

Alkalmazott algebra

Iványos Gábor

2011. szeptember 5.

1. Alapok

1.1. Testek

1.1.1. Definíció

Informálisan: Egy test egy négy alpművelettel $(+, -, \cdot, /)$ ellátott halmaz, amelyen a racionális számokon megszokott azonosságok teljesülnek.

Formálisan: Egy test egy \mathbb{F} halmaz két művelettel és két (különböző) kitüntetett elemmel: $+$, \cdot illetve $0, 1$, amelyekre

- (1) $(x + y) + z = x + (y + z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\forall x, y, z \in \mathbb{F}$) – mindkét művelet *asszociatív*
- (2) $x + y = y + x$, $x \cdot y = y \cdot x$ ($\forall x, y \in \mathbb{F}$) – mindkét művelet *kommutatív*
- (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 $x/y := x \cdot y^{-1}$.

Megjegyzés: Ezekből tényleg levezethető minden, a racionális számokra érvényes azonosság ($G_1 = G_2$ alakú, ahol G_1 és G_2 az alpműveletek és a $0, 1$ konstansok segítségével felépített kifejezés.) Pl. a mások oldali disztributivitás levezethető az eredetiből a szorzás kommutativitása segítségével: $z \cdot (x + y) = (x + y) \cdot z = (x \cdot z) + (y \cdot z) = (z \cdot x) + (z \cdot y)$.

Konvenció: Zárójelek elhagyása, műveletek kötési sorrendje, \cdot elhagyása a szokásos módon

1.1.2. Példák

- \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 (ún. izomorfia erejéig) egyértelmű.

1.1.3. Polinomok

n -ed fokú egyváltozós polinom: $f(x) = a_n x^n + \dots + a_1 x + a_0$ ($a_i \in \mathbb{F}$, $a_n \neq 0$).

Áll. (gyöktényező kiemelése): $a \in \mathbb{F}$, $f(a) = 0$ esetén létezik egy eggyel alacsonyabb fokú $g(x)$ polinom, hogy $f(x) = (x - a)g(x)$

Biz.: Az egészekhez hasonló maradékos osztással $f(x) = (x - a)g(x) + c$, ahol $c \in \mathbb{F}$. Ebből $0 = f(a) = (a - a)g(a) + c = c$.

Köv.: Egy n -ed fokú polinomnak legfeljebb n gyöke van.

Biz.: A fokszám szerinti indukcióval. Elsőfokúra nyilván igaz. Ha $n > 1$ és α egy gyöke $f(x)$ -nek, akkor $f(x) = (x - \alpha)g(x)$ az előző állítás értelmében. Ha $\beta \neq \alpha$ és $g(\beta) \neq 0$ akkor $f(\beta) = (\beta - \alpha)g(\beta) \neq 0$, így $f(x)$ összes α -tól különböző gyöke $g(x)$ -nek is gyöke, amelyből legfeljebb $n - 1$ van az indukciós feltevés szerint.

Algebra alaptétele. Minden komplex együtthatós polinomnak van gyöke \mathbb{C} -ben (multiplicitással számolva összesen fokszámnyi)

1.2. Vektorterek

1.2.1. Definíció, példák

Vektortér \mathbb{F} felett.: Egy V halmaz egy $+: V \times V \rightarrow V$ (összeadás) művelettel, egy kitüntetett 0 elemmel, továbbá egy $\cdot: \mathbb{F} \times V \rightarrow V$ (skalárokkal való szorzás) 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: $(x + y) \cdot (u + v) = x \cdot u + y \cdot u + x \cdot v + y \cdot v$ ($x, y \in \mathbb{F}, u, v \in V$)

Megjegyzés.: Additív inverz V -ben: $-v := (-1) \cdot v$.

Példák.:

- S halmaz, $S \rightarrow \mathbb{F}$ függvények; értékek szerinti összeadással és beszorzással.
~ 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.
- $\mathbb{R} \rightarrow \mathbb{R}$ folytonos függvények $\mathbb{F} = \mathbb{Q}$ vagy $\mathbb{F} = \mathbb{R}$.
- \mathbb{C} az $\mathbb{F} = \mathbb{Q}$ vagy $\mathbb{F} = \mathbb{R}$ felett.

1.2.2. Alterek, bázis, dimenzió

Lineáris kombináció.: $\alpha_1 v_1 + \dots + \alpha_n v_n$ alakú kifejezés, ahol $0 \neq v_i$ és $v_i \neq v_j$ ha $i \neq j$. Mindig véges számú tagból álló összeget tekintünk! Az üres összeg is lineáris kombináció, 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. Tartalmazásra nézve $\{0\} = (0)$ (vagy kissé hanyag módon: 0) a legszűkebb, V a legtágabb altere V -nek.

Példák.:

- 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.: $S \subseteq V$ által generált altér $\langle S \rangle$ az a legszűkebb altér, amely tartalmazza S -t.

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

$$\langle \emptyset \rangle = \{0\}, \langle v \rangle = \langle \{v\} \rangle = \{\alpha v \mid \alpha \in \mathbb{F}\}.$$

Példák.

- polinomok között az $1, x, x^2, \dots, x^{n-1}$ monomok az n -nél alacsonyabb fokú polinomok alterét generálják
- (Feladat) Mely alteret 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 ($i = 1, \dots, n$) $\sum_{i=1}^n \alpha_i v_i = 0$ esetén az összes $\alpha_i = 0$. Ha S nem lineárisan független, akkor lineárisan összefüggő. Az \emptyset lineárisan független, $\{0\}$ lineárisan összefüggő. Világos, hogy lineárisan független halmazok részhalmazai is lineárisan függetlenek.

Áll.: Ha S lineárisan független, de $S \cup \{v\}$ lineárisan összefüggő, akkor v (egyértelműen) előáll S -beli elemek lineáris kombinációjaként.

Példák:

- $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ és $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ lineárisan függetlenek:

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

- $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ 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: $S \subseteq V$ akkor és csak akkor lineárisan független, ha tetszőleges $S_1 \subsetneq S$ esetén $\langle S_1 \rangle \subsetneq \langle S \rangle$ (\Leftrightarrow tetszőleges $v \in S$ esetén $v \notin \langle S \setminus \{v\} \rangle$). Más szavakkal S akkor és csak akkor lineárisan független, ha S egy 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. Általában sorba rendezzük a bázis elemeit, és a más sorrendű bázist az eredetitől különbözőnek tekintünk (hiába ugyanaz, mint halmaz).

Példák:

- standard bázis \mathbb{F}^n -ben $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

- polinomok közt $1, x, x^2, \dots$

Áll.: B_1, B_2 bázis V -ben $\Rightarrow |B_1| = |B_2|$.

Biz.: Először a következő kicserélési tulajdonságot látjuk be: tetszőleges $v \in B_1$ -hez létezik olyan $v' \in B_2$, amelyre $(B_1 \setminus \{v\}) \cup \{v'\}$ is bázis V -ben. Ugyanis mivel $B_1 \setminus \{v\}$ nem generálja V -t, van olyan $v' \in B_2$ elem, amely nem áll elő $B_1 \setminus \{v\}$ -beli vektorok lineáris kombinációjaként. Ekkor $(B_1 \setminus \{v\}) \cup \{v'\}$ lineárisan független. Ahhoz, hogy $\langle (B_1 \setminus \{v\}) \cup \{v'\} \rangle = V$, elég belátni, hogy v' előáll $(B_1 \setminus \{v\}) \cup \{v'\}$ -beli elemek lineáris kombinációjaként. Tudjuk, hogy $v' = \alpha v + \sum_{i=1}^m \alpha_i v_i$, ahol $\alpha_i \in \mathbb{F}$ és $v_i \in B_1 \setminus \{v\}$. A v' -re vonatkozó feltevés miatt $\alpha \neq 0$ és így $v = \frac{1}{\alpha} v' - \sum_{i=1}^m \frac{\alpha_i}{\alpha} v_i$. Ezzel igazoltuk a kicserélési tulajdonságot.

Tegyük fel, hogy B_1 véges. Ekkor legfeljebb $|B_1|$ lépésben alkalmazva a kicserélési tulajdonságot egy olyan B_1' bázist nyerhetünk, amely ugyanakkora, mint B_1 és összes eleme B_2 -ből van. Ez csak úgy lehet, hogy $B_1' = B_2$. Szimmetrikusan kezelhető az az eset, amikor B_2 véges.

Tegyük végül fel, hogy B_1 is és B_2 is végtelen. Minden B_1 -beli v vektor egyértelműen felírható $\sum_{i=1}^{m_v} \alpha_{v,i} w_{v,i}$ alakban, ahol $m_v > 0$ egész, $0 \neq \alpha_{v,i} \in \mathbb{F}$ és $w_{v,i} \in B_2$ ($i = 1, \dots, m_v$). Legyen $i > m_v$ -re $w_{v,i} := w_{v,m_v}$. Ekkor a $(v, i) \mapsto w_{v,m_v}$ egy $\mathbb{Z}_{>0} \times B_1 \rightarrow B_2$ függvény, ami szürjektív, hiszen a képben előforduló vektorok generálják V -t. Tehát $|\mathbb{Z}_{>0} \times B_1| \geq |B_2|$. Mivel B_1 végtelen, $|\mathbb{Z}_{>0} \times B_1| \geq |B_1|$, így $|B_1| \geq |B_2|$. A $|B_1| \leq |B_2|$ egyenlőtlenség szimmetrikus érveléssel igazolható.

Dimenzió: $\dim V$, pontosabban $\dim_{\mathbb{F}} V = V$ tetszőleges bázisának számossága (elemszáma).

Példák:

- ha S véges, akkor $\dim\{S \rightarrow \mathbb{F} \text{ függvények}\} = |S|$
- 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 $\dim_{\mathbb{R}} V = 2n$

Megállapodás. Ezentúl – hacsak kifejezetten nem jelezzük az ellenkezőjét – **csak véges dimenziós vektorterekkel foglalkozunk.**

1.3. Lineáris leképezések

1.3.1. Definíció, példák

Lineáris leképezés: V, W vektorterek \mathbb{F} felett. Egy $\phi : V \rightarrow W$ leképezés lineáris, ha $\phi(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 \phi(v_1) + \alpha_2 \phi(v_2)$. Továbbiakban elhagyjuk a zárójelet: $\phi v := \phi(v)$.

Fontos példa: A $m \times n$ -es mátrix \mathbb{F} -beli elemekkel. $\phi_A : \mathbb{F}^n \rightarrow \mathbb{F}^m$: $\phi_A v := Av$.

Vektortér-műveletek leképezésekkel: $\phi, \phi' : U \rightarrow W, \alpha \in \mathbb{F}$ -re $(\alpha\phi + \phi')v := \alpha(\phi v) + (\phi' v)$. Ezekkel az $U \rightarrow V$ lineáris leképezések vektorteret alkotnak.

Kiterjesztés bázisról: Legyen $\{v_1, \dots, v_n\}$ egy bázis V -ben és legyenek w_1, \dots, w_n W -beli vektorok. Ekkor $\exists! \phi : V \rightarrow W$ lineáris leképezés, amelyre $\phi v_i = w_i$ ($i = 1, \dots, n$):

$$\phi \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n \alpha_i w_i.$$

Köv.: A $V \rightarrow W$ lineáris leképezések terének dimenziója $\dim V \cdot \dim W$.

Speciális esetek:

Lineáris függvény: $V \rightarrow \mathbb{F}$ lineáris leképezés.

Lineáris transzformáció: $V \rightarrow V$ lineáris leképezés.

Példák:

- Adott $0 \neq u \in \mathbb{R}^n$ 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.
- Legyen $a \in \mathbb{R}$. Ekkor az $f(x) \mapsto f(a)$ egy $\mathbb{R}[x] \rightarrow \mathbb{R}$ lineáris függvény.

1.3.2. Képtér, magtér, dimenziótétel

Képtér: $\phi : V \rightarrow W$ lineáris leképezés képtere a

$$\phi V = \{\phi v \mid v \in V\}$$

halmaz. (Szokásos még az $\text{Im } \phi$ jelölés is.) Könnyen ellenőrizhető, hogy ϕV altér W -ben. A ϕ leképezés *szürjektív*, ha $\phi V = W$

Magtér: $\phi : V \rightarrow W$ lineáris leképezés magja vagy magtere a

$$\ker \phi = \{v \in V \mid \phi v = 0\}$$

halmaz. Könnyen ellenőrizhető, hogy ez egy altér V -ben. A ϕ leképezés *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. $\ker \pi = \mathbb{R}u$, $\pi \mathbb{R}^n = u^\perp = \{w \in \mathbb{R}^n \mid u^T w = 0\}$.

Izomorfizmus: A $\phi : V \rightarrow W$ lineáris leképezés izomorfizmus V és W között, ha ϕ bijektív, azaz egyszerre injektív és szürjektív. Ekkor a $\phi^{-1} : W \rightarrow V$ **inverz** leképezés is lineáris izomorfizmus. Két vektortér izomorf, ha létezik közöttük izomorfizmus. Ez akkor és csak akkor áll fenn, ha egyenlő a dimenziójuk.

Dimenziótétel: Legyen $\phi : V \rightarrow W$ lineáris leképezés. Ekkor $\dim \phi V = \dim V - \dim \ker \phi$.

Biz: Legyen $d = \dim \ker \phi$ és legyen $v_1, \dots, v_d, v_{d+1}, \dots, v_{d+\ell}$ egy olyan bázisa V -nek, hogy v_1, \dots, v_d bázisa $\ker \phi$ -nek. Ha $v = \sum_{i=1}^{d+\ell} \alpha_i v_i$. Ekkor $\phi v = \sum_{i=1}^{d+\ell} \alpha_i \phi v_i = \sum_{i=d+1}^{d+\ell} \alpha_i \phi v_i$, így a $\phi v_{d+1}, \dots, \phi v_{d+\ell}$ vektorok kifeszítik a ϕV képteret. Belátjuk, hogy ezek a vektorok egyben lineárisan függetlenek is. Evégett tegyük fel, hogy a $\sum_{i=d+1}^{d+\ell} \gamma_i \phi v_i$ lineáris kombináció 0, vagyis $\phi \sum_{i=d+1}^{d+\ell} \gamma_i v_i = 0$, azaz $\sum_{i=d+1}^{d+\ell} \gamma_i v_i \in \ker \phi$, akkor, mivel a v_1, \dots, v_d a $\ker \phi$ magtér egy bázisa, léteznek olyan $\beta_1, \dots, \beta_d \in \mathbb{F}$ skalárok, hogy $\sum_{j=1}^d \beta_j v_j = \sum_{i=d+1}^{d+\ell} \gamma_i v_i$. A $v_1, \dots, v_{d+\ell}$ vektorok lineáris függetlensége miatt az csak úgy lehet, hogy az $\beta_1 = \dots = \beta_d = \gamma_{d+1} = \dots = \gamma_{d+\ell} = 0$. Tehát a $\phi v_{d+1}, \dots, \phi v_{d+\ell}$ vektorok a ϕV képtér egy bázisát alkotják, ezért $\dim \phi V = \ell = \dim V - \dim \ker \phi$.

A dimenziótételből adódik:

Egy egyszerű izomorfizmus-kritérium: Legyen $\phi : V \rightarrow W$ lineáris leképezés. Ekkor ϕ akkor és csak akkor izomorfizmus, ha $\ker \phi = (0)$ és $\dim V = \dim W$.

Alkalmazás (Lagrange-interpoláció): Legyen V az n -nél alacsonyabb fokú \mathbb{F} feletti polinomok tere, és legyenek a_1, \dots, a_n páronként különböző \mathbb{F} -beli elemek. Legyen $\phi : V \rightarrow \mathbb{F}^n$ az

$$f(x) \mapsto \begin{pmatrix} f(a_1) \\ f(a_2) \\ \vdots \\ f(a_n) \end{pmatrix}$$

leképezés. A ϕ leképezés lineáris, hiszen a kép minden koordinátájában lineáris. A mag:

$$\ker \phi = \{f(x) \mid \deg f(x) < n, f(a_1) = \dots = f(a_n) = 0\} = \{0\},$$

hiszen csak a 0 az az n -nél alacsonyabb fokú polinom, amelynek lehet n különböző gyöke. A dimenziótétel miatt $\phi V = \mathbb{F}^n$, tehát ϕ izomorfizmus és így létezik inverze. A $\phi^{-1} : \mathbb{F}^n \rightarrow V$ leképezés adott b_1, \dots, b_n értékekhez azt az egyértelműen meghatározott n -nél alacsonyabb fokú $f(x)$ polinomot rendeli, amelyre $f(a_1) = b_1, \dots, f(a_n) = b_n$.

Megjegyzés. A behelyettesítés-interpoláció páros speciális esetként tartalmazza a népszerű diszkrét Fourier transzformációt (DFT, ld. később). Ha $n + d$ pontot helyettesítünk be, az $f(x)$ n -nél alacsonyabb fokú polinom meghatározható az $n + d$ hely közül bármely n helyen felvett érték segítségével. Ha $d/2$ -nél kevesebb helyen elrontjuk a behelyettesített értékeket, a polinom akkor is visszaállítható. Ezen az ötleten alapulnak az úgynevezett (általánosított) Reed-Solomon kódok.

1.3.3. Alkalmazás: a Shamir-féle titokmegosztási rendszer

A feladatban n résztvevő között szeretnénk egy titkot megosztani úgy, hogy közülük semelyik $n - 1$ -nek ne legyen semennyi információja se a titokról, együttesen viszont meg tudják fejteni.

Legyen \mathbb{F} egy véges test, $|\mathbb{F}| > n$, a titok \mathbb{F} egy eleme lesz. Előzetesen szétosztunk az n résztvevő között n különböző $\alpha_1, \dots, \alpha_n$ nem-nulla elemet az \mathbb{F} testből. Tegyük fel, hogy a titok a $\beta \in \mathbb{F}$ elem. Választunk függetlenül és egyenletesen $\beta_1, \dots, \beta_{n-1}$ véletlen elemet \mathbb{F} -ből. Legyen $f(x) = \beta + \sum_{i=1}^{n-1} \beta_i x^i$. Az i -edik résztvevőnek az $f(\alpha_i)$ értéket küldjük el titkos csatornán.

Ekkor $f(x)$ egy n -nél alacsonyabb fokú polinom, így n helyen ismerve az értékét egyértelműen meg tudjuk határozni Lagrange-interpoláció segítségével. A β titok az $f(x)$ polinom konstans tagja, amit tehát az n résztvevő együtt ki tud találni.

Tegyük fel, hogy $n - 1$ résztvevő találkozik, mondjuk az első $n - 1$. Tekintsük a

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

behelyettesítő leképezést. A ϕ leképezés bijekció \mathbb{F}^n és \mathbb{F}^n között. (Két bijekció kompozíciója: az első az n -nél alacsonyabb polinomok azonosítása együtttható-sorozatukkal, a második pedig a behelyettesítés-interpoláció páros.) Így rögzített β -ra a

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

leképezés is bijekció \mathbb{F}^{n-1} és \mathbb{F}^{n-1} között, tehát – mivel a $\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}$ vektort egyenletesen választottuk \mathbb{F}^{n-1} -ből –

az $\begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$ vektor egyenletes eloszlású \mathbb{F}^{n-1} -ben, β értékétől teljesen függetlenül. Azaz az $\begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$ vektor

eloszlása minden β -ra ugyanaz. Más szavakkal $\begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_{n-1}) \end{pmatrix}$ semmilyen statisztikai információt nem szolgáltat β -ról.

1.3.4. Lineáris leképezések kompozíciója

Kompozíció. $\phi : V \rightarrow V', \phi' : V' \rightarrow V''$ lineáris leképezések. Ekkor a $\phi' \phi$ kompozíció $((\phi' \phi)v = \phi'(\phi v))$ egy $V \rightarrow V''$ lineáris leképezés. A kompozíció asszociatív: ha még $\phi'' : V'' \rightarrow W$ akkor $\phi''(\phi' \phi) = (\phi'' \phi') \phi$ és mindkét oldalról lineáris:

$$(\alpha_1 \phi'_1 + \alpha_2 \phi'_2)(\beta_1 \phi_1 + \beta_2 \phi_2) = \alpha_1 \beta_1 \phi'_1 \phi_1 + \alpha_1 \beta_2 \phi'_1 \phi_2 + \alpha_2 \beta_1 \phi'_2 \phi_1 + \alpha_2 \beta_2 \phi'_2 \phi_2.$$

Az asszociativitás alapján a 2-nél több tényező (de értelmes) kompozíciókban elhagyhatjuk a zárójeleket.

Inverz tulajdonságai. $(\phi \psi)^{-1} = \psi^{-1} \phi^{-1}$ és $(\phi^{-1})^{-1} = \phi$.

Hatványozás. $\phi : V \rightarrow V$ lineáris transzformáció, $k > 0$ egész. $\phi^k := \phi \cdots \phi$ (k tényező); $\phi^0 = I_V$; $\phi^{-k} = (\phi^{-1})^k$.

1.4. Mátrixok

1.4.1. Definíció, formális műveletek

$m \times n$ -es mátrix. $\sim m \times n$ -es táblázat \mathbb{F} -beli elemekkel. Az elemenkénti műveletekkel $m \times n$ dimenziós vektorteret alkotnak.

Mátrixszorzás. Ha $A = (a_{ij})$ egy $m \times \ell$ -es, $B = (b_{ij})$ pedig egy $\ell \times n$ -es mátrix, akkor AB az a (d_{ij}) $m \times n$ -es mátrix, ahol

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

Szavakban: az AB szorzat i -edik sorának j -edik eleme az A mátrix i -edik sorának és a B mátrix j -edik oszlopának a "skaláris" szorzata.

Tulajdonságok. A szorzás asszociatív és mindkét változójában lineáris (értelemszerűen a megfelelő méreteknek egyezniük kell). A szorzat tényezői általában nem felcserélhetők (gyakran nem is végezhető el a szorzás a fordított sorrendben).

Példák.

- diagonális mátrixok:

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

ahol az üres helyeken 0-k állnak.

$$\text{diag}(a_1, \dots, a_n)\text{diag}(b_1, \dots, b_n) = \text{diag}(a_1b_1, \dots, a_nb_n),$$

ezért az azonos méretű diagonális mátrixok felcserélhetők a szorzásra nézve.

- egységmátrix $I_n = \text{diag}(1, \dots, 1)$ (n darab 1-es)
- felső háromszög-mátrixok

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

Transzponált mátrix:. Ha A egy $m \times n$ -es (a_{ij}) mátrix, akkor A^T az az $n \times m$ -es (a'_{ij}) mátrix, amelyre $a'_{ij} = a_{ji}$. Ha A egy $m \times n$ -es, B pedig egy $n \times k$ -es mátrix, akkor $(AB)^T = B^T A^T$.

Blokk-mátrixok szorzása. Gyakran hasznos a következő: Legyen A felbontható $m \times \ell$ darab A_{ij} részmátrixra, B pedig $\ell \times n$ darab B_{ij} részmátrixra:

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1\ell} \\ A_{21} & A_{22} & \dots & A_{2\ell} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \dots & A_{m\ell} \end{pmatrix}, \quad B = \begin{pmatrix} B_{11} & \dots & B_{1n} \\ B_{21} & \dots & B_{2n} \\ B_{31} & \dots & B_{3n} \\ \vdots & \ddots & \vdots \\ B_{\ell 1} & \dots & B_{\ell n} \end{pmatrix},$$

ahol minden $1 \leq i \leq m$, $1 \leq k \leq \ell$, $1 \leq j \leq n$ -re A_{ik} -nak ugyanannyi oszlopa van, mint ahány sora B_{kj} -nek. Ekkor a $D = AB$ szorzat felbontható $m \times n$ darab D_{ij} részmátrixra:

$$D = \begin{pmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ D_{m1} & D_{m2} & \dots & D_{mn} \end{pmatrix},$$

ahol

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

Szavakban: kompatibilis blokk-felbontás esetén a mátrixszorzat blokkjai a tényezők a blokkjaiból a szokásoshoz hasonló eljárással kaphatók. (A skalárok szorzása és összeadása helyett mátrixok szorzását és összeadását tekintjük. Vigyázat, számíts szorzásnál a tényezők sorrendjére!)

1.4.2. Lineáris leképezések mátrixa

Definíció: Legyen $\phi : V \rightarrow W$ lineáris leképezés, v_1, \dots, v_n bázis V -ben, w_1, \dots, w_m pedig bázis W -ben. Ekkor $j = 1, \dots, n$ -re $\phi v_j = \sum_{i=1}^m \alpha_{ij} w_i$. Az $m \times n$ -es $A = (\alpha_{ij})$ mátrix a ϕ mátrixa a v_1, \dots, v_n , illetve w_1, \dots, w_m bázisokra vonatkozóan.

Lineáris transzformációkra ($W = V$) szokásos egyetlen bázist kijelölni mind a bemeneti, mind a kimeneti oldalra. A $\phi : V \rightarrow V$ mátrixa a v_1, \dots, v_n bázisban tehát valójában a $(v_1, \dots, v_n), (v_1, \dots, v_n)$ bázispárra vonatkozó mátrix.

Példa: permutációmátrixok. Legyen π az $\{1, \dots, n\}$ indexhalmaz egy permutációja (azaz $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ bijektív leképezés). Legyen V egy n -dimenziós vektortér egy v_1, \dots, v_n bázissal. Legyen továbbá ϕ az a lineáris transzformáció az \mathbb{R}^n -en, ami az i -edik báziselemet $\pi(i)$ -be viszi. ($\phi v_i = v_{\pi(i)}$ és legyen $P = (p_{ij})$ a ϕ transzformáció mátrixa a v_1, \dots, v_n bázisban. Ekkor

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

Tehát P minden egyes sorában és oszlopában pontosan egy darab 1 áll és a többi elem 0. Ez a tulajdonság jellemzi is a báziselemek permutációból kapható mátrixokat. Az $(12 \dots n)$ ciklushoz tartozó mátrix a következő:

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

Mátrixhoz tartozó lineáris leképezés: Legyen v_1, \dots, v_n bázis V -ben, w_1, \dots, w_m pedig bázis W -ben, $A = (\alpha_{ij})$ pedig egy $m \times n$ -es mátrix. Ekkor egyértelműen létezik egy olyan $\phi : V \rightarrow W$ lineáris leképezés, aminek a mátrixa A a $(v_1, \dots, v_n), (w_1, \dots, w_m)$ bázispárra vonatkozóan.

