

If the mathematic is not yet useful, it should at least be beautiful.

Albrecht Pietsch, Jena

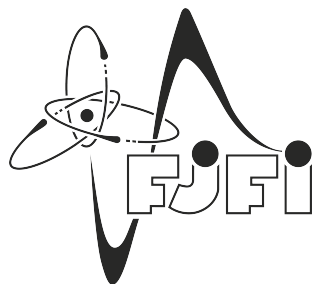
Mathematics has advanced a bit since the time of Euclid.

Terence Tao, UCLA

Matematické miniatury

Jan Vybíral

Katedra matematiky
Fakulta jaderná a fyzikálně inženýrská
České vysoké učení technické v Praze



Věnováno památce Jiřího Matouška

Následující text vznikl jako doplněk k základním kurzům matematiky přednášeným v Čechách a na Moravě. Hlavní cíle celého tohoto spisku jsou ve zkratce následující:

- Ukázat studentům, že základní kurz matematiky není jen o Dirichletově kritériu a Eulerově substituci, ale že má úzkou souvislost i s moderními partiemi teoretické i aplikované matematiky.
- Ukázat studentům, že jednotlivé obory matematiky spolu úzce souvisejí. Tedy, že řadu výsledků v analýze dostaneme nejjednodušeji pomocí statistiky, že analýza je základním nástrojem numeriky, a že všechny tyto směry je třeba správně skloubit, když dojde na aplikovanou matematiku.

Pokud se tento text dostane do ruky studentům se zájmem o některé z téma zde zpracovaných, neváhejte se na mě obrátit!

Pokud se tento text dostane do ruky komukoliv, kdo bude znát nějaké jiné vhodné téma, dejte mi prosím vědet!

Obsah

1	Rychlá Fourierova transformace (FFT)	6
2	Pronyho metoda & Lasso	9
3	Metoda nejmenších čtverců	13
4	Khintchinovy nerovnosti	16
5	Diskrepance	21
6	Objem jednotkové koule - klasicky a moderně	26
7	Koncentrace míry a Johnson-Lindenstraussovo vnoření	31
8	Geometrické nerovnosti	36
9	Disperze	39
10	Maticové normy: Spektrální, Frobeniova a nukleární	43
11	Náhodná procházka v obecné dimenzi	47
12	Support Vector Machines	51
13	Principal Component Analysis	56
14	Princip neurčitosti	60
15	Náhodné algoritmy	64
16	Laplacův operátor	69
17	Atom vodíku	75
18	Entropy numbers	80
	18.1 Preparations	82
	18.2 Proof of Theorem 18.2	87
	18.3 Extensions	92
	18.4 Alternative use of volume arguments	92
	18.5 Alternative use of combinatorial arguments	93
	18.6 Complex spaces	93
19	Carl-Triebelova nerovnost	97
20	=====	100
21	Cauchy-Schwartz pro Riemannův integrál	101

22 Bochnerova věta - jednoduchá část	102
23 =====	103
24 Fourierova transformace - 0/5	104
25 Approximační a další čísla - 0/5	105
26 Other topics:	106
27 PageRank	107
28 Shannon's theorem	108
29 Monte Carlo - 4. semestr (?) - 0/5	109
30 Numerická integrace - u Riemannova integrálu - 2.-3. semestr - 0/5	110

1 Rychlá Fourierova transformace (FFT)

Nechť \mathbb{Z}_N je množina N -tých odmocnin jedničky v oboru komplexních čísel, tedy

$$\mathbb{Z}_N = \{1, e^{2\pi i/N}, e^{2 \cdot 2\pi i/N}, \dots, e^{(N-1) \cdot 2\pi i/N}\}.$$

Pak \mathbb{Z}_N s obvyklým násobením komplexních čísel je Abelovská (tedy komutativní) grupa. Dále je \mathbb{Z}_N isomorfní s množinou $\{0, 1, \dots, N-1\}$ vybavenou sumací modulo N . A dále je isomorfní s $\mathbb{Z}/N\mathbb{Z}$, množině tříd ekvivalence celých čísel definovaných pomocí zbytku při dělení N .

Definujeme vektory $e_l \in \mathbb{C}^N$ s komponentami $e_l(k), k = 0, \dots, N-1$

$$e_l(k) = e^{2\pi i l k / N} \quad \text{pro } l = 0, 1, \dots, N-1 \text{ a } k = 0, 1, \dots, N-1.$$

Stejně tak je možné se na dívat na e_l jako na funkce $e_l : \{0, 1, \dots, N-1\} \rightarrow \mathbb{C}$. Konečně označíme V vektorový prostor komplexních funkcí na $\{0, 1, \dots, N-1\}$ se skalárním součinem

$$\langle F, G \rangle_V = \sum_{k=0}^{N-1} F(k) \overline{G(k)},$$

a normou

$$\|F\|_V^2 = \sum_{k=0}^{N-1} |F(k)|^2.$$

Jednoduchý výpočet dává

Lemma 1.1. *Pro $0 \leq l, m \leq N-1$ platí*

$$\langle e_l, e_m \rangle_V = N \cdot \delta_{m,l} = \begin{cases} N & \text{pro } l = m, \\ 0 & \text{jinak.} \end{cases}.$$

Vektory $e_l^* = e_l / \sqrt{N}, l = 0, 1, \dots, N-1$, tvoří tedy ortonormální bázi V . Pro každé $F \in V$ tedy dostaneme

$$F = \sum_{n=0}^{N-1} \langle F, e_n^* \rangle_V e_n^*,$$

$$\|F\|^2 = \sum_{n=0}^{N-1} |\langle F, e_n^* \rangle_V|^2.$$

Pro $n \in \mathbb{Z}$ definujeme n -tý Fourierův koeficient F jako

$$a_n = \hat{F}(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) e^{-2\pi i k n / N} = \frac{1}{\sqrt{N}} \langle F, e_n^* \rangle.$$

Věta 1.2. *Pro $F \in V$ máme*

$$F(k) = \sum_{n=0}^{N-1} \langle F, e_n^* \rangle_V e_n^*(k) = \sum_{n=0}^{N-1} \sqrt{N} a_n e_n^*(k) = \sum_{n=0}^{N-1} a_n e_n(k) = \sum_{n=0}^{N-1} a_n e^{2\pi i n k / N},$$

$$\sum_{n=0}^{N-1} |a_n|^2 = \frac{1}{N} \sum_{n=0}^{N-1} |\langle F, e_n^* \rangle_V|^2 = \frac{1}{N} \|F\|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2.$$

Naivní způsob výpočtu $\hat{F}(0), \dots, \hat{F}(N-1)$ pro dané $F(0), \dots, F(N-1)$ a $\omega_N = e^{-2\pi i/N}$ je

$$a_k^N(F) := \frac{1}{N} \sum_{r=0}^{N-1} F(r) \omega_N^{kr}.$$

Zahrnuje tedy $N-2$ multiplikací vedoucí k $\omega_N^2, \dots, \omega_N^{N-1}$ a každé a_k^N vyžaduje $N+1$ multiplikací a $N-1$ součtů. Celkem tedy potřebujeme $2N^2 + N - 2 \leq 2N^2 + N$ operací. .

Věta 1.3. (Fast Fourier Transform) *Pro dané $\omega_N = e^{-2\pi i/N}$ s $N = 2^n$ potřebujeme nejvýše*

$$4 \cdot 2^n \cdot n = 4N \log_2(N) = O(N \log N)$$

operací k výpočtu všech Fourierových koeficientů F .

Důkaz. Nechť $\#(M)$ je minimální počet operací potřebných k výpočtu všech Fourierových koeficientů na \mathbb{Z}_M . Tvrdíme, že platí

$$\#(2M) \leq 2\#(M) + 8M$$

pokud $\omega_{2M} = e^{-2\pi i/(2M)}$ je dáno.

Použitím tohoto tvrzení lze již větu snadno dokázat indukcí. Pro $N = 2^1 = 2$ potřebujeme jistě méně než 8 operací, abychom vypočetli

$$a_0^N(F) = 1/2(F(1) + F(-1)), \quad a_1^N(F) = 1/2(F(1) - F(-1)).$$

Pokud věta platí pro $N = 2^{n-1}$, pak dostaneme

$$\#(2N) \leq 2 \cdot 4 \cdot 2^{n-1}(n-1) + 8 \cdot 2^{n-1} = 8n2^{n-1} = 4n2^n.$$

Důkaz tvrzení:

Potřebujeme nejvýše $2M$ operací, abychom získali $\omega_{2M}^2, \dots, \omega_{2M}^{2M-1}$. Dále, pro F definovanou na \mathbb{Z}_{2M} , uvažujeme F_0 a F_1 definované na \mathbb{Z}_M , které jsou zadány pomocí $F_0(r) = F(2r)$ a $F_1(r) = F(2r+1)$. Předpokládáme dále, že jsme schonpni jejich vypočítat jejich Fourierovy koeficienty (na \mathbb{Z}_M) v $\#(M)$ operacích.

Tvrzení pak plyne z následujícího výpočtu ($0 \leq k \leq 2M-1$)¹

$$\begin{aligned} a_k^{2M}(F) &= \frac{1}{2M} \sum_{r=0}^{2M-1} F(r) \omega_{2M}^{kr} = \frac{1}{2} \left(\frac{1}{M} \sum_{l=0}^{M-1} F(2l) \omega_{2M}^{k(2l)} + \frac{1}{M} \sum_{m=0}^{M-1} F(2m+1) \omega_{2M}^{k(2m+1)} \right) \\ &= \frac{1}{2} \left(\frac{1}{M} \sum_{l=0}^{M-1} F_0(l) \omega_M^{kl} + \frac{1}{M} \sum_{m=0}^{M-1} F_1(m) \omega_M^{km} \omega_{2M}^k \right) \\ &= \frac{1}{2} \left(a_k^M(F_0) + a_k^M(F_1) \omega_{2M}^k \right). \end{aligned}$$

□

¹Všimněte si, že $a_k^M(F_0) = a_{k-M}^M(F_0)$ pro $k \geq M$.

Cvičení:

1. Jiná forma téhož definuje *Diskrétní Fourierovu Transformaci (DFT)* $\mathcal{F}x$ signálu $x \in \mathbb{C}^N$ jako

$$\mathcal{F}x := \mathbb{F}_N x,$$

kde \mathbb{F}_N je N -dimenzionální *Fourierova matice*

$$\mathbb{F}_N = (e^{-2\pi i k \ell / N})_{k, \ell = 0, \dots, N-1}.$$

2. Rozmyslete si, že jsme již vlastně dokázali, že $\frac{1}{\sqrt{N}} \cdot \mathbb{F}_N$ je unitární matice, a že tedy

$$\mathbb{F}_N^{-1} = \frac{1}{N} (e^{2\pi i k \ell / N})_{k, \ell = 0, \dots, N-1}.$$

3. *Cyklická konvoluce* $x * y \in \mathbb{C}^N$ signálů $x, y \in \mathbb{C}^N$ nad \mathbb{Z}_N je definována jako

$$(x * y)_k := \sum_{\ell=0}^{N-1} x_{(k-\ell) \bmod N} y_\ell, \quad k \in \mathbb{Z}_N = \{0, \dots, N-1\}.$$

4. Dokažte, že platí

$$\mathcal{F}(x * y) = (\mathcal{F}x) \cdot (\mathcal{F}y),$$

kde “ \cdot ” je bodový součin dvou vektorů.

5. Odvoďte vzorce pro DFT shiftu a modulace daného vektoru, tedy pro

$$\mathcal{F}(\{x_n e^{2\pi i \frac{nm}{N}}\}) \quad \text{a} \quad \mathcal{F}(\{x_{n-m}\}).$$

6. Dokažte, že

$$\left(\frac{1}{\sqrt{N}} \mathbb{F}_N \right)^4 = Id,$$

a že tedy vlastní čísla matice $\frac{1}{\sqrt{N}} \mathbb{F}_N$ leží v množině $\{\pm 1, \pm i\}$.

7. Cooley–Tukey FFT algorithm: Zkuste si rozmyslet, že popsany algoritmus pro FFT lze použít i pro libovolnou faktorizaci $N = N_1 N_2$, kde není nutné, aby N_1 nebo N_2 bylo rovno dvěma.

2 Pronyho metoda & Lasso

Pronyho metoda (vyvinutá Gaspardem Riche de Prony v roce 1795) se dá přeformulovat jako metoda řešení podurčených soustav lineárních rovnic $Ax = y$, kde $A \in \mathbb{R}^{2s \times N}$, $y \in \mathbb{R}^{2s}$ a $x \in \mathbb{R}^N$ je s -sparse, tedy má nejvýše s nenulových koeficientů. Matice A bude prvních $2s$ řádků diskrétní Fourierovy transformace. Proto se nám bude hodit následující lemma.

Lemma 2.1. *Nechť $z \in \mathbb{C}^N$ má nejvýše s nenulových souřadnic, tedy $\#\text{supp}(z) \leq s$. Nechť dále $\hat{z}(k) = 0$ pro s po sobě jdoucích indexů $k \in \{0, 1, \dots, N-1\}$. Pak $z = 0$.*

Důkaz. Položme $S := \text{supp}(z)$ a předpokládejme, že existuje $t \in \{0, 1, \dots, N-1\}$ tak, že platí

$$0 = \hat{z}(k) = \sum_{l=0}^{N-1} e^{-2\pi i \frac{kl}{N}} z(l) = \sum_{l \in S} e^{-2\pi i \frac{kl}{N}} z(l) \quad \text{pro } k = t, t+1, \dots, t+s-1.$$

Tedy i

$$0 = \sum_{l \in S} e^{-2\pi i \frac{(t+j)l}{N}} z(l) = \sum_{l \in S} e^{-2\pi i \frac{jl}{N}} e^{-2\pi i \frac{tl}{N}} z(l) \quad \text{pro } j = 0, 1, \dots, s-1.$$

Definujeme-li tedy vektor $w(l) = e^{-2\pi i \frac{tl}{N}} z(l)$ pro $l \in S$ a nula jinak, je

$$0 = \sum_{l \in S} \left(e^{-2\pi i \frac{jl}{N}} \right)^j w(l) \quad \text{pro } j = 0, 1, \dots, s-1.$$

Protože daná soustava rovnic odpovídá Vandemondově soustavě a je regulární, je $w = 0$, a tedy i $z = 0$. \square

Pronyho metoda pak říká, že s -sparse vektory lze najít pomocí jejich prvních $2s$ Fourierových koeficientů.

Věta 2.2. *Pro všechna přirozená čísla $N \geq 2s$ existuje konstruktivní způsob, jak z prvních $m = 2s$ koeficientů diskrétní Fourierovy transformace zrekonstruovat libovolný s -sparse vektor.*

Důkaz. Nechť $x \in \mathbb{C}^N$ je s -sparse vektor, který budeme interpretovat jako funkci definovanou na množině $\{0, 1, \dots, N-1\}$ s nosičem S o nejvýše s prvích. Předpokládáme, že prvních $2s$ Fourierových koeficientů $\hat{x}(0), \hat{x}(1), \dots, \hat{x}(2s-1)$ je dáno, kde

$$y(j) = \hat{x}(j) = \sum_{k=0}^{N-1} x(k) e^{-2\pi i jk/N}, \quad 0 \leq j \leq 2s-1.$$

Nejprve popíšeme Pronyho algoritmus, a posléze dokážeme, že skutečně najde to, co má.

Algoritmus:

- Najdeme libovolné řešení soustavy²

$$\begin{pmatrix} y(s-1) & + & \dots & + & y(0) \\ y(s) & + & \dots & + & y(1) \\ \vdots & & \ddots & & \vdots \\ y(2s-2) & + & \dots & + & y(s-1) \end{pmatrix} \begin{pmatrix} z(1) \\ z(2) \\ \vdots \\ z(s) \end{pmatrix} = - \begin{pmatrix} y(s) \\ y(s+1) \\ \vdots \\ y(2s-1) \end{pmatrix}. \quad (2.1)$$

²Později dokážeme, že daná soustava má vždy alespoň jedno řešení.

- Dále položíme $z(0) = 1, z(s+1) = \dots = z(N-1) = 0$.
- Pak $S := \text{supp}(x) \subset \tilde{S} := (\text{supp } z^\vee)^c$ a $\#\tilde{S} \leq s$.
- Odtud již pak snadno dopočteme x jako řešení přeurčeného systému $2s$ rovnic o s neznámých

$$y(j) = \sum_{k \in \tilde{S}} x(k) e^{-2\pi i \frac{jk}{N}}, \quad j = 0, \dots, 2s-1.$$

1. *krok*: Existence řešení (2.1):

Soustavu (2.1) řeší například Fourierova transformace trigonometrického polynomu (=vektoru)

$$p(t) := \frac{1}{N} \prod_{k \in S} (1 - e^{-2\pi i k/N} e^{2\pi i t/N}), \quad 0 \leq t \leq N-1. \quad (2.2)$$

Zřejmě $p(t) = 0$, právě když se v součinu v (2.2) někde vyskytuje nula, a tedy právě tehdy, pokud $t \in S$. Proto je tedy $p(t) \cdot x(t) = (p \cdot x)(t) = 0$ pro všechna $0 \leq t \leq N-1$. Protože $\hat{p} * \hat{x} = \widehat{p \cdot x} = 0$, je tedy

$$(\hat{p} * \hat{x})(j) := \sum_{k=0}^{N-1} \hat{p}(k) \cdot \hat{x}(j - k \bmod N) = 0, \quad 0 \leq j \leq N-1. \quad (2.3)$$

Dále spočteme, že

$$\begin{aligned} \hat{p}(0) &= \sum_{l=0}^{N-1} p(l) = \frac{1}{N} \sum_{l=0}^{N-1} \prod_{k \in S} (1 - e^{-2\pi i k/N} e^{2\pi i l/N}) \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \sum_{S' \subset S} \prod_{k \in S'} [(-1) e^{-2\pi i k/N} e^{2\pi i l/N}] \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \sum_{S' \subset S} (-1)^{\#S'} e^{2\pi i l(\#S')/N} \prod_{k \in S'} [e^{-2\pi i k/N}] \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \sum_{S' \subset S} (-1)^{\#S'} e^{2\pi i l(\#S')/N} \exp\left(-2\pi i \left(\sum_{k \in S'} k\right)/N\right) \\ &= \frac{1}{N} \sum_{S' \subset S} (-1)^{\#S'} \exp\left(-2\pi i \left(\sum_{k \in S'} k\right)/N\right) \sum_{l=0}^{N-1} e^{2\pi i l(\#S')/N}. \end{aligned}$$

Poslední suma přes l je rovna nule, pokud $\#S'$ je různé od nuly a pro $\#S' = 0$, tedy $S' = \emptyset$, je rovna N . Celkem je tedy $\hat{p}(0) = 1$. Zcela analogicky pak obdržíme pro $j > s$

$$\begin{aligned} \hat{p}(j) &= \sum_{l=0}^{N-1} e^{-2\pi i \frac{jl}{N}} p(l) = \frac{1}{N} \sum_{l=0}^{N-1} e^{-2\pi i \frac{jl}{N}} \sum_{S' \subset S} \prod_{k \in S'} [(-1) e^{-2\pi i k/N} e^{2\pi i l/N}] \\ &= \frac{1}{N} \sum_{l=0}^{N-1} e^{-2\pi i \frac{jl}{N}} \sum_{S' \subset S} (-1)^{\#S'} e^{2\pi i l(\#S')/N} \exp\left(-2\pi i \left(\sum_{k \in S'} k\right)/N\right) \\ &= \frac{1}{N} \sum_{S' \subset S} (-1)^{\#S'} \exp\left(-2\pi i \left(\sum_{k \in S'} k\right)/N\right) \sum_{l=0}^{N-1} e^{2\pi i l(\#S' - j)/N} = 0. \end{aligned}$$

Dosadíme-li $\hat{p}(0) = 1$ a $\hat{p}(s+1) = \dots = \hat{p}(N-1) = 0$ do (2.3) a přepíšeme-li tuto rovnici pro $s \leq j \leq 2s-1$, dostaneme (2.1).

2. *krok*: Pokud má soustava (2.1) jediné řešení, musí být tímto řešením $z = \hat{p}$, o kterém víme, že $S = \text{supp}(x) = (\text{supp } p)^c = (\text{supp } z^\vee)^c$. Tím je tedy nalezen nosič x a úloha se stává triviální.

3. *krok*: Předpokládejme tedy, že soustava (2.1) nemusí mít nutně jediné řešení. Nechť z je libovolné řešení (2.1). Jak navrženo v algoritmu, dodefinujeme $z(0) = 1, z(s+1) = \dots = z(N-1) = 0$. Konečně položíme $q = z^\vee$.

Vektor $q \cdot x$ je tedy s -sparse (už x byl s -sparse) a má Fourierovu transformaci rovnu nule na s po sobě jdoucích indexech $s, s+1, \dots, 2s-1$, protože $\widehat{q \cdot x}(j) = \hat{q} * \hat{x}(j) = y * z(j) = 0$ plyne pro $j = s, s+1, \dots, 2s-1$ z (2.1). Podle Lemmatu je tedy $q \cdot x = 0$. Vektor q má tedy nulové souřadnice na S . Tím jsme vlastně dokázali, že $S \subset \tilde{S}$. Konečně, protože

$$q(t) = \frac{1}{N} \sum_{k=0}^s \hat{q}(k) e^{2\pi i \frac{kt}{N}} = P(e^{2\pi i t/N}),$$

kde

$$P(z) = \frac{1}{N} \sum_{k=0}^s \hat{q}(k) z^k$$

je P polynom nejvýše stupně s (a q trigonometrický polynom nejvýše stupně s), je $i \notin S' \leq s$. \square

Cvičení:

- Naprogramujte Pronyho metodu (v Matlabu)
- Zjistěte její chování při defektu sparsity
- Zjistěte její chování při šumu

Nápověda:

```
x=sprand(100,1,.2);
x_full=full(x);
y=fft(x_full);

y=y+0.000000000001*randn(100,1);

c=wkeep(y,20,20);
r=wkeep(y,20,1);
R=flipud(r);
Y=toeplitz(c,R);

yy=wkeep(y,20,21);
zz=linsolve(Y,-1*yy);
z=[1;zz;zeros(79,1)];
S=ifft(z);
Supp=find(abs(S)<1e-8);
FMat=dftmtx(100);
xout=sparse(Supp,1,FMat(1:40,Supp)\y(1:40),100,1);
norm(x-xout,2)
```

Předchozí cvičení ukazuje, že Pronyho metoda je sice funkční pro $x \in \mathbb{R}^N$ s nejvýše s nulovými koeficienty, ale katastrofálně selhává pro “skoro sparse” x a pro Fourierovy koeficienty určené se šumem. Stabilní metoda rekonstrukce sparse vektorů byla představena o dvě století později Tibsiranim v roce 1996:

Nahradíme-li ℓ_2 -normu při regularizaci (3.4) ℓ_1 -normou, tak řešení následující minimalizace

$$\begin{aligned} \min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \sum_{j=1}^n \alpha_j (x^i)_j \right)^2 + \lambda \sum_{j=1}^n |\alpha_j| &= \min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \langle \alpha, x^i \rangle \right)^2 + \lambda \|\alpha\|_1 \\ &= \min_{\alpha \in \mathbb{R}^n} \|y - X\alpha\|_2^2 + \lambda \|\alpha\|_1, \end{aligned}$$

jsou sparse, tedy mají (v závislosti na parametru $\lambda > 0$) větší či menší počet souřadnic nulových. Matematické vysvětlení tohoto efektu je předmětem oboru Compressed Sensing (Donoho 2006, Candes, Romberg & Tao 2006).

Cvičení:

- implementace v matlabu
- chování při defektu sparsity
- chování při šumu

Nápověda: Metodu není třeba implementovat, stačí použít příkaz `lasso`.

3 Metoda nejmenších čtverců

Metodu nejmenších čtverců lze pojmut jako cvičení na lokální a globální extrémy funkcí více proměnných:

1. Úloha: Necht' je dáno n bodů $(x_i, y_i) \in \mathbb{R}^2$, $i = 1, 2, \dots, n$. Určete přímku $y = Ax + B$ tak, že $f(A, B) := \sum_{i=1}^n (y_i - Ax_i - B)^2$ je minimální.

Funkce f je všude definovaná všude hladká, takže lokální extrémy najdeme pomocí rovnice $\nabla f = 0$:

$$\frac{\partial f}{\partial A} = \sum_{i=1}^n 2(y_i - Ax_i - B)(-x_i) = -2 \sum_{i=1}^n (y_i x_i - Ax_i^2 - Bx_i) = 0, \quad (3.1)$$

$$\frac{\partial f}{\partial B} = \sum_{i=1}^n 2(y_i - Ax_i - B)(-1) = -2 \sum_{i=1}^n (y_i - Ax_i - B) = 0. \quad (3.2)$$

Pro zjednodušení notace polořme

- $\mathbb{1} = (1, \dots, 1) \in \mathbb{R}^n$, $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$,
- $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ a $\|x\|_2^2 = \langle x, x \rangle$.

Pak můřeme přepsat (3.1) a (3.2) jako

$$\begin{aligned} -2[\langle x, y \rangle - A\langle x, x \rangle - B\langle x, \mathbb{1} \rangle] &= 0, \\ -2[\langle y, \mathbb{1} \rangle - A\langle x, \mathbb{1} \rangle - nB] &= 0 \end{aligned}$$

a tedy jako

$$\begin{aligned} A\langle x, x \rangle + B\langle x, \mathbb{1} \rangle &= \langle x, y \rangle, \\ A\langle x, \mathbb{1} \rangle + nB &= \langle y, \mathbb{1} \rangle. \end{aligned}$$

Dostali jsme tedy soustavu dvou lineárních rovnic o dvou neznámých A a B . Abychom zjistili, kdy má tato soustava právě jedno řešení, vypočteme

$$\begin{vmatrix} \langle x, x \rangle & \langle x, \mathbb{1} \rangle \\ \langle x, \mathbb{1} \rangle & n \end{vmatrix} = n\|x\|_2^2 - \langle x, \mathbb{1} \rangle^2 \geq n\|x\|_2^2 - \|x\|_2^2 \cdot \|\mathbb{1}\|_2^2 = n\|x\|_2^2 - n\|x\|_2^2 = 0,$$

kde jsme použili Cauchy-Schwartzovu nerovnost $|\langle x, y \rangle| \leq \|x\|_2 \cdot \|y\|_2$. Determinant je roven nule, jen pokud je x násobek $\mathbb{1}$, tedy pokud všechna vstupní data x_1, \dots, x_n jsou stejná. Tento případ je samozřejmě prakticky nezařímavý, takže budeme v dalřím předpokládat, ře tomu tak není. V tom případě obdrříme jediné řešení:

$$A = \frac{n\langle x, y \rangle - \langle x, \mathbb{1} \rangle \langle y, \mathbb{1} \rangle}{n\langle x, x \rangle - \langle x, \mathbb{1} \rangle^2}, \quad B = \frac{\langle x, y \rangle \langle x, \mathbb{1} \rangle - \langle y, \mathbb{1} \rangle \langle x, x \rangle}{\langle x, \mathbb{1} \rangle^2 - n\langle x, x \rangle}.$$

Vzhledem k tomu, že $\lim_{(A,B) \rightarrow \infty} f(A,B) = \infty$ a tento bod je jediný kandidát na lok. minimum, snadno si rozmyslíme, že se jedná o glob. minimum. Lze to ověřit i pomocí matice druhých derivací:

$$\frac{\partial^2 f}{\partial A^2} = 2\langle x, x \rangle, \quad \frac{\partial^2 f}{\partial B^2} = 2n, \quad \frac{\partial^2 f}{\partial A \partial B} = 2\langle x, \mathbb{1} \rangle.$$

Je tedy

$$Hf = \begin{pmatrix} 2\langle x, x \rangle & 2\langle x, \mathbb{1} \rangle \\ 2\langle x, \mathbb{1} \rangle & 2n \end{pmatrix} \quad \text{a} \quad \det Hf = 4n\langle x, x \rangle - 4\langle x, \mathbb{1} \rangle^2$$

Z Chauchyho nerovnosti opět plyne, $\det Hf > 0$ a že tedy Hesseho matice je pozitivně definitní a f má v bodě (A, B) lokální minimum.

Metoda nejmenších čtverců, Gauss & Legendre, ca. 1800

2. Úloha: Buď x^1, \dots, x^N vektory v \mathbb{R}^n (vstupy) a buďte y_1, \dots, y_N reálná čísla (výstupy). Chceme najít lineární závislost $y \approx \langle \alpha, x \rangle$, která nejlépe odpovídá těmto datům. Minimalizujeme tedy

$$\min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \sum_{j=1}^n \alpha_j (x^i)_j \right)^2 = \min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \langle \alpha, x^i \rangle \right)^2 = \min_{\alpha \in \mathbb{R}^n} \|y - X\alpha\|_2^2, \quad (3.3)$$

kde $y = (y_1, \dots, y_N) \in \mathbb{R}^N$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$ a $X \in \mathbb{R}^{N \times n}$ je matice s řádky x^1, \dots, x^N .

Řešení odvodte pomocí následujících kroků:

- Přesvědčete se, že $f_{X,y}(\alpha) = \|y - X\alpha\|_2^2$ je konvexní funkce proměnné $\alpha \in \mathbb{R}^n$.
- Derivujte $f_{X,y}(\alpha)$ podle $\alpha_1, \dots, \alpha_n$ a tyto derivace položte rovny nule.
- Dokažte, že minimum se nabývá v bodě $\hat{\alpha} = (X^T X)^{-1} X^T y$, pokud má $X^T X$ inverzi.

Návod:

Z trojúhelníkové nerovnosti plyne snadno, že $\sqrt{f_{X,y}}$ je konvexní:

$$\begin{aligned} \sqrt{f_{X,y}}(\lambda\alpha^0 + (1-\lambda)\alpha^1) &= \|y - X(\lambda\alpha^0 + (1-\lambda)\alpha^1)\|_2 \\ &= \|(\lambda y - X(\lambda\alpha^0)) + ((1-\lambda)y - X((1-\lambda)\alpha^1))\|_2 \\ &\leq \|\lambda y - X(\lambda\alpha^0)\|_2 + \|(1-\lambda)y - X((1-\lambda)\alpha^1)\|_2 \\ &= \lambda \|y - X\alpha^0\|_2 + (1-\lambda) \|y - X\alpha^1\|_2 \\ &= \lambda \sqrt{f_{X,y}}(\alpha^0) + (1-\lambda) \sqrt{f_{X,y}}(\alpha^1). \end{aligned}$$

Pro $f_{X,y}$ pak dostaneme:

$$\begin{aligned} f_{X,y}(\lambda\alpha^0 + (1-\lambda)\alpha^1) &\leq \lambda^2 f_{X,y}(\alpha^0) + (1-\lambda)^2 f_{X,y}(\alpha^1) + 2\lambda(1-\lambda) f_{X,y}(\alpha^0) f_{X,y}(\alpha^1) \\ &= \lambda f_{X,y}(\alpha^0) + (1-\lambda) f_{X,y}(\alpha^1) + \lambda(\lambda-1) f_{X,y}(\alpha^0) + \lambda(\lambda-1) f_{X,y}(\alpha^1) + 2\lambda(1-\lambda) f_{X,y}(\alpha^0) f_{X,y}(\alpha^1) \\ &= \lambda f_{X,y}(\alpha^0) + (1-\lambda) f_{X,y}(\alpha^1) + \lambda(\lambda-1) [f_{X,y}(\alpha^0) + f_{X,y}(\alpha^1) - 2f_{X,y}(\alpha^0) f_{X,y}(\alpha^1)] \\ &\leq \lambda f_{X,y}(\alpha^0) + (1-\lambda) f_{X,y}(\alpha^1). \end{aligned}$$

Derivování dává:

$$\begin{aligned}
\frac{\partial f_{X,y}(\alpha)}{\partial \alpha_l} &= 2 \sum_{i=1}^N \left(y_i - \sum_{j=1}^n \alpha_j (x^i)_j \right) \cdot (x^i)_l = 2 \sum_{i=1}^N \left(y_i - \langle \alpha, x^i \rangle \right) \cdot (x^i)_l \\
&= 2 \sum_{i=1}^N y_i (x^i)_l - 2 \sum_{i=1}^N \langle \alpha, x^i \rangle (x^i)_l = 2 \sum_{i=1}^N (X^T)_{l,i} y_i - 2 \sum_{i=1}^N (X^T)_{l,i} (X\alpha)_i \\
&= 2(X^T y)_l - 2(X^T X\alpha)_l.
\end{aligned}$$

Je tedy

$$\nabla f_{X,y}(\alpha) = 2X^T y - 2(X^T X\alpha) = 0$$

ekvivalentní s $X^T y = X^T X\alpha$ a tedy $\alpha = (X^T X)^{-1} X^T y$, pokud má $X^T X$ inverzi.

