Lineární algebra II

látka z

II. semestru informatiky MFF UK
dle přednášek Jiřího Fialy

Zpracovali:

Jan „Zaantar“ Štětina,
Ondřej „Keddie“ Profant

Obsah

Determinanty

Opakování:

Permutace na *n* prvcích je zobrazení $p:\{1,\dots,n\}\to\{1,\dots,n\}$, které je prosté a na.

S_n značí **množinu všech permitací** na *n* prvcích.

$(S_n,\circ)$ tvoří grupu (existují neutrální prvek, identita a všechny inverzní permutace).

Inverze v permutaci je dvojice *i,j* taková, že $i<j$ a $p(i)>p(j)$.

Znaménko permutace *p* je $sgn(p)=(-1)^{\#\text{ inverzí v }p}$.

Sudé permutace tvoří normální podgrupu S_n ; Faktorgrupa je izomorfní grupě $(\{1,-1\},\cdot)$.

Def: Nechť *A* je čtvercová matice řádu *n* nad tělesem *K*,
potom **determinant** matice *A* je dán výrazem

$$det(A):=\sum_{p\in S_n}(sgn(p)\cdot\prod_{i=1}^{n}a_{i,p(i)}) .$$

Formálně jde o zobrazení $K^{m\times n}\to K$.

Determinanty matic se značí $\begin{vmatrix}0 & 1\\ 1 & 0\end{vmatrix}$ místo $det(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix})$.

☼: $det(A^T)=det(A)$

Důkaz: $det(A^T)=\sum_{p\in S_n}(sgn(p)\cdot\prod_{i=1}^{n}(A^T)_{i,p(i)})=\sum_{p\in S_n}(sgn(p)\cdot\prod_{j=1}^{n}(A^T)_{\underbrace{p(i)}_{\cdot},i})=\sum_{p\in S_n}(sgn(p^{-1})\cdot\prod_{j=1}^{n}a_{j,p^{-1}(j)})=det(A)$

(*) víme, že $j=p(i);\ i=p^{-1}(j)$ a $sgn(p)=sgn(p^{-1})$. Q.E.D.

Důsl.: Pokud řádková úprava nemění determinant, pak ani stejná sloupcová úprava jej nezmění.

☼: Přerovnání sloupců matice *A* podle permutace *q*

(a) nezmění determinant, pokud $sgn(q)=1$

(b) změní znaménko determinantu, pokud $sgn(q)=-1$

Důkaz: Budiž *A* původní matice,
B přerovnaná matice.

$det(B)=\sum_{p\in S_n}(sgn(p)\cdot\prod_{i=1}^{n}b_{i,p(i)})=\sum_{p\in S_n}(sgn(p)\cdot\prod_{i=1}^{n}a_{i,q^{-1}(p(i))})$, protože $b_{i,q(j)}=a_{i,j};\ b_{i,j}=a_{i,q^{-1}(j)}$, a dále se rovná

$\sum_{p\in S_n}(sgn(q)\cdot sgn(q^{-1})\cdot sgn(p)\cdot\prod_{i=1}^{n}a_{i,q^{-1}(p(i))})$, kde vždy $sgn(q)\cdot sgn(q^{-1})=1$ a $sgn(q^{-1})\cdot sgn(p)=sgn(q^{-1}\circ p)$, takže

$sgn(q)\cdot\sum_{p\in S_n}(sgn(q^{-1}\circ p)\cdot\prod_{i=1}^{n}a_{i,q^{-1}(p(i))})=sgn(q)\cdot det(A)$. Q.E.D.

Důsl.: (a) záměna dvou řádků změní znaménko,
(b) jsou-li dva řádky matice *A* shodné, potom $det(A)=0$.

Tvrz.: Determinant matice je lineárně závislý na každém řádku matice.

Důkaz: Na *i*-tém řádku provedeme (a) skalární násobek řádku
(b) součet dvou řádků

(a) Linearita vůči násobku.

Budiž *A* původní matice,

A′ pozměněná matice (*i*-tý řádek vynásobený $t\in K$).

Pak $det(A')=\sum_{p\in S_n}(sgn(p)\cdot a'_{1,p(1)}\cdot\ldots\cdot a'_{i,p(i)}\cdot\ldots\cdot a'_{n,p(n)})=\sum_{p\in S_n}(sgn(p)\cdot a_{1,p(1)}\cdot\ldots\cdot(t\cdot a_{i,p(i)})\cdot\ldots\cdot a_{n,p(n)})=t\cdot det(A)$.

(b) Linearita vůči sčítání.

Budiž *A* původní matice.

Zkonstruujeme *B,C* předpisem $\forall j\,\forall k\neq i: a_{k,j}=b_{k,j}=c_{k,j}$,

$\forall j: a_{i,j}=b_{i,j}+c_{i,j}$.

Pak $det(A)=\sum_{p\in S_n}(sgn(p)\cdot a_{1,p(1)}\cdot\ldots\cdot a_{i,p(i)}\cdot\ldots\cdot a_{n,p(n)})=\sum_{p\in S_n}(sgn(p)\cdot a_{1,p(1)}\cdot\ldots\cdot(b_{i,p(i)}+c_{i,p(i)})\cdot\ldots\cdot a_{n,p(n)})=$

$=\sum_{p\in S_n}(sgn(p)\cdot a_{1,p(1)}\cdot\ldots\cdot b_{i,p(i)}\cdot\ldots\cdot a_{n,p(n)})+\sum_{p\in S_n}(sgn(p)\cdot a_{1,p(1)}\cdot\ldots\cdot c_{i,p(i)}\cdot\ldots\cdot a_{n,p(n)})=det(B)+det(C)$. Q.E.D.

Důsl.: Přičtení *t*-násobku *j*-tého řádku k *i*-tému (pro $i\neq j$) nemění determinant matice.

Důkaz: obrázkem

Postup: Výpočet determinantu
Převedením na odstupňovaný tvar přičtením násobků ostatních řádků,
ale nesmíme prohazovat řádky ani násobit $t\in K$,
zato můžeme provádět úpravy i na sloupcích.

(přednáška 2.3.09)

Lin. algebra – determinanty, polynomy, vlast. čísla a vektory, charakteristický mnohočlen, skalární součin, pos.def. matice, bilineární a kvadratické formy

Věta: Nechť A a B jsou čtvercové matice stejného řádu nad K, potom platí $det(A\cdot B)=det(A)\cdot det(B)$.

Důkaz:

Je-li A nebo B singulární, pak $A\cdot B$ je singulární.

Některý řádek singulární matice lze složit lineární kombinací ostatních, odečtením této kombinace získáme matici s nulovým řádkem a stejným determinantem $=0$.

Je-li A regulární, lze ji rozložit na součin elementárních matic $A=E_1\cdot\ldots\cdot E_k$.

Potom platí $det(A\cdot B)=det((E_1\cdot\ldots\cdot E_k)\cdot B)=det(E_1\cdot(E_2\cdot\ldots\cdot E_k\cdot B))\overset{*}{=}$

$\overset{*}{=} det(E_1)\cdot det(E_2\cdot\ldots\cdot E_k\cdot B)$.

Ad. *, máme dvě možnosti.

(a) E_1 odpovídá vynásobení i-tého řádku $t\neq 0$

$\Rightarrow$ determinant součinu t-krát vzroste: $det(E_1)=\begin{vmatrix}1&&&&0\\&\ddots&&&\\&&t&&\\&&&\ddots&\\0&&&&1\end{vmatrix}=t$

(b) E_1 odpovídá přičtení j-tého řádku k i-tému.

$\Rightarrow$ determinant součinu se nezmění: $det(E_1)=\begin{vmatrix}1&&&&0\\&\ddots&&&\\&&1&&\\&&&\ddots&\\0&&&&1\end{vmatrix}=1$

Tedy $det(E_1)\cdot\ldots\cdot det(E_k)\cdot det(B)=det(E_1\cdot\ldots\cdot E_k)\cdot det(B)=det(A)\cdot det(B)$.

Q.E.D.

Důsl.: (a) Čtvercová matice A je regulární, právě když $det(A)\neq 0$.

(b) $det(A^{-1})=(det(a))^{-1}$, respektive $det(A)\cdot det(A^{-1})=1$.

Značení: $A^{i,j}$ značí matici, která vznikne z matice A vypuštěním i-tého řádku a j-tého sloupce.

Tvrz.: **Rozvoj determinantu** podle i-tého řádku.

Pro libovolnou matici A řádu $n\geq 2$ a libovolné $i\in\{1,\ldots,n\}$

platí $det(A)=\sum_{j=1}^{n} a_{i,j}\cdot(-1)^{i+j}\cdot det(A^{i,j})$.

Pozn., toto je efektivní pro řádky s $n-1$ nulami.

Důkaz:

(a) Vytýkání prvků $a_{i,j}$ z předpisu pro determinant – nebudeme dokazovat

(b) Využití linearity: zapíšeme i-tý řádek jako vhodnou lineární kombinaci:

$$(a_{i,1},\ldots,a_{i,n})=\overbrace{a_{i,1}\cdot(1,0,\ldots,0)}^{e_1^T}+a_{i,2}\cdot(0,1,\ldots,0)+\ldots+a_{i,n}\cdot(0,0,\ldots,1)$$

$$det\begin{pmatrix}a_{i,1}&\ldots&a_{i,n}\\&&\end{pmatrix}=a_{i,1}\cdot det\begin{pmatrix}1&\ldots&0\\&&\end{pmatrix}+\ldots+a_{i,n}\cdot det\begin{pmatrix}0&\ldots&1\\&&\end{pmatrix}$$

Zbývá určit:

$$det\Big(\underbrace{\begin{pmatrix}0&\ldots&1&\ldots&0\\&&&&\end{pmatrix}}_{1\text{ je na }[i,j]}\Big)=\underbrace{(-1)^{i+1}}_{\text{permutace řádků}}\cdot det\Big(\underbrace{\begin{pmatrix}0&\ldots&1&\ldots&0\\&&&&\end{pmatrix}}_{1\text{ je na }[1,j]}\Big)=\underbrace{(-1)^{i+1}\cdot(-1)^{j+1}}_{\text{permutace sloupců}}\cdot det\Big(\underbrace{\begin{pmatrix}1&0&\ldots&\ldots&0\\x&&&&\\x&&&&\end{pmatrix}}_{x\text{ - nikdy nevyužijeme}}\Big)=(-1)^{i+j}\cdot det(A^{i+j})$$

, Q.E.D.

Def.: Pro čtvercovo matici A definujeme **adjungovanou matici** $adj(A)$

předpisem $(adj(A))_{i,j}=(-1)^{i+j}\cdot det(\overbrace{A^{j,i}}^{\text{změna pořadí indexů!}})$.

Věta: Pro každou regulární matici A platí $A^{-1}=\frac{1}{det(A)}\cdot adj(A)$.