Biz.: Legyen $u_j = \sum_{i=1}^m \alpha_{ij} w_i$. Tudjuk, hogy egyértelműen létezik olyan ϕ , amelyre $\phi v_j = u_j$ $j = 1, \dots, n$. ϕ mátrixa éppen A .

Megjegyzés: Ha $V = \mathbb{F}^n$, $W = \mathbb{F}^m$, $v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, \dots , $v_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ és $w_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$, \dots , $w_m = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$, (előbbieket

n hosszú, utóbbiak m hosszú oszlopvektorok) akkor a fenti ϕ éppen az n hosszú oszlopvektorok A -val való (balról) szorzása. (Egy korábbi példában ϕ_A -val jelölt leképezés.)

1.4.3. Műveletek transzformációkkal és mátrixokkal

Rögzített bázisok esetén megfelelnek egymásnak. Leképezések lineáris kombinációjának a mátrixa az egyedi mátrixok lineáris kombinációja, a kompozíciónak pedig a mátrixok szorzata lesz a mátrixa. Utóbbi pontosabban: ha $\phi : V \rightarrow V'$ és $\phi' : V' \rightarrow V''$ lineáris leképezések, B bázis V -ben, B' bázis V' -ben, B'' bázis V'' -ben, ϕ mátrixa a B, B' bázispárra vonatkozóan A , ϕ' mátrixa a B', B'' bázispárra vonatkozóan A' , akkor a $\phi' \phi$ kompozíció mátrixa a B, B'' bázispárra vonatkoztatva $A'A$.

Biz. Egyszerű számolás (HF).

Inverz: Legyen A egy $n \times n$ -es mátrix. Legyen $V = \mathbb{F}^n$, az n hosszú oszlopvektorok tere és $\phi : V \rightarrow V$ az A -val való balról szorzás. Azt mondjuk, hogy A **invertálható (nemelfajuló, reguláris, nem-szinguláris)**, ha a $\phi : V \rightarrow V$ lineáris

transzformáció bijektív. Ez esetben az A mátrix A^{-1} inverze a ϕ^{-1} lineáris leképezés mátrixa szintén a $v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$,

\dots , $v_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ bázisban felírva. Ha A invertálható, akkor $A^{-1}A = AA^{-1} = I_n$. A dimenziótétel miatt ϕ akkor

és csak akkor invertálható, ha $\ker \phi = 0$ és ez azzal is ekvivalens, hogy $\phi V = V$. Ezért, ha létezik B , amelyre $BA = I_n$ vagy $AB = I_n$, akkor A invertálható. Ez esetben $A^{-1} = B$. (Ez a véges dimenziós vektorterek sajátossága,

végtelen dimenzióban elképzelhető, hogy egy transzformációnak csak egyoldali inverze van.) Következésképpen ha A invertálható, akkor A^{-1} is és $(A^{-1})^{-1} = A$. Ha A és B invertálható mátrixok, akkor $(AB)^{-1} = B^{-1}A^{-1}$.

Szinguláris (elfajuló) mátrix, lineáris transzformáció: nem invertálható négyzetes mátrix illetve lineáris transzformáció.

Áll.: Egy A négyzetes mátrix akkor és csak akkor invertálható, ha oszlopai lineárisan függetlenek.

Biz.: A fenti értelmezésben az A -val való balról szorzás képtere az A oszlopai által generált altér. Ez pont akkor a teljes tér, ha ezen oszlopvektorok lineárisan függetlenek.

Példa (Vandermonde-mátrix). Legyen V az n -nél alacsonyabb fokú \mathbb{F} feletti polinomok tere és a_1, \dots, a_n páronként különböző \mathbb{F} -beli elemek. Legyen $\phi : V \rightarrow \mathbb{F}^n$ az

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

leképezés. Ekkor ϕ mátrixa az

$$(1, x, \dots, x^{n-1}), \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

bázispárra vonatkozóan

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

Mivel a behelyettesítés bijekció V és \mathbb{F}^n között, M egy invertálható mátrix (és az inverze a Lagrange-interpoláció mátrixa).

1.4.4. Báziscsere

Báziscsere mátrixa: Legyen V -ben v_1, \dots, v_n és v'_1, \dots, v'_n két bázis. Ekkor létezik $C = (c_{ij})$ illetve $C' = (c'_{ij})$ $n \times n$ -es mátrixok, amelyekre: $v'_j = \sum_{i=1}^n c_{ij} v_i$ illetve $v_j = \sum_{i=1}^n c'_{ij} v'_i$ ($j, k = 1, \dots, n$). Innen

$$v_j = \sum_{k=1}^n c'_{kj} v'_k = \sum_{k=1}^n \sum_{i=1}^n c'_{kj} c_{ik} v_i = \sum_{i=1}^n \sum_{k=1}^n c_{ik} c'_{kj} v_i.$$

Mivel v_1, \dots, v_n bázis, $\sum_{k=1}^n c_{ik} c'_{kj} = \delta_{ij}$. (Kronecker delta: $\delta_{ii} = 1$ és $\delta_{ij} = 0$ $i \neq j$ esetén.) Tehát $CC' = I_n$, az $n \times n$ -es egységmátrix, így C invertálható és $C' = C^{-1}$.

Megjegyzés: Fenti C mátrix a $v_i \mapsto v'_i$ leképezés lineáris kiterjesztésének a mátrixa a $(v_1, \dots, v_n), (v_1, \dots, v_n)$ bázispárra vonatkozóan. A C' mátrix pedig a $v'_i \mapsto v_i$ leképezés lineáris kiterjesztésének a mátrixa a $(v'_1, \dots, v'_n), (v'_1, \dots, v'_n)$ bázispárra vonatkozóan.

Fontosabb megjegyzés: Fenti C mátrix az identikus leképezés mátrixa a $(v'_1, \dots, v'_n), (v_1, \dots, v_n)$ bázispárra vonatkozóan. A $C' = C^{-1}$ mátrix pedig az identikus leképezés mátrixa a $(v_1, \dots, v_n), (v'_1, \dots, v'_n)$ bázispárra vonatkozóan.

Báziscsere hatása lineáris leképezések mátrixára: Legyenek V -ben v_1, \dots, v_n és v'_1, \dots, v'_n két bázis; W -ben pedig w_1, \dots, w_m és w'_1, \dots, w'_m két bázis. Legyen a $\phi : V \rightarrow W$ lineáris transzformáció mátrixa a $(v_1, \dots, v_n), (w_1, \dots, w_m)$ vonatkozóan A . Legyenek $C, C' = C^{-1}$ a fenti mátrixok V két adott bázisára, illetve $D, D' = D^{-1}$ a hasonlóan definiált mátrixok W két bázisára. Ekkor ϕ mátrixa a $(v'_1, \dots, v'_n), (w'_1, \dots, w'_m)$ bázispárra vonatkozóan

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

Ha a $\phi : V \rightarrow V$ lineáris transzformáció ($W = V$) mátrixa a v_1, \dots, v_n bázisban (azaz a $(v_1, \dots, v_n), (v_1, \dots, v_n)$ bázispárra vonatkozó mátrixa) A , akkor ϕ mátrixa a v'_1, \dots, v'_n bázisban a

$$C^{-1}AC$$

konjugált mátrix.

Biz. A "fontosabb megjegyzés" és a kompozíció mátrixára vonatkozó eredmény alapján $\phi = I_W \phi I_V$ mátrixa az új bázispárra éppen $D^{-1}AC$. A második állítás az első állítás speciális esete.

Hasonló mátrixok. Két $n \times n$ -es A és A' mátrix hasonló, ha létezik egy olyan invertálható C $n \times n$ -es mátrix, amelyre $A' = C^{-1}AC$. A báziscsere tulajdonsága alapján A és A' hasonló, ha ugyanannak a lineáris transzformációnak a mátrixai két (esetleg) különböző bázisban felírva. Az A -val való balról szorzás mátrixa a standard bázisban A a C oszlopaiból álló bázisban $C^{-1}AC$.

Műveletek konjugált mátrixokkal.

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

Példa: Legyen M a következő $2n \times 2n$ -es mátrix:

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

ahol A, B, C, D $n \times n$ -es mátrixok. Cseréljük ki az első báziselemet az $n + 1$ -edikkel, a másodikat az $n + 2$ -edikkel, és így tovább. A báziscsere mátrixa

$$T = \begin{pmatrix} & I \\ I & \end{pmatrix},$$

ahol I most az $n \times n$ -es I_n egységmátrix. Mivel $T^2 = I_{2n}$, $T^{-1} = T$. A blokk-mátrixok szorzását használva könnyen adódik, hogy

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

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

1.5. Determináns

1.5.1. Mátrixok determinánisa, példák

Permutációk, előjel: Az $\{1, \dots, n\}$ halmaz egy permutációja egy $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ bijektív leképezés. A különböző permutációk száma $n!$, köztük van az identikus is. Egy $1 \leq i < j \leq n$ pár inverzió π -ben, ha $\pi(i) > \pi(j)$. A π permutáció páros, ha páros sok inverziót tartalmaz, egyébként pedig páratlan. A π permutáció $\text{sgn}(\pi)$ előjele 1, ha π páros, a páratlan esetben pedig -1 . Az $\text{sgn}()$ függvény multiplikatív:

$$\text{sgn}(\pi_1 \pi_2) = \text{sgn}(\pi_1) \text{sgn}(\pi_2).$$

Determináns: Legyen $A = (a_{ij})$ egy $n \times n$ -es mátrix. Ekkor

$$\det A = \sum_{\pi} \text{sgn}(\pi) \prod_{i=1}^n a_{i, \pi(i)},$$

ahol az összegzés az $\{1, \dots, n\}$ halmaz $n!$ permutációjára vonatkozik.

Példák:

- $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ -ra $\det A = ad - bc$.

- Az általános 3×3 -as $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ mátrix determinánisa 6 tagú:

$$a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

- Ha π egy permutáció és P a mátrixa, akkor $\det P = \text{sgn}(\pi)$.
- Egy alsó vagy felső háromszögmátrix determinánisa a diagonális elemek szorzata.
- Legyen $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ alakú, ahol A és C négyzetes. Ekkor $\det M = \det A \cdot \det C$.

- Legyenek $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$, $D = \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$. Ekkor $\det A = \det B = \det C = \det D = 0$, míg $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = -abcd$, mutatva azt, hogy $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ nem számítható ki pusztán $\det A$, $\det B$, $\det C$, $\det D$ felhasználásával.

1.5.2. Oszlop és sor szerinti kifejtés

Kifejtési tétel (Laplace): Legyen $A = (a_{ij})$ egy $n \times n$ -es mátrix. Adott (i, j) párra legyen C_{ij} az $(n-1) \times (n-1)$ -es mátrix, amely A -ból az i -edik sor és a j oszlop elhagyásával adódik. Emellett a jelölés mellett tetszőleges $1 \leq i, j \leq n$ -re

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

Biz.: Egyszerű számolás.

1.5.3. Elemi tulajdonságok:

Transzponált mátrix determinánsa: $\det A^T = \det A$

Oszlopokban lineáris: Legyen A egy $n \times n$ -es mátrix. Adott $1 \leq j \leq n$ indexre és $v \in \mathbb{F}^n$ vektorra jelöljük $A_j(v)$ -vel azt a mátrixot, amit úgy kapunk, hogy az A mátrix j -edik oszlopát helyettesítjük v -vel. (Megj.: $A_j(v)$ nem függ A -nak a j -edik oszlopában levő elemektől, csak a többitől.) Ezzel a jelöléssel:

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

Biz.: A j -edik oszlop szerinti kifejtésből.

Hasonló állítás fogalmazható meg sorokra is.

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 $\det A = 0$.

Biz. Kétszer alkalmazva a kifejtési tételt, nézzük meg egy $n - 2 \times n - 2$ -es aldetermináns együtthatóját.

Sor- és oszlopműveletek hatása.

- $\det A$ nem változik, ha A egy oszlopához (sorához) hozzáadjuk egy másik oszlopának (sorának) skalárszorosát.
Biz.: Tegyük fel, hogy az i -edik oszlophoz adjuk a j -edik oszlop α -szorosát. A j -edik oszlop szerinti linearitásból adódik, hogy az új mátrix determinánsa az eredeti determinánsnak és annak a mátrixnak a determinánsának az összege, amely úgy adódik az eredetiből, hogy az i -edik oszlopot kicseréljük a j -edik oszlop α -szorosával. Ebből a sorokra vonatkozó állítás transzponálás segítségével nyerhető.
Megj. Az i -edik oszlophoz a j -edik oszlop α -szorosának a hozzáadása az $I + \alpha E_{ji}$ mátrixszal való jobbról szorzást jelenti, ahol E_{ji} az az $n \times n$ -es mátrix, amely minden eleme 0, kivéve az i -edik sor j -edik helyét, ahol pedig 1 áll. A hasonló sorművelethez pedig az $I + \alpha E_{ij}$ mátrixszal történő balról szorzás tartozik.
- $\det A$ nem változik, ha A egy oszlopához (sorához) hozzáadjuk néhány, tőle különböző indexű oszlopának (sorának) egy tetszőleges lineáris kombinációját.
Biz.: Az előző eredményt alkalmazzuk többször.
- $\det A$ α -szorosára változik, ha A egy oszlopát (sorát) α -szorosára kicseréljük.
Megj.: A -nak egy diagonális mátrixszal való jobbról szorzása A oszlopainak a diagonális mátrix megfelelő elemivel való beszorzását eredményezi. A balról szorzás pedig a sorokra ugyanezt. A determináns a diagonális elemek szorzatával (azaz a diagonális mátrix determinánsával szorzódik).
- $\det A$ előjelet vált (-1 -szeresére változik), ha A két oszlopát megcseréljük.
Megj.: Egy $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ permutáció mátrixa az az $n \times n$ -es (p_{ij}) mátrix, amelyre $p_{ij} = 0$, ha $i \neq \pi(j)$ és $p_{ij} = 1$, ha $i = \pi(j)$. Egy mátrixnak egy permutáció mátrixával való jobbról szorzás az oszlopok megfelelő permutálását jelenti, a balról szorzás pedig a sorok permutálását. Ezek a műveletek a determinánst a permutáció előjelével szorozzák meg.

Nem invertálható mátrixok determinánása. Ha A nem invertálható akkor $\det A = 0$.

Biz.: Tegyük fel, hogy A nem invertálható, azaz az oszlopai lineárisan összefüggenek. Az oszlopok egy nem 0-t adó lineáris kombinációjából nyerhető, hogy valamely oszlop előáll a többi oszlop lineáris kombinációjaként. Levonva ezt a kombinációt az adott oszlopból, a determináns nem változik, ugyanakkor lesz egy csupa 0-ból álló oszlop, ami szerint kifejtve 0 determinánst kapunk.

Megj.: Ha A sorai lineárisan összefüggenek, $\det A$ akkor is 0. (Az előző állításból transzponálással.)

1.5.4. Szorzat determinánása

Determinánsok szorzástétele.: Ha A és B $n \times n$ -es mátrixok, akkor

$$\det(AB) = (\det A)(\det B).$$

Biz.: B determinánása, és ezért a $(\det A)(\det B)$ jobboldal lineáris B bármelyik oszlopa szerint. Belátjuk ezt a $\det(AB)$ baloldaltól is. A B mátrix j -edik oszlopa szerinti linearitáshoz vegyünk észre, hogy tetszőleges v n hosszú oszlopvektorra $A \cdot B_j(v) = (AB)_j(v)$, ezért

$$\det(A \cdot B_j(\lambda u + \mu v)) = \det((AB)_j(\lambda u + \mu v)) = \lambda \det((AB)_j(u)) + \mu \det((AB)_j(v)) = \lambda \det(A \cdot B_j(u)) + \mu \det(A \cdot B_j(v)).$$

Legyenek $v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, ..., $v_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$. Ekkor $\det B$ B első sora szerinti linearitása miatt

$$\det(A) \det(B) = b_{11} \det(A) \det(B_1(v_1)) + b_{21} \det(A) \det(B_1(v_2)) + \dots + b_{n1} \det(A) \det(B_1(v_n))$$

és $\det(AB)$ B első sora szerinti linearitása miatt

$$\det(AB) = b_{11} \det(A \cdot B_1(v_1)) + b_{21} \det(A \cdot B_1(v_2)) + \dots + b_{n1} \det(A \cdot B_1(v_n)).$$

Ennek megfelelően elegendő belátni, hogy

$$\det(A \cdot B_1(v_i)) = \det A \det B_1(v_i) \quad (i = 1, \dots, n).$$

A $B_1(v_i)$ mátrixok olyan mátrixok, amelyek első oszlopában pontosan egy darab 1-es van, a többi elem 0. Elegendő tehát a $\det(AB) = \det A \det B$ egyenlőséget olyan B mátrixokra igazolni, amelyek első sorában pontosan egy darab 1-es van, a többi elem 0. Az ilyen B mátrixok kezelését második oszlop linearitásának felhasználásával folytatjuk. Azt kapjuk, hogy immár elegendő olyan B mátrixokkal foglalkozni, amelyekben az első két oszlop mindegyikében pontosan egy darab 1-es van, a többi elem 0. Így folytatva végül is arra jutunk, hogy elég a $\det(AB) = \det A \det B$ egyenlőséget arra az esetre belátni, amikor B minden oszlopában pontosan egy darab 1-es van, a többi elem 0. Ha egy ilyen B valamely sora 0, akkor $\det B = 0$, továbbá van két megegyező oszlopa, így az AB szorzatnak is, ezért $\det(AB)$ is 0, tehát ez esetben az egyenlőség triviálisan teljesül. Végül is elég azzal az esettel foglalkozni, amikor B egy permutációmátrix. Mivel

$$\det A = \det A^T \text{ és } \det(AB) = \det((AB)^T) = \det(B^T A^T),$$

az A^T mátrixra (B megtartása mellett) ugyanez a visszavezetés működik, tehát A -ról is feltehető, hogy permutációmátrix. Permutációmátrixok determinánása a megfelelő permutációk előjelével egyezik meg, így a fennmaradó eset a permutációk előjelének multiplikatívitasából adódik.

Fontos megjegyzés.: Ez a bizonyítás szó szerint átmegy tetszőleges kommutatív egységelemes gyűrűk feletti négyzetes mátrixok determinánására, például olyan mátrixok esetére, amelyeknek az elemei testek feletti polinomok.

Következmény.: Ha A invertálható (más neveken reguláris, etc.), akkor $\det A \neq 0$ és $\det A^{-1} = \frac{1}{\det A}$.

Következmény.: A invertálható $\Leftrightarrow \det A \neq 0 \Leftrightarrow A^T$ invertálható.

Következmény.: A invertálható $\Leftrightarrow A$ sorai lineárisan függetlenek $\Leftrightarrow A$ oszlopai lineárisan függetlenek.

1.5.5. Inverz mátrix előjeles aldeterminánsokkal

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

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

Biz.: Legyen A tetszőleges $n \times n$ -es mátrix és A'' az az $n \times n$ -es (a''_{ij}) mátrix, amelynek elemeire $a''_{ij} = (-1)^{i+j} \det C_{ji}$. Ekkor

$$\sum_{k=1}^n a_{ik} a''_{kj} = \delta_{ij} \det A,$$

ugyanis $i = j$ -re éppen $\det A$ -nak az i -edik sor szerinti kifejtését látjuk, különben pedig annak a mátrixnak a determinánsának a j -edik sora szerinti kifejtését, amelyet úgy kapunk A -ból, hogy a j -edik sorát lecseréljük az i -edikre (következésképpen két sora egyenlő).

Megj.: Igazából azt láttuk be, hogy

$$AA'' = (\det A)I_n$$

akkor is, ha A nem feltétlenül invertálható. Hasonlóan igazolható $A''A = (\det A)I_n$.

1.5.6. Lineáris transzformációk determinánsa

Legyen ϕ egy $V \rightarrow V$ lineáris transzformáció és legyen ϕ mátrixa a B bázisban A . Ha B' egy másik bázis, amelyre a $B \leftrightarrow B'$ báziscseréhez tartozó mátrixok C illetve C^{-1} , akkor ϕ mátrixa a B' bázisban $C^{-1}AC$, a determinánsok szorzástétele miatt

$$\det(C^{-1}AC) = \det C^{-1} \det A \det C = \det A \det C^{-1} \det C = \det A \det(C^{-1}C) = \det A \det I = \det A,$$

így ϕ mátrixának a determinánsa független a bázis választásától. Más szavakkal, hasonló mátrixok determinánsa megegyezik.

1.6. Lineáris egyenletrendszerek

1.6.1. Definíció

Egy lineáris egyenletrendszer egy

$$Ax = b$$

alakú egyenletrendszer, ahol $A = (a_{ij})$ egy $m \times n$ -es mátrix, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ változó-vektor és $b \in \mathbb{F}^m$. Az egyenletrendszer mátrixa A , a *kibővített mátrixa* az $(A|b)$ $m \times (n+1)$ mátrix.

1.6.2. Megoldás Gauss-eliminációval

Ha egy egyenlethez (a kibővített mátrix egy sorához) egy másik egyenlet (sor) skalárszorosát adjuk, az eredetivel ekvivalens egyenletrendszert kapunk. Nyilván megváltoztathatjuk a rendszerben az egyenletek (azaz a kibővített mátrix sorainak) sorrendjét is. Egy kis óvatossággal átindexelhetjük a változókat (azaz a kibővített mátrix első részének oszlopait is cserélgethetjük). Az ilyen lépéseknél a szükséges óvatosság abban áll, hogy az új egyenletrendszerre kapott megoldásokra majd vissza kell csinálni az átindexelést. Ha csak nem az összes együttható 0, átindexeléssel (oszlop-cserével) és esetleges sorcserével elérhető, hogy az első egyenletben az első változó (a mátrix bal felső eleme) nem 0 együtthatóval szerepel. Ezután az első egyenlet (sor) alkalmas többszörösét levonva a többiből kiküszöböljük az első változót. Így a maradék $m-1$ egyenletben csak az x_2, \dots, x_n változók szerepelnek nem 0 együtthatóval. Az eljárást rekurzív módon folytatjuk a maradék $m-1$ egyenletre és $n-1$ változóra, egészen addig, amíg csupa 0 együtthatót nem kapunk. Az eredmény r darab egyenlet lesz valamilyen r -re, az elsőben az x_1 a legelső változó, aminek az együtthatója nem 0, a másodikban x_2 , és így tovább. A többi $n-r$ egyenletben nem szerepelnek változók. Ha van ezek között olyan, aminek a jobboldalán $b_j \neq 0$ áll, akkor nyilván nincs az egyenletrendszernek megoldása.

Ha nincs ilyen, folytatásként az első egyenletből a többi alkalmas lineáris kombinációját levonva elérhetjük, hogy az első r változó közül az első egyenletben csak az x_1 szerepeljen nem 0 együtthatóval. Hasonlóan, $i = 2, \dots, r$ -re elérhető, hogy az i -edik egyenletben az első r változó közül csak az x_i szerepeljen. (Így az egyenletrendszer kibővített mátrixának felső $r \times r$ -es blokkja diagonális, és mindkét alsó blokkja $((n-r) \times r)$, illetve $(n-r) \times (n-r+1)$ -es része csupa 0.) Leosztva x_1, \dots, x_r együtthatójával és a maradék változókat tartalmazó kifejezéseket átvéve a jobboldalra x_1, \dots, x_r -re konstansokat és esetleg az x_{r+1}, \dots, x_n változókat tartalmazó lineáris kifejezéseket kapunk, amelyek $n > r$ esetén az x_{r+1}, \dots, x_r tetszőleges értéke mellett megoldást adnak.

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:

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

Az első sort levonjuk másodikból:

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

A második sort levonjuk a negyedikből:

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

A második sort levonjuk az ötödikből:

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

A harmadik sort levonjuk a negyedikből:

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

Az utolsó sor a $0 = 1$ ellentmondásnak felel meg, ez az egyenletrendszer tehát nem megoldható. Ha viszont az utolsó, $x_2 + x_5 = 1$ egyenlet helyett az $x_2 + x_5 = 0$ áll, akkor az eljárás eddigi részével az utóbbi mátrixunk helyett az

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

mátrixot kapjuk. Levonjuk a második sort az elsőből:

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

és itt az első 3×3 -as blokk már diagonális. Ekkor a megoldás: x_4, x_5 tetszőleges és $x + 1 = x_5 + 1$, $x_2 = x_5$, $x_3 = x_4 + 1$.

1.6.3. A Cramer-szabály

Tekintsük az $m = n$ esetet. Jelölje $j = 1, \dots, n$ -re $A_j(b)$ azt a mátrixot, amely úgy kapható A -ból, hogy a j -edik oszlopát helyettesítjük a b oszlopvektorral. Ha $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ egy megoldása az $Ax = b$ egyenletnek, akkor

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

Biz.: Jelölje a_k az A mátrix k -edik oszlopát ($k = 1, \dots, n$). Mivel $b = Ax = \sum_{k=1}^n x_k a_k$, az $A_j(b)$ mátrix illetve az $A_j(x_k a_k)$ mátrixok determinánsának j -edik oszlopa szerinti kifejtéseket összevetve azt kapjuk, hogy $\det A_j(b) = \sum_{k=1}^n \det(A_j(x_k a_k))$. Vegyük észre, hogy $k \neq j$ esetén $\det A_j(x_k a_k) = 0$, hiszen az $A_j(x_k a_k)$ mátrix j -edik oszlopa a k -edik oszlop x_k -szorososa. Ezért

$$\det A_j(b) = \det A_j(x_j a_j) = x_j \det A_j(a_j) = x_j \det A.$$

Következésképp:

Cramer-szabály. Legyenek $A, x, b, A_j(b)$ mint fent. Tegyük fel továbbá, hogy $\det A \neq 0$. Ekkor

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

1.7. A Gauss-elimináció további alkalmazásai

1.7.1. Mátrix rangja:

Lineárisan független oszlopok maximális száma.: Az oszlopok közül kiválasztható max. lineárisan független rendszerek mérete azonos: maximális független rendszer = az oszlopok által generált tér egy, az oszlopok közül kiválasztott bázisa.

Max. invertálható négyzetes részmátrix. Egy invertálható részmátrixot tartalmazó oszlopok nyilván függetlenek. Fordítva, ha van r független n hosszú oszlopunk, akkor sorcserékkel és elemi oszlopműveletekkel elérhetjük, hogy a felső $r \times r$ -es részmátrix felső háromszög alakú legyen. Az érintett (a felső r -be mozgatott) r sorhoz tartozó részmátrix invertálható.

Lineárisan független sorok maximális száma.: Transzponált gondolatmenettel szintén ugyanaz, mint a legnagyobb méretű invertálható részmátrix.

