Alkalmazott algebra - bevezető

Ivanyos Gábor

2011 ősz

A Pagerank-ről

- Sergey Brin, Larry Page (1998)
- eljárás weblapok rangsorolására
- a linkek alapján készült gráf elemzésével

Első megközelítés

- **Elv:** az a lap az értékes, amelyre sok értékes lap mutat.
- n weblap
- i. lap súlya (értéke) a t-edik időpontban: v_i^t $(t = 0, 1, 2, \ldots)$
- kezdetben $v_i^0 = \frac{1}{n}$ $(i = 1, \ldots, n)$
- $t \to t+1$ időpont:

$$v_i^{t+1} = \sum_{j=1}^{n} a_{ij} v_j^t,$$

- ahol $a_{ij} = \frac{\#j \to i \text{ linkek}}{\#j \to \text{ linkek}}$
- $\sim$ milyen valószínűséggel merre jár a linkek mentén véletlenül továbblépő szörfölő

Első megközelítés

- vektor/mátrix segítségével: $v^t = \begin{pmatrix} v_1^t \\ \vdots \\ v_n^t \end{pmatrix}$, $A = (a_{ij})$,

$$v^{t+1} = Av^t$$

- az "ideális" weblap-súlyok vektora:

$$v^\infty = \lim_{t\to\infty} v^t, \qquad \text{ha létezik}$$

- Problémák:
  - vannak weblapok, ahonnan nincs egy link se
  - lehetnek weblapokból álló csoportok, ahonnan nincs kiút
  - lehet ilyen csoport pl. egy irányított kör

  ekkor csak kivételes v^0-kra van konvergencia!

Módosított modell - a türelmetlen szörfölő

- **Módosított mátrix:** A helyett

$$A' = (1-\alpha)A + \alpha\frac{1}{n}E,$$

ahol $E = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$.

- Szemléletesen: a türelmetlen szörfölő α valószínűséggel megunja a barangolást, és egy véletlenül választott lapra lép.
- Erre már létezik

$$\lim_{t\to\infty} v^t := \lim_{t\to\infty} {A'}^t v^0$$

- **Pagerank** rangsora ${A'}^K v_0$ súlyai szerint, ahol K elég nagy.

Test

- **Informálisan:** Egy négy alapművelettel $(+, -, \cdot, /)$ ellátott halmaz, amelyen a racionális számokon megszokott azonosságok teljesülnek.
- **Formálisan:** egy $\mathbb{F}$ halmaz két művelettel és két (különböző) kitüntetett elemmel: $+, \cdot$ illetve $0, 1$, amelyekre
  (1) $(x + y) + z = x + (y + z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $(\forall x, y, z \in \mathbb{F})$ (*asszociativitás*)
  (2) $x + y = y + x$, $x \cdot y = y \cdot x$ $(\forall x, y \in \mathbb{F})$ (*kommutativitás*)
  (3) $0 + x = x$, $0 \cdot x = 0$, $1 \cdot x = x$ $(\forall x \in \mathbb{F})$ (0 *neutrális elem*, 1 *egységelem*)
  (4) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ $(\forall x, y, z \in \mathbb{F})$ (*disztributivitás*)
  (5) $\forall x \in \mathbb{F}$-re van $(-x) \in \mathbb{F}$, hogy $x + (-x) = 0$,
  $\forall 0 \neq x \in \mathbb{F}$-re van $x^{-1} \in \mathbb{F}$, hogy $x \cdot x^{-1} = 1$,
  ($+$-ra minden, $\cdot$-ra minden nem-nulla elemnek van inverze)
- **Kivonás, osztás:** Belátható, hogy $-x$ és x^{-1} egyértelmű.
  $x - y := x + (-y)$ és $x/y := x \cdot y^{-1}$.

Példák testekre

- $\mathbb{Q}$ racionális számok
- $\mathbb{R}$ valós számok
- $\mathbb{C}$ komplex számok
- $\mathbb{Z}_p$ vagy $\mathbb{F}_p$: egész számok modulo p prím
  $\mathbb{Z}_2$ másképpen: $\{1 = \text{"igaz"}, 0 = \text{"hamis"}\}$
  $+ =$ "kizáró vagy", $\cdot =$ "és".
- $\mathbb{F}_q$, q elemű test, ahol $q = p^r$ (p prím). Lényegében (azaz: izomorfia erejéig) egyértelmű.
- **Feladat:** legyen $\mathbb{F}$ egy véges test. Ekkor létezik egy (és csak egy) olyan p prímszám, hogy $1 + \ldots + 1(p\text{-szer}) = 0$.

Polinomok

- ***n*-ed fokú egyváltozós polinom:** $f(x) = a_n x^n + \cdots + a_1 x + a_0 \; (a_i \in \mathbb{F}, \; a_n \neq 0)$.
- **gyök** olyan $\alpha \in \mathbb{F}$, amelyre $f(\alpha) = 0$.
- **Fontos tul.:** Egy n-ed fokú polinomnak legfeljebb n gyöke van.
- **Algebra alaptétele:** Minden komplex együtthatós polinomnak van gyöke $\mathbb{C}$-ben (multiplicitással számolva összesen fokszámnyi)

Vektortér $\mathbb{F}$ felett

- Egy V halmaz
  - $+ : V \times V \to V$ (*összeadás*) művelettel,
  - kitüntetett 0 elemmel,
  - $\cdot : \mathbb{F} \times V \to V$ (skalárokkal való *szorzás* vagy *beszorzás*) művelettel,
- amelyekre:
  - $+$ kommutatív és asszociatív, 0 neutrális elemmel,
  - $\cdot$ asszociatív: $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ $(x, y \in \mathbb{F}, v \in V)$
  - $\cdot$ mindkét oldalról disztributív: $(x + y) \cdot (u + v) = x \cdot u + y \cdot u + x \cdot v + y \cdot v$ $(x, y \in \mathbb{F}, u, v \in V)$
- Megj.: Additív inverz V-ben: $-v := (-1) \cdot v$.
- **Fontos példa:** az n hosszú oszlopvektorok $\mathbb{F}^n$ tere

Példák

- S halmaz, $S \to \mathbb{F}$ függvények; értékek szerinti összeadással és beszorzással.
  $\sim$ S elemeivel indexelt táblázatok, $\mathbb{F}$–beli elemekkel kitöltve.
- Spec. eset: $n \times m$-es mátrixok $\mathbb{F}$–beli elemekkel. Műveletek elemenként.
- Speciális eset: $m = 1$, n hosszú **oszlopvektorok.**
- Polinomok. (Összeadás, beszorzás érték szerint ugyanazt adják, mintha az együtthatókon külön-külön hajtanánk végre.)
- n-nél alacsonyabb fokú polinomok.
- $\mathbb{R} \to \mathbb{R}$ folytonos függvények.
- $\mathbb{C}$ az $\mathbb{F} = \mathbb{Q}$ vagy $\mathbb{F} = \mathbb{R}$ felett.

