $\sqrt{L}$ is sűrű X felett.*

Bizonyítás Tegyük fel, hogy L sűrű nyelv X felett. Legyen $q \in Q(X)$ tetszőleges primitív szó, $|q| = m$ és $x, y \in X$ $(x \neq y)$. Nyilvánvaló, hogy $p = xy^{9m}xqqxy^{9m}x \in Q(X)$. A 12.74 Következmény szerint vannak olyan $u, v \in X^*$ szavak, hogy $upv \in L$. Ha $upv \in Q(X)$, akkor $upv \in \sqrt{L}$. Ha $upv \notin Q(X)$, akkor a 12.45 Tétel szerint $xpv = r^i$, ahol $r \in \sqrt{L}$ és $i \geq 2$. A p szó definíciójából látható, hogy $|r| > 2|q|$. Ezért $r = sqt$ valamilyen $s, t \in X^*$ szavakra, azaz $\sqrt{L} \cap X^*qX^* \neq \emptyset$. A 12.72 Lemma és a 12.74 Következmény szerint $\sqrt{L}$ sűrű nyelv X felett.

Megfordítva, ha $\sqrt{L}$ sűrű nyelv X felett, akkor minden $p \in X^*$ szóhoz vannak olyan $u, v \in X^*$ szavak, amelyekre $upv \in \sqrt{L}$. A 12.45 Tétel szerint $(upv)^i \in L$ valamilyen i pozitív egész számra. Ez azt jelenti, hogy $L \cap X^*pX^* \neq \emptyset$, vagyis L sűrű nyelv X felett. □

12.76. Lemma. *Az X ábécé feletti L és K nyelvekre $L + K$ akkor és csak akkor ritka, ha L és K is ritka. Ha L és K ritka, akkor LK is ritka. Ha L sűrű és K ritka, akkor $L - K$ sűrű.*

Bizonyítás Mivel ritka nyelv minden részNyelve is ritka, ezért, ha $L+K$ ritka, akkor L és K is ritka.

Ha L és K ritka, akkor vannak olyan $p, q \in X^+$, amelyekre $L \cap X^*pX^* = \emptyset$ és $K \cap X^*qX^* = \emptyset$. Így

$$(L + K) \cap X^*pqX^* = (L \cap X^*pqX^*) + (K \cap X^*pqX^*) \subseteq$$

$$\subseteq (L \cap X^*pX^*) + (K \cap X^*qX^*) = \emptyset,$$

azaz $L+K$ is ritka. Továbbá $LK \cap X^*pqX^* = \emptyset$, azaz LK is ritka. Ha ugyanis $LK \cap X^*pqX^* \neq \emptyset$, akkor $L \cap X^*pX^* \neq \emptyset$ vagy $X^*qX^* \cap K \neq \emptyset$.

Ha L sűrű és K ritka, akkor $L - K$ nem lehet ritka, mert akkor az előzőek szerint $L = (L - K) + K$ is ritka lenne. □

A 12.76 Lemma szerint az X ábécé feletti ritka nyelvek az X feletti nyelvek félgyűrűjének részfélgyűrűjét alkotják a nyelvek összeadására és szorzására.

Mivel minden X ábécére X^* sűrű nyelv X felett, ezért 12.76 Lemmából nyilvánvalóan adódik a

12.77. Következmény. *Tetszőleges X ábécé felett az L nyelv vagy az $\overline{L}$ nyelv sűrű nyelv.*

A 12.77 Következményből a 8.6 Tétel felhasználásával kapjuk az alábbi következményt.

12.78. Következmény. *Ha L reguláris nyelv a véges X ábécé felett, akkor L vagy $\overline{L}$ sűrű nyelv.*

12.79. Következmény. *Minden korlátos nyelv ritka.*

Bizonyítás Legyen L korlátos nyelv és k olyan nemnegatív egész szám, hogy minden L-beli szó hossza legfeljebb k. Ha $p \in X^l$ $(l > k)$, akkor $L \cap X^* p X^* = \emptyset$, azaz L ritka. □

12.80. Lemma. *Ha L egy Z halmaz feletti nyelv és $Z \subset X$, akkor L ritka nyelv X felett.*

Bizonyítás Ha $x \in X - Z$, akkor $L \cap X^* x X^* = \emptyset$, azaz L ritka nyelv X felett. □

A 12.79 Következmény szerint minden véges nyelv ritka.

Feladatok

12.1. Konstruáljunk egy automatát, amelyik felismeri az

$$L = \{xy, x^2y^2, \ldots, x^n y^n\} \quad (1 \leq n)$$

véges nyelvet. Mennyi L felismerési száma?
12.2. Ha $p, q \in Q(X)$ $(p \neq q)$ és $pq^n \notin Q(X)$, akkor minden $2 \leq k$ egész számra $pq^{n+k} \in Q(X)$).
12.3. Az X^* szabad monoid egy S részfélcsoportja akkor és csak akkor kommutatív, ha $|S \cap Q(X)| \leq 1$. Ebben az esetben S minden elemének gyöke ugyanaz a $q \in Q(X)$ primitív szó.
12.4. Ha $u, v \in X^+$ szavakra $uv \in Q(X)$, akkor minden $2 \leq n$ egész számra $(uv)^n u, v(uv)^n \in Q(X)$.
12.5. Legalább kételemű X véges ábécé felett a $Q(X)\overline{Q}(X)$ nyelv diszjunktív.
12.6. Legalább kételemű X ábécé felett a $\overline{Q}^2(X)$ nyelv diszjunktív.
12.7. Legyen L diszjunktív nyelv az $X = \{x_1, x_2, \ldots, x_k\}$ $(2 \leq k)$ ábécé felett. Ha W azoknak az X^*-beli szavaknak a nyelve, amelyekben nem szerepel az $x_1, x_2, \ldots, x_k$ betűk mindegyike, akkor $L - W$ is diszjunktív.
12.8. Ha L a legalább kételemű véges X ábécé feletti diszjunktív nyelv, akkor tetszőleges $w \in X^+$ szóra $L - w^*$ is diszjunktív.
12.9. Ha X legalább kételemű ábécé, akkor az $X^* - Q$ nemprimitív szavak nyelve nem környezetfüggetlen.

III. rész

KÓDOK

A 6.8. alfejezetben megbeszéltük, hogy egy X ábécé elemeivel megfogalmazott *információk*on az X elemeiből képezett véges sorozatokat, azaz X^*-beli szavakat értjük. *formációátalakítás*on pedig $\alpha : X^* \to Y^*$ un. *alfabetikus leképezések*et értettünk. Az információközlés folyamatát a gyakorlatban az adó- és vevőberendezések, valamint az ezeket összekötő információs csatornák, az ún. *hírközlési rendszer*ek információátalakításokkal valósítják meg. Az információs csatorna a gyakorlatban véges sok, de legalább két különböző jelet továbbít egyenlő időközönként. Ezeknek a jeleknek a halmazát *csatornaábécé*nek nevezhetjük. Az információforrás az adónak az információt valamilyen nyelven szolgáltatja. Ennek a nyelvnek az ábécéje a *forrásábécé*. Az adóban egy kódoló berendezés a közölt információt általában fizikai jelekké, jelsorozatokká alakítja, amelyeket az adó az *információs csatorná*n keresztül juttat a vevőhöz. A vevő képes a jeleket felfogni és egy dekódoló berendezéssel a jelsorozatokat visszaalakítani. Sok esetben az adó először az adott nyelv ábécéjének betűit egy másik ábécé jelsorozataivá alakítja, amelyeket könnyen tud az információs csatornán küldhető jelsorozatokká átkódolni.

Egy hírközlési rendszer végeredményben olyan kimenő jeles véges automaták soros kapcsolásanak tekinthető (l. [2]), amelyben az egyes automaták bemenő és kimenő halmazai kódok, speciálisan az első automata bemenő halmaza és az utolsó automata kimenő halmaza a forrásábécé, a kimeneti függvények kódolások, átkódolások és dekódolások, s amelyben ha az információs csatorna hiba nélkül működik, másképpen mondva *zajmentes*, akkor ugyanazt a jelsorozatot adja ki, mint amit bemenő jelsorozatként kapott. Az információt ilyen módon nagy távolságokra is el tudjuk küldeni.

Előfordul, hogy nem akarjuk azt, hogy az elküldött üzenet illetéktelen kezekbe kerüljön, ezért még ún. *titkosítási kódolás*t is végzünk. Ezzel ma már egy önálló tudományág, a *kriptográfia* foglalkozik.

A számítógépek programozásában, az *információ (adatok) tárolás*ában és ha szükséges titkosításában is alapvető szerepet játszanak a kódok. Sok esetben fontos az *információ tömörítése*, amely szintén kódolással, illetve felhasználáskor dekódolással oldható meg.

Megemlítjük még a *hibajavító kódok* alkalmazását, amelyek az információ továbbítása vagy tárolása során fellépő hibák kiküszöbölésére szolgálnak.

A kódelmélet részletes tárgyalására nem térhetünk ki, csupán a változó hosszúságú kódok, mint speciális nyelvek rövid félcsoportelméleti megalapozásával foglalkozunk, különös tekintettel a prefix kódokra. Az általános kódelmélettel részletesen foglalkozik Jean Berstel és Dominique Perrin [4] kiváló monográfiája.

13. fejezet

A kódelmélet alapjai

13.1. A kód fogalma

Legyenek X és Y tetszőleges nemüres halmazok. Ha φ az Y halmaz olyan egy-egyértelmű leképezése az X^+ szabad félcsoportba, amelynek homomorf kiterjesztése Y^*-ra az Y^* szabad monoid izomorf leképezése X^*-ba, akkor a φ leképezést Y (X *feletti*) *kódolás*ának, $C = \varphi(Y)$-t (X *feletti*) *kód*nak, a φ^{-1} leképezést pedig C *dekódolás*ának nevezzük. Azt is mondjuk, hogy az Y halmaz elemei *kódolhatók* C elemeivel, vagy φ az Y halmaz C-re való kódolása. A C elemeit *kódszavak*nak is nevezzük. Ha Y csak egy hosszúságú szavakat tartalmaz, akkor *betű szerinti kódolás*ról beszélünk.

A gyakorlatban a kódok, mint más formális nyelvek, véges ábécé felettiek. Az Y halmaz az információküldésnél a forrásábécének, φ pedig az adó kódoló berendezésének felel meg.

Ha a C kód véges vagy megszámlálhatóan végtelen halmaz, akkor *véges* ill. *megszámlálhatóan végtelen kód*nak nevezzük. Ha C legfeljebb megszámlálhatóan végtelen halmaz, akkor a *megszámlálható kód* elnevezést is használjuk.

Ha az I indexhalmaz megszámlálható, akkor I-n az $[n] = \{1, \dots, n\}$ vagy az N_+ halmazt értjük. Ha $Y = \{y_k; k \in I\}$ és φ az Y egy kódolása az (X halmaz feletti) C kódra, akkor $C = \{p_k; k \in I\}$ jelentse azt, hogy $\varphi(y_k) = p_k$ $(k \in I)$.

Az X feletti L nyelvet *korlátos*nak nevezzük, ha van olyan n nemnegatív egész szám, hogy $|p| \leq n$ minden $p \in L$ szóra. Minden véges nyelv korlátos. Ha az L korlátos nyelv kód, akkor *korlátos kód*nak nevezzük. Egy véges ábécé feletti korlátos nyelv mindig véges.

Ha $|X| = 1$, akkor az X feletti kódok X^+ egyelemű részhalmazai. Ha $|X| = 2$, akkor az X feletti kódokat *bináris kódok*nak nevezzük. Ebben az esetben leggyakrabban az $X = \{0, 1\}$ halmazt használjuk. Az X^+ elemeit *bi-*

*náris szavak*nak vagy *bináris sorozatok*nak is nevezzük. Ha φ az Y halmaz egy kódolása egy kételemű ábécé feletti kódra, akkor φ-t *bináris kódolás*nak is nevezzük. A bináris kódoknak az információközlés gyakorlati megvalósításában fontos szerepük van. A legegyszerűbbek azok az információs csatornák, amelyek csak két különböző jelet tudnak továbbítani. Például, ha a hírközlést elektromos árammal valósítjuk meg, akkor a 0 jelentheti azt, hogy alacsony a feszültség (küszöb alatti) az információs csatornán, az 1 pedig azt, hogy magas (küszöb feletti).

Sokszor egy X halmaz feletti kód helyett egyszerűen csak kódot mondunk. Ha vizsgálatainkban egyszerre több kód is szerepel, s nem jelezzük, hogy mely halmazok feletti kódokról van szó, akkor ezeken mindig ugyanazon X halmaz feletti kódokat értünk. Egy kód bármely nemüres részhalmaza szintén kód. Megállapodunk abban, hogy az üres halmazt is kódnak tekintjük.

Ha Y csak egy hosszúságú szavakat tartalmaz és elemei kódolhatók C elemeivel, akkor bármely egy hosszúságú szavakat tartalmazó Y-nal ekvivalens halmaz elemei is kódolhatók C elemeivel, azaz a kód független az Y halmaz választásától és így φ-től is. A csak egy hosszúságú szavakat tartalmazó halmaznak egy másik egy hosszúságú szavakat tartalmazó halmazba való injektív leképezése nyilvánvalóan kódolás. Megállapodunk abban, hogy ezeket a kódolásokat nem tekintjük különbözőknek, s ebben az esetben mindig a halmaz *triviális kódolás*áról beszélünk, a halmaz részhalmazait pedig *triviális kódok*nak nevezzük. A triviális kódokat a kriptográfiában megkülönböztetik, fontos szerepet játszanak a titkosításban.

13.2. Félcsoportelméleti jellemzés

Az alfejezetben megadjuk a kódok algebrai, pontosabban félcsoportelméti fogalmát.

13.1. Lemma. *Az X^+ szabad félcsoport C részhalmaza akkor és csak akkor kód, ha bármely $p_1, p_2, \dots p_k, q_1, q_2, \dots q_l$ elemeire*

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_l \quad \Longrightarrow \quad k = l, \quad p_1 = q_1, \dots, p_k = q_k. \tag{13.1}$$

Bizonyítás Ha $C = \emptyset$, akkor az állítás triviálisan teljesül, ezért feltehetjük, hogy $C \neq \emptyset$. Tegyük fel, hogy C kód. Legyen Y olyan C-vel ekvivalens halmaz és φ az Y halmaz olyan egy-egyértelmű leképezése C-re, amelynek homomorf kiterjesztése Y^*-ra az Y^* szabad monoid izomorf leképezése X^*-ba. Tegyük fel, hogy a C halmaz $p_1, p_2, \dots p_k, q_1, q_2, \dots q_l$ elemeire $p_1 \dots p_k = q_1 \dots q_l$.

$$\varphi(x_i) = p_i, \ \varphi(y_j) = q_j \quad (x_i, y_j \in Y, \ i = 1, \dots, k, \ j = 1, \dots, l).$$

Akkor

$$\varphi(x_1 \dots x_k) = \varphi(x_1) \dots \varphi(x_k) = p_1 \dots p_k =$$
$$= q_1 \dots q_l = \varphi(y_1) \dots \varphi(y_l) = \varphi(y_1 \dots y_l),$$

amiből $x_1 \dots x_k = y_1 \dots y_l$, vagyis $k = l$ és $x_1 = y_1, \dots, x_k = y_k$, s így

$$p_1 = \varphi(x_1) = \varphi(y_1) = q_1, \dots, p_k = \varphi(x_k) = \varphi(y_k) = q_k.$$

Ez azt jelenti, hogy (13.1) teljesül.

Megfordítva, tegyük fel, hogy az X^+ szabad félcsoport $C \neq \emptyset$ részhalmaza teljesíti a (13.1) feltételt. Legyen Y egy C-vel ekvivalens halmaz és φ az Y halmaz egy-egyértelmű leképezése C-re. Terjesszük ki φ-t az Y^* szabad monoidra homomorf módon. Jelöljük a kiterjesztést is φ-vel. Akkor definíció szerint $\varphi(e) = e$, ahol e az üres szó. Legyenek $x_1, \dots, x_k, y_1, \dots, y_l \in Y$, amelyekre

$$\varphi(x_1) \dots \varphi(x_k) = \varphi(x_1 \dots x_k) = \varphi(y_1 \dots y_l) = \varphi(y_1) \dots \varphi(y_l),$$

amiből (13.1) miatt $k = l$ és $\varphi(x_1) = \varphi(y_1), \dots, \varphi(x_k) = \varphi(y_k)$, azaz $x_1 = y_1, \dots, x_k = y_k$. Ez éppen azt jelenti, hogy φ az Y^* szabad monoid izomorf leképezése X^*-ba. □

Megjegyezzük, hogy a kódokat szokás egyszerűen a (13.1) feltétellel is definiálni. A következő lemma azt mondja ki, hogy (13.1) helyettesíthető egy egyszerűbb feltétellel.

13.2. Lemma. *Az X^+ szabad félcsoport C részhalmaza akkor és csak akkor kód, ha bármely $p_1, p_2, \dots p_n, q_1, q_2, \dots q_n$ elemeire*

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_n \quad \Longrightarrow \quad p_1 = q_1, p_2 = q_2, \dots, p_n = q_n. \tag{13.2}$$

Bizonyítás Ha C kód, akkor (13.1)-ből következik (13.2).

Megfordítva, tegyük fel, hogy az X^+ szabad félcsoport C részhalmazára (13.2) teljesül. Feltehetjük, hogy $C \neq \emptyset$. Ha $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ $(k \leq l)$ C olyan elemei, amelyekre $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, akkor

$$p_1 p_2 \dots p_k q_1 q_2 \dots q_l = q_1 q_2 \dots q_l p_1 p_2 \dots p_k.$$

Tegyük fel, hogy $k < l$, akkor ebből (13.2)-t $n = k + l$ esetre felhasználva kapjuk, hogy

$$p_1 = q_1, p_2 = q_2, \dots, p_k = q_k.$$

Így $e = q_{k+1} \dots q_l$, ahol e az üres szó. Ez azonban lehetetlen, ezért $k = l$, vagyis (13.1) teljesül. □

Legyen C X feletti, D pedig Z feletti kód. Ha ψ C-nek D-re való egy-egyértelmű leképezése, akkor ψ-t a C kód D-re való *átkódolás*ának nevezzük. A ψ átkódolás homomorf kiterjesztése C^*-ra C^* szabad monoid izomorf leképezése D^*-ra. (Természetesen ψ^{-1} a D kód C-re való átkódolása.) Ha minden $p \in C$ esetén $|\psi(p)| = |p|$, akkor ψ-t *szóhossztartó átkódolás*nak hívjuk. Átkódolás valósul meg a gyakorlatban, ha a kódolás több lépésben történik, például akkor amikor az adó először a forrásábécé betűit egy másik ábécé jeleivé, jelsorozataivá alakítja, amelyeket azután az információs csatornán küldhető jelsorozatokká átalakít. Ebben a folyamatban az első lépés betű szerinti kódolás, a második azonban a kapott kódnak, amelyben legalább kettő hosszúságú szavak is vannak, egy másik kódra való átkódolása, amit *nem betű szerinti kódolás*nak is nevezünk. Nem betű szerinti kódolás megvalósulhat már az első lépésben is, ha az adott közlemény felbontható a forrásábécé feletti olyan kód szavaira, amelyek közül legalább egy kódszó egynél több betűből áll.

Az X^* szabad monoid automorfizmusai X permutációinak homomorf kiterjesztései X^*-ra. Ebből következik, hogy ha C egy X feletti kód és φ az X halmaz egy permutációja, akkor $\varphi(C)$ is kód X felett és φ szóhossztartó átkódolás.

13.3. Szabad részfélcsoportok

Az X^* szabad monoid bármely M részmonoidjának a

$$B = (M - e) - (M - e)^2$$

halmaz olyan generátorrendszere, amely M minden generátorrendszerének részhalmaza, azaz M egyetlen minimális generátorrendszere. A B-t M *bázisá*nak nevezzük. Az X^* szabad monoid két részmonoidja akkor és csak akkor egyenlő, ha bázisuk megegyezik. Az $M = \{e\}$ részmonoid bázisa $\emptyset$. Az X^+ egy M részfélcsoportjának ugyanaz a bázisa, mint az X^* szabad monoid $M + e$ részmonoidjának. Az X^* szabad monoid és az X^+ szabad félcsoport bázisa X.

13.3. Lemma. *Ha C kód X felett, akkor az X^* szabad monoid C által generált részmonoidjának bázisa C.*

Bizonyítás Jelölje az X^* szabad monoid C által generált részmonoidját $\langle C\rangle$. Az nyilvánvaló, hogy $(\langle C\rangle - e) - (\langle C\rangle - e)^2 \subseteq C$. Tegyük fel, hogy van olyan $p \in (\langle C\rangle - e)^2$, amelyre $p \in C$. Mivel $p \in (\langle C\rangle - e)^2$, ezért $p = q_1 q_2 \dots q_k$, ahol $q_1, q_2, \dots, q_k \in C$ és $k > 1$. Ez azonban (13.1) szerint lehetetlen. Ez azt jelenti, hogy $p \notin C$, amiből kapjuk, hogy $C \cap (\langle C\rangle - e)^2 = \emptyset$, azaz $C = (\langle C\rangle - e) - (\langle C\rangle - e)^2$. □

Az alábbi egyszerű példából következik, hogy nem minden bázis kód.

13.4. Példa. *Az $\{a,b\}^+$ szabad félcsoport $M=\{a^2,a^3,\dots,a^k,\dots\}$ részfélcsoportjának bázisa $\{a^2,a^3\}$, de például $a^5=a^2a^3=a^3a^2$, ezért (13.2) szerint nem kód.*

Az X^* [X^+] szabad monoid [félcsoport] M részmonoidját [részfélcsoportját] X^* [X^+] *szabad részmonoidjá*nak [*részfélcsoport*jának] nevezzük, ha izomorf egy szabad monoiddal [félcsoporttal], azaz ha a C bázisa kód, szokásos jelöléssel $M=C^*$ [$M=C^+$]. Ha $M=\{e\}$, akkor bázisa $\emptyset$, amelyre (13.1) nyilvánvalóan teljesül, azaz $e=\emptyset^*$ az üres halmaz feletti szabad monoid, amit már az 1.1. alfejezetben is láttunk.

A következő tétel szükséges és elegendő feltételeket ad arra, hogy egy szabad monoid részmonoidja mikor szabad.

13.5. Tétel. *Az X^* szabad monoid bármely M részmonoidjára az alábbi három feltétel ekvivalens:*
(i) M az X^* szabad részmonoidja;
(ii) Minden $p\in X^*$ szóra, az $Mp\cap M\neq\emptyset$ és a $pM\cap M\neq\emptyset$ feltételekből következik, hogy $p\in M$;
(iii) Minden $p\in X^*$ szóra, az $Mp\cap M\cap pM\neq\emptyset$ feltételből következik, hogy $p\in M$.

Bizonyítás Az $(i)\Longrightarrow(ii)$ implikáció helyességének igazolásához tegyük fel, hogy M az X^* szabad részmonoidja és C az M bázisa. Mivel $e\in M$, ezért e-re (ii) triviálisan teljesül. Legyen $p\in X^+$ olyan szó, amelyre $Mp\cap M\neq\emptyset$ és $pM\cap M\neq\emptyset$. Akkor vannak olyan $m_1,m_2\in M$, amelyekre $m_1p\in M$ és $pm_2\in M$. Mivel M félcsoport, ezért

$$(m_1p)m_2=m_1(pm_2)\in M.$$

De C az M bázisa, így C-nek vannak olyan

$$p_1,\dots,p_i,p_{i+1},\dots p_k,q_1,\dots,q_j,q_{j+1},\dots,q_l$$

elemei, amelyekre

$$m_1p=p_1\dots p_i,\quad m_2=p_{i+1}\dots p_k,\quad m_1=q_1\dots q_j,\quad pm_2=q_{j+1}\dots q_l.$$

De M szabad monoid, ezért (13.1) szerint

$$k=l\quad\text{és}\quad p_1=q_1,p_2=q_2,\dots,p_k=q_k,$$

amiből kapjuk, hogy $p=p_{j+1}\dots p_i\in M$. Ezzel megmutattuk az $(i)\Longrightarrow(ii)$ implikációt.

Az $(ii) \Longrightarrow (iii)$ implikáció nyilvánvalóan igaz.

Az $(iii) \Longrightarrow (ii)$ implikáció helyességének igazolásához legyen a $p \in X^*$ olyan szó, amelyre $Mp \cap M \neq \emptyset$ és $pM \cap M \neq \emptyset$, azaz vannak olyan $m_1, m_2 \in M$, amelyekre $m_1 p \in M$ és $pm_2 \in M$. Mivel M félcsoport, ezért

$$(pm_2m_1)p = p(m_2m_1p) = (pm_2)(m_1p) \in M,$$

ami azt jelenti, hogy $Mp \cap M \cap pM \neq \emptyset$, s így $p \in M$.

Végül megmutatjuk, hogy az $(ii) \Longrightarrow (i)$ implikáció is igaz. Legyenek a C bázisnak $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_n$ olyan elemei, amelyekre

$$p_1p_2 \ldots p_n = q_1q_2 \ldots q_n$$

teljesül. Így van olyan $u \in X^*$, amelyre $p_1 = q_1u$ vagy $q_1 = p_1u$, azaz $up_2 \ldots p_n = q_2 \ldots q_n$ vagy $p_2 \ldots p_n = uq_2 \ldots q_n$. Mindkét esetben azt kapjuk, hogy $Mu \cap M \neq \emptyset$ és $uM \cap M \neq \emptyset$, amiből (ii) szerint következik, hogy $u \in M$. Mivel C bázis, ezért $u = e$, azaz $p_1 = q_1$, amiből $p_2 \ldots p_n = q_2 \ldots q_n$. Ezt az eljárást folytatva, kapjuk, hogy $p_2 = q_2, \ldots, p_n = q_n$. Ez a 13.2 Lemma szerint azt jelenti, hogy M szabad részmonoidja X^*-nak. □

13.4. A Sardinas–Patterson kritérium

Szükséges és elegendő feltételt adunk arra, hogy egy nyelv milyen fetételek mellett kód.

13.6. Tétel. *(Sardinas–Patterson kritérium) Legyen C az X^+ szabad félcsoport egy nemüres részhalmaza. Vezessük be a $D_0 = C$ jelölést és definiáljuk minden pozitív egész n-re a*

$$D_n = \{p \in X^+; D_{n-1}p \cap C \neq \emptyset \text{ vagy } Cp \cap D_{n-1} \neq \emptyset\} \tag{13.3}$$

halmazt. A C halmaz akkor és csak akkor kód, ha minden pozitív egész n-re $C \cap D_n = \emptyset$.

Bizonyítás Tegyük fel, hogy C kód. azaz $M = C^*$. Először n szerinti teljes indukcióval megmutatjuk, hogy ha $p \in D_n$, akkor $C^*p \cap C^* \neq \emptyset$. Ha $p \in D_0 = C$, akkor nyilvánvalóan igaz az állítás. Tegyük fel, hogy az állítás igaz D_{n-1} $(n \geq 1)$ minden elemére és legyen $p \in D_n$. Akkor van olyan $c \in C$ és $d \in D_{n-1}$, hogy $dp = c$ vagy $cp = d$. Az indukciós feltevés szerint vannak olyan $m_1, m_2 \in M$, amelyekre $m_1d = m_2$. Ebből következik, hogy

$$m_1c = m_1dp = m_2p \quad \text{vagy} \quad m_2 = m_1d = m_1cp.$$

Mindkét esetben azt kapjuk, hogy $C^*p \cap C^* \neq \emptyset$.

Tegyük fel most, hogy van olyan n pozitív egész szám, amelyre $C \cap D_n \neq \emptyset$. Akkor léteznek olyan $c, c_1 \in C$ és $d_1 \in D_{n-1}$, amelyekre $d_1c = c_1$ vagy $c_1c = d_1$. Az előzőek szerint $C^*d_1 \cap C^* \neq \emptyset$. Ha $d_1c = c_1$, akkor $d_1C^* \cap C^* \neq \emptyset$. Így a 13.5 Tétel szerint $d_1 \in C^*$. Ez azonban lehetetlen, mivel C a C^* bázisa. Következésképpen $c_1c = d_1 \in C^* \cap D_{n-1}$. Ha $n = 1$, akkor $d_1 \in D_0 = C$, ami szintén lehetetlen. Ezért $n > 1$. Ebben az esetben van olyan $d_2 \in D_{n-2}$ és $c_2 \in C$, hogy $d_2d_1 = c_2$ vagy $c_2d_1 = d_2$. Ha $d_2d_1 = c_2$, akkor $d_2C^* \cap C^* \neq \emptyset$. Mivel $C^*d_2 \cap C^* \neq \emptyset$, ezért újra a 13.5 Tétel szerint $d_2 \in C^*$. Ez azonban, mert C bázis, ismét lehetetlen. Tehát

$$d_2 = c_2d_1 = c_2c_1c \in C^* \cap D_{n-2}.$$

Ha $n = 2$, akkor ez ismét lehetetlen. Ha $n > 2$, akkor ezt az eljárást folytatva, az n-edik lépésben kapjuk, hogy $d_n = c_n \dots c_2c_1c \in C$, ami lehetetlen. Ez azt jelenti, hogy minden pozitív egész n-re $C \cap D_n = \emptyset$.

Megfordítva, tegyük fel, hogy minden pozitív egész n-re $C \cap D_n = \emptyset$. Először k szerinti teljes indukcióval megmutatjuk, hogy minden $k \geq 1$ és $n \geq 1$ esetén $C^k \cap D_n = \emptyset$. Ha $k = 1$, akkor a feltevés miatt igaz az állítás. Tegyük fel, hogy $1 \leq k$ esetén minden n pozitív egész számra igaz az állítás. Ha $D_n = \emptyset$, akkor nyilvánvalóan $C^{k+1} \cap D_n = \emptyset$. Tegyük fel, hogy $D_n \neq \emptyset$. Ha $p \in C^{k+1} \cap D_n$, akkor $p = c_1c_2 \dots c_{k+1} \in D_n$. Így D_{n+1} definíciója miatt $c_2 \dots c_{k+1} \in C^k \cap D_{n+1}$, ami az indukciós feltevés miatt lehetetlen. Ez azt jelenti, hogy $C^{k+1} \cap D_n = \emptyset$. Másodszor szintén k szerinti teljes indukcióval belátjuk, hogy minden $k \geq 1$, $n \geq 1$ és $t \geq 0$ esetén $C^k \cap D_nC^t = \emptyset$. A $k = 1$ esetben az állítás nyilvánvalóan igaz. Tegyük fel, hogy $k \geq 1$ esetben igaz az állítás. Ha $p \in C^{k+1} \cap D_nC^t$, akkor az először bebizonyítottak szerint $t > 0$. Ez azt jelenti, hogy

$$p = c_1c_2 \dots c_{k+1} = d_nc_1'c_2' \dots c_t' \quad (c_1, c_2, \dots c_{k+1}, c_1', c_2', \dots c_t' \in C,\ d_n \in D_n).$$

Amiből következik, hogy van olyan $d_{n+1} \in X^*$, amelyre

$$d_n = c_1d_{n+1}, \quad c_2 \dots c_{k+1} = d_{n+1}c_1'c_2' \dots c_t',$$

vagy

$$c_1 = d_nd_{n+1}, \quad d_{n+1}c_2 \dots c_{k+1} = c_1'c_2' \dots c_t'.$$

Az első esetben

$$d_{n+1} \in D_{n+1}, \quad c_2 \dots c_{k+1} = d_{n+1}c_1'c_2' \dots c_t' \in C^k \cap D_{n+1}C^t,$$

ami az indukciós feltevés miatt lehetetlen. Mivel $d_n \neq e$, ezért $d_nd_{n+1} = c_1 \in C$ miatt a második esetben $d_{n+1} = e$ és $d_n = c_1$, ami a $C \cap D_n = \emptyset$ feltevés miatt lehetetlen. Így $C^{k+1} \cap D_nC^t = \emptyset$.

Legyenek végül $c_1, c_2, \dots c_n, c'_1, c'_2, \dots c'_n$ a C halmaz olyan elemei, amelyekre

$$c_1 c_2 \dots c_n = c'_1 c'_2 \dots c'_n.$$

Akkor van olyan $d \in X^*$, amelyre $c_1 = c'_1 d$ vagy $c'_1 = c_1 d$. Az általánosság megszorítása nélkül elegendő a $c_1 = c'_1 d$ esettel foglalkozni. Ebben az esetben $dc_2 \dots c_n = c'_2 \dots c'_n$. Ha $d \neq e$, akkor $d \in D_1$ és $n > 1$. Ekkor viszont

$$dc_2 \dots c_n = c'_2 \dots c'_n \in C^{n-1} \cap D_1 C^{n-1},$$

ami szintén lehetetlen. Ezért $d = e$, s így $c_1 = c'_1$. Az eljárást folytatva kapjuk, hogy $c_2 = c'_2, \dots, c_n = c'_n$. A 13.2 Lemma szerint ez azt jelenti, hogy C kód. □

A tétel akkor is igaz, ha

$$D_n = \{p \in X^+; pD_{n-1} \cap C \neq \emptyset \text{ vagy } pC \cap D_{n-1} \neq \emptyset\}, \tag{13.4}$$

azaz a D_n halmazokat C elemeinek bizonyos prefixeivel definiáljuk. A D_n halmazok definíciójából látható, hogy elemeik a C elemeinek megfelelő szuffixei [prefixei], ezért minden véges C halmazhoz véges sok különböző D_n konstruálható. Vagyis a tétel egy algoritmust ad annak eldöntésére, hogy az X^+ egy nemüres véges részhalmaza kód vagy nem. (Vannak olyan n és k pozitív egész számok, amelyekre $D_{n+k} = D_n$.) Ezt az algoritmust *Sardinas–Patterson algoritmus*nak nevezzük.

Kódok közös része és különbsége szintén kód. Ha kódokra a reguláris műveleteket alkalmazzuk, akkor azonban nem kapunk mindig kódot. Ezt a következő egyszerű példa is mutatja.

13.7. Példa. *A 13.6 Tétel segítségével (vagy más módon) megmutatható, hogy* $C_1 = \{a, ba\}$ *és* $C_2 = \{a, ab\}$ *nyelvek kódok az* $\{a, b\}$ *halmaz felett. Ha például* C_1*-re alkalmazzuk a Sardinas–Patterson algoritmust, akkor* $D_1 = \emptyset$ *és így* $D_n = \emptyset$ $(n = 2, 3, \dots)$*. A 13.2 Lemmát használva kapjuk, hogy* $C_1 + C_2 = \{a, ab, ba\}$ *nem kód, mert például* $aba = (ab)a = a(ba)$*. A* $C_1 C_2 = \{a^2, ba^2, a^2b, ba^2b\}$ *szorzat sem kód, mivel például az* a^2ba^2 *szó előállítható az* a^2 *és a* ba^2 *ill. az* a^2b *és az* a^2 *szavak szorzataként is.*

A 13.1 Lemmából következik ugyan az alábbi állítás, de nyilvánvaló, hogy egy kód iteráltja nem kód.

13.8. Következmény. *Ha* C *kód, akkor minden* $n > 1$ *egész számra* C^n *is kód.*

13.5. Prefix, szuffix és bifix kódok

A kódoknak jól kezelhető osztályait kapjuk, ha (13.3)-ban vagy (13.4)-ben $D_1 = \emptyset$, s így minden n pozitív egész számra $D_n = \emptyset$. Ezeket a kódokat *prefix kódok*nak ill. *szuffix kódok*nak nevezzük. Vagyis a prefix [szuffix] kódok azok a $C \subseteq X^+$ nyelvek, amelyekre

$$CX^+ \cap C = \emptyset \quad [X^+C \cap C = \emptyset]. \tag{13.5}$$

A prefix [szuffix] kódok tehát azok a nyelvek, amelyek nem tartalmazzák elemeik egyetlen valódi kezdő [záró] szeletét sem. Prefix [szuffix] kód minden részhalmaza szintén prefix [szuffix] kód. Ha C prefix és szuffix kód, akkor *bifix kód*nak hívjuk.

Megjegyezzük, hogy a 4.3 Tétel bizonyításában az

$$\{a, b, \longrightarrow, \#, S, X_1, X_2, \dots\}$$

halmaz elemeit kódoltuk a a^+b prefix kód elemeivel.

Minden n pozitív egész számra X^n bifix kód X felett. Az X^n $(n \geq 1)$ részhalmazait *n hosszúságú kódok*nak hívjuk. Ha valamely n pozitív egész számra $C \subseteq X^n$, akkor azt is mondjuk, hogy C *uniform kód* vagy *blokk kód*. Az $\emptyset$ üres kódot is uniform kódnak tekintjük. Az uniform kódok fontos szerepet játszanak a kódok gyakorlati alkalmazásában. Az uniform kódok között kiemelkedő jelentőségűek a lineáris kódok. Egy n dimenziós vektortér k dimenziós altereit *[n,k] lineáris kód*oknak nevezzük. A lineáris kódokkal nem foglalkozunk, de tanulmányozásukhoz bőséges irodalom áll az olvasó rendelkezésére. Ezek közül az olvasó figyelmébe ajánljuk Jacob van Lint [32] monográfiáját.

Ha $L(\subseteq X^+)$ tetszőleges nyelv, akkor

$$L - LX^+ \quad [L - X^+L,\ L - (LX^+ + X^+L)]$$

prefix [szuffix, bifix] kód. Ez azt jelenti, hogy véges nyelvből véges számú lépésben előállíthatunk prefix [szuffix, bifix] kódot, ha elhagyjuk a nyelvből azokat a szavakat, amelyek egy másik szónak kezdő [záró, kezdő vagy záró] szeletei.

Egy S félcsoport M részfélcsoportját *bal* [*jobb*] *unitér*nek nevezzük, ha minden $s \in S$ elemre az $Ms \cap M \neq \emptyset$ $[sM \cap M \neq \emptyset]$ feltételből következik, hogy $s \in M$, vagyis, ha $m, ms[sm] \in M$, akkor $s \in M$. Ha M bal és jobb unitér, akkor M-et *unitér*nek hívjuk. A 13.5 Tételből következik, hogy X^* minden [bal, jobb] unitér részmonoidja X^*-nak szabad részmonoidja.

13.9. Tétel. *Az X feletti C nyelv akkor és csak akkor prefix [szuffix, bifix] kód, ha X^* egy bal unitér [jobb unitér, unitér] részmonoidjának bázisa.*

Bizonyítás Az $\emptyset$ kód bifix kód és az $\{e\}$ unitér részmonoid bázisa. Ezért a továbbiakban feltehetjük, hogy $C \neq \emptyset$.

Legyen C prefix kód. Ha $p \in C^+$, $q \in X^+$ és $pq \in C^+$, akkor $p = c_1c_2 \dots c_k$ és $pq = d_1d_2 \dots d_l$ valamilyen C-beli $c_1, c_2, \dots, c_k$ és $d_1, d_2, \dots, d_l$ elemekre, azaz

$$c_1c_2 \dots c_kq = d_1d_2 \dots d_l.$$

Ez azt jelenti, hogy c_1 a d_1 kezdőszelete vagy d_1 a c_1 kezdőszelete. Mivel C prefix kód, ezért $c_1 = d_1$, s így

$$c_2 \dots c_kq = d_2 \dots d_l.$$

Ugyanígy kapjuk, hogy $c_2 = d_2$, $\dots c_k = d_k$. Ezért $q = d_{k+1} \dots d_l \in C^+$, tehát C^* az X^* bal unitér részmonoidja. Hasonlóan kapjuk szuffix [bifix] kód esetén az állítást.

Megfordítva, tegyük fel, hogy $C \neq \emptyset$ az X^* M bal unitér részmonoidjának bázisa. Legyenek $c, d \in C$ és c kezdőszelete d-nek, azaz van olyan $u \in X^*$, hogy $d = cu$. Mivel M bal unitér, ezért $u \in M$. Minthogy C az M bázisa, így $u = e$ és $c = d$. Ez azt jelenti, hogy C prefix kód. Hasonlóan látható be, hogy X^* egy jobb unitér [unitér] részmonoidjának bázisa szuffix [bifix] kód. □

13.6. Erős kódok

A felfogásunk szerint ez az alfejezet már nem tartozik az algebrai kódelmélet alapjaihoz. Azonban az alábbi 13.11 Tétel is mutatja, hogy szorosan kapcsolódik az algebrai nyelvelmélethez, ezért célszerűnek látszott ebben a bevezető fejezetben tárgyalni.

Az X ábécé feletti C kódot *erős kód*nak nevezzük, ha

$$\forall(u, v \in X^*, w \in C^*) \quad (uwv \in C^* \iff uv \in C^*). \tag{13.6}$$

Nyilvánvaló, hogy minden erős kód bifix kód. Ha $C \subseteq X$, akkor C erős kód. Az X^n $(n \geq 1)$ uniform kódok is erős kódok. Az üres kód is ($\emptyset^* = e$!) erős kód. Mint a következő példa is mutatja, az erős kódok osztálya a bifix kódok osztályának valódi részosztálya.