Důkaz: z rozvoje podle i-tého řádku:

$\underbrace{A_i\cdot adj(A)_i}_{\text{i-tý řádek}}=det(A)$ a pro $j\neq i$:

$A_j\cdot adj(A)_i=$ rozvoj podle i-tého řádku v matici, která vznikne z A nahrazením i-tého řádku j-tým řádkem $=0$

$$\underbrace{\begin{pmatrix}\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\end{pmatrix}}_{A}\cdot\underbrace{\begin{pmatrix}\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\\\cdot&\cdot&\cdot&\cdot&\cdot\end{pmatrix}}_{adj(A)}=\begin{pmatrix}det(A)&&&&0\\&\ddots&&&\\&&\ddots&&\\&&&\ddots&\\0&&&&det(A)\end{pmatrix}\Rightarrow A\cdot\underbrace{(\frac{1}{det}(A)\cdot adj(A))}_{A^{-1}}=I_n$$

, Q.E.D.

Věta: **Cramerovo pravidlo**

Nechť A je regulární matice, potom

řešení každé soustavy $A\cdot x=b$ lze spočítat po složkách výrazem $x_i=\frac{det(A_{i\to b})}{det(A)}$,

kde $A_{i\to b}$ znamená matici, která vznikne z A nahrazením i-tého sloupce vektorem pravých stran b

Důkaz (1):

$X=A^{-1}\cdot b=\frac{1}{det(A)}\cdot(adj(A)\cdot b)$

$X_i=\frac{1}{det(A)}\cdot(adj(A)\cdot b)_i=\frac{1}{det(A)}\cdot\sum_{j=1}^{n}(adj(A))_{i,j}\cdot b_j=$

Provedeme rozvoj podle i-tého sloupce v $A_{i\to b}$

$=\frac{1}{det(A)}\cdot det(A_{i\to b})$, Q.E.D.

Důkaz (2):

Označme $I_{i\to x}$ matici, která vznikne z I_n nahrazením i-tého sloupce vektorem x.

$A\cdot I_{i\to x}=(A\cdot e_1,A\cdot e_2,\ldots,\underbrace{A\cdot x}_{=b},\ldots)=A_{i\to b}$

Víme $det(I_{i\to x})=x_i$ a tedy $det(A)\cdot x_i=det(A_{i\to b})$, Q.E.D

Lin. algebra – determinanty, polynomy, vlast. čísla a vektory, charakteristický mnohočlen, skalární součin, pos.def. matice, bilineární a kvadratické formy

Postup: Výpočet determinantu (ze cvičení)

I) V **odstupňovaném tvaru** stačí součin diagonály: $\begin{vmatrix} a_1 & & \ddots \\ & \ddots & \\ 0 & & a_n \end{vmatrix} = \prod_{i=1}^{n} a_i$

II) **Vytýkání** z řádku: $\begin{vmatrix} 1 & 3 & 5 \\ 2 & 0 & 4 \\ 6 & 7 & 3 \end{vmatrix} \simeq \begin{vmatrix} 1 & 3 & 5 \\ 0 & -6 & -6 \\ 0 & -11 & -27 \end{vmatrix} \simeq (-6)\cdot \begin{vmatrix} 1 & 3 & 5 \\ 0 & 1 & 1 \\ 0 & -11 & -27 \end{vmatrix} = (-6)\cdot(-16) = 96$

III) $n=2 \Rightarrow \begin{vmatrix} a & b \\ c & d \end{vmatrix} = a\cdot d - b\cdot c$

IV) $n=3 \Rightarrow$ Sarrusovo pravidlo: $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \Rightarrow \begin{matrix} \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \\ \begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{matrix} \end{matrix} = 1\cdot5\cdot9 + 4\cdot8\cdot3 + 7\cdot2\cdot6 - 7\cdot5\cdot3 - 1\cdot8\cdot6 - 4\cdot2\cdot6 = 225 - 225 = 0$

V) **Rozvoj** dle *i*-tého řádku $det(A) = \sum_{j=1}^{n} a_{i,j}\cdot(-1)^{i+j}\cdot det(A^{i,j})$; př: $\begin{vmatrix} 1 & 2 & 5 \\ 2 & 0 & 4 \\ 6 & 7 & 3 \end{vmatrix} \simeq \begin{vmatrix} 1 & 3 & 3 \\ 2 & 0 & 0 \\ 6 & 7 & 9 \end{vmatrix} = (-1)^{1+2}\cdot 2\cdot \begin{vmatrix} 3 & 3 \\ 7 & 9 \end{vmatrix} = (-6)\cdot \begin{vmatrix} 1 & 1 \\ 7 & 9 \end{vmatrix} = (-6)\cdot 2 = 12$

Geometrický význam determinantu

Pozn., Známe různé druhy obalů $X \in \mathbb{R}^n$, $X = \{x_1, \dots, x_k\}$

(1) $\mathcal{L}(X)$ Lineární obal — nejmenší vektorový prostor obsahující *X*.

$$\mathcal{L}(X) = \{\sum_{i=1}^{k} a_i\cdot x_i \,;\, x_i \in X,\, a_i \in \mathbb{R}\}$$

(2) $\mathcal{A}(X)$ Afinní obal — nejmenší afinní prostor obsahující *X*.

$$\mathcal{A}(X) = \{\sum_{i=1}^{k} a_i\cdot x_i ; x_i \in X,\, a_i \mathbb{R},\, \sum_{i=1}^{k} a_i = 1\}$$

(3) $\mathcal{K}(X)$ Konvexní obal — nejmenší konvexní množina obsahující *X*.

$$\mathcal{K}(X) = \{\sum_{i=1}^{k} a_i\cdot x_i ;\, x_i \in X,\, a_i \in \mathbb{R},\, \sum_{i=1}^{k} a_i = 1, \forall i : a_i \in [0,1]\}$$

(4) $\mathcal{R}(X)$ **Rovnoběžnostěn** vymezený *X*.

$$\mathcal{R}(X) = \{\sum_{i=1}^{k} a_i\cdot x_i ;\, x_i \in X,\, a_i \in \mathbb{R}, \forall i : a_i \in [0,1]\}$$

Věta: Pro vektory $x_1, \dots, x_n$ udává $|det(A)|$, kde *A* sestává z $x_1, \dots, x_n$ (po řádcích anebo po sloupcích), objem rovnoběžnostěnu určeného $x_1, \dots, x_n$.
Důkaz (idea): Protože přičítání jiných řádků nemění ani determinant, ale ani objem.

Důsl.: Je-li *f* lineární zobrazení $\mathbb{R}^n \to \mathbb{R}^n$ a
$A = [f]_{KK}$ je matice tohoto zobrazení,
tak platí, že objem $\underbrace{vol(f(v))}_{\text{objem obrazu}} = |det(A)|\cdot \underbrace{vol(v)}_{\text{těleso}}$.

Polynomy

Def.: **Polynom** (též mnohočlen) stupně *n* v proměnné *x* nad tělesem *K* je výraz
$p(x) = a_n\cdot x^n + a_{n-1}\cdot x^{n-1} + \dots + a_1\cdot x + a_0$, kde $a_n \dots a_0 \in K$, $a_n \neq 0$.
Značení $p \in K(x)$.

Operace s polynomy

$p, q \in K(x) : p(x) = \sum_{i=0}^{n} a_i\cdot x^i$ a $q(x) = \sum_{i=0}^{m} b_i\cdot x^i$, *BÚNO* $n \geq m$.

Sčítání a odčítání

$$(p \pm q)(x) = \sum_{i=0}^{n} c_i\cdot x^i, \text{ kde } c_i = \begin{matrix} a_i \pm b_i \text{ pro } i \in \{0, \dots, m\} \\ a_i \text{ jinak} \end{matrix}$$

Násobení skalárem

$t \in K$, pak $t\cdot p(x) = \sum_{i=0}^{n} (t\cdot a_i)\cdot x^i$

Násobení mezi sebou

$$(p\cdot q)(x) = \sum_{i=0}^{m+n} c_i\cdot x^i, \text{ kde } c_i = \sum_{j=max(0,i-m)}^{min(i,n)} a_j\cdot b_{i-j}$$

Dělení se zbytkem

$$\exists r,t\in K(X):(\underbrace{deg(t)}_{\text{stupeň t}}<deg(q))\wedge(p=r\cdot q+t)$$

Konstrukce řešení: $p(x)-\underbrace{\frac{a_1}{b_1}\cdot x^{n-m}\cdot q(x)}_{\text{první člen } r}$ má stupeň nižší než $p(x)$.

Pozn., Typicky za x volíme prvky z tělesa K, ale lze i jiné struktury, např. čtvercové matice nad K.

$$p(x)=a_n\cdot x^n+\ldots+a_1\cdot x+a_0\cdot x^0$$
$$p(A)=a_n\cdot A^n+\ldots+a_1\cdot A+a_0\cdot I_n$$

☼: Pro $p\in\mathbb{R}(x)$ platí, že $p(x)=0$ (tj. $p(x)=0(x)=0$), právě když $a_0=\ldots=a_n=0$.

Věta: Malá Fermatova

Pro každé $a\in\mathbb{Z}_p, a\neq 0$ platí $a^{p-1}=1$.

Důkaz: Zafixuji a, uvážím zobrazení $f:i\to a\cdot i$.

Tedy $f:\{1,\ldots,p-1\}\to\{1,\ldots,p-1\}$ je prosté a f je permutací na $\{1,\ldots,p-1\}$.

$\prod_{i=1}^{p-1} i=\prod_{i=1}^{p-1} a\cdot i=a^{p-1}\cdot\prod_{i=1}^{p-1} i\Rightarrow 1=a^{p-1}$, Q.E.D.

Důsl.: V $\mathbb{Z}_p: x^p-x=0$.

$\forall q\in\mathbb{Z}_p(x)\ \exists r\in Z_p(x)\ ,\ deg(r)\le p-1:\ \forall x\in\mathbb{Z}_p:\ q(x)=r(x)$

Def.: **Kořen polynomu** $p\in K(x)$ je takové $a\in K$, že $p(a)=0$.

Např. polynom $p(x)=x^2+1$

(1) má kořen i v $K=\mathbb{C}$
(2) nemá kořen v $K=\mathbb{R}$
(3) nemá kořen v $K=\mathbb{Z}_3$
(4) má kořen 2 v $K=\mathbb{Z}_5$.

Def.: Tělesa, kde všechny polynomy mají kořen, se nazývají **algebraicky uzavřená**.

Věta: Základní věta algebry

Každý mnohočlen stupně alespoň 1 nad $\mathbb{C}$ má kořen.

Důsl.: Každý mnohočlen stupně alespoň 1 nad $\mathbb{C}$ lze rozložit jakou součin n monomů

$p(x)=a_n\cdot(x-x_1)\cdot\ldots\cdot(x-x_n)$, kde $x_1,\ldots,x_n$ jsou kořeny.

Důkaz (idea): Základní věta algebry:

$p(x)=a_n\cdot x^n+\ldots+a_1\cdot x+a_0$ ……

(přednáška 16.3.09)

Otázka: Reprezentace polynomů $p(x)$ stupně n.