Alterek

- **Lineáris kombináció:** $\alpha_1 v_1 + \ldots + \alpha_n v_n$, ahol $0 \neq v_i$ és $v_i \neq v_j$ ha $i \neq j$.
  Megj. Mindig véges sok tagból álló összeg! Az üres összeg is lin. komb., értéke 0.
- **Altér:** $U \subseteq V$ altere V-nek (jel. $U \leq V$), ha $0 \in U$ is zárt a műveletekre: $u, v \in U, \alpha \in \mathbb{F}$ esetén $u + v, \alpha u \in U$.
  Ekvivalens feltétel: U zárt a lineáris kombinációkra is.
- **Példák:**
  - A legszűkebb altér: $\{0\} = (0)$ (hanyagul: 0),
  - a legtágabb: V.
  - origón átmenő síkok, egyenesek $\mathbb{R}^3$-ben
  - polinomok, folytonos függvények, stb. altere a függvények terében
  - homogén lineáris n-változós egyenletrendszerek megoldásai $\mathbb{R}^n$-ben (Spec. eset: hipersík $\mathbb{R}^n$-ben: egy nem-triviális n változós homogén lineáris egyenlet megoldásai)

Generált (kifeszített) altér

- $S \subseteq V$-re $\langle S \rangle$ a legszűkebb altér, amely tartalmazza S-t.

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} \alpha_i v_i | n \in \mathbb{Z}_{\geq 0}, \alpha_i \in \mathbb{F}, v_i \in S \right\}.$$

- $\langle \emptyset \rangle = \{0\}$, $\langle v \rangle = \langle \{v\} \rangle = \{\alpha v | \alpha \in \mathbb{F}\}$.
- **További példák:**
  - polinomok között az $1, x, x^2, \ldots, x^{n-1}$ monomok az n-nél alacsonyabb fokú polinomok alterét generálják
  - **Feladat:** Mely altered feszítik ki a következő polinomok: $x^3 + x^2 + x$, $x^3 + 2x^2 + 3x$, $x^3 + x$, $x^3 + 3x^2$?

Lineáris függetlenség

- $S \subseteq V$ lineárisan független, ha $n \in \mathbb{Z}_{>0}$, α_i, v_i $(i = 1, \ldots n)$ $\sum_{i=1}^{n} \alpha_i v_i = 0$ esetén az összes $\alpha_i = 0$.
- $\emptyset$ lineárisan független, $\{0\}$ lineárisan összefüggő.
- **Áll.:** Ha S lineárisan független, de $S \cup \{v\}$ lineárisan összefüggő, akkor v (egyértelműen) előáll S–beli elemek lineáris kombinációjaként.
- **Példa:** $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ és $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ lineárisan függetlenek:

$$\alpha \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha + \beta \\ \alpha + \beta + \gamma \end{pmatrix}.$$

Lineáris függetlenség

- **Példa:** $\begin{pmatrix}1\\1\\1\end{pmatrix}$, $\begin{pmatrix}0\\1\\1\end{pmatrix}$ és $\begin{pmatrix}1\\0\\0\end{pmatrix}$ lineárisan összefüggenek:

$$\begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}0\\1\\1\end{pmatrix} - \begin{pmatrix}1\\0\\0\end{pmatrix} = 0.$$

- **Kapcsolat a generált alterekkel:** $S \subseteq V$ lineárisan független $\iff S$ egy irredundáns (tartalmazásra minimális) generátorrendszere az $\langle S \rangle$ altérnek.
- **Feladat:** Lineárisan függetlenek-e a következő polinomok: $x^3 + x^2 + x$, $x^3 + 2x^2 + 3x$, $x^3 + x$, $x^3 + 3x^2$?

Bázis

- Olyan lineárisan független rendszer, amely generálja V-t.
- **Ekvivalens jellemzések:**
  - minimális generátorrendszere V-nek,
  - maximális lineárisan független rendszer V-ben,
  - minden v–beli elem **egyértelműen felírható** a rendszer elemeinek lineáris kombinációjaként.
- **Megj.:** Sorba rendezzük a bázis elemeit, különböző sorrend $\to$ különböző bázis.
- **Példák:**
  - standard bázis $\mathbb{F}^n$-ben $\begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\\vdots\\0\\0\end{pmatrix}, \ldots, \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}$
  - polinomok közt $1, x, x^2, \ldots$

Dimenzió

- $\dim V$, pontosabban $\dim_{\mathbb{F}} V = V$ egy bázisának elemszáma (számossága).
- független a bázis választásától
- **Példák:**
  - ha S véges, akkor $\dim\{S \to \mathbb{F}$ függvények$\} = |S|$
  - spec. eset: $\dim\{n \times m\text{-es mátrixok}\} = nm$
  - $\dim\{\text{polinomok}\} = \infty$ (megszámlálható)
  - $\dim\{n\text{-nél alacsonyabb fokú polinomok}\} = n$
  - $\dim_{\mathbb{R}} \mathbb{C} = 2$, $\dim_{\mathbb{Q}} \mathbb{R} = \dim_{\mathbb{Q}} \mathbb{C} = \infty$ (kontinuum)
  - Ha $\dim_{\mathbb{C}} V = n$, akkor $\dim_{\mathbb{R}} V = 2n$

Az órán általában **csak véges dimenziós** vektorterekkel foglalkozunk.

Lineáris leképezések

- V, W vektorterek $\mathbb{F}$ felett. A $\phi : V \to W$ lekép. **lineáris**, ha

$$\phi(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 \phi(v_1) + \alpha_2 \phi(v_2).$$

- **Konvenció:** elhagyjuk a zárójelet: $\phi v := \phi(v)$.
- **Fontos példa:** A $m \times n$-es mátrix $\mathbb{F}$-beli elemekkel.

$$\phi_A : \mathbb{F}^n \to \mathbb{F}^m, \quad \phi_A v := Av.$$

- **Vektortér-műveletek:** $\phi, \phi' : U \to W$ esetén $(\alpha\phi + \phi')v := \alpha(\phi v) + (\phi' v)$.
- **Kiterjesztés bázisról:** Ha $v_1, \ldots, v_n$ egy bázis V-ben; $w_1, \ldots, w_n \in W$, $\exists! \phi : V \to W$ lin. lekép., hogy $\phi v_i = w_i$ $(i = 1, \ldots, n)$: $\phi \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha_i w_i$.
- A $V \to W$ lin. lekép. terének dimenziója $\dim V \cdot \dim W$.

Lineáris leképezések

- **Speciális esetek:**
  Lineáris függvény: $V \to \mathbb{F}$ lin. lekép.
  Lineáris transzformáció: $V \to V$ lin. lekép.
- **Példák:**
  - $0 \neq u \in \mathbb{R}^n$ rögzített oszlopvektor.
    - A $v \mapsto u^T v$ egy lineáris függvény $\mathbb{R}^n$-en.
    - A $v \mapsto v - \frac{u^T v}{u^T u} u$ egy lineáris transzformáció $\mathbb{R}^n$-en: az u-ra merőleges hipersíkra történő vetítés.
    - A $v \mapsto v - 2\frac{u^T v}{u^T u} u$ pedig az u-ra merőleges hipersíkra való tükrözés
  - Az $I_V : v \mapsto v$ a V tér identikus lineáris transzformációja.
  - Rögzített $a \in \mathbb{F}$. Ekkor az $f(x) \mapsto f(a)$ egy $\mathbb{F}[x] \to \mathbb{F}$ lineáris függvény.