13.10. Példa. *Az $X = \{a, b\}$ ábécé felett $C = \{ab, a^2b^2\}$ bifix kód, de nem erős kód. (Például $a^3b^3 = a(a^2b^2)b \notin C^*$, bár $ab, a^2b^2 \in C^*$.)*

Legyen L tetszőleges X feletti nyelv.Továbbá ϑ_L a (7.5) feltétellel definiált szintaktikus kongruencia, és $\vartheta_L[p]$ a $p \in X^*$ szót tartalmazó ϑ_L-osztály.

13.11. Tétel. *Tetszőleges X ábécé feletti L nyelv esetén $\vartheta_L[e]$ az X^* szabad monoid olyan unitér részmonoidja, amelynek bázisa erős kód. Megfordítva, bármely X feletti C erős kódhoz van olyan $L(\subseteq X^*)$ nyelv, amelyre $\vartheta_L[e] = C^*$.*

Bizonyítás Minthogy $L = \emptyset$ akkor és csak akkor, ha $\vartheta_L[e] = e = \emptyset^*$, ezért a továbbiakban feltehetjük, hogy $L \neq \emptyset$.

Mivel ϑ_L az X^* szabad monoid kongruenciája, ezért $\vartheta_L[e]$ részmonoidja X^*-nak. Megmutatjuk, hogy $\vartheta_L[e]$ C bázisa kód. Tegyük fel, hogy

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_n, \quad p_i, q_j \in C, i, j = 1, 2, \dots, n.$$

Legyen például $p_1 = q_1 t \ \ (t \in X^*)$, akkor

$$(e, q_1) \in \vartheta_L \quad \Longrightarrow \quad (t, p_1) \in \vartheta_L \quad \Longrightarrow \quad (t, e)\vartheta_L,$$

amiből $t = e$, s így $p_1 = q_1$ következik. (A $q_1 = p_1 t$ esetből hasonlóan $p_1 = q_1$ következik.) Kaptuk, hogy $p_2 \dots p_n = q_2 \dots q_n$. Ezt folytatva adódik, hogy $p_2 = q_2, \dots, p_n = q_n$. A 13.2 Lemma szerint C kód.

Az nyilvánvaló, hogy $\vartheta_L[e]$ bázisa erős kód. Mivel minden erős kód bifix kód, ezért 13.9 Tétel szerint $\vartheta_L[e]$ unitér.

Megfordítva, megmutatjuk, hogy ha C erős kód X felett és $L = C^*$, akkor $\vartheta_L[e] = C^*$. Mivel $e \in L$, ezért a 7.3 Lemma szerint, ha $w \notin L$, akkor $w \notin \vartheta_L[e]$. Legyen $w \in L = C^*$. C erős kód, ezért bármely $u, v \in X^*$ szavakra $uv = uev \in C^* = L$ akkor és csak akkor, ha $uwv \in C^* = L$. Ez azt jelenti, hogy $w \in \vartheta_L[e]$, azaz $\vartheta_L[e] = C^*$. □

Az alfejezet további részében a gyakorlati szempontból is fontos véges erős kódokkal foglalkozunk.

13.12. Lemma. *Bármely X ábécé feletti egyelemű C kód akkor és csak akkor erős kód, ha valamely $a \in X$ betűre és k pozitív egész számra $C = a^k$.*

Bizonyítás Bármely $a \in X$ elemre és k pozitív egész számra a^k erős kód.

Megforditva, legyen az X feletti C egyelemű kód erős kód. Ha $|X| = 1$, akkor nyilvánvalóan igaz az állítás, ezért feltehetjük, hogy $|X| \geq 2$. Legyen $C = u \ \ (u \in X^+)$ és $u = a^i bw$, ahol $a, b \in X$, $a \neq b$, $1 \leq i$ és $w \in X^*$. Minthogy $a^i ubw \neq u$, ezért u nem erős kód. □

13.13. Lemma. *Az X ábécé feletti kételemű C kód akkor és csak akkor erős kód, ha $C \subseteq X$.*

Bizonyítás Ha $C \subseteq X$, akkor nyilvánvalóan erős kód. Tegyük fel, hogy $C = \{p, q\}$ erős kód X felett, de $C \not\subseteq X$. Legyen például $|p| > |q|$ és $p = ar,\ a \in X$, $r \in X^+$. (A $|q| > |p|$ eset ugyanígy bizonyítható.) Tekintsük a $w = aqr$ szót.

Ha $w = pq = arq$, akkor $qr = rq$. Ebből a 12.42 Lemma szerint $p = af^i$ és $q = f^j$, ahol $f \in X^+$ primitív szó és $1 \leq j \leq i$. Mivel C szuffix kód, ez nem lehetséges.

Ha $w = qp = qar$, akkor $aq = qa$. Szintén a 12.42 Lemma szerint $q = a^i$ $(1 \leq i)$. Tekintsük most az $apr = a(ar)r$ szót. Könnyen belátható, hogy $a(ar)r \neq q^k$ bármely k pozitív egész számra. Ha $apr = a(ar)r = pp = (ar)(ar)$, akkor $ar = ra$, vagyis a 12.42 Lemma szerint $r = a^j$ és $p = a^{j+1}$ valamilyen j pozitív egész számra. Ez lehetetlen, mivel $q = a^i$. De $apr = a(ar)r$ nem lehet egyenlő a $pq^k,\ q^kp$ és q^spq^{k-s} szavak egyikével sem.

Ha $w = q^i$, akkor $i \geq 3$. Mivel C szuffix kód, ez is lehetetlen.

Ez azt jelenti, hogy $|p| = |q|$. Legyen $|p| = |q| \geq 2$. Tegyük fel, hogy $p = a^n$ vagy $q = a^n\ \ (a \in X)$. Ha például $p = a^n$ és $2 \leq n$, akkor $aqa^{n-1} \in C^+$. Ha $q = rb$, ahol $r \in X^+$ és $b \in X$, akkor $ar, ba^{n-1} \in C$. Ha $ar = p = a^n$, akkor $r = a^{n-1}$. Ha $ba^{n-1} = p = a^n$, akkor $b = a$ és $q = rb = a^n = p$. Ha pedig $ba^{n-1} = q = rb$, akkor $a = b$ és ismét $p = q$, ami lehetetlen. (A $q = a^n\ \ (n \geq 2)$ eset hasonlóan bizonyítható.)

Ha $ar = q = rb$ és $ba^{n-1} = p = a^n$, akkor $b = a$ és $ar = q = ra$. Ha pedig $ar = q = rb$ és $ba^{n-1} = q = rb$, akkor $a = b$ és ismét $ar = q = ra$. Mivel $|q| = n$, ezért mindkét esetben a 12.42 Lemma szerint $r = a^{n-1}$ és így $p = q$. Ellentmondás.

Tegyük fel, hogy $p \neq a^n$. Legyen $p = a^ibw$, ahol $1 \leq i,\ b \in X,\ b \neq a$ és $w \in X^*$. Akkor minden k pozitív egész számra $(a^i)^k(bw)^k \in C^+$. Ezért valamilyen $j \geq 2$ egész számra $q = a^j$, ami fentebbiek szerint szintén ellentmondás.

Ezek azt jelentik, hogy $|p| = |q| = 1$, vagyis $C \subseteq X$. □

13.14. Lemma. *Legyen C az X ábécé felett legalább háromelemű véges erős kód. Ha $C \not\subseteq X$, akkor léteznek olyan $a, b \in X$ betűk és olyan $n \geq 2$ egész szám, amelyekre $a^n, b^n \in C$.*

Bizonyítás Ha nincs olyan szó C-ben, amelyben szerepel legalább két különböző betű, akkor $C \not\subseteq X$ feltétel miatt van olyan $a \in X$ és $n \leq 2$ egész szám, hogy $a^n \in C$. Ha $b \in X$, $b \neq a$ és i olyan olyan pozitív egész szám, hogy $b^i \in C$, akkor $ab^ia^{n-1} \in C^+$. Ha $i = 1$, akkor $aba^{n-1} \in C$. Ha pedig $i > 1$, akkor $ab^j \in C$ valamilyen $1 \leq j < i$ egész számra. Ellentmondás.

Tehát van van olyan szó C-ben, amelyben szerepel legalább két különböző betű, azaz vannak olyan $a, b \in X\ \ (a \neq b)$ betűk, i pozitív egész szám és $v \in X^*$ szó, amelyekre $a^ibv \in C$. Tegyük fel, hogy i_0 a legkisebb ilyen tulajdonságú i. Minthogy C erős kód, ezért minden k pozitív egész számra $(a^{i_0})^k(bv)^k \in C^+$.

De C véges, így van olyan $n > i_0$ pozitív egész szám, hogy $a^n \in C$. Mivel $(a^{i_0})^n(bc)^n \in C^+$, ezért $(bv)^n = bw \in C^+$, ahol $w = v(bv)^{n-1}$. Amiből minden k pozitív egész számra $b^k w^k \in C^+$, így $b^j \in C$ valamilyen j pozitív egész számra.

Megmutatjuk, hogy $j = n$. Mivel $a^n, b^j \in C$, ezért minden k pozitív egész számra $a^s(b^j)^k a^{n-s} \in C^+$ $(s = 1, \ldots, n-1)$. Ismét C végessége miatt $a^s b^{m_s} \in C$ valamilyen m_s $(s = 1, \ldots, n-1)$ pozitív egész számokra. Mivel C szuffix kód, ezért az m_s $(s = 1, \ldots, n-1)$ számok mind különbözőek és $j > m_s$, azaz $j \geq n$. Hasonlóan látható be, hogy $n \geq j$, vagyis $n = j$. □

13.15. Következmény. *Ha C az X ábécé felett véges erős kód, akkor*

$$(\forall a \in X, p \in X^*) \quad (ap \in C^+ \iff pa \in C^+). \tag{13.7}$$

Bizonyítás Feltehetjük, hogy $p \neq e$. Ha $|C| = 1$, akkor 13.12 Lemmából következik az állítás. Tegyük fel, hogy $|C| \geq 2$. Ha $C \subseteq X$, akkor állítás nyilvánvalóan igaz. Ha $C \not\subseteq X$ és $ap \in C^+$, akkor az előző lemma bizonyítása szerint van olyan $n \geq 2$ egész szám, amelyre $a^n \in C$. De C erős kód, ezért $a^n(pa) = a^{n-1}(ap)a \in C^+$, s így $pa \in C^+$. Ha $pa \in C^+$, akkor $(ap)a^n = a(pa)a^{n-1} \in C^+$, azaz $ap \in C^+$. □

13.16. Lemma. *Legyen C az X ábécé felett véges erős kód. Ha $a^n, b^n \in C$ $a, b \in X$ és $n \geq 1$, akkor*

$$ab^{n-1},\ b^{n-1}a,\ a^{n-1}b, ba^{n-1} \in C.$$

Bizonyítás Azt mutatjuk meg, hogy $ab^{n-1} \in C$. A 13.15 Következmény segítségével könnyen belátható, hogy $ba^{n-1} \in C$. Az $a^{n-1}b,\ ba^{n-1} \in C$ hasonlóan látható be.

Ha $a = b$ vagy $n = 1$, az állítás semmitmondó, ezért feltehetjük, hogy $a \neq b$ és $n \geq 2$. Mivel C erős kód, ezért $ab^n a^{n-1} \in C^+$. De C bifix kód, így $ab^r \in C$ valamely $1 \leq r < n$ egész számra. Ha $n = 2$, akkor $n - 1 = r = 1$.

Legyen $n \geq 3$ és $r \leq n-2$. A C kód erős kód, ezért $a^{n-1}b^{(n-1)r} \in C^+$. De $a^{n-1} \notin C$, így van olyan $1 \leq m \leq n-1$ egész szám, amelyre $a^{n-1}b^m \in C$. Ha $m = 1$, akkor $b^{(n-1)r-1} \in C^+$, azaz $(n-1)r - 1 = kn$ valamilyen k pozitív egész számra. Amiből $n(r-k) = r+1$. De $r \leq n-2$, ezért ez lehetetlen. Ez azt jelenti, hogy $1 < m \leq n-1$. A 13.15 Következmény szerint $b^{m-1}a^{n-1}b \in C^+$. Amiből következik, hogy van olyan $1 \leq j < n-1$ egész szám, amelyre $a^j b \in C$. A 13.15 Következmény szerint $ba^j \in C^+$. Nyilvánvaló, hogy $ba^j \in C$. Mivel C erős kód, ezért $a^{n-1}(ba^j)a \in C^+$. Sőt

$$a^{n-1}(ba^j)a = (a^{n-1}b)a^{j+1} \in C,$$

így minden i pozitív egész számra

$$p_i = (a^{n-1}b)(a^jb)^ia^{j+1} \in C^+.$$

Teljes indukcióval megmutatjuk, hogy minden i pozitív egész számra $p_i \in C$.

Legyen $i = 1$, azaz $p_1 = (a^{n-1}b)(a^jb)a^{j+1}$. Már az előzőekben láttuk, hogy $a^{n-1}b \notin C$. Mivel $(a^{n-1}b)a^{j+1} \in C$, ezért minden $1 \leq s \leq j$ egész számra $(a^{n-1}b)a^s \notin C$. De $a^{n-1}b)(a^jb)a^t \notin C$ bármely $0 \leq t \leq j$ egész számra, mert $a^{j+1-t} \notin C$. Kaptuk, hogy $p_1 \in C$.

Tegyük fel, hogy $p_i \in C$. Megmutatjuk, hogy

$$p_{i+1} = (a^{n-1}b)(a^jb)^{i+1}a^{j+1} \in C.$$

Az indukciós feltevésből következik, hogy $(a^{n-1}b)(a^jb)^i \notin C$, továbbá

$$(a^{n-1}b)(a^jb)^ia^s \notin C \quad (1 \leq s \leq j.$$

Mivel $a^jb \in C$ és C szuffix kód, ezért

$$a^{n-1}b)(a^jb)^i(a^jb) \notin C.$$

Ebből már a $p_1 \in C$ bizonyításának utolsó lépéséhez hasonló módon kapjuk, hogy $p_{i+1} \in C$. Ez viszont azt jelenti, hogy $|C| = \infty$, ami lehetetlen. Így szükségképpen $r = n - 1$, azaz $a^{n-1}b \in C$. □

13.17. Következmény. *Ha C olyan véges erős kód az $\{a, b\}$ kételemű ábécé felett, amelyre $a^n, b^n \in C$ és $1 \leq n \leq 4$, akkor $C = \{a, b\}^n$.*

Bizonyítás A 13.16 Lemma és a 13.15 Következmény segítségével megmutatható, hogy $1 \leq n \leq 4$ esetekben $\{a, b\}^n \subseteq C$. Mivel C bifix kód, ebből már következik, hogy $C = \{a, b\}^n$. Az $n = 4$ esetben $abab \in C$ igazolásához fel kell közvetlenűl használni a (13.6) definíciót. $((ab^3)(b^2ab) = ab^5ab \in C^+$, de $ab^5ab = (ab)b^4(ab)$, amiből $abab \in C^+$. Könnyen belátható, hogy $abab \in C$. Ebből már az is következik, hogy $baba \in C$.) □

Legyen X tetszőleges ábécé és $p \in X^+$. Legyen $p = a_1^{i_1} \dots a_k^{i_k}$, ahol $a_1, \dots, a_k$ az ábécé X olyan betűi, amelyekre $a_j \neq a_{j+1}$ $(j = 1, \dots, k-1)$. A $p_v = a_1 \dots a_k \in X^+$ szót a p *szó vázá*nak nevezzük. Jelölje az $L \in X^*$ nyelv szavaiban előforduló betűk halmazát $X_L (\subseteq X)$. Ha L véges nyelv, akkor nyilvánvalóan X_L is véges. A következő tétel azt mondja ki, hogy a véges erős kódok uniform kódok.

13.18. Tétel. *Az X ábécé feletti $C \neq \emptyset$ véges kód akkor és csak akkor erős kód X felett, ha $C = Y^n$, ahol $Y \neq \emptyset$ az X ábécé véges részhalmaza és n pozitív egész szám.*

Bizonyítás Ha $Y \neq \emptyset$ az X ábécé (nem szükségképpen véges) részhalmaza és n egy pozitív egész szám, akkor Y^n nyilvánvalóan erős kód.

Megfordíta tegyük fel, hogy $C \neq \emptyset$ az X ábécé felett véges erős kód. Akkor $X_C \neq \emptyset$ az X ábécé véges részhalmaza. Megmutatjuk, hogy $C = X_C^n$ valamiyen n pozitív egész számra. Ha $|C| = 1$, akkor a 13.12 Lemma szerint $C = a^n$ valamilyen n pozitív egész számra. Ha $|C| = 2$, akkor 13.13 Lemma szerint $C = X_C$.

Legyen $|C| \geq 3$. Ha $C \subseteq X$, akkor $C = X_C$. Tegyük fel, hogy $C \not\subseteq X$, akkor a 13.14 Lemma bizonyítása szerint vannak olyan $a, b \in X_C$, $(a \neq b)$ betűk, amelyek előfordulnak egy C-beli szóban. Ebben az esetben azt kaptuk, hogy létezik olyan $n \geq 2$ egész szám, hogy $a^n, b^n \in C$. Ha egy p C-beli szóban csak egy $c \in X_C$ betű szerepel, akkor nyilvánvalóan $p = c^i$ valamilyen i pozitív egész számra. Ezért minden $d \in X_C$ esetén valamilyen i pozitiv egész számra $d^i \in C$. Ha $d \neq a, b$, akkor például $ad^i a^{n-1} \in C^+$. Ha $i = 1$, akkor $ada^{n-1} \in C$. Ha pedig $i > 1$, akkor $ad^j \in C$ valamilyen $1 \leq j < i$ egész számra. A 13.14 Lemma bizonyítása szerint mindkét esetben azt kapjuk, hogy $d^n \in C$, azaz $i = n$. (Így $i = 1$ nem is lehetséges.) Ezek szerint minden $a \in X_C$ esetén $a^n \in C$, ahol $n \geq 2$. Megmutatjuk, hogy $C = X_C^n$.

Ha $a, b \in X_C$, akkor a 13.16 Lemma szerint $ab^{n-1}, ba^{n-1} \in C$. Ha $1 \leq n \leq 4$, akkor 13.17 Következmény alapján $\{a, b\}^n \subseteq C$. Tegyük fel, hogy $n \geq 5$. Mivel $ab^{n-1} \in C$, ezért

$$a^2 b^{n-2} b^n = a^2 (b^{n-1})^2 \in C^+,$$

így $a^2 b^{n-2} \in C^+$. Nem nehéz meggondolni, hogy $a^2 b^{n-2} \in C$. Hasonlóan látható be, hogy minden $2 < r \leq n-2$ egész számra $a^r b^{(n-r)} \in C$. Ezek azt jelentik, hogy minden olyan i és j pozitív egész számra, amelyekre $i+j = n \geq 2$, $a^i b^j \in C$.

Most megmutatjuk, hogy ha $a_1, \ldots, a_k \in X_C$, $a_j \neq a_{j+1}$ $(j = 1, \ldots, k-1)$ és $j_1 + \ldots j_k = n$, akkor

$$p = a_1^{j_1} \ldots a_k^{j_k} \in C.$$

A bizonyítást a p szó p_v vázának hossza szerinti indukcióval végezzük el. Fentebb beláttuk, hogy $|p_v| = 2$ esetben igaz az állítás. Tegyük fel, hogy az állítás igaz minden p olyan szóra, amelyre $|p_v| = i$ és $2 \leq i \leq k < n$. Legyenek

$$a_1, \ldots, a_k, a_{k+1} \in X_C, \quad j_1 + \ldots j_k + j_{k+1} = n, \quad q = a_1^{j_1} \ldots a_k^{j_k} a_{k+1}^{j_{k+1}}.$$

Mivel $j_1 + \ldots j_k + j_{k+1} = n$, ezért

$$a_1^{j_1} \ldots a_k^{j_k + j_{k+1}} \in C.$$

De

$$a_1^{j_1} \ldots a_k^{j_k} a_{k+1}^n a_k^{j_{k+1}} = (a_1^{j_1} \ldots a_k^{j_k} a_{k+1}^{j_{k+1}})(a_{k+1}^{n-j_{k+1}} a_k^{j_{k+1}}) \in C^+.$$

Az indukciós feltevés miatt

$$a_{k+1}^{n-j_{k+1}} a_k^{j_{k+1}} \in C.$$

Ebből következik, hogy

$$q = a_1^{j_1} \dots a_k^{j_k} a_{k+1}^{j_{k+1}} \in C^+.$$

De $a_1^{j_1} \dots a_k^{j_k} \notin C$, ezért valamilyen $1 \le s \le j_{k+1}$ egész számra

$$a_1^{j_1} \dots a_k^{j_k} a_{k+1}^{s} \in C.$$

Ha $s < j_{k+1}$, akkor $a_{k+1}^{j_{k+1}-s} \in C^+$. Ez azonban lehetetlen, mivel $a_{k+1}^{j_{k+1}-s} \notin C$. Ezért $s = j_{k+1}$, azaz $q \in C$. Így az indukció szerint $X_C^n \subseteq C$, de C bifix kód, ezért $C = X_C^n$. □

Feladatok

13.1. Legyen φ az $X \neq \emptyset$ halmaz tetszőleges leképezése az $Y \neq \emptyset$ halmazra. Terjesszük ki φ-t homomorf módon X^*-ra. Ha az X feletti L nyelv nem kód X felett, akkor $\varphi(L)$ sem kód Y felett.

13.2. Legyen n tetszőleges pozitív egész szám. Ha a nemnegatív egész számok valamely I és J részhalmazára

$$i + j \equiv i' + j' \pmod{n} \quad \Longrightarrow \quad (i = i',\ j = j') \quad (i, i' \in I, j, j' \in J),$$

akkor $L = \{a^i b a^j,\ i \in I, j \in J\} \cup \{a^n\}$ kód $\{a, b\}$ felett.

13.3. Az X^+ szabad félcsoport különböző p és q elemeire $\{p, q\}$ akkor és csak akkor kód, ha $pq \neq qp$.

13.4. Mint azt a 12.6. alfejezetben bevezettük, egy $p \in X^+$ szót *primitív*nek nevezünk, ha a $p = q^n$ $(q \in X^+)$ feltételből $n = 1$ és így $p = q$ következik. Ha az $u, v \in X^+$ szavak esetén uv primitív szó, akkor $\{u, v\}$ kód.

13.5. Az $L \subseteq X^*$ nyelvet *reflexív*nek nevezzük, ha minden $p, q \in X^*$ szóra a $pq \in L$ feltételből következik, hogy $qp \in L$. A $C \subseteq X^+$ kódra C^* akkor és csak akkor reflexív, ha

$$(\forall p, q, r \in X^*) \quad (pq, prq \in C^* \quad \Longrightarrow \quad r \in C^*). \tag{13.8}$$

13.6. Az $L \subseteq X^+$ nyelvet *félkód*nak nevezzük, ha

$$p_1 \dots p_k = q_1 \dots q_l \quad (p_1, \dots, p_k, q_1, \dots, q_l \in L) \quad \Longrightarrow \quad k = l. \tag{13.9}$$

(Az (13.1) feltétel szerint minden kód félkód.) Az $L \subseteq X^+$ nyelv akkor és csak akkor félkód, ha minden $n \ge 2$ egész számra L^n félkód.

Ha L félkód, akkor bármely $a \in X$ esetén $|L \cap a^+| \le 1$. Továbbá L egyetlen eleme sem bontható fel L-beli elemek szorzatára.

13.7. Az $L \subseteq X^+$ nyelvet *n-kód*nak nevezzük, ha bármely n elemű részhalmaza kód. Minden félkód 2-kód.

14. fejezet

A kód mértéke

Tetszőleges X ábécé esetén bevezetünk a $P(X^*)$ hatványhalmazon egy mértéket, és segítségével olyan feltételt adunk, amelyet minden X feletti kód teljesít. Megjegyezzük, hogy ha X megszámlálható, akkor X^* is megszámlálható, ezért minden X feletti kód is megszámlálható.

14.1. A Bernoulli mérték

Legyen R_0 [R_+] a nemnegatív [pozitív] valós számok halmaza. Terjesszük ki a valós számok összeadásának és szorzásának műveletét az $R_0 \cup \{\infty\}$ halmazra úgy, hogy

$$r + \infty = \infty + r = \infty \quad (r \in R_0 \cup \{\infty\}),$$

$$r\infty = \infty r = \infty \quad (r \in R_+ \cup \{\infty\}), \quad 0\infty = \infty 0 = 0.$$

Könnyen belátható, hogy $(R_0 \cup \{\infty\}, +, \cdot)$ kommutatív félgyűrű. Az előzőekből következik, hogy minden n pozitív egész számra $(\infty)^n = \infty$. Legyen továbbá $0^0 = (\infty)^0 = 1$. Terjesszük ki a valós számok szokásos rendezését is az $R_0 \cup \{\infty\}$ halmazra, úgy, hogy ∞ legyen a halmaz legnagyobb eleme.

Legyen $V(I)$ az I indexhalmaz véges részhalmazainak halmaza. Definiáljuk az $r_k \in R_0 \cup \{\infty\}$ $(k \in I)$ elemek összegét a

$$\sum_{k \in I} r_k = \bigvee \{ \sum_{j \in J} r_j ; J \in V(I) \}$$

összefüggéssel. Az $R_0 \cup \{\infty\}$-beli *sorok*ra

$$\sum_{k=0}^{\infty} r_k = \bigvee \{ \sum_{k=0}^{n} r_k ; n \in N \} \quad (r_k \in R_0 \cup \{\infty\}).$$

Tetszőleges X halmaz esetén legyen $\mathcal{X}$ az X részhalmazainak olyan halmaza, amelyre ha $A, B \in \mathcal{X}$, akkor $A - B, A + B \in \mathcal{X}$. Ebből következik, hogy $\emptyset \in \mathcal{X}$. A $\pi : \mathcal{X} \to R_0 \cup \{\infty\}$ leképezést *mérték*nek, $\pi(A)$-t pedig A *mérték*ének nevezzük az $\mathcal{X}$ halmazon, ha $\pi(\emptyset) = 0$ és $\mathcal{X}$ tetszőleges A_k $(k \in I)$ páronként diszjunkt részhalmazaira, ha $\sum_{k\in I} A_k \in \mathcal{X}$, akkor

$$\pi(\sum_{k\in I} A_k) = \sum_{k\in I} \pi(A_k).$$

Tekintsük az X halmaz olyan π leképezését a nemnegatív valós számok halmazába, amelyre

$$\sum_{x\in X} \pi(x) = 1 \tag{14.1}$$

teljesül. Jelölje az egyszerűség kedvéért π monoid-homomorf kiterjesztését X^*-ra szintén π. Ez azt jelenti, hogy

$$\pi(x_1 x_2 \dots x_n) = \pi(x_1)\pi(x_2)\dots\pi(x_n) \quad (x_1, x_2, \dots, x_n \in X), \tag{14.2}$$

és

$$\pi(e) = 1. \tag{14.3}$$

Ezután terjesszük ki π értelmezését az X feletti nyelvekre, a kiterjesztést továbbra is π-vel jelölve, a

$$\pi(\emptyset) = 0, \quad \pi(L) = \sum_{q\in L} \pi(q) \quad (L \subseteq X^*) \tag{14.4}$$

összefüggésekkel. Nyilvánvaló, hogy

$$\pi(L) = \bigvee\{\sum_{q\in L(k)} \pi(q); k \in N\}.$$

A (14.1) - (14.4) feltételekkel megadott π függvényt X *Bernoulli mérték*ének vagy *eloszlás*ának nevezzük. Ha minden $x \in X$ elemre $\pi(x) > 0$, akkor π-t *pozitív Bernoulli mérték*nek vagy *eloszlás*nak nevezzük. Ha $X = \{x_j; j \in I\}$, akkor a $\{\pi(x_j); j \in I\}$ halmazt is szokás X *Bernoulli eloszlás*ának nevezni.

Szemléletesen azt mondhatjuk, hogy ha egy jelforrás az X halmaz elemeit meghatározott időközönként véletlenszerűen, a π valószínűségi eloszlás szerint egymástól függetlenül bocsátja ki, akkor egy n hosszúságú információ (közlemény) a jelforrás által véletlenszerűen kibocsátott n hosszúságú jelsorozat, egy n hosszúságú szó az X^* szabad monoidból, amely kibocsátásának valószínűsége (14.2) szerint számítható ki. A $\pi(x)$ számot $x \in X$ jel *előfordulási valószínűség*ének is nevezzük. Ez az elnevezés onnan ered, hogy valamely természetes

nyelven közölt információkban bizonyos betűk gyakrabban fordulnak elő, mint más betűk.

Legyen $L_k \subseteq X^*$ $(k \in I)$. A (14.4) kiterjesztés alapján kapjuk a

$$\pi(\sum_{k\in I} L_k) \leq \sum_{k\in I} \pi(L_k) \tag{14.5}$$

egyenlőtlenséget. Ha az L_k $(k \in I)$ nyelvek páronként diszjunktak, akkor

$$\pi(\sum_{k\in I} L_k) = \sum_{k\in I} \pi(L_k). \tag{14.6}$$

Ebből az X feletti L_1 és L_2 nyelvekre adódik, hogy

$$\pi(L_1L_2) = \pi(\{pq; p \in L_1, q \in L_2\}) \leq \sum_{p\in L_1, q\in L_2} \pi(pq) =$$

$$= \sum_{p\in L_1, q\in L_2} \pi(p)\pi(q) = \sum_{p\in L_1} \pi(p) \sum_{q\in L_2} \pi(q) = \pi(L_1)\pi(L_2).$$

Ezt felhasználva tetszőleges X feletti $L_1, L_2, \ldots, L_n$ nyelvekre fennáll a

$$\pi(L_1L_2 \ldots L_n) \leq \pi(L_1)\pi(L_2) \ldots \pi(L_n) \tag{14.7}$$

egyenlőtlenség. Speciálisan tetszőleges X feletti L nyelvre és minden k nemnegatív egész számra

$$\pi(L^k) \leq (\pi(L))^k, \tag{14.8}$$

továbbá

$$\pi(L^*) \leq \sum_{k=0}^{\infty} \pi(L^k) \leq \sum_{k=0}^{\infty} (\pi(L))^k. \tag{14.9}$$

Így ha $\pi(L) < 1$, akkor $\pi(L^*) < \infty$.

14.1. Lemma. *Az X halmaz bármely π Bernoulli eloszlása olyan mérték az X^* szabad monoidon, amelyre minden n nemnegatív egész számra*

$$\pi(X^n) = 1.$$

Bizonyítás Az előző meggondolásokból látható, hogy egy Bernoulli eloszlás valóban mérték az X^* szabad monoidon.

Megmutatjuk, hogy minden n nemnegatív egész számra

$$\pi(X^n) = \pi(X^{n+1}).$$

Felhasználjuk, hogy 14.4) alapján a 14.1) feltétel $\pi(X) = 1$ alakban is írható. A 1.1. alfejezetben megállapodtunk abban, hogy $X^0 = e$, s így $\pi(X^0) = \pi(e) = 1$. Ezekből már következik, hogy minden n nemnegatív egész számra $\pi(X^n) = 1$.

Ugyanis (14.1) - (14.4) segítségével kapjuk, hogy ha $n \geq 0$, akkor

$$\pi(X^{n+1}) = \sum_{q \in X^{n+1}} \pi(q) = \sum_{p \in X^n, x \in X} \pi(px) = \sum_{p \in X^n, x \in X} \pi(p)\pi(x) =$$

$$= \sum_{p \in X^n} \pi(p) \sum_{x \in X} \pi(x) = \sum_{p \in X^n} \pi(p) = \pi(X^n).$$

□

A (14.1) - (14.4) feltételekkel megadott mértéket az X^*-on is *Bernoulli eloszlás*nak vagy *mérték*nek nevezzük. A 14.1 Lemmából következik, hogy ha $X \neq \emptyset$, akkor $\pi(X^*) = \pi(X^+) = \infty$.

14.2. Kódok Bernoulli mértéke

14.2. Lemma. *Legyen π az X halmaz egy Bernoulli eloszlása. Bármely X feletti C kódra*

$$\pi(C^n) = (\pi(C))^n \quad (n = 0, 1, 2, \dots) \tag{14.10}$$

és

$$\pi(C^*) = \sum_{n=0}^{\infty} (\pi(C))^n. \tag{14.11}$$

Megfordítva, ha π pozitív Bernoulli eloszlás, továbbá az X feletti C nyelvre $\pi(C) < \infty$ és (14.10) teljesül, akkor C kód.

Bizonyítás Először megmutatjuk, hogy bármely (X feletti) kódra (14.10) teljesül. A 14.2 Lemmát is felhasználva

$$\pi(C^n) = \sum_{p_1 \dots p_n \in C^n} \pi(p_1 \dots p_n) = \sum_{p_1, \dots, p_n \in C} \pi(p_1) \dots \pi(p_n) = (\pi(C))^n.$$

Ebből a (14.6) összefüggés miatt

$$\pi(C^*) = \sum_{n=0}^{\infty} \pi(C^n) = \sum_{n=0}^{\infty} (\pi(C))^n.$$

Megfordítva, legyen minden $x \in X$ elemre $\pi(x) > 0$. Tegyük fel, hogy az X feletti C nyelvre $\pi(C) < \infty$ és teljesül (14.10), de C nem kód. A 14.2 Lemma

szerint vannak olyan $p_1, \dots, p_n, q_1, \dots, q_n \in C$, hogy $p_1 \dots p_n = q_1 \dots q_n$ és $p_j \neq q_j$ valamilyen $1 \leq j \leq n$ esetén. Így

$$(\pi(C))^n = \sum_{t_1,\dots,t_n \in C} \pi(t_1) \dots \pi(t_n) = \sum_{t_1,\dots,t_n \in C} \pi(t_1 \dots t_n) \geq$$

$$\geq \sum_{t_1 \dots t_n \in C^n} \pi(t_1 \dots t_n) + \pi(p_1 \dots p_n) = \pi(C^n) + \pi(p_1 \dots p_n).$$

Mivel $\pi(C) < \infty$ és (14.10) szerint

$$\pi(C^n) = (\pi(C))^n < \infty,$$

így $\pi(p_1 \dots p_n) \leq 0$, azaz $\pi(p_1 \dots p_n) = 0$. Ebből következik (14.2) alapján, hogy van olyan $x \in X$, amelyre $\pi(x) = 0$, ami a feltevés miatt lehetetlen. □

14.3. Tétel. *Ha π az X halmaz egy Bernoulli eloszlása, akkor bármely X feletti C kódra*

$$\pi(C) \leq 1, \tag{14.12}$$

továbbá

$$\pi(C) = 1 \quad \Longleftrightarrow \quad \pi(C^*) = \infty. \tag{14.13}$$

Bizonyítás Tegyük fel, hogy (14.12) nem teljesül, azaz van olyan C kód, amelyre $\pi(C) > 1$.

Legyen először C korlátos kód. Ha k az $\{|p|; p \in C\}$ halmaz szuprémuma, akkor $C \subseteq \sum_{j=1}^{k} X^j$. Ebből (14.4), (14.6) és a 14.1 Lemma alkalmazásával kapjuk, hogy minden n pozitív egész számra

$$\pi(C^n) \leq \pi(\sum_{j=1}^{kn} X^j) = \sum_{j=1}^{kn} \pi(X^j) = kn.$$

De (14.10) szerint $\pi(C^n) = (\pi(C))^n$, amiből minden n pozitív egész számra

$$(\pi(C))^n \leq kn.$$

Az elemi analízisből ismert, hogy ez lehetetlen, ha $\pi(C) > 1$. Kaptuk, hogy minden C korlátos kódra $\pi(C) \leq 1$.

Tegyük fel másodszor, hogy C nem korlátos kód. Legyen $C_l = \{p \in C; |p| \leq l\}$. Mivel egy kód minden részhalmaza kód, ezért C_l kód. A C_l definíciója szerint korłátos kód. Az előzőek szerint $\pi(C_l) \leq 1$. Mivel

$$\pi(C) = \bigvee \{\pi(C_l); l = 1, 2, \dots\},$$

ezért $\pi(C) \leq 1$.

A 14.2 Lemma szerint $\pi(C^*) = \sum_{n=0}^{\infty}(\pi(C))^n$, azaz geometriai sor, amelyről az elemi analízisben megmutatják, hogy $\pi(C^*) < \infty$ akkor és csak akkor, ha $\pi(C) < 1$. Ebből pedig következik, hogy $\pi(C) = 1$ akkor és csak akkor, ha $\pi(C^*) = \infty$. □

A 14.3 Tétel szerint minden kódra teljesül a (14.12) egyenlőtlenség. A következő példa mutatja, hogy a (14.12) egyenlőtleséget teljesítő halmazok nem mindegyike kód.

14.4. Példa. *Az $\{a, b\}$ feletti $L = \{ab, aba, a^2b\}$ nyelv minden Bernoulli mértéke teljesíti a (14.12) egyenlőtlenséget. Legyen ugyanis $0 \leq r \leq 1$, amelyre $\pi(a) = r$ és $\pi(b) = 1 - r$. Akkor*

$$\pi(L) = r(1-r) + 2r^2(1-r) = r(1-r)(1+2r).$$

Mivel $r(1-r) \leq \frac{1}{4}$, ezért $\pi(L) < \frac{3}{4}$. Az L nyelv azonban nem kód, minthogy például $(aba)(ab) = (ab)(a^2b)$.

Ha X egy m elemű ábécé és minden $x \in X$ elemre $\pi(x) = m^{-1}$, akkor a π leképezés teljesíti a (14.1) feltételt. Így π-nek a (14.2) - (14.4) feltételekkel megadott kiterjesztése az X ábécé egy Bernoulli eloszlása, amelyet *egyenletes eloszlás*nak vagy *uniform mérték*nek nevezünk. Az egyenletes eloszlás felhasználásával a 14.3 Tételből következik az alábbi egyenlőtlenség.

14.5. Következmény. *(Szilárd–Kraft–McMillan egyenlőtlenség) Ha $X \neq \emptyset$ egy m elemű ábécé és $C = \{p_j; j \in I\}$ egy X feletti kód, akkor*

$$\sum_{j \in I} m^{-|p_j|} \leq 1. \tag{14.14}$$

Bizonyítás Legyen π az X ábécé uniform mértéke. Mivel C kód, ezért a 14.3 Tétel szerint $\pi(C) \leq 1$. A (14.2) és (14.4) feltételek felhasználásával kapjuk, hogy

$$\pi(C) = \sum_{p_j \in C} \pi(p_j) = \sum_{j \in I} m^{-|p_j|}.$$

□

14.6. Példa. *A Szilárd–Kraft–McMillan egyenlőtlenség teljesül az*

$$\{a, a^3b, aba\}, \quad \{a, a^2b, bab, b^2\}$$

nyelvekre, ezért mind a kettő lehet kód az $\{a, b\}$ ábécé felett.

Legyen $C = \{a, a^3b, aba\}$. *Vizsgáljuk meg általánosabban, hogy van-e olyan* $0 < r < 1$ *valós szám, amelyre* $\pi(a) = r$, $\pi(b) = 1 - r$ *és* π *(14.2) - (14.4) kiterjesztésére* $\pi(C) > 1$. *Ha van ilyen* r, *akkor a 14.3 Tétel szerint* C *nem kód. Mivel* $\pi(C) = r + r^3(1 - r) + r^2(1 - r) > 1$ *akkor és csak akkor, ha* $r^3(1 - r) + r^2(1 - r) > 1 - r$, *vagyis* $r^3 + r^2 > 1$. *A számtani és mértani középre vonatkozó egyenlőtlenség szerint* $r^3 + r^2 \geq 2\sqrt{r^5}$, *amiből, ha* $\sqrt[5]{4^{-1}} < r < 1$, *akkor* $\pi(C) > 1$, *azaz* C *nem kód. Persze most a 13.1 Lemma alapján egyszerűbben is beláthattuk volna, hogy* C *nem kód. (Használjuk fel például, hogy* $(a^3b)a = aa(aba)$.*)*

Legyen $C = \{a, a^2b, bab, b^2\}$. *Minthogy* $\pi(C) = r+r^2(1-r)+r(1-r)^2+(1-r)^2 > 1$ *akkor és csak akkor, ha* $r^2(1-r)+r(1-r)^2+(1-r)^2 > 1-r$, *amiből* $1 = r^2+r(1-r)+1-r > 1$, *ez pedig lehetetlen. Így* $\pi(C) = 1$, *ami azt jelenti, hogy* C *lehet kód. A 13.6 Tétel segítségével eldönthetjük, hogy* C *valóban kód-e. Használjuk a 13.6 Tétel jelöléseit, azaz* $D_0 = C$, $D_1 = \{ab\}$, $D_2 = \{b\}$, $D_3 = \{ab, b\} = D_4$. *A* C *halmaz kód* $\{a, b\}$ *felett, mivel* $n = 1, 2, 3$ *esetén* $C \cap D_n = \emptyset$. *(Egyszerűbb a feladatot prefixekkel megoldani, mert ebben az esetben* $D_1 = \emptyset$.*)*

15. fejezet

Maximális kódok

A C kódot *maximális*nak nevezzük, ha nincs olyan D kód, amelyre $C \subset D$ teljesülne. A következő lemma azt mutatja, hogy a maximális kódokból minden kód megkapható.

