Mátrixrang ekvivalens leírásai

$A \in K^{m\times n}$-re ekvivalens:

(i) $\operatorname{rang} A = r$;
(ii) $\mathbf{x} \mapsto A\mathbf{x}$ rangja r;
(iii) A oszloptere r-dimenziós;
(iv) A sortere r-dimenziós;
(v) A lépcsős alakjában r db $\neq \mathbf{0}$ sor van (azaz r db vezérelem van);
(vi) A-ban a legnagyobb méretű $\neq 0$ aldetermináns $r \times r$-es.

Invertálhatóság

$A \in K^{n\times n}$-re ekvivalens:

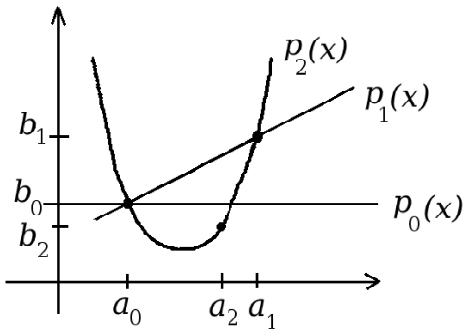
(i) A invertálható;
(ii) $f : K^n \to K^n$, $f : \mathbf{x} \mapsto A\mathbf{x}$ izomorfizmus;
(iii) $|A| \neq 0$;
(iv) A redukált lépcsős alakja I;
(v) $\operatorname{rang} A = n$;
(vi) minden $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek van megoldása;
(vii) az $A\mathbf{x} = \mathbf{0}$ egyenletrendszernek csak triviális megoldása van.

Az inverz kiszámítása Gauss-módszerrel:

$$[A|I] \mapsto\mapsto\mapsto [I|A^{-1}].$$

Polinominterpoláció

Ⓑ K test, $a_0, \dots, a_n, b_0, \dots, b_n \in K$, $a_0, \dots, a_n$ különbözők $\Rightarrow \exists! p(x) \in K[x]_{\leq n}$: $p(a_i) = b_i$ $\forall i$.



Bizonyítás. $f : K[x]_{\leq n} \to K^{n+1}$, $f : p(x) \mapsto \begin{bmatrix} p(a_0) \\ \vdots \\ p(a_n) \end{bmatrix}$ lineáris leképezés. $\operatorname{Ker} f = 0$, ui. ha $p(x) \in \operatorname{Ker} f \Rightarrow p(a_0) = \dots = p(a_n) = 0 \Rightarrow p(x) = (x - a_0)\cdots(x - a_n)q(x)$, de $\deg p \leq n$, így $p(x) = 0$. $\dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim K[x]_{\leq n} = n + 1$ miatt $\dim \operatorname{Im} f = n + 1$, azaz f

szürjektív, és $\operatorname{Ker} f = 0$ miatt injektív is, vagyis f izomorfizmus. Ez pontosan azt jelenti, hogy minden $\mathbf{b} = \begin{bmatrix} b_0 \\ \vdots \\ b_n \end{bmatrix}$-hez pontosan egy $p(x) \in K[x]_{\leq n}$ van, amelyre $f(p(x)) = \mathbf{b}$. $\square$

Newton-féle interpoláció (ld. még: Lagrange-féle) Adott $a_0, \ldots, a_n, b_0, \ldots, b_n$-hez legyen $p_i(x) \in K[x]_{\leq i}$ olyan, ami $a_0, \ldots, a_i$-ben jó. $p_0(x) \equiv b_0$. Ha p_i megvan, akkor

$$p_{i+1}(x) = p_i(x) + A \cdot (x - a_0) \cdots (x - a_i)$$

szintén jó a_i-ig tetszőleges $A \in K$-ra, ráadásul $\deg p_{i+1}(x) \leq i + 1$. Továbbá A megválasztható úgy, hogy $p_{i+1}(a_{i+1}) = b_{i+1}$ (ha behelyettesítjük a_{i+1}-et, akkor A együtthatója nem 0, mivel az a_j-k különbözők). Tehát megfelelő $p_n(x)$ is létezik.

Megjegyzés: A Newton-féle interpolációval könnyű javítani az interpolációt a már meglevő interpolációs polinom helyett, ha még néhány pontbeli értéket megtudunk.

Shamir-féle titokmegosztás

n ember között úgy akarjuk megosztani egy titok (legyen ez egy c természetes számban elkódolva) részleteit, hogy közülük bármely k ember együtt kitalálhassa a titkot, de ha csak $k - 1$ ember osztja meg egymással az információt, ők ne tudhassanak meg semmit a titokról.