Képtér, magtér

$\phi : V \to W$ lineáris leképezés

- ϕ **képtere** a
  $$\phi V = \{\phi v | v \in V\}$$
  halmaz. Ez altér W-ben.
  (Szokásos még az $\mathrm{Im}\,\phi$ jelölés is.)
  ϕ *szürjektív*, ha $\phi V = W$
- ϕ **magja** (magtere) a
  $$\ker \phi := \{v \in V | \phi v = 0\}$$
  halmaz. Ez altér V-ben.
  ϕ *injektív*, ha $\phi(v_1) = \phi(v_2)$ csak $v_1 = v_2$ esetén teljesül. Ez azzal ekvivalens, hogy $\ker \phi = (0)$.
- **Példa:** $u \in \mathbb{R}^n$, $\pi : v \mapsto v - \frac{u^T v}{u^T u} u$ vetítés. $\ker \pi = \mathbb{R}u$, $\pi \mathbb{R}^n = u^\perp = \{w \in \mathbb{R}^n | u^T v = 0\}$.

Dimenziótétel

$\phi : V \to W$ lineáris leképezés

- **Dimenziótétel:** $\dim \phi V = \dim V - \dim \ker \phi$.
- **Izomorfizmus:** A $\phi : V \to W$ lineáris lekép. izomorfizmus V és W között, ha ϕ bijektív, azaz egyszerre injektív és szürjektív.
  Ekkor a $\phi^{-1} : W \to V$ **inverz** leképezés is lineáris (és így izomorfizmus).
  $V \cong W$, ha létezik $\phi : V \to W$ izomorfizmus.
  $V \cong W \Leftrightarrow \dim V = \dim W$.
  A dimenziótételből adódik:
- **Egy egyszerű izomorfizmus-kritérium:** $\phi : V \to W$ lin. lekép. izomorfizmus $\Leftrightarrow \ker \phi = (0)$ és $\dim V = \dim W$.

Alkalmazás: Lagrange-interpoláció

- $V = \{n\text{-nél} < \text{fokú } \mathbb{F} \text{ feletti polinomok}\}$
- rögzített $a_1, \ldots, a_n \in \mathbb{F}$ ($a_i \neq a_j$ ha $i \neq j$)
- **Behelyettesítés:** $\phi : V \to \mathbb{F}^n$ a következő lin. lekép. a köv.:

$$\phi f(x) := \begin{pmatrix} f(a_1) \\ f(a_2) \\ \vdots \\ f(a_n) \end{pmatrix}$$

- ϕ **lineáris**, mert minden összetevője az.
- $\ker \phi = (0)$
  (n-nél alacsonyabb fokú nem 0 polinomnak nem lehet n kül. gyöke)
- $\dim V = n = \dim \mathbb{F}^n$
  az előző kritérium miatt
- ϕ **izomorfizmus**, létezik tehát inverze.

Alkalmazás: Lagrange-interpoláció

- **Interpoláció:**
  Tétel: ($a_1, \ldots, a_n$ páronként kül. $\in \mathbb{F}$), tetsz. $b_1, \ldots, b_n \in \mathbb{F}$ esetén $\exists!$ $f(x)$ n-nél $<$ fokú pol., amelyre:
  $$f(a_1) = b_1, \ldots, f(a_n) = b_n.$$
- **konkrétan:**
  $$f(x) = \phi^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$
- **Megj.:** Spec. eset: Diszkrét Fourier Transzformáció (**DFT**), ld. később
- **Megj.:** Ha $n + d$ helyen helyettesítünk be, akkor $f(x)$ rekonstruálható az $n + d$ közül bármely n helyen felvett értékéből. Fontos **hibajavító kódok** működnek ezen az elven.

Alkalmazás: A Shamir-féle titokmegosztás

- **A feladat:** n résztvevő között osszunk szét egy titkot, hogy
  - semelyik $n-1$ ne tudja együtt se kitalálni,
  - de az n résztvevő együtt ki tudja találni
- **A titok:** egy $\mathbb{F}$ véges test egy eleme, ahol $|\mathbb{F}| > n$)
- **Előkészület:** $\alpha_1, \dots, \alpha_n \in \mathbb{F} \setminus \{0\}$ $(\alpha_i \neq \alpha_j)$
  i-edik résztvevőé α_i (nyilvánosan)
- **Titokmegosztás:**
  - Tfh. a titok β.
  - $\beta_1, \dots, \beta_{n-1}$ véletlen elemek $\mathbb{F}$-ből (függetlenül, egyenletes eloszlással)
  - $f(x) = f_{\beta,\beta_1,\dots,\beta_{n-1}}(x) := \beta + \sum_{i=1}^{n-1} \beta_i x^i$
  - i-edik résztvevő kapja $f(\alpha_i) - t$ (privát csatornán)

A Shamir-féle titokmegosztás

- **Együtt kitalálják:** $f(x)$ interpolálható az n helyen felvett értékből, $\beta = f(0)$.
- **Kevesebben nem találják ki:** (pl. az első $n-1$ a véletlen tippnél jobbat nem tud)

$$\phi : \begin{pmatrix} \beta \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} f(0) \\ f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$$

- $\phi : \mathbb{F}^n \to \mathbb{F}^n$ bijekció. mert $\ker \phi = (0)$.

A Shamir-féle titokmegosztás

- Ezért minden rögzített β-ra

$$\phi_\beta : \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$$

- is bijekció $\mathbb{F}^{n-1}$ és $\mathbb{F}^{n-1}$ között.
- Így az $\begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$ vektor egyenletesen véletlen $\mathbb{F}^{n-1}$-ből, β-tól teljesen függetlenül.
- Azaz: minden β-ra ugyanaz az $f(\alpha_1), \ldots, f(\alpha_{n-1})$ értékek eloszlása.

Kompozíció, inverz

- $\phi : V \to V', \phi' : V' \to V''$ lin. lekép.
- Ekkor $\phi'\phi : V \to V''$ is lin.

$$(\phi'\phi)v = \phi'(\phi v)$$

- Asszociatív:
  ha még $\phi'' : V'' \to W$ akkor $\phi''(\phi'\phi) = (\phi''\phi')\phi$
- Mindkét oldalról lineáris:
  $(\alpha_1\phi_1' + \alpha_2\phi_2')(\beta_1\phi_1 + \beta_2\phi_2) = \alpha_1\beta_1\phi_1'\phi_1 + \alpha_1\beta_2\phi_1'\phi_2 + \alpha_2\beta_1\phi_2'\phi_1 + \alpha_2\beta_2\phi_2'\phi_2$.
- **Inverz:** $\phi^{-1} : V' \to V$, ha ϕ bijektív.
- **Inverz tul.:** $(\phi\psi)^{-1} = \psi^{-1}\phi^{-1}$ és $(\phi^{-1})^{-1} = \phi$.
- **Hatványozás:** Tfh. $\phi : V \to V$. Ekkor $\phi^n = \phi \cdots \phi$ (n-szer).