- pomocí koeficientů $a_0\ldots a_n\in K$ (+ def.);
- na algebraicky uzavřeném tělese pomocí n kořenů a a_0;
- hodnotami $p(x)$ v $n+1$ různých bodech.

$$p(x)=\sum_{i=0}^{n} a_i\cdot x^i \overbrace{\underbrace{\rightarrow}_{\text{snadné}}}^{\text{snadné}} x_1,\ldots,x_{n+1}$$

- jakým způsobem lze užít koeficienty $a_0\ldots a_n$ polynomu $p(x)$,

  známe-li dvojice $\underbrace{(x_i;y_i)}_{=p(x_i)}$ pro $n+1$ různých bodů $x_1\ldots x_{n+1}$?

- řešíme soustavu o neznámých $a_0\ldots a_n$

$$\begin{aligned} a_n x_1^n+\ldots+a_1 x_1+a_0&=y_1\\ &\vdots\\ a_n x_{n+1}^n+\ldots+a_1 x_{n+1}+a_0&=y_{n+1}\end{aligned}$$

Maticově:

$$\underbrace{\begin{pmatrix}1 & x_1 & \cdots & x_1^n\\ \vdots & \vdots & \ddots & \vdots\\ 1 & x_{n+1} & \cdots & x_{n+1}^n\end{pmatrix}}_{\text{Vandermondova matice}}\cdot\begin{pmatrix}a_0\\ \vdots\\ a_n\end{pmatrix}=\begin{pmatrix}y_1\\ \vdots\\ y_{n+1}\end{pmatrix}$$

Lin. algebra – determinanty, polynomy, vlast. čísla a vektory, charakteristický mnohočlen, skalární součin, pos.def. matice, bilineární a kvadratické formy

Věta: Vandermondova matice je regulární, právě když hodnoty $x_1 \dots x_{n+1}$ jsou navzájem různé.

Důkaz:

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{vmatrix} \overset{\text{První řádek odečteme od ostatních}}{=} \begin{vmatrix} 1 & x_1 & \cdots & x_1^n \\ 0 & x_2 - x_1 & \cdots & x_2^n - x_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & x_{n+1} - x_1 & \cdots & x_{n+1}^n - x_1^n \end{vmatrix}$$

Provedeme rozvoj dle prvního sloupce a vytkneme $x_k^i - x_1^i = (x_k - x_i)(x_k^{i-1} + x_k^{i-2} \cdot x_1 + \dots + x_1^{i-1})$

$$\prod_{j=2}^{n} (x_j - x_1) \cdot \begin{vmatrix} 1 & x_1 + x_1 & x_2^2 + x_2 \cdot x_1 + x_1^2 & \dots \\ \vdots & \vdots & \vdots & \ddots \\ 1 & x_{n+1} + x_1 & x_{n+1}^2 + x_{n+1} \cdot x_1 + x_1^2 & \dots \end{vmatrix} = \prod_{j=2}^{n} (x_j - x_1) \cdot \left| \begin{matrix} \text{Vandermantova matice na} \\ \text{proměnných } x_2 \dots x_{n+1} \end{matrix} \right| = \prod_{1 \le i < j \le n+1} (x_j - x_i)$$

produkt nenulový ($\Rightarrow$ matice regulární) $\Leftrightarrow \forall x_i$ různé. Q.E.D.

Postup: Lagrangerova interpolace - alternativní postup, jak proložit polynom stupně *n* body (x_i, y_i), $i \in \{1 \dots n\}$.

Pro $i \in \{1 \dots n+1\}$ označme $P_i(x) = \dfrac{(x - x_1)(x - x_2) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_{n+1})}{(x_i - x_1)(x_i - x_2) \cdot \dots \cdot (x_i - x_{i-1})(x_i - x_{i+1}) \cdot \dots \cdot (x_i - x_{n+1})}$

Platí $P_i(x_i) = 1$ a pro $j \neq i$: $P_i(x_j) = 0$ (někde máme $x - x_j = 0$ ... nenulový čitatel).

Položíme $P(x) = y_1 \cdot P_1(x) + \dots + y_{n+1} P_{n+1}(x)$.

Úloha: Jakým způsobem sestavit *m* klíčů, aby libovolný $n < m$ klíčů dokázalo odemknout kód, ale libovolných méně než *n* nikoliv?

Sestavme $\underbrace{\text{polynom stupně } n-1 \text{ a určíme}}_{\text{kód}}$ jeho $\underbrace{\text{hodnoty v } m}_{\text{klíč}}$ různých bodech.

Vlastní čísla a vlastní vektory

Úvod: Jednoduchý abstraktní model dynamického systému.

Systém … reprezentován vektorovým prostorem V nad K

Dynamika … reprezentována lineárním zobrazením $f : V \to V$

Stabilní stavy (a) pevné body zobrazení f čili $f(u) = u$

(b) body jejichž obraz je skalárním násobkem vzoru: $f(u) = a \cdot u$, $a \in K$

Př: Osová souměrnost v $\mathbb{R}^2$

Def: Nechť V je vektorový prostor nad K a $f : V \to V$ je lin. zobrazení.

Vlastním číslem zobrazení f je takové $\lambda \in K$ pro které existuje netriviální $u \in V$ takový, že $f(u) = \lambda \cdot u$.

Vlastním vektorem příslušný vlastnímu číslu λ je libovolné $u \in V$, tž. $f(u) = \lambda \cdot u$.

(Pozn: Zdvojená definice, abychom obešli $u = 0$.)

Je-li V konečně generovaný, tj. $dim(V) = n \in \mathbb{N}$,

potom lze f reprezentovat maticí zobrazení $A = [f]_{VV}$ a rozšířit definici na matice:

Vlastní číslo matice A je libovolné $\lambda \in K$ takové, že $A \cdot x = \lambda \cdot x$ pro $x \in K^n$, $x \neq 0$.

Vlastní vektor příslušný vlastnímu číslu λ je takové $x \in K^n$, že $Ax = \lambda \cdot x$

Množina všech vlastních čísel matice se nazývá **spektrum matice.**

Charakteristický mnohočlen

Úvod: $f(u) = \lambda \cdot u$, $u \neq 0$

$A \cdot x = \lambda \cdot x \;\Rightarrow\; A \cdot x - \lambda \cdot x = 0 \;\Rightarrow\; A \cdot x - \lambda \cdot I \cdot x = 0 \;\Rightarrow\; (A - \lambda \cdot I) \cdot x = 0$

Def: **Charakteristickým mnohočlenem** matice A nazveme polynom $p_a(t)$, který je určen výrazem: $p_a(t) = det(A - t \cdot I)$

Věta: Pro každou čtvercovou matici A platí, že λ je jejím vlastním číslem,
právě když je λ kořenem charakteristického mnohočlenu $p_A(t)$, čili $p_A(\lambda) = 0$

Důkaz: viz. úvod... $(A - \lambda I)_x = 0 \;\Leftrightarrow\; A - \lambda I$ je singulární $\Leftrightarrow\; det(A - t \cdot I) = 0$, x netriviální! Q.E.D.

Př: Viz slidy.

Tvrz.: Jsou-li A, B čtvercové matice stejného řádu nad stejným tělesem, potom $A \cdot B$ a $B \cdot A$ mají stejná vlastní čísla.

Důkaz: ☼ Pro násobení blokových matic platí: $\begin{pmatrix} I & J \\ K & L \end{pmatrix} \cdot \begin{pmatrix} P & Q \\ R & S \end{pmatrix} = \begin{pmatrix} IP + JR & IQ + JS \\ KP + LR & KQ + LS \end{pmatrix}$

$$\overbrace{\begin{pmatrix} AB & 0 \\ B & 0 \end{pmatrix}}^{C} \cdot \overbrace{\begin{pmatrix} I & A \\ 0 & I \end{pmatrix}}^{R} = \begin{pmatrix} AB & ABA \\ B & BA \end{pmatrix} = \overbrace{\begin{pmatrix} I & A \\ 0 & I \end{pmatrix}}^{R} \cdot \overbrace{\begin{pmatrix} 0 & 0 \\ B & BA \end{pmatrix}}^{D}$$

Def: Platí: $C \cdot R = R \cdot D$, říkáme, že C a D jsou **podobné**.

☼**:** Podobné matice mají shodné charakteristické mnohočleny.

$$C = R \cdot D \cdot R^{-1}$$

$$p_C(t) = det(C - t \cdot I) = det(R \cdot D \cdot R^{-1} - t \cdot I) = det(R \cdot D \cdot R^{-1} - t \cdot (R \cdot I \cdot R^{-1})) = det(R(D - t - I) \cdot R^{-1}) = \underbrace{det(R)}_{(*)} \cdot det(D - t \cdot I) \cdot \underbrace{det(R^{-1})}_{*\cdot toto=1} = P_d(t)$$

Podobné matice mají tedy shodná i vlastní čísla.

Čili $\begin{vmatrix} A \cdot B - t \cdot I & 0 \\ B & -t \cdot I \end{vmatrix} = |A \cdot B - t \cdot I| \cdot |-t \cdot I| = p_{AB}(t) = p_{BA}(t) = |-t \cdot I| \cdot |B \cdot A - t \cdot I| = \begin{vmatrix} -t \cdot I & 0 \\ B & B \cdot A - t \cdot I \end{vmatrix}$

Stejné charakteristické mnohočleny ⇒ stejná charakteristická čísla, Q.E.D.

Věta: Cayley-Hamilton

Nechť $p_A(t)$ je charakteristický mnohočlen matice A. Potom platí $p_A(A) = 0$.

Důkaz: Využijeme faktu, že $M \cdot adj(M) = det(M) \cdot I_n$, a dosadíme $M := A - t \cdot I \Rightarrow \begin{pmatrix} p_A(t) & 0 & 0 & 0 \\ 0 & p_A(t) & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots \\ 0 & 0 & 0 & p_A(t) \end{pmatrix}$.

$adj(A - t \cdot I)$ Má na každém místě polynom proměnné t.

Můžeme zapsat $adj(A - t \cdot I) = t^{n-1} \cdot B_{n-1} + ... + t \cdot B_1 + B_0$, tedy $(A - t \cdot I) \cdot (t^{n-1} \cdot B_{n-1} + ... + t \cdot B_1 + B_0) = p_A(t) \cdot I = a_n \cdot t^n \cdot I + ... + a_1 \cdot t \cdot I + a_0 \cdot I$.

Koeficient u t^n : $\quad -I \cdot B_{n-1} = a_n \cdot I \quad | \cdot A^n$

u t^i : $\quad A \cdot B_i - I \cdot B_{i-1} = a_i \cdot I \quad | \cdot A^i$

u t^0 : $\quad A \cdot B_0 = a_0 \cdot I \quad |$ nic

Provedeme úpravy (násobení jsou zleva) a sečteme. Pravá strana je $a_n \cdot a^n + ... + a_1 \cdot A + a_0 \cdot I = p_A(A)$

$-A^n \cdot B_{n-1} + A^{n-1} \cdot (A \cdot B_{n-1} - B_{n-2}) + A^{n-2} \cdot (A \cdot B_{n-2} - B_{n-3}) + ... + A^2 \cdot (A \cdot B_2 - B_1) + A \cdot (A \cdot B_1 - B_0) + A \cdot B_0 = 0$, Q.E.D.