1.7.2. Rang és determináns kiszámítása Gauss-eliminációval

Az eliminációs lépések (oszlopok illetve sorok cseréje, skalárszorosának levonása más oszlopokból, illetve sorokból) megtartják a rangot és a determináns értékét kontrollált módon változtatják meg (esetleg előjelet vált vagy nem változik). Ilyen lépésekkel a mátrix háromszög alakra (sőt, végül is diagonális alakra) hozható. Nagy méretű mátrixokra sokkal gyorsabb, mint a determinánst kifejteni vagy az összes négyzetes részmátrixot végignézni.

HF.: Mutassuk meg, hogy egy lineáris egyenletrendszer akkor és csak akkor megoldható, ha a kibővített mátrixának a rangja megegyezik a kibővítetlen mátrixának (a változók együtthatóiból álló mátrixnak) a rangjával.

1.8. Sajátértékek, sajátvektorok, sajátalterek

1.8.1. Definíció

Sajátvektor, sajátérték. : Legyen $\phi : V \rightarrow V$ lineáris transzformáció. A $0 \neq v \in V$ vektor sajátvektora ϕ -nek $\lambda \in \mathbb{F}$ sajátértékkel, ha

$$\phi v = \lambda v.$$

Áll.: Ha $\phi v = \lambda v$ és $\phi v' = \lambda v'$, akkor $\phi(\alpha v + \alpha' v') = \lambda(\alpha v + \alpha' v')$,

Sajátalter.: és így a λ sajátértékhez tartozó sajátvektorok a 0-val együtt egy alteret alkotnak, a λ sajátértékhez tartozó sajátalteret.

Példa.: $\phi : V \rightarrow V$ szinguláris $\Leftrightarrow 0$ egy sajátértéke. Ekkor a magtér a megfelelő sajátalter.

Példa. Az \mathbb{R}^n -en a $\pi : v \mapsto v - \frac{u^T v}{u^T u} u$ ($0 \neq u \in \mathbb{R}^n$) vetítésnek u egy sajátvektora 0 sajátértékkel, az u^\perp hipersík minden nem 0 vektora pedig sajátvektor 1 sajátértékkel. Az $\langle u \rangle$ egyenesen és az u^\perp hipersíkon kívül nincs sajátvektor: ha $v \in \mathbb{R}^n \setminus \langle u \rangle \setminus u^\perp$, akkor $v = \alpha u + w$ alakú, ahol $0 \neq \alpha \in \mathbb{F}$ és $0 \neq w \in u^\perp$ és így $\pi v = w \notin \langle v \rangle$. Tehát π -nek pontosan két sajátértéke van: 0 és 1. A hozzájuk tartozó sajátalterek pedig $\langle u \rangle$ illetve u^\perp .

1.8.2. Sajátalterek együttesen

Alterek lineáris függetlensége. A $(0) \neq W_1, \dots, W_s \leq V$ alterek lineárisan függetlenek, ha $w_1 + \dots + w_s = 0$ ($w_1 \in W_1, \dots, w_s \in W_s$) esetén $w_1 = \dots = w_s = 0$.

Megj.: A $v_1, \dots, v_s \in V$ vektorok akkor és csak akkor lineárisan függetlenek, ha az általuk generált 1 dimenziós alterek lineárisan függetlenek.

Áll.: A $(0) \neq W_1, \dots, W_s \leq V$ alterek lineárisan függetlenek $\Leftrightarrow \dim(W_1 + \dots + W_s) = \dim W_1 + \dots + \dim W_s$

Biz.: HF

A sajátalterek lineárisan függetlenek. Tegyük fel, hogy $\lambda_1, \dots, \lambda_s$ páronként különböző sajátértékei ϕ -nek továbbá v_i sajátvektora ϕ -nek λ_i sajátértékkel ($i = 1, \dots, s$): $\phi v_1 = \lambda_1 v_1, \dots, \phi v_s = \lambda_s v_s$. Ekkor $v_1 + \dots + v_s = 0$ esetén $v_1 = \dots = v_s = 0$.

Biz.: Az alterek s száma szerinti indukció. Az $s = 1$ eset triviális. tegyük fel, hogy $s \geq 2$ és $v_1 + \dots + v_s = 0$. Ekkor

$$0 = \phi(v_1 + \dots + v_s) = \lambda_1 v_1 + \dots + \lambda_s v_s$$

és

$$0 = \lambda_1 v_1 + \dots + \lambda_1 v_s.$$

Kivonva egymásból a két egyenlőséget azt kapjuk, hogy

$$(\lambda_2 - \lambda_1)v_2 + \dots + (\lambda_s - \lambda_1)v_s = 0,$$

ezért az indukciós feltevés miatt itt minden tag 0, ami $\lambda_j \neq \lambda_1$ ($j \neq 1$) miatt csak úgy lehet, ha $v_2 = \dots = v_s = 0$. Ekkor v_1 nyilván 0.

Köv.: A sajátalterek dimenzióinak összege legfeljebb $\dim V$. Legfeljebb $\dim V$ különböző sajátérték van.

Köv.: Ha a $\phi : V \rightarrow V$ lineáris transzformációnak $\dim V$ különböző sajátértéke van, akkor van V -nek ϕ sajátvektoraiból álló bázisa.

Diagonalizálható mátrixok. Az A $n \times n$ -es \mathbb{F} -beli elemű mátrix diagonalizálható \mathbb{F} felett, ha hasonló egy diagonális mátrixhoz, azaz ha van olyan C szintén $n \times n$ -es \mathbb{F} feletti elemű mátrix, amelyre $C^{-1}AC$ diagonális. Ez utóbbi akkor és csak akkor teljesül, ha C oszlopai az A -nak egy sajátvektorokból álló bázisát alkotják. Tehát A pontosan akkor diagonalizálható, ha létezik \mathbb{F}^n -nak A sajátvektoraiból álló bázisa.

1.8.3. Karakterisztikus polinom

Legyen V egy n dimenziós vektortér az \mathbb{F} test felett, $\phi : V \rightarrow V$ lineáris transzformáció, $\lambda \in \mathbb{F}$ skalár.

Áll.: λ sajátértéke ϕ -nek $\Leftrightarrow \lambda I - \phi$ nem invertálható $\Leftrightarrow \det(\lambda I - \phi) = 0$.

Karakterisztikus polinom. Legyen V egy bázisában ϕ mátrixa A és tekintsük az $xI_n - A$ mátrixot (elemei $\mathbb{F}[x]$ -beli polinomok). Ennek $\det(xI_n - A)$ determinánsa egy $\mathbb{F}[x]$ -beli 1 főegyütthatós n -ed fokú polinom. Tekintsünk egy másik bázist, ahol a báziscsere mátrixa C . Ebben a bázisban ϕ mátrixa az új bázisban $C^{-1}AC$ lesz. Az $\mathbb{F}[x]$ polinomgyűrű felett számolva

$$\begin{aligned} \det(xI_n - C^{-1}AC) &= \det(C^{-1}(xI_n - A)C) \\ &= \det C^{-1} \det(xI_n - A) \det C \\ &= \det C \det C^{-1} \det(xI_n - A) \\ &= \det I_n \det(xI_n - A) \\ &= \det(xI_n - A). \end{aligned}$$

Itt a második egyenlőségénél a mátrixok szorzástételét az $\mathbb{F}[x]$ gyűrű felett használtuk. Tehát a

$$\det(xI - \phi) := \det(xI_n - A)$$

polinom független a bázis választásától. Elnevezés: a ϕ lineáris transzformáció karakterisztikus polinomja. Egy B $n \times n$ -es mátrix karakterisztikus polinomja ennek megfelelően $\det(xI_n - B)$. Hasonló mátrixok karakterisztikus polinomja megegyezik.

HF.: Mi lesz $\det(xI_n - A)$ konstans tagja? Mi lesz az $n - 1$ -ed fokú tag együtthatója?

Áll.: $\lambda \in \mathbb{F}$ sajátértéke ϕ -nek (A -nak) $\Leftrightarrow \lambda$ gyöke ϕ (A) karakterisztikus polinomjának.

Köv.: $\mathbb{F} = \mathbb{C}$ esetén minden lineáris transzformációnak van legalább egy sajátértéke.

Blokk-háromszög alakú mátrix determinánsa és karakterisztikus polinomja.: A diagonális blokkok determinánsának illetve karakterisztikus polinomjának a szorzata. Azaz ha A

$$A = \begin{pmatrix} A_{11} & & & \\ A_{21} & A_{22} & & \\ \vdots & \vdots & \ddots & \\ A_{r1} & A_{r2} & \dots & A_{rr} \end{pmatrix} \text{ vagy } A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1r} \\ & A_{22} & \dots & A_{2r} \\ & & \ddots & \vdots \\ & & & A_{rr} \end{pmatrix}$$

alakú $n \times n$ -es, ahol az A_{ii} diagonális blokk $n_i \times n_i$ méretű ($i = 1, \dots, r$). Ekkor

$$\det A = \prod_{i=1}^r \det A_{ii},$$

illetve

$$\det(xI_n - A) = \prod_{i=1}^r \det(xI_{n_i} - A_{ii}).$$

Biz.: Egyszerű a determináns definícióját használva.

1.8.4. Spektrálfelbontás spec. esetben

Négyzetmentes polinom.: aminek nincs többszörös gyöke.

Áll. Ha egy komplex test feletti vektortér lineáris transzformációjának (egy négyzetes mátrixnak) a karakterisztikus polinomja négyzetmentes, akkor van sajátértékeiből álló bázis (diagonalizálható, azaz hasonló egy diagonális mátrixhoz).

Példa (DFT).: Legyen $\phi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ az a lineáris transzformáció, amely a (standard) bázis elemeit ciklikusan permutálja: $\phi v_i = v_{i+1}$ (ahol $v_{n+1} := v_1$). Legyen $\omega = e^{2\pi i/n}$.

- (HF) ϕ karakterisztikus polinomja $x^n - 1$
- $x^n - 1$ gyökei $1 = \omega^0, \omega, \dots, \omega^{n-1}$

- (HF) $w_j := \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{j(n-1)} \end{pmatrix}$ sajátvektora ϕ -nek ω^{-j} sajátértékkel

- a $v_i \mapsto w_i$ báziscsere mátrixa

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

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

Példa nem diagonalizálható mátrixra:. Legyen

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Ekkor M karakterisztikus polinomja x^2 , így M -nek csak a 0 a sajátértéke. Tegyük fel, hogy M diagonalizálható, azaz hasonló a

$$D = \begin{pmatrix} d_1 & \\ & d_2 \end{pmatrix}$$

mátrixhoz. Ekkor M és D karakterisztikus polinomjai és így sajátértékei is megegyeznek. Mivel D -nek d_1 és d_2 is sajátértéke, az csak úgy lehet, hogy $D = 0$. Azonban hasonló mátrixok rangja is ugyanaz, tehát, mivel M rangja 1, M nem lehet hasonló a 0 mátrixhoz sem.

1.9. A Jordan-féle normálalak

1.9.1. Invariáns altér

Def.: Az $U \leq V$ altér invariáns a $\phi : V \rightarrow V$ lineáris transzformációra, (vagy más szavakkal egy ϕ -invariáns altér), ha $u \in U$ esetén $\phi u \in U$ is teljesül. Például ϕ sajátalterei, vagy a ϕ néhány sajátvektora által generált altér ϕ -invariánsak.

HF.: Mutassuk meg, hogy ha $\phi, \psi : V \rightarrow V$ két felcserélhető lineáris transzformáció (azaz $\phi\psi = \psi\phi$), akkor ϕ tetszőleges sajátaltère ψ -invariáns.

Blokk-háromszög alak.: Egészítsük ki az $U \leq V$ ϕ -invariáns altér egy u_1, \dots, u_m bázisát V egy

$$u_1, \dots, u_m, v_{m+1}, \dots, v_n$$

bázisává. Ebben a bázisban ϕ mátrixa felső blokk háromszög, azaz

$$\begin{pmatrix} A & B \\ & C \end{pmatrix}$$

alakú, ahol a bal felső $m \times m$ -es blokkban ϕ U -ra való megszorításának A mátrixa látható az u_1, \dots, u_m bázisban, a bal alsó $(n - m) \times m$ -es blokk csupa 0.

1.9.2. Direkt összeg, komplementer altér

Direkt összeg (belső):. A V vektortér direkt összege a $0 < V_1, \dots, V_\ell \leq V$ altereknek (Jelölés: $V = V_1 \oplus \dots \oplus V_\ell$), ha minden $v \in V$ vektor egyértelműen előáll $v = v_1 + \dots + v_\ell$ alakban, ahol $v_1 \in V_1, \dots, v_\ell \in V_\ell$. Kicsit más megfogalmazásúan $V = \langle V_1, \dots, V_\ell \rangle$ és a V_1, \dots, V_ℓ alterek lineárisan függetlenek.

Példa: bázis. A $0 \neq v_1, \dots, v_n$ vektorok bázist alkotnak V -ben $\Leftrightarrow V = \langle v_1 \rangle \oplus \dots \oplus \langle v_n \rangle$

Példa: külső direkt összeg. W_1, \dots, W_ℓ vektorterek. $V = \{(w_1, \dots, w_\ell) | w_i \in W_i\}$, összeadás: koordinátánként. Legyen $V_i = \{(w_1, \dots, w_\ell) \in V | w_j = 0 \text{ ha } j \neq i\} \cong W_i$. Ekkor $V = V_1 \oplus \dots \oplus V_\ell$. Azonosítva V_i -t W_i -vel azt is mondjuk, hogy V a W_1, \dots, W_ℓ vektorterek (külső) direkt összege.

Komplementer altér.: Legyen $U \leq V$. Ekkor U egy komplementere egy olyan $W \leq V$ altér, amelyre $V = U \oplus W$. Ha U egy bázisát kiegészítjük V egy bázisává, az U -ba nem eső báziselemek pl. egy komplementer alteret generálnak.

Invariáns alterek direkt összege.: Tegyük fel, hogy $V = V_1 \oplus \dots \oplus V_\ell$, ahol a $V_1, \dots, V_\ell \leq V$ alterek invariánsak a $\phi : V \rightarrow V$ lineáris transzformációra. Legyen B_i bázis V_i -ben és tekintsük V -nek azt a bázisát, amelynek első $|B_1|$ eleme B_1 elemei, ezt követik B_2 elemei, és így tovább. Ebben a bázisban ϕ mátrixa blokk diagonális:

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_\ell \end{pmatrix}$$

Az i -edik blokkban ϕ -nek a $V_i \times V_i$ -re való megszorításának B_i bázisban felírt A_i mátrixa áll.

Fontos példa. Ha ϕ -nek $\dim V$ különböző sajátértéke van, az 1 dimenziós sajátaltér direkt összege szerinti felbontás $\leftrightarrow \phi$ mátrixának diagonalizálása.

1.9.3. Nilpotens transzformációk

Lemma. Tegyük fel, hogy $\phi^k v = 0$ valamely $0 \neq v \in V$ -re és $k > 0$ egészre, és tegyük fel, hogy k a legkisebb ilyen szám. Ekkor a $v, \phi v, \dots, \phi^{k-1} v$ vektorok lineárisan függetlenek. Következésképpen $k \leq \dim V$.

Biz. k szerinti indukcióval. A $k = 1$ eset nyilvánvaló. A $k > 1$ esetben ϕv -re $k - 1$ az a legkisebb ℓ kitevő, amelyre $\phi^\ell \phi v = 0$, így az indukciós feltevés miatt a $\phi v, \phi^2 v, \dots, \phi^{k-1} v$ vektorok lineárisan függetlenek. Legyen $U = \langle \phi v, \phi^2 v, \dots, \phi^{k-1} v \rangle$. Vegyük észre hogy U fenti bázisának minden elemére és így persze U minden u vektorára igaz, hogy $\phi^{k-1} u = 0$. Viszont $\phi^{k-1} v \neq 0$, ezért $v \notin U$ és így az egész $v, \phi v, \dots, \phi^{k-1} v$ rendszer lineárisan független.

Definíció. Egy $\phi : V \rightarrow V$ lineáris transzformáció nilpotens, ha $\phi^k = 0$ valamely k természetes számra. A lemma miatt ez azzal egyenértékű, hogy $\phi^n = 0$ ($n = \dim V$) és azzal is, hogy minden $v \in V$ vektorra $\phi^{k_v} v = 0$ valamely $k_v > 0$ egészre.

Példa. Deriválás n -nél alacsonyabb fokú polinomokra. Az összes polinom példája mutatja, hogy a végtelen dimenziós térben a harmadik feltétel nem elegendő.

Jordan-bázis nilpotens transzformációkra. Legyen $\phi : V \rightarrow V$ nilpotens lin. transzformáció. Ekkor léteznek olyan $n_1 \geq n_2 \geq \dots \geq n_t$ pozitív egészek, és v_1, \dots, v_t vektorok, amelyekre a $v_1, \phi v_1, \dots, \phi^{n_1-1} v_1, \dots, v_t, \phi v_t, \dots, \phi^{n_t-1} v_t$ a V tér egy bázisát alkotják és $\phi^{n_i} v_i = 0$. Azaz létezik olyan bázisa a V térnek, amelyben ϕ mátrixa

$$\begin{pmatrix} \boxed{\begin{matrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{matrix}} & & & & \\ & & \dots & & & & \\ & & & \dots & & & \\ & & & & \boxed{\begin{matrix} 1 & & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{matrix}} & & & \end{pmatrix}$$

alakú. A t valamint az n_1, \dots, n_t számok egyértelműek.

Biz. A létezés indukció $\dim V$ szerint. Mivel $\phi^n V = (0)$, nem lehet $\phi V = V$. Legyen $W = \phi V$. Ekkor W -re alkalmazzuk az indukciós feltevést: léteznek olyan $w'_1, \dots, w'_s \in W$ vektorok, és n'_1, \dots, n'_s számok, amelyekre a $w_1, \phi w_1, \dots, \phi^{n'_1-1} w_1, \dots, w_s, \phi w_s, \dots, \phi^{n'_s-1} w_s$ a W altér egy bázisát alkotják, továbbá $\phi^{n'_i} w_i = 0$ ($i = 1, \dots, s$). Könnyen ellenőrizhető, hogy a $\phi^{n'_1-1} w_1, \dots, \phi^{n'_s-1} w_s$ vektorok szükségszerűen a ϕ transzformáció W -re való megszorításának a magjának (azaz a $W \cap \ker \phi$ altérnek) egy bázisát alkotják. Legyenek $t = \dim \ker \phi$ és v_{s+1}, \dots, v_t olyan vektorok, amelyek a $\phi^{n'_1-1} w_1, \dots, \phi^{n'_s-1} w_s$ rendszert a $\ker \phi$ magtér bázisává egészítik ki. Legyenek továbbá $n_1 = n'_1 + 1, \dots, n_s = n'_s + 1, n_{s+1} = \dots = n_t = 1$. A $v_1, \phi v_1, \dots$ vektorok száma $\sum_{i=1}^t n_i = \sum_{i=1}^s n'_i + s + t - s = \dim \phi V + t = \dim \phi V + \dim \ker \phi = \dim V$. Azt kell tehát belátni, hogy vektoraink lineárisan függetlenek. Tegyük fel, hogy az $\alpha_{11} v_1 + \alpha_{12} \phi v_1 + \dots + \alpha_{1n_1} \phi^{n_1-1} v_1 + \dots + \alpha_{s1} v_s + \alpha_{s2} \phi v_s + \dots + \beta_{s+1} v_{s+1} + \dots + \beta_t v_t$ lineáris kombináció a nulla vektort adja. Alkalmazzuk az összegre a ϕ leképezést. Kapjuk, hogy az $\alpha_{11} w_1 + \alpha_{12} \phi w_1 + \dots + \alpha_{s1} w_s + \alpha_{s2} \phi w_s + \dots + \alpha_{sn_s} \phi^{n'_s-1} w_s$ kombináció is nulla. Ebből – mivel a $w_1, \phi w_1, \dots$ vektorok lineárisan függetlenek – adódik, hogy az összes α_{ij} együttható 0, kivéve esetleg a ϕ alkalmazásával kieső α_{in_i} együtthatókat. Beírva a nullákat az eredeti kombinációba, marad a $0 = \alpha_{1n_1} \phi^{n_1-1} v_1 + \dots + \alpha_{sn_s} \phi^{n_s-1} v_s + \beta_{s+1} v_{s+1} + \dots + \beta_t v_t$ egyenlőség. Itt a jobboldalon $\ker \phi$ egy bázisának elemeiből képzett lineáris kombinációja látható, ezért mind a "maradék" α együtthatók, mind a β együtthatók is nullák. Így tényleg lineárisan független rendszerünk van.

Az egyértelműség: $t = \# \text{láncok}$, $\dim \ker \phi^2 - \dim \ker \phi = \# \text{legalább 2 hosszú láncok}$, $\dim \ker \phi^j - \dim \ker \phi^{j-1} = \# \text{legalább } j \text{ hosszú láncok}$.

1.9.4. Általánosított sajátvektor, sajátaltér

Általánosított sajátvektor.: Legyen λ egy skalár. A $0 \neq v \in V$ vektor ϕ -nek általánosított sajátvektora ϕ -nek λ sajátértékkel, ha $(\phi - \lambda I)^k v = 0$ valamely k pozitív egészre. A lemma miatt ez azzal ekvivalens, hogy $(\phi - \lambda I)^n = 0$ ($n = \dim V$). A sajátérték elnevezést az indokolja, hogy ha k a legkisebb, a feltételnek elegendő szám, akkor $(\phi - \lambda I)^{k-1} v$ sajátvektora ϕ -nek λ sajátértékkel.

Általánosított sajátaltér.: Ha λ sajátvektora ϕ -nek, akkor a λ -hoz tartozó általánosított sajátaltér $\ker(\phi - \lambda I)^n$. (Azaz a λ -hoz tartozó általánosított sajátvektorokból és 0 vektorból álló altér.) Ez egyben a legtágabb altér, amelyen $\phi - \lambda I$ nilpotens.

Áll.: Legyen V_λ a $\phi : V \rightarrow V$ lineáris transzformáció λ sajátértékéhez tartozó általánosított sajátaltere. Legyen m_λ a λ gyök multiplicitása ϕ karakterisztikus polinomjában. (Azaz a karakterisztikus polinom $(x - \lambda)^{m_\lambda} g(x)$, ahol $g(\lambda) \neq 0$. Ekkor $\dim V_\lambda = m_\lambda$.)

Biz.: Olyan bázist veszünk, amelynek első néhány vektora V_λ egy bázisa. Egy ilyen bázisban ϕ mátrixa blokk felső háromszög alakú:

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

és így a karakterisztikus polinom az A mátrix illetve a C mátrix karakterisztikus polinomjainak a szorzata. A ϕ transzformációnak a V_λ altérre való megszorításának megfelelő A mátrix a karakterisztikus polinomja $(x - \lambda)^{\dim V_\lambda}$. (Ez a következőképpen látható: Legyen $W_0 = V_\lambda$, $W_i = (\phi - \lambda I)W_{i-1}$. Ekkor $W_k = 0$ valamely $k \leq n$ számra. Vegyük W_{k-1} egy bázisát, majd ezt egészítsük ki W_{k-2} egy bázisává, és így tovább. Így végül V_λ olyan bázisát kapjuk, amelyben ϕ (és $xI - \phi$) mátrixa alsó háromszög alakú csupa λ -val (illetve $(x - \lambda)$ -val) a főátlóban.)

Jelöljük $h(x)$ -szel a C mátrix karakterisztikus polinomját, Ekkor ϕ karakterisztikus polinomja $(x - \lambda)^{\dim V_\lambda} h(x)$, ahol $h(x) = g(x)(x - \lambda)^t$ valamely $t \geq 0$ egészre. Tegyük fel, hogy $h(\lambda) = 0$. Ekkor $(C - \lambda I)w = 0$ valamely nem csupa nulla $n - \dim V_\lambda$ hosszú w oszlopvektorra. Legyen v egy olyan vektor V -ben, amelyet ha felírunk a választott bázisunkban, a "hátsó" koordináták éppen a w oszlopvektort adják ki. Ekkor $(\phi - \lambda I)v$ "hátsó" koordinátái éppen a $(C - \lambda I)w = 0$ oszlopvektort adják, ezért $(\phi - \lambda I)v \in V_\lambda$, és így $v \in V_\lambda$, ellentmondás azzal hogy v "hátsó" koordinátái a $w \neq 0$ vektort adják. Tehát $h(\lambda) = 0$, és így $h(x) = g(x)$ és $m_\lambda = \dim V_\lambda$.

Áll.: Ha $\lambda \neq \mu$ skalárok, k_1, k_2 pozitív egészek és $v \in V$, amelyekre $(\phi - \lambda I)^{k_1} v = (\phi - \mu I)^{k_2} v = 0$, akkor $v = 0$.

Biz. Ha valamely α skalárra $(\phi - \alpha I)v = 0$, akkor $\phi v = \alpha v$. Ha $\alpha \neq \lambda$, akkor $(\phi - \lambda I)v = (\alpha - \lambda)v$. Ezért $(\phi - \lambda I)^{k_1} v = (\phi - \lambda)^{k_2} v = 0$, ahonnan $v = 0$. Hasonlóan kapjuk a $v = 0$ egyenlőséget az $\alpha = \lambda$ esetben, hiszen akkor $\alpha \neq \mu$ és λ helyett μ használható. Feltehető tehát, hogy $(\phi - \alpha I)v \neq 0$ semelyik α skalárra sem. Ekkor tetszőleges α skalárra legyen U_α az a legszűkebb v -t tartalmazó altér V -nek, amely $\phi - \alpha I$ -invariáns. Mivel $\phi = (\phi - \alpha I) + \alpha I$, U_α ugyanaz, mint a legszűkebb v -t tartalmazó ϕ -invariáns altér, tehát $U_\alpha = U_0 = U_\beta$ tetszőleges α, β skalárookra. Az $\alpha = \lambda$ választással U_α egy generátorrendszer $v, (\phi - \lambda I)v, \dots, (\phi - \lambda I)^{k_1-1}v$ míg $\alpha = \mu$ választással a kézenfekvő generátorrendszer $v, (\phi - \mu I)v, \dots, (\phi - \mu I)^{k_2-1}v$. Ha $v \neq 0$, akkor legyen u az első sorozatnak azon nem 0 tagja, amelyre $(\phi - \lambda I)u = 0$. Ekkor, mivel u előáll mint a második sorozat tagjainak lineáris kombinációja, így $(\phi - \mu I)^{k_1} u = 0$ és így a már tárgyalt eset miatt $u = 0$, ellentmondás.