15.1. Lemma. *Bármely kód részhalmaza egy maximális kódnak.*

Bizonyítás Legyen C tetszőleges kód és $\mathcal{C}$ a C-t tartalmazó kódok halmaza. Nyilvánvaló, hogy $\mathcal{C}$ a halmazelméleti tartalmazásra részbenrendezett halmaz. Mivel kódok bármely láncának elemeit egyesítve ismét kódot kapunk, ezért a Zorn lemma szerint $\mathcal{C}$-ben van maximális elem, azaz van olyan maximális kód, amely tartalmazza C-t. □

15.1. Félcsoportelméti kritérium

15.2. Tétel. *Ha C maximális kód, akkor minden $p \in X^*$ szóra*

$$C^* \cap X^* p X^* \neq \emptyset. \tag{15.1}$$

Bizonyítás Nem nehéz belátni, hogy $|X| = 1$ esetben igaz az állítás. A továbbiakban legyen $|X| > 1$. Tegyük fel, hogy van olyan $p \in X^*$, hogy $C^* \cap X^* p X^* = \emptyset$. Akkor $p \neq e$ és $p \notin C$. Feltehetjük azt is, hogy bármely $r \in X^+$ és $s \in X^*$ esetén $p \neq rsr$. Ha ugyanis ez nem teljesülne, akkor vegyük p helyett a $t = px^{|p|}$ szót, ahol x az X-nek olyan eleme, amely különbözik p első betűjétől. Mivel $X^* t X^* \subseteq X^* p X^*$, így t is olyan szó, amelyre $C^* \cap X^* t X^* = \emptyset$ és ezért $t \notin C$. Továbbá bármely $r \in X^+$ és $s \in X^*$ szavakra $t \neq rsr$.

Azt mutatjuk meg, hogy $C' = C + p$ is kód. Mivel C maximális kód, ezért ez nem lehetséges. Így ebből kapjuk, hogy minden $p \in X^*$ szóra $C^* \cap X^* p X^* \neq \emptyset$.

A 13.2 Lemma szerint C' akkor és csak akkor kód, ha minden C'-beli $c_1, c_2, \ldots, c_n$, $c'_1, c'_2, \ldots, c'_n$ $(n \geq 2)$ elemre a

$$c_1c_2 \ldots c_n = c'_1c'_2 \ldots c'_n$$

egyenletből következik, hogy

$$c_1 = c'_1, c_2 = c'_2, \ldots, c_n = c'_n.$$

Mivel C kód, ezért ha $c_i, c'_i (i = 1, 2, \ldots, n)$ C-beli elemek, akkor igaz az állítás. A $C^* \cap X^*pX^* = \emptyset$ feltétel miatt a $c_1c_2 \ldots c_n = c'_1c'_2 \ldots c'_n$ egyenletben valamely c_i akkor és csak akkor egyenlő p-vel, ha van p-vel egyenlő c'_j is. Tegyük fel, hogy az egyenletben vannak olyan c_i, c'_j, amelyek egyenlők p-vel. Az elemek száma szerinti teljes indukcióval megmutatjuk, hogy ebben az esetben is $c_1 = c'_1, c_2 = c'_2, \ldots, c_n = c'_n$.

Legyen $c_1c_2 = c'_1c'_2$ $(c_1, c_2, c'_1, c'_2 \in C')$. Ha $c_1 = p$, akkor $c'_1 = p$ vagy $c'_2 = p$. Ha $c'_2 = p$, akkor $c_2 = c'_1 = e$, ami lehetetlen. Így $c'_1 = p$, s ezért $c_2 = c'_2$. Hasonlóan látható be a állítás, ha $c_2 = p$.

Tegyük fel, hogy a $2 \leq n$ egész számra igaz az állítás. Legyen

$$c_1c_2 \ldots c_nc_{n+1} = c'_1c'_2 \ldots c'_nc'_{n+1} \quad (c_i, c'_i \in C', i = 1, 2, \ldots, n+1),$$

továbbá c_i ill. c'_j a p első előfordulása balról az egyenlet bal ill. jobb oldalán.

Legyen először $1 < i, j < n + 1$, azaz

$$c_1c_2 \ldots c_{i-1}pc_{i+1} \ldots c_n = c'_1c'_2 \ldots c'_{j-1}pc'_{j+1} \ldots c'_n.$$

Az általánosság megszorítása nélkül feltehetjük, hogy

$$|c_1c_2 \ldots c_{i-1}| \geq |c'_1c'_2 \ldots c'_{j-1}|.$$

Akkor van olyan $u \in X^*$, amelyre

$$c_1c_2 \ldots c_{i-1} = c'_1c'_2 \ldots c'_{j-1}u, \quad upc_{i+1} \ldots c_n = pc'_{j+1} \ldots c'_n.$$

A p szó nem lehet az u prefixe, mert akkor

$$c_1c_2 \ldots c_{i-1} = c'_1c'_2 \ldots c'_{j-1}u$$

miatt $C^* \cap X^*pX^* \neq \emptyset$. Ezért

$$p = uq \quad \text{és} \quad pc_{i+1} \ldots c_n = qc'_{j+1} \ldots c'_n$$

valamilyen $q \in X^+$ szóra. Az utóbbi egyenlőség azt jelenti, hogy van olyan $v \in X^*$, amelyre $p = qv$. Így $p = uq = qv$. Ha $u \neq e$, akkor $|u| = |v|$, s így

$v \neq e$. Ha $u = qu'$ ($u' \in X^*$) vagy $v = v'q$ ($v' \in X^*$), akkor $p = qu'q$ vagy $p = qv'q$, ami azonban a feltétel miatt lehetetlen. Így $|q| > |u|$ és $|q| > |v|$. Ebből nem nehéz belátni, hogy van q-nak olyan nemüres prefixe és szuffixe, amelyek egyenlők, azaz van olyan $r \in X^+$ és $s \in X^*$, amelyekre $p = rsr$. Ez is lehetetlen, ezért $u = e$, azaz

$$c_1c_2 \dots c_{i-1} = c'_1c'_2 \dots c'_{j-1}, \quad c_{i+1} \dots c_{n+1} = c'_{j+1} \dots c'_{n+1}$$

Az első egyenletben csak C-beli elemek szerepelnek, ezért

$$i = j, \quad c_1 = c'_1, \dots, c_{i-1} = c'_{i-1}.$$

A második egyenletből az indukciós feltevés miatt kapjuk, hogy

$$c_{i+1} = c'_{i+1}, \dots, c_{n+1} = c'_{n+1}.$$

Legyen most $i = 1$ és $1 \leq j < n + 1$. (A $j = n + 1$ eset nem lehetséges, mert akkor $c_2 \dots c_{n+1} = c'_1 \dots c'_n = e$.) Tegyük fel, hogy $j > 1$, akkor

$$pc_2 \dots c_{n+1} = c'_1c'_2 \dots c'_{j-1}pc'_{j+1} \dots c'_{n+1}.$$

A $C^* \cap X^*pX^* = \emptyset$ feltétel miatt p nem lehet $c'_1 \dots c'_{j-1}$ kezdőszelete. Tehát van olyan $q \in X^+$, hogy $p = c'_1 \dots c'_{j-1}q$. Ebből

$$qc_2 \dots c_{n+1} = pc'_{j+1} \dots c'_{n+1},$$

azaz van olyan $r \in X^+$ és $s \in X^*$, hogy $p = rsr$, ami p választása miatt szintén lehetetlen. Ez azt jelenti, hogy $j = 1$. Ebből kapjuk, hogy

$$c_2 \dots c_{n+1} = c'_2 \dots c'_{n+1}.$$

Az indukciós feltevés szerint

$$c_2 = c'_2, \dots, c_{n+1} = c'_{n+1}.$$

Az állítás hasonlóan látható be a $c_{n+1} = p$ esetben. □

A 15.2 Tétel azt mondja ki, hogy ha C maximális kód X felett, akkor X^* bármely $I \neq \emptyset$ ideáljára $C^* \cap I \neq \emptyset$. A tétel segítségével bizonyos kódokról meg tudjuk mutatni, hogy nem maximális kódok. (Ha találunk olyan $p \in X^*$ szót, amelyre $C^* \cap X^*pX^* = \emptyset$, akkor C nem maximális kód.)

15.2. Maximális kódok Bernoulli mértéke

A 14.3 Tételből kaphatunk egy elegendő feltételt arra, hogy egy kód mikor maximális kód.

15.3. Tétel. *Legyen C kód X felett. Ha X-nek π olyan pozitív Bernoulli mértéke, amelyre $\pi(C) = 1$, akkor minden n pozitív egész számra C^n maximális kód.*

Bizonyítás Tegyük fel, hogy teljesülnek a feltételek és a C kód nem maximális. Akkor van olyan $p \in X^+ - C$, hogy $C + p$ is kód. A 14.3 Tételből következik, hogy $\pi(C + p) \leq 1$. Másrészről, (14.6) szerint

$$\pi(C + p) = \pi(C) + \pi(p) = 1 + \pi(p).$$

Így $\pi(p) = 0$, amely a feltevés miatt lehetetlen. Ami azt jelenti, hogy C maximális kód.

A 13.8 Következmény szerint minden n pozitív egész számra C^n is kód. A 14.2 Lemma szerint $\pi(C^n) = (\pi(C))^n = 1$, s így az előbbiek miatt C^n maximális kód. □

A 15.3 Tétel alapján a Szilárd–Kraft–McMillan egyenlőtlenségből kapjuk az alábbi következményt.

15.4. Következmény. *Ha egy m elemű ábécé feletti $C = \{p_j; j \in I\}$ kódra $\sum_{j \in I} m^{-|p_i|} = 1$ teljesül, akkor minden n pozitív egész számra C^n maximális kód.*

15.3. Felbontható kódok

label15.3

A C nem triviális X feletti kódot a (D *kód felett*) *felbontható*nak nevezzük, ha $C \subseteq D^+$. A C nem triviális kódot *felbonthatatlan*nak mondjuk, ha csak önmaga és X felett bontható fel, azaz ha a D kódra $C \subseteq D^+$, akkor $C = D$ vagy $D = X$.

15.5. Lemma. *Minden felbonthatatlan kód maximális kód.*

Bizonyítás Legyen a nem triviális C kód felbonthatatlan, D olyan nem triviális kód, amelyre $C \subseteq D$. Akkor $C \subseteq D^+$, azaz C felbontható D felett. Mivel C felbonthatatlan, ezért $C = D$, vagyis C maximális kód. □

15.6. Lemma. *Végtelen halmaz felett minden maximális kód végtelen.*

Bizonyítás Tegyük fel, hogy C véges maximális kód az X végtelen halmaz felett. C végessége miatt van olyan $x \in X$, amely nem szerepel egyetlen C-beli kódszóban sem. Ebből következik, hogy $C^* \cap X^* x X^* = \emptyset$, ami ellentmond a 15.2 Tétel állításának, s így C nem lehet véges. □

A 15.6 Lemmából adódik, hogy a következő két tételben véges ábécék feletti kódok szerepelnek.

15.7. Tétel. *Ha a C nem triviális véges maximális kód felbontható a D nem triviális kód felett, akkor D is véges maximális kód.*

Bizonyítás Legyen C nem triviális véges maximális kód X felett. Tegyük fel, hogy C felbontható a D nem triviális kód felett. Mivel $C \subseteq D^+$, ezért a

$$pD' = \{d \in D; D^* d D^* \cap C \neq \emptyset\}$$

halmaz nemüres részhalmaza D-nek, így maga is kód. Továbbá minden $c \in C$ szóhoz vannak olyan $d_1, d_2, \ldots d_k \in D$, hogy $c = d_1 d_2 \ldots d_k$. A D' definíciójából következik, hogy $d_1, d_2, \ldots d_k \in D'$, azaz $C^+ \subseteq D'^+$. Ha van olyan $u \in X^+$, amelyre $u \notin D'$ és $D' + u$ kód, akkor $u \notin C$ és $C + u$ szintén kód. Ez azonban ellentmond annak, hogy C maximális kód. Ez azt jelenti, hogy D' is maximális kód, s így $D' = D$. Ebből viszont következik, hogy minden $d \in D$ szóhoz vannak olyan $p, q \in D^*$, hogy $pdq \in C$. De C minden eleme egyértelműen bontható fel véges sok D-beli elem szorzatára. Ezért C végessége miatt D is véges. □

15.8. Tétel. *Bármely C nem triviális véges maximális kód elemei egyértelműen felbonthatók valamely véges nem triviális felbonthatatlan kód elemeinek szorzatára.*

Bizonyítás Legyen C_0 nem triviális véges maximális kód X felett. Ha C_0 felbonthatatlan, akkor definíció szerint önmaga felett felbontható, azaz ebben az esetben az állítás igaz. Ha C_0 felbontható a $C_1 (\neq C_0)$ nem triviális kód felett, akkor ez azt jelenti, hogy C_0 minden eleme egyértelműen bontható fel C_1-beli elemek szorzatára. A 15.7 Tétel szerint C_1 is nem triviális véges maximális kód. Mivel $C_1 \neq C_0$, ezért van olyan $c_0 \in C_0$, amely legalább két C_1-beli elem szorzatára bontható fel, azaz $c_0 \notin C_1$. Ha C_1 felbonthatatlan, akkor készen vagyunk a bizonyítással. Ha C_1 felbontható a $C_2 (\neq C_1)$ nem triviális kód felett, akkor C_0 is felbontható C_2 felett, azaz C_0 elemei egyértelműen felbonthatók C_2-beli elemek szorzatára. Ismét a 15.7 Tétel szerint C_2 nem triviális véges maximális kód. A $C_2 \neq C_1$ feltétel miatt van olyan $c_1 \in C_1$, amely legalább két C_2-beli elem szorzatára bontható fel, ezért $c_1 \notin C_2$. Ezt az eljárást folytatva

a C_0 végessége miatt van olyan n nemnegatív egész szám, hogy C_n nem triviális véges felbonthatatlan kód és C_0 felbontható C_n felett. Kaptuk, hogy C_0 elemei egyértelműen felbonthatók C_n elemeinek szorzatára. □

Az X^* [X^+] szabad monoid [félcsoport] $M \neq X^*$ [X^+] szabad részmonoidját [részfélcsoportját] X^* [X^+] *maximális szabad részmonoidjá*nak [*részfélcsoportjá*nak] nevezzük, ha nincs X^*-nak [X^+-nak] olyan M' szabad részmonoidja [részfélcsoportja], amelyre $M \subset M' \subset X^*$ [X^+] teljesül.

15.9. Tétel. *Az X feletti C nem triviális kód akkor és csak akkor felbonthatatlan, ha X^+ szabad félcsoport valamely maximális szabad részfélcsoportjának bázisa.*

Bizonyítás Legyen C az X^+ szabad félcsoport M maximális szabad részfélcsoportjának bázisa. Tegyük fel, hogy C felbontható a D nem triviális kód felett, azaz $C \subseteq D^+$. Ebből következik, hogy $M \subseteq D^+$. Mivel $M = C^+$ maximális szabad részfélcsoportja X^+-nak, ezért $C^+ = D^+$, amiből $C = D$ adódik. Tehát C valóban felbonthatatlan.

Legyen most C egy X feletti nem triviális kód és C^+ nem maximális. Akkor X^+-nak van olyan $F \neq X^+$ szabad részfélcsoportja, amelyre $C^+ \subset F$, s így $C \subset F$, azaz C felbontható F bázisa felett. □

A tételből következik, hogy szabad félcsoport maximális szabad részfélcsoportjainak bázisai maximális kódok.

15.10. Lemma. *Bármely n pozitív egész számra X^n maximális kód.*

Bizonyítás Ha $p \in X^+$ olyan szó, hogy $p \notin X^n$, akkor $X^n + p$ nem kód, mert ha $|p| = k(\neq n)$, akkor vannak olyan $q_1, \ldots q_k \in X^n$, hogy $p^n = q_1 \ldots q_k$, azaz p^n két különböző módon bontható fel $X^n + p$ elemeinek szorzatára. Ez azt jelenti, hogy X^n maximális kód. □

Az X^n kódot (n *hosszúságú*) *maximális kód*nak vagy általában *maximális uniform kód*nak nevezzük. A 15.5 Lemma szerint minden felbonthatatlan kód maximális. A következő tétel mutatja, hogy nem minden maximális kód felbonthatatlan.

15.11. Tétel. *Bármely n pozitív egész számra X^n akkor és csak akkor bontható fel egy D kód felett, ha $D = X^m$, ahol m az n osztója. X^n akkor és csak akkor felbonthatatlan, ha n prímszám.*

Bizonyítás Ha m osztója n-nek, akkor $X^n \subseteq (X^m)^+$, azaz X^n felbontható X^m felett.

Megfordítva, legyen D olyan kód, amelyre $X^n \subseteq D^+$. Tegyük fel, hogy p egy minimális hosszúságú szó D-ben. Ha $|p| = m$, akkor vannak olyan $u_1, u_2, \ldots, u_m \in X^n$ szavak, amelyekre $p^n = u_1 u_2 \ldots u_m$. Mivel $X^n \subseteq D^+$, ezért $u_1, u_2, \ldots, u_m \in D^+$. Ezért a (13.1) szerint van olyan k pozitív egész szám, amelyre $km = n$ és $u_1 = u_2 = \cdots = u_m = p^k$. Minden $q \in X^m$ szóra $p^{2k-1}q, qp^{2k-1} \in X^{2n} \subseteq D^+$, ezért a 13.5 Tétel szerint $q \in D^+$. Az m definíciója miatt $q \in D$. Innen kapjuk, hogy $X^m \subseteq D$. A 15.1 Lemma szerint X^m maximális, ezért $D = X^m$.
A tétel második állítása az előzőekből azonnal adódik. □

15.4. Csoportkódok

Végül a maximális kódok egy hasznos részosztályával foglalkozunk.

15.12. Lemma. *Ha φ az X^* szabad monoid homomorf leképezése egy G csoportra, akkor G bármely H részcsoportjára*

$$\varphi^{-1}(H) = \{p \in X^*; \varphi(p) \in H\} \tag{15.2}$$

az X^* szabad monoid unitér részmonoidja.

Bizonyítás Ha $p, pu \in \varphi^{-1}(H)$, akkor $\varphi(p), \varphi(pu) \in H$. Így

$$\varphi(u) = ((\varphi(p))^{-1}\varphi(p))\varphi(u) = (\varphi(p))^{-1}(\varphi(p)\varphi(u)) = (\varphi(p))^{-1}\varphi(pu) \in H,$$

amiből következik, hogy $u \in \varphi^{-1}(H)$, azaz $\varphi^{-1}(H)$ az X^* szabad monoid bal unitér részmonoidja. Hasonlóan látható be, hogy ha $p, up \in \varphi^{-1}(H)$, akkor $u \in \varphi^{-1}(H)$, vagyis $\varphi^{-1}(H)$ az X^* szabad monoid jobb unitér részmonoidja.□

A 13.9 Tétel szerint az X^* szabad monoid (15.2) unitér részmonoidjainak bázisai bifix kódok. Ezeket a kódokat X feletti *csoportkód*oknak nevezzük.

15.13. Tétel. *Minden X feletti csoportkód maximális kód X felett.*

Bizonyítás Legyen φ az X^* szabad monoid homomorf leképezése a G csoportra és H részcsoportja G-nek. Ha $H = G$, akkor $\varphi^{-1}(H) = X^*$, amelynek bázisa X, s ez nyilvánvalóan maximális kód X felett.

Tegyük fel, hogy $H \subset G$. Akkor $\varphi^{-1}(H) \subset X^*$. Legyen C a $\varphi^{-1}(H)$ bázisa. Megmutatjuk, hogy ha $p \notin \varphi^{-1}(H)$, akkor $C + p$ nem kód X felett, azaz C maximális kód X felett. Legyen $\varphi(p) = g$. Mivel φ szürjektív, van olyan $q \in X^*$, hogy $\varphi(q) = g^{-1}$. Ebből következik, hogy $pq, qp \in \varphi^{-1}(H)$. De $(pq)p = p(qp)$, ami (13.1) szerint azt jelenti, hogy $C + p$ nem kód X felett. □

Legyen $X \neq \emptyset$ tetszőleges halmaz és $x \in X$. Jelölje $|p|_x$ ($p \in X^*$) az x betű előfordulásainak számát a p szóban.

15.14. Példa. *Legyen* $X = \{a, b\}$ *és*

$$M = \{p \in X^*; |p|_a \equiv 0 \pmod 2\}.$$

M az X^* szabad monoid olyan részmonoidja, amelynek bázisa maximális kód.

Legyen ugyanis $Z_2 = \{0, 1\}$ a mod 2 maradékosztályok additív csoportja és $\varphi : X \to Z_2$ az a leképezés, amelyre $\varphi(a) = 1$ és $\varphi(b) = 0$. Terjesszük ki φ értelmezését X^*-ra homomorf módon. A 15.12 Lemma szerint $M = \varphi^{-1}(0)$ unitér részfélcsoport, amelynek $b + ab^*a$ bázisa csoportkód. A 15.13 Tétel szerint $b + ab^*a$ maximális kód.

A 15.13 Tétel miatt az alábbi lemmából következik a 15.10 Lemma:

15.15. Lemma. *Bármely n pozitív egész számra X^n csoportkód.*

Bizonyítás Legyen Z_n a mod n maradékosztályok additív csoportja. Tekintsük azt a $\varphi : X^* \to Z_n$ homomorfizmust, amelyre minden $p \in X^*$ esetén $\varphi(p) = k$ akkor és csak akkor, ha $k \equiv |p| \pmod n$. Nem nehéz belátni, hogy $(X^n)^* = \varphi^{-1}(0)$. □

Feladat

15.1. Az $L = \sum_{n=0}^{\infty} a^n b(a + b)^n$ nyelv maximális kód az $X = \{a, b\}$ ábécé felett.

16. fejezet

Ritka és sűrű kódok

A 15.1 Lemma szerint minden kód részhalmaza egy maximális kódnak, ezért a kódelméletben alapvető feladat a maximális kódok szerkezetének vizsgálata. A vizsgálatokban fontos szerepük van a szabad monoidok ideáljainak.

16.1. Teljes kódok

Mint azt már (12.26)-ban is definiáltuk, az X feletti L nyelvet *sűrű*nek nevezzük X felett, ha X^* minden $J \neq \emptyset$ ideáljára $L \cap J \neq \emptyset$, más szóval, ha

$$(\forall p \in X^*)(L \cap X^* p X^* \neq \emptyset) \tag{16.1}$$

A továbbiakban is, ha ugyanazon X halmaz feletti nyelvekről lesz szó, akkor az "X feletti" kifejezést az egyszerűség kedvéért elhagyjuk.

Ha az L nyelv L^* iteráltja sűrű, akkor L-et *teljes*nek hívjuk. Minden sűrű nyelv teljes. A definícióból látható, hogy ha L sűrű [teljes] és $L \subseteq L' \subseteq X^*$, akkor L' is sűrű [teljes]. A 12.8. alfejezetben a nemsűrű nyelveket *ritka nyelvek*nek is neveztük. Ritka nyelv minden résznyelve is ritka. Ha egy C kód sűrű [teljes, ritka] nyelv, akkor C-t *sűrű* [*teljes, ritka*] *kód*nak mondjuk.

Ha $|X| = 1$, akkor az X feletti véges nyelvek a ritka, a végtelen nyelvek pedig a sűrű nyelvek. Az X^+ minden nemüres részhalmaza teljes, mivel X^* végtelen részmonoidját generálja. A 15.2 Tételből közvetlenül adódik a

16.1. Lemma. *Minden maximális kód teljes kód.*

A következő példa segítségével megmutatjuk, hogy a 16.1 Lemma megfordítása nem igaz.

16.2. Példa. *Legyen* $X = \{a, b\}$ *és* $M = \{p \in X^*; |p|_a = |p|_b\}$.

Nem nehéz belátni, hogy M az X^*-nak unitér részmonoidja. A 13.9 Tétel szerint az M monoid $D = (M - e) - (M - e)^2$ bázisa bifix kód. Az X^* elemei az $a^{k_1}b^{l_1} \dots a^{k_m}b^{l_m}$ alakú szavak, amelyekben $k_1, l_1, \dots k_m, l_m$ nemnegatív egész számok ($a^0 = b^0 = e$). Ezért D azoknak az $a^{k_1}b^{l_1} \dots a^{k_m}b^{l_m}$ és $b^{k_1}a^{l_1} \dots b^{k_m}a^{l_m}$ szavaknak a halmaza, amelyekben

$$k_1 + \dots + k_m = l_1 + \dots + l_m \quad (k_1, l_1, \dots k_m, l_m \in N_+),$$

és $m > 1$ esetben

$$k_1 + \dots + k_j > l_1 + \dots + l_j \quad (j = 1, \dots, m-1).$$

Ha $p \in X^+$, akkor $q = a^{2|p|_b}pb^{|p|} \in M = D^*$. Ezenkívül q-nak nincs valódi kezdőszelete D^+-ból, így $q \in D$. Ami éppen azt jelenti, hogy D sűrű kód.

A 16.2 Példában definiált D kódot (*bináris*) *Dyck kód*nak nevezzük. (A 3.8. alfejezetben definiált Dyck nyelv $n = 2$ esetben M résznyelve.) Mivel a Dyck kód sűrű kód, ezért teljes is. Legyen $p \in D$. A 12.76 Lemma és a 12.79 Következmény szerint $D - p$ is sűrű, s így teljes kód. A $D - p$ azonban nem maximális kód. Ez azt jelenti, hogy a 16.1 Lemma állítása nem fordítható meg. A Dyck kód csoportkód, ezért a 15.13 Tétel szerint maximális kód. A következőképpen láthatjuk be, hogy a Dyck kód csoportkód:

Legyen Z az egész számok additív csoportja. Definiáljuk a $\varphi : X^* \to Z$ leképezést a $\varphi(p) = |p|_a - |p|_b$ összefüggéssel ($\varphi(a) = 1,\ \varphi(b) = -1$). Nem nehéz megmutatni, hogy φ az X^* szabad monoid homomorf leképezése Z-re és $M = \varphi^{-1}(0)$.

16.2. Ritka kódok Bernoulli mértéke

A következő állítás alapján azt mondhatjuk, hogy a ritka nyelvek "kevés" szót tartalmaznak.

16.3. Lemma. *Ha π az X halmaz pozitív Bernoulli mértéke és L ritka nyelv X felett, akkor*

$$\pi(L) < \infty. \tag{16.2}$$

Bizonyítás Legyen $p \in X^+$ olyan, amelyre $L \cap X^*pX^* = \emptyset$ és $|p| = n$. Tekintsük az

$$L_j = \{q \in L; |q| = kn + j, k \in N\} \quad (j = 0, 1, \dots, n-1).$$

Mivel $L = \sum_{j=0}^{n-1} L_j$, elegendő megmutatni, hogy

$$\pi(L_j) < \infty \quad (j = 0, 1, \dots, n-1).$$

A p definíciója miatt

$$L_j \subseteq X^j(X^n - p)^*.$$

De $X^n - p$ kód, ezért (14.11) miatt

$$\pi((X^n - p)^*) = \sum_{k=0}^{\infty}(\pi(X^n - p))^k = \sum_{k=0}^{\infty}(1 - \pi(p))^k = \frac{1}{\pi(p)},$$

s így (14.7) és a 14.1 Lemma szerint

$$\pi(L_j) \leq \pi(X^j(X^n - p)^*) \leq \pi(X^j)\pi((X^n - p)^*) =$$

$$= \pi((X^n - p)^*) = \frac{1}{\pi(p)} < \infty.$$

□

16.4. Lemma. *Ha π az X halmaz pozitív Bernoulli mértéke, L pedig teljes ritka nyelv, akkor*

$$\pi(L) \geq 1. \tag{16.3}$$

Bizonyítás Mivel L ritka, ezért van olyan $p \in X^+$, hogy $L \cap X^*pX^* = \emptyset$. De L teljes, így minden $q \in X^*$ szóra $L^* \cap X^*pqpX^* \neq \emptyset$, azaz valamely $u, v \in X^*$ szavakra $upqpv \in L^*$. Jelölje K_p a p szó valódi $r \neq e$ kezdő szeleteinek, Z_p pedig valódi $t \neq e$ zárószeleteinek halmazát. Az $L \cap X^*pX^* = \emptyset$ feltétel miatt nincs olyan L-beli szó, amelynek p részszava lenne. Ezért van olyan $(r, t) \in K_p \times Z_p$, hogy $tqr \in L^*$. Legyen

$$L_{r,t} = \{q \in X^*; tqr \in L^*\} \quad ((r, t) \in K_p \times Z_p).$$

Nyilvánvaló, hogy

$$X^* = \sum_{(r,t)\in K_p\times Z_p} L_{r,t}.$$

A 14.1 Lemmából következik, hogy $\pi(X^*) = \infty$. A $K_p \times Z_p$ halmaz végessége és (14.5) miatt van olyan $(r, t) \in K_p \times Z_p$, amelyre $\pi(L_{r,t}) = \infty$. Ebből (14.2) és (14.4) miatt

$$\pi(t)\pi(L_{r,t})\pi(r) = \pi(tL_{r,t}r) \leq \pi(L^*).$$

Minthogy π pozitív Bernoulli mérték, ezért $\pi(r), \pi(t) \neq 0$. Ami azt jelenti, hogy $\pi(L^*) = \infty$. Továbbá (14.9) szerint

$$\pi(L^*) = \pi(\sum_{k=0}^{\infty} L^k) \leq \sum_{k=0}^{\infty}\pi(L^k) \leq \sum_{k=0}^{\infty}\pi(L)^k.$$

Ebből pedig $\pi(L) \geq 1$ adódik. (A $\pi(L) < 1$ esetben az előbbi mértani sor véges.) □

16.3. Ritka teljes kódok

Ritka kódokra érvényesek a 15.3 Tétel és a 16.1 Lemma megfordításai:

16.5. Tétel. *Az X halmaz feletti C ritka kódra a következő állítások ekvivalensek:*
(1) *C maximális kód X felett;*
(2) *C teljes kód X felett;*
(3) *Az X bármely π pozitív Bernoulli mértékére $\pi(C) = 1$.*
(4) *X-nek van olyan π pozitív Bernoulli mértéke, amelyre $\pi(C) = 1$.*

Bizonyítás (1) $\Longrightarrow$ (2): Ha a C ritka kód maximális kód X felett, akkor a 16.1 Lemma szerint C teljes kód X felett.

(2) $\Longrightarrow$ (3): Ha C ritka kód teljes kód X felett, akkor a 14.3 Tétel és a 16.4 Lemma szerint az X bármely pozitív Bernoulli mértékére $\pi(C) = 1$.
A (3) feltételből triviálisan következik (4).

(4) $\Longrightarrow$ (1): Ha az X halmaz π pozitív Bernoulli mértékére $\pi(C) = 1$, akkor a 15.3 Tételből következik, hogy C maximális kód X felett. □

A 16.5 Tétel véges esetre meglepően egyszerű algoritmust ad annak eldöntésére, hogy egy ritka kód maximális kód vagy nem. Elegendő X egy π pozitív Bernoulli mértékét tekinteni, s megvizsgálni, hogy $\pi(C) = 1$ vagy $\pi(C) \neq 1$. Sűrű kódokra ez az eljárás nem jó. A 16.2 Példában megmutattuk, hogy a bináris Dyck kód sűrű, s így teljes kód. Beláttuk azt is, hogy csoportkód, s ezért maximális kód. Megmutatható, hogy csak az uniform mértéke 1.

A 16.5 Tételből az is következik, hogy egy teljes ritka nyelv akkor és csak akkor kód, ha maximális kód. A következő tétel segítségével teljes ritka nyelvekről dönthetjük el, hogy maximális kódok vagy nem kódok.

16.6. Tétel. *Legyen π az X halmaz pozitív Bernoulli mértéke. Az X feletti L teljes ritka nyelv akkor és csak akkor kód X felett, ha $\pi(L) = 1$.*

Bizonyítás Ha L kód, akkor a 16.5 Tétel szerint $\pi(L) = 1$.

Megfordítva, tegyük fel, hogy $\pi(L) = 1$. Először megmutatjuk, hogy minden n pozitív egész számra L^n teljes ritka nyelv. A 12.76 Lemma szerint L^n ritka nyelv. Mivel L teljes, ezért bármely $p \in X^*$ elemre vannak olyan $u, v \in X^*$, hogy $upv \in L^*$. Akkor $upv \in L^k$ valamilyen k nemnegatív egész számra. Így

$$(upv)^n \in (L^k)^n = (L^n)^k \subset (L^n)^*,$$

azaz $(L^n)^* \cap X^*pX^* \neq \emptyset$, vagyis L^n teljes nyelv. A 14.8) egyenlőtlenség és a 16.4 Lemma szerint $\pi(L^n) = 1$. Tehát minden n pozitív egész számra $\pi(L^n) = 1 = (\pi(L))^n$, ez a 14.2 Lemma szerint azt jelenti, hogy L kód. □

16.7. Példa. *Az a^*b nyelv teljes ritka kód $\{a, b\}$ felett.*
Az ugyanis nyilvánvaló, hogy a^*b prefix kód. Például

$$a^*b \cap \{a, b\}^*ba\{a, b\}^* = \emptyset,$$

ezért a^*b ritka kód. Ha $\pi(a) = r,\ \pi(b) = 1 - r\ (0 < r < 1)$, akkor $\pi(a^*b) = 1$. A 16.5 Tétel szerint a^*b valóban teljes kód.

16.8. Tétel. *Egy kód akkor és csak akkor teljes kód, ha sűrű vagy maximális kód.*

Bizonyítás Legyen C egy kód az X felett. Tegyük fel, hogy C teljes kód. Ha C ritka kód, akkor a 16.5 Tétel szerint maximális kód X felett.

Megfordítva, ha C sűrű kód, akkor teljes kód is, ha pedig maximális kód, akkor a 16.1 Lemma szerint teljes kód. □

16.9. Tétel. *Ha C korlátos maximális kód az X ábécé felett, akkor X bármely $Z \neq \emptyset$ részhalmazára $C \cap Z^+$ maximális kód Z felett.*

Bizonyítás A 12.78 Következmény szerint minden korlátos kód ritka kód, így a 16.5 Tétel miatt elegendő megmutatni, hogy $C \cap Z^+$ teljes kód Z felett. Legyen n olyan pozitív egész szám, hogy minden $q \in C$ kódszóra $|q| \leq n$. Tegyük fel, hogy $p \in Z^+$ és $z \in Z$. Tekintsük a $z^{n+1}pz^{n+1}$ szót. A 16.5 Tétel szerint C teljes, ezért vannak olyan $u, v \in X^*$ és $q_1, \ldots, q_k \in C$, amelyekre

$$uz^{n+1}pz^{n+1}v = q_1 \ldots q_k.$$

Az n definíciója miatt léteznek olyan i, j $(1 \leq i < j \leq k)$ pozitív egész számok, amelyekre

$$z^r p z^t = q_i \ldots q_j$$

valamely r, t $(1 \leq r, t \leq n)$ pozitív egész számokra. Ez pedig azt jelenti, hogy $q_i, \ldots, q_j \in C \cap Z^+$, azaz $C \cap Z^+$ teljes kód. □

16.10. Következmény. *Ha C korlátos maximális kód az X halmaz felett, akkor bármely $x \in X$ betűhöz egyetlen olyan n pozitív egész szám van, amelyre $x^n \in C$.*

Bizonyítás Alkalmazzuk a 16.9 Tételt a $Z = \{x\}$ esetre. Akkor $Z^+ = x^+$, így van olyan n pozitív egész szám, amelyre $x^n \in C$. Mivel C kód, ezért egyetlen ilyen pozitív egész szám van. □

A 16.10 Következményben szereplő n-et *az x betű C-re vonatkoztatott rendjé*nek nevezzük.

16.4. Jobbról teljes kódok

Az X feletti L nyelvet *jobbról* [*balról*] *sűrű*nek nevezzük, (X felett), ha X^* bármely $J \neq \emptyset$ jobb [bal] ideáljára $L \cap J \neq \emptyset$, vagyis ha

$$(\forall p \in X^*)(L \cap pX^* \neq \emptyset, \quad [L \cap X^*p \neq \emptyset]). \tag{16.4}$$

Az X^* szabad monoid minden nemüres bal [jobb] ideálja jobbról [balról] sűrű X felett. (Az X^* bármely L bal ideáljára és M jobb ideáljára $ML \subseteq L \cap M$.)

Nyilvánvaló, hogy az $L \subseteq X^*$ nyelv akkor és csak akkor jobbról sűrű, ha felismerhető valamely $\mathbf{A} = (A, a_0, X, \delta, F)$ terminálisan összefüggő automatában. (A 7.1. alfejezetben is mondtuk, hogy elegendő iniciálisan összefüggő automatákat tekinteni.)

Ha az L nyelv L^* iteráltja jobbról [balról] sűrű, akkor L-et *jobbról* [*balról*] *teljes*nek hívjuk. Minden jobbról [balról] sűrű nyelv jobbról [balról] teljes. Ha L jobbról [balról] sűrű [teljes] és $L \subseteq L' \subseteq X^*$, akkor L' is jobbról [balról] sűrű [teljes]. Továbbá minden jobbról vagy balról sűrű [teljes] nyelv sűrű [teljes].

A nem jobbról [balról] sűrű nyelveket *jobbról* [*balról*] *ritka nyelvek*nek nevezzük. Jobbról [balról] ritka nyelv minden résznyelve is jobbról [balról] ritka. Minden ritka nyelv jobbról és balról ritka. Hasonlóan beszélünk jobbról vagy balról sűrű [teljes, ritka] kódokról. A teljes kódok egy részosztályát alkotják a jobbról [balról] teljes kódok.

16.11. Tétel. *Legyen L tetszőleges nyelv X felett és $\overline{L}$ [$\underline{L}$] az L-beli elemek valódi kezdő [záró] szeleteinek halmaza. A következő állítások ekvivalensek:*
(1) *L jobbról [balról] teljes nyelv;*
(2) *$X^* = \overline{L} + LX^*$ [$X^* = \underline{L} + X^*L$];*
(3) *$X^* = L^*\overline{L}$ [$X^* = \underline{L}L^*$];*
(4) *LX^* [X^*L] jobbról [balról] sűrű nyelv X felett, azaz minden $p \in X^*$ szóhoz vannak olyan $u, v \in X^*$ és $q \in L$ szavak, amelyekre $pu = qv$ [$up = vq$].*

Bizonyítás (1) $\Longrightarrow$ (3): Tegyük fel, hogy L jobbról teljes nyelv. Legyen $p \in X^*$. Ha $p \in L^*$, akkor $p = pe \in L^*\overline{L}$. Legyen $p \notin L^*$. Mivel L jobbról teljes, ezért van olyan $u \in X^+$, hogy $pu \in L^*$. De $pu \neq e$, így $pu \in L^+$. Ha $pu \in L$, akkor $p \in \overline{L}$, amiből $p = ep \in L^*\overline{L}$. Tegyük fel most, hogy $pu = q_1 \dots q_n$ $(q_1, \dots, q_n \in L, n > 1)$. Két lehetőség van, mégpedig, $p = q_1 \dots q_k t$, $q_{k+1} = ts$ $(t, s \in X^+, k \geq 1)$ vagy $q_1 = pt$ $(t \in X^+)$. Az első esetben $t \in \overline{L}$, s így $p \in L^*\overline{L}$. A második esetben $p \in \overline{L}$, s innen $p = ep \in L^*\overline{L}$. Ez bizonyítja, hogy $X^* = L^*\overline{L}$.

(3) $\Longrightarrow$ (1): Legyen $X^* = L^*\overline{L}$. Ha $p = e$, akkor $LX^* \cap pX^* = LX^* \neq \emptyset$. Ha $p \in X^+$, akkor $p = uv$ $(u \in L^*,\ v \in \overline{L})$. Így van olyan $t \in X^+$, amelyre

$vt \in L$. Amiből $pt = uvt \in L^+$, vagyis $L^* \cap pX^* \neq \emptyset$. Ami éppen azt jelenti, hogy L jobbról teljes.

(2) $\Longrightarrow$ (4): Tegyük fel, hogy $X^* = \overline{L} + LX^*$. Így ha $p \in X^*$, akkor $p \in \overline{L}$ vagy $p \in LX^*$, ezért vannak olyan $u, v \in X^*$ és $q \in L$, hogy $pu = qv$. Így $pX^* \cap LX^* \neq \emptyset$, azaz (16.4) szerint LX^* jobbról sűrű.

(4) $\Longrightarrow$ (2): Legyen LX^* jobbról sűrű nyelv. Így bármely $p \in X^*$ szóra $pX^* \cap LX^* \neq \emptyset$, azaz vannak olyan $u, v \in X^*$ és $q \in L$, hogy $pu = qv$, azaz $p \in \overline{L}$ vagy $p \in LX^*$. Tehát $X^* = \overline{L} + LX^*$.

(1) $\Longrightarrow$ (4): Tegyük fel, hogy L jobbról teljes. Ha $p = e$, akkor $LX^* \cap pX^* = LX^* \neq \emptyset$. Ha $p \in X^+$, akkor

$$\emptyset \neq L^* \cap pX^* = L^+ \cap pX^* \subseteq LX^* \cap pX^*,$$

vagyis LX^* jobbról sűrű.