☼: (1) Každá matice řádu n má nejvýše n vlastních čísel.

(2) Každá komplexní matice řádu n má „právě“ n vlastních čísel (některá mohou být vícenásobná):

$$p_A(t) = (\lambda_1 - t) \cdot ... \cdot (\lambda_n - t) \rightarrow p_A(t) = (\lambda_1 - t)^{r_1} \cdot ... \cdot (\lambda_k - t)^{r_k}; \sum_{i=1}^{k} r_i = n$$

(3) $a_0 = det(A)$ dosazením $t = 0$

$$p_A(t) = a_n \cdot t^n + ... + a_1 \cdot t + a_0 = det(A - t \cdot I) = \begin{vmatrix} a_{1,1} - t & & & \\ & a_{2,2} - t & & \\ & & \ddots & \\ & & & a_{n,n} - t \end{vmatrix}$$

(4) $a_n = (-1)^n$

(5) $a_0 = \lambda_1 \cdot ... \cdot \lambda_n$ dosazením $t = 0$ do $p_A(t) = (\lambda_1 - t) \cdot ... \cdot (\lambda_n - t)$

(6) $a_{n-1} = (-1)^{n-1} \cdot \sum_{i=1}^{n} a_{i,i} = (-1)^{n-1} \cdot \sum_{i=1}^{n} \lambda_i$

Úloha: (ze cvičení) Ve městě Pupákově jsou tři strany: Asketičtí, Bohatí a Chudí. Podrobným výzkumem se zjistilo, že 75% z těch, co volilo Askety, je bude volit opět, 5% bude volit Bohaté a 20% chudé. Podobně z těch co volili Bohaté zvolí 60% Bohaté, 20% Askety a 20% Chudé. 80% voličů chudých je bude volit i v následujícím období, o zbylé hlasy se podělí 10% Asketi a 20% Bohatí. Jak bude vypadat limitní rozložení sil v místním (stočlenném) zastupitelstvu?

$$A = \begin{matrix} \\ A \\ B \\ C \end{matrix} \begin{matrix} \begin{matrix} A & B & C \end{matrix} \\ \begin{pmatrix} 0{,}75 & 0{,}20 & 0{,}10 \\ 0{,}05 & 0{,}60 & 0{,}10 \\ 0{,}20 & 0{,}30 & 0{,}80 \end{pmatrix} \end{matrix} \Rightarrow \begin{matrix} Ax = \lambda x \\ 20\,Ax = 20\lambda x \end{matrix} \Rightarrow 20\,A = A' := \begin{pmatrix} 15 & 4 & 2 \\ 1 & 12 & 2 \\ 4 & 4 & 16 \end{pmatrix}$$

☼ Rozdělení dle popisků okolo matice, např. na diagonále jsou ti co volí stejně.

☼ Součet sloupců matice dá vždy 1 (100%)

$$\lambda: \begin{vmatrix} 15-t & 4 & 2 \\ 1 & 12-t & 2 \\ 4 & 4 & 16-t \end{vmatrix} = \begin{matrix} (15-t)(12-t)(16-t) + 8 + 32 - 8(12-t) - 8(15-t) - 4(16-t) = \\ = (20-t)(12-t)(11-t) \Rightarrow \end{matrix} \begin{matrix} \lambda_1 = 11 \\ \lambda_2 = \frac{1}{10} = \frac{3}{5} \\ \lambda_3 = \frac{11}{20} \end{matrix}$$

$$\vec{x}(p): \begin{pmatrix} -5 & 4 & 2 \\ 1 & -8 & 2 \\ 4 & 4 & -4 \end{pmatrix} \simeq \begin{pmatrix} 0 & 9 & -3 \\ 0 & -9 & 3 \\ 1 & 1 & -1 \end{pmatrix} \simeq \begin{pmatrix} 1 & 1 & -1 \\ 0 & -3 & 1 \\ 0 & 0 & 0 \end{pmatrix} \Rightarrow \begin{matrix} x_3 = p \\ -3 + p = 0 \Rightarrow x_2 = p/3 \\ x_1 = -2\mathrm{p} \end{matrix} \Rightarrow \vec{x} = p\left(\frac{2}{3}; \frac{1}{3}; 1\right)$$

$$\Rightarrow \frac{2\mathrm{p}}{3} + \frac{p}{3} + p = 1 \Rightarrow p = \frac{1}{2} \Rightarrow \vec{x_1} = \left(\frac{1}{3}; \frac{1}{6}; \frac{1}{2}\right)$$, kde každá složka je zastoupení přislušné strany.

☼ Pokud bychom dosadili jiné vlastní číslo příklad by nevyšel smysluplně.

Věta: Nechť $x_1, ..., x_k$ jsou vlastní vektory příslušné navzájem různým vlastním číslům $\lambda_1, ..., \lambda_k$ lineárního zobrazení f.

Potom $x_1, \dots, x_k$ jsou lineárně nezávislé.
Důkaz: indukcí a sporem.
Nechť $x_1 \dots x_n$ tvoří nejmenší protipříklad, tj. $\exists a_1, \dots, a_k \neq 0 : \sum_{i=1}^{k} a_i \cdot x_i = 0$

$0 = f(0) = f\left(\sum_{i=1}^{k} a_i \cdot x_i\right) = \sum_{i=1}^{k} a_i \cdot f(x_i) = \sum_{i=1}^{k} a_i \cdot \lambda_i \cdot x_i$ a $0 = \lambda_k \cdot 0 = \lambda_k \cdot \sum_{i=1}^{k} a_i \cdot x_i = \sum_{i=1}^{k} a_i \cdot \lambda_k \cdot x_i$

$0 = 0 - 0 = \sum_{i=1}^{k} a_i \cdot \lambda_i \cdot x_i - \sum_{i=1}^{k} a_i \cdot \lambda_k \cdot x_i = \sum_{i=1}^{k-1} \underbrace{(\lambda_i - \lambda_k)}_{\neq 0} \cdot \underbrace{a_i}_{\neq 0} \cdot x_i \Rightarrow x_1 \dots x_{k-1}$ jsou lineárně závislé, *SPOR* s minimalitou protipříkladu. Q.E.D.

Def: Čtvercové matice *A, B* nazveme **podobné**, pokud existuje regulární matice *R* taková, že platí: $A = R^{-1} \cdot B \cdot R$

Věta: Nechť matice *A, B* jsou si podobné a $\lambda, \vec{x}$ jsou vlastní číslo a příslušný vlastní vektor matice *A*,
potom $y = R \cdot \vec{x}$ je vlastní vektor matice *B* příslušný vlastnímu číslu λ.
Důkaz: $B \cdot y = (R \cdot A \cdot R^{-1}) \cdot (R \cdot \vec{x}) = R \cdot A \cdot \vec{x} = R \cdot \lambda \cdot \vec{x} = \lambda \cdot R \cdot \vec{x} = \lambda \cdot y$
$A = R^{-1} \cdot B \cdot R \Rightarrow B = R^{-1} \cdot A \cdot R$, Q.E.D.

☼: Vlastní čísla diagonální matice jsou prvky na diagonále a kanonická báze dává vlastní vektory.

Def: Matice *A* je **diagonalizovatelná**, pokud je podobná nějaké diagonální matici.

Aplikace: (a) $A = R^{-1} \cdot D \cdot R$; $\lambda = (D)_{ii}$ je *i*-té vlastní číslo a *j*-tý sloupec R^{-1} je vlastní vektor *A*.
(b) mocnění matic $A^k = R^{-1} \cdot D^k \cdot R \Rightarrow (D^k)_{i,i} = (D)_{i,i}^k$

Tvrz.: Matice *A* řádu *n* je diagonalizovatelná, právě když má *n* lineárně nezávislých vlastních vektorů.
Důkaz: Má-li platit $R^{-1} \cdot A \cdot R = D$, pak sloupce *R* jednoznačně odpovídají vlastním vektorům.

Důsl: (1) Má-li matice *A* řádu *n*, *n* různých čísel potom je diagonalizovatelná.
(2) Platí, že $A \in \mathbb{C}^{n \times n}$ má vlastní čísla $\lambda_1, \dots, \lambda_k$ násobnosti $r_1, \dots, r_k$ a navíc $\forall i \in \{1, \dots, k\} : rank(A - \lambda \cdot I) = n - r_i$,
právě když *A* je diagonalizovatelná.

Fakt: Každá čtvercová komplexní matice *A* je podobná matici v tzv. **Jordanově** normálním tvaru, což je
...
Tento tvar je dán jednoznačně až na pořadí bloků.

Př: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ není diagonalizovatelná.

☼: Nechť $A = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$ má vlastní číslo λ s příslušným vlastním vektorem *x*.

Pak $A \cdot x = \lambda \cdot x \Leftrightarrow (A - \lambda \cdot I) \cdot x = 0$, tedy $\underbrace{\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}}_{(A - \lambda \cdot I)} \dots x_n = \begin{pmatrix} * \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ (* značí „cokoliv“)

a lze nalézt posloupnost vektor, tzv. zobecněné vektory, takovou, že $(A - \lambda \cdot I) \cdot x_i = x_{i+1}$.

Def.: Komplexní čtvercová matice *A* je **hermitovská**, pokud platí $a_{i,j} = \bar{a}_{j,i}$ (komplexně sdružené číslo).

Def.: **Hermitovská transpozice** *A* je A^H, kde $(A^H)_{i,j} = (\bar{A})_{j,i}$

Jinými slovy:	hermitovská	$\Leftrightarrow A^H = A$
analogie:	symetrická	$\Leftrightarrow A^T = A$

Def.: Komplexní čtvercová matice *A* se nazývá **unitární**, pokud platí $A^H \cdot A = I$.

☼: Součin unitárních matic je unitární: $A^H \cdot A = I$, $B^H \cdot B = I \Rightarrow (AB)^H \cdot (AB) = B^H \cdot A^H \cdot A \cdot B = I$.

Př.: $A = \begin{pmatrix} 1 & 1+i \\ 1-i & t \end{pmatrix}$; $P_a(t) = t^2 - 3t \Rightarrow \lambda_1 = 3, \lambda_2 = 0$ $\quad R = \begin{pmatrix} \frac{1+i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{-1}{\sqrt{3}} & \frac{1-i}{\sqrt{3}} \end{pmatrix} \rightarrow R^{-1} = R^H = \begin{pmatrix} \frac{1-i}{\sqrt{3}} & \frac{-1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \frac{1+i}{\sqrt{3}} \end{pmatrix}$ $\quad R^{-1} \cdot A \cdot R = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$

☼: *A* je diagonizovatelná: $A \cdot R = R \cdot D$
☼ *A* je podobná *J*: $A \cdot R = R \cdot J$
Věta: Každá hermitovská matice má všechna vlastní čísla reálná a existuje unitární matice *R*, že $R \cdot A \cdot R^{-1}$ je diagonální.

Lin. algebra – determinanty, polynomy, vlast. čísla a vektory, charakteristický mnohočlen, skalární součin, pos.def. matice, bilineární a kvadratické formy

Důkaz: Indukcí podle řádu matice $A_n := A \in C^{n\times n}$.