Mátrixok, formális műveletek

- $m \times n$-es mátrixok $\sim$ $m \times n$-es táblázatok $\mathbb{F}$–beli elemekkel.
- $m \times n$ dimenziós vektortér (műveletek elemenként)
- **Mátrixszorzás:** Ha $A = (a_{ij})$ $m \times \ell$-es, $B = (b_{ij})$ $\ell \times n$-es, akkor $AB = (d_{ij})$ $m \times n$-es:

$$d_{ij} = \sum_{k=1}^{\ell} a_{ik} b_{kj}, \ (i = 1, \ldots, m, j = 1, \ldots, n.$$

- Azaz: AB i-edik sorának j-edik eleme az A i-edik sorának és a B j-edik oszlopának a "skaláris szorzata".
- **Szorzás tul.:** A szorzás asszociatív és mindkét változójában lineáris.
- **Vigyázat:** Nem kommutatív, sőt gyakran nem is végezhető el a szorzás a fordított sorrendben.

Mátrixok: példák

- **diagonális mátrixok:**

$$diag(a_1, \ldots, a_n) := \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix},$$

- $diag(a_1, \ldots, a_n) diag(b_1, \ldots, b_n) = diag(a_1 b_1, \ldots, a_n b_n)$, zárt a szorzásra, felcserélhetőek
- **egységmátrix:** $I_n = diag(1, \ldots, 1)$ (n darab 1-es)
- **négyzetes felső háromszög-mátrixok**

$$\begin{pmatrix} a_{11} & * & * & * \\ & a_{22} & * & * \\ & & \ddots & \vdots \\ & & & a_{nn} \end{pmatrix}$$

Zárt a szorzásra

További felső háromszög-mátrixok

- "lapos" $(m < n)$

$$\begin{pmatrix} a_{11} & * & * & * & * & * \\ & a_{22} & * & * & * & * \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & a_{mm} & * & * \end{pmatrix}$$

- "magas" $(m > n)$

$$\begin{pmatrix} a_{11} & * & * & * \\ & a_{22} & * & * \\ & & \ddots & \vdots \\ & & & a_{nn} \\ & & & \end{pmatrix}$$

Transzponált mátrix

- ha $A = (a_{ij})$ $m \times n$-es, akkor $A^T = (a'_{ij})$ $n \times m$-es, ahol
$$a'_{ij} = a_{ji}.$$
- **Tul.:** Ha A $m \times n$-es, B $n \times k$-as, akkor
$$(AB)^T = B^T A^T.$$
- Felső háromszög transzponáltja alsó háromszög

Blokk-mátrixok szorzása

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1\ell} \\ A_{21} & A_{22} & \dots & A_{2\ell} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{12} & \dots & A_{m\ell} \end{pmatrix}, \quad B = \begin{pmatrix} B_{11} & \dots & B_{1n} \\ B_{21} & \dots & B_{2n} \\ B_{31} & \dots & B_{3n} \\ \vdots & \ddots & \vdots \\ B_{\ell 1} & \dots & B_{\ell n} \end{pmatrix},$$

ahol a blokkméretek kompatibilisek. Ekkor

$$AB = \begin{pmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ D_{m1} & D_{12} & \dots & D_{mn} \end{pmatrix},$$

ahol

$$D_{ij} = \sum_{k=1}^{\ell} A_{ik} B_{kj}.$$

Vigyázat: a blokkok szorzása általában nem kommutatív!
Hasznos, ha 0-blokkok vannak, pl. blokk felső háromszög.

Strassen algoritmusa mátrixszorzásra

A, B $2^n \times 2^n$-es, felosztva $2^{n-1} \times 2^{n-1}$-es blokkokra:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \quad B = \begin{pmatrix} B_{11} & B12 \\ B_{21} & B_{22} \end{pmatrix},$$

$$AB = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix},$$

ahol

$$\begin{aligned} D_{11} &= A_{11}B_{11} + A_{12}B_{21}, \\ D_{12} &= A_{11}B_{12} + A_{12}B_{22}, \\ D_{21} &= A_{21}B_{11} + A_{22}B_{21}, \\ D_{22} &= A_{21}B_{12} + A_{22}B_{22}. \end{aligned}$$

Strassen-mátrixszorzás - 7 szorzat

$$T_1 = (A_{11} + A_{22})(B_{11} + B_{22}),$$
$$T_2 = (A_{21} + A_{22})B_{11},$$
$$T_3 = A_{11}(B_{12} - B_{22}),$$
$$T_4 = A_{22}(B_{21} - B_{11}),$$
$$T_5 = (A_{11} + A_{12})B_{22},$$
$$T_6 = (A_{21} - A_{11})(B_{11} + B_{12}),$$
$$T_7 = (A_{12} - A_{22})(B_{21} + B_{22}).$$

Ezekkel:

$$D_{11} = T_1 + T_4 - T_5 + T_7,$$
$$D_{12} = T_3 + T_5,$$
$$D_{21} = T_2 + T_4,$$
$$D_{22} = T_1 - T_2 + T_3 + T_6.$$

Strassen-mátrixszorzás - rekurzió

- Költség: 7 db. 2^{n-1}-es mátrixszorzás, 18 db. összeadás - kivonás
- $K_n = 7K_{n-1} + c4^{n-1}$
- $K_n = O((7 + o(1))^n)$
- $N \times N$-es mátrixokra ($N \sim 2^n$):

$$O(N^{\log_2 7 + o(1)}) = O(N^{2.808})$$

Lineáris leképezés mátrixa

- $\phi : V \to W$ lin. lekép. $v_1, \dots v_n$ bázis V-ben, $w_1, \dots, w_m$ bázis W-ben. Ekkor minden $1 \leq j \leq n$-re

$$\phi v_j = \sum_{i=1}^{m} \alpha_{ij} w_j$$

- ϕ mátrixa (a fenti bázispárra) $A = (\alpha_{ij})$.
- lin. transzformációra ($V = W$) egyetlen (közös) bázis a szokás ($w_i = v_i$).
- **Példa: permutációmátrix:** π permutáció, $\phi v_j = v_\pi(j)$.

$$\alpha_{ij} = \begin{cases} 1, & \text{ha } i = \pi(j) \\ 0, & \text{ha } i \neq \pi(j) \end{cases}$$

Minden sorban és oszlopban egyetlen 1-es, a többi 0.

Példa permutációmátrixra

- az $(12\ldots n)$ ciklus mátrixa

$$\begin{pmatrix} & & & & & 1 \\ 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \end{pmatrix}$$

Mátrixhoz tartozó lineáris leképezés:

- $v_1, \dots v_n$ bázis V-ben, $w_1, \dots, w_m$ bázis W-ben, A $m \times n$-es mátrix.
- Ekkor $\exists! \phi : V \to W$, aminek A a mátrixa (a fenti bázispárra).
- **Megj.:** $V = \mathbb{F}^n$, $W = \mathbb{F}^m$, $v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, v_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

  és $w_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, w_m = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ esetén ez a ϕ éppen a korábban már említett ϕ_A, az oszlopvektorok A-val balról szorzása. Ezután ϕ_A helyett gyakran A.