Az általánosított sajátaltérek lineárisan függetlenek.: Legyenek v_1, \dots, v_s olyan vektorok, amelyekre $(\phi - \lambda_j I)^n v_j = 0$, ahol $\lambda_1, \dots, \lambda_s$ páronként különböző skalárok. Ekkor a $v_1 + \dots + v_s$ összeg csak úgy lehet 0, hogy $v_1 = \dots = v_s = 0$.

Biz.: s szerinti indukció. Alkalmazzuk az összegre a $(\phi - \lambda_s I)^n$ lineáris transzformációt. kapjuk, hogy $v'_1 + \dots + v'_{s-1} = 0$, ahol $v'_j = (\phi - \lambda_s I)^n v_j$. A $(\phi - \lambda_j I)(\phi - \lambda_s I) = (\phi - \lambda_s I)(\phi - \lambda_j I)$ felcserélhetőségi tulajdonság segítségével a $(\phi - \lambda_j I)^n v'_j = 0$ egyenlőség könnyen igazolható. Így az indukciós feltevés miatt $v'_1 = \dots, v'_{s-1} = 0$. Az előző állítás miatt ebből $v_1 = \dots, v_{s-1} = 0$ következik, majd ezeket beírva az eredeti egyenlőségbe marad a $v_s = 0$ egyenlőség.

Tétel.: $\mathbb{F} = \mathbb{C}$ -re V a ϕ általánosított sajátaltéréinek direkt összege.

Biz.: Ezek az altérek lineárisan függetlenek. Ugyanakkor a ϕ karakterisztikus polinom gyökeinek multiplicitását az általánosított sajátaltérek dimenziójával összekapcsoló állítás alapján a dimenziók összege $\dim V$.

1.9.5. Jordan-bázis

Általánosított sajátaltér Jordan-bázisa: Legyen V_λ a ϕ lineáris transzformációjának λ sajátértékéhez tartozó általánosított sajátaltere. Ekkor $\phi - \lambda I$ megszorítása V_λ -n nilpotens. Ennek a nilpotens transzformációnak egy Jordan-bázisát tekintjük. A V_λ altér egy Jordan-bázisban ϕ megszorításának a mátrixa blokk-diagonális, ahol a főátlóban elhelyezkedő blokkok speciális szerkezetűek:

Jordan-blokk: Legyen $v \in V$, amelyre $(\phi - \lambda I)^m v = 0$, de $v, (\phi - \lambda I)v, \dots, (\phi - \lambda I)^{m-1}v$ lineárisan függetlenek. A $\langle v, (\phi - \lambda I)v, \dots, (\phi - \lambda I)^{m-1}v \rangle$ altér ϕ -invariáns és ϕ megszorításának a mátrixa a $v, (\phi - \lambda I)v, \dots, (\phi - \lambda I)^{m-1}v$ bázisban:

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

Egy ilyen mátrixot **Jordan-blokknak** hívunk. Megfordítva a bázisvektorok sorrendjét,

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

alakú, a fentihez hasonló mátrixot kapunk. Szokás a fenti helyett az ilyen (felső háromszög alakú) mátrixokat tekinteni Jordan-blokknak.

Jordan-normálalak. Egy négyzetes mátrixot Jordan-normálalakúnak hívunk, ha blokk-diagonális, és a főátlóban elhelyezkedő blokkok Jordan-blokkok:

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

illetve felső háromszö-alakban

$$\left(\begin{array}{c} \boxed{\begin{array}{cccc} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \lambda & 1 \\ & & & & \lambda \end{array}} \\ \dots \\ \boxed{\begin{array}{cccc} \mu & 1 & & \\ & \mu & 1 & \\ & & \ddots & \ddots \\ & & & \mu & 1 \\ & & & & \mu \end{array}} \\ \dots \\ \boxed{\begin{array}{cccc} \nu & 1 & & \\ & \nu & 1 & \\ & & \ddots & \ddots \\ & & & \nu & 1 \\ & & & & \nu \end{array}} \end{array} \right)$$

Tétel. $\mathbb{F} = \mathbb{C}$ esetén V -nek van olyan bázisa, amelyben ϕ mátrixa Jordan-normálalakú. (Mátrixokra megfogalmazva: egy négyzetes komplex mátrix hasonló egy Jordan-normálalakú mátrixhoz.) Az adott λ paraméterű és m méretű diagonális blokkok száma a ϕ transzformáció (illetve a mátrix) által egyértelműen meghatározott.

Biz.: Az előző tétel miatt V a ϕ általánosított sajátaltéréinek direkt összege. A λ sajátértékhez tartozó altéren $\phi - \lambda I$ nilpotens így a nilpotens mátrixok Jordan-bázisáról szóló állítás miatt fenti típusú altérek direkt összegére bontható tovább: Létezik V -nek olyan bázisa, amelyben ϕ mátrixa blokk-diagonális és ahol a diagonális blokkok Jordan-blokkok. Ugyanezen tétel alapján az adott λ paraméterű és m méretű diagonális blokkok száma a ϕ egyértelműen meghatározott.

Elnevezés: A mátrix, illetve transzformáció Jordan-normálalakja.

A Hamilton–Cayley-tétel. Legyen $\phi : V \rightarrow V$ lineáris transzformáció és legyen ϕ karakterisztikus polinomja $f(x)$. Ekkor $f(\phi) = 0$. Ha egy A négyzetes mátrix karakterisztikus polinomja $f(x)$, akkor $f(A) = 0$.

Tetszőleges alaptestre igaz. A komplex (következésképpen a valós, a racionális, stb.) számok testje feletti vektorok lineáris transzformációira illetve komplex (valós, racionális) mátrixokra és annak résztestjeire a Jordan-normálalaktól könnyen következik.

Minimálpolinom. Legyen $\phi : V \rightarrow V$ egy lineáris transzformáció és $0 \neq f(x), g(x) \in \mathbb{F}[x]$ polinomok. Ha $f(\phi) = g(\phi) = 0$, továbbá $\deg f(x) \leq \deg g(x)$, akkor $g(x)$ -nek a az $f(x)$ szerinti maradékos osztásánál kapott $h(x)$ $f(x)$ -nél alacsonyabb fokú maradékra is igaz, hogy $h(\phi) = 0$. Ezért egyértelműen létezik egy legalacsonyabb 1 főegyütthatós $f(x)$ polinom, amire $f(\phi) = 0$, továbbá az összes olyan $g(x)$ polinom, amire $g(\phi) = 0$ az $f(x)$ -nek többszöröse $\mathbb{F}[x]$ -ben. A karakterisztikus polinom tehát többszöröse a minimálpolinomnak.

1.10. Euklideszi terek

1.10.1. Szimmetrikus bilineáris függvények:

Bilineáris függvény.: Legyen V vektortér az \mathbb{F} test felett. A $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$ függvény bilineáris, ha mindkét változójában lineáris, azaz

- $\langle u + u', v \rangle = \langle u, v \rangle + \langle u', v \rangle$ és $\langle u, v + v' \rangle = \langle u, v \rangle + \langle u, v' \rangle$ ($\forall u, u', v, v' \in V$)
- $\langle \lambda u, v \rangle = \lambda \langle u, v \rangle$ és $\langle u, \lambda v \rangle = \lambda \langle u, v \rangle$ ($\forall u, v \in V, \lambda \in \mathbb{F}$)

Gram-mátrix.: Legyen v_1, \dots, v_n egy bázis V -ben. A $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$ bilineáris függvény v_1, \dots, v_n bázisára vonatkozó Gram-mátrixa az $A = (a_{ij})$ mátrix, ahol $a_{ij} = \langle v_i, v_j \rangle$. Ha $u = \sum_{i=1}^n \alpha_i v_i$ és $v = \sum_{i=1}^n \beta_i v_i$, akkor a bilinearitás miatt $\langle u, v \rangle = \sum_{i,j=1}^n \alpha_i \beta_j a_{ij}$, tehát egy tetszőleges rögzített bázis esetén a Gram-mátrix egyértelműen meghatározza a bilineáris függvényt. Fordítva, az is világos, hogy az előbbi szabály segítségével minden előírt A mátrixhoz tudunk is olyan bilineáris függvényt fabrikálni, aminek A a Gram-mátrixa. A megfeleltetés nyilván lineáris is, tehát egy izomorfizmust ad a bilineáris függvények tere és az $n \times n$ -es mátrixok tere között.

Példa: Legyen A egy $n \times n$ -es \mathbb{F} -beli elemekből felépülő mátrix. Legyen az \mathbb{F}^n -beli u, v vektorpárokon

$$\langle u, v \rangle = u^T A v.$$

Ekkor \langle, \rangle egy bilineáris függvény \mathbb{F}^n -en, aminek Gram- mátrixa a $v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, v_{n-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} v_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$

vektorokból álló standard bázisban éppen A .

Standard skalárszorzat F^n -en: $(u, v) = u^T v$. A fenti példa $A = I_n$ egységmátrixszal.

Kapcsolat:

$$u^T A v = (u, A v) = (A^T u, v).$$

Az első egyenlőség a standard skalárszorzat definíciója alapján világos, míg a harmadik alak a transzponálás tulajdonsága alapján a következőképpen vezethető le: $(A^T u, v) = (A^T u)^T v = (u^T A) v = u^T (A v)$.

Báziscsere hatása a Gram-mátrixra: Legyen v_1, \dots, v_n és v'_1, \dots, v'_n két bázis V -ben, amelyekben az $\langle, \rangle : V \times V \rightarrow \mathbb{F}$ bilineáris függvény Gram-mátrixa A , illetve A' . Ha az első bázist a másodikba vivő báziscsere mátrixa C , akkor $A' = C^T A C$.

Biz: Legyen $A = (a_{ij}), A' = (a'_{ij}), C = (c_{ij})$. Ekkor

$$\begin{aligned} a'_{ij} &= \langle v'_i, v'_j \rangle = \left\langle \sum_{k=1}^n c_{ki} v_k, \sum_{\ell=1}^n c_{\ell j} v_\ell \right\rangle \\ &= \sum_{k=1}^n c_{ki} \sum_{\ell=1}^n c_{\ell j} a_{k\ell} \end{aligned}$$

Itt adott k -ra a belső összegben az AC mátrix k -adik sorának j -edik eleme áll, majd ez a C^T mátrix i -edik sorának k -edik elemével van megszorozva. Ezért a végső összeg a $C^T A C$ mátrix i -edik sorának j -edik eleme.

Szimmetrikus bilineáris függvény: A $\langle, \rangle : V \times V \rightarrow \mathbb{F}$ bilineáris függvény szimmetrikus, ha $\langle u, v \rangle = \langle v, u \rangle$ tetszőleges $u, v \in V$ esetén. A bázisról történő egyértelmű lineáris kiterjesztés miatt világos, hogy egy bilineáris függvény akkor és csak akkor szimmetrikus, ha Gram- mátrixa valamely (\Leftrightarrow bármely) bázisban szimmetrikus.

Példa: A standard skalárszorzat \mathbb{F}^n -en egy szimmetrikus bilineáris függvény.

Kvadratikus alakok: Legyen F olyan test, amelyben $2(= 1 + 1) \neq 0$. Legyen $A = (a_{ij})$ egy $n \times n$ -es szimmetrikus mátrix, azaz egy szimmetrikus bilineáris függvény Gram-mátrixa. Ekkor $\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ vektorra

$$\underline{x}^T A \underline{x} = \sum_{i=1}^n a_{ii} x_i^2 + \sum_{1 \leq i \neq j \leq n} 2a_{ij} x_i x_j$$

egy homogén másodfokú polinom az x_1, \dots, x_n változóiban. Elnevezés: kvadratikus alak.

Fordítva, ha $Q(\underline{x}) = \sum_{1 \leq i \leq j} b_{ij} x_i x_j$ egy homogén másodfokú polinom, akkor az

$$a_{ii} := b_{ii}, \quad a_{ij} := a_{ji} = \frac{1}{2} b_{ij} \quad (1 \leq i < j \leq n)$$

egyenlőségekkel definiált $A = (a_{ij})$ mátrix szimmetrikus és $\underline{x}^T A \underline{x} = Q(\underline{x})$.

Ortogonalis, ortonormált bázis. A V vektortér v_1, \dots, v_n bázisa ortogonalis a $\langle, \rangle : V \times V \rightarrow \mathbb{F}$ bilineáris függvényre nézve, ha $1 \leq i \neq j \leq n$ esetén $\langle v_i, v_j \rangle = 0$. Ortonormált, ha még $1 \leq i \leq n$ esetén $\langle v_i, v_i \rangle = 1$. Azaz a bázis ortogonalis, ha szerinte felírva \langle, \rangle mátrixa diagonális és ortonormált, ha a mátrix I_n .

Példa. \mathbb{R}^n -ben a standard bázis ortonormált a standard skalárszorzásra nézve. \mathbb{R}^2 -ben az $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ és az $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$ vektorok is ortonormált bázist alkotnak

Merőlegesség, merőleges altér:. Legyen $\langle, \rangle : V \times V \rightarrow \mathbb{F}$ szimmetrikus bilineáris függvény. Azt mondjuk, hogy az $u, v \in V$ vektorok merőlegesek egymásra (\langle, \rangle szerint) – jel.: $u \perp v$ –, ha $\langle u, v \rangle = 0$. Ha G egy részhalmaz V -ben, akkor a G -re merőleges V -beli vektorok egy altérre alkotnak, amelyre a G^\perp jelölést alkalmazzuk. Világos, hogy $G \subseteq H$ esetén $G^\perp \supseteq H^\perp$ és $\langle G \rangle^\perp = G^\perp$. Továbbá $G \subseteq (G^\perp)^\perp$ és így $\langle G \rangle \subseteq (G^\perp)^\perp$.

1.10.2. Euklideszi terek

Definíció:. A $\langle, \rangle : V \times V \rightarrow \mathbb{R}$ szimmetrikus bilineáris függvény

- pozitív definit, ha $\forall 0 \neq v \in V$ vektorra $\langle v, v \rangle > 0$
- pozitív szemidefinit, ha $\forall v \in V$ vektorra $\langle v, v \rangle \geq 0$
- negatív definit, negatív szemidefinit hasonlóan definiálható
- indefinit, ha $\exists u, v \in V$, amelyekre $\langle u, u \rangle > 0$, $\langle v, v \rangle < 0$

Példa:. \mathbb{R}^2 -en $\left\langle \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \right\rangle := \alpha_1\beta_1 - \alpha_2\beta_2$ egy indefinit szimmetrikus bilineáris függvény.

HF. Legyen \langle, \rangle szimmetrikus bilineáris függvény Gram-mátrixa a v_1, \dots, v_n bázisban A .

- Mutassuk meg, hogy ha A akkor és csak akkor szinguláris, ha van olyan $0 \neq v \in V$ vektor, amely merőleges (azaz $\langle v, w \rangle = 0$) minden $w \in V$ vektorra.
- Mutassuk meg, hogy amellett a feltevés mellett, hogy \langle, \rangle pozitív szemidefinit, A akkor és csak akkor szinguláris, ha van olyan $0 \neq v \in V$ vektor, amely merőleges önmagára (azaz $\langle v, v \rangle = 0$).
- Mutassuk meg, hogy a szemidefinititás feltevése nélkül az önmagára merőleges nem-nulla vektor létezése szükséges, de nem elégséges feltétele A szingularitásának.

Euklideszi tér:. Valós vektortér egy pozitív definit \langle, \rangle szimmetrikus bilineáris függvényvel. Euklideszi térben a v vektor **hossza** a $\sqrt{\langle v, v \rangle}$ szám.

Példa: \mathbb{R}^n a standard skalárszorzattal

Euklideszi tér altéré is euklideszi tér:. a \langle, \rangle megszorításával.

Ortonormált bázis létezése:. Legyen V, \langle, \rangle egy euklideszi tér. Ekkor létezik V -ben ortonormált bázis.

Biz. (Gram–Schmidt-ortogonalizáció): Legyen V -nek egy bázisa v_1, \dots, v_n . A definíció miatt $\langle v_1, v_1 \rangle \neq 0$, azaz $v_1 \notin v_1^\perp$; továbbá értelmes és lineáris a

$$\pi : w \mapsto w - \frac{\langle v_1, w \rangle}{\langle v_1, v_1 \rangle} v_1$$

leképezés. Ennek a magja $\langle v_1 \rangle$, képtere pedig v_1^\perp . Cseréljük ki a v_2, \dots, v_n bázisvektorokat rendre a $\pi v_2, \dots, \pi v_n$ vektorokkal. Mivel v_j -ből v_1 skalárszorosa voltunk le, az új rendszer ismét egy bázis és így az új v_2, \dots, v_n vektorok a v_1^\perp altér egy bázisát alkotják. Iteráljuk a konstrukciót a v_1^\perp altérre: tekintsük a $0 \neq v_2 \in v_1^\perp$ vektort, majd folytassuk az eljárást v_1 helyett v_2 -vel a $\{v_1, v_2\}^\perp$ altérben, és így tovább. Az iteráció során mindig olyan vektorokból álló altérekben dolgozunk, amelyek merőlegesek az addig kiválasztott vektorokra. Ezért világos, hogy ortogonális bázist kaptunk. Végül, mivel $\langle v_i, v_i \rangle > 0$, a v_i vektort leosztva $\sqrt{\langle v_i, v_i \rangle}$ -vel ortonormált bázist kapunk.

Megjegyzések.

- A Gram-Schmidt-eljárásban az iteráció végére kialakuló báziscsere mátrixa – mivel minden lépésben egy bázisvektorhoz egy kisebb indexű bázisvektor skalárszorosa adjuk hozzá – olyan felső háromszög alakú mátrix, amelynek a főátlójában csupa 1 áll:

$$\begin{pmatrix} 1 & * & * & \dots & * \\ & 1 & * & \dots & * \\ & & 1 & \dots & * \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix}$$

A normálást is tartalmazó báziscsere mátrixa is felső háromszög alakú, pozitív elemekkel a főátlóban.

- Az utolsó normáló lépés kivételével a módszer alkalmas változata elég széles körben alkalmazható. Például racionális számok feletti vektorok szimmetrikus bilineáris függvényekre is értelmezhető a definités, sőt, a definités helyettesíthető a $V^\perp = (0)$ feltétellel és az alaptestre vonatkozó elég enyhe megszorítással is. (Arra kell vigyázni, hogy esetleg olyan v_i bázisvektorba botlunk, amelyre $\langle v_i, v_i \rangle = 0$. Ebben az esetben v_i -t alkalmas más vektorra le kell cserélni. A testre vonatkozó megszorítás az $1 + 1 \neq 0$ feltétel, azaz a kételemű test és az azt tartalmazó testek kivételével ez a csere $V^\perp = (0)$ esetén mindig végrehajtható.)
- Az eljárás alkalmas egy adott szimmetrikus bilineáris függvény pozitív definitésének eldöntésére is. Ugyanis az eljárás nyilván végigmegy, ha annak során nem jön elő olyan v vektor, amelyre $\langle v, v \rangle \leq 0$. Ekkor viszont a végső v_1, \dots, v_n bázis ortogonális és $\langle v_i, v_i \rangle > 0$, így

$$\left\langle \sum_{i=1}^n \alpha_i v_i, \sum_{i=1}^n \alpha_i v_i \right\rangle = \sum_{i=1}^n \alpha_i^2 \langle v_i, v_i \rangle > 0,$$

ha legalább egy $\alpha_i \neq 0$.

Példa. Legyen V bázisa v_1, v_2, v_3 , és ebben a bázisban legyen a \langle, \rangle Gram-mátrixa

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 4 \\ 1 & 4 & 4 \end{pmatrix}$$

Első menetben a v_2 és v_3 vektorokat vetítjük a v_1^\perp síkra: $v'_2 = v_2 - 2v_1, v'_3 = v_3 - v_1$. A $v_1 \mapsto v_1, v_2 \mapsto v'_2, v_3 \mapsto v'_3$ báziscsere mátrixa

$$\begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

így az új bázisban a Gram-mátrix

$$\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 4 \\ 1 & 4 & 4 \end{pmatrix} \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix}.$$

A következő körben a v'_3 vektort vetítjük a v'_2 -re merőleges egyenesre: $v''_3 = v'_3 - 2v'_2$. Az v_1, v'_2, v''_3 bázisban a Gram-mátrix

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

tehát \langle, \rangle indefinit: $\langle v_1, v_1 \rangle > 0$, de $\langle v''_3, v''_3 \rangle < 0$. A $v_1, v_2, v_3 \rightarrow v_1, v'_2, v''_3$ báziscsere mátrixa

$$\begin{pmatrix} 1 & -2 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Megj. A Gram-mátrix karbantartásánál sok esetben érdemes sorok és oszlopok szerinti Gauss-eliminációként felfogni: Például a v_i v_1^\perp -ra való vetítésénél le kell vonni a j -edik sorból az első sor $\frac{\langle v_1, v_i \rangle}{\langle v_1, v_1 \rangle}$ -szeresét, hogy kiküszöbölődjön az i -edik sor első eleme; ezután pedig az i -edik oszlopból az első oszlop $\frac{\langle v_1, v_j \rangle}{\langle v_1, v_1 \rangle}$ -szeresét vonjuk le, kiküszöbölve az első sor i -edik elemét. A fenti példában először – akárcsak a Gauss-eliminációnál – levonjuk a második sorból az első sor kétszeresét. Az eredmény

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 4 & 4 \end{pmatrix}.$$

Ezután levonjuk az első oszlop kétszeresét a második oszlopból. Az eredmény

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix}.$$

Ennek a két lépésnek az eredménye a \langle, \rangle Gram-mátrixa abban a bázisban, amit úgy kapunk az eredetiből, hogy a második bázisvektort kicseréltük az első bázisvektorra – \langle, \rangle szerint – merőleges vetületére. A harmadik bázisvektor elsőre merőleges vetítésének eredménye két lépésben:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix}, \text{ majd } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix}.$$

Végül az új harmadik bázisvektornak az új másodikkra merőleges vetítésének eredménye két lépésben:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix}, \text{ majd } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

HF.: Mutassuk meg, hogy ha V egy valós vektortér és \langle, \rangle egy szimmetrikus bilineáris függvény V -n és $u \in V$ olyan vektor, amelyre $\langle u, u \rangle = 0$ de $u \notin V^\perp$, akkor \langle, \rangle nem lehet pozitív szemidefinit.

Ennek a megállapításnak a felhasználásával hogyan lehet módosítani a fenti eljárást pozitív szemidefinités eldöntésére?

Megj.: A fenti eljárás segítségével igazolható, hogy \mathbb{R}^n -en \langle, \rangle akkor és csak akkor pozitív definit, ha valamely (bármely) bázisban felírt A Gram-mátrixára igaz az hogy minden $1 \leq j \leq n$ -re A bal felső $n \times n$ -es blokkjának a determinánsa pozitív.

Izometria.: Legyenek V_1, \langle, \rangle_1 és V_2, \langle, \rangle_2 szimmetrikus bilineáris függvényvel ellátott terek. Azt mondjuk, hogy a $\phi : V_1 \rightarrow V_2$ lineáris bijekció izometria a két tér között, ha még tetszőleges $v, w \in V_1$ vektorokra $\langle v, w \rangle_1 = \langle \phi v, \phi w \rangle_2$. A két tér izometrikus, ha létezik közöttük izometria. Az bázisról való (bi)lineáris kiterjesztés miatt ez azzal ekvivalens, hogy létezik a két térnek egy-egy bázisa, amelyekben a bilineáris függvények Gram-mátrixa ugyanaz. Speciálisan:

Azonos dimenziójú euklideszi terek izometrikusak.: Ha v_1, \dots, v_n a V, \langle, \rangle euklideszi tér egy ortonormált

bázisa, akkor a $v_1 \mapsto \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $v_2 \mapsto \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, \dots , $v_{n-1} \mapsto \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$, $v_n \mapsto \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ leképezés lineáris kiterjesztése izometria V, \langle, \rangle

és $\mathbb{R}^n, (\cdot, \cdot)$ között.

Megj.: Az izometria távolságtartó leképezést jelent. A két térben a távolság $\sqrt{\langle u - v, u - v \rangle}$, illetve $\sqrt{\langle u - v, u - v \rangle_2}$. Nem nehéz belátni, hogy a 0-t 0-be vivő $\phi : V_1 \rightarrow V_2$ nem feltétlenül lineáris távolságtartó leképezések éppen a fenti értelemben vett (lineáris) izometriák.

1.10.3. Komplex euklideszi terek

Más nevenek: véges dimenziós Hilbert-terek, unitér terek, Hermite-féle terek, hermitikus terek.

Másfél-lineáris (sesquilinear) függvények.: Legyen V egy komplex test feletti vektortér. A $\langle, \rangle : V \times V \rightarrow \mathbb{C}$ függvény másfél-lineáris, ha második változójában lineáris, az első változójában pedig konjugált-lineáris (avagy antilineáris):

- $\langle u, v + v' \rangle = \langle u, v \rangle + \langle u, v' \rangle$ ($\forall u, v, v' \in V$)
- $\langle u, \lambda v \rangle = \lambda \langle u, v \rangle$ ($\forall u, v \in V, \lambda \in \mathbb{C}$)
- $\langle u + u', v \rangle = \langle u, v \rangle + \langle u', v \rangle$ ($\forall u, u', v \in V$)
- $\langle \lambda u, v \rangle = \bar{\lambda} \langle u, v \rangle$ ($\forall u, v \in V, \lambda \in \mathbb{C}$)

ahol $\bar{\lambda}$ az λ szám komplex konjugáltját jelenti.

Gram-mátrix.: Ugyanaz, mint a bilineáris esetben. Tetszőleges mátrixhoz egyértelműen található olyan másfél-lineáris függvény, amelynek ő a Gram-mátrixa az adott bázisban. (Az első változó szerinti kiterjesztést konjugált-lineárisan kell csinálni.)

Hermitikus függvény (vagy Hermite-féle függvény): Legyen V egy komplex test feletti vektortér. A $\langle, \rangle : V \times V \rightarrow \mathbb{C}$ másfél-lineáris függvény hermitikus, ha konjugált-szimmetrikus:

$$\langle v, u \rangle = \overline{\langle u, v \rangle} \quad \forall u, v \in V.$$

Példa: standard skalárszorzás \mathbb{C}^n -en: $(u, v) = u^*v$.

