Souhrn lingebry

s Hladíkem

A jako bonus jsem důkazy přepsal jak vandrák… a bez předpokladů
Takže je potřeba si projít ještě ten druhej formálnější soubor

Programování I (NPRG030)

1. ročník Bc. studia MFF UK - Informatika

Autor: Milan Veselý

Dobře no, možná je tohle formátovaní úplně zbytečný xd

Obsah

(Tučně jsou témata u zkoušky)

Pomocné odkazy

Milan Hladík: https://kam.mff.cuni.cz/~hladik/LA/
Videa: https://kam.mff.cuni.cz/~hladik/LA/Video-la1-ZS2021/
Skripta: https://www.ms.mff.cuni.cz/~sejkoraji/sbirka/zalohy/skripta_la.pdf
Vzorové cvičení: https://kam.mff.cuni.cz/~hladik/LA/cviceni_la_vzor_pub.pdf
Naše cvičení: https://kam.mff.cuni.cz/~hladik/LA/cv_la_slides_zoom_zs2021.pdf
Naše úkoly: https://kam.mff.cuni.cz/~hladik/LA/dcv_LA_ZS2021.pdf
Moje řešení: https://bit.ly/3hGbdU4
Videa z přednášek: https://kam.mff.cuni.cz/~hladik/LA/Video-la1-ZS2021/

Pozn. na úvod: všechny důkazy jsem psal co nejkratší a chybí jim spoustu detailů

Soustavy lineárních rovnic (řešení a řešitelnost)

Maticová reprezentace

Matice – obdélníková tabulka reálných čísel

(m × n, m je # řádek, n je # sloupec, čtvercová matice, …)

Vektor (matice n × 1) - může být ale také řádkový vektor

Notace:

A_{i*} je i-tý řádek, …

Soustava lineárních rovnic

Jak vypadá… že má koeficienty a neznámé…

Řešení: vektor, který vyhovuje všem rovnicím

Efektivnější zápis -> Matice soustavy

Rozšířená matice soustavy (není nutné zobrazovat svislou čáru)

Geometrický význam soustavy rovnic

Za předpokladů… ~~(0,0)~~ popisují přímku

Řešení je průnik přímek, rovin

Elementární řádkové úpravy

Vynásobení α
Přičtení α násobku
Výměna

Dalo by se to zjednodušit

Elementární řádkové úpravy zachovávají množinu řešení

Symetrie, protože každá úprava má svoji inverzi…

Gaussova eliminace

Dopředná fáze a zpětná substituce

Odstupňovaný tvar (REF)

Pozice prvního nenulového prvku v řádku je ostře menší v následujících řádcích

Pozice nenulových prvků jsou pivoty

Pokud mají pivot, tak jsou sloupce bázické

Hodnost matice je počet nenulových řádků v REF

Řešení Gaussovy eliminace

Rozšířenou matici převedeme na REF a mohou nastat následující situace:

Soustava nemá řešení

Je-li poslední sloupec bázický

rank(a) < rank (A | B)
Důkaz : r-tý řádek má tvar 0 = b

Soustava má řešení (rank(a) = rank (A | B))

Jedno

Počet proměnných = počtu pivotů
-> Zpětná substituce

Důkaz : ukázka REF tvaru a zpětné substituce

Nekonečně mnoho

Alespoň jeden další nebázický
Parametrický popis
Množiny řešení…

Nadbytečné rovnice jsou lineárně závislé

Ale ztratíme informaci které to byly
rank (A | B) udává počet významných rovnic v soustavě

Výpočetní složitost

V prvním cyklu n^2 součinů a odečítání
-> Vzoreček sumy n^2

Celkem $\frac{2}{3}n^3$

Gaussova-Jordanova eliminace

Druhý algoritmus řešení soustavy

Místo REF používá redukovaný odstupňovaný tvar (RREF)

Redukovaný odstupňovaný tvar

Pokud je v REF a navíc na pozici pivotů jsou jedničky a nad každým pivotem jsou nuly

Řešení G-J

Soustava nemá řešení

Pokud je poslední sloupec bázický

Soustava má řešení

Jedno

r = n a tedy tvar $(x_1, x_2, \dots, x_n) = (b_1, b_2, \dots, b_n)$
Důkaz : přepisem

Nekonečně mnoho

r < n

Složitost n^3

Jednoznačnost RREF

Sporem, máme dvě různé RREF A_1 a A_2. Označme i první sloupec ve kterém se matice liší. Odstraňme z matic A, A_1 a A_2 všechny sloupce za i a všechny nebázické před ním. Výsledné matice jsou stále RREF tvary základní matice. Rozdíl je pouze v posledních sloupcích a pokud interpretujeme matici jako soustavu lin. rovnic tak vzniká spor různých řešení.

Aplikace např. Kirchhoffovy zákony

Základní operace s maticemi a jejich vlastnosti.

Rovnost: stejné rozměry a pro všechny $A_{ij} = B_{ij}$
Součet: $(A+B)_{ij} = A_{ij} + B_{ij}$
Násobek: $(\alpha A)_{ij} = \alpha A_{ij}$

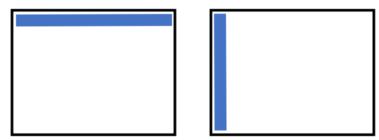
Nulová matice 0, jednotková matice I_n , jednotkový vektor e_i …

Vlastnosti:

Komutativita	Asociativita	$A + 0 = A$	$A - A = 0$
$\alpha(\beta A) = (\alpha\beta)A$	$1A = A$	$\alpha(A + B) = \alpha A + \alpha B$	$(\alpha + \beta)A = \alpha A + \beta A$

Trivlní důkazy z definice a vlastnotí reálných čísel

Součin matic:



A má m×p a B má p×n
První řádek, druhá sloupec
Formálně: $(AB)_{ij} = \sum_{k=1}^{p} A_{ik} B_{kj}$

Vlastnosti součinu

Asociativita	Distributivita zleva a zprava	$\alpha(AB) = (\alpha A)B = A(\alpha B)$
$0A = A0 = 0$	$I_m A = A I_n = A$ (A je m×n)	

Důkazy :

triviálně, např. Asociativita – matice A, B, C (m×p, p×r, r×n)

1. (AB)C i A(BC) mají stejný tvar
2. prvku jsou shodné, protože rozepsání sum

Transpozice

$(A^T)_{ij} = A_{ji}$ a typ m×n -> n×m
„překlopení dle hlavní diagonály“
(Použití na zapisování vektorů do řádků(

Vlastnosti:

$(A^T)^T = A$ $\quad$ $(A + B)^T = A^T + B^T$ $\quad$ $(\alpha A)^T = \alpha A^T$ $\quad$ $(AB)^T = B^T A^T$

Důkazy:

opět triviálně z definice, prvně tvar a pak prvky

Umožňuje důkaz symetrické matice

(Uzavřenost na součet, ale ne na součin)
matice $A^T A$ je mimochodem vždy symetrická

Další speciální matice jsou diagonální a horní nebo dolní trojúhelníková

Součin vektorů $x, y \in R^n$

$x^T y$ je takzvaný skalární součin – matice 1x1 neboli také $\sqrt{x^T x}$ nebo $\sqrt{\sum_{i=1}^{n} x_i^2}$

xy^T je vnější součin – matice řádu n

např. $e_i e_j^T$ je matice s jedničkou na (i, j) hodnost nula nebo jedna – všechny řádky násobkem vektoru y^T

tvrzení platí i opačně

Vlastnosti součinu

$A_{ej} = A_{*j}$ $e_i^T A = A_{i*}$ $(AB)_{*j} = AB_{*j}$ $(AB)_{i*} = A_{i*}B$

$Ax = \sum_{j=1}^{n} x_j A_{*j}$ $y^T A = \sum_{i=1}^{m} y_i A_{i*}$

Důkazy:

1. $Ae_j = \sum_{k=1}^{n} A_{ik}(e_j)_k = \sum_{k!=j}^{n} A_{ik} 0_j + a_{ij}$ (na přednášce pouze schéma)
3. se akorát vynásobí jednotkovým vektorem
5. opět pouze schéma, říká to ale, že sloupce matice se vynásobí x_1, x_2, ...