Základní věta algebry $\Rightarrow$ existuje vlastní číslo λ

a k němu vlastní vektor x^1

Fakt: x^1 lze doplnit dalšími vektory na unitární matici $P_n = \begin{pmatrix} \vdots & \\ x^1 & \cdots \\ \vdots & \end{pmatrix}$

(Důkaz: Gran-Schmidtova ortogonizace)

Nyní máme matici z které jsme vyšli, její vlastní vektor a unitární matici.

$$\left(P_n^H \cdot A \cdot P_n\right)^H \underset{\text{☼}}{=} P_n^H \cdot \underbrace{A^H}_{\text{z def.}} \cdot \underbrace{\left(P_n^H\right)^H}_{\text{2x na H}} = \underbrace{P_n^H \cdot A \cdot P_n}_{\text{hermitovská}}$$

$A \cdot P_n$ má v prvním sloupci vektor $\lambda \cdot x^1$.

$P_n^H \cdot A \cdot P_n$ má v prvním sloupci $(\lambda, 0, \ldots, 0)^T \Rightarrow \lambda \in \mathbb{R}$

(z ☼, je hermitovská)

A_{n-1} je hermitovská matice řádu $n-1$,

z indukce existuje R_{n-1} unitární tž. $R_{n-1}^{-1} \cdot A_{n-1} \cdot R_{n-1} = D_{n-1}$.

Definujme: $\underbrace{R_n}_{\text{unitární}} := \underbrace{P_n}_{\text{unitární}} \cdot \underbrace{\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & R_{n-1} & \\ 0 & & & \end{pmatrix}}_{\text{unitární}} = S_n$

$$R_n^{-1} \cdot A \cdot R_n = R_n^H \cdot A_n \cdot R_n = S_n^H \cdot P_n^H \cdot A_n \cdot P_n \cdot S_n =$$

$$= \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & R_{n-1}^H & \\ 0 & & & \end{pmatrix} \cdot \begin{pmatrix} \lambda & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A_{n-1} & \\ 0 & & & \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & R_{n-1} & \\ 0 & & & \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & R_{n-1}^H & \cdot A_{n-1} \cdot & R_{n-1} \\ 0 & & & \end{pmatrix} \overset{\text{IP}}{=} \begin{pmatrix} \lambda & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & D_{n-1} & \\ 0 & & & \end{pmatrix}$$, Q.E.D.

Opak.: $\kappa(K_n) = n^{n-2}$ je počet koster úplného grafu.

Def.: **Laplaceova matice** grafu G na n vrcholech $v_1, \ldots, v_n$ je matice Q taková,

že $$q_{i,j} = \begin{matrix} -1 \Leftrightarrow (v_i, v_j) \in E(G) \\ 0 \text{ jinak} \end{matrix} ;\ i \neq j$$

$$q_{i,i} = deg(v_i)$$

$Q^{i,j}$ je matice vyniklá y Q vyškrtnutím i-tého řádku a j-tého sloupce.

Věta: Pro každý graf G platí $K(G) = det(Q^{11})$

Poznámka – důkaz:

$$Q = \underbrace{\begin{vmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & n-1 \end{vmatrix}}_{n} \rightarrow det(Q^{11}) = \begin{vmatrix} n-1 & -1 & \cdots & \cdots & -1 \\ -n & n & 0 & \cdots & 0 \\ \vdots & 0 & n & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ -n & 0 & \cdots & 0 & n \end{vmatrix} = n^{n-2}$$

Věta: **Bimet-Cauchyho**

Pro $A, B \in K^{m\times n}$ platí $\left|A^T \cdot B\right| = \sum_{*} \left|A_I^T \cdot B_I\right|$; $*:\ I \in \binom{\{1 \ldots n\}}{m}$.

Důkaz věty o $\kappa(G)$:

Zvolíme orientaci $\vec{G}$,

zavedeme orientovanou matici incidence

$$D \in \mathbb{R}^{n\times m};\ n = |V(G)|,\ m = |E(G)|;\ d_{i,j} = \begin{Bmatrix} 1 & v_i \text{začátek } e_j \\ -1 & v_i \text{ konec } e_j \\ 0 & jinak \end{Bmatrix}$$

☼: $D \cdot D^T = Q$. Zavedeme $D^1 = D$ bey prvního řádku.

Platí $D^1 \cdot D^{1T} = Q^{1,1}$ a dle Bimet-Cauchyho:

$$det(Q^{1,1}) = det(D^1 \cdot D^{1T}) = \sum_{I = \binom{\{1,\ldots,m\}}{n-1}} \left|D_I^1 \cdot D_I^{1T}\right| = \sum_{I = \binom{\{1,\ldots,m\}}{n-1}} \left|D_I^{12}\right| \overset{\text{lemma}}{=} \kappa(G)$$

Lemma 1: $\left|D_I^1\right| = \pm 1$, právě když $\{e_i; i \in I\}$ indukují strom.

Lemma 2: $\left|D_I^1\right| = 0$, právě když $\{e_i; i \in I\}$ neindukují strom.

Stačí již jen dokázat lemmátka.

(1) $\{e_i; i \in I\}$ indukují strom, spořádáme vrcholy $w_1, \ldots, w_n$ tak, že w_i je list ve zbylém stromu $w_{i+1}, \ldots, w_n$.

Přeuspořádáme sloupce D_I^1 podle pořadí $w_1, \ldots, w_n$.

$$D_I^1 = \begin{pmatrix} \pm 1 & 0 & \ldots & \ldots & \ldots & 0 \\ & \pm 1 & 0 & \ldots & \ldots & 0 \\ & & \ddots & 0 & \ldots & 0 \\ & & & \ddots & \ddots & \vdots \\ & & & & \ddots & 0 \\ & & & & & \pm 1 \end{pmatrix}$$

...determinant ± 1 .

(2) $\{e_i; i \in I\}$ neindukují strom, pak existuje cyklus.

$v_1 \notin$ cyklus $\Rightarrow$ sloupce hran, které jsou LZ $\Rightarrow det = 0$.

$\rightarrow$ má komponentu, která obsahuje v_1 :

$$\begin{matrix} & e_1 & e_2 & \\ v_2 & 0 & 1 & 1 \\ & 0 & -1 & -1 \end{matrix} \rightarrow \text{LZ}$$, Q.E.D.

Prostory se skalárním součinem

Úvod: Vektory můžeme násobit jako matici: $\vec{x}\cdot\vec{y} = xy \in \mathbb{R}$

$\forall a \in \mathbb{C}$: (*i*) $a+\overline{a} \in \mathbb{R}$ (*ii*) $a\cdot\overline{a} \in \mathbb{R}$ (*iii*) $|a| \in \mathbb{R}$

Def.: Nechť je V vektorový prostor nad $\mathbb{C}$. Zobrazení, které dvěma vektorům $\vec{u}, \vec{v} \in V$ přiřadí číslo $\langle \vec{u}|\vec{v}\rangle \in \mathbb{C}$, se nazývá **skalární součin** (ss), pokud splňuje axiomy:

(N)	$\forall \vec{u} \in V$:	$\langle \vec{u}|\vec{u}\rangle = 0 \Leftrightarrow \vec{u} = \vec{0}$
$(L1)$	$\forall a \in \mathbb{C}, \forall \vec{u}, \vec{v} \in V$:	$\langle a\cdot\vec{u}|\vec{v}\rangle = a\cdot\langle \vec{u}|\vec{v}\rangle$
$(L2)$	$\forall \vec{u}, \vec{v}, \vec{w} \in V$:	$\langle \vec{u}+\vec{v}|\vec{w}\rangle = \langle \vec{u}|\vec{w}\rangle + \langle \vec{v}|\vec{w}\rangle$
(KS)	$\forall \vec{u}, \vec{v} \in V$:	$\langle \vec{v}|\vec{u}\rangle = \overline{\langle \vec{u}|\vec{v}\rangle}$
(P)	$\forall \vec{u} \in V$:	$\langle \vec{u}|\vec{u}\rangle \geq 0$

Pozn., (1) Formálně: $\langle \square|\square\rangle$: $V \times V \to \mathbb{C}$

(2) Pro prostory nad $\mathbb{R}$ se skalární součin definuje stejně, (KS) se interpretuje jako $\forall \vec{u}, \vec{v} \in V$: $\langle \vec{v}|\vec{u}\rangle = \langle \vec{u}|\vec{v}\rangle$.

☼ SS pro $\mathbb{R}$ stejné až na axiom (KS): (KS) $\forall \vec{u}, \vec{v} \in V$: $\langle \vec{v}|\vec{u}\rangle = \langle \vec{v}|\vec{u}\rangle$

Př.: (1) Standardní SS pro aritmetické vektorové prostory:

$V = \mathbb{C}^n$: $\langle \vec{u}|\vec{v}\rangle = \sum_{i=1}^{n} u_i \overline{v}_i = v^H \cdot u \neq u^H \cdot v$

$V = \mathbb{R}^n$: $\langle \vec{u}|\vec{v}\rangle = \sum_{i=1}^{n} u_i v_i = v^T \cdot u = u^T \cdot v$

☼ $\langle \vec{u}|a\cdot\vec{v}\rangle = \overline{\langle a\cdot\vec{v}|\vec{u}\rangle} = \overline{a\cdot\langle \vec{v}|\vec{u}\rangle} = \overline{a}\cdot\overline{\langle \vec{v}|\vec{u}\rangle} = \overline{a}\cdot\langle \vec{u}|\vec{v}\rangle$

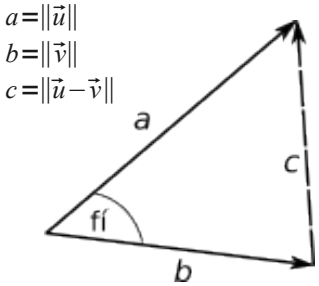
(2) SS na $\mathbb{R}^n$ definovaný pomocí regulární matice A: $\langle \vec{u}|\vec{v}\rangle := \vec{u}^T \cdot A^T \cdot A \cdot \vec{v}$,

například $V := \mathbb{R}^2$ $A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ $\langle \vec{u}|\vec{v}\rangle = u^T \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \vec{v} = u_1\cdot v_1 + 2\cdot u_1 \cdot v_1 + 2\cdot u_2 \cdot v_1 + 5\cdot u_2 \cdot v_2$

(3) SS na prostoru spojitých funkcí integrovatelných na intervalu $[a, b]$:

$$\langle f|g\rangle = \int_a^b f(x)\cdot g(x)\cdot dx$$

Def.: Nechť V je vektorový prostor se SS.
Potom **norma** určená tímto SS je zobrazení $\|\square\|$: $V \to \mathbb{R}$ dané předpisem $\|\vec{u}\| = \sqrt{\langle \vec{u}|\vec{u}\rangle}$.