Műveletek leképezésekkel ill. mátrixaikkal

- összeadás $\leftrightarrow$ összeadás
- skalárral való szorzás $\leftrightarrow$ skalárral való szorzás (= skalármátrixszal való szorzás)
- kompozíció $\leftrightarrow$ mátrixszorzás
- **Inverz:** A $n \times n$-es. A **invertálható**, (**reguláris, nemelfajuló, nem-szinguláris**) ha a ϕ_A bijektív. Ekkor A^{-1} a $(\phi_A)^{-1}$ mátrixa a standard bázisban.
- Ha A invertálható, akkor $AA^{-1} = A^{-1}A = I_n$
- **Képtér:** A (azaz ϕ_A) képtere az A oszlopai által generált altér
- **Köv.:** A $n \times n$-es invertálható $\Leftrightarrow$ oszlopai lin. függetlenek

Példa: Vandermonde-mátrix

- $V = \{\text{az } n\text{-nél} < \text{fokú polinomok}\}$, $W = \mathbb{F}^n$.
- Bázisok: $1, x, x^2, \dots, x^{n-1}$, ill. a standard.
- $a_1, \dots, a_n \in \mathbb{F}$ páronként kül. $\phi : V \to \mathbb{F}^n$ behelyettesítés

$$\phi : f(x) \mapsto \begin{pmatrix} f(a_1) \\ \vdots \\ f(a_n) \end{pmatrix}$$

- ϕ mátrixa

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}.$$

- Tudjuk: ϕ izomorfizmus, így M invertálható (és az inverze a Lagrange-interpoláció mátrixa).

Báziscsere, hasonló mátrixok

- $v_1, \ldots, v_n$ ill. $v'_1 \ldots, v'_n$ bázisok
- **Báziscsere mátrixa** $C = (c_{ij})$

$$v'_j = \sum_{i=1}^{n} c_{ij} v_i$$

  (C a $v_j \mapsto v'_j$ lin. transzf. mátrixa $v_1, \ldots, v_n$-ben)
- $\phi : V \to V$ lin. transzf. mátrixa $v_1, \ldots, v_n$-ben A
- ϕ mátrixa $v'_1, \ldots, v'_n$-ben

$$C^{-1}AC.$$

- **Megj.:** különböző terek közti lin. leképezésekre két cseremátrix van

Báziscsere - példa

- legyen

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

- ahol A, B, C, D $n \times n$-es mátrixok.
- **Báziscsere:** $1. \leftrightarrow n+1.$, $\ldots$, $n. \leftrightarrow 2n.$, mátrixa

$$T = \begin{pmatrix} & I_n \\ I_n & \end{pmatrix}.$$

- Mivel $T^2 = I_{2n}$, $T^{-1} = T$.
- A blokk-mátrixok szorzását használva:

$$\begin{pmatrix} & I \\ I & \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} & I \\ I & \end{pmatrix} = \begin{pmatrix} C & D \\ A & B \end{pmatrix} \begin{pmatrix} & I \\ I & \end{pmatrix} = \begin{pmatrix} D & C \\ B & A \end{pmatrix}.$$

- Például a $B = 0$ esetben M alsó blokk-háromszög mátrix, amiből a báziscsere felső blokk-háromszög mátrixot csinál.

Hasonló mátrixok

- A, A' $n \times n$-es hasonlóak ($A \sim A'$), ha létezik C invertálható, hogy $A' = C^{-1}AC$.
- ugyanannak a lin. transzformációnak a mátrixai csak más-más bázisban
- Az A-val való balról szorzás mátrixa a standard bázisban A a C oszlopaiból álló bázisban $C^{-1}AC$.
- $A \mapsto C^{-1}AC$ leképezés kompatibilis a mátrixműveletekkel:

$$C^{-1}(\lambda A + \mu B)C = \lambda C^{-1}AC + \mu C^{-1}BC,$$

$$C^{-1}ABC = C^{-1}ACC^{-1}BC.$$

Determináns

- **Permutáció előjele:**
  - $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ permutáció (bijekció)
  - (i, j) inverzió π-re, ha $1 \leq i < j \leq n$ és $\pi(i) > \pi(j)$
  - $\operatorname{sgn}(\pi) = (-1)^{\text{inverziók száma}}$
  - multiplikatív: $\operatorname{sgn}(\pi_1\pi_2) = \operatorname{sgn}(\pi_1)\operatorname{sgn}(\pi_2)$.
- **Determináns:** $A = (a_{ij})$ $n \times n$-es

$$\det A = \sum_{\pi \text{ perm}} \operatorname{sgn}(\pi) a_{1\pi(1)} \cdots a_{n\pi(n)}.$$

- $n!$ tag van
- permutációmátrixra: Ha P π mátrixa, akkor $\det P = \operatorname{sgn}(\pi)$.

Példák

- $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$-ra $\det A = ad - bc$.
- $\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$
$$a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$
- Egy alsó vagy felső háromszögmátrix determinánsa a diagonális elemek szorzata.
- Ha $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, ahol A és C négyzetes, akkor $\det M = \det A \cdot \det C$.
- Ha $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$, $D = \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$, akkor
$$\det A = \det B = \det C = \det D = 0,$$
míg $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = -abcd$, tehát $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ általában nem fejezhető ki pusztán $\det A$,$\det B$,$\det C$,$\det D$-vel.

Elemi tulajdonságok

- **Transzponált determinánsa:** $\det A^T = \det A$
- **Kifejtési tétel (Laplace):** $A = (a_{ij})$ $n \times n$-es. Minden egyes (i, j)-re C_{ij} az az $(n-1) \times (n-1)$-es, amely A-ból az i-edik sor és a j oszlop elhagyásával adódik.

  Tetsz. i-re és j-re:

  $$\det A = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det C_{kj} = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det C_{ik}.$$

- **Linearitás oszlopok szerint:** Minden egyes $j$re és $v \in \mathbb{F}^n$ vektorra $A_j(v)$ az a mátrix, ami az A mátrixból j-edik oszlopának v-vel való helyettesítésével kapható.

  Ekkor $\det A_j(\lambda u + \mu v) = \lambda \det A_j(u) + \mu \det A_j(v)$.

- Linearitás sorok szerint...