Tikhonovova regularizace, Tikhonov & Phillips, ca. 1940

Regularizace (3.3) spočívá v penalizaci velkých vektorů α . Pro $\lambda > 0$ uvažujeme tedy

$$\begin{aligned}
\min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \sum_{j=1}^n \alpha_j (x^i)_j \right)^2 + \lambda \sum_{j=1}^n \alpha_j^2 &= \min_{\alpha \in \mathbb{R}^n} \sum_{i=1}^N \left(y_i - \langle \alpha, x^i \rangle \right)^2 + \lambda \|\alpha\|_2^2 \\
&= \min_{\alpha \in \mathbb{R}^n} \|y - X\alpha\|_2^2 + \lambda \|\alpha\|_2^2, \tag{3.4}
\end{aligned}$$

- Dokažte opět, že se jedná o minimalizaci konvexní funkce.
- Dokažte, že se minimum nabývá v bodě $\alpha = (X^T X - \lambda I)^{-1} X^T y$, pokud má $X^T X - \lambda I$ inverzi.

Konvexitu prvního členu jsme již dokázali, druhý člen je norma, je tedy také konvexní.

$$\begin{aligned}
\frac{\partial g_{X,y}(\alpha)}{\partial \alpha_l} &= 2 \sum_{i=1}^N \left(y_i - \sum_{j=1}^n \alpha_j (x^i)_j \right) \cdot (x^i)_l + 2\lambda \alpha_l = 2 \sum_{i=1}^N \left(y_i - \langle \alpha, x^i \rangle \right) \cdot (x^i)_l + 2\lambda \alpha_l \\
&= 2 \sum_{i=1}^N y_i (x^i)_l - 2 \sum_{i=1}^N \langle \alpha, x^i \rangle (x^i)_l + 2\lambda \alpha_l = 2 \sum_{i=1}^N (X^T)_{l,i} y_i - 2 \sum_{i=1}^N (X^T)_{l,i} (X\alpha)_i + 2\lambda \alpha_l \\
&= 2(X^T y)_l - 2(X^T X\alpha)_l + 2\lambda \alpha_l.
\end{aligned}$$

Tedy je

$$\nabla g_{X,y}(\alpha) = 2X^T y - 2(X^T X\alpha) + 2\lambda \alpha = 0$$

ekvivalentní s $X^T y = (X^T X - \lambda I)\alpha$ a tedy $\alpha = (X^T X - \lambda I)^{-1} X^T y$, pokud má $X^T X - \lambda I$ inverzi.

4 Khintchinovy nerovnosti

Khintchinovy nerovnosti jsou jednou z nejpěknějších partií matematické analýzy, a to z dlouhé řady důvodů. Původní Khintchinův důkaz (který se zachoval v nezměněné podobě dodnes a i my na něm nebudeme mnoho měnit) je jak elementární, tak elegantní. Khintchinovy nerovnosti překvapivým způsobem demonstrují výjimečnou úlohu $p = 2$ v teorii Lebesgueových prostorů. A v neposlední řadě mají Khintchinovy nerovnosti zajímavé důsledky pro geometrii Lebesgueových prostorů, statistiku, diskrétní geometrii a funkcionální analýzu. A v úplně neposlední řadě se nekomutativní verze Khintchinovy nerovnosti těší v posledních letech velkému zájmu pro aplikace v teorii náhodných matic.

Onzačme

$$r_n(t) := \text{sign} \sin(2^n \pi t), \quad t \in [0, 1], n \in \mathbb{N}_0.$$

Rademacherovy funkce. Funkce $(r_n)_{n=0}^\infty$ tvoří ortogonální systém v $L_2(0, 1)$, není to ale báze (uvažujte například funkci $f(t) = 1 - 2t$??).

Věta 4.1. *Nechť $p \in [1, \infty)$. Pak existují pozitivní konstanty A_p a B_p takové že*

$$A_p \left(\sum_{n=1}^m |a_n|^2 \right)^{1/2} \leq \left(\int_0^1 \left| \sum_{n=1}^m a_n r_n(t) \right|^p dt \right)^{1/p} \leq B_p \left(\sum_{n=1}^m |a_n|^2 \right)^{1/2}$$

platí pro každé $m \in \mathbb{N}$ a každou posloupnost reálných čísel a_1, \dots, a_m .

Důkaz. Označme A_p a B_p nejlepší možné konstanty (jejichž hodnota je dokonce přesně známa - my ale dokážeme poněkud slabší odhady). Z ortogonalitity Rademacherových funkcí plyne ihned $A_2 = B_2 = 1$. Konečně, díky monotonii L_p -norm, platí $A_r \leq A_p$ a $B_r \leq B_p$ pro $r \leq p$.

Stačí tedy, pokud ukážeme, že $A_1 > 0$ a $B_{2k} < \infty$ pro všechna $k \in \mathbb{N}$.

Začneme s odhadem B_{2k} . Užitím binomické věty dostaneme

$$\begin{aligned} E &:= \int_0^1 \left| \sum_{n=1}^m a_n r_n(t) \right|^{2k} dt = \int_0^1 \left(\sum_{n=1}^m a_n r_n(t) \right)^{2k} dt \\ &= \sum_{|\alpha|=2k} \frac{(2k)!}{\alpha_1! \dots \alpha_m!} a_1^{\alpha_1} \dots a_m^{\alpha_m} \int_0^1 r_1^{\alpha_1}(t) \dots r_m^{\alpha_m}(t) dt \\ &= \sum_{|\alpha|=k} \frac{(2k)!}{(2\alpha_1)! \dots (2\alpha_m)!} a_1^{2\alpha_1} \dots a_m^{2\alpha_m} \int_0^1 r_1^{2\alpha_1}(t) \dots r_m^{2\alpha_m}(t) dt \\ &= \sum_{|\alpha|=k} \frac{(2k)!}{(2\alpha_1)! \dots (2\alpha_m)!} a_1^{2\alpha_1} \dots a_m^{2\alpha_m}, \end{aligned}$$

kde jsme navíc použili i zajímavý fakt, že

$$\int_0^1 r_1^{\alpha_1}(t) \dots r_m^{\alpha_m}(t) dt$$

je rovno nule pokud nějaké z α_i je liché a rovno jedné, pokud jsou všechna α_i sudá.

Nechť $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}_0^m$ jsou přirozená čísla s $|\alpha| = k$, pak

$$2^k \alpha_1! \dots \alpha_m! = (2^{\alpha_1} \alpha_1!) \dots (2^{\alpha_m} \alpha_m!) \leq (2\alpha_1)! \dots (2\alpha_m)!.$$

Odtud dostaneme

$$\begin{aligned} E &\leq \frac{(2k)!}{2^k k!} \sum_{|\alpha|=k} \frac{k!}{\alpha_1! \dots \alpha_m!} a_1^{2\alpha_1} \dots a_m^{2\alpha_m} \\ &= \frac{(2k)!}{2^k k!} \left(\sum_{n=1}^m |a_n|^2 \right)^k = \frac{(2k)!}{2^k k!} \|a\|_2^{2k} \end{aligned}$$

a

$$E^{1/(2k)} \leq \left(\frac{(2k)!}{2^k k!} \right)^{1/(2k)} \|a\|_2.$$

Tvrzení tedy platí pro³

$$B_{2k} \leq \left(\frac{(2k)!}{2^k k!} \right)^{1/(2k)}.$$

Konečně musíme dokázat existenci $A_1 > 0$. Použijeme elegantní trik s dualitou a (již dokázanou) první část věty. Necht $f(t) := \sum_{n=1}^m a_n r_n(t)$. Z Hölderovy nerovnosti pro $p = 3/2$ a $p' = 3$ dostaneme

$$\begin{aligned} \int_0^1 |f(t)|^2 dt &= \int_0^1 |f(t)|^{2/3} \cdot |f(t)|^{4/3} dt \leq \left(\int_0^1 |f(t)| dt \right)^{2/3} \cdot \left(\int_0^1 |f(t)|^4 dt \right)^{1/3} \\ &\leq \left(\int_0^1 |f(t)| dt \right)^{2/3} B_4^{4/3} \cdot \|a\|_2^{4/3} = \left(\int_0^1 |f(t)| dt \right)^{2/3} B_4^{4/3} \cdot \|f\|_2^{4/3}. \end{aligned}$$

Platí tedy

$$\left(\int_0^1 |f(t)| dt \right)^{2/3} \geq B_4^{-4/3} \left(\int_0^1 |f(t)|^2 dt \right)^{1/3},$$

nebo-li

$$\int_0^1 |f(t)| dt \geq B_4^{-2} \left(\int_0^1 |f(t)|^2 dt \right)^{1/2} = B_4^{-2} \|a\|_2.$$

Dokázali jsme tedy, že $A_1 \geq B_4^{-2}$ a důkaz je hotov. \square

Khintchinovy nerovnosti lze například použít ve funkcionální analýze ke konstrukci překvapivě mnoha “téměř ortogonálních” vektorů. Pro ten účel nejprve přeformulujeme Khintchinovy nerovnosti jako

$$A_p \left(\sum_{n=1}^m |a_n|^2 \right)^{1/2} \leq \left(\frac{1}{2^m} \sum_{e \in \{-1, +1\}^m} |\langle a, e \rangle|^p dt \right)^{1/p} \leq B_p \left(\sum_{n=1}^m |a_n|^2 \right)^{1/2}$$

pro všechny $m \in \mathbb{N}$ a $a \in \mathbb{R}^m$. Konstrukce “skoro-ortogonálních” vektorů je pak popsána následujícím lemmatem (a jeho důkazem).

Lemma 4.2. *Necht m a n jsou přirozená čísla. Pak existují $x_1, \dots, x_m \in \ell_2^m$ takové že $\|x_i\|_2 = 1$ pro všechna $i = 1, 2, \dots, m$ a*

$$|\langle x_i, x_j \rangle| \leq 2 \left[\frac{\log_2 m}{n} \right]^{1/2} \quad \text{pro } i \neq j.$$

³Ze Stirlingovy formule snadno plyne, že B_{2k} roste nejvýše jako $\sqrt{2k}$ pro $k \rightarrow \infty$.

Důkaz. Je-li $m \leq n$, pak stačí vzít libovolné ortonormální vektory $(x_1, \dots, x_m) \subset \mathbb{R}^n$. Předpokládejme tedy, že $m \geq n$ a že tvrzení bylo již dokázáno pro nějaké m . Pak

$$\sum_{i=1}^m \sum_{e \in \{-1, +1\}^n} |\langle x_i, e \rangle|^p \leq B_p^p m 2^n.$$

Tedy alespoň pro jedno $e \in \{-1, +1\}^n$ platí

$$\sum_{i=1}^m |\langle x_i, e \rangle|^p \leq B_p^p m.$$

Položme $x_{m+1} := n^{-1/2}e$. Pak $\|x_{m+1}\|_2 = 1$ a

$$|\langle x_i, x_{m+1} \rangle| \leq B_p m^{1/p} n^{-1/2} \quad \text{pro } i = 1, 2, \dots, m.$$

Zvolíme-li $p := \log_2 m$, pak obdržíme

$$|\langle x_i, x_{m+1} \rangle| \leq 2 \left[\frac{\log_2 m}{n} \right]^{1/2} \quad \text{pro } i = 1, 2, \dots, m.$$

□

Tato geometrická konstrukce je značně nekonstruktivní. Víme, že jeden z vektorů $\{-1/\sqrt{n}, 1/\sqrt{n}\}$ je vhodným kandidátem, ale nevíme, který to je. Protože průměr přes všechny tyto vektory je malý, musí být (alespoň) jeden z nich vhodný. Konstrukce tohoto typu jsou dnes standardními nástroji řady oborů včetně kombinatoriky, teorie grafů nebo funkcionální analýzy.⁴ Pro mnoho tvrzení tohoto typu není znám žádný konstruktivní důkaz. V případě lemmatu 4.2 tomu tak ale není. Pro zajímavost uveďme konstruktivní důkaz podobného (vlastně o maličko silnějšího) tvrzení.

Lemma 4.3. *Bud' $0 < \lambda < 1$. Pak existuje konstanta $c_\lambda > 0$ taková, že pro všechny $m^\lambda \leq n \leq m$ existuje m jednotkových vektorů x_1, x_2, \dots, x_m v ℓ_2^n , pro které platí*

$$|\langle x_i, x_j \rangle| \leq \frac{c_\lambda}{n^{1/2}}, \quad i \neq j.$$

Důkaz. Necht' p je prvočíslo a necht' $GF(p)$ je Galoisovo těleso, tedy množina $\{0, 1, \dots, p-1\}$ vybavná sčítáním a násobením modulo p . Necht' $k \in \mathbb{N}$ a necht' \mathcal{P}_k značí polynomy nad $GF(p)$ stupně nejvýše k . Pro každé $\pi \in \mathcal{P}_k$ definujeme vektor

$$x^\pi \in \ell_2^{p^2}, \quad x_{i,j}^\pi = \begin{cases} 1 & \text{pokud } \pi(i) = j, \\ 0 & \text{jinak.} \end{cases}$$

Platí tedy

- $\|x^\pi\|_2 = \sqrt{p}$ pro všechna $\pi \in \mathcal{P}_k$,
- $|\langle x^\pi, x^\sigma \rangle| \leq k$ pro všechna $\pi, \sigma \in \mathcal{P}_k$ s $\pi \neq \sigma$,

⁴Alon: Probabilistic method

- celkově takto obdržíme $\#\mathcal{P}_k = p^{k+1}$ vektorů.

Systém

$$\left\{ \frac{x^\pi}{\sqrt{p}} \right\}_{\pi \in \mathcal{P}_k}$$

má tedy všechny požadované vlastnosti pro

$$n = p^2, \quad \lambda = \frac{2}{k+1}, \quad m = p^{k+1}, \quad c_\lambda = k.$$

□

Khinchinovy nerovnosti přeformulovány do řeči funkcionální analýzy pak říkají, že $L_p([0, 1])$ obsahuje pro $1 < p < \infty$ podprostor isomorfní s ℓ_2 .⁵

Remark 1. Reformulace Khinchinových nerovností v řeči statistiky vypadá následovně. Nechť $\epsilon_i, i = 1, \dots, m$ jsou nezávislé nahodné proměnné s $\mathbb{P}(\epsilon_i = 1) = 1/2$ a $\mathbb{P}(\epsilon_i = -1) = 1/2$. Nechť $1 \leq p < \infty$. Pak existují konstanty A_p, B_p takové, že pro všechna $a_1, \dots, a_m \in \mathbb{R}$

$$A_p \|a\|_2 \leq \left(\mathbb{E} \left| \sum_{i=1}^m a_i \epsilon_i \right|^p \right)^{1/p} \leq B_p \|a\|_2. \quad (4.1)$$

Vezmeme-li p dostatečně velké, lze pomocí standardního argumentu ze statistiky odvodit *tail bound estimates on sum of independent Rademacher variables*, neboli asymptotické chování

$$\mathbb{P} \left(\left| \sum_{i=1}^m a_i \epsilon_i \right| > t \right)$$

pro $t \rightarrow \infty$.

Využijeme tuto reformulaci Khinchinových nerovností k jejich alternativnímu důkazu.

Důkaz. (horního odhadu ve větě 4.1).

Díky normalizaci můžeme předpokládat, že $\|a\|_2 = 1$. Pak

$$\mathbb{E} \exp \left(\sum_{i=1}^m a_i \epsilon_i \right) = \mathbb{E} \prod_{i=1}^m \exp(a_i \epsilon_i) = \prod_{i=1}^m \mathbb{E} \exp(a_i \epsilon_i) = \prod_{i=1}^m \cosh(a_i).$$

Z Taylorova rozvoje plzne snadno $\cosh(a_j) \leq \exp(a_j^2/2)$. Tedy,

$$\mathbb{E} \exp \left(\sum_{i=1}^m a_i \epsilon_i \right) \leq \prod_{i=1}^m \exp(a_i^2/2) = e^{1/2},$$

a pomocí Markovovy nerovnosti

$$\begin{aligned} \mathbb{P} \left(\sum_{i=1}^m a_i \epsilon_i > \lambda \right) &= \mathbb{P} \left(\exp \left(\sum_{i=1}^m a_i \epsilon_i \right) > \exp(\lambda) \right) = \mathbb{P} \left(\exp \left(\sum_{i=1}^m a_i \epsilon_i - \lambda \right) > 1 \right) \\ &\leq \mathbb{E} \exp \left(\sum_{i=1}^m a_i \epsilon_i - \lambda \right) \leq e^{1/2 - \lambda}. \end{aligned}$$

⁵M. Fabian, P. Habala, P. Hájek, V. Montesinos, V. Zizler: *Banach Space Theory: The Basis for Linear and Nonlinear Analysis*, Springer 2011, strana 210.

Díky symetrii ε_i dostaneme $\mathbb{P}\left(\left|\sum_{i=1}^m a_i \varepsilon_i\right| > \lambda\right) \lesssim e^{-\lambda}$. Zbytek pak plyne z distributivní reprezentace L_p -normy. \square

Khintchinovy nerovnosti (4.1) platí i pro mnoho jiných náhodných proměnných. Necht' jsou například $\omega_1, \dots, \omega_m$ nezávislé normální proměnné. Pak (z 2-stability normálního rozdělení, viz kapitolu o JL-vnoření),

$$\sum_{i=1}^m a_i \omega_i \approx \|a\|_2 \cdot \omega,$$

kde $\omega \approx N(0, 1)$, a tedy

$$\left(\mathbb{E}\left|\sum_{i=1}^m a_i \omega_i\right|^p\right)^{1/p} = \|a\|_2 \cdot (\mathbb{E}|\omega|^p)^{1/p}.$$

Máme tedy (4.1) s rovností pro $A_p = B_p = (\mathbb{E}|\omega|^p)^{1/p}$, tedy p -té momenty standardní normální proměnné. Při troše další práce je možné dokázat podobné tvrzení i pro všechna subgaussovské proměnné.⁶

Khintchinovy nerovnosti mají zajímavou aplikaci v teorii operátorů. Necht' $1 \leq p < \infty$ a necht' $T : L_p(\mathbb{R}^n) \rightarrow L_p(\mathbb{R}^n)$ je omezený lineární operátor. Pak

$$\left\|\left(\sum_{j=0}^N |Tf_j|^2\right)^{1/2}\right\|_p \leq c_p \left\|\left(\sum_{j=0}^N |f_j|^2\right)^{1/2}\right\|_p, \quad (4.2)$$

kde konstanta c_p závisí jen na p a $\|T\|$.

Důkaz provedeme pomocí Rademacherových funkcí r_1, \dots, r_N a následujícího výpočtu

$$\begin{aligned} \left\|\left(\sum_{j=0}^N |Tf_j|^2\right)^{1/2}\right\|_p^p &= \int_{\mathbb{R}^n} \left(\sum_{j=1}^N |(Tf_j)(x)|^2\right)^{p/2} dx \leq c \int_{\mathbb{R}^n} \left(\int_0^1 \left|\sum_{j=1}^N Tf_j(x)r_j(t)\right|^p dt\right)^{p/p} dx \\ &= c \int_0^1 \int_{\mathbb{R}^n} \left|\sum_{j=1}^N Tf_j(x)r_j(t)\right|^p dx dt = c \int_0^1 \int_{\mathbb{R}^n} |T\left(\sum_{j=1}^N f_j r_j(t)\right)(x)|^p dx dt \\ &\leq c \|T\|^p \int_0^1 \int_{\mathbb{R}^n} \left|\sum_{j=1}^N f_j(x)r_j(t)\right|^p dx dt \leq c' \int_{\mathbb{R}^n} \left(\sum_{j=1}^N |f_j(x)|^2\right)^{p/2} dx \\ &= c_p^p \left\|\left(\sum_{j=0}^N |f_j|^2\right)^{1/2}\right\|_p^p. \end{aligned}$$

Uvažujeme-li $N \rightarrow \infty$ (a vyjasníme otázky konvergence), pak stejný výsledek platí i pro nekonečné součty.

⁶Vershynin...

5 Diskrepance

The proof is a two-page gem due to Roth.
 Jiří Matoušek, Geometric Discrepancy

Rothův důkaz dolního odhadu diskrepance

Cílem této kapitolky není nic jiného než předvést Rothův důkaz dolního odhadu diskrepance libovolné množiny bodů. Ve své klasické podobě studuje teorie diskrepance, jak co nejrovnoměrněji rozprostřít množinu bodů v jednotkové krychli $[0, 1]^d$. Je-li P množina n bodů v $[0, 1]^d$ a je-li $R \subset [0, 1]^d$ krychle se stěnami rovnoběžnými se souřadnicovými osami, tedy

$$R = [a_1, b_1) \times \cdots \times [a_d, b_d) \subset [0, 1]^d, \quad (5.1)$$

pak by (pokud jsou tedy body P dobře rovnoměrně rozdělené) měl objem krychle R přibližně odpovídat poměru bodů z P , které leží v R a počtu bodů P , tedy

$$\frac{\text{vol}(R)}{\text{vol}([0, 1]^d)} \approx \frac{\#(P \cap R)}{\#(P)}, \quad \text{neboli} \quad n \text{vol}(R) \approx \#(P \cap R).$$

Ještě jinak, $n \text{vol}(R)$ je očekávaný počet bodů, které padnou do R , pokud zkonstruujeme nezávisle n náhodných a rovnoměrně rozdělených bodů v $[0, 1]^d$. Definujme tedy

$$D(P, R) := n \cdot \text{vol}(R) - \#(P \cap R)$$

jako odchylku P od rovnoměrného rozdělení na R . Diskrepance množiny P

$$D(P, \mathcal{R}_d) = \sup_{R \in \mathcal{R}_d} |D(P, R)|$$

je pak největší odchylka P od rovnoměrného rozdělení braná přes množinu všech krychlí (5.1).

Konečně, hledání nejlépe rozložené množiny P lze pak vyjádřit jako minimalizaci $D(P, \mathcal{R}_d)$ přes všechny n -prvkové podmnožiny $[0, 1]^d$, tedy jako

$$D(n, \mathcal{R}_d) = \inf_{\substack{P \subset [0, 1]^d \\ \#P=n}} D(P, \mathcal{R}_d).$$

Základní otázka teorie diskrepance zní, jestli je $D(n, \mathcal{R}_d)$ omezená posloupnost. Odpověď na tuto otázku je záporná, jak ukazuje

Věta 5.1 (Rothův dolní odhad diskrepance). *Pro každé přirozené číslo d existuje konstanta $c_d > 0$ taková, že pro všechna přirozená čísla n platí*

$$D(n, \mathcal{R}_d) \geq c_d \log^{(d-1)/2} n. \quad (5.2)$$

Důkaz. Důkaz provedeme pouze pro $d = 2$. Necht $P \subset [0, 1]^2$ s $\#(P) = n$. Naším cílem je najít obdélník $R \in \mathcal{R}_2$, pro který bude platit

$$D(P, R) \geq c_2 \sqrt{\log n}. \quad (5.3)$$

Vzhledem k tomu, že množina P může být zcela libovolná, explicitní konstrukce obdélníku R by byla příliš technická a složitá. Místo toho ukážeme, že průměrná hodnota $D(P, R)$ přes všechny $R \in \mathcal{R}_2$ s jedním vrcholem v počátku je alespoň $c_2\sqrt{\log n}$. Existence obdélníka R s (5.3) pak plyne implicitně.

Pro $x \in [0, 1]^2$ definujme tedy $C_x = [0, x_1) \times [0, x_2)$. Dokážeme, že

$$D_2(P, \mathcal{C}_2) := \sqrt{\int_{[0,1]^2} D(P, C_x)^2 dx} \geq c_2\sqrt{\log n}. \quad (5.4)$$

Klíčovým bodem Rothova důkazu je konstrukce pomocné funkce $F: [0, 1]^2 \rightarrow \mathbb{R}$ (v závislosti na P), pro kterou platí

$$\int_{[0,1]^2} F^2(x) dx \leq c \log n, \quad (5.5)$$

$$\int_{[0,1]^2} F(x) D(P, C_x) dx \geq c' \log n \quad (5.6)$$

s konstantami $c, c' > 0$ nezávislými na P a n . Vybavení (5.5) a (5.6) pak dokážeme (5.4) pomocí prosté Cauchy-Schartzovy norevnosti

$$c' \log n \leq \int_{[0,1]^2} F(x) D(P, C_x) dx \leq \sqrt{\int_{[0,1]^2} F^2(x) dx} \cdot \sqrt{\int_{[0,1]^2} D(P, C_x)^2 dx} \leq \sqrt{c \log n} \cdot D_2(P, \mathcal{C}_2).$$

Zbytek důkazu se tedy budeme věnovat konstrukci funkce F s (5.5) a (5.6). Zvolme přirozené číslo m s $2n \leq 2^m < 4n$ a definujme pro každé $j = 0, 1, \dots, m$ funkci $f_j: [0, 1]^2 \rightarrow \{-1, 0, 1\}$ následujícím způsobem. Interval $I = [0, 1]$ rozdělíme na dyadické intervaly

$$I = [0, 1] = [0, 2^{-j}) \cup [2^{-j}, 2 \cdot 2^{-j}) \cup [2 \cdot 2^{-j}, 3 \cdot 2^{-j}) \cup \dots \cup [(2^j - 1) \cdot 2^{-j}, 1] = I_{j,1} \cup \dots \cup I_{j,2^j}.$$

Rozdělíme $[0, 1]^2$ na 2^m obdélníčků s plochou 2^{-m}

$$I^2 = [0, 1]^2 = \bigcup_{s=1}^{2^j} \bigcup_{t=1}^{2^{m-j}} I_{j,s} \times I_{m-j,t}.$$

Pokud obdélníček $I_{j,s} \times I_{m-j,t}$ obsahuje alespoň jeden bod z množiny P , definujme $f_j = 0$ na celém $I_{j,s} \times I_{m-j,t}$. Pokud ale v tomto obdélníčku žádný bod P neleží, rozdělíme jej na čtvrtiny a definujme $f_j = +1$ v jeho levém dolním a v pravém horním kvadrantu a $f_j = -1$ v levém horním a v pravém dolním kvadrantu. Konečně definujme $F = f_0 + f_1 + \dots + f_m$.

Důkaz (5.5):

Nejprve ukážeme, že $\int f_i f_j = 0$ pro $i < j$. Skutečně, nechť f_i není identicky rovna nule na $I_{i,s} \times I_{m-i,t}$ a f_j na $I_{j,u} \times I_{m-j,v}$ a nechť tyto dva obdélníčky mají neprázdný průnik. Pak $I_{j,u} \subset I_{i,s}$ a $I_{m-i,t} \subset I_{m-j,v}$ a

$$(I_{i,s} \times I_{m-i,t}) \cap (I_{j,u} \times I_{m-j,v}) = I_{j,u} \times I_{m-i,t} =: Q.$$

Funkce f_i na Q nezávisí na x_1 a f_j nezávisí na x_2 . Jejich součin je pak na polovině množiny Q roven 1 a na druhé polovině -1 . Celkem je tedy $\int_Q f_i f_j = 0$. Protože toto platí pro každý z

2^{m+j-i} potenciální obdélníků Q , dostaneme i $\int_{[0,1]^2} f_i f_j = 0$. Odtud již snadno plyne

$$\int_{[0,1]^2} F^2(x) dx = \sum_{i,j=0}^m \int_{[0,1]^2} f_i(x) f_j(x) dx = \sum_{j=0}^m \int_{[0,1]^2} f_i(x)^2 dx \leq \sum_{j=0}^m 1 = m+1 \leq \log(4n)+1 = \log n+3.$$

Důkaz (5.6):

Dokážeme, že $\int_{[0,1]^2} f_j(x) D(P, C_x) dx$ je zdola omezen $c'' > 0$ pro všechna $j = 0, 1, \dots, m$; (5.6) pak plyne prostě součtem přes všechna j . Nechť tedy $j \in \{0, 1, \dots, m\}$ je pevné. Budeme uvažovat pouze ty obdélníky $I_{j,s} \times I_{m-j,t}$, na kterých není f_j identicky rovna nule, tedy ty, které neobsahují žádný bod z P . Vzhledem k tomu, že počet všech obdélníčků z definice f_j je $2^m \geq 2n$ a množina P má jen n bodů, je f_j nenulová alespoň na polovině obdélníčků typu $I_{j,s} \times I_{m-j,t}$. Stačí tedy dokázat, že na každém z nich je

$$\int_{I_{j,s} \times I_{m-j,t}} f_j(x) D(P, C_x) dx \geq \tilde{c}/n.$$

Zvolme tedy $Q := I_{j,s} \times I_{m-j,t}$ pevné. Označme $\tilde{Q} = 2^{-j}[s-1, s-1/2) \times 2^{m-j}[t-1, t-1/2)$ levnou dolní čtvrtinu Q , $a = (2^{-j-1}, 0)$ a $b = (0, 2^{-m+j-1})$.

$$\begin{aligned} \int_Q f_j(x) D(P, C_x) dx &= \int_{\tilde{Q}} D(P, C_x) dx - \int_{a+\tilde{Q}} D(P, C_x) dx - \int_{b+\tilde{Q}} D(P, C_x) dx + \int_{a+b+\tilde{Q}} D(P, C_x) dx \\ &= \int_{\tilde{Q}} D(P, C_x) - D(P, C_{x+a}) - D(P, C_{x+b}) + D(P, C_{x+a+b}) dx \\ &= n \int_{\tilde{Q}} \text{vol}(C_x) - \text{vol}(C_{x+a}) - \text{vol}(C_{x+b}) + \text{vol}(C_{x+a+b}) dx \\ &\quad - \int_{\tilde{Q}} \#(C_x \cap P) - \#(C_{x+a} \cap P) - \#(C_{x+b} \cap P) + \#(C_{x+a+b} \cap P) dx. \end{aligned}$$

Funkce v prvním integrálu je rovna

$$x_1 x_2 - (x_1 + 2^{-j-1}) x_2 - x_1 (x_2 + 2^{-m+j-1}) + (x_1 + 2^{-j-1})(x_2 + 2^{-m+j-1}) = 2^{-m-2}$$

pro všechna $x \in \tilde{Q}$. Podobně se ukáže, že příspěvek každého bodu P , který neleží v Q je nulový. V Q samotném ale žádné body neleží, takže druhý integrál je nulový. Celkem tedy máme

$$\int_Q f_j(x) D(P, C_x) dx = n \int_{\tilde{Q}} 2^{-m-2} dx = n 2^{-2m-4} \geq \frac{n}{16} \cdot \frac{1}{(4n)^2} \geq \frac{\tilde{c}}{n}.$$

□

Nerovnost Koksmy a Hlawky

Nechť nejprve $d = 1$ a nechť $f : [0, 1] \rightarrow \mathbb{R}$ je hladká⁷ funkce. Obor numerické integrace se zabývá tím, jak co nejlépe aproximovat integrál této funkce $\int_0^1 f(t) dt$ pomocí konečně mnoha funkčních hodnot. Logicky se nabízí aproximovat tento integrál pomocí sumy $\sum_{j=1}^n f(x_j)$, kde body

⁷ Jak moc hladká upřesníme později.

$x_1, \dots, x_n \subset [0, 1]$ jsou co nejrovnoměrněji rozloženy v intervalu $[0, 1]$ - tedy mají malou diskrepanci.