Mátrixok, vektorok adjungáltja: Az A $m \times n$ -es (a_{ij}) mátrix A^* adjungáltja az az (a'_{ij}) $n \times m$ -es mátrix, amelyre $a'_{ij} = \overline{a_{ji}}$ ($i = 1, \dots, n, j = 1, \dots, m$). Ha A egy $m \times n$ -es mátrix, B pedig egy $n \times k$ -es mátrix, akkor $(AB)^* = B^*A^*$.

Példa: Legyen A egy tetszőleges $n \times n$ -es komplex mátrix. Ekkor $\langle u, v \rangle_A = u^*Av = (u, Av)$ egy másfél-lineáris bilineáris függvény \mathbb{C}^n -en, amelynek Gram-mátrixa a standard bázisban éppen A .

Megj.: $(A^*u, v) = (A^*u)^*v = u^*Av = (u, Av)$.

Báziscsere hatása a Gram-mátrixra: Legyen v_1, \dots, v_n és v'_1, \dots, v'_n két bázis V -ben, amelyekben az $\langle, \rangle : V \times V \rightarrow \mathbb{C}$ hermitikus függvény Gram-mátrixa A , illetve A' . Ha az első bázist a másodikba vivő báziscsere mátrixa C , akkor $A' = C^*AC$.

Biz.: Legyen $A = (a_{ij})$, $A' = (a'_{ij})$, $C = (c_{ij})$. Ekkor

$$\begin{aligned} a'_{ij} &= \langle v'_i, v'_j \rangle = \left\langle \sum_{k=1}^n c_{ki}v_k, \sum_{\ell=1}^n c_{\ell j}v_\ell \right\rangle \\ &= \sum_{k=1}^n \overline{c_{ki}} \sum_{\ell=1}^n c_{\ell j} a_{k\ell} \end{aligned}$$

Itt adott k -ra a belső összegben az AC mátrix k -adik sorának j -edik eleme áll, majd ez a C^* mátrix i -edik sorának k -adik elemével van megszorozva. Ezért a végső összeg a C^*AC mátrix i -edik sorának j -edik eleme.

Megj.: Hermitikus függvényre $\langle u, u \rangle = \overline{\langle u, u \rangle}$, tehát $\langle u, u \rangle$ mindig valós.

Definítség: A valós szimmetrikus esetekkel analóg fogalmak: A $\langle, \rangle : V \times V \rightarrow \mathbb{C}$ hermitikus függvény

- pozitív definit, ha $\forall 0 \neq v \in V$ vektorra $\langle v, v \rangle > 0$
- pozitív szemidefinit, ha $\forall 0 \neq v \in V$ vektorra $\langle v, v \rangle \geq 0$
- negatív definit, negatív szemidefinit hasonlóan definiálható
- indefinit, ha $\exists u, v \in V$, amelyekre $\langle u, u \rangle > 0$, $\langle v, v \rangle < 0$

Komplex euklideszi tér: Komplex vektortér egy pozitív definit \langle, \rangle hermitikus függvénnyel. Euklideszi térben a v vektor **hossza** a $\sqrt{\langle v, v \rangle}$ szám.

Példa: \mathbb{C}^n a standard skalárszorzattal

Euklideszi tér altere is euklideszi tér.

Ortogonalis, ortonormált bázis. A valós szimmetrikus esettel megegyező definíció

Merőlegesség, merőleges altér: A valós szimmetrikus esettel analóg reláció.

Ortonormált bázis létezése: A valós esetre bemutatott Gram-Schmidt-ortogonalizáció működik.

Izometria: A valós esettel azonos definíció.

Azonos dimenziójú euklideszi terek izometrikusak: Ha v_1, \dots, v_n a V, \langle, \rangle euklideszi tér egy ortonormált

bázisa, akkor a $v_1 \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $v_2 \mapsto \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, \dots , $v_{n-1} \mapsto \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$, $v_n \mapsto \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}$ leképezés lineáris kiterjesztése izometria V, \langle, \rangle

és $\mathbb{C}^n, (,)$ között.

Ezután:. Valós vagy komplex euklideszi terekben a $(,)$ jelölést használjuk \langle, \rangle -ra.

Vektorok hossza:. (valós vagy komplex) euklideszi terekben $|v| = \sqrt{(v, v)}$

Valós \rightarrow komplex áttérés. : Legyen v_1, \dots, v_n egy ortonormált bázis egy V valós euklideszi térben. Ekkor V mint valós vektortér izometrikus módon beágyazható egy V' n dimenziós komplex euklideszi térbe (ami a valós test felett $2n$ dimenziós) úgy, hogy a v_1, \dots, v_n báziselemeknek V' egy v'_1, \dots, v'_n ortonormált bázisa felel meg.

konstrukció: $v_1, \dots, v_n \leftrightarrow \mathbb{R}^n$ standard bázisa: $V \leftrightarrow \mathbb{R}^n$ izometria. A beágyazás második része: $\mathbb{R}^n \leq \mathbb{C}^n$ (valós koordinátájú vektorok), és \mathbb{R}^n standard skalárszorosa a \mathbb{C}^n skalárszorzásának megszorítása.

Metaköv:. Fenti beágyazást használva sokszor elég valós euklideszi terekre vonatkozó tételt a komplex esetre igazolni.

Alkalmazás: a Cauchy-Schwarz-egyenlőtlenség:.

- Komplex (vagy valós) euklideszi térben

$$|(u, v)| \leq |u||v|.$$

Biz:. Az ekvivalens $|(u, v)|^2 \leq (u, u)(v, v)$ egyenlőtlenséget igazoljuk. Ha $u = 0$, akkor mindkét oldal 0. Az $u \neq 0$ esetben bontsuk fel v -t u -val párhuzamos és u -ra merőleges vektorok összegére: $v = \mu u + v'$, ahol $\mu = \frac{(u, v)}{(u, u)}$ és $v' = v - \mu u$. Ekkor $(v, v) = |\mu|^2(u, u) + (v', v')$ és $|(u, v)|^2 = |\mu|^2(u, u)^2$. A baloldalon tehát $|\mu|^2(u, u)^2$ áll, míg a jobboldalon $|\mu|^2(u, u)^2 + (u, u)(v', v')$. A két oldal különbsége $(u, u)(v', v')$ a jobboldal javára.

Megj. A bizonyítás során végül is az u és v vektorokat tartalmazó síkban (vagy egyenesen) dolgoztunk.

- Kifejtett alak:

$$\left(\sum_{i=1}^n \overline{x_i} y_i \right) \left(\sum_{i=1}^n x_i \overline{y_i} \right) \leq \left(\sum_{i=1}^n \overline{x_i} x_i \right) \left(\sum_{i=1}^n y_i \overline{y_i} \right).$$

- Négyzetesen integrálható függvényekre

$$\left| \int f(x)g(x)dx \right|^2 \leq \int |f(x)|^2 dx \int |g(x)|^2 dx.$$

(Itt $(h_1(x), h_2(x)) = \int \overline{h_1(x)} h_2(x)$ és a Cauchy-Schwarz-egyenlőtlenséget az $\overline{f(x)}, g(x)$ párra alkalmazzuk.)

1.10.4. Normális mátrixok

Ebben részben a $V = \mathbb{C}^n$ vektortérben dolgozunk, a standard skalárszorzáttal és a mátrixok (hacsak mást nem mondunk) $n \times n$ -es komplex mátrixok. Diagonalizálható mátrixok egy széles körét definiáljuk.

Unitér mátrixok. Az U $n \times n$ -es mátrix unitér, ha $U^*U = I$.

Áll:. U unitér $\Leftrightarrow U^*$ unitér.

Biz:. \Rightarrow : Ha U unitér, akkor $U^* = U^{-1}$, így $(U^*)^*U^* = UU^* = I$.

Áll:. U, U' unitér $\Rightarrow UU'$ unitér.

Áll:. U unitér $\Leftrightarrow U$ oszlopai egy ortonormált rendszert alkotnak $\Leftrightarrow U$ sorai ortonormált rendszert alkotnak.

Átfogalmazva:. Ekvivalensek:

- U unitér
- U a standard bázist egy ortonormált bázisba viszi
- $U : \mathbb{C}^n \rightarrow \mathbb{C}^n$ izometria
- U \mathbb{C}^n valamely ortonormált bázisát ortonormált bázisba viszi
- U \mathbb{C}^n bármely ortonormált bázisát ortonormált bázisba viszi

Schur-felbontás. Tetszőleges $A n \times n$ -es komplex mátrixhoz létezik olyan $U n \times n$ -es unitér mátrix, amelyre $U^{-1}AU$ felső háromszög alakú.

Biz. Indukció n szerint. Legyen v_1 egy 1 hosszú sajátvektora A -nak λ sajátértékkel. Válasszunk olyan v_2, \dots, v_n oszlopvektorokat, hogy a v_1, v_2, \dots, v_n rendszer egy olyan ortonormált bázis legyen \mathbb{C}^n -ben. Legyen U_1 az az $n \times n$ -es mátrix, amelynek j -edik oszlopa v_j . Ekkor U_1 unitér és $U_1^{-1}AU_1$ első oszlopa csupa 0, kivéve esetleg az legelső λ elemet. Legyen A' ennek a mátrixnak a jobb alsó $(n-1) \times (n-1)$ -es blokkja:

$$U_1^{-1}AU_1 = \begin{pmatrix} \lambda & * \\ & \boxed{A'} \end{pmatrix}.$$

Az indukciós feltevés alapján legyen U' egy olyan $(n-1) \times (n-1)$ -es unitér mátrix, amelyre $T' = U'^{-1}A'U'$ felső háromszög alakú. Ekkor az

$$U_2 = \begin{pmatrix} 1 & * \\ & \boxed{U'} \end{pmatrix}$$

mátrix unitér és így

$$U_2^{-1}U_1^{-1}AU_1U_2 = \begin{pmatrix} \lambda & * \\ & \boxed{T'} \end{pmatrix}$$

felső háromszög alakú. Ezért $U = U_1U_2$ egy jó választás.

Megj.: A Schur-felbontás általában nem egyértelmű, de a diagonális elemek az eredeti mátrix sajátértékei. A bizonyításból látható, hogy a háromszögmátrix bal felső eleme az eredeti mátrix tetszőleges sajátértéke lehet.

Def.: A normális, ha felcserélhető az adjungáltjával: $AA^* = A^*A$. (Valósra: $AA^T = A^T A$.)

Példák:

- Diagonális mátrixok
- Önadjungált vagy hermitikus (valósra: szimmetrikus) mátrixok: $A^* = A$ (valósra $A^T = A$)
Megj.: ugyanaz, mintha az $\langle u, v \rangle := (u, Av)$ hermitikus (valósra szimmetrikus)
- Unitér (valósra ortogonális) mátrixok: $U^*U = I$ (valósra $U^T = U$)
- Ferdén hermitikus (valósra ferdén szimmetrikus) mátrixok: $A^* = -A$ ($A^T = -A$).

HF.: Mutassuk meg, hogy egy felső háromszögmátrix akkor és csak akkor normális, ha diagonális.

HF.: Ha U unitér és A normális, akkor $U^{-1}AU$ is normális.

Ebből a két feledatból és a Schur-felbontásból azonnal adódik, hogy

Normális mátrixok jellemzése.: A normális \Leftrightarrow létezik U unitér, hogy $U^{-1}AU$ diagonális.

Megj.: Azaz egy mátrix akkor és csak akkor normális, ha valamely (egyenértékűleg: bármely) Schur-felbontásában szereplő háromszögmátrix diagonális.

Normalitás-jellemzés átfogalmazása.: A normális \Leftrightarrow létezik A -nak sajátvektoraiból álló bázis.

Biz. \Leftarrow : Legyenek u_1, \dots, u_n olyan sajátvektora A -nak, amelyek a \mathbb{C}^n tér egy ortonormált bázisát adják. Legyen U az a mátrix, amelynek j -edik oszlopa u_j . Ekkor U unitér, és mivel a standard bázist az u_1, \dots, u_n sajátvektor-bázisba viszi, $U^{-1}AU$ diagonális mátrix, ahol a főátlóban A sajátértékei állnak.

\Rightarrow : Legyen U egy olyan unitér mátrix, amire $U^{-1}AU$ diagonális. Ekkor U a standard bázist az U oszlopaiból álló ortonormált bázisba viszi, és mivel $U^{-1}AU$ diagonális, ezek a vektorok sajátvektorok is.

Valós ortogonális mátrixok.: O valós mátrix ortogonális, ha komplex mátrixként tekintve unitér: $O^T O = I$.

Példa: Hipersíkra való tükrözés. Legyen $0 \neq u \in \mathbb{C}^n$, $\tau : v \mapsto v - 2 \frac{\langle u, v \rangle}{\langle u, u \rangle} u$. Sajátértékei 1 és -1 , a megfelelő sajátalterek v^\perp , illetve $\langle v \rangle$.

Példa: minden permutációs mátrix ortogonális.

Alkalmazás: DFT és inverz DFT kapcsolata: Legyen $\phi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ az a lineáris transzformáció, amely a (standard) bázis elemeit ciklikusan permutálja: $\phi v_i = v_{i+1}$ (ahol $v_{n+1} := v_1$). Legyen $\omega = e^{2\pi i/n}$. A ϕ transzformáció (mátrixa a standard bázisban) ortogonális, így ϕ normális. Tudjuk, ϕ sajátértékei $\omega^0, \omega^1, \dots, \omega^{n-1}$ és az ω^{-j}

sajátértékhez tartozó 1 hosszú sajátvektor $w_j = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{j(n-1)} \end{pmatrix}$. Ezért az

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

mátrix unitér, tehát $M^{-1} = M^*$. Mivel $M^* = \overline{M}$: az a mátrix, amelyben ω -t kicseréltük $\bar{\omega}$ -ra. Tehát az $\omega \leftrightarrow \bar{\omega}$ csere erejéig az inverz DFT ugyanolyan, mint a DFT.

Mátrixok definitisége: A önadjungált mátrix pozitív szemidefinit (pozitív definit), ha $v^*Av \geq 0$ ($v^*Av > 0$) minden $v \in \mathbb{C}^n$ vektorra.

Megj.: Ekvivalens a $\langle u, v \rangle := (u, Av)$ hermitikus függvény megfelelő definitiségével.

Példa: Ha A tetszőleges $m \times n$ -es mátrix, akkor A^*A pozitív szemidefinit. A^*A pontosan akkor pozitív definit, ha A oszlopai lineárisan függetlenek.

Biz.: HF

Áll.: Legyen U unitér. Ekkor A normális $\Leftrightarrow U^*AU$ normális. Hasonló ekvivalenciák unitér, önadjungált, pozitív definit, pozitív szemidefinit, ferdén hermitikus mátrixokra.

Biz.: HF

Fontos típusok spektruma: Legyen A komplex normális. Ekkor:

- A unitér $\Leftrightarrow A$ sajátértékei 1 abszolút értékűek
- A önadjungált $\Leftrightarrow A$ sajátértékei valósak
- A pozitív szemidefinit $\Leftrightarrow A$ sajátértékei nemnegatív valós számok
- A pozitív definit $\Leftrightarrow A$ sajátértékei pozitív valós számok
- A ferdén hermitikus $\Leftrightarrow A$ sajátértékei tiszta képzetesek

(Az $a + bi$ komplex szám tiszta képzetes, ha $a = 0$.)

Áll.: Ha A valós szimmetrikus akkor létezik \mathbb{R}^n -ben is A sajátvektoraiból álló ortonormált bázis. Másképpen: létezik O valós ortogonális mátrix, hogy $O^T A O$ diagonális.

Biz.: Legyen $\lambda \in \mathbb{R}$ sajátértéke A -nak. Az $(A - \lambda I)\underline{x} = 0$ lineáris egyenletrendszer valós megoldásai ugyanannyi dimenziós teret alkotnak, mint a komplexek. Válasszunk a valós sajátaltereken egy-egy ortonormált bázist. Ezek az előbbi dimenzió-megfontolás alapján összesen n elemet tartalmaznak. Másrészt páronként merőlegesek is egymásra, hiszen $\lambda \neq \mu$, $Av = \lambda v$, $Aw = \mu w$ esetén $\lambda(v, w) = (Av, w) = (v, Aw) = \mu(v, w)$ miatt $(v, w) = 0$.

1.10.5. Projekciók

Projekciók (vetítések): A $\pi : V \rightarrow V$ lineáris transzformáció **projekció** a W altérre, ha $W = \pi V$ és π megszorítása W -re az identitás. Ekkor V nyilván a 0 sajátértékhez tartozó sajátaltér és az 1 sajátértékhez tartozó sajátaltér összege. (Ebben az állításban megengedjük, hogy ezen alterek valamelyike a (0) altér legyen, ebben az esetben 0 vagy 1 a szigorú értelemben nem sajátérték.) Fordítva, ha V előáll a $\pi : V \rightarrow V$ lineáris transzformáció 0 és 1 sajátértékéhez tartozó sajátalterek összegeként, akkor π projekció az 1 sajátértékhez tartozó sajátaltérre.

HF.: Igazoljuk, hogy $\pi : V \rightarrow V$ lineáris transzformáció akkor és csak akkor projekció, ha $\pi^2 = \pi$.

Ortogonalis projekciók (merőleges vetítések): Euklideszi térben egy ortogonalis projekció egy olyan projekció, amely normális lineáris transzformáció, azaz olyan, aminek a mátrixa normális egy (\Leftrightarrow bármely) ortonormált bázisban. Mivel a sajátértékek nemnegatív valós számok, szükségképpen önadjungált (valósra szimmetrikus) és **pozitív szemidefinit**. Egy normális transzformáció projekció \Leftrightarrow (komplex) sajátértékei a $\{0, 1\}$ halmazból kerülnek ki. Pl. a Gram-Schmidt eljárásnál használtunk projekciókat.

Ortogonalis projekció \mathbb{C}^n alterére: Legyen a W altér egy ortonormált bázisa w_1, \dots, w_k . Legyen π egy olyan merőleges vetítés, aminek a képtere W . Ekkor π mátrixa

$$w_1 w_1^* + \dots + w_k w_k^*,$$

illetve \mathbb{R}^n -ben

$$w_1 w_1^T + \dots + w_k w_k^T.$$

Következésképpen π a W altér által egyértelműen meghatározott.

Biz.: A W képtér az 1 sajátvektorhoz tartozó sajátaltér, a magtér pedig W^\perp . Egészítsük ki a w_1, \dots, w_k rendszert egy $w_1, \dots, w_k, w_{k+1}, \dots, w_n$ ortonormált bázissá. Ekkor w_{k+1}, \dots, w_n a W^\perp magtér bázisa. Legyen $v = \sum_{i=1}^n \alpha_i w_i$. Ekkor $(w_i, v) = \alpha_i$ és így

$$\begin{aligned} \pi v &= \pi \sum_{i=1}^n \alpha_i w_i = \sum_{i=1}^k \alpha_i w_i \\ &= \sum_{i=1}^k (w_i, v) w_i = \sum_{i=1}^k (w_i^* v) w_i \\ &= \sum_{i=1}^k (w_i^* w_i) v. \end{aligned}$$

Itt az utolsó egyenlőségnél az azonos hosszú vektorokra vonatkozó

$$(u^* v) u = (u u^*) v$$

azonosságot használtuk. Ennek igazolása: $u = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, $v = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$ akkor az $(u^* v) u$ vektor i -edik eleme $\sum_{j=0}^n \bar{\alpha}_j \beta_j \alpha_i$,

míg az $u u^*$ mátrix i -edik sorának j -edik eleme $\alpha_i \bar{\alpha}_j$, így az $(u^* u) v$ mátrix i -edik eleme $\sum_{j=0}^n \alpha_i \bar{\alpha}_j \beta_j$, ami ugyanaz, mint az előbbi összeg.

Megj.: Ha $\pi : \mathbb{C}^n \rightarrow W$ a W altérre való merőleges vetítés (azaz az az ortogonalis projekció, aminek a képtere W), akkor tetszőleges $u \in \mathbb{C}^n$ esetén πu a W altérnek az u vektorhoz legközelebbi eleme:

$$w \in W \text{ esetén } |u - w| \geq |u - \pi u|$$

és egyenlőség csak $w = \pi u$ -ra áll fenn.

Biz.: Legyen $w \in W$ és $w' = w - (u - \pi u)$. Ekkor, mivel $u - \pi u \in \ker \pi = W^\perp$,

$$(u - w, u - w) = ((u - \pi u) - w', (u - \pi u) - w') = (u - \pi u, u - \pi u) + (w', w') \geq (u - \pi u, u - \pi u),$$

ahol egyenlőség csak a $w' = 0$ esetben áll.

Négyzetes mátrix nyoma (emlékeztető): $\text{tr } A$ az A mátrix főátlójában levő elemeinek összege. A karakterisztikus polinom $n - 1$ -ed fokú tagjának az együtthatója. Ezért tetszőleges C invertálható mátrixra $C^{-1} A C$ nyoma ugyanaz, mint A nyoma.

Ortogonalis projekciók főátlója: Legyen $A = (a_{ij})$ egy ortogonalis projekció mátrixa. Ekkor

- $\text{tr } A = A$ rangja,

Biz.: A diagonális alakjában az egyesek száma, azaz a képtér dimenziója.

- $a_{ii} \geq 0$

Biz.: Legyen v_1, \dots, v_n a standard bázis. $A^2 = A^* A = A$, így

$$a_{ii} = (v_i, A v_i) = (v_i, A^* A v_i) = (A v_i, A v_i) \geq 0.$$

- $a_{ii} \leq 1$:

Biz.: $v_i - Av_i \in \ker A = (AC^n)^\perp$, így $(Av_i, v_i - Av_i) = 0$, és ezért

$$\begin{aligned} 1 &= (v_i, v_i) = (Av_i, Av_i) + (v_i - Av_i, v_i - Av_i) \\ &\geq (Av_i, Av_i) = (v_i, A^* Av_i) = (v_i, Av_i) \\ &= a_{ii}. \end{aligned}$$

Példák.

- Az $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \mapsto \begin{pmatrix} \frac{\alpha_1 + \dots + \alpha_n}{n} \\ \frac{\alpha_1 + \dots + \alpha_n}{n} \\ \vdots \\ \frac{\alpha_1 + \dots + \alpha_n}{n} \end{pmatrix}$ leképezés merőleges vetítés az $\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ irányú egyenesre. Mátixa

$$\begin{pmatrix} \frac{1}{n} & \cdots & \frac{1}{n} \\ \frac{1}{n} & \cdots & \frac{1}{n} \\ \vdots & \ddots & \vdots \\ \frac{1}{n} & \cdots & \frac{1}{n} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{n}} \\ \vdots \\ \frac{1}{\sqrt{n}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{n}} & \cdots & \frac{1}{\sqrt{n}} \end{pmatrix}$$

- az első néhány standard bázisvektor által feszített altérre való merőleges vetítés:

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \end{pmatrix} = (1 \ 0 \ \dots \ 0) (1 \ 0 \ \dots \ 0)^T + \dots + (1 \ \dots \ 0 \ 1) (1 \ \dots \ 0 \ 1)^T.$$

- Ha π egy ortogonális projekció a W altérre, akkor $I - \pi$ egy ortogonális projekció a W^\perp altérre. Például ha $u \in \mathbb{C}^n$ egy egységvektor, akkor uu^* az $\langle u \rangle$ altérre való merőleges vetítés, míg $I_n - uu^*$ az u^\perp altérre vetít merőlegesen.

2. Szinguláris értékek szerinti felbontás

2.1. Mögöttes szemantikájú indexelés és alacsony rangú közelítés

Tegyük fel, hogy adott egy m dokumentumból álló gyűjtemény és egy n szóból álló szótár és $A = (a_{ij})$ egy olyan valós $m \times n$ -es mátrix, amelyben az a_{ij} elem a j -edik szónak az i -edik dokumentumban való előfordulását jellemzi (valamilyen módszer szerint számított módon, pl. előfordulások súlyozott száma). Modellünkben azt tételezzük fel, hogy a szavak mögött (általunk nem ismert) fogalmak, jelentések állnak és minden szó jól közelíthető alapvető jelentések elegyeként. Formálisabban: azt tételezzük fel, hogy léteznek olyan

$$f_1 = \begin{pmatrix} f_{11} \\ f_{21} \\ \vdots \\ f_{m1} \end{pmatrix}, \dots, f_k = \begin{pmatrix} f_{1k} \\ f_{2k} \\ \vdots \\ f_{mk} \end{pmatrix} \in \mathbb{R}^m$$

oszlopvektorok (az alapvető fogalmak "profiljai"), amelyekre az A mátrix oszlopai (a szavak "profiljai") jól közelíthetők az f_1, \dots, f_k vektorok lineáris kombinációival. Másképpen fogalmazva létezik olyan B $k \times n$ -es mátrix, hogy ha F az az $m \times k$ -es mátrix, aminek oszlopai az f_1, \dots, f_k vektorok, akkor

$$A \approx FB.$$

Áll.: Legyen M egy $m \times n$ -es mátrix. Ekkor M rangja akkor és csak akkor legfeljebb k , ha léteznek olyan B $k \times n$ -es és F $m \times k$ -es mátrixok, amelyekre $M = FB$.

Biz.: A fenti gondolatmenet közelítés helyett egyenlőséggel.

Az elvi feladat tehát A minél jobb közelítése egy A' legfeljebb k rangú mátrixszal. A közelítés hibáját "zaj", illetve "kevésbé fontos" vagy "esetleges" jelentések fellépésének tudhatjuk be.

Ha $A' \approx A$, akkor persze $A'^T A' \approx A^T A$, ami egy pozitív szemidefinit szimmetrikus mátrix, és ennek vizsgálatára már vannak eszközeink.

2.2. Szinguláris értékek

Emlékeztető: A^*A pozitív szemidefinit.

Def.: Az A $m \times n$ -es mátrix szinguláris értékei az A^*A sajátértékeinek a négyzetgyökei.

Terminológiai eltérés: Szokás (és nem egészen indokolatlan) kizárólag a pozitív szinguláris értékeket tekinteni szinguláris értékeknek.

Áll. A^*A rangja = A rangja.

Biz.: Tegyük fel, hogy valamely $v \in AC^n$ vektorra $v \in \ker A^*$. Ekkor $v = Au$ valamely $u \in C^n$ vektorra és $A^*Au = 0$. Innen $0 = (u, A^*Au) = (Au, Au) = (v, v)$, és ezért $v = 0$. A dimenziótételt alkalmazva A^* -nak az AC^n -re való megszorítására $\dim A^*AC^n = \dim AC^n$. A baloldalon A^*A rangja áll, a jobboldalon pedig A rangja.