Elemi tulajdonságok

- **Köv. (Nullákból álló oszlop (sor)):** Ha van ilyen, akkor a determináns 0.
- **Skalárszoros oszlopok** Ha A-nak van két olyan oszlopa (sora), hogy az egyik a másik skalárszorosa, akkor $\det A = 0$.
- **Sor- és oszlopműveletek hatása:** $\det A$
  - marad, ha A egy oszlopához (sorához) hozzáadjuk egy másik oszlopának (sorának) skalárszorosát.
  - marad, ha A egy oszlopához (sorához) hozzáadjuk néhány, tőle különböző indexű oszlopának (sorának) egy tetszőleges lineáris kombinációját.
  - α-vak szorzódik, ha A egy oszlopát (sorát) α-val beszorozzuk.
  - előjelet vált (-1-gyel szorzódik), ha A két oszlopát megcseréljük.
- $\Rightarrow$ **számolható Gauss-eliminációval**
- $\Rightarrow$ **Szinguláris mátrix determinánsa** 0

Szorzat determinánsa

- **Determinánsok szorzástétele:** Ha A és B $n \times n$-es mátrixok, akkor
$$\det(AB) = (\det A)(\det B).$$
- **Köv. (Inverz determinánsa):** Ha A invertálható, akkor $\det A \neq 0$ és
$$\det A^{-1} = \frac{1}{\det A}.$$
- **Köv. (Hasonló mátrixok determinánsa):** $\det(C^{-1}AC) = \det A$.
- **Lineáris transzformációk determinánsa:** Bármely bázis szerinti mátrix determinánsa.

Inverz mátrix előjeles aldeterminánsokkal

- $A = (a_{ij})$ $n \times n$-es.
- C_{ij} az A-ból az i-edik sor és a j-edik oszlop elhagyásával adódó $n-1 \times n-1$-es mátrix
- (i,j)-edik előjeles aldetermináns $(-1)^{i+j} \det C_{ij}$.
- Ha A invertálható és $A^{-1} = (a'_{ij})$, akkor

$$a'_{ij} = (-1)^{i+j} \frac{\det C_{ji}}{\det A}.$$

- **Figyelem:** C_{ji}, nem C_{ij}!

Mátrixok rangja

- **Lin. független oszlopok max. száma** (A képtér dimenziója)
- **Max. méretű. invertálható négyzetes részmátrix**
- **Lin. független sorok max. száma**

Lineáris egyenletrendszer

- $$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$
- másképpen: $Ax = b$,

  ahol $A = (a_{ij})$ $m \times n$-es, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$.
- Az egyenletrendszer **mátrixa** A,
- a **kibővített mátrixa** az $(A|b)$ $m \times (n+1)$-es.

A Cramer-szabály

$m = n$ és tfh. A invertálható.

$$x_j = \frac{\det A_j(b)}{\det A} \quad (j = 1, \dots, n),$$

ahol $A_j(b)$: A j-edik oszlopát helyettesítjük a b oszlopvektorral.

nem praktikus

Megoldás Gauss-eliminációval

- Összetevők: Ekvivalens egyenletrendszert kapunk, ha
  - egy egyenlethez egy másik egyenlet skalárszorosát adjuk
  - egyenletet egy skalárral beszorozzuk
  - átrendezzük az egyenletek sorrendjét
  - átrendezzük a változók sorrendjét

  Az első három összetevő a determinánsnál már alkalmazott sorműveleteknek felel meg, az utolsó az oszlopok cseréjének.
- **Első iteráció**
  - Legelső lépés: cserékkel elérhető, hogy $a_{11} \neq 0$. Az első egyenlet segítségével x_1-et kiküszöböljük a többi egyenletből.
  - Folytatjuk a többi egyenlettel, a többi változóra
- Az üres egyenletekkel $(0 = 0)$ nem törődünk
- Ha lett $0 = b_i$ egyenlet, $(b_i \neq 0)$, nincs megoldás

Gauss-elimináció II.

- Az első menet után felső háromszög alakú:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1m}x_m + \ldots + a_{1n}x_n &= b_1 \\ a_{22}x_2 + \ldots + a_{2m}x_m + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{mm}x_m + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

- **Második iteráció:** A főátló feletti részt kiküszöböljük:

$$\begin{aligned} a_{11}x_1 \qquad\qquad + a_{1,m+1}x_{m+1} + \ldots + a_{1n}x_n &= b_1 \\ a_{22}x_2 \qquad\qquad + a_{2,m+1}x_{m+1} + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{mm}x_m + a_{m,m+1}x_{m+1} + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

Gauss-elimináció III.

- Majd leosztunk az átlós együtthatókkal:

$$\begin{array}{rcl} x_1 \qquad\qquad + a_{1,m+1}x_{m+1} + \ldots + a_{1n}x_n & = & b_1 \\ x_2 \qquad + a_{2,m+1}x_{m+1} + \ldots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ x_m + a_{m,m+1}x_{m+1} + \ldots + a_{mn}x_n & = & b_m \end{array}$$

- **Eredmény:** $x_{m+1}, \ldots, x_n$ szabad paraméterek,

$$\begin{array}{rcl} x_1 & = & b_1 - a_{1,m+1}x_{m+1} - \ldots - a_{1n}x_n \\ x_2 & = & b_2 - a_{2,m+1}x_{m+1} - \ldots - a_{2n}x_n \\ & \vdots & \\ x_m & = & b_m - a_{m,m+1}x_{m+1} - \ldots - a_{mn}x_n \end{array}$$

Példa

Egyenletrendszer $\mathbb{Z}_2$ fölött:

$$\begin{aligned} x_1 + x_2 &= 1 \\ x_1 + x_5 &= 1 \\ x_3 + x_4 &= 1 \\ x_2 + x_3 + x_4 + x_5 &= 1 \\ x_2 + x_5 &= 1. \end{aligned}$$

A kibővített mátrix:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Példa II

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Az első sort levonjuk másodikból

Példa III

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

A második sort levonjuk a negyedikből

Példa IV

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

A második sort levonjuk az ötödikből

Példa V

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A harmadik sort levonjuk a negyedikből

Példa VI

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Az utolsó sor a $0 = 1$ ellentmondásnak felel meg, ez az egyenletrendszer tehát **nem megoldható**.

Példa VII

Tfh. az $x_2 + x_5 = 1$ egyenlet helyett az $x_2 + x_5 = 0$ áll. Ekkor az eddigi lépések eredménye

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Levonjuk a második sort az elsőből:

Példa VIII

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

A megoldás: x_4, x_5 tetszőleges és $x_1 = x_5 + 1$, $x_2 = x_5$, $x_3 = x_4 + 1$.

Gauss-elimináció további alkalmazásai

- Rang számolása
- Determináns számolása

Ezekhez elegendő az első iterációs menet

Sajátértékek, sajátvektorok, sajátalterek

- $\phi : V \to V$ lin. transzf.
- $0 \neq v \in V$ sajátvektora ϕ-nek $\lambda \in \mathbb{F}$ sajátértékkel, ha $\phi v = \lambda v$.
- **Példa:** Legyen $v_0 \in \mathbb{R}^n$, $v_{t+1} = \phi v_t$ (mint pl. Pagerank-nél.) Tfh. létezik
$$v = \lim_{t\to\infty} v_t \text{ és } v \neq 0.$$
Ekkor v sajátvektora ϕ-nek 1 sajátértékkel.
  - **Biz.** $v_{t+1} = \phi v_t$
  - $v \mapsto \phi v$ folytonos
  - $\lim_{t\to\infty} v_{t+1} = \phi \lim_{t\to\infty} v_t$
  - $v = \phi v$.
- **Sajátaltér:** a λ sajátértékhez tartozó sajátvektorok a 0-val együtt.
- **Példa:** ϕ szinguláris $\Leftrightarrow$ 0 egy sajátértéke. Ekkor a magtér a megfelelő sajátaltér.