Z 5. nám ale vyplývá, že soustavu rovnic můžeme zapsat jako Ax = b

na to se lze dívat řádkově i sloupcově

řádkově to jsou rovnice soustavy a tedy nadroviny

sloupcově to je vyjádření b pomocí sloupečků matice

Matice zobrazení – později

(Násobení znamená skládat zobrazení)

Blokové násobení matic

Rozdělení matice na podmatice -> některé operace jsou snazší

Regulární matice

Taková čtvercová matice, která v reprezentaci Ax = b má jediné řešení x = 0

V opačném případě je singulární

Ekvivalence:

A je regulární

$RREF(A) = I_n$

rank(A) = n

Důkaz plyne z rozboru G-J eliminace:

Soustava (A | 0) má jediné řešení, když RREF tvar matice (A | 0) je (In | 0)

Navíc je ekvivalentní, že pro každé (nějaké) b ∈ R n má soustava Ax = b jediné řešení

Opět plyne z rozboru

Vlastnosti:

součin regularitu zachová, součet nemusí (I – I = 0)

Důkaz: ABx = 0 -> Ay a z regularity y = 0 -> Bx = 0

A pokud je A nebo B singulární Ay = 0 a buď Bx = 0 a x !=0 a nebo y !=0

Matice elementárních úprav

A se dá vyjádřit jako EA a E je regulární

$EI_n = E$

To, že to ale opravdu funguje se musí dokázat pro každou operaci zvlášť

Reprezentace (násobení zleva):

vynásobení i-tého řádku je jednotková matice, ale místo i-té jedničky má α přičtení je jednotková matice ale na i-tém sloupci j-tém řádku má 1

analogicky výměna např. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Je regulární, protože má inverzní operaci zpět na jednotkovou

Tvrzení RREF(A) = QA (pro A je m×n a Q je regulární a m×m)

Důkaz přes skládání matice úprav $E_k \ldots E_1 A$

Tvrzení každá regulární matice se dá vyjádřit součinem konečně mnoho elementárních matic

Důkaz Pokud k úpravami převedu A na jednotkovou, tak obrácené úpravy

Inverzní matice

Motivace: A + B + (– B) = A, ale co při součinu?

$ABB^{-1} = A$ a tedy $BB^{-1} = I$

Inverzní k 0_n evidentně neexistuje -> k čemu ano? – K regulárním

Věta o tom, že regulární má jednoznačný inverz a naopak má-li inverz, tak je regulární

$A-1$ je inverzní maticí k A, pokud splňuje $AA^{-1} = A^{-1}A = I_n$

Konstrukční *Důkaz:*

Z regularity $Ax = e_j$ má jediné řešení pro každé j po n

Matice A^{-1} pak bude mít jako sloupce vektory řešení

Rovnost $AA^{-1} = I$ se ukáže po sloupcích

$(AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = I_{*j}$

Druhá rovnost potřebuje „trik"

$A(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$

Z regularity A pak $(A^{-1}A - I) = 0$…

Důkaz jednoznačnosti:

$AB = BA = I$

$B = BI = B(AA^{-1}) = (BA)\,A^{-1} = IA^{-1} = A^{-1}$

Důkaz regularity inverze:

$Ax = 0$ a následně $x = Ix = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}0 = 0$

Na základě toho můžeme snadno dokázat, že je-li A regulární, pak A^T je regulární

Důkaz: je regulární, tak má inverz a tedy $AA^{-1} = A^{-1}A = I_n$ můžeme celou transponovat. To znamená, že A^T má taky inverz

Důkaz o tom, že stačí jedna rovnost (Je-li $BA = I_n$ pak A, B jsou regulární a k sobě inverzní):

Regularita vyplývá z regularity I_n a tedy víme, že A, B mají inverzi

Následně $B = BI_n = B(AA^{-1}) = (BA)A^{-1} = I_nA^{-1} = A^{-1}$ a analogicky A…

Výpočet inverzní matice:

Je-li RREF $(A \mid I_n) = (I_n \mid B)$ pak B je inverze, jinak je A singulární

Proč?

$(I_n \mid B) = Q\,(A \mid I_n)$ -> $I_n = QA$ -> $Q = A^{-1}$ jinak RREF A != I_n …

Tvrzení:

$(A^{-1})^{-1} = A$ $\quad$ $(A^{-1})^T = (A^T)^{-1}$ $\quad$ $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1}$, když α!=0 $\quad$ $(AB)^{-1} = B^{-1}A^{-1}$

Důkazy:

1. $A^{-1}A = I_n$ 2. transpozice definice inverzní matice 3. $\alpha A \frac{1}{\alpha} A^{-1} = \frac{\alpha}{\alpha} I_n$ 4. $AB(AB)^{-1}$

Také platí, že pro $Ax = b$ je $x = A^{-1}b$, protože $x = Ix = A^{-1}Ax = A^{-1}b$ (to se používá spíš opačně)

$Ax = b$ je ekvivalentní s $QAx = Qb$

L a P se rovnají a tedy po násobení Q zůstane množina stejná nebo se zvětší ($Q = 0$)

Pokud je Q regulární, tak zůstane množina stejná, zpět můžeme přejít přes Q^{-1}
Lze dokázat i přes matice el. úprav

Inverzní matice geometrie

Zobrazení vynásobením regulární maticí je bijekce a má svoji inverzi
pozn. skládání bijekcí je opět bijekce (násobení regulárních matic)

Geometricky lze dokázat i inverzi součinu/skládání matic

Grupy

(bez permutací je to jedno téma)

Grupa je abstraktní struktura s binární operací s určitými vlastnostmi

Základní vlastnosti

Buď $\circ : G^2 \to G$ binární operace na množině G. Pak grupa je dvojice $(G, \circ)$ splňující:

Asociativitu
Existenci neutrálního prvku
Existenci inverzního prvku

Abelova grupa

Navíc také splňuje komutativitu

Příklady grup: $(Z, +)$, $(Q, +)$, …
$(R^{m \times n}, +)$
Konečná grupa $(Z_n, +)$ pozn. používá se modulo sčítání
$(Q \setminus \{0\}, \cdot)$, …
polynomy

Neabelovské grupy: Násobení regulárních matic
Zobrazení na množině se skládáním, např. rotace v R^n

Negrupy: $(N, +)$ – inverze , $(Z, -)$ – asociativita, $(R \setminus \{0\}, :)$ – asociativita

Vlastnosti prvků v grupě G:

1. Krácení $a \circ c = b \circ c$ implikuje $a = b$
2. Jednoznačnost e (neutrální prvek)
3. Jednoznačnost inverzního prvku pro každý prvek
4. Rovnice $a \circ x = b$ má právě jedno řešení pro každé a, b z G
5. Inverze inverzního prvku je původní prvek
6. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Důkaz:

1. Přidat inverzi c zprava
2. Spor $e_1 = e_1 \circ e_2 = e_2$
3. Existují-li dvě různé inverze $a \circ a_1 = e = a \circ a_2$ -> krácení
4. Vynásobit zleva a^{-1}

Podgrupa

Stejně definovaná operace, existence inverzního a neutrálního prvku a uzavřenost

Každá grupa má dvě triviální

Permutace

Příklad grup

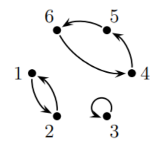
Permutace je vzájemně jednoznačné zobrazení