Köv.: A pozitív szinguláris értékeinek multiplicitással tekintett száma megegyezik A rangjával.

Áll. (A és A^* szinguláris értékei)

Ha σ pozitív szinguláris értéke A -nak, akkor A^* -nak is, és viszont. Részletesebben: Ha v sajátvektora A^*A -nak σ^2 sajátértékkel, akkor Av sajátvektora AA^* -nak szintén σ^2 sajátértékkel.

Biz.: Legyen v egy sajátvektora A^*A -nak σ^2 sajátértékkel Ekkor $v \neq 0$ és

$$(AA^*)(Av) = A(A^*A)v = A\sigma^2v = \sigma^2Av.$$

Azt kell még belátni, hogy $Av \neq 0$. Ehhez tegyük fel indirekte, hogy $Av = 0$. Ekkor $v = \frac{1}{\sigma^2}(A^*A)v = \frac{1}{\sigma^2}A^*(Av) = 0$, ellentmondás

Megj. A fenti állításban a pozitív szinguláris értékek multiplicitásai is ugyanazok.

Biz.: Az $\frac{1}{\sigma}A$ leképezés az A^*A σ^2 -sajátalterét az AA^* σ^2 -sajátalterébe, az $\frac{1}{\sigma}A^*$ pedig az utóbbi teret az előbbi térbe viszi. A két leképezés megszorítása a σ^2 -sajátalterekre inverzei egymásnak.

2.3. SVD

Nemnégyzetes mátrixok főátlója. Egy $m \times n$ -es mátrix főátlója az $(1, 1), \dots, (k, k)$ pozíciókból áll (ebben a sorrendben), ahol $k = \min(m, n)$.

2.3.1. A fő lemma

Lemma: Legyen A egy $m \times n$ -es komplex (valós) mátrix. Ekkor léteznek olyan M' $m \times m$ -es, illetve M $n \times n$ -es unitér (valós ortogonális) mátrixok, amelyekre M'^*AM az az $m \times n$ -es Σ' mátrix, amelynek a főátlójában A szinguláris értékei helyezkednek el nem növekvő sorrendben, a többi helyén pedig 0 áll. Azaz ha A szinguláris értékei a $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n$ számok, akkor M'^*AM vagy

$$\begin{pmatrix} \sigma_1 & & & & \\ & \sigma_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \sigma_n \end{pmatrix}, \begin{pmatrix} \sigma_1 & & & & \\ & \sigma_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \sigma_n \end{pmatrix} \text{ vagy } \begin{pmatrix} \sigma_1 & & & & \\ & \sigma_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \sigma_n \end{pmatrix}$$

alakú, aszerint, hogy $m < n$, $m = n$ vagy $m > n$.

Biz. Az $n \times n$ -es pozitív szemidefinit A^*A mátrixnak sajátvektoraiból álló ortonormált bázist veszünk, a sajátértékek szerint nem növekvő sorrendben. Az erre a bázisra való áttérés mátrixa egy olyan M unitér (ortogonális) mátrix, amire M^*A^*AM az a D diagonális mátrix, amelynek a főátlójában a σ_j^2 elemek állnak. A $D = (AM)^*(AM)$ diagonalitásból következik, hogy az AM mátrix oszlopai ortogonális rendszert alkotnak. A diagonális elemek az oszlopvektorok hosszának négyzetét adják: a j -edik oszlop hossza $\sqrt{\sigma_j}$. Legyen r az A mátrix rangja, azaz a nem 0 szinguláris értékek száma (multiplicitással). Legyen M' egy olyan $m \times m$ -es unitér (ortogonális) mátrix, amelynek első r oszlopa AM első r oszlopa 1 hosszúra normálva. Ekkor, mivel AM további $(r + 1)$ -edik, stb.) oszlopai 0-k, $AM = M'\Sigma'$ és így $M'^*AM = \Sigma'$.

2.3.2. Redukált SVD

Tétel: Legyen A egy $m \times n$ -es komplex (valós), legyen A rangja r és legyen Σ az az $r \times r$ -es diagonális mátrix, amelynek a főátlójában A pozitív szinguláris értékei vannak nem növekvő sorrendben. Ekkor léteznek olyan U' $m \times r$ -es, illetve U $n \times r$ -es hogy U' oszlopai ortonormált rendszert alkotnak (azaz $U'^*U' = I_r$), U oszlopai is ortonormált rendszert alkotnak (azaz $U^*U = I_r$), és

$$A = U'\Sigma U^*.$$

Biz.: Legyen $\Sigma' = M'^*AM$ a lemma szerint. Ekkor $A = M'\Sigma'M^*$. Legyen U' az M' mátrix első r oszlopából álló $m \times r$ -es mátrix, U pedig az M mátrix első r oszlopából $n \times r$ -es mátrix. Legyen U' illetve U maradéka T' , illetve T . Ekkor

$$A = (U' \mid T') \begin{pmatrix} \Sigma & \mid & 0 \\ 0 & & \mid & 0 \end{pmatrix} \begin{pmatrix} U^* \\ T^* \end{pmatrix} = (U'\Sigma \mid 0) \begin{pmatrix} U^* \\ T^* \end{pmatrix} = U'\Sigma U^*.$$

2.3.3. Teljes SVD

$$A = M'\Sigma'M^*$$

a fő lemma szerint.

2.3.4. Egyértelműség kérdése

Legyen $A = U'\Sigma U^*$, ahol Σ $r \times r$ -es diagonális mátrix pozitív átlós elemekkel nem növekvő sorrendben, U' $m \times r$ -es U pedig $n \times r$ -es, amelyekre $U'^*U' = I_r$, $U^*U = I_r$. Ekkor

$$A^*A = U\Sigma U'^*U'\Sigma U^* = U\Sigma^2 U^*,$$

így

$$\Sigma^2 = U^*A^*AU.$$

Ez csak úgy lehet, hogy U mátrix oszlopai az A^*A mátrix nem 0 sajátértékeihez tartozó sajátaltéréinek báziselemeiből áll. (Egészítsük ki U -t egy $n \times n$ -es unitér mátrixszá az A^*A magjából vett oszlopvektorokkal. Ez a mátrix diagonalizálja az A^*A mátrixot, így oszlopai A^*A sajátvektoraiból álló bázis \mathbb{C}^n -ben (illetve \mathbb{R}^n -ben).) Hasonlóan,

$$\Sigma^2 = U'^*AA^*U',$$

ezért az U' mátrix oszlopai az AA^* mátrix nem 0 sajátértékeihez tartozó sajátaltéréinek báziselemeiből áll. Következésképpen, ha A pozitív szinguláris értékei különbözők, akkor U és U' az oszlopok egységszerese erejéig egyértelmű.

2.3.5. Példa

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad A^T A = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}, \quad M^T A^T A M = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix}, \quad M = \begin{pmatrix} +\frac{1}{\sqrt{2}} & +\frac{1}{\sqrt{2}} \\ +\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

$$AM = \begin{pmatrix} \sqrt{2} & 0 \\ \sqrt{2} & 0 \\ \sqrt{2} & 0 \end{pmatrix}, \quad M' = \begin{pmatrix} \frac{1}{\sqrt{3}} & c_{12} & c_{13} \\ \frac{1}{\sqrt{3}} & c_{22} & c_{23} \\ \frac{1}{\sqrt{3}} & c_{32} & c_{33} \end{pmatrix},$$

$$\Sigma = \sqrt{6}, \quad U = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \quad U' = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \end{pmatrix}, \quad A = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \end{pmatrix} \sqrt{6} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

2.3.6. SVD önadjungált mátrixokra

$A^* = A$ esetén a szinguláris értékek A sajátértékeinek abszolút értékei multiplicítással). Ha

$$A = U \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} U^*,$$

ahol U egy $n \times n$ -es unitér mátrix és $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_n|$, akkor A egy lehetséges SVD-je

$$A = U' \begin{pmatrix} |\lambda_1| & & & \\ & |\lambda_2| & & \\ & & \ddots & \\ & & & |\lambda_n| \end{pmatrix} U^*,$$

ahol U' i -edik oszlopa U i -edik oszlopának ± 1 -szerese, aszerint, hogy $\lambda_i \geq 0$ vagy $\lambda_i < 0$.

2.4. Kapcsolat a poláris felbontással

2.4.1. Négyzetgyök

Áll.: Ha A egy $n \times n$ -es pozitív szemidefinit mátrix, akkor $\exists!$ olyan B $n \times n$ -es pozitív szemidefinit mátrix, amelyre $A = B^2$ (jel.: $B = \sqrt{A}$). Ha A valós, akkor B is valós. Ha A pozitív definit, akkor B is az.

Biz.: Legyen U egy olyan unitér (valós esetben ortogonális), mátrix, amelyre $D = U^* A U$ diagonális (nemnegatív elemekkel). Legyen továbbá B' az a diagonális mátrix, amelyre D -ből úgy kapható, hogy elemeit kicseréljük a nemnegatív négyzetgyökökre. Ekkor B' valós, pozitív szemidefinit és $B'^2 = D$. Így $B = UB'U^*$ is pozitív szemidefinit, továbbá

$$B^2 = UB'U^*UB'U^* = UB'^2U^* = UDU^* = A.$$

Az egyértelműséghez: Legyen $A = B^2$ és v az A mátrixnak egy sajátvektora λ sajátértékkel. Mivel V -nek van B sajátvektoraiból álló bázisa, v felírható B mátrix néhány lineárisan független sajátvektorának összegeként: $v = \sum_{i=1}^{\ell} v_i$, ahol $Bv_i = \lambda_i v_i$, Ekkor

$$\sum_{i=1}^{\ell} \lambda v_i = \lambda v = Av = B^2 v = \sum_{i=1}^{\ell} \lambda_i^2 v_i.$$

Ez a v_1, \dots, v_{ℓ} vektorok lineáris függetlensége miatt csak úgy lehet, hogy $\lambda_i^2 = \lambda$ ($i = 1, \dots, \ell$), ami viszont B szemidefinitésége miatt azt jelenti, hogy $\lambda_i = \sqrt{\lambda}$, és így $Bv = \sqrt{\lambda}v$. Legyen u_1, \dots, u_n az \mathbb{R}^n -nek egy olyan bázisa, ami az A mátrix sajátvektoraiból áll. A fenti gondolatmenetet alkalmazzuk $v = u_1, v + v_2, \dots, v = u_n$ helyettesítéssel. Azt kapjuk, hogy ha $Au_i = \lambda_i u_i$, akkor $Bu_i = \sqrt{\lambda_i} u_i$, tehát B tényleg egyértelműen meghatározott.

2.4.2. Poláris felbontás

Tétel. Tetszőleges $n \times n$ -es komplex (valós) A mátrix felírható PM alakban, ahol M egy $n \times n$ -es unitér (ortogonális) mátrix, P pedig egy $n \times n$ -es pozitív szemidefinit komplex (valós) mátrix. A felbontásbeli P mátrix egyértelmű, és ha A invertálható, akkor M is egyértelmű és P pozitív definit.

Megj: 1 dimenziós eset: komplex számok felbontása $re^{i\phi}$ alakban.

Biz. Létezés: szükség esetén "párnázzuk ki" A szinguláris érték szerinti felbontását: $A = U'\Sigma U^*$, ahol U és U' $n \times n$ -es unitér (ortogonális) mátrixok, Σ pedig egy $n \times n$ -es diagonális nemnegatív elemekkel. Legyen $P = U'\Sigma U'^*$ és $M = U'U^*$.

P egyértelműsége: $AA^* = PMM^*P = P^2$, így $P = \sqrt{AA^*}$. Ha A invertálható, akkor P is az és $M = P^{-1}A$.

Megj.: Hasonlóan, A felírható $M'P'$ alakban, ahol M' unitér és P' pozitív szemidefinit. $P' = P$ akkor és csak akkor teljesül, ha $A^*A = AA^*$, azaz ha A normális.

2.5. Alacsony rangú közelítések

2.5.1. Mátrixok Frobenius-normája

Def. Legyen A egy $m \times n$ -es komplex mátrix. Ekkor

$$\|A\| = \sqrt{\sum_{i=1}^m \sum_{j=1}^n |a_{ij}|^2}.$$

Tulajdonképpen az $m \cdot n$ dimenziós tér euklideszi normája.

Hasznos megadás: $\|A\|^2 = A^*A$ nyoma.

Áll. A $m \times n$ -es mátrix, B $m' \times m$ -es amelynek az oszlopai ortonormált rendszert alkotnak (azaz $B^*B = I_m$), C pedig $n \times n'$ -es, amelynek a sorai ortonormált rendszert alkotnak (azaz $CC^* = I_n$), $\Rightarrow \|BA\| = \|A\| = \|AC\|$

Biz.: Ha A oszlopai a^1, \dots, a^n , akkor BA oszlopai Ba^1, \dots, Ba^n , és mivel B a \mathbb{C}^m (vagy \mathbb{R}^m) standard bázisát B képterének egy ortonormált bázisába viszi, B egy izometria \mathbb{C}^m (\mathbb{R}^m) és B képtere között, így $|Ba^j|^2 = |a^j|^2$. Ezért $\|BA\|^2 = \sum |Ba^j|^2 = \sum |a^j|^2 = \|A\|^2$. A második egyenlőség ebből $A \leftarrow A^T$, $B \leftarrow C^T$ helyettesítéssel adódik.

Másik biz.:

$$\|BA\|^2 = \text{tr } A^*B^*BA = \text{tr } A^*I_m A = \text{tr } A^*A = \|A\|^2.$$

2.5.2. Az Eckart-Young-tétel

Tétel. Legyen A egy $m \times n$ -es komplex (valós) r rangú mátrix az $A = U'\Sigma U^*$ szinguláris érték szerinti felbontással. Ekkor tetszőleges $0 \leq k \leq r$ -re

$$U'^{(k)}\Sigma^{(k)}U^{(k)*}$$

a A -hoz a Frobenius-normában (az egyik) lehető legközelebbi olyan $m \times n$ -es mátrix, amelynek a rangja legfeljebb k . Itt $U^{(k)}$, illetve $U'^{(k)}$ U , illetve U' első k oszlopából álló részmatrixa, $\Sigma^{(k)}$ pedig Σ bal felső $k \times k$ -as része. A közelítés hibája

$$\sqrt{\sum_{i=k+1}^r \sigma_i^2},$$

ahol $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r$ az A mátrix szinguláris értékei.

Biz.: Legyen $\Sigma' = M'^*AM$, mint az SVD fő lemmájában. (Ezen belül M , illetve M' az U , illetve U' mátrixok kiegészítése négyzetes unitér mátrixra.) Tegyük fel, hogy B egy $m \times n$ -es mátrix. Ekkor

$$\|B - A\| = \|M'^*(B - A)M\| = \|M'^*BM - M'^*AM\| = \|M'^*BM - \Sigma'\|.$$

Legyen $B_0 = U'^{(k)}\Sigma^{(k)}U^{(k)*}$. Az SVD-tétel befejező bizonyításához hasonló gondolatmenettel látható, hogy $B_0 = M'\Sigma'^{(k)}M^*$, ahol $\Sigma'^{(k)}$ az az $n \times n$ -es mátrix, ami $\Sigma^{(k)}$ -ből úgy kapható, hogy az utolsó $n - k$ diagonális eleme helyébe 0-t írunk. Innen $M'^*B_0M = \Sigma'^{(k)}$, és így

$$\begin{aligned} \|B_0 - A\| &= \sqrt{\|M'^*B_0M - \Sigma'\|} \\ &= \sqrt{\|\Sigma_0 - \Sigma'\|} \\ &= \sqrt{\sum_{i=k+1}^r \sigma_i^2}. \end{aligned}$$

Ha B rangja $\leq k$, akkor, mivel M'^* és M invertálható mátrixok, M'^*BM rangja is $\leq k$. Az M'^*BM helyébe C -t írva elég tehát belátni, hogy ha C rangja legfeljebb k , akkor $\|C - \Sigma'\|^2 \geq \sum_{i=k+1}^r \sigma_i^2$. Ha C rangja legfeljebb k , akkor C bal felső $r \times r$ -es részének a rangja is legfeljebb k , továbbá $C - \Sigma$ normája legalább akkora, mint az bal felső $r \times r$ -es részéé. Így elég a következő állítást igazolni:

Áll. Legyen D az az $r \times r$ -es diagonális mátrix, amelynek átlós elemei a $\mu_1 \geq \dots \geq \mu_r$ pozitív valós számok, legyen C egy $0 \leq k < r$ rangú $r \times r$ -es (komplex) mátrix. Ekkor

$$\|C - D\|^2 \geq \sum_{i=k+1}^r \mu_i^2.$$

Biz.: Legyen $W = \ker C$ és legyen w_1, \dots, w_{r-k} a W altér egy ortonormált bázisa, míg w_{r-k+1}, \dots, w_r a W^\perp egy ortonormált bázisa. Legyen U_1 a w_1, \dots, w_{r-k} oszlopvektorokból álló mátrix, U_2 pedig a w_{r-k+1}, \dots, w_r oszlopokból álló. Ekkor az $U = (U_1|U_2)$ $r \times r$ -es mátrix unitér, így

$$\|C - D\| = \|U^*(C - D)U\| = \left\| \begin{pmatrix} U_1^* \\ U_2^* \end{pmatrix} (C - D) (U_1|U_2) \right\| = \left\| \begin{pmatrix} U_1^*(C - D) \\ U_2^*(C - D) \end{pmatrix} (U_1|U_2) \right\| = \left\| \begin{pmatrix} U_1^*(C - D)U_1 & U_1^*(C - D)U_2 \\ U_2^*(C - D)U_1 & U_2^*(C - D)U_2 \end{pmatrix} \right\|,$$

Így az a norma legalább akkora, mint a bal felső $U_1^*(C - D)U_1$ rész mátrix normája. Mivel a W altéren C megszorítása 0 így $CU_1 = 0$, ezért $U_1^*(C - D)U_1 = U_1^*DU_1$, tehát

$$\|C - D\| \geq \|U_1^*DU_1\|.$$

Belátjuk, hogy $\|U_1^*DU_1\|^2 \geq \sum_{i=k+1}^r \mu_i^2$. Ehhez a Frobenius-norma nyomos megadását és a nyom tulajdonságait használjuk.

$$\|U_1^*DU_1\|^2 = \text{tr}(U_1^*DU_1)(U_1^*DU_1)^* = \text{tr}U_1^*D^2U_1 = \text{tr}U_1U_1^*D^2 = \sum_{i=1}^r \beta_{ii}\mu_i^2,$$

ahol a $(\beta_{ij}) = B = U_1U_1^*$. Itt $B^* = B$ és $B^2 = I$, így B egy ortogonális projekció. B rangja = U_1 rangja = $n - k$. Tehát $0 \leq \beta_{ii} \leq 1$ és $\sum_{i=1}^r \beta_{ii} = 1$. Ezek mellett a feltételek mellett a $\sum_{i=1}^r \beta_{ii}\mu_i^2$ akkor lesz a legkisebb, ha a $\beta_{11} = \dots = \beta_{kk} = 0$, a többi 1.

2.5.3. LSI alapú keresés

Keresőkérdés \sim dokumentum $\sim A$ sorai. Ha w A egy sora, a legjobb Frobenius-normában közelítő A' mátrixnak a megfelelő sora nem más, mint w merőleges vetülete az A' sorai által generált altérre.

Ennek megfelelő eljárás az, hogy a keresőkérdéshez tartozó (dokumentum-típusú) sorvektort levetítjük az A' mátrix sorai által generált altérre.

2.6. A QR-felbontás

Felbontás $A = QR$ alakban, ahol Q $m \times m$ -es unitér (ortogonális) és R $m \times n$ -es felső háromszög alakú: $R = (r_{ij})$, ahol $r_{ij} = 0$, ha $i > j$.

2.6.1. Gram-Schmidt ortogonalizációval

Tegyük fel az egyszerűség kedvéért, hogy A négyzetes ($n \times n$ -es) nemelfajuló mátrix. Alkalmazzuk a Gram-Schmidt-eljárást az A^*A (pozitív definit) $n \times n$ -es mátrixra, mint Gram-mátrixra: $G^*A^*AG = I$, ahol G a Gram-Schmidt báziscsere mátrixa. Emlékeztetőül: az eljárás első fázisban egy eredeti báziselemet nála kisebb indexű báziselemek lineáris kombinációjának hozzáadásával módosítjuk, majd a második menetben normáljuk. Ezért G egy $n \times n$ -es felső háromszögmátrix: egy j indexű új báziselem az $i \leq j$ indexű régi báziselemek lineáris kombinációja. Az $G^*A^*AG = I$ egyenlőség azt jelenti, hogy az AG $n \times n$ -es mátrix oszlopai egy ortonormált rendszert alkotnak, ezért a $Q = AG$ mátrix unitér. Legyen $R = G^{-1}$ az inverz bázistranszformáció. Ekkor R is felső háromszögmátrix alakú: Ha v_1, \dots, v_n a standard bázis és w_1, \dots, w_n a Gram-Schmidt-féle ortonormált bázis az $\langle u, v \rangle = (Au, Av)$ formára vonatkozóan, akkor $r_{ij} = \langle w_i, v_j \rangle = \langle w_i, Av_j \rangle = \langle w_i, a^j \rangle$, ahol a^j az A mátrix j -edik oszlopa.

2.6.2. Householder-tükrözésekkel

Hipersíkra tükrözés.: $0 \neq u$ rögzített,

$$\tau_u : v \mapsto v - 2 \frac{\langle u, v \rangle}{\langle u, u \rangle} u = v - 2 \frac{u^*v}{u^*u} u.$$

Azaz τ_u mátrixa a standard bázisban: $I - \frac{2}{u^*u} uu^*$. Ez egy unitér (valós esetben ortogonális) mátrix.

Alkalmos tükrözés. Legyen v, w két nem 0 vektor. Ekkor van olyan tükrözés, amely v -t w egy skalárszorosaiba viszi: legyen $u = \frac{|v|}{|w|}w - v$, ez merőleges v és w szögfelező hipersíkjára, így $\tau_u v = \frac{|v|}{|w|}w$.

Első oszlop. Legyenek A első oszlopa a^1 . Ekkor ha $a^1 \neq 0$, akkor a $v = a^1$ és a $w = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ vektorok szögfelező

hipersíkjára való τ_1 tükrözés az a^1 vektort egy $\begin{pmatrix} \alpha \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ alakú vektorba viszi. Tehát a τ_1 tükrözés T_1 unitér mátrixával balról szorzás A első oszlopában kinullázza a főátló alatti elemeket:

$$T_1 A = \begin{pmatrix} * & * \\ & \boxed{A'} \end{pmatrix}$$

alakú, ahol A' -nek eggyel kevesebb sora és oszlopa van. (Ha $a^1 = 0$, akkor $T_1 = I$.)

Rekurzió. A jobb alsó A' blokkraja. A rekurzióban során fellépő T'_i $(n-1) \times (n-1)$ -szeres unitér szorzómátrixokat ($i = 2, \dots$) blokk-diagonálisan kiegészítjük egy bal felső 1-essel:

$$T_i = \begin{pmatrix} 1 & \\ & \boxed{T'_i} \end{pmatrix}.$$

Végeredmény:. $T_n \cdots T_2 T_1 A = R$, $A = QR$, ahol $Q = T_1 T_2 \cdots T_n$

Egyértelműség:. Akkor, ha A oszlopai lineárisan függetlenek, és amellett a megszorítás mellett, hogy R diagonális elemei pozitív valós számok.

Változat:. $AP = QR$, ahol P permutációs mátrix és R felső delta alakú: valamely k indexre $r_{jj} \neq 0$, ha $j \leq k$; $r_{ij} = 0$ ha $i > j$ vagy ha $i > k$. Az eredeti módszer azzal, hogy amint csupa 0 maradékú oszlopra bukkanunk, kicseréljük egy olyanmal, aminek a maradéka nem csupa 0 (ha van ilyen oszlop).

Alkalmazás:. A determinánsa, rangja, képtere meghatározása. Numerikusan stabilabb, mint a Gauss-elimináció vagy a Gram-Schmidt-ortogonalizáció. LSI-ben is használható, SVD-típusú közelítések helyett bizonyos esetekben viszonylag tűrhető, gyorsan számolható alacsony rangú közelítést tesz lehetővé.

QR-algoritmus:.

$$\begin{aligned} A_1 &:= A \\ A_1 &= Q_1 R_1, \text{ ahol } Q_1 \text{ unitér (ortogonális), } R_1 \text{ felső háromszög.} \\ &\vdots \\ A_i &= Q_i R_i, \text{ ahol } Q_i \text{ unitér (ortogonális), } R_i \text{ felső háromszög.} \\ A_{i+1} &:= R_i Q_i \\ A_{i+1} &= Q_{i+1} R_{i+1}, \text{ ahol } Q_{i+1} \text{ unitér (ortogonális), } R_{i+1} \text{ felső háromszög.} \\ &\vdots \end{aligned}$$

Észrevétel:

$$A_{i+1} = Q_i^* A_i Q_i,$$

az $A_1, A_2, \dots, A_i, A_{i+1}, \dots$ mátrixoknak ugyanazok a sajátértékei. Alkalmos feltételek mellett felső háromszögmátrixhoz konvergál, az átlóban a sajátértékekkel. Pl. ha A pozitív definit valós szimmetrikus, a határérték diagonális, sőt, a Q_i -k szorzatának határértéke diagonalizálja A -t. Az eljárásnak több javított változata van.

Kézenfekvő diagonalizáló módszer: A sajátértékei a karakterisztikus polinomból, sajátvektorok lineáris egyenletrendszerekkel: nem elég gyors és nagyon érzékeny a numerikus hibákra.

