Alkalmazott algebra - skalárszorzat

Ivanyos Gábor

2011 ősz

Skalárszorzat

Ebben a részben: a standard skalárszorzat:

$$u^T v = \sum_{i=1}^{n} \mu_i \nu_i$$

és a kapcsolódó lineáris algebra absztrakt tárgyalással

$$u = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} \quad v = \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix}$$

Miért:

- általánosítások is kezelhetők
- betekintés a mögöttes struktúrákba
- okos bizonyítások (számolás helyett)

Oddtown

- **Forrás:** L. Babai, P. Frankl: Linear algebra methods in combinatorics
- n lakos
- **Szabályok Oddtown klubjaira:**
  - Bármely klubnak csakis **páratlan** sok tagja lehet
  - Bármely két klubnak csakis **páros** sok közös tagja lehet
- **Kérdés:** Max. hány klub lehet?

Oddtown

- Incidencia-mátrix:
  - sorok $\sim$ lakosok (n)
  - oszlopok $\sim$ klubok (k)
  - $A = (a_{ij})$ n-szer k-as

$$a_{ij} = \begin{cases} 1 & \text{ha } i\text{. lakos tagja a } j\text{. klubnak} \\ 0 & \text{különben} \end{cases}$$

- a szabályok:
  - $\sum_{i=1}^{n} a_{ij}$ páratlan $(1 \leq j \leq k)$
  - $\sum_{i=1}^{n} a_{ij}a_{ij'}$ páros $(1 \leq j \neq j' \leq k)$

Oddtown

- Modulo 2 (azaz a $\mathbb{Z}_2$ testben dolgozunk): $a_{ij} \in \mathbb{Z}_2$
- A szabályok:
  - $\sum_{i=1}^n a_{ij} = 1 \ (1 \leq j \leq k)$
  - $\sum_{i=1}^n a_{ij}a_{ij'} = 0 \ (1 \leq j \neq j' \leq k)$
- "szimmetrikusabb" megfogalmazás:
  - $\sum_{i=1}^n a_{ij}a_{ij} = 1 \ (1 \leq j \leq k)$
  - $\sum_{i=1}^n a_{ij}a_{ij'} = 0 \ (1 \leq j \neq j' \leq k)$
- mátrixosan:

$$A^T A = I_k$$

Oddtown

- $A^T A = I_k$
- $A^T A$ képtere k-dimenziós
- A^T képtere $\geq k$-dimenziós
  (mivel $A^T A$ képtere $\leq A^T$ képtere)
- A^T rangja $\geq k$,sőt, $= k$, mert k sora van
- A rangja k
- **konklúzió:** $k \leq n$
- ennyi klub lehet is (pl. az egyeleműek)

Oddtown

- mátrixosan: $A^T A = I_k$
- oszlopvektorokkal: $v_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$

$$v_j^T v_{j'} = \begin{cases} 1 & \text{ha } j = j' \\ 0 & \text{különben} \end{cases}$$

- szavakban: A oszlopvektorai **"ortonormált"** rendszert alkotnak $\mathbb{F}_2^n$-ben

  a standard "skalárszorzatra"

Eventown

- Bármely klubnak csakis **páros** sok tagja lehet
- Bármely két klubnak csakis **páros** sok közös tagja lehet
- különböző klubok tagsága különböző halmazok
- Incidencia-mátrixszal (mod 2):

$$A^T A = 0$$

- oszlopvektorokkal

$$v_j^T v_{j'} = 0$$

  akár $j \neq j'$, akár $j = j'$.
- **Példa:** tfh. a város lakói házaspárok (esetleg $+1$ szingli) Legyenek a klubok a házaspárokból álló halmazok.
- **Köv.:** $k = 2^{[n/2]}$ lehetséges
- **Kérdés:** lehet-e több?

Szimmetrikus bilineáris függvény

olyan $\langle , \rangle : V \times V \to \mathbb{F}$, ami

- **mindkét változójában lineáris**, azaz $\langle u+u', v\rangle = \langle u, v\rangle + \langle u', v\rangle$ és $\langle u, v+v'\rangle = \langle u, v\rangle + \langle u, v'\rangle$ $(\forall u, u', v, v' \in V)$; továbbá $\langle \lambda u, v\rangle = \lambda\langle u, v\rangle$ és $\langle u, \lambda v\rangle = \lambda\langle u, v\rangle$ $\quad (\forall u, v, \in V, \lambda \in \mathbb{F})$
- és **szimmetrikus**, azaz $\langle u, v\rangle = \langle v, u\rangle \quad (\forall u, v \in V)$.
- **Példa (standard skalárszorzat $\mathbb{F}^n$-en):**

$$(u, v) = u^T v = \sum_{i=1}^{n} u_i v_i$$

- **Végtelen dimenziós példa:** négyzetesen integrálható $[0, 1] \to \mathbb{R}$ függvények

$$\langle f, g\rangle := \int f(x)g(x)dx$$

Merőlegesség

- u és v **merőlegesek** ($u \perp v$), ha $\langle u, v\rangle = 0$.
- szimmetrikus reláció
- **Def.:** $v_1, \ldots, v_\ell$ rendszer **ortogonális**, ha $v_i \perp v_j$ $(i \neq j)$

  ortonormált rendszer: ha még $\langle v_i, v_i\rangle = 1$
- Ha $v_1, \ldots, v_\ell$ ortogonális, de semelyik v_j nem merőleges önmagára, akkor $v_1, \ldots, v_\ell$ lineárisan függetlenek.
  - **Biz.**: Tfh. $0 = \sum_{i=1}^{\ell} \alpha_i v_i$.
  - Ekkor bármely j-re: $0 = \langle 0, v_j\rangle = \sum_{i=1}^{\ell} \alpha_i \langle v_i, v_j\rangle = \alpha_j \langle v_j, v_j\rangle$
  - Azaz bármely j-re $\alpha_j = 0$.
- Innen: Oddtown vektorai lin. függetlenek

Merőlegesség

- **Def.:** A $v_1, \ldots, v_n$ bázis **ortogonális**, ha $v_i \perp v_j$ $(i \neq j)$

  ortonormált bázis: ha még $\langle v_i, v_i \rangle = 1$
- **Példa:** $\mathbb{F}^n$-ben a standard skalárszorzatra a standard bázis.
- **Példa:** $\mathbb{R}^2$-ben $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ és $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$
- **Def. (merőleges altér):** $S \subseteq V$-re

$$S^{\perp} := \{v \in V | u \perp v \text{ minden } u \in S\text{-re}\}$$

  altér. $S^{\perp\perp} \geq \langle S \rangle$.