(4) $\Longrightarrow$ (1): Tegyük fel, hogy LX^* jobbról sűrű. Legyen $p \in X^*$. Ha $p \in \overline{L} + L$, akkor $pu \in L$ valamilyen $u \in X^*$ szóra. Máskülönben, (2) szerint, $p \in LX^+$. Így $p = qr$ valamely $q \in L$ és $r \in X^+$ szóra. Mivel $|r| < |p|$, folytatva az eljárást p helyett r-rel, véges számú lépésben elérjük, hogy $ru \in L^*$ valmilyen $u \in X^*$ szóra. Amiből kapjuk, hogy $L^* \cap pX^* \neq \emptyset$, azaz L jobbról teljes.

Az állítások zárószeletekre hasonlóan bizonyíthatók. □

16.5. Reguláris kódok

Kleene tétele szerint a véges ábécé feletti reguláris nyelvek megegyeznek a véges automatákban előállítható nyelvekkel. Most megmutatjuk, hogy egy X véges ábécé feletti reguláris kódok osztálya az X feletti ritka kódok egy részosztálya.

16.12. Tétel. *Véges ábécé feletti reguláris kódok ritka kódok az adott ábécé felett.*

Bizonyítás Tegyük fel, hogy az X véges ábécé feletti C kód felismerhető az $\mathbf{A} = (A, a_0, X, \delta; F)$ véges automatában, azaz a (7.1) definíció szerint

$$C = \{p \in X^*; a_0 p \in F\}.$$

Legyen tetszőleges $p \in X^*$ bemenő szóra

$$Ap = \{ap; \quad a \in A\}.$$

Nyilvánvaló, hogy bármely $u, p, v \in X^*$ esetén

$$|Aupv| \leq |Ap|.$$

Jelölje J az X^* szabad monoid azon p elemeinek halmazát, amelyekre $|Ap|$ minimális. Ha $p \in J$, akkor minden $u, v \in X^*$ párra

$$|Aupv| = |Ap|.$$

Ez azt jelenti, hogy J az X^* szabad monoid ideálja. Ha $p \in J$, akkor

$$Ap^2 = (Ap)p \subseteq Ap,$$

amiből következik, hogy $Ap^2 = Ap$. Így, az A állapothalmaz végessége miatt, az $\alpha(ap) = ap^2$ $(a \in A)$ leképezés az Ap halmaz egy permutációja. Ezért van olyan n pozitív egész szám, hogy $\alpha^n = \iota_{Ap}$, azaz minden $a \in A$ állapotra

$$ap = \alpha^n(ap) = ap^{n+1}$$

teljesül. Tegyük fel, hogy $C \cap J \neq \emptyset$. Ha $p \in C \cap J$, akkor

$$a_0 p^{n+1} = a_0 p \in F,$$

azaz $p^{n+1} \in C$. Ez azonban lehetetlen, mivel C kód X felett. Kaptuk, hogy $C \cap J = \emptyset$, vagyis C ritka kód X felett. □

A 16.12 Tétel megfordítása nem igaz. Tekintsük ugyanis a

$$C = \{a^n b^n;\ n \in N_+\}$$

bináris kódot. Nem nehéz belátni, hogy C ritka kód $X = \{a, b\}$ felett $(C \cap X^*baX^* = \emptyset)$. A 8.9 Tétel bizonyításából látható, hogy C környezetfüggetlen, de nem reguláris. Ritka csoportkódokra azonban megfordítható az állítás.

16.13. Tétel. *Véges ábécé feletti ritka csoportkódok reguláris kódok az adott ábécé felett.*

Bizonyítás Legyen C ritka csoportkód az X véges ábécé felett. Mivel C csoportkód X felett, ezért X^*-nak van olyan φ homomorf leképezése egy olyan G csoportra, amelynek valamely H részcsoportjára $C^* = \varphi^{-1}(H)$. Mivel C ritka kód X felett, így van olyan $p \in X^+$, amelyre $C \cap X^*pX^* = \emptyset$.

Megmutatjuk, hogy G előáll olyan $H(\varphi(q))^{-1}$ mellékosztályok egyesítéseként, amelyekben a q szavak p prefixei. Ez azt jelenti, hogy H a G véges indexű részcsoportja. Valóban, legyen $g \in G$ és legyenek $q, r \in X^*$ olyanok, amelyekre

$$\varphi(q) = g, \quad \varphi(r) = (g\varphi(p))^{-1}.$$

Akkor

$$\varphi(qpr) = g\varphi(p)\varphi(r) = 1 \in H,$$

ahol 1 a G csoport egységeleme. Innen $qpr \in C^+$. Minthogy $C \cap X^*pX^* = \emptyset$, ez csak úgy lehetséges, hogy vannak olyan $p_1, p_2 \in X^*$, amelyekre $p = p_1p_2$ és $qp_1, p_2r \in C^*$. Amiből

$$g\varphi(p_1) = \varphi(q)\varphi(p_1) = \varphi(qp_1) \in H,$$

s így $g \in H\varphi(p_1)^{-1}$.

Jelölje G/H a G H-szerinti jobb oldali mellékosztályainak halmazát. Definiáljuk a $\mathbf{G/H} = (G/H, X, \delta)$ kimenő jel nélküli automata δ átmenetfüggvényét a

$$\delta(Hg, x) = Hg\varphi(x) \quad (q \in G,\ x \in X)$$

összefüggéssel. Az előbbiek szerint $\mathbf{G/H}$ véges automata. A δ átmenetfüggvény (6.2) - (6.4) kiterjesztését is figyelembe véve kapjuk, hogy minden $g \in G$ csoportelemre és $q \in X^*$ bemenő szóra

$$(Hg)q = Hg\varphi(q).$$

Ezért, ha a $\mathbf{G/H}$ automatában a kezdőállapot H, amely egyben az egyetlen végállapot is, akkor az így kapott akceptor éppen a C^* nyelvet ismeri fel, azaz C^* reguláris nyelv.

A 8.6 Tételből kapjuk, hogy ábécé feletti reguláris nyelvek különbsége is reguláris az adott ábécé felett. Mivel e reguláris, ezért $C^+ = C^* - e$ is reguláris X felett. A 2.7 Tétel szerint $(C^+)^2$ is reguláris, s így $C = C^+ - (C^+)^2$ is reguláris X felett. □

Feladatok

16.1. A 3.2. feladatban szereplő L_k nyelv bármely k pozitív egész számra az $\{a, b\}^*$ szabad monoid unitér részmonoidja, amelynek bázisa sűrű csoportkód $\{a, b\}$ felett. (A feladat a 16.2 Példa egy általánosítása.)

16.2. Jelölje $X(k)$ az X^* szabad monoid legfeljebb k hosszúságú szavainak részhalmazát. Az $L \subseteq X^*$ nyelvet *jobbról k sűrű*nek nevezzük, ha minden $p \in X^*$ szóra $pX(k) \cap L \neq \emptyset$. (Nyilvánvalóan minden jobbról k sűrű nyelv jobbról sűrű. Továbbá minden $l \geq k$ egész számra jobbról l sűrű.) Adjunk példát egy X ábécé feletti jobbról k sűrű nyelvre, amely jobbról nem $k-1$ sűrű.

16.3. Véges X ábécé feletti jobbról sűrű L reguláris nyelv jobbról k sűrű valamilyen k nemnegatív egész számra.

16.4. Legyen B az X^* szabad monoid M részmonoidjának bázisa. Ha M jobbról sűrű nyelv és B ritka nyelv X felett, akkor M jobbról k sűrű valamilyen k nemnegatív egész számra.

17. fejezet

Prefix kódok

A prefix [szuffix, bifix] kódok fogalmát már megadtuk a (13.5) feltétellel. Legyen $\mathcal{K}$-kódoknak egy osztálya, például a prefix, a szuffix, a bifix vagy a véges kódok osztálya. Ha φ az Y halmaz kódolása egy $\mathcal{K}$-kódra, akkor azt mondjuk, hogy φ egy *$\mathcal{K}$-kódolás*. Így beszélhetünk *prefix*, *szuffix*, *bifix* vagy *véges kódolás*ról. Hasonlóan beszélhetünk *$\mathcal{K}$-átkódolás*ról is.

17.1. Prefix kódok megadása algoritmussal

labelsec:17.1

17.1. Lemma. *Legyen l_k $(k \in I)$ pozitív egész számok egy sorozata. Ha az $m > 1$ pozitív egész számra teljesül a*

$$\sum_{k\in I} m^{-l_k} \leq 1 \tag{17.1}$$

feltétel, akkor van olyan m elemű ábécé feletti $C = \{p_k; k \in I\}$ prefix [szuffix] kód, amelyre $|p_k| = l_k$ $(k \in I)$.

Bizonyítás Az általánosság megszorítása nélkül feltehetjük, hogy $l_k \leq l_{k+1}$ $(k \in I)$. Tekintsük az $r_1 = 0$ és az $r_k = \sum_{j=1}^{k-1} m^{-l_j}$ $(k > 1)$ racionális számokat. A $\sum_{k\in I} m^{-l_k} \leq 1$ egyenlőtlenség miatt $0 \leq r_k < 1$ és valamennyi r_k $(k \in I)$ egyféleképpen írható fel $r_k = \sum_{j=1}^{l_k} a_{kj} m^{-j}$ alakban, ahol $0 \leq a_{kj} < m$. Ha $s > k$, akkor $r_s \geq r_k + m^{-l_k}$, ezért

$$D = \{p_k = a_{k1} \dots a_{kl_k};\ k \in I\}$$

prefix kód a $\{0, 1, \dots, m-1\}$ halmaz felett és $|p_k| = l_k$ $(k \in I)$. (Az $a_{k1} \dots a_{kl_k}$ kódszó az r_k szám m-edes tört alakban való felírásánál a törtrész első l_k jegyét jelenti.) A D prefix kód tükörképe nyilván egy megfelelő szuffix kód. □

Pozitív egész számok

$$l_1 \leq l_2 \leq \cdots \leq l_n$$

véges sorozatához mindig van olyan $m > 1$ egész szám, amely teljesíti a (17.1) feltételt. Ha ugyanis $\sqrt[l_1]{n} \leq m$, akkor

$$\sum_{j=1}^{n} m^{-l_j} \leq n m^{-l_1} \leq 1.$$

Szigorúan monoton növekvő

$$l_1 < l_2 < \cdots < l_n < \ldots$$

sorozathoz már $m = 2$ is teljesíti a (17.1) feltételt, mivel

$$\sum_{j=1}^{\infty} 2^{-l_j} \leq \sum_{j=1}^{\infty} 2^{-j} = 1.$$

17.2. Példa. *A 17.1 Lemma bizonyításában leírt algoritmussal megadunk három kettő hosszúságú és öt négy hosszúságú szóból álló prefix kódot.*

Az $m = 3$ a legkisebb olyan pozitív egész szám, amely teljesíti a (17.1) feltételt. A 17.1 Lemma bizonyításában szereplő jelöléseket használva:

$$r_1 = 0,\ r_2 = 1 \cdot 3^{-2},\ r_3 = 2 \cdot 3^{-2},\ r_4 = 1 \cdot 3^{-1},$$

$$r_5 = 1 \cdot 3^{-1} + 1 \cdot 3^{-4},\ r_6 = 1 \cdot 3^{-1} + 2 \cdot 3^{-4},$$

$$r_7 = 1 \cdot 3^{-1} + 1 \cdot 3^{-3},\ r_8 = 1 \cdot 3^{-1} + 1 \cdot 3^{-3} + 1 \cdot 3^{-4},$$

amiből

$$p_1 = 00,\ p_2 = 01,\ p_3 = 02,\ p_4 = 1000,$$

$$p_5 = 1001,\ p_6 = 1002,\ p_7 = 1010,\ p_8 = 1011.$$

17.3. Tétel. *Legyen $m > 1$ tetszőleges egész szám. Ha a $C = \{q_k; k \in I\}$ megszámlálható kódra*

$$\sum_{k \in I} m^{-|q_k|} \leq 1$$

feltétel teljesül, akkor C-nek létezik m elemű ábécé feletti prefix [szuffix] szóhossztartó átkódolása. Speciálisan, minden m elemű ábécé feletti kódnak létezik m elemű ábécé feletti prefix [szuffix] szóhossztartó átkódolása.

Bizonyítás A bizonyítást csak prefix kódokra végezzük el. Mivel a szavak tükrözése szóhossztartó átkódolás, ezért ebből már következik az állítás szuffix kódokra. Vezessük be a $|q_k| = l_k$ $(k \in I)$ jelölést. Feltehető, hogy $l_k \leq l_{k+1}$ $(k \in I)$. Tekintsük a 17.1 Lemma bizonyításában megadott D prefix kódot. A $\varphi(q_k) = p_k$ $(k \in I)$ leképezés C szóhossztartó átkódolása D-re. Ha C egy m elemű ábécé feletti kód, akkor a Szilárd–Kraft–McMillan egyenlőtlenség szerint $\sum_{k \in I} m^{-l_k} \leq 1$ teljesül. □

Megszámlálható kódnak mindig van bináris prefix átkódolása. Legyen ugyanis $C = \{p_k; k \in I\}$ megszámlálható kód. A $D = a^*b$ nyelv prefix kód az $\{a, b\}$ kételemű ábécé felett. A $\varphi(p_k) = a^{k-1}b$ $(k \in N_+)$ leképezés C átkódolása. (a^0 az üres szót jelöli.) Ez azt jelenti, hogy a gyakorlatban az információk prefix kódokkal is továbbíthatók, s kétféle jel küldésére alkalmas információs csatornákon is. Ez a tény alátámasztja a prefix kódok vizsgálatának fontosságát.

17.2. Maximális prefix kódok

A további definíciókat és tételeket az egyszerűség kedvéért csak prefix kódokra adjuk meg, de az olvasó könnyen átfogalmazhatja szuffix kódokra is. A C prefix kódot *maximális prefix kód*nak nevezzük, ha nincs olyan D prefix kód, amelyre $C \subset D$ teljesülne. Mivel a láncot alkotó prefix kódok egyesítése is prefix kód, ezért a 15.1 Lemmához hasonló módon látható be a következő állítás.

17.4. Lemma. *Bármely prefix kód egy maximális prefix kód részhalmaza.*

A következő tétel alapján prefix kódokra a 16.11 Tétel kiegészíthető azzal az ekvivalens feltétellel, hogy a prefix kód maximális prefix kód.

17.5. Tétel. *Prefix kód akkor és csak akkor maximális prefix kód, ha jobbról teljes.*

Bizonyítás Legyen C maximális prefix kód X felett. Bármely $p \in X^*$ szóra $p \in \overline{C}$ vagy $p \in CX^*$, mert különben $C + p$ szintén prefix kód lenne. Ez azt jelenti, hogy $X^* = \overline{C} + CX^*$. A 16.11 Tétel (2) feltétele miatt C jobbról teljes kód.

Megfordítva, legyen a C prefix kód jobbról teljes X felett. Tegyük fel, hogy létezik olyan D prefix kód, amelyre $C \subset D$ teljesül. Legyen $d \in D - C$. A 16.11 Tétel (3) feltétele szerint van olyan $u \in X^*$, amelyre $du \in C^+$, vagyis $du = c_1 c_2 \ldots c_k$ valamilyen C-beli $c_1, c_2, \ldots, c_k$ elemekre. Ebből azonban $d = c_1$ következik, ami ellentmond annak, hogy $d \notin C$, azaz nem létezik olyan D prefix kód, hogy $C \subset D$. □

A maximális uniform kódok maximális kódok, s egyúttal maximális prefix kódok is. Ez azonban minden prefix kódra igaz, mint azt az alábbi nyilvánvaló állítás mutatja.

17.6. Lemma. *Legyen $\mathcal{C}$ és $\mathcal{D}$ az X feletti kódok két osztálya, amelyekre $\mathcal{C} \subseteq \mathcal{D}$. Ha $C \in \mathcal{C}$ maximális $\mathcal{D}$ kód , akkor maximális $\mathcal{C}$ kód is. Speciálisan, ha egy prefix kód maximális kód, akkor maximális prefix kód.*

A következő példa azt mutatja, hogy egy maximális prefix kód nem szükségképpen maximális kód.

17.7. Példa. *Ha $X = \{x_i; i \in N_+\}$ és*

$$L = \{p \in X^+; p = x_{i_1}x_{i_2}\dots x_{i_n},\ n \geq 2,\ 2(i_1 + i_2 + \cdots + i_{n-1}) = i_n\},$$

akkor $C = L - LX^+$ olyan bifix kód, amely maximális prefix kód, de nem maximális szuffix kód, s így nem maximális kód.

Ugyanis bármely $q \in X^+$ esetén a

$$qx_{i_1}x_{i_2}\dots x_{i_n} \quad (x_{i_1}, x_{i_2}, \dots, x_{i_n} \in X,\ n \geq 2,\ 2(i_1 + i_2 + \cdots + i_{n-1}) = i_n)$$

alakú szavak nincsenek C-ben, ezért $X^+C \cap C = \emptyset$, azaz C szuffix kód, s így bifix kód. Nem nehéz belátni, hogy C teljesíti a 16.11 Tétel (3) feltételét, vagyis a 17.5 Tétel szerint maximális prefix kód. A C definíciójából kapjuk, hogy x_1 egyetlen C-beli szónak sem zárószelete, ezért $C + x_1$ is szuffix kód. Ez pedig azt jelenti, hogy C nem maximális szuffix kód, s így nem maximális kód.

Az előző példában X megszámlálhatóan végtelen halmaz volt. Ha tekintjük X-nek azt a φ átkódolását az $a + ba^*b$ bináris bifix kódra, amelyre

$$\varphi(x_1) = a, \quad \varphi(x_k) = ba^{k-2}b \quad (k = 2, 3, \dots),$$

akkor $\varphi(C)$ maximális bináris prefix kód, de nem maximális bináris szuffix kód, s ezért nem maximális bináris kód.

17.8. Tétel. *Ha C prefix kód X felett és π X-nek olyan pozitív Bernoulli mértéke, amelyre $\pi(C) = 1$, akkor C maximális prefix kód.*

Bizonyítás A 15.3 Tétel szerint C maximális kód, s így a 17.6 Lemma szerint maximális prefix kód is. □

Ritka prefix kódokra érvényes a 17.6 Lemma megfordítása.

17.9. Tétel. *Az X halmaz feletti C ritka prefix kód akkor és csak akkor maximális prefix kód, ha maximális kód.*

Bizonyítás Ha C maximális kód, akkor a 17.6 Lemma szerint maximális prefix kód. Megfordítva, ha C maximális prefix kód, akkor a 17.5 Tétel szerint jobbról teljes kód, s így teljes kód. Akkor a 16.5 Tétel szerint C maximális kód. □

A 16.5 és a 17.9 Tételek alapján ritka prefix kódokról egyszerűen a halmaz valamely pozitív Bernoulli mértéke segítségével eldönthető, hogy maximális prefix kód, s egyben maximális kód-e? A 12.78 Következményt felhasználva az előző tételből kapjuk az alábbi eredményt.

17.10. Következmény. *Korlátos, speciálisan véges prefix kód akkor és csak akkor maximális prefix kód, ha maximális kód.*

Mivel véges ábécé feletti korlátos kódok véges kódok, ezért ebből az egyenletes eloszlás segítségével jól használható szükséges és elegendő feltételt kapunk arra, hogy véges ábécé feletti véges prefix kód mikor maximális prefix kód.

17.11. Tétel. *Egy m elemű ábécé feletti $C = \{p_1, p_2, \ldots, p_k\}$ prefix kód akkor és csak akkor maximális prefix kód, ha*

$$\sum_{i=1}^{k} m^{-|p_i|} = 1.$$

17.3. Prefix kódok megadása gráfokkal

Most megmutatjuk, hogy egy $X = \{x_1, x_2, \ldots, x_m\}$ ábécé feletti (nemüres) prefix kód megadható egy irányított fával. Vegyük fel az irányított fa gyökérpontját és jelöljük (címkézzük) meg az e üres szóval. A gyökérpontból indítsunk ki m irányított élt úgy, hogy balról jobbra haladva az i-edik él végpontját címkézzük meg az x_i betűvel. Az i-edik irányított él végpontját az első szint i-edik pontjának nevezzük. Az első szint j-edik pontjából ($j = 1, 2, \ldots, k$) ismét indítsunk m irányított élt úgy, hogy balról jobbra haladva az i-edik él végpontját címkézzük meg az $x_j x_i$ szóval. Az eljárást folytatva a második, harmadik stb. szint pontjaiból, olyan végtelen irányított (címkézett) fához jutunk, amelyben bármely

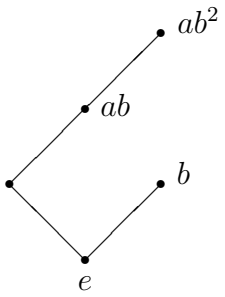
$$p = x_{i_1} x_{i_2} \ldots x_{i_n} \quad (x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in X)$$

szónak egy-egyértelműen megfeleltethetjük az e-ből x_{i_n}-be vezető

$$(e, x_{i_1}), (x_{i_1}, x_{i_1} x_{i_2}), \ldots, (x_{i_1} \ldots x_{i_{n-1}}, x_{i_1} \ldots x_{i_{n-1}} x_{i_n})$$

n hosszúságú irányított út p-vel címkézett végpontját. Az egyszerűség kedvéért ezt az irányított utat is p-vel jelöljük. Az így definiált (címkézett) gráfot az X^* *szabad monoid gráfjá*nak nevezzük.

Legyen $L \neq \emptyset$ egy X feletti nyelv. Tekintsük minden $p \in L - e$ szóra a p irányított utat, amelynek a végpontját címkézzük meg p-vel. Ha $e \in L$, akkor a gyökérpontot címkézzük meg e-vel. Az így kapott irányított utak egyesítését az L *nyelv gráfjá*nak hívjuk. Például az $\{a, b\}$ ábécé feletti $L = \{e, b, ab, ab^2\}$ nyelv gráfja:



17.1. ábra.

A konstrukcióból látható, hogy $\emptyset \subset L \subseteq X^+$ akkor és csak akkor prefix kód, ha minden megcímkézett pontja elsőfokú, azaz olyan út vezet hozzá, amelynek csak ez a pontja van megcímkézve. Továbbá, L akkor és csak akkor maximális prefix kód, ha gráfjában a gyökérpont foka m és minden más címkézetlen pontjának foka $m + 1$.

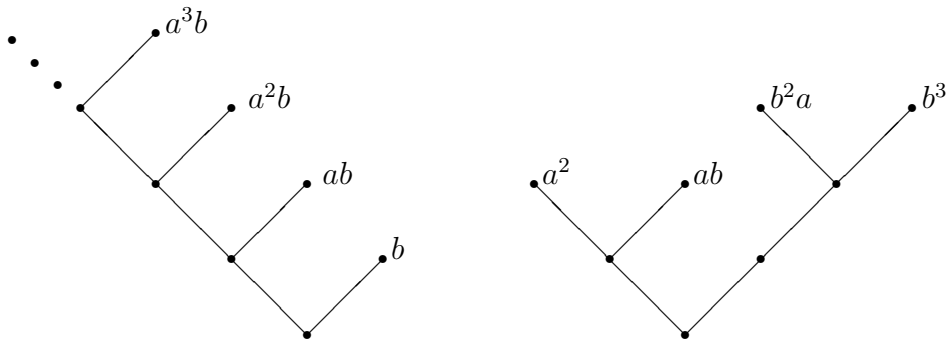
17.12. Példa. *Az $\{a, b\}$ feletti $C = a^*b$ és $D = \{a^2, ab, b^2a, b^3\}$ prefix kódok gráfjaiból leolvasható, hogy C maximális prefix kód, a D viszont nem:*

17.4. Felbontható prefix kódok

A 15.6 Lemma azt mondta ki, hogy végtelen halmaz felett nincs véges maximális kód. Az alábbi lemmából következik, hogy végtelen halmaz felett véges maximális prefix kód sincs.

17.13. Lemma. *Ha C egy X feletti maximális prefix kód, akkor $|X| \leq |C|$.*

Bizonyítás Ha C maximális prefix kód az X halmaz felett, akkor minden $x \in X$ elemhez van olyan $q \in X^*$, hogy $xq \in C$. (Ha ugyanis ez nem lenne igaz valamely $x \in X$ elemre, akkor $C + x$ is prefix kód lenne X felett.) Ez pedig azt jelenti, hogy $|X| \leq |C|$. □



17.2. ábra.

Legyenek C és D nem triviális prefix kódok. A C kódot D *felett prefix felbontható*nak nevezzük, ha $C \subseteq D^+$. A C nem triviális prefix kódot *prefix felbonthatatlan*nak mondjuk, ha nincs saját magán kívül olyan nem triviális prefix kód, amely felett C felbontható. Természetesen minden prefix felbonthatatlan prefix kód maximális prefix kód.

Érvényesek a 15.7 és a 15.8 Tételek alábbi megfelelői prefix kódokra. A bizonyításokat nem végezzük el, mivel csak az előbbi tételek bizonyítását kell úgy megismételni, hogy kód helyett mindig prefix kódot kell tekinteni. A 17.13 Lemma szerint végtelen halmaz felett nincsenek véges maximális prefix kódok, ezért ezekben az állításokban véges ábécé feletti prefix kódok szerepelnek.

17.14. Lemma. *Ha a C nem triviális véges maximális prefix kód felbontható a D nem triviális prefix kód felett, akkor D is véges maximális prefix kód.*

17.15. Tétel. *Bármely C nem triviális véges maximális prefix kód elemei egyértelműen felbonthatók valamely véges prefix felbonthatatlan prefix kód elemeinek szorzatára.*

17.5. A prefix kódok algebrája

Az alfejezetben értelmezett műveletek segítségével adott [maximális] prefix kódokból újabb [maximális] prefix kódokat állíthatunk elő.

17.16. Lemma. *Ha C, D_k $(k \in I)$ nemüres nyelvek X felett, $\{C_k; k \in I\}$ a C nyelv egy osztályozása és $D = \sum_{k\in I} C_k D_k$, akkor a következő állítások igazak:*
(1) *Ha C prefix kód és $D_k = e$ vagy D_k prefix kód minden $k \in I$ indexre, akkor D is prefix kód.*

(2) *Ha C maximális prefix kód és $D_k = e$ vagy D_k maximális prefix kód minden $k \in I$ indexre, akkor D is maximális prefix kód.*
(3) *Ha D prefix kód, akkor minden $k \in I$ esetén $D_k = e$ vagy D_k prefix kód.*
(4) *Ha C prefix kód és D maximális prefix kód, akkor C maximális prefix kód és minden $k \in I$ esetén $D_k = e$ vagy D_k maximális prefix kód.*

Bizonyítás (1) Tegyük fel, hogy $p, pu \in D$ ($p \in X^+, u \in X^*$). Akkor $p = qr$ és $pu = q'r'$ valamilyen $q \in C_k, r \in D_k, q' \in C_l, r' \in D_l$ $(k, l \in I)$. Ebből kapjuk, hogy $qru = q'r'$. Mivel C prefix kód, ezért $q = q'$, s így $ru = r'$ és $k = l$. Ha $D_k = e$, akkor $r = r' = e$, amiből $u = e$. Ha pedig D_k is prefix kód, akkor $r = r'$ és $u = e$. Ez azt jelenti, hogy D prefix kód.

(2) Legyen C maximális prefix kód és $D_k = e$ vagy D_k $(k \in I)$ maximális prefix kód. Ha $p \in X^*$, akkor a 17.5 Tétel és a 16.11. Tétel (4) feltétele szerint, vannak olyan $u, v \in X^*$ és $q \in C$, hogy $pu = qv$. Legyen $q \in C_k$ $(k \in I)$. Ha $D_k = e$, akkor $pu = (qe)v$. Ha pedig D_k maximális prefix kód, akkor szintén a 17.5 Tétel és a 16.11 Tétel (2) feltétele szerint vannak olyan $u', v' \in X^*$ és $q' \in D_k$, amelyekre $vu' = q'v'$. Így $pu = (qe)v$ vagy $p(uu') = (qq')v'$, amiből a 16.11 Tétel (4) feltételének újra alkalmazásával kapjuk, hogy D maximális prefix kód.

(3) Tegyük fel, hogy $D_k \neq e$. Legyen $r, ru \in D_k$ $(k \in I)$. Bármely $q \in C_k$ esetén $qr, qru \in D$. Mivel D prefix kód, ezért $u = e$, amiből nyerjük, hogy D_k $(k \in I)$ is prefix kód.

(4) A 16.11 Tétel (4) feltétele szerint minden $p \in X^*$ szóhoz van olyan $u, v \in X^*$ és $q \in D$, hogy $pu = qv$. Akkor $q = rt$, ahol $r \in C_k, t \in D_k$ valamilyen $k \in I$ indexre. Amiből $pu = r(tv)$ a 16.11 Tétel (4) feltétele szerint C maximális prefix kód. Hasonlóan minden $s \in C_k$ és $p \in X^*$ párhoz van olyan $u, v \in X^*$ és $q \in D$, hogy $(sp)u = qv$. Ugyanúgy, mint az előbb $q = rt$ $(r \in C_k, t \in D_k)$. De C prefix kód, ezért $s = r$ és így $pu = tv$. Ha $D_k \neq e$, akkor a 17.5 Tétel szerint azt jelenti, hogy D_k maximális prefix kód.□

17.17. Tétel. *Legyenek C és D prefix kódok. Ha $\{C_1, C_2\}$ a C prefix kód osztályozása, akkor $C_1 + C_2D$ is prefix kód. Továbbá, $C_1 + C_2D$ akkor és csak akkor maximális prefix kód, ha C és D is maximális prefix kód.*

Bizonyítás Alkalmazzuk a 17.16 Lemmát az $I = \{1, 2\}$ és a $D_1 = e$, $D_2 = D$ esetre. □

17.18. Következmény. *Ha $C \neq \emptyset$, $D \neq \emptyset$ prefix kódok és $c \in C$, akkor $(C - c) + cD$ is prefix kód. Továbbá $(C - c) + cD$ akkor és csak akkor maximális prefix kód, ha C és D is maximális prefix kód.*

A 17.18 Következmény szerint C és D gráfjából egyszerűen úgy kapjuk $(C-c)+cD$ gráfját, hogy D gráfját úgy vesszük fel, hogy gyökérpontja egyezzen meg C gráfjának c-vel címkézett pontjával, s az így kapott gráfból töröljük a c címkét.

17.19. Következmény. *Ha C és D prefix kódok, akkor CD is prefix kód. Továbbá, a C és D prefix kódokra CD akkor és csak akkor maximális prefix kód, ha C és D is maximális prefix kód.*

Bizonyítás Ha $C = \emptyset$ vagy $D = \emptyset$, akkor $CD = \emptyset$, s így prefix kód. Ha $C \neq \emptyset$ és $D \neq \emptyset$, akkor alkalmazzuk az 17.16 Lemmát az $|I| = 1$ és $C_1 = C$, $D_1 = D$ esetre. □

Az előbbi következmény alapján C és D gráfjából úgy kapjuk CD gráfját, hogy minden $c \in C$ kódszóra D gráfját úgy vesszük fel, hogy gyökérpontja egyezzen meg C gráfjának c-vel címkézett pontjával. Az így kapott gráfból töröljük a c címkét, és minden $d \in D$ esetén átcímkézzük a d-vel címkézett pontot cd-re.

A 13.8 Következmény [maximális] prefix kódokra megfordítható.

17.20. Következmény. *Legyen C tetszőleges X feletti nyelv és $n > 1$ tetszőleges pozitív egész szám. A C nyelv akkor és csak akkor [maximális] prefix kód, ha C^n is [maximális] prefix kód.*

Bizonyítás Ha $C = \emptyset$, akkor az állítás nyilvánvalóan igaz. Tegyük fel, hogy $C \neq \emptyset$. A 17.19 Következmény alapján teljes indukcióval megmutatható, hogy ha C [maximális] prefix kód, akkor C^n is [maximális] prefix kód.

Megfordítva, ha C^n $(n > 1)$ prefix kód, akkor $C^n = C^{n-1}C$, ezért a 17.16 Lemma (3) feltétele szerint C prefix kód. Ha speciálisan C^n maximális prefix kód, akkor a $C^n = CC^{n-1}$ felbontást használva, a 17.16 Lemma (4) feltétele miatt C maximális prefix kód. □

17.6. Irreducibilis prefix kódok

Egy S félcsoport F nemüres részhalmazát *filter*nek nevezzük, ha bármely $s, t \in S$ elemekre $st \in F$ akkor és csak akkor teljesül, ha $s, t \in F$. Minden filter unitér részfélcsoport. Az S félcsoport egy részfélcsoportját az S *szabad részfélcsoportjá*nak nevezzük, ha izomorf egy szabad félcsoporttal.

A 17.19 Következmény szerint az X feletti prefix kódok $\mathcal{P}(X)$ halmaza a nyelvek szorzására félcsoport, amelynek a maximális prefix kódok $\mathcal{MP}(X)$ halmaza filtere. A $\mathcal{P}(X)$-et az X feletti prefix kódok félcsoportjának, az $\mathcal{MP}(X)$-t

pedig az X feletti maximális prefix kódok félcsoportjának nevezzük. Megmutatjuk, hogy $\mathcal{P}(X) - \emptyset$ szabad félcsoport, amelynek $\mathcal{MP}(X)$ szabad részfélcsoportja. Ehhez szükségünk lesz a 13.2 Lemma következő, ahhoz hasonlóan bizonyítható általánosítására.

17.21. Lemma. *Egy S félcsoport T részfélcsoportja akkor és csak akkor szabad részfélcsoportja S-nek, ha van olyan C generátorrendszere, amelynek bármely $s_1, s_1, \ldots, s_n, t_1, t_2, \ldots t_n$ elemeire*

$$s_1 s_2 \ldots s_n = t_1 t_2 \ldots t_n \quad \Leftrightarrow \quad s_1 = t_1, s_2 = t_2, \ldots, s_n = t_n. \tag{17.2}$$

Ha a $C \neq \emptyset$ prefix kódhoz vannak olyan A és B prefix kódok, hogy $C = AB$, azaz C felbontható az A és B prefix kód szorzatára, akkor azt mondjuk, hogy C *reducibilis*. Ha C nem bontható fel két prefix kód szorzatára, akkor C-t *irreducibilis prefix kód*nak nevezzük. Például, ha C X feletti kód és $C \cap X \neq \emptyset$, akkor C irreducibilis.

17.22. Tétel. *$\mathcal{P}(X) - \emptyset$ szabad félcsoport, amelynek az X feletti irreducibilis prefix kódok halmaza a bázisa és $\mathcal{MP}(X)$ szabad részfélcsoportja.*

Bizonyítás Először megmutatjuk, hogy minden nemüres prefix kód felbontható irreducibilis prefix kódok szorzatára, vagyis az irreducibilis kódok halmaza $\mathcal{P}(X)$ egy generátorrendszere.

Legyen $C \neq \emptyset$ tetszőleges prefix kód. Ha C irreducibilis, akkor önmagának egytényezős szorzata. Tegyük fel, hogy C reducibilis, azaz vannak olyan A és B prefix kódok, hogy $C = AB$. Jelölje általában egy D prefix kód esetén $\underline{D}$ a D legkisebb hosszúságú szavainak halmazát. Nyilvánvalóan $\underline{D}$ uniform kód. Nem nehéz belátni, hogy $\underline{C} = \underline{A}\ \underline{B}$ és az $\underline{A}$ és $\underline{B}$ uniform kódokban a szavak hossza kisebb, mint az $\underline{C}$ uniform kód szavainak hossza. Ha A vagy B nem irreducibilis, akkor tovább bonthatók prefix kódok szorzatára. De a kapott prefix kódok legkisebb hosszúságú szavainak hossza csökken, ezért véges számú lépésben megkapjuk C irreducibilis prefix kódok szorzatára való bontását.

Másodszor k szerinti teljes indukcióval megmutatjuk, hogy irreducibilis prefix kódokra

$$A_1 A_2 \ldots A_k = B_1 B_2 \ldots B_k \quad \Longrightarrow \quad A_1 = B_1, A_2 = B_2, \ldots, A_k = B_k.$$

Ebből, a 17.6 Lemmát felhasználva következik, hogy $P(X) - \emptyset$ szabad félcsoport és bázisa az irreducibilis prefix kódok halmaza.

Ha $k = 1$, akkor az állítás nyilvánvalóan teljesül. Tegyük fel, hogy az állítás igaz $(1 \leq) k - 1$ pozitív egész számra. Legyen

$$A_1 A_2 \ldots A_k = B_1 B_2 \ldots B_k$$

az A_j, B_j $(j = 1, 2, \ldots, k)$ irreducibilis prefix kódokra. A 17.19 Következmény szerint $A = A_1 A_2 \ldots A_{k-1}$ és $B = B_1 B_2 \ldots B_{k-1}$ is prefix kódok. Az általánosság megszorítása nélkül feltehetjük, hogy ha $a \in \underline{A}$ és $b \in B$, akkor $|a| \leq |b|$. Definiáljuk $\underline{A}$ tetszőleges a elemére az

$$U_a = \{u \in X^*; au \in B\}$$

halmazt. Ha $U_a \neq e$, akkor prefix kód. Legyenek ugyanis $u \in X^+$ és $v \in X^*$ olyanok, amelyekre $u, uv \in U_a$, azaz $au, auv \in B$. Mivel B prefix kód, ezért $v = e$, ami azt jelenti, hogy U_a is prefix kód.

Tegyük fel, hogy $U_a \neq e$. Legyen $u \in U_a$ és $b_k \in B_k$. Mivel $BB_k = AA_k$, ezért van olyan $a' \in A$ és $a_k \in A_k$, hogy $aub_k = a'a_k$. De A prefix kód, ezért $a = a'$ és $ub_k = a_k$. Amiből $U_a B_k \subseteq A_k$ adódik. Az $AA_k = BB_k$ feltételből az is következik, hogy minden $a_k \in A_k$ elemhez van olyan $b \in B$ és $b_k \in B_k$, hogy $aa_k = bb_k$. Az $|a| \leq |b|$ feltevés miatt van olyan $u \in U_a$, amelyre $b = au$. Így $aa_k = aub_k$, azaz $a_k = ub_k$. Ezek szerint $A_k \subseteq U_a B_k$, s így $A_k = U_a B_k$. Ez azonban lehetetlen, mivel A_k irreducibilis prefix kód. Ezért $U_a = e$, $A_k = B_k$ és $AA_k = BA_k$.

Megmutatjuk, hogy $A = B$. Legyen $a_k \in \underline{A}_k$. Ha $c \in A$, akkor van olyan $b \in B$ és $d \in A_k$, hogy $ca_k = bd$. Mivel $a_k \in \underline{A}_k$, ezért $d = va_k$ $(v \in X^*)$, amiből $c = bv$. Hasonlóan kapható, hogy $ba_k = a'd'$ $(a' \in A, d' \in A_k)$, azaz $b = a'v'$ $(v' \in X^*)$. Tehát $c = bv = a'v'v$. Minthogy A prefix kód, ezért $c = a'$ és $v' = v = e$, azaz $c = b$. Ez pedig azt jelenti, hogy $A \subseteq B$. Hasonlóan látható, hogy $B \subseteq A$, vagyis

$$A_1 A_2 \ldots A_{k-1} = A = B = B_1 B_2 \ldots B_{k-1}.$$

Az indukciós feltevés miatt $A_1 = B_1, \ldots, A_{k-1} = B_{k-1}$.

Végül, mivel a 17.19 Következmény szerint maximális prefix kód csak maximális prefix kódok szorzatára bontható, minden maximális prefix kód irreducibilis prefix kódokra való felbontásában csak maximális prefix kódok szerepelnek. Ez azt jelenti, hogy $\mathcal{MP}(X)$ is szabad félcsoport. ($\mathcal{MP}(X)$ bázisa a irreducibilis maximális prefix kódok halmaza.) □

A 17.6 Lemma és a 17.22 Tétel szerint a nyelvek szorzására az X feletti prefix kódok halmaza az X feletti nyelvek szabad részfélcsoportja. A 1.1. alfejezetben láttuk, hogy az X feletti nyelvek a nyelvek összeadására és szorzására félgyűrűt alkotnak. A prefix kódok halmaza azonban nem részfélgyűrűje ennek a félgyűrűnek, mivel nem zárt az összeadásra.

A 17.22 Tételből közvetlenül adódik az alábbi állítás. (Az $\emptyset$ prefix kódra az állítás üresen teljesül.)

17.23. Következmény. *Minden [maximális] prefix kód egyértelműen bontható fel irreducibilis [maximális] prefix kódok szorzatára.*

17.7. Prefix kódok Bernoulli mértéke

17.24. Lemma. *Legyen C prefix kód X felett, $\overline{C}$ a C-beli elemek valódi kezdőszeleteinek halmaza és $Q(\subseteq \overline{C})$ prefix kód X felett. Bármely $q \in \overline{C}$ kezdőszeletre $C_q = \{r \in X^+; qr \in C\}$ és $D_Q = Q + (C - \sum_{q\in Q} qC_q)$ szintén prefix kódok X felett. Továbbá, ha C maximális prefix kód, akkor C_q és D_Q is maximális prefix kódok.*

Bizonyítás Ha $r, ru \in C_q$ $(r \in X^+, u \in X^*)$, akkor $qr, qru \in C$. Mivel C prefix kód, ezért $u = e$. Ez pedig azt jelenti, hogy C_q is prefix kód.

Prefix kód minden részhalmaza is prefix kód, ezért $C - \sum_{q\in Q} qC_q$ prefix kód. Ez utóbbi prefix kód elemeinek kezdőszeletei között nincs Q-beli elem, így D_Q is prefix kód.