Nahradíme-li tedy $f(x)$ pomocí $f(1) - \int_x^1 f'(t)dt$, dostaneme

$$\begin{aligned} \int_0^1 f(x)dx - \frac{1}{n} \sum_{j=1}^n f(x_j) &= \int_0^1 \left(f(1) - \int_x^1 f'(t)dt \right) dx - \frac{1}{n} \sum_{j=1}^n \left(f(1) - \int_{x_j}^1 f'(t)dt \right) \\ &= \frac{1}{n} \sum_{j=1}^n \int_{x_j}^1 f'(t)dt - \int_0^1 \int_x^1 f'(t)dt dx \\ &= \int_0^1 \frac{1}{n} \sum_{j=1}^n \chi_{(x_j, 1]}(t) f'(t) dt - \int_0^1 \int_0^t f'(t) dx dt \\ &= \int_0^1 f'(t) \left[\frac{1}{n} \sum_{j=1}^n \chi_{(x_j, 1]}(t) - t \right] dt = \int_0^1 f'(t) \left[\frac{1}{n} \sum_{j=1}^n \chi_{[0, t)}(x_j) - t \right] dt. \end{aligned}$$

Vezmeme-li nyní absolutní hodnotu, dostaneme

$$\begin{aligned} \left| \int_0^1 f(x)dx - \frac{1}{n} \sum_{j=1}^n f(x_j) \right| &\leq \int_0^1 |f'(t)| dt \cdot \sup_{t \in [0, 1]} \left| \frac{1}{n} \sum_{j=1}^n \chi_{[0, t)}(x_j) - t \right| \\ &= \int_0^1 |f'(t)| dt \cdot \frac{1}{n} \cdot \sup_{t \in [0, 1]} \left| \#(P \cap [0, t)) - n \text{vol}([0, t)) \right|. \end{aligned}$$

Zde jsme opět položili $P = \{x_1, \dots, x_n\}$. Označíme-li teď \mathcal{A}_1 ty intervaly z \mathcal{R}_1 , které mají jeden vrchol v počátku, je poslední výraz napravo roven $D(P, \mathcal{A}_1)$ ⁸ a dostaneme

$$\left| \int_0^1 f(x)dx - \frac{1}{n} \sum_{j=1}^n f(x_j) \right| \leq \int_0^1 |f'(t)| dt \cdot \frac{D(P, \mathcal{A}_1)}{n}. \quad (5.7)$$

Chyba numerické integrace je tedy omezena součinem dvou výrazů, z nichž jeden měří regularitu funkce f a druhý zase kvalitu rozložení bodů z P . Nerovnost (5.7) je nejjednodušším příkladem nerovnosti Koksmy a Hlawky.

Ve zbytku této kapitoly naznačíme, jak vypadá d -dimenzionální analogie (5.7). Označme \mathcal{A}_d ty obdélníky z \mathcal{R}_d , které mají jeden vrchol v počátku. Pro jednoduchost předpokládejme, že $f : [0, 1]^d \rightarrow \mathbb{R}$ a $f(x) = 0$ je identicky rovna nule, pokud je alespoň jedna ze souřadnic vektoru x rovna jedné. V tom případě obdržíme

$$\begin{aligned} -f(y) &= f(y_1, y_2, \dots, y_{n-1}, 1) - f(y_1, \dots, y_n) = \int_{y_n}^1 \frac{\partial f(y_1, \dots, y_{n-1}, t_n)}{\partial x_n} dt_n \\ &= \int_{y_n}^1 \frac{\partial f(y_1, \dots, y_{n-1}, t_n)}{\partial x_n} - \frac{\partial f(y_1, \dots, y_{n-2}, 1, t_n)}{\partial x_n} dt_n \\ &= - \int_{y_n}^1 \int_{y_{n-1}}^1 \frac{\partial^2 f(y_1, \dots, y_{n-2}, t_{n-1}, t_n)}{\partial x_{n-1} \partial x_n} dt_{n-1} dt_n \\ &= \dots = (-1)^{n-1} \int_{(y, 1]} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} dt, \end{aligned}$$

⁸tzv. *star discrepancy*

kde $(y, 1] := (y_1, 1] \times \dots \times (y_n, 1]$. Dosazením této identity pak dostaneme podobně jako v jedno-rozměrném případě

$$\begin{aligned}
\int_{[0,1]^d} f(x) dx - \frac{1}{n} \sum_{j=1}^n f(x_j) &= \int_{[0,1]^d} (-1)^n \int_{(x,1]} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} dt dx - \frac{(-1)^n}{n} \sum_{j=1}^n \int_{(x_j,1]} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} dt \\
&= (-1)^n \int_{[0,1]^d} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} \int_{[0,t]} 1 dx dt - (-1)^n \int_{[0,1]^d} \frac{1}{n} \sum_{j=1}^n \chi_{(x_j,1]}(t) \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} dt \\
&= (-1)^n \int_{[0,1]^d} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} \left[t_1 \dots t_n - \frac{1}{n} \sum_{j=1}^n \chi_{(x_j,1]}(t) \right] dt \\
&= (-1)^n \int_{[0,1]^d} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} \left[t_1 \dots t_n - \frac{1}{n} \sum_{j=1}^n \chi_{[0,t]}(x_j) \right] dt \\
&= \frac{(-1)^n}{n} \int_{[0,1]^d} \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} \left[n \text{vol}([0, t]) - \#(P \cap [0, t]) \right] dt.
\end{aligned}$$

Odtud již pak snadno plyne

$$\left| \int_{[0,1]^d} f(x) dx - \frac{1}{n} \sum_{j=1}^n f(x_j) \right| \leq \frac{1}{n} \cdot \int_{[0,1]^d} \left| \frac{\partial^n f(t)}{\partial x_1 \partial x_2 \dots \partial x_n} \right| dt \cdot D(P, \mathcal{A}_d),$$

tedy opět odhad chyby numerické integrace pomocí součinu dvou výrazů, z nichž jeden měří regularitu funkce a druhý rovnoměrnost rozložení bodů z P .

6 Objem jednotkové koule - klasicky a moderně

Lebesgueova míra λ_n v \mathbb{R}^n je normovaná tak, aby $\lambda_n([0, 1]^n) = 1$. Objemy jiných konvexních těles hrají zásadní roli v řadě oborů matematiky.⁹ Pro většinu těles v \mathbb{R}^n je vcelku obtížné jejich objem přesně spočítat a musíme se proto spokojit s více či méně přesnými odhady. Vyjímkou z tohoto pravidla je objem jednotkové koule, resp. jednotkové koule prostoru ℓ_p^n , kde

$$\|x\|_{\ell_p^n} = \|x\|_p = \left(\sum_{j=1}^n |x_j|^p \right)^{1/p}, \quad 0 < p < \infty.$$

Pro $p = \infty$ definujeme samozřejmě $\|x\|_\infty = \max_j |x_j|$. Ukážeme několik způsobů, jak spočítat objem “koule”

$$B_p^n = \{x \in \mathbb{R}^n : \|x\|_p \leq 1\}$$

v závislosti na p a n .

Výsledek je vyjádřen pomocí gamma (a beta) funkce a všechny způsoby tedy dříve či později tyto funkce potřebují. Takže pro připomenutí:

$$\Gamma(t) = \int_0^\infty x^{t-1} e^{-x} dx, \quad t > 0$$

a

$$B(x, y) = \int_0^1 t^{x-1} (1-t)^{y-1} dt$$

Cvičení:

1. Dokažte $\Gamma(t+1) = t\Gamma(t)$, $t > -1$.
2. Dokažte $\Gamma(n) = (n-1)!$, kde $n \in \mathbb{N}$.
3. Dokažte $\Gamma(1/2) = \sqrt{\pi}$.
4. Dokažte $B(x, y) = \Gamma(x)\Gamma(y)/\Gamma(x+y)$.

Nejstarší z přístupů, které projdeme, pochází od Dirichleta.

1. Postup

$$\lambda_n(B_p^n) = \int_{x \in \mathbb{R}^n : \|x\|_p \leq 1} 1 dx = 2^n \int_{x \geq 0 : \|x\|_p \leq 1} 1 dx,$$

kde $x \geq 0$ znamená, že $x = (x_1, \dots, x_n)$ a $x_j \geq 0$ pro všechna $j = 1, \dots, n$. Provedeme substituci $t_j = x_j^p$ a dostaneme

$$\begin{aligned} \lambda_n(B_p^n) &= 2^n \int_{\substack{t \geq 0 \\ t_1 + \dots + t_n \leq 1}} \frac{1}{p^n} \prod_{j=1}^n t_j^{1/p-1} dt \\ &= \frac{2^n}{p^n} \int_0^1 t_n^{1/p-1} \int_{\substack{t_1, \dots, t_{n-1} \geq 0 \\ t_1 + \dots + t_{n-1} \leq 1-t_n}} \prod_{j=1}^{n-1} t_j^{1/p-1} dt_1 \dots dt_{n-1} dt_n. \end{aligned}$$

⁹Pisier: Volumes of convex bodies

Dále substituujeme $s_j = t_j/(1 - t_n)$ pro $j = 1, \dots, n - 1$ a dostaneme

$$\begin{aligned}\lambda_n(B_p^n) &= \frac{2^n}{p^n} \int_0^1 t_n^{1/p-1} \int_{\substack{s \geq 0 \\ s_1 + \dots + s_{n-1} \leq 1}} \prod_{j=1}^{n-1} s_j^{1/p-1} (1 - t_n)^{1/p} ds dt_n \\ &= \frac{2^n}{p^n} \int_0^1 t_n^{1/p-1} (1 - t_n)^{(n-1)/p} dt_n \int_{\substack{s \geq 0 \\ s_1 + \dots + s_{n-1} \leq 1}} \prod_{j=1}^{n-1} s_j^{1/p-1} ds \\ &= \frac{2^n}{p^n} B(1/p, (n-1)/p + 1) \cdot \frac{p^{n-1}}{2^{n-1}} \lambda_{n-1}(B_{n-1}^p) \\ &= \frac{2}{p} \frac{\Gamma(1/p)\Gamma((n-1)/p + 1)}{\Gamma(n/p + 1)} \lambda_{n-1}(B_{n-1}^p).\end{aligned}$$

Z této rekursivní formule a z $\lambda_1(B_p^1) = 2$, dostaneme

$$\lambda_2(B_p^2) = 2^2 \frac{\Gamma(1/p + 1)^2}{\Gamma(2/p + 1)} \quad \text{a obecně} \quad \lambda_n(B_p^n) = 2^n \frac{\Gamma(1/p + 1)^n}{\Gamma(n/p + 1)}.$$

Pro $p = 1, 2$ a $p = \infty$ dostaneme speciálně

$$\lambda_n(B_1^n) = \frac{2^n}{n!}, \quad \lambda_n(B_2^n) = \frac{\pi^{n/2}}{\Gamma(n/2 + 1)}, \quad \lambda_n(B_\infty^n) = 2^n.$$

2. Postup, $p = 2$

Poněkud modernější postup je inspirován Gaussovskými náhodnými proměnnými. Integrujme funkci $f(x) = e^{-x_1^2 - \dots - x_n^2}$ v polárních souřadnicích. Tím obdržíme

$$\left(\int_{-\infty}^{\infty} e^{-t^2} dt \right)^n = \int_{\mathbb{R}^n} f(x) dx = \int_0^\infty A(\mathbb{S}^{n-1}) r^{n-1} e^{-r^2} dr,$$

kde $A(\mathbb{S}^{n-1})$ je povrch jednotkové koule v \mathbb{R}^n . Použijeme-li

$$\left(\int_{-\infty}^{\infty} e^{-t^2} dt \right)^2 = \int_{\mathbb{R}^2} e^{-x^2 - y^2} d(x, y) = \int_0^\infty (2\pi r) e^{-r^2} dr = \pi$$

a (substituce $t = r^2$)

$$\int_0^\infty r^{n-1} e^{-r^2} dr = \int_0^\infty t^{(n-1)/2} e^{-t} \frac{dt}{2\sqrt{t}} = \frac{1}{2} \int_0^\infty t^{n/2-1} e^{-t} dt = \frac{1}{2} \Gamma(n/2).$$

Je tedy

$$A(\mathbb{S}^{n-1}) = \frac{2\pi^{n/2}}{\Gamma(n/2)} \quad \text{a} \quad \lambda_2(B_2^n) = A(\mathbb{S}^{n-1}) \int_0^1 r^{n-1} dr = \frac{2\pi^{n/2}}{n\Gamma(n/2)} = \frac{\pi^{n/2}}{\Gamma(n/2 + 1)}.$$

2. Postup, obecně p :

Na první pohled se zdá být nemožné zobecnit předchozí postup na $p \neq 2$. Využili jsme totiž polárních souřadnic a Gaussovských integrálů s e^{-t^2} . Přesto je toto zobecnění možné, a nedá ani tolik práce.¹⁰

¹⁰G. Schechtman & J. Zinn: *On the volume of the intersection of two L_p^n balls*, Proc. Amer. Math. Soc. 110 (1990), 217–224

Začneme malým pozorováním: Náhodný bod na sféře \mathbb{S}^{n-1} lze vygenerovat například tak, že vezmeme n nezávislých Gaussovských proměnných $\omega_1, \dots, \omega_n$ a vynormujeme je, tedy

$$\mathbb{P}\left(\frac{(\omega_1, \dots, \omega_n)}{\|\omega\|_2} \in A\right) = \sigma(A), \quad A \subset \mathbb{S}^{n-1},$$

kde σ je normalizovaná povrchová míra na \mathbb{S}^{n-1} a A je libovolná měřitelná podmnožina \mathbb{S}^{n-1} .¹¹

Pro $0 < p < \infty$ definujeme $\omega_1, \dots, \omega_n$ jako nezávislé náhodné proměnné s hustotou rozdělení

$$c_p e^{-t^p}, \quad t > 0.$$

Konstanta c_p je samozřejmě volena tak, aby šlo o pravděpodobnostní míru, tedy aby

$$c_p \int_0^\infty e^{-t^p} dt = 1.$$

Jednoduchá substituce $r = t^p$ dává, že $c_p = p/\Gamma(1/p) = 1/\Gamma(1/p + 1)$. Dále definujeme

$$\Delta_p^n = \{(t_1, \dots, t_n) : t_i \geq 0, \|t\|_p^p = 1\}$$

a *cone measure*¹²

$$\mu(A) = \frac{\lambda_n([0, 1] \cdot A)}{\lambda_n([0, 1] \cdot \Delta_p^n)}, \quad A \subset \Delta_p^n,$$

kde symbolem $[0, 1] \cdot A$ myslíme samozřejmě množinu $\{\alpha \cdot t : \alpha \in [0, 1], t \in A\}$.

Dokážeme postupně několik zajímavých vlastností zobecněných Gaussovských proměnných a cone measure.

- Náhodné veličiny

$$\frac{(\omega_1, \dots, \omega_n)}{\|\omega\|_p} \quad \text{a} \quad \|\omega\|_p$$

jsou nezávislé a

$$\mathbb{P}\left(\frac{(\omega_1, \dots, \omega_n)}{\|\omega\|_p} \in A\right) = \mu(A), \quad A \subset \Delta_p^n.$$

Důkaz. Necht' $A \subset \Delta_p^n$. Pak

$$\begin{aligned} \mathbb{P}\left(\frac{\omega}{\|\omega\|_p} \in A \mid \|\omega\|_p = a\right) &:= \lim_{\varepsilon \rightarrow 0} \frac{\mathbb{P}(\omega \in (a - \varepsilon, a + \varepsilon) \cdot A)}{\mathbb{P}(a - \varepsilon < \|\omega\|_p < a + \varepsilon)} \\ &= \lim_{\varepsilon \rightarrow 0} \frac{\int_{(a-\varepsilon, a+\varepsilon) \cdot A} e^{-\|t\|_p^p} dt}{\int_{(a-\varepsilon, a+\varepsilon) \cdot \Delta_p^n} e^{-\|t\|_p^p} dt} \\ &\leq \limsup_{\varepsilon \rightarrow 0} \frac{e^{(a+\varepsilon)^p - (a-\varepsilon)^p} \lambda_n((a - \varepsilon, a + \varepsilon) \cdot A)}{\lambda_n((a - \varepsilon, a + \varepsilon) \cdot \Delta_p^n)} \\ &= \lim_{\varepsilon \rightarrow 0} \frac{\lambda_n((a + \varepsilon) \cdot [0, 1] \cdot A) - \lambda_n((a - \varepsilon) \cdot [0, 1] \cdot A)}{\lambda_n((a + \varepsilon) \cdot [0, 1] \cdot \Delta_p^n) - \lambda_n((a - \varepsilon) \cdot [0, 1] \cdot \Delta_p^n)} \\ &= \lim_{\varepsilon \rightarrow 0} \frac{\lambda_n([0, 1] \cdot A)((a + \varepsilon)^n - (a - \varepsilon)^n)}{\lambda_n([0, 1] \cdot \Delta_p^n)((a + \varepsilon)^n - (a - \varepsilon)^n)} = \mu(A). \end{aligned}$$

¹¹Formální důkaz tohoto tvrzení plyne nejjednodušeji z Haarovy věty - obě míry jsou rotačně invariantní pravděpodobnostní míry na \mathbb{S}^{n-1} .

¹²... kuželovou míru?!

Stejně se dokáže odhad zezdola. Pravděpodobnost, že $\omega/\|\omega\|_p$ padne či nepadne do A , tedy opravdu nezávisí na hodnotě $\|\omega\|_p$, a je rovna $\mu(A)$. \square

- Pro $A \subset \mathbb{R}_+^n$ měřitelnou platí

$$\frac{\lambda_n(A)}{\lambda_n([0, 1] \cdot \Delta_p^n)} = n \int_0^\infty r^{n-1} \mu(A/r) dr.$$

Důkaz. Důkaz provedeme pro $A = [a, b] \cdot B$, kde $B \subset \Delta_p^n$ a $a < b$ (zbytek plyne ze standardních aproximačních argumentů)

$$\begin{aligned} n \int_0^\infty r^{n-1} \mu(A/r) dr &= n \int_0^\infty r^{n-1} \mu\left(\frac{[a, b] \cdot B}{r}\right) dr = n \int_a^b r^{n-1} \mu(B) dr \\ &= \mu(B)(b^n - a^n) = \frac{\lambda_n([0, 1] \cdot B)(b^n - a^n)}{\lambda_n([0, 1] \cdot \Delta_p^n)} \\ &= \frac{\lambda_n([0, b] \cdot B) - \lambda_n([0, a] \cdot B)}{\lambda_n([0, 1] \cdot \Delta_p^n)} = \frac{\lambda_n([a, b] \cdot B)}{\lambda_n([0, 1] \cdot \Delta_p^n)}. \end{aligned}$$

\square

- Pro každou integrovatelnou $f : \mathbb{R}_+^n \rightarrow \mathbb{R}$ platí *polarizační identita*

$$\frac{\int_{\mathbb{R}_+^n} f(x) d\lambda(x)}{\lambda([0, 1] \cdot \Delta_p^n)} = n \int_0^\infty r^{n-1} \int_{\Delta_p^n} f(rx) d\mu(x) dr.$$

Důkaz. Pro $f = \chi_A$, $A \subset \mathbb{R}_+^n$ se polarizační identita redukuje na rovnost v předchozím bodě. Zbytek jsou opět standardní aproximační argumenty. \square

- Použijeme-li polarizační identitu na funkci $f(x) = e^{-x_1^p - \dots - x_n^p}$, dostaneme

$$\frac{\left(\int_0^\infty e^{-t^p} dt\right)^n}{2^{-n} \lambda_n(B_p^n(\mathbb{R}))} = n \int_0^\infty r^{n-1} e^{-r^p} dr.$$

Po substituci $s = t^p$ a použití definice funkce gamma již dostaneme hledanou formuli pro objem koule.

3. Postup, obecné p

Předchozí postup lze zjednodušit.¹³ Nechť f je hladká nezáporná funkce na $[0, \infty)$ rychle klesající k nule u nekonečna. Pak platí

$$\begin{aligned} \int_{\mathbb{R}^n} f(\|x\|_p) dx &= - \int_{\mathbb{R}^n} \int_{\|x\|_p}^\infty f'(t) dt dx = - \int_0^\infty \int_{x:\|x\|_p \leq t} 1 dx f'(t) dt \\ &= - \int_0^\infty \text{vol}(tB_p^n) f'(t) dt = - \text{vol}(B_p^n) \int_0^\infty t^n f'(t) dt \\ &= \text{vol}(B_p^n) \cdot \int_0^\infty n t^{n-1} f(t) dt. \end{aligned} \tag{6.1}$$

¹³Tento přístup je možné najít např. v Pisierově knize o konvexních tělesech na str. 11. . .

Dosadíme-li $f(t) = e^{-t^p}$, obdržíme

$$\begin{aligned} \int_{\mathbb{R}^n} e^{-\|x\|_p^p} dx &= \text{vol}(B_p^n) \cdot \int_0^\infty n t^{n-1} e^{-t^p} dt = \text{vol}(B_p^n) \cdot \frac{n}{p} \cdot \int_0^\infty s^{n/p-1} e^{-s} ds \\ &= \frac{n \text{vol}(B_p^n) \Gamma(n/p)}{p} = \text{vol}(B_p^n) \Gamma(1 + n/p). \end{aligned} \tag{6.2}$$

Celý výpočet je pak dokončen Fubiniovou větou

$$\begin{aligned} \text{vol}(B_p^n) \Gamma(1 + n/p) &= \int_{\mathbb{R}^n} e^{-\|x\|_p^p} dx = \left(2 \int_0^\infty e^{-t^p} dt \right)^n = 2^n \left(\frac{1}{p} \int_0^\infty s^{1/p-1} e^{-s} ds \right)^n \\ &= 2^n \left(\frac{\Gamma(1/p)}{p} \right)^n = 2^n \Gamma(1 + 1/p)^n. \end{aligned}$$

7 Koncentrace míry a Johnson-Lindenstraussovo vnoření

Normální náhodná proměnná je definována svým rozdělením

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}.$$

Pro ty, kteří nemají rádi statistiku, ale přesto nechtějí ignorovat posledních čtyřicet let vývoje funkcionální analýzy¹⁴, bude možná schůdnější představa pravděpodobnostního prostoru $\Omega = (\mathbb{R}, \mu)$, kde $\mu(A) = \int_A f$. Normální náhodná proměnná je pak prostě funkce $\omega(x) = x$ na tomto Ω . Její střední hodnota je

$$\mathbb{E} \omega = \int_{\mathbb{R}} x d\mu(x) = \int_{\mathbb{R}} x f(x) dx = 0$$

a její variance

$$\sigma^2 = \int_{-\infty}^{\infty} x^2 d\mu(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x^2 e^{-x^2/2} dx = \frac{1}{\sqrt{2\pi}} [-x \cdot e^{-x^2/2}]_{-\infty}^{\infty} - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} -e^{-x^2/2} dx = 1.$$

Konečně n nezávislých náhodných proměnných $\omega = (\omega_1, \dots, \omega_n)$ si můžeme představit jako funkci $f(x) = x$ na $\Omega = (\mathbb{R}^n, \mu)$, kde $\mu(A) = \int_A f(x_1) \dots f(x_n) dx = \frac{1}{(2\pi)^{n/2}} \int_A e^{-\|x\|_2^2/2} dx$.

Normální náhodné proměnné mají řadu pěkných (např. geometrických) vlastností. V následujícím budeme potřebovat tyto dvě:

Lemma 7.1. (i) *Nechť ω je normální proměnná. Pak $\mathbb{E}(e^{\lambda\omega^2}) = 1/\sqrt{1-2\lambda}$ pro $-\infty < \lambda < 1/2$.*

(ii) *(2-stabilita normálního rozdělení) Nechť $m \in \mathbb{N}$, nechť $\lambda = (\lambda_1, \dots, \lambda_m) \in \mathbb{R}^m$ a nechť $\omega_1, \dots, \omega_m$ jsou nezávislé normální proměnné. Pak $\lambda_1\omega_1 + \dots + \lambda_m\omega_m \sim (\sum_{i=1}^m \lambda_i^2)^{1/2} \cdot \mathcal{N}(0, 1)$, neboli má stejné rozdělení jako násobek normální proměnné.*

Důkaz. Důkaz (i) plyne ze substituce $s := \sqrt{1-2\lambda} \cdot t$ následujícím způsobem.

$$\begin{aligned} \mathbb{E}(e^{\lambda\omega^2}) &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{\lambda t^2} \cdot e^{-t^2/2} dt = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{(\lambda-1/2)t^2} dt \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-s^2/2} \cdot \frac{ds}{\sqrt{1-2\lambda}} = \frac{1}{\sqrt{1-2\lambda}}. \end{aligned}$$

Vlastnost (ii) je sice dobře známá, pro úplnost ale uvedeme jednoduchý geometrický důkaz. Stačí dokázat případ $m = 2$, zbytek plyne snadno indukci.

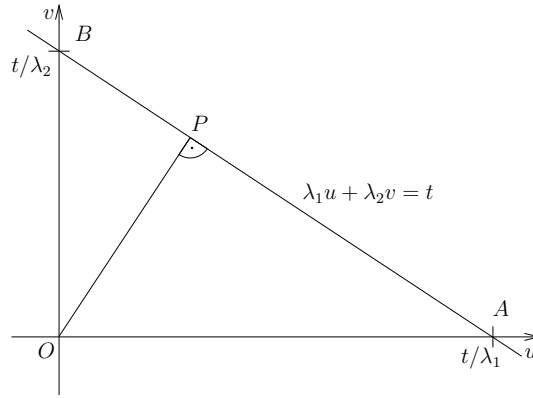
¹⁴... jako jsem třeba já ...

Nechť tedy $\lambda = (\lambda_1, \lambda_2) \in \mathbb{R}^2, \lambda \neq 0$ je pevné a nechť ω_1 a ω_2 jsou dvě nezávislé normální náhodné proměnné. Položme $S := \lambda_1\omega_1 + \lambda_2\omega_2$. Nechť $t \geq 0$ je libovolné nezáporné reálné číslo. Pak platí

$$\begin{aligned} \mathbb{P}(S \leq t) &= \frac{1}{2\pi} \int_{(u,v): \lambda_1 u + \lambda_2 v \leq t} e^{-(u^2+v^2)/2} dudv = \frac{1}{2\pi} \int_{u \leq c; v \in \mathbb{R}} e^{-(u^2+v^2)/2} dudv \\ &= \frac{1}{\sqrt{2\pi}} \int_{u \leq c} e^{-u^2/2} du. \end{aligned}$$

Přitom jsme použili rotační invariance funkce $(u, v) \rightarrow e^{-(u^2+v^2)/2}$. Hodnota c je dána vzdáleností přímky $\{(u, v) : \lambda_1 u + \lambda_2 v = t\}$ od počátku. Pomocí elementární geometrie a Pythagorovy věty (cf. $\triangle OAP \simeq \triangle BAO$ v obr. 1) dostaneme

$$c = |OP| = |OB| \cdot \frac{|OA|}{|AB|} = \frac{t}{\sqrt{\lambda_1^2 + \lambda_2^2}}.$$



Obrázek 1: Výpočet $c = |OP|$ pomocí elementární geometrie pro $\lambda_1, \lambda_2 > 0$

Dostaneme tedy

$$\mathbb{P}(S \leq t) = \frac{1}{\sqrt{2\pi}} \int_{\sqrt{\lambda_1^2 + \lambda_2^2} \cdot u \leq t} e^{-u^2/2} du = \mathbb{P}\left(\sqrt{\lambda_1^2 + \lambda_2^2} \cdot \omega \leq t\right).$$

Stejný odhad platí pro negativní t pomocí symetrie a důkaz je hotov. \square

Pokud jsou $\omega_1, \dots, \omega_m$ normální náhodné proměnné (ne nutně nezávislé), pak $\mathbb{E}(\omega_1^2 + \dots + \omega_m^2) = m$. Pokud jsou ale $\omega_1, \dots, \omega_m$ dokonce i nezávislé, pak se hodnota $\omega_1^2 + \dots + \omega_m^2$ koncentruje velice silně okolo m . Tento efekt je znám jako *koncentrace míry*¹⁵

Lemma 7.2. *Nechť $m \in \mathbb{N}$ a nechť $\omega_1, \dots, \omega_m$ jsou nezávislé normální proměnné. Nechť $0 < \varepsilon < 1$. Pak*

$$\mathbb{P}(\omega_1^2 + \dots + \omega_m^2 \geq (1 + \varepsilon)m) \leq e^{-\frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]}$$

¹⁵concentration of measure, cf.

Ledoux, M.: The concentration of measure phenomenon. American Mathematical Society, Providence, (2001)

Ledoux, M., Talagrand, M.: Probability in Banach spaces. Isoperimetry and processes. Springer, Berlin, (1991)

Milman, V.D., Schechtman, G.: Asymptotic theory of finite-dimensional normed spaces. Springer, Berlin (1986)

a

$$\mathbb{P}(\omega_1^2 + \dots + \omega_m^2 \leq (1 - \varepsilon)m) \leq e^{-\frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]}.$$

Důkaz. Dokážeme pouze první nerovnost. Důkaz druhé probíhá velice podobně. Položme $\beta := 1 + \varepsilon > 1$ a počítejme

$$\begin{aligned} \mathbb{P}(\omega_1^2 + \dots + \omega_m^2 \geq \beta m) &= \mathbb{P}(\omega_1^2 + \dots + \omega_m^2 - \beta m \geq 0) \\ &= \mathbb{P}(\lambda(\omega_1^2 + \dots + \omega_m^2 - \beta m) \geq 0) \\ &= \mathbb{P}(\exp(\lambda(\omega_1^2 + \dots + \omega_m^2 - \beta m)) \geq 1) \\ &\leq \mathbb{E} \exp(\lambda(\omega_1^2 + \dots + \omega_m^2 - \beta m)), \end{aligned}$$

kde $\lambda > 0$ je kladné reálné číslo, které určíme později. V posledním kroku jsme použili Markovovu nerovnost. Dále použijeme elementární vlastnosti exponenciální funkce a

$$\mathbb{E} \left[\prod_{j=1}^N X_j \right] = \prod_{j=1}^N \mathbb{E}(X_j).$$

pro nezávislé proměnné X_1, \dots, X_m . To vede k

$$\mathbb{E} \exp(\lambda(\omega_1^2 + \dots + \omega_m^2 - \beta m)) = e^{-\lambda\beta m} \cdot \mathbb{E} e^{\lambda\omega_1^2} \dots e^{\lambda\omega_m^2} = e^{-\lambda\beta m} \cdot (\mathbb{E} e^{\lambda\omega_1^2})^m$$

a s pomocí Lemma 7.1 dostaneme konečně (pro $0 < \lambda < 1/2$)

$$\mathbb{E} \exp(\lambda(\omega_1^2 + \dots + \omega_m^2 - \beta m)) = e^{-\lambda\beta m} \cdot (1 - 2\lambda)^{-m/2}.$$

Nyní hledáme optimální hodnotu $0 < \lambda < 1/2$, která bude minimalizovat poslední výraz. Proto derivujeme $e^{-\lambda\beta m} \cdot (1 - 2\lambda)^{-m/2}$ a položíme rovno nule. Přímočarý výpočet vede k

$$\lambda = \frac{1 - 1/\beta}{2},$$

kteří zjevně splňuje také podmínku $0 < \lambda < 1/2$. Použitím této hodnoty λ dostaneme

$$\begin{aligned} \mathbb{P}(\omega_1^2 + \dots + \omega_m^2 \geq \beta m) &\leq e^{-\frac{1-1/\beta}{2} \cdot \beta m} \cdot (1 - (1 - 1/\beta))^{-m/2} = e^{-\frac{\beta-1}{2}m} \cdot \beta^{m/2} \\ &= e^{-\frac{\varepsilon m}{2}} \cdot e^{\frac{m}{2} \ln(1+\varepsilon)}. \end{aligned}$$

Výsledek pak plyne z nerovnosti

$$\ln(1+t) \leq t - \frac{t^2}{2} + \frac{t^3}{3}, \quad -1 < t < 1.$$

□

Do konce této sekce označíme

$$A = \frac{1}{\sqrt{m}} \begin{pmatrix} \omega_{1,1} & \dots & \omega_{1n} \\ \vdots & \ddots & \vdots \\ \omega_{m1} & \dots & \omega_{mn} \end{pmatrix}, \quad (7.1)$$

kde $\omega_{ij}, i = 1, \dots, m, j = 1, \dots, n$, jsou nezávislé normální proměnné.

Použitím 2-stability normálního rozdělení, Lemma 7.2 dokážeme, že A definované pomocí (7.1) je s vysokou pravděpodobností skoro isometrie pro jedno pevné $x \in \mathbb{R}^n$.

Věta 7.3. *Nechť $x \in \mathbb{R}^n$ s $\|x\|_2 = 1$ a necht' A je definováno pomocí (7.1). Pak*

$$\mathbb{P}\left(\left|\|Ax\|_2^2 - 1\right| \geq t\right) \leq 2e^{-\frac{m}{2}[t^2/2 - t^3/3]} \leq 2e^{-Cmt^2} \quad (7.2)$$

pro $0 < t < 1$ s absolutní konstantou $C > 0$.