  $u^{\perp} := \{u\}^{\perp}$
- lehetséges $u \in u^{\perp}$ (ilyen u: *izotróp* vektor)
- **rendezésfordító:** $U \leq W$-re $U^{\perp} \geq W^{\perp}$

Merőlegesség

Áll.: Ha $V^\perp = (0)$, akkor $U \leq V$-re $\dim U^\perp = \dim V - \dim U$.

Biz.: Legyen $v_1, \ldots, v_n$ bázis V-ben, $u_1, \ldots, u_k$ bázis U-ban. Legyen $A = (a_{ij})$ $k \times n$-es, ahol $a_{ij} = \langle u_i v_j \rangle$:

$$A = \begin{pmatrix} \langle u_1, v_1 \rangle & \ldots & \langle u_1, v_n \rangle \\ \vdots & \ddots & \vdots \\ \langle u_k, v_1 \rangle & \ldots & \langle u_k, v_n \rangle \end{pmatrix}$$

Legyen $\phi : V \mapsto \mathbb{F}^k$ a $v \mapsto \begin{pmatrix} \langle u_1, v \rangle \\ \vdots \\ \langle u_k, v \rangle \end{pmatrix}$, $\psi : U \mapsto \mathbb{F}^n$ az $u \mapsto \begin{pmatrix} \langle u, v_1 \rangle \\ \vdots \\ \langle u, v_n \rangle \end{pmatrix}$ lin. lekép.

Ezekre: $\ker \phi = U^\perp$, $\ker \psi = V^\perp \cap U = (0)$. A ϕ mátrixa A, a ψ mátrixa A^T.

$$\dim \phi V = A \text{ rangja} = \dim \psi U.$$

A dimenziótétel miatt $\dim \phi V = \dim V - \dim \ker \phi = \dim V - \dim U^\perp$, míg $\dim \psi U = \dim U - \dim \ker \psi = \dim U$. Összeolvasva $\dim V - \dim U^\perp = \dim U$.

Merőlegesség

- **Köv.:** Ha $V^\perp = (0)$, akkor $U \leq V$-re $U^{\perp\perp} = U$.

  Biz.: A definícióból $U^{\perp\perp} \geq U$ nyilvánvaló.
  Az előző állításból

$$\dim U^{\perp\perp} = \dim V - \dim U^\perp = \dim V - \dim V + \dim U = \dim U,$$

  így $U^{\perp\perp} > U$ kizárt.

- **Áll.:** $V = \mathbb{F}^n$ standard skalárszorzatára $V^\perp = (0)$

  Biz.: Legyen $v_1, \ldots, v_n$ a standard bázis. Ekkor $u = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$-ra

$$(u, v_i) = \alpha_i,$$

  innen $V^\perp = (0)$.

Alkalmazás: Eventown

- **Köv.:** Ha $V^\perp = (0)$ és $U \leq V$, hogy $U \leq U^\perp$, akkor $\dim U \leq \frac{1}{2} \dim V$.

  Biz.: $\dim V = \dim U + \dim U^\perp \geq \dim U + \dim U$

  Eventown szabályai:

- Bármely klubnak csakis **páros** sok tagja lehet
- Bármely két klubnak csakis **páros** sok közös tagja lehet

  oszlopvektorokkal:

$$v_j v_{j'} = 0$$

  akár $j \neq j'$, akár $j = j'$.

- Legyen $U = \langle v_1, \ldots, v_k \rangle$. Ekkor $U \leq U^\perp$.
- **Köv.:** $k = 2^{[n/2]}$ a lehető legnagyobb klubszám

Lineáris kódok

- $\mathbb{F}$ véges test $\sim$ ábécé v. jegyhalmaz (pl. $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$)
- **lineáris kód:** U altér $\mathbb{F}^n$-ben
- **kódszavak:** U-beli vektorok
- **Hamming-távolság** $\mathbb{F}^n$-en: $d(u, v) = |\{i : \mu_i \neq \nu_i\}|$, ahol $u = (\mu_1, \ldots, \mu_n)^T$, $v = (\nu_1, \ldots, \nu_n)^T$
- **Hamming-súly:** $s(u) := d(u, 0)$ (nem 0 helyek száma)
- $d(u, v) = s(u - v)$

Lin. kódok paraméterei:

- **kódhossz:** n - ilyen hosszú egy kódszó
- **dimenzió:** $k = \dim U$ - ilyen hosszú sorozatot kódol egy kódszó
- **kódtávolság:** $d = \min_{u \neq v \in U} d(u, v) = \min_{0 \neq u \in U} s(u)$
- $[(d-1)/2]$ hibát ki tudunk javítani
- **Megj.:** A kódtávolság értelmes nemlin. kódra ($\mathbb{F}^n$ részhalmazaira, és itt az se kell, hogy $\mathbb{F}$ test legyen), csak nem feltétlenül azonos a min. súllyal.

Példák kódokra

- Kódolás: $\mathbb{F}^k \to U$ bijekció (nem feltétlenül lin.)
- **triviális** kódok - a teljes: $v \mapsto v$ (nincs redundancia)
  $U = \mathbb{F}^n$, $k = n$, $d = 1$

  triviális kódok - a nulla: (nulla információ)
  $U = (0)$, $k = 0$, $d = \infty$
- **Ismétlő** kód: $a \mapsto (a, a, \dots, a)^T$
  $U = \{(a, \dots, a)^T\}$, $k = 1$, $d = n$
- **Paritás**-kód:
  $(\alpha_1, \dots, \alpha_{n-1})^T \mapsto (\alpha_1, \dots, \alpha_{n-1}, -\alpha_1 - \dots - \alpha_{n-1})^T$
  $U = \{(\alpha_1, \dots, \alpha_n)^T | \alpha_1 + \dots + \alpha_n = 0\}$, $k = n - 1$, $d = 2$:
  egy hibát tud jelezni

Hadamard-kódok (elsőrendű Reed–Muller-kódok)

- $\mathbb{F} = \mathbb{Z}_2$, $n = 2^m$.
- $k = m + 1$: Egy $v = (\alpha_1, \ldots, \alpha_m, \beta)^T$ vektorra

$$f_v(x_1, \ldots, x_m) := \alpha_1 x_1 + \ldots + \alpha_m x_m + \beta$$

  a kódszó-vektor: az f_v értékei a lehetséges 2^m helyen
- $d = 2^{m-1}$:
  - Ha $\beta = 0$ akkor f_v egy lineáris függvény $\mathbb{Z}_2^m$-en, a magja vagy m dimenziós ($f_v \equiv 0$) vagy $m - 1$ dimenziós. Utóbbi esetben f_v a maradék 2^{m-1} helyen lesz 1.
  - Ha $\beta = 1$, akkor $f_v - 1$ egy lineáris függvény. A magja vagy m dimenziós ($f_v \equiv 1$) vagy $m - 1$. Tehát f_v vagy 2^m vagy 2^{m-1} helyen lesz 1.
- Mariner 9 Mars-szonda (1971): $m = 5$: $n = 32$, $k = 6$, $d = 16$.
- ugyanilyen távolságú ismétlő kód ($n = 16$, $k = 1$, $d = 16$), a "sebessége" (k/n) 3-szor lassabb.

