A lineáris algebra alkalmazásai

Wettl, Ferenc

2014

Tartalom

A lineáris algebra alkalmazásai

Tartalom

Bevezető

A lineáris algebra fogalmai, eredményei, számítási módszerei meglepően sok alkalmazásra leltek a matematikán kívüli területeken is, a műszaki tudományoktól a közgazdaságtanon át az informatikáig. E rövid jegyzet egy nagyobb lineáris algebráról szóló műbe való feldolgozáshoz készült önállóan is használható előtanulmányként. A szükséges előismereteket e nagyobb mű tartalmazza.

Célunk a lineáris algebra alkalmazásainak rendkívül változatos és színes kavalkádjából - ezt a változatosságot is tükröző - néhány elemet fölmutatni. Elemi és mélyebb előismeretet kívánó, játékos és komoly, klasszikus és a legújabb technikákhoz kapcsolódó modern alkalmazások egyaránt szerepelnek e műben.

Először a matematikai alkalmazásokkal kezdjük, de itt is a matematikán kívüli világ volt a fő célpont. Mérnökhallgatók sok évtizedes oktatásának egyik tapasztalata, hogy kevesen értik a matematika egyik legfontosabb fogalmát, a deriválást, ha nem csak egy egyváltozós valós függvényről van szó. E fogalom nem is érthető meg a lineáris leképezés megértése nélkül. Hasonlóan fontos az elsőrendű differencia- és differenciálegyenlet-rendszerek tárgyalása, melynek megértéséhez a

Jordan-normálalak, illetve a mátrixfüggvények elemi ismerete szükséges. A kombinatorikai alkalmazások a véges testek fölötti lineáris terek alkalmazására mutatnak két szép példát, egyikük a statisztikai eredetű Fischer-egyenlőtlenség. A természetben sok helyütt fölbukkanó Fibonacci-sorozat másik fontos témánk. A kombinatorikai részt végül egy szórakoztató játék megoldásának megértésével zárjuk. A nemnegatív mátrixok elmélete egy nyilvánvalóan komoly alkalmazott téma - a Markov-láncok - elméletének alapját képezi. Ezzel zárjuk az első fejezetet.

A második fejezet egy mára a lineáris algebrától különvált, önálló tudomány - a lineáris programozás - alapjait ismerteti. Az anyag tárgyalásában igyekszünk az elemi sorműveletekkel megoldható elemi szinten maradni. E fejezetet egy egy-két órás előadás kísérőanyagának szánjuk.

A harmadik fejezet egy ugyancsak a lineáris algebrához közel álló téma, a kódelmélet és a kriptográfia alapjait tárgyalja.

Végül a negyedik fejezet a lineáris algebra közvetlen műszaki alkalmazásaira koncentrál. Egy elemi - lineáris egyenletrendszerekkel megoldható - bevezető után a web-en való keresés matematikai alapjairól, végül a szinguláris érték szerinti felbontás néhány szép alkalmazásáról lesz szó. Itt olyan modern műszaki témák is szóba kerülnek, mint a GPS, a Google PageRank algoritmusa, az arcfelismerés, vagy az információtömörítés.

Ezúton szeretnék köszönetet mondani Szőke Magdolna alapos lektori munkájáért, a szöveg érthetőbbé tételét eredményező javaslataiért, valamint Tóth László technikai segítségéért.

Budapest, 2013-11-11

1 Alkalmazások a matematika különböző területein keresztül

1.1 Differenciálhatóság

A lineáris leképezés fogalma az alkalmazott matematika sok területén bukkan föl, aminek az az egyik oka, hogy tetszőleges vektor-vektor függvény differenciálhatósága azt jelenti, hogy létezik a függvény megváltozását „jól közelítő” lineáris leképezés.

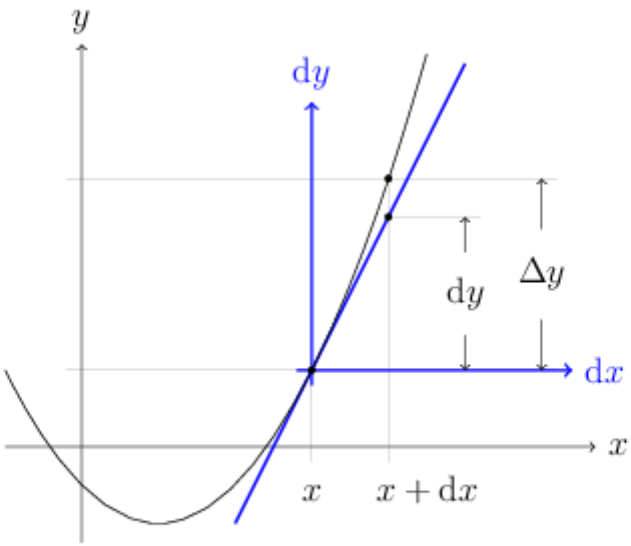
Vektor-vektor függvények differenciálhatósága

Az $\mathbb{R}^n$ -ből $\mathbb{R}^m$ -be képző lineáris leképezések egy igen fontos alkalmazása a vektor-vektor függvények differenciálhatóságának fogalma.

A differenciálhatóság szokásos definíciója a következő: azt mondjuk, hogy az $f : \mathbb{R} \to \mathbb{R}$ függvény differenciálható az x helyen, ha létezik és véges a

$$D = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

határérték. A D számnak fontos jelentése van: az f függvény x körüli megváltozása jól közelíthető a $\mathrm{d}x \mapsto D\mathrm{d}x$ függvény 0 körüli megváltozásával. Szemléltetve ez azt jelenti, hogy ha az f grafikonján az $(x, f(x))$ pontra helyezünk egy $\mathrm{d}x$ és $\mathrm{d}y$ változójú koordinátarendszert, akkor a $\mathrm{d}x \mapsto \mathrm{d}y = D\mathrm{d}x$ grafikonja az f függvény grafikonjának érintője (ld. az 1 ábrát). Eszerint, kicsit leegyszerűsítve a megfogalmazást, a differenciálhatóság azt jelenti, hogy a függvény „jól közelíthető” egy $\mathbb{R} \to \mathbb{R}$ lineáris leképezéssel, hisz a $\mathrm{d}x \mapsto D\mathrm{d}x$ leképezés ilyen.



1. ábra. A $\mathrm{d}x$ és $\mathrm{d}y$ koordinátatengelyeket és a $\mathrm{d}y = D\mathrm{d}x$ függvény grafikonját színezéssel kiemeltük. Az ábra egyúttal a $\Delta y \approx \mathrm{d}y$ kapcsolatot is szemlélteti.

A „jól közelítés” szemléletesen azt jelenti, hogy az f grafikonjára „zoomolva”, azaz azt folyamatosan nagyítva, a grafikon kiegyenesedni látszik. Ez az az egyenes, melyet a grafikon érintőjének nevezünk, és amelynek $\mathrm{d}y = D\mathrm{d}x$ az egyenlete az új koordinátarendszerben.

Ez a definíció ekvivalens módon átfogalmazható: azt mondjuk, hogy az $f : \mathbb{R} \to \mathbb{R}$ függvény differenciálható az x helyen, ha van olyan D szám, hogy

$$\lim_{h \to 0} \frac{f(x+h) - f(x) - Dh}{h} = 0.$$

Ez utóbbi alak azzal az előnnyel is jár, hogy könnyen általánosítható. Az általánosítás legfőbb nehézsége az, hogy a vektorral való osztás nem definiálható megfelelően, ezért e formulán még egy apró, de még mindig ekvivalens változtatást teszünk: nem h-val, hanem annak abszolút értékével osztunk:

$$\lim_{h\to 0} \frac{f(x+h)-f(x)-Dh}{|h|} = 0.$$

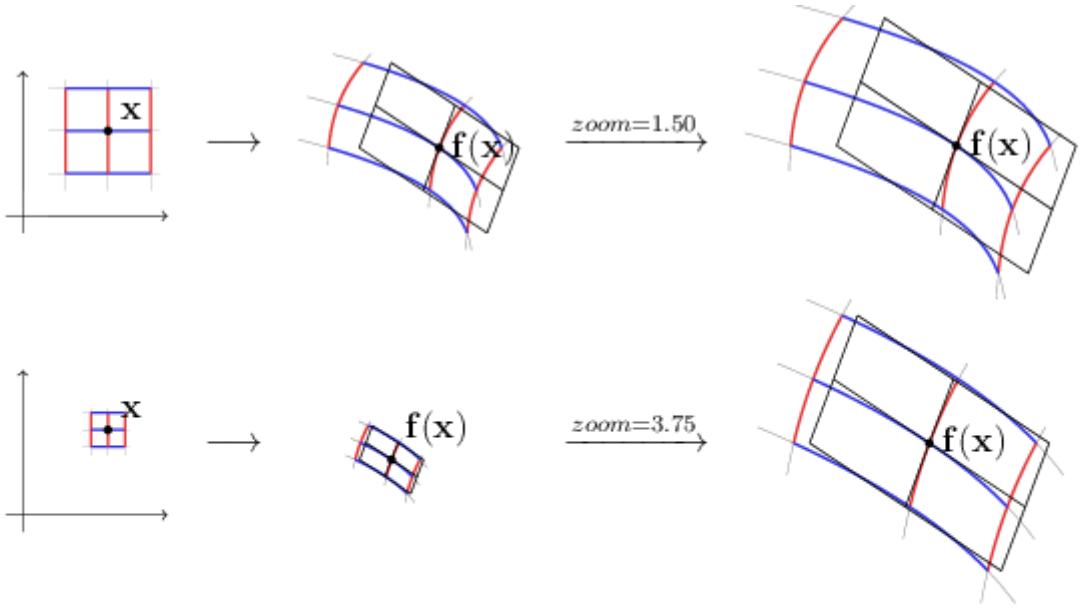
Mindezek a következő definícióhoz vezetnek:

1.1. Definíció (Differenciálhatóság) Azt mondjuk, hogy az $\mathbf{f}:\mathbb{R}^n \to \mathbb{R}^m$ függvény differenciálható az $\mathbf{x}$ helyen, ha létezik olyan $D_{\mathbf{f},\mathbf{x}}:\mathbb{R}^n \to \mathbb{R}^m$ lineáris leképezés, melyre

$$\lim_{\mathbf{h}\to \mathbf{0}} \frac{\mathbf{f}(\mathbf{x}+\mathbf{h})-\mathbf{f}(\mathbf{x})-D_{\mathbf{f},\mathbf{x}}\mathbf{h}}{|\mathbf{h}|} = \mathbf{0}.$$

A $D_{\mathbf{f},\mathbf{x}}$ leképezést az $\mathbf{f}$ függvény $\mathbf{x}$ ponthoz tartozó deriváltleképezésének nevezzük.

- A $D_{\mathbf{f},\mathbf{x}}$ jelölés arra utal, hogy a deriváltleképezés az $\mathbf{f}$ függvénytől és az $\mathbf{x}$ helytől is függ, maga viszont mint leképezés egy $\mathbf{h}$ vektorhoz a $D_{\mathbf{f},\mathbf{x}}\mathbf{h}$ vektort rendeli.
- Elterjedtebb a $D_{\mathbf{x}}(\mathbf{f})$ jelölés, itt didaktikai okból választottunk olyat, mely jobban világossá teszi, hogy ez egy lineáris leképezés, mely majd hat valamely $\mathbf{h}$ vektoron, és annak képe $D_{\mathbf{x}}(\mathbf{f})\mathbf{h}$ vagy $D_{\mathbf{x}}(\mathbf{f})(\mathbf{h})$ - az általunk használt jelölésben $D_{\mathbf{f},\mathbf{x}}\mathbf{h}$.
- Egy $\mathbb{R}^2 \to \mathbb{R}^2$ függvényen könnyen szemléltethető a derivált jelentése. Tekintsük az értelmezési tartomány egy négyzetrácsát, annak középpontja legyen $\mathbf{x}$. Tekintsük e rács képét az $\mathbf{f}$ függvény által, és a $D_{\mathbf{f},\mathbf{x}}$ deriváltleképezés hatását e rácson, ha az origót $\mathbf{x}$-be tesszük. A rács méretét folyamatosan csökkentve, a képeket pedig arányosan fölnagyítva azt látjuk, hogy a két kép egyre jobban „összesimul” (ld. 2 ábra). Ez emlékeztet arra - bár nem tökéletesen analóg vele -, ahogy az egyváltozós függvény grafikonjának egy pontjára „zoomolva” a grafikon az érintőhöz közelít, rásimul.



2. ábra. Egy $\mathbb{R}^2 \to \mathbb{R}^2$ függvény egy $\mathbf{x}$ pontban való differenciálhatóságának szemléltetésére tekintsük az értelmezési tartomány egyre sűrűbb négyzetrácsainak az $\mathbf{x}$ pontot körülvevő négyzeteit, valamint ezek $\mathbf{f}$ függvény általi képét (színes rács), és a $\mathbf{D}_{\mathbf{f},\mathbf{x}}$ deriváltleképezés hatását e rácson, ha az értelmezési tartományának origóját $\mathbf{x}$-be, értékkészletének origóját $\mathbf{f}(\mathbf{x})$-be tesszük. Az egyre kisebb képeket fölnagyítva látható, hogy a függvény általi kép egyre jobban közelít a deriváltleképezés általi képhez.

Jacobi-mátrix

A deriváltleképezés mátrixa könnyen megkapható a koordinátafüggvények parciális deriváltjai segítségével.

1.2. Tétel (Jacobi-mátrix) Ha az $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^m; (x_1, x_2, \ldots, x_n) \mapsto (f_1, f_2, \ldots, f_m)$ függvény differenciálható az $\mathbf{x}$ helyen, akkor a lineáris $D_{\mathbf{f},\mathbf{x}}$ deriváltleképezés mátrixa a következő, ún. Jacobi-mátrix:

$$\mathbf{D}_{\mathbf{f},\mathbf{x}} = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(x_1, x_2, \ldots, x_n)}(\mathbf{x}) = \frac{\partial f_1}{\partial x_1}(\mathbf{x})\frac{\partial f_1}{\partial x_2}(\mathbf{x})\frac{\partial f_1}{\partial x_n}(\mathbf{x})\frac{\partial f_2}{\partial x_1}(\mathbf{x})\frac{\partial f_2}{\partial x_2}(\mathbf{x})\frac{\partial f_2}{\partial x_n}(\mathbf{x})\frac{\partial f_m}{\partial x_1}(\mathbf{x})\frac{\partial f_m}{\partial x_2}(\mathbf{x})$$

Bizonyítás. Ha $\mathbf{f}$ differenciálható, akkor a definícióbeli határérték akkor is fönnáll, ha $\mathbf{h}$ speciális módon tart a nullvektorhoz, például ha $\mathbf{h} = t\mathbf{e}_j$, és $t \to 0$. Ekkor

$$\lim_{t\to 0} \frac{\mathbf{f}(\mathbf{x} + t\mathbf{e}_j) - \mathbf{f}(\mathbf{x}) - D_{\mathbf{f},\mathbf{x}}(t\mathbf{e}_j)}{|t|} = \mathbf{0}.$$

Az $\mathbf{f}$ függvény i-edik koordinátafüggvénye f_i, a $D_{\mathbf{f},\mathbf{x}}(t\mathbf{e}_j)$ vektor i-edik koordinátája $\mathbf{e}_i^\mathsf{T} D_{\mathbf{f},\mathbf{x}}(t\mathbf{e}_j)$. Ennek alapján

$$\lim_{t\to 0} \frac{f_i(\mathbf{x}+t\mathbf{e}_j) - f_i(\mathbf{x}) - \mathbf{e}_i^\mathsf{T} D_{\mathbf{f},\mathbf{x}}(t\mathbf{e}_j)}{|t|} = 0.$$

Ez a határérték viszont már egy egyváltozós függvény deriváltja, ami nem más, mint az f_i függvény j-edik parciális deriváltja, ugyanis átrendezve az egyenlőséget és t előjelével is osztva kapjuk, hogy

$$\lim_{t\to 0} \frac{f_i(\mathbf{x}+t\mathbf{e}_j) - f_i(\mathbf{x})}{t} = \mathbf{e}_i^\mathsf{T} D_{\mathbf{f},\mathbf{x}}\mathbf{e}_j, \text{ azaz } \mathbf{e}_i^\mathsf{T} D_{\mathbf{f},\mathbf{x}}\mathbf{e}_j = \frac{\partial f_i}{\partial x_j}(\mathbf{x}).$$

Ez bizonyítja állításunkat. [QED]

- A gyakorlatban az $\mathbb{R}^n \to \mathbb{R}$ függvények, vagyis az n-változós skalárértékű függvények esetén az egyetlen sorból álló Jacobi-mátrix helyett annak vektoralakját használják, melyet gradiensvektornak neveznek, és ∇f-fel jelölnek.
- Hasonlóképp, mivel az $\mathbb{R} \to \mathbb{R}^n$ függvények Jacobi-mátrixa egyetlen oszlopból áll, gyakran használják annak vektoralakját. Ha például egy $\mathbf{r} : \mathbb{R} \to \mathbb{R}^3; t \mapsto \mathbf{r}(t)$ függvény a térben mozgó tárgy mozgását az idő függvényében írja le, e vektor épp a mozgás sebességvektora.

1.3. Példa (Jacobi-mátrix kiszámítása) Határozzuk meg az alábbi függvények egy általános ponthoz és a megadott ponthoz tartozó Jacobi-mátrixát!

1. $f(x,y) = x^2y - xy^3 + 1$, $(x,y) = (0,1)$.
2. $\mathbf{f}(x,y) = (-x^3/2 + y^3/8, x + y)$, $(x,y) = (1,1)$.
3. $\mathbf{r}(t) = (t^3, t^2, t)$, $t = 2$.
4. $\mathbf{f}(x_1,x_2,x_3) = (2x_1 + 3x_2, x_1 - x_2 - x_3)$, $(x_1,x_2,x_3) = (1,2,0)$.

Megoldás

1. $f(x,y) = x^2y - xy^3$, parciális deriváltjai $\frac{\partial}{\partial x} f(x,y) = 2xy - y^3$, $\frac{\partial}{\partial y} f(x,y) = x^2 - 3xy^2$. A deriváltleképezés mátrixa, azaz a Jacobi-mátrix itt

$$2xy - y^3 x^2 - 3xy^2$$

E mátrix vektor alakja, azaz a gradiensvektor

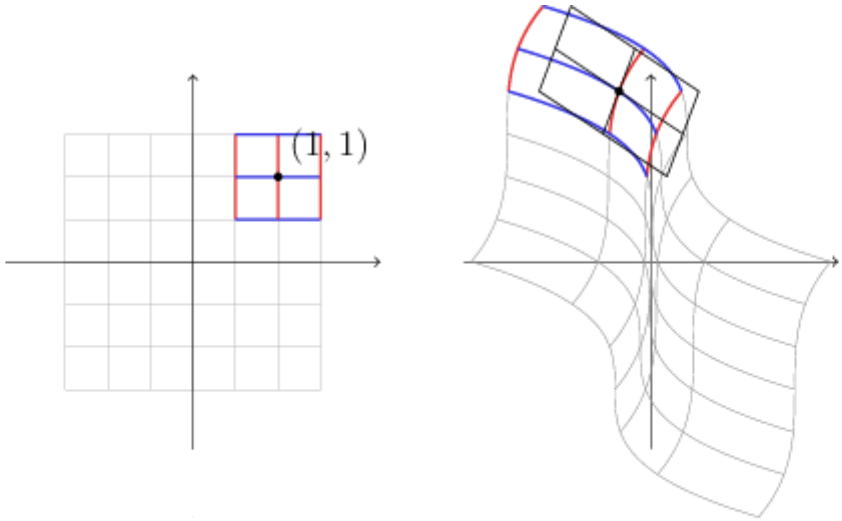
$$\nabla f(x,y) = (2xy - y^3, x^2 - 3xy^2).$$

Ennek értéke a $(0,1)$ helyen $\nabla f(0,1) = (-1,0)$, illetve a Jacobi-mátrix e helyen $[-1\ 0]$.

2.Az $\mathbf{f}(x,y) = (-x^3/2 + y^3/8, x+y)$ függvény Jacobi-mátrixa és annak értéke a megadott $(x,y) = (1,1)$ pontban

$$-\frac{3}{2}x^2\frac{3}{8}y^211, \text{ illetve } -\frac{3}{2}\frac{3}{8}11.$$

Például az első sor első eleme $\frac{\partial}{\partial x}(-x^3/2 + y^3/8) = -\frac{3}{2}x^2$. Az $\mathbf{f}$ függvény deriváltleképezésének, vagyis Jacobi-mátrixának hatását szemlélteti a 3 és a 2 ábra.



3. ábra. A bal ábra az $\mathbf{f}(x,y) = (-x^3/2 + y^3/8, x+y)$ függvény értelmezési tartományán megadott rácsot, és annak egy kis 2×2-es részét mutatja, melynek középpontja az $(1,1)$ pont. Az alsó ábra egyrészt halványan jelöli e rács és színesen a kiemelt rács képét, valamint az $(1,1)$ ponthoz tartozó deriváltleképezés hatását e kiemelt rácson.

3.Az $\mathbf{r}(t) = (t^3, t^2, t)$ függvény Jacobi-mátrixa

$$3t^22t1, \text{ ami a } t = 2 \text{ helyen } 1241.$$

A térben mozgó pont (test) mozgásának leírására is $\mathbb{R} \to \mathbb{R}^3$ függvényt használunk. Ha e függvény egy ilyen mozgást ír le, akkor sebességvektora egy tetszőleges pontban

$$\dot{\mathbf{r}}(t) = (3t^2, 2t, 1),$$

a $t = 2$ paraméterhez tartozó pontban $\dot{\mathbf{r}}(2) = (12, 4, 1)$.

4.Az utolsó példa fontos állítást szemléltet, nevezetesen azt, hogy egy lineáris leképezés deriváltja minden $\mathbf{x}$ helyen megegyezik magával a leképezéssel, azaz a deriváltja önmaga. Világos, hogy a megadott leképezés egy lineáris leképezés, melynek mátrixszorzatos alakja:

$$\mathbf{f}(x_1, x_2, x_3) = 2301 - 1 - 1x_1x_2x_3.$$

Ennek Jacobi-mátrixa valóban bármely (x_1, x_2, x_3) helyen

$$2301 - 1 - 1,$$

ugyanis az i -edik koordinátafüggvény j -edik parciális deriváltja épp az együtthatómátrix i -edik sor-, j -edik oszlopbeli eleme, azaz egy konstans. Így minden helyen e mátrix lesz a Jacobi-mátrix, speciálisan az $(x_1, x_2, x_3) = (1, 2, 0)$ helyen is.

1.4. Példa (Függvényérték becslése Jacobi-mátrixszal) Ismerjük egy differenciálható függvény értelmezési tartományának egy pontjához tartozó Jacobi-mátrixát és a függvényértéket ugyan ebben a pontban. Becsüljük meg a függvény értékét egy e ponthoz közeli helyen az alábbi adatok ismeretében!

1. $f(0,1) = 1$, $\mathbf{D}_{f,(0,1)} = [-1 \quad 0]$, $(x, y) = (-0.05, 1.1)$,
2. $\mathbf{f}(1,1) = (-\frac{3}{8}, 2)$, $\mathbf{D}_{\mathbf{f},(1,1)} = -3/23/811$, $(x, y) = (0.8, 1.1)$.

Mennyire lennének jók e becslések, ha a függvények az előző feladatbeli 1. és 2. függvényei lennének?

Megoldás

A függvény megváltozásának becsléséhez az $\mathbf{f}(\mathbf{x} + \mathbf{h}) - \mathbf{f}(\mathbf{x})$ értéket kell megbecsülni. A differenciálhatóság definíciója szerint erre a $\mathbf{D}_{\mathbf{f},\mathbf{x}}\mathbf{h}$ mennyiség alkalmas, ha a függvény differenciálható az $\mathbf{x}$ pontban. Eszerint tehát

$$\mathbf{f}(\mathbf{x} + \mathbf{h}) \approx \mathbf{f}(\mathbf{x}) + \mathbf{D}_{\mathbf{f},\mathbf{x}}\mathbf{h}.$$

E képletet felhasználva az alábbi megoldásokra jutunk:

1.E feladatban $\mathbf{h} = (-0.05, 0.1)$, így a függvény megváltozása a

$$\mathbf{D}_{f,(0,1)}\mathbf{h} = -10 - 0.050.1 = 0.05$$

értékkel becsülhető, tehát a függvény értéke

$$f(\mathbf{x}+\mathbf{h}) = f(-0.05, 1.1) \approx f(0,1) + \mathbf{D}_{f,(0,1)} - 0.050.1 = 1.05,$$

azaz $f(-0.05, 1.1) \approx 1.05$. Ha f az előző 1. feladatbeli függvény, azaz $f(x,y) = x^2y - xy^3 + 1$, akkor a pontos érték $f(-0.05, 0.1) = 1.0693$.

2.Itt $\mathbf{h} = (-0.2, 0.1)$, így a függvény megváltozása a

$$\mathbf{D}_{\mathbf{f},(1,1)}\mathbf{h} = -\frac{3}{2}\frac{3}{8}11 - 0.20.1 = \frac{3}{2}\cdot\frac{2}{10} + \frac{3}{8}\cdot\frac{1}{10} - \frac{2}{10} + \frac{1}{10} = 0.3375 - 0.1$$

értékkel becsülhető, tehát a függvény értéke $\mathbf{f}(0.8, 1.1) \approx \mathbf{f}(1,1) + (0.3375, -0.1) = (-0.0375, 1.9)$. Ha $\mathbf{f}$ az előző 2. feladatbeli függvény, azaz $\mathbf{f}(x,y) = (-x^3/2 + y^3/8, x+y)$, akkor a pontos érték $f(0.8, 1.1) = (-0.089625, 1.9)$.

Jacobi-determináns és az integrál transzformációja

A 2- és 3-dimenziós tér leírására leggyakrabban használt koordinátarendszerek közötti váltás a többváltozós integrálok kiszámításában fontos szerepet kap. Az a kérdés, hogy az integrálközelítő összegben szereplő „téglányoknak” mennyi a mértékük. E szakasz kalkulus-előismereteket igényel.

Felidézzük a síkbeli polárkoordináta-rendszernek, a térbeli henger- és gömbi koordinátarendszereknek a derékszögű koordinátarendszerrel való kapcsolatát:

(a) Polár	*(b)* Henger	*(c)* Gömbi
$x = r\cos\vartheta$	$x = r\cos\vartheta$	$x = \rho\sin\varphi\cos\vartheta$
$y = r\sin\vartheta$	$y = r\sin\vartheta$	$y = \rho\sin\varphi\sin\vartheta$
	$z = m$	$z = \rho\cos\varphi$

A felsorolt változók jelentése: r az xy-síkban az origótól való távolság, ρ a térben az origótól való távolság, ϑ az x-tengely pozitív felével bezárt szög az xy-síkban, φ a z-tengely pozitív felével bezárt szög.

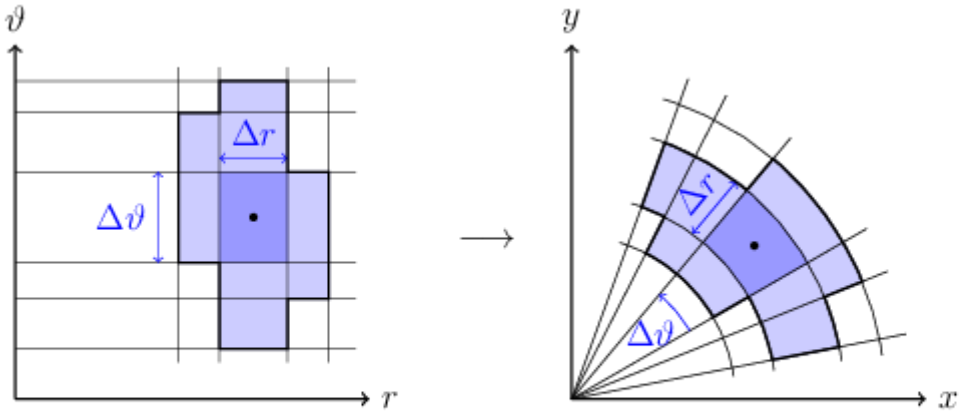
Jacobi-determinánsnak nevezzük egy $\mathbb{R}^n \to \mathbb{R}^n$ függvény deriváltleképezésének determinánsát.

A síkbeli polárkoordináta-rendszerről a derékszögűre való áttérés egy $\mathbb{R}^2 \to \mathbb{R}^2; (r,\vartheta) \mapsto (x,y)$ függvény, melyet a fönti (a)-beli képletek

definiálnak. Ennek deriváltleképezése, pontosabban a leképezés $\mathbf{D}$ mátrixa (szokás Jacobi-mátrixnak is hívni), és annak determinánsa, a Jacobi-determináns:

$$\mathbf{D} = \frac{\partial x}{\partial r}\frac{\partial x}{\partial \vartheta}\frac{\partial y}{\partial r}\frac{\partial y}{\partial \vartheta} = \cos\vartheta - r\sin\vartheta \sin\vartheta r\cos\vartheta \qquad |\mathbf{D}| = \cos\vartheta - r\sin\vartheta \sin\vartheta r\cos\vartheta = r.$$

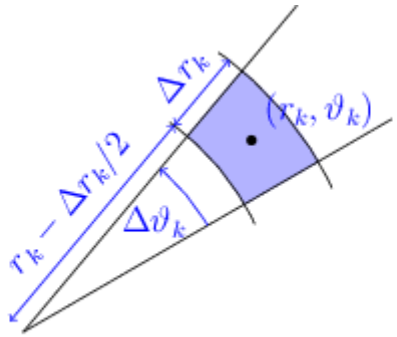
Az, hogy a Jacobi-determináns értéke r , azt jelenti, hogy egy „kicsiny” $\Delta r \times \Delta\vartheta$ méretű téglány - melynek területe $\Delta r \Delta\vartheta$ - a transzformáció után, azaz a polárkoordináta-rendszerben „nagyjából” r -szerese lesz az eredetinek, azaz $r\Delta r\Delta\vartheta$, ahol r a téglány egy pontjának origótól való távolsága. Ezt a leképezést a 4 ábrával szemléltetjük.



4. ábra. A síkbeli polárkoordinátarendszerre való áttérést megadó leképezés szemléltetése egy téglányokból álló tartomány képének ábrázolásával.

Az r -szereződés geometriailag is könnyen igazolható, ahogy azt az 5 ábra mutatja. Kiszámoljuk egy polár-rendszerbeli téglány területét. Ez két körcikk területének különbsége. A nagyobbik sugara $r_k + \Delta r_k/2$, a határoló ív hossza $(r_k + \Delta r_k/2)\Delta\vartheta_k$, így területe $\frac{1}{2}(r_k + \Delta r_k/2)^2\Delta\vartheta_k$. Hasonlóan kiszámolva a kisebbik körcikk területét, majd kivonva a nagyobbikéból kapjuk, hogy a téglány ΔA_k területe

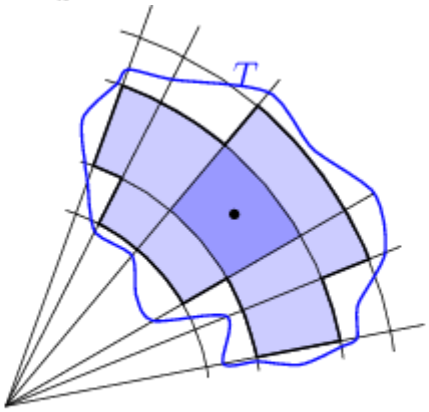
$$\Delta A_k = \frac{1}{2}\left(r_k + \frac{\Delta r_k}{2}\right)^2 \Delta\vartheta_k - \frac{1}{2}\left(r_k - \frac{\Delta r_k}{2}\right)^2 \Delta\vartheta_k = r_k \Delta r_k \Delta\vartheta_k.$$



5. ábra. A síkbeli polárkoordinátarendszer téglányának területe $r_k \Delta r_k \Delta \vartheta_k$.

Eszerint egy T tartományon értelmezett $f(r, \vartheta)$ függvény integrálközelítő összege és annak határértéke, amint a legnagyobb átmérőjű téglány átmérője tart 0-hoz (ld. 6 ábra):

$$\sum_k f(r_k, \vartheta_k) \Delta A_k = \sum_k f(r_k, \vartheta_k) r_k \Delta r_k \Delta \vartheta_k \to \int_T f(r, \vartheta) r \, \mathrm{d}r \, \mathrm{d}\vartheta.$$



6. ábra. Egy T tartományba eső téglányok, és a k-adik téglány kiemelve.

A két térbeli koordinátarendszerre való áttérés hasonló módon való megértését és a leképezések elképzelését már az Olvasóra hagyjuk, de a leképezések deriváltjának determinánsát még fölírjuk. A hengerkoordináták esetén az $(r, \vartheta, m) \mapsto (x, y, z)$ leképezésre ez

$$|\mathbf{D}| = \frac{\partial x}{\partial r}\frac{\partial x}{\partial \vartheta}\frac{\partial x}{\partial m}\frac{\partial y}{\partial r}\frac{\partial y}{\partial \vartheta}\frac{\partial y}{\partial m}\frac{\partial z}{\partial r}\frac{\partial z}{\partial \vartheta}\frac{\partial z}{\partial m} = \cos\vartheta - r\sin\vartheta 0 \sin\vartheta r\cos\vartheta 0 0 0 1 = r.$$

A gömbi koordinátarendszer esetén a leképezés $(\rho, \varphi, \vartheta) \mapsto (x, y, z)$, amelynek Jacobi-determinánsa:

$$\frac{\partial x}{\partial \rho}\frac{\partial x}{\partial \varphi}\frac{\partial x}{\partial \vartheta}\frac{\partial y}{\partial \rho}\frac{\partial y}{\partial \varphi}\frac{\partial y}{\partial \vartheta}\frac{\partial z}{\partial \rho}\frac{\partial z}{\partial \varphi}\frac{\partial z}{\partial \vartheta} = \sin\varphi\cos\vartheta\rho\cos\varphi\cos\vartheta - \rho\sin\varphi\sin\vartheta\sin\varphi\sin\vartheta\rho\cos\varphi\sin\vartheta\rho$$

Így tehát az integrál kiszámításának képletei e három koordinátarendszerre:

$$\begin{aligned}
&\text{Polár:} && \iint_T f(r,\vartheta)\,\mathrm{d}A = \iint_T f(r,\vartheta)\,r\,\mathrm{d}r\,\mathrm{d}\vartheta \\
&\text{Henger:} && \iiint_T f(r,\vartheta,m)\,\mathrm{d}V = \iiint_T f(r,\vartheta,m)\,r\,\mathrm{d}m\,\mathrm{d}r\,\mathrm{d}\vartheta \\
&\text{Gömbi:} && \iiint_T f(\rho,\varphi,\vartheta)\,\mathrm{d}V = \iiint_T f(\rho,\varphi,\vartheta)\,\rho^2\sin\varphi\,\mathrm{d}\rho\,\mathrm{d}\varphi\,\mathrm{d}\vartheta.
\end{aligned}$$

Függvények kompozíciójának deriváltja

E paragrafusnak nem célja a függvényanalízis területére tartozó témák feldolgozása, de a többváltozós függvények kompozíciójának deriváltleképezése az egyváltozós függvények láncszabályához hasonló módon számolható, és erre érdemes egy pillantást vetnünk, mert a megoldást a deriváltleképezések kompozíciója, azaz a Jacobi-mátrixok szorzata adja.

Bizonyítás nélkül közöljük a következő tételt.

1.5. Tétel (Láncszabály) Legyen $\mathbf{f} : \mathbb{R}^k \to \mathbb{R}^m$, $\mathbf{g} : \mathbb{R}^n \to \mathbb{R}^k$ két függvény.
Ha $\mathbf{g}$ differenciálható az $\mathbf{x}$ helyen, és $\mathbf{f}$ a $\mathbf{g}(\mathbf{x})$ helyen,
akkor $\mathbf{f} \circ \mathbf{g}$ differenciálható az $\mathbf{x}$ helyen, és deriváltleképezése, illetve annak mátrixa:

$$D_{\mathbf{f}\circ\mathbf{g},\mathbf{x}} = D_{\mathbf{f},\mathbf{g}(\mathbf{x})} \circ D_{\mathbf{g},\mathbf{x}}, \quad \text{illetve} \quad \mathbf{D}_{\mathbf{f}\circ\mathbf{g},\mathbf{x}} = \mathbf{D}_{\mathbf{f},\mathbf{g}(\mathbf{x})}\mathbf{D}_{\mathbf{g},\mathbf{x}}.$$

1.6. Példa (Láncszabály) Írjuk fel a láncszabály általános képleteit a megadott függvénytípusokra, az összetett függvény deriváltját pedig a láncszabállyal és behelyettesítéssel is számítsuk ki!

1. $f : (x,y) \mapsto x^2 - y$, $\mathbf{g} : u \mapsto (u^2 + u, u - 1)$, $u = 1$.
2. $\mathbf{f} : \mathbb{R} \to \mathbb{R}^2; x \mapsto (x^2, x-1)$, $g : \mathbb{R}^2 \to \mathbb{R}; (u,v) \mapsto x = u^2 v$, $(u,v) = (1,2)$.
3. $\mathbf{f}(x,y) = (xy^2 - 1, x - y)$, $\mathbf{g}(u,v) = (u+1, u-v)$, $(u,v) = (0,1)$.

Megoldás

Az 1. esetben az f -hez, illetve $\mathbf{g}$-hez tartozó láncszabály általános alakja

$$\frac{\mathrm{d}f}{\mathrm{d}u} = \frac{\partial f}{\partial x}\frac{\partial f}{\partial y}\frac{\mathrm{d}g_1}{\mathrm{d}u}\frac{\mathrm{d}g_2}{\mathrm{d}u} = \frac{\partial f}{\partial x}\frac{\mathrm{d}g_1}{\mathrm{d}u} + \frac{\partial f}{\partial y}\frac{\mathrm{d}g_2}{\mathrm{d}u},$$

a függvények parciális deriváltjait kiszámolva és a helyet megadva

$$\frac{\mathrm{d}f}{\mathrm{d}u}(1) = 2x{-}1_{\mathbf{g}(1)=(2,0)}2u + 11_{u=1},$$

végül a behelyettesítést is elvégezve:

$$4 - 131 = 11.$$

Ugyanezt az eredményt kapjuk, ha a deriválás előtt elvégezzük a helyettesítést: $(f \circ \mathbf{g})(u) = (u^2+u)^2 - (u-1) = u^4 + 2u^3 + u^2 - u + 1$, ennek u szerinti deriváltja $4u^3 + 6u^2 + 2u - 1$, és ennek értéke az $u = 1$ helyen 11.

A 2. esetben $\mathbf{f} : \mathbb{R} \to \mathbb{R}^2$, $g : \mathbb{R}^2 \to \mathbb{R}$, így $\mathbf{f} \circ g : \mathbb{R}^2 \to \mathbb{R}^2$, és

$$\frac{\partial f_1}{\partial u}\frac{\partial f_1}{\partial v}\frac{\partial f_2}{\partial u}\frac{\partial f_2}{\partial v} = \frac{\mathrm{d}f_1}{\mathrm{d}x}\frac{\mathrm{d}f_2}{\mathrm{d}x}\frac{\partial g}{\partial u}\frac{\partial g}{\partial v} = \frac{\mathrm{d}f_1}{\mathrm{d}x}\frac{\partial g}{\partial u}\frac{\mathrm{d}f_1}{\mathrm{d}x}\frac{\partial g}{\partial v}\frac{\mathrm{d}f_2}{\mathrm{d}x}\frac{\partial g}{\partial u}\frac{\mathrm{d}f_2}{\mathrm{d}x}\frac{\partial g}{\partial v}$$

A megadott függvényekre és a helyettesítendő értékeket is megadva:

$$2x1_{x=g(1,2)=2}2uvu^2{}_{u=1,v=2} = 4141 = 16441.$$

Behelyettesítés után a függvény $(u,v) \mapsto (u^4v^2, u^2v - 1)$, aminek deriváltja az $(u,v) = (1,2)$ helyen

$$4u^3v^2 2u^4 v 2uvu^2{}_{(1,2)} = 16441,$$

ami természetesen megegyezik az előző eredménnyel.

Végül a 3. esetben az általános alak

$$\frac{\partial f_1}{\partial u}\frac{\partial f_1}{\partial v}\frac{\partial f_2}{\partial u}\frac{\partial f_2}{\partial v} = \frac{\partial f_1}{\partial x}\frac{\partial f_1}{\partial y}\frac{\partial f_2}{\partial x}\frac{\partial f_2}{\partial y}\frac{\partial g_1}{\partial u}\frac{\partial g_1}{\partial v}\frac{\partial g_2}{\partial u}\frac{\partial g_2}{\partial v}.$$

A parciális deriváltakat kiszámolva és a helyettesítési értékeket is megadva kapjuk, hogy

$$\frac{\partial f_1}{\partial u}\frac{\partial f_1}{\partial v}\frac{\partial f_2}{\partial u}\frac{\partial f_2}{\partial v}_{(0,1)} = y^2 2xy1 - 1_{(1,-1)}101 - 1_{(0,1)}$$
$$= 1 - 21 - 1101 - 1 = -1201.$$

Itt fölhasználtuk, hogy $\mathbf{g}(0,1) = (1,-1)$. Ha a deriválás előtt elvégezzük a függvények kompozícióját, akkor ugyanerre az eredményre jutunk, ugyanis

$$(\mathbf{f}(\mathbf{g}(u,v)) = \big((u+1)(u-v)^2 - 1, v+1)\big),$$

aminek a deriváltmátrixa

$$(u-v)^2 + 2(u+1)(u-v) - 2(u+1)(u-v)01_{(0,1)} = -1201.$$

1.2 Elsőrendű lineáris differencia- és differenciálegyenletek

Bár a differencia- és differenciálegyenletek külön résztudományai a matematikának, nem részei a lineáris algebrának, a gyakorlati alkalmazásokban közöttük rendkívüli jelentőségűek a lineárisak. Ezek elmélete viszont tekintélyes részben lineáris algebrai eszközökre épül, egyúttal növelve ezen eszközök fontosságát.

Legyen adva az $\mathbf{A} \in \mathbb{T}^{n\times n}$ mátrix, valamint az $\mathbf{x}_0 \in \mathbb{T}^n$, és az $\mathbf{x}(t_0) \in \mathbb{T}^n$ vektor. Tekintsük az alábbi két egyenletet:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k,\ k = 0,1,2,\ldots, \tag{1.1}$$
$$\mathbf{x}'(t) = \mathbf{A}\mathbf{x}(t),\ t > t_0. \tag{1.2}$$

Az $\mathbf{A}$ mátrix Jordan-féle normálalakja segítségével meg fogjuk vizsgálni ezek aszimptotikus viselkedését.

Az (1) egyenletből világos, hogy $\mathbf{x}_k = \mathbf{A}^k\mathbf{x}_0$ minden nemnegatív egész k -ra. Továbbá tudjuk azt is, hogy ha $\mathbf{A} = \mathbf{C}\mathbf{J}\mathbf{C}^{-1}$, ahol $\mathbf{J}$ az $\mathbf{A}$ Jordan-féle normálalakja, akkor

$$\mathbf{x}_k = \mathbf{C}\mathbf{J}^k\mathbf{C}^{-1}\mathbf{x}_0,\ k = 0,1,2,\ldots$$

Itt $\mathbf{C} = [\mathbf{c}_1 \ldots \mathbf{c}_n]$ az általánosított sajátvektorok mátrixa. Inverzének sorvektoraira is szükségünk lehet: legyen $(\mathbf{C}^{-1})^{\mathsf{T}} = [\mathbf{d}_1 \ldots \mathbf{d}_n]$. Ha $\mathbf{J}$ diagonális, akkor tudjuk, hogy $\mathbf{x}_0$ előáll a sajátvektorok lineáris kombinációjaként, azaz $\mathbf{x}_0 = \sum_{i=1}^n b_i\mathbf{c}_i$. Mindezeket figyelembe véve, igaz a következő tétel:

1.7. Tétel (Differenciaegyenlet megoldása diagonalizálható esetben)
Ha $\mathbf{A}$ diagonalizálható, azaz $\mathbf{J} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, akkor a fenti jelölésekkel

$$\mathbf{x}_k = \sum_{i=1}^{n} b_i \lambda_i^k \mathbf{c}_i \tag{1.3}$$

$$= \sum_{i=1}^{n} \lambda_i^k \mathbf{c}_i \mathbf{d}_i^{\mathsf{T}} \mathbf{x}_0. \tag{1.4}$$

Ebből adódik, hogy ha $|\lambda_1| > |\lambda_i|$ minden $i > 1$ esetén, akkor

$$\lim_{n\to\infty} \frac{1}{\lambda_1^n} \mathbf{x}_k = \mathbf{c}_1 \mathbf{d}_1^{\mathsf{T}} \mathbf{x}_0. \tag{1.5}$$

Bizonyítás. A (3) és a (4) képletek az $\mathbf{x}_k = \mathbf{A}^k \mathbf{x}_0$ és
az $\mathbf{x}_k = \mathbf{C}\mathbf{J}^k\mathbf{C}^{-1}\mathbf{x}_0$ összefüggésekből azonnal adódnak, míg (5) a (4) azonnali következménye. [QED]

1.8. Példa Legyen

$$\mathbf{A} = 10501/20001/6.$$

Határozzuk meg az $\mathbf{x}_k = \mathbf{A}^k \mathbf{x}_0$ vektort, ha $\mathbf{x}_0 = (a, b, c)$ és annak végtelenbeli határértékét! Hogyan számolunk, ha csak $\lim_{k\to\infty} \mathbf{x}_k$ a kérdés?

Megoldás

Az $\mathbf{A}$ mátrix sajátértékei, sajátvektorai:

$$\lambda_1 = 1, \quad (1, 0, 0)$$
$$\lambda_2 = \frac{1}{2}, \quad (0, 1, 0)$$
$$\lambda_3 = \frac{1}{6}, \quad (1, 0, -\frac{1}{6})$$

Ebből

$$\mathbf{C} = 10101000 - \frac{1}{6}, \quad \mathbf{J}^k = 1000\frac{1}{2^k}000\frac{1}{6^k}, \quad \mathbf{C}^{-1} = 10601000 - 6,$$

ahonnan

$$\mathbf{x}_k = \mathbf{A}^k\mathbf{x}_0 = \mathbf{C}\mathbf{J}^k\mathbf{C}^{-1}\mathbf{x}_0 = a + (6 - \frac{1}{6^{k-1}})c\frac{b}{2^k}\frac{c}{6^k}.$$

Egy megjegyzés a fenti szorzat kiszámításához: az $\mathbf{y} = \mathbf{C}^{-1}\mathbf{x}_0$ szorzat mátrixinvertálás helyett a $\mathbf{C}\mathbf{y} = \mathbf{x}_0$ egyenletrendszer megoldásával gyorsabban megkapható! Innen

$$\lim_{k\to\infty} \mathbf{x}_k = a + 6c00.$$

Ha csak e határérték a kérdés, használhatjuk az (5) képletet. Itt $\lambda_1 = 1$ miatt

$$\lim_{k\to\infty} \mathbf{x}_k = \lim_{k\to\infty} \frac{1}{\lambda_1^k}\mathbf{x}_k = \mathbf{c}_1\mathbf{d}_1^{\mathsf{T}}\mathbf{x}_0 = 100[1\ 0\ 6]abc = a + 6c00,$$

ahol $\mathbf{d}_1$ a $\mathbf{C}^{-1}$ mátrix első sora. (Ehhez sincs szükség az egész inverzmátrix kiszámítására.)

Ha $\mathbf{J}$ nem diagonális, akkor a Jordan-féle normálalakot kell hatványozni, amihez csak a normálblokkok hatványozása szükséges.

1.9. Példa Legyen

$$\mathbf{A} = 120014001.$$

Határozzuk meg az $\mathbf{x}_k = \mathbf{A}^k\mathbf{x}_0$ vektort, ha $\mathbf{x}_0 = (1, 2, 1)$.

Megoldás

Meghatározva az $\mathbf{A}$ mátrix Jordan-féle alakját, kapjuk, hogy

$$\mathbf{A} = 800040001110011001\frac{1}{8}000\frac{1}{4}0001.$$

Innen

$$\mathbf{x}_k = \mathbf{A}^k\mathbf{x}_0 = 800040001110011001^k\frac{1}{8}000\frac{1}{4}0001121 = 4k^2 + 14k + 21$$

Itt fölhasználtuk, hogy

$$110011001^k = 1k\frac{k(k-1)}{2}01k001.$$

A homogén differenciálegyenlet-rendszerek megoldása kísértetiesen hasonlít az előzőkhöz, de itt az együtthatómátrix hatványa helyett exponenciális függvénye játssza a főszerepet.

Miután $(e^{\mathbf{A}t})' = \mathbf{A}e^{\mathbf{A}t}$, ezért azonnal adódik, hogy a (2) differenciálegyenlet-rendszer egy megoldása

$$\mathbf{x}(t) = e^{\mathbf{A}(t-t_0)}\mathbf{x}_0,$$

ahol $\mathbf{x}_0 = \mathbf{x}(t_0)$ a kezdeti feltétel. Hasonlóan az előzőkhöz, ha $\mathbf{A} = \mathbf{C}\mathbf{J}\mathbf{C}^{-1}$, ahol $\mathbf{J}$ az $\mathbf{A}$ Jordan-féle normálalakja, akkor

$$\mathbf{x}(t) = \mathbf{C}e^{\mathbf{J}(t-t_0)}\mathbf{C}^{-1}\mathbf{x}_0. \tag{1.6}$$

1.10. Tétel (Differenciálegyenlet-rendszer megoldása diagonalizálható esetben) Ha $\mathbf{A}$ diagonalizálható, azaz $\mathbf{J} = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, továbbá $\mathbf{C} = [\mathbf{c}_1 \ldots \mathbf{c}_n]$ a sajátvektorok mátrixa, és $(\mathbf{C}^{-1})^{\mathsf{T}} = [\mathbf{d}_1 \ldots \mathbf{d}_n]$, akkor

$$\mathbf{x}(t) = \sum_{i=1}^{n} e^{(t-t_0)\lambda_i}\mathbf{c}_i\mathbf{d}_i^{\mathsf{T}}\mathbf{x}_0.$$

Továbbá, ha $\lambda_1 > |\lambda_i|$ minden $i > 1$ esetén, akkor

$$\lim_{t\to\infty} e^{-t\lambda_1}\mathbf{x}(t) = e^{-t_0\lambda_1}\mathbf{c}_1\mathbf{d}_1^{\mathsf{T}}\mathbf{x}_0.$$

Bizonyítás. A bizonyítás első felel a (6) mátrixegyenlet kifejtése, míg a második fele az exponenciális függvény monoton növekvő voltának következménye. [QED]

1.11. Példa Oldjuk meg az

$$\mathbf{x}'(t) = 120014001\mathbf{x}(t), \quad \mathbf{x}_0 = \mathbf{x}(0) = 121$$

lineáris differenciálegyenlet-rendszert.

Megoldás

A megoldáshoz fölhasználhatjuk az $\mathbf{A}$ mátrixnak a 1.9 példában megadott fölbontását. Most $t_0 = 0$, így

$$\mathbf{x}(t) = \mathbf{C}e^{\mathbf{J}t}\mathbf{C}^{-1}\mathbf{x}_0 = 800040001e^t1t\frac{t^2}{2}01t001\frac{1}{8}000\frac{1}{4}0001121 = e^t(2t+1)^24t+21.$$

Itt fölhasználtuk, hogy

$$\exp(t\lambda 100\lambda 100\lambda) = e^{\lambda t}1t\frac{t^2}{2}01t001.$$

1.12. Tétel (A megoldás egyértelműsége) A (2) differenciálegyenlet-rendszernek csak egyetlen folytonosan deriválható megoldása van a $[t_0, t_1]$ intervallumon, mely kielégíti az $\mathbf{x}(t_0) = \mathbf{x}_0$ kezdeti feltételt.

Bizonyítás. Legyen $\mathbf{x}(t)$ és $\mathbf{y}(t)$ két megoldás. Megmutatjuk, hogy különbségük, azaz a $\mathbf{d}(t) = \mathbf{x}(t) - \mathbf{y}(t)$ függvény azonosan 0, azaz az

$$m = \max\{\, \|\mathbf{d}(t)\| \mid t_0 \leqslant t \leqslant t_1 \,\}$$

jelöléssel $m = 0$. A

$$\mathbf{d}(t) = \mathbf{x}(t) - \mathbf{y}(t) = \int_{t_0}^{t} \mathbf{x}'(\tau) - \mathbf{y}'(\tau)\mathrm{d}\tau = \int_{t_0}^{t} \mathbf{A}(\mathbf{x}(\tau) - \mathbf{y}(\tau))\mathrm{d}\tau = \int_{t_0}^{t} \mathbf{A}\mathbf{d}(\tau)\mathrm{d}\tau$$

összefüggést rekurzívan alkalmazva kapjuk, hogy

$$\mathbf{d}(t) = \mathbf{A}^k \int_{t_0}^{t}\int_{t_0}^{\tau_1}\int_{t_0}^{\tau_2}\cdots\int_{t_0}^{\tau_{k-1}} \mathbf{d}(\tau_k)\mathrm{d}\tau_k \ldots \mathrm{d}\tau_2\mathrm{d}\tau_1.$$

Innen kapjuk, hogy

$$m \leqslant m\|\mathbf{A}^k\|\frac{(t_1-t_0)^k}{k!} \leqslant m\|\mathbf{A}\|^k\frac{(t_1-t_0)^k}{k!}.$$

Ha k elég nagy, akkor $\|\mathbf{A}\|^k(t_1-t_0)^k/k! < 1$. Ezt és az előzőket összevetve kapjuk, hogy

$$0 \leqslant m\left(1 - \|\mathbf{A}\|^k\frac{(t_1-t_0)^k}{k!}\right) \leqslant 0,$$

azaz $m = 0$, amit bizonyítani akartunk. [QED]

1.3 Kombinatorika

Páratlanváros

Első példánk azt demonstrálja, hogy a lineáris algebra olyan elemi fogalmai is, mint a lineáris függetlenség, milyen nem triviális összefüggések megvilágítására képesek.