Důkaz. Necht' $x = (x_1, x_2, \dots, x_n)^T$. Pomocí 2-stability normálního rozdělení a Lemma 7.2 dostaneme

$$\begin{aligned} & \mathbb{P}\left(\left|\|Ax\|_2^2 - 1\right| \geq t\right) \\ &= \mathbb{P}\left(\left|(\omega_{1,1}x_1 + \dots + \omega_{1,n}x_n)^2 + \dots + (\omega_{m,1}x_1 + \dots + \omega_{m,n}x_n)^2 - m\right| \geq mt\right) \\ &= \mathbb{P}\left(\left|\omega_1^2 + \dots + \omega_m^2 - m\right| \geq mt\right) \\ &= \mathbb{P}\left(\omega_1^2 + \dots + \omega_m^2 \geq m(1+t)\right) + \mathbb{P}\left(\omega_1^2 + \dots + \omega_m^2 \leq m(1-t)\right) \\ &\leq 2e^{-\frac{m}{2}[t^2/2 - t^3/3]}. \end{aligned}$$

To dává první nerovnost v (7.2). Druhá pak plyne prostým přepočtením (pro $C = 1/12$). \square

Remark 2. (i) Všimněme si, že (7.2) lze snadno homogenizovat na

$$\mathbb{P}\left(\left|\|Ax\|_2^2 - \|x\|_2^2\right| \geq t\|x\|_2^2\right) \leq 2e^{-Cmt^2}, \quad (7.3)$$

které platí pro všechna $x \in \mathbb{R}^n$.

(ii) Poněkud odlišný důkaz (7.2) je založen na rotační invariance rozdělení matic definovaných pomocí (7.1). Stačí tedy dokázat (7.2) pro jeden pevný prvek $x \in \mathbb{R}^n$ s $\|x\|_2 = 1$. Vezměme-li $x = e_1 = (1, 0, \dots, 0)^T$ jako první kanonický vektor, můžeme použít Lemma 7.2 bez nutnosti aplikovat 2-stabilitu normálního rozdělení.

Koncentrační nerovnosti podobné (7.2) hrají zásadní roli v mnoha oblastech matematiky. My ukážeme jejich souvislost s klasickým výsledkem funkcionální analýzy zvaným Johnson-Lindenstraussovo lemma¹⁶. Toto lemma říká, že množinu bodů ve vysocedimenzionálním prostoru je možné vnořit do prostoru mnohem menší dimenze, a to takovým způsobem, že vzájemné vzdálenosti mezi body jsou téměř zachovány.

Lemma 7.4. *Nechť $0 < \varepsilon < 1$ a necht' m, N a n jsou přirozená čísla s*

$$m \geq 4(\varepsilon^2/2 - \varepsilon^3/3)^{-1} \ln N.$$

Pak pro každou množinu $\{x^1, \dots, x^N\} \subset \mathbb{R}^n$ existuje zobrazení $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$, takové že

$$(1 - \varepsilon)\|x^i - x^j\|_2^2 \leq \|f(x^i) - f(x^j)\|_2^2 \leq (1 + \varepsilon)\|x^i - x^j\|_2^2, \quad i, j \in \{1, \dots, N\}. \quad (7.4)$$

Důkaz. Položme $f(x) = Ax$, kde opět

$$Ax = \frac{1}{\sqrt{m}} \begin{pmatrix} \omega_{1,1} & \dots & \omega_{1,n} \\ \vdots & \ddots & \vdots \\ \omega_{m,1} & \dots & \omega_{m,n} \end{pmatrix} x,$$

¹⁶cf. Johnson, W.B., Lindenstrauss, J.: Extensions of Lipschitz mappings into a Hilbert space. In: Conf. in Modern Analysis and Probability, pp. 189–206, (1984)

a $\omega_{ij}, i = 1, \dots, m, j = 1, \dots, n$ jsou nezávislé normální proměnné. Ukážeme, že s touto volbou splňuje f podmínku (7.4) s kladnou pravděpodobností. Tím bude existence takového zobrazení dokázána.

Nechť $i, j \in \{1, \dots, N\}$ jsou libovolné s $x^i \neq x^j$. Pak položíme $z = \frac{x^i - x^j}{\|x^i - x^j\|_2}$ a vypočteme pravděpodobnost, že pravá strana (7.4) neplatí. Věta 7.3 pak implikuje

$$\begin{aligned} \mathbb{P}\left(\left|\|f(x^i) - f(x^j)\|_2^2 - \|x^i - x^j\|_2^2\right| > \varepsilon \|x^i - x^j\|_2^2\right) &= \mathbb{P}\left(\left|\|Az\|^2 - 1\right| > \varepsilon\right) \\ &\leq e^{-\frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]}. \end{aligned}$$

Tentýž odhad platí i pro všechny $\binom{N}{2}$ páry $\{i, j\} \subset \{1, \dots, N\}$ s $i \neq j$. Pravděpodobnost, že jedna z nerovností v (7.4) neplatí, je tedy nejvýše

$$2 \cdot \binom{N}{2} \cdot e^{-\frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]} < N^2 \cdot e^{-\frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]} = \exp\left(2 \ln N - \frac{m}{2}[\varepsilon^2/2 - \varepsilon^3/3]\right) \leq e^0 = 1$$

pro $m \geq 4(\varepsilon^2/2 - \varepsilon^3/3)^{-1} \ln N$. Pravděpodobnost, že (7.4) platí pro všechna $i, j \in \{1, \dots, N\}$ je tedy pozitivní a důkaz je hotov. \square

8 Geometrické nerovnosti

17

Dokážeme Prekopa-Leindlerovu nerovnost a Brunn-Minkowského nerovnost, které poté použijeme při důkazu isoperimetrické nerovnosti a Brunnova principu.

Věta 8.1. (i) (Brunn-Minkowski) Pro libovolné měřitelné $A, B \subset \mathbb{R}^n$ platí

(1) (aditivní forma) $\text{vol}(A + B)^{1/n} \geq \text{vol}(A)^{1/n} + \text{vol}(B)^{1/n}$,

(2) (multiplikativní forma) $\text{vol}(\lambda A + (1 - \lambda)B) \geq \text{vol}(A)^\lambda \text{vol}(B)^{1-\lambda}$.

(ii) (Prekopa-Leindler) Nechť $f, g, h : \mathbb{R}^n \rightarrow [0, \infty)$ jsou měřitelné funkce a nechť $\lambda \in (0, 1)$. Předpokládejme, že pro všechna $x, y \in \mathbb{R}^n$

$$h(\lambda x + (1 - \lambda)y) \geq f(x)^\lambda g(y)^{1-\lambda}.$$

Pak

$$\int_{\mathbb{R}^n} h \geq \left(\int_{\mathbb{R}^n} f \right)^\lambda \left(\int_{\mathbb{R}^n} g \right)^{1-\lambda}.$$

Důkaz. 1. krok: (1) a (2) v Brunn-Minkowského nerovnosti jsou ekvivalentní.

Nechť platí (1) - do které dosadíme λA místo A a $(1 - \lambda)B$ místo B . Použitím nerovnosti mezi aritmetickým a geometrickým průměrem (nebo konkávnosti logaritmu) dostaneme

$$\begin{aligned} \log\left(\text{vol}(\lambda A + (1 - \lambda)B)^{1/n}\right) &\geq \log\left(\text{vol}(\lambda A)^{1/n} + \text{vol}((1 - \lambda)B)^{1/n}\right) \\ &= \log\left(\lambda \text{vol}(A)^{1/n} + (1 - \lambda) \text{vol}(B)^{1/n}\right) \\ &\geq \lambda \log\left(\text{vol}(A)^{1/n}\right) + (1 - \lambda) \log\left(\text{vol}(B)^{1/n}\right) \\ &= \log\left(\text{vol}(A)^{\lambda/n} \text{vol}(B)^{(1-\lambda)/n}\right), \end{aligned}$$

a tedy (2).

Pokud platí (2), dosadíme

$$A' = \frac{A}{\text{vol}(A)^{1/n}}, \quad B' = \frac{B}{\text{vol}(B)^{1/n}}, \quad \lambda = \frac{\text{vol}(A)^{1/n}}{\text{vol}(A)^{1/n} + \text{vol}(B)^{1/n}}$$

a obdržíme

$$\text{vol}\left(\frac{A + B}{\text{vol}(A)^{1/n} + \text{vol}(B)^{1/n}}\right) = \text{vol}(\lambda A' + (1 - \lambda)B') \geq \text{vol}(A')^\lambda \text{vol}(B')^{1-\lambda} = 1.$$

2. krok: Jednodimenzionální Brunn-Minkowski.

Díky regularitě Lebesgueovy míry stačí uvažovat A a B kompaktní. Díky její translační invarianci navíc můžeme předpokládat

$$\sup A = 0 = \inf B.$$

Pak $A \subset A + B$ a $B \subset A + B$. Celkem tedy $|A| + |B| = |A \cup B| \leq |A + B|$.

¹⁷Převzato z R. Vershynin, Lectures in Geometric Functional Analysis

3. krok: *Jednodimenzionální Prekopa-Leindler.*

Nechť $a \geq 0$. Jestliže pro $x, y \in \mathbb{R}$ platí $f(x) \geq a$ a $g(y) \geq a$, pak i

$$h(\lambda x + (1 - \lambda)y) \geq f(x)^\lambda g(y)^{1-\lambda} \geq a,$$

a tedy $\lambda x + (1 - \lambda)y \in \{z : h(z) \geq a\}$. Celkem tedy máme

$$\lambda\{f \geq a\} + (1 - \lambda)\{g \geq a\} \subset \{h \geq a\}.$$

Z jednodimenzionální Brunn-Minkowského nerovnosti pak plyne

$$\begin{aligned} \lambda|\{f \geq a\}| + (1 - \lambda)|\{g \geq a\}| &= |\lambda\{f \geq a\}| + |(1 - \lambda)\{g \geq a\}| \\ &\leq |\lambda\{f \geq a\} + (1 - \lambda)\{g \geq a\}| \leq |\{h \geq a\}|. \end{aligned}$$

Konečně využijeme

$$\int f = \int_0^\infty |\{f \geq a\}| da$$

a obdržíme

$$\left(\int f\right)^\lambda \left(\int g\right)^{1-\lambda} \leq \lambda \int f + (1 - \lambda) \int g \leq \int h,$$

kde první nerovnost je opět nerovnost mezi aritmetickým a geometrickým průměrem.

4. krok: *Indukce přes dimenzi v Prekopa-Leindler.*

Předpokládejme, že tvrzení platí na \mathbb{R}^{n-1} . Pro $t \in \mathbb{R}$ uvažujme funkce

$$f_t, g_t, h_t : \mathbb{R}^{n-1} \rightarrow \mathbb{R}$$

definované $f_t(x) = f(t, x)$ a obdobně pro g, h . Nechť $t = \lambda t_1 + (1 - \lambda)t_2$. Pak

$$\begin{aligned} h_t(\lambda x + (1 - \lambda)y) &= h(t, \lambda x + (1 - \lambda)y) = h(\lambda t_1 + (1 - \lambda)t_2, \lambda x + (1 - \lambda)y) \\ &\geq f(t_1, x)^\lambda g(t_2, y)^{1-\lambda} = f_{t_1}(x)^\lambda g_{t_2}(y)^{1-\lambda} \end{aligned}$$

pro všechna $x, y \in \mathbb{R}^{n-1}$. Podle indukčního kroku tedy platí

$$\int_{\mathbb{R}^{n-1}} h_t \geq \left(\int_{\mathbb{R}^{n-1}} f_{t_1}\right)^\lambda \left(\int_{\mathbb{R}^{n-1}} g_{t_2}\right)^{1-\lambda}.$$

Konečně, použijeme jednodimenzionální Prekopa-Leindlerovu nerovnost pro funkce

$$F : t_1 \rightarrow \int_{\mathbb{R}^{n-1}} f_{t_1}, \quad G : t_2 \rightarrow \int_{\mathbb{R}^{n-1}} g_{t_2}, \quad H : t \rightarrow \int_{\mathbb{R}^{n-1}} h_t$$

a dostaneme

$$\int_{\mathbb{R}^n} h = \int_{\mathbb{R}} H \geq \left(\int_{\mathbb{R}} F\right)^\lambda \left(\int_{\mathbb{R}} G\right)^{1-\lambda} = \left(\int_{\mathbb{R}^n} f\right)^\lambda \left(\int_{\mathbb{R}^n} g\right)^{1-\lambda}.$$

5. krok: *Obecná dimenze Brunn-Minkowského nerovnosti.*

Položme $f = \chi_A, g = \chi_B, h = \chi_{\lambda A + (1-\lambda)B}$ a dosaďme do Prekopa-Leindlerovy nerovnosti. Obdržíme multiplikativní formu Brunn-Minkowského nerovnosti. \square

Isoperimetrická nerovnost v \mathbb{R}^n

Nechť $A \subset \mathbb{R}^n$ je měřitelná. Pak definujeme její *povrch* jako

$$\text{vol}(\partial A) = \lim_{\varepsilon \rightarrow 0^+} \frac{\text{vol}(A + \varepsilon B_2^n) - \text{vol}(A)}{\varepsilon}$$

(pokud tato limita existuje).

Věta 8.2. (*Isoperimetrická nerovnost v \mathbb{R}^n*) Mezi všemi tělesy daného objemu v \mathbb{R}^n (které mají povrch) má koule nejmenší povrch.

Důkaz. Buď $A \subset \mathbb{R}^n$ a B Eukleidovská koule s $\text{vol}(B) = \text{vol}(A)$. Chceme dokázat, že $\text{vol}(\partial A) \geq \text{vol}(\partial B)$. Z Brunn-Minkowského nerovnosti plyne

$$\begin{aligned} \text{vol}(A + \varepsilon B_2^n)^{1/n} &\geq \text{vol}(A)^{1/n} + \text{vol}(\varepsilon B_2^n)^{1/n} = \text{vol}(B)^{1/n} + \text{vol}(\varepsilon B_2^n)^{1/n} \\ &= \text{vol}(B + \varepsilon B_2^n)^{1/n}. \end{aligned}$$

Nyní stačí umocnit obě strany nerovnosti na n , odečíst od obou stran $\text{vol}(A) = \text{vol}(B)$, vydělit $\varepsilon > 0$ a vzít limitu pro $\varepsilon \rightarrow 0^+$. \square

Brunnův princip

Věta 8.3. Nechť K je konvexní těleso v \mathbb{R}^n a $u \in \mathbb{R}^n \setminus \{0\}$. Označíme-li

$$H_t = \{x \in \mathbb{R}^n : \langle x, u \rangle = t\},$$

pak funkce

$$t \rightarrow \text{vol}(K \cap H_t)^{\frac{1}{n-1}}$$

je konkávní na svém nosiči.

Důkaz. Objem v zadání je $(n-1)$ -dimenzionální Lebesgueova míra na H_t . Ekvivalentně můžeme uvažovat ortogonální projekci na H_0 a $(n-1)$ -dimenzionální Lebesgueovu míru na H_0 , tedy $\text{vol}(K \cap H_t) = \text{vol}(P_{H_0}(K \cap H_t))$.

Označme ještě $K_t = K \cap H_t$. Z konvexity K plyne pro každé $r, s \in \mathbb{R}$ a $\lambda \in (0, 1)$

$$K_{\lambda r + (1-\lambda)s} \supset \lambda K_r + (1-\lambda)K_s$$

a totéž platí i pro projekce do H_0

$$P_{H_0}(K_{\lambda r + (1-\lambda)s}) \supset \lambda P_{H_0}(K_r) + (1-\lambda)P_{H_0}(K_s).$$

Výsledek pak plyne z Brunn-Minkowského nerovnosti na H_0

$$\begin{aligned} \text{vol}(K_{\lambda r + (1-\lambda)s})^{\frac{1}{n-1}} &= \text{vol}(P_{H_0}(K_{\lambda r + (1-\lambda)s}))^{\frac{1}{n-1}} \geq \text{vol}(\lambda P_{H_0}(K_r) + (1-\lambda)P_{H_0}(K_s))^{\frac{1}{n-1}} \\ &\geq \text{vol}(\lambda P_{H_0}(K_r))^{\frac{1}{n-1}} + \text{vol}((1-\lambda)P_{H_0}(K_s))^{\frac{1}{n-1}} \\ &= \lambda \text{vol}(P_{H_0}(K_r))^{\frac{1}{n-1}} + (1-\lambda) \text{vol}(P_{H_0}(K_s))^{\frac{1}{n-1}} \\ &= \lambda \text{vol}(K_r)^{\frac{1}{n-1}} + (1-\lambda) \text{vol}(K_s)^{\frac{1}{n-1}}. \end{aligned}$$

\square

9 Disperze

Nechť $d \in \mathbb{N}$ a necht' $\mathcal{P} \subset [0, 1]^d$ je libovolná množina. Pak definujeme *disperzi* \mathcal{P}

$$\text{disp}(\mathcal{P}) := \sup_{B: B \cap \mathcal{P} = \emptyset} |B|,$$

(supremum je bráno přes všechny kvádry s hranami rovnoběžnými se souřadnými osami, tedy $B = I_1 \times \dots \times I_d$, $I_\ell \subset [0, 1]$ jsou intervaly, a $|B|$ je objem B). Disperze \mathcal{P} je tedy objem největšího kvádru, který neobsahuje žádný bod z \mathcal{P} .

Pro pevné $n \geq 1$ budeme hledat množinu \mathcal{P} s n prvky, která bude mít minimální disperzi, definujeme tedy

$$\text{disp}(n, d) := \inf_{\substack{\mathcal{P} \subset [0, 1]^d: \\ \#\mathcal{P} = n}} \text{disp}(\mathcal{P})$$

a její inverzní funkci

$$N(\varepsilon, d) := \min \left\{ n : \text{disp}(n, d) \leq \varepsilon \right\}.$$

Jakub Sosnovec dokázal v roce 2017, že pro každé pevné $0 < \varepsilon < 1/4$ existuje $c_\varepsilon > 0$ tak, že platí

$$N(\varepsilon, d) \leq c_\varepsilon \log_2(d).$$

Cílem této kapitoly je zjemnění Sosnovcova argumentu, které vylepší závislost c_ε na $\varepsilon > 0$.

Věta 9.1. *Nechť $d \geq 2$ je přirozené číslo a necht' $\varepsilon \in (0, 1/2)$. Pak existuje $\mathcal{P} \subset [0, 1]^d$ s $\text{disp}(\mathcal{P}) \leq \varepsilon$ a*

$$\#\mathcal{P} \leq 2^7 \log_2(d) \frac{(1 + \log_2(\varepsilon^{-1}))^2}{\varepsilon^2}.$$

Toto lze přímočaře přeformulovat jako odhad pro $\text{disp}(n, d)$.

Důsledek 9.2. *Nechť $n, d \in \mathbb{N}$ s $n \geq 2$ a $d \geq 2$. Pak*

$$\text{disp}(n, d) \leq c \log_2(n) \sqrt{\frac{\log_2(d)}{n}}$$

pro absolutní konstantu $c > 0$.

Pro $0 < \varepsilon < 1/2$ zvolme $k \in \mathbb{N}$ tak, aby $2^{-k} \leq \varepsilon < 2^{-k+1}$, tedy $k = \lceil \log_2(1/\varepsilon) \rceil \geq 2$, a definujeme

$$M_k = \left\{ \frac{1}{2^k}, \frac{2}{2^k}, \dots, \frac{2^k - 1}{2^k} \right\} \subset [0, 1].$$

Budeme uvažovat náhodnou množinu bodů $X = \{x^1, x^2, \dots, x^n\} \subset M_k^d$ se složkami $(x^j)_l$ vybranými náhodně a stejnoměrně z M_k .

Ukážeme, že pro n rostoucí polynomiálně v $1/\varepsilon$ a logaritmičsky v d , X má s nenulovou pravděpodobností neprázdný průnik s každým kvádrem s hranami rovnoběžnými se souřadnými osami a objemem alespoň ε . Množinu všech kvádrů s objemem alespoň 2^{-k} rozdělíme na několik skupin. Pro $p \in M_k^d$ a $s \in \{0, \dots, 2^k - 1\}^d$ položme

$$\Omega_k := \{B \subset [0, 1]^d : |B| > 2^{-k}\}$$

a

$$\Omega_k(p, s) := \left\{ I_1 \times \cdots \times I_d \in \Omega_k: \frac{s_\ell}{2^k} < |I_\ell| \leq \frac{s_\ell + 1}{2^k} \right. \\ \left. \text{a } \inf I_\ell \in \left[p_\ell - \frac{1}{2^k}, p_\ell \right) \text{ pro všechna } \ell = 1, \dots, d \right\}.$$

Zřejmě, $\Omega_k(p, s) = \emptyset$ pokud $s_\ell = 0$ pro nějaké $\ell = 1, \dots, d$.

Hlavním krokem je následující lemma.

Lemma 9.3. *Nechť x náhodně a rovnoměrně vybrané z M_k^d . Pak pro každé $B \in \Omega_k$ platí*

$$\mathbb{P}(x \in B) > 2^{-k-4}.$$

Dále pro každé $p \in M_k^d$ a $s \in \{1, \dots, 2^k - 1\}^d$ platí

$$\mathbb{P}(\exists B \in \Omega_k(p, s): x \notin B) < \exp(-2^{-k-4}).$$

Důkaz. Nechť x je náhodně vybráno z M_k^d a $B = I_1 \times \cdots \times I_d \in \Omega_k$. Pak $B \in \Omega_k(p, s)$ pro nějaké $p \in M_k^d$ a $s \in \{1, \dots, 2^k - 1\}^d$. Dále položme $B(p, s) := \prod_{\ell=1}^d [p_\ell, p_\ell + \frac{s_\ell - 1}{2^k}]$. Zřejmě tedy $B \cap M_k^d \supset B(p, s) \cap M_k^d$ a

$$\mathbb{P}(x \in B) \geq \mathbb{P}(x \in B(p, s)) = \prod_{\ell=1}^d \left(\frac{s_\ell}{2^k - 1} \right) = \prod_{\ell \in D_s} \left(\frac{s_\ell}{2^k - 1} \right),$$

kde $D_s := \{\ell \in \{1, \dots, d\} : s_\ell < 2^k - 1\}$. Pro další postup využijeme nerovnost

$$\left(\frac{j}{2^k - 1} \right) \geq \left(1 - \frac{1}{k2^k} \right) \left(\frac{j+1}{2^k} \right)^{\frac{k}{k-1}} \text{ pro všechna } j = 1, \dots, 2^k - 2, \quad (9.1)$$

jejíž důkaz provedem později. Tím dostaneme

$$\mathbb{P}(x \in B) \geq \left(1 - \frac{1}{k2^k} \right)^{|D_s|} \prod_{\ell \in D_s} \left(\frac{s_\ell + 1}{2^k} \right)^{\frac{k}{k-1}} \\ \geq \left(1 - \frac{1}{k2^k} \right)^{|D_s|} |B|^{\frac{k}{k-1}}.$$

Protože $|D_s| = m_1(s) < \ln(2)k2^k$, see (9.3), můžeme dále odhadovat

$$\mathbb{P}(x \in B) \geq \left(1 - \frac{1}{k2^k} \right)^{\ln(2)k2^k} 2^{-\frac{k^2}{k-1}} \geq \left(1 - \frac{1}{8} \right)^{8 \ln(2)} 2^{-\frac{k^2}{k-1}} \\ > \frac{1}{4} \cdot 2^{-\frac{k^2}{k-1}} \geq \frac{1}{16} \cdot 2^{-k},$$

kde jsme použili monotonii posloupnosti $(1 - 1/k)^k$ a $\frac{k^2}{k-1} \leq k + 2$ for $k \geq 2$.

Pro důkaz (9.1) využijeme ekvivalentní reformulace

$$\min_{j=1,2,\dots,2^k-2} \frac{j}{(j+1)^{\frac{k}{k-1}}} \geq (2^k - 1) 2^{-\frac{k^2}{k-1}} \left(1 - \frac{1}{k2^k} \right). \quad (9.2)$$

Protože funkce $t \rightarrow \frac{t}{(1+t)^{\frac{k}{k-1}}}$ má jen jeden lokální extrém na $(0, \infty)$ a tento extrém je lokální maximum, stačí uvažovat $j \in \{1, 2^k - 2\}$ a dokázat

$$\min\left(\frac{1}{2^{\frac{k}{k-1}}}, \frac{2^k - 2}{(2^k - 1)^{\frac{k}{k-1}}}\right) \geq (2^k - 1)2^{-\frac{k^2}{k-1}}\left(1 - \frac{1}{k2^k}\right).$$

Tato nerovnost se přirozeně rozpadá na dvě části. První (pro $j = 1$) plyne z

$$\frac{1}{2^{\frac{k}{k-1}}} = 2^k \cdot 2^{-\frac{k^2}{k-1}}.$$

Druhá, pro $j = 2^k - 2$, je ekvivalentní

$$\frac{2^k - 2}{2^k - 1} \geq \left(\frac{2^k - 1}{2^k}\right)^{\frac{k}{k-1}}\left(1 - \frac{1}{k2^k}\right),$$

kteřá bude (díky monotonii) dokázána, pokud ji dokážeme s exponentem $\frac{k}{k-1}$ nahrazeným jedničkou, tedy

$$\frac{2^k - 2}{2^k - 1} \geq \left(\frac{2^k - 1}{2^k}\right)\left(1 - \frac{1}{k2^k}\right).$$

Pomocí jednoduchých úprav je tato nerovnost ekvivalentní

$$2^{2k} - 2 \cdot 2^k \geq (2^k - 1)^2\left(1 - \frac{1}{k2^k}\right) = 2^{2k} - 2 \cdot 2^k + 1 - \frac{2^{2k} - 2 \cdot 2^k + 1}{k2^k}$$

a

$$2^{2k} - 2 \cdot 2^k + 1 \geq k \cdot 2^k,$$

kteřá platí pro $k \geq 2$. Tím je hotov důkaz $\mathbb{P}(x \in B) > 2^{-k-4}$ pro všechna $B \in \Omega_k$.

Pro důkaz druhé části lemmatu si všimněme, že $B \cap M_k^d \supset B(p, s) \cap M_k^d$ pro všechna $B \in \Omega_k(p, s)$. Tím dostaneme

$$\mathbb{P}(\forall B \in \Omega_k(p, s): x \in B) \geq \mathbb{P}(x \in B(p, s)) > 2^{-k-4}$$

a tedy i

$$\mathbb{P}(\exists B \in \Omega_k(p, s): x \notin B) < 1 - 2^{-k-4} \leq \exp(-2^{-k-4}).$$

□

Připomeňme, že konstruovaná množina X je rovna $X = \{x^1, x^2, \dots, x^n\} \subset M_k^d$. Pomocí jednoduché nerovnosti pro míru sjednocení množin (*union bound*) a Lemma 9.3 dostaneme

$$\begin{aligned} \mathbb{P}(\exists B \in \Omega_k: X \cap B = \emptyset) &\leq \sum_{p, s: \Omega_k(p, s) \neq \emptyset} \mathbb{P}(\exists B \in \Omega_k(p, s): X \cap B = \emptyset) \\ &= \sum_{p, s: \Omega_k(p, s) \neq \emptyset} \mathbb{P}(\exists B \in \Omega_k(p, s): x^1 \notin B)^n \\ &< \#\{p, s: \Omega_k(p, s) \neq \emptyset\} \exp(-n2^{-k-4}). \end{aligned}$$

Ještě potřebujeme odhadnout počet těch dvojic (p, s) , pro které $\Omega_k(p, s) \neq \emptyset$. Nejprve si všimněme, že $\Omega_k(p, s) = \emptyset$ pokud $p_\ell 2^k > 2^k - s_\ell$ pro nějaké $\ell = 1, \dots, d$. Pokud tedy s je takové,

že $\Omega_k(p, s) \neq \emptyset$ pro nějaké $p \in M_k^d$, pak existuje přesně $\prod_{\ell=1}^d (2^k - s_\ell)$ takových p , pro které $\Omega_k(p, s) \neq \emptyset$. Označíme-li $m_1(s) := \#\{\ell: s_\ell < 2^k - 1\}$, tak je tento počet omezen shora $2^{km_1(s)}$.
Je-li dále $B \in \Omega_k(p, s)$, pak

$$2^{-k} < |B| \leq \prod_{\ell=1}^d \left(\frac{s_\ell + 1}{2^k} \right) \leq \left(1 - \frac{1}{2^k} \right)^{m_1(s)}.$$

Pokud je tedy $\Omega_k(p, s) \neq \emptyset$, pak i

$$m_1(s) < A_k := \ln(2) k 2^k. \quad (9.3)$$

Skutečně,

$$2^{-k} < \left(1 - \frac{1}{2^k} \right)^{m_1(s)} \quad \text{and} \quad 2^{-k} > \left(1 - \frac{1}{2^k} \right)^{\ln(2)k2^k},$$

kde první z těchto nerovností plyne z monotónní konvergence $(1 - 1/2^k)^{2^k}$ k e^{-1} .

Počet těch $s \in \{0, \dots, 2^k - 1\}^d$, pro které $m_1(s) = \#\{l: s_l < 2^k - 1\} < A_k$ je dále omezen

$$\binom{d}{A_k} 2^{kA_k} < \left(\frac{4d}{k} \right)^{A_k},$$

kde jsme použili $\binom{d}{A_k} \leq (ed/A_k)^{A_k}$ a $e/\ln(2) < 4$. Celkem tedy dostaneme

$$\begin{aligned} \#\{p, s: \Omega_k(p, s) \neq \emptyset\} &< \left(\frac{4d}{k} \right)^{A_k} 2^{kA_k} \leq \exp\left(k 2^k \left(k + \log_2(4d/k)\right)\right) \\ &\leq \exp\left(k 2^k \log_2(2^{k+1}d)\right) \end{aligned}$$

a

$$\mathbb{P}(\exists B \in \Omega_k: X \cap B = \emptyset) < \exp\left(k 2^k \log_2(2^{k+1}d) - n 2^{-k-4}\right).$$

Tento výraz je ostře menší než jedna, pokud

$$n \geq 2^4 k 2^{2k} \log_2(2^{k+1}d).$$

V tom případě tedy existuje množina X s n body, pro kterou $X \cap B \neq \emptyset$ pro všechny kvádry B s $|B| > 2^{-k}$. Celkem tedy

$$N(2^{-k}, d) \leq 2^4 k 2^{2k} \log_2(2^{k+1}d).$$

Konečně, z $2^{-k} \leq \varepsilon < 2^{-k+1}$, $2^{k-1} < \varepsilon^{-1} \leq 2^k$ a $k \geq \log_2(1/\varepsilon) > k - 1$ dostaneme

$$N(\varepsilon, d) \leq 2^6 \frac{(1 + \log_2(\varepsilon^{-1})) \log_2(4d\varepsilon^{-1})}{\varepsilon^2} \leq 2^7 \log_2(d) \frac{(1 + \log_2(\varepsilon^{-1}))^2}{\varepsilon^2}.$$

10 Maticové normy: Spektrální, Frobeniova a nukleární

Příklady metrických a normovaných prostorů se často omezují na prostory posloupností. Díky aplikacím v numerice či zpracování signálů hrají ale čím dál důležitější roli prostory matic. Budeme se zabývat $m \times n$ reálnými maticemi, komplexní by bylo možné uvažovat podobně. Normy, které projdeme, jsou založené na spektrálních vlastnostech těchto matic. Připomeňme tedy *Singular value decomposition theorem*:

Věta 10.1. *Bud' $A \in \mathbb{R}^{m \times n}$ reálná $m \times n$ matice. Pak lze napsat A jako*

$$A = U\Sigma V^T,$$

kde U je $m \times m$ ortogonální matice, Σ je $m \times n$ diagonální matice s nezápornými reálnými koeficienty na diagonále a V je $n \times n$ ortogonální matice.

Diagonální koeficienty matice Σ označíme $\sigma_1(A) \geq \sigma_2(A) \geq \dots \geq 0$ a nazýváme je singulárními čísly matice A .