Két kézenfekvő mód lin. kódok megadására

- Bázissal **(Generátormátrix):** olyan G $n \times k$-as, hogy

$$G \text{ oszlopai } U \text{ egy bázisa}$$

  azaz

$$U = G\mathbb{F}^k$$

  Lehetséges kódolás: $v \mapsto Gv$.
- Lin. egyenletekkel **(Ellenőrző mátrix):** olyan H $n \times (n-k)$-as, hogy H^T sorai lin. egyenletek U meghatározására azaz $u \in U \Leftrightarrow H^T u = 0$, azaz

$$U = \ker H^T$$

- **Feladat:** Ismétlő és paritás-kódok mátrixai

Duális kód

- **A duális kód:** $U^\perp$ (a standard skalárszorzásra)
- **Tudjuk:** $\dim U^\perp = n - k = n - \dim U$, $U^{\perp\perp} = U$
- U bármely ellenőrző mátrixa $U^\perp$ egy generátormátrixa
  - **Biz.:** Ha H egy ell. mátrixa U-nak, akkor
  - $H^T u = 0$ minden $u \in U$-ra, így $(Hv)^T u = v^T H^T u = 0$ minden $u \in U$, $v \in \mathbb{F}^{n-k}$-ra. Tehát $H\mathbb{F}^{n-k} \leq U^\perp$, így
$$U \leq (H\mathbb{F}^{n-k})^\perp.$$
  - Ha $u \in (H\mathbb{F}^{n-1})^\perp$ azaz minden $v \in \mathbb{F}^{n-k}$-ra $0 = (Hv)^T u = v^T H^T u = v^T(H^T u)$, tehát $H^T u \in \mathbb{F}^{n-k^\perp} = (0)$, így $H^T u = 0$, azaz $u \in U$. Tehát
$$U \geq (H\mathbb{F}^{n-k})^\perp.$$
  - együtt: $U = (H\mathbb{F}^{n-k})^\perp$, és így $U^\perp = H\mathbb{F}^{n-k}$ is igaz.
- U bármely generátormátrixa $U^\perp$ egy ellenőrző mátrixa

Az Hadamard-kód fele és annak duálisa

- **Köv.:** Ismétlő és paritás-kódok egymás duálisai.
- **Hadamard-kód:** a legf. elsőfokú m-változós polinomok értékei $\mathbb{F}_2^m$-en
- **Hadamard-kód fele:** a homogén lineáris m-vált. polinomok azaz a lineáris függvények értékei $\mathbb{F}_2^m$-en
- kidobjuk a 0 helyet: ott minden lin. fvény értéke 0.
- paraméterek: $n = 2^m - 1$, $k = m$, $d = 2^{m-1}$.
- lin. fvények standard bázisa: $f_1, \dots, f_m$, ahol $f_i \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha_i$:

  f_1 mátrixa $(1, 0, \dots, 0)$,..., f_m mátrixa $(0, \dots, 0, 1)$.
- egy gen. mátrix: (sorai $\mathbb{F}_2^m$ nem nulla vektoraival indexelve): $G = (g_{vj})$, ahol $g_{vj} = f_j v$, ami v-nek j-edik komp.
- **Konklúzió:** G sorai: $\mathbb{F}_2^m$ nem 0 vektorai

Az Hadamard-kód fele és annak duálisa

- G gen. mátrix sorai: $\mathbb{F}_2^m$ nem 0 vektorai
- **Hamming-kód:** a duális kód, paraméterek: $n = 2^m - 1, k = 2^m - m - 1, d = ?$
- Hamming-kód (egyik) ellenőrző mátrixa G
- **Áll.:** A Hamming-kód távolsága 3:

Biz: Tfh. 2: létezik $v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ hogy $\alpha_\ell = 0$, ha $\ell \notin \{i, j\}$, de $\alpha_i = \alpha_j = 1$.

$v \in$ Hamming, azaz $G^T v = 0$. De $G^T v$ a G i-edik és j-edik sorának az összege. Ez nem lehet 0, mert G sorai kül. nem 0 vektorok. Ellentmondás.

A Hamming-kód távolsága

- **Áll.:** A Hamming-kód távolsága 3:

  Biz (folyt): Tfh. 1: ekkor olyan $v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ kódszó van, amelyre $\alpha_\ell = 0$, hacsak nem $\ell = i$ és $G^T v$ a G i-edik sora, ezek közt nem szerepel a 0. Ellentmondás.

  ≤ 3: G-nek van 3 sora, amelyek összege 0.

- **Tanulság:** Ha egy U lin. kód (egyik) ellenőrző mátrixa H, akkor U kódtávolsága $\leq \ell \Leftrightarrow H$-nak van ℓ lin. összefüggő sora

  kódtáv. $=$ ell. mátrix min. lin. összefüggő sorainak a száma

- **Megj.:** A kódtávolság kiszámítása NP-nehéz.

A Hamming-korlát

- **Tétel:** Legyen C egy nem feltétlenül lineáris kód a q elemű A ábécé felett. Tfh. C szavainak távolsága $\geq 2t+1$. Ekkor

$$|C|\sum_{s=0}^{t}\binom{n}{s}(q-1)^s \leq q^n.$$

Biz.: A^m minden v szavához legyen

$$B(v,t)=\{w\in A^n | d(v,w)\leq t\}.$$

ún. Hamming-gömb, "térfogat": $|B(v,t)|=\sum_{s=0}^{t}\binom{n}{s}(q-1)^s$
Ha $u,v\in C$, akkor $d(u,v)>2t$ miatt $B(u,t)\cap B(v,t)=\emptyset$, így

$$\sum_{v\in C} B(v,t)\leq q^n.$$

- **Perfekt kódok:** ahol a Hamming-korlát egyenlőséggel telj.
- a Hamming-kódok perfektek.