Páratlanváros ügyeit hatékonyan intézi. Minden feladatának irányítását bizottságokra bízza. Elkerülendő a szavazategyenlőség okozta bénult helyzeteket, törvénybe foglalták, hogy minden bizottságot csak páratlan számú taggal lehet létrehozni és működtetni. Ha két bizottság egy időben ülésezik, a közös tagok fele az egyik, másik fele a másik bizottság ülésén vesz részt két-két szavazati joggal. Hogy ez megvalósítható legyen, azt is törvénybe foglalták, hogy bármely két bizottságnak csak páros sok közös tagja lehet.

1.13. Állítás (Páratlanváros bizottságainak száma) Páratlanváros e feltételek mellett legfeljebb v bizottságot tud létrehozni, ha (közügyekkel foglalkozó) lakóinak száma v.

Ez meglepően kevésnek tűnik, ahhoz képest, hogy egy v elemű halmaznak $2^v - 1$ nem üres részhalmaza van.

Bizonyítás. Indexeljük a város lakóit 1-től v-ig, bizottságaik legyenek B_1, B_2,... B_b. Legyen $\mathbf{M}$ e halmazrendszer illeszkedési mátrixa, azaz sorai reprezentálják a város lakóit, oszlopai a bizottságokat, és legyen

$$m_{ij} = \begin{cases} 1, & \text{ha } i \in B_j, \\ 0, & \text{egyébként.} \end{cases}$$

Az $\mathbf{M}^\mathsf{T}\mathbf{M}$ mátrix $b \times b$-es, és i-edik sorának j-edik eleme a $B_i \cap B_j$ halmaz elemszámát adja, ami $i = j$ esetén páratlan, $i \neq j$ esetén páros. Mivel a feladatban csak a paritásokat figyeljük, elég a halmazok és metszeteik elemszáma helyett annak paritását nézni, azaz ha $\mathbf{M}$-et $\mathbb{F}_2$ fölötti mátrixnak tekintjük, $\mathbf{M}^\mathsf{T}\mathbf{M} = \mathbf{I}_b$. Eszerint $\mathrm{r}(\mathbf{M}^\mathsf{T}\mathbf{M}) = b$. Ebből következik, hogy $\mathrm{r}(\mathbf{M}) \geqslant b$, de mivel $\mathbf{M}$ sorainak száma b, ezért $\mathrm{r}(\mathbf{M}) = b$. Másrészt $\mathrm{r}(\mathbf{M}) \leqslant v$, hisz $\mathbf{M}$ egy $v \times b$-es mátrix, következésképp $b \leqslant v$. [QED]

A véges halmazrendszerek nyelvén fogalmazva: ha P egy v-elemű halmaz, és B_1, B_2,..., $B_b \subseteq P$ olyan páratlan elemű részhalmazok, melyek közül bármely kettő metszete páros, akkor $b \leqslant v$.

A $b \leqslant v$ becslés éles, amint azt az egyelemű halmazok esete mutatja, ekkor ugyanis bármely két részhalmaz metszete üres, és $b = v$.

Párosváros

Párosváros elégedetlen volt a Páratlanvárosbeli szabályokkal: csak kevés bizottság volt létrehozható, és nem tartották megnyugtatónak, hogy a kritikus eseteket is gyorsan eldöntik szavazással. Úgy határoztak, hogy legyen minden bizottságnak páros sok tagja, azaz kényes szavazategyenlőségek esetén vizsgálják tovább az ügyet, hogy megfontoltabb döntés születhessen. A másik szabályt viszont megtartották. E változtatás meglepő módon másik problémájukat is megoldotta.

1.14. Állítás (Párosváros bizottságainak száma) Párosváros legfeljebb $2^{\lfloor v/2 \rfloor} - 1$ bizottságot tud létrehozni, ha (közügyekkel foglalkozó) lakóinak száma v.

Bizonyítás. Indexeljük a város lakóit 1-től v-ig, bizottságaik legyenek B_i ($i = 1, 2 \ldots, b$), a B_i -hez tartozó $\mathbf{b}_i \in \mathbb{F}_2^v$ karakterisztikus vektort definiáljuk a következőképp:

$$[\mathbf{b}_i]_j = \begin{cases} 1, & \text{ha } j \in B_i, \ (j = 1, 2, \ldots, v), \\ 0, & \text{egyébként.} \end{cases}$$

Mivel két bizottság közös tagjainak száma páros, és tagjainak száma is páros, ezért $\mathbf{b}_i \cdot \mathbf{b}_j = 0$ minden i és j esetén. Így a $\mathbf{b}_i$ vektorok páronként merőlegesek egymásra. Másrészt azonban minden vektor önmagára is merőleges, így a $\mathbf{b}_1$, $\mathbf{b}_2$,..., $\mathbf{b}_b$ vektorok által kifeszített $\mathcal{W}$ altér bármely $\mathbf{x}$ és $\mathbf{y}$ vektorára

$$\mathbf{x} \cdot \mathbf{y} = (x_1\mathbf{b}_1 + \ldots + x_b\mathbf{b}_b) \cdot (y_1\mathbf{b}_1 + \ldots + y_b\mathbf{b}_b) = \sum_{i,j} x_i y_j \mathbf{b}_i \cdot \mathbf{b}_j = 0.$$

Eszerint a $\mathcal{W}$ altér minden vektora merőleges az altér minden vektorára.

A dimenziótétel szerint, ha $\mathcal{V}$ olyan euklideszi tér, hogy $\mathcal{V}^\perp = \{\mathbf{0}\}$, márpedig $\mathbb{F}_2^v$ a standard skaláris szorzattal ilyen, és $\mathcal{W} \leqslant \mathcal{V}$ egy tetszőleges altér, akkor

$$\dim \mathcal{V} = \dim \mathcal{W} + \dim \mathcal{W}^\perp.$$

Ennek azonnali következménye, hogy ha $\mathcal{W}$ olyan altér, melynek minden vektora merőleges az altér összes vektorára, azaz $\mathcal{W} \leqslant \mathcal{W}^\perp$, akkor

$$\dim \mathcal{W} \leqslant \frac{1}{2} \dim \mathcal{V}.$$

Ez abból adódik, hogy a dimenziótétel $\dim \mathcal{V} + \dim \mathcal{W} \geqslant 2 \dim \mathcal{W}$ szerint $\dim \mathcal{W} \leqslant \frac{v}{2}$. Így $2^{\lfloor v/2 \rfloor} - 1$ az altér nullvektortól különböző elemeinek száma tehát legföljebb $\lfloor v/2 \rfloor$. E becslés éles, hisz egy v elemű halmazból $\lfloor v/2 \rfloor$ pár képezhető, e párok összes nem üres részhalmazainak száma megegyezik a felső becsléssel. Mondjuk ezt kapjuk, ha minden bizottságnak házaspárok a tagjai, és mindenki házas (kivéve esetleg egyetlen embert, aki egyik bizottságba sem kerül be). [QED]

Fischer-egyenlőtlenség

Sok egyedre vonatkozó, és minden variációs lehetőség kipróbálását lehetővé nem tevő statisztikai kísérletek megtervezésének vizsgálata vezetett a következő kérdésre: hogyan lehet egy v-elemű halmazból azonos k-méretű részhalmazokat kiválasztani úgy, hogy bármely két elem azonos λ számú részhalmazban legyen benne. A Fischer-egyenlőtlenség szerint ez csak úgy lehetséges, ha a részhalmazok száma legalább v.

A Fischer-egyenlőtlenséget kissé általánosabb alakban bizonyítjuk. Tekintsük a v-elemű P halmaz részhalmazainak egy halmazát. E részhalmazokat blokkoknak is szokás hívni, míg P elemeit pontoknak. Azt mondjuk, hogy e blokkok 2-struktúrát alkotnak, ha P bármely két pontja pontosan $\lambda > 0$ számú blokkban van, és van legalább egy nem triviális blokk a rendszerben, azaz amelynek legalább 2 pontja van, de nem tartalmazza P összes pontját.

A Fischer-egyenlőtlenség eredetileg azonos méretű blokkokat tartalmazó 2-struktúrára vonatkozott, de e regularitási kikötés a tételből elhagyható.

1.15. Tétel Bármely 2-struktúra blokkjainak száma legalább annyi, mint pontjaié, azaz $b \geqslant v$.

A Páratlanvárosra vonatkozó kérdésben két részhalmaz mindegyikében szereplő pontok számát vizsgáltuk az $\mathbf{M}$ illeszkedési mátrix $\mathbf{M}^{\mathsf{T}}\mathbf{M}$ szorzatával. Most egy duális jellegű kérdést vizsgálunk, vagyis itt két pont mindegyikét tartalmazó blokkok számát figyeljük, ehhez az $\mathbf{M}\mathbf{M}^{\mathsf{T}}$ mátrixot kell vizsgálnunk.

Bizonyítás. Az előző alkalmazáshoz hasonlóan, jelöljük a 2-struktúra pontjait az 1-től v-ig terjedő egészekkel, a j-edik blokkot jelölje B_j, ahol $j = 1, 2, \ldots, b$. E struktúra illeszkedési mátrixa legyen $\mathbf{M}$, ahol

$$m_{ij} = \begin{cases} 1, & \text{ha } i \in B_j, \\ 0, & \text{egyébként.} \end{cases}$$

A mátrix i-edik sora megadja, hogy az i pont mely indexű blokkok eleme. Így

$$\mathbf{A} = \mathbf{M}\mathbf{M}^{\mathsf{T}} = r_1\lambda\lambda\lambda r_2\lambda\lambda\lambda r_v = \lambda\mathbf{J}_v + \operatorname{diag}(r_1 - \lambda, r_2 - \lambda, \ldots, r_v - \lambda),$$

ahol $\mathbf{J}_v$ a csupa 1-esből álló $v \times v$-es mátrix, és r_i az i pont foka.
Az $\mathbf{A}$ mátrixról megmutatjuk, hogy reguláris.

A $\mathbf{J}$ pozitív szemidefinit, ugyanis szimmetrikus és ha $\mathbf{x} \in \mathbb{R}^v$ egy tetszőleges nemzérus vektor, akkor $\mathbf{x}^{\mathsf{T}}\mathbf{J}_v\mathbf{x} = \sum_{i,j} x_i x_j = (\sum_i x_i)^2 \geqslant 0$.

Az $\mathbf{A}$ diagonális összetevőjének minden főátlóbeli eleme pozitív, ugyanis $r_i > \lambda$. Ha ugyanis pl. az i pontra $r_i = \lambda$ volna, akkor minden $j \neq i$ pont esetén az i-t tartalmazó blokkok tartalmaznák j-t is, vagyis minden blokk tartalmazná az összes pontot, vagyis nem létezne nem triviális blokk. Ha viszont $r_i - \lambda > 0$, akkor a diagonális mátrix pozitív definit, ugyanis

$$\mathbf{x}^{\mathsf{T}} \operatorname{diag}(r_1 - \lambda, r_2 - \lambda, \ldots, r_v - \lambda)\mathbf{x} = \sum_{i=1}^{v} (r_i - \lambda)x_i^2 > 0,$$

ha $\mathbf{x} \neq \mathbf{0}$. Egy pozitív definit és egy pozitív szemidefinit mátrix összege pozitív definit, pozitív definit mátrix pedig nem szinguláris, tehát $\mathbf{A}$ nem szinguláris, vagyis rangja v. Eszerint a $v \times b$ méretű $\mathbf{M}$ rangja v, akkor pedig $b \geqslant v$. [QED]

Fibonacci-sorozat

Bár Fibonacci a nyulak szaporodására vonatkozó kérdését csak példatári feladatnak gondolta, ráadásul a nyulak nem is e sorozat szerint szaporodnak, szerencsésen beletalált egy különösen érdekes témába. A róla elnevezett sorozat számtalan helyen megjelenik, a természet bizonyos növekedési folyamatainak leírásától (fillotaxis) informatikai alkalmazásokon (Fibonacci kereső technika) át a művészetekig.[1]

Fibonacci feladata a következőképp szól: a nősténynyulak szaporodása a következők szerint zajlik (a hímekről most ne essék szó, ők csak végzik a dolgukat). Minden felnőtt ($=$ ivarérett) nőstény havonta egy nőstény nyulat szül, és sose hal meg. A gyerek nyulak a második hónapra válnak felnőtté. Nézzük meg, hogy kezdődik a nyulak szaporodása 1 felnőtt nyúllal. Kezdő állapot vektora $(0, 1)$, az első koordináta a gyerekek, a második a felnőttek száma. A következő hónapokban rendre $(1, 1)$, $(1, 2)$, $(2, 3)$, $(3, 5)$,... lesz a nyulak száma. A szabály tehát az, hogy ha egy évben a gyerek és b felnőtt van, akkor a következőben b gyerek és $a + b$ felnőtt lesz, az azt követően $a + b$ gyerek és $a + 2b$ felnőtt. E vektorok képzési szabálya mátrixművelettel megkapható, ugyanis az $\mathbf{F}(a, b) = (b, a + b)$ egyenletből kapjuk, hogy $\mathbf{F} = 0111$.

A nyulak száma e három évben $a+b$, $a+2b$ és $2a+3b$, vagyis a nyulak száma minden évben az előző kettő összege. Ez a következő definícióhoz vezet.

A Fibonacci-sorozatot az $F_0 = 0$, $F_1 = 1$ kezdeti értékek és az $F_{n+1} = F_n + F_{n-1}$ rekurzív képlet definiálja. 1000-nél kisebb tagjai: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987[2]. A sorozat explicit alakban is fölírható. Két alakját is megadjuk, egyikben egy mátrixhatvány mellékátlóbeli elemei, másikban - igen meglepő módon - irracionális számok hatványai segítségével.

1.16. Tétel (Fibonacci-sorozat explicit alakjai)

$$F_n = (0111^n)_{1,2} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Bizonyítás.

Az első alak bizonyítása: A $\mathbf{F} = 0111$ mátrix hatványai mind Fibonacci számokból állnak, legalábbis az első néhányuk tanúsága szerint:

$$\mathbf{F} = 0111,\ \mathbf{F}^2 = 1112,\ \mathbf{F}^3 = 1223,\ \mathbf{F}^4 = 2335,\ \mathbf{F}^5 = 3558, \ldots$$

Teljes indukcióval könnyen igazolható, hogy

$$\mathbf{F}^n = F_{n-1}F_nF_nF_{n+1}, \quad n = 0, 1, 2, \ldots,$$

ugyanis az állítás $n = 1$ -re igaz ($n = 0$ -ra is az $F_{-1} = 1$ értékkel), és öröklődik n -ről $n+1$ -re:

$$\mathbf{F}^{n+1} = F_{n-1}F_nF_nF_{n+1}0111 = F_nF_{n-1} + F_nF_{n+1}F_n + F_{n+1} = F_nF_{n+1}F_{n+1}F_{n+2}.$$

Így $\mathbf{F}^n$ mellékátlóbeli elemei valóban F_n -nel egyenlők. Megjegyezzük, hogy a hatványozás az n bináris alakjából ismételt négyzetre emelésekkel gyorsan számolható. Nevezetesen ha n bináris alakjában a b_1 , b_2 ,..., b_k indexű jegyek az 1 -esek, akkor $\mathbf{F}^n = \mathbf{F}^{2^{b_1}}\mathbf{F}^{2^{b_2}} \ldots \mathbf{F}^{2^{b_k}}$, ami legföljebb $2\log_2 n$ mátrixszorzást igényel.

A második alak 1.bizonyítása: Mátrix hatványa a diagonális alakból még gyorsabban számolható, igaz itt már nem csak egészekkel kell számolni, viszont így megkapjuk a tételbeli második képletet is. $\mathbf{F}$ karakterisztikus polinomja $x^2 - x - 1$, melyből $\mathbf{F}$ sajátértékei $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{5})$ és a hozzájuk

tartozó sajátvektorok $\mathbf{x}_{1,2} = (1, \frac{1}{2}(1 \pm \sqrt{5}))$. Innen $\mathbf{F}^n$ sajátfelbontását használva kapjuk, hogy

$$\mathbf{F}^n = 11\frac{1+\sqrt{5}}{2}\frac{1-\sqrt{5}}{2}\frac{1+\sqrt{5}}{2}00\frac{1-\sqrt{5}}{2}^n 11\frac{1+\sqrt{5}}{2}\frac{1-\sqrt{5}}{2}^{-1}$$

ami az

$$11\frac{1+\sqrt{5}}{2}\frac{1-\sqrt{5}}{2}^{-1} = \frac{1}{\sqrt{5}}\frac{\sqrt{5}-1}{2}1\frac{1+\sqrt{5}}{2} - 1$$

behelyettesítése után a tételbeli képletet adja (elég csak a szorzatmátrix első sorának második elemét kiszámolni).

2.bizonyítás: Az előzőtől csak kissé eltérő megoldáshoz jutunk, ha észrevesszük, hogy

$$F_n F_{n+1} = \mathbf{F}^n 01.$$

Az $\mathbf{x}_1$ és $\mathbf{x}_2$ sajátvektorok bázist alkotnak $\mathbb{R}^2$-ben, így a $[0\ 1]$ vektor előáll azok lineáris kombinációjaként, azaz létezik olyan c_1 és c_2 konstans, hogy $[0\ 1] = c_1\mathbf{x}_1 + c_2\mathbf{x}_2$. Megoldjuk ezt az egyenletrendszert (ez itt az előző megoldásbeli mátrixinvertálásnak megfelelő lépés), a megoldás $c_1 = -c_2 = 1/\sqrt{5}$. Így fölhasználva, hogy $\mathbf{F}^n[0\ 1] = c_1\lambda_1^n\mathbf{x}_1 + c_2\lambda_2^n\mathbf{x}_2$, behelyettesítés után ezt kapjuk:

$$\mathbf{F}^n 01 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n 1\frac{1+\sqrt{5}}{2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n 1\frac{1-\sqrt{5}}{2}.$$

Itt csak az első koordinátát kiszámolva, a tételbeli állítást igazoltuk.

3.bizonyítás: Utolsó bizonyításunk igen szép lineáris algebrai gondolatra épül. Tekintsük az összes $s_{n+1} = s_n + s_{n-1}$ rekurzív összefüggést kielégítő sorozatot. Minden ilyen sorozatot egyértelműen megad első két eleme (s_0 és s_1), így e sorozatok egy 2-dimenziós vektorteret alkotnak. E térben olyan sorozatokat keresünk, melyek explicit módon is könnyen megadhatók. Ha találunk két ilyen független sorozatot, akkor azok lineáris kombinációjaként a Fibonacci sorozatot előállítva, arra is explicit alakot kapunk. Próbálkozzunk mértani sorozattal, tekintsük az 1, r, r^2,...sorozatot. A rekurzív összefüggés szerint $r^2 = r + 1$ (nem véletlenül ez épp az előző megoldásokban is megkapott karakterisztikus egyenlet). A rekurzív egyenlet az összes többi elemre is teljesül, hisz ebből $r^{n+1} = r^n + r^{n-1}$. A másodfokú egyenlet megoldásai épp az előző megoldásokban kapott

sajátértékek: $r_{1,2} = \frac{1}{2}(1 \pm \sqrt{5})$. Az 1, r_1, r_1^2,..., és az 1, r_2, r_2^2,... sorozatok lineárisan függetlenek. Az

$$(F_n) = (0, 1, 1, 2, 3, \dots) = c_1(1, r_1, r_1^2, r_1^3, r_1^4, \dots) + c_2(1, r_2, r_2^2, r_2^3, r_2^4, \dots)$$

lineáris kombináció konstansainak meghatározásához elég csak az első két-két koordináták összevetése, ahonnan épp az előző megoldásban kapott egyenletrendszerre jutunk, azaz $c_1 = -c_2 = 1/\sqrt{5}$, ami ismét a tételbeli összefüggést adja. [QED]

A lámpácskás játék

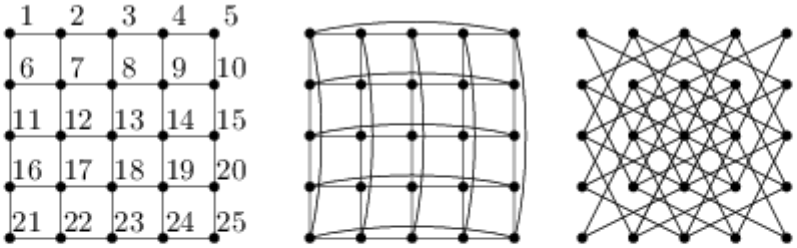
A 80-as évektől kezdve több változatban, egymástól részben függetlenül is többen kitaláltak és meg is valósítottak olyan játékokat, amelyek világítani is képes nyomógombokból álltak. A nyomógombok megnyomásukra megváltoztatták saját, és szomszédaik (vagy valamilyen egyéb módon definiált egyéb lámpák) állapotát, vagyis ha azok épp világítottak, akkor kialudtak, ha nem világítottak, fölgyulladtak.

A legnépszerűbbé egy „Lights Out!” nevű játék vált a 90-es évek végén, amely egy négyzetrácsra 5×5-ös alakban elhelyezett 25 gombból állt, és bármely gomb megnyomására rajta kívül a fölötte, alatta és mellette lévő gombok váltottak állapotukon. A feladvány az volt, hogy induláskor néhány lámpa égett, amiket le kellett kapcsolni úgy, hogy végül a 25 lámpa egyike se égjen. E játékot Mérő László találta ki, és 83-ban be is mutatta XL25 néven egy Nemzetközi Játékvásáron, de abból akkor nem lett termék. Azon a játékon volt egy olyan változat is, melynél egy gomb a tőle lóugrásnyira lévő lámpák állapotát változtatta. Ma a játék több verziója fut online formában az Interneten és okostelefonokon. A teljesség igénye nélkül néhányat felsorolunk az egyéb változatok közül:

- „Button Madness”, ahol a szomszédság a határon átnyúlik és a szemközti oldalon folytatódik, ez olyan, mintha a játékot egy tóruszon játszanánk,
- „Gamze”, ahol a lámpák rombuszalakban vannak elhelyezve,
- „Lights Out 2000”, ahol a lámpáknak nem két, hanem három állapotuk van (kikapcsolt, piros, zöld),
- „Lights Out Cube”, ahol a lámpák egy $3 \times 3 \times 3$-as kocka oldalain vannak,
- „Orbix”, ahol a lámpák egy dodekaéder csúcsaira vannak helyezve,
- „Merlin”, ami a hetvenes években jelent meg, 3×3-as táblán kellett játszani, és valószínűleg a legelső megjelent lámpás játék lehetett.

A játék mindegyikéhez hozzárendelhető egy gráf, melyben a csúcsok a gombok, és két csúcs akkor van összekötve, ha egyik megnyomására a másik megváltoztatja állapotát. A játék szabályai szerint minden csúcsra kéne rajzolnunk egy hurokélet is, mert minden gomb megnyomására a saját állapota is megváltozik, de az

egyszerűség kedvéért ettől eltekintünk. Ekkor a játék három változatának gráfja a 7. ábrán látható módon néz ki.



7. ábra. Három játékváltozat gráfja: *(a)* az eredeti változat (XL25, Lights Out!), *(b)* tórusz-változat (Button Madness), *(c)* a lóugrásos változat (XL25)

A továbbiakban csak az első változattal foglalkozunk, a többi hasonló módon vizsgálható. Először írjuk fel a gráf szomszédsági (adjacencia-) mátrixát. Ez egy 25×25-ös mátrix lesz. Jelölje $\mathbf{A}$. A gráf csúcsainak számozása a 7. (a) ábrán látható.

$$\mathbf{A} = \begin{bmatrix}
1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1
\end{bmatrix}$$

Világos, hogy a játékban egy gomb páros sokszori megnyomása olyan, mintha egyszer sem nyomtuk volna meg, míg páratlan sokszori megnyomása egy nyomással ekvivalens. Eszerint a nyomások számát modulo 2 számolhatjuk,

vagyis $\mathbb{F}_2$ elemeivel. Másrészt a fenti mátrix is tekinthető $\mathbb{F}_2$ fölötti mátrixnak, melynek i -edik oszlopa azt adja meg, hogy az i jelű gomb megnyomására mely lámpák állapota változik meg. Jelölje $\mathbf{x} \in \mathbb{F}_2^{25}$ azt a vektort, melynek x_i koordinátája akkor 1, ha az i gombot páratlan sokszor nyomtuk meg, és akkor 0, ha páros sokszor. E jelölésekkel $\mathbf{Ax}$ azt a vektort adja eredményül, melynek i -edik koordinátája akkor 1, ha az i gomb állapota az $\mathbf{x}$ vektor szerinti gombok megnyomása után megváltozik, és akkor 0, ha nem. Természetesen a számításokat $\mathbb{F}_2$ -ben végezzük. Eszerint, ha kezdetben a lámpák állapotát egy $\mathbf{b}$ vektor írja le ($b_i = 1$, ha az i lámpa ég, $b_i = 0$, ha nem), akkor e lámpák pontosan akkor kapcsolhatók le, ha van olyan $\mathbf{x}$ vektor, melyre $\mathbf{Ax} = \mathbf{b}$. Például ha minden lámpa ég, akkor az $\mathbf{Ax} = \mathbf{1}$ egyenletet kell megoldani, ahol $\mathbf{1} = (1, 1, \ldots, 1) \in \mathbb{F}_2^{25}$. Ehhez hozzuk $\mathbf{A}$-t redukált lépcsős alakra. E számolás elemi, bár kissé hosszadalmas (a komputer viszont gyorsan számol):

$$\mathbf{R} = \operatorname{rref}(\mathbf{A}) = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

A redukált lépcsős alakból a játékra vonatkozóan is több minden leolvasható:

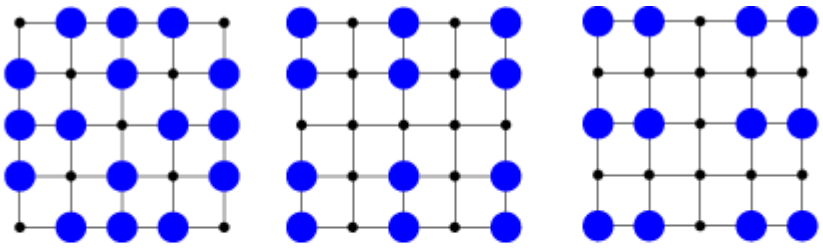
- Az $\mathbf{A}$ mátrix nem invertálható, tehát az $\mathbf{Ax} = \mathbf{b}$ egyenlet nem oldható meg minden $\mathbf{b}$ vektorra, tehát nem minden feladvány oldható meg.
- Az $\mathbf{A}$ rangja 23, tehát $\mathbf{A}$ magterének dimenziója $25 - 23 = 2$.
- Eszerint az $\mathbf{Ax} = \mathbf{0}$ homogén egyenlet megoldásai 2-dimenziós teret feszítenek ki. A megoldások elő is állíthatók a fenti alakból:

$$\mathbf{x} = s\mathbf{u} + t\mathbf{v}, \quad \text{ahol}$$
$$\mathbf{u} = (01110101011101110101011 0),$$
$$\mathbf{v} = (10101101010000010101101 01),$$

Ez az altér összesen négy vektorból áll, a nullvektorból, a fenti képletbeli két vektorból, és azok összegéből, azaz az

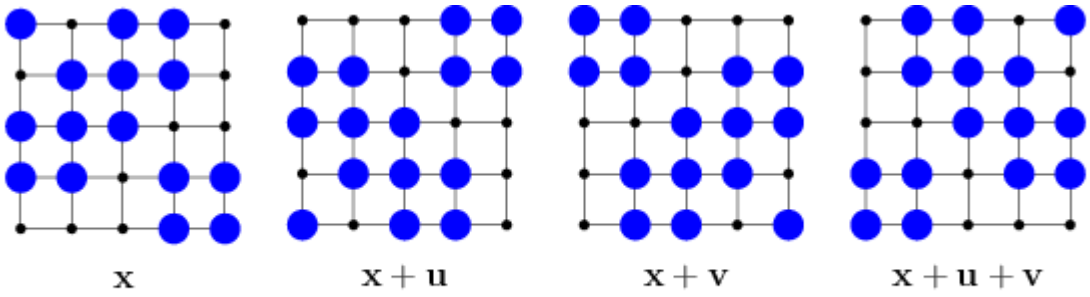
$$\mathbf{u} + \mathbf{v} = (11011000001101100000110 11)$$

vektorból. Ezek a vektorok tehát azokat a mintákat írják le, amelyek nem változtatják meg egyetlen lámpa állapotát sem. E három vektornak a 8 ábrán látható minták felelnek meg.



8. ábra. A nulltér elemei, azaz azok a minták, amelyek nem változtatják a lám állapotát (a nullvektorhoz tartozó esetet kivéve, amikor egyik gombhoz sem nyúlunk

- Az $\mathbf{R}$ mátrixban összesen 5 olyan sor van, amelyben csak egyetlen 1-es szerepel. Ez azt jelenti, hogy csak 5 olyan lámpa van, amely leoltható a többi állapotának megváltoztatása nélkül. Ez az öt lámpa a 7, 9, 13, 17, 19 jelű.
- Az $\mathbf{A}$ szimmetrikus, így sortere és oszloptere megegyezik, az $\mathbf{A}$ és az $\mathbf{R}$ sortere ugyancsak megegyezik, hisz az elemi sorműveletek nem változtatják a sorteret. Az $\mathbf{R}$ sorainak összege pedig az $\mathbf{1}$ vektort adja, tehát $\mathbf{1}$ benne van az $\mathbf{A}$ oszlopterében, és így az $\mathbf{Ax} = \mathbf{1}$ egyenlet megoldható. A megoldások száma négy, amit úgy kapunk meg, hogy az egyenlet egy megoldásához hozzáadjuk a homogén négy megoldását. E megoldások a 9 ábrán láthatók.



9. ábra. A négy megoldás

Ha az a kérdés, hogy néhány lámpa ég, hogyan kapcsolhatók le, akkor legegyszerűbb, ha csak az első 23 lámpára szorítkozunk. Az $\mathbf{A}$ mátrix bal felső 23×23-as része invertálható, inverze könnyen megkapható például a szokásos sorlépcsős alakra hozással:

$$\mathrm{rref}[\mathbf{A}_{23\times 23}|\mathbf{I}_{23}] = [\mathbf{X}|\mathbf{I}_{23}]$$

Az inverz

$$\mathbf{X} = \begin{bmatrix}
0&1&1&1&0&0&0&1&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0\\
1&1&0&1&1&0&1&0&0&0&0&0&1&1&1&0&0&0&1&0&0&0&0\\
1&0&1&1&1&1&0&1&1&0&0&0&1&1&0&1&1&1&1&1&0&1&0\\
1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1\\
0&1&1&0&1&1&0&0&0&0&1&0&1&0&1&0&0&1&0&1&1&1&0\\
0&0&1&0&1&0&1&1&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&1&0&1&0&1&1&0&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0\\
1&0&1&0&0&1&0&1&1&0&0&0&0&0&1&1&0&1&0&1&1&0&1\\
0&0&1&0&0&0&1&1&1&0&1&0&0&1&1&1&0&0&1&0&0&1&1\\
1&0&0&0&0&1&1&0&0&0&1&0&1&0&1&0&1&1&0&1&0&0&1\\
0&0&0&0&1&0&0&0&1&1&0&0&1&0&1&1&1&1&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1\\
0&1&1&0&1&1&0&0&0&1&1&0&1&1&0&0&0&1&0&0&1&1&0\\
1&1&1&0&0&0&1&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0\\
1&1&0&0&1&0&0&1&1&1&1&0&0&1&1&1&1&0&1&0&1&0&0\\
0&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1&0&1&0&1&1&0&1\\
0&0&1&1&0&0&1&0&0&1&1&1&0&0&1&0&1&1&1&0&0&0&1\\
0&0&1&0&1&0&1&1&0&1&1&0&1&0&0&1&1&0&1&1&1&0&0\\
0&1&1&0&0&1&0&0&1&0&1&0&0&1&1&0&1&1&1&0&0&0&1\\
1&0&1&0&1&1&0&1&0&1&0&0&0&0&0&1&0&1&0&1&1&0&1\\
0&0&0&1&1&0&0&1&0&0&0&1&1&0&1&1&0&1&0&1&1&1&0\\
0&0&1&1&1&0&1&0&1&0&1&1&1&0&0&0&0&0&0&0&1&1&1\\
0&0&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1&0&1&1&0&1&0
\end{bmatrix}$$

Ezzel a mátrixszal ugyan csak az első 23 lámpára kapunk megoldást, viszont épp azt kapjuk a 4 megoldás közül, amelyikben az utolsó két gombot nem kell megnyomni.

Ha az Olvasónak nem is kellett végigkövetnie a számolást, elhihette, hogy a fenti $\mathbf{A}$ szomszédsági mátrix esetén az $\mathbf{Ax} = \mathbf{1}$ egyenlet megoldható. Meglepő azonban, hogy ez tetszőleges gráf esetén is igaz, azaz tetszőleges szimmetrikus $\mathbf{A}$ mátrixra, melynek főátlójában minden elem 1.

1.17. Tétel Legyen $\mathbf{A}$ egy tetszőleges, de minden csúcsában hurokélt tartalmazó gráf szomszédsági mátrixa, azaz legyen $\mathbf{A}$ egy szimmetrikus, főátlójában 1-eket tartalmazó mátrix. Ekkor az $\mathbf{Ax} = \mathbf{1}$ egyenletrendszer megoldható $\mathbb{F}_2$ fölött.

Ez a következővel ekvivalens: ha a lámpácskákat egy tetszőleges gráf csúcsaiba tesszük, és bármely csúcsban lévő lámpácskát megnyomva az, és annak összes szomszédjában lévő lámpácska állapotot vált, akkor minden lámpácska leoltható, ha kezdetben mindegyikük égett.

Bizonyítás. Az $\mathbf{Ax} = \mathbf{1}$ egyenletrendszer pontosan akkor oldható meg, ha az $\mathbf{1}$ vektor benne van az $\mathbf{A}$ mátrix oszlopterében, ott pedig pontosan akkor van, ha az $\mathbf{1}$ vektor merőleges $\mathbf{A}^\mathsf{T}$ nullterére. Eszerint tehát azt kell igazolnunk, hogy ha $\mathbf{A}^\mathsf{T}\mathbf{x} = \mathbf{0}$, akkor $\mathbf{1}^\mathsf{T}\mathbf{x} = 0$. Ha $\mathbf{A}^\mathsf{T}\mathbf{x} = \mathbf{0}$, akkor $\mathbf{x}^\mathsf{T}\mathbf{Ax} = 0$. Másrészt megmutatjuk, hogy $\mathbf{x}^\mathsf{T}\mathbf{Ax} = \mathbf{1}^\mathsf{T}\mathbf{x}$, ami igazolja, hogy $\mathbf{1}^\mathsf{T}\mathbf{x} = 0$. Az alábbi egyenlőségek helyességét utóbb indokoljuk:

$$\begin{aligned}
\mathbf{x}^\mathsf{T}\mathbf{Ax} &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i a_{ij} x_j \\
&= \sum_{i=1}^{n} a_{ii} x_i^2 \qquad (1.7)\\
&= \sum_{i=1}^{n} a_{ii} x_i \qquad (1.8)\\
&= \mathbf{1}^\mathsf{T}\mathbf{x}. \qquad (1.9)
\end{aligned}$$

A (8) egyenlőség azért igaz, mert $\mathbf{A}$ szimmetrikus, így a kvadratikus alak vegyes tagjai kiesnek, hisz $\mathbb{F}_2$-ben bármely x-re $x + x = 0$, így $x_i a_{ij} x_j + x_j a_{ji} x_i = x_i a_{ij} x_j + x_i a_{ij} x_j = 0$. Másrészt $\mathbb{F}_2$-ben minden x elemre $x^2 = x$, hisz $0^2 = 0$, $1^2 = 1$, ami igazolja a (9) egyenlőséget. Végül $a_{ii} = 1$ minden i-re, hisz $\mathbf{A}$ főátlója csupa 1-esből áll, amiből következik (10). [QED]

1.4 Markov-láncok

Számtalan olyan folyamattal találkozhatunk, melyeknél egy adott rendszer következő állapota csak a pillanatnyi állapot függvénye, a múlté nem. E - Markov-láncoknak nevezett - folyamatokra mi is mutatunk példát a webes dokumentumok

rangsorolásáról szóló fejezetben (ld. sec:web. oldal), de számtalan hasonló modellel találkozhatunk a populációk fejlődésének, bizonyos kémiai, termodinamikai vagy gazdasági folyamatok vizsgálatában, tömegkiszolgálási és sorbanállási rendszerekben, statisztikában.... E rövid fejezetben megpróbáljuk mélyebb valószínűségszámítási ismerettel nem rendelkezők számára is érthetővé tenni e téma alapfogalmainak lineáris algebrai kapcsolatait.

Markov-lánc és lineáris algebrai modellje

Tekintsünk egy kísérletet, melynek megszámlálhatóan sok kimenetele van (azaz véges, vagy megszámlálhatóan végtelen). Azt mondjuk, hogy e kimenetelek sorozata Markov-láncot alkot, ha minden kimenetel csak annak függvénye, hogy mi volt az előző kísérlet kimenetele, annak viszont nem, hogy mik voltak a korábbi kimenetelek. A Markov-láncnak tehát nincs memóriája. A valószínűségszámítás nyelvén az előzőeket így írhatjuk le:

1.18. Definíció (Markov-lánc) Legyen $\mathcal{S}$ egy megszámlálható halmaz, az egyszerűség kedvéért legyen $\mathcal{S} = \{1, 2, \ldots, N\}$, vagy $\mathcal{S} = \mathbb{N}$. Az $\mathcal{S}$-értékű valószínűségi változók egy X_0, X_1, X_2,..., X_n,... sorozata diszkrét paraméterű homogén Markov-lánc, a továbbiakban egyszerűen Markov-lánc, ha

$$\mathbb{P}(X_{n+1} = j \mid X_n = i, X_{n-1} = k, \ldots, X_0 = \ell) = \mathbb{P}(X_{n+1} = j \mid X_n = i) \text{ és} \tag{1.11}$$

$$\mathbb{P}(X_{n+1} = j \mid X_n = i) = \mathbb{P}(X_1 = j \mid X_0 = i) = p_{ij}, \tag{1.12}$$

Az $\mathcal{S}$ halmazt a Markov-lánc állapotterének nevezzük.

A „diszkrét paraméter” kifejezés a valószínűségi változók indexeire vonatkozik. A (11) összefüggést Markov-tulajdonságnak is nevezik. A (12) összefüggés azt fejezi ki, hogy az sem számít, melyik kísérletről van szó (azaz a folyamat időben homogén). Tehát a p_{ij} annak valószínűsége, hogy egy kísérlet kimenetele j, feltéve, hogy az előző i volt.

A definíció következménye, hogy a jelen állapot ismerete alapján, a múlt ismerete nélkül „megjósolható” a jövő útja. Ha adva van állapotok egy i_0, i_1, i_2,..., i_{m-1}, i_m sorozata, akkor kiszámolható, hogy ha az n-edik állapot i_0, akkor mennyi az esélye, hogy a következő állapotok épp az i_1, i_2,..., i_{m-1}, i_m sorozatot adják:

$$\begin{aligned}
&\mathbb{P}(X_{n+m} = i_m, X_{n+m-1} = i_{m-1}, \ldots, X_{n+2} = i_2, X_{n+1} = i_1 \mid X_n = i_0) \\
&= \mathbb{P}(X_{n+m} = i_m \mid X_{n+m-1} = i_{m-1}) \ldots \mathbb{P}(X_{n+2} = i_2 \mid X_{n+1} = i_1)\mathbb{P}(X_{n+1} = i_1 \mid X_n = i_0) \\
&= p_{i_0 i_1} p_{i_1 i_2} \cdots p_{i_{m-1} i_m}.
\end{aligned} \tag{1.13}$$

A legelső kísérlet eredményére persze e képlet nem használható. A folyamat ismeretéhez ezt is meg kell adni: jelölje $p_i = \mathbb{P}(X_0 = i)$ a kezdeti valószínűségeloszlás vektorát, ahol $\mathbf{p}_0 = (p_1, p_2, \ldots)$. E vektor elemei nemnegatív számok, melyekre $\sum_i p_i = 1$. A $\mathbf{P} = [p_{ij}]$ egy $|\mathcal{S}| \times |\mathcal{S}|$-es mátrix, melyet az átmenetvalószínűségek mátrixának, vagy átmenetmátrixnak nevezünk. A kezdeti állapotból a j-be való jutás valószínűsége

$$\mathbb{P}(X_1 = j) = \sum_i \mathbb{P}(X_1 = j \mid X_0 = i)\mathbb{P}(X_0 = i) = \sum_i p_{ij} p_i = [\mathbf{p}_0^\mathsf{T}\mathbf{P}]_j,$$

tehát a második állapot eloszlásvektora $\mathbf{p}_0^\mathsf{T}\mathbf{P}$. Hasonlóképp a következőé $(\mathbf{p}_0^\mathsf{T}\mathbf{P})\mathbf{P} = \mathbf{p}_0^\mathsf{T}\mathbf{P}^2$, és így az n-edik állapot valószínűségeloszlása $\mathbf{p}_n^\mathsf{T} = \mathbf{p}_0^\mathsf{T}\mathbf{P}^n$. Ezt azt jelenti, hogy időtől függetlenül, bármely állapotból az m lépéssel későbbi állapotra való áttérés mátrixa $\mathbf{P}^m$, azaz $\mathbb{P}(X_{n+m} = j \mid X_n = i) = [\mathbf{P}^m]_{ij}$. Ha tehát $\mathbf{p}$ az állapotok pillanatnyi valószínűségeloszlása, akkor m lépéssel később $\mathbf{p}^\mathsf{T}\mathbf{P}^m$ lesz.

A Markov-lánc lineáris algebrai fogalmakkal való leírását a következő tétel biztosítja:

1.19. Tétel Ha $\mathcal{S}$ egy megszámlálható halmaz, $\mathbf{p}$ egy valószínűségeloszlás $\mathcal{S}$-en, és $\mathbf{P}$ egy $|\mathcal{S}| \times |\mathcal{S}|$ méretű (sor)sztochasztikus mátrix, akkor létezik olyan $\mathcal{S}$ állapotterű Markov-lánc, melynek kezdeti eloszlása $\mathbf{p}$, és átmenetmátrixa $\mathbf{P}$.

Bolyongás egy gráfon

A (13) képlet lehetővé teszi, hogy minden Markov-lánc modellezhető egy súlyozott élű irányított gráfon való bolyongással. A gráf csúcsai az állapotok, és az i-edik csúcsból akkor vezet egy p_{ij} súlyú él a j-edikbe, ha $\mathbb{P}(X_1 = j \mid X_0 = i) = p_{ij}$, azaz az i-edik állapotot p_{ij} valószínűséggel követi a j-edik. A bolyongót - legyen az mondjuk egy programozott robot - letesszük a gráf egyik csúcsára a kezdeti $\mathbf{p}$ valószínűségeloszlás szerint. A robot időegységenként körbenéz, és a kifutó élekre írt valószínűségeknek megfelelően véletlenül választ közülük, majd a kiválasztott élen átgurul a következő csúcsba. Ha egy hurokélt választ, helyben marad. Mivel $\mathbf{P}$ sorsztochasztikus, e gráf minden csúcsából kifutó élek súlyainak összege 1.

Néhány egyszerű példa

A következő példákban felrajzoljuk a Markov-lánc gráfját, és felírjuk átmenetmátrixát! A példák kapcsán a későbbiekben a következő kérdésekre keressük majd a választ, némelyiken már most érdemes elgondolkodni!

- Ha a folyamatot sokáig figyeljük, azaz rendre kiszámoljuk a $\mathbf{p}_m^\mathsf{T} = \mathbf{p}_0^\mathsf{T}\mathbf{P}_m$ eloszlásvektorokat, ezek sorozata konvergens-e, azaz létezik-e a $\lim_{m\to\infty} \mathbf{p}_m$ határérték?
- Ha ez nem létezik, létezik-e e vektorok átlagának határértéke, azaz létezik-e a

$$\lim_{m\to\infty} \frac{\mathbf{p}_0 + \mathbf{p}_1 + \dots \mathbf{p}_{m-1}}{m}$$

határérték függetlenül $\mathbf{p}_0$ értékétől? Egyszerűen fogalmazva hosszú ideig figyelve a folyamatot, megmondható-e, hogy mennyi egy-egy állapotba kerülés valószínűsége függetlenül az induló állapottól?

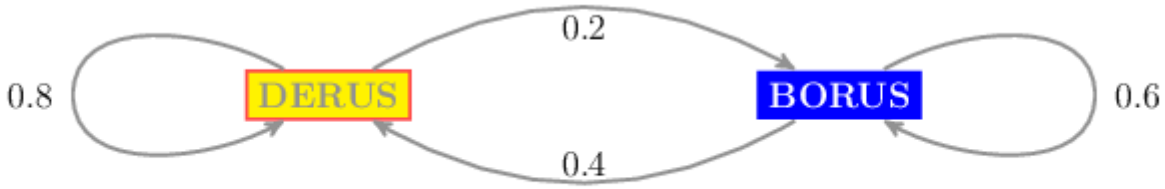
1.20. Példa (Időjárásmodell) Megfigyelések szerint a derűs és borús napok úgy váltják egymást, hogy derűst 80% eséllyel derűs, míg borúst 60% eséllyel borús nap követ.

Megoldás

Az átmenetmátrix

$$\mathbf{P} = 0.80.20.40.6$$

A folyamat gráfja a 10 ábrán látható.



10. ábra. Az időjárás változása

1.21. Példa (Csön-csön gyűrű) Páros sok gyerek körben ül, egyikük kezében rejtve egy gyűrű. Egy gyermekdal ritmusára mindenki úgy tesz, mintha egyik szomszédja kezébe adná a gyűrűt. A Markov-lánc állapota legyen az, hogy kinél van a gyűrű (a játék célja, hogy egy kívülálló ezt kitalálja, de ez most mellékes). Tegyük fel, hogy minden játékos a szomszédjai iránti szimpátia fix mértéke szerinti valószínűséggel, véletlenül választva adja át a gyűrűt. Mi történik, ha van olyan játékos, aki mindig jobbra, és olyan is, aki mindig balra adja a gyűrűt?

Megoldás

A Markov-lánc átmenetmátrixában legyen $a_{i,i-1} = p_i$, $a_{i,i+1} = 1 - p_i$, ahol $p_i \in [0,1]$, és $i = 1, 2, \ldots, n$, azaz

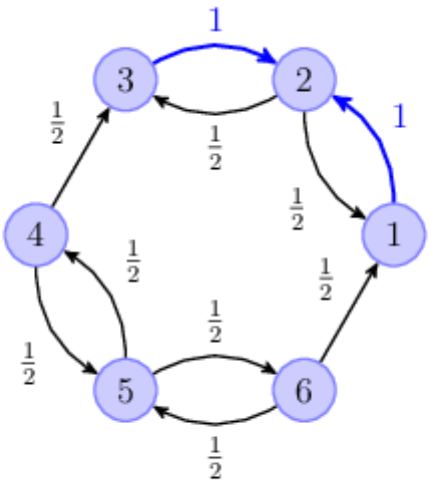
$$\mathbf{P} = \begin{bmatrix} 0 & 1-p_1 & 0 & 0 & \ldots & 0 & p_1 \\ p_2 & 0 & 1-p_2 & 0 & \ldots & 0 & 0 \\ 0 & p_3 & 0 & 1-p_3 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1-p_n & 0 & 0 & 0 & \ldots & p_n & 0 \end{bmatrix}$$

Mivel a résztvevők n száma páros, ezért minden lépésben változik a Markov-lánc állapotának paritása (a játékos sorszámának paritása), így a $\mathbf{P}_m$ vektorok határértéke nem létezik, hisz $\mathbf{P}_m$-ben paritástól függően vagy a páros, vagy a páratlan indexű koordináták egyenlők 0-val.

Legyen példaként egy 6-fős játék mátrixa a következő:

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 \end{bmatrix}$$

A gráfját a 11 ábra mutatja. Látszik, hogy ha a gyűrű egyszer az $\{1,2,3\}$ halmazba kerül, onnan többé nem jut ki, másrészt ha egyszer elhagyja a $\{4,5,6\}$ halmazt, oda többé nem tér vissza.



11. ábra. Csön-csön gyűrű olyan játékosokkal, akik csak egy oldalra adják a gyűrűt.

1.22. Példa (Ki nevet a végén?) Egy leegyszerűsített dobókockás táblás játékot vizsgálunk. A táblán a Starttól a Célig öt további mező van. A játékos dob, majd annyit lép a Cél felé, amennyi a dobás eredménye, de ha nagyobbat dob, mint amennyi a célba éréshez szükséges, vissza kell fordulnia. Akkor ér a Célba, ha épp ott fejezi be a lépéseket. A tábla a 12 ábrán látható.

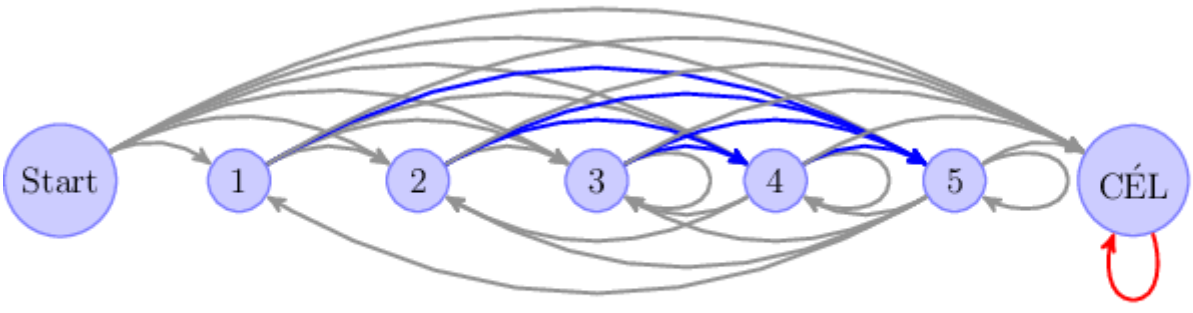
12. ábra. Egy leegyszerűsített „Ki nevet a végén?” játék táblája.

Megoldás

A játék grafikonja és átmenetmátrixa megkonstruálásakor csak azt kell észrevenni, hogy a célból való visszalépések miatt egyik mezőről a másikra lépésnek $1/6$ vagy $2/6$lehet a valószínűsége. A játékhoz tartozó átmenetmátrix

$$\mathbf{P} = \frac{1}{6}\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 \end{bmatrix}$$

A kezdeti eloszlás kötelezően $(1, 0, 0, 0, 0, 0, 0)$, és a Start-ba sosem jutunk vissza (ld. 13 ábra).



13. ábra. A dobókockás táblás játék gráfja. A szürke élekhez $\frac{1}{6}$, a kékekhez $\frac{2}{6}$, míg a piroshoz 1 valószínűség tartozik.

Gyermekkori ismereteink alapján azt sejtjük, hogy a játékos 1 valószínűséggel véges időn belül CÉL-ba ér, ezért az állapotvektorok határértéke $(0,0,0,0,0,0,1)$.

Az állapotok osztályozása

Azt mondjuk, hogy az i állapotból a j elérhető (jelölése $i \to j$), ha van olyan $n \geqslant 0$ egész, hogy $\mathbb{P}(X_n = j \mid X_0 = i) > 0$. Az $n = 0$ lehetősége azt jelenti, i mindig elérhető i-ből. Az elérhetőség algebrailag azt jelenti, hogy van olyan n, hogy $[\mathbf{P}^n]_{ij} > 0$, a gráfon pedig azt, hogy van irányított út az i csúcsból a j-be (itt i-bőli-be a 0 hosszúságú utat is megengedjük az $n = 0$ esetnek megfelelően).

Azt mondjuk, hogy az i és j állapotok érintkeznek, vagy közlekednek ($i \leftrightarrow j$), ha $i \to j$ és $j \to i$. E reláció ekvivalenciareláció, hisz reflexív (minden i-re $i \leftrightarrow i$), szimmetrikus (ha $i \leftrightarrow j$, akkor $j \leftrightarrow i$) és tranzitív (ha $i \leftrightarrow j$ és $j \leftrightarrow k$, akkor $i \leftrightarrow k$), így osztályozza az állapotokat. Egy osztályba kerülnek az egymással érintkező állapotok, két különböző osztály állapotai közt (legfeljebb) csak egy irányban lehet közlekedni[3]. Az egyszerűsített „Ki nevet a végén?” játékban három osztály van, a Start, a Cél, és a harmadik osztályba tartozik a többi állapot. (Ebben az osztályban nem vezet irányított él 2-ből 1-be. El lehet jutni 2-ből 1-be?) A „Csön-csön gyűrű”-ben két osztály van, az $\{1,2,3\}$ és a $\{4,5,6\}$.

