Jordan-mátrix hatványozása

Elég Jordan-blokkokra:

$$J = \begin{bmatrix} \lambda & 0 & \dots & 0 \\ 1 & \lambda & \dots & 0 \\ & \ddots & \ddots & \\ 0 & \dots & 1 & \lambda \end{bmatrix}_{n\times n} = \lambda I + N, \text{ ahol } N = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ & \ddots & \ddots & \\ 0 & \dots & 1 & 0 \end{bmatrix}.$$

$J^m = \sum\limits_{k=0}^{n} \binom{m}{k} N^k \lambda^{m-k}$, ahol N^k-ban ugyanúgy egy főátlóval párhuzamos 1-es sor van, mint N-ben, csak k-val a főátló alatt. Ebből leolvashatók a J^m elemei, amelyek a főátlóval párhuzamos sávokban ugyanazok:

$$J^m = \begin{bmatrix} \lambda^m & 0 & 0 & \dots & 0 \\ \binom{m}{1}\lambda^{m-1} & \lambda^m & 0 & \dots & 0 \\ \binom{m}{2}\lambda^{m-2} & \ddots & \ddots & & \\ & \ddots & \ddots & & \\ & & & & \lambda^m \end{bmatrix} = \begin{bmatrix} p(\lambda) & 0 & 0 & \dots & 0 \\ \frac{1}{1!}p'(\lambda) & \ddots & 0 & \dots & 0 \\ \frac{1}{2!}p''(\lambda) & \ddots & \ddots & & \\ & \ddots & \ddots & & \\ \dots & \dots & & \frac{1}{1!}p'(\lambda) & p(\lambda) \end{bmatrix},$$

ahol $p(x) = x^m$, és az ij helyen levő elem $\frac{1}{(i-j)!}p^{(i-j)}(\lambda)$, ha $i \geq j$, és 0 különben. Ebből tetszőleges $p(x)$ polinomra, sőt bármely Taylor-sorba fejthető $f(x)$ függvényre hasonló képlettel kiszámítható $f(J)$, és abból $f(A)$ is.

Ennek egy alkalmazása a lineáris differenciálegyenlet-rendszerekre:

$$\dot{\mathbf{x}} = A\mathbf{x}, \ \mathbf{x} = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix}$$

megoldása $\mathbf{x} = e^{At} \cdot \mathbf{c}$ alakú ($\mathbf{c}$ tetszőleges konstans vektor), és ez kiszámítható e^{Jt}-ből.

Skalárszorzat

K^n-ben standard skalárszorzat:

$$\mathbf{u}^T \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i$$

(a K^n elemeit oszlopvektorokként írva.)

Általánosabban:

Def. szimmetrikus bilineáris függvény:
$\langle\ ,\ \rangle : V \times V \to K$,
ami mindkét változóban lineáris:
$\langle \mathbf{u}+\mathbf{u}', \mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{u}', \mathbf{v}\rangle$
$\langle \mathbf{u}, \mathbf{v}+\mathbf{v}'\rangle = \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{u}, \mathbf{v}'\rangle$
$\langle \lambda\mathbf{u}, \mathbf{v}\rangle = \lambda\langle \mathbf{u}, \mathbf{v}\rangle$
$\langle \mathbf{u}, \lambda\mathbf{v}\rangle = \lambda\langle \mathbf{u}, \mathbf{v}\rangle$
és szimmetrikus:
$\langle \mathbf{u}, \mathbf{v}\rangle = \langle \mathbf{v}, \mathbf{u}\rangle$

Pl.: **1.** K^n-en a standard skalárszorzat
$\mathbb{R}^2$-en és $\mathbb{R}^3$-ön a geometriai skalászorzat
2. $C[0,1]$-en $\langle f, g \rangle = \int_0^1 f(x)g(x)\,\mathrm{d}x$
3. K^n-en egy $A \in K^{n\times n}$ mátrixszal, amelyre $A^T = A$: $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T A\mathbf{y}$.
Ez nyilván lineáris, és $\mathbf{y}^T A\mathbf{x} = (\mathbf{x}^T A^T \mathbf{y})^T = (\mathbf{x}^T A\mathbf{y})^T = \mathbf{x}^T A\mathbf{y}$, mert 1×1-es mátrix transzponáltja önmaga.