Legyen C maximális prefix kód. Tegyük fel ennek ellenére, hogy C_q $(q \in \overline{C})$ nem maximális prefix kód. Akkor van olyan $t \in X^+$, hogy $t \notin C_q$ és $C_q + t$ prefix kód. Mivel $t \notin C_q$, ezért $qt \notin C$. Ha $qt \in \overline{C}$, akkor van olyan $v \in X^+$, hogy $qtv \in C$, azaz $tv \in C_q$. Ez azonban lehetetlen, mert $C_q + t$ prefix kód. Akkor a 16.11 és a 17.5 Tételek szerint $qt \in CX^+$, azaz $qt = qt_1t_2$ $(t_1, t_2 \in X^+)$ és $qt_1 \in C$. Ebből pedig $t_1 \in C_q$ adódik. Ez sem lehetséges, mert $C_q + t$ prefix kód és t_1 kezdőszelete t-nek. Kaptuk tehát, hogy C_q maximális prefix kód.

Legyen továbbra is C maximális prefix kód. Tegyük fel, hogy D_Q $(Q \subseteq \overline{C})$ nem maximális prefix kód. Akkor van olyan $t \in X^+$, hogy $t \notin D_Q$ és $D_Q + t$ prefix kód. Ha $t \in \overline{C}$, akkor van olyan $v \in X^+$, hogy $tv \in C$. A $t \notin D_Q$ feltétel miatt $t \notin Q$, ezért $tv \in C - \sum_{q\in Q} qC_q$. Ez ellentmond annak, hogy $D_Q + t$ prefix kód. Ezért a 16.11 és a 17.5 Tételek szerint $t \in CX^*$, azaz $t = uv$ $(u \in C,\ v \in X^*)$. Mivel $D_Q + t$ prefix kód, így $u \notin \sum_{q\in Q} qC_q$. Amiből $u \in C - \sum_{q\in Q} qC_q$, ami szintén lehetetlen. Vagyis D_Q maximális prefix kód.□

17.25. Következmény. *Ha C [maximális] prefix kód, akkor bármely $q \in \overline{C} - e$ kezdőszeletre $D_q = (C - qC_q) + q$ is [maximális] prefix kód.*

A 17.24 Lemmából prefix kódokra (14.12)-nél erősebb szükséges feltétel adódik:

17.26. Következmény. *Ha π az X halmaz egy Bernoulli mértéke és C prefix kód X felett, akkor*

$$\pi(C) \le \sum_{x\in(\overline{C}+C)\cap X} \pi(x).$$

Bizonyítás Mivel $\{xC_x; x \in \overline{C} \cap X\}$ a $C - X$ prefix kód osztályozása, így (14.2), (14.4), (14.6) és (14.12) miatt

$$\pi(C) = \pi\Big(\sum_{x\in C\cap X} x + \sum_{x\in\overline{C}\cap X} xC_x\Big) = \sum_{x\in C\cap X} \pi(x) + \sum_{x\in\overline{C}\cap X} \pi(x)\pi(C_x) \le$$

$$\leq \sum_{x\in C\cap X} \pi(x) + \sum_{x\in \overline{C}\cap X} \pi(x) = \sum_{x\in(\overline{C}+C)\cap X} \pi(x).$$

□

A 17.25 Következmény bizonyítása szerint, ha C maximális prefix kód, akkor

$$\sum_{x\in(\overline{C}+C)\cap X} \pi(x) = \sum_{x\in X} \pi(x) = \pi(X) = 1,$$

azaz visszakapjuk a (14.12) feltételt.

17.27. Következmény. *Ha π az X halmaz egy Bernoulli mértéke, C és $Q(\subseteq \overline{C})$ prefix kódok X felett, akkor*

$$\pi(C) \leq \pi(D_Q).$$

Bizonyítás A 17.24 Lemmát és a (14.2), (14.4), (14.5), (14.6) és (14.12) összefüggéseket használva

$$\pi(D_Q) = \pi(Q) + \pi(C) - \pi(\sum_{q\in Q} qC_q) \geq \pi(Q) + \pi(C) - \sum_{q\in Q} \pi(qC_q) =$$

$$= \pi(Q) + \pi(C) - \sum_{q\in Q} \pi(q)\pi(C_q) \geq \pi(Q) + \pi(C) - \sum_{q\in Q} \pi(q) = \pi(C).$$

□

Legyen π az X halmaz egy Bernoulli mértéke. Az X feletti L nyelv (π *szerinti*) *átlagos hosszá*nak nevezzük a

$$d(L) = \sum_{p\in L} |p|\pi(p) \tag{17.3}$$

valós számot. Ha $d(L) = \infty$, akkor azt mondjuk, hogy L *átlagos hossza végtelen.*

17.28. Tétel. *Legyen C prefix kód az X halmaz felett. Ha az X halmaz π pozitív Bernoulli mértékére $\pi(C) = 1$, akkor $d(C) = \pi(\overline{C})$. Ha C ritka maximális prefix kód X felett, akkor X bármely π pozitív Bernoulli mértékére $d(C) < \infty$.*

Bizonyítás A bizonyítás során a 17.24 Lemma jelöléseit használjuk. Először megmutatjuk, hogy minden $q \in \overline{C}$ kezdő szeletre $\pi(qC_q) = \pi(q)$. Mivel $C_e = C$, ezért $q = e$ esetben az állítás (14.3)-ból következik. Tegyük fel, hogy $q \neq e$. A 17.24 Lemma szerint C_q prefix kód, ezért (14.2)-t, (14.4)-et és (14.12)-t is felhasználva,

$$\pi(qC_q) = \pi(q)\pi(C_q) \leq \pi(q).$$

A 17.25 Következmény szerint $D_q = (C - qC_q) + q$ is prefix kód, ezért $qC_q \subseteq C$ miatt

$$1 \geq \pi(D_q) = \pi(C) - \pi(qC_q) + \pi(q) = 1 - \pi(qC_q) + \pi(q).$$

Ebből $\pi(q) \leq \pi(qC_q)$, azaz $\pi(q) = \pi(qC_q)$. (Innen még az is adódik, hogy $\pi(q) = \pi(q)\pi(C_q)$, vagyis $\pi(C_q) = 1$.) Nyilvánvaló, hogy $C = \sum_{q\in\overline{C}} qC_q$. Másrészt, ha $x_1 \dots x_k \in C$ $(x_1, \dots, x_k \in X)$, akkor $\pi(x_1 \dots x_k)$ a

$$\pi(eC_e) = \pi(C), \pi(x_1C_{x_1}), \dots, \pi(x_1 \dots x_{k-1}C_{x_1\dots x_{k-1}})$$

összegek mindegyikében pontosan egyszer szerepel összeadandóként és más $\pi(qC_q)$ $(q \in \overline{C})$ összegben nem szerepel. Így

$$\pi(\overline{C}) = \sum_{q\in\overline{C}} \pi(q) = \sum_{q\in\overline{C}} \pi(qC_q) = \sum_{p\in C} |p|\pi(p) = d(C).$$

Ha a C ritka maximális prefix kód X felett, akkor a 16.5 Tétel alapján $\pi(C) = 1$. Így a tétel első állítása szerint $d(C) = \pi(\overline{C})$. De C ritka nyelv, amiből nem nehéz belátni, hogy $\overline{C}$ is ritka nyelv. A 16.3 Lemmából következik, hogy $d(C) = \pi(\overline{C}) < \infty$. □

17.29. Példa. *Legyen $X = \{a, b\}$ és $0 < r < 1$ tetszőleges valós szám. Ha $\pi(a) = 1 - r$ és $\pi(b) = r$, akkor az a^*b prefix kód átlagos hossza $\frac{1}{r}$.*

Ugyanis $\overline{a^*b} = a^*$, ezért

$$d(a^*b) = \pi(a^*) = \sum_{k=0}^{\infty} \pi(a^k) = \sum_{k=0}^{\infty} \pi(a)^k = \sum_{k=0}^{\infty} (1-r)^k = \frac{1}{r}.$$

17.30. Példa. *Ha π az X halmaz tetszőleges pozitív Bernoulli mértéke, akkor bármely pozitív egész k esetén az X^k maximális uniform kód átlagos hossza k. (Mivel $\overline{X^k} = \sum_{j=0}^{k-1} X^j$, ezért, a 14.1 Lemmát is felhasználva,*

$$d(X^k) = \pi(\overline{X^k}) = \sum_{j=0}^{k-1} \pi(X^j) = k.)$$

17.8. Reguláris prefix kódok

Az $\mathbf{A} = (A, X, \delta)$ automata tetszőleges $a \in A$ állapotára definiáljuk az X^* bemenő monoid X_a részhalmazát következőképpen:

$$X_a = \{r \in X^*;\ ar = a\}. \tag{17.4}$$

Ezt a részhalmazt $a \in A$ *stabilizátor*ának nevezzük.

Az $\mathbf{A} = (A, X, \delta)$ automatát *erősen összefüggő*nek nevezünk, ha bármely állapotból minden állapot elérhető, azaz bármely $a, b \in A$ állapotpárhoz van olyan $p \in X^*$, hogy $ap = b$. Emlékeztetünk a δ átmenetfüggvény (6.2)- (6.4) feltételekkel definiált kiterjesztésére. Nyilvánvaló az is, hogy bármely $a \in A$ állapotra és $p, q \in X^*$ bemenő szavakra $(ap)q = apq$.

17.31. Lemma. *Az $\mathbf{A} = (A, X, \delta)$ automata bármely állapotának stabilizátora az X^* bemenő monoid bal unitér részmonoidja, azaz bázisa prefix kód. Ha $\mathbf{A}$ erősen összefüggő, akkor bármely állapotának stabilizátora X^* olyan bal unitér részmonoidja, amelynek bázisa maximális prefix kód.*

Bizonyítás Ha $p, q \in X_a$, akkor $apq = aq = a$ és $ae = a$, azaz X_a X^* részmonoidja. Ha pedig $p, pq \in X_a$, akkor $a = apq = aq$, tehát $q \in X_a$, vagyis X_a bal unitér. Legyen C X_a bázisa, azaz $X_a = C^*$. A 13.9 Tétel szerint C prefix kód.

Legyen $\mathbf{A}$ erősen összefüggő és $a \in A$ tetszőleges állapot. Legyen $p \in X^+$ és $ap = b$. Tegyük fel, hogy $q \in X^*$ a p szó leghosszabb olyan kezdőszelete, amelyre $aq = a$. Ha $p = qr$ $(r \in X^*)$, akkor $ar = b$. Mivel $\mathbf{A}$ erősen összefüggő, van olyan $t \in X^*$, amelyre $art = bt = a$. Ez azt jelenti, hogy $r \in \overline{C}$. Ebből következik, hogy $X^* = C^*\overline{C}$. A 16.11 és a 17.5 Tételek szerint C maximális prefix kód. □

A következő eredmény a reguláris prefix kódok egy egyszerű jellemzését adja. A 16.12 Tétel szerint a véges ábécé feletti reguláris prefix kódok ritka kódok.

17.32. Lemma. *Az X véges ábécé feletti C prefix kód akkor és csak akkor reguláris, ha C valódi kezdőszeleteinek $\overline{C}$ halmaza véges.*

Bizonyítás Az (1.1) definíciót használva a C prefix kód $p \in X^*$ szerinti bal oldali deriváltján a

$$C_p^{(b)} = \{q \in X^*; pq \in C\}$$

nyelvet értjük. Nyilvánvaló, hogy $C_p^{(b)} \neq \emptyset$ akkor és csak akkor, ha $p \in \overline{C} + C$. Továbbá minden $p \in C$ kódszóra $C_p^{(b)} = \{e\}$. Ezekből és a 8.7 Tételből következik az állítás. □

A 2.8 Tétel szerint a 17.32 Lemma megfelelő átfogalmazása teljesül szuffix kódokra.

A következő tétel szerint minden (nemüres) prefix kód felismerhető inicálisan összefüggő automatában egy állapottal.

17.33. Tétel. *Ha* $\mathbf{A} = (A, a_0, X, \delta)$ *iniciális automata* $d \in A - a_0$ *állapotára* $X_d = \{e\}$*, akkor* $L(\mathbf{A}, d)$ *prefix kód. Megfordítva, minden* X *feletti* C *prefix kódhoz van olyan* $\mathbf{A} = (A, a_0, X, \delta)$ *automata, amelynek valamely* $d \in A - a_0$ *állapotára* $X_d = \{e\}$ *és* $C = L(\mathbf{A}, d)$*. Ha* $C \neq \emptyset$*, akkor* $\mathbf{A}$ *választható iniciálisan összefüggőnek. Ha* X *véges ábécé és* L *reguláris, akkor az* $\mathbf{A}$ *automata választható végesnek.*

Bizonyítás Legyen az $\mathbf{A} = (A, a_0, X, \delta)$ iniciális automata $d \in A - a_0$ állapotának stabilizátora $X_d = \{e\}$. Ha $L(\mathbf{A}, d) = \emptyset$, akkor nyilvánvalóan prefix kód. Tegyük fel, hogy $L(\mathbf{A}, d) \neq \emptyset$ és $a_0 p = a_0 q = d$ $(p, q \in X^+)$. Ha $p = qu$ $(u \in X^*)$, akkor $du = a_0 qu = a_0 p = d$, azaz $u = e$. Hasonlóan kapjuk, hogy p sem valódi kezdőszelete q-nak, vagyis $L(\mathbf{A}, d)$ prefix kód.

Megfordítva, legyen C prefix kód X felett. Ha $C = \emptyset$ és $\mathbf{A} = (A, a_0, X, \delta)$ legalább kétállapotú *diszkrét automata*, azaz amelynek minden állapota csapda, akkor bármely $d \in A - a_0$ állapotára $\emptyset = L(\mathbf{A}, d)$. Tegyük fel, hogy $C \neq \emptyset$ és $\overline{C}$ a C prefix kód valódi kezdőszeleteinek halmaza. Továbbá $c, d \notin \overline{C}$, $c \neq d$ és $A = \overline{C} \cup \{c, d\}$. Definiáljuk az $\mathbf{A} = (A, e, X, \delta)$ iniciális automata δ átmenetfüggvényét a következőképpen:

$$\delta(q, x) = \begin{cases} qx, & \text{ha } q, qx \in \overline{C}, \\ d, & \text{ha } q \in \overline{C}, qx \in C, \\ c, & \text{minden más esetben.} \end{cases} \tag{17.5}$$

Az $\mathbf{A}$ automata iniciálisan összefüggő és $C = L(\mathbf{A}, d)$.

Ha X véges ábécé és C reguláris, akkor a 17.31 Lemma szerint $\overline{C}$ véges, s így A is véges. □

A (17.5) definíció egy eljárást ad véges ábécé feleltti reguláris prefix kódokat felismerő automaták szerkesztésére.

17.9. Ciklikus automaták

Az alfejezetben megmutatjuk a ciklikus automaták és a prefix kódok, speciálisan erősen összefüggő automaták és a maximális prefix kódok szoros kapcsolatát. Megjegyezzük, hogy az erősen összefüggő automaták központi szerepet játszanak az automaták algebrai elméletében. A ciklikus automaták az információátalakító és a nyelvfelismerő rendszereknél alapvető jelentőségűek.

Az $\mathbf{A} = (A, X, \delta)$ automatát *ciklikus*nak nevezünk, ha van olyan állapota, amelyből minden állapot elérhető, azaz van olyan $a_0 \in A$, hogy minden $b \in A$ állapothoz létezik olyan $p \in X^*$ bemenő szó, amelyre $a_0 p = b$. Ebben az esetben a_0-t az $\mathbf{A}$ automata *generátorelem*ének nevezzük. Nyilvánvaló, hogy egy

iniciálisan összefüggő automata olyan ciklikus automata, amelyben a kezdőállapot generátor elem. Ezek szerint a 17.8. alfejezetben definált erősen összefüggő automata olyan ciklikus automata, amelynek minden állapota generátorelem.

Legyen ρ az X^* ($X \neq \emptyset$) szabad monoid jobb kongruenciája. Definiáljuk az $\mathbf{X}^*/\rho = (X^*/\rho, X, \delta_\rho)$ automata átmenetfüggvényét a

$$\delta_\rho(\rho[p], x) = \rho[px] \quad (p \in X^*, x \in X) \tag{17.6}$$

feltétellel. Nem nehéz belátni, hogy $\mathbf{X}^*/\rho$ ciklikus automata és $\rho[e]$ az automata egy generátoreleme. Ha $\rho[e] = \{e\}$, akkor azt mondjuk, hogy az $\mathbf{X}^*/\rho$ automata az *üres szóval*, ha pedig $\rho[e] \neq \{e\}$, akkor az *üres szó nélkül ciklikus*. Ez utóbbi pontosan azt jelenti, hogy van olyan $r \in X^+$, amelyre $(e, r) \in \rho$. Ekkor a ρ-t *moduláris jobb kongruenciá*nak nevezzük.

Most megmutatjuk, hogy az $\mathbf{A} = (A, X, \delta)$ ciklikus automaták izomorfiától eltekintve éppen az $\mathbf{X}^*/\rho$ automaták, ahol a ρ relációk X^* jobb kongruenciái. Ehhez szükségünk lesz a (6.15) feltétellel definiált $\rho_{\mathbf{A},a}$ ($a \in A$) relációkra.

17.34. Lemma. *Ha a_0 az $\mathbf{A} = (A, X, \delta)$ ciklikus automata egy generátoreleme, akkor $\mathbf{A} \cong \mathbf{X}^*/\rho_{\mathbf{A},a_0}$.*

Bizonyítás Definiáljuk a $\varphi : A \to X^*/\rho_{\mathbf{A},a_0}$ leképezést a

$$\varphi(a_0 p) = \rho_{\mathbf{A},a_0}[p], \quad p \in X^*$$

feltétellel. Könnyen megmutatható, hogy φ az $\mathbf{A}$ automata izomorf leképezése az $\mathbf{X}^*/\rho_{\mathbf{A},a_0}$ automatára. □

17.35. Lemma. *Ha ρ az X^* szabad monoid jobb kongruenciája, akkor $\rho[e]$ az X^* szabad monoid bal unitér részfélcsoportja.*

Bizonyítás Ha $(e, p) \in \rho$ és $(e, q) \in \rho$ ($p, q \in X^*$), akkor $(q, pq) \in \rho$. De $(e, q) \in \rho$, ezért $(e, pq) \in \rho$, azaz $\rho[e]$ X^* részmonoidja. Ha pedig $(e, p) \in \rho$ és $(e, pq) \in \rho$ ($p, q \in X^*$), akkor $(q, pq) \in \rho$ és így $(e, q) \in \rho$, azaz $\rho[e]$ bal unitér.□

A 13.9 Tétel szerint X^* minden bal unitér részmonoidjának bázisa prefix kód X felett és minden X feletti prefix kód X^* egy bal unitér részmonoidjának bázisa. Ha $\rho[e] = \{e\}$, akkor bázisa $\emptyset$. Ha ρ moduláris, akkor van olyan X feletti $C \neq \emptyset$ prefix kód, hogy $\rho[e] = C^*$.

17.36. Lemma. *Ha C prefix kód X felett, akkor a*

$$\mathcal{C} = \{C^* p \ ; \ p \in X^* - CX^*\}. \tag{17.7}$$

rendszer az X^* szabad monoid egy osztályozása.

Bizonyítás Ha $p, q \in X^* - CX^*$ szavakra $C^*p \cap C^*q \neq \emptyset$, akkor vannak olyan $r, t \in C^*$, amelyekre $rp = tq$. Ebből $p \in C^+q$ vagy $q \in C^+p$ vagy $p = q$. Mivel $p, q \in X^* - CX^*$, ezért $p = q$.

Ha $p \in CX^*$, akkor vannak olyan $q \in C^+$ és $r \in X^* - CX^*$, amelyekre $p = qr \in C^*r$. Ezekből következik, hogy $\mathcal{C}$ valóban X^* egy osztályozása. □

Jelöljük a $\mathcal{C}$-hez tartozó ekvivalenciát ρ_C-vel. A definícióból látható, hogy $\rho_C = \iota_{X^*}$ akkor és csak akkor, ha $C = \emptyset$, és $\rho_C = \omega_{X^*}$ akkor és csak akkor, ha $C = X$.

17.37. Lemma. *Bármely X feletti C prefix kódra ρ_C az X^* egy jobb kongruenciája és $\rho_C[e] = C^*$. Továbbá, ha ρ az X^* szabad monoid olyan jobb kongruenciája, amelyre $\rho[e] = C^*$, akkor $\rho_C \subseteq \rho$. (Ha $C \neq \emptyset$, akkor ρ moduláris jobb kongruencia.)*

Bizonyítás A 17.36 Lemmából következik, hogy ρ_C jobb kongruencia és $\rho_C[e] = C^*$.

Legyen ρ az X^* szabad monoid olyan jobb kongruenciája, amelyre $\rho[e] = C^*$. Ha $(p, q) \in \rho_C$, akkor van olyan $r \in X^* - CX^*$, amelyre $p, q \in C^*r$, azaz vannak olyan $t, s \in C^*$, hogy $p = tr$ és $q = sr$. Mivel $\rho[e] = C^*$, ezért $(e, t) \in \rho$ és $(e, s) \in \rho$. Amiből következik, hogy $(t, s) \in \rho$. De ρ jobb kongruencia, így $(tr, sr) \in \rho$, vagyis $(p, q) \in \rho$. Ez azt jelenti, hogy $\rho_C \subseteq \rho$. □

17.38. Tétel. *Legyen ρ az X^* szabad monoid jobb kongruenciája és C prefix kód, amelyre $\rho[e] = C^*$. Az $\mathbf{X}^*/\rho = (X^*/\rho, X, \delta_\rho)$ automata akkor és csak akkor erősen összefüggő, ha C maximális prefix kód.*

Bizonyítás Legyen C maximális prefix kód. Tekintsük először az

$$\mathbf{X}^*/\rho_C = (X^*/\rho_C, X, \delta_{\rho_C}) \tag{17.8}$$

automatát. A 16.11 és a 17.5 Tételek szerint a (17.7) definíciót felhasználva kapjuk, hogy

$$X^*/\rho_C = \{C^*q;\ q \in \overline{C}\}. \tag{17.9}$$

Legyenek $q_1, q_2 \in \overline{C}$ tetszőlegesek. Van olyan $r \in X^+$, hogy $q_1r \in C$, ezért

$$(C^*q_1)rq_2 = (C^*q_1r)q_2 = C^*q_2,$$

azaz $\mathbf{X}^*/\rho_C$ erősen összefüggő. A 17.37 Lemma szerint $\rho_C \subseteq \rho$, amiből következik, hogy az $\mathbf{X}^*/\rho$ automata az $\mathbf{X}^*/\rho_C$ automata homomorf képe. Mivel erősen összefüggő automata homomorf képe is erősen összefüggő, ezért $\mathbf{X}^*/\rho$ erősen összefüggő.

Megfordítva, legyen $\mathbf{X}^*/\rho$ erősen összefüggő. (Ebben az esetben ρ mindig moduláris jobb kongruencia.) Nyilvánvaló, hogy $\overline{C} \subseteq X^* - CX^*$. Legyen $q \in X^* - CX^*$ és $r \in \overline{C}$. A 17.36 Lemma alapján $\rho_C \subseteq \rho$, ezért $C^*r \subseteq \rho[r]$. Az $\mathbf{X}^*/\rho$ automata erősen összefüggősége miatt van olyan $p \in X^*$, hogy

$$\rho[qp] = \rho[q]p = \rho[r],$$

azaz $(qp, r) \in \rho$. De $r \in \overline{C}$, így van olyan $t \in X^+$, hogy $rt \in C$. Minthogy ρ jobb kongruencia, $(qpt, rt) \in \rho$. Mivel $\rho[e] = C^*$, ebből következik, hogy $(e, qpt) \in \rho$, vagyis $qpt \in C^*$. De $q \in X^* - CX^*$, ezért $q \in \overline{C}$. Kaptuk, hogy $X^* - CX^* \subseteq \overline{C}$, azaz $X^* - CX^* = \overline{C}$, vagyis $X^* = \overline{C} + CX^*$. A 16.11 és a 17.5 Tételek szerint a C maximális prefix kód. □

Feladatok

17.1. Az X feletti nemüres C nyelv akkor és csak akkor prefix kód, ha minden X feletti A és B nyelvre $C(A \cap B) = CA \cap CB$.
17.2. A C X feletti prefix kódra és L X feletti nyelvre CL akkor és csak akkor prefix kód, ha L is prefix kód.
17.3. Legyenek $C_1, C_2, \ldots C_n$ nemüres nyelvek X felett. Ha $C_1C_2 \ldots C_n$ prefix kód, akkor $C_2C_3 \ldots C_n, C_3 \ldots C_n, \ldots, C_{n-1}C_n, C_n$ is prefix kódok. Fogalmazzuk meg az állítást szuffix kódokra is.
17.4. Legyen $C \neq \emptyset$ prefix kód az X ábécé felett. Ha C nem maximális prefix kód, akkor $V = X^* - (\overline{C} + CX^*)$ az X^+ szabad félcsoport jobb ideálja.
17.5. Tetszőleges $C \neq \emptyset$ X feletti prefix kódra $C + (V - VX^+)$ maximális prefix kód és $\overline{V - VX^+} \subseteq \overline{C}$, ahol V a 17.4. feladatban definiált halmaz.
17.6. Ha $C \neq \emptyset$ prefix kód X felett és D a C kódot tartalmazó maximális prefix kód X felett, akkor

$$\overline{D} = \overline{C} \quad \Longleftrightarrow \quad D = C + (V - VX^+),$$

ahol V a 17.4. feladatban definált halmaz.
17.7. Ha C a legalább kételemű X ábécé felett prefix [szuffix] kód és L diszjunktív nyelv, akkor CL [LC] is diszjunktív nyelv X felett.
17.8. Ha C a legalább kételemű X ábécé felett prefix kód és D diszjunktív prefix kód, akkor CD is diszjunktív prefix kód X felett.
17.9. Jelölje $X(k)$ X^* legfeljebb k hosszúságú szavainak részhalmazát. Az $L \subseteq X^*$ nyelvet *jobbról k teljes*nek nevezzük, ha minden $p \in X^*$ szóra

$$pX(k) \cap L^* \neq \emptyset.$$

(Minden jobbról k teljes nyelv jobbról teljes.) Ha $L \subseteq X^+$ jobbról k teljes (l. 16.2 feladatot!), akkor $C(L) = L - LX^+$ jobbról k teljes maximális prefix kód.

17.10. Legyen C maximális prefix kód X felett és $\overline{C}$ a C-beli kódszavak valódi prefixeinek halmaza. C akkor és csak akkor jobbról k teljes, ha minden $u \in \overline{C}$ esetén $uX(k) \cap C \neq \emptyset$.

17.11. Ha $L \subseteq X^*$ jobbról k teljes nyelv, akkor tartalmaz minimális jobbról k teljes nyelvet.

17.12. Ha $L \subseteq X^*$ minimális jobbról k teljes nyelv, akkor maximális prefix kód X felett.

18. fejezet

Szemafor kódok

Ebben a fejezetben az X^+ szabad félcsoport nemüres részhalmazai segítségével adunk meg maximális prefix [szuffix] kódokat. Ezek a prefix [szuffix] kódok egy érdekes részosztályát alkotják. Az eredményeket prefix kódokra adjuk meg, szuffix kódokra való átfogalmazásuk a következő lemma mintájára könnyen megtehető.

18.1. Lemma. *Legyen C prefix [szuffix] kód X felett. Az X^* szabad monoid egy L részhalmazára $LX^* = CX^*$ [$X^*L = X^*C$] akkor és csak akkor, ha $C = L - LX^+$ [$C = L - X^+L$].*

Bizonyítás A bizonyítást csak prefix kódokra végezzük el. Ha $C = \emptyset$, úgy $LX^* = CX^*$ akkor és csak akkor, ha $L = \emptyset$, ezért feltehetjük, hogy $C \neq \emptyset$.

Legyen $C = L - LX^+$. Az nyilvánvaló, hogy $CX^* \subseteq LX^*$. Megmutatjuk hogy $LX^* \subseteq CX^*$. Ha $p \in L$, akkor van olyan $q \in C$ és $u \in X^*$, hogy $p = qu$. Ezért bármely $v \in X^*$ esetén $pv = quv \in CX^*$. Ezzel megmutattuk hogy $LX^* \subseteq CX^*$. Tehát $LX^* = CX^*$.

Megfordítva, tegyük fel, hogy $LX^* = CX^*$. Ebből

$$LX^+ = LX^*X = CX^*X = CX^+.$$

Legyen $p \in L - LX^+$. Akkor $p = qr$ $(q \in C, r \in X^*)$. Ha $r \neq e$, akkor $p \in CX^+ = LX^+$, ami lehetetlen. Ezért $r = e$ és $p = q \in C$, vagyis $L - LX^+ \subseteq C$. Ha $p \in C$, akkor $p = qr$ $(q \in L, r \in X^*)$. Hasonlóan $q = st$ $(s \in C, t \in X^*)$. Így $p = str$. Mivel C prefix kód, ezért $tr = e$, amiből $p = q$, azaz $C \subseteq L - LX^+$.□

18.2. Következmény. *Ha az X feletti C és D prefix kódokra $CX^* = DX^*$, akkor $C = D$.*

18.3. Tétel. *Az X^+ szabad félcsoport L részhalmazára $L - LX^+$ akkor és csak akkor maximális prefix kód, ha L jobbról teljes.*

Bizonyítás A 16.11 Tétel szerint L akkor és csak akkor jobbról teljes, ha LX^* jobbról sűrű. A 18.1 Lemma szerint $LX^* = (L - LX^+)X^*$. Ebből az 17.5 Tételt alkalmazva kapjuk, hogy $(L - LX^+)X^*$ akkor és csak akkor jobbról sűrű, ha $L - LX^+$ maximális prefix kód. □

18.4. Lemma. *Az X^+ szabad félcsoport tetszőleges $L \neq \emptyset$ részhalmazára*

$$C = X^*L - X^*LX^+ \tag{18.1}$$

maximális prefix kód X felett.

Bizonyítás Az X^*L halmaz az X^* szabad monoid bal ideálja, következésképpen jobbról sűrű, s így jobbról teljes. A 18.3 Tétel szerint C maximális prefix kód. □

A (18.1) feltételt teljesítő C kódot (*az L-hez tartozó*) *szemafor prefix kód*nak nevezzük. Az L halmazt a C kód egy *szemafor prefix halmaz*ának, elemeit pedig C *szemafor prefixei*nek nevezzük. Egy uniform kód olyan szemafor prefix kód, amely saját magának szemafor prefix halmaza.

A szemafor prefix kódok szemafor prefixre végződnek, de nincs olyan valódi prefixük, amely szintén szemafor prefixre végződne. Szemafor prefix kódszavakkal kódolt szöveg könnyebb dekódolást tesz lehetővé, balról jobbra olvasva a szöveget a szemafor prefixek mintegy elválasztják a kódszavakat egymástól.

A 18.4 Lemmát szuffix kódokra átfogalmazva kapjuk, hogy az X^+ szabad félcsoport tetszőleges $L \neq \emptyset$ részhalmazára

$$C = LX^* - X^+LX^* \tag{18.2}$$

maximális szuffix kód X felett. A (18.2) feltételt teljesítő kódot (*az L-hez tartozó*) *szemafor szuffix kód*nak nevezzük. Az L halmazt a C kód egy *szemafor szuffix halmaz*ának, elemeit pedig C *szemafor szuffixei*nek nevezzük. Egy uniform kód olyan szemafor szuffix kód is, amely saját magának szemafor szuffix halmaza. A szemafor szuffix kódok szemafor szuffixre végződnek, de nincs olyan valódi szuffixük, amely szintén szemafor szuffixre végződne. A szemafor prefix és a szemafor szuffix kódokat együttvéve *szemafor kódok*nak is mondjuk.

18.5. Példa. *Legyen $X = \{a, b\}$. Megadjuk az $L = \{b\}$ halmazhoz tartozó C szemafor prefix kódot. A (18.1) feltétel szerint*

$$C = \{a, b\}^*b - \{a, b\}^*b\{a, b\}^+ = a^*b.$$

Ez a kód a 16.7 Példában is szerepelt. Megemlítjük, hogy

$$C = \{a, b\}^*a^+ - \{a, b\}^*a^+\{a, b\}^+$$

is igaz, vagyis egy szemafor prefix kódhoz nem csak egy szemafor prefix halmaz tartozhat.

18.6. Példa. *Legyen továbbra is* $X = \{a, b\}$ *és* $L = \{a^2, ab\}$. *Minthogy* $X^*L = \{a, b\}^*a\{a, b\}$, *ezért* $C = X^*L - X^*LX^+ = b^*a\{a, b\}$, *azaz* C *az* L *halmazhoz tartozó szemafor prefix kód.*

A következő tétel jellemzi a szemafor prefix kódokat a kódok között.

18.7. Tétel. *Az* X *feletti* C *prefix kód akkor és csak akkor szemafor prefix kód, ha*

$$X^*C \subseteq CX^*. \tag{18.3}$$

Bizonyítás Legyen $C = X^*L - X^*LX^+$ szemafor prefix kód. Tegyük fel, hogy $p \in X^*C$. Akkor $p \in X^*L$, ezért van részszava L-ből. Ha q a p legrövidebb kezdőszelete, amelyre $q \in X^*L$, akkor $q \in C$, s ezért $p \in CX^*$.

Megfordítva, tegyük fel, hogy a C prefix kódra teljesül (18.3). Ha $L = CX^*$, akkor $LX^* = CX^*X^* = CX^*$. A 18.1 Lemma szerint $C = L - LX^+$. A (18.3) feltételből következik, hogy

$$X^*L = X^*CX^* \subseteq CX^* = L,$$

így $L = X^*L$ és $C = X^*L - X^*LX^+$. □

A 18.4 Lemma szerint minden szemafor prefix kód maximális prefix kód. A következő példa szerint nem minden maximális prefix kód szemafor prefix kód.

18.8. Példa. *Legyen* $C = \{a^2, aba, ab^2, b\}$. *A* C *gráfja segítségével könnyen megmutatható, hogy* C *maximális prefix kód, azonban nem szemafor prefix kód, mivel* $ab \in X^*C$, *de* $ab \notin CX^*$, *s így nem teljesül (18.3):*

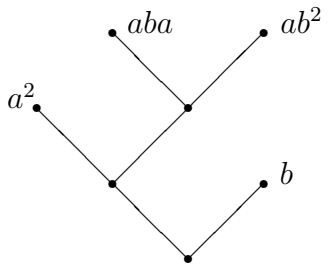
Egy szemafor prefix kód maximális prefix kód, ezért jobbról teljes kód is. Most megmutatjuk, hogy egy jobbról teljes nyelv pontosan milyen esetben szemafor prefix kód.

18.9. Tétel. *Az* X *feletti jobbról teljes* L *nyelv akkor és csak akkor szemafor prefix kód, ha*

$$L \cap X^*LX^+ = \emptyset. \tag{18.4}$$

Bizonyítás Legyen az X feletti jobbról teljes L nyelv szemafor prefix kód. A (18.3) feltételből következik, hogy

$$X^*LX^+ \subseteq LX^*X^+ = LX^+,$$



18.1. ábra.

így

$$L \cap X^*LX^+ \subseteq L \cap LX^+ = \emptyset.$$

Megfordítva, tegyük fel, hogy (18.4) teljesül. Ebből következik, hogy L prefix kód. Megmutatjuk, hogy teljesül (18.3), azaz L szemafor prefix kód. Legyen $rs \in X^*L$ ($r \in X^*$, $s \in L$). Mivel L jobbról teljes, ezért a 16.11 Tétel (4) feltétele miatt $rsu = tv$ valamely $t \in L$, $u, v \in X^*$ esetén. A (18.4) feltételből következik, hogy rs nem valódi kezdőszelete t-nek. Így $rs \in tX^* \subseteq LX^*$. □

18.10. Következmény. *Minden szemafor prefix kód ritka kód.*

Bizonyítás Legyen C szemafor prefix kód X felett. Ha $p \in CX^+$, akkor (18.4) miatt $C \cap X^*pX^* \subseteq C \cap X^*CX^+ = \emptyset$. □

A 17.8 Tételből kapjuk, hogy minden szemafor kód maximális kód.

18.11. Következmény. *Ha C szemafor prefix kód X felett, akkor $\overline{C}C \subseteq C\overline{C} + C^2$, ahol $\overline{C}$ a C-beli elemek valódi kezdőszeleteinek halmaza.*

Bizonyítás Legyen $p \in \overline{C}$ és $u \in C$. A (18.3) feltétel szerint $pu = tv$ valamely $t \in C$ és $v \in X^*$ esetén. Mivel C prefix kód, ezért p a t szó valódi kezdőszelete. Következésképpen v az u valódi zárószelete. Ezért (18.4) szerint $v \notin CX^+$. A C maximális prefix kód, így $v \in \overline{C} + C$. Ebből $pu = tv \in C(\overline{C} + C) = C\overline{C} + C^2$.□

A (18.4) feltétel azt fejezi ki, hogy szemafor prefix kód olyan kód, amelyben egy kódszó egy másik kódszóban csak zárószeletként fordulhat elő. Ezt a tényt használjuk fel a szemafor prefix kódok jellemzésére a maximális prefix kódok között.

Az X^* szabad monoid egy L részhalmazát *prefixre* [*szuffixre*] *zárt*nak nevezzük, ha bármely elemének minden prefixét [szuffixét] tartalmazza. Prefixre [szuffixre] zárt részhalmaz akkor és csak akkor szuffixre [prefixre] zárt, ha bármely elemének minden részszavát tartalmazza.

18.12. Tétel. *Az X feletti C maximális prefix kód akkor és csak akkor szemafor prefix kód, ha $\overline{C}$ szuffixre zárt.*

Bizonyítás Legyen C szemafor prefix kód X felett. Ha $p = uq \in \overline{C}$ $(u, q \in X^*)$, akkor van olyan $v \in X^+$, hogy $pv \in C$. Így $q \notin CX^*$, mert különben $pv = uqv \in X^*CX^+$, ami ellentmond (18.4)-nek. A 17.5 Tétel szerint $q \in \overline{C}$.

Legyen most $\overline{C}$ szuffixre zárt. Tegyük fel, hogy $C \cap X^*CX^+ \neq \emptyset$. Legyen $p \in C \cap X^*CX^+$. Akkor $p = uqv$ $(u \in X^*,\ q \in C,\ v \in X^+)$. Ebből következik, hogy $uq \in \overline{C}$, s így $q \in \overline{C}$, ami lehetetlen. Kaptuk, hogy $C \cap X^*CX^+ = \emptyset$, azaz a 18.9 Tétel szerint C szemafor prefix kód. □

18.13. Tétel. *Az X^+ nemüres L és K részhalmazaihoz akkor és csak akkor tartozik ugyanaz a szemafor prefix kód, ha $X^*LX^* = X^*KX^*$. Ha C szemafor prefix kód, akkor $C - X^+C$ a legkisebb szemafor prefix halmaza, azaz C bármely L szemafor prefix halmazára $C - X^+C \subseteq L$.*

Bizonyítás Legyen $C = X^*L - X^*LX^+$ és $D = X^*K - X^*KX^+$. A 18.1 Lemmát felhasználva nyerjük, hogy $CX^* = X^*LX^*$ és $CX^* = X^*KX^*$. A 18.2 Következmény miatt $C = D$ akkor és csak akkor, ha

$$X^*LX^* = CX^* = DX^* = X^*KX^*.$$

Legyen $C = X^*L - X^*LX^+$ szemafor prefix kód és $K = C - X^+C$. A 18.1 Lemma szuffix kódokra vonatkozó állításából kapjuk, hogy $X^*K = X^*C$. Ismét a 18.1 Lemmát használva, $X^*KX^* = X^*CX^* = X^*LX^*$, azaz $K = C - X^+C$ valóban C egy szemafor prefix halmaza.

Legyen T a C tetszőleges szemafor prefix halmaza és $p \in K = C - X^+C$. Akkor $X^*TX^* = X^*KX^*$. Így $p = uqv$ $(u, v \in X^*,\ q \in T$ és $q = u'q'v'$ $(u', v' \in X^*,\ q' \in K)$, azaz $p = uu'q'v'v$. Mivel $K \subseteq C$, ezért (18.4) szerint $v'v = e$. Azonban K szuffix kód, ezért $uu' = e$, vagyis $p = q \in T$. □

A 18.13 Tétel szerint egy szemafor prefix kód legkisebb szemafor prefix halmaza éppen a szemafor prefix kód legnagyobb szuffix részkódja.

18.14. Tétel. *Ha C és D szemafor prefix kód, akkor CD is szemafor prefix kód. Megfordítva, ha CD szemafor prefix kód és C prefix kód, akkor C is szemafor prefix kód.*

Bizonyítás Ha C és D szemafor prefix kód X felett, akkor a 17.18 Következmény miatt CD is prefix kód X felett. Akkor (18.3) szerint

$$X^*CD \subseteq CX^*D \subseteq CDX^*,$$

azaz CD is szemafor prefix kód.