Egy Markov-lánc irreducibilis, ha egyetlen osztályból áll, azaz bármely eleméből bármelyikbe el lehet jutni. Ez a gráfok nyelvén azt jelenti, hogy a lánc gráfja erősen összefüggő. A Markov-lánc irreducibilis, ha átmenetmátrixa irreducibilis, azaz minden (i,j) párhoz van olyan m, hogy $[\mathbf{P}^m]_{ij} > 0$. (Ebből nem következik, hogy van olyan m is, hogy $\mathbf{P}^m > \mathbf{O}$, azaz nem következik, hogy $\mathbf{P}$ primitív mátrix!) A Markov-lánc reducibilis, ha nem irreducibilis. Ekkor átmenetmátrixa is reducibilis. Az Időjárásmodell irreducibilis, a „Csön-csön gyűrű” és a „Ki nevet a végén?” reducibilis.

Az i állapot d_i periódusa azon kísérletek sorszámának legnagyobb közös osztója, amelyekben a Markov-lánc az i állapotból indulva visszatérhet i-be, azaz

$$d_i = \text{lnko}\{n > 0 : \mathbb{P}(X_n = i \mid X_0 = i) > 0\}.$$

Például a „Csön-csön gyűrű” játék mindegyik állapotának 2 a periódusa. Az állapot aperiodikus, ha $d_i = 1$. A Markov-lánc aperiodikus, ha minden állapota aperiodikus. Az „Időjárásmodell” és a „Ki nevet a végén?” aperiodikus.

Az i állapot visszatérő, ha a Markov-lánc az i-ből indulva 1 valószínűséggel visszatér az i-be, azaz

$$\exists n > 0 : \mathbb{P}(X_n = i \mid X_0 = i) = 1.$$

Egy állapot átmeneti, ha nem visszatérő.

A „Csön-csön gyűrű” $\{1, 2, 3\}$ -beli állapotai visszatérők, a $\{4, 5, 6\}$ -beliek átmenetiek. Általában is igaz, hogy a visszatérés, az átmenetiség és a periódus ún. osztálytulajdonság, azaz egy osztály minden elemére azonos.

1.23. Állítás Egy véges állapotterű Markov-láncban egy osztály pontosan akkor átmeneti, ha gráfján vezet ki belőle él, és pontosan akkor visszatérő, ha nem. Ha a Markov-lánc elhagy egy átmeneti osztályt, akkor oda többé nem jut vissza, ha belép egy visszatérő osztályba, akkor onnan többé nem tud kijönni. Minden Markov-lánc állapottere diszjunkt átmeneti és visszatérő osztályok uniója.

A „Csön-csön gyűrű” és az Időjárámodell állapotai egyetlen visszatérő osztályt alkotnak, míg a „Ki nevet a végén?” játék két átmeneti és egy visszatérő osztály uniója.

Irreducibilis Markov-láncok

A továbbiakban kizárólag csak véges állapotterű Markov-láncokkal foglalkozunk.

1.24. Definíció (Stacionárius eloszlás) A $\mathbf{P}$ átmenetmátrixú véges Markov-lánc állapotterén értelmezett valamely π eloszlásvektort stacionáriusnak nevezzük, ha $\pi^\mathsf{T}\mathbf{P} = \pi^\mathsf{T}$.

A nemnegatív mátrixok Perron-Frobenius-elméletéből tudjuk, hogy primitív mátrixok hatványainak határértéke megegyezik a jobb és bal Perron-vektor diadikus és skaláris szorzatának hányadosával. Mivel egy $n \times n$ -es átmenetmátrix jobb Perron-vektora $\frac{1}{n}\mathbf{1}$, ahol $\mathbf{1}$ a csupa-1 vektor, ezért ha π jelöli a bal Perron-vektort, akkor

$$\lim_{m\to\infty} \mathbf{P}^m = \frac{(\mathbf{1}/n)\pi^\mathsf{T}}{(\mathbf{1}/n)^\mathsf{T}\pi} = \mathbf{1}\pi^\mathsf{T},$$

ugyanis $\mathbf{1}^\mathsf{T}\pi = 1$. Ebből azonnal adódik, hogy

$$\lim_{m\to\infty} \mathbf{p}_m = \pi, \tag{1.14}$$

ugyanis tetszőleges $\mathbf{p}_0$ eloszlásvektorra $\mathbf{p}_0^\mathsf{T}\mathbf{1} = 1$, így

$$\lim_{m\to\infty} \mathbf{p}_m^\mathsf{T} = \lim_{m\to\infty} \mathbf{p}_0^\mathsf{T}\mathbf{P}^m = \mathbf{p}_0^\mathsf{T}\mathbf{1}\pi^\mathsf{T} = \pi^\mathsf{T}.$$

Az Időjárásmodell esetén a $\mathbf{P} = .8.2.4.6$ átmenetmátrix primitív, az sajátértékhez tartozó bal sajátvektora, s vele a stacionárius eloszlás , vagyis a napoknak -a derűs. Másrészt

$$\lim_{m\to\infty} \mathbf{P}^m = \frac{2}{3}\frac{1}{3}\frac{2}{3}\frac{1}{3}.$$

A „Ki nevet a végén?” átmenetmátrixának bal sajátvektora fejben számolással is ellenőrizhető, hogy $\pi = (0,0,0,0,0,0,1) = \mathbf{e}_7$, így az állapotvektorok határértéke a (14) egyenlőség szerint $\mathbf{e}_7$, vagyis valóban a CÉL-ban végzünk (1 valószínűséggel).

Irreducibilis és imprimitív Markov-láncok

Ha $\mathbf{P}$ irreducibilis ugyan, de imprimitív, mint például a „Csön-csön gyűrű”-nél, akkor létezik ugyan stacionárius megoldás, de az nem az állapotvektorok határértéke. Ugyanakkor a stacionárius vektor i -edik koordinátája - itt is, mint a primitív esetben - megadja, hogy a Markov-lánc „idejének” átlagosan hányad részét tölti az i -edik állapotban.

Az állapotvektoroknak ugyan nincs határértékük, de átlaguknak igen, és az épp a stacionárius vektor, ugyanis a pozitív mátrixok elmélete szerint

$$\lim_{m\to\infty} \frac{\mathbf{I} + \mathbf{P} + \mathbf{P}^2 + \cdots + \mathbf{P}^{m-1}}{m} = \mathbf{1}\pi^{\mathsf{T}},$$

amiből azonnal adódik, hogy

$$\lim_{m\to\infty} \frac{\mathbf{p}_0 + \mathbf{p}_1 + \cdots + \mathbf{p}_{m-1}}{m} = \pi.$$

Bár általában nem egyszerű fölírni a „Csön-csön gyűrű” átmenetmátrixának bal sajátvektorát, a konkrét 6 fős esetben a játék természetéből is kitalálható, és könnyen ellenőrizhető, hogy $\pi = (\frac{1}{4}, \frac{1}{2}, \frac{1}{4}, 0, 0, 0)$. Ebből látszik, hogy az átmeneti osztályban töltött idő elenyészik a visszatérő osztályhoz képest, hisz ha egyszer kilép onnan, többé nem tér vissza.

2 Lineáris programozás

A lineáris programozás az alkalmazott matematika talán legtöbbet használt területe. Része az operációkutatásnak, mely összetett gazdasági, államigazgatási, műszaki, katonai kérdések megválaszolásához, az optimális döntések meghozatalához nyújt segítséget, és általában számítástechnikai eszközök használatát igényli. A lineáris programozás nevét onnan kapta, hogy az itt szereplő függvények lineárisak, az

eredmények pedig tipikus esetben a teendők tervezésében, programozásában lesznek használhatók.

2.1 Bevezetés

A lineáris programozás alapfeladata egy lineáris egyenlőtlenségrendszer olyan megoldásának megkereséséből áll, melyben valamely ugyancsak lineáris célfüggvény extremális értéket vesz fel.

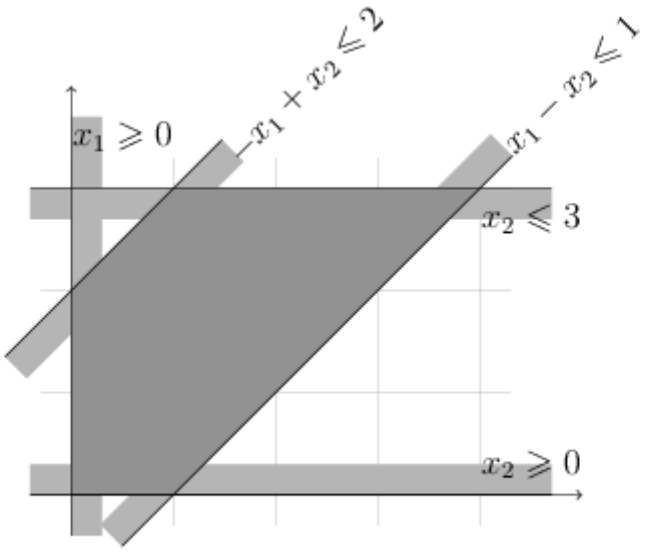
Kezdjük egy fejben is megoldható feladattal. Ajándékot szeretnék vásárolni két rokonomnak. Beával abban maradtunk, hogy nem költhetünk az egymásnak szánt ajándékra 3000 Ft-nál többet. Bármennyiért is veszek neki ajándékot, nem lenne jó, ha Adélnak több, mint 1000 Ft-tal drágábbat vennék. Adél kevésbbé érzékeny, de azért a Beának vett ajándék se legyen 2000 Ft-nál többel drágább. Mennyi pénzt vigyek magammal a vásárlásra?

Geometriai szemléltetés két változó esetén

Legyen az Adélnak vett ajándék értéke 1000 Ft-ban mérve x_1, a Beának vetté pedig x_2. Annyi pénzt kell magammal vinni, amennyi $x_1 + x_2$ értéke legföljebb lehet. Tehát a kétváltozós $z = x_1 + x_2$ függvény maximumát keressük. A feltételek egyenlőtlenségek formájában fejezhetők ki, pl. azt, hogy Adél ajándéka legföljebb 1000 Ft-tal lehet drágább Bea ajándékánál az $x_1 - x_2 \leqslant 1$ egyenlőtlenség írja le (1000 Ft-ban mérünk mindent). A feladat képletekkel így írható le:

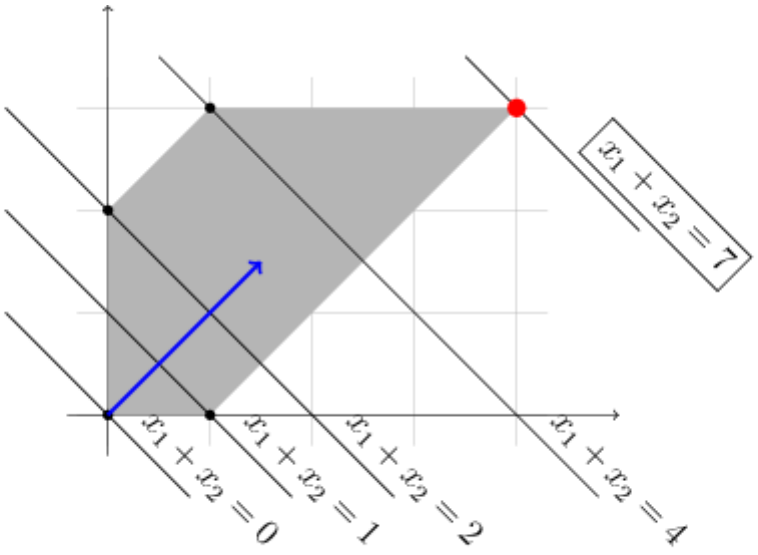
$$\begin{aligned} x_1 - x_2 &\leqslant 1 \\ -x_1 + x_2 &\leqslant 2 \\ x_2 &\leqslant 3 \\ x_1, x_2 &\geqslant 0 \\ z = x_1 + x_2 &\to \max \end{aligned}$$

A feladatot először grafikusan oldjuk meg. Mindegyik egyenlőtlenség egy-egy félsíkot határoz meg, melyek metszete egy konvex sokszög. E sokszögbe tartozó pontok azok, amelyek kielégítik az egyenlőtlenségek mindegyikét. Ezeket lehetséges megoldásoknak nevezzük (ld. 14 ábra).



14. ábra. A lehetséges megoldások halmaza

Szemléletesen világos, hogy a maximalizálandó függvény - az ún. célfüggvény - szélsőértékét valamelyik csúcspontban veszi föl. A 15 ábra a sokszög csúcsain áthaladó, $x_1 + x_2 = \text{const}$ egyenletű egyeneseket mutatja. Tekinthetjük úgy, hogy az $x_1 + x_2 = 0$ egyenest normálvektorának irányába toljuk addig, míg a maximális értékét el nem éri.



15. ábra. A célfüggvény értékei a sokszög csúcsaiban

Az ábráról tehát leolvashatjuk az eredményt: a maximum 7, azaz 7000 Ft-ot kell magammal vinnem.

LP-feladat

A gyakorlati feladatokban nem csak azonos irányú egyenlőtlenségek, hanem mindkét egyenlőtlenség és egyenlőség is szerepelhet, a változók pedig nem csak nemnegatívak, de előjelkorlátozatlanok is lehetnek.

2.1. Definíció (LP feladat) Lineáris programozási feladaton olyan többváltozós optimalizálási feladatot értünk, melyre a következők igazak:

1. Az optimalizálandó (maximalizálandó vagy minimalizálandó) függvény

$$f(x_1, x_2, \ldots, x_n) = c_1x_1 + c_2x_2 + \cdots + c_nx_n = \mathbf{c}^\mathsf{T}\mathbf{x}$$

   alakú, ahol $\mathbf{c}$ konstans vektor.

2. A változók kielégítik a korlátozó feltételeket, melyek mindegyike vagy valamilyen irányú nem szigorú egyenlőtlenség ($\leqslant$ vagy $\geqslant$) vagy egyenlőség, és amelynek bal oldalán a változók egy lineáris függvénye, jobb oldalán egy konstans áll.
3. A változók mindegyike vagy nemnegatív, vagy előjelkorlátozatlan, azaz tetszőleges előjelű lehet.

Az LP feladat geometriai értelmezése

E rövid paragrafusban csak szemléletünkre hagyatkozva, a precíz matematikai bizonyításokat mellőzve, áttekintjük az LP feladat geometriai értelmezésének alapfogalmait.

Egy $\mathbf{a} \in \mathbb{R}^n$ vektorral és $b \in \mathbb{R}$ valós számmal felírt $\mathbf{a}^\mathsf{T}\mathbf{x} = b$ egyenlet egy hipersík egyenlete, mely egy affin altér, nevezetesen $\mathbf{a} \neq \mathbf{0}$ esetén egy $n-1$-dimenziós altér eltoltja. Ez egy konvex halmaz. Az $\mathbf{a}^\mathsf{T}\mathbf{x} \leqslant b$ egyenlőtlenséget kielégítő pontok egy - az előző hipesíkkal határolt - félteret alkotnak. Ugyanez igaz az $\mathbf{a}^\mathsf{T}\mathbf{x} \geqslant b$ egyenlőtlenséggel megadott féltérre is. (Gondoljuk meg, a hipersík valóban a féltér határpontjaiból áll az analízis határpontfogalma szerint is.) A féltér is konvex halmaz, és mivel konvex halmazok metszete is konvex, ezért egy lineáris egyenletekből és egyenlőtlenségekből álló rendszer összes megoldásainak halmaza is konvex. Affin alterek és félterek véges halmazának nem üres metszete konvex poliéder. Ez nem feltétlenül korlátos.

Tekintsük az $\mathbf{a}_i \in \mathbb{R}^n$ vektorokat, és a segítségükkel felírt

$$\mathbf{a}_i^\mathsf{T}\mathbf{x} \lesseqgtr b_i, \quad i = 1, 2, \ldots, m$$

egyenlőtlenségrendszert, ahol $\lesseqgtr$ a $\leqslant$, $\geqslant$ vagy az $=$ jelek valamelyike. Az általuk meghatározott poliéder határán azon pontok halmazát értjük, melyek a fenti relációk legalább egyikét egyenlőséggel teljesítik, tehát a relációk által megadott

affin alterek legalább egyikének pontjai. (Természetesen, ha a fenti egyenletek közt akár csak egy egyenlőség is akad, akkor a poliéder minden pontja határpont. Ilyen eset pl. az, ha a 3-dimenziós térben tekintünk egy háromszöget.) Tehát a fenti relációkkal megadott poliéder egy $\bar{x}$ pontja határpont, ha az $\mathbf{a}_i^T \bar{x} \leqslant b_i$ ($i = 1, 2, \ldots, m$) relációk mind teljesülnek, de legalább egyikükben az egyenlőség is teljesül, azaz valamely i -re $\mathbf{a}_i^T \bar{x} = b_i$. Speciálisan, egy poliéder csúcspontján olyan határpontját értjük, mely azoknak a relációknak, melyeket egyenlőséggel teljesít, az egyetlen megoldása. Ha egy n -ismeretlenes egyenletrendszer egyértelműen megoldható, akkor egyenletei között van n darab lineárisan független, melyeknek ez az egyetlen megoldása. Ez azt jelenti, hogy $\bar{x}$ a poliédernek pontosan akkor csúcsa, ha van az indexeknek egy n - elemű $I \subseteq \{1, 2, \ldots, m\}$ részhalmaza, hogy $\mathbf{a}_i^T \bar{x} = b_i$, ha $i \in I$, és ezen $\mathbf{a}_i$ vektorok lineárisan függetlenek.

A 3 definícióbeli LP feladatban szereplő korlátozó feltételek mellett a változókra kirótt nemnegativitási feltételek kifejezhetők $\mathbf{a}_i^T \mathbf{x} \geqslant 0$ alakban, ha $\mathbf{a}_i$ valamelyik standard bázisvektor. Így a fenti geometriai modell teljes lesz, ha tudjuk, hogy a célfüggvény hogy viselkedik a poliéder pontjain. Analízisből tudjuk, hogy a lineáris függvény folytonos, így ha a poliéder pontjain fölvett értékei felülről korlátosak, akkor a poliéderen van maximuma. Megmutatható, hogy a maximális értékét vagy egyetlen pontban, egy csúcspontban veszi fel, vagy ha több pontban is, akkor van köztük csúcspont. Ez azonnal ad egy módszert az LP feladat megoldására: tekintsük az LP feladat korlátozó feltételeiből és a nemnegativitási feltételekből adódó relációkat. Legyen ezek száma m . Válasszunk ki minden lehető módon n relációt az m -ből, és próbáljuk meg megoldani azt az egyenletrendszert, amit a relációjelek egyenlőségre cserélésével kapunk. Ha az n egyenletből álló egyenletrendszer egyértelműen megoldható, és a megoldás benne van az eredeti poliéderben - azaz kielégíti a ki nem választott egyenlőtlenségeket, tehát annak egy csúcspontja -, akkor kiértékeljük e pontban a célfüggvényt. Így megtaláljuk azt a csúcspontot, ahol a függvény a maximális értékét veszi föl. Ezt a megoldási módot követtük a 15 ábrán szemléltetett megoldásnál is. Hasonlóan járunk el a minimumfeladat esetén is.

A megoldhatóság esetei

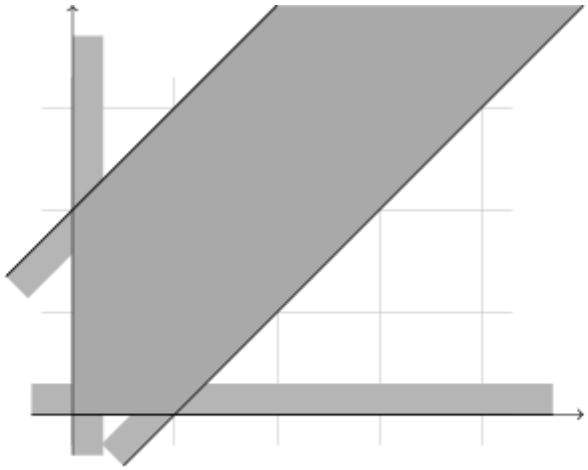
A 2-változós LP feladaton szemléltethetők a megoldhatóság különböző esetei.

Könnyen igazolható, hogy egy LP feladat megoldásaira az alábbi négy eset valamelyike teljesül: A feladatnak

1. egyetlen optimális megoldása van (a lehetséges megoldások poliéderének egy csúcsa),
2. végtelen sok optimális megoldása van (a lehetséges megoldások poliéderén egy él/lap/... összes pontja),

3. végtelen sok lehetséges megoldása van, de azok halmaza s rajta a célfüggvény sem korlátos, tehát optimális megoldás nincs,
4. egyetlen lehetséges megoldása sincs (nem megoldható).

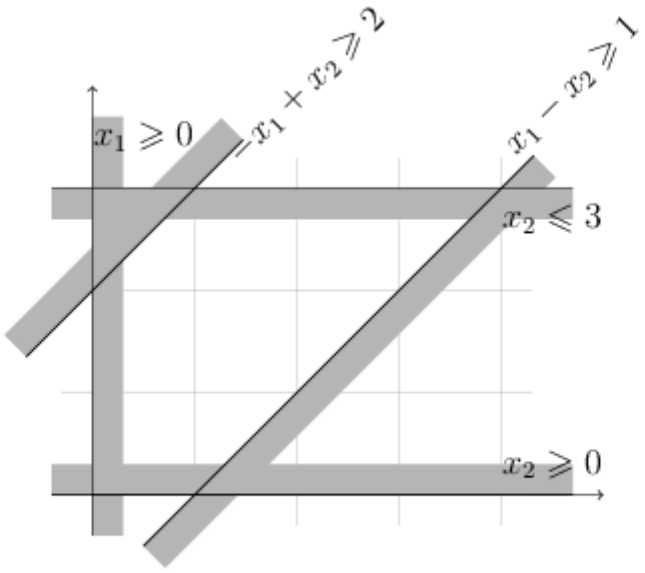
Változtassunk egy kicsit a bevezető feladaton: hagyjuk el azt a feltételt, hogy Bea ajándékára nem költhetek 3000 Ft-nál többet. Világos, hogy ekkor bármennyit költhetek ajándékra, a lehetséges megoldások halmaza nem korlátos, ahogy ezt a 16 ábra mutatja.



16. ábra. A lehetséges megoldások halmaza nem korlátos, és nincs optimális megoldás

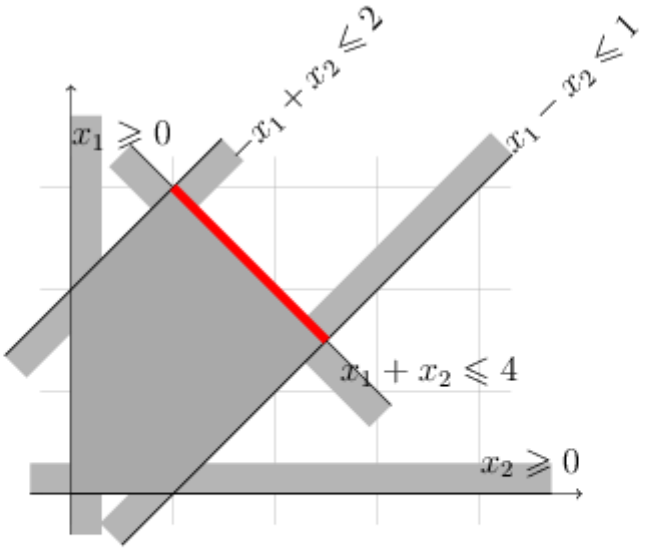
Változtassuk a feladatot a következőképp: Beára nem költhetek 3000 Ft-nál többet. Bármennyiért is veszek neki ajándékot, Adélnak legalább 1000 Ft-tal drágábbat szeretnék venni. Adél érzékenyebb, ezért neki legalább 2000 Ft-tal drágább ajándékot kell vennem, mint Adélnak. Mennyi pénzt vigyek magammal a vásárlásra?

Látható, hogy a feladat ellentmondást tartalmaz, a feltételek mindegyike egyszerre nem teljesíthető, nincs lehetséges megoldás. A $-x_1 + x_2 \geqslant 2$ és az $-x_1 + x_2 \leqslant -1$ egyenlőtlenségek egyszerre nem teljesülhetnek. Geometriai nyelven fogalmazva, a tekintett féltereknek (itt félsíkoknak) üres a metszete (ld. 17 ábra).



17. ábra. Ellentmondásos, lehetséges megoldással nem rendelkező LP feladat

Végül az eredeti feladatból azt a feltételt, hogy Beára nem költhetek 3000 Ft-nál többet, cseréljük ki arra, hogy Adélra és Beára összesen legföljebb 4000 Ft-ot költhetek. A többi feltétel változatlan marad. Mennyit költhetek Adélra és Beára összesen? A választ az Olvasóra hagyjuk, de a teljesség kedvéért itt is ábrázoljuk a lehetséges és az optimális megoldások halmazát (ld. 18 ábra).



18. ábra. Végtelen sok optimális megoldás esete: (x_1, x_2) értéke az $(1, 3)$ és $(2.5, 1.5)$ pontokat összekötő szakasz bármelyike lehet. E szakasz minden pontja kielégíti az összes feltételt, és a célfüggvény értéke mindegyikükben 4, azaz legföljebb 4000 Ft-ért vásárolhatok ajándékot.

2.2 LP feladatra vezető néhány probléma

A lineáris programozás számtalan alkalmazása közül mutatunk néhány fontosnak vagy érdekesnek tekinthetőt.

Termelés korlátozott erőforrások mellett

Egy elterjedt közgazdasági alkalmazással kezdjük: n különböző terméket kell előállítani, a j -edikből x_j -t, mely egy nemnegatív valós szám ($j = 1, 2, \ldots, n$). E modell tehát vagy folytonosan változtatható mennyiségű - pl. tömegével, űrmértékével mérhető - termékekre, vagy nagy darabszámban termelt termékekre működik, ahol a megoldást megadó valós szám és annak egészrésze közti különbség elhanyagolható.

A termelés erőforrásai (nyersanyag mennyisége, munkaerő nagysága, a felhasználható munkaórák száma, a felhasználható gépek száma, a rendelkezésre álló idő, stb.) korlátosak. Minden egyes korlát egy egyenlőtlenséggel írható le. Legyen az i -edik erőforrásnak a j -edik termék előállításához szükséges mennyisége a_{ij} , és legyen ezen erőforrás összes rendelkezésünkre álló mennyisége b_i . Ekkor fönnáll a következő egyenlőtlenség:

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \leqslant b_i.$$

Végül a j -edik termék árát jelölje c_j . Keressük a termékeknek olyan legyártandó mennyisége, mely a legnagyobb bevételt biztosítja. A maximalizálandó függvény tehát:

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n.$$

Az $\mathbf{A} = [a_{ij}]$, $\mathbf{b} = [b_i]$, $\mathbf{c} = [c_j]$ ($i = 1, \ldots, m$, $j = 1, \ldots, n$) jelölések mellett a feladat a következő alakba írható:

$$\mathbf{Ax} \leqslant \mathbf{b},\ \mathbf{x} \geqslant \mathbf{0},\ \mathbf{c}^{\mathsf{T}}\mathbf{x} \to \max.$$

2.2. Példa (Parfüm összetevők) Egy cég két különleges parfümöt gyárt (az elsőből időegységenként x_1, a másodikból x_2 cl-t), melyekbe titkos illatanyagát keveri. Az elsőbe cl-enként 1, a másikba 4 egységnyit kever, de az időegységenként fölhasználható mennyiség legföljebb 16 egység lehet ($x_1 + 4x_2 \leqslant 16$). A csomagolókapacitás legföljebb 7 cl parfüm előállítását engedi időegységenként ($x_1 + x_2 \leqslant 7$). Az első parfümöt kétszer, a másodikat egyszer kell egy különleges eljárás alá vetni, melyből a gyártás során időegységenként 12 -re van lehetőség ($2x_1 + x_2 \leqslant 12$). Az első parfüm 3$, a második 4$ áron adható a nagykereskedőnek. Mennyit kell gyártani az elsőből és mennyit a másodikból időegységenként, hogy a bevétel a lehető legnagyobb legyen?

A következő LP feladatra jutunk:

$$\begin{aligned} x_1 + 4x_2 &\leqslant 16 \\ x_1 + x_2 &\leqslant 7 \\ 2x_1 + x_2 &\leqslant 12 \\ x_1, x_2 &\geqslant 0 \\ z = 3x_1 + 4x_2 &\to \max \end{aligned} \tag{2.1}$$

A feladat grafikusan is megoldható (ezt most az Olvasóra hagyjuk), de számtalan - akár online is elérhető - programot hívhatunk segítségül a megoldáshoz. Mi a sage nevű programnak a következő kóddal adjuk át a feladatot:

```
p = MixedIntegerLinearProgram()
x, y = p['x'], p['y']
p.add_constraint(x + 4*y <= 16)
p.add_constraint(x + y <= 7)
p.add_constraint(2*x + y <= 12)
p.set_objective(3*x + 4*y)
p.solve()
```

E kódra a sage válasza 24, azaz ennyi a célfüggvény értéke, azaz időegységenként ennyi a maximális bevétel. A gyártandó mennyiségek a következő paranccsal kaphatók meg:

```
p.get values( x, y )
```

Erre válasz $x = 4$, $y = 3$, azaz az elsőből időegységenként 4, a másodikból 3 cl parfüm gyártandó.

Diétás feladat

Ismerjük az emberek átlagos napi vitaminszükségletét, ismerjük a gyümölcsök vitamintartalmát és árát. Állítsunk össze egy olyan gyümölcssalátát a mai napra, mely fedezi egy ember napi vitaminszükségletét minden vitaminból, és a lehető legolcsóbb. Az adatokat az 1 táblázatban foglaljuk össze (csak az első néhány sorát és oszlopát mutatjuk).

	alma	kajszi	meggy	...	szükséglet
A-vitamin (mg)	0.05	1.8	0.3	...	0.8
C-vitamin (mg)	5	10	10	...	60
⋮	⋮	⋮	⋮	...	
Ár (Ft)	30	45	50	...	

1. táblázat. Gyümölcsök 10 dkg-ra vonatkozó vitamintartalma, ára, és a napi vitaminszükséglet táblázata.

Jelölje x_1 az alma, x_2 a kajszi, x_3 a meggy... mennyiségét (10 dkg-ban mérve). Világos, hogy e változók nem negatívak, így a belőlük alkotott vektorra fennáll az $x \geqslant 0$ egyenlőtlenség. Az A-vitamin napi szükségletére vonatkozó feltétel a következő:

$$0.05x_1 + 1.8x_2 + 0.3x_3 + \ldots \geqslant 0.8$$

Hasonlóan fölírható a többi vitaminra is a megfelelő egyenlőtlenség. A célfüggvény az ár, ami minimalizálandó:

$$30x_1 + 45x_2 + 50x_3 + \cdots \to \min.$$

A feladat mátrixalakban is fölírható. Legyen

$$\mathbf{A} = 0.051.80.3\ldots;51010\ldots;\vdots\vdots\ddots;, \quad \mathbf{b} = 0.860\vdots, \quad \mathbf{c} = 304550\vdots.$$

E jelölésekkel a feladat:

$$\mathbf{Ax} \geqslant \mathbf{b},\ \mathbf{x} \geqslant \mathbf{0},\ \mathbf{c}^{\mathsf{T}}\mathbf{x} \to \min.$$

Szállítási feladat

A szállítási feladat bizonyos termékek kínálati pontokból felvevő pontokba való optimális költségű eljuttatásának módját keresi. Az elektromos áram erőművekből a városokba szállítása, egy gyár különböző raktáraiból egy alkatrész kiszállítása a különböző gyáregységekbe tipikus példák e feladattípusra.

Adva van m kínálati pont, és ismerjük az i -edik által kínált termék s_i mennyiségét ($i = 1, 2, \ldots, m$). Hasonlóképp ismerjük az n felvevő pont mindegyikének szükségletét, a j -edikét jelölje d_j ($j = 1, 2, \ldots, n$). Feltételezzük, hogy

$$\sum_{i=1}^{m} s_i = \sum_{j=1}^{n} d_j.$$

Ha e feltétel nem teljesülne, a feladatot fiktív keresleti vagy fiktív kínálati ponttal módosítjuk úgy, hogy azok az összes felesleget fölvegyék, illetve az összes hiányzó szükségletet kielégítsék. Jelölje c_{ij} az i -edik kínálati pontból a j -edik felvevőbe való szállítás költségét (a fiktív pontokból/ba szállítás költsége 0). Keresendő az i -edik kínálati pontból a j -edik felvevő pontba valóban szállított termék x_{ij} mennyisége, amely mellett a szállítás összköltsége minimális.

E feladat a következő LP-feladatra vezet:

$$\sum_{j=1}^{n} x_{ij} \leqslant s_i \qquad i = 1, 2, \ldots, m,$$

$$\sum_{i=1}^{m} x_{ij} \geqslant d_j \qquad j = 1, 2, \ldots, n,$$

$$x_{ij} \geqslant 0 \qquad i = 1, 2, \ldots, m, \;\; j = 1, 2, \ldots, n,$$

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} x_{ij} \to \min$$

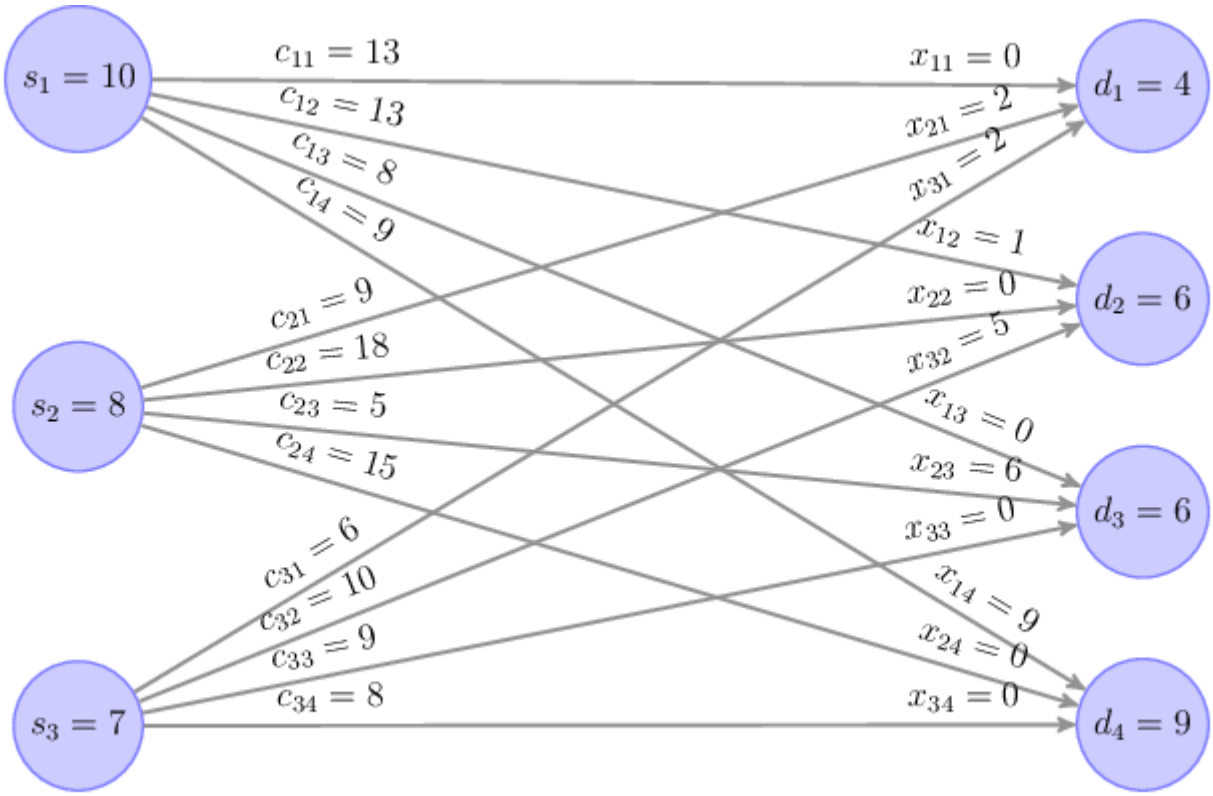
A feladat szemléltethető egy irányított, súlyozott élű páros gráffal, amint az a 19 ábrán látható. Ott a következő konkrét feladat gráfját látjuk. Egy olajfinomító három hatalmas tárolóban tárolja az olajat, amit onnan szállít négy finomítójába. A tartályokból naponta rendre legföljebb $100\,000$, $80\,000$, illetve $70\,000$ tonna kőolaj szállítható el, a finomítók napi kapacitása rendre $40\,000$, $60\,000$, $60\,000$, illetve $90\,000$ tonna. Itt tehát $m = 3$, $n = 4$ és a kínálat, illetve a felvevő értékek vektora $10\,000$tonnában mérve $\mathbf{s} = (10, 8, 7)$, illetve $\mathbf{d} = (4, 6, 6, 9)$. A költségek mátrixa, ahol az értékek $100\$$-ban értendők

$$\mathbf{C} = 131389; 918515; 61098; .$$

A feladat megoldása

$$\mathbf{X} = 0109; 2060; 2500; ,$$

a minimális költség tehát 204, azaz $20\,400\$$ naponta.



19. ábra. Szállítási feladat 3 kínálati és 4 felvevő ponttal.

A kapacitás változtatása és a raktározás költségei

A szezonálisan erősen változó mennyiségben eladott termékek termelésének egyik nehézsége, hogy a termelés mennyiségének megváltoztatása extra költségekkel jár, ezért kerülendő, ugyanakkor az egyenletes termelés megnöveli a raktározási költségeket.

Tegyük fel, hogy a korábbi évek tapasztalatai alapján egy termékre az idei év i -edik hónapjában várható igény b_i lesz. Meg kell terveznünk a termelés és raktározás havi mennyiségét. A termelés tervezett mennyiségét x_i , a raktározandó mennyiséget r_i ($i = 1, 2, \ldots, 12$) jelöli. Tegyük fel, hogy a termelt mennyiségből a piacra, illetve a raktárba való szállítás mindig a hónap végén esedékes. Ez azt jelenti, hogy az i -edik hónap végén a termelt mennyiség és az előző havi raktárkészlet összege épp annyi, mint az ahavi eladás és raktárkészlet összege, azaz

$$x_i + r_{i-1} = b_i + r_i, \quad i = 1, 2, \ldots, 12.$$

A termékek tárolása t $-ba, míg a termelés átállítása termékenként a $-ba kerül. Ez azt jelenti, hogy akár növeljük, akár csökkentjük a termelést, ha a növekmény vagy a csökkenés mennyisége egy hónapban x darab, akkor az ax $ extra kiadást okoz. Tehát a célfüggvény, melyet minimalizálni kell:

$$t\sum_{i=1}^{12} r_i + a\sum_{i=1}^{12} |x_i - x_{i-1}|.$$

E függvényt egy szép trükkel lineárissá lehet tenni. Legyen u_i az $i-1$-dik hónapról az i -edikre való termelésnövekedés, míg v_i a csökkenés mértéke (mindkettő nemnegatív szám). Így $x_i - x_{i-1} = u_i - v_i$, ugyanakkor $|x_i - x_{i-1}| = u_i + v_i$. A lineáris program tehát a következő:

$$\begin{aligned} x_i + r_{i-1} - r_i &= b_i, \quad i = 1, 2, \ldots, 12 \\ x_i - x_{i-1} - u_i + v_i &= 0, \quad i = 1, 2, \ldots, 12 \\ x_0 = r_0 = r_{12} &= 0, \\ x_i, r_i, u_i, v_i &\geqslant 0 \quad i = 1, 2, \ldots, 12 \\ \sum_{i=1}^{12} (tr_i + au_i + av_i) &\to \min \end{aligned}$$

Ez egy 50 -változós, 27 korlátozó feltételből álló program.

Oldjuk meg egy ilyen feladatot, a konkrétum kedvéért legyen $t = 1$, $a = 3$ és

$$\mathbf{b} = (300, 200, 320, 400, 700, 500, 300, 250, 500, 400, 800, 1200).$$

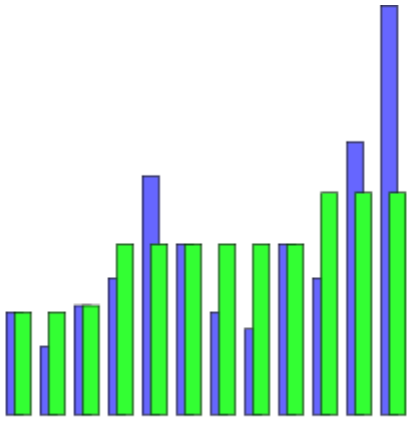
A megoldásához a sage programot használjuk. A parancsok magukért beszélnek, a változók automatikusan nemnegatívak, a célfüggvénynek a programcsomag mindig a maximumát keresi, ezért beszoroztuk -1-gyel, mivel mi a minimumot keressük.

```
p = MixedIntegerLinearProgram()
x = p.new_variable()
r = p.new_variable()
u = p.new_variable()
v = p.new_variable()
b = (300,200,320,400,700,500,300,250,500,400,800,1200)
p.add_constraint(x[0] == 0)
p.add_constraint(r[0] == 0)
p.add_constraint(r[12] == 0)
for i in range(1,13):
    p.add_constraint(x[i] + r[i-1] - r[i] == b[i-1])
    p.add_constraint(x[i] - x[i-1] - u[i] + v[i] == 0)
p.set_objective(-sum(3*u[i] + 3*v[i] + r[i] for i in range(1,13)))
p.solve()
```

A sage válasza az utolsó sorra -4700 , azaz a minimális költség (raktározási és átállási) összesen 4700$. A get_values metódus megadja az $\mathbf{x}$ vektor koordinátáit:

```
p.get_values( x )
  {0: 0.0, 1: 300.0, 2: 300.0, 3: 320.0, 4: 500.0, 5: 500.0, 6: 500.0, 7:
  500.0, 8: 500.0, 9: 500.0, 10: 650.0, 11: 650.0, 12: 650.0}
```

A 20 ábrán mind az eladás, mind a termelés oszlopdiagrammja látható.



20. ábra. A havonta várható eladások (kék) és a termelés (zöld) oszlopdiagrammja.

2.3 Szimplex módszer

A szimplex módszer az LP-feladat megoldásának egy módszere, mára kifinomult algoritmusok egy igen hatékony rendszerévé vált. Mi csak a legfontosabb alapfogalmakat tekintjük át.

Az elemi sorműveletek alkalmazása

Az elsőként vizsgált ajándékozási feladatot az egyenletrendszerek megoldásánál megismert technikával - az elemi sorműveletek segítségével - ismét megoldjuk.

Ahhoz, hogy az egyenletrendszerek megoldásánál tanult technikát alkalmazhassuk, az egyenlőtlenségrendszert új változók bevezetésével egyenletrendszerré alakítjuk. Feltételezhetjük, hogy az egyenletrendszer együtthatómátrixa sorfüggetlen, de legalábbis ezt egyszerűen elérhetjük. Az ötlet egyszerű, minden egyenlőtlenség bal oldalához egy nemnegatív értékű változót adunk, mely az egyenlőtlenséget egyenlőséggé teszi. Esetünkben ezt kapjuk:

$$\begin{aligned} x_1 - x_2 + s_1 &= 1 \\ -x_1 + x_2 + s_2 &= 2 \\ x_2 + s_3 &= 3 \end{aligned} \tag{2.2}$$

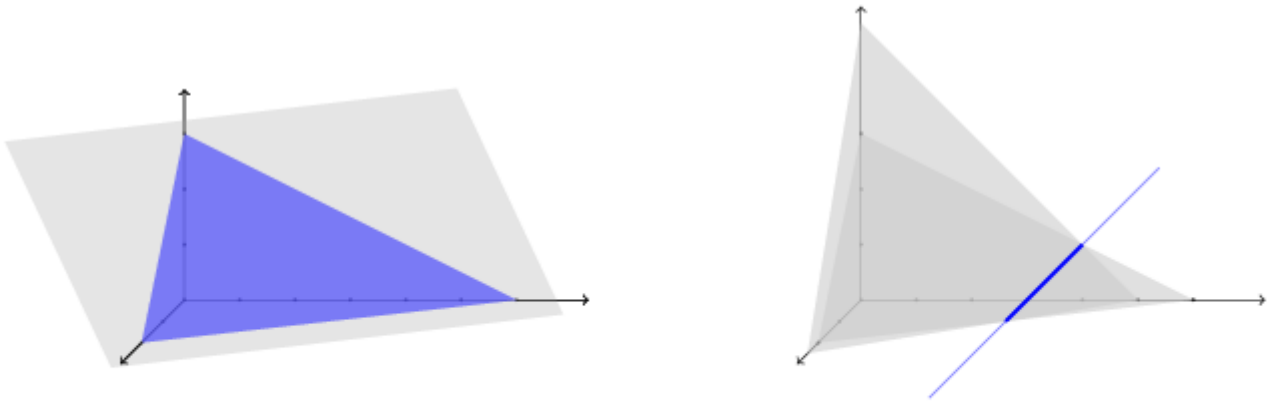
A három egyenletből álló ötismeretlenes egyenletrendszer megoldható, megoldásai egy affin alteret alkotnak, és ezt az egyenletrendszer bármiféle manipulációja nélkül is azonnal föl tudjuk írni, hisz az egyenletrendszer hasonlít a Gauss-Jordan-módszer végén kapott alakhoz (csak most egy vezéregyes az együtthatómátrix egy sorának nem az első, hanem az utolsó nemnulla eleme). Az egyenletrendszer összes megoldása esetünkben

$$x_1x_2s_1s_2s_3 = x_1x_21 - x_1 + x_22 + x_1 - x_23 - x_2 = 00123 + x_110 - 110 + x_2011 - 1 - 1. \quad (2.3)$$

Tehát egy 2-dimenziós affin alteret kaptunk, ennek azonban minket csak azok a pontjai érdekelnek, amelyek egyetlen koordinátája sem negatív. Sőt, a nemnegatív koordinátájú pontok térrésze e síkból egy poliédert vág ki, melynek minket csak a csúcspontjai érdekelnek, mert az optimális megoldást egy ilyen pontban remélhetjük.

Egy 5-dimenziós térbeli 2-dimenziós affin altérből kivágott poliédert (sokszöget) nem könnyű elképzelni, ezért először analógiaként hasonló, de kisebb dimenziós példát mutatunk. Legyen a 3-változós egyenletrendszer egyetlen egyenlete $x_1 + 2x_2 + 3x_3 = 6$. Ennek összes megoldása egy síkot alkot (affin altér), melynek az első térnyolcadba eső része egy háromszög (2-dimenziós poliéder, melynek csúcsai $(6, 0, 0)$, $(0, 3, 0)$, $(0, 0, 2)$). E csúcsok mindegyikében két koordináta is 0.

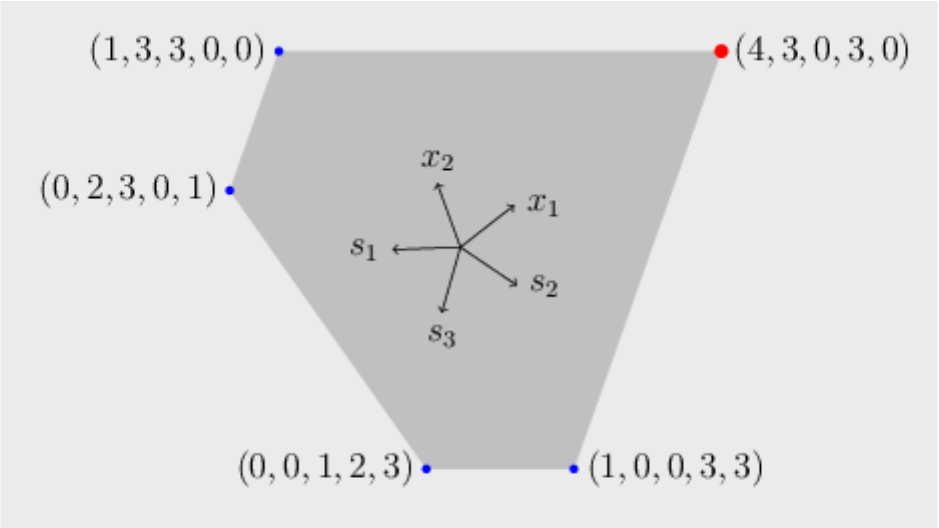
Ha az $x_1 + 2x_2 + 3x_3 = 6$ és $x_1 + x_2 + 2x_3 = 5$ egyenletekből álló egyenletrendszert tekintjük, melynek megoldása egy 1-dimenziós affin altér, akkor annak az első térnyolcadba eső része egy szakasz (1-dimenziós poliéder, csúcspontjai $(4, 1, 0)$, $(3, 0, 1)$, ezek egy-egy koordinátája 0). E szakasz megkapható a két egyenlethez tartozó két háromszög metszeteként is (ld. 21 ábra).



21. ábra. Egy affin altér (az első ábrán egy sík, a másodikon egy egyenes) és nemnegatív koordinátájú pontokból álló része (az elsőn egy háromszög, a másodikon egy szakasz)

Az analógia alapján sejthető, de később igazoljuk is, hogy az 5-dimenziós térbeli 2-dimenziós poliéderünk csúcsai olyan pontok, amelyekben a koordináták közül kettő értéke 0, a többi nemnegatív. A (2) egyenletrendszerben könnyen találunk ilyen megoldást: ha $x_1 = x_2 = 0$, akkor $s_1 = 1$, $s_2 = 2$, $s_3 = 3$, így az $(x_1, x_2, s_1, s_2, s_3) = (0, 0, 1, 2, 3)$ vektor a poliéder egyik csúcsa. Az e ponthoz

tartozó célfüggvényérték $z = x_1 + x_2 = 0$. A poliéder többi pontja a korábbi ábrából, és a (3) megoldásokból fölírható. Végül a poliédert szemléltetjük a 22 ábrán.



22. ábra. Az egyenletrendszer megoldását adó sík az 5-dimenziós térben, és abban a lehetséges megoldások poliédere. (E sík egyetlen pontban metszi a 3-dimenziós $x_1x_2s_1$, $x_2s_1s_3$, $s_1s_3s_2$, $s_3s_2x_1$ és az $s_2x_1x_2$ koordinátatereket, így mindig a kimaradó két koordináta 0.)

A további lépések egyszerű követhetősége érdekében a célfüggvényt megadó $x_1 + x_2 = z$ egyenlőséget is az egyenletrendszerhez írjuk. A feladathoz tartozó egyenletrendszer tehát a következő:

$$\begin{array}{rrrrr} x_1 - x_2 + s_1 & & & = & 1 \\ -x_1 + x_2 & + s_2 & & = & 2 \\ x_2 & & + s_3 & = & 3 \\ \hline x_1 + x_2 & & & = & z \end{array} \tag{2.4}$$

Az ehhez az egyenletrendszerhez tartozó bővített mátrixot szimplex táblának, a feladat megoldását adó eljárást szimplex módszernek vagy szimplex algoritmusnak nevezzük. Ez leegyszerűsítve a szimplex tábla több lépésben való módosításából áll. Az algoritmus kezdő táblája esetünkben a következő:

x_1	x_2	s_1	s_2	s_3	
1	−1	1	0	0	1
−1	1	0	1	0	2
0	1	0	0	1	3
1	1	0	0	0	z

(2.5)

A táblázatba húzott elválasztó vonalak és az első sorba írt változók a jobb áttekinthetőséget segítik. A tankönyvi szimplex táblák sok apróságban különböznek egymástól, van ennél tömörebb alak is, mi kizárólag didaktikai szempontokat vettünk figyelembe.

A Gauss-Jordan-módszer lényeges gondolata az volt, hogy az első lehetséges m lineárisan független oszlop helyén egy egységmátrixot hoztunk létre elemi sorműveletekkel. Most annyit változtatunk ezen, hogy bármely m lineárisan független oszlop helyén ezt megtehetjük, de a sorokat nem rendezzük át, így egységmátrix helyett ezekben az oszlopokban egy permutációmátrixot kapunk. Ez megad egy megoldást az ezen oszlopokhoz tartozó változókra, a többit pedig 0-nak választjuk, ami majd garantálja, hogy a megoldás a lehetséges megoldások poliéderének egy csúcsa legyen. Az, hogy az együtthatómátrixban van egy $m \times m$ -es permutációmátrix, azt jelenti, hogy a hozzájuk tartozó változókat kifejeztük a többi segítségével. Ha e változókra kapott kifejezéseket ezután behelyettesítjük a célfüggvénybe, akkor abban e változók nem fognak szerepelni. Ezt az alakot elemi sorműveletekkel úgy kaphatjuk meg, hogy az $\mathbf{A}$ mátrix alá írt $\mathbf{c}^\mathsf{T}\mathbf{x} = z$ egyenletben is eliminálják a fenti permutációmátrixhoz tartozó változókat. Végezzük el e lépést az ajándékozási feladaton.