Pozn: Význam:
$\|\vec{u}\|$ …délka vektoru $\vec{u}$
$\|\vec{u}\cdot\vec{v}\|$ …vzdálenost vektorů $\vec{u}$ a $\vec{v}$
$\langle \vec{u}|\vec{v}\rangle$ …určuje úhel mezi $\vec{u}$ a $\vec{v}$

☼ Na $\mathbb{R}^n$: $\langle \vec{u}|\vec{v}\rangle = \|\vec{u}\|\cdot\|\vec{v}\|\cdot\cos(\varphi)$, kde φ je úhel sevřený vektory *u* a *v*.

☼ Plyne z cosinové věty: $c^2 = a^2 + b^2 - 2ab\cdot\cos\varphi$

$\langle \vec{u}-\vec{v}|\vec{u}-\vec{v}\rangle = \langle \vec{u}|\vec{u}\rangle + \langle \vec{v}|\vec{v}\rangle - 2\cdot\|\vec{u}\|\cdot\|\vec{v}\|\cdot\cos\varphi$

$\langle u|u\rangle \underbrace{-\langle u|v\rangle - \langle v|u\rangle + \langle u|u\rangle}_{=-2\cdot\langle u|v\rangle} = \langle u|u\rangle + \langle v|v\rangle - 2\cdot\|u\|\cdot\|v\|\cdot\cos\varphi$

Věta: Cauchy-Schwarzova nerovnost

Nechť V je vektorový prostor se SS a normou z něj odvozenou, potom platí $\forall \vec{u}, \vec{v} \in V$: $\underbrace{|\langle \vec{u}|\vec{v}\rangle|}_{\text{kvůli } \mathbb{C}} \leq \|\vec{u}\|\cdot\|\vec{v}\|$.

Důkaz: Je-li $u = 0$ nebo $v = 0 \Rightarrow 0 \leq 0$ platí.

$a \in \mathbb{C}$: $\|u + a\cdot v\| \geq 0$ a tedy $0 \leq \|u + a\cdot v\|^2 = \langle u + a\cdot v|u + a\cdot v\rangle = \langle u|u\rangle + a\cdot\langle v|u\rangle + \overline{a}\cdot\langle u|v\rangle + a\cdot\overline{a}\cdot\langle v|v\rangle$.

Zvolíme $a := -\frac{\langle u|v\rangle}{\langle v|v\rangle} \Rightarrow$ eliminuje poslední dva členy.

$0 \leq \langle u|u\rangle - \underbrace{\frac{\langle v|u\rangle\cdot\langle u|v\rangle}{\langle v|v\rangle}}_{\neq 0} \Rightarrow \underbrace{\langle v|u\rangle\cdot\langle u|v\rangle}_{|\langle u|v\rangle|^2} \leq \langle u|u\rangle\langle v|v\rangle \Rightarrow |\langle u|v\rangle|^2 \leq \|u\|^2\cdot\|v\|^2 \underbrace{=}_{\text{BÚNO}} |\langle u|v\rangle| \leq \|u\|\cdot\|v\|$, Q.E.D.

Důsl.: (1) Nerovnost mezi aritmetickým a kvadratickým průměrem: $u \in \mathbb{R}^n$: $\frac{1}{n}\sum_{i=1}^{n} u_i \leq \sqrt{\frac{1}{n}\sum_{i=1}^{n} u_i^2}$

Důkaz: Zvolíme $v = (1, \ldots, 1)^T \in \mathbb{R}^n$

$\sum_{i=1}^{n} u_i = \langle u|v\rangle \leq \|u\|\cdot\|v\| = \sqrt{\sum_{i=1}^{n} u_i^2}\cdot\sqrt{n}$, Q.E.D.

(2) Norma odvozená ze SS splňuje trojúhelníkovou nerovnost: $\|u+v\| \leq \|u\| + \|v\|$

Důkaz: $\|u+v\| = \sqrt{\langle u+v|u+v\rangle} = \sqrt{\langle u|u\rangle+\langle u|v\rangle+\langle v|u\rangle+\langle v|v\rangle} \le \sqrt{\|u\|^2+2|\langle u|v\rangle|+\|v\|^2} \le$
$\le \sqrt{\|u\|^2+2\cdot\|u\|\cdot\|v\|+\|v\|^2} = \sqrt{(\|u\|+\|v\|)^2} = \|u\|+\|v\|$ Q.E.D.

Odbočka do analýzy

Obecně je norma nad prostorem zobrazení $V \to \mathbb{R}$

1)	$\forall u \in V$:	$\|u\| \ge 0$	pozitivnost
2)	$\forall u \in V$:	$\|u\| = 0 \Leftrightarrow u = 0$	jednoznačnost nuly
3)	$\forall u \in V, a \in \mathbb{C}$:	$\|a\cdot u\| = \|a\|\cdot\|u\|$	linearita (?)
4)	$\forall u, v \in V$:	$\|u+v\| \le \|u\|+\|v\|$	trojúhelníková nerovnost

Př.: jiných norem: L_p normy na $\mathbb{R}^n$: $\|u\|p = \sqrt[p]{\sum_{i=1}^{n} |u_i^{\,p}|}$

stat. norma odpovídá p =2.

$p=1 \ldots \|u\|_1 = \sum_{i=1}^{n} u_i$

$p=\infty \ldots \|u\|_\infty = \underbrace{\max}_{i=1,\ldots,n} u_i$

Ortogonalita

Def.: Dva vektory $\vec{u}$ a $\vec{v}$ v prostoru se SS jsou navzájem kolmé (značíme $\vec{u} \perp \vec{v}$), pokud platí, že $\langle \vec{u}|\vec{v}\rangle = 0$.

☼: Každý systém vzájemně kolmých vektorů je lineárně nezávislý.

Důkaz sporem: Máme: $u_1, \ldots, u_n$: $\forall u_i \perp u_j \ \wedge \ \forall i \ne j$, ale LZ $\Rightarrow$ $u_i = \sum_{i=2}^{n} a_i u_i$

$0 < \langle u_i|u_j\rangle = \left\langle u_1 \middle| \sum_{i=2}^{n} a_i u_i \right\rangle = \sum a_i \langle u_1|u_i\rangle = 0 \quad \Rightarrow$ SPOR Q.E.D.

Def.: Nechť Z je báze prostoru V se SS taková, že $\forall \vec{v} \in Z$: $\|\vec{v}\| = 1$ a navíc $\forall \vec{v}, \vec{v}\,' \in Z$: $\vec{v} \ne \vec{v}\,' \ \Rightarrow \ \vec{v} \perp \vec{v}\,'$.
Potom takovou bázi nazveme **ortonormální bází** prostoru V.

☼: Mějme Z ortonormální bázi prostoru $\mathbb{R}^n$.

Pak $A = \begin{pmatrix} \ddots & \ldots & \ddots \\ v_1 & \ldots & v_n \\ \ddots & \ldots & \ddots \end{pmatrix} \Rightarrow A^T \cdot A = I \Rightarrow A$ je ortogonální.

(analogicky $\mathbb{C}^n$: $A^H \cdot A = I_n \ \Rightarrow A$ je unitární)

(27. 4. 2009)

Tvrz: Nechť $Z = (v_1, \ldots, v_n)$ je ortonormální báze prostoru V,

potom $\forall \vec{u} \in V$: $\vec{u} = \sum_{i=1}^{n} \langle \vec{u}|\vec{v}_1\rangle \cdot v_1 + \langle \vec{u}|\vec{v}_2\rangle \cdot v_2 + \ldots + \langle \vec{u}|\vec{v}_n\rangle \cdot v_n$.

Důkaz: $\vec{v}_1, \ldots, \vec{v}_n$ je báze, vyjádříme: $\vec{v} = \sum_{i=1}^{n} a_i \vec{v}_i$, chceme ukázat: $a_i = \langle \vec{u}|\vec{v}_i\rangle$

$\langle \vec{u}|\vec{v}_i\rangle = \left\langle \sum_{j=1}^{n} a_j \vec{v}_j \middle| \vec{v}_i \right\rangle = \sum_{j=1}^{n} a_j \underbrace{\langle v_j|v_i\rangle}_{\text{2 možnosti}} = a_i$; možnosti: a) „<> = 0“ pro $i \ne j$, b) „<>= 1“ pro $i = j$ Q. E. D.

Def: Pro ortonormální bázi $(v_1, \ldots, v_n)$ a vektor $\vec{u} \in V$ se koeficientům $\langle \vec{u}|\vec{v}_i\rangle$ říká Fourierovy koeficienty.

Tvrz: **Parsevalova rovnost**: Je-li $Z = (v_1, \ldots, v_n)$ ortogonální báze prostoru V, potom $\forall \vec{u}, \vec{w} \in V$: $\langle \vec{u}|\vec{w}\rangle = [w]_Z^H [u]_Z$

Důkaz: $\vec{u} = \sum_{i=1}^{n} \langle u|v_i\rangle v_i$; $\vec{w} = \sum_{i=1}^{n} \langle w|v_i\rangle v_i$

$\langle u|w\rangle = \left\langle \sum_{i=1}^{n} \langle u|v_i\rangle v_i \middle| \sum_{j=1}^{n} \langle w|v_j\rangle v_j \right\rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \langle u|v_i\rangle \overline{\langle w|v_j\rangle} \langle v_i|v_j\rangle = \sum_{i=1}^{n} \langle u|v_i\rangle \overline{\langle w|v_i\rangle} = [w]_Z^H [u]_Z$ Q. E. D.

Def: Lineární zobrazení $f: V \to W$ mezi prostory s SS se nazývá unitární, pokud f zachovává SS.
$\forall \vec{u}, \vec{v} \in V$: $\langle \vec{u}|\vec{v}\rangle = \langle f(\vec{u})|f(\vec{v})\rangle$

Tvrz: Zobrazení $f: V \to W$ je unitární právě když pro normy odvozené se SS platí:
$\forall \vec{u} \in V$: $\|u\| = \|f(u)\|$

Důkaz: „=>“ $\|u\| = \sqrt{\langle u|u\rangle} = \sqrt{\langle f(u)|f(u)\rangle} = \|f(u)\|$

„<=“ Jako u CS nerovnosti.

$\|v + a\cdot w\| = \|w\| =$

Def: Unitární isomorfismus prostorů s SS se nazývá ISOMETRIE.

Věta: Nechť V a W jsou prostory s ortogonálními bázemi X=Y, stejné konečné dimenze,
potom platí, že $f: V \to W$ je isometrie právě když $[f]_{XY}$ je unitární.

Def: Nechť W je prostor se SS, $V \subseteq W$, a $Z = (v_1, \dots, v_n)$ je ortonormální báze V.

Zobrazení $p: W \to V$ je definováno předpisem: $p(u) := \sum_{i=1}^{n} \langle u|v_i\rangle v_i$ se nazývá **ortogonální projekcí** prostoru W na V.

Lemma: Nechť p je ortogonální projekcí W na V, potom $\vec{u} - p(\vec{u}) \perp \vec{v}_i$ pro $\forall\, v_i \in Z$

Důkaz: $\langle \vec{u} - p(\vec{u})|v_i\rangle = \left\langle \vec{u} - \sum_{i=1}^{n} \langle u|v_i\rangle \middle| v_i \right\rangle = \langle u|v_i\rangle - \sum_{j=1}^{n} \langle u|v_j\rangle\langle v_j|v_i\rangle = \langle u|v_i\rangle - \langle u|v_i\rangle = 0$ Q. E. D.