Značení

Tabulkou

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

Grafem



Rozložením na cykly

$$p = (1,2)(3)(4,5,6)$$

Inverzní permutace

Taková permutace pro kterou platí $p^{-1}(i) = j$ pokud p(j) = i

Skládání permutací

$(p \circ q)(i) = p(q(i))$ pozn. prvně se provádí permutace na konci

Skládání operací je asociativní, ale není komutativní

Transpozice

Příklad jednoduché permutace, kde se prohazují dva prvky

Jednoduší je už jenom identita

Znaménko permutace

$sgn(p) = (-1)^{n-k}$

$sgn(id) = 1, sgn\big((i,j)\big) = -1$

Sudé (1) a liché permutace (– 1)

Věta: $sng(p) = -sgn(t \circ p) = -sgn(p \circ t)$ pro $t = (i,j)$

Důkaz:

Permutace p se skládá z několika cyklů a my rozlišíme dva případy

Stejný cyklus a odlišný cyklus

Stejný cyklus se roztrhne a odlišené se spojí (změna znaménka)

Rozložení permutace na složení transpozic

Můžeme rozložit libovolný cyklus stylem

$(u_1, u_2, \dots, u_r) = (u_1, u_2) \circ (u_2, u_3) \circ \dots \circ (u_{r-1}, u_r)$

Není ale jednoznačný (pouze parita zůstává)

Z toho platí, že $sgn(p) = (-1)^r$, kde r je počet transpozic

Zároveň z toho platí, že $sgn(p \circ q) = sgn(p) \cdot sng(q)$

Dohromady jdou rozložit na $r_1 + r_2$ $transpozic$

Věta $sgn(p) = sgn(p^{-1})$

Dokážeme z id, kterou rozložíme na $p \circ p^{-1}$

Znaménko se dá vyjádřit i přes počet inverzí

Inverze je uspořádaná dvojice i<j a p(i)>p(j)

Platí, že $sgn(p) = -1^{I(p)}$

Symetrická grupa

Množina permutací s operací skládání tvoří nekomutativní grupu

Tzv. symetrickou grupu

Dá se ukázat, že každá grupa je isomorfní nějaké symetrické podgrupě

Těleso

Množina $\mathbb{T}$ se dvěma komutativními operacemi $+$ a $\cdot$ splňující

$(\mathbb{T}, +)$ je Abelova grupa, neutrální prvek 0 a inverze a je – a

$(\mathbb{T}\ \{0\}, \ \cdot)$ je Abelova grupa, neutrální prvek 1 a inverze k a je a^{-1}

$\forall a, b, c \in \mathbb{T}: a \cdot (b + c) = a \cdot b + b \cdot c$ (distributivita)

Komutativitu operací jsme explicitně vyžadovali proto, že druhá grupa nic neříká o 0

Mohou ale existovat i nekomutativní tělesa

Příklady těles $\mathbb{Q}, \mathbb{R}$ nebo $\mathbb{C}$ (nebo také *kvaterniony*)

Základní vlastnosti:

$0a = 0$ $\quad ab = 0 \Rightarrow a = 0$ nebo $b = 0$ $\quad -a = (-1)a$

Důkazy:

Přes $0a = (0 + 0)a$ a přičtu $-0a$

Buď je a nula a nebo existuje a^{-1} a tím to vynásobíme zleva

$(1 - 1)a = 0$

Konečná tělesa

Modulo operace

$\mathbb{Z}_n$ (*to jest* $\{0,1, \dots, n - 1\}$) je těleso právě tehdy, když n je prvočíslo

Pokud každý prvek (modulo) vynásobíme nenulovým prvkem $a \in \mathbb{Z}_n$ dostaneme opět všechny prvky $\mathbb{Z}_n$ a to právě jednou

Důkaz:

Předpoklad $ak = al\ pro\ k, l \in \mathbb{Z}_n, k \neq l$ a tedy a nebo $(k - l)$ jsou 0

To ale nastat nemůže

$\mathbb{Z}_n$ je těleso právě tehdy, když n je prvočíslo

Důkaz:

Je-li n složené, pak $n = pq$, kde $1 < p, q < n$

Kdyby $\mathbb{Z}_n$ těleso pak $pq = 0$ implikuje, že buď $p = 0$ nebo $q = 0$

Pro prvočíslo ověříme všechny axiomy

Hledání inverze prvku – Eukleidův algoritmus $ax + bp = 1$

Konečná tělesa mohou mít i velikost p^n – Galoisova tělesa

Prvky jsou polynomy stupně nejvýše n – 1 s koeficienty $\mathbb{Z}_p$

Sčítání je normální

Násobení je definováno jako normální modulo ireducibilní polynom n

Charakteristika tělesa

Nejmenší $n \in \mathbb{N}$, že součet n jedniček je 0

Charakteristika je buď nula nebo prvočíslo

Důkaz přes $n = pq$

Pokud charakteristika není 2 můžeme zavést průměr

Malá Fermatova věta

$Buď\ p\ prvočíslo\ a\ buď\ 0 \neq a \in \mathbb{Z}_p. Pak\ a^{p-1} = 1\ v\ \mathbb{Z}_p$

Důkaz

$\{0,1, \dots , p-1\} = \{0a, 1a, \dots , (p-1)a\}$

Bez nul tedy $1 \cdot 2 \cdot \dots \cdot (p-1) = 1a \cdot 2a \cdot \dots \cdot (p-1)a$

A krácením dostaneme $1 = a \cdot \dots \cdot a = a^{p-1}$

Aplikace např samoopravné kódy – generující matice v $\mathbb{Z}_2^{3\times 4}$

Vektorové prostory a podprostory

Motivace: zobecnění aritmetického vektoru $\mathbb{R}^n$

Základní pojmy

Reprezentace jako vektor nebo bod

Sčítání, násobení číslem, …

Vektorový prostor nad tělesem $\mathbb{T}$ rozumíme množinu s vektorovým součtem $+: V^2 \to V$ a násobením vektoru skalárem $\mathbb{T} \times V \to V$, který pro každé $\alpha, \beta \in \mathbb{T}$ a $u, v \in V$:

$(V, +)$ je Abelova grupa $\qquad \alpha(\beta v) = (\alpha\beta)v \qquad 1v = v$

$(\alpha + \beta)v = \alpha v + \beta v \qquad (u + v)\alpha = u\alpha + v\alpha$

Příklady: aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, prostor matic, prostor polynomů, funkcí, …

Základní vlastnosti:

$0v = o \qquad \alpha o = o \qquad \alpha v = o \Rightarrow a = 0\ nebo\ v = 0 \qquad -1v = -v$

Důkazy analogicky jako u tělesa

Podprostory

Musí platit existence nulového prvku, uzavřenost na sčítání a součin se skalárem

Ostatní platí automaticky, protože je to podmnožina

Příklady: dva triviální podprostory, v $\mathbb{R}^2$ to jsou přímky přes počátek, …

Musí být nad stejným tělesem BTW

Platí: jsou-li $U, V \Subset$ W a $U \subseteq V$ pak $U \Subset V$ $\qquad$ tranzitivita $U \Subset V \Subset$ W $\Rightarrow$ $U \Subset W$

Průnik podprostorů je podprostor, sjednocení ale obecně ne

Díky poslednímu tvrzení můžeme definovat **lineární obal**

Buď V vektorový obal na $\mathbb{T}$ a $W \subseteq V$ pak lineární obal $span(W)$ je průnik všech podprostorů V obsahující W neboli $span(W) = \bigcap_{U: W \subseteq U \Subset V} U$