Ha a (4) egyenletrendszer első egyenletére tekintünk, látjuk, növelni tudnánk a célfüggvényt, ha s_1 helyett x_1 értéke lenne 1. Ez azt jelenti, hogy míg a poliéder e táblából leolvasható $(0,0,1,2,3)$ pontjához a $z=0$ célfüggvényérték tartozik, egy $(1,0,0,?,?)$ alakú pontban $z=1$ lenne, vagyis közelebb kerülnénk az optimális megoldáshoz. Kiindulva tehát az (5) táblából, válasszuk első oszlopának pozitív elemét főelemnek, és eliminálják az oszlop többi elemét:

x_1	x_2	s_1	s_2	s_3	
1	-1	**1**	0	0	1
-1	1	0	**1**	0	2
0	1	0	0	**1**	3
1	1	0	0	0	z

$\Longrightarrow$

x_1	x_2	s_1	s_2	s_3	
1	-1	1	0	0	1
0	0	1	**1**	0	3
0	1	0	0	**1**	3
0	2	-1	0	0	$z-1$

Az új táblázathoz tartozó megoldás: $(x_1, x_2, s_1, s_2, s_3) = (1,0,0,3,3)$, és mivel az utolsó sor bal oldala most is 0, ezért $z=1$. Még tovább növelhetjük z értékét, ha s_3 rovására növeljük x_2 értékét:

x_1	x_2	s_1	s_2	s_3	
1	-1	1	0	0	1
0	0	1	**1**	0	3
0	**1**	0	0	**1**	3
0	2	-1	0	0	$z-1$

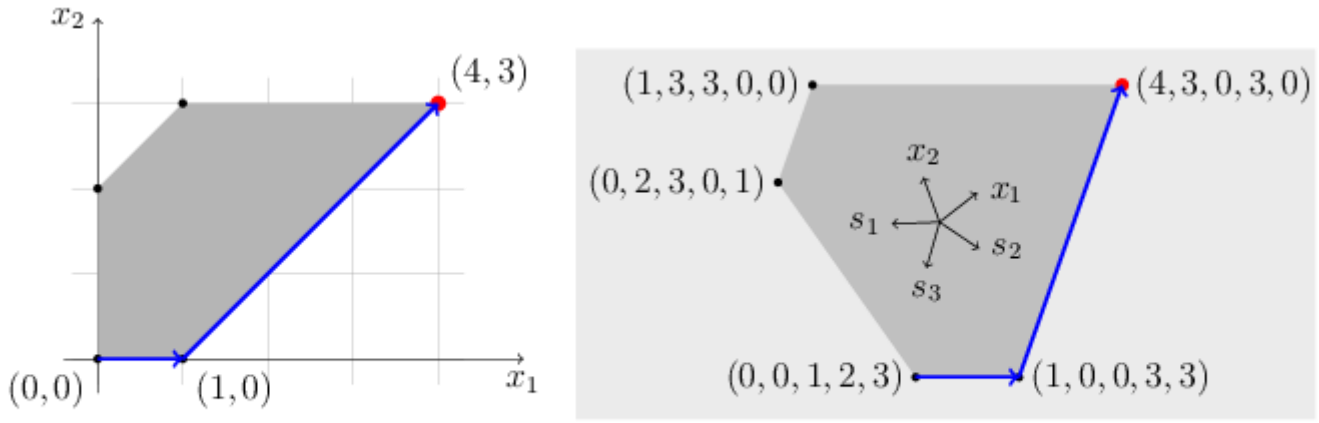
$\Longrightarrow$

x_1	x_2	s_1	s_2	s_3	
1	0	1	0	1	4
0	0	1	**1**	0	3
0	**1**	0	0	1	3
0	0	-1	0	-2	$z-7$

(2.6)

Az innen leolvasható megoldás: $(x_1, x_2, s_1, s_2, s_3) = (4, 3, 0, 3, 0)$, $z = 7$, amivel rá is találtunk az optimális megoldásra. Tovább nem növelhetjük értékét, mert bármely más megengedett megoldásban, sőt, a tér bármely más pontjában a célfüggvény aktuális alakja értéket ad, hisz minden együttható nulla vagy negatív a táblázat legalsó sorának bal oldalán! Így , tehát .

E megoldás csúcsról csúcsra való lépései mind az eredeti 2-dimenziós, mind az 5-dimenziós ábrán jól szemléltethetők, ezt mutatja a 23 ábra.



23. ábra. A szimplex algoritmus követése a 2-dimenziós és az 5-dimenziós térbeli poliéderen.

Végül összefoglaljuk a 2 táblázat segítségével a Gauss-Jordan-módszer és a szimplex módszer közti különbséget.

	Gauss–Jordan-módszer	Szimplex-módszer
Feladat	$\mathbf{Ax} = \mathbf{b}$	$\mathbf{Ax} = \mathbf{b}$, $\mathbf{x} \geqslant \mathbf{0}$, $\mathbf{c}^{\mathsf{T}}\mathbf{x} \to \max$
Feltétel $\mathbf{A}$-ra	nincs	$m \times n$-es, $m < n$, sorfüggetlen
Cél	az összes megoldás meghatározása	egy optimális megoldás megtalálása
Megoldás	affin altér	az affin altér nemnegatív koordinátájú pontjai alkotta poliéder egy csúcsa
Algoritmus célja	elemi sorműveletekkel $\mathbf{A}$-t redukált lépcsős alakra hozni	elemi sorműveletekkel $\mathbf{A}$-t olyan alakra hozni, melyben van egy $m \times m$-es permutációmátrix, és a célfüggvény együtthatói nem pozitívak

2. táblázat. A Gauss-Jordan-módszer és a szimplex módszer összehasonlítása

Standardizálás

Az LP feladat megoldására kidolgozott ún. szimplex módszert azonos alakú feladatokon fogjuk végrehajtani, melyet standard alaknak nevezünk.

2.3. Definíció (LP feladat standard alakja) Az LP feladat standard alakú, ha

1. minden korlátozó feltétele egyenlőség,
2. minden változója nemnegatív,
3. a célfüggvény maximalizálandó.

A standard alakú LP-feladat általános alakja tehát a következő:

$$\begin{aligned} \mathbf{A}\mathbf{x} &= \mathbf{b} \\ \mathbf{x} &\geqslant \mathbf{0} \\ \mathbf{c}^{\mathsf{T}}\mathbf{x} &\to \max \end{aligned} \tag{2.7}$$

2.4. Állítás (Standard alakra hozás) Minden LP feladat standard alakra hozható.

Az átalakítások öteletei nagyon egyszerűek, egy példán szemléltetjük.

2.5. Példa Hozzuk standard alakra az alábbi LP feladatot:

$$\begin{aligned} 2x_1 + x_2 &\leqslant 4 \\ 2x_1 - x_2 &\geqslant 0 \\ x_1 &\geqslant 0 \\ z = -x_1 + 2x_2 &\to \max \end{aligned}$$

Megoldás

Az első feltétel egyenlőséggé tehető egy új változó bal oldalhoz adásával: $2x_1 + x_2 + s_1 = 4$. A célfüggvényen nem változtatunk.

A második egyenlőtlenség bal oldalából egy új nemnegatív változó kivonandó: $2x_1 - x_2 - s_2 = 0$. Ez $-2x_1 + x_2 + s_2 = 0$ alakba is írható. A célfüggvényen nem változtatunk.

Az x_2 változó előjelkorlátozatlan. Mivel minden valós előáll két nemnegatív szám különbségekét, ezért x_2 helyébe minden korlátozó feltételben és a célfüggvényben is helyettesíthetjük az $x_{21} - x_{22}$ kifejezést. Így a következő standard alakú LP feladatra jutunk (mely elé a változást szemléltetendő az eredeti feladatot is felírtuk):

$$
\begin{array}{rcl}
2x_1 + x_2 \leqslant 4 & & 2x_1 + x_{21} - x_{22} + s_1 = 4 \\
2x_1 - x_2 \geqslant 0 & & -2x_1 + x_{21} - x_{22} + s_2 = 0 \\
x_1 \geqslant 0 & \Rightarrow & x_1, \quad x_{21}, \quad x_{22}, \quad s_1, \quad s_2 \geqslant 0 \\
z = -x_1 + 2x_2 \to \max & & z = -x_1 + 2x_{21} - 2x_{22} \to \max .
\end{array}
$$

A 3 táblázatban összefoglaljuk a standard alakra hozás lépéseit.

az eredeti feladatban	az ekvivalens standard alakban
$a_{i1}x_1 + \cdots + a_{in}x_n \leqslant b_i$	$a_{i1}x_1 + \cdots + a_{in}x_n + s_i = b_i$ $s_i \geqslant 0$
$a_{i1}x_1 + \cdots + a_{in}x_n \geqslant b_i$	$a_{i1}x_1 + \cdots + a_{in}x_n - s_i = b_i$ $s_i \geqslant 0$
x_j előjelkorlátozatlan	$x_j = x_{j1} - x_{j2}$ $x_{j1} \geqslant 0,\ x_{j2} \geqslant 0$
$\mathbf{c}^{\mathsf{T}}\mathbf{x} \to \min$	$(-\mathbf{c})^{\mathsf{T}}\mathbf{x} \to \max$

3. táblázat. Egy LP feladat korlátozó feltételeinek és előjelkorlátozatlan változóinak átírása standard alak létrehozásához.

Bázismegoldások

Az ajándékozási példánk megoldásánál láttuk, amit a 22 ábrán szemléltettünk is, hogy a standard alakú feladathoz tartozó poliéder csúcsainak mindegyikében 2 koordináta 0. Ez általánosítható:

2.6. Állítás Az m -rangú $m \times n$ -es $\mathbf{A}$ mátrixszal fölírt

$$\mathbf{Ax} = \mathbf{b}, \quad \mathbf{x} \geqslant \mathbf{0} \tag{2.8}$$

egyenlőtlenségrendszer összes megoldásának $\mathcal{P}$ poliéderén minden csúcspont koordinátái közt van $n - m$ darab 0.

Bizonyítás. Tegyük fel, hogy $\bar{\mathrm{x}}$ a $\mathcal{P}$ poliéder egy csúcsa. Mivel $\mathbf{A}\bar{\mathrm{x}} = \mathrm{b}$, ezért $\bar{\mathrm{x}}$ rajta van m hipersíkon. Hogy egyértelmű megoldás legyen, még rajta kell lennie $n - m$ további hipersíkon, azok viszont mind csak a nemnegativitási feltételekből valók lehetnek. Egyenletük $\bar{x}_i = 0$, azaz $\mathbf{e}_i^{\mathsf{T}}\bar{\mathrm{x}} = 0$ alakú, tehát találtunk $n - m$ koordinátát, ami 0. [QED]

Ez a következő definícióhoz vezet:

2.7. Definíció (Bázismegoldás) A standard (8) alakú egyenlőtlenségrendszer egy $\bar{\mathrm{x}}$ megoldását bázismegoldásnak nevezzük, ha $\bar{\mathrm{x}}$-nak van m olyan koordinátája, hogy az $\mathbf{A}$ azonos indexű oszlopvektorai lineárisan függetlenek, az $\bar{\mathrm{x}}$ maradék koordinátái pedig mind nullák. A kiemelt m indexhez tartozó változókat bázisváltozóknak nevezzük. Ha az $\bar{\mathrm{x}}$ bázismegoldásnak több mint $n-m$ koordinátája 0, akkor degenerált bázismegoldásnak nevezzük.

Az $\mathbf{A}$ oszlopvektoraira vonatkozó kikötés szükséges, enélkül ugyanis a fenti bizonyításban konstruált egyenletrendszernek nem csak egy megoldása lenne, ez pedig szükséges ahhoz, hogy $\bar{\mathrm{x}}$ csúcspont legyen.

A lineáris programozás alaptétele

A szimplex módszer arra a felismerésre épül, hogy az LP feladat optimális megoldását elég a bázismegoldások közt keresni. Ezt biztosítja a lineáris programozás alaptétele.

2.8. Tétel (A lineáris programozás alaptétele) Ha a standard alakban adott LP feladatnak van lehetséges megoldása (azaz megoldható), és a célfüggvény a lehetséges megoldások halmazán felülről korlátos, akkor van optimális bázismegoldása.

A tételből azonnal következik az az állítás is, hogy ha a standard LP feladatnak van optimális megoldása, akkor van optimális bázismegoldása is. Másrészt következik az is, hogy ha a standard LP feladatnak van lehetséges megoldása, de nincs optimális, akkor az csak azért lehet, mert a célfüggvény nem korlátos a lehetséges megoldások halmazán.

Bizonyítás. Elég lesz megmutatni, hogy ha a tétel feltételeinek teljesülése mellett $\mathbf{x}$ egy lehetséges megoldás, akkor létezik olyan $\bar{\mathrm{x}}$ bázismegoldás, hogy $\mathbf{c}^{\mathsf{T}}\bar{\mathrm{x}} \geqslant \mathbf{c}^{\mathsf{T}}\mathbf{x}$. Ha ugyanis minden lehetséges megoldáshoz találunk olyan bázismegoldást, melyben a célfüggvény értéke nem kisebb, akkor a bázismegoldások számának végessége és a célfüggvény felülről való korlátossága miatt találunk olyan bázismegoldást is, mely optimális.

Legyen tehát $\mathbf{x}$ egy lehetséges megoldás, és $\bar{\mathrm{x}}$ egy olyan megoldás, melyre $\mathbf{c}^{\mathsf{T}}\bar{\mathrm{x}} \geqslant \mathbf{c}^{\mathsf{T}}\mathbf{x}$, és $\bar{\mathrm{x}}$-ban a lehetséges legtöbb koordináta nulla. Legyen I az $\bar{\mathrm{x}}$ pozitív koordinátáihoz tartozó indexek halmaza, azaz $I = \{\, i \in \{1,2,\ldots,n\} \mid \bar{x}_i > 0 \,\}$, és jelölje $\mathcal{A}_I$ az $\mathbf{A}$ mátrix I-be eső indexű oszlopvektorainak halmazát.

Ha $\mathcal{A}_I$ lineárisan független vektorokból áll, akkor $|I| \leqslant m$, hisz $\mathbf{A}$ rangja m.
Ha $|I| = m$, kész is vagyunk, ekkor $\bar{\mathrm{x}}$ definíció szerint bázismegoldás.
Ha $|I| < m$, akkor - mivel $\mathbf{A}$ oszlopterének dimenziója m -, $\mathcal{A}_I$ kiegészíthető az

oszloptér bázisává, azaz léteznek további vektorok $\mathbf{A}$ oszlopai közt, melyekkel egy független m -elemű rendszert kapunk. Tehát $\bar{\mathrm{x}}$ bázismegoldás, igaz degenerált, mivel több mint $n-m$ koordinátája nulla.

Megmutatjuk, hogy $\mathcal{A}_I$ nem lehet lineárisan összefüggő. Indirekt módon tegyük fel, hogy az, azaz létezik vektorainak egy nullvektort adó lineáris kombinációja. E feltevés azt jelenti, hogy létezik egy olyan $\mathbf{y}$ vektor, melyre $\mathbf{Ay}=\mathbf{0}$, és $y_i=0$, ha $i \notin I$. Ekkor ugyanis az y_i ($i \in I$) együtthatók adják az $\mathcal{A}_I$ vektorainak zérusvektort adó lineáris kombinációját.

Az $\mathbf{y}$ vektorról föltehető, hogy legalább egy koordinátája negatív, ellenkező esetben megszorozzuk -1-gyel. Sőt, az is föltehető, hogy $\mathbf{c}^{\mathsf{T}}\mathbf{y} \geqslant 0$. Tegyük fel ugyanis, hogy $\mathbf{c}^{\mathsf{T}}\mathbf{y}<0$. Ha ezen nem tudunk változtatni egy -1-gyel való beszorzással, akkor $\mathbf{y}$-nak egy koordinátája sem lehet pozitív, azaz $\mathbf{y} \leqslant \mathbf{0}$. Legyen $\mathbf{x}_\varepsilon=\bar{\mathrm{x}}+\varepsilon\mathbf{y}$. Ha $\varepsilon<0$, akkor $\mathbf{x}_\varepsilon \geqslant \mathbf{0}$, másrészt $\mathbf{A}\mathbf{x}_\varepsilon=\mathbf{A}\bar{\mathrm{x}}+\varepsilon\mathbf{A}\mathbf{y}=\mathbf{b}$, azaz $\mathbf{x}_\varepsilon$ lehetséges megoldás, ugyanakkor $\mathbf{c}^{\mathsf{T}}\mathbf{x}_\varepsilon=\mathbf{c}^{\mathsf{T}}\bar{\mathrm{x}}+\varepsilon\mathbf{c}^{\mathsf{T}}\mathbf{y}$, ami nem korlátos, ha $\varepsilon \to -\infty$.

Összefoglalva: indirekt feltevésünk szerint létezik egy olyan $\mathbf{y}$ vektor, hogy $\mathbf{Ay}=\mathbf{0}$, $\mathbf{y}$-nak van negatív koordinátája, és $\mathbf{c}^{\mathsf{T}}\mathbf{y} \geqslant 0$. Megmutatjuk, hogy ez ellentmond az $\bar{\mathrm{x}}$ definíciójának. Legyen $\mathbf{x}_\varepsilon=\bar{\mathrm{x}}+\varepsilon\mathbf{y}$ mint előbb, de most legyen $\varepsilon \geqslant 0$. Ha ε -t 0-tól indulva „lassan” növeljük, akkor $\mathbf{x}_\varepsilon \geqslant \mathbf{0}$, tehát lehetséges megoldás mindaddig, amíg $\varepsilon<\varepsilon_0=\min\{x_i/y_i \mid y_i<0\}$. Amint azonban $\varepsilon=\varepsilon_0$, az $\mathbf{x}_\varepsilon$ pozitív koordinátáinak száma legalább eggyel csökken, ami ellentmond $\bar{\mathrm{x}}$ definíciójának. [QED]

A szimplex tábla, és a hozzá tartozó bázismegoldás

A standard (7) alakú LP feladathoz vagy az abból elemi sorműveletekkel kapott ekvivalens feladathoz a következő táblázatot fogjuk rendelni:

x_1	x_2	$\dots$	x_n	
a_{11}	a_{12}	$\dots$	a_{1n}	b_1
$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$
a_{m1}	a_{m2}	$\dots$	a_{mn}	b_m
c_1	c_2	$\dots$	c_n	$z-z_0$

mátrixjelöléssel

$\mathbf{x}^{\mathsf{T}}$	
$\mathbf{A}$	$\mathbf{b}$
$\mathbf{c}^{\mathsf{T}}$	$z-z_0$

(2.9)

ahol $\mathbf{x}^{\mathsf{T}}$ helyén csak e vektor koordinátáinak neve szerepel, és z csak a célfüggvényt megadó változó neve. Ezek csak a táblázat értelmezését segítik, akár el is hagyhatók. Az $\mathbf{A}$, $\mathbf{b}$, $\mathbf{c}$ és z_0 értéke viszont a szimplex algoritmus során lépésről lépésre változhat. (A standard LP-feladatban $z_0=0$, mivel $\mathbf{c}^{\mathsf{T}}\mathbf{x}=z$, de

az elemi sorműveletek eredményeként z mellett nem nulla konstans is megjelenhet.)

Néhány jelölés a továbbiakhoz. Legyen $\mathcal{B} \subset \{1, 2, \ldots, n\}$ az oszlopindexek egy m -elemű rendezett részhalmaza, és $\mathcal{N}$ a komplementer halmaz, azaz $\mathcal{N} = \{1, 2, \ldots, n\} \setminus \mathcal{B}$. Jelölje az $\mathbf{A}$ mátrix ezen indexekhez tartozó részmátrixait $\mathbf{A}_\mathcal{B}$ és $\mathbf{A}_\mathcal{N}$. Ezek mérete $m \times m$, illetve $m \times (n - m)$. Hasonlóképp jelölje $\mathbf{c}_\mathcal{B}$, $\mathbf{x}_\mathcal{B}$, $\mathbf{c}_\mathcal{N}$, $\mathbf{x}_\mathcal{N}$ a $\mathbf{c}$ és $\mathbf{x}$ vektorok megfelelő részvektorait. Az előbbiek m -, az utóbbiak $(n - m)$ -dimenziósak.

2.9. Definíció (Szimplex tábla) Egy standard alakú, vagy abból elemi átalakításokkal kapott ekvivalens feladathoz rendelt (9) alakú táblázatot szimplex táblának nevezzük, ha eleget tesz a következő tulajdonságoknak:

1. $\mathbf{b} \geqslant \mathbf{0}$,
2. van az oszlopindexeinek egy olyan m -elemű rendezett $\mathcal{B}$ halmaza, hogy $\mathbf{A}_\mathcal{B}$ az egységmátrix (azaz a $\mathcal{B}$ indexeihez tartozó oszlopokban egy permutációmátrixot látunk),
3. $\mathbf{c}_\mathcal{B} = \mathbf{0}$.

Hamarosan részletezzük, hogy hogyan alakítható át egy standard LP-feladat úgy, hogy már az indulásnál eleget tegyen e feltételeknek, és hogyan őrizhetők meg e tulajdonságok az algoritmus lépései közben is. Célunk tehát az LP-feladatot olyan alakban tartani, hogy létezzék szimplex táblája.

Ha egy LP-feladathoz tartozó (9) alakú táblázat szimplex tábla, akkor az $\mathbf{Ax} = \mathbf{b}$, $\mathbf{x} \geqslant \mathbf{0}$ egyenlőtlenségrendszernek $\mathbf{x}_\mathcal{B} = \mathbf{A}_\mathcal{B}^{-1}\mathbf{b} = \mathbf{b}$ és $\mathbf{x}_\mathcal{N} = \mathbf{0}$ egy bázismegoldása, ami azonnal látszik az $\mathbf{A}_\mathcal{B}\mathbf{x}_\mathcal{B} = \mathbf{b}$, $\mathbf{A}_\mathcal{B} = \mathbf{I}$ és $\mathbf{b} \geqslant \mathbf{0}$ összefüggésekből. Mivel pedig $\mathbf{c}_\mathcal{B} = \mathbf{0}$ ezért

$$\mathbf{c}^\mathsf{T}\mathbf{x} = \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{x}_\mathcal{B} + \mathbf{c}_\mathcal{N}^\mathsf{T}\mathbf{x}_\mathcal{N} = \mathbf{0}^\mathsf{T}\mathbf{x}_\mathcal{B} + \mathbf{c}_\mathcal{N}^\mathsf{T}\mathbf{0} = 0,$$

vagyis a célfüggvényt leíró egyenlet bal oldala a szimplex táblában mindig 0, így a jobb oldalon megjelenő z_0 konstans lesz a célfüggvénynek az adott bázismegoldáshoz tartozó értéke.

Optimális megoldás

Mikor oldottuk meg, az LP-feladatot? Hogyan olvasható le a szimplex tábláról, hogy a hozzá tartozó bázismegoldás optimális?

2.10. Állítás Ha $\mathbf{c}_\mathcal{N} \leqslant \mathbf{0}$, akkor a bázismegoldás optimális.

Bizonyítás. $z - z_0 = \mathbf{c}^{\mathsf{T}}\mathbf{x} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{x}_{\mathcal{B}} + \mathbf{c}_{\mathcal{N}}^{\mathsf{T}}\mathbf{x}_{\mathcal{N}} = \mathbf{c}_{\mathcal{N}}^{\mathsf{T}}\mathbf{x}_{\mathcal{N}}$, és a jobb oldali kifejezés bármely $\mathbf{x} \geqslant \mathbf{0}$ esetén $\leqslant \mathbf{0}$, ami a maximumát $\mathbf{x}_{\mathcal{N}} = \mathbf{0}$ esetén veszi fel, vagyis épp e táblához tartozó bázismegoldásban. [QED]

1. lépés: a bázisba kerülő oszlop kiválasztása

A szimplex algoritmus minden lépésének két fontos feltételt ki kell elégítenie: a célfüggvény értéke nem csökkenhet, és táblája szimplex tábla kell, hogy maradjon. A $\mathcal{B}$ bázisba kerülő oszlop kiválasztásának szabálya egyszerű: csak olyan nem-bázis oszlop választható a bázisoszlopok közé, mely alatt a célfüggvény együtthatója pozitív! Ennek oka, hogy csak ilyen változó értékének növelése fogja a célfüggvény értékét is növelni. Ha több ilyen oszlop is van, bármelyiket választhatjuk!

Danzig eredeti javaslata szerint azt az oszlopot érdemes választani, amelyik a célfüggvény legnagyobb együtthatójához tartozik, mert pl. eggyel növelve a hozzá tartozó változó értékét, itt lesz a legnagyobb a célfüggvény növekedése. Ez ugyan igaz, de mivel oszloponként változó, hogy legföljebb mennyivel lehet növelni a változó értékét, nem mindig ez a választás vezet leggyorsabban a cél felé!

2. lépés: a főelem kiválasztása

Az oszlop kiválasztása után egy sort is ki kell választani, melyek kereszteződésében lévő főelemmel eliminálju a kiválasztott oszlop többi elemét. Mivel az eliminációközben nem fordulhat elő, hogy az egyenletrendszer jobb oldalán negatív szám jelenjen meg, azt a sort kell választani, amelyre a jobb oldali elem és a főelem hányadosa minimális. Összefoglalva: ha a kiválasztott oszlop indexe j, akkor olyan sor választandó, melynek i indexére:

$$\frac{b_i}{a_{ij}} = \min_i k \left\{ \frac{b_k}{a_{kj}} \;\middle|\; a_{kj} > 0 \right\}.$$

Ha több ilyen sor is van, bármelyiket választhatjuk. Ha ilyen sor nincs, azaz $a_{kj} \leqslant 0$, akkor x_j tetszőlegesen nagynak választva is kielégíti az egyenletrendszert a bázisváltozók megfelelő megváltoztatása mellett, így viszont a célfüggvény tetszőlegesen naggyá válik, azaz a feladatnak nincs optimális megoldása!

A főelem oszlopának és sorának kiválasztására több különböző szabály is létezik, melyek vagy az algoritmus gyorsaságát növelik, vagy valamely elméleti kérdés tisztázását segítik, ezeket itt nem részletezzük.

3. lépés: eliminálás

A főelem kiválasztása után a szokásos elemi sorműveletekkel az oszlopot standard egységvektorrá transzformáljuk. Ha a főelem a k -adik sor és a j -edik oszlop kereszteződésében van, akkor ez annak felel meg, hogy az x_j változót kifejezzük a k -adik egyenletből, és behelyettesítjük az összes többi egyenletbe, valamint a célfüggvénybe. Ezután e három lépés ismétlésével vagy megtalálunk egy optimális megoldást, mert az utolsó sorban csupa nemnegatív együttható áll, vagy igazoljuk, hogy a feladatnak nincs optimális megoldása.

E lépéseket kövessük végig egy egyszerű feladaton.

2.11. Példa Oldjuk meg a parfümökről szóló 2.2 példához tartozó LP-feladatot!

$$\begin{aligned} x_1 + 4x_2 &\leqslant 16 \\ x_1 + \ x_2 &\leqslant 7 \\ 2x_1 + \ x_2 &\leqslant 12 \\ x_1, \quad x_2 &\geqslant 0 \\ z = 3x_1 + 4x_2 &\to \max \end{aligned}$$

Megoldás

Először hozzuk a feladatot három új változó bevezetésével standard alakra, majd írjuk fel a tábláját, mely az új változók miatt azonnal szimplex tábla:

x_1	x_2	x_3	x_4	x_5	
1	4	1	0	0	16
1	1	0	1	0	7
2	1	0	0	1	12
3	4	0	0	0	z

Az első két oszlop bármelyikét választhatjuk, mert $3 \geqslant 0$ és $4 \geqslant 0$. Válasszuk a második oszlopot (követve Danzig tanácsát)! Ekkor az alábbi halmaz minimumát keressük a főelem kiválasztásához: $\{\frac{16}{4}, \frac{7}{1}, \frac{12}{1}\}$. A minimum 4, amit csak az első sorban kapunk meg, így ezt az elemet kell kiválasztanunk.

x_1	x_2	x_3	x_4	x_5	
1	**4**	1	0	0	16
1	1	0	1	0	7
2	1	0	0	1	12
3	4	0	0	0	z

$\to$

x_1	x_2	x_3	x_4	x_5	
$\frac{1}{4}$	1	$\frac{1}{4}$	0	0	4
$\frac{3}{4}$	0	$-\frac{1}{4}$	1	0	3
$\frac{7}{4}$	0	$-\frac{1}{4}$	0	1	8
2	0	-1	0	0	$z - 16$

Ezután az oszlopok közül már csak az első választható ki. A sor kiválasztásához

$$\min\left\{\frac{4}{\frac{1}{4}}, \frac{3}{\frac{3}{4}}, \frac{8}{\frac{7}{4}}\right\} = \min\left\{16, 4, \frac{32}{7}\right\} = 4,$$

és ezt a minimumot a második sorban kapjuk.

x_1	x_2	x_3	x_4	x_5	
$\frac{1}{4}$	1	$\frac{1}{4}$	0	0	4
$\frac{3}{4}$	0	$-\frac{1}{4}$	1	0	3
$\frac{7}{4}$	0	$-\frac{1}{4}$	0	1	8
2	0	-1	0	0	$z-16$

$\rightarrow$

x_1	x_2	x_3	x_4	x_5	
0	1	$\frac{1}{3}$	$-\frac{1}{3}$	0	3
1	0	$-\frac{1}{3}$	$\frac{4}{3}$	0	4
0	0	$\frac{1}{3}$	$-\frac{7}{3}$	1	1
0	0	$-\frac{1}{3}$	$-\frac{8}{3}$	0	$z-24$

A feladat megoldása tehát $x_1 = 4$, $x_2 = 3$, a célfüggvény értéke e helyen $z = 24$ (a segédváltozók értékei $x_3 = x_4 = 0$, $x_5 = 1$).

Az induló tábla konstrukciója

A standard LP-feladatbeli $\mathbf{A}$ mátrixban általában nem található $m \times m$ -es részmátrix, ami permutációmátrix lenne, és a $\mathbf{b} \geqslant \mathbf{0}$ feltétel sem teljesül automatikusan. Az utóbbival könnyű elbánni, azt az egyenletet, amelynek jobb oldalán negatív szám áll, szorozzuk be -1-gyel, így egy ekvivalens feladatot kaptunk, ahol $\mathbf{b} \geqslant \mathbf{0}$. A standard LP-feladathoz ezután a következő segédfeladatot konstruáljuk. Az $\mathbf{x}$ vektort új változókkal $(n+m)$-változóssá bővítjük, az új változókat jelölje x_{n+1}, x_{n+2},..., x_{n+m}, a bővített vektort $\bar{\mathrm{x}}$.

$$[\mathbf{A} \mid \mathbf{I}_m]\bar{x} = \mathbf{b}$$

$$\mathrm{x} \geqslant \mathbf{0}$$

$$z' = -(x_{n+1} + x_{n+2} + \ldots + x_{n+m}) \rightarrow \max . (2.10)$$

Az eredeti LP-feladat pontosan akkor oldható meg, ha e segédfeladat bármely optimális megoldásában $x_{n+1} = x_{n+2} = \ldots = x_{n+m} = 0$. Egyrészt ha (10) egy optimális megoldásában $x_{n+1} = x_{n+2} = \ldots = x_{n+m} = 0$, akkor ahhoz nyilván tartozik a standard feladat egy megengedett megoldása. Másrészt ha a standard feladat egy megengedett megoldásához hozzávesszük az $x_{n+1} = x_{n+2} = \ldots = x_{n+m} = 0$ értékeket, akkor (10) egy optimális megoldását kapjuk, hisz a célfüggvény értéke ekkor 0, annál nagyobb pedig nem lehet.

E segédfeladat láthatóan megoldható, hisz van megengedett megoldása (mégpedig $x_1 = x_2 = \cdots = x_n = 0$, $x_{n+j} = b_j$), és felülről korlátos (a célfüggvénynek 0 felső korlátja). Az optimális megoldást megkapjuk a szimplex módszerrel, hisz induló táblája szimplex táblává válik, ha azonos átalakításként az egyenletrendszer minden sorát a célfüggvénysorhoz adjuk. Ebből azonnal leolvasható egy induló megoldás az x_{n+1}, x_{n+2},..., x_{n+m} változókra és annak célfüggvényértéke. Ha az optimális megoldásra

az $x_{n+1} = x_{n+2} = \ldots = x_{n+m} = 0$ feltétel nem teljesül, az eredeti feladatnak nincs megengedett megoldása! Ha teljesül, és az összes bázisváltozó az x_1 ,..., x_n változók közül kerül ki, akkor kész vagyunk, a segédfeladat első n oszlopa az utolsó oszloppal és az eredeti célfüggvénnyel együtt az eredeti feladat egy olyan táblája, melyben van permutációmátrix, így az eredeti célfüggvény megfelelő együtthatóinak eliminálásával szimplex táblává válik, ahonnan a szimplex módszerrel már megoldható lesz. Végül abban az esetben, ha az új változók közt van bázisváltozó, akkor az optimális megoldásban m -nél kevesebb a nemzérus elem, az ezekhez tartozó oszlopok mellé $\mathbf{A}$-ban találhatunk tőlük független oszlopot, mely bevehető a bázisba, így ekkor is elérhető, hogy végül az eredeti feladat egy megengedett bázismegoldásához jussunk.

Példaként a 21 második ábráján bemutatott poliéderhez (szakaszhoz) konstruálunk LP-feladatot. A két egyenlet legyen az ott megadott két sík egyenlete.

2.12. Példa Oldjuk meg az

$$\begin{aligned} x_1 + \ x_2 + 2x_3 &= 5 \\ x_1 + 2x_2 + 3x_3 &= 6 \\ x_1, \quad x_2, \quad x_3 &\geqslant 0 \\ z = 2x_1 + \ x_2 + \ x_3 &\to \max \end{aligned}$$

LP-feladatot.

Megoldás

A feladat táblája nem szimplex tábla, ezért két új változó bevetésével egy segédfeladatot kreálunk. Az első két sort a célfüggvény sorához adjuk,

x_1	x_2	x_3	x_4	x_5	
1	1	2	1	0	5
1	2	3	0	1	6
0	0	0	−1	−1	z'

$\rightarrow$

x_1	x_2	x_3	x_4	x_5	
1	1	2	1	0	5
1	2	3	0	1	6
2	3	5	0	0	$z' + 11$

amivel máris szimplex táblához jutottunk, amelyen működik az algoritmus. Először vonjuk le az első sort a másodikból (pivotelem az első oszlopban), majd a második sort az elsőből (pivotelem a második oszlopban):

x_1	x_2	x_3	x_4	x_5	
1	1	2	1	0	5
0	1	1	−1	1	1
0	1	1	−2	0	$z' + 1$

$\rightarrow$

x_1	x_2	x_3	x_4	x_5	
1	0	1	2	−1	4
0	1	1	−1	1	1
0	0	0	−1	−1	z'

Ezután visszatérünk az eredeti célfüggvényhez, és a célfüggvény bázismegoldás -2 alatti elemeinek eliminálásával ~~a~~ lismét szimplex táblához jutunk. Ezt az első sor -szeresének és a második sor -szeresének a célfüggvény sorához való adásával érjük el.

x_1	x_2	x_3	x_4	x_5	
1	0	1	2	-1	4
0	1	1	-1	1	1
2	1	1	0	0	z

$\rightarrow$

x_1	x_2	x_3	x_4	x_5	
1	0	1	2	-1	4
0	1	1	-1	1	1
0	0	-2	-3	1	$z-9$

Ezután a szimplex algoritmus egyetlen lépésével megoldjuk a feladatot:

x_1	x_2	x_3	x_4	x_5	
1	1	2	1	0	5
0	1	1	-1	1	1
0	-1	-3	-2	0	$z-10$

Ez az $(x_1, x_2, x_3) = (5, 0, 0)$ megoldást adja, melyben valóban $2x_1 + x_2 + x_3 = 10$ a célfüggvény értéke.

2.4 Dualitás

Az esztétikailag szép matematikai eredmények és a nem triviális alkalmazások találkozásának egyik meggyőző példáját nyújtja a dualitás-tétel. A lineáris programozási feladat dualitásának fogalmát egy geometriai dualitásfogalmon keresztül közelítjük meg.

Kúpok

Alkalmazásokban egyes változók nem lehetnek negatívak, így különösen érdekesek a térnek olyan részhalmazai, melyekből nem vezet ki a nemnegatív együtthatókkal vett lineáris kombináció. E halmazok a kúpok.

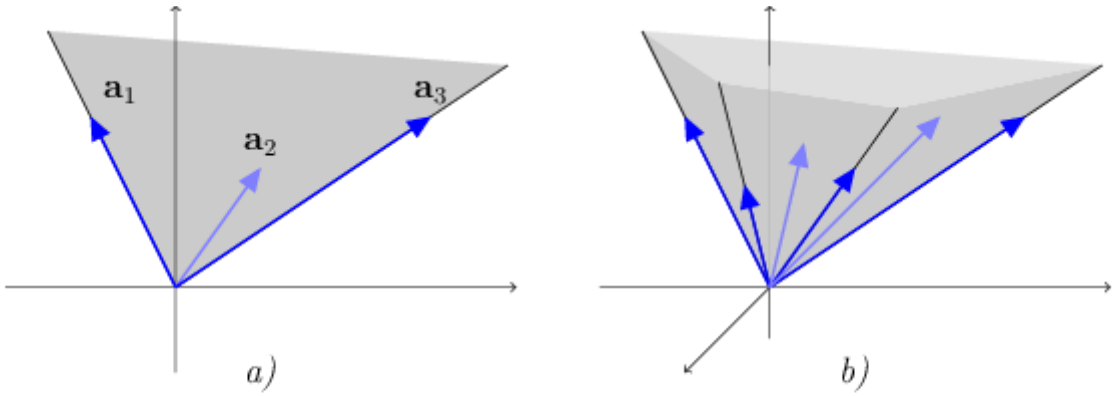
2.13. Definíció (Véges kúp) $\mathbb{R}^m$ -beli vektorok egy $\mathcal{C}$ halmazát kúpnak nevezzük, ha $\mathcal{C}$ elemeinek bármely nemnegatív lineáris kombinációja is $\mathcal{C}$ -beli. $\mathcal{C}$ véges kúp vagy polihedrikus kúp, ha véges sok vektor generálja, azaz találunk olyan $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n \in \mathbb{R}^m$ vektort, hogy

$$\mathcal{C} = \{\, \mathbf{y} \mid \mathbf{y} = x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n,\ x_1, x_2, \ldots, x_n \geqslant 0 \,\}$$

Az $\mathbf{A} = [\mathbf{a}_1 | \mathbf{a}_2 | \ldots | \mathbf{a}_n]$ jelöléssel

$$\mathcal{C} = \{\, \mathbf{y} \mid \mathbf{y} = \mathbf{A}\mathbf{x},\ \mathbf{x} \geqslant \mathbf{0} \,\}.$$

Egy síkbeli és egy térbeli véges kúpot szemléltet a 24 ábra. A 3-dimenziós tér véges kúpjaira elemi geometriai tanulmányaink alapján inkább azt mondanánk, hogy origó-csúcsú végtelen gúlák, ahol a végesség az oldallapok, illetve az élek számára vonatkozik.



24. ábra. *a)* Egy síkbeli ($\mathbf{a}_1$ és $\mathbf{a}_3$ által kifeszített) kúp. $\mathbf{a}_2$ a kúpba esik, ezért $\mathbf{a}_1$, $\mathbf{a}_2$ és $\mathbf{a}_3$ ugyanezt a kúpot feszíti ki. *b)* Egy térbeli (négy vektor által kifeszített) kúp, két – a kúpba eső – további vektorral, így e hat vektor ugyanazt a kúpot feszíti ki.

Igazolható, és szemléletesen világosnak tűnik, hogy egy véges kúp - mint ponthalmaz - zárt. Megjegyezzük, hogy ez az állítás nem igaz tetszőleges (nem véges) kúpra (konstruáljunk pl. olyan kúpot, melyből az origót elhagyva nyílt halmazt kapunk).

Igazolható az az állítás is, hogy - hasonlóan a poliéderekhez -, minden véges kúp előáll véges sok féltér metszeteként. Ráadásul e féltereket határoló hipersíkok mindegyike átmegy az origón, tehát a félterek mindegyikéhez létezik olyan $\mathbf{b}$ vektor, hogy egyenlete $\mathbf{b} \cdot \mathbf{x} \leqslant 0$ alakú. Eszerint minden $\mathcal{C}$ kúphoz található olyan $\mathbf{B}$ mátrix, hogy

$$\mathcal{C} = \{ \mathbf{x} \mid \mathbf{x}^{\mathsf{T}}\mathbf{B} \leqslant \mathbf{0} \}$$

A véges kúpok ezen előállítása vezet a kúp duálisának fogalmához:

2.14. Definíció (Kúp duálisa) A $\mathcal{C} = \{ \mathbf{y} \mid \mathbf{y} = \mathbf{A}\mathbf{x},\ \mathbf{x} \geqslant \mathbf{0} \}$ kúp duálisán a

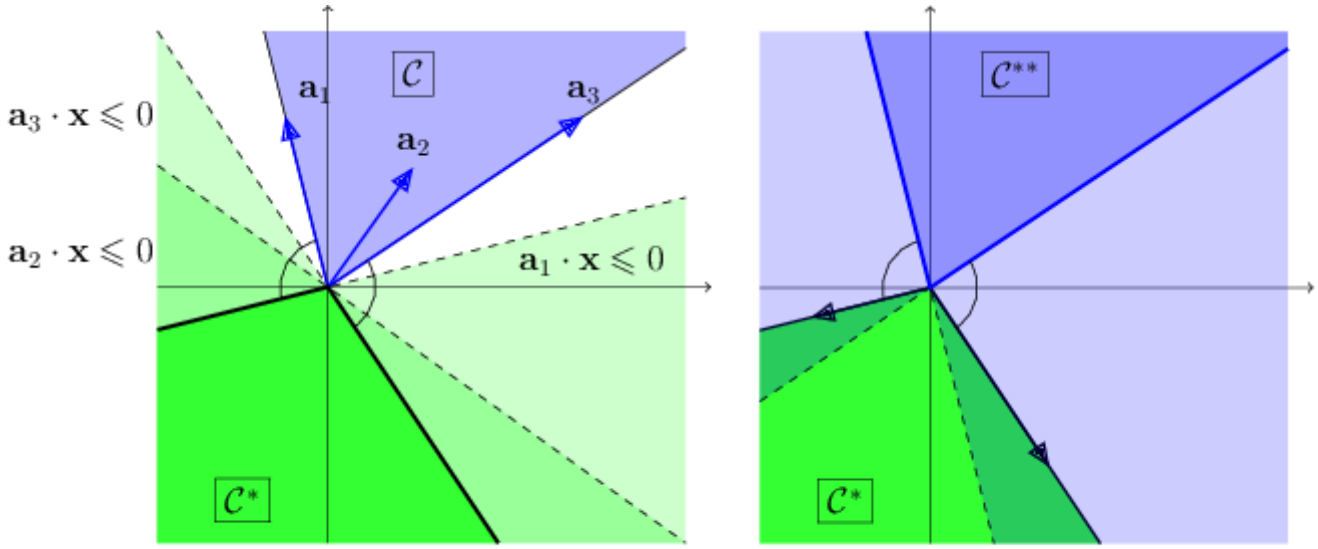
$$\mathcal{C}^* = \{ \mathbf{z} \in \mathbb{R}^m \mid \forall \mathbf{y} \in \mathcal{C} \text{ esetén } \mathbf{z}^{\mathsf{T}}\mathbf{y} \leqslant 0 \} \tag{2.11}$$

halmazt értjük. Szavakban: egy kúp duálisába azok a vektorok tartoznak, amelyeknek a kúp bármely vektorával bezárt szöge legalább derékszög.

Könnyen látható, hogy véges kúp duálisa véges kúp (általában is kúp duálisa kúp). Ráadásul a definícióbeli $\mathcal{C}$ kúpra az $\mathbf{y} = \mathbf{A}\mathbf{x}$ behelyettesítéssel kapjuk, hogy

$$\begin{aligned} \mathcal{C}^* &= \left\{ \mathbf{z} \in \mathbb{R}^m \;\middle|\; \forall \mathbf{x} \geqslant \mathbf{0} \text{ esetén } \mathbf{z}^\mathsf{T}\mathbf{A}\mathbf{x} \leqslant 0 \right\} \\ &= \left\{ \mathbf{z} \in \mathbb{R}^m \;\middle|\; \mathbf{z}^\mathsf{T}\mathbf{A} \leqslant 0 \right\} \end{aligned}$$

Ez tehát azt jelenti, hogy az $\mathbf{a}_1, \mathbf{a}_2 \ldots, \mathbf{a}_n$ vektorok által kifeszített kúp duálisa az ilyen normálvektorú félterek metszete. Ezt szemlélteti a 25 ábra első képe. A 2-dimenziós esetben nagyon egyszerűen leolvasható az ábráról, hogy a duális duálisa, amit jelöljön $\mathcal{C}^{**}$ megegyezik $\mathcal{C}$ -vel. Ez magasabb dimenzióban nem látszik ennyire egyszerűen. Erről szól a következő paragrafus.



25. ábra. A $\mathcal{C}$ kúp és $\mathcal{C}^*$ duálisa, majd a duális $\mathcal{C}^{**}$ duálisa, ami láthatóan megegyezik $\mathcal{C}$-vel

Farkas-lemma

A Farkas-lemma igen széles körben fölhasznált eredmény. Egyik fontos következménye a lineáris programozás alaptételének tekinthető dualitástétel.

A Farkas-lemma talán legelegánsabb, és legegyszerűbben kimondható alakja a következő:

2.15. Tétel (Farkas-lemma -- kúp duálisáról) Véges kúp duálisának duálisa megegyezik az eredeti kúppal, azaz minden véges $\mathcal{C}$ kúpra $\mathcal{C}^{**} = \mathcal{C}$.

Bizonyítás. A $\mathcal{C} \subseteq \mathcal{C}^{**}$ tartalmazás nyilvánvaló, hisz a kúp duálisának (11)-beli definíciója alapján $\mathcal{C}^*$ bármely $\mathbf{z}$ elemének és $\mathcal{C}$ bármely $\mathbf{y}$ elemének hajlásszöge legalább derékszög, így $\mathbf{y} \in \mathcal{C}^{**}$ is fönnáll.

A fordított $\mathcal{C}^{**} \subseteq \mathcal{C}$ tartalmazás bizonyításához megmutatjuk, hogy ha $\mathbf{w} \notin \mathcal{C}$, akkor $\mathbf{w} \notin \mathcal{C}^{**}$. Tegyük fel tehát, hogy $\mathbf{w} \notin \mathcal{C}$. Föl fogunk használni egy olyan

eredményt, melynek bizonyítását itt nem közöljük, de amelynek tartalma jól érthető, szemléletesen világos. Minkowski ún. hipersík-szeparációs tétele szerint két zárt, konvex, diszjunkt halmaz szétválasztható egy hipersíkkal, ha legalább egyikük korlátos is.[4] (A bizonyítás alapötlete az, hogy a két halmaz egymáshoz legközelebb fekvő pontjainak távolsága 0-nál nagyobb, és az őket összekötő szakaszt merőlegesen metsző bármely hipersík egyik oldalán lesz az egyik halmaz, másik oldalán a másik.) Nekünk annyit is elég lenne bizonyítani, hogy egy $\mathcal{C}$ véges kúp, és egy rajta kívül fekvő $\mathbf{w}$ pont egy hipersíkkal elválasztható. Megmutatható, hogy olyan hipersík is létezik, mely átmegy az origón (azaz tartalmazza a kúp csúcsát, de a kúp többi része az egyik, a pont a másik oldalán van). Egy ilyen origón átmenő hipersík egyenlete $\mathbf{b}^\mathsf{T}\mathbf{x} = 0$ alakra hozható, ahol $\mathbf{b}$ a hipersík normálvektora, és $\mathbf{b}^\mathsf{T}\mathbf{w} > 0$, $\mathbf{b}^\mathsf{T}\mathbf{A} \leqslant \mathbf{0}$ (ahol $\mathbf{A}$ a $\mathcal{C}$ kúpot kifeszítő vektorok mátrixa). Eszerint $\mathbf{b} \in \mathcal{C}^*$, de $\mathbf{b}^\mathsf{T}\mathbf{w} > 0$ miatt $\mathbf{w} \notin \mathcal{C}^{**}$, és ezt akartuk igazolni. [QED]

A Farkas-lemma legelterjedtebb megfogalmazása az ún. alternatíva alak, amelyben a $\mathcal{C} = \mathcal{C}^{**}$ összefüggést a kúp kétféle fölírásával úgy írjuk le, hogy egy vektor vagy eleme a $\mathcal{C}$ kúpnak, vagy nem eleme a $\mathcal{C}^*$ duálisának. Részletesen kifejtve:

2.16. Tétel (Farkas-lemma -- alternatíva alak) Legyen $\mathbf{A} \in \mathbb{R}^{m\times n}$, $\mathbf{b} \in \mathbb{R}^m$. Ekkor az alábbi állítások közül pontosan az egyik teljesül:

1. Van olyan $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \geqslant \mathbf{0}$ vektor, hogy $\mathbf{A}\mathbf{x} = \mathbf{b}$.
2. Van olyan $\mathbf{y} \in \mathbb{R}^m$ vektor, hogy $\mathbf{y}^\mathsf{T}\mathbf{A} \leqslant \mathbf{0}$ és $\mathbf{y}^\mathsf{T}\mathbf{b} < 0$.

Világos, hogy az első állítás azzal ekvivalens, hogy $\mathbf{b} \in \mathcal{C}$, a második azzal, hogy $\mathbf{b} \notin \mathcal{C}^{**}$. Tehát ezek valóban egymást kizáró alternatívák. Egy nagyon hasonló alternatívatételt ismerünk, a Fredholm-félét, mely azt mondja ki, hogy vagy megoldható az $\mathbf{A}\mathbf{x} = \mathbf{b}$ egyenletrendszer, vagy van olyan $\mathbf{y}$ vektor, hogy $\mathbf{y}^\mathsf{T}\mathbf{A} = \mathbf{0}^\mathsf{T}$ de $\mathbf{y}^\mathsf{T}\mathbf{b} \neq 0$. Az alternatívatételek további változatai származtathatók azzal a trükkel, ahogy egy egyenlőtlenségrendszerből egyenletrendszert kapunk új változók bevezetésével.

2.17. Tétel (Farkas-lemma -- alternatíva alak egyenlőtlenségrendszerre) Legyen $\mathbf{A} \in \mathbb{R}^{m\times n}$, $\mathbf{b} \in \mathbb{R}^m$. Ekkor az alábbi állítások közül pontosan az egyik teljesül:

1. Van olyan $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \geqslant \mathbf{0}$ vektor, hogy $\mathbf{A}\mathbf{x} \leqslant \mathbf{b}$.
2. Van olyan $\mathbf{y} \in \mathbb{R}^m$, $\mathbf{y} \geqslant \mathbf{0}$ vektor, hogy $\mathbf{y}^\mathsf{T}\mathbf{A} \leqslant \mathbf{0}$ és $\mathbf{y}^\mathsf{T}\mathbf{b} < 0$.

A bizonyítást az olvasóra hagyjuk. A 4 táblázatban egy további alternatívatétellel együtt összefoglaljuk e tételeket.

	vagy van olyan $\mathbf{x}$, hogy		vagy van olyan $\mathbf{y}$, hogy	
1.	$\mathbf{Ax} \leqslant \mathbf{b}$	és $\mathbf{x}$ tetszőleges	$\mathbf{y}^\mathsf{T}\mathbf{A} = \mathbf{0}^\mathsf{T}$, $\mathbf{y}^\mathsf{T}\mathbf{b} < 0$	és $\mathbf{y} \geqslant \mathbf{0}$
2. ?? tétel		és $\mathbf{x} \geqslant 0$	$\mathbf{y}^\mathsf{T}\mathbf{A} \geqslant \mathbf{0}^\mathsf{T}$, $\mathbf{y}^\mathsf{T}\mathbf{b} < 0$	
3. ?? tétel	$\mathbf{Ax} = \mathbf{b}$			és $\mathbf{y}$ tetszőleges
4. Fredholm		és $\mathbf{x}$ tetszőleges	$\mathbf{y}^\mathsf{T}\mathbf{A} = \mathbf{0}^\mathsf{T}$, $\mathbf{y}^\mathsf{T}\mathbf{b} \neq 0$	

4. táblázat. A Farkas-lemma három alternatíva-változata, az utolsó sorban a Fredholm alternatíva-tétellel

Az alternatívatételek ekvivalencia típusú tételekké is átfogalmazhatók! Például a 2.17 tétel a következővé válik:

2.18. Tétel (Farkas-lemma -- ekvivalencia alak) Az $\mathbf{Ax} \leqslant \mathbf{b}$ egyenlőtlenségnek pontosan akkor van nemnegatív $\mathbf{x}$ megoldása, ha bármely $\mathbf{y} \geqslant \mathbf{0}$ és $\mathbf{y}^\mathsf{T}\mathbf{A} \geqslant \mathbf{0}^\mathsf{T}$ esetén$\mathbf{y}^\mathsf{T}\mathbf{b} \geqslant 0$.

Mind a négy alternatívatétel átfogalmazható ekvivalencia típusú tétellé, ezt a feladatot az Olvasóra hagyjuk!

A Farkas-lemma egy közgazdasági reprezentációja

Tegyük fel, hogy egy piacon m különböző eszközzel kereskednek, és egy időszak végén a piac n különböző állapotba kerülhet az eszközök árait tekintve. Legyen az i -edik eszköz ára az időszak elején b_i , azaz legyen $\mathbf{b}$ a kezdőárak vektora. Legyen továbbá $\mathbf{A} = [a_{ij}]_{m\times n}$ a kifizetési mátrix, ahol a_{ij} az i -edik eszköz ára, ha a piac a j -edik állapotba jut. Portfólión egy olyan $\mathbf{y} \in \mathbb{R}^m$ vektort értünk, ahol y_i az i -edik eszköz mennyiségét jelöli. Egy portfólió beszerzésének ára $\mathbf{y}^\mathsf{T}\mathbf{b}$, míg értéke az időszak végére a j állapotban $[\mathbf{y}^\mathsf{T}\mathbf{A}]_j$ lesz. Megengedjük, hogy y_i negatív legyen, ekkor az időszak elején eladjuk, és a végén vesszük az eszközt.