2.7. Az SVD közelítő kiszámításáról

Alapvető észrevétel: A $m \times n$ -es, T $m \times m$ -es unitér, T' $n \times n$ -es unitér:
 $\text{SVD } A\text{-ra} \longleftrightarrow \text{SVD } TAT'\text{-re}$

Általános módszer

Első menetben A -t Householder-tükrözésekkel balról-jobbról szorozva bidiagonális alakra hozzuk: Legelőször egy tükrözés mátrixával való balról szorzással elintézzük, hogy az első oszlop főátló alatti elemei 0-k legyenek, majd jobbról egy

$$\begin{pmatrix} 1 & & & & \\ & \boxed{T'} & & & \\ & & & & \\ & & & & \\ & & & & \end{pmatrix}.$$

alakú mátrixszal szorozzuk, ahol T' egy olyan alkalmas tükrözés mátrixa, amely az első sor második, harmadik, stb. koordinátáiból álló $n - 1$ hosszú sorvektort az $(1, 0, \dots, 0)$, szintén $n - 1$ hosszú vektorba képezi. Ezzel elérjük, hogy az első oszlopban harmadik elemtől kezdve csupa 0 álljon:

$$\begin{pmatrix} * & * & & & \\ & * & \dots & * & * \\ & \vdots & \ddots & \vdots & \vdots \\ & * & \dots & * & * \end{pmatrix}$$

Ezután a második oszlopot, majd a második sor vesszük hasonló módon kezelésbe, és így tovább. Végeredményül egy bidiagonális – szintén $A = (a_{ij})$ -vel jelölt – mátrixot kapunk:

$$A = \begin{pmatrix} * & * & & & & \\ & * & * & & & \\ & & * & * & & \\ & & & \ddots & \ddots & \\ & & & & * & * \\ & & & & & * \end{pmatrix}.$$

(A bidiagonalitás azzal jellemezhető, hogy $a_{ij} = 0$, ha $j \notin \{i, i + 1\}$.) Ekkor $B = A^*A$ tridiagonális alakú:

$$B = \begin{pmatrix} * & * & & & & \\ * & * & * & & & \\ & * & * & * & & \\ & & \ddots & \ddots & \ddots & \\ & & & * & * & * \\ & & & & * & * \end{pmatrix},$$

azaz $b_{ij} = 0$, ha $|i - j| > 1$. Második menetben a QR-algoritmus alkalmas változatát használják A^*A sajátértékeinek meghatározására. Az algoritmus során vigyázni kell a tridiagonalitás megőrzésére, így tükrözések helyett bizonyos forgatásokat használnak.

Lánczos-típusú módszerek ritka mátrixokra

Lánczos-eljárás: Szimmetrikus (önadjungált) mátrix tridiagonalizálása n -darab mátrix×vektor szorzással. Ha a mátrix ritka vagy két ritka szorzata (mint pl. A^*A , ha A ritka), akkor nagyon megéri.

Lánczos-típusú módszerek: Ritka A -ra (ilyenek merülnek fel LSI esetén) A^*A tridiagonalizálására a Lánczos-eljárás változatai. Aztán a tridiagonális mátrix sajátértékeire/sajátvektoraira QR-algoritmus valamely változata.

2.8. Az SVD néhány további alkalmazása

2.8.1. Homogén lineáris egyenletrendszer megoldása

$Ax = 0$ megoldása, azaz $\ker A$ számítása.

Emlékeztető: A^*A rangja ugyanaz, mint A rangja, így $\ker A^*A = \ker A$.

Teljes SVD:

$$A = M'\Sigma'M^*,$$

itt M azon oszlopai, amelyekre Σ' megfelelő sora 0, a $\ker A^*A = \ker A$ egy ortonormált bázisát adják.

2.8.2. Pszeudo inverz

Moore-Penrose-féle pszeudo inverz: Az A egy $m \times n$ -es komplex (valós) mátrix pszeudo inverze egy olyan A^+ $n \times m$ -es komplex mátrix, amelyre

- $AA^+A = A$,
- $A^+AA^+ = A^+$,
- AA^+ önadjungált,
- A^+A önadjungált.

Áll. (pszeudo inverz az SVD-ből): Ha A (redukált) SVD-je

$$A = U'\Sigma U^*,$$

akkor

$$A' = U\Sigma^{-1}U'^*$$

egy pszeudo inverze A -nak.

Biz.: Felhasználjuk, hogy $U^*U = U'^*U' = I_r$. Innen

$$AA' = U'\Sigma U^*U\Sigma^{-1}U'^* = U'U'^*$$

és

$$A'A = U\Sigma^{-1}U'^*U'\Sigma U^* = UU^*.$$

(Vigyázat, általában ha pl. $r < n$, akkor $UU^* \neq I_n$.)

- $AA'A = U'U'^*A = U'U'^*U'\Sigma U^* = U'\Sigma U^* = A$.
- $A'AA' = A'U'U'^* = U\Sigma^{-1}U'^*U'U'^* = U\Sigma^{-1}U'^* = A'$
- $(AA')^* = (U'U'^*)^* = U'U'^* = AA'$.
- $(A'A)^* = (UU^*)^* = UU^* = A'A$.

Lemma. Legyen A^+ egy pszeudo inverze A -nak. Ekkor AA^+ a \mathbb{C}^m tér merőleges vetítése A képterére, A^+A pedig a \mathbb{C}^n tér merőleges vetítése A^* képterére.

Biz.: (1) AA^+ önadjungált és $(AA^+)^2 = AA^+$, így AA^+ ortogonális projekció. AA^+ képtere nyilván benne van A képterében. A fordított tartalmazás az $A = (AA^+)A$ egyenlőségből látható.

(2) Hasonlóan, A^+A is merőleges vetítés. A^+A önadjungáltsága miatt $A^+A = A^*(A^+)^*$, így A^+A képtere benne van A^* képterében. Mivel $A = AA^+A$, A^+A rangja legalább akkora, mint A rangja, ami egyben A^* rangja is, tehát a két képtér megegyezik.

Áll. (pszeudo inverz egyértelmősége): A^+ és A' két pszeudo inverze A -nak $\Rightarrow A' = A^+$.

Biz.: A lemma miatt AA^+ , akárcsak AA' az ortogonális projekció A képterére, tehát $AA' = AA^+$. Hasonlóan, $A'A = A^+A$. Ezért $A' = A'AA' = A'AA^+ = A^+AA^+ = A^+$.

Köv.: Ha $A = U'\Sigma U^*$ az A mátrix (redukált) SVD-je, akkor A pszeudo inverze $A^+ = U\Sigma^{-1}U'^*$. Ha A valós, a pszeudo inverze is valós.

Példa. Legyen $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$. Ekkor A SVD-je $A = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \end{pmatrix} \sqrt{6} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$, ezért

$$A^+ = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \frac{1}{\sqrt{6}} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix} = \frac{1}{6} A^T.$$

Példa. Legyen $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Ekkor $A^*A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, így A SVD-je $A = \begin{pmatrix} 1 \\ 0 \end{pmatrix} 1 \begin{pmatrix} 0 & 1 \end{pmatrix}$, ezért

$$A^+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix} 1 \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = A^*.$$

HF. $(A^+)^+ = A$.

HF. $(A^*)^+ = (A^+)^*$.

HF. A^+ rangja = A rangja.

HF. Ha A invertálható négyzetes mátrix, akkor $A^+ = A^{-1}$.

HF. Ha A egy merőleges vetítés (négyzetes) mátrixa, akkor $A^+ = A$.

Példa. Legyen

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad AB = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{pmatrix},$$

Ekkor A, B merőleges vetítés, így $A^+ = A, B^+ = B$.

$$(AB)(BA) = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} = \frac{1}{2}A,$$

nem vetítés, így $(AB)^+ \neq BA = B^+A^+$. Valójában AB szinguláris érték szerinti felbontása:

$$AB = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \end{pmatrix},$$

így

$$(AB)^+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \sqrt{2} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = 2BA.$$

Magtér meghatározása. A^+A merőleges vetítés A^* képterére, $I - A^+A$ merőleges vetítés A magjára. Így $I - A^+A$ oszlopai $\ker A$ egy ortonormált bázisát adják. Ez is használható homogén lineáris egyenletrendszerek megoldására.

Biz.: Az $I - A^+A$ az ortokomplementer altérre való vetítés, tehát a bizonyításhoz az hiányzik még, hogy A^* képtere A magjának ortokomplementere. Az $(A^*v, w) = v^*Aw = (v, Aw)$ egyenlőségekből azonban ez könnyen adódik.

2.8.3. Legkisebb négyzetek

$Ax = b$ közelítő megoldása a legkisebb hibával (négyzetösszeg-értelmenben):

$$|Ax - b|^2 \longrightarrow \min$$

Tétel. Ha A pszeudoinverze A^+ , akkor $x = A^+b$ minimalizálja az $|Ax - b|^2$ -t.

Biz.: Legyen $W = A$ képtere. Bontsuk fel b -t $b_0 + b_1$ alakban, ahol $b_0 \in W, b_1 \in (A\mathbb{C}^n)^\perp$. Ekkor b_0 a b vektor merőleges vetülete W -n. Létezik olyan x_0 , amelyre $b_0 = Ax_0$. Ekkor

$$|Ax - b|^2 = |Ax - Ax_0 + Ax_0 - b|^2 = |A(x - x_0) - b_1|^2 = |A(x - x_0)|^2 + |b_1|^2.$$

Itt az utolsó egyenlőség abból következik, hogy $A(x - x_0) \in W$ és $b_1 \in W^\perp$, tehát a két vektor merőleges egymásra. Ezért az $|Ax - b|^2$ mennyiséget pontosan azok az x vektorok minimalizálják, amelyekre $Ax = b_0$. Az általános inverznél bizonyított lemma miatt AA^+ a W térre való merőleges vetítés, így $b_0 = AA^+b$, tehát az optimumot megvalósító x vektorok az $Ax = AA^+b$ egyenlettel jellemezhetők, és így $x = A^+b$ tényleg optimumot ad.

HF. Mutassuk meg, hogy akkor és csak akkor egyértelmű az optimális x , ha A oszlopai lineárisan függetlenek.

2.8.4. Képvektorhossz-minimalizálás ("total least squares")

$Ax = 0$ közelítő megoldása a legkisebb hibával $|x| = 1$ mellett:

$$|Ax|^2 \longrightarrow \min, \text{ feltéve } |x| = 1.$$

Legyen v_1, \dots, v_n $A^T A$ sajátvektoraiból álló ortonormált bázis, a megfelelő sajátértékek (tehát A szinguláris értékeinek négyzetei) $\sigma_1^2 \geq \dots \geq \sigma_n^2$. Legyen $x = \sum \alpha_i v_i$, ahol $\sum |\alpha_i|^2 = 1$. Ekkor

$$\begin{aligned} |Ax|^2 &= (Ax, Ax) \\ &= (x, A^T Ax) \\ &= \left(\sum \alpha_i v_i, \sum \alpha_i \sigma_i^2 v_i \right) \\ &= \sum \sigma_i^2 |\alpha_i|^2 \\ &\geq \sum |\alpha_i|^2 \sigma_n^2 \\ &= \sigma_n^2, \end{aligned}$$

tehát az elérhető optimum σ_n^2 , ami az $x = v_n$ vektornál fel is vétetik. Amennyiben $\sigma_{n-1} > \sigma_n$, akkor az optimális x skalárszoros erejéig egyértelmű.

3. Nemnegatív mátrixok

3.1. Jelölések:

Legyen $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$ és $v' = \begin{pmatrix} \gamma'_1 \\ \vdots \\ \gamma'_n \end{pmatrix}$ valós vektorok, továbbá $A = (a_{ij})$ és $A' = (a'_{ij})$ $n \times n$ -es valós mátrixok.

- $v \geq 0$, ha $\gamma_j \geq 0$ ($j = 1, \dots, n$)
- $v > 0$, ha $\gamma_j > 0$ ($j = 1, \dots, n$)
- $A \geq 0$, ha $a_{ij} \geq 0$ ($i, j = 1, \dots, n$)
- $A > 0$, ha $a_{ij} > 0$ ($i, j = 1, \dots, n$)
- $v \geq v'$ (illetve $v > v'$), ha $v - v' \geq 0$ ($v - v' > 0$)
- $A \geq A'$ (illetve $A > A'$), ha $A - A' \geq 0$ ($A - A' > 0$)

3.2. Elemi észrevételek

- $A \geq 0 \Leftrightarrow Av \geq 0$ minden $v \geq 0$ vektorra.
- $A > 0 \Leftrightarrow Av > 0$ minden $0 \neq v \geq 0$ vektorra.
- $A \geq A', v \geq v' \Rightarrow Av \geq A'v$.
- $A \geq A', B \geq B' \Rightarrow AB \geq A'B'$.

3.3. Spektrálsugár

Def.: Az $A = (a_{ij})$ négyzetes valós vagy komplex mátrix **spektrálsugara** (jel.: $\rho(A)$) A legnagyobb komplex sajátértékének abszolút értéke.

Def.: Ha $A = (a_{ij}) \geq 0$, és $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \geq 0$, akkor legyen

$$\rho'_v(A) = \max \{r \mid r \in \mathbb{R}, Av \geq rv\} = \min \left\{ \sum_{j=1}^n a_{ij} \frac{\gamma_j}{\gamma_i} \mid i = 1, \dots, n \right\},$$

ahol a 0 nevezőjű törtet $+\infty$ -ként értelmezzük. Legyen végül

$$\rho'(A) = \sup \{\rho_v(A) \mid 0 \neq v \geq 0\} = \sup \{\rho_v(A) \mid v \geq 0, |v| = 1\} = \max \{\rho_v(A) \mid v \geq 0, |v| = 1\}.$$

Itt az első egyenlőség azért teljesül, mert $\rho'_v(A)$ ugyanaz marad, ha v -t kicseréljük egy pozitív skalárszorosával, a második pedig azért, mert a $\{v \mid v \geq 0, |v| = 1\}$ halmaz kompakt.

3.3.1. A két definíció egyenértékűsége

Áll.: $0 \leq A \leq A'$ esetén $\rho'(A) \leq \rho'(A')$.

Biz.: Minden $v \geq 0$ -ra $\rho'_v(A) \leq \rho'_v(A')$.

Áll.: Legyen $B = (b_{ij})$ komplex, $A = (a_{ij})$ pedig nemnegatív valós $n \times n$ -es mátrix, hogy $|b_{ij}| \leq a_{ij}$. Ekkor

$$\rho(B) \leq \rho(A),$$

speciálisan $\rho(A) \leq \rho(A)$.

Biz.: Legyen λ egy sajátértéke B -nek és legyen $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$ egy megfelelő sajátvektor: $v \neq 0$ és $Bv = \lambda v$. Ekkor az

i -edik koordinátát felírva $i = 1, \dots, n$ -re $\lambda \gamma_i = \sum_{j=1}^n b_{ij} \gamma_j$, és innen

$$|\lambda| |\gamma_i| = \left| \sum_{j=1}^n b_{ij} \gamma_j \right| \leq \sum_{j=1}^n |b_{ij}| |\gamma_j| \leq \sum_{j=1}^n a_{ij} |\gamma_j|,$$

így

$$|\lambda| \leq \min \left\{ \sum_{j=1}^n a_{ij} \frac{|\gamma_j|}{|\gamma_i|} \mid i = 1, \dots, n \right\} = \rho'_w(A) \leq \rho'(A),$$

ahol $w = \begin{pmatrix} |\gamma_1| \\ |\gamma_2| \\ \vdots \\ |\gamma_n| \end{pmatrix}$.

Áll.: Tegyük fel, hogy $A > 0$ és $0 \neq v \geq 0$ egy olyan vektor, amelyre $Av \geq \rho'(A)v$ (azaz $\rho'_v(A) = \rho'(A)$). Ekkor $Av = \rho'(A)v$.

Biz.: Legyen $\rho = \rho'(A)$. Tegyük fel, hogy $Av \neq \rho v$. Ekkor $w = Av - \rho v \geq 0$, $w \neq 0$, így $A > 0$ miatt $Aw > 0$, és ezért $0 < Aw = A(Av) - \rho \cdot (Av)$, azaz $A(Av) > \rho \cdot (Av)$. De ez azt jelenti, hogy $\rho'_{Av}(A) > \rho$, ellentmondás.

Köv.: Ha $A > 0$, akkor van olyan $0 \neq v \geq 0$ vektor, amelyre $Av = \rho'(A)v$. Következésképpen $\rho(A) = \rho'(A)$.

Biz.: Tudjuk, hogy $\rho = \rho'_v(A)$ valamely $0 \neq v \geq 0$ vektorra. Az előző állítás alkalmazható.

Áll.: Ha $A \geq 0$, akkor van olyan $v \geq 0$ vektor, amelyre $Av = \rho'(A)v$. Következésképpen $\rho(A) = \rho'(A)$.

Biz.: Legyen $1 \geq \epsilon > 0$ -ra $A_\epsilon = A + \begin{pmatrix} \epsilon & \dots & \epsilon \\ \vdots & \ddots & \vdots \\ \epsilon & \dots & \epsilon \end{pmatrix}$.

Ekkor $A_\epsilon > 0$ és tetszőleges $0 \neq v \geq 0$ vektorra

$$\rho'_v(A) \leq \rho'_v(A_\epsilon) \leq \rho'_v(A_1),$$

ahol $A_1 = A + \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$. Így

$$\rho'(A) \leq \rho'(A_\epsilon) \leq \rho'(A_1).$$

Az előző állítás miatt van olyan v_ϵ vektor, amelyre $|v_\epsilon| = 1$, $v_\epsilon \geq 0$ és $A_\epsilon v_\epsilon = \rho'(A_\epsilon)v_\epsilon$. Mivel mind a v_ϵ vektorok, mind a $\rho'(A_\epsilon)$ számok egy-egy kompakt halmazból vannak, kiválasztható egy olyan ϵ_j $j = 1, 2, \dots$, sorozat, hogy $\epsilon_j \rightarrow 0$ és a v_{ϵ_j} sorozat is konvergál valamely v vektorhoz, továbbá ρ'_{ϵ_j} is konvergál valamely ρ' számhoz. Nyilván $v \geq 0$, $|v| = 1$ és $\rho' \geq \rho(A)$. Minden j -re

$$A_{\epsilon_j} v_{\epsilon_j} = \rho'(A_{\epsilon_j}) v_{\epsilon_j},$$

igaz marad az egyenlőség a $A_{\epsilon_j} \rightarrow A$, $v_{\epsilon_j} \rightarrow v$, $\rho' A_{\epsilon_j} \rightarrow \rho'$ határátmenettel:

$$Av = \rho'v.$$

De ekkor $\rho' = |\rho'| \leq \rho(A) \leq \rho'(A)$.

3.3.2. Alsó és felső korlátok

Áll.: Ha $A \geq 0$, akkor

$$\min \left\{ \sum_{j=1}^n a_{ij} \mid i = 1, \dots, n \right\} \leq \rho(A) \leq \max \left\{ \sum_{j=1}^n a_{ij} \mid i = 1, \dots, n \right\}.$$

Biz.: Felső korlát: Legyen $0 \neq v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \geq 0$ olyan vektor, amelyre $\rho'_v(A) = \rho(A)$. Legyen i_0 olyan index, amelyre a γ_{i_0} az összes γ_j érték közül a legnagyobb. Ekkor

$$\rho(A) = \rho'_v(A) \leq \sum_{j=1}^n a_{i_0j} \frac{\gamma_j}{\gamma_{i_0}} \leq \sum_{j=1}^n a_{i_0j} \leq \max \left\{ \sum_{j=1}^n a_{ij} \mid i = 1, \dots, n \right\}.$$

Alsó korlát: Legyen $v = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$. Ekkor

$$\rho'_v(A) = \min \left\{ \sum_{j=1}^n a_{ij} \mid i = 1, \dots, n \right\},$$

és $\rho(A) = \rho'(A) \geq \rho'_v(A)$.

Köv.: Ha $A \geq 0$, akkor

$$\min \left\{ \sum_{i=1}^n a_{ij} \mid j = 1, \dots, n \right\} \leq \rho(A) \leq \max \left\{ \sum_{i=1}^n a_{ij} \mid j = 1, \dots, n \right\}.$$

Biz.: $\rho(A^T) = \rho(A)$ (ugyanaz a karakterisztikus polinom).

HF. Legyen $\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} > 0$. Mutassuk meg, hogy $A \geq 0$ esetén

$$\min \left\{ \sum_{j=1}^n a_{ij} \frac{\gamma_j}{\gamma_i} \mid i = 1, \dots, n \right\} \leq \rho(A) \leq \max \left\{ \sum_{j=1}^n a_{ij} \frac{\gamma_j}{\gamma_i} \mid i = 1, \dots, n \right\}.$$

Javaslat: Legyen

$$D = \begin{pmatrix} \gamma_1 & & & \\ & \gamma_2 & & \\ & & \ddots & \\ & & & \gamma_n \end{pmatrix}$$

és $A' = D^{-1}AD$. Ekkor, mivel A és A' hasonló mátrixok, $\rho(A) = \rho(A')$. Alkalmazzuk a fent bizonyított sorösszeg-bebecsléseket az A' mátrixra.

3.4. Pozitív mátrixok – Perron elmélete

Ebben a részben $A > 0$.

Áll.: $\rho(A) > 0$.

Biz.: A legkisebb sorösszeg alsó korlát.

Áll.: Létezik pozitív sajátvektor $\rho(A)$ sajátértékkel.

Biz.: Tudjuk már, hogy van $0 \neq v \geq 0$ vektor, amelyre $Av = \rho(A)v$. Mivel $A > 0$, Av is > 0 , így $v = \frac{1}{\rho(A)}Av > 0$.

Áll.: A $\rho(A)$ sajátértékhez tartozó pozitív sajátvektor skalárszoros erejéig egyértelmű.

Biz.: Legyen $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} > 0$ és $v' = \begin{pmatrix} \gamma'_1 \\ \vdots \\ \gamma'_n \end{pmatrix} > 0$ két sajátvektor. Legyen $\mu = \min\{\frac{\gamma'_i}{\gamma_i} \mid i = 1, \dots, n\}$. Ekkor $w = (v' - \mu v) \geq 0$, de $w \not\geq 0$, ugyanakkor $\rho(A)w = Aw$. Utóbbi > 0 , ha $w \neq 0$, így csakis $w = 0$ lehetséges, azaz $v' = \mu v$.

HF. Mutassuk meg, hogy ha $0 \neq v' \geq 0$ egy nemnegatív sajátvektora A -nak $\lambda \in \mathbb{C}$ komplex sajátértékkel, akkor $\lambda = \rho(A)$.

Javaslat: Először lássuk be, hogy $v' > 0$ és $\lambda > 0$, majd az előző gondolatmenethez hasonlóan járjunk el.

Áll. Ha λ komplex sajátértéke A -nak, amelyre $|\lambda| = \rho(A)$ és $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$ egy λ sajátértékhez tartozó komplex sajátvektor, akkor $\lambda = \rho(A)$ és v egy pozitív vektor komplex skalárszorosa.

Biz.: Tetszőleges $i = 1, \dots, n$ -re

$$\rho(A)|\gamma_i| = |\lambda||\gamma_i| = \left| \sum_{j=1}^n a_{ij}\gamma_j \right| \leq \sum_{j=1}^n a_{ij}|\gamma_j|,$$

tehát a $0 \neq w = \begin{pmatrix} |\gamma_1| \\ \vdots \\ |\gamma_n| \end{pmatrix}$ nemnegatív elemű vektorral $Aw \geq \rho(A)w = \rho'(A)w$. Egy korábbi állítás miatt w egy nemnegatív sajátvektor $\rho(A)$ sajátértékkel, így szükségképpen pozitív is. Az abszolút értékekre vonatkozó egyenlőtlenségben akkor és csak akkor van egyenlőség, ha az összes γ_j egy irányba mutat: γ_i/γ_j pozitív valós számok.

Áll.: Legyen B egy $n \times n$ -es $n-1$ rangú valós mátrix. Legyen $v \in \ker B$, $u \in \ker B^T$. Ha $v^T u \neq 0$, akkor B -nek a $B\mathbb{R}^n$ képtérre vett megszorítása nemelfajuló. Következésképpen B karakterisztikus polinomjának 0 egyszerűs gyöke.

Biz.: A rangra vonatkozó feltevés miatt B magját a v vektor generálja. Elég tehát azt belátni, hogy $v \notin B\mathbb{R}^n$. Tegyük fel indirekte, hogy létezik egy w vektor, amelyre $Bw = v$. Ekkor $v^T u = (Bw)^T u = w^T B^T u = 0$, ellentmondás.

A karakterisztikus polinomra vonatkozó állítás úgy látható, hogy a v -ből és B képterének bázisvektoraiból álló bázisra való áttérés mutatja, hogy B hasonló egy

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

alakú blokk-diagonális mátrixhoz, ahol a jobb alsó $(n-1) \times (n-1)$ -es blokk nemelfajuló, ezért a karakterisztikus polinomjának 0 nem gyöke. B karakterisztikus polinomja ezen blokk karakterisztikus polinomjának és az x polinomnak a szorzata.

Köv.: A karakterisztikus polinomjának $\rho(A)$ egyszeres gyöke.

Biz.: Legyen $v > 0$, amelyre $Av = \rho(A)v$ és $u > 0$, amelyre $A^T u = \rho(A)u$. Ekkor $uv > 0$ és alkalmazzuk az előző állítást $B = A - \rho(A)I$ -vel.

Tétel. $\left(\frac{A}{\rho(A)}\right)^k$ egy n rangú mátrixhoz konvergál. Következésképpen minden $u_0 = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$ vektorra az $u_{k+1} :=$

normált (Au_k) egy u_0 -tól független vektorhoz konvergál, ahol $\text{normált}(v) := \frac{1}{|v|}v$.

Később bizonyítjuk, általánosabban.

3.5. Irreducibilis mátrixok – Frobenius elmélete

Def. $A \geq 0$ $n \times n$ -es mátrix reducibilis, ha léteznek i_1, \dots, i_ℓ indexek ($0 < \ell < n$), hogy $a_{i_s j} = 0$ $j \notin \{i_1, \dots, i_\ell\}$ esetén. Más szóval A reducibilis, ha a sorok és oszlopok szimultán permutációjával A felső blokk-háromszög alakra hozható:

$$P^{-1}AP = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix},$$

ahol valamely $0 < \ell < n$ -re A_{11} egy $\ell \times \ell$ -es A_{12} egy $\ell \times (n-\ell)$ -es, A_{22} pedig egy $(n-\ell) \times (n-\ell)$ -es mátrix. Azt mondjuk, hogy A irreducibilis, ha nem reducibilis.

Gráfok átfogalmazás. Legyen $A \geq 0$ $n \times n$ -es mátrixhoz G_A az az n pontú irányított gráf az $\{1, \dots, n\}$ csúcshalmazon, aminek az élei azon (j, i) párok, amelyekre $a_{ij} > 0$. Ekkor A reducibilitása azt jelenti, hogy a G_A csúcsainak feloszthatók két részre úgy, hogy az első részből a másodikba nem megy él (a második részből az elsőbe még mehet.)

Példák. Reducibilisek:

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

Irreducibilisek:

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

HF. Mutassuk meg, hogy ha $A \geq 0$ irreducibilis, akkor A^T is irreducibilis.