Perfekt kódokról:

- **Hamming-kódok tetsz. $\mathbb{F}_q$ felett:** paraméterek: $n = \frac{q^m-1}{q-1}, k = \frac{q^m-1}{q-1} - m, d = 3$.
- Az összes nem-triviális perfekt lineáris kód vagy páratlan hosszú ismétlő kód, vagy Hamming-kód, vagy Golay-kód.
- A perfekt Golay-kódok paraméterai: $\mathbb{F}_2$ felett: $n = 23, k = 12, d = 7$; $\mathbb{F}_3$ felett: $n = 11, k = 6, d = 5$.
- vannak **kiegészített** Hamming-kódok és kiegészített Golay-kódok
  Paritás-kódhoz hasonló konstrukció: kiegészítjük a kódszavakat egy új jeggyel, hogy a jegyek összege 0 legyen. Hamming és Golay kódokra a hossz és a kódtáv 1-gyel nő.
- **példa:** A teljes Hadamard-kód duálisa a kiegészített bináris Hamming-kód. Paraméterek: $n = 2^m, k = 2^m - m - 1, d = 4$.

Gram-mátrix

Legyen $v_1, \ldots, v_n$ bázis V-ben. Ebben a bázisban

- $\langle , \rangle$ Gram-mátrixa $A = (a_{ij})$, ahol $a_{ij} = \langle v_i, v_j \rangle$.
- A szimmetrikus: $A^T = A$
- $u = \sum_{i=1}^n \alpha_i v_i$ $v = \sum_{i=1}^n \beta_i v_i$-re

$$\langle u, v \rangle = \sum_{i,j=1}^n \alpha_i \beta_j a_{ij}$$

- rögz. bázisra: szimm. bilin. fvények$\leftrightarrow$szimm. mátrixok
- Ortogonális bázisban a Gram-mátrix diagonális, ortonormáltban az egységmátrix.

Gram-mátrixok $\mathbb{F}^n$ standard bázisában

- Ha A szimm. $n \times n$-es mátrix, akkor $\langle u, v\rangle := u^T A v$ szimm. bilin. fvény $\mathbb{F}^n$-en,
- ennek a Gram-mátrixa A.
- a $(,)$ standard skalárszorzat Gram-mátrixa I
- **Tul.:** $u^T A v = (u, Av) = (A^T u, v)$

Báziscsere hatása a Gram-mátrixra:

Legyen $v_1, \ldots, v_n$ és $v_1', \ldots, v_n'$ két bázis, a $v_i \to v_i'$ báziscsere mátrixa $C = (c_{ij})$: $v_j' = \sum_{i=1}^n c_{ij} v_i$.

Áll.: Ha $\langle , \rangle$ Gram-mátrixa az első bázisban A, akkor a másodikban

$$C^T AC.$$

Biz.: Jel.: $A = (a_{ij})$. A másik bázisban a Gram-mátrix $A' = (a_{ij}')$.

$$\begin{aligned} a_{ij}' &= \langle v_i', v_j' \rangle = \langle \sum_{k=1}^n c_{ki} v_k, \sum_{\ell=1}^n c_{\ell j} v_\ell \rangle \\ &= \sum_{k=1}^n c_{ki} \sum_{\ell=1}^n c_{\ell j} a_{k\ell} = \sum_{k=1}^n c_{ki} \sum_{\ell=1}^n a_{k\ell} c_{\ell j} \end{aligned}$$

Belső összegek vektora AC j-edik oszlopa. Ez van skalárszorozva C i-edik oszlopával, azaz C^T i-edik sorával.

Euklideszi terek

$\mathbb{R}^n$ standard skalárszorzatáról

Definitség

V vektortér $\mathbb{R}$ felett, $\langle , \rangle$ szimm. bilin. fvény V-n

- 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
- indefinit, ha $\exists\, u, v \in V$, amelyekre $\langle u, u \rangle > 0$, $\langle v, v \rangle < 0$
- Példa: $\mathbb{R}^2$-en $\left\langle \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \right\rangle := \alpha_1\beta_1 - \alpha_2\beta_2$ és $\left\langle \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \right\rangle := \alpha_1\beta_2 + \alpha_2\beta_1$ indefinitek. **Feladat:** mik a Gram-mátrixok a standard bázisban?

Néhány feladat

$V = \mathbb{R}^n$, tfh. $\langle u, v \rangle = u^T A v$, azaz a Gram-mátrix a standard bázisban A.

- Mutassuk meg, hogy $\ker A = V^\perp$.
- **Köv:** A szing. $\Leftrightarrow V^\perp \neq (0)$
- **Megj.:** szokásos elnevezés: $\langle , \rangle$ nemelfajuló, ha $V^\perp = (0)$.
- Tfh. $\langle , \rangle$ poz. szemidef. Mutassuk meg, hogy ekkor: A szinguláris $\Leftrightarrow \exists\, 0 \neq v \in \mathbb{R}^n$, hogy $v \in v^\perp$.
- Mut. meg, hogy indefinit $\langle , \rangle$ esetén a fenti ekvivalenciából csak $\Rightarrow$ igaz.

Euklideszi tér

- Valós vektortér pozitív definit $\langle , \rangle$ bilineáris függvénnyel
- **Példa:** $\mathbb{R}^n$, a standard skalárszorzattal
- **Fontos tul.:** Euklideszi tér altere is euklideszi tér
- $\langle f, g \rangle : \int f(x)g(x)dx$ is poz. def., a négyzetesen integrálható fvények tere ∞ dimenziós,
  véges sok fvény által generált altér euklideszi tér
- **hossz:** $|v| = \sqrt{\langle v, v \rangle}$
- **távolság:** $|u - v|$

A Gram–Schmidt-Ortogonalizáció

$\langle , \rangle$ poz. def. V-n

- $v_1, \ldots, v_n$ bázis V-ben
- $\langle v_1, v_1 \rangle \neq 0$, azaz $v_1 \notin v_1^{\perp}$.
- $\pi : w \mapsto w - \frac{\langle v_1, w \rangle}{\langle v_1, v_1 \rangle} v_1$ lin. transzf.
  (πw a w-nek a v_1-re merőleges komponense)
- $\ker \pi = \langle v_1 \rangle$, $\pi V = v_1^{\perp}$
- $v_2, \ldots, v_n \leftarrow \pi v_2, \ldots, \pi v_n$ bázis $v_1^{\perp}$-ben **(Miért?)**
- folytassuk $v_1^{\perp}$-ben
- $\vdots$
- eredmény: **ortogonális bázis**
- **normáló lépés:** $v_i \leftarrow \frac{1}{\sqrt{\langle v_i, v_i \rangle}} v_i$
- végeredmény: **ortonormált bázis**