Megoldás: Legyen $p > c$ prím, $q(x) \in \mathbb{F}_p[x]_{<k}$, amelyre $q(0) = c$ (azaz c a konstans tag). Az i. ember a $q(i) \in \mathbb{F}_p$ értéket kapja meg ($i = 1, \ldots, n$). Ekkor k ember együtt k helyettesítési értéket tud, ami az interpolációs tétel szerint egyértelműen meghatározza a polinomot. De $k - 1$ embernek adott helyettesítési érték mellett $q(0)$ még akármi lehet, akkor is van hozzá interpoláló, k-nál kisebb fokú polinom.

Kérdés: Miért $\mathbb{F}_p$? Miért nem $\mathbb{Z}[x]$ fölötti polinommal dolgozunk? Erre nem igaz, hogy $k-1$ helyettesítési érték mellett $p(0)$ bármi lehet: esetleg csak $\mathbb{Q}$ fölötti interpoláló polinom létezik, de $\mathbb{Z}$ fölötti nem.

Áttérés másik bázisra

Legyen $\mathcal{B} = \{ \mathbf{b}_1, \ldots, \mathbf{b}_n \}$ és $\mathcal{B}' = \{ \mathbf{b}'_1, \ldots, \mathbf{b}'_n \}$ a V két bázisa. $P := \big[[\mathbf{b}'_1]_{\mathcal{B}} \big| \ldots \big| [\mathbf{b}'_n]_{\mathcal{B}} \big]$ az áttérés mátrixa, ezzel

$[\mathbf{v}]_{\mathcal{B}} = P[\mathbf{v}]_{\mathcal{B}'}$, azaz $P = [id]_{\mathcal{B}',\mathcal{B}}$, és
$P^{-1}[\mathbf{v}]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}'}$.

Pl. (az első előadás koordinátázós példája) $\mathcal{B} = \{(1,0),(0,1)\}$ az $\mathbb{R}^2$ eredeti bázisa (a standard bázis), $\mathcal{B}' = \{(1,1),(-1,1)\}$. Számítsuk ki a $[(2,1)]_{\mathcal{B}'}$ koordinátavektort!

Az áttérés mátrixa $P = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$.

$$[P|I] = \left[\begin{array}{cc|cc} 1 & -1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right] \mapsto \left[\begin{array}{cc|cc} 1 & -1 & 1 & 0 \\ 0 & 2 & -1 & 1 \end{array}\right] \mapsto \left[\begin{array}{cc|cc} 1 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & -\frac{1}{2} & \frac{1}{2} \end{array}\right] = [I|P^{-1}].$$

$$[(2,1)]_{\mathcal{B}'} = P^{-1} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 3/2 \\ -1/2 \end{bmatrix}$$

Lineáris leképezés új bázispárban

$(\mathcal{B},\mathcal{C})$-ről $(\mathcal{B}',\mathcal{C}')$-re való áttérés (az áttérés mátrixa P, illetve Q), $[f]_{\mathcal{B},\mathcal{C}} = A$, $[f]_{\mathcal{B}',\mathcal{C}'} = A'$. Ekkor $A' = Q^{-1}AP$:

$$[f(\mathbf{v})]_{\mathcal{C}'} \xleftarrow{Q^{-1}} [f(\mathbf{v})]_{\mathcal{C}} \xleftarrow{A} [\mathbf{v}]_{\mathcal{B}} \xleftarrow{P} [\mathbf{v}]_{\mathcal{B}'}$$

Lineáris transzformáció új bázisban

$\mathcal{B}$, $\mathcal{B}'$ bázisai V-nek, $f : V \to V$, $[f]_{\mathcal{B}} = A$, $[f]_{\mathcal{B}'} = A'$, P az áttérés mátrixa.
Ekkor $A' = P^{-1}AP$.

Pl. (az első előadásból) $z \to \overline{z}$ a standard $\mathcal{B} = \{\, 1, i \,\}$ bázisban $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Írjuk fel a mátrixot a $\mathcal{B}' = \{\, i, 1+i \,\}$ bázisban is!
Az áttérés mátrixa $P = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. $P^{-1} = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$, és a transzformáció mátrixa $\mathcal{B}'$-re nézve $A' = P^{-1}AP = \begin{bmatrix} -1 & -2 \\ 0 & 1 \end{bmatrix}$.

Def. $A, B \in K^{n\times n}$ **hasonlók** (jele: $A \sim B$), ha $\exists P$ invertálható, amelyre $B = P^{-1}AP$. Másképpen: A és B ugyanannak a transzformációnak a mátrixai két bázisban (P oszlopai adják meg az új bázist a régi szerint koordinátázva).

Def. $\mathbf{v} \in V_K$ az $f : V \to V$ lineáris transzformáció **sajátvektora**, ha $\mathbf{v} \neq \mathbf{0}$, és van olyan $\lambda \in K$, amelyre $f(\mathbf{v}) = \lambda\mathbf{v}$, azaz $f(\mathbf{v})$ párhuzamos $\mathbf{v}$-vel (beleértve az $f(\mathbf{v}) = \mathbf{0}$ esetet is). Ekkor λ a $\mathbf{v}$-hez tartozó **sajátérték**. f **spektruma** a sajátértékeinek a halmaza. A λ sajátértékhez tartozó **sajátaltér** $V_\lambda = \{\, \mathbf{v} \in V \mid f(\mathbf{v}) = \lambda\mathbf{v} \,\}$.