Gram-Schmidtova ortogonalizace

Vstup: Libovolná váze $(u_1, \dots, u_n)$ prostoru V se SS.

Výstup: Ortonormální báze $(v_1, \dots, v_n)$

Algoritmus: pro i:=1 do n opakuj

{

1) $w_i := u_i - \sum_{j=1}^{i-1} \langle u_i|v_j\rangle v_j$

2) $v_i = \frac{1}{\|w_i\|} w_i$

}

Korektnost:

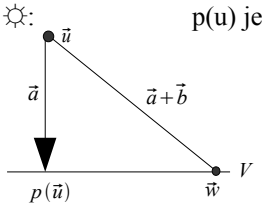
1) $w_i \perp v_j$ pro $j = i$ z … => $w_i \perp v_j$ pro $i \neq j$

2) $\|w_i\| = \left\| \frac{1}{\|w_i\|} w_i \right\| = \frac{1}{\|w_i\|} \|w_i\| = 1$

3) $span(v_1 \dots v_{i-1}, u_i, v_{i+1} \dots v_n)$ z lemmatu o výměně

Pozn, toto je využito ve větě o diagonalizovatelnosti hermitovských matic – potřebujeme G-S algoritmus.

☼: p(u) je nejbližší bod z u v prostoru V.



$\vec{a} = \vec{u} - p(\vec{u}) \quad \vec{a} \perp \vec{b}$

$\vec{b} = \vec{u} - p(\vec{u})$

$\|\vec{a} - \vec{b}\| = \sqrt{\langle a-b|a-b\rangle} = \sqrt{\langle a|a\rangle - \underbrace{\langle a|b\rangle - \langle b|a\rangle}_{=0} + \underbrace{\langle b|b\rangle}_{>0}} > \|\vec{a}\|$

(4. 5. 2009)

Ortogonální doplněk

Def: Nechť V je množina vektorů ve vektorovém prostoru W se SS. Ortogonální doplněk množiny V je množina:

$V^{\perp} := \{\vec{u} \in W : \vec{u} \perp \vec{v} \;\; \forall\, \vec{v} \in V\}$

Př: Když hledáme řešení homogení soustavy, tak hledáme $Ax = 0$ <=> hledáme $(r(a))^{\perp}$ vůči std. SS.

☼: $U \subseteq V \;\Rightarrow\; U^{\perp} \supseteq V^{\perp}$

Důkaz: $u \in V^{\perp} \;\Leftrightarrow\; u \perp v \;\; \forall\, v \in V \;\Rightarrow\; u \perp v \;\; \forall\, v \in U \;\Leftrightarrow\; u \in U^{\perp}$ Q. E. D.

Věta: Nechť V je podprostorem W se SS, potom platí:

(a) $V^{\perp}$ je podprostorem W

(b) $V \cap V^{\perp} = \{\vec{0}\}$

Je-li navíc W konečné dimenze:

(c) $dim(V) + dim(V^{\perp}) = dim(W)$

(d) $(V^{\perp})^{\perp} = V$

Důkaz: (a) I. $u, v \in V^{\perp}$, $\forall w \in W : \langle u+v|w\rangle = \langle u|w\rangle + \langle v|w\rangle = 0+0 = 0 \;\Rightarrow (u+v) \in V^{\perp}$

II. $u \in V^{\perp} \langle a \cdot u|w\rangle = a \cdot \langle u|w\rangle = a \cdot 0 = 0 \;\Rightarrow\; a \cdot u \in V^{\perp}$

$\Rightarrow$ I. $\wedge$ II. $\Rightarrow$ je podprostorem

(b) sporem: kdyby $u \in V \cap V^{\perp}$, $v \neq 0$ $\quad 0 < \left\langle \underset{\in V}{u} \middle| \underset{\in V^{\perp}}{u} \right\rangle = 0$ spor.

Příprava na (c) a (d):

Vezmeme ortonormální bázi X prostoru V a rozšíříme ji na ON bázi Z prostoru W.

$Y = Z \setminus X \qquad X = \{x_1 \dots x_n\} \qquad Y = \{y_1 \dots y_n\}$

Cíl: Chceme ukázat, že $V^{\perp} = span(Y)$

1) $\forall x_i \in X$ a $\forall y_j \in Y : \; x_i \perp y_j \;\Rightarrow\; y_j \perp \sum_{i=1}^{k} \lambda_i x_i \;\Rightarrow\; Y \subseteq V^{\perp}$

navíc: $w \in span(W) \;\Rightarrow\; w = \sum_{j=1}^{l} \beta_j y_j \quad \forall z \in V : Z = \sum_{i=1}^{k} \alpha_i x_i$

$$\langle w|z\rangle = \left\langle \sum_{j=1}^{l} \beta_j y_j \middle| \sum_{i=1}^{k} \alpha_i x_i \right\rangle = \sum_{j=1}^{l}\sum_{i=1}^{k} \beta_j \alpha_i \langle y_j|x_i\rangle = 0 \;\Rightarrow\; span(Y) \subseteq V^{\perp}$$

2) Libovolné $w \in V^{\perp}$ vyjádříme jako $\sum_{j=1}^{l} \beta_j y_j + \sum_{i=1}^{k} \alpha_i x_i$

$0 = \langle w|x_i\rangle = \lambda_i$ $\quad$ Z je ON báze V $\quad$ $\Rightarrow w \in span(Y) \;\Rightarrow\; V^{\perp} \subseteq span(Y)$

– konec přípravy –

(c) $dim(V) = |X| \;;\; dim(V^{\perp}) = |Y| \;;\; dim(W) = |X| + |Y|$

(d) $\left(V^{\perp}\right)^{\perp} = span(Z \setminus Y) = span(X) = V$ Q. E. D.

Pozitivně definitní matice

Tvrz.: Nechť V prostor se SS a $X = (y_1, \ldots, y_n)$ je jeho báze, potom pro matici A definovanou: $a_{i,j} := \langle x_i|x_j\rangle$ platí, že $\forall u, v \in V : \langle u|w\rangle = [w]_X^H \cdot A \cdot [u]_X$

Pozn.: Je-li X ON báze, je A jednotková.

Důkaz: $[u]_X = (\lambda_1, \ldots, \lambda_n) \quad u = \sum_{i=1}^{n} \lambda_i x_i$

$[w]_X = (\beta_1, \ldots, \beta_n) \quad w = \sum_{i=1}^{n} \beta_i x_i$

$$\langle u|w\rangle = \left\langle \sum_{i=1}^{n} \lambda_i x_i \middle| \sum_{j=1}^{n} \beta_j x_j \right\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_i \beta_j \langle x_i|x_j\rangle = [w]_X^H \cdot A \cdot [u]_X$$ Q. E. D.

Jaké vlastnosti musí mít A?

1) $a_{ij} = \langle x_j|x_i\rangle = \overline{\langle x_i|x_j\rangle} = \overline{a_{ij}} \;\Rightarrow$ A je hermitovská
2) musí zaručit, že $\langle u|u\rangle = [u]_X^H \cdot A \cdot [u]_X > 0$ pro $u \neq 0$

Def: Hermitovská matice A řádu n se nazývá pozitivně definitní, pokud $\forall x \in \mathbb{C}^n \setminus \{\emptyset\}$ platí: $x^H \cdot A \cdot x > 0$.

Užití: V MA vyšetřování lokálních a globálních extrémů funkcí více proměnných.

Věta: Pro hermitovskou matici A řádu n jsou následující podmínky ekvivalentní:

a) A je pozitivně definetní
b) A má všechna vlastní čísla kladná
c) existuje regulární matice U taková, že $A = U^H \cdot U$

Důkaz: (a=>b) A hermitovská, λ vlastní číslo $A \;\Rightarrow\; \lambda \in \mathbb{R}$, vezmeme vlastní vektor x, aby $Ax = \lambda x$

$$0 < x^H \cdot A \cdot x = \lambda \cdot x^H \cdot x \quad \Rightarrow \; \lambda > 0$$

$x^H \cdot x > 0$ (ze součinu na $\mathbb{C}$: $a \cdot \overline{a} \geq 0$)

(b=>c) A hermitovská => $\exists$ regulární R, tž. $A = R^H \cdot D \cdot R$, D diagonální

$\tilde{D} : \tilde{d}_{ij} = \sqrt{d_{ij}} \qquad A = R^H \cdot \tilde{D}^H \cdot \tilde{D} \cdot R = U^H \cdot U$

(c=>a) $x^H \cdot A \cdot x = x^H \cdot U^H \cdot U \cdot x = (Ux)^H \cdot Ux > 0 \;\Leftrightarrow$ U je regulární $ax \neq 0$

Tvrz: Pro pozitivně definitní matice existuje jednoznačná trojúhelníková matice U s kladnými prvky na diagonále taková, že $A = U^H \cdot U$, matici U se říká Choleskeho rozklad.

Důkaz: algoritmem:

Vstup: hermitovská matice A

Výstup: choleského rozklad, nebo odpověď, že A není poz. definetní.

Pro i:=1 do V proveď:

{ 1) $U_{ii} := \sqrt{a_{ii} - \sum_{k=1}^{k-1} \overline{U_{ki}} U_{ki}}$

2) není-li $u_{ii} \in \mathbb{R}, u_{ii} > 0 \;\Rightarrow$ STOP, A není pozitivně definetní

3) pro j = (i + 1) do u proveď:

$$\{ u_{ij} := \frac{1}{u_{ii}} \left(a_{ij} - \sum_{k=1}^{i-1} \overline{U_{ki}} \cdot U_{kj} \right) \}$$

} Q. E. D.

(přednáška 11.5.09)

Tvrz.: Bloková matice $A = \begin{pmatrix} \alpha & a^H \\ a & \tilde{A} \end{pmatrix}$ je positivně definitní, právě když $\alpha > 0$ a zároveň $\tilde{A} - \frac{1}{\alpha} \cdot a \cdot a^H$ je positivně definitní.

Pozn., Gaussovou eliminací sloupce pod α dostaneme $\begin{pmatrix} \alpha & a^H \\ a & \tilde{A} \end{pmatrix} = \begin{pmatrix} \alpha & a^H \\ 0 & \tilde{A} - \frac{1}{\alpha}\cdot a\cdot a^H \end{pmatrix}$.