Arbitrázson általában piaci félreárazásból adódó olyan lehetőségek kihasználását értjük, melyek az ún. kockázatmentes hozamhoz képest (mint amilyen pl. a bankbetét kamata) azonnal és kockázatmentesen magasabb hozamot nyújtanak. Ilyen például ha egy bank egy valutát 200 Ft-ért ad, míg egy másik 210 Ft-ért vesz. Az arbitrázselmélet szerint egy piac arbitrázsmentes, ha nincs olyan portfólió, amelynek negatív az ára, de a piac minden állapotában nemnegatív a hozama. Képletben kifejezve, ha nincs olyan $\mathbf{y}$ vektor, hogy $\mathbf{y}^\mathsf{T}\mathbf{b} < 0$, de $\mathbf{y}^\mathsf{T}\mathbf{A} \geqslant \mathbf{0}$. A Farkas-lemma 2.16 változata szerint ez azzal ekvivalens, hogy van olyan $\mathbf{x} \geqslant \mathbf{0}$ vektor, hogy $\mathbf{Ax} = \mathbf{b}$. Miután $\mathbf{x} \geqslant \mathbf{0}$, 1-normájával normálva, azaz a koordináták összegével osztva egy valószínűségeloszlást kapunk. Így a

$$\mathbf{b} = \|\mathbf{x}\|_1 \mathbf{A} \frac{\mathbf{x}}{\|\mathbf{x}\|_1}$$

egyenlőség a következőképp is értelmezhető:

2.19. Állítás Egy piac pontosan akkor arbitrázsmentes, ha létezik a piac állapotainak egy olyan valószínűségeloszlása, hogy a kezdőárak mindegyike a végáraknak e valószínűségeloszlás szerinti várható értékével arányos.

LP feladat duálisa

Tekintsük ismét az (1) LP feladatot:

$$\begin{aligned} x_1 + 4x_2 &\leqslant 16 \\ x_1 + x_2 &\leqslant 7 \\ 2x_1 + x_2 &\leqslant 12 \\ x_1, x_2 &\geqslant 0 \\ z = 3x_1 + 4x_2 &\to \max. \end{aligned}$$

Megoldására lássunk egy új módszert! A $z = 3x_1 + 4x_2$ függvény maximumát keressük. Erre könnyen adhatunk felső becslést, például az első egyenlőtlenség 3-szorosát használva

$$z = 3x_1 + 4x_2 \leqslant 3x_1 + 12x_2 \leqslant 3 \cdot 16 = 48.$$

Ennél jobb becslést kapunk, ha összeadjuk az első és harmadik egyenlőtlenséget:

$$z = 3x_1 + 4x_2 \leqslant 3x_1 + 5x_2 \leqslant 3 \cdot 16 = 28.$$

Talán van ennél kedvezőbb lineáris kombinációja az egyenlőtlenségeknek! Keressünk ilyet, együtthatói legyenek y_1, y_2, y_3:

$$y_1(x_1 + 4x_2) + y_2(x_1 + x_2) + y_3(2x_1 + x_2) \leqslant 16y_1 + 7y_2 + 12y_3.$$

Azonos irányú egyenlőtlenségek lineáris kombinációja csak nemnegatív együtthatókkal vezet mindig érvényes egyenlőtlenségre, tehát $y_1, y_2, y_3 \geqslant 0$. Átalakítás után, és z-vel összevetve kapjuk, hogy fenn kell álljon a következő:

$$3x_1 + 4x_2 \leqslant (y_1 + y_2 + 2y_3)x_1 + (4y_1 + y_2 + y_3)x_2 \leqslant 16y_1 + 7y_2 + 12y_3.$$

Mivel $x_1, x_2 \geqslant 0$, a bal egyenlőtlenség csak akkor állhat fenn, ha

$$3 \leqslant y_1 + y_2 + 2y_3$$
$$4 \leqslant 4y_1 + y_2 + y_3.$$

Másrészt az is világos,
hogy $3x_1 + 4x_2$ maximumának $16y_1 + 7y_2 + 12y_3$ minimuma felső becslését adja.
Ha összegyűjtjük az eddigi feltételeket, látjuk, hogy egy újabb LP-feladatot kaptunk:

$$\begin{aligned} y_1 + y_2 + 2y_3 &\geqslant 3 \\ 4y_1 + y_2 + y_3 &\geqslant 4 \\ y_1, y_2, y_3 &\geqslant 0 \\ w = 16y_1 + 7y_2 + 12y_3 &\to \min . \end{aligned} \tag{2.12}$$

E feladatot az eredeti duálisának nevezzük. Ugyanilyen módon általánosan is fölírhatjuk egy LP-feladat duálisát! Vegyük észre, hogy a fenti példában az együtthatómátrix helyébe a transzponáltja került, a feltételek egyenlőtlenségeinek iránya ellenkezőjére változott, a célfüggvény maximuma helyett minimumát keressük, és a jobb oldal valamint a célfüggvény vektora helyet cserélt.

2.20. Definíció (LP feladat duálisa) Legyen $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$, $\mathbf{c} \in \mathbb{R}^n$. Az

$$\begin{aligned} \mathbf{Ax} &\leqslant \mathbf{b} \\ \mathbf{x} &\geqslant \mathbf{0} \\ \mathbf{c}^\mathsf{T}\mathbf{x} &\to \max . \end{aligned} \tag{2.13}$$

E feladathoz tartozó duál feladaton, illetve e feladat duálisán a következő LP feladatot értjük:

$$\begin{aligned} \mathbf{A}^\mathsf{T}\mathbf{y} &\geqslant \mathbf{c} \\ \mathbf{y} &\geqslant \mathbf{0} \\ \mathbf{b}^\mathsf{T}\mathbf{y} &\to \min . \end{aligned} \tag{2.14}$$

E kontextusban az eredeti feladatot primál feladatnak nevezzük.

A korábbiakban láttuk, hogy könnyű átjárás van a feltételek egyenlőtlenségeinek irányában, így a primál feladatban nem csak „$\leqslant$”, hanem „$\geqslant$” és „$=$” is állhat, és egyes változókra a nemnegativitási feltételt is elhagyhatjuk. Hogy jól áttekinthető legyen a kapcsolat primál és duál feladat egymásnak megfelelő elemei közt, a fenti konkrét feladatot és duálisát egymás mellé írjuk:

$$
\begin{aligned}
x_1 + 4x_2 &\leqslant 16 & y_1 &\geqslant 0\\
x_1 + x_2 &\leqslant 7 & y_2 &\geqslant 0\\
2x_1 + x_2 &\leqslant 12 & y_3 &\geqslant 0\\
x_1 &\geqslant 0 & y_1 + y_2 + 2y_3 &\geqslant 3\\
x_2 &\geqslant 0 & 4y_1 + y_2 + y_3 &\geqslant 4\\
z = 3x_1 + 4x_2 &\to \max & w = 16y_1 + 7y_2 + 12y_3 &\to \min .
\end{aligned}
$$

Az Olvasó itt elgondolkodhat azon, hogy a feltételek általában hogy rakhatók párba. Segítségül mindent megadunk egy egyszerű táblázatban.

	Primál	Duál
Ismeretlen vektor	$\mathbf{x} \in \mathbb{R}^n$	$\mathbf{y} \in \mathbb{R}^m$
Jobb oldali vektor	$\mathbf{b} \in \mathbb{R}^m$	$\mathbf{c} \in \mathbb{R}^n$
Célfüggvény	$\max \mathbf{c}^\mathsf{T}\mathbf{x}$	$\min \mathbf{b}^\mathsf{T}\mathbf{y}$
Együtthatómátrix	$\mathbf{A} \in \mathbb{R}^{m\times n}$	$\mathbf{A}^\mathsf{T} \in \mathbb{R}^{n\times m}$
Korlátozó feltételek	$\mathbf{a}_{i*}\mathbf{x} \leqslant b_i$	$y_i \geqslant 0$
	$\mathbf{a}_{i*}\mathbf{x} \geqslant b_i$	$y_i \leqslant 0$
	$\mathbf{a}_{i*}\mathbf{x} = b_i$	y_i tetszőleges
	$x_j \geqslant 0$	$\mathbf{a}_{*j}^\mathsf{T}\mathbf{y} \geqslant c_i$
	$x_j \leqslant 0$	$\mathbf{a}_{*j}^\mathsf{T}\mathbf{y} \leqslant c_i$
	x_j tetszőleges	$\mathbf{a}_{*j}^\mathsf{T}\mathbf{y} = c_i$

5. táblázat. A primál és duál feladat egymásnak megfelelő elemei ($\mathbf{a}_{i*}$ az $\mathbf{A}$ mátrix i-edik sorvektora, $\mathbf{a}_{*j}^\mathsf{T}$ az $\mathbf{A}$ mátrix j-edik oszlopának transzponáltja.

Az 5 táblázatból leolvasható a dualitás szükséges szimmetriája is, vagyis hogy ha az A feladat duálisa B, akkor a B duálisa A.

Példaként felírjuk egy gyakrabban előforduló típus duálisát: az $\mathbf{Ax} \leqslant \mathbf{b}$, $\mathbf{c}^\mathsf{T}\mathbf{x} \to \max$ ($\mathbf{x}$-re nincs kikötés) feladat duálisa $\mathbf{A}^\mathsf{T}\mathbf{y} = \mathbf{c}$, $\mathbf{y} \geqslant \mathbf{0}$, $\mathbf{b}^\mathsf{T}\mathbf{y} \to \min$.

Dualitás-tétel

A dualitás-tétel a lineáris programozás egyik központi eredménye, bizonyítását a Farkas-lemmára építjük.

2.21. Tétel (Dualitás-tétel) Legyen $\mathbf{A} \in \mathbb{R}^{m\times n}$, $\mathbf{b} \in \mathbb{R}^m$, $\mathbf{c} \in \mathbb{R}^n$. Ha a

(13) $\mathbf{Ax} \leqslant \mathbf{b}$, $\mathbf{x} \geqslant \mathbf{0}$, $\mathbf{c}^\mathsf{T}\mathbf{x} \to \max$

primál feladat, és a hozzá tartozó

(14) $\mathbf{A}^{\mathsf{T}}\mathbf{y} \geqslant \mathbf{c}$, $\mathbf{y} \geqslant \mathbf{0}$, $\mathbf{b}^{\mathsf{T}}\mathbf{y} \to \min$

duál feladat valamelyikének van optimális megoldása, akkor van a másiknak is, és a két célfüggvény optimális értéke azonos, azaz ha $\bar{\mathrm{x}}$ és $\bar{\mathrm{y}}$ optimális megoldásai (13)-nek, illetve (14)-nek, akkor $\mathbf{c}^{\mathsf{T}}\bar{\mathrm{x}} = \mathrm{b}^{\mathsf{T}}\bar{\mathrm{y}}$.

A duál feladat konstrukciójából láttuk, hogy ha $\mathbf{x}$ a primál, $\mathbf{y}$ a duál feladat egy megoldása, akkor $\mathbf{c}^{\mathsf{T}}\mathbf{x} \leqslant \mathbf{b}^{\mathsf{T}}\mathbf{y}$. Ez a tételbeli feltételekből is azonnal adódik:

$$\mathbf{c}^{\mathsf{T}}\mathbf{x} \leqslant (\mathbf{A}^{\mathsf{T}}\mathbf{y})^{\mathsf{T}}\mathbf{x} = \mathbf{y}^{\mathsf{T}}\mathbf{A}\mathbf{x} \leqslant \mathbf{y}^{\mathsf{T}}\mathbf{b} = \mathbf{b}^{\mathsf{T}}\mathbf{y}. \tag{2.15}$$

Eszerint ha mindkét feladatnak van lehetséges megoldása, akkor mindkettőnek optimális megoldása is van, hisz a maximumfeladat felülről, a minimum feladat alulról korlátos. Az is világos, hogy ha az egyik feladat nem korlátos ((13) felülről, (14) alulról), akkor a másiknak nincs megoldása. A tétel szerint ha az egyiknek van optimális megoldása, akkor a másiknak is. Eszerint a primál és a duál feladat megoldhatóságának három esete lehetséges:

1. egyik feladat sem oldható meg,
2. egyik nem korlátos, másik nem oldható meg,
3. mindkettőnek van optimális megoldása, és az optimális célfüggvényértékek egybeesnek.

Bizonyítás.[A dualitástétel bizonyítása] Tegyük fel, hogy (13)-nek $\bar{\mathrm{x}}$ optimális megoldása. A célfüggvény optimumát jelölje m, azaz $m = \mathbf{c}^{\mathsf{T}}\mathbf{x}$. Eszerint az

$$\mathbf{A}\mathbf{x} \leqslant \mathbf{b},\ \mathbf{c}^{\mathsf{T}}\mathbf{x} \geqslant m,\ \text{azaz az } \mathbf{A} - \mathbf{c}^{\mathsf{T}} \leqslant \mathbf{b} - m \tag{2.16}$$

egyenlőtlenségrendszernek van nemnegatív megoldása. Másrészt tetszőleges pozitív ε -ra az

$$\mathbf{A}\mathbf{x} \leqslant \mathbf{b},\ \mathbf{c}^{\mathsf{T}}\mathbf{x} \geqslant m + \varepsilon,\ \text{azaz az } \mathbf{A} - \mathbf{c}^{\mathsf{T}} \leqslant \mathbf{b} - m - \varepsilon \tag{2.17}$$

egyenlőtlenségrendszernek nincs nemnegatív megoldása. A Farkas-lemma alternatíva alakja (2.17 tétel) szerint az, hogy a (17) egyenlőtlenségnek nincs nemnegatív megoldása, azzal ekvivalens, hogy létezik egy olyan $\begin{bmatrix} \mathbf{v} \\ t \end{bmatrix} \geqslant \mathbf{0}$ vektor ($\begin{bmatrix} \mathbf{v} \\ t \end{bmatrix} \in \mathbb{R}^{n+1}$), hogy

$$\mathbf{v}^{\mathsf{T}}t\mathbf{A} - \mathbf{c}^{\mathsf{T}} \geqslant \mathbf{0},\ \text{de } \mathbf{v}^{\mathsf{T}}t\mathbf{b} - m - \varepsilon < 0.$$

Kifejtve a blokkmátrixműveletet, majd átrendezve:

$$\mathbf{v}^{\mathsf{T}}\mathbf{A} \geqslant t\mathbf{c}^{\mathsf{T}},\ \text{de}\ \mathbf{v}^{\mathsf{T}}\mathbf{b} < t(m+\varepsilon). \tag{2.18}$$

Mivel a (16) egyenlőtlenségnek van megoldása, ezért a Farkas-lemma (2.18 tétel) szerint a fenti $\mathbf{v}$ vektorra

$$\mathbf{v}^{\mathsf{T}}t\mathbf{A}-\mathbf{c}^{\mathsf{T}} \geqslant \mathbf{0}\ \text{miatt}\ \mathbf{v}^{\mathsf{T}}t\mathbf{b}-m \geqslant 0,$$

azaz $\mathbf{v}^{\mathsf{T}}\mathbf{b} \geqslant tm$. Itt $t > 0$,
ugyanis $t = 0$ esetén $tm \leqslant \mathbf{v}^{\mathsf{T}}\mathbf{b} < t(m+\varepsilon)$ ellentmondásra vezetne. Legyen tehát $\mathbf{y} = \mathbf{v}/t$. Ekkor a (18) folyományaként $\mathbf{A}^{\mathsf{T}}\mathbf{y} \geqslant \mathbf{c}$ és $m \leqslant \mathbf{b}^{\mathsf{T}}\mathbf{y} < m+\varepsilon$, azaz $\mathbf{y}$ megoldása a duális problémának. Mivel a célfüggvény alulról korlátos, ezért a duál feladatnak is van optimális megoldása, és az csak az $[m, m+\varepsilon)$ intervallumba eshet, tehát csak m lehet. [QED]

A bizonyítás csak egy esetre vonatkozott, de az 5 táblázat szerinti összes esetre átvihető.

A primál és duál feladat szimplex táblái

A két feladat táblái közti kapcsolat alapján a duál feladat megoldása leolvasható a primál szimplex táblájából és viszont. Ennek igazolásával egyúttal új bizonyítást adunk a dualitástételre.

2.22. Példa Oldjuk meg szimplex módszerrel a 2.2 példához tartozó LP-feladat duálisát, melyet fölírtunk a (12)-beli képletekkel!

Megoldás

A duális feladatot a követhetőség érdekében megismételjük:

$$\begin{aligned} y_1 + y_2 + 2y_3 &\geqslant 3 \\ 4y_1 + y_2 + y_3 &\geqslant 4 \\ y_1, y_2, y_3 &\geqslant 0 \\ w = 16y_1 + 7y_2 + 12y_3 &\to \min. \end{aligned}$$

Mivek itt $\geqslant$ jelek állnak a feltételekben, nemnegatív változók kivonásával kaphatunk egyenletrendszert, a célfüggvényt pedig -1-gyel kell szorozni, hogy maximumfeladatot kapjunk. Így a a következő táblát kapjuk, mely még nem szimplex tábla, nincs benne permutációmátrix:

y_1	y_2	y_3	y_4	y_5	
1	1	2	−1	0	3
4	1	1	0	−1	4
−16	−7	−12	0	0	z

Az induló táblát két újabb változó bevételével és a (10) egyenlet megoldásával megkapjuk:

y_1	y_2	y_3	y_4	y_5	y_6	y_7	
1	1	2	−1	0	1	0	3
4	1	1	0	−1	0	1	4
0	0	0	0	0	−1	−1	z

→

y_1	y_2	y_3	y_4	y_5	y_6	y_7	
1	**1**	2	−1	0	1	0	3
4	1	1	0	−1	0	1	4
5	2	3	−1	−1	0	0	$z+7$

→

y_1	y_2	y_3	y_4	y_5	y_6	y_7	
1	1	2	−1	0	1	0	3
3	0	−1	**1**	−1	−1	1	1
3	0	−1	1	−1	−2	0	$z+1$

→

y_1	y_2	y_3	y_4	y_5	y_6	y_7	
4	1	1	0	−1	0	1	4
3	0	−1	1	−1	−1	1	1
0	0	0	0	0	−1	−1	z

Megtaláltuk tehát az egyenletrendszer egy olyan ekvivalens alakját, melyben az együtthatómátrixnak van egy permutációmátrix része. Az eredeti célfüggvényben eliminálva a permutációmátrix alatti elemeket, szimplex táblához jutunk, melyet egyetlen lépésben meg is oldunk:

y_1	y_2	y_3	y_4	y_5	
4	1	1	0	−1	4
3	0	−1	1	−1	1
−16	−7	−12	0	0	z

→

y_1	y_2	y_3	y_4	y_5	
4	1	1	0	−1	4
3	0	−1	1	−1	1
12	0	−5	0	−7	$z+28$

→

y_1	y_2	y_3	y_4	y_5	
0	1	7/3	−4/3	1/3	8/3
1	0	−1/3	1/3	−1/3	1/3
0	0	−1	−4	−3	$z+24$

Vessük össze ezt az eredményt a primál feladat 2.11 példabeli induló és optimális szimplex tábláival, melyeket itt megismétlünk:

x_1	x_2	x_3	x_4	x_5	
1	4	1	0	0	16
1	1	0	1	0	7
2	1	0	0	1	12
3	4	0	0	0	z

x_1	x_2	x_3	x_4	x_5	
0	1	$\frac{1}{3}$	$-\frac{1}{3}$	0	3
1	0	$-\frac{1}{3}$	$\frac{4}{3}$	0	4
0	0	$\frac{1}{3}$	$-\frac{7}{3}$	1	1
0	0	$-\frac{1}{3}$	$-\frac{8}{3}$	0	$z-24$

Az, hogy a két optimális tábla adatai közt szoros kapcsolat látszik, nem véletlen. Elevenítsük fel a (9) egyenletben és utána bevezetett jelöléseket, és írjuk fel értéküket e konkrét esetben, nevezetesen a primál feladathoz tartozó standard alakú LP-feladatra. A primál feladat optimális táblája alapján , , továbbá

$$A = \begin{bmatrix} 0 & 1 & \frac{1}{3} & -\frac{1}{3} & 0 \\ 1 & 0 & -\frac{1}{3} & \frac{4}{3} & 0 \\ 0 & 0 & \frac{1}{3} & -\frac{7}{3} & 1 \end{bmatrix},$$

$$\mathrm{A}_{\mathcal{B}} = \begin{bmatrix} 4 & 1 & 0 & \mathbf{1} & 1 & 0 & \mathbf{1} & 2 & 1 \end{bmatrix}, \quad \mathbf{A}_{\mathcal{B}}^{-1} = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & \frac{4}{3} & 0 \\ \frac{1}{3} & -\frac{7}{3} & 1 \end{bmatrix}, \quad \mathbf{A}_{\mathcal{N}} = \begin{bmatrix} 1 & 0 & \mathbf{0} & 1 & \mathbf{0} & 0 \end{bmatrix},$$

$$\mathbf{c}_{\mathcal{B}} = \begin{bmatrix} 4 \\ 3 \; \mathbf{0} \end{bmatrix}, \quad \mathbf{c}_{\mathcal{N}} = \begin{bmatrix} 0 \; \mathbf{0} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{c}_{\mathcal{B}} = \mathbf{0}, \quad \bar{}$$

$$\mathrm{c}_{\mathcal{N}} = \begin{bmatrix} -\frac{1}{3} \\ -\frac{8}{3} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{x}_{\mathcal{B}} = \begin{bmatrix} 4 \\ 3 \; \mathbf{1} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{x}_{\mathcal{N}} = \mathbf{0}.$$

$$[\mathbf{A}|\mathbf{I}] = \left[\begin{array}{cc|ccc} 1 & 4 & 1 & 0 & 0 \; \mathbf{1} \\ 1 & 0 & 1 & 0 & \\ 2 & 1 & 0 & 0 & 1 \end{array}\right], \quad \mathbf{b} = \begin{bmatrix} 16 \\ 7 \\ 12 \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \quad \bar{}$$

$$\mathrm{A} = \begin{bmatrix} 0 & 1 & \frac{1}{3} & -\frac{1}{3} & 0 \\ 1 & 0 & -\frac{1}{3} & \frac{4}{3} & 0 \\ 0 & 0 & \frac{1}{3} & -\frac{7}{3} & 1 \end{bmatrix},$$

$$\mathrm{A}_{\mathcal{B}} = \begin{bmatrix} 4 & 1 & 0 & \mathbf{1} & 1 & 0 & \mathbf{1} & 2 & 1 \end{bmatrix}, \quad \mathbf{A}_{\mathcal{B}}^{-1} = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & \frac{4}{3} & 0 \\ \frac{1}{3} & -\frac{7}{3} & 1 \end{bmatrix}, \quad \mathbf{A}_{\mathcal{N}} = \begin{bmatrix} 1 & 0 & \mathbf{0} & 1 & \mathbf{0} & 0 \end{bmatrix},$$

$$\mathbf{c}_{\mathcal{B}} = \begin{bmatrix} 4 \\ 3 \; \mathbf{0} \end{bmatrix}, \quad \mathbf{c}_{\mathcal{N}} = \begin{bmatrix} 0 \; \mathbf{0} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{c}_{\mathcal{B}} = \mathbf{0}, \quad \bar{}$$

$$\mathrm{c}_{\mathcal{N}} = \begin{bmatrix} -\frac{1}{3} \\ -\frac{8}{3} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{x}_{\mathcal{B}} = \begin{bmatrix} 4 \\ 3 \; \mathbf{1} \end{bmatrix}, \quad \bar{}$$

$$\mathrm{x}_{\mathcal{N}} = \mathbf{0}.$$

ahol $\bar{\mathrm{A}}$, $\bar{\mathrm{c}}$ és $\bar{\mathrm{x}}$ az optimális szimplex tábla együtthatómátrixát, célfüggvénysorának vektorát és az optimális megoldást jelöli.

A következőkben általánosan kimondjuk és igazoljuk a fönti adatokkal könnyen ellenőrizhető összefüggéseket.

2.23. Állítás Az $\mathbf{Ax} \leqslant \mathbf{b}$, $\mathbf{c}^\mathsf{T}\mathbf{x} \to \max$ feladat standard alakjához tartozó optimális szimplex táblájából leolvasható a feladat duálisának megoldása is: $\mathbf{y} = \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{A}_\mathcal{B}^{-1}$, mely a segédváltozókhoz tartozó célfüggvényvektor -1-szerese.

Bizonyítás. Többet bizonyítunk: új bizonyítást adunk a dualitástételre. A primál feladat standard alakja az $\mathbf{A}_\mathcal{B}\mathbf{x}_\mathcal{B} + \mathbf{A}_\mathcal{N}\mathbf{x}_\mathcal{N} = \mathbf{b}$, $z = \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{x}_\mathcal{B} + \mathbf{c}_\mathcal{N}^\mathsf{T}\mathbf{x}_\mathcal{N}$ alakot ölti, ahol $\mathcal{B}$ az optimális tábla bázisoszlopainak rendezett indexhalmaza. Az előbbit $\mathbf{A}_\mathcal{B}^{-1}$ mátrixszal beszorozva, és kifejezve $\mathbf{x}_\mathcal{B}$-t kapjuk, hogy

$$\mathbf{x}_\mathcal{B} = \mathbf{A}_\mathcal{B}^{-1}\mathbf{b} - \mathbf{A}_\mathcal{B}^{-1}\mathbf{A}_\mathcal{N}\mathbf{x}_\mathcal{N}.$$

Ez a célfüggvénybe helyettesítve a

$$z = \mathbf{c}_\mathcal{B}^\mathsf{T}\left(\mathbf{A}_\mathcal{B}^{-1}\mathbf{b} - \mathbf{A}_\mathcal{B}^{-1}\mathbf{A}_\mathcal{N}\mathbf{x}_\mathcal{N}\right) + \mathbf{c}_\mathcal{N}^\mathsf{T}\mathbf{x}_\mathcal{N}$$

alakra vezet, ahonnan

$$z - \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{A}_\mathcal{B}^{-1}\mathbf{b} = \left(\mathbf{c}_\mathcal{N}^\mathsf{T} - \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{A}_\mathcal{B}^{-1}\mathbf{A}_\mathcal{N}\right)\mathbf{x}_\mathcal{N}. \tag{2.19}$$

Az optimális táblán az $\mathbf{x}_\mathcal{N}$-hez tartozó együtthatók nem pozitívak, azaz

$$\mathbf{c}_\mathcal{N}^\mathsf{T} = \mathbf{c}_\mathcal{N}^\mathsf{T} - \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{A}_\mathcal{B}^{-1}\mathbf{A}_\mathcal{N} \leqslant \mathbf{0}^\mathsf{T}, \tag{2.20}$$

tehát az optimális célfüggvényérték valóban az $\bar{\mathbf{x}}_\mathcal{N} = \mathbf{0}$ helyen adódik, és épp

$$z_0 = \mathbf{c}_\mathcal{B}^\mathsf{T}\mathbf{A}_\mathcal{B}^{-1}\mathbf{b} = \mathbf{c}_\mathcal{B}^\mathsf{T}$$

$\mathbf{x}_\mathcal{B}$,

azaz

$$\mathbf{x}_\mathcal{B} = \mathbf{A}_\mathcal{B}^{-1}\mathbf{b}.$$

Ez összhangban van azzal, hogy az optimális tábla utolsó oszlopában az elemi sorműveletek következtében valóban $\mathbf{A}_\mathcal{B}^{-1}\mathbf{b}$ áll, valóban ezt a megoldást olvassuk le a tábláról.

Most megmutatjuk, hogy $\bar{y}^{\mathsf{T}} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}$ megengedett megoldása a duális feladatnak, azaz hogy $\bar{y}^{\mathsf{T}}\mathbf{A} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{A} \geqslant \mathbf{c}$. Mivel $\mathbf{A}$ bármely oszlopa vagy az $\mathbf{A}_{\mathcal{B}}$ vagy az $\mathbf{A}_{\mathcal{N}}$ egy oszlopa, ezért

$$\mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{A}_{\mathcal{B}} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}},$$

és (20) szerint

$$\mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{A}_{\mathcal{N}} \geqslant \mathbf{c}_{\mathcal{N}}^{\mathsf{T}},$$

ami bizonyítja állításunkat.

Belátjuk, hogy $\mathbf{y}^{\mathsf{T}} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}$ optimális megoldása a duális feladatnak. Ez azonnal következik abból, hogy

$$\mathbf{b}^{\mathsf{T}}$$

$$\mathrm{y} = \mathrm{y}^{\mathsf{T}}\mathbf{b} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{b} = \mathrm{x}\ \mathrm{b},$$

valamint abból, hogy - a gyenge dualitástétel néven is ismert - (15) egyenlőtlenség szerint minden megengedett $\mathbf{x}$ primál és $\mathbf{y}$ duál megoldásra $\mathbf{c}^{\mathsf{T}}\mathbf{x} \leqslant \mathbf{b}^{\mathsf{T}}\mathbf{y}$.

Ha az $\mathbf{Ax} \leqslant \mathbf{b}$ egyenlőtlenségben $\mathbf{A}$ $m \times n$ -es, akkor a standard induló táblában az x_{n+1},..., x_{n+m} változók a segédváltozók, és ezekhez az $\mathbf{I}_m$ egységmátrix tartozik, az induló táblában a célfüggvény együtthatói 0-k, így a (19) egyenletből és a nyilvánvaló $\mathbf{0} = \bar{c}_{\mathcal{B}} = \mathbf{c}_{\mathcal{B}}^{\mathsf{T}} - \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{A}_{\mathcal{B}}$ egyenlőség alapján

$$\bar{c}_{[n+1\ldots n+m]} = \mathbf{0} - \mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1}\mathbf{I}_m = -\mathbf{c}_{\mathcal{B}}^{\mathsf{T}}\mathbf{A}_{\mathcal{B}}^{-1} = -\mathbf{y}^{\mathsf{T}},$$

ahogy állítottuk. [QED]

A dualitástétel közgazdasági jelentése

Ha egy LP feladat egy valóságos probléma megfogalmazásából születik, fontos jelentése van a duálfeladatnak. Erre mutatunk egy elemi példát.

Tekintsük a parfümök gyártásáról szóló 2.2 példát. Ez az (1) feladatra vezet, melynek duálisa a (12) feladat. Mindkettőt megoldottuk, de vajon a duális feladathoz tartozik-e olyan - a parfümök gyártásához kapcsolódó - gazdasági kérdés, melyre a duális feladat megoldása választ ad?

Vajon mennyit ér számunkra erőforrásaink egységnyi mennyisége? Mennyit kérjünk, ha valaki azokat meg akarná vásárolni? Ha y_1 a titkos illatanyag, y_2 az egy cl-re jutó csomagolókapactás és y_3 a különleges eljárásunk értéke, akkor időegységenként $w = 16y_1 + 7y_2 + 12y_3$ kapacitásunk értéke. A vevő ezt nyilván minimalizálni szeretné. Mivel mi sem szeretnénk rosszul járni, nem kaphatunk kevesebbet, mint amennyit saját termékeink eladásával kapnánk, tehát fönn kell, hogy álljon a következő két egyenlőtlenség:

$$y_1 + y_2 + 2y_3 \geqslant 3$$
$$4y_1 + y_2 + y_3 \geqslant 4.$$

Ezek a fenti célfüggvénnyel és az árakra vonatkozó nyilvánvaló nemnegativitási feltételekkel épp a (12) LP-feladatra vezetnek, vagyis a parfüm-feladat duálisához.

A dualitástétel egy mechanikai szemléltetése

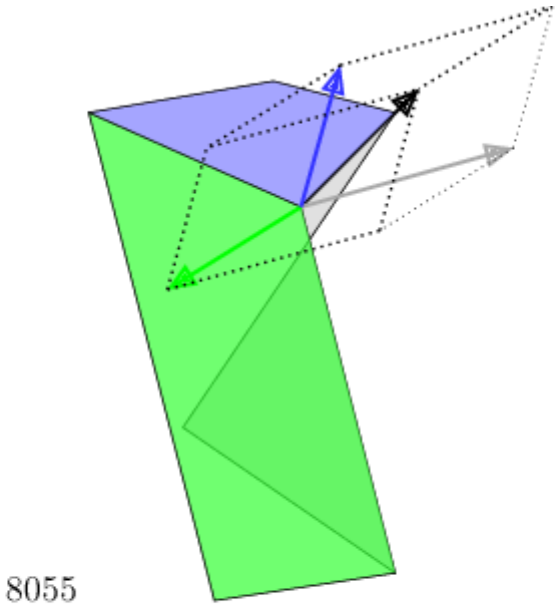
Legyen $\mathbf{Ax} \leqslant \mathbf{b}$, $\mathbf{c}^\mathsf{T}\mathbf{x} \to \max$ a primál feladat. Ennek duálisa az 5 táblázat szerint $\mathbf{A}^\mathsf{T}\mathbf{y} = \mathbf{c}$, $\mathbf{y} \geqslant \mathbf{0}$, $\mathbf{b}^\mathsf{T}\mathbf{y} \to \min$. Legyen $\mathbf{A}$ mérete $m \times 3$. Ha a primál feladatnak van megengedett megoldása, akkor az $\mathbf{A}_{i*}\mathbf{x} \leqslant b_i$ egyenlőtlenségekkel megadott félterek metszete egy nem üres poliéder. Képzeljük el, hogy az $\mathbf{A}_{i*}\mathbf{x} = b_i$ egyenletű, $\mathbf{A}_{i*}$ normálvektorú S_i síkok határolta poliédert dobozként elkészítjük, és belehelyezünk egy golyót az $\mathbf{x}$ helyre. Ez így egy lehetséges megoldást szemléltet. Legyen $\mathbf{c}$ a golyóra ható gravitációs erő, mondjuk legyen $\mathbf{c} = (0, 0, -1)$. Világos, hogy az optimális megoldás a poliéder legalsó pontja lesz, ami lehet a poliéder egy csúcsa, egy vízszintes élének vagy lapjának egy pontja. Ennek megkeresése fizikailag egyszerű: engedjük el a golyót a doboz belsejében, ami egy optimális $\bar{\mathrm{x}}$ helyre fog gurulni a doboz belső falán. (E modellben a golyót elhanyagolható sugarúnak képzeljük, de r -sugarú golyó középpontjába mutató $\mathbf{x}$ vektorral is megvalósítható, csak akkor a doboz falait az eredeti határoló síkokhoz képest r -rel „kijjebb” kell tolni.)

Vizsgáljuk meg az optimális $\bar{\mathrm{x}}$ helyre került golyóra ható erőket. Jelölje I azt az indexhalmazt, amelyre az S_i sík pontosan akkor érinti a golyót, ha $i \in I$. Az S_i síkot a golyó a sík normálvektorával párhuzamos erővel nyomja, legyen e vektor $\bar{y}_i\mathbf{A}_{i*}$. A $\mathbf{c}$ vektor előáll e vektorok összegeként, így

$$\mathbf{c} = \sum_{i \in I} \bar{y}_i \mathbf{A}_{i*}.$$

Legyen $\bar{y}_i = 0$, ha $i \notin I$, így az $\bar{\mathrm{y}}=(1, \bar{y}_2, \ldots, \bar{y}_m)$ vektorra $\bar{\mathrm{y}}^\mathsf{T}\mathbf{A} = \mathbf{c}$. Ez az $\bar{\mathrm{y}}$ vektor optimális megoldása a duális feladatnak. Tekintsük ugyanis az $\bar{\mathrm{y}}^\mathsf{T}(\mathbf{A}\bar{\mathrm{x}}\text{- b})$ kifejezést. Egyrészt, mivel az S_i sík egyenlete $\mathbf{A}_{i*}\mathbf{x} = b_i$, ezért $\mathbf{A}_{i*}\bar{\mathrm{x}}\text{-b}_i = 0$, ha $i \in I$, másrészt $\bar{y}_i = 0$, ha $i \notin I$, így $\bar{\mathrm{y}}^\mathsf{T}(\mathbf{A}\bar{\mathrm{x}}\text{- b})=0$.

Ebből átrendezve $\bar{y}^T\mathbf{b} = \mathbf{y}^T\mathbf{A}\bar{x} = \bar{y}^T\mathbf{c}$ adódik, tehát $\bar{y}^T\mathbf{b} = \mathbf{y}^T\mathbf{c}$, vagyis $\bar{y}$ valóban optimális megoldása a duális feladatnak.



8055

26. ábra. Egy poliéder alsó csúcsa az ott találkozó lapokkal, a csúcsba helyezett, elhanyagolhatóan kis sugarú (így szinte nem is látható) golyóra ható gravitációs erővel és annak komponenseivel. A poliéder oldallapját és a rá merőlegesen ható erőt azonos szín jelzi.

3 Kódelmélet és kriptográfia

3.1 Kódvektorok

Bitvektorok, kódvektorok

A modern számítógépek memóriájában vagy háttértárolóin az adatok tárolásának legkisebb egysége a bit [5]. Egy bittel két állapot tárolható, melyeket a 0 és 1 számokkal jelölünk, de amelyek több mindent is reprezentálhatnak: hamis/igaz, nem/igen, ki/be,.... A biteket a hardver lehetőségei és a feladat igényei szerint csoportokba, sorozatokba, vektorokba gyűjtik, melyekkel különféle műveletek végezhetők. Ezek attól is függnek, hogy a bitvektorok milyen adatokat kódolnak. E műveletek közül minket azok fognak érdekelni, melyek algebrailag a korábban megismert vektorműveletekre hasonlítanak.

Az egyszerűség kedvéért a bitvektorokat gyakran a biteket jelölő számjegyek egyszerű egymás mellé írásával adjuk meg, pl. 01110101 a $(0,1,1,1,0,1,0,1)$ vektort jelöli.

A modern számítástechnika számtalan kódot használ, mely bitvektorokkal (is) leírható. Például karakterek kódolására használatos a 7-dimenziós bitvektorokból

álló ASCII-kód, [6] a decimális számok kódolására a 4-dimenziós bitvektorokból álló BCD-kód. [7]

Az emberek által is elolvasható kódok gyakran decimális számokból állnak. Például az emberek azonosítására használt személyi szám egy olyan vektornak tekinthető, amelynek koordinátái a 10-elemű $\{0, 1, \ldots, 9\}$ halmazból valók.

A kódoláshoz mi a továbbiakban mindig egy rögzített, véges kódábécét használunk, amelynek betűi általában a 0-tól $n-1$-ig terjedő egészek, $n > 10$ esetén a normál ábécé betűi lesznek. A kódábécé „betűiből", azaz elemeiből képzett vektorokat kódvektoroknak vagy kódszavaknak nevezzük. A bitvektorok is kódvektorok, ahol a kódábécé a kételemű $\{0, 1\}$ halmaz.

A kódvektorok koordinátáinak számát, vagyis a kódvektor dimenzióját a kód hosszának nevezzük. Ez természetesen nem analóg fogalom a vektor abszolút értékével.

A személyi szám tehát egy 10-elemű ábécéből képzett 11-hosszú kódszó. Nem minden 11-hosszú decimális vektor lehet személyi szám, mert egyrészt bizonyos helyeken csak bizonyos számok állhatnak, másrészt mert az utolsó koordináta egy ellenőrző jegy, amit a többi koordinátából lehet kiszámolni. Tehát a személyi szám, mint kód, matematikailag a 11-hosszú kódvektorok halmazának egy részhalmazaként írható le. Ezért általában a kódábécé betűiből képzett vektorok részhalmazait fogjuk kódnak nevezni. Főként az információelméletben változó hosszú kódszavak is tartozhatnak egy kódhoz. Mi ilyenekkel nem fogunk foglalkozni, de megemlítjük, hogy a karakterek manapság elterjedt UTF-8 kódolása is változó hosszú kódvektorokból áll: egy karakter kódja 8-, 16-, 24- vagy 32-bites is lehet.

A kód egy közös ábécéből képzett azonos hosszúságú kódszavak egy halmaza. Kódolás során a kódolandó objektumokhoz kódszavakat rendelünk, dekódolás az ellenkező irányú folyamat.

Vektorműveletek $\mathbb{Z}_m^n$-ben

$\mathbb{Z}_m^n$ a $\mathbb{Z}_m$-beli n-hosszú vektorokból áll. E vektorok összeadása, skalárral való szorzása és skaláris szorzása a $\mathbb{Z}_m$-beli műveletekkel az $\mathbb{R}^n$-beli vektorműveletekhez hasonlóan végezhető el. Ennek következtében a lineáris kombináció, lineáris függetlenség itt is ugyanúgy definiálható és használható.

3.1. Példa (Lineáris kombináció $ \mathbb{Z}_m^n$-ben) Számítsuk ki a $\mathbb{Z}_2^5$-beli

$$\mathbf{a} = (1, 0, 0, 1, 1, 0),\ \mathbf{b} = (0, 1, 0, 1, 0, 1) \text{ és } \mathbf{c} = (0, 0, 1, 0, 1, 1)$$

vektorok összes lineáris kombinációját $\mathbb{Z}_2$-beli együtthatókkal, valamint a $\mathbb{Z}_3^3$-beli

$$\mathbf{u} = (1, 1, 0) \text{ és } \mathbf{v} = (0, 1, 1)$$

vektorok összes lineáris kombinációját $\mathbb{Z}_3$-beli együtthatókkal.

Megoldás

A lehetséges $x\mathbf{a} + y\mathbf{b} + z\mathbf{c}$ alakú lineáris kombinációk száma 8, ugyanis $x, y, z \in \mathbb{Z}_2$, mindegyik együtthatónak 0 vagy 1 az értéke, és ez $2 \cdot 2 \cdot 2 = 8$ eshetőség. Az$x = y = z = 0$ eset a zérusvektort adja. Ha x, y és z közül csak egyikük értéke 1, a többi 0, akkor a három adott vektort kapjuk vissza. Azok az esetek maradnak, amikor legalább két vektort kell összeadni.
Például $1\mathbf{a} + 1\mathbf{b} + 0\mathbf{c} = (1, 0, 0, 1, 1, 0) + (0, 1, 0, 1, 0, 1) = (1, 1, 0, 0, 1, 1)$. Az összes lineáris kombináció a 6. (a) táblázatban látható.

$x\ y\ z$	$x\mathbf{a} + y\mathbf{b} + z\mathbf{c}$
0 0 0	$(0, 0, 0, 0, 0, 0)$
1 0 0	$(1, 0, 0, 1, 1, 0)$
0 1 0	$(0, 1, 0, 1, 0, 1)$
0 0 1	$(0, 0, 1, 0, 1, 1)$
1 1 0	$(1, 1, 0, 0, 1, 1)$
1 0 1	$(1, 0, 1, 1, 0, 1)$
0 1 1	$(0, 1, 1, 1, 1, 0)$
1 1 1	$(1, 1, 1, 0, 0, 0)$

(a)

$x\ y$	$x\mathbf{u} + y\mathbf{v}$
0 0	$(0, 0, 0)$
1 0	$(1, 1, 0)$
2 0	$(2, 2, 0)$
0 1	$(0, 1, 1)$
1 1	$(1, 2, 1)$
2 1	$(2, 0, 1)$
0 2	$(0, 2, 2)$
1 2	$(1, 0, 2)$
2 2	$(2, 1, 2)$

(b)

6. táblázat. Vektorok lineáris kombinációi *(a)* $\mathbb{Z}_2$ és *(b)* $\mathbb{Z}_3$ fölött.

Az $x\mathbf{u} + y\mathbf{v}$ alakú lineáris kombinációk száma 9, ugyanis $x, y \in \mathbb{Z}_3$, ami $3 \cdot 3 = 9$ lehetőséget ad. Példaként egy lineáris kombináció, a többi a 6. (b) táblázatban
látható: $2\mathbf{u} + 1\mathbf{v} = 2(1, 1, 0) + (0, 1, 1) = (2, 2, 0) + (0, 1, 1) = (2, 0, 1)$.

Tökéletes biztonságú titkosítás

A következőkben egy egyszerű, de feltörhetetlen titkosító módszert mutatunk a $\mathbb{Z}_m$ -beli vektorműveletek alkalmazására.

3.2. Példa (One time pad -- a tökéletes titkosítás) Az üzenet küldése előtt a küldő és a fogadó megegyezik egy titkos kulcsban, mely egy olyan hosszú véletlen bitvektor, mint amilyen az üzenet legfőljebb lehet. Legyen a kulcs $\mathbf{k} \in \mathbb{Z}_2^n$. Legyen a titkosítandó üzenet $\mathbf{u} \in \mathbb{Z}_2^n$. A titkosítás során a küldő kiszámolja az $\mathbf{u} + \mathbf{k}$ vektort, és azt küldi a fogadónak, aki a titkosított üzenethez maga is hozzáadja a kulcsot, és mivel bármely $\mathbf{x} \in \mathbb{Z}_2^n$ vektorra $\mathbf{x} + \mathbf{x} = \mathbf{0}$, ezért $(\mathbf{u} + \mathbf{k}) + \mathbf{k} = \mathbf{u} + (\mathbf{k} + \mathbf{k}) = \mathbf{u}$, vagyis a fogadó így valóban megfejti az üzenetet.

- Példaként egy üzenet, egy kulcs és a kettő összege - a titkosított üzenet - a tömör bitvektor-jelöléssel

$$\begin{aligned} \text{az üzenet:} \quad & \mathbf{u} = 010101010000111111111111 \\ \text{a kulcs:} \quad & \mathbf{k} = 001011000101101001011010 \\ \text{a titkosított üzenet:} \quad & \mathbf{u} + \mathbf{k} = 011110010101010110100101 \end{aligned}$$

- A bitvektorok ilyen módon való összeadása megegyezik a kizáró vagy nevű logikai művelettel, melyet a XOR szóval (exlusive or), vagy a $\oplus$ műveleti jellel is szoktak jelölni.
- E titkosítás hátránya, hogy a $\mathbf{k}$ kulcs csak egyszer használható fel, mert két különböző $\mathbf{u}_1 + \mathbf{k}$ és $\mathbf{u}_2 + \mathbf{k}$ üzenetet elcsípve és összeadva az $(\mathbf{u}_1 + \mathbf{k}) + (\mathbf{u}_2 + \mathbf{k}) = \mathbf{u}_1 + \mathbf{u}_2$ vektorban már nem szerepel $\mathbf{k}$, és ebből statisztikai módszerekkel már mindkét üzenet megkapható.
- Bizonyítható, hogy e kód megfejthetetlen, ha $\mathbf{k}$ valóban véletlen bitsorozat, és csak egyetlen üzenet titkosítására használjuk.
- A modern kriptográfiai módszer egy része lényegében erre a módszerre épül azzal a módosítással, hogy a véletlen sorozat helyett egy álvéletlen sorozatot használnak, mely egy kulcsszóból generálható.

A fenti módszer nem csak Z_2-vel végezhető. Ha a 26 betűből álló angol ábécé betűnek Z_{26} elemeit feleltetjük meg, az $\mathbf{u} + \mathbf{k}$ vektort $\mathbb{Z}_{26}^n$-ben számolhatjuk. Évszázadokig voltak használatban olyan titkosító technikák, amelyek lényegében a fenti módszert használták azzal a gyengítéssel, hogy a véletlen kulcs helyett egy könnyen megjegyezhetőt választottak. Sokáig hitték feltörhetetlennek például a Vigenere-titkosítást, melyben a kulcs egyetlen szó ismétléseiből állt.

3.3. Példa (Vigen\`ere-titkosítás) Feleltessük meg a magyar ábécé betűinek Z_{32} elemeit:

A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	R	S	T	U	Ú	Ü	Ű	V	Z	Y
0		2		4		6		8	10		12		14		16		18		20		22		24		26		28		30		
	1		3		5		7		9	11		13		15		17		19		21		23		25		27		29		31	

Legyen a kulcs a TITOK szó, és titkosítsuk a JÖVŐHETILOTTÓSZÁMOK szöveget Vigenere módszerével.

Megoldás

Először a fenti táblázat szerint minden betűt a neki megfelelő számmal helyettesítünk mind a titkosítandó szövegben, mind a kulcsban. Ezután a szöveg alá írjuk a kulcsot, a kulcsszót annyiszor ismételgetve, ahányszor szükséges, majd $\mathbb{Z}_{32}$-ben számolva összeadjuk az egymás alá írt számokat, végül az így kapott összegeket a nekik megfelelő betűkkel helyettesítjük:

J	Ö	V	Ő	H	E	T	I	L	O	T	T	Ó	S	Z	Á	M	O	K
12	19	29	20	9	5	24	10	14	17	24	24	18	23	30	1	15	17	13
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
T	I	T	O	K	T	I	T	O	K	T	I	T	O	K	T	I	T	O
24	10	24	17	13	24	10	24	17	13	24	10	24	17	13	24	10	24	17
=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
4	29	21	5	22	29	2	2	31	30	16	2	10	8	11	25	25	9	30
D	V	P	E	R	V	B	B	Y	Z	N	B	I	G	Í	U	U	H	Z

Tehát a titkosított szöveg: DVPERVBBYZNBIGÍUUHZ.

3.2 Kódok, lineáris kódok

Hibajelző és hibajavító kódok

A kódelmélet egyik célja, hogy redundáns információ hozzáadásával elérje az elküldött üzenet megérkezését zajos, veszteséges csatornán keresztül is. Ennek egyik módja hibajelző kód alkalmazása, mely jelez bizonyos - gyakran előforduló - hibákat, lehetővé téve a hibásan megérkezett üzenet újraküldését. Ennél is többet tud a hibajavító kód, mely hibák kijavítására is képes.

Világos, hogy a hibák mérésénél számunkra az a fontos, hogy az elküldött és a fogadott vektor hány koordinátahelyen különbözik. Ezt az értéket a két vektor Hamming-távolságának fogjuk nevezni. Például a 01001110 és a 01101100 vektorok Hamming-távolsága 2, mert a két vektor a 3. és 7. helyen - azaz két helyen - különbözik.

A kódot e-hibajelzőnek nevezzük, ha bármely kódvektorban legföljebb e koordinátát megváltoztatva olyan vektort kapunk, mely nem kódvektor, vagyis amely nem tartozik a kódba. A hibajelzés tehát úgy történik, hogy észleljük, ha egy nem a kódba tartozó vektor érkezik.

Egy kódot d-hibajavítónak nevezünk, ha bármely kódvektorára igaz, hogy benne legföljebb d koordinátát megváltoztatva olyan vektort kapunk melyhez csak ez az egyetlen kódvektor van tőle legföljebb d Hamming-távolságnyira. Világos, hogy ha egy kódban bármely két kódszó távolsága legalább 3, akkor ha egy kódszóban egy koordináta megváltozik, akkor e hiba egyértelműen javítható.

A 3.1 példában előállított lineáris kombinációk hibajelző kódok, egyikük hibajavító is. Határozzuk meg, hogy hány hibát jeleznek, és amelyik javít is, hány hibát javít!

Alappéldák: egyszerű hibajelző és hibajavító kódok

A hibajelzés és hibajavítás legegyszerűbb módja az üzenet többszöri elküldése.

3.4. Példa (Ismétlő kód) Legyen a kódábécé tetszőleges, és a kód álljon azokból az n -hosszú kódszavakból, melyek minden koordinátája azonos. E kód legföljebb $n-1$ hibát jelez, és $\lfloor \frac{n-1}{2} \rfloor$ hibát javít.

Megoldás

n hibát nem tud e kód jelezni minden esetben, pl. ha az $xx\ldots x$ üzenet $yy\cdots y$ -ra változik, az hibátlan üzenetnek tűnik. Másrészt n -nél kevesebb hibát mindig jelez a kód, hisz egy kódvektorban legföljebb $n-1$ koordinátát megváltoztatva, az már nem állhat azonos koordinátákból. Ha egy kódszóban a koordináták felénél kevesebb koordináta változik meg, akkor abból még rekonstruálható az eredeti kódszó. Ha viszont épp a koordináták fele változik meg, ez nem mindig sikerülhet, pl. a 4-hosszú $xxyy$ kódszóról nem dönthető el, hogy az $xxxx$ vagy az $yyyy$ kódszóban történt 2 hiba.

Az elektronikus számítógépek adatkezelésének egyik első ötlete az adattárolás vagy továbbítás biztonságosabbá tételére a paritásbit. Ha egy $(n-1)$ -hosszú $\mathbf{b}$ bitvektorhoz még egy bitet csatolunk, melynek értéke 1, ha $\mathbf{b}$-ben páratlan sok bit egyenlő 1-gyel, egyébként 0, akkor olyan n -hosszú vektort kapunk, melyben páros sok 1-es van. A kód tehát az összes olyan n -hosszú kódszóból áll, melyben az egyesek száma páros. E kódot paritásellenőrző kódnak nevezzük, a hozzáadott bitet paritásbitnek.

A paritásbit $\mathbb{Z}_2$ fölött $\mathbf{1}\cdot\mathbf{b}$ alakba írható, ahol $\mathbf{1}$ a $\mathbf{b}$-vel azonos hosszúságú és csupa 1-esből álló vektor.