HF. Ha egy $A \geq 0$ szimmetrikus mátrix reducibilis, akkor valamely P permutációs mátrixra $P^{-1}AP$ blokk-diagonális alakú.

HF. Minimum hány nulla eleme van egy $n \times n$ -es reducibilis mátrixnak?

Áll. Legyen $A \geq 0$ $n \times n$ -es. Ekkor A irreducibilis $\Leftrightarrow (A + I)^n > 0$.

Biz. \Leftarrow :

$$\begin{pmatrix} A_{11} + I & * \\ 0 & A_{22} + I \end{pmatrix}^n = \begin{pmatrix} (A_{11} + I)^n & * \\ 0 & (A_{22} + I)^n \end{pmatrix} \not> 0.$$

\Rightarrow : Legyen $v \geq 0$ és A irreducibilis. $(A + I)v = v + Av$ pozitív azokon a helyeken, ahol v pozitív. Tegyük fel, hogy v az i_1, \dots, i_ℓ helyeken pozitív és $1 < \ell < n$. Ha A nem reducibilis, akkor vannak olyan $i \in \{i_1, \dots, i_\ell\}$ és $j \notin \{i_1, \dots, i_\ell\}$, amelyekre $a_{ij} > 0$. Ekkor $(A + I)v$ pozitív lesz a j -edik helyen. Tehát $(A + I)v$ több helyen pozitív, mint v . Így minden $0 \neq v \geq 0$ vektorra $(A + I)^{n-1}v > 0$, és ezt $A + I$ oszlopaira alkalmazva kapjuk, hogy $(A + I)^n = (A + I)^{n-1}(A + I) > 0$. (Ha A valamely oszlopa (sora) 0, akkor A nyilván reducibilis.)

Gráfes észrevétel. $A, B \geq 0$ $n \times n$ -es mátrixokra G_{AB} csak G_A -tól és G_B -től függ: a (j, i) pár él G_{AB} -ben, ha van olyan $k \in \{1, \dots, n\}$ szám, amelyre az (k, i) pár él A -ban és a (j, k) pár él B -ben.

Köv.. (j, i) él G_{A^ℓ} -ben \Leftrightarrow van G_A -ban j -ből i -be menő ℓ hosszú irányított séta.

Köv.. (j, i) él $G_{(A+I)^n}$ -ben \Leftrightarrow van G_A -ban j -ből i -be menő irányított út.
Innen:

Irreducibilitás és erős összefüggőség. $A \geq 0$ irreducibilis $\Leftrightarrow G_A$ erősen összefüggő.

Áll. Ha $A \geq 0$ irreducibilis, akkor $\rho(A) > 0$.

Biz. A -ban nincs csupa 0 sor és a legkisebb sorösszeg egy alsó korlát.

Észrevétel. Ha v sajátvektora A -nak λ sajátértékkel, akkor v sajátvektora $(A + I)^n$ -nek is, $(\lambda + 1)^n$ sajátértékkel. Speciálisan: ha v sajátvektora A -nak $\rho(A)$ sajátértékkel (tudjuk, hogy van ilyen $v \geq 0$), akkor v sajátvektora $(A + I)^n$ -nek is, $\rho((A + I)^n) = (\rho(A) + 1)^n$ sajátértékkel. Ha A irreducibilis, akkor tehát alkalmazható $(A + I)^n$ -re a Perron-elmélet. Ebből adódóan:

Tétel. Tegyük fel, hogy $A \geq 0$ $n \times n$ -es irreducibilis mátrix. Ekkor

- $\rho(A)$ sajátértéke A -nak;
- $\rho(A)$ egyszeres gyöke A karakterisztikus polinomjának;
- létezik A -nak pozitív sajátvektora $\rho(A)$ sajátértékkel.

Példa. Az n hosszú ciklusoknak megfelelő n -times n -es permutációs mátrixok irreducibilisek, mindegyik sajátértékük 1 abszolút értékű.

HF. Másmilyen permutációk mátrixa reducibilis.

3.6. Konvergencia primitív mátrixokra

Def.: $A \geq 0$ primitív, ha irreducibilis és $\rho(A)$ az egyetlen $\rho(A)$ abszolút értékű sajátértéke.

HF. Ha $A \geq 0$ irreducibilis, szimmetrikus és pozitív szemidefinit, akkor A primitív.

Lemma: Legyen B egy olyan komplex elemű mátrix, amelynek minden sajátértéke 1-nél kisebb abszolút értékű. Ekkor $\lim_{k \rightarrow \infty} B^k = 0$.

Tétel: Tegyük fel, hogy az $A \geq 0$ irreducibilis mátrix primitív. Ekkor

$$\left(\frac{A}{\rho(A)} \right)^k \rightarrow vu^T,$$

ahol v A -nak, u pedig A^T -nek egy sajátvektora $\rho(A)$ sajátértékkel, amelyekre $u^T v = 1$ teljesül.

Biz.: Tudjuk, hogy $A - \rho(A)$ rangja $n - 1$, továbbá azt is, hogy $v \notin (A - \rho(A)I)\mathbb{R}^n$, tehát van \mathbb{R}^n -nek egy olyan bázisa, amely v -ből és az $(A - \rho(A)I)\mathbb{R}^n$ altér egy bázisából áll. C az a mátrix, amelynek az oszlopai ez a bázis (azaz standard bázist erre a bázisra cserélő báziscsere mátrixa). Ekkor

$$C^{-1} \frac{1}{\rho(A)} AC = \begin{pmatrix} 1 & & \\ & \boxed{B} & \\ & & \end{pmatrix}$$

alakú, ahol $\rho(B) < 1$. Az előző lemma alapján létezik $\lim(C^{-1} \frac{1}{\rho(A)} AC)^k$ és ez a határérték

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

alakú. Innen, mivel

$$(C^{-1} \frac{1}{\rho(A)} AC)^k = C^{-1} \left(\frac{1}{\rho(A)} A \right)^k C,$$

azt kapjuk, hogy $(\frac{A}{\rho(A)})^k$ egy, a v vektor által generált egy dimenziós altérre történő (nem feltétlenül merőleges) vetítés mátrixához konvergál: létezik $P = \lim(\frac{A}{\rho(A)})^k$, amely $P = vu^T$ alakú (azaz P oszlopai v skalárszorosai) valamely $u' \in \mathbb{R}^n$ vektorra és $P^2 = P$. Az A^T mátrixra alkalmazva azt kapjuk, hogy $P^T = Uv^T$ alakú, tehát $P = v'u^T$ valamely v' -re. Így v' a P képterének egy generátora, tehát a v vektor egy skalárszorosa, és hasonlóan, u' az u egy skalárszorosa. Így P a vu^T mátrix egy skalárszorosa, Ez $P^2 = P$ és $vu^T vu^T = vu^T$ miatt csakis úgy lehet, hogy $P = vu^T$.

Köv.: Legyen $A \geq 0$ irreducibilis Ekkor A primitív $\Leftrightarrow A^k > 0$ valamely $k > 0$ egész számra.

HF. Tegyük fel, hogy $A = (a_{ij}) \geq 0$ irreducibilis és $a_{ii} > 0$ valamely i -re. Mutassuk meg, hogy ekkor A primitív.

HF. Legyen A irreducibilis, de imprimitív. Ekkor A^k reducibilis valamely $k > 1$ egészre.

HF. Legyen A irreducibilis és primitív. Ekkor A^k irreducibilis és primitív minden $k \geq 1$ egészre.

Példák: Imprimitívek:

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

primitívek:

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

3.7. Imprimitív irreducibilis mátrixok

Áll.: Legyen $B = (b_{ij})$ komplex, $A = (a_{ij})$ pedig nemnegatív valós irreducibilis $n \times n$ -es mátrix, hogy $|b_{ij}| \leq a_{ij}$. Tudjuk, hogy $\rho(B) \leq \rho(A) = \rho'(A)$. Tegyük fel, hogy $\rho(B) = \rho(A)$ és $\lambda = c\rho(A)$ egy komplex sajátértéke B -nek, ahol

$|c| = 1$. Ekkor $B = cD^{-1}AD$ alakú, ahol D komplex diagonális mátrix 1 abszolút értékű elemekkel az átlóban.

Biz.: Legyen $v = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$ egy λ -sajátvektor: $v \neq 0$ és $Bv = \lambda v$. Tetszőleges $i = 1, \dots, n$ -re

$$\rho(A)|\gamma_i| = |\lambda||\gamma_i| = \left| \sum_{j=1}^n b_{ij}\gamma_j \right| \leq \sum_{j=1}^n a_{ij}|\gamma_j|,$$

tehát a $0 \neq w = \begin{pmatrix} |\gamma_1| \\ \vdots \\ |\gamma_n| \end{pmatrix} \geq 0$ vektorral $Aw \geq \rho(A)w = \rho'(A)w$. Így w egy (a skalárszoros erejéig egyértelmű)

pozitív sajátvektora A -nak $\rho(A)$ sajátértékkel. Legyen $\gamma_i = d_i|\gamma_i|$, ahol $|d_j| = 1$. A fenti képletben az egyenlőtlenségek egyenlőséggel teljesülnek:

$$\rho(A)|d_i\gamma_i| = \left| \sum_{j=1}^n b_{ij}d_j|\gamma_j| \right| = \sum_{j=1}^n a_{ij}|\gamma_j|,$$

ami csak úgy lehet, hogy $|b_{ij}| = a_{ij}$ és a nem-nulla komponensek mind a d_i irányba mutatnak: ha $a_{ij} \neq 0$, akkor $b_{ij}/a_{ij}d_j = d_i$. Ekkor $b_{ij} = d_i^{-1}a_{ij}d_j$, attól függetlenül, hogy $a_{ij} > 0$ vagy sem, és így $B = D^{-1}AD$, ahol D átlójában a d_i komplex számok állnak.

Köv.: Legyen $A \geq 0$ irreducibilis, c komplex szám, amelyre $|c| = 1$. Ekkor $c\rho(A)$ akkor és csak akkor sajátértéke A -nak, ha a cA mátrix, mint komplex mátrix hasonló A -hoz. Ez esetben $c\rho(A)$ egyszeres gyöke A karakterisztikus polinomjának.

Biz.: \Rightarrow : előző állítás $B = A$ -val.

\Leftarrow : Ha $cA = D^{-1}AD$, akkor $A = cDAD^{-1}$, és ha $Av = \rho(A)v$, akkor $w = Dv$ -re $Aw = cDAD^{-1}Dv = cDAv = c\rho(A)Dv = c\rho(A)w$.

Egyszeresség: Ha $\rho(A)$ egyszeres gyöke $\det xI - A$ -nak, akkor $c\rho(A)$ egyszeres gyöke $\det xI - cA$ -nak.

Köv.: Ha $|c| = 1, |c'| = 1$ és $c\rho(A)$ és $c'\rho(A)$ sajátértékei az $A \geq 0$ irreducibilis mátrixnak, akkor c^{-1} és cc' is sajátértéke A -nak.

Biz.: Ha $cA = D^{-1}AD$ és $c'A = D'^{-1}AD'$, akkor $c^{-1}A = DAD^{-1}$ és $cc'A = (D'D)^{-1}AD'D$.

Köv.: Ha az A irreducibilis mátrixnak s darab $\rho(A)$ abszolút értékű sajátértéke van, akkor ezek $e^{2\ell\pi i/s}\rho(A)$, $\ell = 0, \dots, s-1$.

Tétel. Ha az A irreducibilis mátrixnak s darab $\rho(A)$ abszolút értékű sajátértéke van, akkor alkalmas P permutációs mátrixszal

$$P^{-1}AP = \begin{pmatrix} 0 & A_{12} & 0 & \dots & 0 & 0 \\ 0 & 0 & A_{23} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & A_{s-2,s-1} & 0 \\ 0 & 0 & \dots & \dots & 0 & A_{s-1,s} \\ A_{s1} & 0 & \dots & \dots & 0 & 0 \end{pmatrix},$$

ahol A_{ij} illetve az ij helyen álló nulla egy $\mu_i \times \mu_j$ méretű blokk ($i, j = 1, \dots, s$).

Biz.: Legyen $c = e^{2\pi i/s}$ és legyen $D = (d_{ij})$ olyan diagonális mátrix, amelyre $d_i = d_{ii}$ 1 abszolút értékű komplex számok és $D^{-1}AD = cA$. Ekkor $ca_{ij} = \frac{d_j}{d_i}a_{ij}$, tehát $a_{ij} = 0$, hacsak nem $d_j = cd_i$. Legyen $t_0 = 0$. A koordináták alkalmas permutációjával elérhető, hogy $d_1 = \dots = d_{t_1}$ és $d_j \neq d_1$, ha $j \notin \{1, \dots, t_1\}$. Mivel A primitív, létezik olyan $i \in \{1, \dots, t_1\}$, hogy $a_{ij} \neq 0$ valamely j -re. Ezért $d_j = cd_i = cd_1$. Alkalmas cserével elérhető, hogy $t_1 + 1$ ilyen j legyen. Elérhető az is, hogy $d_{t_1+1}, \dots, d_{t_2}$ a D -nek cd_1 -gyel megegyező diagonális értékei. Megint A irreducibilitását használva található egy olyan i, j pár, amelyre $i \leq t_2 < j$ és $a_{ij} \neq 0$. Ekkor $cd_i = d_j \neq d_{t_1+1}$, így $t_1 < i \leq t_2$. Elérhető, hogy $t_2 + 1$ egy ilyen j és gyűjtjük össze egymás utánra D d_{t_2+1} -gyel megegyező elemeit. Ezt folytatva s lépésben elérjük, hogy $d_{t_i+1}, \dots, d_{t_{i+1}}$ éppen a D mátrix $c^i d_1$ -gyel megegyező elemei ($i = 1, \dots, s-1$).

3.8. Sztochasztikus mátrixok és Markov-láncok

3.8.1. Markov-láncok

Véges állapotú, homogén Markov-lánc.:

Állapotok: $\{1, \dots, n\}$

$X_0, X_1, X_2, \dots, \Pr(X_{k+1} = i | X_k = j) = a_{ij}$

a_{ij} : az $j \rightarrow i$ átmenet valószínűsége

X_k eloszlása: $\sim v^k = \begin{pmatrix} \gamma_1^k \\ \vdots \\ \gamma_n^k \end{pmatrix}$ - sztochasztikus vektor: $v^k \geq 0, \sum_{j=1}^n \gamma_j^k = 1$

$A = (a_{ij})$ átmenet-mátrix (oszlop-)sztochasztikus: $A \geq 0$ és $\sum_{i=1}^n a_{ij} = 1$ ($j = 1, \dots, n$)

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

$v^k = A^k v^0$, ahol v^0 a kezdeti eloszlás.

3.8.2. Sztochasztikus mátrixok elemi tulajdonságai

Ebben a részben A (oszlop)sztochasztikus

Áll.: Ha A sztochasztikus, akkor $\rho(A) = 1$

Biz.: HF

Áll.: $\begin{pmatrix} \frac{1}{n} \\ \vdots \\ \frac{1}{n} \end{pmatrix}$ sajátvektora A^T -nak 1 sajátértékkel

Áll.: u sztochasztikus vektor $\Rightarrow Au$ sztochasztikus

Biz.: $A = (a_{ij}), u = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$.

Au elemeinek összege $= \sum_i \sum_j a_{ij} \gamma_j = \sum_j \gamma_j \sum_i a_{ij} = \sum_j \gamma_j = 1$.

Áll.: Sztochasztikus mátrixok szorzata is sztochasztikus.

Biz.: HF

3.8.3. Irreducibilitás értelmezése:

Minden állapotból minden állapot elérhető pozitív valószínűséggel

3.8.4. Imprimitivitás értelmezése:

Ha A irreducibilis és s darab $\rho(A)$ abszolút értékű sajátértéke van, akkor A^k főátlója 0, ha k nem osztható s -sel. Tehát minden j -re a $j \rightarrow j$ átmenet csak s -sel osztható számú lépésben lehetséges: az állapotok periodikusak.

3.8.5. Konvergenciatétel értelmezése:

Ha A primitív, akkor $A^k \rightarrow v \cdot (1 \dots 1)$ ahol v A -nak sztochasztikusra normált sajátvektora $1 = \rho(A)$ sajátértékkel. Így tetszőleges v_0 sztochasztikus vektorra

$$A^k v_0 \rightarrow v.$$

A Markov-láncok nyelvén: ha tetszőleges kezdeti eloszlás esetén X_n eloszlása konvergál az úgynevezett stacionárius eloszláshoz, amennyiben a lánc irreducibilis és az állapotok aperiodikusak.

3.9. Duplán sztochasztikus mátrixok

Def.: $A = (a_{ij}) \geq 0$ duplán sztochasztikus, ha A és A^T is (oszlop-)sztochasztikus.

HF.: Igazoljuk, hogy ha A egy duplán sztochasztikus mátrix, akkor alkalmas P permutációval $P^{-1}AP$ blokk-diagonális alakra hozható, ahol a blokkok irreducibilisek.

Áll.: Duplán sztochasztikus mátrixok konvex kombinációja is duplán sztochasztikus.

Példa.: Permutációs mátrixok.

Tétel (Frobenius-König-Hall): Legyen $G = (U, V, E)$ egy páros gráf. Akkor és csak akkor létezik olyan párosítás (független élrendszer) G -ben, amely U minden pontját lefedi, ha bármely $W \subseteq U$ -ra a W -beli pontok szomszédjai legalább annyian vannak, mint W elemei:

$$\#\{v \in V \mid \exists w \in W : (w, v) \in E\} \geq \#W.$$

Birkhoff tétele: Egy duplán sztochasztikus A mátrix permutációs mátrixok konvex kombinációja.

Biz.: Indukciót alkalmazunk A pozitív elemeinek a száma szerint. Legyen G az a páros gráf, melynek csúcsai az oszlopindexek, illetve a sorindexek, és legyen (i, j) él G -ben, ha $a_{ij} \neq 0$. Belátjuk, hogy G -re teljesül a Hall-feltétel. Tegyük fel, hogy van az oszlopoknak olyan m elemű W halmaza, amellyel a gráfban összekötött sorok m -nél kevesebben vannak. A W -be eső oszlopok elemeinek összege m . Mivel ezen oszlopok nem-nulla elemei m -nél kevesebb sorban helyezkednek el, az összeg m -nél kisebb, ellentmondás. Tehát van G -ben egy teljes párosítás, ami egy olyan P permutációs mátrixnak felel meg, amelynek megfelelő helyein az A mátrix elemei pozitívak. Legyen a a legkisebb ezen n elem közül. Ha $a = 1$, akkor $A = P$ és készen vagyunk. Ha $a < 1$, akkor legyen $B = \frac{1}{1-a}(A - aP)$. Ekkor A a B és a P mátrixok konvex kombinációja, B duplán sztochasztikus, és A -nál kevesebb pozitív eleme van. Indukció B -re.

3.10. Pagerank

Sergei Brin és Larry Page algoritmus a weblapok rangsorolására (1998)

Első megközelítés:

Állapotok \sim weblapok

$$a_{ij} = \frac{\#j \rightarrow i \text{ linkek}}{\#j \rightarrow \text{linkek}}$$

$$v^0 = \begin{pmatrix} \frac{1}{n} \\ \vdots \\ \frac{1}{n} \end{pmatrix},$$

$$v^{k+1} = Av_k$$

Azt modellezi, hogy milyen valószínűséggel, merre jár egy, a linkek közül egy véletlenül kiválasztott mentén továbblépő szörfölő.

Probléma: Még csak nem is reducibilis (vannak lapok, ahonnan nem lehet továbbmenni).

Módosított mátrix: A helyett

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

ahol E a csupa 1-ből álló mátrix: $E = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$. Ez az A' már pozitív elemű, így A'^k konvergens. A rangsor $A'^K v^0$

súlyai szerint, ahol K nagy.

Szemléletesen: A türelmetlen szörfölő modellje: α valószínűséggel elúnja a barangolást, és véletlenül választott lapra lép.

3.11. Gyűjtőlapok és tekintélyek

Jon Kleinberg 1998-ban publikált módszere.

Modell: A lapok kétféle értéket kapnak: gyűjtő (g_i), illetve tekintély értéket (t_i). Az az értékesebb lap, amelyre minél több minél jobb gyűjtő mutat, és az a jó gyűjtő, amely minél több minél értékesebb lapra mutat:

$$t_i = c \cdot \sum_{j \rightarrow i} g_j \quad (i = 1, \dots, n)$$

és

$$g_j = c' \cdot \sum_{i \leftarrow j} t_i \quad (j = 1, \dots, n)$$

c és c' normáló tényezők, hogy pl. $\sum_{j=1}^n g_j^2 = 1$ és $\sum_{i=1}^n t_i^2 = 1$ teljesüljön. (Megfelelő lenne a $\sum_{j=1}^n g_j = \sum_{i=1}^n t_i = 1$ kikötés is.) Kezdetben $g_j = \frac{1}{\sqrt{n}}$, $t_i = \frac{1}{\sqrt{n}}$.

Mátrixokkal és pontosabban: Legyen $A = (a_{ij})$ a web adjacenciamátrixa: $a_{ij} = 1$, ha az i lap mutat a j lapra, különben $a_{ij} = 0$.

$$g^0 = \begin{pmatrix} \frac{1}{\sqrt{n}} \\ \vdots \\ \frac{1}{\sqrt{n}} \end{pmatrix},$$

$$t^k = cA^T g^k,$$

$$g^{k+1} = c' A t^k.$$

Gyűjtőkre:

$$g^0 = \begin{pmatrix} \frac{1}{\sqrt{n}} \\ \vdots \\ \frac{1}{\sqrt{n}} \end{pmatrix},$$

$$g^{k+1} = c' c A A^T g^k.$$

Itt AA^T egy nemnegatív elemű pozitív szemidefinit szimmetrikus mátrix, így sajátértékei nemnegatívek AA^T akkor reducibilis, ha a lapok olyan csoportokra bonthatók, amelyek diszjunkt laphalmazokra mutatnak. Ilyen esetben csoportonként lehet dolgozni. Ha AA^T irreducibilis, akkor AA^T mátrix legnagyobb sajátértéke 1-szeres, így $(AA^T)^k$ alkalmasan lenormálva konvergens, és a g^k sorozat is konvergál a megfelelő sajátvektorhoz.

Gyakorlatban: Nem az egész webre, hanem egy viszonylag kicsi, de az adott témakörben reprezentatív mintára.

4. Egyebek

4.1. Hadamard-kódok

Hibajavító kódok

Kód: Egy \mathbb{F} ábécé feletti n hosszú kód egy $C \subseteq F^n$ halmaz.

Hamming-távolság: Legyen $v = (\gamma_1, \dots, \gamma_n)^T, v' = (\gamma'_1, \dots, \gamma'_n)^T \in \mathbb{F}^n$. Ekkor

$$d(v, v') = \#\{i \mid \gamma'_i \neq \gamma_i\}.$$

Tényleg távolság: $d(v, v') = d(v', v)$; $d(v, v') = 0 \Leftrightarrow v = v'$; és teljesül a háromszög-egyenlőtlenség:

$$d(v, v'') \leq d(v, v') + d(v', v'').$$

Kódtávolság: C minimális távolsága vagy kódtávolsága

$$\min_{v \neq v' \in C} d(v, v').$$

Kódtávolság és hibajavítás: Ha C távolsága d , akkor $\lfloor (d-1)/2 \rfloor$ hibát ki lehet javítani.

Lineáris kódok: Legyen \mathbb{F} test. Egy n hosszú lineáris kód egy $C \leq \mathbb{F}^n$ altér.

Hamming-súly: Ha $v = (\gamma_1, \dots, \gamma_n)^T$, akkor $w(v) = d(0, v)$.

Kódtávolság lineáris kódokra: $C \leq \mathbb{F}^n$ kód távolsága a minimális nem 0 súly C -beli szavakra:

$$\min_{v \in C} w(v).$$

Lineáris kódok paramétereit: $C \leq \mathbb{F}^n$ egy $[n, k, d]$ -kód, ahol:

- n a kódhossz
- $k = \dim_{\mathbb{F}} C$ a dimenzió
- d a kódtávolság

Kódsebesség: $R = k/n$.

Hadamard-kódok

Más néven elsőrendű Reed-Muller-kódok.

$$\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$$

Paraméterek: $[n = 2^m, k = m + 1, d = 2^{m-1}]$.

Kódolás: Legyen $u = (\gamma_1, \dots, \gamma_m)^T, \beta \in \mathbb{F}$. Ekkor a (u, β) párhoz a

$$(u^T v + \beta | v \in \mathbb{F}^m)^T$$

2^m hosszú vektort rendeljük.

A kódszavak: A $\mathbb{F}^m \rightarrow \mathbb{F}$ elsőfokú polinomok, mint függvények. ($\beta = 0$ -ra lineáris függvények.)

A súlyok: az azonosan 0 függvény súlya 0. Egyéb esetben $\beta = 0$ -ra egy lineáris függvényünk van, aminek a magja egy $m - 1$ dimenziós altér, tehát a súly 2^{m-1} . $\beta = 1$ -re vagy az azonosan 1 függvényünk van 2^m súllyal, vagy a zérushelyek egy $m - 1$ dimenziós altér komplementerét alkotják, akkor a súly ismét 2^{m-1} .

Mariner 9 Mars-szonda (1971): $m = 5$ -re Hadamard-kód

$$[32, 6, 16].$$

Hasonló sebességű ismétlődő kód: $b \mapsto (b, b, b, b, b)$

Távolság: 5.

Lokális dekódolhatóság: Ha csak az v -"edik" bitre vagyunk kíváncsiak, vegyünk véletlenül egy v' vektort és legyen $v'' = v - v'$. Tegyük fel, hogy a 2^m bit közül legfeljebb $p2^m$ bit romlott meg, ahol $p < 1/4$: Ha a csatornára a bemenet az $f : \mathbb{F}^m \rightarrow \mathbb{F}$ lineáris függvény és a kimenet a g függvény, akkor $\text{Prob}_v(g(v) = f(v)) \geq 1 - p$. Ekkor $\text{Prob}_{v', v''}(g(v') = f(v') \text{ és } g(v'') = f(v'')) \geq 1 - 2p > 1/2$, így $\text{Prob}_{v', v''}(f(v) = g(v') + g(v'')) \geq 1 - 2p > 1/2$. Néhányszor (p -tól függő konstanssal $O(\log(1/\epsilon))$ -szor) ismételve és a többséget véve tetszőleges konstans $\epsilon > 0$ hibavalószínűség elérhető.