Gram-Schmidt: megjegyzések

- A normáló lépés előttig a báziscsere mátrixa $\begin{pmatrix} 1 & * & * & \dots & * \\ & 1 & * & \dots & * \\ & & 1 & \dots & * \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix}$ alakú
- a normálást is tartalmazó báziscsere mátrixa is felső háromszög alakú, pozitív elemekkel a főátlóban.
- Az utolsó normáló lépés kivételével a más alaptestekre, nem poz. def. $\langle , \rangle$-re is alkalmazható, hacsak nem találunk $v \in v^\perp$ vektort.
- **Feladat:** tehetünk-e valamit, ha $v_1 \in v_1^\perp$?

Gram-Schmidt: megjegyzések

- Alkalmas egy adott szimmetrikus bilineáris függvény pozitív definitségének eldöntésére:
  Az eljárás nyilván végigmegy, ha annak során nem jön elő olyan v vektor, amelyre $\langle v, v\rangle \leq 0$.

  Ha nem jön ilyesmi elő: a végső $v_1, \dots, v_n$ bázis ortogonális és $(v_i, v_i) > 0$, ezért $\langle , \rangle$ poz. def.
- A Gram-mátrix alakulásának követésénél értelmes interpretáció: sorok és oszlopok szerinti Gauss-elimináció:
  Pl. a $v_2 \leftarrow v_2 - \frac{\langle v_1, v_2\rangle}{\langle v_1, v_1\rangle} v_1$ helyettesítésnél
  1. a második sorból elimináljuk az első elemet az első sor segítségével
  2. az így kapott mátrix második oszlopának első elemét elimináljuk az első oszlopának a segítségével

Gram-Schmidt példa

- Tfh. a v_1, v_2, v_3 bázisban $\langle , \rangle$ Gram-mátrixa

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

- A második sorból levonjuk az első sor kétszeresét:

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

- A második oszlopból levonjuk az első oszlop kétszeresét:

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

Gram-Schmidt példa

- A $v_2 \leftarrow \pi v_2$ után:
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix}.$$
- A harmadik sorból levonjuk az elsőt
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix},$$
- A harmadik oszlopból levonjuk az elsőt
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix}.$$
- Innentől a változtatások a jobb alsó blokkot érintik.

Gram-Schmidt példa

- A $v_1^\perp$-re való vetítések után:

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

- kivonjuk a második sort a harmadikból:

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

- kivonjuk a második oszlopot a harmadikból:

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

Keletkezett egy -1 a főátlóban, tehát $\langle , \rangle$ indefinit.

Gram-Schmidt megj.

- **Megj:** A Gram-Schmidt 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 $j \times j$-es blokkjának a determinánsa pozitív.

Izometria

- $V_1, \langle , \rangle$ és $V_2, \langle , \rangle_2$ euklideszi terek. A $\phi : V_1 \to V_2$ lin. bijekció **izometria** V_1 és V_2 között, ha

$$\langle v, w \rangle = \langle \phi v, \phi w \rangle_2$$

minden $v, w \in V_1$-re.

- $V_1, \langle , \rangle$ és $V_2, \langle , \rangle_2$ izometrikusak, ha létezik köztük izometria.
- azaz léteznek olyan bázisok a két térben, amelyekben a Gram-mátrixok megegyeznek.
- **Köv.:** Bármely n-dimenziós eukl. tér izometrikus $\mathbb{R}^n$-nel.
  Gram-Schmidt: létezik ortonormált bázis
- **Megj.:** Az izometria jelentése: távolságtartó .... Eukl. terek közötti távolságot tartó és 0-t 0-ba vivő leképezések automatikusan lineárisak.

Komplex euklideszi terek

- AKA véges dimenziós Hilbert-terek, unitér terek, Hermite–féle terek, hermitikus terek.
- **Probléma** $n \geq 2$-re $\mathbb{C}^n$-ben az $u^T v$-vel:
  - $\exists\, 0 \neq v \in \mathbb{C}^n$, amelyre $v \in v^\perp$
  - **Feladat:** mutassunk ilyen v-t.
- $\mathbb{C}^n$-en $u^T v$ helyett jobb $u^* v$-t használni.

  Def.: u^* az alábbi $m = 1$-gyel:
- **adjungált mátrix**: A $n \times m$-es komplex mátrixra

  $$A^* := \overline{A^T},$$

  a transzponált mátrix elemenkénti komplex konjugáltja.
- Ha A valós, akkor $A^* = A^T$.

Hermitikus függvények

V komplex vektortér, $\langle , \rangle : V \times V \to \mathbb{C}$ hermitikus (vagy Hermite-féle), ha

- a második változójában lineáris, azaz
  - $\langle u, \lambda v + v' \rangle = \lambda \langle u, v \rangle + \langle u, v' \rangle$ $(\forall u, v, v' \in V, \lambda \in \mathbb{C})$,
- és konjugált-szimmetrikus:
  - $\langle u, v \rangle = \overline{\langle v, u \rangle}$ $(\forall u, v \in V)$
- **Megj.:** Egy hermitikus függvény az első változóban konjugált-lineáris (avagy antilin.):
  - $\langle \lambda u + u', v \rangle = \overline{\lambda} \langle u, v \rangle + \langle u', v \rangle$ $(\forall u, u', v \in V, \lambda \in \mathbb{C})$,

Analógiák a valós esettel:

- **standard skalárszorzat** $\mathbb{C}^n$-en: $(u, v) = u^* v$
- **Gram-mátrix:** ugyanúgy $a_{ij} = \langle v_i, v_j \rangle$
- Hermitikus fvény Gram-mátrixa **önadjungált** (avagy hermitikus):
$$A^* = A$$
- $(u, Av) = u^* Av = (A^* u)^* v = (A^* u, v)$
- $u, v \mapsto u^* Av$ hermitikus $\Leftrightarrow$ A önadjungált
- Báziscsere hatása a Gram-mátrixra
$$A \to C^* AC$$