Ha $\mathbf{u}$ jelzi a paritásbittel megnövelt vektort, akkor $\mathbf{u}$ pontosan akkor tartozik a kódhoz, ha $\mathbf{1}\cdot\mathbf{u}=0$ ($\mathbf{1}$ most az $\mathbf{u}$-val azonos hosszúságú).

3.5. Példa (Paritásellenőrző kód)A paritásellenőrző kód 1-hibajelző, de jelez minden olyan hibát, melyben páratlan sok koordináta változik meg.

Megoldás

Ha épp egy bit változik meg, akkor páratlan sok 1-es lesz a vektorban, tehát e hibát e kód jelzi. Ugyanez történik, ha páratlan sok koordináta változik meg, de nem jelzi, ha 2, illetve általában páros sok hiba történik.

A paritásellenőrző kód általánosítható $\mathbb{Z}_2$-ről tetszőleges $\mathbb{Z}_m$-re: nullösszegű kódnak nevezzük a $\mathbb{Z}_m^n$ összes olyan $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ vektorából álló kódot, melyekre $v_1 + v_2 + \cdots + v_n = 0$, azaz melyekre $\mathbf{1} \cdot \mathbf{v} = 0$.

A nullösszegű kódnál több hibát is jeleznek azok a változatai, amelyekben nem az $\mathbf{1}$, hanem valamely más vektorral vett skaláris szorzatokat kell vizsgálni. Ezek a skaláris szorzatok úgy is reprezentálhatók, hogy egy adott üzenetvektorhoz egy vagy több ún. ellenőrző összeget írunk, megnövelve a koordináták számát.

A magyar személyi szám a személyre jellemző 10 jegyből, és az azt követő e ellenőrző összegből áll. Az e kiszámítási képlete

$$\mathbb{Z}_{11}\text{-ben számolva:} \quad e = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \cdot \mathbf{u},$$

ahol $\mathbf{u}$ a személyi szám első 10 jegye. Az egy napon születettek személyi számának megkülönböztetésére a szám $8 - -10$-edik jegyét úgy választják ki, hogy $e \neq 10$, így az ellenőrző összeg mindig egyjegyű. Korábban hasonló képlettel számolták a könyvek ISBN-kódját (International Standard Book Number), de ott ha 10 volt az ellenőrző kód, egy X-et - római tízest - írtak helyébe. Kérdés: miért nem $\mathbb{Z}_{10}$-ben számolják az ellenőrző jegyet e kódoknál?

27. ábra. Egy könyv ISBN-13 kódja, ami egyúttal az EAN kódja is. Az EAN-kódhoz tartozik egy vonalkód is. 2007 óta a könyvek ISBN-száma (ISBN-13) és EAN-kódja megegyezik (korábban az ISBN 10-jegyű volt).

A termékek EAN-kódja (European Article Number) egy 13-jegyű, a termék azonosítására szolgáló kód, melyhez egy vonalkód is tartozik. A 13-dik jegy az ellenőrző összeg. Ha az EAN kódvektort $\mathbf{v}$ jelöli, akkor fönn kell állni

$$\mathbb{Z}_{10}\text{-ben számolva az } (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) \cdot \mathbf{v} = 0$$

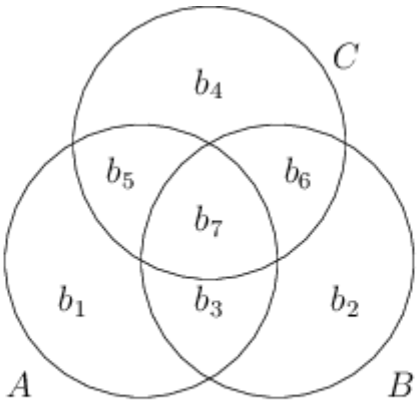
összefüggésnek (27. ábra).

Hamming-kód

A következő kód bináris, 7-hosszú, mely egy 4-hosszú üzenethez három paritásbitet ad. A kódolandó üzenet $b_3b_5b_6b_7$, a kód $\mathbf{b} = b_1b_2b_3b_4b_5b_6b_7$, a b_1, b_2, b_4 paritásbitek a következő egyenlőségekből számolandók:

$$\begin{aligned} b_1 + b_3 + b_5 + b_7 &= 0 \\ b_2 + b_3 + b_6 + b_7 &= 0 \\ b_4 + b_5 + b_6 + b_7 &= 0 \end{aligned} \tag{3.1}$$

E kissé esetlegesnek tűnő összegeket könnyen áttekinthetővé teszi a 28. ábra. Ezen a hét bit mindegyikét egy három halmazt tartalmazó Venn-diagram egy-egy résztartományához rendeltük. Egy vektor akkor tartozik a kódhoz, ha a három halmaz mindegyikébe tartozó bitek összege 0, azaz ha mindhárom halmazban páros sok 1-es bit van.



28. ábra. Hamming-kód konstrukciója

3.6. Példa (Bináris $\lbrack7,4,3\rbrack_2$ Hamming-kód) A fent definiált Hamming-kód $\mathbb{F}_2^7$ 16 vektorából áll, 2-hibajelző, és 1-hibajavító. $\mathbb{F}_2^7$ minden vektora vagy az (1) egyenletek által definiált bináris 7-hosszú Hamming-kódhoz tartozó kódvektor, vagy egyetlen koordináta megváltoztatásával azzá tehető!

Megoldás

Mivel b_3, b_5, b_6, b_7 értéke egymástól függetlenül tetszőlegesen megválasztható, másrészt egyértelműen megadják a maradék három bit értékét, ezért a kódszavak száma valóban $2^4 = 16$.

Tekintsünk egy tetszőleges $\mathbf{b} \in \mathbb{F}_2^7$ vektort. Ez vagy kódszó, vagy a 28 ábra szerinti A, B és C halmazok közül valamelyekben nem 0 a bitek összege. Ezesetben tekintsük azt az egyetlen bitet, mely pontosan a „renitens” halmazok metszetében van. Ekkor ennek az egyetlen bitnek a megváltoztatásával minden „renitens” halmazban 0-ra változik az összeg, így e bit megváltoztatásával kódszót kaptunk. Tehát e kód 1-hibajavító. Ebből az is következik, hogy semelyik két

kódszó Hamming-távolsága nem lehet 3-nál kisebb. Másrészt például a 0111000 és a nullvektor távolsága épp 3, így a kód bármely 2 hibát jelez, de három hibát már nem minden esetben, tehát e kód 2-hibajelző.

E kód optimális abban az értelemben, hogy a kódszavak és a kódszavak egyetlen bitjének elrontásával kapott vektorok kiadják $\mathbb{F}_2^7$ összes vektorát. Ennek egy szép geometriai szemléltetés adható. Nevezzük $\mathbf{b}$-közepű 1-sugarú gömbnek azon pontok (vektorok) halmazát, melyek $\mathbf{b}$-től legföljebb 1 Hamming-távolságnyira vannak. Egy ilyen gömbnek összesen 8 pontja van, maga a kódszó, és az a 7 kódvektor, melyek pont egyetlen koordinátában különböznek $\mathbf{b}$-től. A Hamming-kód szavainak száma $2^4 = 16$, az ezek köré emelt gömbök páronként diszjunktak, $16 \cdot 8 = 128 = 2^7$, azaz e gömbök páronként diszjunktak, és hézagtalanul lefedik $\mathbb{F}_2^7$ összes pontját! Azokat a kódokat, ahol a kódszavak köré emelt azonos sugarú gömbök átfedés nélkül, és hézagtalanul lefedik a teret, perfektnek nevezzük.

Láttuk, hogy semelyik két kódszó távolsága nem lehet 3-nál kisebb, viszont, hogy van két olyan kódszó, amelyek Hamming-távolsága pontosan 3. Azt fogjuk mondani, hogy e kód kódtávolsága, vagy minimális távolsága 3.

A Hamming-kód egy igen meglepő és érdekes feladat megoldásához is segítséget nyújt:

3.2.1. Feladat 7 halálraítélt körben ül, mindegyikük fején egy véletlenül kiválasztott piros vagy fekete sapka. Mindenki látja a többiek sapkáját, de senki se látja a sajátját. Semmi módon nem kommunikálhatnak egymással. Egy idő után egyszerre mindegyiküknek tippelnie kell a saját sapkája színére. Három válasz lehetséges: „nem tudom”, „fekete”, „piros”. Ha senki nem találja el, vagy csak egy is akad, aki téved, mind meghalnak, egyébként mind megmenekülnek. Tudunk-e számukra olyan eljárást javasolni, ami 1/2-nél nagyobb valószínűséggel megmenekíti őket. Mi a legnagyobb valószínűség, amit el tudunk érni?

3.7. Példa (Kiegészített bináris $\lbrack8,4,4\rbrack_2$ Hamming-kód) A 7-hosszú bináris $[7, 4, 3]_2$ Hamming-kódból a kódszavak paritásellenőrző bitjének hozzávételével kapott kódot 8-hosszú kiegészített bináris Hamming-kódnak nevezzük, mely 3-hibajelző és 1-hibajavító.

Megoldás

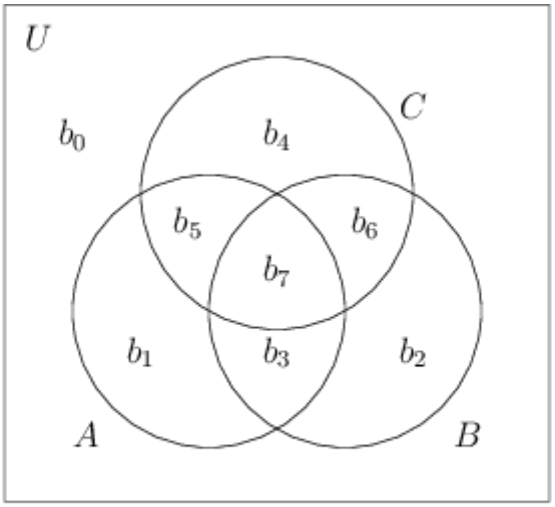
Jelölje a paritásbitet b_0, azaz

$$b_0 + b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7 = 0.$$

Ezt az egyenletet az (1) egyenletrendszerhez véve, majd annak egyenleteit ehhez adva a következő - e kódot definiáló - egyenletrendszert kapjuk:

$$b_0 + b_3 + b_5 + b_6 = 0$$
$$b_1 + b_3 + b_5 + b_7 = 0$$
$$b_2 + b_3 + b_6 + b_7 = 0$$
$$b_4 + b_5 + b_6 + b_7 = 0$$

A kiegészített Hamming-kód is ábrázolható Venn-diagrammal: az A , B és C halmazokat tartalmazó U univerzumban van még egy bit, b_0 , amely az A , B és C halmazokon kívül van, és egy vektor pontosan akkor kódszó, ha az A , B , C és az U halmazok mindegyikében páros sok bit egyes.



29. ábra. Kiegészített Hamming-kód konstrukciója

Tekintsünk két tetszőleges olyan kódszót a Hamming-kódból, amelyek távolsága épp 3. Ekkor egyikükben páros, másikukban páratlan sok 1-es van, így a b_0 bit hozzávételével biztosan 4-re növekszik a távolságuk. Ha távolságuk 4 volt, a kiegészített kódban is az marad, tehát a kiegészített kódban bármely két kódszó távolsága legalább 4. Kaptuk tehát, hogy e kód kódtávolsága 4, így 3-hibajelző. Az 1-hibajavítás következik a Hamming-kód ugyanezen tulajdonságából.

Utolsó példánk a 3-elemű testre épül:

3.8. Példa (4-hosszú ternér $\lbrack4,2,3\rbrack_3$ Hamming-kód) Az $\mathbb{F}_3^4$ tér összes $(a, b, a + b, a - b)$ alakú vektorának halmaza egy 1-hibajavító, 3-kódtávolságú kód.

Megoldás

Mindenekelőtt jegyezzük meg, hogy $\mathbb{F}_3$-ban $-1 = 2$, tehát $a - b$ helyett számolhatunk $a + 2b$-vel is.

Könnyen látható, hogy az a, b, $a + b$, $a - b$ értékek közül bármely kettő egyértelműen megadja a másik kettőt is. Például az

$$a + b = x$$
$$a - b = y$$

egyenletrendszer egyértelműen megoldható a-ra és b-re. Így e kód kódtávolsága legalább 3. Mivel van pontosan 3 távolságra lévő két kódszó: például a 0000 és a 0112 kódszavak, ezért a kód 1-hibajavító.

Korlátok kód méretére

A továbbiakban néhány már említett fogalomhoz jelöléseket is rendelünk.

3.9. Definíció (Kód) Legyen $\mathcal{Y}$ egy q-elemű halmaz - rendszerint $\mathcal{Y} = \mathbb{F}_q$ -, n egy pozitív egész. A $\mathcal{C} \subseteq \mathcal{Y}^n$ halmazt $\mathcal{Y}$ fölötti (n, k)- vagy $(n, k)_q$-kódnak, illetve blokk-kódnak nevezzük, ha $M = |\mathcal{C}|$ és $k = \log_q M$. Egy kölcsönösen egyértelmű $\mathcal{X} \to \mathcal{C}$ leképezést kódolásnak nevezünk, ahol $\mathcal{X}$ a kódolandó objektumok halmaza.

- További elnevezések: $\mathcal{Y}$ a kódábécé, $q = |\mathcal{Y}|$ a kódábécé mérete, n a kódhossz, $M = |\mathcal{C}|$ a kódméret, $k = \log_q M$ a dimenzió vagy az üzenet hossza.
- Ha $k = \log_q M$ nem egész szám, a $\mathcal{C}$ kódra inkább az (n, M) jelölés használatos, de mi ilyen kódokkal nem fogunk foglalkozni.

3.10. Definíció (Hamming-távolság) Legyen $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ két kódszó. Hamming-tá-vol-sá-guk

$$\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i,\ 1 \leqslant i \leqslant n\}|$$

3.11. Definíció (Kódtávolság, minimális távolság)
A $d = \min_{\mathbf{x},\mathbf{y} \in \mathcal{C}} \mathrm{d_H}(\mathbf{x}, \mathbf{y})$ értéket a $\mathcal{C}$ kód kódtávolságának nevezzük.
A d kódtávolságú (n, k)-kódot (n, k, d)-kódnak is mondjuk.

3.12. Tétel (Singleton-korlát) Ha $\mathcal{C}$ egy (n, k, d)-kód, akkor

$$M \leqslant q^{n-d+1}, \text{ azaz } d \leqslant n - k + 1.$$

Bizonyítás. Ha d a kódtávolság, akkor nincs két kódszó, mely az q^{n-d+1} első $M = q^k$ jelen megegyezne, így a szavak száma legfőljebb $n \leqslant n - d + 1$. Mivel $d \leqslant n$, ezért $n + 1$, azaz $d \leqslant n + 1$. [QED]

Azokat a kódokat, amelyekre a Singleton-korlátban egyenlőség áll MDS-kódoknak nevezzük (maximum distance separable). A ternér $[4, 2, 3]$ Hamming-kód MDS-kód.

3.13. Tétel (Hamming-korlát) A d kódtávolságú $\mathcal{C} \subseteq \mathcal{Y}^n$ ($|\mathcal{Y}| = q$) kódra

$$|\mathcal{C}| \leqslant \frac{q^n}{V_q(t,n)}, \quad \text{ahol} \quad V_q(j,n) = \sum_{i=0}^{j} \binom{n}{i} (q-1)^i,$$

és $t = \lfloor \frac{d-1}{2} \rfloor$.

Bizonyítás. Ha d a kódtávolság, akkor két $t = \lfloor \frac{d-1}{2} \rfloor$ -sugarú gömb nem metszheti egymást. Egy ilyen gömb „térfogata” - azaz kódszavainak száma - $V_q(t,n)$, és az egymást nem metsző gömbök számának maximuma a kódszavak számára is felső becslést ad. [QED]

Azokat a kódokat, amelyekben itt egyenlőség áll, perfekt kódoknak nevezzük. A bináris $[7, 4, 3]$ Hamming-kód perfekt kód. Minden $\mathbb{F}_q$ feletti perfekt kód (n, k, d) paraméterhármasa megegyezik az alábbiak valamelyikével:

$$\left(\frac{q^r - 1}{q - 1}, q^{n-r}, 3 \right)_q,$$

ezek az 1-hibajavító kódok, közéjük tartoznak a Hamming-kódok, valamint

$$(23, 12, 7)_2 \text{ és } (11, 6, 5)_3,$$

ez utóbbiak neve bináris, illetve ternér Golay-kód.[8]

Lineáris kód

Az előző részben tárgyalt kódok közös és meglepő tulajdonsága, hogy mindegyik kód zárt az összeadásra és a skalárral való szorzás műveletére, azaz mindegyik kód altér az $\mathbb{F}_q^n$ térben. Az ilyen kódokat lineáris kódnak nevezzük. Pontosabban:

3.14. Definíció (Lineáris kód) Az $\mathbb{F}_q$ test fölött értelmezett $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódot lineáris $[n,k]_q$-kódnak nevezzük, ha $\mathcal{C}$ az $\mathbb{F}_q^n$ vektortér egy k-dimenziós altere. Szokás az $[n,k,d]_q$ jelölés használata a d-távolságú lineáris kódra.

- A definícióból következően a zérus kódszó minden lineáris kódnak eleme, és kódszavak minden lineáris kombinációja is kódszó.
- Az $[n,k,d]_q$ jelölésben a szögletes zárójel utal a kód linearitására. Így már értjük a korábbiakban használt $[7,4,3]_2$, $[8,4,4]_2$ és $[4,2,3]_3$ jelöléseket.

3.2.2. Feladat Ellenőrizzük, hogy az ismétlő kód $[n,1,n]_q$-kód, a paritásellenőrző kód $[n,n-1,2]_2$-kód, a nullösszegű kód $[n,n-1,2]_q$-kód, a bináris Hamming-kód $[7,4,3]_2$-kód, a bináris kiegészített Hamming-kód $[8,4,4]_2$-kód, a ternér Hamming-kód $[4,2,3]_3$-kód, tehát mindannyian lineáris kódok. Másrészt igazoljuk, hogy a magyar személyi szám nem lineáris kód.

Egy $\mathbf{c} \in \mathcal{C}$ kódszó Hamming-súlyán (weight) a nemnulla komponenseinek $\mathrm{wt}(\mathbf{c})$ számát értjük, azaz $\mathrm{wt}(\mathbf{c}) = |\{i : c_i \neq 0,\ i = 1,\dots,n\}|$. A $\mathcal{C}$ kód minimális súlya a legkisebb Hamming súlyú nemnulla kódszó w súlya, azaz $w = \min_{\mathbf{c}\in\mathcal{C},\mathbf{c}\neq\mathbf{0}} \mathrm{wt}(\mathbf{c})$.

3.15. Tétel Egy lineáris $\mathcal{C}$ kód kódtávolsága megegyezik minimális súlyával, azaz $d = w$.

Bizonyítás. Mivel $\mathcal{C}$ lineáris, ezért kódszavainak bármely lineáris kombinációja is kódszó, így, ha $\mathbf{x},\mathbf{y} \in \mathcal{C}$, akkor $\mathbf{x}-\mathbf{y} \in \mathcal{C}$. A távolság kiszámítása így a 0-tól való távolság számításává változtatható:

$$\begin{aligned} d &= \min_{\mathbf{x},\mathbf{y}\in\mathcal{C},\ \mathbf{x}\neq\mathbf{y}} \mathrm{d_H}(\mathbf{x},\mathbf{y}) = \min_{\mathbf{x},\mathbf{y}\in\mathcal{C},\ \mathbf{x}\neq\mathbf{y}} \mathrm{d_H}(\mathbf{x}-\mathbf{y},\mathbf{y}-\mathbf{y}) \\ &= \min_{\mathbf{c}\in\mathcal{C},\ \mathbf{c}\neq\mathbf{0}} \mathrm{wt}(\mathbf{c}) = w. \end{aligned}$$

[QED]

3.16. Tétel (súlyeloszlás $=$ távolságeloszlás) Bármely lineáris kódban a szavak súlyeloszlása megegyezik a távolságok eloszlásával.

Bizonyítás. Legyen a $\mathcal{C}$ kódban a w súlyú kódszavak száma A_w. Ha $\mathbf{c} \in \mathcal{C}$ egy tetszőleges kódszó, akkor az M^2 számú rendezett $(\mathbf{c}',\mathbf{c}'')$ kódszó-pár között pontosan M olyan van, ahol $\mathbf{c}'-\mathbf{c}''=\mathbf{c}$. Így a w távolságú szópárok száma MA_w. [QED]

Generátormátrix

Az, hogy $\mathcal{C}$ lineáris altér, egy egyszerű $\mathbb{F}_q^k \to \mathbb{F}_q^n$ kódolási eljárást tesz lehetővé. Legyen $\mathbf{g}_1$, $\mathbf{g}_2$,..., $\mathbf{g}_k$ a $\mathcal{C}$ egy bázisa. Egy tetszőleges $\mathbf{x} \in \mathbb{F}_q^k$ vektor (üzenet) $\mathbf{c} \in \mathcal{C}$ kódja legyen $\mathbf{c} = x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + \cdots + x_k\mathbf{g}_k$. Ez egy egyszerű mátrixszorzással is előállítható:

$$\mathbf{c} = \mathbf{x}\mathbf{G},$$

ahol a $k \times n$-es $\mathbf{G}$ mátrix - az úgynevezett generátormátrix - sorvektorai $\mathcal{C}$ bázisának elemei. (A kódelméletben a kódszavakat inkább sorvektorokkal szokás reprezentálni.)

3.17. Példa Írjuk fel az eddig vizsgált kódok generátormátrixait!

Megoldás

(a)Ismétlő kód. Természetesen feltesszük, hogy $\mathcal{Y} = \mathbb{F}_q$.
Ekkor $\mathcal{C}$ az $(1, 1, \ldots, 1)$ kódszó által generált egydimenziós altér $\mathbb{F}_q^n$-ben.
Így $\mathbf{G} = [1\ 1\ \ldots\ 1]$.

(b)Paritásellenőrző kód, nullösszegű kód.
Az $(a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^{n-1} \mapsto (a_1, \ldots, a_{n-1}, -\sum_{i=1}^{n-1} a_i) \in \mathbb{F}_q^n$ leképezés mátrixa

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \ldots & 0 & -1 \\ 0 & 1 & \ldots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -1 \end{bmatrix}$$

(c)Bináris $[7, 4, 3]_2$ Hamming-kód. Az $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \ldots, b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$ leképezés mátrixa

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{3.2}$$

Például az $\mathbf{x} = (0, 1, 1, 0)$ üzenet kódja

$$\mathbf{c} = \mathbf{xG} = \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix} \begin{bmatrix}1 & 1 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$$
$$= \begin{bmatrix}1 & 1 & 0 & 0 & 1 & 1 & 0\end{bmatrix}$$

(d)Kiegészített bináris $[8, 4, 4]_2$ Hamming-kód. Az előző generátormátrixot itt csak egy nulladik oszloppal kell kiegészíteni a $b_0 = b_3 + b_5 + b_6$ összefüggésnek megfelelően:

$$\mathbf{G} = \begin{bmatrix}1 & 1 & 1 & 1 & 0 & 0 & 0 & 0\\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$$

(e)Ternér $[4, 2, 3]_3$ Hamming-kód.
A $\mathbb{F}_3^2 \to \mathbb{F}_3^4 : (a, b) \mapsto (a, b, a + b, a + 2b)$ leképezés mátrixa

$$\mathbf{G} = \begin{bmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 1 & 2\end{bmatrix}$$

Világos, hogy a generátormátrix nem egyértelmű, hisz a kódban maga a $\mathcal{C}$ altér fontos, az $\mathbb{F}_q^k$-nak erre való bijektív leképezése nem. Az altérnek több bázisa van, és egy bázis is többféleképp sorolható fel. Tudjuk, hogy $\mathbf{G}$ elemi sorműveletekkel redukált lépcsős alakra hozható, ami egyértelmű, és hogy ennek sorvektorai ugyanazt a teret generálják, mint az eredeti mátrix. A vezető egyesek oszlopait kiemelve egy egységmátrixot kapunk, így ezeken a helyeken megjelenik az üzenetvektor.

Azt mondjuk, hogy az $\mathbb{F}_q^k \to \mathcal{C}$ kódolás szisztematikus az i_1,..., i_k helyeken, ha az üzenet k jegye megjelenik a kódszó i_1-edik,..., i_k-adik helyein. A 3.6 példában megadott Hamming-kódolás szisztematikus a 3-, 5-, 6-, 7-dik helyeken.

3.2.3. Feladat A $\mathcal{C}$ kódnak pontosan akkor van $\mathbb{F}_q^k \to \mathcal{C}$ szisztematikus kódolása az i_1,..., i_k helyeken, ha a $\mathbf{G}$ mátrix i_1-edik,..., i_k-adik oszlopai lineárisan függetlenek. Ekkor elemi sorműveletekkel $\mathbf{G}$ mindig átalakítható olyan $\mathbf{G}'$ mátrixszá, mely ugyancsak $\mathcal{C}$ generátormátrixa, és a vele való kódolás szisztematikus az i_1,..., i_k helyeken.

Ha azt mondjuk, hogy egy kódolás szisztematikus, de nem adjuk meg hogy mely helyeken, akkor az azt jelenti, hogy az első k helyen. Ilyenkor a generátormátrix alakja

$$\mathbf{G} = \left[\begin{array}{c|c} \mathbf{I}_k & \mathbf{A}_{k\times(n-k)} \end{array} \right]$$

Ezt nevezzük a generátormátrix standard alakjának. Ekkor bármely $\mathbf{x}$ üzenethez tartozó $\mathbf{c} = \mathbf{xG}$ kódszó $\mathbf{c} = [\mathbf{x}|\mathbf{xA}_{k\times(n-k)}]$ alakú.

Azokat a koordinátákat, ahol a kódolás szisztematikus, üzenetszegmensnek (information set), a maradék $n-k$ koordinátából álló részt ellenőrző szegmensnek (vagy paritásszegmensnek) nevezzük, hisz ezek valóban az üzenetszegmens koordinátáinak bizonyos „ellenőrző lineáris kombinációi”.

Kódok ekvivalenciája

Elemi sorműveletekkel nem mindig érhető el, hogy egy kódolás az első k helyen szisztematikus legyen, de a koordináták permutációjával igen. Két lineáris kódot permutációekvivalensnek vagy egyszerűen ekvivalensnek nevezünk, ha a koordinátáknak egy adott permutációja erejéig megegyeznek, azaz $\mathcal{C}$ pontosan akkor ekvivalens $\mathcal{C}'$-vel, ha létezik egy $\mathbf{P}$ permutációmátrix,
hogy $\mathbf{c} \in \mathcal{C} \iff \mathbf{cP} \in \mathcal{C}'$. Ha $\mathbf{G}$ a $\mathcal{C}$ generátormátrixa, akkor $\mathbf{G}' = \mathbf{GP}$ a $\mathcal{C}'$-é.

Például az alappéldák közt megadott Hamming-kódolás és kiegészített Hamming-kódolás egy vele permutációekvivalens szisztematikus változatának generátormátrixa:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

A permutációk: (1745263), illetve $(184)(2763)(5)$, a permutációmátrixok:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{és} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

A $\mathcal{C}$ és $\mathcal{C}'$ kódok diagonálisan ekvivalensek, ha létezik egy olyan $\mathbf{D}$ diagonális mátrix, hogy $\mathbf{c} \in \mathcal{C} \iff \mathbf{cM} \in \mathcal{C}'$. E két ekvivalencia egyesítése a monomiális ekvivalencia, ahol $\mathbf{M}$, ahol monomiális mátrix, azaz minden sorában és oszlopában egyetlen nemnulla elem áll. Itt is fennáll a , illetve a összefüggés.

Ellenőrző mátrix

3.18. Definíció A $\mathcal{C}$ kód duálisán a

$$\mathcal{C}^{\perp} = \{\, \mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{c} = 0 \text{ minden } \mathbf{c} \in \mathcal{C} \text{ kódszóra} \,\}$$

kódot értjük, mely egy lineáris kód. A $\mathcal{C}^{\perp}$ kód $\mathbf{H}$ generátormátrixát a $\mathcal{C}$ kód ellenőrző mátrixának nevezzük. (Használatos még a paritásmátrix vagy a paritásellenőrző mátrix elnevezés is, bár paritásról csak a $q = 2$ esetben van szó.)

Azonnal látszik, hogy az ismétlő kód és a nullösszegű kód egymás duálisa, valamint hogy az ismétlő kód generátormátrixa a nullösszegű kód ellenőrző mátrixa és fordítva.

3.19. Tétel Ha $\mathcal{C}$ egy lineáris $[n, k]$-kód, akkor

1. $\mathcal{C}^{\perp} = \{\, \mathbf{v} \in \mathbb{F}_q^n : \mathbf{v}\mathbf{G}^{\mathsf{T}} = \mathbf{0} \,\}$,
2. $\mathcal{C}^{\perp}$ egy $[n, n-k]$-kód,
3. $\mathcal{C}^{\perp\perp} := (\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$,
4. $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{F}_q^n : \mathbf{c}\mathbf{H}^{\mathsf{T}} = \mathbf{0} \,\}$,
5. $\mathbf{G}\mathbf{H}^{\mathsf{T}} = \mathbf{O}_{k\times(n-k)}$, $\mathbf{H}\mathbf{G}^{\mathsf{T}} = \mathbf{O}_{(n-k)\times k}$,
6. ha $\mathbf{G} = [\mathbf{I}_k|\mathbf{A}]$ a $\mathcal{C}$ kód standard alakú generátormátrixa, akkor ellenőrző mátrixa $\mathbf{H} = [-\mathbf{A}^{\mathsf{T}}|\mathbf{I}_{n-k}]$.

Bizonyítás. (1) világos a duális kód definíciójából. Másként fogalmazva a $\mathcal{C}^{\perp}$ kód megegyezik $\mathbf{G}^{\mathsf{T}}$ bal magterével. Mivel a bal magtér dimenziójának és a mátrix rangjának összege megegyezik a sorok számával, ezért $\dim(\mathcal{C}^{\perp}) + k = n$, azaz $\dim(\mathcal{C}^{\perp}) = n - k$, ami bizonyítja (2)-t. Ezt az érvelést megismételve $\mathcal{C}^{\perp\perp}$-re kapjuk, hogy $\mathcal{C}^{\perp\perp}$ egy $[n, k]$-kód. E kód tartalmazza $\mathcal{C}$-t, és dimenziójuk megegyezik, így $\mathcal{C}^{\perp\perp} = \mathcal{C}$, azaz fennáll (3) is. Ezután (1) bizonyítja (4)-et. Mivel minden $\mathbf{x} \in \mathbb{F}_q^k$ vektorra $\mathbf{x}\mathbf{G} \in \mathcal{C}$, azaz $\mathbf{x}\mathbf{G}\mathbf{H}^{\mathsf{T}} = \mathbf{0}$, ezért $\mathbf{G}\mathbf{H}^{\mathsf{T}}$ csak a zérusleképezés lehet, ami bizonyítja (5)-öt. A (6)-ban megadott $\mathbf{G}$ és $\mathbf{H}$ mátrixokra a blokkmátrixok szorzási szabálya szerint $\mathbf{G}\mathbf{H}^{\mathsf{T}} = \mathbf{O}$, így bármely $\mathbf{c} = \mathbf{x}\mathbf{G}$ kódszóra $\mathbf{c}\mathbf{H}^{\mathsf{T}} = \mathbf{x}\mathbf{G}\mathbf{H}^{\mathsf{T}} = \mathbf{x}\mathbf{O} = \mathbf{0}$,

tehát (4) szerint $\mathbf{H}$ valóban ellenőrző mátrix, feltéve, hogy sorai lineárisan függetlenek, ami pedig nyilvánvaló. [QED]

3.20. Tétel ($ \mathcal{C}$ kódtávolsága -- $ \mathbf{H}$ oszlopai)
Legyen $\mathbf{H}$ a $\mathcal{C}$ lineáris kód egy tetszőleges ellenőrző mátrixa, és $s > 0$ egész.
A $\mathcal{C}$ kód kódtávolsága pontosan akkor nagyobb s -nél,
ha $\mathbf{H}$ bármely s különböző oszlopa lineárisan független. Következésképp
a $\mathcal{C}$ kód d minimális távolsága megegyezik a $\mathbf{H}$ mátrix lineárisan összefüggő oszlopai minimális számával.

Bizonyítás. Megmutatjuk, hogy a $\mathbf{H}$ mátrix s különböző (i_1 -edik,... i_s -edik) oszlopa pontosan akkor lineárisan összefüggő, ha van olyan nem nulla $\mathbf{c}$ kódszó, melyben a nem nulla koordináták indexei az $\{i_1, \ldots, i_s\}$ halmazba esnek.

A $\mathbf{c} \in \mathcal{C}$ kódszó súlya legyen s. Mivel $\mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$, ezért $\mathbf{H}$-nak van s oszlopa, melyek lineárisan összefüggők. Fordítva, ha $\mathbf{H}$-nak van s lineárisan összefüggő oszlopa, akkor az ezek közti $c_{i_1}\mathbf{h}_{i_1} + \cdots + c_{i_s}\mathbf{h}_{i_s} = 0$ lineáris összefüggést mátrixalakba írva egy olyan nem nulla, és legfeljebb s súlyú $\mathbf{c}$ vektorhoz jutunk, melyre $\mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$, azaz amely benne van $\mathcal{C}$ -ben. Tehát pontosan akkor van $\mathcal{C}$ -ben legfeljebb s súlyú kódszó, ha $\mathbf{H}$-ban van s lineárisan összefüggő oszlop. Ez azt jelenti, hogy ha $\mathcal{C}$ kódtávolsága d, akkor $\mathbf{H}$-nak minden $d-1$ oszlopa lineárisan független, de van d lineárisan összefüggő oszlopa. [QED]

A 3.20 tétel átfogalmazható a $\mathbf{H}$ mátrix nélkül is a $\mathcal{C}^{\perp}$ kódra való hivatkozással.

Kihasználva hogy $\mathbf{H}$ rangja $n-k$, a lineáris kódok esetére egy új bizonyítást adtunk a Singleton-korlátra.

3.21. Tétel (Singleton-korlát lineáris kódra) Tetszőleges $\mathcal{C}$ lineáris $[n,k,d]$ kódra

$$d \leqslant n - k + 1.$$

Egy kódnak és duálisának szisztematikussága összefügg.

3.22. Tétel A $\mathcal{C}$ kódnak pontosan akkor van szisztematikus kódolása adott k helyen, ha a $\mathcal{C}^{\perp}$ kódnak van a maradék $n-k$ helyen.

Bizonyítás. Feltehető, hogy $\mathcal{C}$ -nek az első k helyen van szisztematikus kódolása. Legyen $\mathcal{C}$ ellenőrző mátrixa $\mathbf{H}$. Meg kell mutatni, hogy $\mathbf{H}$ utolsó $n-k$ oszlopa lineárisan független. Indirekt módon tegyük fel, hogy lineárisan összefüggők, azaz van olyan $\mathbf{0} \neq \mathbf{y} = (0, \ldots, 0, y_{k+1}, \ldots, y_n)$ vektor, hogy $\mathbf{y}\mathbf{H}^{\mathsf{T}} = \mathbf{0}$. Ekkor $\mathbf{y} \in \mathcal{C}$, ami ellentmondásra vezet, hisz $\mathcal{C}$ -nek van $\mathbf{G} = [\mathbf{I}|\mathbf{A}]$ alakú generátormátrixa, így minden $\mathbf{x}$ üzenet kódja $\mathbf{y} = [\mathbf{x}|\ldots]$ alakú, $\mathbf{y}$-ból az olvasható ki, hogy $\mathbf{x} = \mathbf{0}$,

így $\mathbf{y} = \mathbf{xG} = \mathbf{0G} = \mathbf{0}$. Ez ellentmond az $\mathbf{y} \neq \mathbf{0}$ kikötésnek. Megmutattuk tehát, hogy ha $\mathcal{C}$ -nek van szisztematikus kódolása valamely k helyen, akkor $\mathcal{C}^{\perp}$ -nek van a többi $n-k$ helyen. Ezt a duális kódra is alkalmazva kapjuk a tétel állítását. [QED]

3.23. Példa Írjuk fel a 3.17 példabeli generátormátrixokhoz tartozó ellenőrző mátrixokat egy esetleges koordinátapermutáció után a 3.19 tételbeli $\mathbf{H} = [-A^{\mathsf{T}}|I_{n-k}]$képlettel.

Megoldás

(a)Ismétlő kód. A generátormátrix $[1|1\dots1]$ alakú, így

$$\mathbf{H} = \begin{bmatrix} -1 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \dots & 1 \end{bmatrix}$$

(b)Paritásellenőrző kód, nullösszegű kód. Itt $\mathbf{H} = [1\dots1]$, ahol az utolsó 1-es egy 1×1-es egységmátrix.

(c)Bináris $[7,4,3]_2$ Hamming-kód. A (2) generátormátrix a (34) permutációval $[\mathbf{A}|\mathbf{I}]$ alakot ölt, amelyhez az $[\mathbf{I}|-\mathbf{A}^{\mathsf{T}}]$ ellenőrző mátrix tartozik. Ezen a (34) permutáció inverze - ami önmaga - a következő mátrixot adja:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{3.3}$$

(d)Kiegészített bináris $[8,4,4]_2$ Hamming-kód. Az előzőhöz hasonlóan:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(e)Ternér $[4,2,3]_3$ Hamming-kód. $-1 = 2$ és $-2 = 1$ felhasználásával

$$\mathbf{H} = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

Egy $\mathcal{C}$ lineáris kód önortogonális, ha $\mathcal{C}^\perp \geqslant \mathcal{C}$, és önduális, ha $\mathcal{C}^\perp = \mathcal{C}$.

3.2.4. Feladat A páros hosszú bináris ismétlő kód és a $[7,4]$ Hamming-kód duálisa önortogonális, míg a kiegészített $[8,4]_2$ és a $[4,2]_3$ Hamming-kódok önduálisak is.

Dekódolás, szindróma

Tegyük fel, hogy egy $\mathbf{c} \in \mathcal{C}$ kódszó helyett egy $\mathbf{v} = \mathbf{c} + \mathbf{e}$ érkezik, ahol $\mathbf{e}$ az ún. hibavektor. Mivel $\mathbf{c}\mathbf{H}^\mathsf{T} = \mathbf{0}$, ezért

$$\mathbf{v}\mathbf{H}^\mathsf{T} = (\mathbf{c}+\mathbf{e})\mathbf{H}^\mathsf{T} = \mathbf{c}\mathbf{H}^\mathsf{T} + \mathbf{e}\mathbf{H}^\mathsf{T} = \mathbf{e}\mathbf{H}^\mathsf{T},$$

vagyis $\mathbf{v}\mathbf{H}^\mathsf{T}$ csak a hibavektortól függ, így e vektor jelzi a hibát, orvosi hasonlattal élve olyan, mint a szindróma, mely jelzi a betegséget. Az

$$\mathbf{s} = \mathbf{v}\mathbf{H}^\mathsf{T}$$

vektort szindrómának nevezzük. A szindróma arra is lehetőséget ad, hogy segítségével megbecsüljük a hibavektort, és így tippeljünk az üzenetre. A kapott vektorhoz legközelebbi kódszóra tippelünk. Ha több kódszó is azonos távolságra van, véletlenül választunk közülük. A dekódolás módját egy táblázatba is foglalhatjuk, amit standard elrendezési táblázatnak nevezünk. Ennek első sorába a $\mathcal{C}$ kódszavai vannak írva, és minden sorába $\mathcal{C}$ valamely $\mathbf{e}$ vektorral való eltoltja, vagyis egy affin altér vektorai. Arra kell ügyelni, hogy minden sorban a legkisebb súlyú vektorok valamelyikét válasszuk $\mathbf{e}$-nek. Világos, hogy minden affin altérhez egyetlen szindróma tartozik, hisz bármely
két $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ kódszóra $(\mathbf{c}_1+\mathbf{e})\mathbf{H}^\mathsf{T} = (\mathbf{c}_2+\mathbf{e})\mathbf{H}^\mathsf{T} = \mathbf{e}\mathbf{H}^\mathsf{T} = \mathbf{s}$. Így a táblázatnak q^{n-k} sora van, vagyis ennyi hibamintát tudunk javítani.

szindróma	hiba			
$\mathbf{s}_0 = 0$	$\mathbf{e}_0 = \mathbf{c}_0 = \mathbf{0}$	$\mathbf{c}_1$	$\dots$	$\mathbf{c}_{q^k-1}$
$\mathbf{s}_1$	$\mathbf{e}_1$	$\mathbf{c}_1 + \mathbf{e}_1$	$\dots$	$\mathbf{c}_{q^k-1} + \mathbf{e}_1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{s}_{q^{n-k}-1}$	$\mathbf{e}_{q^{n-k}-1}$	$\mathbf{c}_1 + \mathbf{e}_{q^{n-k}-1}$	$\dots$	$\mathbf{c}_{q^k-1} + \mathbf{e}_{q^{n-k}-1}$

3.24. Példa (Táblázatos dekódolás) Tekintsük azt a kódot, melynek ellenőrző mátrixa

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & \mathbf{0} & 1 & 0 & 1 & 0 & \mathbf{0} & 0 \\ 1 & 1 & 1 & & & & & & & & & \end{bmatrix}$$

Adjuk meg egy standard elrendezési táblázatát. Hány ilyen különböző táblázat, azaz hány különböző dekódolás létezik?

Megoldás

E kód szavait megadják a $\mathbf{Hx} = \mathbf{0}$ egyenletrendszer megoldásai, melyek leolvashatók a mátrixról: $\mathbf{x} = u11110 + v10101$,
így $\mathcal{C} = \{00000, 11110, 10101, 01011\}$. Ezután készítsük el a táblázatot:

1. Írjuk a táblázat első sorába $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódszavait, elsőnek a $\mathbf{0}$ szót!
2. Válasszunk ki az $\mathbb{F}_q^n$ megmaradt szavai közül a legkisebb súlyú $\mathbf{e}$ szót, és írjuk a hibaoszlopba! Adjuk ezt hozzá mindegyik kódszóhoz, és a $\mathbf{c} + \mathbf{e}$ összeget írjuk $\mathbf{c}$ oszlopába!
3. Ismételjük meg az előző lépést, amíg $\mathbb{F}_q^n$ vektorai el nem fogynak!
4. Írjuk minden sor fejlécébe a sorhoz tartozó szindrómát!
5. Készítsünk a szindrómára rendezett táblázatot!

szindróma	hiba			
000	**00000**	11110	10101	01011
100	**10000**	01110	00101	11011
010	**01000**	10110	11101	00011
001	**00100**	11010	10001	01111
111	**00010**	11100	10111	01001
101	**00001**	11111	10100	01010
110	**11000**	**00110**	01101	10011
011	**01100**	**10010**	11001	00111

→

szindróma	hiba
000	00000
001	00100
010	01000
011	01100
100	10000
101	00001
110	11000
111	00010

A táblázatban félkövéren szedtük azokat a vektorokat, melyeket egy adott lépésben hibavektornak választhatunk. Így e kódnak 4 különböző dekódolása lehetséges.

A táblázattal való dekódoláshoz valójában elég az utóbbi táblázat, ugyanis egy tetszőleges $\mathbf{v}$ vektorra a táblázatból kikeressük az $\mathbf{s} = \mathbf{v}\mathbf{H}^\mathsf{T}$ szindrómához tartozó $\mathbf{e}$ hibavektort, és a $\mathbf{c} = \mathbf{v} - \mathbf{e}$ kódszóra tippelünk.

3.3 Hamming kód

A Hamming kód tulajdonságai

3.25. Példa Keressünk olyan 1-hibajavító lineáris $\mathbb{F}_q$ feletti kódot, melyre k a lehető legnagyobb, ha a javításra használható jegyek $r = n - k$ száma, azaz a redundancia rögzítve van! Mutassuk meg, hogy e kód perfekt!

Megoldás

E kód $\mathbf{H}$ ellenőrző mátrixa $r \times n$ -es, a $\mathbf{H}^\mathsf{T}$ mátrix i -edik sorvektorát jelölje $\mathbf{h}_i$. Legfeljebb 1 hiba esetén az $\mathbf{e}$ hibavektor Hamming-súlya legföljebb 1, így az $\mathbf{s} = \mathbf{e}\mathbf{H}^\mathsf{T}$ szindróma vagy a 0-vektor, vagy $\mathbf{e}_i\mathbf{h}_i$ valamely i -re, ahol $\mathbf{e}_i$ az $\mathbf{e}$ vektor egyetlen nem-0 koordinátája. Mivel e kód minimális távolsága 3, ezért a 3.20 tétel szerint $\mathbf{H}$ -nak bármely 1 és bármely 2 oszlopa lineárisan független (azaz nincs köztük a 0-vektor, és egyik sem konstansszorosa a másiknak). Rögzített $r = n - k$ mellett k maximális, ha n maximális, és n maximális értéke $(q^r - 1)/(q - 1)$. Fogalmazhatunk úgy is, hogy e feltételeknek megfelelő $\mathbf{H}$ mátrixot úgy kapunk, ha az $\mathbb{F}_q$ feletti $r - 1$ -dimenziós projektív tér pontjainak koordinátás alakját írjuk $\mathbf{H}$ oszlopaiba. Ha $\mathbf{h}_i$ első nem-0 koordinátája mindig 1, akkor az $\mathbf{s} = \mathbf{e}_i\mathbf{h}_i$ szindróma első nem-0 koordinátája épp $\mathbf{e}_i$, vagyis a szindrómából az $\mathbf{e}$ hibavektor azonnal leolvasható.

E kód perfekt, mert $n = (q^r - 1)/(q - 1)$, azaz $1 + n(q - 1) = q^{n-k}$, tehát a Hamming-korlátban egyenlőség áll.

3.26. Definíció (Hamming-kód, Szimplex kód) Vegyünk egy olyan $\mathbf{H}$ mátrixot, melynek oszlopai között $\mathbb{F}_q^r$ minden nemnulla vektorának pontosan egy nem nulla konstansszorosa szerepel. (Például ilyen az a mátrix, mely az összes olyan nemnulla oszlopvektorból áll, melynek első nemnulla koordinátája 1.) Azt a kódot, melynek a $\mathbf{H}$ mátrix az ellenőrző mátrixa, r paraméterű $\mathbb{F}_q$ feletti $\mathrm{H}_{r,q}$ Hamming-kódnak, duálisát $\mathrm{S}_{r,q}$ szimplex kódnak nevezzük. (Rögzített r és q esetén minden $\mathrm{H}_{r,q}$ kód monomiálisan ekvivalens, hasonlóképp a szimplex kódok.)

3.27. Tétel A $\mathrm{H}_{r,q}$ Hamming-kód

$$\left[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3\right]_q$$

paraméterű perfekt kód, a $\mathrm{H}_{2,q}$ kód $q > 2$ esetén $[q+1, q-1, 3]_q$ paraméterű MDS-kód.

Bizonyítás. A Hamming-kód paraméterei a definícióból adódnak, $d = 3$, mert $\mathbf{H}$-ban bármely két oszlop független, de van három összefüggő. A kód perfektségét beláttuk a 3.25 példában. Az $r = 2$ esetben a Singleton-korlát szerint $d \leqslant n - k + 1 = 3$, másrészt $d = 3$, így itt egyenlőség áll. [QED]

3.28. Példa Írjuk fel a $\mathrm{H}_{2,3}$ és $\mathrm{H}_{2,4}$ kódok ellenőrző és generátormátrixát!

Megoldás

A $q = 3$ esetben (felhasználva, hogy $-1 = 2$ és $-2 = 1$)

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & \mathbf{1} \\ 2 & 0 & 1 & & \end{array}\right] \quad G = \left[\begin{array}{cc|ccc} 1 & 0 & 2 & 2 & \mathbf{0} \\ 1 & 2 & 1 & & \end{array}\right]$$

A $q = 4$ esetben legyenek a test elemei 0, 1, α, $\alpha + 1$, ahol az $\mathbb{F}_2$ fölött irreducibilis $\alpha^2 + \alpha + 1$ polinommal végezzük a testbővítést.

$$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & \mathbf{1} \\ \alpha & \alpha+1 & 0 & 1 & & \end{array}\right] \quad G = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & \mathbf{0} \\ 1 & 0 & 1 & \alpha & \mathbf{0} & 0 \\ 1 & 1 & \alpha+1 & & & \end{array}\right]$$

3.3.1. Feladat Dekódoljuk a fogadott 1212121212121 szót, ha a kód ellenőrző mátrixa

$$\begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

A szimplex kód tulajdonságai

A szimplex kód elnevezés onnan származik, hogy - mint egy szimplex csúcsai - a kódszavak egyenlő távolságra vannak egymástól. Ez a távolság q^{r-1}. A 3.16 tétel szerint ezzel ekvivalens, hogy bármely nem nulla szó súlya q^{r-1}.

3.29. Tétel (A szimplex kód egyenlő súlyú) Egy $\mathcal{C} \in \mathrm{S}_{r,q}$ szimplex kód minden nemnulla kódszavának q^{r-1} a súlya.

Bizonyítás. Vegyünk egy tetszőleges kódszót, és válasszunk olyan $\mathbf{G}$ generátormátrixot a kódhoz, melynek első sorába ezt a kódszót írjuk, majd $\mathbf{G}$ minden oszlopát osszuk el az oszlop első nemnulla elemével. Mivel e

mátrixnak nem lehet két oszlopa összefüggő, minden oszlopa különböző.
Az i darab 0-val kezdődő, majd 1-essel folytatódó oszlopok száma legföljebb q^{r-i-1}. Így az oszlopok száma legföljebb $q^{r-1}+\cdots+q+1$, de tudjuk, hogy ez épp az oszlopok száma,
mivel $(q^r-1)/(q-1)=q^{r-1}+q^{r-2}+\cdots+q+1$. Tehát a $i=0$ darab 0-val és egy 1-gyel kezdődő oszlopok száma, azaz az első sorban lévő kódszó súlya épp q^{r-1}. [QED]

3.30. Következmény $\mathrm{S}_{r,q}$ paraméterei

$$\left[\frac{q^r-1}{q-1}, r, q^{r-1}\right]_q.$$

3.3.2. Feladat (Bináris Hamming kód dekódolása) A bináris Hamming-kód $\mathbf{H}$ ellenőrző mátrixát lexikografikusnak nevezzük, ha i -edik oszlopában az i szám bináris alakja szerepel (a legkisebb helyiértékű bittel az első sorban). Például $\mathrm{H}_{3,2}$ lexikografikus ellenőrző mátrixa (3). Hogyan egyszerűsödik a szindróma dekódolás?

3.3.3. Feladat (Kódtömörítés és hibajavítás) Tegyük fel, hogy egy 40 jeles szavakból álló ternér kódot használunk, melyben mind a 3^{40} szó előfordulhat üzenetként, és ha az üzenet továbbításában egy jelhiba történik, azt a szövegkörnyezetet felhasználva még ki tudjuk javítani. Hogyan tudnánk ezt felhasználva információveszteség nélkül tömöríteni az üzenetet?

Bővített bináris Hamming-kód

A bináris Hamming-kódból egy ellenőrző összeg hozzáadásával konstruált kódot bővített bináris Hamming-kódnak nevezzük. Jele $\mathrm{EH}_{r,2}$.

3.31. Tétel Az $\mathrm{EH}_{r,2}$ kód paraméterei $[2^r, 2^r-r-1, 4]$. Ha egy bináris Hamming-kód ellenőrző mátrixa $\mathbf{H}$, akkor az ellenőrző összeg első helyre írásával kapott bővített kód egyik ellenőrző mátrixa

$$\bar{H}=\left[\begin{array}{c|c} 1 & 11\ldots1 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right]$$

Bizonyítás. A bővítés eggyel növeli n értékét, k pedig nem változik. A d érték is nő, mivel a minimális 3-súlyú szavak mindegyikéből 4-súlyú lesz. Így e kód paraméterei

$$[2^r, 2^r - r - 1, 4].$$

Legyen $\mathbf{H}$ egy bináris Hamming-kód egy tetszőleges ellenőrző mátrixa. Mivel $\mathbf{H}$ $r \times n$-es, ezért a paraméterekből következően egy $(r+1) \times n$-es mátrix lesz a bővített kód ellenőrző mátrixa. Elég tehát megmutatnunk, hogy $\bar{H}$ sorai lineárisan függetlenek (ez nyilvánvaló), másrészt ha $\mathbf{c} = (c_1, \ldots, c_n)$ egy Hamming kódszó, azaz $\mathbf{cH} = 0$, akkor a $\bar{c} = (\sum_{i=1}^{n} c_i, c_1, \ldots, c_n)$ szóra $\bar{c}\bar{H} = 0$. Ez is nyilvánvaló, a $\bar{c}$-nak a $\bar{H}$ sorvektoraival való szorzatára vagy a $\mathbf{cH} = 0$ összefüggés vagy a $\sum_{i=1}^{n} c_i + c_1 + \cdots + c_n = 0$ összefüggés használható. [QED]

Például $\mathrm{EH}_{1,2}$, $\mathrm{EH}_{2,2}$, $\mathrm{EH}_{3,2}$, $\mathrm{EH}_{4,2}$ egy-egy ellenőrző mátrixa a Hamming-kód lexikografikus ellenőrző mátrixból konstruálva:

$$\left[\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \end{array}\right] \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

$$\left[\begin{array}{cccccccc|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] \tag{3.4}$$

Elsőrendű bináris Reed-Muller-kód

A bővített bináris $\mathrm{EH}_{m,2}$ Hamming-kód duálisát elsőrendű Reed-Muller-kódnak nevezzük, jelölése $\mathrm{RM}_{1,m}$. (Mivel itt az m paraméter már nem a redundanciát jelenti, nem az r betűt használjuk.) Kis m-ek esetei: $\mathrm{RM}_{1,1} = \mathbb{F}_2^2$, $\mathrm{RM}_{1,2} =$ a 4-hosszú paritásellenőrző kód, $\mathrm{RM}_{1,3} = EH_{3,2}$, mert önduális. Az $\mathrm{RM}_{1,5}$ kód érdekessége, hogy 1969-ben ezt használta a Mariner 6 és 7 a Marsról készült képek továbbításánál.