Spektrální norma matice A je $\|A\| := \sigma_1(A)$. Je-li $x \in \mathbb{R}^n$ s $\|x\|_2 \leq 1$, pak platí

$$\|Ax\|_2 = \|U\Sigma V^T x\|_2 = \|\Sigma V^T x\|_2 \leq \sigma_1(A) \|V^T x\|_2 \leq \sigma_1(A).$$

Pro $x = v_1$ první sloupec matice V ale dostaneme $V^T v_1 = e_1$ a $\|Ax\|_2 = \sigma_1(A)$. Celkem je tedy

$$\|A\| = \sup_{x \in \mathbb{R}^n, \|x\|_2 \leq 1} \|Ax\|_2 = \sup_{x \in \mathbb{R}^n, x \neq 0} \frac{\|Ax\|_2}{\|x\|_2}.$$

Odtud již ihned plyne, že $\|\cdot\|$ je skutečně norma, zejména trojúhelníkovou nerovnost dokážeme pomocí

$$\|A + B\| = \sup_{x \in \mathbb{R}^n, \|x\|_2 \leq 1} \|(A + B)x\|_2 \leq \sup_{x \in \mathbb{R}^n, \|x\|_2 \leq 1} \|Ax\|_2 + \sup_{x \in \mathbb{R}^n, \|x\|_2 \leq 1} \|Bx\|_2 = \|A\| + \|B\|.$$

Hilbert-Schmidtova norma nebo také **Frobeniova norma** je definována pomocí

$$\|A\|_F = \left(\sum_{j=1}^{\min(m,n)} \sigma_j(A)^2 \right)^{1/2}.$$

Nechť v_1, v_2, \dots, v_n jsou sloupce matice V v singulárním rozkladu matice A . Pak

$$\sum_{j=1}^n \|Av_j\|_2^2 = \sum_{j=1}^n \|U\Sigma V^T v_j\|_2^2 = \sum_{j=1}^n \|\Sigma V^T v_j\|_2^2 = \sum_{j=1}^{\min(m,n)} \|\sigma_j(A)v_j\|_2^2 = \sum_{j=1}^{\min(m,n)} \sigma_j(A)^2 = \|A\|_F^2.$$

Dokážeme, že stejná identita platí pro libovolnou ortonormální bázi $\varphi_1, \dots, \varphi_n$, tedy že

$$\|A\|_F^2 = \sum_{j=1}^n \|A\varphi_j\|_2^2. \quad (10.1)$$

Poté tento výsledek aplikujeme na ortonormální bázi e_1, \dots, e_n a obdržíme

$$\|A\|_F^2 = \sum_{j=1}^m \sum_{k=1}^n |a_{j,k}|^2.$$

Z toho pak již ihned plyne, že $\|\cdot\|_F$ je skutečně norma.

Zbývá tedy dokázat (10.1).

$$\begin{aligned} \sum_{j=1}^n \|A\varphi_j\|_2^2 &= \sum_{j=1}^n \|U\Sigma V^T \varphi_j\|_2^2 = \sum_{j=1}^n \|\Sigma V^T \varphi_j\|_2^2 = \sum_{j=1}^n \sum_{k=1}^{\min(m,n)} \sigma_k(A)^2 |\langle v_k, \varphi_j \rangle|^2 \\ &= \sum_{k=1}^{\min(m,n)} \sigma_k(A)^2 \sum_{j=1}^n |\langle v_k, \varphi_j \rangle|^2 = \sum_{k=1}^{\min(m,n)} \sigma_k(A)^2. \end{aligned}$$

Tato norma je samozřejmě generována skalárním součinem

$$\langle A, B \rangle_F = \sum_{j=1}^m \sum_{k=1}^n a_{j,k} b_{j,k} = \text{Tr}(A^T B).$$

Nukleární norma matice A je definována jako

$$\|A\|_* = \sum_{j=1}^{\min(m,n)} \sigma_j(A).$$

Tato norma se v minulých deseti letech stala středem zájmu pro svůj význam v oboru *low-rank matrix recovery*.¹⁸ My se zde omezíme na důkaz faktu, že nukleární norma je opravdu norma. Dokážeme, že je vlastně duální ke spektrální normě vzhledem k párování $\langle A, B \rangle_F$, tedy

$$\|A\|_* = \sup_{B \in \mathbb{R}^{m \times n}, \|B\| \leq 1} \langle A, B \rangle_F. \quad (10.2)$$

Trojúhelníková nerovnost pro $\|\cdot\|_*$ pak plyne lehce z

$$\|A + B\|_* = \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \langle A + B, C \rangle_F = \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} (\langle A, C \rangle_F + \langle B, C \rangle_F) \leq \|A\|_* + \|B\|_*.$$

Nechť $A = U\Sigma V^T$ je singulární rozklad matice A . Nechť $n \geq m$. Položme $C = UIV^T$, kde $I \in \mathbb{R}^{m \times n}$ je diagonální matice s jedničkami na diagonále. Pak samozřejmě $\|C\| = 1$, ale i

$$\begin{aligned} \langle A, C \rangle_F &= \langle U\Sigma V^T, UIV^T \rangle = \text{Tr}((U\Sigma V^T)^T (UIV^T)) = \text{Tr}((V\Sigma^T U^T)(UIV^T)) \\ &= \text{Tr}(V\Sigma^T IV^T) = \text{Tr}(V^T V \Sigma^T I) = \text{Tr}(\Sigma^T I) = \|A\|_*. \end{aligned}$$

Pro $m > n$ použijeme nejprve $\langle A, C \rangle_F = \langle C, A \rangle_F$. Tím je jedna nerovnost v (10.2) dokázána. Použili jsme identitu $\text{Tr}(XYZ) = \text{Tr}(ZXY)$, která platí kdykoliv jsou oba součiny definované.

¹⁸Literature...

Důkaz opačné nerovnosti plyne z

$$\begin{aligned}
\sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \langle A, C \rangle_F &= \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \text{Tr}(A^T C) = \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \text{Tr}((U \Sigma V^T)^T C) \\
&= \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \text{Tr}(V \Sigma^T U^T C) = \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \text{Tr}(\Sigma^T U^T C V) \\
&= \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \langle \Sigma, U^T C V \rangle = \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \sum_{j=1}^{\min(m,n)} \sigma_j(A) (U^T C V)_{j,j} \\
&= \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \sum_{j=1}^{\min(m,n)} \sigma_j(A) (u_j^T C v_j)_{j,j} \leq \sup_{C \in \mathbb{R}^{m \times n}, \|C\| \leq 1} \sum_{j=1}^{\min(m,n)} \sigma_j(A) \sigma_1(C) \\
&= \|A\|_*,
\end{aligned}$$

kde jsme opět použili identitu o stopě součinu třech matic.

Jiný způsob důkazu jde přes *Lidskii inequality*.¹⁹

Pro reálnou čtvercovou symetrickou matici $A = A^T$ označme $\lambda_j(A)$ její (reálná) vlastní čísla. Připomeňme, že jejich součet je roven stopě A - součtu prvků na diagonále. Následující lemma je obdobou trojúhelníkové nerovnosti ori vlastní čísla symetrické matice a singulární čísla obdélníkové matice.

Lemma 10.2. (i) *Nechť $A, B \in \mathbb{R}^{d \times d}$ jsou dvě reálné symetrické matice (i.e. $A = A^T, B = B^T$). Pak*

$$\sum_{j=1}^d |\lambda_j(A) - \lambda_j(B)| \leq \sum_{j=1}^d |\lambda_j(A - B)| = \|A - B\|_*.$$

(ii) *Nechť $A, B \in \mathbb{R}^{n \times N}$. Pak*

$$\sum_{j=1}^n |\sigma_j(A) - \sigma_j(B)| \leq \sum_{j=1}^n \sigma_j(A - B).$$

Důkaz. (i) Použijeme Jordanův rozklad $A - B$ na pozitivně a negativně definitní část

$$A - B = (A - B)^+ - (A - B)^-$$

a dostaneme

$$\|A - B\|_* = \text{tr}(A - B)^+ + \text{tr}(A - B)^-.$$

Položme

$$C := A + (A - B)^- = B + (A - B)^+.$$

Pak $C \succcurlyeq A$ a $C \succcurlyeq B$. Z Weylova principu monotonie²⁰

¹⁹<https://terrytao.wordpress.com/tag/lidskii-inequality/>

²⁰Toto lze dokázat i z minimax-charakterizace vlastních čísel

$$\lambda_k(A) = \max_{\substack{M \subset \mathbb{R}^d \\ \dim(M)=k}} \min_{\substack{x \in M \\ \|x\|_2=1}} \langle x, Ax \rangle \leq \max_{\substack{M \subset \mathbb{R}^d \\ \dim(M)=k}} \min_{\substack{x \in M \\ \|x\|_2=1}} \langle x, Cx \rangle = \lambda_k(C),$$

kde jsme použili, že

$$\langle x, Ax \rangle = \langle x, Cx \rangle + \langle x, (A - C)x \rangle \leq \langle x, Cx \rangle$$

pokud $C - A$ je pozitivně semi-definitní.

$\lambda_j(C) \geq \lambda_j(A)$ a $\lambda_j(C) \geq \lambda_j(B)$. Dostaneme tedy

$$\begin{aligned}\lambda_j(A) - \lambda_j(B) &\leq \lambda_j(2C) - \lambda_j(A) - \lambda_j(B) \quad \text{a} \\ \lambda_j(B) - \lambda_j(A) &\leq \lambda_j(2C) - \lambda_j(A) - \lambda_j(B), \quad \text{a tedy} \\ |\lambda_j(A) - \lambda_j(B)| &\leq \lambda_j(2C) - \lambda_j(A) - \lambda_j(B).\end{aligned}$$

Konečně sečtením obdržíme

$$\begin{aligned}\sum_{j=1}^d |\lambda_j(A) - \lambda_j(B)| &\leq \text{tr}(2C) - \text{tr}(A) - \text{tr}(B) \\ &= \text{tr}(A + (A - B)^-) + \text{tr}(B + (A - B)^+) - \text{tr}(A) - \text{tr}(B) \\ &= \|A - B\|_*.\end{aligned}$$

(ii) Položme

$$\tilde{A} = \begin{pmatrix} 0 & A \\ A^T & 0 \end{pmatrix} \quad \text{a} \quad \tilde{B} = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix}, \quad \text{a tedy} \quad \tilde{A} - \tilde{B} = \begin{pmatrix} 0 & A - B \\ (A - B)^T & 0 \end{pmatrix}.$$

Pak \tilde{A} a \tilde{B} jsou $d \times d$ symetrické matice s $d = n + N$. Navíc, vlastní čísla \tilde{A} jsou²¹ $(\pm\sigma_1(A), \dots, \pm\sigma_n(A))$ a podobně pro B a $A - B$. Použitím (i) dostaneme

$$\begin{aligned}\sum_{j=1}^{n+N} |\lambda_j(\tilde{A}) - \lambda_j(\tilde{B})| &= \sum_{j=1}^n |\sigma_j(A) - \sigma_j(B)| + \sum_{j=1}^n |-\sigma_j(A) + \sigma_j(B)| \\ &= 2 \sum_{j=1}^n |\sigma_j(A) - \sigma_j(B)| \leq \sum_{j=1}^{n+N} |\lambda_j(\tilde{A} - \tilde{B})| \\ &= \sum_{j=1}^n |\sigma_j(A - B)| + \sum_{j=1}^n |-\sigma_j(A - B)| = 2 \sum_{j=1}^n \sigma_j(A - B).\end{aligned}$$

□

²¹... vlastní vektory jsou $(u_j^T, v_j^T)^T$ a $(u_j^T, -v_j^T)^T$

11 Náhodná procházka v obecné dimenzi

Definice 11.1. Necht' $d \geq 1$ je přirozené číslo a necht' X_1, X_2, X_3, \dots je posloupnost \mathbb{R}^d -hodnotových nezávislých stejně rozdělených náhodných proměnných. Pak *náhodná procházka v dimenzi d* je posloupnost $(S_n)_{n \geq 0}$, kde $S_0 = 0$ a

$$S_n = S_{n-1} + X_n = X_1 + X_2 + \dots + X_n, \quad n \geq 1.$$

X_1, X_2, X_3, \dots se nazývají *kroky* náhodné procházky.

Další označení, které budeme používat je následující.

- *Jednoduchá náhodná procházka:* Pro $d = 1$ je $\mathbb{P}(X_j = 1) = \mathbb{P}(X_j = -1) = 1/2$, pro $d > 1$ je $\mathbb{P}(X_j = e_k) = \mathbb{P}(X_j = -e_k) = \frac{1}{2d}$ pro všechna $j \in \mathbb{N}$ a všechna $k = 1, \dots, d$. Vektory $(e_k)_{k=1}^d$ označují kanonickou bázi \mathbb{R}^d .
- *Počet výskytů v počátku:* Náhodná veličina N je definována

$$N = \#\{n \in \mathbb{N}_0 : S_n = 0\}.$$

- *čas prvního návratu do počátku:* Náhodná veličina τ

$$\tau = \inf\{n \geq 1 : S_n = 0\}.$$

Zde užíváme úmluvu $\inf \emptyset = +\infty$. Pokud se tedy náhodná procházka již nikdy do počátku nevrátí ($S_n \neq 0$ pro všechna $n \geq 1$), je $\tau = +\infty$.

- Náhodná procházka je *rekurentní*, pokud $\mathbb{P}(N = +\infty) = 1$, nebo ekvivalentně $\mathbb{P}(N < +\infty) = 0$. Náhodná procházka je *tranzitní*, pokud $\mathbb{P}(N < +\infty) = 1$, nebo ekvivalentně $\mathbb{P}(N = +\infty) = 0$.

Prvním krokem bude dokázat, že náhodná procházka je buď rekurentní, nebo tranzitní. Například $\mathbb{P}(N = +\infty) = 1/2$ (tedy jedna polovina procházek se nekonečněkrát vrací do počátku, druhá polovina nikoliv) tedy nemůže nastat.

Lemma 11.2. *Pro libovolnou náhodnou procházku v libovolné dimenzi a pro každé $n \geq 1$ platí*

$$\mathbb{P}(N = n) = \mathbb{P}(\tau = +\infty)\mathbb{P}(\tau < \infty)^{n-1}.$$

Důkaz. Nejprve dokážeme

$$\mathbb{P}(N = n + 1) = \mathbb{P}(N = n)\mathbb{P}(\tau < +\infty), \quad n \geq 1.$$

Skutečně - návratem do počátku v kroce k se náhodná procházka rozpadá na dvě nezávislé části, první (konečnou) s $S_0 = S_k = 0$, a druhou (nekonečnou) $(S_{k+j})_{j \geq 0}$, která má stejný tvar (a stejné rozdělení stavů) jako $(S_j)_{j \geq 0}$. Celkem tedy máme

$$\begin{aligned} \mathbb{P}(N = n + 1) &= \sum_{k \geq 1} \mathbb{P}(N = n + 1 \ \& \ \tau = k) = \sum_{k \geq 1} \mathbb{P}(N' = n \ \& \ \tau = k) \\ &= \sum_{k \geq 1} \mathbb{P}(N' = n)\mathbb{P}(\tau = k) = \mathbb{P}(N' = n) \sum_{k \geq 1} \mathbb{P}(\tau = k) = \mathbb{P}(N = n)\mathbb{P}(\tau < \infty), \end{aligned}$$

kde $N' = \#\{l \in \mathbb{N}_0 : S_{k+l} = 0\}$.

Tvrzení lemmatu pak snadno dokážeme indukcí. Pro $n = 1$ je $\mathbb{P}(N = 1) = \mathbb{P}(\tau = +\infty)$. Pro $n > 1$ je pak $\mathbb{P}(N = n + 1) = \mathbb{P}(N = n)\mathbb{P}(\tau < +\infty) = \mathbb{P}(\tau = +\infty)\mathbb{P}(\tau < +\infty)^n$. \square

Důsledek 11.3. Každá náhodná procházka je buď rekurentní nebo tranzitní.

Důkaz. Pokud $\mathbb{P}(\tau = +\infty) = 0$, pak z lemmatu plyne, že $\mathbb{P}(N = n) = 0$ pro každé $n \geq 1$ a tedy i $\mathbb{P}(N < +\infty) = 0$ a procházka je rekurentní.

Pokud ale $\mathbb{P}(\tau = +\infty) > 0$, pak je i $\mathbb{P}(\tau < +\infty) < 1$ a

$$\begin{aligned} \mathbb{P}(N < +\infty) &= \sum_{n \geq 1} \mathbb{P}(N = n) = \sum_{n \geq 1} \mathbb{P}(\tau = +\infty) \mathbb{P}(\tau < +\infty)^{n-1} \\ &= \mathbb{P}(\tau = +\infty) \frac{1}{1 - \mathbb{P}(\tau < +\infty)} = \frac{1 - \mathbb{P}(\tau < +\infty)}{1 - \mathbb{P}(\tau < +\infty)} = 1 \end{aligned}$$

a procházka je tranzitní. □

Charakterizovat, zda je náhodná procházka rekurentní nebo tranzitní, nám pomůže následující lemma.

Lemma 11.4. Náhodná procházka je tranzitní pokud $\mathbb{E}N < +\infty$, a rekurentní pokud $\mathbb{E}N = +\infty$.

Důkaz. Při použití konvence (obvyklé v teorii míry a pravděpodobnosti) " $0 \cdot (+\infty) = 0$ " dostaneme

$$\mathbb{E}N = \sum_{n \geq 1} n \mathbb{P}(N = n) + \infty \cdot \mathbb{P}(N = +\infty).$$

Pokud $\mathbb{E}N < +\infty$, je tedy $\mathbb{P}(N = +\infty) = 0$ a procházka je tranzitní.

Pokud naopak $\mathbb{P}(N = +\infty) = 0$, a tedy $\mathbb{P}(N < +\infty) = 1$, je podle předchozího lemmatu $\mathbb{P}(\tau = +\infty) > 0$ a tedy i $\mathbb{P}(\tau < +\infty) < 1$. Celkem je tedy

$$\begin{aligned} \mathbb{E}N &= \sum_{n \geq 1} n \mathbb{P}(N = n) = \sum_{n \geq 1} n \mathbb{P}(\tau = +\infty) \mathbb{P}(\tau < +\infty)^{n-1} \\ &= \mathbb{P}(\tau = +\infty) \sum_{n \geq 1} n \mathbb{P}(\tau < +\infty)^{n-1} = \frac{\mathbb{P}(\tau = +\infty)}{[1 - \mathbb{P}(\tau < +\infty)]^2} = \frac{1}{\mathbb{P}(\tau = +\infty)} < +\infty. \end{aligned}$$

□

Veličinu $\mathbb{E}N$ lze explicitně spočítat pomocí Fourierovy transformace, v teorii pravděpodobnosti známé spíše pod názvem *charakteristická funkce*.

Lemma 11.5. Nechť náhodná procházka v \mathbb{Z}^d (tedy $S_n \in \mathbb{Z}^d$ pro všechna $n \geq 1$) má kroky X_1, X_2, X_3, \dots a nechť $\varphi(\xi) = \mathbb{E}(e^{i\xi \cdot X_1}) = \mathbb{E} \cos(\xi \cdot X_1) + i \mathbb{E} \sin(\xi \cdot X_1)$ pro $\xi \in \mathbb{R}^d$. Pak

$$\mathbb{E}N = \lim_{t \rightarrow 1^-} \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \frac{1}{1 - t\varphi(\xi)} d\xi$$

Důkaz. Pro $d = 1$ je

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} e^{im\theta} d\theta = \frac{1}{2\pi} \int_{-\pi}^{\pi} (\cos(m\theta) + i \sin(m\theta)) d\theta = \begin{cases} 1 & \text{pro } m = 0, \\ 0 & \text{pro } m \in \mathbb{Z} \setminus \{0\}. \end{cases}$$

Pro $d \geq 1$ platí tedy

$$\frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} e^{im \cdot \xi} d\xi = \prod_{j=1}^d \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{im_j \xi_j} d\xi_j = \begin{cases} 1 & \text{pro } m = (0, \dots, 0), \\ 0 & \text{pro } m \in \mathbb{Z}^d \setminus \{(0, \dots, 0)\}. \end{cases}$$

Dosadíme-li za m polohu náhodné procházky po n krocích, tedy $m = S_n$ (zde poprvé využíváme, že $S_n \in \mathbb{Z}^d$), dostaneme

$$\frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} e^{iS_n \cdot \xi} d\xi = \chi_{\{S_n=0\}} = \begin{cases} 1 & \text{pro } S_n = (0, \dots, 0), \\ 0 & \text{pro } S_n \in \mathbb{Z}^d \setminus \{(0, \dots, 0)\}. \end{cases}$$

Integrací přes trajektorie náhodné procházky a s využitím nezávislosti jejich kroků obdržíme

$$\begin{aligned} \mathbb{P}(S_n = 0) &= \mathbb{E}\chi_{\{S_n=0\}} = \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \mathbb{E}(e^{iS_n \cdot \xi}) d\xi = \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \mathbb{E}(e^{iX_1 \cdot \xi} \cdot e^{iX_2 \cdot \xi} \dots e^{iX_n \cdot \xi}) d\xi \\ &= \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \mathbb{E}(e^{iX_1 \cdot \xi}) \cdot \mathbb{E}(e^{iX_2 \cdot \xi}) \dots \mathbb{E}(e^{iX_n \cdot \xi}) d\xi = \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \varphi(\xi)^n d\xi. \end{aligned}$$

Tuto identitu pronásobíme t^n pro $0 < t < 1$, sečteme a vyrobíme příslušnou mocninnou řadu (tento postup se v české literatuře označuje termínem *vytvorující funkce*)

$$\begin{aligned} \sum_{n \geq 0} t^n \mathbb{P}(S_n = 0) &= \sum_{n \geq 0} \frac{t^n}{(2\pi)^d} \int_{[-\pi, \pi]^d} \varphi(\xi)^n d\xi = \sum_{n \geq 0} \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} t^n \varphi(\xi)^n d\xi \\ &= \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \sum_{n \geq 0} [t\varphi(\xi)]^n d\xi \\ &= \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \frac{1}{1 - t\varphi(\xi)} d\xi. \end{aligned}$$

Při tomto výpočtu jsme užili

- $|\varphi(\xi)| = |\mathbb{E}(e^{i\xi \cdot X_1})| \leq \mathbb{E}(|e^{i\xi \cdot X_1}|) = \mathbb{E}1 = 1$,
- $|t\varphi(\xi)| \leq t < 1$,
- stejnoměrné konvergence řady $\sum_n [t\varphi(\xi)]^n$ na $[-\pi, \pi]^d$ pro záměnu integrálu a řady,
- a nakonec součtu geometrické řady.

Funkce

$$t \rightarrow \sum_{n \geq 0} t^n \mathbb{P}(S_n = 0)$$

je na intervalu $(0, 1)$ neklesající, má tedy (konečnou nebo nekonečnou) limitu pro $t \rightarrow 1^-$. Pokud je $\sum_n \mathbb{P}(S_n = 0)$ konečná, pak z Abelovy věty o mocninných řadách plyne, že

$$\lim_{t \rightarrow 1^-} \sum_{n \geq 0} t^n \mathbb{P}(S_n = 0) = \sum_{n \geq 0} \mathbb{P}(S_n = 0). \quad (11.1)$$

Jako (lehké) cvičení si rozmyslete, že pokud je pravá strana (11.1) nekonečná, tak ani levá strana nemůže být konečná. Rovnost (11.1) tedy platí vždy. Důkaz tedy už dokončíme pozorováním

$$\sum_{n \geq 0} \mathbb{P}(S_n = 0) = \sum_{n \geq 0} \mathbb{E}\chi_{\{S_n=0\}} = \mathbb{E}\left(\sum_{n \geq 0} \chi_{\{S_n=0\}}\right) = \mathbb{E}N.$$

□

Následující věta je v matematickém folklóru označována: “A drunken man will always find his way home but a drunken bird may get lost forever”.

Věta 11.6. *Jednoduchá náhodná procházka na \mathbb{Z}^d je rekurentní pro $d = 1, 2$ a tranzitní pro $d \geq 3$.*

Důkaz. Pro jednoduchou procházku je $X_j \in \{\pm e_1, \dots, \pm e_d\}$ a tedy

$$\varphi(\xi) = \mathbb{E}(e^{iX \cdot \xi}) = \frac{1}{2d} \left(e^{i\xi_1} + e^{-i\xi_1} + \dots + e^{i\xi_d} + e^{-i\xi_d} \right) = \frac{\cos(\xi_1) + \dots + \cos(\xi_d)}{d}$$

a $\varphi(\xi) \leq 1$ je tedy reálná funkce. Navíc platí

$$\begin{aligned} & \lim_{t \rightarrow 1^-} \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \frac{1}{1 - t\varphi(\xi)} d\xi \\ &= \lim_{t \rightarrow 1^-} \left[\frac{1}{(2\pi)^d} \int_{\xi \in [-\pi, \pi]^d, \varphi(\xi) \leq 0} \frac{1}{1 - t\varphi(\xi)} d\xi + \frac{1}{(2\pi)^d} \int_{\xi \in [-\pi, \pi]^d, \varphi(\xi) > 0} \frac{1}{1 - t\varphi(\xi)} d\xi \right] \\ &= \frac{1}{(2\pi)^d} \int_{\xi \in [-\pi, \pi]^d, \varphi(\xi) \leq 0} \frac{1}{1 - \varphi(\xi)} d\xi + \frac{1}{(2\pi)^d} \int_{\xi \in [-\pi, \pi]^d, \varphi(\xi) > 0} \frac{1}{1 - \varphi(\xi)} d\xi \\ &= \frac{1}{(2\pi)^d} \int_{[-\pi, \pi]^d} \frac{1}{1 - \varphi(\xi)} d\xi. \end{aligned}$$

První záměna limity a integrálu plyne ze stejnoměrné omezenosti $0 \leq (1 - t\varphi(\xi))^{-1} \leq 1$ pro všechna $0 < t < 1$ a $\xi \in [-\pi, \pi]^d$ s $\varphi(\xi) \leq 0$, druhá pak z monotónní konvergence $(1 - t\varphi(\xi))^{-1} \nearrow (1 - \varphi(\xi))^{-1}$.

Na $[-\pi, \pi]^d$ je tedy $\varphi(\xi) = 1$ jen pro $\xi = (0, \dots, 0)$ a toto je tedy jediný kritický bod $\int_{[-\pi, \pi]^d} \frac{d\xi}{1 - \varphi(\xi)}$. Pro zjištění konvergence či divergence tohoto integrálu je tedy důležité chování $1 - \varphi(\xi)$ pro $\xi \rightarrow 0$. Pomocí následující posloupnosti jinak triviálních faktů obdržíme

- $1 - \cos x = 2 \sin^2(x/2), \quad x \in \mathbb{R},$
- $\frac{2x}{\pi} \leq \sin x \leq x, \quad x \in [0, \pi/2],$
- $\frac{2\xi_i^2}{\pi^2} \leq 1 - \cos(\xi_i) \leq \frac{\xi_i^2}{2}, \quad \xi_i \in [-\pi, \pi],$
-

$$1 - \varphi(\xi) = \frac{(1 - \cos(\xi_1)) + \dots + (1 - \cos(\xi_d))}{d} = \begin{cases} \geq \frac{1}{d} \cdot \frac{2|\xi|^2}{\pi^2}, \\ \leq \frac{1}{2d} |\xi|^2. \end{cases}$$

Pro $d = 1, 2$ máme tedy

$$\frac{1}{1 - \varphi(\xi)} \geq \frac{1}{|\xi|^2/(2d)}$$

a integrál z této funkce přes $[-\pi, \pi]^d$ diverguje. Celkem tedy $\mathbb{E}N = +\infty$ a procházka je rekurentní.

Pro $d \geq 3$ je

$$\frac{1}{1 - \varphi(\xi)} \leq \frac{1}{\frac{2}{\pi^2 d} |\xi|^2}$$

a integrál přes $[-\pi, \pi]^d$ konverguje. Celkem je tedy $\mathbb{E}N < +\infty$ a procházka je tranzitní. \square

12 Support Vector Machines

Support Vector Machines jsou jedny z nejpobulárnějších metod strojového učení pro klasifikační problémy. Předpokládejme, že vektory $x_1, \dots, x_n \in \mathbb{R}^d$ jsou rozděleny do dvou (předem známých) skupin, tedy

$$\{x_1, \dots, x_n\} = A_{-1} \cup A_1,$$

kde A_{-1} a A_1 jsou disjunktní. Přírozeně definujeme

$$y_i = \begin{cases} +1, & \text{pokud } x_i \in A_1, \\ -1, & \text{pokud } x_i \in A_{-1}. \end{cases}$$

Celkem tedy máme na vstupu páry

$$(x_1, y_1), \dots, (x_n, y_n) \in \mathbb{R}^d \times \{-1, 1\}.$$

Hlavní myšlenka support vector machines je oddělit body z množin A_{-1} a A_1 od sebe nadrovinou (=afinní funkcí), tedy najít vektor $\omega \in \mathbb{R}^d$ a $b \in \mathbb{R}$ tak, aby množiny $\{x_i : y_i = 1\}$ a $\{x_i : y_i = -1\}$ ležely v opačných poloprostorech určených nadrovinou

$$E_\omega = \{z \in \mathbb{R}^d : \langle z, \omega \rangle = b\}. \quad (12.1)$$

Celkem tedy chceme, aby

$$\langle x_i, \omega \rangle - b \begin{cases} \geq 0 & \text{pro } y_i = +1, \\ \leq 0 & \text{pro } y_i = -1. \end{cases}$$

Toto lze shrnout jako $y_i(\langle x_i, \omega \rangle - b) \geq 0$ pro všechna $i = 1, \dots, n$.

Než se s z tohoto prostého konceptu stanou support vector machines, je třeba si rozmyslet několik maličností.

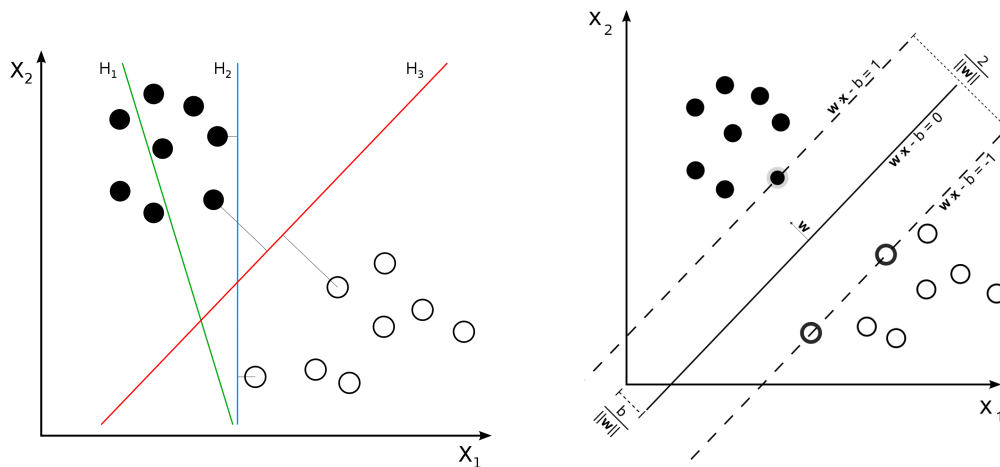
- V principu není jasné, jestli lze body na vstupu opravdu oddělit nějakou nadrovinou - tedy jestli se podaří najít alespoň jednu dvojici $\omega \in \mathbb{R}^d$ a $b \in \mathbb{R}$, které by splňovaly předchozí nerovnosti.
- Pokud body separovatelné jsou (tedy nějaké takové $\omega \in \mathbb{R}^d$ existuje), tak jich typicky bude existovat i více. Pro stabilitu klasifikace nových dat je pak přirozené vzít takovou nadrovinu (12.1), která bude mít největší vzdálenost (v nějakém smyslu) od A_{-1} i A_1 . Tím (alespoň intuitivně) zvýšíme pravděpodobnost, že nová data padnou na správnou stranu (12.1), viz obr.
- Spojením $(\omega, -b) \in \mathbb{R}^d \times \mathbb{R}$ do $\omega' \in \mathbb{R}^{d+1}$ a rozšířením vstupních dat o jedničku, tedy $x'_j = (x_j, 1)$ můžeme trochu zjednodušit notaci. Opravdu, poté $\langle \omega', x'_j \rangle = \langle \omega, x_j \rangle - b$. Můžeme tedy (bez větší újmy na obecnosti) předpokládat, že $b = 0$.

Jak tedy poznáme, která z nadrovin splňujících $y_i \langle \omega_i, x_i \rangle \geq 0$ pro všechna $i = 1, \dots, n$ má největší vzdálenost od vstupních dat?