Definitség

$\langle , \rangle : V \times V \to \mathbb{C}$ hermitikus fvény

- **Észrevétel:** $\langle u, u \rangle = \overline{\langle u, u \rangle}$, tehát $\langle u, u \rangle$ mindig valós.
- $\langle , \rangle$ pozitív definit, ha $\forall\, 0 \neq v \in V$ vektorra $\langle v, v \rangle > 0$
- pozitív szemidefinit, indefinit, stb. hasonlóan

Komplex euklideszi tér

- **Def.:** komplex vektortér poz. def. $\langle , \rangle$ hermitikus fvénnyel ellátva
- eukl. tér altere is eukl.
- n-dim. komplex eukl. tér izometrikus $\mathbb{C}^n$-nel

  Biz.: (Gram-Schmidt átmegy)
- **Ezután:** euklideszi terekben a $(,)$ jelölést használjuk.
- **hossz:** $\sqrt{(v, v)}$
- **Pythagorasz-tétel:** ha $u \perp v$, akkor $|u + v|^2 = |u|^2 + |v|^2$

Pótlap: A Cauchy-Schwarz egyenlőtlenség

- Cauchy (1821):

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

- Bunyakovszkij (1859), Schwartz (1888):

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

Alkalmazás: a Cauchy-Schwarz–egyenlőtlenség

Komplex (vagy valós) euklideszi térben (Weyl 1918?):

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

- **Biz.:** ekvivalens megfogalmazás: $|(u,v)|^2 \leq (u,u)(v,v)$
- Feltehető $u \neq 0$ (különben akkor mindkét oldal 0)
- v felboml. u-val $\|$ és u-ra $\perp$ összetevőkre:

  $v = \mu u + v'$, ahol $\mu = \frac{(u,v)}{(u,u)}$ és $v' = v - \mu u$.
- $(v,v) = |\mu|^2(u,u) + (v',v')$ és $|(u,v)|^2 = |\mu|^2(u,u)^2$.
- A bizonyítandó $\leq$-ség baloldala $|\mu|^2(u,u)^2$
- jobboldala $|\mu|^2(u,u)^2 + (u,u)(v',v')$.
- **Megj.** A bizonyítás során végül is az u és v vektorokat tartalmazó síkban (vagy egyenesen) dolgoztunk.

A Cauchy-Schwarz–egyenlőtlenség

- Komplex (vagy valós) euklideszi térben

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

- Kifejtett alak:

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

- Négyzetesen integrálható függvényekre

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

(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.)

Normális mátrixok

- diagonalizálható (diagonálishoz hasonló) komplex mátrixok fontos családja
- **Def.:** A $n \times n$-es komplex mátrix **normális**, ha

$$AA^* = A^*A$$

- valós A-ra: $A^TA = AA^T$
- **Példa:** $A = A^*$ önadjungált (valós esetben szimmetrikus)
- **Példa:** $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ és $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ normális (szimmetrikus), de $AB = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ nem normális. **Miért?**
  $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ normális (ferdén szimmetrikus: $C^T = -C$), de $A + C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ nem normális. **Miért?**

Normális mátrixok

- **Áll.:** Legyen $M = \begin{pmatrix} a & v \\ & \boxed{C} \end{pmatrix}$, ahol $a \in \mathbb{C}$, $v^T \in \mathbb{C}^{n-1}$, C pedig $n-1 \times n-1$-es. Ekkor M normális $\Leftrightarrow$ $v = 0$ és C normális.
  - **Biz.:**
  - $MM^* - M^*M$ bal felső eleme $a\bar{a} + vv^* - \bar{a}a = vv^*$.
  - tehát ha M normális akkor $vv^* = 0$, így $v = 0$.
  - Ha $v = 0$, akkor M blokk diagonális és $MM^* - M^*M$ is. Utóbbi diag. blokkjai 0, illetve $CC^* - C^*C$.
- **Köv:** Felső (vagy alsó) háromszögmátrix normális $\Leftrightarrow$ diagonális

Unitér mátrixok

U $n \times n$-es.

- **Def.:** Az U $n \times n$-es mátrix **unitér**, ha $U^*U = I$.
  Minden unitér mátrix normális.
- **Áll.:** U unitér $\Leftrightarrow$ U^* unitér. Ekkor $U^* = U^{-1}$.
- **Áll.:** U, U' unitér $\Rightarrow$ I, U^{-1} és UU' unitérek.
- **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
  - $U : \mathbb{C}^n \to \mathbb{C}^n$ izometria
  - U $\mathbb{C}^n$ valamely ortonormált bázisát ortonormált bázisba viszi
  - U $\mathbb{C}^n$ bármely ortonormált bázisát ortonormált bázisba viszi
- valós unitér $=$ ortogonális ($UU^T = I$)

Unitér/ortogonális mátrixok: példák

- tetszőleges permutációs mátrix
- $v \mapsto v - 2\frac{u^T v}{u^T u} u$ az $u^\perp$ hipersíkra való tükrözés
- **Hadamard-kód fele:**
  - A $\mathbb{Z}_2^m \to \mathbb{Z}_2$ lineáris függvények, mint 2^m hosszú $0-1$ vektorok.
  - Ezek közül bármely két különböző 2^{m-1} helyen egyezik, 2^{m-1} helyen különbözik

    (Egy nem 0 lin. fvény 2^{m-1} helyen 0, 2^{m-1} helyen 1)
  - $0 \to 1$, $1 \to -1$
  - 2^m darab 2^m hosszú páronként merőleges ± 1-vektor
  - $2^{m/2}$-vel normálva ortogonális mátrixot alkotnak.
- Hadamard-mátrixok $n \times n$-es ± 1-mátrixok, páronként merőleges oszlopokkal (sorokkal).
- **Feladat:** van $n \times n$-es Hadamard-mátrix $\Rightarrow$ $n = 2$ vagy $4|n$
- **Sejtés:** Ha $4|n$, akkor van $n \times n$-es Hadamard-mátrix.

A Schur-felbontás

Tétel: Tetszőleges A $n \times n$-es komplex mátrixhoz létezik olyan U $n \times n$-es unitér mátrix, amelyre U^*AU felső háromszög alakú.

- **Biz.:** Indukció n szerint. $n = 1$: triviális.
- $n > 1$: λ A-nak egy sajátértéke, v megf. 1 hosszú sajátvektor. Legyen U egy olyan $n \times n$-es unitér mátrix, aminek v az első oszlopa. (U további oszlopai $v^\perp$ egy ortonormált bázisa.) A U oszlopaiból álló bázisban az A-val való szorzás mátrixa $U^*AU = \begin{pmatrix} \lambda & * \\ & \boxed{A'} \end{pmatrix}$.
- az indukciós feltevés miatt létezik U' $n-1 \times n-1$-es unitér, hogy $U'^*A'U'$ felső háromszög.
- legyen $U'' = \begin{pmatrix} 1 & \\ & \boxed{U'} \end{pmatrix}$. Ekkor UU'' unitér és
- $(UU'')^*A(UU'') = U''^*U^*AUU''$ felső háromszög.