Legyen CD szemafor prefix kód és C prefix kód X felett. Megmutatjuk, hogy $X^*C \subseteq CX^*$. A 18.7 Tétel szerint ez azt jelenti, hogy C szemafor prefix kód. Legyen $up \in X^*C$ ($u \in X^*, p \in C$) és q egy minimális hosszúságú szó D-ből. Akkor a (18.3) feltétel szerint $upq = p'q'u'$ valamely $p' \in C,\ q' \in D,\ u' \in X^*$ szavakra. A q szó választása miatt $|q| \leq |q'| \leq |q'u'|$, így $|up| \geq |p'|$, amiből következik, hogy $up \in CX^*$. □

A következő példa azt mutatja, hogy ha CD szemafor prefix kód, akkor D nem szükségképpen szemafor prefix kód még akkor sem, ha C szemafor prefix kód és D maximális prefix kód.

18.15. Példa. *A 18.5 Példában láttuk, hogy $C = a^*b$ szemafor prefix kód, az 18.8 Példában pedig azt, hogy $D = \{a^2, aba, ab^2, b\}$ maximális prefix kód, de nem szemafor prefix kód $\{a, b\}$ felett. A 18.4 Lemma szerint CD maximális prefix kód és*

$$\overline{CD} = a^*\{e, b, ba, bab\}$$

szuffixre zárt. A 18.12 Tétel miatt C szemafor prefix kód.

18.16. Következmény. *Legyen C tetszőleges X feletti nyelv és $n > 1$ tetszőleges pozitív egész szám. A C nyelv akkor és csak akkor szemafor prefix kód, ha C^n is szemafor prefix kód.*

Bizonyítás Ha C^n szemafor prefix kód, akkor a 17.19 Következmény miatt C prefix kód. Az 18.14 Tétel szerint C is szemafor prefix kód. Az állítás megfordítása teljes indukcióval kapható a 18.14 Tételből. □

Feladatok

18.1. Egy $\emptyset \subset L \subseteq X^+$ nyelvre $L - LX^+$ akkor és csak akkor szemafor prefix kód, ha $X^*L \subseteq LX^*$.

18.2. Az X feletti C kód akkor és csak akkor szemafor prefix kód, ha $X^*C \subseteq CX^*$. (A 18.7 Tétel egy általánosítása.)

18.3. Jelölje az X feletti C jobbról teljes kódra $\overline{C}$ ill. $\underline{C}$ a valódi kezdőszeleteinek ill. valódi zárószeleteinek halmazát. C akkor és csak akkor szemafor prefix kód, ha $\overline{C}C \subseteq C\underline{C}$.

19. fejezet

Bifix kódok

A fejezetben részletesebben vizsgáljuk azokat a kódokat, amelyek egyszerre prefix és szuffix kódok, azaz bifix kódok. A bifix kódok tehát olyan kódszavakból állnak, amelyek egyetlen valódi kezdőszelete és zárószelete sem kódszó. Az előző fejezetben a prefix [szuffix] kódok egy másik részosztályát, a szemafor prefix [szuffix] kódokat vizsgáltuk. Most a bifix kódok halmazának és a szemafor prefix [szuffix] kódok halmazának közös részével foglalkozunk. Ehhez először a maximális uniform kódok egy jellemzését adjuk.

19.1. Lemma. *Az X feletti C kód [szuffix kód] akkor és csak akkor maximális uniform kód, ha $X^+C \subseteq CX^+$ [$X^*C \subseteq CX^*$].*

Bizonyítás Az nyilvánvaló, hogy ha C maximális uniform kód, akkor $X^+C \subseteq CX^+$, s így $X^*C \subseteq CX^*$.

Megfordítva, tegyük fel, hogy az X feletti C kód teljesíti az $X^+C \subseteq CX^+$ feltételt. Legyen n a minimális szóhosszúság C-ben és

$$p = x_1x_2 \dots x_n \in C \quad (x_1, x_2, \dots, x_n \in X).$$

Akkor minden $x \in X$ esetén van olyan $q \in C$, hogy $xp = qx_n$. Így $q = xx_1x_2 \dots x_{n-1}$, azaz $Xx_1x_2 \dots x_{n-1} \subseteq C$. Ha $p \in Xx_1x_2 \dots x_{n-1}$, akkor minden $x \in X$ esetén van olyan $q \in C$, hogy $xp = qx_{n-1}$. Ebből kapjuk, hogy $X^2x_1x_2 \dots x_{n-2} \subseteq C$. Folytatva az eljárást, n lépés után adódik, hogy $X^n \subseteq C$. Minthogy X^n maximális kód, így $C = X^n$.

Legyen C olyan szuffix kód, amelyre $X^*C \subseteq CX^*$. A szuffix kód definíciója szerint $C \cap X^+C = \emptyset$. Amiből

$$C + X^+C = X^*C \subseteq CX^* = C + CX^+$$

miatt $X^+C \subseteq CX^+$. Az előzőekből következik, hogy C maximális uniform kód. □

A tételben az $X^+C \subseteq CX^+$ feltétel helyettesíthető a $CX^+ \subseteq X^+C$ feltétellel, s így az $X^+C = CX^+$ feltétellel is. Hasonlóan helyettesíthető prefix [bifix] kódokra a $CX^* \subseteq X^*C$ feltétel az $X^*C \subseteq CX^*$ [$X^*C = CX^*$] feltétellel.

19.2. Tétel. *Bifix kód akkor és csak akkor szemafor kód, ha maximális uniform kód.*

Bizonyítás A bizonyítást csak szemafor prefix kódokra végezzük el. Maximális uniform kód nyilvánvalóan szemafor prefix kód.

Megfordítva, legyen az X feletti C bifix kód szemafor prefix kód. Ez azt jelenti, hogy C maximális prefix kód. A 16.11, a 17.5 és a 18.7 Tételek szerint $X^*C \subseteq CX^*$. De C bifix kód, ezért $C \cap X^+C = \emptyset = C \cap CX^+$. Ebből kapjuk, hogy $X^+C \subseteq CX^+$. A 19.1 Lemmából következik, hogy C maximális uniform kód. □

A bifix kódok bármely láncának egyesítése is bifix kód, ezért, mint már említettük, a Zorn lemma szerint a 17.4 Lemma bifix kódokra is igaz, vagyis minden bifix kód részhalmaza egy maximális bifix kódnak. Természetesen a 17.6 Lemma szerint minden maximális kód ha bifix kód, akkor maximális bifix kód.

19.3. Lemma. *Minden maximális bifix kód maximális prefix kód vagy maximális szuffix kód.*

Bizonyítás C maximális bifix kód nem maximális prefix kód és nem maximális szuffix kód X felett. A 16.11 és a 17.5 Tétel szerint vannak olyan $u, v \in X^+$, amelyekre $uX^* \cap CX^* = \emptyset$ és $X^*v \cap X^*C = \emptyset$. Ebből következik, hogy $uv \notin C$. Minthogy C maximális bifix kód, ezért $C + \{uv\}$ nem bifix kód. Így vannak olyan $p_1, p_2, p_3, p_4 \in C$ és $q_1, q_2, q_3, q_4 \in X^+$ szavak, amelyekre az $uv = p_1q_1$, $uv = q_2p_2$, $uvq_3 = p_3$ és a $q_4uv = p_4$ összefüggések közül legalább egy teljesül. Ez minden esetben ellentmond u és v választásának. □

Ha egy kód maximális prefix kód és maximális szuffix kód, akkor nyilvánvalóan maximális bifix kód is. Ritka kódokra igaz ennek az állításnak a megfordítása is. A következő tételben további ekvivalens állításokat fogalmazunk meg. Ehhez először egy ritka nyelvekre vonatkozó lemmát bizonyítunk be.

19.4. Lemma. *Egy ritka nyelv akkor és csak akkor maximális prefix [szuffix] kód, ha jobbról [balról] teljes kód.*

Bizonyítás Ha az X feletti L ritka nyelv maximális prefix kód, akkor a 17.5 Tétel szerint jobbról teljes kód.

Megfordítva, legyen L jobbról teljes kód. Akkor $C = L - LX^+$ prefix kód. A 18.1 Lemma szerint $LX^* = CX^*$. A 16.11 Tétel alapján C jobbról teljes. Minthogy minden jobbról teljes kód teljes kód, ezért a 16.5 Tétel szerint C maximális kód. De $C \subseteq L$, s így $C = L$, vagyis L maximális prefix kód. A lemma szuffix kódra hasonlóan bizonyítható. □

19.5. Tétel. *Az X halmaz feletti L ritka nyelvre a következő állítások ekvivalensek:*
(i) L maximális bifix kód;
(ii) L maximális prefix és maximális szuffix kód;
(iii) L balról [jobbról] teljes prefix [szuffix] kód;
(iv) L balról és jobbról teljes kód.

Bizonyítás Először megmutatjuk, hogy $(i) \Longleftrightarrow (ii)$. Már a tétel előtt megbeszéltük, hogy $(ii) \Longrightarrow (i)$.

$(i) \Longrightarrow (ii)$: Ha L maximális prefix kód, akkor a 17.5 Tétel szerint L jobbról teljes kód. De minden jobbról teljes kód teljes kód, ezért a 16.5 Tétel miatt L maximális kód. Mivel L szuffix kód, így maximális szuffix kód. Hasonlóan kapjuk, hogy ha L maximális szuffix kód, akkor maximális prefix kód is. Tegyük fel ezért, hogy L nem maximális prefix kód és nem maximális szuffix kód. Akkor vannak olyan $p, q \in X^+ - L$, hogy $L + p$ prefix kód és $L + q$ szuffix kód. Ebből következik, hogy $L + pq$ bifix kód és $pq \notin L$. Ez ellentmond annak, hogy L maximális bifix kód.

A 17.5 Tétel szerint $(ii) \Longrightarrow (iii)$.

$(iii) \Longrightarrow (iv)$: Mivel L balról teljes prefix kód, ezért teljes kód is. A 16.5 Tételből következik, hogy L maximális kód. A 17.6 Lemma szerint L maximális prefix kód. A 17.5 Tételből kapjuk, hogy L jobbról teljes kód.

$(iv) \Longrightarrow (ii)$: pedig a 19.4 Lemmából következik. □

A következő példa mutatja, hogy egy maximális bifix kód nem szükségképpen maximális prefix és maximális szuffix kód.

19.6. Példa. *Tekintsük az $X = \{x, y\}$ ábécé feletti $L = \{pxy^{|p|}; p \in X^*\}$ nyelvet. Megmutatjuk, hogy $L - LX^+$ olyan maximális bifix kód, amely maximális prefix kód, de nem maximális szuffix kód.*

Nem nehéz belátni, hogy L jobbról sűrű, s így jobbról teljes szuffix kód, de nem prefix kód. Megmutatjuk, hogy L maximális szuffix kód. Legyen π az X ábécé uniform mértéke, azaz $\pi(x) = \pi(y) = \frac{1}{2}$. Akkor

$$\pi(L) = \sum_{n=0}^{\infty} \sum_{p \in X^n} \pi(pxy^{|p|}) = \sum_{n=0}^{\infty} 2^n \frac{1}{2^{2n+1}} = \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} = 1.$$

A 15.3 Tétel szerint L maximális kód, azaz maximális szuffix kód. A 18.3 Tétel szerint $L - LX^+$ maximális prefix kód. De $L - LX^+ \subseteq L$, ezért szuffix kód is. Ez azt jelenti, hogy maximális bifix kód. De $L - LX^+ \subset L$, ezért nem maximális szuffix kód.

A következő eredmény a maximális bifix kódok előzőektől különböző jellemzését adja a ritka kódok között.

19.7. Tétel. *Az X halmaz feletti C ritka kód akkor és csak akkor maximális bifix kód, ha minden $p \in X^*$ szóhoz van olyan n pozitív egész szám, amelyre $p^n \in C^*$.*

Bizonyítás Ha minden $p \in X^*$ szóhoz van olyan $n \in N_+$, amelyre $p^n \in C^*$, akkor C nyilvánvalóan balról és jobbról teljes kód. A 19.5 Tétel szerint C maximális bifix kód.

Megfordítva, tegyük fel, hogy a C ritka kód maximális bifix kód és $p \in X^*$. Mivel C ritka kód, ezért van olyan $u \in X^+$ szó, amely egyetlen C-beli szónak sem részszava. A 19.5 Tétel miatt C jobbról teljes kód, ezért minden i pozitív egész számhoz van olyan $v_i \in X^*$, hogy $p^i u v_i \in C^*$. Minthogy u nem részszava egyetlen C-beli szónak sem, így van u-nak olyan valódi s prefixe, hogy $p^i s \in C^*$. De u-nak véges sok valódi prefixe van, amiből kapjuk, hogy u-nak van olyan s valódi prefixe, amelyhez vannak olyan $k > l$ pozitív egész számok, hogy $p^k s, p^l s \in C^*$. A 13.9 Tételből kapjuk, hogy C^* az X^* szabad monoid unitér részmonoidja. Ebből $p^k s = p^{k-l} p^l s$ átalakítást felhasználva $p^{k-l} \in C^*$ következik. □

A 13.5. alfejezetben foglalkoztunk a bifix kódok egy nevezetes osztályával, az erős kódokkal . A bifix kódok egy további fontos osztályát, a csoportkódokat vizsgáltuk a 15.4. alfejezetben. Megemlítjük a bifix kódok további speciális osztályait az ún. *infix kódok*at és az *outfix kódok*at. Az X^+ szabad félcsoport L részhalmazát *infix kód*nak nevezzük, ha elemeinek egyetlen valódi részszavát sem tartalmazza, azaz tetszőleges $p, q, u \in X^*$ szavakra az $u, puq \in L$ feltételekből következik, hogy $p = q = e$. A definícióból könnyen adódik, hogy L valóban bifix kód. Az L részhalmazt *outfix kód*nak mondjuk, ha bármely $p, q, u \in X^*$ esetén a $pq, puq \in L$ feltételekből $u = e$ következik, azaz kódszóba nem lehet olyan nemüres szót beszúrni, hogy továbbra is kódszót kapjunk. Az uniform kódok nyilvánvalóan infix és outfix kódok.

A 17.4 Lemma infix [outfix] kódokra is teljesül, azaz minden infix [outfix] kód egy maximális infix [outfix] kód részhalmaza.

Feladatok

19.1. Ha az X feletti L_1 és L_2 nyelvek L_1L_2 szorzata bifix kód, akkor L_1 szuffix kód és L_2 prefix kód.
19.2. Egy $\emptyset \subset L \subseteq X^+$ nyelvre $X^+L \subseteq LX^+$ akkor és csak akkor, ha $X^n \subseteq L$, ahol n a minimális szóhosszúság L-ben.
19.3. Minden C infix kód ritka kód és egy ϑ_C-osztály, ahol ϑ_C a (7.5) feltétellel definiált szintaktikus kongruencia.
19.4. Legyenek $L_1 = \{p_1, p_2, \dots\}$, $L_2 = \{q_1, q_2, \dots\}$, $L_3 = \{r_1, r_2, \dots\}$ megszámlálható nyelvek az X ábécé felett és $|L_1| = |L_2| = |L_3|$. Ha L_1 prefix kód és L_3 szuffix kód, akkor az $L = \{p_1q_1r_1, p_2q_2r_2, \dots\}$ nyelv outfix kód X felett.
19.5. Mutassuk meg, hogy ha $\{X_1, X_2\}$ a legalább kételemű X ábécé egy osztályozása, akkor

$$M = \{p \in X^*; \sum_{a \in X_1} |p|_a = \sum_{b \in X_2} |p|_b\}$$

az X^* szabad monoid olyan unitér részmonoidja, amelynek bázisa csoportkód. Adjuk meg M bázisát. (Az így definiált kód a bináris Dyck kód egy általánosítása.)
19.6. Az X ábécé feletti C erős kódra a következő állítások ekvivalensek:
(1) C maximális prefix [szuffix] kód X felett;
(2) $\forall a \in X)$ $(aX^* \cap C \neq \emptyset [X^*a \cap C \neq \emptyset])$;
(3) C maximális kód X felett.
(Ha egy erős kód maximális kód, akkor *maximális erős kód*nak nevezzük.)
19.7. Tartalmazza az X ábécé feletti C kód az ábécé minden betűjét valamelyik szavában. A C kód akkor és csak akkor maximális erős kód, ha reflexív.

20. fejezet

Szinkron kódok

Legyen C kód X felett. Azt mondjuk, hogy az $s \in X^*$ szó *szinkronizálja a* $p \in X^*$ *szót*, ha $ps \in C^*$. Az $s \in X^*$ szót C *szinkronizáló szavá*nak nevezzük, ha X^* minden elemét szinkronizálja, azaz

$$X^*s \subseteq C^*. \tag{20.1}$$

A (20.1) definícóból következik, hogy $s \in C^*$. Pontosabban, ha $C \neq X$, akkor $s \in C^+$. Továbbá, ha $s \in C^*$ szinkronizáló szó, akkor bármely $t \in C^*$ esetén st is szinkronizáló szó. A C kódot *szinkron kód*nak nevezzük, ha van szinkronizáló szava, és *aszinkron*nak, ha nincs.

20.1. Lemma. *Minden X feletti C szinkron kód ritka maximális prefix kód.*

Bizonyítás Legyen C szinkron kód X felett és $s \in C^+$ egy szinkronizáló szava. Tegyük fel, hogy $p, pu \in C$ ($u \in X^*$). Mivel s szinkronizáló szó, ezért $us \in C^*$. Akkor $p(us) = (pu)s$. A 13.2 Lemma szerint $p = pu$ (és $us = s$), azaz $u = e$, vagyis C prefix kód.

A (20.1) definícióból következik, hogy C jobbról teljes. A 17.5 Tétel szerint C maximális prefix kód. Ha a (20.1) feltételt $sX^* \subseteq C^*$ alakban adjuk meg, akkor a szinkron kódok természetesen ritka maximális szuffix kódok.

Ha $s \in C^+$ a C szinkron kód egy szinkronizáló szava, akkor C-ben nincs olyan szó, amelynek s^2 részszava lenne. Ugyanis, ha valamely $u, v \in X^*$ szavakra $us^2v \in C$, akkor $us \in C^+$ miatt C nem prefix kód, ami lehetetlen. Ez azt jelenti, hogy C ritka kód. □

A 17.9 Tétel szerint minden szinkron kód maximális kód.

20.2. Példa. *Az 18.5 Példában láttuk, hogy $C = a^*b$ szemafor prefix kód és így maximális prefix kód az $X = \{a, b\}$ ábécé felett. C szinkron kód. Valóban $X^*b \subseteq C^*$, azaz b egy szinkronizáló szó.*

20.3. Példa. *Tetszőleges X ábécé feletti $C \neq X$ maximális bifix kód aszinkron kód. (A 19.5 Tétel szerint C maximális prefix kód.) Ha ugyanis $s \in C^*$ szinkronizáló szó, akkor minden $p \in X^*$ esetén $ps \in C^*$. De C^* az X^* szabad monoid jobb unitér részmonoidja, ezért $p \in C^*$, azaz $X^* = C^*$, vagyis $C = X$.*

A szinkron kód elnevezés a következőkből ered. Ha egy $p \in X^*$ szót fel akarunk bontani egy C prefix kód szavainak szorzatára, azaz dekódolni szeretnénk C szavaival, akkor meg kell győződnünk arról, hogy $p \in C^*$. (C^* X^* bal unitér részmonoidja.) Ha p-nek van egy $s \in C^*$ szinkronizáló részszava, azaz $p = usv$ $(u, v \in X^*)$, akkor $us \in C^*$ miatt elegendő megvizsgálni, hogy v dekódolható-e C-beli szavakkal? Vagyis $p \in C^*$ akkor és csak akkor, ha $v \in C^*$.

Szükségünk lesz a következőkben bevezetésre kerülő irányítható automatákra. Az erősen összefüggő automatákhoz hasonlóan ezek az automaták lényeges szerepet játszanak az algebrai automataelméletben.

Az $\mathbf{A} = (A, X, \delta)$ automatát *irányíthatónak* vagy *szinkronizálhatónak* nevezzük, ha van olyan $p \in X^*$ bemenő szó és $d \in A$ állapot, hogy minden $a \in A$ állapot esetén $ap = d$. Az ilyen p szót $\mathbf{A}$ irányító vagy szinkronizáló szavának, d-t $\mathbf{A}$ irányított vagy szinkronizált állapotának neveztük. Másképpen azt is mondtuk, hogy az $\mathbf{A}$ automata a p szóval irányítható a d állapothoz.

A 20.1 Lemma alapján a következő eredmény a 17.31 Lemma specializálása szinkron kódokra.

20.4. Lemma. *Az $\mathbf{A} = (A, X, \delta)$ erősen összefüggő irányítható automata bármely állapotának stabilizátora az X^* bemenő monoid bal unitér részmonoidja, amelynek bázisa szinkron kód.*

Bizonyítás Legyen $a \in A$ tetszőleges állapot. A 17.31 Lemma szerint $X_a = C^*$, ahol C maximális prefix kód. Nyilvánvaló, hogy erősen összefüggő irányítható automata minden állapota irányított állapot. Legyen $p \in X^+$ olyan irányító szó, amelyre $Ap = a$. Ebből következik, hogy $AX^*p = a$, azaz $X^*p \subseteq C^*$, vagyis a (20.1) definíció szerint C szinkron kód. □

A 16.11 és a 17.5 Tételekből nyilvánvalóan adódik, hogy egy X ábécé feletti C maximális prefix kód akkor és csak akkor szinkron kód, ha van olyan $p \in C^*$, amelyre $\overline{C}p \subseteq C^*$. A 20.1 Lemma szerint minden X feletti C szinkron kód ritka maximális prefix kód X felett. A következő tétel szerint ritka maximális prefix kódokra nem kell megkövetelni, hogy az előbbi szükséges és elegendő feltételben $\overline{C}$ minden eleméhez ugyanaz a p szó tartozzon.

20.5. Tétel. *Az X ábécé feletti C ritka maximális prefix kód akkor és csak akkor szinkron kód, ha minden $q \in \overline{C}$ szóhoz van olyan $s \in C^*$, amelyre $qs \in C^*$.*

Bizonyítás A feltétel nyilvánvalóan szükséges. Megmutatjuk, hogy elegendő is. Mivel C ritka kód, ezért van olyan $p \in X^+$, amely nem részszava egyetlen C-beli kódszónak sem. Legyen $K = \{p_1, p_2, \ldots, p_n\}$ a p szó azon zárószeleteinek halmaza, amelyek elemei $\overline{C}$-nek. A K halmaz nemüres, mivel $e \in K$. Definiáljuk a $q_1, q_2, \ldots, q_n$ C^*-beli szavak sorozatát a következő módon. Legyen $q_1 \in C^*$ olyan, hogy $p_1 q_1 \in C^*$. Tegyük fel, hogy a $q_1, q_2, \ldots, q_{i-1}$ sorozatot már definiáltuk. A 16.11 és a 17.5 Tételek szerint van olyan $t \in C^*$ és $r \in \overline{C}$, hogy

$$p_i q_1 \ldots q_{i-1} = tr.$$

Legyen $q_i \in C^*$ olyan, amelyre $rq_i \in C^*$. Ebből következik, hogy

$$p_i q_1 \ldots q_{i-1} q_i \in C^*, \quad i = 1, 2, \ldots, n. \tag{20.2}$$

Az $s = pq_1 q_2 \ldots q_n$ szó a C kód egy szinkronizáló szava. Valóban, legyen $u \in X^*$. Akkor $up = tr$ valamilyen $t \in C^*$ és $r \in \overline{C}$ szavakra. Az r szó a p zárószelete, mert különben p egy C-beli szó részszava lenne. Így $r \in K$, azaz $r = p_i$ valamilyen $p_i \in K$ szóra. Felhasználva (20.2)-t kapjuk, hogy

$$us = upq_1 q_2 \ldots q_n = tp_i q_1 q_2 \ldots q_n = t(p_i q_1 \ldots q_i) q_{i+1} \ldots q_n \in C^*.$$

Tehát $X^* s \subseteq C^*$. □

20.6. Lemma. *Ha C szinkron kód az X ábécé felett, akkor a C-beli szavak hosszának legnagyobb közös osztója* 1.

Bizonyítás Legyen a C-beli szavak hosszának legnagyobb közös osztója d. Mivel C szinkron kód, ezért van olyan $p \in C^+$, amelyre $X^* p \subseteq C^+$. Nyilvánvaló, hogy $|p|$ osztható d-vel. Bármely $x \in X$ esetén $xp \in C^+$, így $|xp| = 1 + |p|$ is osztható d-vel. Amiből következik, hogy $d = 1$. □

A 16.10 Következmény alapján az $x \in X$ betű X feletti C korlátos maximális kódra vonatkoztatott rendjének neveztük azt az egyetlen n pozitív egész számot, amelyre $x^n \in C$. Erősebb oszthatósági feltétel mellett véges maximális prefix kódokra igaz a 20.6 Lemma megfordítása.

20.7. Tétel. *Ha az X ábécé betűinek az X feletti C véges maximális prefix kódra vonatkoztatott rendjei relatív prímek, akkor C szinkron kód X felett.*

Bizonyítás Legyen az X ábécé feletti C maximális prefix kód véges. A 17.13 Lemma szerint X véges ábécé. Definiáljuk a $\overline{\mathbf{C}} = (\overline{C}, X, \delta)$ véges automata δ állapotfüggvényét a következőképpen:

$$\delta(q, x) = \begin{cases} qx, & \text{ha } qx \in \overline{C}, \\ e, & \text{ha } qx \in C. \end{cases} \tag{20.3}$$

(Ez az automata (17.9) szerint izomorf a (17.8)-ban megadott X^*/ρ_C erősen összefüggő automatával.) Jelölje az (1.4) és (1.5) kiterjesztések alapján minden $r \in \overline{C}$ és $p \in X^*$ szóra $r \cdot p$ a $\delta(r,p)$ állapotsorozat utolsó állapotát. Legyen továbbá

$$\overline{C} \cdot p = \{r \cdot p \ ; \ r \in \overline{C}\} \quad (p \in X^*).$$

Nyilvánvaló, hogy $\overline{C} \cdot p \subseteq \overline{C}$, valamint minden $p', p \in X^*$ párra

$$\overline{C} \cdot p'p \subseteq \overline{C} \cdot p, \quad |\overline{C} \cdot p'p| \leq |\overline{C} \cdot p'|. \tag{20.4}$$

Legyen $u \in X^*$ olyan, amelyre minden $p \in X^*$ esetén

$$|\overline{C} \cdot u| \leq |\overline{C} \cdot p|.$$

A 16.11 és a 17.5 Tételek szerint C jobbról teljes, ezért van olyan $v \in X^*$, amelyre $t = uv \in C^+$. (20.4) szerint $|\overline{C} \cdot t| = |\overline{C} \cdot u|$. Továbbá a (20.3) definíció miatt $e \in \overline{C} \cdot t$.

Megmutatjuk, hogy $\overline{C} \cdot t = e$. Ez a 16.11 és a 17.5 Tételek, valamint (20.3) szerint pontosan azt jelenti, hogy $X^*t \subseteq C^*$, azaz C szinkron kód.

Legyen az $x \in X$ betű C-re vonatkoztatott rendje n, továbbá

$$J = \{j \in N_+ \ ; \ (\overline{C} \cdot t)x^j \cap C \neq \emptyset\}$$

és

$$K = \{k \in \{0, \ldots, n-1\} \ ; \ x^k t \in C^*\}.$$

Először megmutatjuk, hogy

$$|J| = |\overline{C} \cdot t|. \tag{20.5}$$

Valóban, legyen $p \in \overline{C} \cdot t (\subseteq \overline{C})$. Minthogy C véges maximális kód, van olyan j pozitív egész szám, amelyre $px^j \in C$. Mivel C prefix kód, ezért egyetlen ilyen j van. Ilyen módon minden $p \in \overline{C} \cdot t$ szónak egyértelműen megfeleltettünk egy pozitív egész számot. Ez $\overline{C} \cdot t$ egy φ szürjektív leképezése J-re. Tegyük fel, hogy $p, p' \in \overline{C} \cdot \mathrm{t}, p \neq p'$ és $px^j, p'x^j \in C$. Ebből következik, hogy $|\overline{C} \cdot tx^j| < |\overline{C} \cdot t|$. Ez $|\overline{C} \cdot t|$ minimalitása miatt lehetetlen. Tehát φ bijektív, azaz $|J| = |\overline{C} \cdot t|$.

Legyen $m = max\{j + k \ ; \ j \in J, k \in K\}$. Nyilvánvalóan

$$m \leq maxJ + maxK \leq maxJ + n - 1.$$

Tekintsük a

$$T = \{m, m+1, \ldots, m+n-1\}$$

halmazt. Megmutatjuk, hogy $|T| = |J||K|$. Ehhez legyen $l \in T$ és minden $p \in \overline{C} \cdot t$ szóra legyen $\psi(p) = p \cdot x^l t$. Akkor

$$\psi(p) = (p \cdot x^l) \cdot t \in \overline{C} \cdot t.$$

Így $\psi(\overline{C}\cdot t)\subseteq \overline{C}\cdot t$, azaz $|\overline{C}\cdot t|$ minimalitása miatt $\psi(\overline{C}\cdot t)=\overline{C}\cdot t$, vagyis ψ a $\overline{C}\cdot t$ halmaz permutációja. De $e\in\overline{C}\cdot t$, ezért egyetlen olyan $p_l\in\overline{C}\cdot t$ létezik, amelyre $p_la^lt\in C^*$. Legyen j_l az az egyetlen pozitív egész szám, amelyre $p_lx^{j_l}\in C$. Akkor $j_l\in J$, ahonnan $j_l\le m\le l$. Legyen

$$l=j_l+an+k_l,\quad (a\in N,\ 0\le k_l<n). \tag{20.6}$$

Ez egyértelműen definiálja k_l-t, valamint

$$p_lx^lt=(p_lx^{j_l})(x^n)^a(x^{k_l}t).$$

Mivel $p_lx^{j_l}\in C$ és C^* bal unitér, ezért $(x^n)^a(x^{k_l}t)\in C^*$, s így $x^{k_l}t\in C^*$. Amiből következik, hogy $k_l\in K$. Az előbbi konstrukció definiál egy

$$\alpha: T\to J\times K$$

leképezést, amelyre $\alpha(l)=(j_l,k_l)$. Ez a leképezés injektív. Valóban, ha $l\ne l'$, akkor vagy $j_l\ne j_{l'}$, vagy következik (20.6)-ból és $l\not\equiv l'\pmod n$ miatt, hogy $k_l\ne k_{l'}$.

Most megmutatjuk, hogy α szürjektív. Legyen $(j,k)\in J\times K$ és legyen $a\in N$, amelyre

$$l=j+an+k\in T.$$

J definíciója szerint létezik (egyetlen) olyan $q\in\overline{C}\cdot t$, amelyre $qx^j\in C$. A K halmaz definíciója miatt kapjuk, hogy $qx^lt\in C$. Így $q=p_l$, $j=l_l$, $k=k_l$ jelölés mutatja, hogy α szürjektív, s ezért bijektív. Ebből következik, (20.5)-öt is felhasználva, hogy

$$n=|T|=|J||K|=|\overline{C}\cdot t||K|,$$

azaz $|\overline{C}\cdot t|$ osztója az $x\in X$ betű C-re vonatkoztatott rendjének. Mivel $x\in X$ tetszőleges betű volt és az X-beli betűk C-re vonatkoztatott rendjei a tétel feltétele szerint relatív prímek, ezért $|\overline{C}\cdot t|=1$, vagyis $\overline{C}\cdot t=e$. □

Végül bizonyítás nélkül megemlítjük a következő érdekes és mély eredményt. Az egyáltalán nem könnyű bizonyítás megtalálható Jean Berstel és Dominique Perrin már idézett [4] monográfiájában.

20.8. Tétel. *Bármely X feletti C szemafor prefix kódhoz van olyan X feletti D szinkron szemafor prefix kód és olyan n pozitív egész szám, hogy $C=D^n$.*

Feladatok

20.1. Ha C egy X feletti maximális prefix kód, akkor C^n $(2\le n)$ aszinkron kód.

20.2. Legyen C egy X feletti maximális prefix kód. Ha $2\le n$ és $C'\subseteq C^n$, akkor $(C^n-C')+C'C^n$ aszinkron kód.

21. fejezet

Hibajavító kódok

A gyakorlatban valamely nyelven megadott információ továbbítása a következőképpen valósulhat meg. Az információs csatornán továbbítható (legtöbbször fizikai) jelek halmazát (csatornaábécé) leképezzük bijektív módon egy X ábécére. Egy adott, Y ábécéjű nyelven megírt szöveget betűnként kódolunk valamely X feletti nem triviális C kód elemeivel. A kapott X betűiből álló szöveget betűnként a csatornaábécé jeleivé alakítva elküldjük a vevőnek. Az információ továbbításakor egyes jelek megváltozhatnak a továbbított jelsorozatokban, vagyis a vevő hibás információt kaphat. Bizonyos kódok felhasználhatók hibák felismerésére ill. kijavítására is. Ebben a fejezetben a *hibafelismerő* és a *hibajavító kódok* egy rövid bevezetésével foglalkozunk.

A fejezetben végig legalább kételemű ábécé feletti kódokat tekintünk. Legyen C egy ilyen kód. Tegyük fel, hogy az információs csatorna a $p \in C$ szóban bizonyos helyeken megváltoztatja a betűket. Ha az így kapott q szó eleme C-nek, akkor a vevő, hiába ismeri a C kódot, nem veszi észre a változást. Tegyük fel, hogy a vevő meg tudja mutatni, hogy $q \notin C$. A hiba kijavítására azonban nincs lehetősége akkor, ha van p-től különböző C-beli szó, amelyből bizonyos betűk megváltoztatásával megkapható q. Ez indokolja a következő definíciókat.

A C kódot h *hibát felismerő kód*nak nevezzük, ha a C-beli szavak legalább egy és legfeljebb h betűjének megváltoztatásával kapott szavak nem elemei C-nek. A h hibát felismerő C kódot h *hibát javító kód*nak hívjuk, ha bármely két különböző C-beli szó legalább egy és legfeljebb h betűjének megváltoztatásával kapott szavak is különbözőek.

Ha a C kódhoz van olyan h pozitív egész szám, amelyre C h hibát felismerő [javító] kód, akkor C-t egyszerűen *hibafelismerő* [*hibajavító*] *kód*nak mondjuk.

A következő lemma mutatja, hogy bármely nemüres kódból szerkeszthetünk tetszőleges számú hibát felismerő [javító] kódot.

21.1. Lemma. *Ha $C \neq \emptyset$ kód, akkor minden h pozitív egész számra*

$$C_h = \{p^h; p \in C\}$$

kód, C_{h+1} h hibát felismerő kód és C_{2h+1} h hibát javító kód.

Bizonyítás A 13.8 Következmény szerint C^h kód. Mivel $C_h \subseteq C^h$, ezért C_h is kód.

Legyen $p \in C$, $|p| = k$ és $q \in X^+$ a p^{h+1} szó legalább egy és legfeljebb h betűjének megváltoztatásával kapott szó. Tegyük fel, hogy p^{h+1} $i + jk$-adik betűje $x \in X$, a q szóé pedig $y \in X$ $(y \neq x)$, ahol $1 \leq i \leq k$ és $0 \leq j \leq h$. A q szó definíciója miatt $i + tk$-adik betűi, ahol $t = 0, 1, \ldots, h$, nem mind egyenlők y-nal, ezért $q \notin C^{h+1}$.

Legyen továbbá $q \in X^+$ a p^{2h+1} és r^{2h+1} $(p, r \in C)$ szavakból legalább egy és legfeljebb h betű megváltoztatásával kapott szó. Ebből $|p|^{2h+1} = |q| = |r|^{2h+1}$ és így $|p| = |r|$. Ha $p \neq r$, akkor van olyan $1 \leq i \leq |p|$, hogy p és r i-edik betűje nem egyenlő. Ez pedig azt jelenti, hogy q nem kapható meg p^{2h+1}-ből és r^{2h+1}-ből legfeljebb h betű megváltoztatásával. □

Az egyelemű kódok nyilvánvalóan hibafelismerő és egyúttal hibajavító kódok is. A legalább kételemű hibafelismerő [hibajavító] kódok vizsgálatához az X^* szabad monoidot metrikus térré tesszük.

Tekintsünk minden $x_1 \ldots x_k$ $(x_1, \ldots, x_k \in X)$ szót $(x_1, \ldots, x_k, x_{k+1}, \ldots)$ sorozatként, ahol $x_{k+j} = e$ $(j = 1, 2, \ldots)$. (Az e üres szót fogjuk fel az $(e, e, \ldots)$ sorozatként.) A $d : X^* \times X^* \to R$ függvényt *Hamming távolság*nak nevezzük, ha bármely $p = (x_1, \ldots x_k, x_{k+1}, \ldots)$ és $q = (y_1, \ldots, y_l, y_{l+1}, \ldots)$ X^*-beli szóra

$$d(p, q) = |\{j; x_j \neq y_j\}|. \tag{21.1}$$

Az X^* szabad monoid a Hamming távolsággal metrikus teret alkot, amelyet az X feletti *Hamming tér*nek is nevezünk. Speciálisan, bármely n nemnegatív egész számra X^n-et *n dimenziós Hamming tér*nek nevezzük.

Ezek szerint C akkor és csak akkor h hibát javító kód, ha bármely $q \in X^+$ szóhoz legfeljebb egy olyan $p \in C$ szó van, amelyre $d(q, p) \leq h$.

Legyen $C \neq \emptyset$ tetszőleges kód és

$$D_C = \{d(p, q) : p \neq q,\ p, q \in C\},$$

ahol d a Hamming távolság. A D_C halmaz legkisebb elemét a C kód *minimális távolság*ának nevezzük.

21.2. Lemma. *Minden legalább kételemű kód akkor és csak akkor h hibát felismerő [javító] kód, ha minimális távolsága legalább $h + 1$ [$2h + 1$].*

Bizonyítás A definícióból következik, hogy legalább kételemű kód akkor és csak akkor h hibát felismerő kód, ha minimális távolsága $h+1$.

Ha C nem h hibát javító kód, akkor vannak olyan $r \in X^+$ és $p, q \in C (p \neq q)$, amelyekre $d(p,r) \leq h$ és $d(q,r) \leq h$. Ebből

$$d(p,q) \leq d(p,r) + d(r,q) \leq 2h,$$

azaz C minimális távolsága legfeljebb $2h$.

Megfordítva, tegyük fel, hogy C minimális távolsága legfeljebb $2h$. Mivel C h hibát felismerő kód, ezért minimális távolsága legalább $h+1$. Így vannak olyan $p, q \in C$ kódszavak, amelyekre $p \neq q$ és $h+1 \leq d(p,q) \leq 2h$. Legyen l olyan egész szám, amelyre $0 < l, d(p,q) - l \leq h$. Ha $r \in X^+$ olyan szó, amelyet úgy kapunk a p szóból, hogy l számú, q megfelelő komponenseitől különböző komponenseit kicseréljük q-nak ezekre a komponenseire, akkor $p \neq r$, $q \neq r$, $d(p,r) \leq h$ és $d(q,r) \leq h$, azaz C nem h hibát javító kód. □

21.3. Lemma. *Ha X legalább kételemű halmaz és $\emptyset \subset X' \subset X$, akkor bármely X' feletti C korlátos kód átkódolható olyan X feletti uniform kóddá, amelynek minimális távolsága megegyezik C minimális távolságával.*

Bizonyítás Legyen n olyan pozitív egész szám, amelyre minden $p \in C$ esetén $|p| \leq n$. Legyen továbbá $y \in X - X'$ és

$$D = \{py^{n-|p|}; p \in C\}, \tag{21.2}$$

ahol y^0 jelentse az üres szót. A D nyelv uniform kód $X' + y$ felett. Mivel minden $p, q \in C$ párra

$$d(p,q) = d(py^{n-|p|}, qy^{n-|q|}),$$

ezért C és D minimális távolsága egyenlő. A $\varphi(p) = py^{n-|p|}$ $(p \in C)$ leképezés C átkódolása D-re. □

Természetesen az átkódoláshoz célszerű a legkisebb n-et, azaz a C-beli leghosszabb szó (szavak) hosszát választani.

Az 21.3 Lemma alapján a X feletti h hibát felismerő [javító] korlátos (nem uniform) kódok, amelyek szavaiban nem fordul elő X minden eleme, átkódolhatók X feletti h hibát felismerő [javító] uniform kódokká. Egy átkódolás a lemma bizonyításából leolvasható. Ha a korlátos kód szavaiban X minden eleme megtalálható, akkor tetszőleges $y \notin X$ jelet alkalmazva az eljárás egy $X+y$ feletti uniform kódot ad. Ez azt jelenti, hogy korlátos, speciálisan véges, hibafelismerő [javító] kódok mindig tekinthetők uniform kódoknak. Ezt a következő eredmények bizonyításakor meg is tesszük.

21.4. Tétel. *Ha C az X ábécé feletti legalább kételemű n hosszúságú h hibát felismerő kód, akkor*

$$|C| \leq |X|^{n-h}. \tag{21.3}$$

Bizonyítás Mivel C minimális távolsága legalább $h+1$, ezért ha például töröljük minden C-beli szó h hosszúságú prefixét, akkor X^{n-h} különböző elemeit kapjuk. Ami pontosan azt jelenti, hogy $|C| \leq |X|^{n-h}$. □

Az n hosszúságú C kódot (*n hosszúságú h hibát javító*) *perfekt kód*nak nevezzük, ha minden $r \in X^n$ szóhoz pontosan egy olyan $p \in C$ kódszó van, amelyre $p \neq r$ és $d(p,r) \leq h$. A kételemű perfekt kódokat *triviális perfekt kódok*nak is mondjuk.