Nechť $\|\cdot\|$ je norma na \mathbb{R}^d . Pak definujeme duální normu pomocí

$$\|\cdot\|' : \mathbb{R}^d \rightarrow [0, \infty), \quad \|w\|' = \sup_{v \in \mathbb{R}^d: \|v\|=1} \langle v, w \rangle = \sup_{v \in \mathbb{R}^d: \|v\|=1} |\langle v, w \rangle|.$$

Jako lehké cvičení (na Hahn-Banachovu větu?) si rozmyslete, že



Obrázek 2: Support vector machines; vlevo: nadrovina H_1 body dvou různých skupin neodděluje vůbec. H_2 je odděluje, ale nestabilně - je zde velká pravděpodobnost, že nové body (které očekáváme sice blízko už známých vzorků, ale přece jen mírně odlišné) padnou na “špatnou stranu” H_2 . H_3 odděluje body co nejstabilněji.

- $\|\cdot\|'$ je norma na \mathbb{R}^d ,
- $|\langle v, w \rangle| \leq \|v\| \cdot \|w\|'$,
- $(\|\cdot\|)' = \|\cdot\|$.

Následující lemma charakterizuje vzdálenost $a \in \mathbb{R}^d$ od E_ω v normě $\|\cdot\|$, tedy

$$d_{\|\cdot\|}(a, E_\omega) = \inf_{v \in E_\omega} \|a - v\|.$$

Lemma 12.1. *Nechť $\omega \in \mathbb{R}^d \setminus \{0\}$ a $a \in \mathbb{R}^d$. Pak*

$$d_{\|\cdot\|}(a, E_\omega) = \frac{|\langle a, \omega \rangle|}{\|\omega\|'}. \quad (12.2)$$

Důkaz. Pro $a \in E_\omega$ je tvrzení zřejmé. Nechť tedy $a \notin E_\omega$. Nechť $z = a + \lambda_z e_z \in E_\omega$ je libovolný bod z E_ω s $\lambda_z \in \mathbb{R}$ a $\|e_z\| = 1$. Protože $z \in E_\omega$, tak

$$0 = \langle z, \omega \rangle = \langle a, \omega \rangle + \lambda_z \langle e_z, \omega \rangle, \quad \text{i.e.} \quad \lambda_z = -\frac{\langle a, \omega \rangle}{\langle e_z, \omega \rangle}.$$

Dále

$$\|a - z\| = |\lambda_z| = \frac{|\langle a, \omega \rangle|}{|\langle e_z, \omega \rangle|}.$$

Pokud vezmeme infimum přes všechna $z \in E_\omega$, dostaneme

$$d_{\|\cdot\|}(a, E_\omega) = \inf_{z \in E_\omega} \|a - z\| = \inf_{z \in E_\omega} |\lambda_z| = \frac{|\langle a, \omega \rangle|}{\sup_{z \in E_\omega} |\langle e_z, \omega \rangle|} = \frac{|\langle a, \omega \rangle|}{\|\omega\|'}.$$

V poslední identitě využíváme toho, že

$$\sup_{z \in E_\omega} |\langle e_z, \omega \rangle| = \sup_{\|e\|=1, \langle e, \omega \rangle \neq 0} |\langle e, \omega \rangle| = \sup_{\|e\|=1} |\langle e, \omega \rangle| = \|\omega\|'.$$

□

Identita (12.2) už umožňuje zdefinovat support vector machines pro případ, kdy data jsou opravdu separovatelná, tzv. *hard-margin support vector machines*. Hledáme tedy

$$(*) = \max_{\omega: y_i \langle x_i, \omega \rangle \geq 0} \min_{i=1, \dots, n} \frac{|\langle x_i, \omega \rangle|}{\|\omega\|'} = \max_{\omega: y_i \langle x_i, \omega \rangle \geq 0} \frac{1}{\|\omega\|'} \min_{i=1, \dots, n} |\langle x_i, \omega \rangle|.$$

Poslední výraz je homogenní v ω - nahradíme-li tedy ω výrazem $\lambda\omega$ pro $\lambda \neq 0$, hodnota výrazu se nezmění. Můžeme tedy (bez újmy na obecnosti) zafixovat velikost ω . Nabízí se několik možností, např. vyžadovat $\|\omega\| = 1$ nebo $\|\omega\|' = 1$. My použijeme $\min_{i=1, \dots, n} |\langle x_i, \omega \rangle| = 1$. Vektory s $\min_{i=1, \dots, n} |\langle x_i, \omega \rangle| = 0$ nejsou zjevně optimální a můžeme je tedy vynechat. Celkem tak dostaneme

$$\begin{aligned} (*) &= \max \left\{ \frac{1}{\|\omega\|'} : y_i \langle x_i, \omega \rangle \geq 0 \quad \& \quad \min_{i=1, \dots, n} |\langle x_i, \omega \rangle| = 1 \right\} \\ &= \min \left\{ \|\omega\|' : y_i \langle x_i, \omega \rangle \geq 0 \quad \& \quad \min_{i=1, \dots, n} |\langle x_i, \omega \rangle| = 1 \right\} \\ &= \min \left\{ \|\omega\|' : \min_{i=1, \dots, n} y_i \langle x_i, \omega \rangle = 1 \right\}. \end{aligned}$$

Poslední výraz bývá obvyklé psát ve tvaru

$$(*) = \min \|\omega\|' \quad \text{such that} \quad \min_{i=1, \dots, n} y_i \langle x_i, \omega \rangle = 1,$$

nebo - a to ještě častěji -

$$(*) = \min \|\omega\|' \quad \text{such that} \quad \min_{i=1, \dots, n} y_i \langle x_i, \omega \rangle \geq 1. \quad (12.3)$$

Definice 12.2. Pro $(x_1, y_1), \dots, (x_n, y_n) \in \mathbb{R}^d \times \mathbb{R}$, které jsou separovatelné nějakou nadrovinou, se optimalizační problém

$$\min \|\omega\|' \quad \text{such that} \quad \min_{i=1, \dots, n} y_i \langle x_i, \omega \rangle \geq 1$$

nazývá *hard-margin support vector machine*. Označíme-li $\tilde{\omega}$ jeho řešení (tedy takový bod \mathbb{R}^d , ve kterém se nabývá minimum), pak $x \rightarrow \text{sgn}(\langle x, \tilde{\omega} \rangle)$ je hledaný *klasifikátor* nových dat. Konečně, vektory x_i , pro které $y_i \langle \tilde{\omega}, x_i \rangle = 1$ se nazývají *support vectors*.

V případě, že data nejsou bezchybně separovatelná lineární nadrovinou, tak penalizujeme ty vektory ω , které klasifikují špatně (a výrazně) mnoho vektorů x_i , ale nezakážeme tento jev kompletně. Zavádím tedy tzv. *hinge loss function*

$$L(\omega, x_i, y_i) = \max(0, 1 - y_i \langle x_i, \omega \rangle) = [1 - y_i \langle x_i, \omega \rangle]_+.$$

Definice 12.3. Pro $(x_1, y_1), \dots, (x_n, y_n) \in \mathbb{R}^d \times \mathbb{R}$, nikoliv nezbytně separovatelné nějakou nadrovinou, a $\lambda > 0$ se optimalizační problém

$$\min_{\omega \in \mathbb{R}^d} \left[\lambda \|\omega\|' + \frac{1}{n} \sum_{i=1}^n L(\omega, x_i, y_i) \right] = \min_{\omega \in \mathbb{R}^d} \left[\lambda \|\omega\|' + \frac{1}{n} \sum_{i=1}^n [1 - y_i \langle x_i, \omega \rangle]_+ \right]$$

nazývá *soft-margin support vector machine*. Označíme-li $\tilde{\omega}$ jeho řešení, pak $x \rightarrow \text{sgn}(\langle x, \tilde{\omega} \rangle)$ je opět hledaný *klasifikátor* nových dat.

Úloha parametru $\lambda > 0$ je vcelku zřejmá: je to váha mezi šířkou separačního pruhu okolo nadroviny E_ω a chybou klasifikace. Soft-margin support vector machine má řadu variant a modifikací. Pro $\|\cdot\|$ Eukleidovskou normu je možné brát $\lambda \|\omega\|^2$ místo $\lambda \|\omega\|'$. Stejně tak je možné uvažovat $[1 - y_i \langle x_i, \omega \rangle]_+^2$. Další varianta užívá tzv. *slack variables* $\xi_i = [1 - y_i \langle x_i, \omega \rangle]_+ \geq 0$ a

$$\min_{\omega \in \mathbb{R}^d, \xi \in \mathbb{R}_+^n} \left[\lambda \|\omega\|' + \|\xi\|_1 \right] \quad \text{such that} \quad y_i \langle x_i, \omega \rangle \geq 1 - \xi_i.$$

Různé aspekty (např. implementaci) by bylo možné jistě rozebrat do detailu, my se zaměříme jen na jeden z nich. Obě varianty SVM představené výše jsou *lineární*. Rozšíření na nelineární klasifikátory je možné provést pomocí tzv. *kernel trick*. Tento trik spočívá v tom, že data nejprve zobrazíme nelineárním zobrazením $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^N$, kde $N \gg d$ (nebo dokonce $N = +\infty$). Pokud je zvolená norma Eukleidovská, je pro celý předchozí postup dostačující, když spočteme skalární součiny $\langle u, v \rangle$ pro $u, v \in \mathbb{R}^d$. Aplikujeme-li tedy SVM na $(\Phi(x_1), y_1), \dots, (\Phi(x_n), y_n)$, je nutné umět (rychle) spočítat $\langle \Phi(u), \Phi(v) \rangle$. To je bohužel tím obtížnější, čím vyšší je N , a tedy i čím více nelineárních operací Φ zahrnuje. Někdy je ale možné najít relativně jednoduchou funkci $k : \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}$, pro kterou $\langle \Phi(u), \Phi(v) \rangle = k(u, v)$.

Například volba (keyword: *quadratic kernel*)

$$\Phi(u) = \Phi(u_1, \dots, u_d) = (u_1^2, \dots, u_d^2, \sqrt{2}u_1u_2, \dots, \sqrt{2}u_{d-1}u_d)$$

dává

$$\langle \Phi(u), \Phi(v) \rangle = \sum_{j=1}^d u_j^2 v_j^2 + 2 \sum_{1 \leq i < j \leq d} u_i u_j v_i v_j = \sum_{i,j=1}^d u_i u_j v_i v_j = \left(\sum_{i=1}^d u_i v_i \right)^2 = \langle u, v \rangle^2,$$

a tedy $k(u, v) = \langle u, v \rangle^2$.

Samozřejmě, ne pro každou funkci k existuje příslušné Φ (a ne pro každou Φ lze k spočítat jednoduše). Definujeme-li k danému Φ jádro k pomocí $k(u, v) := \langle \Phi(u), \Phi(v) \rangle$, pak k splňuje

- symetrie: $k(u, v) = k(v, u)$,
- pozitivně semidefinitní: pro každé $c_1, \dots, c_n \in \mathbb{R}$ a $u_1, \dots, u_n \in \mathbb{R}^d$ platí

$$\sum_{i,j=1}^n c_i c_j k(u_i, u_j) = \sum_{i,j=1}^n c_i c_j \langle \Phi(u_i), \Phi(u_j) \rangle = \left\langle \sum_{i=1}^n c_i \Phi(u_i), \sum_{j=1}^n c_j \Phi(u_j) \right\rangle \geq 0.$$

Naopak, je-li $k : X \times X \rightarrow \mathbb{R}$ symetrická a pozitivně semidefinitní (X je libovolná množina), pak definujeme

$$\Phi(x) = k(\cdot, x) \in \mathbb{R}^X, \quad x \in X.$$

Na vektorovém prostoru

$$\text{span}\{\Phi(x) : x \in X\} = \left\{ f = \sum_{i=1}^n \alpha_i k(\cdot, x_i) : n \in \mathbb{N}, x_i \in X, \alpha_i \in \mathbb{R} \right\}$$

definujeme skalární součin

$$\langle f, g \rangle = \left\langle \sum_i \alpha_i k(\cdot, u_i), \sum_j \beta_j k(\cdot, v_j) \right\rangle := \sum_{i,j} \alpha_i \beta_j k(u_i, v_j).$$

Všimněme si, že

$$\langle f, k(\cdot, x) \rangle = \sum_i \alpha_i \langle k(\cdot, u_i), k(\cdot, x) \rangle = \sum_i \alpha_i k(x, u_i) = f(x),$$

jde tedy o tzv. *Reproducing Kernel Hilbert-Space* (RKHS). Zbývá ověřit, že $\langle f, g \rangle$ je dobře definován (různé reprezentace f a g dávají stejný výsledek) a že jde opravdu o skalární součin. Aby platilo, že $\langle f, f \rangle = 0$ jen pro $f = 0$, je navíc třeba, aby k bylo pozitivně definitní, tedy aby pro různá x_1, \dots, x_n a nenulové $(c_1, \dots, c_n) \neq 0$ bylo $\sum_{i,j} c_i c_j k(x_i, x_j) > 0$.

Oblíbené volby k zahrnují

- Gaussian radial basis function: $k(x, y) = \exp(-\|x - y\|_2^2/c)$,
- Polynomial: $k(x, y) = (\langle x, y \rangle + \theta)^d$,
- Sigmoidal: $\tanh(\varkappa(\langle x, y \rangle) + \theta)$,
- Inverse multiquadratic: $(\|x - y\|_2^2 + c^2)^{-1/2}$.

13 Principal Component Analysis

Připomeňme opět *Singular value decomposition theorem*:

Věta 13.1. *Bud' $A \in \mathbb{R}^{n \times d}$ reálná $n \times d$ matice. Pak lze napsat A jako*

$$A = U\Sigma V^T,$$

kde U je $n \times n$ ortogonální matice, Σ je $n \times d$ diagonální matice s nezápornými reálnými koeficienty na diagonále a V je $d \times d$ ortogonální matice.

Diagonální koeficienty matice Σ označíme $\sigma_1(A) \geq \sigma_2(A) \geq \dots \geq 0$ a nazýváme je singulárními čísly matice A . Sloupce matice U označíme $u_1, \dots, u_n \in \mathbb{R}^n$, sloupce matice V pak $v_1, \dots, v_d \in \mathbb{R}^d$.

Alternativní forma singulárního rozkladu je dána

$$A = \sum_{j=1}^{\min(n,d)} \sigma_j(A) u_j v_j^T. \quad (13.1)$$

Věta 13.2. *Nechť $A \in \mathbb{R}^{n \times d}$ a $1 \leq k \leq \min(n, d)$. Pak*

$$\min_{\text{rank}(B) \leq k} \|A - B\|_F^2 = \sum_{j=k+1}^{\min(n,d)} \sigma_j(A)^2 = \|A - A_k\|_F^2,$$

kde

$$A_k = \sum_{j=1}^k \sigma_j(A) u_j v_j^T$$

je částečný součet (13.1)

Důkaz. Z Weylova principu²² plyne

$$\sigma_{i+j-1}(X + Y) \leq \sigma_i(X) + \sigma_j(Y)$$

pro všechna $X, Y \in \mathbb{R}^{n \times d}$, $1 \leq i, j \leq \min(n, d)$ a $i + j - 1 \leq \min(n, d)$. Pro $Y := B$, $j := k + 1$ a $X := A - B$ dostaneme

$$\sigma_{i+k}(A) \leq \sigma_i(A - B) + \sigma_{k+1}(B) = \sigma_i(A - B),$$

protože B má hodnost k . Celkem je tedy

$$\|A - B\|_F^2 \geq \sum_{i=1}^{\min(n,d)-k} \sigma_i(A - B)^2 \geq \sum_{i=1}^{\min(n,d)-k} \sigma_{i+k}(A)^2 = \sum_{i=k+1}^{\min(n,d)} \sigma_i(A)^2 = \|A_k\|_F^2.$$

Opačná nerovnost je zřejmá. □

²²3.3.16 in Topics in Matrix Analysis....

Optimální redukce dimenze

Nechť nyní $x_1, \dots, x_n \in \mathbb{R}^d$ jsou body v \mathbb{R}^d a necht' $k \leq d$. Hledáme k -dimenzionální podprostor $L \subset \mathbb{R}^d$, který nejlépe aproximuje tyto body. Vzdálenost $x \in \mathbb{R}^d$ od L je dána jako $\|x - P_L x\|_2$, kde $P_L : \mathbb{R}^d \rightarrow \mathbb{R}^d$ je ortogonální projekce na L . Pokud $n \leq k \leq d$, tak můžeme vzít za L lineární obal bodů x_1, \dots, x_n . Budeme tedy předpokládat, že $1 \leq k \leq \min(n, d)$.

Hledáme tedy

$$\min_{\dim(L)=k} \sum_{j=1}^n \|x_j - P_L x_j\|_2^2. \quad (13.2)$$

Nechť $X \in \mathbb{R}^{d \times n}$ je matice se sloupci x_1, \dots, x_n . Pak lze (13.2) zapsat jako

$$\min_{\dim(L)=k} \|X - P_L X\|_F^2.$$

Nechť z_1, \dots, z_k je ortonormální báze L . Pak

$$P_L x = \sum_{j=1}^k \langle x, z_j \rangle z_j = \sum_{j=1}^k z_j z_j^T x$$

a tedy

$$P_L = \sum_{j=1}^k z_j z_j^T$$

má hodnotu k - a tedy i $P_L X$ má hodnotu nejvýše k . Celkem je tedy

$$\min_{\dim(L)=k} \sum_{j=1}^n \|x_j - P_L x_j\|_2^2 = \min_{\dim(L)=k} \|X - P_L X\|_F^2 \geq \min_{\text{rank}(Y) \leq k} \|X - Y\|_F^2 = \min_{\text{rank}(Y)=k} \|X - Y\|_F^2. \quad (13.3)$$

Podle předchozí věty uvažujeme tedy singulární rozklad $X = U \Sigma V^T$ a optimální $Y = X_k$ je dáno ořezaným rozkladem $Y = U_k \Sigma_k V_k^T$, kde $U_k \in \mathbb{R}^{d \times k}$ má sloupce $u_1, \dots, u_k \in \mathbb{R}^d$, $\Sigma_k \in \mathbb{R}^{k \times k}$ je diagonální matice s $\sigma_1(X) \geq \dots \geq \sigma_k(X) \geq 0$ na diagonále a $V_k \in \mathbb{R}^{n \times k}$ se sloupci $v_1, \dots, v_k \in \mathbb{R}^n$.

Naopak volbou $L = \text{span}\{u_1, \dots, u_k\}$ a $P_L = U_k U_k^T = \sum_{j=1}^k u_j u_j^T$ dostaneme

$$\begin{aligned} P_L X &= \sum_{j=1}^k u_j u_j^T \left(\sum_{l=1}^{\min(n,d)} \sigma_l(X) u_l v_l^T \right) = \sum_{l=1}^{\min(n,d)} \sigma_l(X) \sum_{j=1}^k u_j u_j^T u_l v_l^T \\ &= \sum_{l=1}^{\min(n,d)} \sigma_l(X) \sum_{j=1}^k u_j \delta_{j,l} v_l^T = \sum_{l=1}^k \sigma_l(X) u_l v_l^T = X_k. \end{aligned}$$

Lineární obal prvních k sloupců matice U tedy dává k -dimenzionální podprostor \mathbb{R}^d , který nejlépe aproximuje počáteční data, resp. projekci do nějž dojde k nejmenší chybě. Chceme-li tedy zredukovat dimenzi počátečních dat z \mathbb{R}^d na \mathbb{R}^k , tak podprostor, který toto umožňuje s co nejmenší chybou, získáme ze singulárního rozkladu maticové reprezentace těchto dat.

Maximalizace rozptylu dat

Mějme opět dány body $x_1, \dots, x_n \in \mathbb{R}^d$ a necht' nejprve $k = 1$. Chceme snížit dimenzionalitu dat při co největším zachování informační hodnoty. Ta je (zcela intuitivně a heuristicky) nejnížší, pokud se všechny body zprojekují do jednoho bodu. Cílem je tedy najít přímku takovou, aby data po projekci na ni byla co nejrozptýlenější, neboli měla co největší rozptyl. Pokud definujeme

$$\bar{x} = \frac{x_1 + \dots + x_n}{n},$$

pak hledáme v s $\|v\|_2 = 1$ tak, aby

$$\begin{aligned} \frac{1}{n} \sum_{j=1}^n \|\langle v, x_j \rangle v - \langle v, \bar{x} \rangle v\|_2^2 &= \frac{1}{n} \sum_{j=1}^n (\langle v, x_j \rangle - \langle v, \bar{x} \rangle)^2 = \frac{1}{n} \sum_{j=1}^n \langle v, x_j - \bar{x} \rangle^2 \\ &= \frac{1}{n} \sum_{j=1}^n v^T (x_j - \bar{x})(x_j - \bar{x})^T v = v^T S v \end{aligned}$$

bylo co největší, kde

$$S = \frac{1}{n} \sum_{j=1}^n (x_j - \bar{x})(x_j - \bar{x})^T$$

je "kovarianční matice dat".

Zkusme danou úlohu řešit pomocí Lagrangeových multiplikátorů. Položme tedy $J(v) = v^T S v$ a (vazba je $\|v\|_2^2 = v^T v = 1$)

$$L(v, \lambda) = J(v) + \lambda(1 - v^T v) = v^T S v + \lambda(1 - v^T v).$$

Pak je

$$\nabla_v L(v, \lambda) = 2(Sv - \lambda v) = 0,$$

a tedy $Sv = \lambda v$. Kritické body podezřelé z extrému jsou tedy vlastní vektory matice S .

Výsledný rozptyl v každém takovém bodě je pak $J(v) = v^T S v = v^T \lambda v = \lambda$. Maximum tedy získáme pro největší vlastní číslo matice S . Vztah k předchozí kapitole pak dostaneme, pokud si uvědomíme, že pokud matice $X \in \mathbb{R}^{d \times n}$ je opět tvořena sloupcovými vektory x_1, \dots, x_n , pak je

$$(XX^T)_{u,v} = \sum_{z=1}^n X_{u,z}(X^T)_{z,v} = \sum_{z=1}^n X_{u,z}X_{v,z} = \sum_{z=1}^n (x_z)_u(x_z)_v = \left(\sum_{z=1}^n x_z x_z^T \right)_{u,v},$$

tedy $XX^T = \sum_{z=1}^n x_z x_z^T$. Tedy (pokud pro jednoduchost $\bar{x} = 0$) $XX^T = nS$ a největší vlastní číslo S tak odpovídá největšímu singulárnímu číslu X .

Pro obecné k by bylo možno postupovat indukcí (a de fakto takto dokázat větu o singulárním rozkladu matice), nebo stačí použít předchozí kapitolku. Pro podprostor $L \subset \mathbb{R}^d$ je totiž $x = (x - P_L x) + P_L x$ rozklad x na dvě na sebe kolmé komponenty. Je tedy $\|x\|_2^2 = \|x - P_L x\|_2^2 + \|P_L x\|_2^2$ a chceme-li maximalizovat (předpokládejme opět pro jednoduchost, že $\bar{x} = 0$)

$$\frac{1}{n} \sum_{j=1}^n \|P_L x_j\|_2^2 = \frac{1}{n} \sum_{j=1}^n (\|x_j\|_2^2 - \|x_j - P_L x_j\|_2^2) = \frac{1}{n} \sum_{j=1}^n \|x_j\|_2^2 - \frac{1}{n} \sum_{j=1}^n \|x_j - P_L x_j\|_2^2,$$

tak stačí minimalizovat druhý sčítanec, protože první je nezávislý na L .

Ve strojovém učení se často na data nahlíží jako na náhodné nezávislé vektory vygenerované z nějaké neznámé distribuce \mathcal{D} . Terminologie střední hodnoty a rozptylu je pak naprosto přirozená.

Poslední poznámka k terminologii. Volba báze $u_1, \dots, u_d \in \mathbb{R}^d$ umožňuje vyjádřit každé $x_j \in \mathbb{R}^d$ jako

$$x_j = \sum_{l=1}^d \langle x_j, u_l \rangle u_l,$$

tedy vyjádřit počáteční data jako lineární kombinaci u_l . Přičemž ořezání tohoto rozvoje (tedy sčítání přes $l = 1, \dots, k$) zachová maximum možné informace pro dané k . Je to tedy rozvoj x_j do komponent u_1, \dots, u_d , z nichž u_1 je nejdůležitější, pak následuje u_2 , atd. Odtud tedy název “Principal Component Analysis” (nebo-li analýza hlavních komponent). Nalezené komponenty jsou navíc “nezávislé” (nebo-li na sebe kolmé).

14 Princip neurčitosti

Princip neurčitosti z matematického pohledu říká, že funkce a její Fourierova transformace nemohou být obě zároveň silně koncentrované. Ve své nejjednodušší formě (občas nazývané *Heisenberg-Pauli-Weylova nerovnost*) vypadá následovně.

Věta 14.1. *Nechť $f \in L_2(\mathbb{R})$ a nechť $a, b \in \mathbb{R}$ jsou libovolná reálná čísla. Pak*

$$\left(\int_{-\infty}^{\infty} (x-a)^2 |f(x)|^2 dx \right)^{1/2} \cdot \left(\int_{-\infty}^{\infty} (\xi-b)^2 |\mathcal{F}f(\xi)|^2 d\xi \right)^{1/2} \geq \frac{1}{2} \|f\|_2^2. \quad (14.1)$$

Důkaz. Nejprve provedeme (instruktivní) důkaz pro hladké funkce $f \in \mathcal{S}(\mathbb{R})$. Jednoduchými substitucemi (tzv. translací a modulací, tedy pomocí funkcí typu $e^{-i\langle x, \beta \rangle} f(x - \alpha)$ místo f) se můžeme omezit na $a = b = 0$. Navíc můžeme předpokládat, že $\|f\|_2 = 1$. Poté dostaneme

$$1 = \int_{-\infty}^{\infty} |f(x)|^2 dx = - \int_{-\infty}^{\infty} x \frac{d}{dx} |f(x)|^2 dx = - \int_{-\infty}^{\infty} \left(x f'(x) \overline{f(x)} + x \overline{f'(x)} f(x) \right) dx,$$

kde jsme použili parciální integraci a identitu $|f|^2 = f \overline{f}$. Platí tedy

$$1 \leq 2 \int_{-\infty}^{\infty} |x| \cdot |f(x)| \cdot |f'(x)| dx \leq 2 \left(\int_{-\infty}^{\infty} x^2 |f(x)|^2 dx \right)^{1/2} \left(\int_{-\infty}^{\infty} |f'(x)|^2 dx \right)^{1/2}.$$

Důkaz pak již snadno dokončíme Parsevalovou identitou

$$\|f'\|_2 = \|\mathcal{F}(f')\|_2 = \|\xi \cdot \mathcal{F}f(\xi)\|_2.$$

Tím je (14.1) dokázáno pro hladké f .

Důkaz pro $f \in L_2(\mathbb{R})$ plyne pak pomocí obvyklé aproximace. Budeme předpokládat, že $xf(x)$ i $\xi \mathcal{F}f(\xi)$ leží obě v $L_2(\mathbb{R})$. Pro $\varphi \in \mathcal{S}(\mathbb{R})$, $\varphi \geq 0$ a $\int_{\mathbb{R}} \varphi = 1$ položíme $f_n = \varphi_n * f$, kde $\varphi_n(x) = n\varphi(nx)$.

Potom $\|f_n - f\|_2 \rightarrow 0$ pro $n \rightarrow \infty$. Dále platí, že

$$\xi(\mathcal{F}f)(\xi) - \xi(\mathcal{F}f_n)(\xi) = \xi(\mathcal{F}f)(\xi)(1 - (\mathcal{F}\varphi)(\xi/n))$$

a $\|\xi(\mathcal{F}f_n)(\xi)\|_2 \rightarrow \|\xi(\mathcal{F}f)(\xi)\|_2$ plyne z $\xi(\mathcal{F}f)(\xi) \in L_2(\mathbb{R})$ a Lebesgueovy věty o dominantní konvergenci.

Z $xf(x) \in L_2(\mathbb{R})$ plyne na druhou stranu, že pro $L > 0$ velké, je $\int_{|x|>L} |xf(x)|^2 dx$ malé a (uniformně v n) i $\int_{|x|>L} |xf_n(x)|^2 dx$ je malé, a odtud, že i $\|xf(x) - xf_n(x)\|_2 \rightarrow 0$. Tím je důkaz hotov. \square

V \mathbb{R}^d platí téměř stejné tvrzení, důkaz (opět pro hladké f) plyne z identity

$$\sum_{j=1}^n \frac{1}{2} x_j \frac{\partial}{\partial x_j} |f(x)|^2 = \operatorname{Re} \left(\nabla f(x) \cdot \overline{xf(x)} \right).$$

Vyintegrováním přes \mathbb{R}^d a užitím parciální integrace dostaneme

$$\begin{aligned} \frac{d}{2} \|f\|_2^2 &= \operatorname{Re} \left(\int_{\mathbb{R}^d} \nabla f(x) \cdot \overline{xf(x)} dx \right) \leq \left| \int_{\mathbb{R}^d} \nabla f(x) \cdot \overline{xf(x)} dx \right| \\ &= \|\nabla f\|_2 \cdot \|xf(x)\|_2 = \|\xi(\mathcal{F}f)(\xi)\|_2 \cdot \|xf(x)\|_2. \end{aligned}$$

Princip neurčitosti platí v překvapivé obecnosti, předchozí věta pak vyplyne jako speciální případ.

Věta 14.2. *Nechť A a B jsou (omezené či neomezené) samoadjungované operátory na Hilbertově prostoru H . Pak*

$$\|(A - aI)f\| \cdot \|(B - bI)f\| \geq \frac{1}{2} |\langle [A, B]f, f \rangle|$$

pro všechna $a, b \in \mathbb{R}$ a všechna f v definičním oboru AB a BA . Poznamenejme, že $[A, B] = AB - BA$ je komutátor A a B .

Důkaz. Platí

$$\begin{aligned} \langle [A, B]f, f \rangle &= \langle (AB - BA)f, f \rangle \\ &= \langle \{(A - aI)(B - bI) - (B - bI)(A - aI)\}f, f \rangle \\ &= \langle (B - bI)f, (A - aI)f \rangle - \langle (A - aI)f, (B - bI)f \rangle \\ &= 2i \operatorname{Im} \langle (B - bI)f, (A - aI)f \rangle. \end{aligned}$$

Zbytek pak plyne z Cauchy-Schwartzovy nerovnosti. \square

Věta 14.1 plyne volbou

$$Xf(x) = xf(x), \quad Pf(x) = if'(x).$$

Definiční obory těchto zobrazení jsou dány přirozeně, $D(X) = \{f \in L_2(\mathbb{R}) : xf(x) \in L_2(\mathbb{R})\}$ a $D(P) = \{f \in L_2(\mathbb{R}) : \xi \mathcal{F}f(\xi) \in L_2(\mathbb{R})\}$.