Schur-felbontás - megjegyzések

- általában nem egyértelmű, de
- a diagonális elemek az eredeti mátrix sajátértékei.
- a bal felső eleme az eredeti mátrix tetszőleges sajátértéke lehet.

Spektráltétel normális mátrixokra

- **Észrevétel:** U $n \times n$-es unitér, A $n \times n$-es. Ekkor A normális $\Leftrightarrow$ U^*AU normális
  Biz.:
  $\Rightarrow$: $(U^*AU)^*U^*AU = U^*A^*UU^*AU = U^*A^*AU = U^*AA^*U = U^*AUU^*A^*U = U^*AU(U^*AU)^*$
  $\Leftarrow$: Ha $A' = U^*AU$, akkor $A = (U^*)^*A(U^*)$, így alkalmazható a másik irányú.
- **Köv.:** A normális $\Leftrightarrow$ van U unitér, hogy U^*AU diagonális (azaz valamely Schur-felbontására U^*AU diagonális) ($\Leftrightarrow$ bármely Schur-felbontására U^*AU diagonális)
- **Átfogalmazva.:** A normális
  $\Leftrightarrow$ van A sajátvektoraiból álló ortonormált bázis
  (fenti U oszlopai)

Alkalmazás: DFT és inverze

- Az $(12\ldots n)$ permutáció mátrixa ortog. ,így normális
- n kül. sajátérték $\Rightarrow$ a megf. sajátvektorok merőlegesek.
- Az ω^{-j} sajátértékhez tartozó 1 hosszú sajátvektor
  $$w_j = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{j(n-1)} \end{pmatrix}$$
- Tehát $M = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix}$ unitér: $M^{-1} = M^*$
- Itt $M^* = \overline{M}$: M-ből $\omega \leftrightarrow \overline{\omega}$ cserével kapható
- Ezen csere erejéig az inverz DFT ugyanolyan, mint a DFT.

Mátrixok definitsége

- **Def.:** az A **önadjungált** mátrix pozitív szemidefinit (pozitív definit), ha $v^*Av \geq 0$ ($v^*Av \geq 0$) minden $v \in \mathbb{C}^n$ vektorra.
  Megj.: Ekvivalens a $\langle u, v \rangle := u^*Av$ hermitikus függvény megfelelő definitségével.
- **Példa:** A tetszőleges $m \times n$-esre A^*A poz. szemidef. A^*A pontosan akkor poz. def., ha A oszlopai lineárisan függetlenek.
  Biz.: $v^*A^*Av = (Av)^*(Av)$ miatt $v^*A^*Av \geq 0$ és $v^*A^*Av = 0$ pont akkor, ha $Av = 0$.

Pótlap: fontos típusú diagonális mátrixok

A komplex diagonális. Ekkor:

- A unitér $\Leftrightarrow$ A diag. elemei 1 abszolút értékűek
- A önadjungált $\Leftrightarrow$ A diag. elemei valósak
- A pozitív szemidefinit $\Leftrightarrow$ A diag. elemei nemnegatív valósak
- A pozitív definit $\Leftrightarrow$ A diag. elemei pozitív valósak
- A ferdén hermitikus $\Leftrightarrow$ A diag. elemei tiszta képzetesek
  (Az $a + bi$ komplex szám tiszta képzetes, ha $a = 0$.)

Fontos típusú normális mátrixok spektruma

- **Áll.:** Legyen U unitér. Ekkor A önadjungált $\Leftrightarrow$ U^*AU önadj. Hasonló ekvivalenciák unitér, pozitív definit, pozitív szemidefinit, ferdén hermitikus ($A^* = -A$) mátrixokra.
- **Jellemzés:** 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

Schur-felbontás valós sajátértékekre

- **Tétel.:** Tfh. A $n \times n$-es valós, és A sajátértékei valósak. Ekkor létezik olyan U $n \times n$-es valós ortogonális, amelyre $U^T AU$ felső háromszög.
  Biz.: A Schur-felbontás bizonyítása átmegy.
- **Köv.:** A valós szimmetrikusra létezik U valós ortog., hogy $U^T AU$ diagonális.

Pótlap: valós Schur-felbontás biz. I

Áll.: Ha A valós és A kar. polinomjának λ egy valós gyöke, akkor létezik A-nak valós sajátvektora λ sajátértékkel.

Biz.: $\det(\lambda I - A) = 0$ miatt $\lambda I - A$ mint $\mathbb{R}^n \to \mathbb{R}^n$ lin. transzf. szing., azaz a magja $\neq (0)$. Egy nemnulla elem a magból egy sajátvektor λ sajátértékkel.

Pótlap: valós Schur-felbontás biz. II.

Tétel.: Tfh. A $n \times n$-es valós, és A sajátértékei valósak. Ekkor létezik olyan U $n \times n$-es valós ortogonális, amelyre $U^T AU$ felső háromszög.

Biz.: Indukció n szerint. $n = 1$: triviális.
$n > 1$: λ A-nak egy sajátértéke, v megf. 1 hosszú sajátvektor. Legyen U egy olyan $n \times n$-es ortog., aminek v az első oszlopa. (U további oszlopai $v^\perp$ egy ortonormált bázisa.) A U oszlopaiból álló bázisban az A-val való szorzás mátrixa

$$U^T AU = \begin{pmatrix} \lambda & * \\ & \boxed{A'} \end{pmatrix}.$$

Az ind. felt. miatt $\exists$ U' $n-1 \times n-1$-es ortog., hogy $U'^T A' U'$ felső háromszög.

Legyen $$U'' = \begin{pmatrix} 1 & \\ & \boxed{U'} \end{pmatrix}.$$

Ekkor $(UU'')^T A(UU'') = U''^T U^T AUU''$ felső háromszög. (És persze UU'' ortog.).