A (4) mátrixai tehát generátormátrixai e kódoknak. Ezek rekurzív tulajdonsága leolvasható e mátrixokról, ha másként blokkosítjuk:

$$\left[\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \end{array}\right] \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \tag{3.16}$$

$$\left[\begin{array}{cccccccc|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

A rekurzív összefüggés tehát:

$$H_0 = [1], \quad H_m = \left[\begin{array}{c|c} H_{m-1} & H_{m-1} \\ \hline 00\ldots0 & 11\ldots1 \end{array}\right]$$

3.32. Tétel Az $\mathrm{RM}_{1,m}$ kód bináris $[2^m, m+1, 2^{m-1}]_2$-kód.

Bizonyítás. Az $n = 2^m$, $k = m+1$ világos a definícióból. Az $\mathrm{RM}_{1,m}$ kód generátormátrixának konstrukciójából következik, hogy az $\mathrm{S}_{m,2}$ kód kódszavai egy vezető 0-val, valamint ezek komplementerei (az $111\ldots1$ vektorral való összeg miatt) mind kódszavak, ezzel viszont meg is kaptuk mind a 2^{m+1} kódszót. E szavak súlya a $000\ldots0$ és az $111\ldots1$ kódszavakat kivéve 2^{m-1}. [QED]

Az $\mathrm{RM}_{1,m}$ kód tehát egyenlő súlyú (két vektort kivéve), illetve egyenlő súlyú (ekvidisztáns), hisz - a komplementer vektorpárokat kivéve - bármely két szó távolsága 2^{m-1}.

Hadamard dekódolás

Végezzük el az $\mathrm{RM}_{1,m}$ kód szavain az alábbi $\mathbb{F}_2 \to \mathbb{R}$ jelcserét: $0 \mapsto 1$, $1 \mapsto -1$. A $\mathbf{c}$ kódszó képét jelölje $\mathbf{c}^{\pm} \in \{1,-1\}^n$, az így kapott kódot $\mathrm{RM}^{\pm}_{1,m}$.

3.33. Lemma $\mathrm{RM}^{\pm}_{1,m}$ kódszavaira igazak az alábbiak:

1. Ha $\mathbf{c}^{\pm} \in \mathrm{RM}^{\pm}_{1,m}$, akkor $-c^{\pm} \in \mathrm{RM}^{\pm}_{1,m}$, így a kód 2^{m+1} szava indexelhető úgy, hogy $c^{\pm}_i = -c^{\pm}_j$, ha $|j-i| = 2^m$.
2. Ha $c^{\pm}_i, c^{\pm}_j \in \mathrm{RM}^{\pm}_{1,m}$, akkor

$$c_i^{\pm} \cdot c_j^{\pm} = \begin{cases} 2^m & \text{ha } c_i^{\pm} = c_j^{\pm} \\ -2^m & \text{ha } c_i^{\pm} = -c_j^{\pm} \\ 0 & \text{ha } c_i^{\pm} \neq \pm c_j^{\pm}. \end{cases}$$

Bizonyítás. A csupa-1 kódszóra $(1+c)^{\pm} = -c^{\pm}$, ami igazolja az első állítást.

Ha $x^{\pm}, y^{\pm} \in \{1,-1\}^n$ két tetszőleges ± 1-vektor,
akkor $x^{\pm} \cdot y^{\pm} = n - 2\,\mathrm{d_H}(x^{\pm}, y^{\pm})$, ugyanis a skaláris szorzat megegyezik azon koordináták száma, ahol a két kód megegyezik ($n - \mathrm{d_H}(x^{\pm}, y^{\pm})$), mínusz azon koordináták száma, ahol különböznek ($\mathrm{d_H}(x^{\pm}, y^{\pm})$). Az $x^{\pm} = c_i^{\pm}$, $y^{\pm} = c_j^{\pm}$, $c_i^{\pm} = c_j^{\pm}$, $c_i^{\pm} = -c_j^{\pm}$ esetben $\mathrm{d_H}(x^{\pm}, y^{\pm}) = n/2$, ami bizonyítja a második állítást. [QED]

A lemma szerinti indexeléssel készítsünk egy M mátrixot az $\mathrm{RM}_{1,m}^{\pm}$ kód első 2^m szavából. Például az $\mathrm{RM}_{1,2}^{\pm}$ kódnál a (16)-beli generátormátrixából kiindulva, és az 1-vektor helyett a 0-vektort használva:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \Longrightarrow$$
$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \Longrightarrow M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Mivel így egyik kódszó ellentettje sem szerepel e mátrix soraiban, ezért fennáll az $MM^{\mathsf{T}} = nI$ összefüggés.

Azokat az $n \times n$-es ± 1-mátrixokat, melyek eleget tesznek az

$$MM^{\mathsf{T}} = nI_n$$

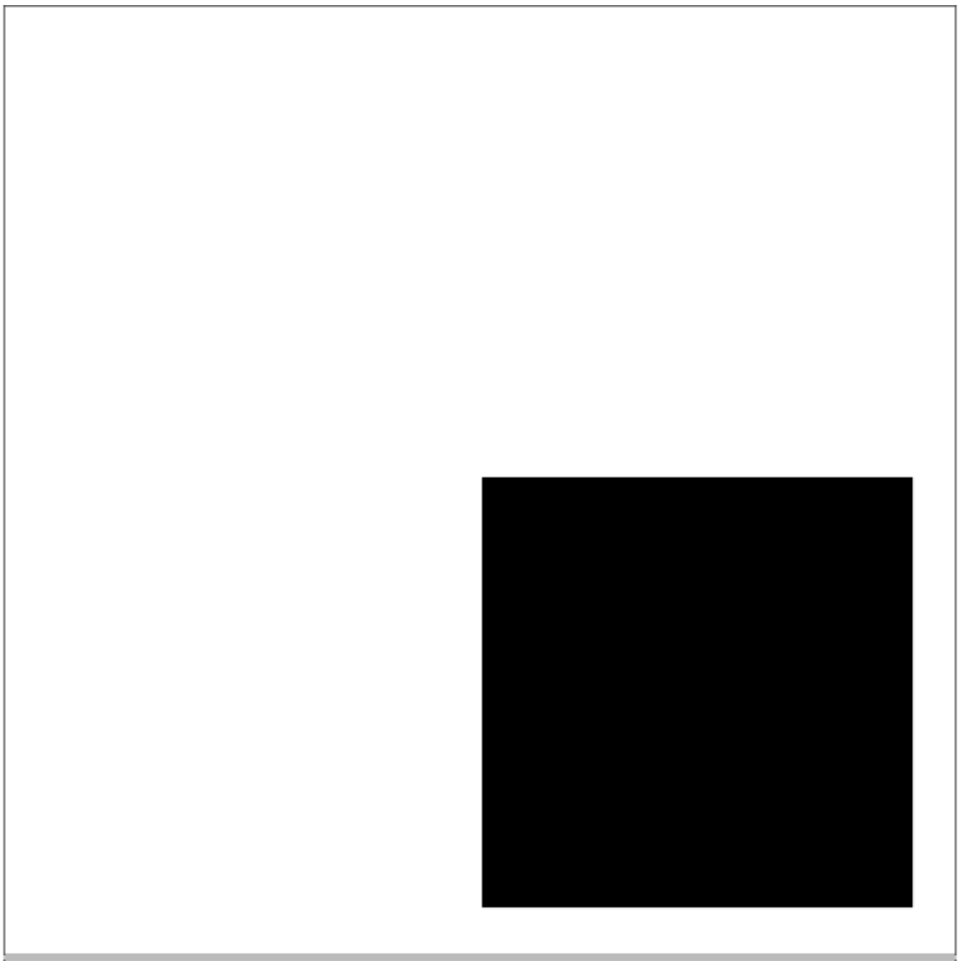
összefüggésnek, n-edrendű Hadamard-mátrixoknak nevezzük.

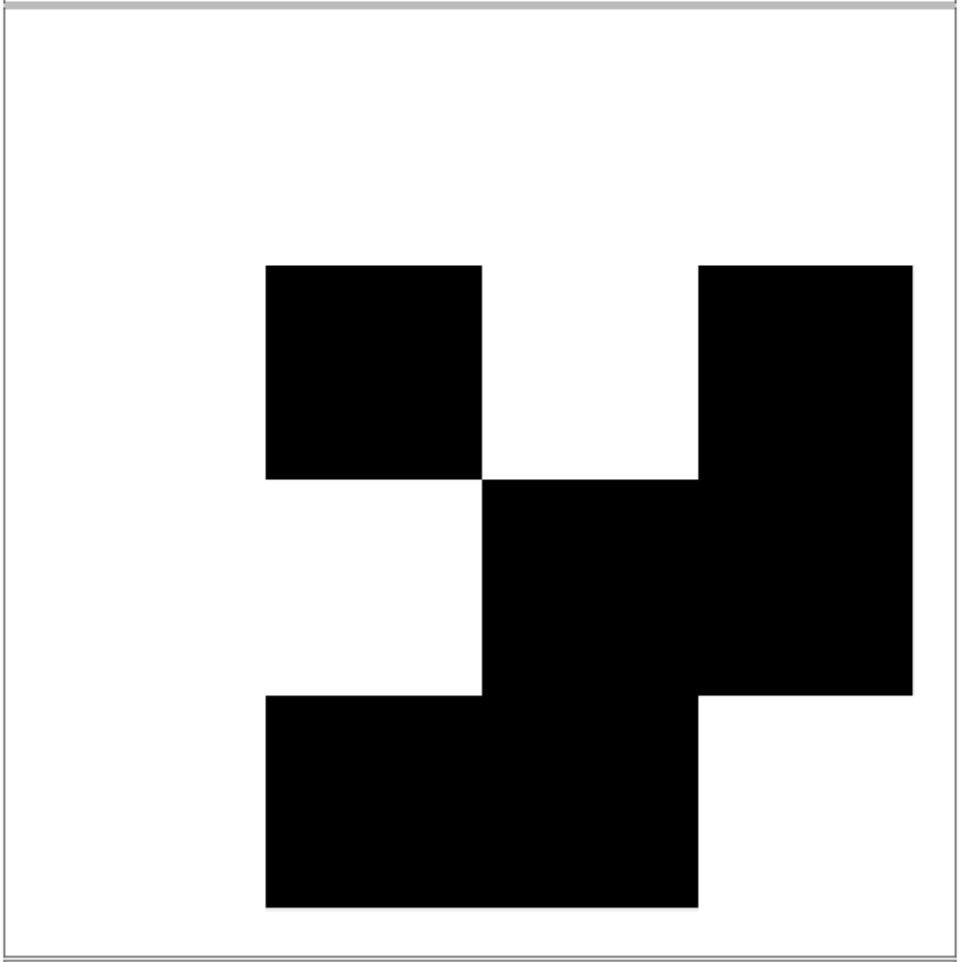
3.3.4. Feladat Ha M_n egy n-edrendű Hadamard mátrixot jelöl, akkor

1. $n = 1$, $n = 2$ vagy $n \equiv 0 \pmod 4$.
2. $M_n \otimes M_m$ egy nm-rendű Hadamard-mátrix ($\otimes$ a Kronecker-szorzatot jelöli).

3. Ha $M_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, akkor a rekurzív $M_{2^n} = M_2 \otimes M_{2^{n-1}}$ összefüggés Hadamard-mátrixokat ad (ld. a 30. ábrát).

Az mindmáig nyitott kérdés, hogy milyen n -ekre létezik n -edrendű Hadamard-mátrix. Sejtés, hogy minden 4-gyel osztható értékre létezik. 1000 alatti eldöntetlen értékek: 668, 716, 892.





Mivel $x^{\pm} \cdot y^{\pm} = n - 2\,\mathrm{d_H}(x^{\pm}, y^{\pm})$, ezért egy fogadott x szó ahhoz az kódszóhoz van legközelebb, mellyel vett skaláris szorzata maximális abszolút értékű. A Hadamard-dekódolás az az eljárás, melyben a fogadott szóhoz az mátrixnak azt a sorát választjuk, amellyel vett skaláris szorzata maximális abszolút értékű, azaz amely az legnagyobb abszolút értékű koordinátájához tartozik.

Például legyen a fogadott vektor $x = (-1, -1, -1, 1, 1, 1, -1, -1)$. Ekkor az $M_8 x^{\mathsf{T}}$ legnagyobb abszolút értékű koordinátája a 7-dik, és negatív előjelű:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} -2 \\ -2 \\ 2 \\ 2 \\ -2 \\ -2 \\ -6 \\ 2 \end{bmatrix}$$

Ezért az M 7-dik sorvektorának -1-szerese lesz x Hadamard-dekódoltja, azaz a

$$c_{7+8} = c_{15} = (-1, -1, 1, 1, 1, 1, -1, -1)$$

kódszó. E módszer lágy dekódolásnál is ugyanúgy használható (azaz amikor nem a dekóder által meghatározott jelet, hanem a demodulátor által nyújtott, bizonytalanabb értéket kapjuk vissza). Például ha az $y = (-1.3, 0.1, 0, 0.6, 1.6, -1.1, 0.2, 0.1)$ vektort mérjük a csatornán, az $My^{\mathsf{T}} = (0.2, 0.8, -1.6, 1.8, -1.4, -4.8, -2.0, -3.4)$ alapján a 6-dik sor ellentettje a legvalószínűbb üzenet.

3.4 Titokmegosztás

A titokmegosztás egy kriptográfiai protokoll, melyben egy titkot úgy osztanak fel több résztvevő közt, hogy azt csak a résztvevők bizonyos előre megadott koalíciói - azaz a felhatalmazottak - legyenek képesek rekonstruálni a résztitkaikból.

Legyen $P = \{ p_1, p_2, \ldots, p_n \}$ egy titokmegosztási séma n résztvevőjének halmaza. E sémában a P egy A részhalmazát felhatalmazottnak, vagy felhatalmazott koalíciónak nevezzük, ha az A -beli résztvevők közösen, résztitkaikból hozzájuthatnak a titokhoz. A felhatalmazottak halmazát jelölje Γ, melyet a séma elérési struktúrájának nevezünk.

Valós kikötés, hogy ha A felhatalmazott, akkor minden $B \supset A$ halmaz is az legyen. Az e feltételt kielégítő halmazrendszereket felszállónak nevezzük, azaz Γ felszálló, ha $A \in \Gamma$ és $A \subset B$, akkor $B \in \Gamma$. A kérdés az lesz, hogy ha adva van résztvevők egy tetszőleges P halmaza, és azon részhalmazok egy felszálló Γ halmaza, akkor hogyan valósítható meg a titok résztitkokra osztása, a résztvevők közti szétosztása, hogy P-nek csak a Γ-ba tartozó elemei legyenek képesek hozzájutni a titokhoz.

A titokmegosztás fontos szerephez jut a biztonságos közös számításokban, ahol egy többváltozós függvényt kell a résztvevőknek kiértékelni, melynek minden argumentumát más-más résztvevő tudja, akik azonban e titkukat nem akarják egyik más résztvevő számára sem kiadni. (Például ilyen közös számítás minden titkos választás.)

A (t, n)-küszöb séma

Első példaként a gyakorlatban legtöbbet használt esetet vizsgáljuk, az ún. (t, n)-küszöb sémát, melyben felhatalmazott minden koalíció, melynek létszáma elérii a t küszöbértéket, azaz $\Gamma = \{ A \subseteq P \mid |A| \geqslant t \}$. Ilyen eset fordul elő, ha egy bank széfjének kinyitásához a bank vezetéséből legalább 3 tag hozzájárulása szükséges. Történelmi példa: a szovjet atomfegyverek megindítását olyan rendszer biztosította, melyben a három legfőbb vezető közül legalább kettő egyetértésére volt szükség.

Perfekt titokmegosztási sémákat keresünk, ahol a résztvevők fel nem hatalmazott koalíciói semmivel sem tudhatnak meg a titokról többet, mint a protokoll bármely külső megfigyelője.

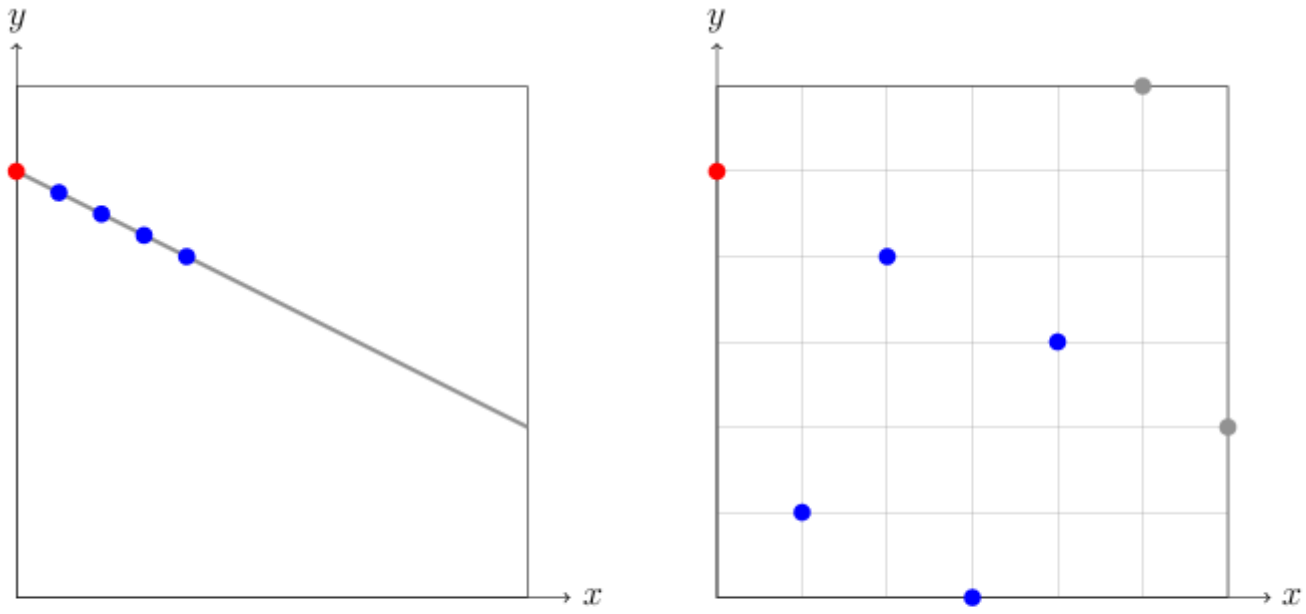
Például ha a titok a SECRET szó, és a három résztvevő rendre a SE****, **CR**, ****ET szavakat kapja, egy $(3, 3)$-küszöb sémát kapunk, hisz csak mindhárom résztvevő együtt képes a titkot meghatározni. Világos azonban, hogy ez a titokmegosztás nem perfekt: míg a lehetséges titkok száma 26^6, addig minden résztvevő számára a titok csak 26^4 lehetőséget, míg bármely kettőjük számára már csak 26^2 lehetőséget rejt.

A perfekt titokmegosztás gondolatára Shamir és Blakley lelt 1979-ben egymástól függetlenül. Shamir az interpolációs polinomokra építette ötletét. Legyen az a_0 titok az $\mathbb{F}_q$ véges test egy véletlen eleme. A titok megosztója - ami lehet egy komputer program is - választ egy véletlen $t-1$-edfokú $\mathbb{F}_q$ fölötti polinomot, melyre $f(0) = a_0$. Ennek alakja tehát $f(x) = a_{t-1}x^{t-1} + \cdots + a_2x^2 + a_1x + a_0$, ahol $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$ tetszőleges (véletlenül választott) elemek. A résztvevők résztitka e függvény egy-egy helyettesítési értéke, nevezetesen a p_i résztvevő az $f(i)$ értéket kapja ($\mathbb{F}_q$ elemeit a $0, 1, \ldots, q-1$ számokkal jelöljük). Ha

tetszőleges t résztvevő összeáll - indexeik halmazát jelölje T -, akkor meg tudják határozni a polinom együtthatóit, és abból a titkot, ugyanis a

$$a_{t-1}i^{t-1} + \cdots + a_2 i^2 + a_1 i + a_0 = f(i), \quad i \in T$$

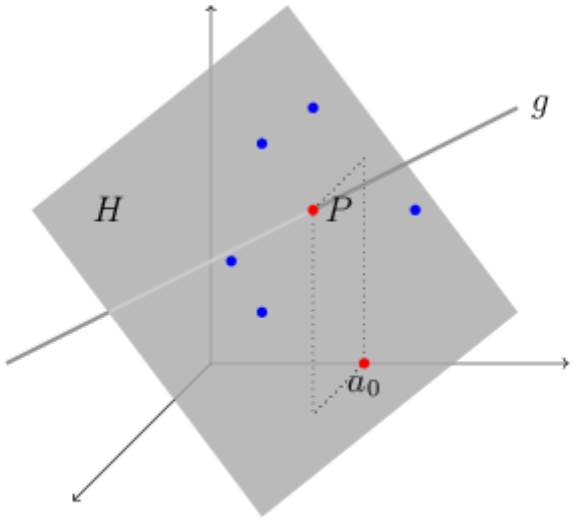
egy t egyenletből álló t -ismeretlenes egyenletrendszer, melynek Vandermonde-típusú az együtthatómátrixa, így egyértelműen megoldható. Másrészt az is világos, hogy kevesebb, mint t résztvevő csak egy legföljebb $t-1$ egyenletből álló rendszert írhat föl, ami megoldható lesz bármely a_0 megválasztása mellett, vagyis semmit nem tudnak a titokról. A 31 ábra egy $(2,4)$-küszöb sémát mutat, ahol a résztitkok egy egyenesen vannak (ez az elsőfokú polinom grafikonja), amelynek egyenletét bármely két résztvevő föl tudja írni, és abból meghatározni az egyenesnek az y -tengellyel való metszéspontját.



31. ábra. Egy $(2,4)$-küszöb séma sematikus ábrája (bal ábra). Persze véges test fölötti koordinátarendszerben az egyenes nem feltétlenül néz ki az euklideszi síkon is egyenesnek. Például a jobb oldali ábra az $\mathbb{F}_7$ fölötti $f(x) = 3x + 5$ egyenletű egyenes pontjait mutatja, külön színezve a titkot pirossal és a résztitkokat kékkel.

Blakley konstrukciójában a t -dimenziós $\mathcal{V} = \mathbb{F}_q^t$ tér egy véletlen $P = (a_0, \ldots, a_{t-1}$ pontjának első koordinátája a titok. Publikálva van egy ezen a ponton átmenő g egyenes, mely nem merőleges az $\mathbf{e}_1 = (1, 0, \ldots, 0)$ vektorra, így pontjainak első koordinátái végigfutnak $\mathbb{F}_q$ elemein. A résztvevők megkapják egy P -n átmenő, de $\mathbf{e}_1$-re nem merőleges és g -t nem tartalmazó H (affin) hipersík általános helyzetű pontjait. Ez azt jelenti, hogy bármely t résztvevő egyértelműen föl tudja írni H egyenletét, így a g -vel való metszéspontját is. A 32 ábra egy $(3,5)$-küszöb sémát mutat, ahol a

résztitkok a 3-dimenziós térben egy síkon vannak, amelynek egyenletét bármely három résztvevő föl tudja írni, és abból meghatározni a síknak a g egyenessel való metszéspontját.



32. ábra. Egy $(3, 5)$-küszöb séma sematikus ábrája. A P pont és annak első koordinátáját megadó pont az x tengelyen pirossal, a résztitkok kékkel vannak jelölve.

Ideális sémák

Sok titokmegosztási séma született, fontossá vált azonban az is, hogy információelméleti szempontból is hatékonyak legyenek, azaz a résztitok ne legyen sokkal hosszabb, mint maga a titok, ideális esetben ugyanabból a halmazból való legyen. Az ilyen sémákat ideálisnak nevezzük. Shamir konstrukciója ideálisnak tekinthető, ha a résztvevők sorszáma publikálva van, vagyis a titoknak nem része i , csak $f(i)$. Hasonlóan ideálissá tehető Blakley konstrukciója is, ha g mellett minden résztvevő pontjának koordinátái is publikálva vannak, kivéve az első koordinátát!

Egy Brickelltől származó ötletet ismertetünk, mellyel ideális, perfekt titokmegosztási séma konstruálható.

A titkot kiosztó választ egy tetszőleges $\mathbf{a} = (a_0, a_1, \ldots, a_t) \in \mathbb{F}_q^{t+1}$ vektort, melynek első koordinátája, az $a_0 \in \mathbb{F}_q$ elem lesz a titok. A p_i résztvevőnek ad egy $\mathbf{v}_i \in \mathbb{F}_q^t$ vektort, és ezeket nyilvánosságra hozza. A résztitok az $s_i = \mathbf{v}_i \cdot \mathbf{a} \in \mathbb{F}_q$ elem lesz.

3.34. Állítás Jelölje $T \subseteq P$ a résztvevők egy halmazát. A T -be tartozó résztvevők pontosan akkor tudják meghatározni a_0-t, ha az $\mathbf{e}_1 = (1, 0, \ldots, 0)$ vektor benne van a T -beli résztvevők vektorai által kifeszített altérben. Ha $\mathbf{e}_1$ nincs ebben az altérben, a T -beli résztvevők semmit nem tudnak meg a titokról.

Bizonyítás. Legyen $\mathbf{V}$ az a mátrix, melynek sorai a T -beliek vektorai, és $\mathbf{s}$ az a vektor, melynek koordinátái a T -beliek résztitkai. Tegyük fel, hogy $\mathbf{e}_1$ benne van $\mathbf{V}$ sorterében. Ekkor létezik olyan $\mathbf{w}$ vektor, hogy $\mathbf{w}^\mathsf{T}\mathbf{V} = \mathbf{e}_1^\mathsf{T}$, így $\mathbf{w}^\mathsf{T}\mathbf{V}\mathbf{a} = a_0$. Mivel a konstrukció szerint $\mathbf{V}\mathbf{a} = \mathbf{s}$, ezért $\mathbf{w}^\mathsf{T}\mathbf{s} = a_0$, hisz $\mathbf{w}$ a T -beli résztvevők által meghatározható.

Tegyük fel, hogy $\mathbf{e}_1$ nincs benne $\mathbf{V}$ sorterében. Jelölje $\mathbf{V}$ oszlopvektorait $\mathbf{u}_0$, $\mathbf{u}_1$,..., $\mathbf{u}_t$. Ha $\mathbf{u}_0 \notin \operatorname{span}(\mathbf{u}_1, \ldots, \mathbf{u}_t)$, akkor van olyan $\mathbf{d}$ vektor, hogy $\mathbf{d} \cdot \mathbf{u}_i = 0$, ha $i = 1, 2, \ldots, t$, és $\mathbf{d} \cdot \mathbf{u}_0 = 1$. Eszerint $\mathbf{d}^\mathsf{T}\mathbf{V} = \mathbf{e}_1$, ami ellentmond feltevésünknek. Ezért $\mathbf{u}_0 \in \operatorname{span}(\mathbf{u}_1, \ldots, \mathbf{u}_t)$, így van olyan $\mathbf{w}$ vektor, hogy $\mathbf{V}\mathbf{w} = \mathbf{0}$, de $w_0 \neq 0$. Az ugyan igaz, hogy $\mathbf{s} = \mathbf{V}\mathbf{a}$, de tetszőleges $c \in \mathbb{F}_q$ konstansra $\mathbf{s} = \mathbf{V}\mathbf{a} = \mathbf{V}(\mathbf{a} + c\mathbf{w})$ is teljesül. Így bármely c_0-hoz található olyan $\mathbf{c} = (c_0, c_1 \ldots, c_t)$ vektor, hogy $\mathbf{s} = \mathbf{V}\mathbf{c}$. Így a T -beli résztvevők semmit nem tudhatnak a_0-ról. [QED]

Megmutatható, hogy minden többszintű (multilevel) séma e konstrukcióval ideális, perfekt módon megvalósítható, melynek részletezésétől eltekintünk. Többszintű a titokmegosztási séma, ha a résztvevők P halmaza diszjunkt részhalmazokra osztható úgy, hogy minden részhalmazhoz tartozik egy t szám, mely megadja, hogy közülük csak a legalább t -elemű koalíciók a felhatalmazottak. Például 2-szintű séma, ha a bankigazgatók közül bármely kettő, a bank osztályvezetői közül bármely három egyetértése szükséges a széf kinyitásához. Természetesen két osztályvezető és egy igazgatósági tag is kinyithatja a széfet.

Egy egyszerű példát mutatunk e séma alkalmazására.

3.35. Állítás Tegyük fel, hogy P diszjunkt részekre van osztva, azaz $P = P_1 \cup \cdots \cup P_k$, ahol $P_i \cap P_j = \emptyset$, ha $i \neq j$. Ekkor létezik olyan ideális perfekt titokmegosztási séma, melyben két résztvevő pontosan akkor felhatalmazott, ha különböző partícióba tartoznak.

Bizonyítás. Legyenek $x_1, x_2, \ldots, x_k \in \mathbb{F}_q$ különböző elemek, és legyen a $p_i \in P_j$ résztvevő publikált vektora $\mathbf{v}_i = (x_j, 1) \in \mathbb{F}_q^2$. Azonnal látszik, hogy ez kielégíti a 3.34 állítás feltételeit. [QED]

Tetszőleges elérési struktúra megvalósítható

Nem minden elérési struktúra valósítható meg ideális sémával, de perfekt módon igen.

3.36. Tétel Ha Γ az n résztvevő P halmazának részhalmazaiból álló felszálló halmazrendszer, akkor van olyan perfekt titokmegosztási séma, melyben Γ elemei a felhatalmazottak.

Teljes bizonyítást nem adunk, de ismertetjük az előző pontbelire emlékeztető lineáris algebrai alapötletet, ahonnan már könnyű a befejezés.

3.37. Lemma Ha Γ egy elérési struktúra a $P = \{ p_1, p_2, \ldots, p_n \}$ halmazon, akkor tetszőleges $\mathbb{F}_q$ test felett létezik olyan $\mathcal{V}$ vektortér, és altereinek egy olyan $\{ \mathcal{V}_0, \mathcal{V}_1, \ldots, \mathcal{V}_n \}$ rendszere, hogy $\mathcal{V}_0$ pontosan akkor altere a $\mathcal{W} = \mathrm{span}(\mathcal{V}_{i_1}, \mathcal{V}_{i_2}, \ldots, \mathcal{V}_{i_m})$ altérnek, ha $\{ p_{i_1}, p_{i_2}, \ldots, p_{i_m} \} \in \Gamma$, egyébként $\mathcal{V}_0 \cap \mathcal{W} = \{\mathbf{0}\}$.

Bizonyítás. Legyen $\Gamma^+ = \{ U_1, U_2, \ldots, U_u \}$ az összes maximális fel nem hatalmazottak halmaza, azaz ha $U \in \Gamma^+$, akkor $U \notin \Gamma$, de bármely $A \supset U$ halmazra $A \in \Gamma$. Legyen $\mathcal{V} = \mathbb{F}_q^u$, $\mathcal{V}_0 = \mathrm{span}((1, 1, \ldots, 1))$, $\mathcal{V}_j = \mathrm{span}(\{ \mathbf{e}_i \mid p_j \notin U_i \})$. [QED]

A bizonyítás szemléltetésére lássunk egy példát.

3.38. Példa Legyen $n = 4$, $\Gamma_0 = \{ \{p_1, p_2, p_3\}, \{p_1, p_4\}, \{p_2, p_4\} \}$, és legyen Γ a $qGamma_0$ által generált felszálló halmazrendszer. Ekkor

$$\Gamma^+ = \{ \{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}, \{p_3, p_4\} \},$$

továbbá $\mathcal{V}_0 = \mathrm{span}\,((1, 1, 1, 1))$, $\mathcal{V}_1 = \mathrm{span}(\mathbf{e}_3, \mathbf{e}_4)$, $\mathcal{V}_2 = \mathrm{span}(\mathbf{e}_2, \mathbf{e}_4)$, $\mathcal{V}_3 = \mathrm{span}(\mathbf{e}_1)$, $\mathcal{V}_4 = \mathrm{span}(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$. Könnyen látható, hogy például

$$\mathcal{V}_0 \leqslant \mathrm{span}(\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3), \text{ de } \mathcal{V}_0 \cap \mathrm{span}(\mathcal{V}_1, \mathcal{V}_3) = \{\mathbf{0}\},$$

megfelelően annak, hogy $\{p_1, p_2, p_3\} \in \Gamma$, de $\{p_1, p_3\} \notin \Gamma$.

A séma az altérkonstrukcióból a következő. Minden résztvevő megkapja az altérkonstrukciónak megfelelő alterének bázisvektoraiból álló $\mathbf{P}_i$ mátrixot. E mátrixokat a titokgazda publikálja, majd választ egy véletlen $\mathbf{h}$ vektort, és a titok az $s = [1\ 1\ \ldots\ 1]\mathbf{h}$ skalár lesz, míg p_i résztitka a $\mathbf{P}_i\mathbf{h}$ vektor. (Megjegyezzük, az előző lemmában csak a standard alapvektorokat használtuk, és a titkot az $(1, 1, \ldots, 1)$ vektorhoz rendeltük, de mindez működik az alterek más módon konstruált, és tetszőleges bázisával megadott rendszerére is.) Az előző példából származó séma a következő:

3.39. Példa Legyen $q = 3$, a véletlen vektor legyen $\mathbf{h} = (1, 0, 2, 1)$, így a titok $(1, 1, 1, 1) \cdot (1, 0, 2, 1) = 1$. Az alterek nyilvános mátrixai és a belőlük számolt résztitkok a következők:

$$\begin{aligned}
&\mathbf{P}_1 = 00100001, && \mathbf{s}_1 = \mathbf{P}_1\mathbf{h} = 21,\\
&\mathbf{P}_2 = 01000001, && \mathbf{s}_2 = \mathbf{P}_2\mathbf{h} = 01,\\
&\mathbf{P}_3 = 1000, && \mathbf{s}_3 = \mathbf{P}_3\mathbf{h} = [1]\\
&\mathbf{P}_4 = 1000; 0100; 0010;, && \mathbf{s}_4 = \mathbf{P}_4\mathbf{h} = 102.
\end{aligned}$$

Világos, hogy $\mathbf{h}$ minden koordinátáját és így az s titkot csak a felhatalmazott koalícióknak sikerülhet megfejteni.

4 Műszaki és természettudományos alkalmazások

4.1 Lineáris egyenletrendszerekkel leírható problémák

A különféle lineáris egyenletrendszerekkel megoldható alkalmazási problémák száma rendkívül sok, ezért csak arra vállalkozunk, hogy két egészen különböző - de fontos - területről választunk egy-egy példát.

Kémiai reakciók egyensúlyi egyenlete

Egy zárt rendszerben végbemenő kémiai reakciók során a rendszerben lévő kémiai alkotóelemek mennyisége nem változik. Így felírható mindig egy olyan egyenlet - ezt nevezzük reakcióegyenletnek, melynek bal oldalán a reakciók elején jelen lévő vegyületek, jobb oldalán az eredményül kapott vegyületek szerepelnek olyan együtthatókkal megszorozva, melyek a vegyületek mennyiségét fejezik ki.

4.1. Példa (reakcióegyenlet) A hidrogén-peroxid ($\mathrm{H_2O_2}$) bomlékony anyag, mely vízre ($\mathrm{H_2O}$) és oxigénre ($\mathrm{O_2}$) bomlik. Keressük meg azokat a legkisebb x_1, x_2 és x_3 pozitív egész számokat, melyek leírják a reakcióban résztvevő vegyületek mennyiségét, azaz keressük az $x_1\mathrm{H_2O_2} = x_2\mathrm{H_2O} + x_3\mathrm{O_2}$ egyenletben szereplő ismeretlenek legkisebb pozitív egész megoldásait.

Megoldás

A hidrogén (H) és oxigén (O) atomok mennyisége a reakcióegyenlet mindkét oldalán megegyezik, ami két egyenletet ad:

$$\begin{aligned}
\mathrm{H}: &\quad 2x_1 = 2x_2\\
\mathrm{O}: &\quad 2x_1 = x_2 + 2x_3.
\end{aligned}$$

Egy oldalra rendezzük a változókat:

$$\begin{aligned}
\mathrm{H}: &\quad 2x_1 - 2x_2 = 0\\
\mathrm{O}: &\quad 2x_1 - x_2 - 2x_3 = 0,
\end{aligned}$$

majd megoldjuk e homogén lineáris egyenletrendszert:

$$\begin{bmatrix} 2 & -2 & 0 \\ 2 & 1 & -2 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -2 \end{bmatrix}.$$

Így az $x_3 = s$ választással a megoldás $x_2 = 2s$, $x_1 = 2s$, azaz $(x_1, x_2, x_3) = (2s, 2s, s)$. A legkisebb pozitív egész megoldást $s = 1$ adja: $2\mathrm{H_2O_2} = 2\mathrm{H_2O} + \mathrm{O_2}$.

Egy kémiai reakcióegyenletének az anyagmennyiségre vonatkozó megmaradási elv mellett az elektromos töltés megmaradását is ki kell fejeznie. Ha a reakcióegyenletben töltések is szerepelnek, ezekre is fölírható egy egyenlet.

A fenti egyenletrendszer együtthatómátrixához hasonlóan szokás kémiai reakció(k) formulamátrixát vagy atommátrixát megkonstruálni. Ebben a sorok a kémiai elemeknek, illetve egy sor a töltéseknek, az oszlopok a vegyületeknek felelnek meg. Pl. az előző egyenletben szereplő vegyületekhez tartozó formulamátrix:

	$\mathrm{H_2O_2}$	$\mathrm{H_2O}$	$\mathrm{O_2}$
H	2	2	0
O	2	1	2

Ha több reakció is lezajlik egy folyamatban, a folyamatban szereplő összes vegyületre fölírható egy atommátrix. Ennek rangja hozzásegít a folyamatban játszódó független reakciók számának meghatározásához. A formulamátrix arra is alkalmas, hogy segítségével reakcióegyenleteket írjunk fel.

Ha már ismerjük egy folyamatban lejátszódó reakciókat, a köztük lévő lineáris kapcsolatot az ún. sztöchiometriai mátrix segítségével írhatjuk le. Ennek oszlopai egy reakciókhoz, sorai pedig a reakciókban szereplő vegyületekhez tartoznak. Az i -edik sorban, j -edik oszlopban álló szám a j -edik reakció 0-ra rendezett egyenletében az i -edik vegyület mennyisége. A szokás az, hogy az egyenlet bal oldalán szereplő együtthatókatat szorozzuk -1-gyel.[9]

4.2. Példa (Formulamátrix, sztöchiometriai mátrix) A szénsav disszociációját két egyenlet írja le.

$$\begin{aligned} &(1)\quad \mathrm{H_2CO_3} = \mathrm{HCO_3^-} + \mathrm{H^+} \\ &(2)\quad \mathrm{HCO_3^-} = \mathrm{CO_3^{2-}} + \mathrm{H^+} \end{aligned}$$

Írjuk fel e reakció formula mátrixát és sztöchiometriai mátrixát! Határozzuk meg mindkettő rangját!

Megoldás

A formulamátrix

	H_2CO_3	HCO_3^-	H^+	CO_3^{2-}
H :	2	1	1	0
C :	1	1	0	1
O :	3	3	0	3
q :	0	−1	1	−2

Ennek utolsó sora a töltések számát mutatja, melyet q-val jelöltünk. Redukált lépcsős alakja:

$$\begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

tehát a rangja 2. A sztöchiometriai mátrix a fejlécekkel:

	(1)	(2)
H_2CO_3	−1	0
HCO_3^-	1	−1
H^+	1	1
CO_3^{2-}	0	1

redukált lépcsős alakja $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Rangja ennek is 2.

4.3. Példa (Bruttó reakció) Egy több reakcióból álló folyamatban az alábbi bruttó reakciót mérték:

$$5BrO_2^- + 2H^+ = Br_2 + 3BrO_3^- + H_2O$$

E reakcióban a következő elemi reakciók mehetnek végbe:

$$\begin{aligned}
&(1)\quad BrO_2^- + HBrO_2 = BrO_3^- + BrOH \\
&(2)\quad BrO_2^- + H^+ = HBrO_2 \\
&(3)\quad BrO_2^- + H_2O_2 = BrO_3^- + H_2O \\
&(4)\quad 2BrOH = Br_2 + H_2O_2
\end{aligned}$$

Melyik elemi reakciónak hányszor kell végbemennie a bruttó reakcióban?

Megoldás

Írjuk fel az elemi reakciók sztöchometriai mátrixát először fejlécekkel, majd anélkül. Jelölje e mátrixot $\mathbf{A}$:

$$\begin{array}{cccccc} & (1) & (2) & (3) & (4) \\ \mathrm{BrO_2^-} & -1 & -1 & -1 & 0 \\ \mathrm{H^+} & 0 & -1 & 0 & 0 \\ \mathrm{Br_2} & 0 & 0 & 0 & 1 \\ \mathrm{BrO_3^-} & 1 & 0 & 1 & 0 \\ \mathrm{H_2O} & 0 & 0 & 1 & 0 \\ \mathrm{HBrO_2} & -1 & 1 & 0 & 0 \\ \mathrm{BrOH} & 1 & 0 & 0 & -2 \\ \mathrm{H_2O_2} & 0 & 0 & -1 & 1 \end{array} \qquad \mathbf{A} = \begin{bmatrix} -1 & -1 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & -2 \\ 0 & 0 & -1 & 1 \end{bmatrix}$$

Majd írjuk fel a bruttó reakcióra ugyanezeket. Az oszlopmátrixot, mint vektort jelölje $\mathbf{b}$:

$$\begin{array}{cc} & \text{bruttó} \\ \mathrm{BrO_2^-} & -5 \\ \mathrm{H^+} & -2 \\ \mathrm{Br_2} & 1 \\ \mathrm{BrO_3^-} & 3 \\ \mathrm{H_2O} & 1 \\ \mathrm{HBrO_2} & 0 \\ \mathrm{BrOH} & 0 \\ \mathrm{H_2O_2} & 0 \end{array} \qquad \mathbf{b} = \begin{bmatrix} -5 \\ -2 \\ 1 \\ 3 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

A feladat tehát az, hogy állítsuk elő ez utóbbi oszlopvektort az előbbi mátrix oszlopainak lineáris kombinációjaként! Ez pontosan azt jelenti, hogy oldjuk meg az $\mathbf{A}$ együtthatójú és $\mathbf{b}$ jobb oldalú egyenletrendszert. A bővített mátrix redukált lépcsős alakja:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

ahonnan a megoldás $(2, 2, 1, 1)$, azaz $2\mathbf{a}_1 + 2\mathbf{a}_2 + \mathbf{a}_3 + \mathbf{a}_4 = \mathbf{b}$. A feladat nyelvén: az első és második reakció kétszer, a harmadik és negyedik reakció egyszer megy végbe a bruttó reakció során.

Globális navigációs műholdrendszerek (GNSS)

A GNSS (Global Navigation Satellite Systems, magyarul globális navigációs műholdrendszerek) kifejezés alatt elsősorban az USA Védelmi Minisztériuma által kifejlesztett és üzemeltetett GPS rendszert (Global Positioning System - magyarul globális helymeghatározó rendszer) az orosz GLONASS (Global Navigation Satellite System) rendszert, és az Európai Unió (EU) és az Európai Űrügynökség (ESA) Galileo rendszerét értjük, de ide sorolandók mindazok a műholdas vagy földi kiegészítő rendszerek is, amelyek a műholdas navigációt valamilyen módon támogatják.

Ezek matematikájának áttekintésére nem vállalkozhatunk, pusztán csak egy leegyszerűsített modellben megmutatjuk a helymeghatározás egy Bancroft-tól származó lineáris algebrai módszerét.

Geocentrikus Descartes-féle koordinátákat használunk, melynél a koordinátarendszer középpontja egybeesik a föld középpontjával. A helymeghatározásban szatelliták segítenek, melyek folyamatosan közlik pillanatnyi helyzetüket, és az üzenetközlés pontos időpontját. A k -adik szatellita tehát elküldi helyzetének (x_k, y_k, z_k) koordinátás alakját (mindent méterben mérve), és a közlés t_k idejét nanoszekundumban mérve ($1\,\text{nsec} = 10^{-9}\,\text{sec}$). A navigációs eszköz (pl. okostelefon) ezt az információt a T_k időpontban veszi. Így az eszköz távolsága a szatellitától $p_k = c(T_k - t_k)$, ahol $c = 0.299792458\,\text{m/nsec}$, a fénysebesség. A k -adik szatellitáról tehát ismerjük az

$$\mathbf{s}_k = (x_k, y_k, z_k, p_k)$$

vektort. A p_k értéket pszeudotávolságnak (pseudorange) nevezik, mert nem megbízható, hisz tipikus esetben a vevőbeli óra nincs szinkronban a szatellitáéval. Pl. $1000\,\text{nsec}$ eltérés már $300\,\text{m}$-es hibát jelent. Így a vevőkészülék helyzetét jellemző ismeretlenek egyike a vevő helyzetét megadó (x, y, z) vektor, másika az aszinkronitásból adódó $b = c\Delta T$ távolság, ahol ΔT a szatelliták egymással szinkronban lévő idejétől való eltérés mértéke nanoszekundumban. Ismeretlen tehát a vevőt jellemző

$$\mathbf{v} = (x, y, z, b)$$

vektor. Az $\mathbf{s}_k$ és $\mathbf{v}$ koordinátái közt fönnáll a

$$\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + b = p_k,$$

azaz a

$$(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2 = (p_k - b)^2$$

egyenlőség. Mivel négy ismeretlenünk van, legalább négy egyenletet fel kell írnunk, vagyis legalább négy szatellita adataira szükség lesz. Végezzük el a négyzetre emeléseket, majd rendezzük át az egyenletet:

$$(x_k^2 + y_k^2 + z_k^2 - p_k^2) - 2(x_k x + y_k y + z_k z - p_k b) + (x^2 + y^2 + z^2 - b^2) = 0. \tag{4.1}$$

Pusztán az egyszerűbb jelölés kedvéért használjuk a Lorenz-féle skaláris szorzatot, ami a következőképp definiálható:

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3 - x_4 y_4.$$

E jelöléssel és 2-vel való osztás után az (1) egyenlet a következő alakot ölti:

$$\frac{1}{2}\langle \mathbf{s}_k, \mathbf{s}_k \rangle - \langle \mathbf{s}_k, \mathbf{v} \rangle + \frac{1}{2}\langle \mathbf{v}, \mathbf{v} \rangle = 0. \tag{4.2}$$

Tegyük fel, hogy n szatellitáról kapunk adatokat. Az így kapott n egyenlet mátrixszorzat alakja

$$\mathbf{a} - \mathbf{B}\mathbf{v} + C\mathbf{1} = \mathbf{0}, \tag{4.3}$$

ahol

$$\mathbf{a} = \frac{1}{2}\begin{bmatrix} \langle \mathbf{s}_1, \mathbf{s}_1 \rangle \\ \langle \mathbf{s}_2, \mathbf{s}_2 \rangle \\ \vdots \\ \langle \mathbf{s}_n, \mathbf{s}_n \rangle \end{bmatrix}, \ \mathbf{B} = \begin{bmatrix} x_1 & y_1 & z_1 & p_1 \\ x_2 & y_2 & z_2 & p_2 \\ \vdots & \vdots & \vdots & \vdots \\ x_n & y_n & z_n & p_n \end{bmatrix}, \ C = \frac{1}{2}\langle \mathbf{v}, \mathbf{v} \rangle, \mathbf{1} = \begin{bmatrix} 1 & \mathbf{1} \\ \vdots & \mathbf{1} \end{bmatrix}. \tag{4.4}$$

A (3) átrendezve a

$$\mathbf{B}\mathbf{v} = \mathbf{a} + C\mathbf{1} \tag{4.5}$$

egyenletre vezet, mely $n = 4$ esetén bármely C konstanssal egyértelműen megoldható, $n > 4$ esetén pedig bármely C esetén egyetlen optimális (a legkisebb négyzetek elve szerinti) megoldást ad. Jelölje ezt $\bar{\mathrm{v}}$. Az optimális megoldás:

$$\bar{\mathrm{v}} = \mathrm{B}^{+}(\mathbf{a} + C\mathbf{1}),$$

ahol $\mathbf{B}^{+} = (\mathbf{B}^{\mathsf{T}}\mathbf{B})^{-1}\mathbf{B}^{\mathsf{T}}$, mivel $n \geqslant 4$ esetén $\mathbf{B}$ teljes oszloprangú. A nehézséget az okozza, hogy C-t sem ismerjük, az épp az ismeretlen $\mathbf{v}$ kvadratikus függvénye.

Helyettesítsük C (4)-beli definíciójába a még ki nem számolt $\bar{v}$ vektort. Kihasználva a Lorenz-szorzat bilinearitását kapjuk, hogy

$$C = \frac{1}{2}\langle \mathbf{B}^+(\mathbf{a}+C\mathbf{1}), \mathbf{B}^+(\mathbf{a}+C\mathbf{1})\rangle = \frac{1}{2}\langle \mathbf{B}^+\mathbf{a}, \mathbf{B}^+\mathbf{a}\rangle + C\langle \mathbf{B}^+\mathbf{a}, \mathbf{B}^+\mathbf{1}\rangle + \frac{1}{2}C^2\langle \mathbf{B}^+\mathbf{1}, \mathbf{B}^+\mathbf{1}\rangle.$$

Ezt átrendezve egy C -ben másodfokú egyenletet kapunk, melynek minden együtthatója konstans:

$$C^2\langle \mathbf{B}^+\mathbf{1}, \mathbf{B}^+\mathbf{1}\rangle + 2C(\langle \mathbf{B}^+\mathbf{a}, \mathbf{B}^+\mathbf{1}\rangle - 1) + \langle \mathbf{B}^+\mathbf{a}, \mathbf{B}^+\mathbf{a}\rangle = 0. \qquad (4.6)$$

Ennek az egyenletnek 2 megoldása van, jelölje ezeket C_1 és C_2. Kiszámoljuk a $\bar{v}_i = \mathbf{B}^+(\mathbf{a}+C_i\mathbf{1})$ ($i=1,2$) vektorokat. Ezek egyike lesz a megoldás, amit úgy döntünk el, hogy megnézzük, melyik megoldás van a földfelszín közelében (a másik attól általában nagyon messze lesz). Ehhez csak azt kell tudni, hogy a földfelszín távolsága a Föld középpontjától 6353 km és 6384 km között változik.

4.2 Keresés az Interneten

E fejezetben egy kérdést vizsgálunk: hogyan rangsorolhatók egy internetes keresés találatai, vagy akár az Internet összes dokumentuma.

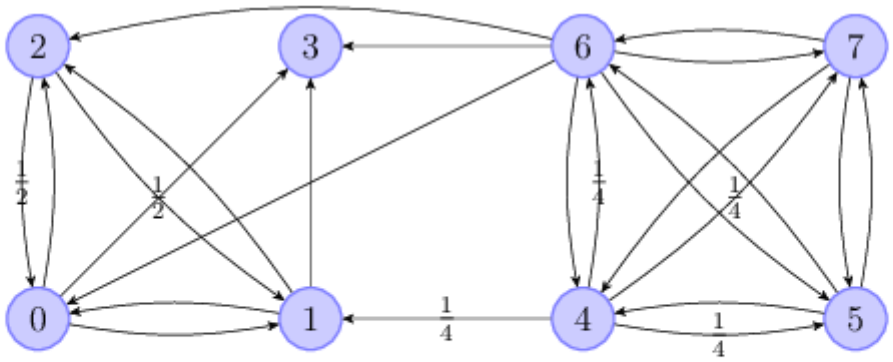
PageRank - a Google kereső alapötlete

A ma legnépszerűbb webes kereső program alapötlete a webes dokumentumok rangsorolására egy egyszerű sajátvektorkeresési feladatra épül. Az eljárás neve PageRank (amibe Larry Page és Sergey Brin, a Google alapítói egyikének neve is el van rejtve). A fogalom öndefinálónak tűnik: egy dokumentum PageRank értéke annál magasabb, minél több nagy PageRank érékű dokumentum mutat rá.

Az első ötlet az, hogy modellezzük egy weben szörfölő útját, aki minden oldal linkjei közül véletlenszerűen választ és így dokumentumról dokumentumra bolyong a weben. Ha e bolyongást nagyon sokáig folytatja, kialakul egy természetes sorrend, melyben minden dokumentum azzal arányos számú pontot kap, ahányszor ott járt a szörfölő.

Tekintsük a webdokumentumok irányított, súlyozott élű gráfját, ahol a dokumentumok a gráf csúcsai, és az i -edik csúcsból él megy a j -edik csúcsba, ha az i -edik dokumentumban van link a j -edikre. Egy él súlya legyen $1/k$, ha egy k ki-fokú csúcsból indul ki.

Tegyük fel, hogy egy témában csak 8 releváns dokumentum van, ráadásul mindegyikre épp 3 másik hivatkozik, ezért első ránézésre nehéz sorrendet felállítani köztük. Gráfja a 33 ábrán látható.