Je to tedy nejmenší prostor obsahující W

(Lineární obal bodu je přímka, dvou nezávislých bodů rovina, …)

Generátory prostoru jsou prvky množiny jejíž *span* tvoří daný prostor

Zavádí se i pojem konečně generovaný prostor

Lineární kombinace

Sčítáním vektorů a nebo násobením můžeme vytvořit lineární kombinace

Lineární kombinace je výraz typu $\sum_{i=1}^{n} a_i v_i$, kde $a_i \in \mathbb{T}$ a $v \in V$ (výsledek je vektor)

Nyní uvažujeme pouze lineární kombinace konečně mnoho vektorů

Pomocí lineárních kombinací můžeme vygenerovat celý lineární obal množiny vektorů

Neboli $Buď\ V\ vektorový\ prostor\ nad\ \mathbb{T}\ a\ mějmě\ v_1, v_2, \dots, v_n \in V. Pak$

$$span\{v_1, v_2, \dots, v_n\} = \{\sum_{i=1}^{n} a_i v_i\,; a_1, a_2, \dots, a_n \in \mathbb{T}\}$$

Důkaz:

Inkluze $\supseteq$ musí být uzavřený na násobky a součty a tedy…

Inkluze $\subseteq$ ukáže se tak, že obsahuje každý vektor, nulový vektor a je uzavřený na součin a součet

$u + u' = \sum_{i=1}^{n} \beta_i v_i + \sum_{i=1}^{n} \beta'_i v_i = \sum_{i=1}^{n} (\beta + \beta'_i) v_i$ a násobky analogicky

Umožňuje nám to i jiný pohled na $Ax = b$

Výraz $Ax = \sum_j x_j A_{*j}$ je vlastně lineární kombinace sloupců

Řešení b tedy existuje, když b náleží do sloupcového prostoru A

Dokonce i pohled na AB

$\sum_{k=1}^{p} A_{*k} B_{k*}$

Lineární nezávislost

Znamená, že $\sum_{i=1}^{n} a_i v_i = o$ nastane pouze pro $\alpha_1 = \alpha_2 = \dots = 0$

Lin. nezávislost nekonečné množiny je když každá její podmnožina je lin. nezávislá

Zjišťování nezávislosti přes matici…

Nezávislost a regulární matice spolu souvisí

Její sloupce jsou lineárně nezávislé

Množina vektorů jsou lineárně závislé, pokud jeden z nich můžeme vyjádřit kombinací

Důkaz

$\Rightarrow$ Jsou-li vektory závislé, tak $\sum_{i=1}^{n} \beta_i v_i = o$ a vezmeme-li $\beta_k \neq 0$, tak

$$\beta_k v_k = \sum_{i \neq k}^{n} \beta_i v_i$$

… a z toho už snadno vyjádříme, že v_k je kombinací

$\Leftarrow v_k - \sum_{i \neq k}^{n} \alpha_i v_i = o$

Důsledek: vektory jsou závislé, právě tehdy když se odebráním některého $span$ nezmenší

$span(v_1, \dots, v_n) = span(v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n)$

Důkaz: Jsou-li vektory závislé, existuje v_k, které můžeme vyjádřit $v_k = \sum_{i \neq k}^{n} \alpha_i v_i$

Inkluze $\supseteq$ platí triviálně. Libovolný vektor $u \in span\{v_1, \dots, v_n\}$ se dá vyjádřit:

$$u = \sum_{i=1}^{n} \beta_i v_i = \beta_k v_k + \sum_{i \neq k} \beta_i v_i = \beta_k \sum_{i \neq k} \alpha_i v_i + \sum_{i \neq k} \beta_i v_i = \sum_{i \neq k}^{n} (\beta_k \alpha_i + \beta_i) v_i$$

Je to tedy opět lineární kombinace.

Obrácená implikace je již důsledek předchozí věty.

Báze

Jakýkoliv lineárně nezávislý systém generátorů (uspořádaná množina)

Kanonická báze v $\mathbb{R}^n$ například $e_1, \dots, e_n$

$Nechť\ v_1, \dots v_n\ je\ báze\ prostoru\ V. Pak\ pro\ každé\ u \in V\ existují\ jednoznačné\ koeficitny\ lineární\ kombinace$

Důkaz: Každé u se dá vyjádřit jako lineární kombinace, protože báze

Jednoznačnost se ukáže sporem – vyjádříme dvě lineární kombinace a jejích rozdíl o

Z lineární nezávislosti se ale všechny prvky rovnají

Souřadnice

Nechť B je báze a u vektor v prostoru V s vyjádřením $u = \sum_{i=1}^{n} \alpha_i v_i$ pak souřadnice vektoru jsou koeficienty α_i a vektor souřadnic značíme $[u]_B : p = (\alpha_1, \dots, \alpha_n)^T$

Pro každé $v \in \mathbb{R}^n$ je $[v]_{kan} = v$, u polynomů to jsou koeficienty, …

Pozorování

Ze systému generátorů V dostaneme vektor $u \in V$ alespoň jedním způsobem

Z lineárně nezávislých vektorů ve V dostaneme $u \in V$ nejvýše jedním způsobem

Z báze V dostaneme $u \in V$ právě jedním způsobem

Pro bázi B prostoru V nad $\mathbb{T}$ platí

$[u + v]_B = [u] + [v]_B$ $\qquad$ $[\alpha v]_B = \alpha [v]_B$

Důkaz: u a v vyjádříme jako lineární kombinaci a sumy sečteme

Násobek analogicky $\quad$ pozn. ještě to musíme rozepsat

Zobecnění: souřadnice lineární kombinace jsou rovny lineární kombinaci souřadnic

Každý vektorový prostor má bázi

Důkaz: Máme systém generátorů a buď nějaký vektor odstraníme nebo už to je báze

Navíc báze jednoho prostoru jsou stejně velké → pojem dimenze

Lemma o výměně: V systému generátorů, kterým můžu vyjádřit vektor x můžu libovolné y s nenulovým koeficientem v kombinaci nahradit vektorem x

Důkaz: $x = \sum_{k=1}^{n} \alpha_k y_k \to y_k = \frac{1}{\alpha_k}(x - \sum_{i \neq k} \alpha_i y_i)$ a potom libovolný vektor vyjádříme jako:

$\sum_{k=1}^{n} \beta_i y_i = \beta_k y_k + \sum_{i \neq k} \beta_i y_i = \frac{\beta_k}{\alpha_k}(x - \sum_{i \neq k} \alpha_i y_i) + \sum_{i \neq k} \beta_i y_i = \frac{\beta_k}{\alpha_k} x + \sum_{i \neq k} (\beta_i - \frac{\beta_k}{\alpha_k} \alpha_i)\, y_k$

Steinitzova věta o výměně:

Buď $x_1, \dots, x_m$ lineárně nezávislý systém v prostoru V a $y_1, \dots, y_n$ systém generátorů V

Pak platí, že $m \leq n$

Existují různé indexy $k_1, \dots, k_{n-m}$ takové, že $x_1, \dots, x_m, y_{k_1}, \dots, y_{k_{n-m}}$ generují V

Důkaz matematickou indukcí podle m. Triviálně $m = 0$, předpoklad: platí pro $m - 1$

Vektory $x_1, \dots, x_{m-1}$ jsou lineárně nezávislé a podle indukčního předpokladu existují indexy $\ell_1, \dots, \ell_{n-m+1}$, že vektory $x_1, \dots, y_{\ell_1}, \dots, y_{\ell_{n-m+1}}$ generují V

Kdyby $m - 1 = n$, pak ale $x_1, \dots, x_{m-1}$ generují V a tedy $x_m \in span\{x_1, \dots, x_{m-1}\} \rightarrow \perp$