Projekció (vetítés)

- **Def.:** $\pi : V \to V$ lin. transzf. projekció, ha $\pi^2 = \pi$.
- **Áll.:** π projekció $\Leftrightarrow$ π megszorítása πV-re az identitás.
  $\pi^2 x = \pi x \Leftrightarrow \pi(\pi x) = (\pi x)$
- projekciók sajátértékei $\in \{0, 1\}$.
- **Ortogonális projekciók (merőleges vetítések):** Euklideszi térben egy olyan projekció, aminek mátrixa normális egy ortonormált bázisban.
- Ortog. proj. mátrixa önadjungált (valósra szimmetrikus).
- Egy normális mátrix projekció $\Leftrightarrow$ (komplex) sajátértékei a $\{0, 1\}$ halmazból kerülnek ki.

Merőleges vetítés altérre

- Legyen P ortogonális projekció mátrixa. Legyen U unitér, hogy $U^*PU = \operatorname{diag}(1, \ldots, 1, 0, \ldots, 0)$. Ekkor U első néhány oszlopa P képterének egy ortonormált bázisa, a többi pedig P magjáé, ami éppen a képtér $\perp$-komplementuma.
- **Köv.:** Egy ortogonális projekciót egyért meghatároz a képtere.
- Elnevezés: az altérre való merőleges vetítés.
  - létezés/konstrukció $W \leq V$-re:
  - $w_1, \ldots, w_r$ ortonormált bázis W-ben
  - kiegészítjük $w_{r+1}, \ldots, w_n$-nel V ortonormált bázisává
  - $v = \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^r \alpha_i w_i + \sum_{i=r+1}^n \alpha_i w_i$
  - elő rész: vetület W-re, második rész: vetület $W^\perp$-re
- Példa: $v \mapsto v - \frac{u^*v}{u^*u}u$ merőleges vetítés az $u^\perp$ hipersíkra
  $v \mapsto \frac{u^*v}{u^*u}u$ merőleges vetítés az $\langle u \rangle$ egyenesre.

Merőleges vetítések további tul.

- **Áll.:** A vetület az altér legközelebbi vektora:
  Legyen $v \in V$, $w \in W$ v merőleges vetülete W-n
  $u \in W$-re
  a $W \leq V$-re való merőleges vetítés és $v \in V$, akkor
  tetsz. $u \in W$-re
  $$|v - u| \geq |v - w|,$$
  egyenlőség csakis $u = w$-re.
  - **Biz.:** $v = w + w'$, itt $w' \in W^{\perp}$.
  - Legyen $u \in W$. Ekkor
    $v - u = (v - w) + (w - u) = w' + (w - u)$.
  - $w' \perp (w - u) \in W$, így $|v - u|^2 = |w'|^2 + |w - u|^2 \geq |w'|^2$
  - $u \neq w$-re a különbség $|w - u| > 0$

Példák ortog. projekciókra

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

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

Példák ortog. projekciókra

- az első néhány standard bázisvektor által feszített altérre való merőleges vetítés: $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & & \\ & & & & \end{pmatrix} =$
$(1 \quad 0 \quad \dots \quad 0)^T (1 \quad 0 \quad \dots \quad 0) + (0 \quad 1 \quad \dots \quad 0)^T (0 \quad 1 \quad \dots \quad 0) + \dots$
- Általában, ha $W \leq \mathbb{R}^N$-nek $w_1, \dots, w_r$ egy ortonormált bázisa, akkor a W-re való merőleges vetítés mátrixa $w_1 w_1^T + \dots + w_r w_r^T$.
- 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.

Ortogonális projekciók főátlója

- **Négyzetes mátrix nyoma:** $\mathrm{tr}A$ az A mátrix főátlójában levő elemeinek összege. A karakterisztikus polinom $n-1$-ed fokú tagjának az együtthatója, $-$ előjellel.
- Ezért $\mathrm{tr}C^{-1}AC = \mathrm{tr}A$.
- **Ortogonális projekciók főátlója:** Legyen $A = (a_{ij})$ egy ortog. proj. mátrixa (a standard bázisban).
  - $\mathrm{tr}A = A$ rangja,
    Biz.: A diag. alakjában az 1-ek száma, azaz a képtér dim.
  - $a_{ii} \geq 0$
    Biz.: Legyen $v_1, \dots, v_n$ a standard bázis. $A^2 = A^*A = A$, így $a_{ii} = (v_i, Av_i) = (v_i, A^*Av_i) = (Av_i, Av_i) \geq 0$.
  - $a_{ii} \leq 1$:
    Biz.: $v_i - Av_i \in \ker A = (A\mathbb{C}^n)^\perp$, így $(Av_i, v_i - Av_i) = 0$, így

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

Pótlap: Tükrözések

- **Def.** τ lin. transzf. **involúció**, ha $\tau^2 = I$.
- **Áll.** π projekció $\Leftrightarrow$ $I - 2\pi$ involúció
  $(I - 2\pi)^2 = I - 4\pi + 4\pi^2 = I + 4(\pi^2 - \pi)$
- **Áll.** τ involúció $\Leftrightarrow$ $\frac{1}{2}(I - \tau)$ projekció
- **Def.:** tükrözés = (standard bázsiban) normális mátrixú involúció
- **Áll.** π ortogt. proj. $\Leftrightarrow$ $I - 2\pi$ tükrözés
- **Áll.** τ tükr. $\Leftrightarrow$ $\frac{1}{2}(I - \tau)$ ortog. proj.
- **Áll.:** T normális mátrix egy tükr. $\Leftrightarrow$ T sajátértékei ± 1
- **Köv.:** tükrözés egyszerre unitér és önadj. (valósra egyszerre ortog. és szimm.)
- **Példa:** $u^\perp$-re tükr: $v \mapsto v - 2\frac{u^*v}{u^*u}u$

Gyakorló feladaok:

Az alábbi mátrixok közül melyek normálisak, melyek pozitív definitek és miért?

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ B = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix},\ C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$D = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},\ E = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix},\ F = \begin{pmatrix} 1 & -1 \\ -1 & 3 \end{pmatrix},$$

$$G = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 1 \end{pmatrix},\ H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 1 \end{pmatrix},\ J = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 3 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

2×2-es valós normális mátrixok

- A 2×2-es valós
- másodfokú valós kar. pol
- a sajátértékek: vagy egy/két valós, vagy egy konjugált pár
- egy/két valós sajátérték: Ekkor A normális $\Leftrightarrow$ A szimmetrikus.
- konjugált pár: $a + bi, a - bi$. Ekkor A normális $\Leftrightarrow$ $A - aI$ normális $\Leftrightarrow$ $A - aI$ ferdén szimmetrikus:

$$A = \begin{pmatrix} a & c \\ -c & a \end{pmatrix}$$

alakú.