33. ábra. A web egy 8 dokumentumból álló részén minden dokumentumra épp 3 másik hivatkozik. A 3-as nem hivatkozik más dokumentumra, a $\{0,1,2,3\}$ halmazbeliek csak e halmazbeliekre. Minden él a kezdőcsúcs kifokának reciprokát kapja súlyként. Az ábrán csak a 2-es és 4-es pontokból kifutó élekre írtuk rá a súlyokat.

Egy irányított, súlyozott élű gráf adjacenciamátrixának (i,j) indexű eleme legyen az i -ből j -be vezető él súlya, és 0, ha ilyen él nincs. A web-re imént definiált gráfra tehát e mátrix a következő:

$$[\mathbf{A}]_{ij} = \begin{cases} \frac{1}{k}, & \text{ha megy } i\text{-ből } j\text{-be él és } i \text{ ki-foka } k, \\ 0 & \text{egyébként,} \end{cases}$$

Konkrét példánkban a következő mátrixot kapjuk:

$$\mathbf{A} = \begin{pmatrix} 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 & 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{6} & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{6} \\ 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \end{pmatrix}$$

E mátrix (sor)sztohasztikus lenne, ha minden sorban lenne 0-tól különböző elem, hisz a sorösszeg minden nemzérus sorban 1. A zérussor olyan dokumentumnak felel meg, amely nem hivatkozik másikra. A bolyongás itt elakadna, ezért úgy módosítjuk a modellt, hogy ilyen pontban a szörfölő ugorjon egy véletlen dokumentumra. A mátrix ekkor így változik:

$$[\mathbf{A}]_{ij} = \begin{cases} \frac{1}{k}, & \text{ha megy i-ből j-be él és i ki-foka k,} \\ \frac{1}{n}, & \text{ha i ki-foka 0 és n a csúcsok száma,} \\ 0 & \text{egyébként.} \end{cases} \tag{4.7}$$

Ez még mindig nem tökéletes modell, mert lehet, hogy vannak olyan dokumentumok, amelyek csak egymásra hivatkoznak, így a szörfölő itt is beragadhat. Ez a mátrixok nyelvén épp azt jelenti, hogy a mátrix reducibilis, a gráfok nyelvén, hogy nem erősen összefüggő. Példabeli gráfunkon $\{3,1,2,5\}$ az 4×4 csúcshalmazból nem vezet ki él, a hozzá tartozó mátrix jobb felső -es része pedig zérusmátrix, vagyis reducibilitása azonnal látható.

Még egy hibája van a modellnek: ha egy dokumentum csak másokra hivatkozik, de semelyik sem hivatkozik rá, a bolyongás során nem jut oda a szörfölő, ezért nem kap pontot. Mindkét hiba javítható, ha a modellen úgy módosítunk, hogy a szörfölő minden csúcsban d valószínűséggel egyenletes eloszlás szerint választ az összes csúcs közül, és $1-d$ valószínűséggel a csúcsból kifutó élek végpontjai közül egyenletes eloszlás szerint. A bolyongást leíró mátrix ekkor a következő alakú:

$$\mathbf{M} = (1-d)\mathbf{A} + d\frac{1}{n}\mathbf{J},$$

ahol $\mathbf{A}$ a (7)-beli mátrix, $\mathbf{J}$ a csupa 1-esből álló mátrix, n e négyzetes mátrixok rendje, és $d \in (0,1)$. Tapasztalatok szerint érdemes d -t a $(0.1, 0.2)$ intervallumból választani. Konkrét példánkban legyen $d = 0.15$, így $1-d = 0.85$.
Ekkor 3 tizedesre kerekített jegyekkel

$$\mathbf{M} = \begin{pmatrix} 0.019 & 0.302 & 0.302 & 0.302 & 0.019 & 0.019 & 0.019 & 0.019 \\ 0.302 & 0.019 & 0.302 & 0.302 & 0.019 & 0.019 & 0.019 & 0.019 \\ 0.444 & 0.444 & 0.019 & 0.019 & 0.019 & 0.019 & 0.019 & 0.019 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.019 & 0.231 & 0.019 & 0.019 & 0.019 & 0.231 & 0.231 & 0.231 \\ 0.019 & 0.019 & 0.019 & 0.019 & 0.302 & 0.019 & 0.302 & 0.302 \\ 0.160 & 0.019 & 0.160 & 0.160 & 0.160 & 0.160 & 0.019 & 0.160 \\ 0.019 & 0.019 & 0.019 & 0.019 & 0.302 & 0.302 & 0.302 & 0.019 \end{pmatrix}$$

Világos, hogy e mátrix pozitív, sztochasztikus mátrix, hisz $\mathbf{A}$ is sztochasztikus, $\frac{1}{n}\mathbf{J}$ is, így az 1-összegű súlyokkal vett összegük is az. ($\mathbf{M}$ tehát egy Markov-lánc átmenetmátrixa.) Mivel $\mathbf{M}$ pozitív, Perron-tételéből tudjuk, hogy spektrálsugara 1, az 1 egyszeres sajátérték, nincs több 1-abszolút értékű sajátértéke, és az 1-hez tartozik az egyetlen olyan pozitív $\mathbf{v}$ bal sajátvektor, melyre $\|\mathbf{v}\|_1 = 1$, azaz amelynek koordinátái valószínűségeloszlást adnak. Ha $\mathbf{x}$ a bolyongás kiindulópontjának valószínűségeloszlását megadó vektor, akkor az első lépés után a gráf i pontjában $[\mathbf{x}^\mathsf{T}\mathbf{M}]_i$ valószínűséggel leszünk, az m -edik lépés után $[\mathbf{x}^\mathsf{T}\mathbf{M}^m]_i$ valószínűséggel. Ugyancsak a pozitív mátrixok elméletéből (és a 1.4 fejezetből) tudjuk, hogy

$$\lim_{m\to\infty} \mathbf{x}^\mathsf{T}\mathbf{M}^m = \mathbf{v}.$$

A Markov-láncok nyelvén $\mathbf{v}$ a stacionárius eloszlás. Épp ezt kerestük. Példánkban

$$\mathbf{v} = (0.151, 0.157, 0.137, 0.137, 0.106, 0.100, 0.112, 0.100).$$

Ennek alapján a dokumentumok sorrendje: 1, 0, $2\&3$, 6, 4, $5\&7$ (két holtversennyel).

Valóságos, tehát hatalmas mátrixok esetén $\mathbf{A}$ még ritka, de $\mathbf{M}$ már nem, vele csak reménytelenül lassan lehetne számolni. Viszont

$$\mathbf{x}^\mathsf{T}\mathbf{M} = \mathbf{x}^\mathsf{T}\left((1-d)\mathbf{A} + d\frac{1}{n}\mathbf{J})\right) = (1-d)\mathbf{x}^\mathsf{T}\mathbf{A} + \frac{d}{n}\mathbf{1}^\mathsf{T},$$

ahol $\mathbf{1}$ a csupa-1 vektort jelöli. Ez azt mutatja, hogy ha megelégszünk a $\mathbf{v}$-hez konvergáló $\mathbf{x}_{m+1} = \mathbf{x}_m^\mathsf{T}\mathbf{M}$ iteráció néhány lépésének kiszámolásával, akkor elég csak az $\mathbf{x}^\mathsf{T}\mathbf{A}$ vektor-mátrix szorzást elvégezni, ami a ritka $\mathbf{A}$ mátrixszal hatalmas adathalmazon is gyors, utána csak vektorok lineáris kombinációját kell számolni.

A HITS algoritmus

A PageRank-kel egy időben Jon Kleinberg egy hasonló, de egy-egy témában releváns oldalak felfedezésére alkalmas HITS[10] nevű algoritmust dolgozott ki. A PageRank önmeghatározását itt egy kettős önmeghatározás váltja. A web-en fontos oldalak közt vannak tekintélyes alkotások (tekintélyek - authorities), és gyűjtőoldalak (hubs), melyek egy téma fontos és releváns oldalaira mutatnak. Egy tekintély mértéke annál nagyobb, minél több nagy értékű gyűjtő mutat rá, míg egy gyűjtő értéke annál nagyobb, minél több nagy értékű tekintélyre mutat.

Most induljunk ki abból, hogy minden egyes linket figyelembe veszünk. Arra számítunk, hogy a linkek értéke majd úgyis csak attól fog függeni, hogy mennyire értékes helyre mutat. Ezért most az adjacenciamátrixszal számolunk:

$$[\mathbf{A}]_{ij} = \begin{cases} 1, & \text{ha megy } i\text{-ből } j\text{-be él,} \\ 0, & \text{egyébként.} \end{cases}$$

Minden weboldal két értéket kap. A tekintélyértékek vektora legyen $\mathbf{a}$, a gyűjtőértékek vektora $\mathbf{h}$ ('a', mint authorities, 'h', mint hubs). Azt szeretnénk, hogy minden oldal tekintélyértéke megegyezzen a rá mutató oldalak gyűjtőértékének összegével, és minden oldal gyűjtőértéke megegyezzen a benne lévő linkekhez tartozó oldalak tekintélyértékének összegével. E két feltétel mátrixszorzással fölírva ezt adja:

$$\mathbf{h} = \mathbf{A}\mathbf{a}$$
$$\mathbf{a} = \mathbf{A}^\mathsf{T}\mathbf{h}$$

E két egyenlőség egyszerre általában nem fog sikerülni, mert e két egyenletből $\mathbf{a} = \mathbf{A}^\mathsf{T}\mathbf{A}\mathbf{a}$ adódik, és $\mathbf{A}^\mathsf{T}\mathbf{A}$-nak az 1 általában nem sajátértéke. Ezért ismét iteratív megoldással próbálkozunk, bár ez most nem a gráfon való bolyongást szimulál. Induljunk egy tetszőleges $\mathbf{a}_0$ tippből, és képezzük a következő sorozatot:

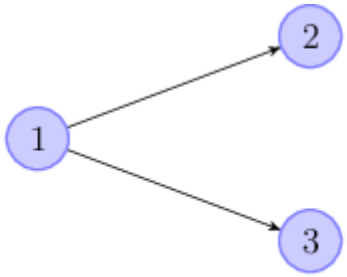
$$\mathbf{h}_{m+1} = \mathbf{A}\mathbf{a}_m$$
$$\mathbf{a}_{m+1} = \mathbf{A}^\mathsf{T}\mathbf{h}_{m+1}$$

amiből behelyettesítéssel adódik, hogy

$$\mathbf{h}_{m+1} = \mathbf{A}\mathbf{A}^\mathsf{T}\mathbf{h}_m$$
$$\mathbf{a}_{m+1} = \mathbf{A}^\mathsf{T}\mathbf{A}\mathbf{a}_m \tag{4.8}$$

Nézzünk egy nagyon egyszerű konkrét példát e sorozatokra.

4.4. Példa A web álljon három oldalból, és az első hivatkozzon a másik kettőre (ld. 34 ábra). Mennyi a tekintély- és mennyi a gyűjtőértéke az oldalaknak?



34. ábra. Egy gyűjtő és két tekintély

Megoldás

A gráf adjacenciamátrixa

$$\mathbf{A} = 011000000.$$

Legyen a tekintélyértékek induló vektora $\mathbf{a}_0 = (1, 1, 1)$. Ebből

$$\mathbf{h}_1 = \mathbf{A}\mathbf{a}_0 = 011000000111 = 200.$$

Innen

$$\mathbf{a}_1 = \mathbf{A}^\mathsf{T}\mathbf{h}_1 = 000100100200 = 022.$$

Folytatva kapjuk, hogy $\mathbf{h}_2 = (4,0,0)$, $\mathbf{a}_2 = (0,4,4)$, stb. Ezek nem konvergensek, de ha a vektorsorozatok vektorait minden lépésben leosztjuk az m-normájukkal, akkor $m > 0$ esetén a $\mathbf{h}_m = (1,0,0)$, $\mathbf{a}_m = (0,1/2,1/2)$ vektorokat kapjuk, így ezek határértéke is létezik. A határértékként kapott $\mathbf{h} = (1,0,0)$, $\mathbf{a} = (0,1/2,1/2)$ vektorokat tekinthetjük tehát a gyűjtő és tekintély mértékének. Valóban, az 1-es dokumentum 1-értékű gyűjtő és 0-értékű tekintély, míg a másik két dokumentum 0-értékű gyűjtő, és azonos értékű tekintélyek az ábra alapján is.

A példában tapasztalt eredmény általában is igaz, ugyanis
ha $\mathbf{A}\mathbf{A}^\mathsf{T}$ és $\mathbf{A}^\mathsf{T}\mathbf{A}$ primitív mátrixok, akkor a lenormált (8) vektorsorozatok határértékei léteznek, és a határértékül kapott

$$\mathbf{h} = \lim_{m\to\infty} \frac{\mathbf{h}_m}{\|\mathbf{h}_m\|_1}, \text{ és } \mathbf{a} = \lim_{m\to\infty} \frac{\mathbf{a}_m}{\|\mathbf{a}_m\|_1}$$

vektorok az $\mathbf{A}$ mátrix jobb, illetve bal Perron-vektorai. Másként fogalmazva $\mathbf{h}$ az $\mathbf{A}\mathbf{A}^\mathsf{T}$ mátrix legnagyobb sajátértékhez tartozó sajátvektora, míg $\mathbf{a}$ az $\mathbf{A}^\mathsf{T}\mathbf{A}$ mátrix legnagyobb sajátértékhez tartozó sajátvektora. A 34 ábrabeli esetben

$$\mathbf{A}\mathbf{A}^\mathsf{T} = 200000000, \mathbf{A}^\mathsf{T}\mathbf{A} = 000011011,$$

ezek legnagyobb sajátértéke 2, a hozzájuk tartozó sajátvektorok $(1,0,0)$, illetve $(0,1/2,1/2)$, ami megegyezik korábbi eredményünkkel.

A 33 ábrán megadott gráf esetén a két Perron-vektor:

$$\mathbf{h} = (0.1176, 0.1276, 0.0696, 0, 0.1608, 0.1283, 0.2678, 0.1283)$$
$$\mathbf{a} = (0.1194, 0.0894, 0.1317, 0.1317, 0.1346, 0.1430, 0.1072, 0.1430).$$

Eszerint 6-os a legjobb gyűjtő és 3-as a legrosszabb (valóban, hisz semmire nem hivatkozik), a tekintélyek közt kicsi a különbség, ami érthető, hisz mindegyikre három oldal mutat: holtversenyben első az 5-ös és 7-es, és az 1-es a legrosszabb (valóban, rá gyengébb gyűjtők hivatkoznak).

A webes rangsorolás népszerű téma, itt csak lineáris algebrai alapjainak felvillantására volt lehetőség.

4.3 Az SVD alkalmazásai

A szinguláris érték szerinti felbontás számtalan alkalmazásra lelt a statisztikától kezdve műszaki-fizikai alkalmazásokig. Itt az adatokban rejlő tartalmi

összefüggések megértéséhez, a lényeges információk kiemeléséhez, információtömörítéshez kapcsolódó technikákat ismertetünk, többükre vizuálisan is megjeleníthető példákat mutatva.

Képtömörítés

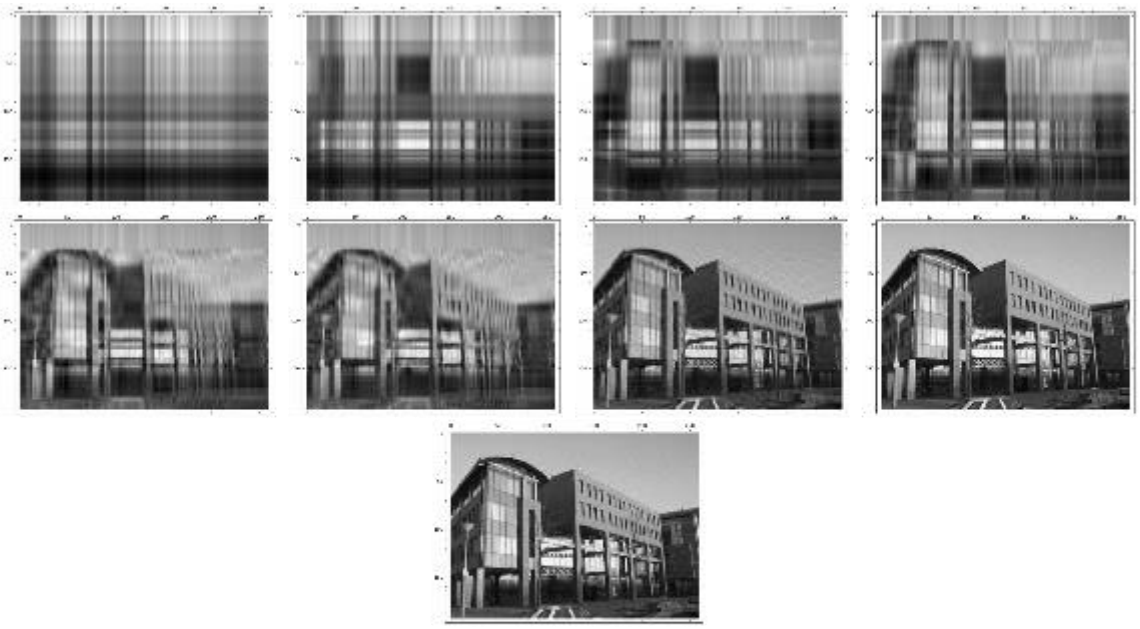
Bár a képtömörítés leghatékonyabb módja nem a most ismertetendő módszer, mégis érdemes a megmutatásra, mert egyszerű módon teszi láthatóvá a kis rangú approximáció tételét, más néven az Eckart-Young-tételt. Eszerint egy tetszőleges r -rangú $\mathbf{A}$ mátrixnak a legföljebb k -rangú mátrixok közti legjobb $\mathbf{A}_k$ approximációja fölírható

$$\mathbf{A}_k = \sum_{i=1}^{k} \sigma_i \mathbf{u}_i \mathbf{v}_i^{\mathsf{T}}.$$

alakban, ahol σ_i az $\mathbf{A}$ mátrix i -edik szinguláris értékét, $\mathbf{v}_i$, illetve $\mathbf{u}_i$ a hozzá tartozó jobb és bal szinguláris vektort jelöli. A „legjobb approximáción” akár a Frobenius-, akár a 2-normában való távolság szerinti legjobb becslést értjük. Még a távolság is könnyen becsülhető e két norma esetén a szinguláris értékek segítségével, nevezetesen

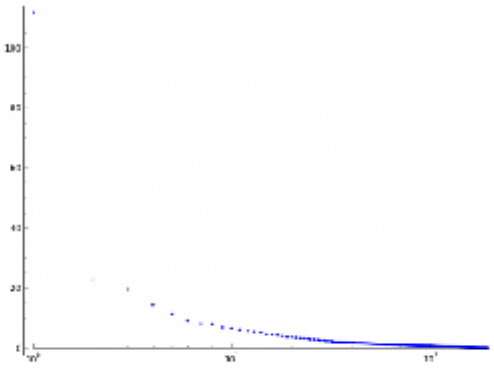
$$\min_{\mathrm{r}(\mathbf{B})\leqslant k} \|\mathbf{A}-\mathbf{B}\|_F = \|\mathbf{A}-\mathbf{A}_k\|_F = \sqrt{\sum_{i=k+1}^{r} \sigma_i^2},$$
$$\min_{\mathrm{r}(\mathbf{B})\leqslant k} \|\mathbf{A}-\mathbf{B}\|_2 = \|\mathbf{A}-\mathbf{A}_k\|_2 = \sigma_{k+1}.$$

Legyen tehát $\mathbf{A}$ egyszerűen egy szürkeárnyalatos fénykép pixelmátrixa. A példában szereplő kép a BME egyik épületének 194×259 pixeles képe (ld. 35 ábra). Az ábra az $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$, $\mathbf{A}_8$, $\mathbf{A}_{12}$, $\mathbf{A}_{40}$, $\mathbf{A}_{97}$ és az $\mathbf{A}_{194} = \mathbf{A}$ mátrixok képe.



35. ábra. Egy fénykép 9 különböző, SVD-vel tömörített változata. A figyelembe vett szinguláris értékek száma rendre 1, 2, 3, 4, 8, 12, 40, 97, 194. Az utolsó becslés magával az eredeti képpel azonos.

Az $\mathbf{A}$ első és utolsó néhány szinguláris értéke: $\sigma_1 = 111.644$, $\sigma_2 = 22.803$, $\sigma_3 = 19.5021$, $\sigma_4 = 14.3708$,..., $\sigma_{193} = 0.00277355$, $\sigma_{194} = 0.00239575$. Az összes szinguláris értéket mutatja a 36 ábra. Látjuk, a 194 szinguláris érték és vektorpár közül már az első 8 is felismerhető eredményt ad, de az összes negyedével már az eredetitől alig különböző képet kapunk.



36. ábra. A szinguláris értékek eloszlása (az x-tengelyen logaritmikus skálával)

Mögöttes tartalom analízise

Hasonló módszereket alkalmaznak nagy mennyiségű dokumentum tartalmi feldolgozásában is. Az ún. mögöttes tartalom analízise - angolul latent semantic indexing (LSI) vagy latent semantic analysis (LSA) - az SVD segítségével lehetővé teszi, hogy a szavak és fogalmak közt olyan kapcsolatokat fedezzünk fel, amelyekre csak a szavak dokumentumokban való előfordulásait figyelve nem

volnánk képesek. A módszert megalapozó gondolat az, hogy az egy dokumentumban szereplő szavakat összekapcsolja a dokumentum tartalma. E kapcsolatokat - a szavak mögött lévő tartalmat - az SVD kiemeli, mint lényeges információt. Az ilyen technikákkal adott tartalmú dokumentumok keresésében sokkal jobb eredmény érhető el, mintha csak kulcsszavak szerint keresnénk, hisz itt pl. legegyszerűbb esetként a szinonimák is szoros kapcsolatba kerülnek. Ugyanakkor a többjelentésű szavak alkalmazása sem okoz gondot, mert néhány szó megadásával a mögöttes tartalom a szónak csak az adott szavakhoz tartozó jelentése szerinti értelmét fogja figyelembe venni. A módszer így dokumentumok tartalmának osztályozására, indexelésére is alkalmas anélkül, hogy előzetesen ember alkotta bonyolult tezauruszokat kellene alkalmazni. Az eredeti módszert 1989, a többnyelvű és nyelvek közti alkalmazását 1994 óta szabadalom védi.

Egy n dokumentumból álló, vagy egy nagyméretű és n bekezdést tartalmazó szöveggyűjteményt fogunk vizsgálni. Az ezekben előforduló szavak száma legyen m . Képezzük az $\mathbf{A}$ mátrixot, melynek sorai a szavakat, oszlopai a különböző dokumentumokat (vagy az egyetlen dokumentum bekezdéseit) reprezentálják.

Jelölje t_{ij} az i -edik szó gyakoriságát a j -edik dokumentumban és T_i a teljes szöveggyűjteményben. Az $\mathbf{A}$ mátrix a_{ij} elemét az i -edik szóhoz tartozó e két gyakoriság fogja meghatározni. Sok függvénnyel folyt kísérletezés, tapasztalatok szerint a következő adja a legjobb eredményt:

$$a_{ij} = \left(1 + \sum_{k=1}^{n} \frac{\frac{t_{ik}}{T_i} \log \frac{t_{ik}}{T_i}}{\log n}\right) \log(1 + t_{ij}).$$

E bonyolultnak tűnő formula egy olyan szorzat, melynek első tényezője egy csak az i -edik szónak az egész gyűjteményhez való kapcsolatától függő globális súly, míg a második csak a lokális érték - vagyis csak a szó adott dokumentumban való gyakoriságának - függvénye. Annak vizsgálata, hogy miért épp e függvény ad jó eredményt, már az információelmélet területére vezet, és az entrópia fogalmához kapcsolódik.

Tekintsük az így konstruált $\mathbf{A}$ mátrix szinguláris $\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^\mathsf{T}$ felbontását és az abból származó $\mathbf{A}_k = \mathbf{U}_k\mathbf{\Sigma}_k\mathbf{V}_k^\mathsf{T}$ közelítést. Az $\mathbf{U}_k$, illetve $\mathbf{V}_k$ oszlopainak vektorterében a szavak, illetve dokumentumok kapcsolatát a hozzájuk tartozó vektorok helyzete jellemzi: nyilván a közelebbi vektorok erősebb kapcsolatot jelentenek. Ha ezek után egy új dokumentumot, vagy keresőszavak egy halmazát akarjuk vizsgálni, a fenti képlet szerint kell súlyozott vektort képezni belőle. Ennek a $\mathbf{V}_k$ oszlopai által kifeszített vektortérbe eső vetülete és a többi dokumentumhoz tartozó vektor vetülete közti távolság fogja a hozzájuk való kapcsolat erősségét jellemezni.

Főkomponens-analízis

A főkomponens-analízis Pearson angol statisztikustól származó módszer. Tulajdonképpen megegyezik az előző pontban használt SVD-alapú módszerrel egy alapvető különbséget leszámítva. Az előzőekben - általánosan fogalmazva - adatvektorok terében kerestünk egy olyan kisebb, k -dimenziós alteret, amelyikre a vektorok tőle mért távolságainak négyzetösszege a lehető legkisebb. Ez azonban nem mindig a legjobb módszer az adatok kapcsolatainak jellemzésére. Ha egy n -dimenziós adathalmaz a térben egy k -dimenziós affin altérbe esik, a legközelebbi altérre vetítés elmossa e tulajdonságát. Nyilván jobb lenne, ha nem csak az alterek, hanem az affin alterek között is keresnénk megfelelő jelöltet. Ez nagyon egyszerűen megvalósítható, ha induláskor az adatvektorokat centrális helyzetbe hozzuk, azaz az $\mathbf{a}_1$, $\mathbf{a}_2$,..., $\mathbf{a}_m$ vektorok helyett az $\mathbf{a}_1 - \bar{a}$, $\mathbf{a}_2 - \bar{a}$,..., $\mathbf{a}_m - \bar{a}$ vektorokat vizsgáljuk, ahol

$$\bar{a} = \sum_{i=1}^{m} \mathbf{a}_j \frac{}{m.}$$

E lépéssel visszavezettük a kérdést az alterekre vonatkozó, már megoldott kérdésre (ezt az állítást itt nem bizonyítjuk). Elvben e technika az előzőekben leírt mögöttes tartalom utáni nyomozásban is jobban használható lenne, ha a mátrix sorvektorainak centrális helyzetbe hozás nem járna azzal a következménnyel, hogy az eredetileg ritka mátrix ezáltal sűrűvé válna, ezzel reménytelenné téve a feladat numerikus megoldását.

Gyakori társadalomtudományi alkalmazás például egy kérdőíves felmérés kiértékelése. m kitöltött és n kérdésből álló kérdőív adatai egy $m \times n$ -es mátrixba kerülnek, oszlopvektorairól már feltételezzük, hogy koordinátáik összege 0. Ekkor a kérdőívvektorok - melyek most a mátrix sorvektorai és melyeket tekinthetünk egy valószínűségi vektorváltozó kimeneteleinek - 0 várható értékűek, és tapasztalati szórásnégyzetük $\sum_{i=1}^{m} \|\mathbf{a}_i\|^2$ -tel arányos. A feltételezés az, hogy a „mögöttes lényeges” tartalom legfontosabb összetevőjét az a vektor jellemzi, melynek irányában a legnagyobb a szórás, hisz ezen irány mentén különböztethetők meg legjobban a kérdőívek, s vele a válaszolók. Ezt az irányt nevezzük első főkomponensnek. Ha ez valamelyik tengelyirányba esik, akkor csak azt tudtuk meg, hogy az ehhez tartozó koordináta, illetve az ehhez tartozó kérdés a legfontosabb, a kérdezők lineáris sorbarendezéséhez elég ezt a koordinátát (kérdést) figyelembe venni. Egyéb esetekben viszont egy olyan összefüggésre jutottunk, mely csak a kérdések együtteséből olvasható ki. Tudjuk, hogy ez az irány épp az első jobb szinguláris vektor, és a szórás a legnagyobb szinguláris értékkel lesz arányos, nevezetesen

$$\sigma_1 = \|\mathbf{A}\mathbf{v}_1\|,$$

ahol

$$\mathbf{v}_1 = \arg\max\{\, \|\mathbf{A}\mathbf{v}\| \,|\, \|\mathbf{v}\| = 1 \,\}.$$

Ezután e főkomponens irányára merőleges (vele nem korreláló) irányok közt megismételjük a főkomponens keresését, majd ezt ciklikusan ismételve a szinguláris értékek csökkenő sorozatához, és a hozzájuk tartozó jobb szinguláris vektorok sorozatához jutunk:

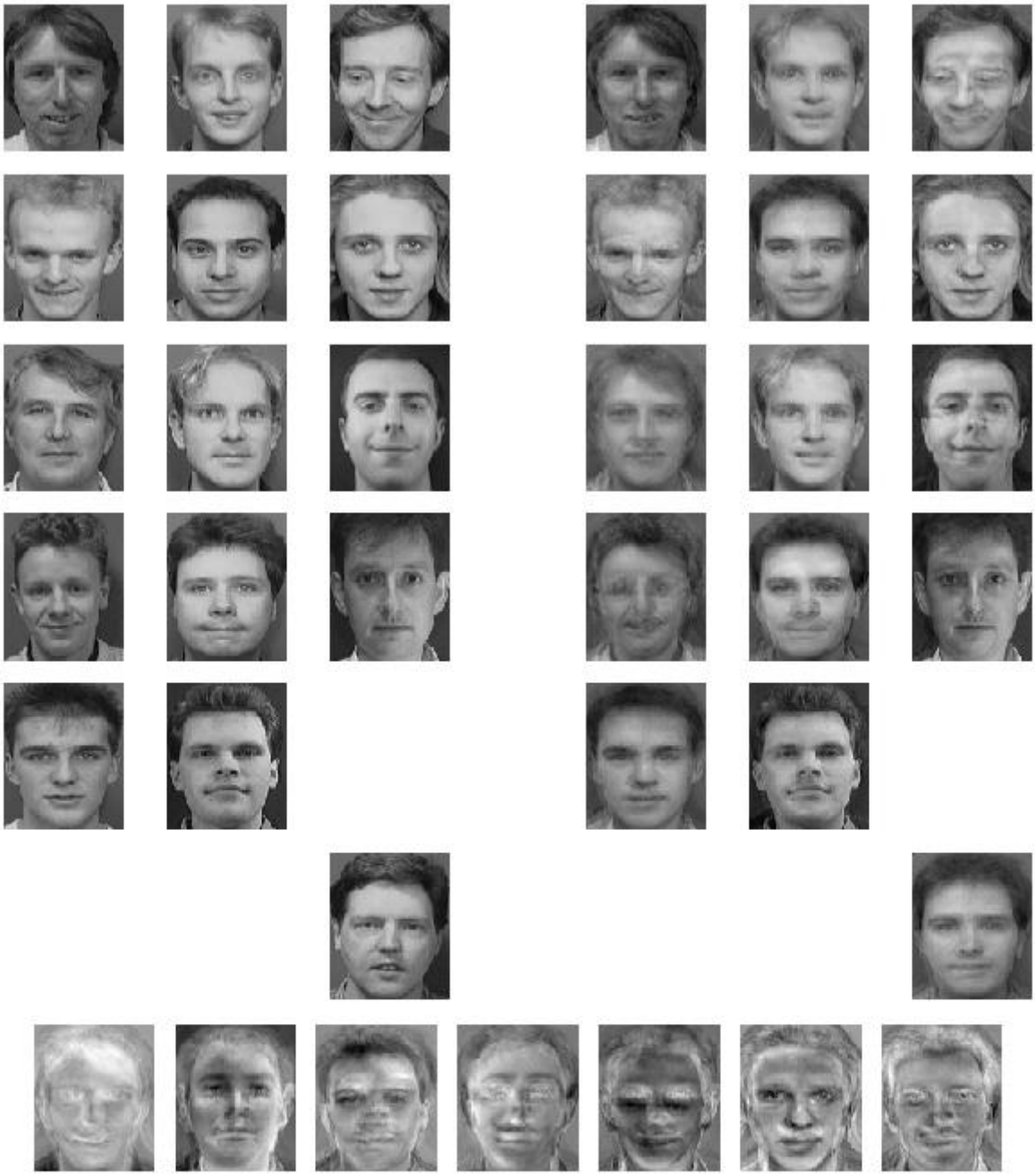
$$\sigma_i = \|\mathbf{A}\mathbf{v}_i\|,$$

ahol

$$\mathbf{v}_i = \arg\max\{\, \|\mathbf{A}\mathbf{v}\| \,|\, \|\mathbf{v}\| = 1, \mathbf{v} \perp \operatorname{span}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}) \,\}.$$

E módszer szemléltetésére vizuálisan megjeleníthető adathalmazt, nevezetesen arcképeket választunk. A főkomponens-analízis arcképekre való alkalmazásában keletkező jobb szinguláris vektoroknak az arcfelismerés friss műszaki tudományában külön nevük van: „sajátarcok” (eigenfaces). Mi most kevés adattal, minimális eszközökkel dolgozunk. 14 darab 92×112 pixeles szürkeárnyalatos kép mátrixából egy 14×10304-es mátrixot képezünk a képek vektorként való kezelésével. A képek vektorizálása egyszerűen az adatok sorfolytonos egybeolvasását jelenti ($10304 = 92 \times 112$). E mátrix minden sorából kivonjuk a sorvektorok $\bar{\mathrm{a}}$ átlagát, és az így kapott $\mathbf{A}$ mátrix legnagyobb 7 szinguláris értékhez tartozó szinguláris vektorok által kifeszített altérre vetítjük $\mathbf{A}$ sorvektorait, majd visszatoljuk $\bar{\mathrm{a}}$-sal. A 37 képen látható az eredmény:
az $\mathbf{R}^{10304}$ tér 14 centralizált képvektora által kifeszített 14-dimenziós alteréhez megkeressük azt a 7-dimenziósat, melytől való távolságnégyzeteinek összege minimális. Így az erre az altérre eső vetületei a centralizált képvektoroknak őrzik a legjobban a képekben lévő eredeti információt (az egyéb 7-dimenziós alterek közül). A főkomponensek a kép alsó sorában láthatók. Lényegesen nagyobb adathalmaz esetén a főkomponensek többet mondanak az arcban rejtett információ lényegéről. Kísérletképpen egy 15-dik kép - a 14 képből számolt $\bar{\mathrm{a}}$-sal való eltoltját - rávetítettük az altérre, majd a vetületet vissza, hogy lássuk, mennyire van e vetület közel az eredetihez.[11]

Az arcfelismerés mára igen széles körben alkalmazott műszaki tudománnyá vált, melynek matematikai hátteréből csak egy apró részletet mutat a fenti leegyszerűsített példa.



37. ábra. A két egymás mellett lévő tábla bal első 14 képe 14 arckép. A mellette lévő 14 kép az előbbiek pixelmátrixaiból alkotott vektorokhoz legközelebb fekvő 7-dimenziós affin altérre eső merőleges vetületeikből származik. A 15-dik kép párja egy – az előzőektől különböző – új képnek a 14-dimenziós térre való merőleges vetületének megjelenítése. Az alsó sorban a 7-dimenziós affin altérhez tartozó alteret kifeszítő 7 szinguláris vektor ábrája. A színek negatívba játszó megjelenésének oka az, hogy ezek centralizált vektorok, nem az affin altérből valók.

Tárgymutató

4.4 Digitális jelfeldolgozás

A XX. század második felétől napjainkig terjedő időszak történelemformáló technikai vívmányainak jelentős része kapcsolatban van a digitális jelfeldolgozással (multimédia, mobiltelefónia, internet...). E műszaki terület pedig hemzseg a lineáris algebrai fogalmaktól. Arra azonban még e könyvben sem vállalkozhatunk, hogy e műszaki tudomány mélyére ássunk. Az egyetlen célunk, hogy néhány elemi alapfogalmán keresztül bemutassuk, hogy a lineáris algebra fogalmai milyen természetes módon jelennek meg e műszaki tudományban.

Időtartomány

Jelen egy konkrét jelenség valamely objektumának információt hordozó valamely jellemzőjét értjük. Ha ezt egy valós intervallumot is tartalmazó tartományon értelmezett függvénnyel/függvényekkel tudjuk leírni, folytonos paraméterű jelről beszélünk. Ez a paraméter az alkalmazások nagy részében az idő, de lehet más is, pl. a hely. Lehet, hogy a jelet egy sorozattal - egy $\mathbb{Z}$ -n értelmezett függvénnyel - tudjuk leírni. Lehet, hogy maga a jelenség ilyen diszkrét természetű, de sokkal izgalmasabb műszaki és matematikai szempontból is az, ha a jel ugyan folytonos paraméterű, de csak minták sorozatával tudjuk a magunk számára leírhatóvá tenni. E sorozatot idősornak nevezi a műszaki gyakorlat, ha paramétere az idő.

Legyen s egy folytonos jelet leíró egyváltozós valós (esetleg komplex értékű) függvény, a tipikus alkalmazások okán az idő függvénye. Ezt diszkrét pontokban kiértékeljük, ami a gyakorlatban legtöbbször egyenlő időközönként való mintavétellel történik. A mintavételezés periódusideje legyen $T > 0$, eredménye az $s_n = s(nT)$ sorozat, ahol $n \in \mathbb{Z}$ - egyelőre az általánosság kedvéért n fusson végig az összes egészen. A „szóba jöhető” $s = [s_n]$ sorozatok terét jelölje $\mathcal{S}$. Nem fog félreértésre vezetni, hogy a továbbiakban az s függvényből képzett sorozatot is s fogja jelölni. Értelmes - de képzeletben végtelen időintervallumra kiterjesztett - alkalmazásokban $\mathcal{S}$ része az ℓ_∞, de gyakran az ℓ_2 vagy ℓ_1 tereknek is.
Az $\mathcal{S}$ teret időtartománynak nevezzük. Az a mérnöki megfogalmazás, hogy egy jelet az diszkrét időtartományban vizsgálunk azt jelenti, hogy e tér elemeinek előállítása és tulajdonságaik megismerése a cél.

Az $\mathcal{S}$ tér elemei közt kitüntetett szerepe van a δ egységimpulzus jelnek, melyet úgy definiálunk, hogy $\delta_0 = 1$, és $\delta_n = 0$, ha $n \neq 0$.

Digitális szűrők

Bármely rendszer viselkedése jól jellemezhető azzal, ahogy a jeleket transzformálja. Ezek meglepően nagy része vagy egy lineáris $\mathcal{S} \to \mathcal{S}$ leképezés, vagy ilyennel nagyon jól közelíthető, ezért a továbbiakban csak ezekkel foglalkozunk. Az ilyen módon nem megközelíthető kaotikus jelenségekkel a matematika más fejezetei foglalkoznak.

A $Z : \mathcal{S} \to \mathcal{S}; s_n \mapsto s_{n-1}$ ($n \in \mathbb{Z}$) leképezést eltolásnak vagy késleltetésnek nevezzük. Világos, hogy az egységimpulzus késleltetéseinek végtelen lineáris kombinációival minden $\mathcal{S}$ -beli vektor fölírható:

$$s = \sum_{k=-\infty}^{\infty} s_k Z^k \delta.$$

A késleltetés gyakorlati fontossága nyilvánvaló, hisz a jelenségek leírásában nem játszhat szerepet az, hogy melyik időpillanatot nevezzük 0-nak. Így csak azok a transzformációk az érdekesek, amelyek hatása azonos az eltolt idősoron is. Pontosabban fogalmazva, az $L : \mathcal{S} \hookrightarrow \mathcal{S}$ leképezés eltolásinvariáns, ha felcserélhető Z -vel, azaz $LZ = ZL$.
Mivel $LZZ = (LZ)Z = (ZL)Z = Z(LZ) = ZZL$, kapjuk, hogy ha L eltolásinvariáns, akkor bármely k egészre $LZ^k = Z^k L$. Az eltolásinvariáns lineáris leképezéseket a jelfeldolgozásban digitális szűrőknek, vagy egyszerűen csak szűrőknek nevezik.

A L szűrő válaszát az egységimpulzusra impulzusválasznak nevezzük és h -val jelöljük, azaz az impulzusválasz az egységimpulzus L -képe:

$$h = L\delta.$$

Fontosságát az adja, hogy bármely rendszert jól leír az egységimpulzusra adott válasza, mindjárt látjuk hogyan.

Fontos szűrőt kapunk a konvolúció műveletével. Legyen $g \in \mathcal{S} \cap \ell_1$, $x \in \mathcal{S} \cap \ell_\infty$. Konvolúciójukon azt az $s = g * x = x * g$ sorozatot értjük, melyre

$$s_n = \sum_k x_k g_{n-k}.$$

Könnyen igazolható, hogy az $L : x \mapsto g * x$ leképezés eltolásinvariáns és lineáris, azaz szűrő. Sőt az is belátható, hogy minden $L : \ell_\infty \to \ell_\infty$ szűrő felírható ilyen alakban az impulzusválasz segítségével. Nevezetesen megmutatjuk, hogy ha az L szűrő impulzusválasza h , akkor $L : s \mapsto h * s$.

$$
\begin{aligned}
Ls &= L\left(\sum_k s_k Z^k \delta\right) && L \text{ linearitása következtében} \\
&= \sum_k s_k L Z^k \delta && L \text{ eltolásinvarianciája miatt} \\
&= \sum_k s_k Z^k L\delta && \text{mivel } L\delta = h = \sum_n h_n Z^n \delta \\
&= \sum_k s_k Z^k \left(\sum_n h_n Z^n \delta\right) && \text{a } \Sigma\text{-jelek felcserélése után} \\
&= \sum_n \sum_k s_k h_{n-k} Z^n \delta && (h * s)_n = \sum_k s_k h_{n-k} \\
&= h * s.
\end{aligned}
$$

Az hogy csak az $\ell_\infty \to \ell_\infty$ leképezéseket tekintsük - vagyis csak olyanokat, melyek korlátos sorozatokon vannak értelmezve és a képeik is korlátosak -, az alkalmazások felől nézve is természetes kikötés. Hasonlóképpen az is természetes korlátozás, hogy az impulzusválasz megfelelőképp „lecsengjen”, vagyis az általa keltett jel elemei abszolút értékének összege se lehessen végtelen. Mindez összecseng azzal a matematikai ténnyel, hogy Ls pontosan akkor lesz minden ℓ_∞-beli s-re az ℓ_∞-ben, ha $h \in \ell_1$.

Végül megemlítünk még egy természetes korlátozást a szűrőkre. Egy s jel kauzális, ha $n < 0$ esetén $s_n = 0$. Egy L szűrő kauzális, ha minden kauzális s jelre Ls is kauzális. Ez más szóval azt jelenti, hogy mindaddig, amíg a bemeneten csak 0 érkezik, addig a szűrő kimenetén sem jelenhet meg más, mint 0.

Frekvenciatartomány .....

4.5 Lineáris predikció

A lineáris predikció egy széles körben alkalmazott módszer idősoradatok jövőbeni értékeinek becslésére, melyben a becslés a korábbi adatok lineáris kombinációjával történik. Az audiojelek feldolgozásában való szerepe különösen fontos, pl. a beszédtömörítésben való alkalmazása tette lehetővé a mobiltelefonok gyors elterjedését, de szeizmológiai, orvostechnikai közgazdasági alkalmazásai is jelentősek.

A lineáris predikció (LP) olyan rendszereknél használatos, amelyeknél az input nem, vagy csak nehezen vizsgálható, mérhető, míg a rendszer válasza könnyen. Ilyen pl. az emberi beszédképző szervek rendszere, ahol a hangkeltés egész folyamata nehezen írható le, mondjuk amikor épp egy telefonba beszélünk, de a telefonba épített elektronika a rendszer outputját, vagyis a szánkat elhagyó levegő

rezgését leíró függvényt legalább diszkrét időpontokban mérni tudja. A mai telefonok 8000 kiértékelést végeznek (ennyi mintát vesznek) e függvényből egy másodperc alatt. Ha azonban e mérések eredményeit kéne továbbítani, nem lenne ma több milliárd eladott mobiltelefon a világon.

.....

A feladat az lesz, hogy s_n értékét a megelőző s_{n-1}, s_{n-2},..., s_{n-p} elemek egyszerű lineáris kombinációjával becsüljük. A becslést jelölje $\hat{s}_n$:

$$\hat{s}_n = -a_1 s_{n-1} - a_2 s_{n-2} - \cdots - a_p s_{n-p} = -\sum_{k=1}^{p} a_k s_{n-k}. \tag{4.9}$$

A negatív előjel csak a becslés hibájának - az ún. predikciós hibának - a felírását egyszerűsíti:

$$e_n = s_n - \hat{s}_n = \sum_{k=0}^{p} a_k s_{n-k}, \text{ ahol } a_0 = 1. \tag{4.10}$$

Tárgymutató

Hivatkozások

@MISCshortJordan, author=Wildon, Mark, title=A short proof of the existence of Jordan normal form, howpublished=*www.maths.bris.ac.uk/~mazmjw/Maths/JNFfinal.pdf*, year=2007,

@MISCrref, author=Holzmann, Wolf, title=Uniqueness of Reduced Row Echelon Form, howpublished=*http://www.cs.uleth.ca/~holzmann/notes/reduceduniq.pdf*, year=2002

@MISCCRS, author=Missen, Ronald W, author=Smith, William R, title=Chemical Reaction Stoichiometry (CRS): A Tutorial, howpublished=*http://www.chemical-stoichiometry.net/CRS_tut.pdf*, year=1998

@BOOKpotagy, author=Póta, György, title=Mathematical Problems for Chemistry Students, publisher=Elsevier, year=2006

@BOOKXu, author=Xu, Gouchang, title=GPS: Theory, Algorithms and Applications, publisher=Springer, year=2007

4.5. Példa (Maximális árbevétel erőforrás-korlátok mellett) Egy cég n különböző terméket állít elő, melyhez m különféle erőforrásra van szüksége (pl. nyersanyagok, munkaóra, gépidő,...). Az erőforrások mindegyike korlátos mennyiségben áll rendelkezésre, e korlátok vektorát jelölje $\mathbf{b}$. Jelölje $\mathbf{A}$ a szükségletek mátrixát, azaz a_{ij} jelölje a j -edik termék egységnyi mennyiségének előállításához szükséges mennyiséget az i -edik erőforrásból.

Mátrixjelöléssel

$$\begin{aligned} \mathbf{Ax} &= \mathbf{b} \\ \mathbf{x} &\geqslant \mathbf{0} \\ z = \mathbf{c}^{\mathsf{T}}\mathbf{x} &\to \max \end{aligned} \tag{4.11}$$

ahol

$$\mathbf{A} = 1 - 1100; -11010; 01001; \quad \mathbf{b} = 123 \quad \mathbf{x} = x_1 x_2 s_1 s_2 s_3 \quad \mathbf{c} = 11000.$$

Tekintsünk két nagyon leegyszerűsített feladatot.

A-vitamin 0,8 mg 0,8 mg 0,8 mg Ffi:0,8 mg Nő:1 mg B1-vitamin 1,5 mg 1,4 mg 1,4 mg Ffi: 1,4 mg Nő: 1,3 mg B2-vitamin 1,7 mg 1,6 mg 1,6 mg Ffi: 1,8 mg Nő: 1,5 mg Niacin 20 mg 18 mg 18 mg Ffi: 18 mg Nő: 15 mg B6-vitamin 2 mg 2 mg 2 mg 2 mg B6-vitamin 2 mg 2 mg 2 mg 2 mg B12-vitamin 0,006 mg 0,001 mg 0,001 mg 0,00 mg C-vitamin 60 mg 60 mg 60 mg 60 mg D-vitamin 0,005 mg 0,005 mg 0,005 mg 0,005 mg E-vitamin 10 mg 10 mg 10 mg 12 mg K-vitamin 0,08 mg Ffi: Nő: Folsav 0,4 mg 0,2 mg 0,2 mg 0,2 mg Biotin 0,3 mg 0,15 mg Ffi: Nő: Kalcium 1000 mg 800 mg 800 mg 800 mg Foszfor 1000 mg 800 mg 800 mg 620 mg Jód 0,15 mg 0,15 mg 0,15 mg 0,15 mg Vas 18 mg 14 mg 14 mg Ffi: 12 mg Nő: 15 mg Magnézium 400 mg 300 mg 300 mg Ffi: 350 mg Nő: 300 mg Réz 2 mg Nincs javasolt érték 1,4 mg 1,4 mg Cink 15 mg 15 mg 15 mg Ffi: 10 mg Nő: 15 mg Mangán 2 mg Nincs javasolt érték 4,0 mg 4,0 mg Kálium Nincs javasolt érték Nincs javasolt érték 3500 mg 3500 mg Klór Nincs javasolt érték Nincs javasolt

érték 3000 mg 3000 mg Króm 0,12 mg Nincs javasolt érték 0,12 mg 0,12 mg Molibdén 0,075 mg Nincs javasolt érték 0,25 mg 0,25 mg Szelén 0,07 mg Nincs javasolt érték 0,08 mg Ffi: 0,075 mg Nő: 0,06 mg Fluor Nincs javasolt érték Nincs javasolt érték

megnevezés Kvit (ug) karotin (mg) E-vit (mg) B1- vit (ug) B2- vit (ug) B6- vit (mg) biotin (ug) folsav (ug) C-vit (mg) niacim (mg) alma 2,5 0,05 0,6 50 50 0,07 1,0 6 5 0,5 csipkebogyó 90 - - 100 - - - - 400 - dió - 0.05 24,7 400 100 0,34 6,3 33 25 0,1 kajszibarac k - 1,8 0,5 20 30 0,06 1,7 33 10 0,7 málna - 0,08 1,4 20 30 0,05 2,3 - 30 0,4 meggy - 0,3 - 50 20 0,05 0,8 - 10 0,3 mogyoró - 0,03 28 400 500 0,19 34 30 6 1,0 õszibarack - 0,4 0,6 20 20 0,07 1,8 2,5 7 0,9 vörös ribizke - 0,04 0,2 40 30 0,02 4,2 - 30 0,2 fekete ribizke - 0.1 1,0 60 10 0,02 2,4 - 160 0,3 szõlõ - 0,3 - 50 50 1,4 5,2 - 5 0,4 szilva - 0,2 0,8 50 20 0,04 0,1 0,9 6 0,5 3. táblázat A felnõtt lakosság napi vitaminszükséglete K-vit (ug) A-vit (mg) E-vit (mg) B1-vit (ug) B2-vit (ug) B6-vit (mg) biotin (ug) folsav (ug) C-vit (mg) niacim (mg) 65 0,8 12 1,3 15 2 60 200 60 1,7 A VITAMINOK

---

[1] Pl. Bartók Béla Zene húros hangszerekre ütőkre és cselesztára című műve első tételének szerkezete a Fibonacci-sorozatra épül.

[2] Az OEIS (The On-Line Encyclopedia of Integer Sequences) katalógusban az A000045-ös sorszámot viseli. A *http://oeis.org/A000045* oldalon hatalmas mennyiségű matematikai érdekesség van felsorolva.

[3] Az osztályok közt futó élek az osztályokon parciális rendezést adnak meg, azaz egy reflexív, antiszimmetrikus és tranzitív relációt.

[4] Az $\{ (x,y) \in \mathbb{R}^2 \mid y \leqslant 0 \}$ és az $\{ (x,y) \in \mathbb{R}^2 \mid y \geqslant \frac{1}{x} \}$ halmazok zártak és diszjunktak, de nem szeparálhatók.

[5] Bit: az angol binary digit kifejezésből képzett szó, ami magyarul bináris, azaz kettes számrendszerbeli számot jelent. A szoftver (software) szót is megalkotó John W. Tukey ötlete.

[6] Az ASCII-kód (American Standard Code for Information Interchange) 7-hosszú, de egy 0-val az elején kiegészítve 8 biten (1 bájton) tárolható kód. Az angol nyelv betűi, írásjelei, és néhány számítógépet vezérlő karakter van benne kódolva. Pl. a "z" betű ASCII-kódja 01111010, decimális alakban 122.

[7] A BCD-kód (binary-coded decimal) decimális számok egyik szokásos kódolása, mely a szám kettes számrendszerbe való átírása helyett a számjegyenként való kódolást választja. Több változata is van, a legegyszerűbbikben minden

számjegynek 4-4 bit felel meg, így a 16 lehetséges 4-hosszú kódszó helyett csak tízet használ: a 0, 1,..., 9 jegyek kódja rendre 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001. Így az 561 BCD-kódja három kódvektorból áll: $0101\ 0110\ 0001$. A kettes számrendszerbeli alak 1000110001.

[8] A ternér Golay-kódot Golay előtt 2 évvel, 1947-ben Virtakallio publikálta a Veikaaja című fociújságban TOTO-kulcs készítéséhez.

[9] Sztöchiometria: a kémiai reakciók során tapasztalható tömeg- és térfogatviszonyok törvényszerűségeivel foglalkozik (az alapanyag és mérték jelentésű görög sztoicheión és metron szavakból).

[10] Bár a HITS (Hyperlink-Induced Topic Search) látszólag többre lehet képes a PageRank-nél, bonyolultsága miatt kevésbbé terjedt el. Az *www.Ask.com* használja.

[11] A felhasznált képek az Olivetti Research Laboratoryban készültek 1992 és 94 között, és szabadon letölthetők a*http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html* oldalról. Felhasználásuk kizárólagos célja egyszerű lineáris algebrai ismeretek szemléltetése, nem az arcok eltorzítása.