Sajátértékek, sajátvektorok, sajátalterek -példa

$\mathbb{R}^n$-en $\pi : v \mapsto v - \frac{u^T v}{u^T u} u$ vetítés

- 1 egy sajátérték, ha $n > 0$. Ekkor a sajátaltér $u^\perp$
- 0 sajátérték, u egy sajátvektor
- $u^\perp$-en és $\langle u \rangle$-n kívül nincs más sajátvektor:
  Tfh. $v = \alpha u + w$ sajátvektor $0 \neq \lambda$ sajátértékkel. Ekkor

  $$\lambda \alpha u + \lambda w = \lambda v = \pi v = \pi \alpha u + \pi w = w,$$

  így $\alpha = 0$ és $\lambda = 1$.
- $n > 1$: két sajátérték: 1 és 0, a két sajátaltér $u^\perp$ és $\langle u \rangle$.

Sajátalterek együttesen

- **Alterek lineáris függetlensége:** $(0) \neq W_1, \ldots, W_s \leq V$ lin. függetlenek, ha $w_1 + \ldots + w_s = 0$ $(w_i \in W_i) \Rightarrow w_i = 0$ $(i = 1, \ldots, s)$
- $v_1, \ldots, v_s$ lin. ftlenek $\Leftrightarrow \langle v_1 \rangle, \ldots, \langle v_s \rangle$ lin. ftlenek
- **Áll.:** $(0) \neq W_1, \ldots, W_s \leq V$ lin. ftlenek $\Leftrightarrow$ $\dim\langle W_1, \ldots, W_s \rangle = \dim W_1 + \ldots + \dim W_s$
- **Áll.: A sajátalterek lin. ftlenek.:** $\phi v_i = \lambda_i v_i$, $\lambda_i \neq \lambda_j$, $v_1 + \ldots + v_s = 0 \Rightarrow v_1 = \ldots = v_s = 0$.
  - **Biz.** indukció s szerint. $s = 1$-re triviális.
  - $s > 1$: $v_1 + \ldots + v_s = 0$. Ekkor
  - $0 = \phi(v_1 + \ldots + v_s) = \lambda_1 v_1 + \ldots + \lambda_s v_s$, ugyanakkor
  - $0 = \lambda_1(v_1 + \ldots + v_s) = \lambda_1 v_1 + \ldots + \lambda_1 v_s$. Kivonva:
  - $(\lambda_2 - \lambda_1)v_2 + \ldots + (\lambda_s - \lambda_1)v_s = 0$. Innen
  - az indukciós feltevés miatt $(\lambda_i - \lambda_1)v_i = 0$, így $v_i = 0$ $(i > 1)$.
  - marad a $v_1 = 0$

Alterek lin. függetlesége - pótlap

$(0) \neq W_1, \ldots, W_s \leq V$

- **Áll.:** $W_1, \ldots, W_s$ lin. ftlenek $\Leftrightarrow \dim\langle W_1, \ldots, W_s\rangle = \dim W_1 + \ldots + \dim W_s$
- **konkrétabban:** Legyen $w_1^1, \ldots, w_{n_1}^1$ bázis W_1-ben, ... $w_1^s, \ldots, w_{n_s}^s$ bázis W_1-ben. Ekkor: $W_1, \ldots, W_s$ lin. ftlenek $\Leftrightarrow$ $w_1^1, \ldots, w_{n_1}^1$, ..., $w_1^s, \ldots, w_{n_s}^s$ lin. ftlen.

  Biz. $\Rightarrow$: Tfh. $\alpha_1^1 w_1^1 + \ldots + \alpha_{n_1}^1 w_{n_1}^1 + \ldots + \alpha_1^s w_1^s + \ldots + \alpha_{n_s}^s w_{n_s}^s = 0$. Ekkor $W_1, \ldots, W_s$ lin. ftlensége miatt $\alpha_1^1 w_1^1 + \ldots + \alpha_{n_1}^1 w_{n_1}^1 = 0$, ..., $\alpha_1^s w_1^s + \ldots + \alpha_{n_s}^s w_{n_s}^s = 0$. $w_1^i, \ldots, w_{n_i}^i$ lin. ftlensége miatt az összes $\alpha_j^i = 0$.
  $\Leftarrow$: Tfh. $u_i \in W_i$-vel $\sum_{i=1}^s u_i = 0$. Ekkor $u_i = \sum_{j=1}^{n_i} \alpha_j^i w_j^i$ alakú és $\alpha_1^1 w_1^1 + \ldots + \alpha_{n_1}^1 w_{n_1}^1 + \ldots + \alpha_1^s w_1^s + \ldots + \alpha_{n_s}^s w_{n_s}^s = 0$, így $w_1^1, \ldots, w_{n_1}^1$, ..., $w_1^s, \ldots, w_{n_s}^s$ lin ftlensége miatt az összes $\alpha_j^i = 0$, így mindegyik $w_i = 0$.

Sajátalterek együttesen, diagonalizálható mátrixok

Következmények ($\mathbb{C}$ felett)

- ϕ sajátaltereinek dimenzióinak összege $\leq \dim V$
- ϕ-nek legfeljebb $\dim V$ különböző sajátértéke van
- **Spektráltétel spec. esetre:** Ha ϕ-nek van $\dim V$ különböző sajátértéke, akkor V-nek van ϕ sajátvektoraiból álló bázisa, azaz olyan bázis, amiben ϕ mátrixa diagonális
- **Mátrixokra.: Def.:** az A $n \times n$-es komplex mátrix **diagonalizálható**, ha hasonló agy diagonális mátrixhoz: azaz $\exists$ C invertálható, hogy $C^{-1}AC$ diag.
  azaz $\exists$ A-nak (az A-val való balról szorzásnak) sajátvektoraiból álló bázisa $\mathbb{C}^n$-nek
- Ha A-nak van n kül. sajátértéke $\mathbb{C}$-ben, akkor A diagonalizálható

Példák diagonalizálható és nem diagonalizálható mátrixra

- a λI skalármátrix diagonális, pedig csak 1 sajátértéke van
- $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sajátértékei 1 és -1, az $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, illetve $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ sajátvektorokkal.
- $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ nem diagonalizálható.
  - **Biz.:** Tfh. $C^{-1}AC = \begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix}$
  - Mivel $A^2 = 0$, $(C^{-1}AC)^2 = C^{-1}ACC^{-1}AC = C^{-1}A^2C = 0$,
  - tehát $\lambda_i^2 = 0$ $(i = 1, 2)$
  - ugyanakkor $A \neq 0 = \mathrm{diag}(0, 0)$.