Pokud f není v $D(X)$ nebo $D(P)$, pak je levá strana (14.1) nekonečná. Pokud je f v $D(PX)$ i v $D(XP)$, pak obdržíme

$$[X, P]f(x) = ix f'(x) - i(xf(x))' = -if(x)$$

a

$$\frac{\|f\|_2^2}{2} = \frac{1}{2} |\langle -if(x), f(x) \rangle| \leq \|(X - aI)f\|_2 \cdot \|(P - bI)f\|_2,$$

kde

$$\|(P - bI)f\|_2 = \|\mathcal{F}(P - bI)f\|_2 = \|(\xi - b)\mathcal{F}f(\xi)\|_2.$$

Princip neurčitosti Donoha a Starka

Jiné vyjádření faktu, že funkce i její Fourierova transformace nemohou být koncentrované zároveň, poskytuje princip neurčitosti pocházející od Donoha a Starka. Řekneme, že $f \in L_2(\mathbb{R}^d)$ je ε -koncentrovaná na měřitelné množině $T \subset \mathbb{R}^d$, pokud

$$\left(\int_{T^c} |f(x)|^2 dx \right)^{1/2} \leq \varepsilon \|f\|_2.$$

Věta 14.3. *Nechť $f \in L_2(\mathbb{R}^d)$, $f \neq 0$, je ε_T -koncentrovaná na $T \subset \mathbb{R}^d$ a $\mathcal{F}f$ je ε_Ω -koncentrovaná na $\Omega \subset \mathbb{R}^d$. Pak*

$$|T| \cdot |\Omega| \geq (1 - \varepsilon_T - \varepsilon_\Omega)^2.$$

Důkaz. Můžeme jistě předpokládat, že T a Ω mají konečnou míru. Definujeme dva operátory obvyklé v analýze signálů

$$\begin{aligned} P_T f &= \chi_T \cdot f \\ Q_\Omega f(x) &= \mathcal{F}^{-1}(\chi_\Omega \mathcal{F}f)(x) = \frac{1}{(2\pi)^{d/2}} \int_{\mathbb{R}^d} e^{ix \cdot \xi} \mathcal{F}f(\xi) d\xi. \end{aligned}$$

Oba tyto operátory jsou ortogonální projekce; P_T je projekce na $\{f \in L_2(\mathbb{R}^d) : \text{supp } f \subset T\}$ a Q_Ω je projekce na $\{f \in L_2(\mathbb{R}^d) : \text{supp } \mathcal{F}f \subset Q\}$. Při tomto označení platí, že f je ε_T -koncentrovaná na T , pokud

$$\|f - P_T f\|_2 \leq \varepsilon_T \cdot \|f\|_2$$

a $\mathcal{F}f$ je ε_Ω -koncentrovaná na Ω , pokud

$$\|f - Q_\Omega f\|_2 = \|\chi_{\Omega^c} \mathcal{F}f\|_2 \leq \varepsilon_\Omega \cdot \|f\|_2.$$

Nejprve odhadneme

$$\|f - Q_\Omega P_T f\|_2 \leq \|f - Q_\Omega f\|_2 + \|Q_\Omega(f - P_T f)\|_2 \leq (\varepsilon_\Omega + \varepsilon_T) \|f\|_2$$

a dostaneme

$$\|Q_\Omega P_T f\|_2 \geq \|f\|_2 - \|f - Q_\Omega P_T f\|_2 \geq (1 - \varepsilon_\Omega - \varepsilon_T) \|f\|_2.$$

Pro dokončení důkazu potřebujeme odhadnout $\|Q_\Omega P_T f\|_2$.

$$\begin{aligned} Q_\Omega P_T f(x) &= \mathcal{F}^{-1}(\chi_\Omega \mathcal{F}(P_T f))(x) = \frac{1}{(2\pi)^{d/2}} \int_{\mathbb{R}^d} \chi_\Omega(\xi) \mathcal{F}(P_T f)(\xi) e^{ix \cdot \xi} d\xi \\ &= \frac{1}{(2\pi)^{d/2}} \int_{\Omega} \mathcal{F}(P_T f)(\xi) e^{ix \cdot \xi} d\xi = \frac{1}{(2\pi)^d} \int_{\Omega} \int_{\mathbb{R}^d} (\chi_T f)(z) e^{-i\xi \cdot z} dz e^{ix \cdot \xi} d\xi \\ &= \frac{1}{(2\pi)^d} \int_{\Omega} \left(\int_T f(z) e^{-i\xi \cdot z} dz \right) e^{ix \cdot \xi} d\xi. \end{aligned}$$

Protože $f \in L_2(T) \subset L_1(T)$ a T i Ω mají konečnou míru, integrál konverguje absolutně a můžeme použít Fubiniho větu.

$$\begin{aligned} Q_\Omega P_T f(x) &= \frac{1}{(2\pi)^d} \int_T f(z) \left(\int_{\Omega} e^{ix \cdot \xi} e^{-i\xi \cdot z} d\xi \right) dz \\ &= \int_{\mathbb{R}^d} K(x, t) f(t) dt, \end{aligned}$$

kde

$$K(x, t) = \frac{\chi_T(t)}{(2\pi)^d} \int_{\Omega} e^{i(x-t) \cdot \xi} d\xi = \frac{\chi_T(t)}{(2\pi)^{d/2}} \cdot T_t(\mathcal{F}^{-1} \chi_\Omega)(x).$$

Hilbert-Schmidtovu normu $Q_\Omega P_T$ spočteme jako

$$\|Q_\Omega P_T\|_{HS}^2 = \int_{\mathbb{R}^d} \int_{\mathbb{R}^d} |K(x, t)|^2 dx dt,$$

kde

$$\int_{\mathbb{R}^d} |K(x, t)|^2 dx = \frac{\chi_T(t)}{(2\pi)^d} \cdot \|T_t \mathcal{F}^{-1} \chi_\Omega\|_2^2 = \frac{\chi_T(t)}{(2\pi)^d} \cdot \|\chi_\Omega\|_2^2 = \frac{\chi_T(t)}{(2\pi)^d} \cdot |\Omega|$$

a

$$\|Q_\Omega P_T\|_{HS}^2 = \int_{\mathbb{R}^d} \int_{\mathbb{R}^d} |K(x, t)|^2 dx dt = |\Omega| \cdot |T|.$$

Nakonec využijeme toho, že operátorová norma je nejvýše rovna Hilbert-Schmidtově normě a dostaneme

$$\begin{aligned}(1 - \varepsilon_T - \varepsilon_\Omega)^2 \cdot \|f\|_2^2 &\leq \|Q_\Omega P_T f\|_2^2 \leq \|Q_\Omega P_T\|^2 \cdot \|f\|_2^2 \\ &\leq \|Q_\Omega P_T\|_{HS}^2 \cdot \|f\|_2^2 = |T| \cdot |\Omega| \cdot \|f\|_2^2.\end{aligned}$$

□

Z předchozí věty plyne jednoduchý důsledek: Má-li $f \in L_2(\mathbb{R}^d)$ jak $\text{supp } f \subset T$ tak i $\text{supp } \mathcal{F}f \subset Q$, pak $|T| \cdot |Q| \geq 1$ - v předchozí větě stačí zvolit $\varepsilon_T = \varepsilon_\Omega = 0$.

15 Náhodné algoritmy

23

Cílem je představit algoritmus pro tzv. *Approximate Counting*. Pokud máme v klasickém případě určit počet výskytů nějaké události, tak inicializujeme počítadlo na nulu a při každém výskytu dané události přičteme jedničku. Toto řešení je tak triviální, že se zdá, že není možné (a že ani není důvod) postupovat jinak. Pokud nepotřebujeme znát ale přesný počet těchto událostí, ale chceme (drasticky) snížit paměťovou náročnost (například proto, že daných počítadel máme uloženo velké množství), pak můžeme postupovat podle algoritmu *Robert Morris, CACM '78*.

Triviální řešení (viz výše) vyžaduje $\lceil \log_2(n) \rceil$ bitů při n událostech. Chceme-li znát přesný počet událostí, pak je tento počet i optimální. Použijeme-li méně bitů (např. $t < \lceil \log_2(n) \rceil$) a zakódujeme-li čísla od 1 do n pomocí tohoto počtu bitů (což znamená, že každému přiřadíme jednu z 2^t kódů, které lze z těchto bitů vytvořit), pak se nutně některé dvě z těchto čísel musí zobrazit na stejný kód a jsou tedy nerozlišitelné. Keyword: *pidgeonhole principle*.

Pokud potřebujeme znát počet událostí jen přibližně, pak toto lze zařídit randomizovaným algoritmem. Přesněji, budeme chtít, aby výstup algoritmu (označený \tilde{n}) splňoval

$$\mathbb{P}(|\tilde{n} - n| > \varepsilon n) < \delta$$

pro nějaké malé $\varepsilon, \delta > 0$. Typické hodnoty budou např. $\varepsilon = \frac{1}{3}$ a $\delta = 0.01$ (tedy $2n/3 \leq \tilde{n} \leq 4n/3$ s pravděpodobností alespoň 99%). Toto lze určitě zařídit s menším počtem bitů. V intervalu $[2n/3, 4n/3)$ leží právě jedno dyadické číslo, tedy číslo tvaru $2^k, k \in \mathbb{N}$. Dyadických čísel mezi 0 a $4n/3$ je ca. $\log_2(n)$ a na jejich zakódování tedy stačí $\log_2(\log_2(n))$ bitů. Podle stejného principu je toto minimální počet bitů. Je ale tato mez dosažitelná?

Algorithm 1 Morrisův algoritmus

- 1: **Inicializuj:** $X = 0$
 - 2: **Při každé události:** zvětš X o 1 s pravděpodobností $\frac{1}{2^X}$
 - 3: **Výstup:** $2^X - 1$
-

Tedy $\tilde{n} = 2^X - 1$. Intuitivně by tedy mělo platit, že $X \sim \log_2(n)$. Samozřejmě, X je náhodná proměnná, a všechny vlastnosti X platí s větší či menší pravděpodobností. Analýza tohoto algoritmu spočívá v důkazu jeho vlastností. Pro ten účel potřebujeme nějaké vlastnosti náhodných proměnných.

- Nechť X je náhodná proměnná s diskrétním oborem hodnot S .
- Pak $\mathbb{E}X = \sum_{j \in S} j \mathbb{P}(X = j)$,
- $\mathbb{E}(X + Y) = \mathbb{E}X + \mathbb{E}Y$ (linearita střední hodnoty),
- Markovova nerovnost: Pokud $X > 0$, pak

$$\forall \lambda > 0 : \mathbb{P}(X > \lambda) < \frac{\mathbb{E}X}{\lambda},$$

²³Podle první přednášky Jelaniho Nelsona, Random Algorithms (později Algorithms for Big Data, Harvard)

- Chebysheva nerovnost

$$\forall \lambda > 0 : \mathbb{P}(|X - \mathbb{E}X| > \lambda) < \frac{\mathbb{E}[(X - \mathbb{E}X)^2]}{\lambda^2}.$$

Důkaz: Markovova nerovnost a

$$\mathbb{P}(|X - \mathbb{E}X| > \lambda) = \mathbb{P}(|X - \mathbb{E}X|^2 > \lambda^2).$$

Stejně projde i s $p \neq 2$.

- Chernoff: Pro X_1, \dots, X_n nezávislé s $X_i \in [0, 1]$. Pak pro $X = \sum_i X_i$ platí

$$\mathbb{P}(|X - \mathbb{E}X| > \lambda \mathbb{E}X) \leq 2 \exp(-\lambda^2 \mathbb{E}X/3), \quad 0 < \lambda < 1.$$

Důkaz: Označme $p_i = \mathbb{E}X_i \in [0, 1]$ a $p = \sum_i p_i = \mathbb{E}X$. Necht' opět $t > 0$. Pak $X_i = 0 \cdot (1 - X_i) + 1 \cdot X_i$ a z konvexity funkce $x \rightarrow e^{tx}$ plyne

$$e^{tX_i} \leq (1 - X_i)e^{t \cdot 0} + X_i \cdot e^{t \cdot 1} = (1 - X_i) + e^t X_i$$

a ve střední hodnotě

$$\mathbb{E}e^{tX_i} \leq 1 - \mathbb{E}X_i + e^t \mathbb{E}X_i = 1 - p_i + e^t p_i.$$

Protože

$$\mathbb{P}(|X - p| > \lambda p) \leq \mathbb{P}(X > (1 + \lambda)p) + \mathbb{P}(X < (1 - \lambda)p),$$

budeme odhadovat jen první z obou pravděpodobností napravo, druhá je podobná.

Pro $t > 0$ tedy upravujeme (pomocí nerovnosti $1 + s \leq e^s$)

$$\begin{aligned} \mathbb{P}(X > (1 + \lambda)p) &= \mathbb{P}(tX > (1 + \lambda)tp) = \mathbb{P}(e^{tX} > e^{(1+\lambda)tp}) \\ &\leq e^{-(1+\lambda)tp} \mathbb{E}e^{tX} = e^{-(1+\lambda)tp} \prod_{i=1}^n \mathbb{E}e^{tX_i} \leq e^{-(1+\lambda)tp} \prod_{i=1}^n (1 - p_i + e^t p_i) \\ &= e^{-(1+\lambda)tp} \prod_{i=1}^n (1 + p_i(e^t - 1)) \leq e^{-(1+\lambda)tp} \prod_{i=1}^n e^{p_i(e^t - 1)} \\ &= e^{-(1+\lambda)tp} e^{p(e^t - 1)}. \end{aligned}$$

Položme nyní $t = \ln(1 + \lambda)$

$$\mathbb{P}(X > (1 + \lambda)p) \leq e^{-(1+\lambda) \ln(1+\lambda)p} e^{p\lambda} = \left(\frac{e^\lambda}{(1 + \lambda)^{1+\lambda}} \right)^p.$$

Poslední výraz je pak menší než $(e^{-\lambda^2/3})^p$, což lze ukázat pomocí elementárního kalkulu.

V dalším budeme postupně analyzovat Algoritmus 1, odvozovat jeho vlastnosti a navrhnout úpravy k jejich vylepšení.

Věta 15.1. *Necht' X_n je hodnota proměnné X po n krocích. Pak $\mathbb{E}[2^{X_n} - 1] = n$.*

Důkaz. Důkaz provedeme indukcí. Pro $n = 0$ je $X_n = 0$ a $2^{X_n} - 1 = 0 = n$. V prvním kroce je $X = 0$ a X je tedy zvětšeno o 1 s pravděpodobností $1/2^0 = 1$, tedy (skoro) jistě. Tedy i pro $n = 1$ je $\mathbb{E}[2^{X_1}] = 2^1 = 2$.

Nechť $n \geq 2$. Pak předpokládáme, že $\mathbb{E}[2^{X_{n-1}}] = n$, použijeme, že $\mathbb{P}(X_{n-1} = 0) = 0$, a počítáme

$$\begin{aligned}\mathbb{E}[2^{X_n}] &= \sum_{i=1}^{\infty} 2^i \mathbb{P}(X_n = i) \\ &= \sum_{i=1}^{\infty} 2^i \left(\mathbb{P}(X_{n-1} = i-1) \cdot \frac{1}{2^{i-1}} + \mathbb{P}(X_{n-1} = i) \cdot \left(1 - \frac{1}{2^i}\right) \right) \\ &= \sum_{i=1}^{\infty} 2\mathbb{P}(X_{n-1} = i-1) + \sum_{i=1}^{\infty} 2^i \mathbb{P}(X_{n-1} = i) - \sum_{i=1}^{\infty} \mathbb{P}(X_{n-1} = i) \\ &= \sum_{i=2}^{\infty} 2\mathbb{P}(X_{n-1} = i-1) + \mathbb{E}[2^{X_{n-1}}] - 1 \\ &= \mathbb{E}[2^{X_{n-1}}] + 1 = n + 1.\end{aligned}$$

□

Věta 15.2. Uložení X po n krocích vyžaduje $O(\ln \ln n)$ bitů s pravděpodobností $\geq 90\%$.

Důkaz. Z Markovovy nerovnosti plyne

$$\mathbb{P}(2^{X_n} - 1 > 10n) = \mathbb{P}\left(\frac{2^{X_n} - 1}{10n} > 1\right) \leq \mathbb{E}\left[\frac{2^{X_n} - 1}{10n}\right] = 0.1.$$

Na uložení X_n budeme tedy (s pravděpodobností alespoň 90%) potřebovat nejvýše

$$\ln \ln(10n) = O(\ln \ln n)$$

bitů.

□

Náhodná veličina $2^{X_n} - 1$ má nejen střední hodnotu n , ale umíme odhadnout i jak silně se okolo této hodnoty koncentruje.

Věta 15.3. $\text{var}[2^{X_n} - 1] = \frac{n(n-1)}{2}$.

Důkaz.

$$\begin{aligned}\text{var}[2^{X_n} - 1] &= \mathbb{E}[2^{X_n} - 1 - n]^2 = \mathbb{E}[2^{X_n} - 1]^2 - 2n\mathbb{E}[2^{X_n} - 1] + n^2 = \mathbb{E}[2^{X_n} - 1]^2 - n^2 \\ &= \mathbb{E}[2^{2X_n}] - 2\mathbb{E}[2^{X_n}] + 1 - n^2 = \mathbb{E}[2^{2X_n}] - 2(n+1) + 1 - n^2 \\ &= \mathbb{E}[2^{2X_n}] - n^2 - 2n - 1.\end{aligned}$$

Nyní spočteme $\mathbb{E}[2^{2X_n}]$

$$\begin{aligned}
\mathbb{E}[2^{2X_n}] &= \sum_{i=1}^{\infty} 2^{2i} \mathbb{P}(X_n = i) \\
&= \sum_{i=1}^{\infty} 2^{2i} \left(\mathbb{P}(X_{n-1} = i-1) \cdot \frac{1}{2^{i-1}} + \mathbb{P}(X_{n-1} = i) \cdot \left(1 - \frac{1}{2^i}\right) \right) \\
&= \sum_{i=1}^{\infty} 2^{i+1} \mathbb{P}(X_{n-1} = i-1) + \sum_{i=1}^{\infty} 2^{2i} \mathbb{P}(X_{n-1} = i) - \sum_{i=1}^{\infty} 2^i \mathbb{P}(X_{n-1} = i) \\
&= 4\mathbb{E}[2^{X_{n-1}}] + \mathbb{E}[2^{2X_{n-1}}] - \mathbb{E}[2^{X_{n-1}}] = 3\mathbb{E}[2^{X_{n-1}}] + \mathbb{E}[2^{2X_{n-1}}] = 3n + \mathbb{E}[2^{2X_{n-1}}].
\end{aligned}$$

Celkem tedy můžeme použít indukci. $\mathbb{E}[2^{2X_0}] = \mathbb{E}[1] = 1$, $\mathbb{E}[2^{2X_1}] = \mathbb{E}[2^2] = 4$ a

$$\mathbb{E}[2^{2X_n}] = \sum_{i=1}^n 3i + 1 = \frac{3n(n+1)}{2} + 1.$$

Celkem je tedy

$$\text{var}[2^{X_n} - 1] = \frac{3n(n+1)}{2} + 1 - n^2 - 2n - 1 = \frac{3n^2 + 3n - 2n^2 - 4n}{2} = \frac{n(n-1)}{2}.$$

□

Dohromady s Chebyshevovou nerovností pak okamžitě dostaneme

$$\mathbb{P}(|2^{X_n} - 1 - n| > \lambda n) \leq \frac{\text{var}[2^{X_n} - 1]}{\lambda^2 n^2} = \frac{n(n-1)}{2\lambda^2 n^2} \leq \frac{1}{2\lambda^2}.$$

Tento odhad už dává jakousi představu o velikosti $\mathbb{E}[2^{X_n} - 1]$, ale chtěli bychom ještě lepší odhad. Dosáhneme toho jednoduchým trikem, paralelními kopiemi Morrisova počítadla.

Algorithm 2 Morris+ algoritmus

- 1: **Paralelně spustíme k nezávislých Morrisových počítadel X^1, \dots, X^k**
 - 2: **Výstup:** $Y_n = \frac{1}{k} \sum_{j=1}^k (2^{X_n^j} - 1)$.
-

Věta 15.4. Platí $\mathbb{E}[Y_n] = n$, $\text{var}[Y_n] = \frac{n(n-1)}{2k}$.

Důkaz. Z linearitě střední hodnoty plyne $\mathbb{E}[Y_n] = \frac{1}{k} \sum_{j=1}^k \mathbb{E}[2^{X_n^j} - 1] = n$. Dále z nezávislosti X^j

$$\begin{aligned}
\text{var}[Y_n] &= \mathbb{E}[Y_n - n]^2 = \mathbb{E}\left[\frac{1}{k} \sum_{j=1}^k (2^{X_n^j} - 1) - n\right]^2 = \mathbb{E}\left[\frac{1}{k} \sum_{j=1}^k (2^{X_n^j} - 1 - n)\right]^2 \\
&= \frac{1}{k^2} \sum_{j=1}^k \mathbb{E}(2^{X_n^j} - 1 - n)^2 = \frac{1}{k^2} \sum_{j=1}^k \text{var}[2^{X_n^j} - 1] = \frac{1}{k} \text{var}[2^{X_n} - 1] = \frac{n(n-1)}{2k}.
\end{aligned}$$

□

Stejně jako dřív pak dostaneme

$$\mathbb{P}(|Y_n - n| > \lambda n) \leq \frac{\text{var}[Y_n]}{\lambda^2 n^2} = \frac{n(n-1)}{2k\lambda^2 n^2} \leq \frac{1}{2k\lambda^2}.$$

Aby byl předchozí výraz menší než $\delta > 0$, museli bychom zvolit $\frac{1}{2k\lambda^2} = \delta$, tedy $k = \frac{1}{2\delta\lambda^2}$, tedy zbytečně veliké. Následujícím trikem snížíme δ^{-1} na $\ln(\delta^{-1})$.

Algorithm 3 Morris++ algoritmus

- 1: **Paralelně spustíme l nezávislých Morrisových+ počítadel Y^1, \dots, Y^l s $k = \frac{1}{2 \cdot 1/3 \cdot \lambda^2}$, tedy $\delta = 1/3$**
 - 2: **Výstup:** Z_n bude medián Y_n^1, \dots, Y_n^l , output je Z_n .
-

Potom víme, že $|Y_n^j - n| \leq \lambda n$ s pravděpodobností alespoň $2/3$. Definujme

$$\Lambda_j = \begin{cases} 1, & \text{pokud Morris+ neuspěl, tedy pokud } |Y_n^j - n| > \lambda n, \\ 0, & \text{jinak.} \end{cases}$$

Pokud Morris++ neuspěje, tedy $|Z_n - n| > \lambda n$, pak to znamená, že neuspěla aspoň polovina Morris+ instancí, tedy když $\sum_{m=1}^l \Lambda_m > l/2$. Použijeme $\mathbb{E}\Lambda_j \leq 1/3$ a Chernoff bound a dostaneme

$$\begin{aligned} \mathbb{P}\left(\sum_{m=1}^l \Lambda_m > \frac{l}{2}\right) &\leq \mathbb{P}\left(\sum_{m=1}^l \Lambda_m - \sum_{m=1}^l \mathbb{E}[\Lambda_m] > \frac{l}{6}\right) \\ &\leq \mathbb{P}\left(\left|\sum_{m=1}^l [\Lambda_m - \mathbb{E}[\Lambda_m]]\right| > \frac{l}{6}\right) \\ &\leq \mathbb{P}\left(\left|\sum_{m=1}^l [\Lambda_m - \mathbb{E}[\Lambda_m]]\right| > \frac{1}{6\mathbb{E}\Lambda} \cdot l\mathbb{E}\Lambda\right) \\ &\leq 2 \exp\left(-\frac{1}{36[\mathbb{E}\Lambda]^2} \cdot l\mathbb{E}\Lambda \cdot \frac{1}{3}\right) = 2 \exp\left(-\frac{l}{3 \cdot 36\mathbb{E}\Lambda}\right) \leq 2 \exp\left(-\frac{l}{36}\right). \end{aligned}$$

Chceme-li poslední výraz zmenšit pod $\delta > 0$, stačí volit $l = O(\ln(\delta^{-1}))$.

16 Laplacův operátor

Polární souřadnice²⁴

(Skoro) každý bod roviny $(x, y) \in \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ lze vyjádřit jako

$$x = r \cos \varphi, \quad (16.1)$$

$$y = r \sin \varphi, \quad (16.2)$$

kde $r > 0$ a $\varphi \in (-\pi, \pi)$. Tento zápis můžeme zkrátit jako $(x, y) = \Phi(r, \varphi)$, kde $\Phi : (0, \infty) \times (-\pi, \pi)$ je dáno (16.1) a (16.2).

Převodem funkce (a operátoru) do polárních souřadnic rozumíme následující úlohu: Pokud je $f(x, y)$ (hladká) funkce proměnných x a y , najděte funkci $w(r, \varphi)$, tak aby $w(r, \varphi) = f(\Phi(r, \varphi)) = (f \circ \Phi)(r, \varphi)$. Dále pak chceme vyjádřit parciální derivace prvního a vyšších řádů funkce f (podle x a y) pomocí parciálních derivací w (podle r a φ). Při tom chceme, aby se v daných výrazech vyskytovaly parciální derivace Φ podle r a φ (které jsou na první pohled snadno vyjádřitelné), ale rádi bychom se vyhlí derivacím Φ^{-1} , které jsou mnohem techničtější.

Pro polární souřadnice lze tuto úlohu vyřešit “hrubou silou”. Definujeme

$$w(r, \varphi) = f(r \cos \varphi, r \sin \varphi) \quad (16.3)$$

a tento vztah derivujeme tolikrát (podle r a φ), kolikrát bude zapotřebí. Dostaneme

$$\frac{\partial}{\partial r} w(r, \varphi) = \frac{\partial}{\partial x} f(r \cos \varphi, r \sin \varphi) \cdot \cos \varphi + \frac{\partial}{\partial y} f(r \cos \varphi, r \sin \varphi) \cdot \sin \varphi, \quad (16.4)$$

$$\frac{\partial}{\partial \varphi} w(r, \varphi) = \frac{\partial}{\partial x} f(r \cos \varphi, r \sin \varphi) \cdot (-r \sin \varphi) + \frac{\partial}{\partial y} f(r \cos \varphi, r \sin \varphi) \cdot (r \cos \varphi). \quad (16.5)$$

Z této soustavy dvou rovnic o dvou neznámých vyjádříme

$$\begin{aligned} \frac{\partial}{\partial x} f(x, y) &= \frac{\partial}{\partial x} f(r \cos \varphi, r \sin \varphi) = \frac{1}{r} \left(r \cos \varphi \cdot \frac{\partial}{\partial r} w(r, \varphi) - \sin \varphi \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) \right) \\ \frac{\partial}{\partial y} f(x, y) &= \frac{\partial}{\partial y} f(r \cos \varphi, r \sin \varphi) = \frac{1}{r} \left(r \sin \varphi \cdot \frac{\partial}{\partial r} w(r, \varphi) + \cos \varphi \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) \right). \end{aligned}$$

Máme-li tedy rovnici (16.3), vyjádříme parciální derivace f podle x a y tak, že vezmeme parciální derivace w podle r a φ a dosadíme do předchozích rovnic. Formálně bývá zvykem tento zápis zkracovat na

$$\begin{aligned} \frac{\partial}{\partial x} &= \frac{1}{r} \left(r \cos \varphi \cdot \frac{\partial}{\partial r} - \sin \varphi \cdot \frac{\partial}{\partial \varphi} \right) \\ \frac{\partial}{\partial y} &= \frac{1}{r} \left(r \sin \varphi \cdot \frac{\partial}{\partial r} + \cos \varphi \cdot \frac{\partial}{\partial \varphi} \right), \end{aligned}$$

nebo dokonce

$$\nabla = \left(\frac{1}{r} \left(r \cos \varphi \cdot \frac{\partial}{\partial r} - \sin \varphi \cdot \frac{\partial}{\partial \varphi} \right), \frac{1}{r} \left(r \sin \varphi \cdot \frac{\partial}{\partial r} + \cos \varphi \cdot \frac{\partial}{\partial \varphi} \right) \right),$$

²⁴Antonín Češík, 20. 3. 2019

nebo

$$\begin{pmatrix} \frac{\partial}{\partial x} \\ \frac{\partial}{\partial y} \end{pmatrix} = \begin{pmatrix} \cos \varphi & -\frac{\sin \varphi}{r} \\ \sin \varphi & \frac{\cos \varphi}{r} \end{pmatrix} \begin{pmatrix} \frac{\partial}{\partial r} \\ \frac{\partial}{\partial \varphi} \end{pmatrix}.$$

Tyto formule lze aplikovat kdykoliv, máme-li nějakou funkci převedenu do polárních souřadnic (jako v (16.3)), tedy například i na $\frac{\partial}{\partial x} f$. Dostaneme tak

$$\begin{aligned} \frac{\partial^2}{\partial x^2} f(x, y) &= \frac{\partial}{\partial x} \left(\frac{\partial}{\partial x} f(x, y) \right) \\ &= \frac{1}{r} \left(r \cos \varphi \cdot \frac{\partial}{\partial r} - \sin \varphi \cdot \frac{\partial}{\partial \varphi} \right) \left(\cos \varphi \cdot \frac{\partial}{\partial r} w(r, \varphi) - \frac{\sin \varphi}{r} \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) \right) \\ &= \frac{1}{r} \left\{ r \cos^2 \varphi \frac{\partial^2}{\partial r^2} w(r, \varphi) - r \cos \varphi \sin \varphi \left[-\frac{1}{r^2} \frac{\partial}{\partial \varphi} w(r, \varphi) + \frac{1}{r} \frac{\partial^2}{\partial r \partial \varphi} w(r, \varphi) \right] \right. \\ &\quad \left. - \sin \varphi \left[(-\sin \varphi) \cdot \frac{\partial}{\partial r} w(r, \varphi) + \cos \varphi \cdot \frac{\partial^2}{\partial r \partial \varphi} w(r, \varphi) \right] \right. \\ &\quad \left. + \frac{\sin \varphi}{r} \left[\cos \varphi \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) + \sin \varphi \cdot \frac{\partial^2}{\partial \varphi^2} w(r, \varphi) \right] \right\} \end{aligned}$$

a

$$\begin{aligned} \frac{\partial^2}{\partial y^2} f(x, y) &= \frac{\partial}{\partial y} \left(\frac{\partial}{\partial y} f(x, y) \right) \\ &= \frac{1}{r} \left(r \sin \varphi \cdot \frac{\partial}{\partial r} + \cos \varphi \cdot \frac{\partial}{\partial \varphi} \right) \left(\sin \varphi \cdot \frac{\partial}{\partial r} w(r, \varphi) + \frac{\cos \varphi}{r} \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) \right) \\ &= \frac{1}{r} \left\{ r \sin^2 \varphi \frac{\partial^2}{\partial r^2} w(r, \varphi) + r \sin \varphi \cos \varphi \left[-\frac{1}{r^2} \frac{\partial}{\partial \varphi} w(r, \varphi) + \frac{1}{r} \frac{\partial^2}{\partial r \partial \varphi} w(r, \varphi) \right] \right. \\ &\quad \left. + \cos \varphi \left[\cos \varphi \cdot \frac{\partial}{\partial r} w(r, \varphi) + \sin \varphi \cdot \frac{\partial^2}{\partial r \partial \varphi} w(r, \varphi) \right] \right. \\ &\quad \left. + \frac{\cos \varphi}{r} \left[(-\sin \varphi) \cdot \frac{\partial}{\partial \varphi} w(r, \varphi) + \cos \varphi \cdot \frac{\partial^2}{\partial \varphi^2} w(r, \varphi) \right] \right\}. \end{aligned}$$

“Prostým sečtením” pak dostaneme

$$\begin{aligned} \Delta f(x, y) &= \frac{\partial^2}{\partial x^2} f(x, y) + \frac{\partial^2}{\partial y^2} f(x, y) \\ &= \frac{\partial^2}{\partial r^2} w(r, \varphi) + \frac{1}{r} \frac{\partial}{\partial r} w(r, \varphi) + \frac{1}{r^2} \frac{\partial^2}{\partial \varphi^2} w(r, \varphi), \end{aligned}$$

což bývá opět zkracováno jako

$$\Delta = \frac{\partial^2}{\partial r^2} + \frac{1}{r} \frac{\partial}{\partial r} + \frac{1}{r^2} \frac{\partial^2}{\partial \varphi^2} = \frac{1}{r} \frac{\partial}{\partial r} \left(r \frac{\partial}{\partial r} \right) + \frac{1}{r^2} \frac{\partial^2}{\partial \varphi^2}.$$

Poznamenejme jen, že převod Laplace do polárních souřadnic je natolik přímočará záležitost, že stačilo například jen vyderivovat (16.4) a (16.5) ještě jednou podle r a φ a vzniklé rovnice vhodně nakombinovat tak, aby napravo vznikl $\Delta f(x, y)$.

Válcové souřadnice

Válcové souřadnice v \mathbb{R}^3 jsou dány prostě jako polární souřadnice v rovinách paralelních s $x - y$ rovinou, tedy

$$\begin{aligned}x &= r \cos \varphi, \\y &= r \sin \varphi, \\z &= \xi \quad (\text{nebo prostě jako } z = z).\end{aligned}$$

Nepřekvapí proto, že dostaneme

$$\begin{aligned}\frac{\partial}{\partial x} &= \frac{1}{r} \left(r \cos \varphi \cdot \frac{\partial}{\partial r} - \sin \varphi \cdot \frac{\partial}{\partial \varphi} \right), \\ \frac{\partial}{\partial y} &= \frac{1}{r} \left(r \sin \varphi \cdot \frac{\partial}{\partial r} + \cos \varphi \cdot \frac{\partial}{\partial \varphi} \right), \\ \frac{\partial}{\partial z} &= \frac{\partial}{\partial \xi}, \\ \Delta &= \frac{1}{r} \frac{\partial}{\partial r} \left(r \frac{\partial}{\partial r} \right) + \frac{1}{r^2} \frac{\partial^2}{\partial \varphi^2} + \frac{\partial^2}{\partial \xi^2}.\end{aligned}$$

Sférické souřadnice

Sférické souřadnice jsou dány (například) pomocí

$$\begin{aligned}x &= r \cos \varphi \cos \theta, \\y &= r \sin \varphi \cos \theta, \\z &= r \sin \theta,\end{aligned}$$

kde $r > 0$, $\varphi \in (-\pi, \pi)$, $\theta \in (-\pi/2, \pi/2)$. Jakkoliv by bylo možné použít hrubé síly a diferencovat výraz

$$w(r, \varphi, \theta) = f(r \cos \varphi \cos \theta, r \sin \varphi \cos \theta, r \sin \theta)$$

podle r , φ , a θ , zdá se být tento způsob více méně neupočítatelný.