A 21.2 Lemma szerint az n hosszúságú h hibát javító kódokban bármely két különböző kódszó legalább $2h+1$ számú ugyanannyiadik komponense különböző. Mivel $2h+1 \leq n$, ezért $n \geq 3$ és egy n hosszúságú kód legfeljebb $\frac{n-1}{2}$ hiba kijavítására alkalmas. A következő tétel megmutatja, hogy egy n hosszúságú h hibát javító kód legfeljebb hány szót tartalmaz.

21.5. Tétel. *Ha C az X ábécé feletti legalább kételemű n hosszúságú h hibát javító kód, akkor*

$$|C| \leq \frac{|X|^n}{\sum_{k=0}^{h} \binom{n}{k}(|X|-1)^k}, \quad 3 \leq 2h+1 \leq n, \tag{21.4}$$

ahol egyenlőség akkor és csak akkor teljesül, ha C perfekt.

Bizonyítás Bármely C-beli p kódszóhoz $\binom{n}{k}(|X|-1)^k$ számú X^n-beli szó van, amely k számú komponense p ugyanannyiadik komponenseitől különbözik. Az n hosszúságú h hibát javító kód definíciója szerint

$$|C|(\sum_{k=0}^{h} \binom{n}{k}(|X|-1)^k) \leq |X|^n,$$

s az egyenlőség pontosan akkor teljesül, ha C perfekt. □

Ha C n hosszúságú h hibát javító bináris kód, akkor (21.4) szerint

$$|C| \leq \frac{2^n}{\sum_{k=0}^{h} \binom{n}{k}}, \quad 3 \leq 2h+1 \leq n. \tag{21.5}$$

Ha C n hosszúságú egy hibát javító bináris kód, akkor $3 \leq n$ és $|C| \leq \frac{2^n}{n+1}$, továbbá C abban az esetben perfekt, ha $n+1$ osztója 2^n-nek.

Nem nehéz megmutatni, hogy minden h pozitív egész számhoz van h hibát javító triviális perfekt bináris kód. (Ha $X = \{0, 1\}$, akkor például $\{0^{2h+1}, 1^{2h+1}\}$ ilyen.)

Ha $n = 3$, akkor (21.5)-ből következik, hogy $|C| \leq 2$. Ha $X = \{0, 1\}$, akkor a triviális perfekt bináris kódok:

$$\{000, 111\}, \quad \{001, 110\}, \quad \{010, 101\}, \quad \{100, 011\}$$

bináris kódok.

Ha $n = 4$, akkor $|C| \leq \frac{16}{5}$, azaz nincs egy hibát javító perfekt bináris kód. Nincs háromelemű egy hibát javító bináris kód sem. Ha $X = \{0, 1\}$, akkor $\{0000, 1110\}$ egy triviális egy hibát javító bináris kód.

22. fejezet

Optimális kódok

Ebben a fejezetben azzal a gyakorlati kérdéssel foglalkozunk, hogy milyen módon lehet a közlemények küldésének költségét csökkenteni.

Az információs csatorna adott számú, legtöbbször két különböző jel továbbítására alkalmas ún. bináris csatorna. Ezek a csatornák a legegyszerűbbek, ezenkívül a különböző jelek számának növelésével a jelek továbbításakor fellépő hibák száma is növekedhet. Az üzenetek küldésének költsége nyilvánvalóan függ az üzenetek hosszától. A hírközlési rendszerek üzemeltetése meglehetősen költséges, arra kell tehát törekedni, hogy egy adott közlemény továbbítása a lehető legrövidebb ideig vegye igénybe a rendszert, vagyis olyan kódot kell választani, hogy a kódolt szöveg hossza, tehát a továbbítás költsége a lehető legkisebb legyen. Ehhez a közleményben gyakrabban előforduló betűkhöz kisebb hosszúságú kódszavakat kellene rendelni, mint a ritkábban előforduló betűkhöz. Például egy magyar nyelvű közleményben az $a, e, \ldots$ betűket általában rövidebb kódszavakkal kellene kódolni, mint például a $c, f, \ldots$ betűket. Adott közleményhez a legkisebb költségű kód megkeresése annyira megnehezítené az információközlés folyamatát, hogy ez az út nem járható. Olyan kódok meghatározását tűzzük ki célul, amelyek a közlemények rendszeres továbbítását a lehető legkisebb költséggel teszik lehetővé. Ennek a gyakorlati kérdésnek egzakt matematikai tárgyalásához bevezetjük az információ mértékét, s ennek segítségével definiáljuk azokat a kódokat, amelyeket a gyakorlatban legkisebb költséggel tudunk alkalmazni.

A természetes nyelveken közölt információk közül számunkra egyesek értékesebbek más információknál, vagyis az információknak valamilyen értéket tulajdonítunk. Természetesen ez az értékelés nagymértékben szubjektív és számításokra nem alkalmas. Mérhetnénk egy $p \in Y^*$ szóval megfogalmazott információt a p szó hosszával. Így azonban minden egyenlő hosszúságú közlemény információtartalma egyenlő lenne, ami csak akkor lenne elfogadható, ha a betűk előfordulási valószínűségei közel egyenlőek lennének.

Az információelméletben az információ mértékét az előfordulási valószínűségek bizonyos függvényeként értelmezik. Ehhez szorítkozzunk a fejezet további részében csak véges ábécékre. Legyen Y tetszőleges véges ábécé és π az Y egy Bernoulli mértéke (l. 14.1 fejzetet.). Ha $\pi(y) > 0$, akkor az $y \in Y$ *jel információtartalmán* értjük a $\log_2 \frac{1}{\pi(y)}$ pozitív valós számot. Ez összhangban van azzal a tapasztalattal, hogy a sűrűbben előforduló jelek kevesebb információt nyújtanak számunkra, mint a ritkábban előfordulók. Annak, hogy az információtartalomban 2 alapú logaritmus szerepel, kizárólag technikai okai vannak. Az információ továbbítása ugyanis elsősorban bináris csatornákon valósul meg.

Ha $Y = \{y_1, \dots, y_k\}$, akkor az egy jelre jutó átlagos információtartalmat, azaz az

$$E(\pi) = \sum_{j=1}^{k} \pi(y_j) \log_2 \frac{1}{\pi(y_j)} \tag{22.1}$$

számot az Y *ábécé* (π*-re vonatkoztatott*) *entrópiá*jának nevezzük. (Ha $\pi(y) = 0$, akkor legyen $\pi(y) \log_2 \frac{1}{\pi(y)} = 0$.)

Megmutatjuk, hogy $E(\pi) \le \log_2 k$. Felhasználva, hogy tetszőleges pozitív x-re $\ln x \le x - 1$,

$$E(\pi) - \log_2 k = \sum_{j=1}^{k} \pi(y_j) \log_2 \frac{1}{\pi(y_j)} - \sum_{j=1}^{k} \pi(y_j) \log_2 k =$$

$$= \sum_{j=1}^{k} \pi(y_j) \log_2 \frac{1}{k\pi(y_j)} = \frac{1}{\ln 2} \sum_{j=1}^{k} \pi(y_j) \ln \frac{1}{k\pi(y_j)} \le$$

$$\le \frac{1}{\ln 2} \sum_{j=1}^{k} \pi(y_j)(\frac{1}{k\pi(y_j)} - 1) = \frac{1}{\ln 2}(\sum_{j=1}^{k} \frac{1}{k} - \sum_{j=1}^{k} \pi(y_j)) = 0,$$

azaz $E(\pi) - \log_2 k \le 0$. Elemi függvénytani eszközökkel az is megmutatható, hogy $E(\pi) = \log_2 k$ akkor és csak akkor, ha $\pi(y_j) = \frac{1}{k}$ $(j = 1, \dots, k)$. Ez azt jelenti, hogy egy ábécé entrópiája akkor a legnagyobb, s ez az érték $\log_2 k$, ha π egyenletes eloszlás, azaz minden betűnek egyenlő az előfordulási valószínűsége.

Az entrópia elnevezés a statisztikus mechanikából ered, ahol ezt a mennyiséget fizikai rendszerek rendezettségének vagy másképpen megfogalmazva a rendszerek információtartalmának mérésére használják. Az entrópia egysége a *bit*. Egy bit entrópiája van például egy kételemű ábécének, ha mindkét elem előfordulási valószínűsége $\frac{1}{2}$. Ha egy k elemű ábécé minden elemének előfordulási valószínűsége egyenlő, azaz $\frac{1}{k}$, akkor entrópiája $\log_2 k$. Ha más alapú logaritmus szerepelne a definícióban, akkor az csak azt jelentené, hogy az információtartalom egysége más lenne. Például k alapú logaritmus esetén az

utóbbi ábécé entrópiája lenne egységnyi, s az előbbi kételemű ábécé entrópiája pedig $\log_k 2 = (log_2 k)^{-1}$.

Egyelemű ábécé feletti nyelven írt közleményeket a legkisebb költséggel egyetlen jellel lehet továbbítani. Az ilyen közleményeknek azonban nincs gyakorlati jelentőségük. Ezért feltehetjük, hogy a közlemények legalább kétféle betűt tartalmaznak.

Legyen π a legalább kételemű Y ábécé egy Bernoulli eloszlása és φ az Y ábécé kódolása egy X ábécé feletti C kóddal. A

$$K(\pi, \varphi) = \sum_{y \in Y} \pi(y)|\varphi(y)|, \tag{22.2}$$

számot a (*(π, φ)-re vonatkoztatott*) *jelköltség várható érték*ének nevezzük. Nyilvánvaló, hogy $K(\pi, \varphi) \geq 1$. Ha φ az Y kódolása a C kódra, akkor $K(\pi, \varphi)$ helyett a $K(\pi, C)$ jelölést is használjuk. A 17.3 Tétel szerint C-nek van szóhossztartó átkódolása egy C' prefix kódra. Nyilvánvaló, hogy $K(\pi, C) = K(\pi, C')$.

A φ kódolást *m elemű ábécé felett (π-re) optimális*nak, a C kódot pedig *m elemű ábécé felett (π-re) optimális kód*nak nevezzük, ha Y bármely m elemű ábécé feletti φ' kódolására $K(\pi, \varphi) \leq K(\pi, \varphi')$. A kételemű ábécé feletti optimális kódokat *optimális bináris kód*oknak hívjuk.

A gyakorlatban az optimális kódok költségcsökkentő szerepét a következő tapasztalatok igazolják. Ha elég sok vagy elég hosszú adott nyelvű, például magyar közleményben megvizsgáljuk az Y ábécé betűinek relatív gyakoriságát, azaz előfordulásuk számát elosztjuk a közlemény hosszával, azt tapasztaljuk, hogy a betűk relatív gyakorisága stabilitást mutat, azaz valamilyen 1-nél kisebb nemnegatív valós szám körül ingadozik. Ez a szám az adott betű *előfordulási valószínűség*e az adott nyelvben. Jelöljük az $y \in Y$ betű előfordulási valószínűségét $\pi(y)$-nal. A nagy számok törvénye szerint ez a valószínűség tetszőleges pontossággal megközelíthető. A betűk előfordulásait a közleményekben egymástól függetlennek vehetjük. Az így kapott $\pi(y)$ $(y \in Y)$ valószínűségeloszlás az Y ábécé egy Bernoulli eloszlásának tekinthető. Már említettük, hogy elgondolhatjuk úgy, hogy a jelforrás az ábécé betűit (jeleit) véletlenszerűen, egymás után a π valószínűségeloszlás szerint egymástól függetlenül bocsátja ki, azaz egy n hosszúságú közlemény a jelforrás által véletlenszerűen kibocsátott n hosszúságú jelsorozat. Ha az n hosszúságú közleményben az $y \in Y$ betű gyakorisága $r(y)$ és φ az Y halmaz egy kódolása a C kóddal, akkor a kódszavak átlagos hossza, vagyis az egy betűre jutó átlagos jelköltség

$$\sum_{y \in Y} \frac{r(y)}{n} |\varphi(y)|. \tag{22.3}$$

Elég hosszú vagy elég sok közlemény esetén (22.3) jól megközelíti (22.2)-t. Ez indokolja azt, hogy (22.2)-t a jelköltség várható értékének nevezzük.

22.1. Lemma. *Ha $Y = \{y_1, y_2, \ldots, y_k\}$ $(k \geq 2)$ és π az Y ábécé Bernoulli eloszlása, akkor Y bármely φ kódolása esetén*

$$\frac{E(\pi)}{\log_2 k} \leq K(\pi, \varphi). \tag{22.4}$$

Bizonyítás Ha valamely y_j-re $\pi(y_j) = 0$, akkor az $E(\pi)$ és a $K(\pi, \varphi)$ összegekben a $\pi(y_j)$ tényezőt tartalmazó tag 0. Ezért az általánosság megszorítása nélkül feltehetjük, hogy minden $y_j \in Y$ elemre $\pi(y_j) > 0$. Akkor

$$\frac{E(\pi)}{\log_2 k} - K(\pi, \varphi) = \sum_{j=1}^{k} \pi(y_j) \log_k \frac{k^{-|\varphi(y_j)|}}{\pi(y_j)}.$$

Mivel tetszőleges pozitív x-re $\ln x \leq x - 1$, ezért

$$\frac{E(\pi)}{\log_2 k} - K(\pi, \varphi) = \frac{1}{\ln k} \sum_{j=1}^{k} \pi(y_j) \ln \frac{k^{-|\varphi(y_j)|}}{\pi(y_j)} \leq \frac{1}{\ln k} \sum_{j=1}^{k} \pi(y_j)(\frac{k^{-|\varphi(y_j)|}}{\pi(y_j)} - 1) =$$

$$\frac{1}{\ln k}(\sum_{j=1}^{k} k^{-|\varphi(y_j)|} - \sum_{j=1}^{k} \pi(y_j)) = \frac{1}{\ln k}(\sum_{j=1}^{k} k^{-|\varphi(y_j)|} - 1).$$

A Szilárd–Kraft–McMillan egyenlőtlenségből kapjuk, hogy $\frac{E(\pi)}{\log_2 k} - K(\pi, \varphi) \leq 0$. □

22.2. Lemma. *Ha $Y = \{y_1, y_2, \ldots, y_k\}$ $(k \geq 2)$ és π az Y pozitív Bernoulli eloszlása, akkor bármely $2 \leq m$ esetén van Y-nak olyan m elemű ábécé feletti φ prefix kódolása, amelyre*

$$K(\pi, \varphi) \leq \frac{E(\pi)}{\log_2 m} + 1. \tag{22.5}$$

Bizonyítás Legyen l_j $(j = 1, \ldots, k)$ az a legkisebb egész szám, amely nem kisebb mint $\log_m \frac{1}{\pi(y_j)}$. Nyilvánvaló, hogy $l_j > 0$ $(j = 1, \ldots, k)$ és

$$\sum_{j=1}^{k} m^{-l_j} \leq \sum_{j=1}^{k} m^{-\log_m \frac{1}{\pi(y_j)}} = \sum_{j=1}^{k} m^{\log_m \pi(y_j)} = \sum_{j=1}^{k} \pi(y_j) = 1.$$

A 17.1 Lemma szerint van olyan m elemű ábécé feletti $C = \{p_1, \ldots, p_k\}$ prefix kód, amelyre $|p_j| = l_j$ $(j = 1, \ldots, k)$. Legyen φ az Y ábécének az a kódolása, amelyre $\varphi(y_j) = p_j$ $(j = 1, \ldots, k)$ teljesül. Akkor

$$K(\pi, \varphi) = \sum_{j=1}^{k} \pi(y_j) l_j \leq \sum_{j=1}^{k} \pi(y_j)(\log_m \frac{1}{\pi(y_j)} + 1) = \frac{E(\pi)}{\log_2 m} + 1.$$

□

Ha $k \leq m$, akkor Y triviális kódolása egy m elemű ábécébe az Y-nak prefix kódolása. Ezért gyakorlati szempontból a 22.2 Lemma állítása $2 \leq m < k$ esetekben érdekes, különösen az $m = 2$ eset, azaz bináris prefix kódra való kódolás.

22.3. Tétel. *Ha $Y = \{y_1, y_2, \ldots, y_k\}$ $(k \geq 2)$ és π az Y pozitív Bernoulli eloszlása, akkor van Y-nak bármely $2 \leq m$ elemű ábécé feletti π-re optimális prefix kódolása. Ha $k > 2$, akkor Y-nak $k-1$ elemű ábécé feletti π-re optimális prefix kódolása Y-nak π-re optimális prefix kódolása.*

Bizonyítás A 22.1 Lemma szerint Y minden kódolásának költsége nagyobb vagy egyenlő, mint az $E(\pi)\log_2 k^{-1}$. Legyen φ az Y ábécének olyan $2 \leq m$ elemű ábécé feletti kódolása, amelyre $K(\pi, \varphi) \leq \frac{E(\pi)}{\log_2 m} + 1$. A 22.2 Lemma szerint ilyen létezik. Akkor

$$1 \leq \varphi(y_j) \leq \frac{E(\pi) + 1}{\pi(y_j)} \quad (j = 1, \ldots, k).$$

Ha ugyanis volna olyan y_j, amelyre $\varphi(y_j) > \frac{\frac{E(\pi)}{\log_2 m}+1}{\pi(y_j)}$, akkor

$$K(\pi, \varphi) \geq \pi(y_j)\varphi(y_j) > \frac{E(\pi)}{\log_2 m} + 1$$

teljesülne, ami a feltevés miatt lehetetlen. Véges sok olyan, pozitív egész számokból álló $l_1, \ldots, l_k$ sorozat van, amely eleget tesz az

$$1 \leq l_j \leq \frac{\frac{E(\pi)}{\log_2 m} + 1}{\pi(y_j)} \ (j = 1, \ldots, k)$$

egyenlőtlenségrendszernek. Ezért Y-nak véges sok olyan φ kódolása van m elemű ábécé felett, amely eleget tesz a $K(\pi, \varphi) \leq \frac{E(\pi)}{\log_2 m}+1$ feltételnek. Így ezek között Y-nak van m elemű ábécé feletti (π-re) optimális kódolása. Legyen φ egy ilyen optimális kódolás. Vezessük be a $\varphi(y_j) = l_j$ $(j = 1, \ldots, k)$ jelöléseket. A 17.3 Tétel szerint van olyan m elemű ábécé feletti $C = \{p_1, \ldots, p_k\}$ prefix kód, amelyre $|p_j| = l_j$ $(j = 1, \ldots, k)$. A $\varphi'(y_j) = p_j$ $(j = 1, \ldots, k)$ leképezés Y m elemű ábécé feletti (π-re) optimális kódolása a C prefix kódra.

Ha $k > 2$, akkor bármely $2 \leq m < k$ esetén egy m elemű ábécé feletti (π-re) optimális kódolás Y nem triviális kódolása. Ezek között, a végesség miatt, van olyan kód, amely jelköltségének várható értéke a legkisebb. A 17.3 Tétel szerint ennek is van szóhossztartó prefix átkódolása. Másrészről, ha Y-t egy j elemű A ábécé felett, ill. egy $k-1$ elemű B ábécé felett kódoljuk és $2 \leq j < k-1$, akkor feltehető, hogy $A \subset B$. Ha C az Y-nak egy B feletti

optimális kódja, akkor van olyan $a \in A$, hogy $a \notin B$, s így $a \notin C$. Mivel $j < k$, ezért C nem triviális kód. Ha kicseréljük a-val C valamelyik legalább kettő hosszúságú szavát, akkor Y-nak olyan A feletti kódolását kapjuk, amely jelköltségének várható értéke kisebb, mint C jelköltségének várható értéke. Ez éppen azt jelenti, hogy Y-nak $k-1$ elemű ábécé feletti π-re optimális prefix kódolása Y-nak π-re optimális prefix kódolása. □

A $k \leq m$ esetben a 22.3 Tétel állítása érdektelen gyakorlati szempontból, hiszen ekkor Y-nak tetszőleges m elemű ábécébe való φ triviális kódolása Y optimális prefix kódolása, mivel $K(\pi, \varphi) = 1$.

22.4. Lemma. *Minden optimális kód maximális vagy korlátos.*

Bizonyítás Legyen Y tetszőleges ábécé és π az Y egy Bernoulli eloszlása. Legyen φ az Y-nak az X ábécé feletti C kódra (π-re) optimális kódolása. Tegyük fel, hogy C nem maximális kód. Akkor van van olyan $p \in X^+$, hogy $C + p$ is kód X felett. Legyen q a C kód olyan eleme, amelyre $|p| < |q|$. Mivel egy kód minden részhalmaza is kód, ezért $D = (C + p) - q$ is kód X felett. Tekintsük Y-nak azt a D-re való φ' kódolását, amelyre $\varphi'(y) = \varphi(y)$, ha $\varphi(y) \neq q$, és $\varphi'(y) = p$, ha $\varphi(y) = q$. Nyilvánvaló, hogy $K(\pi, \varphi') < K(\pi, \varphi)$. Ez pedig ellentmondásban van azzal, hogy C (π-re) optimális kód. Ez azt jelenti, hogy bármely $q \in C$ elemre $|q| \leq |p|$, azaz C korlátos kód. □

A 17.3 Tétel szerint minden (optimális) kód átkódolható szóhossztartó (optimális) prefix kóddá egy adott ábécé felett, ezért a továbbiakban az egyszerűbb szerkezetű optimális prefix kódokra, s ezek közül is a gyakorlati szempontból legfontosabb optimális bináris prefix kódok vizsgálatára szorítkozunk. Az optimális bináris prefix kódokra megadunk néhány eredményt, amelyekből egyszerű eljárás kapható optimális bináris prefix kódok szerkesztésére.

22.5. Tétel. *Minden optimális bináris prefix kód maximális.*

Bizonyítás Legyen Y tetszőleges (legalább kételemű) ábécé, π az Y egy Bernoulli eloszlása, φ pedig Y optimális kódolása az $\{a, b\}$ ábécé feletti C prefix kódra. Tegyük fel, hogy C nem maximális prefix kód. A 17.6 Lemma szerint C nem maximális kód. A 22.4 Lemmát felhasználva, kapjuk, hogy C korlátos. Jelölje a C-beli kódszavak hosszának maximumát n. Mivel Y legalább kételemű és C nem maximális kód, ezért $C \neq \{a, b\}$, s így $n > 1$. A 16.11 és a 17.5 Tételekből következik, hogy létezik olyan legalább n hosszúságú $p \in \{a, b\}^+$ szó, amelynek nincs C-beli kezdőszelete. Ezért, ha r a p n hosszúságú kezdőszelete, akkor r-nek egyetlen kezdőszelete sem eleme C-nek. Tegyük fel például, hogy $r = qa$ ($q \in \{a, b\}^{n-1}$). Akkor q kezdőszeletei sem elemei C-nek. Ha $qb \in C$,

akkor $D = (C - qb) + q$ is prefix kód $\{a, b\}$ felett. Legyen $\varphi'(y) = \varphi(y)$, ha $\varphi(y) \neq qb$ és $\varphi'(y) = q$, ha $\varphi(y) = qb$. A φ' leképezés Y olyan kódolása D-re, amelyre $K(\pi, \varphi') < K(\pi, \varphi)$. Ez azonban lehetetlen, ezért $qb \notin C$. Akkor viszont q egyetlen C-beli szónak sem kezdőszelete. Ha kicseréljük q-val C egy n hosszúságú szavát, akkor ugyanúgy, mint az előbb, olyan prefix kódot kapunk, amely jelköltségének várható értéke kisebb $K(\pi, \varphi)$-nél, ami szintén ellentmond a feltételnek. Így C maximális prefix kód. □

Legyen $Y = \{y_j : j \in I\}$ megszámlálható halmaz és π az Y Bernoulli eloszlása. Nyilvánvalóan Y átindexelhető úgy, hogy a $\pi(y_j)$ $(j \in I)$ sorozat monoton csökkenő legyen. Ez az átindexezés a jelköltség várható értékét nem változtatja meg. Az alábbi két tételben az Y ábécét így adjuk meg.

22.6. Tétel. *Ha az* $Y = \{y_1, y_2, \ldots, y_k\}$ $(2 \leq k)$ *ábécé* π *pozitív Bernoulli eloszlására*

$$\pi(y_1) \geq \pi(y_2) \geq \pi(y_{k-1} \geq \pi(y_k),$$

akkor van olyan φ *optimális prefix kódolása az* $\{a, b\}$ *ábécé felett, amelyre*

$$|\varphi(y_1)| \leq |\varphi(y_2)| \leq \cdots \leq |\varphi(y_{k-1})| = |\varphi(y_k)|,$$

és $\varphi(y_{k-1}) = qa, \varphi(y_k) = qb$ $(q \in \{a, b\}^*)$.

Bizonyítás Legyen φ_1 az Y egy optimális prefix kódolása az $\{a, b\}$ ábécé felett. A 22.3 Tétel szerint ilyen létezik. Vezessük be a $|\varphi_1(y_j)| = l_j$ $(j = 1, \ldots, k)$ jelöléseket.

Tegyük fel, hogy $l_i > l_j$ valamely $i < j$ párra. Ekkor a tétel előtti megállapodás szerint $\pi(y_i) \geq \pi(y_j)$. Ha $\pi(y_i) > \pi(y_j)$, akkor cseréljük fel a $\varphi_1(y_i)$ és $\varphi_1(y_j)$ kódszavakat, vagyis y_i-hez rendeljük $\varphi_1(y_j)$-t, y_j-hez pedig $\varphi_1(y_i)$-t. Így Y egy prefix kódolásához jutunk $\{a, b\}$ felett. Mivel

$$\pi(y_i)(l_i - l_j) > \pi(y_j)(l_i - l_j),$$

vagyis

$$\pi(y_i)l_i + \pi(y_j)l_j > \pi(y_i)l_j + \pi(y_j)l_i.$$

Ebből viszont az adódik, hogy az így kapott prefix kódolás jelköltségének várható értéke kisebb φ_1 jelköltségének várható értékénél. Ez azonban lehetetlen, mert φ_1 optimális prefix kódolás $\{a, b\}$ felett.

Ezért $\pi(y_i) = \pi(y_j)$. Ha most is felcseréljük a $\varphi_1(y_i)$ és $\varphi_1(y_j)$ kódszavakat, vagyis y_i-hez rendeljük $\varphi_1(y_j)$-t, y_j-hez pedig $\varphi_1(y_i)$-t, akkor Y-nak ismét egy optimális prefix kódolását kapjuk $\{a, b\}$ felett, de eggyel csökken azoknak a $i < j$ pároknak a száma, amelyekre $l_i > l_j$. Az ilyen esetek lépésenkénti

kiküszöbölésével Y olyan φ_2 optimális prefix kódolását kapjuk $\{a,b\}$ felett, amelyre

$$l_1 \le l_2 \le \cdots \le l_{k-1} \le l_k.$$

Tegyük fel, hogy $l_{k-1} < l_k$. Jelölje r a $\varphi_2(y_k)$ kódszó l_{k-1} hosszúságú kezdőszeletét. Mivel r hossza l_{k-1}, ezért r nem lehet kezdőszelete a $\varphi_2(y_j)$ $(j = 1,\dots,k-1)$ kódszavak egyikének sem. Ha $\varphi_2(y_k)$-t kicserélnénk r-rel, akkor Y olyan prefix kódolását kapnánk, amely jelköltségének várható értéke kisebb φ_2 jelköltségének várható értékénél. Ez lehetetlen, ezért $l_{k-1} = l_k$.

Legyen végül

$$\varphi_2(y_{k-1}) = qa, \quad \varphi_2(y_k) = q'x \quad (x \in \{a,b\}, q, q' \in \{a,b\}^*).$$

Tegyük fel első esetként, hogy vannak l_k hosszúságú qa és qb $(q \in \{a,b\}^*)$ kódszavak. Akkor, ha szükséges, felcseréljük $\varphi_2(y_{k-1})$-et qa-val és $\varphi(y_k)$-t qb-vel. Ilyen módon Y olyan φ optimális prefix kódolásához jutunk $\{a,b\}$ felett, amely eleget tesz a tétel állításainak.

Tegyük fel második esetként, hogy nincsenek l_k hosszúságú

$$qa, \quad qb \quad (q \in \{a,b\}^*)$$

alakú kódszavak, de vannak l_k hosszúságú

$$qx, \quad q'x \quad (x \in \{a,b\}, q \ne q', q, q' \in \{a,b\}^*)$$

alakúak. Legyen például $x = a$. Ekkor q a qa-n kívül egyetlen kódszónak sem kezdőszelete. Mivel qa kódszó, ezért egy kódszó sem kezdőszelete q-nak, így $q'a$-t qb-vel kicserélve, Y-nak az első esetben megvizsgált típusú optimális prefix kódolásához jutunk.

Tegyük fel utolsó esetként, hogy bármely két l_k hosszúságú kódszó

$$qa, q'b \quad (q \ne q', q, q' \in \{a,b\}^*)$$

alakú. A $q'b$ kódszót kicserélve qb-vel, ismét visszavezetjük a kérdést az első esetre. □

22.7. Tétel. *Legyen megadva az $Y = \{y_1, y_2, \dots, y_k\}$ $(2 \le k)$ ábécé π pozitív Bernoulli eloszlása úgy, hogy*

$$\pi(y_1) \ge \pi(y_2) \ge \cdots \ge \pi(y_{k-1}) \ge \pi(y_k).$$

Legyen továbbá $C = \{p_1, p_2, \dots, p_k\}$ az Y egy optimális prefix kódja $\{a,b\}$ felett. Tegyük fel, hogy $\pi(y_j) = t_1 + t_2$ $(t_1 \ge t_2 > 0)$ és

$$\pi(y_1) \ge \pi(y_2) \ge \cdots \ge \pi(y_{j-1}) \ge \pi(y_{j+1}) \ge \cdots \ge \pi(y_k) \ge t_1 \ge t_2$$

az $Y' = \{y_1, y_2, \ldots, y_k, y_{k+1}\}$ *ábécé egy* π' *Bernoulli eloszlása. Akkor*

$$C' = \{p_1, p_2, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k, p_j a, p_j b\}$$

az Y' *ábécé egy optimális prefix kódja* $\{a, b\}$ *felett és*

$$K(\pi', C') = K(\pi, C) + \pi(y_j).$$

Bizonyítás Mivel C prefix kód, ezért C' is prefix kód. Továbbá

$$K(\pi, C') = \pi(y_1)|p_1| + \cdots + \pi(y_{j-1})|p_{j-1}| +$$

$$+\pi(y_{j+1})|p_{j+1}| + \cdots + \pi(y_k)|p_k| + t_1|p_j a| + t_2)|p_j b| =$$

$$= \pi(y_1)|p_1| + \cdots + \pi(y_{j-1})|p_{j-1}| +$$

$$+\pi(y_{j+1})|p_{j+1}| + \cdots + \pi(y_k)|p_k| + (t_1 + t_2)(|p_j| + 1) =$$

$$= \pi(y_1)|p_1| + \cdots + \pi(y_j)|p_j| + \cdots + \pi(y_k)|p_k| + \pi(y_j) = K(\pi, C) + \pi(y_j).$$

Az előző tételből következik, hogy Y'-nek van π'-re optimális kódolása az $\{a, b\}$ ábécé felett olyan $D' = \{q_1, q_2, \ldots, q_{k-1}, qa, qb\}$ prefix kódra, amelyre

$$|q_1| \leq |q_2| \leq \cdots \leq |q_{k-1}| \leq |qa| = |qb|.$$

Nem nehéz belátni, hogy $D = \{q_1, \ldots, q_{j-1}, q, q_{j+1}, \ldots, q_{k-1}\}$ is prefix kód $\{a, b\}$ felett, s nyilvánvalóan van Y-nak egy kódolása D-re. Ugyanúgy, mint az előbb, belátható, hogy $K(\pi', D') = K(\pi, D) + \pi(y_j)$. Mivel C az Y optimális prefix kódja $\{a, b\}$ felett, ezért $K(\pi, C) \leq K(\pi, D)$, s így

$$K(\pi', D') = K(\pi, D) + \pi(y_j) \leq K(\pi, C) + \pi(y_j) = K(\pi', C').$$

De D' az Y' optimális prefix kódja $\{a, b\}$ felett, ezért $K(\pi', D') \leq K(\pi', C')$. Ebből következik, hogy $K(\pi', D') = K(\pi', C')$, azaz C' is optimális prefix kódja Y'-nek $\{a, b\}$ felett. Továbbá $K(\pi', C') = K(\pi, C) + \pi(y_j)$. □

A 22.7 Tétel lehetőséget nyújt arra, hogy $k + 1$ betűs ábécé bináris optimális prefix kódjának keresését visszavezessük $(2 \leq)k$ elemű ábécé bináris optimális prefix kódjának keresésére. Legtöbbször bináris ábécéként a $\{0, 1\}$ halmazt használjuk. Most leírjuk ezt az eljárást. Ezt az eljárást *Huffmann algoritmus*nak, az eljárással kapott kódokat *Huffmann kód*oknak nevezzük.

Legyenek az $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$ $(k \geq 2)$ ábécé betűinek előfordulási valószínűségei rendre

$$t_1 \geq t_2 \geq \cdots \geq t_k \geq t_{k+1}.$$

Tekintsünk ekkor egy $B = \{b_1, b_2, \ldots, b_k\}$ ábécét, amely betűinek előfordulási valószínűségei legyenek rendre

$$t_1 \geq t_2 \geq \cdots \geq t_{j-1} \geq t_k + t_{k+1} \geq t_j \geq \cdots \geq t_{k-1}.$$

Ha

$$\{p_1, p_2, \ldots, p_k\}$$

a B ábécé bináris optimális prefix kódja, akkor

$$\{p_1, p_2, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k, p_j 0, p_j 1\}$$

az A ábécé bináris optimális prefix kódja.

Az ábécé betűinek számát fokozatosan csökkentve, végül eljutunk ahhoz a feladathoz, amelynél a kétbetűs $\{0, 1\}$ ábécéhez kell bináris optimális prefix kódot megadnunk. Ilyen azonban csak egy van, mégpedig a $\{0, 1\}$ triviális kód.

22.8. Példa. *Legyen egy* 9 *elemű ábécé betűinek előfordulási valószínűségeinek csökkenő sorozata*

$$0,20; 0,17; 0,15; 0,15; 0,10; 0,08; 0,05; 0,05; 0,05.$$

A Huffmann algoritmussal megadunk az ábécéhez bináris optimális prefix kódot.

Legyen a 9 elemű ábécé

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

és a k betű előfordulási valószínűsége a megadott sorozat k-adik eleme. Adjuk össze az utolsó két valószínűséget, s adjuk meg ismét a kapott valószínűségek

$$0,20; 0,17; 0,15; 0,15; 0,10; 0,10; 0,08; 0,05$$

csökkenő sorozatát. Legyen a sorozatnak megfelelő 8 elemű ábécé

$$\{1, 2, 3, 4, 5, 89, 6, 7\}.$$

Ezt folytassuk addig, amíg kételemű ábécéig jutunk. A kapott ábécéket célszerűség miatt fordított sorrendben adtuk meg:

$$\{(23)(4(67)), 1(5(89))\},\ \{1(5(89)), 23, 4(67)\},\ \{23, 4(67), 1, 5(89)\},$$

$$\{4(67), 1, 5(89), 2, 3\},\ \{1, 5(89), 2, 3, 4, 67\},\ \{1, 2, 3, 4, 67, 5, 89\},$$

$$\{1, 2, 3, 4, 5, 89, 6, 7\},\ \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

A kételemű ábécé egyetlen bináris optimális prefix kódja $\{0, 1\}$. A 22.7 Tételt használva a $\{0, 1\}$ kódból kiindulva meg tudunk adni a kapott ábécékhez bináris optimális prefix kódokat:

$$\{0, 1\}, \{1, 00, 01\}, \{00, 01, 10, 11\}, \ \{01, 10, 11, 000, 001\},$$

$$\{10, 11, 000, 001, 010, 011\}, \ \{10, 000, 001, 010, 011, 110, 111\},$$

$$\{10, 000, 001, 010, 110, 111, 0110, 0111\},$$

$$\{10, 000, 001, 010, 110, 0110, 0111, 1110, 1111\}.$$

Ha az eljárásban bárhol a 0-t és 1-et fordított sorrendben írjuk a szavak végéhez, akkor ugyanilyen hosszúságú szavakat kapunk, de nem biztos, hogy ugyanezeket a kódszavakat.

MEGOLDÁSOK

1.1. Teljes indukcióval megmutatható, hogy minden n nemnegatív egész számra

$$M = K^{n+1}M + (K^n + \cdots + K + e)L,$$

amiből $K^*L \subseteq M$. Megfordítva, ha $p \in M$, akkor

$$p \in K^{|p|+1}M + (K^{|p|} + \cdots + K + e)L(= M)$$

miatt $p \in K^*L$, azaz $M \subseteq K^*L$.
1.2. Az előző feladat megoldása alapján.
2.1. Az U ábécé feletti L véges nyelv generálható azzal a $G = (V_N, V_T, S, H)$ 3 típusú grammatikával, amelyre $V_N = \{S\}, V_T = U$ és $H = \{S \longrightarrow p; p \in L\}$.
2.2. Legyen $G = (V_N, V_T, S, H)$ egy grammatika, amelyre $V_N = \{S\}, V_T = U$. Ha $H = \{S \longrightarrow Su; u \in U\}$, akkor G az üres nyelvet, ha pedig $H\{S \longrightarrow e, S \longrightarrow Su, S \longrightarrow u; u \in U\}$, akkor az univerzális nyelvet generálja.
2.3. $(\{S\}, U, S, \{S \longrightarrow e, S \longrightarrow xSy\})$.
2.4. $L = L(G)$, ahol $V_N = \{S, X\}$, $V_T = \{x, y\}$ és a $G = (V_N, V_T, S, H)$ lineáris grammatika szabályai:

$$S \longrightarrow xXy, \quad S \longrightarrow xS, \quad S \longrightarrow Xy, \quad S \longrightarrow yx,$$

$$X \longrightarrow xX, \quad X \longrightarrow Xy, \quad X \longrightarrow yx.$$

3.1. $L_1 = L(G_1)$, ahol $G_1 = (\{S\}, \{a, b\}, S, H_1)$ és a H_1-beli szabályok:

$$S \longrightarrow a^3b, \quad S \longrightarrow a^3Sb.$$

$L_2 = L(G_2)$, ahol $G_2 = (\{S\}, \{a, b\}, S, H_2)$ és a H_2-beli szabályok:

$$S \longrightarrow aSb, \quad S \longrightarrow aS, \quad S \longrightarrow e$$

Az $(L_1L_2 + L_2)^*$ nyelvet generáló környezetfüggetlen grammatikát például a 2.7 Tétel bizonyítása alapján kaphatunk.

3.2. $L = L(G)$, ahol $G = (\{X, Y, S\}, \{a, b\}, S, H)$ és H a következő $(k+1)(k+2)+3$ számú szabályból áll:

$$S \longrightarrow e, \quad X \longrightarrow a, \quad Y \longrightarrow b,$$

továbbá az $S \longrightarrow P$ szabályokból, amelyek P jobb oldala az $S, X, X, \ldots, X, Y$ $k+2$ elemű permutációi.

3.3. $L = L(G)$, ahol $G = (\{A, B, C, D, S\}, \{u, v, w\}, S, H)$ és a H-beli szabályok:

$$S \longrightarrow uAvB, \quad S \longrightarrow CvDw, \quad A \longrightarrow uAv, A \longrightarrow uv,$$

$$D \longrightarrow vDw, \quad D \longrightarrow vw, \quad B \longrightarrow wB, \quad B \longrightarrow w, C \longrightarrow uC, \quad C \longrightarrow u.$$

3.4. Legyen $V = \{x_1, x_2, \ldots, x_n\}$. Ha

$$H = \{S \longrightarrow e, S \longrightarrow x_i, S \longrightarrow x_j S x_j; i, j = 1, 2, \ldots n\},$$

akkor a $G = (\{S\}, V, S, H$ lineáris grammatika generálja az V feletti $P(V)$ palindromok nyelvét. A 3.23 Tétel bizonyításának első részében az $n = 1$ esetre megadott eljárást alkalmazva, $P(V)$ megadható az

$$L_p(V) = (e + x_1 + x_2 + \ldots x_n + x_1 u x_1 + x_2 u x_2 + \cdots + x_n u x_n)^u$$

környezetfüggetlen kifejezéssel, ahol $u \neq V \cup \{S\}$.

3.5. Tegyük fel, hogy az L nyelv környezetfüggetlen. A Bar-Hillel lemma jelöléseit használva, ha $j^2 > k > 0$, akkor $x^{j^2} = ruvwt == (rwt)(uv) = x^{s+m}$, ahol $rwt = x^s$, $uv = x^m$ $(m \geq 1)$ és minden $l \geq 0$ egész számra $q^{s+lm} \in L$. Ez azt jelenti, hogy $s + lm$ minden $l \geq 0$ egészre négyzetszám, ami lehetetlen.