Def. **u merőleges (ortogonális)** $\mathbf{v}$-re (jele: $\mathbf{u}\perp\mathbf{v}$), ha $\langle \mathbf{u}, \mathbf{v} \rangle = 0$.
$\mathbf{v}_1, \mathbf{v}_2, \ldots$ **ortogonális rendszer**, ha $\mathbf{v}_i \perp \mathbf{v}_j$ $\forall i \neq j$
ortonormált rendszer, ha ortogonális, és $\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 1$ $\forall i$

Állítás. Ha $\{ \mathbf{b}_1, \ldots, \mathbf{b}_n \}$ ortonormált rendszer, akkor bázis is, és $\mathbf{v} = \sum x_i \mathbf{b}_i$-re $x_j = \langle \mathbf{v}, \mathbf{b}_j \rangle$ meghatározza a koordinátákat.

Bizonyítás. $\langle \mathbf{v}, \mathbf{b}_j \rangle = \sum x_i \langle \mathbf{b}_i, \mathbf{b}_j \rangle = x_j \cdot 1 = x_j$, és ha $\mathbf{v} = \sum \lambda_i \mathbf{b}_i = \mathbf{0}$, akkor $0 = \langle \mathbf{v}, \mathbf{b}_j \rangle = x_j$ $\forall j$. □

Megjegyzés. Kicsit általánosabban is kijön a fentiekből: ha $\mathcal{H} = \{ \mathbf{b}_1, \mathbf{b}_2, \ldots, \}$ ortogonális rendszer, és $\langle \mathbf{b}_i, \mathbf{b}_i \rangle \neq 0$ $\forall i$, akkor $\mathcal{H}$ független is.

Pl.: 2π periódusú valós folytonos fv.-ek között az $\langle f, g \rangle = \int_0^{2\pi} f(x)g(x)\,\mathrm{d}x$ bilineáris függvényre nézve
$\{ 1, \sin x, \cos x, \sin 2x, \cos 2x, \ldots \}$
végtelen ortogonális rendszer, és
$\{ \frac{1}{\sqrt{2\pi}}, \frac{1}{\sqrt{\pi}} \sin x, \frac{1}{\sqrt{\pi}} \cos x, \frac{1}{\sqrt{\pi}} \sin 2x, \frac{1}{\sqrt{\pi}} \cos 2x, \ldots \}$
ortonormált rendszer. (Fourier-sorfejtésnél használjuk, csak ott ∞ összegekre is működik az összefüggés a koordináták meghatározására.)

Def. $S \subseteq V$-re $S^\perp = \{ \mathbf{v} \in V \mid \mathbf{u}\perp\mathbf{v} \ \forall \mathbf{u} \in S \} \leq V$. Nyilván $S^{\perp\perp} \supseteq S$

Def. Egy szimmetrikus bilineáris függvény **elfajuló**, ha $V^\perp \neq 0$.

Állítás. 1) A standard skalárszorzat K^n-en nem elfajuló.
2) Az $A \in K^{n\times n}$ szimmetrikus mátrix által megadott $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T A\mathbf{y}$ bilineáris függvény K^n-en akkor és csak akkor elfajuló, ha $|A| = 0$.

Bizonyítás. 1) Ha $\mathbf{v} = (x_1, \ldots, x_n)^T \neq \mathbf{0}$, akkor van olyan i, amelyre $x_i \neq 0$, és akkor $\langle \mathbf{v}, \mathbf{e}_i \rangle = x_i \neq 0$, ahol $\mathbf{e}_i$ az i. standard bázisvektor (az i. helyen 1, mindenhol máshol 0). Tehát $\mathbf{v} \notin V^\perp$.
2) Egy $\mathbf{v} \in V$ vektorra:

$$\begin{gathered} \mathbf{v} \in V^\perp \Leftrightarrow \\ \langle \mathbf{u}, \mathbf{v} \rangle = 0 \ \forall\ \mathbf{u} \Leftrightarrow \\ \mathbf{u}^T A\mathbf{v} = 0 \ \forall\ \mathbf{u} \Leftrightarrow \\ A\mathbf{v} = \mathbf{0} \text{ (az 1) miatt)} \end{gathered}$$

Tehát

$$\begin{gathered} V^\perp \neq 0 \Leftrightarrow \\ \exists \mathbf{v} \neq \mathbf{0} : \ A\mathbf{v} = \mathbf{0} \Leftrightarrow \\ A \text{ nem invertálható} \Leftrightarrow \\ |A| = 0 \end{gathered}$$

□

Tétel. Legyen $\langle\ ,\ \rangle$ szimmetrikus bilineáris függvény. Ha $V^\perp = 0$, akkor $U \le V$-re $\dim V = \dim U + \dim U^\perp$. Speciálisan K^n standard skalárszorzatára igaz az összefüggés.