Důkaz: $\Leftarrow$ Nechť $x \in \mathbb{C}^n, x \neq 0$, značme $x = \overbrace{\begin{pmatrix} x_1 \\ \tilde{x} \end{pmatrix}}^{\in \mathbb{C}} \in \mathbb{C}^n$.

$$x^H \cdot A \cdot x = (\overline{x_1}\, \tilde{x}^H) \cdot \begin{pmatrix} \alpha & a^H \\ a & \tilde{A} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \tilde{x} \end{pmatrix} = (\overline{x_1}\cdot\alpha + \tilde{x}^H \cdot a,\ \overline{x_1}\cdot a^H + \tilde{x}^H \cdot \tilde{A}) \cdot \begin{pmatrix} x_1 \\ \tilde{x} \end{pmatrix} =$$

$$= \overline{x_1}\cdot\alpha\cdot x_1 + x_1 \cdot \tilde{x}^H \cdot a + \overline{x_1}\cdot a^H \cdot \tilde{x} + \tilde{x}^H \cdot \tilde{A} \cdot \tilde{x} - \underbrace{\frac{1}{\alpha}\cdot \tilde{x}^H \cdot a \cdot a^H \cdot \tilde{x} + \frac{1}{\alpha}\cdot \tilde{x}^H \cdot a \cdot a^H \cdot \tilde{x}}_{=0} =$$

$$= \underbrace{\tilde{x}^H \cdot (A - \frac{1}{\alpha}\cdot a \cdot a^H)\cdot \tilde{x}}_{\geq 0} + \underbrace{(\sqrt{\alpha}\cdot\overline{x_1} + \frac{1}{\sqrt{\alpha}}\cdot \tilde{x}^H \cdot a)}_{y \in \mathbb{C}} \cdot \underbrace{(\sqrt{\alpha}\cdot x_1 + \frac{1}{\sqrt{\alpha}}\cdot a^H \cdot \tilde{x})}_{\overline{y} \in \mathbb{C}} > 0 \quad ,$$

≥ 0

protože alespoň na jedné straně bude ostrá nerovnost, jinak by muselo platit

zároveň $x_1 = 0 \wedge \tilde{x} = 0$.

$\Rightarrow$ Položíme $\alpha = e_1^H \cdot A \cdot e_1$, $e_1 = (1, 0, \ldots, 0)^T$

Pro libovolné $\tilde{x} \in \mathbb{C}^{n-1}$ zvolíme $x_1 := -\frac{1}{\alpha}\cdot a^H \cdot \tilde{x}$, potom platí:

$$0 < x^H \cdot A \cdot x = \tilde{x}^H \cdot (\tilde{A} - \frac{1}{\alpha}\cdot a \cdot a^H) + \underbrace{(\ldots)}_{=0}\cdot\underbrace{(\ldots)}_{>0}$$

$\Rightarrow \tilde{A} - \frac{1}{\alpha}\cdot a \cdot a^H$ je positivně definitní, Q.E.D.

Důsl.: (1) Positivně definitní matice lze rozeznat Gaussovou eliminací.
(2) Jacobiho podmínka: Hermitovská matice A řádu n je positivně definitní,
právě když mají matice $A_n, \ldots, A_1$ kladný determinant, kde
A_i vznikne z A umazáním posledních $n-i$ řádků a sloupců.
Důkaz: Aplikujeme předchozí tvrzení rekurentně a převedeme do odstupňovaných tvarů …

Bilineární a kvadratické formy

Def: Nechť V je vektorový prostor nad K a f je zobrazení $V \times V \to K$ splňující axiomy:

1. $\forall u, v, w \in V:$ $f(u+v, w) = f(u, w) + f(v, w)$
2. $\forall u, v \in V\ \forall \alpha \in K:$ $f(\alpha\cdot u, v) = \alpha\cdot f(u, v)$
3. $\forall u, v, w \in V:$ $f(u, v+w) = f(u, v) + f(u, w)$
4. $\forall u, v \in V\ \forall \alpha \in K:$ $f(u, \alpha\cdot v) = \alpha\cdot f(u, v)$

Potom se f nazývá **bilineární formou** V.
Bilineární forma je **symetrická**, platí-li $\forall u, v \in V:\ f(u, v) = f(v, u)$.
Zobrazení $g: V \to K$ se nazývá **kvadratická forma**,
pokud existuje bilineární forma taková, že $\forall u \in V:\ g(u) = f(u, u)$.

Def.: Nechť V je vektorový prostor a $X = (v_1, \ldots, v_n)$ je jeho báze, pak
matice bilineární formy f vůči bázi X je B, kde platí $b_{i,j} = f(v_i, v_j)$ a
matice kvadratické formy g je matice symetrické bilineární formy, která g vytvořuje, pokud taková existuje.

☼: $b_{i,j} = f(v_i, v_j) = \frac{1}{2}\cdot(g(v_i + v_j) - g(v_i) - g(v_j)) \Rightarrow$ matice kvadratické formy existuje vždy,
je-li K charakteristiky $\neq 2$.

☼: Počítání s maticemi formy:
$f(u, w) = [u]_X^T \cdot B \cdot [w]_X$, protože $f(\sum_i a_i\cdot v_i, \sum_j b_j\cdot v_j) = \sum_i \sum_j \underbrace{a_i}_{[u]_X}\cdot\underbrace{b_j}_{[w]_X}\cdot\underbrace{f(v_i, v_j)}_{B}$,
$g(u) = [u]_X^T \cdot B \cdot [u]_X$

Def.: Pro bilineární formu f na K^n je její **analytické vyjádření** polynom $f((x_1, \ldots, x_n)^T, (y_1, \ldots, y_n)^T) = \sum_{i=1}^n \sum_{j=1}^n x_i \cdot y_j \cdot b_{i,j}$.
Podobně analytické vyjádření kvadratické formy vůči dané bázi.

Věta: **Sylvesterův zákon o setrvačnosti kvadratických forem**
Nechť V je prostor konečné dimenze nad $\mathbb{R}$ a $g: V \to \mathbb{R}$ je kvadratická forma.
Potom existuje báze X taková, že matice g vůči X je diagonální a prvky na diagonále jsou 1, -1 nebo 0,
navíc počet 1, -1, 0 nezávisí na X a je pro všechny vhodné báze stejný.

(přednáška 18.5.09)

Důkaz: **(a)** existence
Zvolíme libovolnou bázi Y, sestavíme matici B' formy g vůči Y.
Víme, že B' je reálná symetrická.
Platí, že každá symetrická matice A má vlastní čísla reálná a existuje
ortogonální matice R, že $A = R\cdot D\cdot R^{-1}$ (známe v „hermitovské“ verzi).

Tedy existuje R, že $R^{-1}\cdot B'\cdot R = R^T\cdot B'\cdot R = D'$.
Víme, že pro B matici g vůči X a B' vůči Y platí $B = [id]_{XY}^T \cdot B' \cdot [id]_{XY}$.
Zvolíme B, S diagonální matice, že:
$d_{i,i} > 0 \Rightarrow b_{i,i} = 1, s_{i,i} = \sqrt{d_{i,i}}$

$$d_{i,i}<0 \Rightarrow b_{i,i}=-1, s_{i,i}=\sqrt{-d_{i,i}}$$
$$d_{i,i}=0 \Rightarrow b_{i,i}=0, s_{i,i}=1$$

$$\underbrace{\begin{pmatrix}\sqrt{d_{1,1}} & & 0\\ & \ddots & \\ 0 & & \sqrt{d_{i,i}}\end{pmatrix}}_{S^T}\cdot\underbrace{\begin{pmatrix}1 & & 0\\ & -1 & \\ 0 & & \ddots\end{pmatrix}}_{B}\cdot\underbrace{\begin{pmatrix}\sqrt{d_{1,1}} & & 0\\ & \ddots & \\ 0 & & \sqrt{d_{i,i}}\end{pmatrix}}_{S}=\underbrace{\begin{pmatrix}d_{1,1} & & 0\\ & \ddots & \\ 0 & & d_{i,i}\end{pmatrix}}_{D=D^T}$$

Čili platí $R^T\cdot B'\cdot R = S^T\cdot B\cdot S$, *S, R* regulární.

$\Rightarrow B=(S^T)^{-1}\cdot R^T\cdot B'\cdot R\cdot S^{-1}$, čili pro bázi *X*: $[id]_{XY}=R\cdot S^{-1}$ platí, že matice *B* formy *g* vůči *X* je diagonální a dle znění věty „(1, -1, 0)“.
Pozn., sloupce $[id]_{XY}$ jsou tvořeny souřadnicemi vektorů hledané báze *X* vůči bázi *Y*.

(b) jednoznačnost:

Značení: $g: V\to\mathbb{R}$, $X=(v_1,\dots,v_n)$, $Y=(w_1,\dots,w_n)$ dvě báze takové, že matice formy *g* vůči *X, Y* jsou *B, B′* diagonální ve tvaru

$$\begin{pmatrix}1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & 0 & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & 0 & & & 0 & \\ & & & & & & \ddots \\ & & & & & & & 0\end{pmatrix}$$ (odlišné jen délkou úseků).

Pozorování: #0 v $B=n-rank(B)\underbrace{=}_{B=R^T\cdot B'\cdot R} n-rank(B')=$ #0 v *B′*.

Zbývá již jen hranice 1/-1.

Označme $n'=rank(B)=\#1+\#-1$.

Analytické vyjádření formy *g* je

$g(u)= \quad x_1^2+x_2^2+\dots+x_r^2-x_{r+1}^2-\dots-x_{n'}^2$, kde

$[u]_X=(x_1,\dots,x_n)^T$, $r=\#1$ v B

$\quad\quad y_1^2+y_2^2+\dots+y_s^2-y_{s+1}^2-\dots-y_{n'}^2$, kde

$[u]_Y=(y_1,\dots,y_n)^T$, $s=\#1$ v B'

Pro spor ať $r>s$.

Zvolíme netriviální $z\in\underbrace{\mathsf{L}(\{v_1,\dots,v_r\})}_{L_1}\cup\underbrace{\mathsf{L}(\{w_{s+1},\dots,w_n\})}_{L_2}$,

$dim(L_1)=r$, $dim(L_2)=n-s$.

Víme, že pro *U, V* platí

$dim(U)+dim(V)=dim(\mathsf{L}(U\cup V))+dim(\mathsf{L}(U\cap V))$.

$z\in\mathsf{L}(\{v_1,\dots,v_r\})\setminus\{\vec{0}\}\Rightarrow$ pro $[z]_X=(x_1,\dots,x_r)^T$ je alespoň jedno z $x_1,\dots,x_r\neq 0$ a zároveň $x_{r+1},\dots,x_n=0\Rightarrow g(z)>0$.

$z\in\mathsf{L}(\{w_{s+1},\dots,w_n\})\setminus\{\vec{0}\}\Rightarrow$ pro $[z]_Y=(y_{s+1},\dots,y_n)^T$ je alespoň jedno z $y_{s+1},\dots,y_n\neq 0$; $y_1,\dots,y_s=0$, čili

$g(z)=\underbrace{y_1^2+\dots+y_s^2}_{=0}-y_{s+1}^2-\dots-y_{n'}^2\leq 0$, *SPOR*. Q.E.D.

Def: Vektoru $(\#1,\#-1,\#0)$ se říká **signatura formy**, respektive signatura symetrické matice, a příslušná báze se nazývá **polární báze**.

Úloha: Na závěr, kolik lze v $\mathbb{R}^d$ nalézt nejvíce přímek, aby každé dvě svíraly stejný úhel? (pokud někdo chce, abych přepsal i tuto úlohu, nechť se mi ozve)