Tím je dokázána první část $m \leq n$

Protože $x_1, \dots, x_{m-1}, y_{k_1}, \dots, y_{k_{n-m+1}}$ generují V, tak lze vyjádřit x_m jako kombinaci

$x_m = \sum_{i=1}^{m-1} \alpha_i x_i + \sum_{j=1}^{n-m+1} \beta_j y_{\ell_j}$ a nějaká nenulová β_k a y_k vyměním za x_m

Všechny báze konečného prostoru jsou stejně velké

Důkaz máme dvě báze a na ně dvakrát použijeme Steinitzovu větu $\rightarrow m \leq n$ a $m \geq n$

Dimenze

dim konečně generovaného prostoru je velikost nějaké báze, nekonečného ∞

1. m vektorů z V jsou lineárně nezávislé, pak $m \leq \dim V$ (pokud se rovnají tak báze)

2. pro n generátorů V platí $n \geq dimV$ (opět je to báze pokud se rovnají)

Důkaz 1. Podle St. věty můžeme doplnit o $d - m$ generátorů

2. Analogicky podle Steintzovy věty $n \geq d$.

když $n = d$, tak musí být báze, protože jinak $d \leq n - 1 \rightarrow \perp$

Každý lineárně nezávislý systém z V lze rozšířit na bázi V – St. věta a $d = \dim V$

Je-li W podprostorem V, tak $\dim W \leq \dim V$ (rovnost $\rightarrow W = V$)

Důkaz: vytvoříme prázdnou množinu M a pokud $span(M) = W$, tak hotovo

Jinak existuje vektor $v \in W \setminus span(M)$, přidáme ho do množiny M

Protože M je lineárně nezávislá, tak je velikost shora omezena $\dim V$

Spojení podprostorů $U + V = \{u + v, u \in U, v \in V\}$

$U + V = span(U \cup V)$

Důkaz: inkluze $\subseteq$ je triviální, protože $span(U \cup V)$ je uzavřený na součet

Pro druhou stačí ukázat, že $U + V$ obsahuje U, V a je podprostorem

Vyjádříme vektory a ukážeme uzavřenost

Pro spojení platí $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$

Důkaz: $U \cup V$ je podprostor W a má tedy konečnou bázi $z_1, \dots, z_p$

Tu můžeme rozšířit na bázi U $z_1, \dots, z_p, x_1, \dots, x_m$ a analogicky V

Ukážeme, že $z_1, \dots, z_p, x_1, \dots, x_m, y_1, \dots, y_n$ tvoří bázi $U + V$[1]

Direktní součet je pokud jsou podprostory disjunktní

[1] Já to neukážu, protože mi stačí jeden důkaz u tématu xd, ale je to na straně 90

Maticové prostory

Řádkový prostor matice

$\mathcal{S}(A) \coloneqq span\{A_{*1}, \dots, A_{*n}\}$

Sloupcový prostor matice

$\mathcal{R}(A) \coloneqq span\{A_{1*}, \dots, A_{m*}\}$ neboli $\mathcal{S}(A)^T$

Jádro matice

$Ker(A) \coloneqq \{x \in \mathbb{T}^n; Ax = o\}$

Je to podprostor $\mathbb{T}^n$ – splňuje to, že obsahuje nulový vektor ($Ao = o$) a je uzavřený

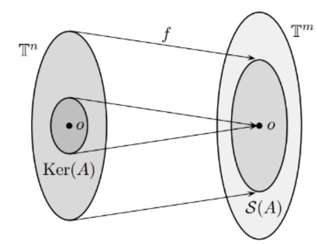
Tvrzení $\mathcal{S}(A) = \{Ax; x \in \mathbb{T}^n\}$ a obdobně pro $\mathcal{R}(A)$ dokážeme tím, že Ax představuje lin. kombinaci

Každý vektorový podprostor lze reprezentovat maticově

Stačí když generátory prostoru dáme do sloupců a řádků matice (jádro později)

Geometrický pohled na maticové prostory

Můžeme uvažovat zobrazení $x \mapsto Ax$…



Změna při násobení maticí zleva

$\mathcal{R}(QA)$ je podprostor $\mathcal{R}(A)$

Pokud $A_{*k} = \sum_{j \neq k} a_j A_{*j}$ pro nějaké… pak $(QA)_{*k} = \sum_{j \neq k} a_j (QA)_{*j}$

Důkaz: 1. pro každé $x \in \mathcal{R}(QA)$ existuje $y \in \mathbb{T}^p$, že $x = (QA)^T y = A^T(Q^T y) \in \mathcal{R}(A)$

2. $(QA)_{*k} = QA_{*k} = Q(\sum \dots) = \sum_{j \neq k} \alpha_j QA_{*j}$

Sloupcové prostory porovnatelné nejsou , ale zachovává se lineární závislost a koeficienty

Porovnatelné nejsou kvůli různým prostorům

Dá se to nahlídnout tak, že se všechny sloupce vynásobí maticí Q

Silnější tvrzení pokud násobíme regulární maticí zleva

$\mathcal{R}(QA) = \mathcal{R}(A)$

$A_{*k} = \sum_{j \neq k} a_j A_{*j}$ platí právě tehdy, když $(QA)_{*k} = \sum_{j \neq k} a_j (QA)_{*j}$

Důkaz: můžeme to ještě vynásobit Q^{-1}

Implikace zleva doprava už máme a zprava doleva je $Q^{-1}(QA)$

Sloupce zůstanou lineárně nezávislé

Pro $RREF(A)$

Nenulové řádky A^R tvoří bázi $\mathcal{R}(A)$ a sloupce $A_{*p_1}, \dots, A_{*p_r}$ tvoří bázi $\mathcal{S}(A)$

$\dim \mathcal{R}(A) = \dim \mathcal{S}(A) = r$

Důkaz: 1. $\mathcal{R}(A) = \mathcal{R}(QA) = \mathcal{R}(A^R)$

2. Sloupce jsou určitě lineárně nezávislé (přímo kanonické) a generují $\mathcal{S}(A^R)$

$A^R_{*j} = \sum_{i=1}^{m} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} A^R_{*p_i}$ **TODO**

3. Hodnota $\dim \mathcal{R}(A)$ je velikost báze $\mathcal{R}(A)$ a tedy r, obdobně $\mathcal{S}(A)$

Důsledek: $rank(A) = \dim \mathcal{R}(A) = \dim \mathcal{S}(A) = \dim \mathcal{R}(A^T) = rank(A^T)$

Frobeinova věta: Uvažujme $Ax = b$. Řešitelnost znamená, že vektor b se dá vyjádřit jako kombinace sloupců matice A. Soustava je tedy řešitelná právě tehdy, když $b \in \mathcal{S}(A)$ a to odpovídá $\mathcal{S}(A) = \mathcal{S}(A|b)$

Pro každou matici platí: $\dim Ker(A) + rank(A) = n$

Důkaz: buď $\dim Ker(A)$ = k, báze ker s vektory $v_1, \dots, v_k$ a tedy $Av_k = o$

Rozšiřme vektory na bázi celého $\mathbb{T}^n$. Stačí ukázat, že $Av_{k+1}, \dots, Av_n$ je báze $\mathcal{S}(A)$, protože potom $rank(A) = \dim \mathcal{S}(A) = n - k$

Generujícnost

$y \in \mathcal{S}(A)$ existuje $x \in \mathbb{T}^n$, že $y = Ax$, to se dá zapsat jako x…

Lineární nezávislost **TODO**

Geometrický pohled: čím větší jádro tím menší obraz

Lineární zobrazení

Základní vlastnosti

Zobrazení je lineární (neboli homomorfismus) pokud U, V prostory nad tělesem $\mathbb{T}$ a platí