Pl. Egy origón átmenő síkra való merőleges vetítés sajátvektorai a sík $\neq \mathbf{0}$ vektorai (1 sajátértékkel), és a síkra merőleges $\neq \mathbf{0}$ vektorok (0 sajátértékkel).

Def. Egy $A \in K^{n\times n}$ **mátrix sajátvektorai, sajátértékei és spektruma** az $\mathbf{x} \mapsto A\mathbf{x}$ transzformáció sajátvektorai, sajátértékei, illetve spektruma.

Diagonalizálás (spektrálfelbontás)

$A \in K^{n\times n}$, $f : K^n \to K^n$, $f : \mathbf{x} \mapsto A\mathbf{x}$. Ha $\exists$ az f sajátvektoraiból álló bázis: $\mathcal{B} = \{\, \mathbf{b}_1, \dots, \mathbf{b}_n \,\}$, $\lambda_1, \dots, \lambda_n$ sajátértékekkel, akkor

$$[f]_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ 0 & 0 & \dots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \dots & \lambda_n \end{bmatrix} = D$$

diagonális mátrix, és $P = [\mathbf{b}_1 | \dots \mathbf{b}_n]$-re $D = P^{-1}AP$, azaz $A = PDP^{-1}$ az A spektrálfelbontása.

Def. $A \in K^{n\times n}$ **diagonalizálható**, ha $\exists P$ invertálható, amelyre $P^{-1}AP$ diagonális, azaz $\exists$ A sajátvektoraiból álló bázis K^n-ben.

Diagonalizálható mátrix hatványozása

Ha $A = PDP^{-1}$, akkor $A^k = (PDP^{-1})(PDP^{-1})\cdots(PDP^{-1}) = PD^kP^{-1}$, és diagonális mátrix hatványát megkapjuk úgy, hogy az átlós elemeit hatványozzuk.

Sajátértékek és sajátvektorok kiszámítása

$\exists \mathbf{v} \neq \mathbf{0} : A\mathbf{v} = \lambda\mathbf{v} \;\Leftrightarrow$

$\exists \mathbf{v} \neq \mathbf{0} : (A - \lambda I)\mathbf{v} = \mathbf{0} \;\Leftrightarrow$

$|A - \lambda I| = 0$

Karakterisztikus polinom

Def. A **karakterisztikus polinomja**

$$k_A(x) = \begin{vmatrix} a_{11} - x & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - x & \dots & a_{2n} \\ & & \ddots & \\ a_{n1} & a_{n2} & \dots & a_{nn} - x \end{vmatrix}$$

A karakterisztikus polinom tulajdonságai:

- $k_A(x)$ gyökei az A sajátértékei
- $k_A(x) = (-1)^n x^n + (-1)^{n-1}(\operatorname{tr} A)x^{n-1} + \ldots + |A|$, ahol $\operatorname{tr} A = a_{11} + \ldots + a_{nn}$ az A mátrix **nyoma**
- Ha $k_A(x)$ lineáris faktorokra bontható: $k_A(x) = (-1)^n(x - \lambda_1)\ldots(x - \lambda_n)$ (λ_i-k az A sajátértékei multiplicitással), akkor $\operatorname{tr} A = \lambda_1 + \ldots + \lambda_n$ és $|A| = \lambda_1 \cdots \lambda_n$.
- $A \sim B \Rightarrow k_A(x) = k_B(x)$,
  ui. $|P^{-1}AP - xI| = |P^{-1}AP - xP^{-1}IP| = |P^{-1}(A - xI)P| = |P|^{-1} \cdot |A - xI| \cdot |P| = |A - xI|$.

Pl.

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

$|A - xI| = \begin{vmatrix} 1 - x & 2 \\ 0 & 2 - x \end{vmatrix}$

$= (x - 1)(x - 2)$

s.é.: $\lambda = 1, 2$

Mindegyikhez van s.vektor, független $\Rightarrow$

$\exists$ belőlük bázis $\Rightarrow$

A diagonalizálható

$B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$|B - xI| = x^2 + 1$

nincs valós gyök $\Rightarrow$

B nem diag.-ható $\mathbb{R}$ fölött

(de $\mathbb{C}$ fölött igen)

$C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$|C - xI| = (x - 1)^2$

s.é. $\lambda = 1$

$(C - 1 \cdot I)\mathbf{v} = \mathbf{0}$, $\mathbf{v} = ?$

$\left[\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right] \Rightarrow \mathbf{v} = \begin{bmatrix} t \\ 0 \end{bmatrix}$

Nincs két ftln s.vektor $\Rightarrow$

C nem diag.-ható

($\mathbb{C}$ fölött sem)