Bizonyítás. Legyen V bázisa $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, U bázisa $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$.

$$A = \begin{bmatrix} & \vdots & \\ \dots & \langle \mathbf{u}_i, \mathbf{v}_j \rangle & \\ & & \end{bmatrix}_{k\times n} \qquad A^T = \begin{bmatrix} & \vdots & \\ \dots & \langle \mathbf{v}_i, \mathbf{u}_j \rangle & \\ & & \end{bmatrix}_{n\times k}$$

a $\varphi : V \to K^k$, $\mathbf{v} \mapsto \begin{bmatrix} \langle \mathbf{u}_1, \mathbf{v} \rangle \\ \ddots \\ \langle \mathbf{u}_k, \mathbf{v} \rangle \end{bmatrix}$ mátrixa

$\operatorname{Ker} \varphi = U^\perp$

$\Rightarrow \operatorname{rang} A = \dim V - \dim U^\perp$

a $\psi : U \to K^n$, $\mathbf{u} \mapsto \begin{bmatrix} \langle \mathbf{v}_1, \mathbf{u} \rangle \\ \ddots \\ \langle \mathbf{v}_n, \mathbf{u} \rangle \end{bmatrix}$ mátrixa

$\operatorname{Ker} \psi = 0$, mert $V^\perp = 0$

$\Rightarrow \operatorname{rang} A^T = \dim U$

Mivel $\operatorname{rang} A = \operatorname{rang} A^T$, azt kaptuk, hogy $\dim V - \dim U^\perp = \dim U$, azaz $\dim V = \dim U + \dim U^\perp$. □

Megjegyzés. Az előző állításból nem következik, hogy $V = U \oplus U^\perp$, mert megtörténhet, hogy $U \cap U^\perp \neq 0$, pl. $\mathbb{F}_2^2$-ben $U = \langle (1,1) \rangle$-re.

Párosváros, páratlanváros Ⓑ

Két n lakosú városban klubok vannak. Két különböző klubnak nem lehet azonos a tagsága.

1) **Páratlanvárosban** minden klubnak páratlan sok tagja van, és bármely két különböző klubnak páros sok közös tagja van. Legföljebb hány klub lehet a városban?

   Megoldás: klub $\mapsto \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}_2^n$ ($x_i = 1$, ha az i. lakos tagja a klubnak, 0, ha nem.)

   Két klub vektorának skalárszorzata a közös tagok száma modulo 2.

   $\Rightarrow$ a klubok vektorai ortonormált rendszert, következésképpen független rendszert alkotnak $\mathbb{F}_2^n$-ben $\Rightarrow$ A klubok száma $\le n$, és ez meg is valósítható 1-tagú klubokkal.

2) **Párosvárosban** minden klubnak páros sok tagja van, és bármely két különböző klubnak is páros sok közös tagja van. Legföljebb hány klub lehet ebben a városban?

   Megoldás: A klubokat az előzőhöz hasonló módon $\mathbb{F}_2^n$ vektoraival reprezentáljuk. Legyen U a klubok vektorai által generált altér, és $r = \dim U$. Ekkor a feltétel szerint $U^\perp \ge U$. Viszont tudjuk, hogy $\dim V = \dim U + \dim U^\perp$, tehát $n - r \ge r$, amiből $r \le [n/2]$, és így a klubok száma $\le |U| \le 2^{[n/2]}$. Ez meg is valósítható, ha az emberekből párokat alkotunk (ha n páratlan, akkor egy ember kimarad), és a párok összes lehetséges részhalmazát vesszük.

Lineáris kódok

Üzenetet akarunk küldeni valamennyire zajos csatornán úgy, hogy ha nem túl sok a hiba, akkor azt észre lehessen venni, illetve javítani lehessen. Módszer: a szöveg részleteit olyan kódszavakká alakítjuk, amelyek közül semelyik kettő nincs túl közel egymáshoz (elegendő számú karakterben különböznek). A kódszavak tekinthetők egy véges test fölötti vektortér vektorainak. A kód lineáris, ha a kódszavak alteret alkotnak.