$f(x+y) = f(x) + f(y) \qquad f(\alpha x) = \alpha f(x)$

Příklady v lineárních zobrazení v rovině pro $x \mapsto Ax$

$A = \begin{pmatrix} v_1 & 0 \\ 0 & v_2 \end{pmatrix}$ je škálování

$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ je rotace

Další maticové zobrazení překlopení, projekce

Další nematicové zobrazení např identita, počátek, transpozice

Vlastnosti zobrazení

$f(\sum_{i=1}^{n} \alpha_i x_i) = \sum_{i=1}^{n} \alpha_i f(x_i) \qquad f(o) = o$

Důkaz:

Rozšíření základní vlastnosti indukcí

$f(o) = f(0 \cdot o) = 0 \cdot f(o)$

Lineární zobrazení zobrazí lineární kombinaci vzorů na lineární kombinaci obrazů

Zachovává lineární závislost včetně koeficientů

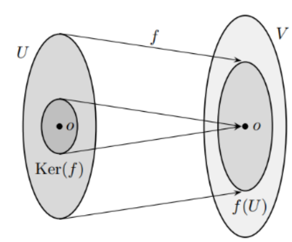
Zobrazuje přímku na přímku, bod na bod

Přímka určená dvěma vektory je množina vektorů $\lambda v_1 + (1-\lambda)v_2 \dots f(v_1) \dots$

Můžeme definovat obraz a jádro $U \mapsto V$

Obraz je $f(U) := \{f(x); x \in U\}$

Jádro je $f(U) := \{x \in U; f(x) = o\}$



Co znamená, když je jádro $\{o\}$, stejná dimenze, degenrace…

Jádro zobrazení souvisí s jádrem matice, …

1. $f(U) je\ podprostorem\ V$
2. $Ker(f) je\ podprostorem\ U$
3. Pro každé $x_1, \dots, x_n \in U\ platí\ f(span\{x_1, \dots, x_n\}) = span\{f(x)_1, \dots, f(x_n)\}$

Důkaz: 1. musí obsahovat nulový vektor a je uzavřený na součty a násobky

$f(o) = o \qquad f(u_1) = v_1, f(u_2) = v_2, f(u_1 + u_2) = \cdots = v_1 + v_2 \dots$

2. Analogicky

3. $\subseteq$ - každý vektor se dá vyjádřit jako $w = \sum \dots$ z linearity pak $f(w) \dots$

$\supseteq$ - $x_1, \dots \in W \to f(x_1, \dots) \in f(W)$ a $f(W)$ je podprostor a tedy má $span$

Z trojky plyne, že, že pro obraz podprostoru můžeme určit obrazy báze

Druhy zobrazení

„Na" – když pokryje celou množinu neboli $f(U) = V$

Zobrazení je tedy na, když se generátory zobrazí na generátory

Prosté znamená, že $f(x) = f(y)$ nastane jen pro $x = y$

Ekvivalentní, že $Ker(f) = \{o\}$ a že obraz lin. nezávislé množiny je lin. nezávislý

Důkaz: (řetěz implikací prosté ⇒ $Ker(f)$ ⇒ $lineární\ nezávislost$)

1 ⇒ 2: $f(o) = o$ a protože je prosté, tak jiný prvek neobsahuje

2 ⇒ 3: nechť $\sum_{i=1}^{n} \alpha_i f(x_i) = o$ a potom f($\sum \dots) = o$ a tedy …

3 ⇒ 1: sporem, předpokládejme, že $f(x) = f(y)$ a

potom $f(x) - f(y) = o = f(x - y)$ tedy … $x - y = o \to \perp$

Bod 3 navíc říká, že prosté zobrazení zobrazuje bázi na bázi a tedy

$$\dim U = \dim\ f(U)$$

Prosté mimochodem nemusí být na

Reprezentace zobrazení

A) Obraz báze

Důkaz existence a jednoznačnosti:

$f(x) = f(\sum_{i=1}^{n} \alpha_i x_i) = \sum_{i=1}^{n} \alpha_i f(x_i) = \sum_{i=1}^{n} \alpha_i y_i$, linearita snadno

Pro spor $f(x_i) = g(x_i) = y_i$

$f(x) = \sum_{i=1}^{n} \alpha_i y_i = \sum_{i=1}^{n} \alpha_i g(x_i) = g(x)$

B) Matice

Vytvoření: zjisti kam se zobrazí kanonická báze a dát do sloupců

Opačný směr dokazuje, že každé lineární zobrazení jde reprezentovat maticí

$f(x) = f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i f(e_i)$ a pak tedy $f(x) = Ax$

To můžeme udělat i s $U \to \mathbb{T}^n$ a potom $f(x) = A \cdot [x]_B$

Zároveň můžeme změnit i druhý prostor

Musíme pracovat v souřadnicích

Matice lineárního zobrazení

Buď lineární zobrazení $U \to V$, báze prostoru, …

Nechť $f(x_j) = f(\sum_{i=1}^{m} a_{ij} y_i)$, potom matice s prvky a_{ij} je matice lineárního zobrazení vzhledem k bázím a značí se ${}_{B_V}[f]_{B_U}$

$$ {}_{B_V}[f]_{B_U} = \begin{pmatrix} | & & | \\ [f(x_1)]_{B_V} & \cdots & [f(x_n)]_{B_V} \\ | & & | \end{pmatrix} $$

Mnemotechnicky je na vstupu vektor souřadnic vzhledem k B_U a na výstupu k B_V

Platí také $[f(x)]_{B_V} = {}_{BV}[f]_{B_U} \cdot [x]_{B_U}$ (získání souřadnic obrazu ze souřadnic x)

Důkaz: **TODO: proč $f(x_j)$ můžeme vyjádřit takhle**

$$ f(x) = f\left(\sum_{j=1}^{n} \alpha_j x_j\right) = \sum_{j=1}^{n} \alpha_j f(x_j) = \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{m} a_{ij} y_i\right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_j a_{ij}\right) y_i $$

A tedy i-tá souřadnice $f(x)$ je $\sum_{j=1}^{n} \alpha_j a_{ij} = \left(A \cdot [x]_{B_U}\right)_i$

Důsledek: každé zobrazení se dá vyjádřit jako $f(x) = Ax$

Důkaz:

$f(x) = [f(x)]_{kan} = {}_{kan}[f]_{kan} \cdot [x]_{kan} = {}_{kan}[f]_{kan} \cdot x$

Tedy $f(x) = Ax$, kde $A = {}_{kan}[f]_{kan}$

Jednoznačnost matice

$A = {}_{B_V}[f]_{B_U}$ je jediná matice, která splňuje $[f(x)]_{B_V} = A \cdot [x]_{B_U}$

Sporem: různé matice $A \neq A'$ a tedy existuje vektor s takový, že $As \neq A's$

Definujme $x \coloneqq \sum_{i=1}^{n} s_i z_i$ a potom $[f(x)]_{B_V} = As \neq A's = [f(x)]_{B_V}$

Tedy každé lin. zobrazení lze reprezentovat maticí a každá matice reprezentuje zobrazení

Matice přechodu ${}_{B_2}[id]_{B_1}$ a pak $[x]_{B_2} = {}_{B_2}[id]_{B_1} \cdot [x]_{B_1}$

Složené a inverzní lineární zobrazení a jejich matice

Složené zobrazení

Definice, …

Složení lin. zobrazení je opět lineární

Důkaz je ez

Maticová reprezentace je akorát vynásobení

Věta ${}_{B_W}[g \circ f]_{B_U} = {}_{B_W}[g]_{B_V} \cdot {}_{B_V}[f]_{B_U}$

Důkaz:

$[(g \circ f)(x)]_{B_W} = {}_{B_W}[g]_{B_V} \cdot [f(x)]_{B_V} = {}_{B_W}[g]_{B_V} \cdot {}_{B_V}[f]_{B_U} \cdot [x]_{B_U}$

Matice zobrazení při změně báze: ${}_{B_4}[id]_{B_2} \cdot {}_{B_2}[f]_{B_1} \cdot {}_{B_1}[id]_{B_3}$

(z ${}_{B_2}[f]_{B_1}$ do ${}_{B_4}[f]_{B_3}$

Isomorfismus

Prostý a na

Příkladem je škálování, překlápění nebo otáčení

Vlastnosti

Pro každý isomorfismus existuje isomorfní inverze

Složení isomorfismů je také isomorfismus

Lin. zobrazení je isomorfismus právě, když se báze zobrazí na bázi

Prostory v isomorfním zobrazení mají stejnou dimenzi

Důkazy

1. f je vzájemně jednoznačné a tedy existuje i jednoznačné f^{-1}

Musíme ale dokázat linearitu $f^{-1}(v_1) = u_1$ a $f^{-1}(v_2) = u_2$

$f^{-1}(v_1 + v_2) = u_1 + u_2 = f^{-1}(v_1) + f^{-1}(v_2)$…

2. je vzájemně jednoznačné a linearita plyne ze skládání

3. „⇒“ f je prosté a tedy f(báze) jsou nezávislé a je „na“…

„⇐“ je „na“ protože generuje a prosté sporem:

Obsahuje nenulové vektory v jádru $f(\sum_{i=1}^{n} \alpha_i x_i) = o$

A tedy $\sum_{i=1}^{n} \alpha_i f(x_i) = o \to \perp$

4. Plyne ze 3.

Tvrzení ${}_{B_U}[f^{-1}]_{B_V} = {}_{B_V}[f]_{B_U}^{-1}$

Důkaz: protože $f^{-1} \circ f = id$, tak ${}_{B_U}[f^{-1}]_{B_V} \cdot {}_{B_V}[f]_{B_U} = {}_{B_U}[f^{-1} \circ f]_{B_U} = I$

Navíc musí platit, že matice je čtvercová, protože isomorfismus

Matice isomorfismu musí být regulární, protože má inverzi a naopak

Z toho také plyne, že ${}_{B_U}[id]_{B_V} = {}_{B_V}[id]_{B_U}^{-1}$

Pozn. Matice přechodu se dají snadno počítat:

$(\mathcal{B}_v \mid \mathcal{B}_u) \sim (I_n \mid {}_{B_V}[id]_{B_U})$

Důkaz:

Víme: $\mathcal{B}_u = {}_{kan}[id]_{B_U} \cdot \mathcal{B}_v = {}_{kan}[id]_{B_V}$

a taky: ${}_{B_W}[g \circ f]_{B_U} = {}_{B_W}[g]_{B_V} \cdot {}_{B_V}[f]_{B_U}$

Tedy ${}_{B_V}[id]_{B_U} = {}_{B_V}[id]_{kan} \cdot {}_{kan}[id]_{B_U} = {}_{kan}[id]_{BV}^{-1} \cdot {}_{kan}[id]_{B_U}$

$\mathcal{B}_v^{-1} \cdot (\mathcal{B}_v \mid \mathcal{B}_u) = (I_n \mid {}_{B_V}[id]_{B_U})$

Tvrzení: mezi prostory, které mají stejnou dimenzi existuje isomorfismus, formálněji:

Máme prostor s dimenzí n a bází B, potom zobrazení $x \to [x]_B$ je isomorfismus mezi V a $\mathbb{T}^n$

Důkaz:

$x \to [x]_B$ je lineární – rozepsat na sumy a ukázat, že $[x+y]_B = [x]_B + [y]_B$…

Zobrazení je prosté z jednoznačnosti souřadnic

Zobrazení je na, protože …

Má důsledek, že všechny n-dimenzionální vektorové prostory nad $\mathbb{T}$ jsou isomorfní

Věta o dimenzi a jádru:

Pro $\mathbb{R}$ se dá říct, že $Ker(f) = Ker(A)$, $f(\mathbb{R}^n) = \mathcal{S}(A)$

Obecněji:

$\dim Ker(f) = \dim Ker(A)$

$\dim f(U) = \dim \mathcal{S}(A) = rank(A)$

Důkaz:

1. Ukážeme, že $x \in Ker(f) \mapsto [x]_{B_U}$ je isomorfismus mezi $Ker\ f$ a A

   Víme, že je lineární a prosté

   „na“: $o = [o]_{B_V} = [f(x)]_{B_V} = {}_{B_V}[f]_{B_U} \cdot [x]_{B_U}$ a obráceně

2. Opět sestrojíme isomorfismus, tentokrát mezi $f(U)$ a $\mathcal{S}(A)$

   TODO

Díky tomu víme jak najít bázi jádra a obrazu

Důsledek: $\dim U = \dim Ker(f) + \dim f(U)$

Důkaz:

Víme, že $n = \dim Ker(A) + rank(A)$ a pro $A = {}_{B_V}[f]_{B_U}$:

$n = \dim U$, $\dim Ker(f) = \dim Ker(A)$ a $\dim f(U) = rank(A)$

f je prosté právě, když ${}_{B_V}[f]_{B_U}$ má lineárně nezávislé sloupce

$Ker(f) = \{o\} \Leftrightarrow \dim U = \dim f(U) \Leftrightarrow n = rank(A)$

f je „na“ právě, když ${}_{B_V}[f]_{B_U}$ má lineárně nezávislé řádky

$\dim V = \dim f(U) \Leftrightarrow m = rank(A)$

Prostor lineárních zobrazení

Množina lineárních zobrazení tvoří vektorový prostor

Můžu je sčítat, násobit skalárem, má nulový vektor, …

Isomorfní s prostorem matic $\mathbb{T}^{m \times n}$

$f \mapsto {}_{B_V}[f]_{B_U}$ to snadno ověřím, že je lineární

Kdybych si vytáhl tohle tak musím mluvit hlavně o zobrazení

Afinní prostory

Afinní podprostor nemusí obsahovat počátek

Formálně to je množina vektorů $M = U + a = \{u + a; u \in U\}$

U je určené jednoznačně, vektor může být různý

Vektorový podprostor nebo vektor jsou také afinní podprostory

Dláždění afinními prostory

Vektorové podprostory jsou uzavřené na afinní kombinace

$y + \alpha(x - y), \alpha \in \mathbb{R}$ je přímka

Formálně afinní kombinace dvou vektorů $x, y \in V$ je $\alpha x + (1 - \alpha)y$

Vektorový prostor různé charakteristiky od 2 a $\emptyset = M \subseteq V$. Pokud pro všechny $x, y \in M$ platí, že $\alpha x + (1 - \alpha)y \in M$, tak je to afinní podprostor

Důkaz:

„⇒“: Nechť $M = U + a$, tedy $x = u + a$ a $y = v + a$ potom:

$\alpha x + (1 - \alpha)y = \alpha(u + a) + (1 - \alpha)(v + a) = \alpha u + (1 - \alpha)v + a \in U + a = M$

„⇐“: zvolme $a \in M$ a $U \coloneqq M - a = \{x - a; x \in M\}$

Musíme zjistit, že U je podprostor, nulový je zřejmý a zjistíme uzavřenost:

$\alpha u = \alpha(x - a) = (\alpha x + (1 - a)a) - a \in M - a$

$u + u' = (x - a) + (x' - a) = (x + x' - a) - a$

Stačí ukázat, že $x + x' - a \in M$

$\frac{1}{2}x + \frac{1}{2}x' \in M$, z toho vyjádřím afinní kombinaci

Afinní kombinace n vektorů

$\sum_{i=1}^{n} \alpha_i x_i$ a $\sum_{i=1}^{n} \alpha_i = 1$

Pro $n = 3$ vytvoříme roviny

Pomyslně můžeme zavést afinní obal

Tvrzení: M je afinní podprostor ⇔ M je uzavřené na afinní kombinace

Věta: množina řešení $Ax = b$ je prázdná nebo afinní

Je-li neprázdná tak $Ker(A) + x_0$ s libovolným řešením

Důkaz:

$x_1 = x_1 - x_0 + x_0$ a dosazením $A(x_1 - x_0) = b - b = o$

Naopak $x_2 + x_0$ je řešením soustavy, protože $A(x_2 + x_0) = o$

Každý afinní podprostor lze popsat i pomocí soustavy rovnic

Poznámka, když změníme pravou stranu, tak buď řešení přestane existovat nebo ${x'}_0$

Dimenze afinního podprostoru $M = U + a$ je definována jako $\dim(M) \coloneqq \dim(U)$

Můžeme definovat přímku jako afinní podprostor dimenze jedna

Nadrovinu jako afinní podprostor dimenze – 1

Množina řešení tvoří afinní podprostor dimenze $n - rank(A)$ (tedy dimenze jádra)

Afinní nezávislost

Minimální množina generátorů afinního podprostoru

Vektory jsou afinně nezávislé pokud jsou $x_1 - x_0, x_2 - x_0, \dots$ nezávisůé

Tři body na přímce jsou afinně závislé

Body v obecné poloze

$x_1, \dots \in \mathbb{R}^n$ jsou v o. p. pokud každá podmnožina velikosti $n + 1$ je nezávislá

Souřadnice v afinním podprostoru, vztah podprostorů, …

Afinní zobrazení

$f(u) = g(u) + b$

Obraz afinního podprostoru je afinní podprostor

Složením dvou afinních zobrazení dostaneme opět afinní zobrazení

Úplný vzor

Množina bodů, které se zobrazí na vektor, formálně $f^{-1}(v) \coloneqq \{u \in U; f(u) = v\}$

je buď prázdná množina nebo podprostor

Důkaz:

$f(\sum_{i=1}^{n} \alpha_i u_i) = \cdots = \sum_{i=1}^{n} \alpha_i v = v$

Je uzavřená na afinní kombinace

Řešit soustavu znamená najít úplný vzor vektoru b

Přehled témat ke zkoušce?

A co k nim zhruba chci říct

- Soustavy lineárních rovnic: řešení a řešitelnost
  - Jak vypadá soustava rovnic, (koeficienty a neznámé), geometrický náhled
  - Množina řešení soustavy je afinní podprostor a naopak s důkazem, najít úplný vzor
- Elementární řádkové úpravy
  - Zachovají množinu řešení – reprezentace regulární maticí a tedy mají inverzi, elementarita
  - Důkazy $RREF(A) = QA$ a Q regulární, regulární lze vyjádřit E
- Redukovaný odstupňovaný tvar matice RREF
  - Úvod k soustavě rovnic, popis tvaru – pivoty, …
  - Kratší důkazy u počtu řešení soustavy, jednoznačnost RREF
- Hodnost matice
  - Jak zjistit – počet nenulových řádků, počet pivotů, že to odpovídá dimenzi, $rank(A^T)$
  - Frobeinova věta, u regulární = n, rank = dim $\mathcal{S}(A)$ = dim $f(U)$ = dim $\mathscr{R}(A)$
  - Důkaz: $rank(A) = rank(A^T)$
- Základní operace s maticemi a jejich vlastnosti
  - $=, +$, násobení skalárem, součin matic – skládání, vlastnosti, transpozice, vlastnosti transpozice, součin vektorů
  - Důkazy vlastností
- Regulární matice
  - $Ax = b$, $RREF = I_n$, $rank(A) = n$, vlastnosti, má inverzi, odpovídá nějakému isomorfismu, uzavřené na součin, ale ne na součet
  - Důkaz: součin je regulární, singulární, …
- Inverzní matice
  - Jen u regulární, odpovídá inverznímu zobrazení, jak vypočítat, jedinečnost, její regularita
  - Důkazy: existence, jednoznačnost, transponovaná, jedna rovnost stačí

Navíc k těmto tématům:

Matice - definice, vlastnosti, druhy, operace, vektory, *, rozšířená matice, elementární řádkové úpravy, REF, RREF, reprezentace zobrazení, maticové prostory

Řešení soustavy – je to vektor, Gaussova eliminace, G-J eliminace, algoritmus, počet řešení

Průřez – lineární kombinace sloupců matice je řešení (Frobeinova věta)

- Grupy (bez permutací)

  Definice, vlastnosti, Abelova grupa, vlastnosti s důkazy, podgrupa

  Důkazy vlastností
- Permutace

  Symetrická grupa, bijekce, skládání, inverze, sgn, transpozice, počet inverzí,

  Důkazy: sgn složení transpozice, rozložení na transpozice, znaménka inverzí
- Tělesa

  Definice, vlastnosti, konečná tělesa, charakteristika, malá Fermatova věta

  Důkaz: vlastnosti, $\mathbb{Z}_n$, Fermat
- Vektorový prostor a podprostor

  Definice, vlastnosti, podprostory, průniky, lineární obal, generátor

  Důkaz: vlastnosti, generace obalu
- Lineární kombinace

  Definice, generace obalu, řešení rovnice

  Důkaz: generace obalu
- Lineární závislost a nezávislost

  Znamená, změna span, Věta o výměně, Steinzova věta, suma = u, (2x) nezmenšení span
- Lineární obal

  Definice, …

  Důkaz span = span
- Báze

  Definice, kanonická, jednoznačná, souřadnice, pozorování, každý má bázi

  Důkaz: Steintzova věta o výměně, stejná velikost bází,
- Dimenze

  Velikost báze, struktura podprostorů, spojení, průnik, podprostor, dimenze spojení

  Důkaz: Steintzova věta o výměně, stejná velikost bází,

- Řádkový a sloupcový prostor matice
  - Definice – span, reprezentace prostorů, zobrazení – geometrický pohled, násobení
  - Důkaz: změna při násobení zleva, R(A) = R(QA), dim R(A) = dim S(A)
- Jádro matice
  - Definice, ker(A) = {Ax…}, je to podprostor, dimenze?, degenerovanost
  - Důkaz: dim Ker(f) = dim Ker(A) isomorfismus
- Lineární zobrazení a základní vlastnosti
  - Přímka na přímku nebo na bod, f(o), suma, jedno zobrazení x na y
- Obraz lineárního zobrazení.
  - Množina všech f(x)
  - Patří do U, f(span) = span(f),
- Jádro lineárního zobrazení
  - Množina všech x
  - f(U), Ker(fNa – generátory na generátory
- Prosté lineární zobrazení
  - prosté x=y, ker o, nezávislé je nezávislý, řetěz implikací, nezávislé sloupce,
- Maticová reprezentace lineárního zobrazení
  - Reprezentace obraz nebo jako matice, kam se zobrazí kanonická a dáme do sloupců, jedinečnost matice, zobrazování souřadnic, …
- Složené a inverzní lineární zobrazení a jejich matice
  - Skládání odpovídá násobení, opět lineární s důkazem, …
- Isomorfismus
  - Definice, má inverzi, složení, báze se zobrazuje na bázi, dim U = dim V s dúkazy
- Prostor lineárních zobrazení
  - Sčítání matice, násobení matic skalárem, lineární forma, duální prostor
- Afinní prostory
  - Definice, jednoznačnost, afinní kombinace, uzavřenost na ně, afinní nezávislost, zobrazení, úplný vzor