3.6. Tegyük fel, hogy az L nyelv környezetfüggetlen. A Bar-Hillel lemma jelöléseit használva, ha $i > k > 0$, akkor $x^i = ruvwt$ $(r, t, u, v, w \in x^*)$, ahol $|uvw| \leq n$, $uw \neq e$ és minden m nemnegatív egész számra $ru^m vw^m t \in L$. Ha $m = 0$, akkor $rvt \in L$, azaz $|rvt|$ prímszám. Ha $m = |rvt|$, akkor $|ru^m vw^m t| = m(|u| + |w| + 1)$, azaz nem prímszám.

3.7. Az első állítás bizonyításához használjuk fel a 3.5 Bar-Hillel lemmát!

Ha $X = a$, akkor a négyzetmentes szavak nyelve $\{e, a\}$. Ha $X = \{a, b\}$, akkor a négyzetmentes szavak nyelve $\{e, a, b, ab, ba, aba, bab\}$.

4.1. Legyenek L és K az U ábécé felett rekurzívek. Akkor bármely $p \in U^*$ szóra algoritmikusan eldönthető, hogy $p \in L$ vagy $p \in K$, azaz $p \in L + K$. Az is nyilvánvaló, hogy L akkor és csak akkor rekurzív, ha $\overline{L}$ is az. Továbbá $L \cap K = \overline{\overline{L} + \overline{K}}$ miatt $L \cap K$ is rekurzív.

4.2. Legyenek L és K az U ábécé felett rekurzívek. Az előbbi feladat megoldása szerint $L + K$ rekurzív. Bármely $p \in X^*$ szó akkor és csak akkor eleme LK-nak, ha vannak olyan $q \in L$ és $r \in K$ szavak, amelyekre $p = qr$. Ez pedig

$|p| < \infty$ miatt algoritmikusan eldönthető. Továbbá $p \in L^*$ akkor és csak akkor, ha vannak olyan $q_1, q_2, \ldots, q_k \in L$ szavak, amelyekre $p = q_1 q_2 \ldots q_k$. Nyilvánvalóan ez is eldönthető algoritmikusan.

5.1. Legyenek az U ábécé feletti L és K nyelvek rekurzíve felsorolhatók. Ha L vagy K véges, akkor nyilvánvalóan $L + K$ és LK rekurzíve felsorolható. Ha L véges, akkor L^* is rekurzíve felsorolható. Tegyük fel, hogy L és K végtelen, valamint

$$L = \{p_1, p_2, p_3, \ldots\}, \quad K = \{q_1, q_2, q_3, \ldots\}.$$

Akkor

$$L + K = \{p_1, q_1, p_2, q_2, p_3, q_3, \ldots\}$$

rekurzíve felsorolható. LK is rekurzíve felsorolható, minthogy például

$$LK = \{p_1q_1, p_1q_2, p_2q_2, p_2q_1, p_1q_3, p_2q_3, p_3q_3, p_3q_2, p_3q_1, \ldots\}.$$

Ez alapján teljes indukcióval megmutatható, hogy minden n pozitív egész számra L^n rekurzíve felsorolható. Ha az L^n-beli szavak valamely felsorolásában az i-edik elemet (n, i) jelöli, akkor a szokásos

$$(1,1), (1,2), (2,1), (3,1), (2,2), (1,3), (1,4), (2,3), (3,2), (4,1), \ldots$$

felsorolás L^+ elemeinek egy felsorolását adja, vagyis L^+ rekurzíve felsorolható. Ebből már nyilvánvaló, hogy L^* is rekurzíve felsorolható.

7.1. Tegyük fel, hogy van olyan $p = x_1 \ldots x_i \ldots x_j \ldots x_n \in L$, amelyre a (6.4)-ben definiált $\delta(a_0, p) = a_1 \ldots a_i \ldots a_j \ldots a_n$ sorozatban $a_i = a_j$. Akkor

$$x_1 \ldots x_i (x_{i+1} \ldots x_j)^k x_{j+1} \ldots x_n \in L,$$

azaz L végtelen. Megfordítva, tegyük fel, hogy L végtelen. Akkor van olyan $p \in L$, hogy $|p| > |A|$. Ez azt jelenti, hogy a $\delta(a_0, p)$ sorozatban vannak egyenlő állapotok.

7.2. Minden $x \in X$ betű esetén $x^* \subseteq P(X)$. Ha $y \in X$ és $y \neq x$, akkor $x^i b x^k \in P(X)$ akkor és csak akkor, ha $k = i$. Így, ha $i \neq j$, akkor $(x^i, x^j) \neq \vartheta_{P(X)}$. A 7.8 Következmény szerint $P(X)$ nem reguláris. (A 3.4. feladat szerint környezetfüggetlen.)

8.1. Az

A	0	1	2	3	4	5	6	7
x	1	5	6	1	4	4	7	4
y	4	2	3	1	4	3	7	5.

átmenettáblázattal megadott automata 0 kezdőállapottal és 3 végállapottal teljesíti a feltételeket. Ha felrajzoljuk az automata átmenetgráfját, könnyen meggyőződhetünk arról, hogy $0p = 3$ $(p \in \{x, y\})$, akkor és csak akkor, ha $p = xqy$, $q \in \{x, y\}(\{x, y\}^3)^*$ és $p \notin \{x, y\}^* x^3 \{x, y\}^*$.

8.2. Ha van olyan $p \in L$, amelyre $|p| \geq n$, akkor a pumpáló lemmában szereplő jelölésekkel, a lemma bizonyítása szerint, $p = uvw$ $v \neq e$ és minden k nemnegatív egész számra $uv^k w \in L$, azaz L végtelen.

8.3. Használjuk a 8.13 Tétel bizonyításának jelöléseit. Annak eldöntésére, hogy L üres vagy nem, legfeljebb

$$|F||X(n-1)| = |F||X^0 \cup X^1 \cup X^2 \cup X^{n-1}| = |F| \sum_{i=0}^{n-1} |X|^i = l \sum_{i=0}^{n-1} k^i$$

lépés szükséges. Ha $k = 1$, akkor $l(n-1)$, ha $k > 1$, akkor $l\frac{k^n-1}{k-1}$. Annak eldöntésére, hogy L végtelen vagy nem, legfeljebb $|F||X(2n-1) - X(n-1)|$ lépés kell. Ha $k = 1$, akkor ln, ha $k > 1$, akkor $lk^n\frac{k^n-1}{k-1}$.

8.4. Használjuk fel a reguláris nyelvekre vonatkozó pumpáló lemmát.

12.1. $\mathbf{A} = (A, 0, \{x, y\}, \delta, v)$, ahol

$$A = \{0, 1, 2, 2_1, 3, 3_1, 3_2, \ldots, n, n_1, \ldots, n_{n-1}, v, c\},$$

$$\delta(k, x) = k + 1, \quad \delta(k + 1_i, y) = k + 1_{i+1},$$

ahol $k = 0, 1, \ldots, n-1$, $i = 1, \ldots, k$, $k + 1_1 = k + 1$ és $k + 1_{k+1} = v$. Minden más esetben

$$\delta(a, x) = \delta(a, y) = c, \quad a \in A.$$

Az L nyelv felismerési száma $|v| = 1$.

12.2. Ha $pq^n = r^i$ $(r \in Q(X),\ i \geq 2)$, akkor $q \neq r$. a 12.48 Következmény szerint $pq^{n+k} = r^i q^k \in Q(X)$.

12.3. Tegyük fel, hogy S kommutatív és $p, q \in S \cap Q(X)$. Akkor $pq = qp$. A 12.42 Lemma és a 12.45 Tétel alapján $p = q$. Ez azt jelenti, hogy $|S \cap Q(X)| \leq 1$. Szintén a 12.42 Lemmából és a 12.45 Tételből következik, hogy S minden elemének gyöke ugyanaz a primitív szó.

Megfordítva, ha $p, q \in \cap Q(X)$ és $p \neq q$, akkor az előzőek szerint $pq \neq qp$.

12.4 Tegyük fel, hogy $(uv)^n u = w^k$ $(w \in Q(X), 2 \leq k)$. Akkor $(uv)^{n+1} = w^k v$ miatt az $(uv)^{n+1}$ és w^k szavaknak van $k|w|$ hosszúságú közös prefixe. Mivel $k|w| = n|w| + |u|$, ezért

$$k|w| = \frac{k|w|}{2} + \frac{n|w| + |u|}{2} \geq |w| + |uv|.$$

A 12.43 Lemma szerint $w = uv$. Ellentmondás. Hasonlóan látható be, hogy $v(uv)^n \in Q(X)$.

12.5. Legyenek $(p, q) \in \vartheta_{Q(X)\overline{Q}(X)}$, $|p| = |q| = n$, $x, y \in X$ és $x \neq y$. Akkor $(xpx, xqx) \in \vartheta_{Q(X)\overline{Q}(X)}$. Mivel $xpxy^{n+2}x \in Q(X)$, ezért $(xpxy^{n+2}x)^3 \in Q(X)\overline{Q}(X)$. De $\vartheta_{Q(X)\overline{Q}(X)}$ kongruencia, így

$$(xpxy^{n+2}x)(xqxy^{n+2}x)(xpxy^{n+2}x) \in Q(X)\overline{Q}(X).$$

Ebből a 12.45 Tétel segítségével könnyen beláthatjuk, hogy $xpxy^{n+2}x = xqxy^{n+2}x$, azaz $p = q$. A 12.61 Lemma szerint $Q(X)\overline{Q}(X)$ diszjunktív.

12.6.

$$\overline{Q}^2(X) = \{p^i;\ p \in Q(X),\ i \geq 4\} \cup \{q^j r^k;\ q, r \in Q(X),\ j, k \geq 2\}.$$

Legyenek $p, q \in X^*$ és $p \neq q$. A 12.62 Tétel szerint minden $2 \leq n$ egész számra $Q(X)$ és $Q^{(n)}(X)$ diszjunktív pár. Így vannak olyan $u, v \in X^*$, amelyekre mondjuk $upv \in Q(X)$ és $uqv \in Q^{(n)}(X)$ $(n \geq 2)$. Ebből következik, hogy $(upv)(upv)^2 \in Q^{(3)}(X)$ és $(uqv)(upv)^2 \in \overline{Q}^2(X)$. Minthogy $Q^{(3)}(X) \cap \overline{Q}^2(X) = \emptyset$, ezért $Q^{(3)}(X)$ és $\overline{Q}^2(X)$ diszjunktív pár. Így $\overline{Q}^2(X)$ diszjunktív.

12.7. Ha $p = x_1 x_2 \dots x_k$, akkor $W \cap X^* p X^* = \emptyset$. A 12.65 Tétel szerint W-nek nincs diszjunktív résznyelve. A 12.67 Tétel alapján $L - W$ diszjunktív.

12.8. Legyen $k = |w|$. Ha $p = x^k y^k w$ $(x, y \in X, x \neq y)$, akkor $(L \cap w^*) \cap X^* p X^* = \emptyset$. A 12.65 Tétel szerint $L \cap w^*$ nem tartalmaz diszjunktív résznyelvet. Mivel $L = (L - w^*) \cup (L \cap w^*)$ és $(L - w^*) \cap (L \cap w^*) = \emptyset$, a 12.67 Tételből következik, hogy $L - w^*$ diszjunktív.

12.9. Tegyük fel, hogy $X^* - Q$ környezetfüggetlen. Legyenek $a, b \in X$ $(a \neq b)$, n a 3.5 Bar-Hillel lemmában szereplő pozitív egész szám. Akkor a $p = (a^{n+1}b^{n+1})^2 \in X^* - Q$ megadható $p = ruvwt$ $(r, t, u, v, w \in X^*)$ alakban, ahol $|uvw| \leq n$ és $uv \neq e$. Ezért bármely m nemnegatív egész számra $ru^m wv^m t \in X^* - Q$. Ebből $m = 0$ esetre kapjuk, hogy

$$rwt \in \{a^i b^j a^k b^l;\ (i, j) \neq (k, l)\} \subseteq Q.$$

Ellentmondás.

13.1. Tegyük fel, hogy $\varphi(L)$ kód Y felett. Legyen

$$p_1 \dots p_k = q_1 \dots q_k \quad (p_1, \dots, p_k, q_1, \dots, q_k \in L).$$

Akkor

$$\varphi(p_1) \dots \varphi(p_k) = \varphi(p_1 \dots p_k) = \varphi(q_1 \dots q_k) = \varphi(q_1) \dots \varphi(q_k).$$

Mivel $\varphi(L)$ kód, ezért a 13.2 Lemma szerint

$$\varphi(p_1) = \varphi(q_1), \dots, \varphi(p_k) = \varphi(q_k),$$

amiből a φ homomorf kiterjesztése miatt $|p_1| = |q_1|, \dots, |p_k| = |q_k|$. A $p_1 \dots p_k = q_1 \dots q_k$ feltételből kapjuk, hogy $p_1 = q_1, \dots, p_k = q_k$, ami ismét a 13.2 Lemma szerint azt jelenti, hogy L kód.

13.2. Használjuk fel a 13.2 Lemmát. Tegyük fel, hogy $p_1 \dots p_k = q_1 \dots q_k$. Ha $p_1 = \dots = p_k = a^n$, akkor $q_1 = \dots = q_k = a^n$. Ha van olyan p_l, hogy $p_l = a^i b a^j$

$(i \in I, j \in J)$, akkor van olyan $q_{l'}$, hogy $q_{l'} = a^{i'}ba^{j'}$ $(i \in I, j' \in J)$. Legyen l és l' a legkisebb ilyen pozitív egész szám. Ebből az oszthatósági feltételt is felhasználva adódik, hogy $l = l'$ és $p_1 = q_1, \ldots, p_l = q_l$. Az eljárást esetleg véges sokszor megismételve kapjuk, hogy L kód.

13.3. Ha $pq = qp$, akkor a 13.2 Lemma szerint $C = \{p, q\}$ nem kód. Tegyük fel, hogy vannak olyan $p, q \in X^+$, amelyekre $pq \neq qp$ és C nem kód. Válasszunk ezek közül olyan p, q párt, hogy $|pq|$ minimális legyen. Mivel C nem kód, ezért van olyan $w \in C^+$, amely legalább kétféleképpen állítható elő C-beli szavak szorzataként, azaz

$$w = pp_1p = qq_1q,\ p_1, q_1 \in C^* \quad \text{vagy} \quad w = pp_2q = qq_2p,\ p_2, q_2 \in C^*.$$

Válasszunk ezek közül is minimális hosszúságú w-t. Az általánosság megszorítása nélkül feltehető, hogy van olyan $u, v \in X^+$, amelyekre $p = qu = vq$. Ha $qu = uq$, akkor $u = v$ és $pq = quq = qp$, ami lehetetlen, ezért $qu \neq uq$. Hasonlóan $qv \neq vq$. De $|qu|, |vq| < |pq|$, ezért $\{q, u\}$ ill. $\{v, q\}$ kód. Mivel

$$qup_1qu = qq_1q \quad \text{vagy} \quad vqp_2q = qq_2vq,$$

így $q = u$ vagy $q = v$, azaz $pq = q^3 = qp$, ami lehetetlen. Ez azt jelenti, hogy C kód.

13.4. Az uv hossza szerinti teljes indukcióval megmutatjuk, hogy ha $uv = vu$, akkor van olyan $p \in X^+$, amelyre $u = p^k$ és $v = p^l$, azaz uv nem primitív szó. Ezért $uv \neq vu$, amiből az előző feladat szerint adódik az eredmény. Ha $|uv| = 2$, akkor nyilvánvalóan igaz az állítás. Tegyük fel, hogy minden olyan uv szóra is igaz, amelyre $2 \leq |uv| \leq n$. Legyen $|uv| = n + 1$. Feltehetjük, hogy $|u| \geq |v|$. Ha $|u| = |v|$, akkor az $uv = vu$ feltételből következik, hogy $u = v$, azaz $p = u = v$. Ha $|u| > |v|$, akkor vannak olyan $u_1, v_1 \in X^+$, hogy $u = vu_1 = v_1v$, azaz $vu_1v = uv = vu = vv_1v$, s ebből $u_1 = v_1$. Így $u = vu_1 = u_1v$. Mivel $|vu_1| \leq n$, ezért az indukciós feltevés miatt van olyan $p \in X^+$, hogy $v = p^k$ és $u_1 = p^l$. Így $u = vu_1 = p^{k+l}$.

13.5. Legyen C^* reflexív és $pq, prqC^*$ $(p, q, r \in X^*)$. Akkor $qpr, rqp, qp \in C^*$. A 13.5 Tétel szerint $r \in C^*$, azaz teljesül (13.7).

Ha (13.7) teljesül és $pq \in C^*$ $(p, q \in X^*)$, akkor $p(qp)q = (pq)(pq) \in C^*$, azaz $qp \in C^*$, vagyis C^* reflexív.

13.6. Ha L félkód és $p_1 \ldots p_k = q_1 \ldots q_l$ $(p_1, \ldots, p_l, q_1, \ldots, q_l \in L^n$, akkor $kn = ln$, így $k = l$. Megfordítva, ha L^n $(n \geq 2)$ félkód és $p_1 \ldots p_k = q_1 \ldots q_l$ $(p_1, \ldots, p_k, q_1, \ldots, q_l \in L)$, akkor $(p_1 \ldots p_k)^n = (q_1 \ldots q_l)^n$. Ebből következik, hogy vannak olyan $u_1, \ldots, u_k, v_1, \ldots, v_l \in L^n$ szavak, hogy $u_1 \ldots u_k = v_1 \ldots v_l$, vagyis $k = l$.

Ha L félkód, $a \in X$ és $a^i \neq a^j \in L$, azaz $i \neq j$, de $(a^i)^j = (a^j)^i$.

13.7. A 12.42 Lemmából, a 13.3. és a 13.6. feladatokból következik.

15.1. L (prefix) kód. Legyen π az X ábécé tetszőleges pozitív Bernoulli mértéke és $0 < \pi(a) = r < 1$. Akkor

$$\pi(L) = \sum_{n=0}^{\infty} r^n(1-r)\pi((a+b)^n) = \sum_{n=0}^{\infty} r^n(1-r) = 1.$$

A 15.3 Tétel szerint L maximális kód.

16.1. Használjuk fel a 16.2 Példával kapcsolatos meggondolásokat. A $\varphi(p) = |p|_a - k|p|_b$ ($p \in \{a,b\}^*$) leképezés az $\{a,b\}^*$ szabad monoid homomorf leképezése az egész számok Z additív csoportjára és $L_k = \varphi^{-1}(0)$. Legyen L_k bázisa D_k. Ha $p \in X^+$, akkor $q = a^{2k|p|_b+(k-1)|p|_a}pb^{|p|} \in L_k = D_k^*$. Továbbá q-nak nincs valódi kezdőszelete D_k^+-ból, így $q \in D_k$, vagyis D_k sűrű kód.

16.2. $L = X^*X^k$.

16.3. Legyen $\mathbf{A} = (A, a_0, X, \delta, F)$ olyan automata, amelyre $L = L(\mathbf{A})$ és $|A| = n$. Mivel L jobbról sűrű, ezért minden $p \in X^*$ szóhoz van olyan $q \in X^*$ szó, amelyre $pq \in L$, vagyis $a_0pq \in F$. Nyilvánvalóan olyan $r \in X^*$ szó is van, hogy $a_0pr = a_0pq \in F$ és $|r| \leq n-1$.

16.4. B ritka, ezért létezik olyan $q \in X^+$ szó, hogy $X^*qX^* \cap B = \emptyset$. De M jobbról sűrű, így minden $p \in X^*$ szóhoz van olyan $r \in X^*$ szó, amelyre $pqr \in M$. Ebből következik, hogy $pu \in M$, ahol $q = uv$ $(u \in X^*,\ v \in X^+)$. Ez azt jelenti, hogy M jobbról $(|q|-1)$ sűrű.

17.1. Tegyük fel, hogy C prefix kód és $A, B \subseteq X^*$. Nyilvánvalóan $C(A \cap B) \subseteq CA \cap CB$. Ha $p \in CA \cap CB$, akkor $p = ca = db$ $(c,d \in C, a \in A, b \in B)$. Mivel C prefix kód, ezért $c = d$, s így $a = b$, azaz $p \in C(A \cap B)$. Tehát $C(A \cap B) = CA \cap CB$.

Megfordítva, tegyük fel, hogy $C(A \cap B) = CA \cap CB$ minden $A, B \subseteq X^*$ esetén. Ha C nem prefix kód, akkor vannak olyan $p, q \in X^+$, hogy $p, pq \in C$. Legyen $A = \{p, qp\}$ és $B = \{q^2p\}$. Akkor $C(A \cap B) = \emptyset$, de $pq^2p \in CA \cap CB$, ami lehetetlen. Így C kód.

17.2. Ha C és L prefix kód, akkor a 17.18 Következmény szerint CL is prefix kód. Ha C és CL prefix kód, akkor indirekt bizonyítással megmutatható, hogy L is prefix kód.

17.3. Tegyük fel, hogy C_1C_2 prefix kód. Ha C_2 nem prefix kód, akkor $C_2X^+ \cap C_2 \neq \emptyset$, ezért

$$\emptyset \neq C_1(C_2X^+ \cap C_2) \subseteq C_1C_2X^+ \cap C_1C_2.$$

Ez azonban lehetetlen, mivel C_1C_2 prefix kód. Kaptuk, hogy C_2 is prefix kód. A bizonyítás $(2 \leq)n$ szerinti teljes indukcióval fejezhető be.

Az állítás szuffix kódokra: Ha $C_1C_2 \dots C_n$ szuffix kód, akkor

$$C_1, C_1C_2, \dots, C_1C_2 \dots C_{n-1}$$

is szuffix kód.

17.4. Legyen $r \in V$. Tegyük fel, hogy van olyan $p \in X^+$, hogy $rp \in \overline{C} + CX^*$. Ha $rp \in \overline{C}$, akkor $r \in \overline{C}$. Ez azonban lehetetlen, ezért $rp \in CX^*$, azaz van olyan $t \in C$ és $q \in X^*$, hogy $rp = tq$. Mivel $r \notin \overline{C}$, ezért $r = tq'$ $(q' \in X^*)$, vagyis $r \in CX^*$, ami szintén lehetetlen. Így $rp \in V$.

17.5. Ha C maximális prefix kód, akkor $V = \emptyset$, s így $V - VX^+ = \emptyset = \overline{V - VX^+}$.

Legyen $V \neq \emptyset$. A 17.4. feladat szerint $VX^+ \subseteq V$, ezért $V = (V - VX^+) + VX^+$. Legyen $p \in V - VX^+$ és $p = qr$ $(q \in X^*,\ r \in X^+)$. Ha $q \in VX^+$, akkor $p \in VX^+$, ami lehetetlen, így $q \notin VX^+$. Mivel $V - VX^+$ prefix kód, ezért $q \notin V - VX^+$. Így $q \in \overline{C} + CX^*$. Ha $q \in CX^*$, akkor $p \in CX^*$, ami lehetetlen. Tehát $q \in \overline{C}$, vagyis $\overline{V} - VX^+ \subseteq \overline{C}$.

Megmutatjuk, hogy $V = (V - VX^+)X^*$, amiből már következik, hogy $C + (V - VX^+)$ maximális prefix kód. Ismét a 17.4. feladat szerint $(V - VX^+)X^* \subseteq V$. Megfordítva, ha $v \in V$, akkor $v \in V - VX^+$ vagy $v \in VX^+$. Ha $v \in V - VX^+$, akkor nyilván $v \in (V - VX^+)X^*$. Ha $v \in VX^+$, akkor van olyan $u \in V - VX^+$ és $t \in X^+$, hogy $v = ut$, így $v \in (V - VX^+)X^*$. Ezek azt jelentik, hogy $V \subseteq (V - VX^+)X^*$.

17.6. Ha $D = C + (V - VX^+)$, akkor az 17.5. feladat szerint

$$\overline{D} = \overline{C} + \overline{V} - VX^+ = \overline{C}.$$

Megfordítva, legyen $C \subseteq D$, $\overline{D} = \overline{C}$ és D maximális prefix kód. A 16.11 Tétel és a 17.5. feladat szerint

$$X^* = \overline{D} + DX^* = \overline{C} + (C + (V - VX^+))X^*.$$

Minthogy $\overline{D} \cap DX^* = \emptyset$ és $\overline{C} \cap (C + (V - VX^+))X^* = \emptyset$, ezért $DX^* = (C + (V - VX^+)X^*$. Ha $q \in D$, akkor van olyan $r \in C + (V - VX^+)$ és $t \in X^*$, hogy $q = rt$. Ha $t \in X^+$, akkor $r \in \overline{D} = \overline{C}$. De $\overline{C} \cap C = \emptyset$ és $\overline{C} \cap V = \emptyset$ miatt ez lehetetlen. Így $t = e$, azaz $q = r \in C + (V - VX^+$. Tehát $D \subseteq C + (V - VX^+$. Mivel D maximális prefix kód, ezért $D = C + (V - VX^+$.

17.7. Csak prefix kódokra mutatjuk meg. Ha $p, q \in X^*$ és $p \neq q$, akkor vannak olyan $u, v \in X^*$, amelyekre $upv \in L$ és $uqv \notin L$. Ha $r \in C$ tetszőleges, akkor $rX^+ \cap C = \emptyset$. Nyilvánvaló, hogy $rupv \in CL$. Megmutatjuk, hogy $ruqv \notin CL$. Valóban, ha $ruqv \in CL$, akkor van olyan $t \in C$ és $w \in L$, hogy $ruqv = tw$. Mivel $r, t \in C$, ezért $r = t$, sígy $w = uqv \in L$, ami lehetetlen.

17.8. A 17.19 Következmény szerint az előző feladatból kapjuk.

17.9. $C(L)$ nyilvánvalóan prefix kód. Mivel L jobbról k teljes, ezért minden $p \in X^*$ szóhoz van olyan $q \in X(k)$ szó, amelyre $pq \in L^*$. $C(L)$ definíciója miatt $pq \in C(L)X^*$. A 16.11 és a 17.5 Tételek szerint $C(L)$ maximális prefix kód. A 16.11 Tétel (3) állítása szerint $p = uv$, ahol $u \in C(L)^*$ és $v \in \overline{C(L)}$.

Mivel L^* jobbról k teljes, van olyan $r \in X(k)$, amelyre $vr \in L^*$. Ha r a legrövidebb hosszúságú ilyen szó, akkor $vr \in C(L)$, azaz $pr = uvr \in C(L)^*$, vagyis $C(L)$ jobbról k teljes.

17.10. Tegyük fel, hogy minden $u \in \overline{C}$ szóra $uX(k) \cap C \neq \emptyset$. A 17.5 Tétel szerint C jobbról teljes. A 16.11 Tétel szerint minden $p \in X^*$ szó felírható $p = uv$ alakban, ahol $u \in C^*$ és $v \in \overline{C}$. A feltétel szerint van olyan $r \in X(k)$, amelyre $vr \in C$, azaz $pr = uvr \in C^*$, vagyis C jobbról k teljes.

Az állítás megfordítása az előző feladat megoldásából következik.

17.11. A 17.9. feladat szerint $C(L) \subseteq L$ és $C(L)$ jobbról k teljes. Ha $K \subset L$ jobbról k teljes nyelv X felett, akkor $C(K) = C(L)$.

17.12. Ha $L \subseteq X^*$ minimális jobbról k teljes nyelv, akkor $L = C(L)$. A 17.9. feladat szerint igaz az állítás.

18.1. Ha L teljesiti az $X^*L \subseteq LX^*$ feltételt és $C = L - LX^+$, akkor $X^*C \subseteq X^*L \subseteq LX^* = CX^*$. A 18.7 Tétel szerint C szemafor prefix kód X felett. Megfordítva, ha C szemafor prefix kód X felett, akkor a 18.7 Tétel szerint $X^*C \subseteq CX^*$. Ha $p \in X^*L$, akkor vannak olyan $u, v \in X^*$ és $q \in C$, hogy $p = uqv$. Így $p \in X^*CX^* \subseteq CX^*X^* = CX^*$. De $CX^* = LX^*$, s így $X^*L \subseteq LX^*$.

18.2. Legyen C olyan kód X felett, amelyre $X^*C \subseteq CX^*$. Az előző feladat szerint $D = C - CX^+$ szemafor prefix kód, így a 18.4 Lemma szerint maximális prefix kód. A 18.10 Következmény szerint D ritka kód. A 18.9 Tételt alkalmazva kapjuk, hogy D maximális kód. De $D \subseteq C$, így $C = D$, azaz C szemafor prefix kód. Megfordítva, ha C szemafor prefix kód, akkor a 18.7 Tételből következik, hogy $X^*C \subseteq CX^*$.

18.3. Ha C szemafor prefix kód, akkor az előző feladat szerint $X^*C \subseteq CX^*$. Legyen $u \in \overline{C}$ és $p \in C$. Akkor van olyan $q \in C$ és $v \in X^*$, hogy $up = qv$. Mivel C prefix kód, ezért $v \in \underline{C}$. Így $\overline{C}C \subseteq C\underline{C}$. Megfordítva, tegyük fel, hogy $\overline{C}C \subseteq C\underline{C}$. Ha $p \in X^*C$, akkor $p = uq$ ($u \in X^*$, $q \in C$). Mivel C jobbról teljes, ezért $pX^* \cap C^* \neq \emptyset$. Így $u \in CX^*$ vagy $u \in \overline{C}$. Ha $u \in CX^*$, akkor $p \in CX^*C \subseteq CX^*$. Ha $u \in \overline{C}$, akkor $p \in \overline{C}C \subseteq C\underline{C} \subseteq CX^*$. Vagyis $X^*C \subseteq CX^*$. Az előző feladat szerint C szemafor prefix kód.

19.1. Ha L_1 nem szuffix kód, akkor vannak olyan $p, q \in X^+$ szavak, amelyekre $p, qp \in L_1$. Ha $r \in L_2$, akkor $pr, qpr \in L_1L_2$, ami ellentmond annak, hogy L_1L_2 bifix kód. Hasonlóan mutatható meg, hogy L_2 prefix kód.

19.2. Ha $X^+L \subseteq LX^+$, akkor a 17.1 Lemma bizonyítása szerint $X^n \subseteq L$. Ha $X^n \subseteq L$, akkor $X^+L \subseteq \cup_{k=n+1}^{\infty} X^k = X^nX^+ \subseteq LX^+$.

19.3. Legyen az X feletti C kód infix kód. Ha $u \in C$ és $p \in X^+$, akkor $X^*puX^* \cap C = \emptyset$, vagyis C ritka kód. A 7.3 Lemmából következik, hogy C egy ϑ_C-osztály.

19.4. Ha L nem outfix kód, akkor vannak olyan $i \neq j$ pozitív egész számok és $w \in X^+$ szó, hogy $p_iq_ir_i = uv$ és $p_jq_jr_j = uwv$ valamilyen $u, v \in X^*$ szavakra.

Az $p_iq_ir_i = uv$ egyenletből következik, hogy $u = p_is$ vagy $v = tr_i$ $(s, t \in X^*)$. Ha $u = p_is$, akkor $p_jq_jr_j = p_iswv$. Ez ellentmondás, mivel $p_i \neq p_j$ és L_1 prefix kód. Ha $v = tr_i$, akkor hasonlóan ellentmondásra jutunk, mert L_3 szuffix kód. Ez azt jelenti, hogy L valóban outfix kód.

19.5. A

$$\varphi(p) = \sum_{a \in X_1} |p|_a - \sum_{b \in X_2} |p|_b \ (p \in X^*)$$

leképezés X^* homomorf leképezése az egész számok Z additív csoportjára $(\varphi(a) = 1 \ (a \in X_1), \varphi(b) = -1 \ (b \in X_2))$, $M = \varphi^{-1}(0)$. A 15.12 Lemma szerint M az X^* unitér részfélcsoportja. A 13.9 Tétel szerint M bázisa bifix kód, amelynek elemei azok a $p_1q_1 \dots p_nq_n$ szavak, amelyekre $p_1, \dots, p_n \in {X_i}^+$, $q_1 \dots q_n \in {X_j}^+$ $(i, j = 1, 2, \ i \neq j)$, $|p_1| + \dots + |p_n| = |q_1| + \dots + |q_n|$ és $n > 1$ esetben $|p_1| + \dots + |p_k| > |q_1| + \dots + |q_k|$ $(k = 1, \dots, n-1)$.

19.6.

(1) $\Longrightarrow$ (2): Az $aX^* \cap C = \emptyset$ $(a \in X)$ feltételből következik, hogy $C \cup a$ prefix kód.

(2) $\Longrightarrow$ (3): Legyen $ua \in C^*$ $(u \in X^*, a \in X)$. Van olyan $v \in X^*$, amelyre $av \in C^*$. Mivel C erős kód, ezért $a(ua)v = (au)(av) \in C^*$, azaz $au \in C^*$. Ebből következik, hogy C^* reflexív. Legyen $w \in X^+ - C$ és $w = x_1 \dots x_k$ $(x_1, \dots, x_k \in X$. Akkor $x_1v_1, \dots, x_kv_k \in C$ valamilyen $v_1, \dots, v_k \in X^*$ szavakra. De C erős kód, így $wv_k \dots v_1 = c_1 \dots c_m$ $(c_1, \dots, c_m \in C)$. Minthogy C^* reflexív, $v_k \dots v_1w = d_1 \dots d_n$ $(d_1, \dots, d_n \in C)$. Innen $c_1 \dots c_mw = wd_1 \dots d_n$, amiből következik, hogy $C \cup w$ nem kód, vagyis C maximális kód.

(3) $\Longrightarrow$ (1): Nyilvánvaló.

19.7 Használjuk fel a 13.5. és a 19.6. feladatokat és megoldásaikat!

20.1. Legyen Y C-vel ekvivalens halmaz és $\varphi(Y) = C$, ahol φ Y X feletti kódolása. A 17.19 Következmény szerint C^n $(n \in N_+)$ maximális prefix kód. Tegyük fel, hogy C^n szinkron kód, azaz van olyan $p \in (C^n)^+$, amelyre $X^*p \subseteq (C^n)^*$. Akkor $(C^*p \subseteq X^*p \subseteq (C^n)^*$, azaz

$$Y^*\varphi^{-1}(p) = \varphi^{-1}(C^*)\varphi^{-1}(p) = \varphi^{-1}(C^*p) \subseteq \varphi^{-1}((C^n)^*)(= ((\varphi^{-1}(C))^n)^* = (Y^n)^*,$$

vagyis Y^n szinkron kód Y felett. Ha $y \in Y$, akkor $y\varphi^{-1}(p), \varphi^{-1}(p) \in (Y^n)^+$ miatt mind a két szó hossza osztható n-nel, s így $n = 1$.

20.2. A 17.19 Következmény és a 17.16 Lemma szerint $D = (C^n - C') + C'C^n$ $(n \in N_+)$ maximális prefix kód. Tekintsük az előző feladat megoldását. Elegendő megmutatni, hogy ha $2 \leq n$, akkor $D = (Y^n - \varphi^{-1}(C')) + \varphi^{-1}(C')Y^n$ aszinkron kód Y felett. Ha ugyanis D szinkron kód lenne, akkor volna olyan $q \in D^+$, amelyre $Y^*q \subseteq D^*$. Minden D^+-beli szó hossza osztható n-nel. Ha $y \in Z$, akkor $yq, q \in D^+$ miatt yq és q hossza is osztható n-nel. Ebből következik, hogy $n = 1$.

Irodalomjegyzék

[1] Babcsányi I., *Automaták, Nyelvek, Kódok*, BME, Matematika Intézet, Algebra Tanszék, 2007, elektronikus jegyzet, `www.math.bme.hu/~babcs/`

[2] Babcsányi I., *Algebrai Automataelmélet*, BME, TTK, Matematika Intézet, 2011, elektronikus jegyet, `http://tankonyvtar.ttk.bme.hu/pdf/18.pdf`, (ISBN: 978-963-279-461-7)

[3] Bach I., *Formális Nyelvek*, Typotex Kiadó, Budapest, 2002

[4] J. Berstel–D. Perrin, *Theory of Codes*, Academic Press, Orlando, 1985

[5] J. Berstel–D. Perrin–C. Reutenauer, *Codes and Automata*, Cambridge University Press, Cambridge, 2010

[6] G. Birkhoff–T.C. Bartee, *A Modern Algebra a Számítástudományban*, Műszaki Könyvkiadó, Budapest, 1974

[7] Csákány B., *Algebra*, Tankönyvkiadó, Budapest, 1974

[8] Csuhaj-Varjú E.–D.Dassow–J.Kelemen–Gh.Paun, *Grammar Systems: A grammatical approach to distribution and cooperation*, Gordon and Breach Science Publications, Topics in Computer Mathematics 5, Yverdon, 1994

[9] Demetrovics J.–J. Denev–R. Pavlov, *A Számítástudomány Matematikai Alapjai*, Tankönyvkiadó, Budapest, 1985

[10] Dömösi P.–Falucskai J.–Horváth G.–Mecsei Z.–Nagy B., *Formális Nyelvek és Automaták*, 2011, elektronikus jegyzet, `http://progmat.hu/tananyagok/formalis_nyelvek_es_automatak/book.html`

[11] Dömösi P.–Horváth S.–M. Ito, *Context Free Languages and Primitive Words*, World Scientific Publishing, 2013

[12] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, New York–London, 1974

[13] S. Eilenberg, *Automata, Languages and Machines*, Vol. B, Academic Press, New York–San Francisco–London, 1976

[14] Ésik Z., *A Számítástudomány Alapjai*, Szegedi Tudományegyetem, Természettudományi és Informatikai Kar, Számítástudomány Alapjai Tanszék, 2011, elektronikus jegyzet

[15] Ésik Z.–Gombás É.–Iván Sz., *Automaták és Formális Nyelvek Példatár*, Szegedi Tudományegyetem, Természettudományi és Informatikai Kar, Számítástudomány Alapjai Tanszék, 2011, elektronikus jegyzet

[16] Fried E., *Általános Algebra*, Tankönyvkiadó, Budapest, 1981

[17] Fülöp Z., *Formális Nyelvek és Szintaktikus Elemzésük*, Polygon, Szeged, 1999

[18] Fülöp Z., *Automaták és Formális Nyelvek*, Szegedi Tudományegyetem, Természettudományi és Informatikai Kar, Számítástudomány Alapjai Tanszék, Szeged, 2012, elektronikus jegyzet

[19] Gécseg F., *Automaták és Formális Nyelvek*, Polygon, Szeged, 2005

[20] Gécseg F.–Peák I., *Az Automaták Algebrai Elmélete*, Matematikai Lapok, 1966, 77-134 o.

[21] Gécseg F.–Peák I., *Algebraic Theory of Automata*, Akadémiai Kiadó, Budapest, 1972

[22] V.M. Gluskov, *Az automaták absztrakt elmélete, I. rész*, Magyar Tud. Akad. III. Oszt. Közl., 13., 1963, 287-309 o.

[23] V.M. Gluskov, *Az automaták absztrakt elmélete, II. rész*, Magyar Tud. Akad. III. Oszt. Közl., 14., 1964, 71-110 o.

[24] W.M.L. Holcombe, *Algebraic Automata Theory*, Cambridge University Press, Cambridge, 1982

[25] J.M. Howie, *Automata and Languages*, Clarendon Press, Oxford, 1991

[26] M. Ito, *Algebraic Theory of Automata and Languages*, World Scientific Publishing, New Jersey, 2004

[27] Iványi A. (szerk.), *Informatikai Algoritmusok I.*, ELTE Eötvös Kiadó, Budapest, 2004

[28] Iványi A. (szerk.), *Informatikai Algoritmusok II.*, ELTE Eötvös Kiadó, Budapest, 2005

[29] Sz.V. Jablonszkij–O.B. Lupanov, *Diszkrét Matematika a Számítástudományban*, Műszaki Könyvkiadó, Budapest, 1980

[30] G. Lallement, *Semigroups and Combinatorial Applications*, John Wiley and Sons, New York, 1979

[31] M.V. Lawson, *Finite Automata*, CRC Press LLC, Boca Raton–London–New York–Washington, 2004

[32] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin–Heidelberg, 1999 (3. javított és bővített kiadás)

[33] Peák I., *Bevezetés az Automaták Elméletébe I.*, Tankönyvkiadó, Budapest, 1977

[34] Peák I., *Bevezetés az Automaták Elméletébe II.*, Tankönyvkiadó, Budapest, 1978

[35] Peák I., *Algebra*, Tankönyvkiadó, Budapest, 1983

[36] D. Perrin–J.É. Pin, *Infinite Words*, Elsevier Academic Press, Amsterdam, 2004

[37] Révész Gy., *Bevezetés a Formális Nyelvek Elméletébe*, Akadémiai Kiadó, Budapest, 1979

[38] Rónyai L.–Ivanyos G.–Szabó R., *Algoritmusok*, Typotex, Budapest, 1999

[39] A. Salomaa, *Theory of Automata*, Pergamon Press, Oxford, 1969

[40] A. Salomaa, *Formal Languages*, Academic Press, New York–London, 1973

[41] H.J.Shyr, *Free Monoids and Languages*, Department of Mathematics, Soochow University, Taipei, Taiwan, R.O.C., 1979

[42] B.A. Trahtenbrot, *Algoritmusok és Absztrakt Automaták*, Műszaki Könyvkiadó, Budapest, Mir Könyvkiadó, Moszkva, 1978

Tárgymutató