Def. K véges test: **abc** (például $K = \mathbb{F}_2 = \{0, 1\}$)
kódszavak: $U \leq K^n$ elemei
kódhossz: n
Hamming-távolság: $d(\mathbf{u}, \mathbf{v}) = |\{i \mid u_i \neq v_i\}|$
Hamming-súly: $s(\mathbf{u}) = |\{i \mid u_i \neq 0\}|$
Ekkor $d(\mathbf{u}, \mathbf{v}) = s(\mathbf{u} - \mathbf{v})$.
dimenzió: $k = \dim U$
Tekinthetjük úgy, hogy a kódolandó szavak k hosszúak a kódolás előtt, és n hosszúak a kódolás után
kódsebesség: $\frac{k}{n}$
kódtávolság: $d = \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in U,\ \mathbf{u} \neq \mathbf{v}\} = \min\{s(\mathbf{u}) \mid \mathbf{0} \neq \mathbf{u} \in \mathbf{U}\}$
Ekkor a kód $\left[\frac{d-1}{2}\right]$-**hibajavító**,
azaz ennyi hibát ki lehet javítani, mert van egy egyértelmű, a hibásan kódolt szóhoz legközelebbi kódszó, és
$(d-1)$-**hibajelző**,
azaz ha legföljebb $d-1$ hiba van, akkor a kapott szó nem egyezik meg semelyik kódszóval, tehát látszik, hogy hibás.

Pl.: 1. triviális kód:
$U = K^n$, $\mathbf{v} \mapsto \mathbf{v}$ a kódolás, $d = 1$ ($\Rightarrow$ nincs hibajavítás, de még hibajelzés sem.)

2. ismétlő kód:
kétszerezés: $a \mapsto (a, a)$, $d = 2$, a kód 1-hibajelző
háromszorozás: $a \mapsto (a, a, a)$, $d = 3$, a kód 1-hibajavító
általánosan d-szerezés: $a \mapsto (a, a, \ldots, a)$, a kódtávolság d, a kód $(d-1)$-hibajelző, $[\frac{d-1}{2}]$-hibajavító, de túl lassú: a kódsebesség $\frac{1}{d}$

3. paritáskód: $(a_1, \ldots, a_{n-1}) \mapsto (a_1, \ldots, a_{n-1}, a_n)$, ahol $a_1 + \ldots + a_{n-1} + a_n = 0$. Itt $k = n-1$, $d = 2$, a kód 1-hibajelző, de a kódsebesség nagy: $\frac{n-1}{n}$.

Hadamard-kódok

$\mathbb{F}_2$ fölött, $n = 2^m$ hosszú kód, $k = m + 1$. A kódolás:

$$\mathbf{v} = (\alpha_1, \ldots, \alpha_m, \beta) \mapsto f_{\mathbf{v}} : \mathbb{F}_2^m \to \mathbb{F}_2$$
$$(x_1, \ldots, x_m) \mapsto \alpha_1 x_1 + \ldots + \alpha_m x_m + \beta$$

A kódszóként kapott affin függvények vektorként is írhatók: az $\mathbb{F}_2^m$ összes elemét sorbarendezzük, és az $f_{\mathbf{v}}$-be való behelyettesítésük eredményét írjuk egy 2^m hosszú vektorba. Ez altér $\mathbb{F}_2^{2^m}$-ben, mert affin függvények összege és skalárszorosa is ilyen.

Pl.: $m = 2$-re $\mathbb{F}_2^m = \{(0,0), (0,1), (1,0), (1,1)\}$ és a kódolás $\mathbf{v} = (1,1,1) \mapsto f_{\mathbf{v}} = x_1 + x_2 + 1$, azaz a kódszó (az $\mathbb{F}_2^m$ előre megadott sorbarendezését használva) $(1,0,0,1)$.

Állítás. Ⓑ $d = 2^{m-1}$

Bizonyítás. Azt kell belátni, hogy minden $\neq \mathbf{0}$ kódszóban legalább 2^{m-1} darab 1-es van.
1. eset: Ha $\exists i : \alpha_i \neq 0$, akkor $\{f_{\mathbf{v}}(x_1, \ldots, 0, \ldots, x_m) = f_{\mathbf{v}}(x_1, \ldots, 1, \ldots, x_m)\} = \{0, 1\}$ (ahol a két vektor csak az i. komponensben különbözik), tehát a behelyettesítési értékeknek pontosan a fele $1 \Rightarrow s(f_{\mathbf{v}}) = 2^{m-1}$.
2. eset: $\alpha_1 = \ldots = \alpha_m = 0$, de akkor $\beta = 1$, és $f_{\mathbf{v}} \equiv 1$, ezért ekkor $s(f_{\mathbf{v}}) = 2^m$. □