Tanulság

- **Áll.:** Ha $f(x)$ egy polinom, hogy $f(A) = 0$, akkor $f(\lambda) = 0$ minden komplex sajátértékre

  Biz.:
  Legyen $0 \neq v$, hogy $Av = \lambda v$.
  Ekkor $A^i v = \lambda^i v$ $(i = 0, 1, \ldots)$
  Így $g(A)v = g(\lambda)v$ tetsz. g polinomra
  $0 = f(A)v = f(\lambda)v$,
  $v \neq 0$ miatt így $f(\lambda) = 0$.
- **fordítva ált. nem igaz**
- **diagonalizálhatóra fordítva is igaz**

Jordan-normálalak

Tétel: Minden négyzetes komplex mátrix hasonló egy alábbi alakúhoz:

$$\begin{pmatrix} \boxed{\begin{matrix} \lambda & 1 & & & & \\ & \lambda & 1 & & & \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ & & & & \lambda & 1 \\ & & & & & \lambda \end{matrix}} & & & & \\ & \boxed{\begin{matrix} \mu & 1 & & & \\ & \mu & 1 & & \\ & & \ddots & \ddots & \\ & & & \mu & 1 \\ & & & & \mu \end{matrix}} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \boxed{\begin{matrix} \nu & 1 & & \\ & \ddots & \ddots & \\ & & \nu & 1 \\ & & & \nu \end{matrix}} \end{pmatrix}$$

Jordan-normálalak

Tétel: Minden négyzetes A komplex mátrix hasonló blokk diagonálishoz, ahol a diagonális blokkok

$$\begin{pmatrix} \lambda & 1 & & & & \\ & \lambda & 1 & & & \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ & & & & \lambda & 1 \\ & & & & & \lambda \end{pmatrix}$$

alakúak.

- λ-k: A sajátértékei
- egy sajátérték esetleg több blokkban is előfordulhat
- a blokkok sorrend erejéig egyértelműek
- *Nem bizonyítjuk.*

Karakterisztikus polinom

A $n \times n$-es mátrix

- **Észrevétel:** λ sajátértéke A-nak $\Leftrightarrow$ $\lambda I_n - A$ szinguláris $\Leftrightarrow$ $\det(\lambda I_n - A) = 0$.
- **Karakterisztikus polinom:** $\det(xI - A) \in \mathbb{F}[x]$
- **Áll.:** hasonló mátrixok karakterisztikus polinomja ugyanaz. $\rightarrow$ Lin. transzformáció karakterisztikus polinomja jól def.
- λ sajátértéke A-nak $\Leftrightarrow$ λ gyöke A karakterisztikus polinomjának.
- **Köv.:** $\mathbb{C}$ felett minden négyzetes mátrixnak van legalább egy sajátértéke.
- **Feladat:** Mi $\det(xI_n - A)$ konstans tagja? Mi az $n-1$-ed fokú tag együtthatója?

Felső háromszög alak

Tétel: Minden $n \times n$-es A komplex mátrix hasonló egy felső háromszög alakú mátrixhoz.

- **Biz.:** Indukció n szerint. $n = 1$: triviális.
- $n > 1$: λ A-nak egy sajátértéke, v megf. sajátvektor. Legyen C egy olyan $n \times n$-es invertálható mátrix, aminek v az első oszlopa. A C oszlopaiból álló bázisban az A-val való szorzás mátrixa $C^{-1}AC = \begin{pmatrix} \lambda & * \\ & \boxed{A'} \end{pmatrix}$.
- az indukciós feltevés miatt létezik C' $n-1 \times n-1$-es, hogy $C'^{-1}A'C'$ felső háromszög.
- legyen $C'' = \begin{pmatrix} 1 & \\ & \boxed{C'} \end{pmatrix}$.
- Ekkor $(CC'')^{-1}A(CC'') = C''^{-1}C^{-1}ACC''$ felső háromszög.

Háromszögmátrixok karakterisztikus polinomja

- **Felső háromszögmátrix karakterisztikus polinomja:**

$$(x - a_{11})(x - a_{22}) \cdots (x - a_{nn}),$$

  ahol a_{ii} a főátló i-edik eleme.
- **Emlékeztető 1:** $C^{-1}AC$ karakterisztikus polinomja ugyanaz, mint A-é
- **Emlékeztető 2:** $M \mapsto C^{-1}MC$ kompatibilis mátrixok szorzásával és lineáris is.
- **Köv.:** Tetszőleges $f(x)$ polinomra $f(C^{-1}AC) = C^{-1}f(A)C$.

A Hamilton–Cayley-tétel

Tétel (Hamilton-Cayley): A gyöke a karakterisztikus polinomjának

- **Biz.:** Elég felső háromszögre. Ilyenekre indukció.
- Legyen $g(x) = (x - a_{22}) \cdots (x - a_{nn})$. Ekkor A karakterisztikus polinomja $f(x) = (x - a_{11})g(x)$, és $g(x)$ A bal alsó $n-1 \times n-1$-es blokkjának karakterisztikus polinomja.
- $f(A) = (A - a_{11}I_n)g(A)$ alakú. Az első tényező $\begin{pmatrix} 0 & * \\ & \boxed{*} \end{pmatrix}$,

  a második $\begin{pmatrix} * & * \\ & \boxed{0} \end{pmatrix}$ alakú az indukciós feltevés miatt.

  Két ilyen mátrix szorzata (ebben a sorrenben) 0.

Minimálpolinom

- Maradékos osztás polinomokra....
- A $n \times n$-es.
- Tfh. $0 \neq f(x), g(x) \in \mathbb{F}[x]$ polinomok, hogy $f(A) = g(A) = 0$, továbbá $\deg f(x) \leq \deg g(x)$
- legyen $h(x) := g(x)$ maradéka modulo $f(x)$.
- ekkor $h(A) = 0$ is igaz.
- **Köv.:** $\exists!$ legalacsonyabb fokú 1 főegyütthatós $f(x)$ polinom, amire $f(A) = 0$, és minden olyan $g(x)$, amire $g(x) = 0$ többszöröse $f(x)$-nek.
- **Elnevezés:** minimálpolinom.
- A karakterisztikus polinom ennek többszöröse.

Példa: DFT

- Legyen P az $(12\ldots n)$ ciklushoz tartozó permutációmátrix:

$$P = \begin{pmatrix} & & & & & 1 \\ 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \end{pmatrix}$$

- **Áll.:** P minimálpolinomja $x^n - 1$
  Biz.: $P^n = I$ **és** $I, P, \ldots, P^{n-1}$ **lin. ftlenek.**
  (mert az első oszlopaik lin. ftlenek).
- **Köv.:** P karakterisztikus polinomja $x^n - 1$
- **Köv.:** P sajátértékei $\omega^0, \omega, \ldots, \omega^{n-1}$, ahol $\omega = e^{2\pi i/n}$.

Példa: DFT

- **Számolás mutatja:** $w_j := \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{j(n-1)} \end{pmatrix}$ sajátvektora P-nek ω^{-j} sajátértékkel
- a megfelelő báziscsere mátrixa

$$\frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix},$$

az $1, \omega, \ldots, \omega^{n-1}$ számokhoz tartozó Vandermonde-mátrix.