Projdeme dva, zcela různé způsoby, založené na dvou odlišných nápadech.

První způsob²⁵ vyjadřuje sférické souřadnice jako složení dvou válcových transformací. Definujeme

$$(x, y, z) = \Phi(\varrho, \varphi', \xi), \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \varrho \cos \varphi' \\ \varrho \sin \varphi' \\ \xi \end{pmatrix}$$

a

$$(\varrho, \varphi', \xi) = \Psi(r, \varphi, \theta), \quad \begin{pmatrix} \varrho \\ \varphi' \\ \xi \end{pmatrix} = \begin{pmatrix} r \cos \theta \\ \varphi \\ r \sin \theta \end{pmatrix}.$$

Prostým dosazením snadno zjistíme, že $(x, y, z) = (\Phi \circ \Psi)(r, \varphi, \theta)$. Aby dále bylo $(\varrho, \varphi', \xi) \in \mathbb{R}_+ \times (-\pi, \pi) \times \mathbb{R}$, je třeba zvolit $(r, \varphi, \theta) \in \mathbb{R}_+ \times (-\pi, \pi) \times (-\pi/2, \pi/2)$. Využitím předchozích

²⁵Radek Fučík, FJFI, ČVUT

vztahů pro válcové souřadnice pak dostaneme

$$\begin{aligned}\Delta &= \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \\ &= \frac{\partial^2}{\partial \varrho^2} + \frac{1}{\varrho} \frac{\partial}{\partial \varrho} + \frac{1}{\varrho^2} \frac{\partial^2}{\partial \varphi'^2} + \frac{\partial^2}{\partial \xi^2} \\ &= \frac{\partial^2}{\partial \varrho^2} + \frac{\partial^2}{\partial \xi^2} + \frac{1}{r \cos \theta} \frac{\partial}{\partial \varrho} + \frac{1}{r^2 \cos^2 \theta} \frac{\partial^2}{\partial \varphi^2}.\end{aligned}$$

Poslední člen je již hotov. Součet prvních dvou členů (tedy součet druhých derivací podle $\varrho = r \cos \theta$ a $\xi = r \sin \theta$) můžeme vyjádřit pomocí formule odvozené pro polární souřadnice

$$\frac{\partial^2}{\partial \varrho^2} + \frac{\partial^2}{\partial \xi^2} = \frac{\partial^2}{\partial r^2} + \frac{1}{r} \frac{\partial}{\partial r} + \frac{1}{r^2} \frac{\partial^2}{\partial \theta^2}.$$

Chybí tedy převést třetí člen, resp. derivaci podle ϱ . Ta opět odpovídá derivaci podle x v polárních souřadnicích, tedy

$$\frac{\partial}{\partial \varrho} = \frac{1}{r} \left(r \cos \theta \cdot \frac{\partial}{\partial r} - \sin \theta \cdot \frac{\partial}{\partial \theta} \right)$$

Dosazením pak

$$\begin{aligned}\Delta &= \frac{\partial^2}{\partial \varrho^2} + \frac{\partial^2}{\partial \xi^2} + \frac{1}{r \cos \theta} \frac{\partial}{\partial \varrho} + \frac{1}{r^2 \cos^2 \theta} \frac{\partial^2}{\partial \varphi^2} \\ &= \frac{\partial^2}{\partial r^2} + \frac{1}{r} \frac{\partial}{\partial r} + \frac{1}{r^2} \frac{\partial^2}{\partial \theta^2} + \frac{1}{r \cos \theta} \left(\cos \theta \cdot \frac{\partial}{\partial r} - \frac{\sin \theta}{r} \cdot \frac{\partial}{\partial \theta} \right) + \frac{1}{r^2 \cos^2 \theta} \frac{\partial^2}{\partial \varphi^2} \\ &= \frac{1}{r^2} \frac{\partial}{\partial r} \left(r^2 \frac{\partial}{\partial r} \right) + \frac{1}{r^2 \cos \theta} \frac{\partial}{\partial \theta} \left(\cos \theta \cdot \frac{\partial}{\partial \theta} \right) + \frac{1}{r^2 \cos^2 \theta} \frac{\partial^2}{\partial \varphi^2} \\ &= \frac{2}{r} \frac{\partial}{\partial r} + \frac{\partial^2}{\partial r^2} + \frac{1}{r^2} \frac{\partial^2}{\partial \theta^2} - \frac{\sin \theta}{r^2 \cos \theta} \frac{\partial}{\partial \theta} + \frac{1}{r^2 \cos^2 \theta} \frac{\partial^2}{\partial \varphi^2}.\end{aligned}$$

Druhý způsob převodu Laplace do sférických a cylindrických souřadnic je založen na tom, že tyto systémy souřadnic jsou ortogonální - jsou určeny vzájemně kolmými plochami.

Nechť u, v, w jsou křivočaré ortogonální souřadnice v \mathbb{R}^3 . Nechť $\vec{e}_x, \vec{e}_y, \vec{e}_z$ je kanonická báze \mathbb{R}^3 . Definujeme (vektorová pole, $g(u, v, w) = (x, y, z)$)

$$\begin{aligned}\vec{e}_u &= \frac{1}{h_u} \partial_u g, \quad \text{kde} \\ \partial_u g &= \left(\frac{\partial x}{\partial u}, \frac{\partial y}{\partial u}, \frac{\partial z}{\partial u} \right), \\ h_u &= \sqrt{\left(\frac{\partial x}{\partial u} \right)^2 + \left(\frac{\partial y}{\partial u} \right)^2 + \left(\frac{\partial z}{\partial u} \right)^2}\end{aligned}$$

a podobně $\vec{e}_v = \frac{1}{h_v} \partial_v g$ a $\vec{e}_w = \frac{1}{h_w} \partial_w g$. V dalším budeme předpokládat, že $\vec{e}_u, \vec{e}_v, \vec{e}_w$ jsou v každém bodě na sebe kolmé.

a) Dokážeme, že $\frac{1}{h_u} \vec{e}_u = \text{grad } u$, $\frac{1}{h_v} \vec{e}_v = \text{grad } v$, $\frac{1}{h_w} \vec{e}_w = \text{grad } w$.

Nejprve spočteme pro hladkou funkci f

$$\begin{aligned} \text{grad } f \cdot \vec{e}_u &= \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \right) \frac{1}{h_u} \left(\frac{\partial x}{\partial u}, \frac{\partial y}{\partial u}, \frac{\partial z}{\partial u} \right) \\ &= \frac{1}{h_u} \left[\frac{\partial f}{\partial x} \frac{\partial x}{\partial u} + \frac{\partial f}{\partial y} \frac{\partial y}{\partial u} + \frac{\partial f}{\partial z} \frac{\partial z}{\partial u} \right] = \frac{1}{h_u} \partial_u f \end{aligned} \quad (16.6)$$

a podobně pro v a w . Celkově platí

$$\text{grad } f = \frac{1}{h_u} \partial_u f \cdot \vec{e}_u + \frac{1}{h_v} \partial_v f \cdot \vec{e}_v + \frac{1}{h_w} \partial_w f \cdot \vec{e}_w.$$

Pro $f(u, v, w) = u$ vychází

$$\text{grad } u = \frac{1}{h_u} \vec{e}_u$$

a stejně pro v a w .

b) Odvoďte pro vektorové pole $\vec{F} = F_u \vec{e}_u + F_v \vec{e}_v + F_w \vec{e}_w$ reprezentaci

$$\text{div } \vec{F} = \frac{1}{h_u h_v h_w} [\partial_u (h_v h_w F_u) + \partial_v (h_u h_w F_v) + \partial_w (h_u h_v F_w)].$$

Návod: Napíšeme $\vec{e}_u, \vec{e}_v, \vec{e}_w$ jako vektorové součiny a použijeme a) a vhodné formule pro divergenci. Obdržíme $\vec{F} = F_u \vec{e}_u + F_v \vec{e}_v + F_w \vec{e}_w$ a $\vec{e}_u = \vec{e}_v \times \vec{e}_w$, $\vec{e}_v = \vec{e}_w \times \vec{e}_u$, $\vec{e}_w = \vec{e}_u \times \vec{e}_v$.

Celkem tedy

$$\begin{aligned} \text{div } \vec{F} &= \text{div}(F_u \vec{e}_u + F_v \vec{e}_v + F_w \vec{e}_w) \\ &= \text{div}(F_u \vec{e}_u) + \text{div}(F_v \vec{e}_v) + \text{div}(F_w \vec{e}_w). \end{aligned}$$

Upravíme první člen²⁶

$$\begin{aligned} \text{div}(F_u \vec{e}_u) &= \text{div}(F_u (\vec{e}_v \times \vec{e}_w)) = \text{div}(h_v h_w F_u (\text{grad } v \times \text{grad } w)) = \\ &= \text{grad}(h_v h_w F_u) (\text{grad } v \times \text{grad } w) + (h_v h_w F_u) \text{div}(\text{grad } v \times \text{grad } w) \\ &= \text{grad}(h_v h_w F_u) \left(\frac{1}{h_v h_w} \vec{e}_v \times \vec{e}_w \right) = \text{grad}(h_v h_w F_u) \left(\frac{1}{h_v h_w} \vec{e}_u \right) \\ &= \frac{1}{h_v h_w} \text{grad}(h_v h_w F_u) \cdot \vec{e}_u = \frac{1}{h_u h_v h_w} \partial_u (h_v h_w F_u), \end{aligned}$$

kde jsme opět použili (16.6).

c) Pro skalární funkci $f = f(u, v, w)$ ukažte, že pro Laplacův operátor platí následující reprezentace

$$\Delta f = \frac{1}{h_u h_v h_w} \left[\partial_u \left(\frac{h_v h_w}{h_u} \partial_u f \right) + \partial_v \left(\frac{h_u h_w}{h_v} \partial_v f \right) + \partial_w \left(\frac{h_u h_v}{h_w} \partial_w f \right) \right].$$

²⁶ $\text{div}(f \vec{V}) = \vec{V} \text{grad } f + f \text{div } \vec{V}$; $\text{div}(\text{grad } v \times \text{grad } w) = \text{rot}(\text{grad } v) \cdot \text{grad } w - \text{grad } v \cdot \text{rot}(\text{grad } w) = 0$

Použijeme b) a vypočteme

$$\begin{aligned}
\Delta f &= \operatorname{div}(\operatorname{grad} f) \\
&= \operatorname{div} \left(\underbrace{\frac{1}{h_u} \partial_u f \cdot \vec{e}_u}_{F_u} + \underbrace{\frac{1}{h_v} \partial_v f \cdot \vec{e}_v}_{F_v} + \underbrace{\frac{1}{h_w} \partial_w f \cdot \vec{e}_w}_{F_w} \right) \\
&= \frac{1}{h_u h_v h_w} [\partial_u (h_v h_w F_u) + \partial_v (h_u h_w F_v) + \partial_w (h_u h_v F_w)] \\
&= \frac{1}{h_u h_v h_w} \left[\partial_u \left(h_v h_w \frac{1}{h_u} \partial_u f \right) + \partial_v \left(h_u h_w \frac{1}{h_v} \partial_v f \right) + \partial_w \left(h_u h_v \frac{1}{h_w} \partial_w f \right) \right].
\end{aligned}$$

Konečně toto použijeme pro transformaci Laplacova operátoru.
Sférické souřadnice:

$$\begin{aligned}
x &= r \sin \theta \cos \varphi, \\
y &= r \sin \theta \sin \varphi, \\
z &= r \cos \theta.
\end{aligned}$$

$$g_r = \begin{pmatrix} \sin \theta \cos \varphi \\ \sin \theta \sin \varphi \\ \cos \theta \end{pmatrix}, \quad g_\theta = \begin{pmatrix} r \cos \theta \cos \varphi \\ r \cos \theta \sin \varphi \\ -r \sin \theta \end{pmatrix}, \quad g_\varphi = \begin{pmatrix} -r \sin \theta \sin \varphi \\ r \sin \theta \cos \varphi \\ 0 \end{pmatrix}$$

und

$$h_r = \|g_r\| = 1, \quad h_\theta = \|g_\theta\| = r, \quad h_\varphi = \|g_\varphi\| = r \sin \theta.$$

$$\begin{aligned}
\Delta f &= \frac{1}{r^2 \sin \theta} \left[\partial_r \left(r^2 \sin \theta \frac{\partial f}{\partial r} \right) + \partial_\theta \left(\sin \theta \frac{\partial f}{\partial \theta} \right) + \partial_\varphi \left(\frac{1}{\sin \theta} \frac{\partial f}{\partial \varphi} \right) \right] \\
&= \frac{2}{r} \frac{\partial f}{\partial r} + \frac{\partial^2 f}{\partial r^2} + \frac{\cos \theta}{r^2 \sin \theta} \frac{\partial f}{\partial \theta} + \frac{1}{r^2} \frac{\partial^2 f}{\partial \theta^2} + \frac{1}{r^2 \sin^2 \theta} \frac{\partial^2 f}{\partial \varphi^2}.
\end{aligned}$$

Válcové souřadnice:

$$\begin{aligned}
x &= r \cos \varphi, \quad y = r \sin \varphi, \quad z = z. \\
h_r &= 1, \quad h_\varphi = r, \quad h_z = 1.
\end{aligned}$$

$$\begin{aligned}
\Delta f &= \frac{1}{r} \left[\partial_r \left(r \frac{\partial f}{\partial r} \right) + \partial_\varphi \left(\frac{1}{r} \frac{\partial f}{\partial \varphi} \right) + \partial_z \left(r \frac{\partial f}{\partial z} \right) \right] \\
&= \frac{\partial^2 f}{\partial r^2} + \frac{1}{r} \frac{\partial f}{\partial r} + \frac{1}{r^2} \frac{\partial^2 f}{\partial \varphi^2} + \frac{\partial^2 f}{\partial z^2}.
\end{aligned}$$

17 Atom vodíku

V této kapitole²⁷ projdeme řešení Schrödingerovy rovnice pro atom vodíku. Druhá mocnina absolutní hodnoty funkce $\psi = \psi(x, y, z, t)$ tedy bude odpovídat hustotě pravděpodobnosti nalezení elektronu v čase t v daném bodě, tedy pro každé $t \geq 0$ platí

$$\int_{\mathbb{R}^3} |\psi(x, y, z, t)|^2 d(x, y, z) = 1.$$

Dále z toho plyne, že ψ je určena jen na konstantu - komplexní číslo s absolutní hodnotou jedna.

Vývoj funkce $\psi(x, y, z, t)$ v čase je dán rovnicí²⁸

$$i\hbar \frac{\partial \psi}{\partial t} = \hat{\mathcal{H}}\psi,$$

kde Hamiltonián $\hat{\mathcal{H}}$ je dán

$$\hat{\mathcal{H}} = -\frac{\hbar^2}{2m}\Delta + V(r).$$

Zde je m hmotnost elektronu a $V(r)$ potenciální energie elektrostatického protonu, tedy

$$V(r) = -\frac{e^2}{r}, \quad r = \sqrt{x^2 + y^2 + z^2}.$$

Celkem tedy budeme řešit rovnici

$$i\hbar \frac{\partial \psi}{\partial t} = -\frac{\hbar^2}{2m}\Delta\psi - \frac{e^2}{r}\psi. \quad (17.1)$$

• Sféricky symetrická řešení - s -orbitaly

Budeme hledat stacionární řešení této rovnice, tedy řešení, kde $|\psi(x, y, z, t)|$ nezávisí na čase: $\psi = e^{if(t)}\psi(x, y, z)$. Díky sférické symetrii původního problému je přirozené hledat řešení, které závisí jen na poloměru, tedy $\psi = e^{if(t)}\psi(r)$. Po dosazení tohoto tvaru do (17.1) je vidět, že $f'(t)$ musí být konstanta, tedy funkce f musí být lineární: $f(t) = -Et/\hbar$. Celkem tedy hledáme řešení (17.1) ve tvaru $\psi(x, y, z, t) = e^{-(i/\hbar)Et}\psi(r)$.

Po dosazení do (17.1) vidíme, že $\psi(r)$ musí splňovat

$$-\frac{\hbar^2}{2m}\Delta\psi = \left(E + \frac{e^2}{r}\right)\psi.$$

Po převodu do sférických souřadnic

$$x = r \sin \theta \cos \phi, \quad y = r \sin \theta \sin \phi, \quad z = r \cos \theta$$

je

$$\Delta f(r, \theta, \phi) = \frac{1}{r} \frac{\partial^2}{\partial r^2}(rf) + \frac{1}{r^2} \left\{ \frac{1}{\sin \theta} \frac{\partial}{\partial \theta} \left(\sin \theta \frac{\partial f}{\partial \theta} \right) + \frac{1}{\sin^2 \theta} \frac{\partial^2 f}{\partial \phi^2} \right\}. \quad (17.2)$$

Protože ale ψ nebude záviset na θ a ϕ , vše se zjednoduší na

$$\frac{1}{r} \frac{d^2}{dr^2}(r\psi) = -\frac{2m}{\hbar^2} \left(E + \frac{e^2}{r} \right) \psi.$$

²⁷ viz. http://www.feynmanlectures.caltech.edu/III_19.html; na semináři přednášel Jan Krejčí 14. 3. 2019

²⁸ e je náboj elektronu, \hbar je Planckova konstanta.

Abychom zjednodušili konstanty, přeškálujeme problém zavedením

$$r = \frac{\hbar^2}{me^2}\varrho, \quad E = \frac{me^4}{2\hbar^2}\epsilon \quad (17.3)$$

a dostaneme

$$\frac{d^2(\varrho\psi)}{d\varrho^2} = -\left(\epsilon + \frac{2}{\varrho}\right)\varrho\psi.$$

Přeškálování znamená, že měříme energii a poloměr v přirozených “atomárních” jednotkách, tedy

$$\begin{aligned} \varrho &= r/r_B, & r_B &= \frac{\hbar^2}{me^2} && \text{Bohrův poloměr, ca. 0.528 Angstromů} \\ \epsilon &= E/E_R, & E_R &= me^4/2\hbar^2 && \text{Rydbergova energie, ca. 13.6 eV.} \end{aligned}$$

Dále označíme $f = \varrho\psi$ a řešíme rovnici

$$\frac{d^2 f}{d\varrho^2} = -\left(\epsilon + \frac{2}{\varrho}\right)f.$$

Dále předpokládáme f ve tvaru $f(\varrho) = e^{-\alpha\varrho}g(\varrho)$, kde $\alpha \in \mathbb{R}$ a $g(\varrho)$ splňuje

$$\frac{d^2 g}{d\varrho^2} - 2\alpha \frac{dg}{d\varrho} + \left(\frac{2}{\varrho} + \epsilon + \alpha^2\right)g = 0.$$

Parametr $\alpha > 0$ můžeme zvolit, a podle předchozí rovnice bude výhodné zvolit $\alpha^2 = -\epsilon$. Zde je nutné si uvědomit, že $E < 0$ - nulová energie odpovídá protonu a elektronu nekonečně vzdáleným od sebe, E je energie elektronu a protonu ve vazbě, a čím nižší E , tím stabilnější stav. Celkem dostaneme

$$\frac{d^2 g}{d\varrho^2} - 2\alpha \frac{dg}{d\varrho} + \frac{2}{\varrho}g = 0.$$

Tuto rovnici můžeme vcelku snadno vyřešit pomocí mocninných řad. Dosadíme

$$g(\varrho) = \sum_{k=1}^{\infty} a_k \varrho^k, \quad g'(\varrho) = \sum_{k=1}^{\infty} a_k k \varrho^{k-1}, \quad g''(\varrho) = \sum_{k=1}^{\infty} a_k k(k-1) \varrho^{k-2}$$

a dostaneme

$$\sum_{k=1}^{\infty} [(k+1)ka_{k+1} - 2\alpha ka_k + 2a_k] \varrho^{k-1} = 0.$$

Zvolíme tedy a_1 libovolně (vlastní funkce ψ je určena až na konstantu!) a dopočteme

$$a_{k+1} = \frac{2(\alpha k - 1)}{k(k+1)} a_k, \quad k \geq 1. \quad (17.4)$$

Ne všechna tato řešení ale mají matematický či fyzikální smysl. Výběr lze provést dvěma (navzájem ekvivalentními způsoby). Z pohledu funkcionální analýzy je nutné nejen splnit rovnici $\hat{\mathcal{H}}\psi = E\psi$, ale i $\psi \in L_2(\mathbb{R}^3)$. Z fyzikálního pohledu jsou zajímavá jen řešení s $\psi(r) \rightarrow 0$ pro $r \rightarrow \infty$: elektron má být vázán protonem.

Lehce neformálně lze postupovat takto: Při $k \rightarrow \infty$ je (17.4) aproximovatelné $a_{k+1} = \frac{2\alpha}{k} a_k$ a $a_{k+1} \sim \frac{(2\alpha)^k}{k!}$. To jsou ale koeficienty řady $e^{2\alpha\varrho}$, což ani v kombinaci s faktorem $e^{-\alpha\varrho}$ není

použitelné. Pokud ale $\alpha = 1/k > 0$, pak a_{k+1} (a i všechny následující a_l , $l \geq k + 1$) bude nulové. To už spolu s faktorem $e^{-\alpha\varrho}$ plně postačuje.

Celkem tedy máme řešení pro $\alpha = \frac{1}{n}$, $n = 1, 2, \dots$ a $-\epsilon = 1, \frac{1}{4}, \frac{1}{9}, \dots$. Tím jsme našli všechny sféricky symetrické orbitály elektronu, jejich energie je dána jako

$$E_n = -E_R \cdot \frac{1}{n^2}, \quad n = 1, 2, 3, \dots; \quad E_R = \frac{me^4}{2\hbar^2} \sim 13.6\text{eV}$$

je Rydbergova energie.

První tři vlastní funkce k $n = 1, 2, 3$ pak mají tvar

$$\begin{aligned} \psi_1(\varrho) &= e^{-\varrho}, \\ \psi_2(\varrho) &= \left(1 - \frac{\varrho}{2}\right)e^{-\varrho/2}, \\ \psi_3(\varrho) &= \left(1 - \frac{2\varrho}{3} + \frac{2}{27}\varrho^2\right)e^{-\varrho/3}. \end{aligned}$$

• Řešení závisující na θ a ϕ

Dosadíme-li $\psi(x, y, z, t) = e^{-(i/\hbar)Et}\psi(x, y, z)$ do (17.1) a uijeme obecný tvar Laplaceova operátoru ve sférických souřadnicích, dostaneme

$$\frac{1}{r} \frac{\partial^2}{\partial r^2}(r\psi) + \frac{1}{r^2} \left\{ \frac{1}{\sin\theta} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial\psi}{\partial\theta} \right) + \frac{1}{\sin^2\theta} \frac{\partial^2\psi}{\partial\phi^2} \right\} = -\frac{2m}{\hbar^2} \left(E + \frac{e^2}{r} \right) \psi.$$

Rovnici budeme řešit předpokladem separovatelnosti proměnných, tedy $\psi(x, y, z) = Y(\theta, \phi)F(r)$, čímž dostaneme

$$\frac{Y}{r} \frac{\partial^2}{\partial r^2}(rF) + \frac{F}{r^2 \sin\theta} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial Y}{\partial\theta} \right) + \frac{F}{r^2 \sin^2\theta} \frac{\partial^2 Y}{\partial\phi^2} = -\frac{2m}{\hbar^2} \left(E + \frac{e^2}{r} \right) YF.$$

Celou rovnici vynásobíme $\frac{r^2}{YF}$ a separujeme závislost na θ a ϕ od závislosti na r

$$\frac{1}{Y} \left\{ \frac{1}{\sin\theta} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial Y}{\partial\theta} \right) + \frac{1}{\sin^2\theta} \frac{\partial^2 Y}{\partial\phi^2} \right\} = -\frac{r^2}{F} \left\{ \frac{1}{r} \frac{d^2}{dr^2}(rF) + \frac{2m}{\hbar^2} \left(E + \frac{e^2}{r} \right) F \right\}.$$

Protože obě strany závisí na jiných proměnných, musí být rovny konstantě - kterou označíme $-K$ a řešíme tedy soustavu dvou rovnic

$$\frac{1}{\sin\theta} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial Y}{\partial\theta} \right) + \frac{1}{\sin^2\theta} \frac{\partial^2 Y}{\partial\phi^2} = -KY, \quad (17.5)$$

$$\frac{1}{r} \frac{d^2}{dr^2}(rF) + \frac{2m}{\hbar^2} \left(E + \frac{e^2}{r} \right) F = \frac{KF}{r^2}. \quad (17.6)$$

Rovnici (17.5) vyřešíme (opět) separací, tedy dosazením $Y(\theta, \phi) = f(\theta)g(\phi)$. Poté pronásobíme $\frac{\sin^2\theta}{f(\theta)g(\phi)}$ a dostaneme

$$\frac{\sin\theta}{f(\theta)} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial f(\theta)}{\partial\theta} \right) - K \sin^2\theta + \frac{1}{g(\phi)} \frac{\partial^2 g(\phi)}{\partial\phi^2} = 0.$$

První dva členy závisí jen na θ , poslední člen zase jen na ϕ - oba jsou tedy rovny jedné konstantě (která opět závisí na K)

$$\frac{\sin \theta}{f(\theta)} \frac{\partial}{\partial \theta} \left(\sin \theta \frac{\partial f(\theta)}{\partial \theta} \right) - K \sin^2 \theta = M \quad (17.7)$$

$$\frac{1}{g(\phi)} \frac{\partial^2 g(\phi)}{\partial \phi^2} = -M. \quad (17.8)$$

Začneme rovnicí (17.8). Protože hledáme periodická řešení na $[-\pi, \pi]$, dostaneme $M = m^2$ (kde $m \in \mathbb{Z}$) a $g_m(\theta) = e^{im\theta}$.²⁹ Tuto hodnotu dosadíme do (17.7) a dostaneme

$$\sin \theta \frac{\partial}{\partial \theta} \left(\sin \theta \frac{\partial f(\theta)}{\partial \theta} \right) - K \sin^2 \theta f(\theta) - m^2 f(\theta) = 0.$$

Toto je Sturm-Liouvillova rovnice, jejíž periodické řešení existuje pro $K = l(l+1)$ pro celočíselné l s $l \geq |m|$. Celkem tedy máme pro $-l \leq m \leq l$ funkce $Y_{l,m}(\theta, \phi)$, tzv. *spherical harmonics*.

Když toto dosadíme do (17.6), dostaneme rovnici

$$\frac{1}{r} \frac{d^2}{dr^2} (rF) = -\frac{2m}{\hbar^2} \left\{ E + \frac{e^2}{r} - \frac{l(l+1)\hbar^2}{2mr^2} \right\} F.$$

Opět přeškálujeme, cf. (17.3)

$$\frac{1}{\varrho} \frac{d^2(\varrho F)}{d\varrho^2} = -\left\{ \epsilon + \frac{2}{\varrho} - \frac{l(l+1)}{\varrho^2} \right\} F$$

Pro $\varrho F(\varrho) = e^{-\alpha\varrho} G(\varrho)$ a $\alpha^2 = -\epsilon$, konečně dostáváme

$$\frac{d^2 G}{d\varrho^2} - 2\alpha \frac{dG}{d\varrho} + G \left\{ \frac{2}{\varrho} - \frac{l(l+1)}{\varrho^2} \right\} = 0.$$

Dosadíme opět

$$G(\varrho) = \sum_{k=1}^{\infty} a_k \varrho^k, \quad \frac{d}{d\varrho} G = \sum_{k=1}^{\infty} k a_k \varrho^{k-1}, \quad \frac{d^2}{d\varrho^2} G = \sum_{k=1}^{\infty} k(k-1) a_k \varrho^{k-2}$$

a dostaneme

$$\sum_{k=1}^{\infty} [\{(k+1)k - (l+1)l\} a_{k+1} - (2\alpha k - 1) a_k] \varrho^{k-1} - \frac{l(l+1) a_1}{\varrho} = 0.$$

U ϱ^{-1} je jen jeden člen, takže musí být nulový, tedy $l(l+1) a_1 = 0$. Pro $l = 0$ bychom dostali naše předchozí řešení, musí tedy být $a_1 = 0$. Pro ostatní k pak vychází

$$[k(k+1) - l(l+1)] a_{k+1} = 2(\alpha k - 1) a_k,$$

což pro $k \neq l$ můžeme přepsat i jako

$$a_{k+1} = \frac{2(\alpha k - 1)}{k(k+1) - l(l+1)} a_k.$$

²⁹Přesněji, $g_m(\theta) = \alpha_1 \cos(m\theta) + \alpha_2 \sin(m\theta)$.

Z $a_1 = 0$ tedy plyne, že $a_k = 0$ pro $k \leq l$. Člen a_{l+1} můžeme zvolit libovolně (přesněji řečeno bude nakonec určen L_2 -normalizací) a dopočítávat a_{l+2}, a_{l+3}, \dots .

Pokud $\alpha n - 1 \neq 0$ pro všechna přirozená $n \geq l + 1$, řada bude opět nekonečná a výsledná funkce nebude ležet v $L_2(\mathbb{R}^3)$. Toho lze tedy dosáhnout jen tak, že zvolíme $n \geq l + 1$ pevné a $\alpha = 1/n$. Nakonec obdržíme $a_{n+1} = 0$ a odtud již $a_{n+2} = a_{n+3} = \dots = 0$.

Celkem tedy máme pro každé $l \geq 1$ možná řešení $F_{n,l}$ pro $n \geq l + 1$. Každé řešení má energii

$$E_n = -\frac{me^4}{2\hbar^2} \cdot \frac{1}{n^2}.$$

Příslušná vlnová funkce pak má tvar

$$\psi_{n,l,m} = aY_{l,m}(\theta, \phi)F_{n,l}(\varrho),$$

kde $Y_{l,m}$ jsou sférické harmoniky a

$$\varrho F_{n,l}(\varrho) = e^{-\alpha\varrho} \sum_{k=l+1}^n a_k \varrho^k.$$

Čísla l , n a m se nazývají kvantová čísla. Číslo $n = 1, 2, 3, \dots$ (*hlavní kvantové číslo*) určuje slupku elektronové vrstvy. *Orbitální kvantové číslo* $l = 0, 1, 2, \dots$ určuje podslupku: $l = 0$ odpovídá s -orbitalům, $l = 1$ odpovídá p -orbitalům, \dots . Konečně *magnetické kvantové číslo* $m = -l, -l+1, \dots, l-1, l$ rozlišuje mezi jednotlivými podslupkami, např. pro $l = 1$ a $m = -1, 0, 1$ dostáváme tři p -orbitaly p_x, p_y, p_z .

18 Entropy numbers

The concept of covering numbers can be traced back to the work of Kolmogorov [23, 24] and became since then an important tool used in several areas of theoretical and applied mathematics. Furthermore, Pietsch introduced in his book [30] a formal definition of an inverse function of covering numbers under the name of entropy numbers. Later on, Carl and Triebel [6, 9] investigated the relation between entropy numbers and other geometric and approximation quantities related to sets and operators, most importantly to eigenvalues of compact operators.

Due to the natural definition of covering and entropy numbers, and due to their relations to other geometric notions, these concepts found applications in many areas of pure and applied mathematics, including geometry of Banach spaces [3, 4, 7, 16, 31], information theory [20, 32, 36, 37, 38], and random processes [27, 28]. They also appeared in the theory of compressed sensing [5, 11] in the study of optimality of recovery of sparse vectors and in the study of eigenvalue problems in Banach spaces [13, 25]. One of the most important classes of operators, whose entropy numbers are well understood and often applied, are the identities between finite-dimensional vector spaces. The main aim of this note is to present a self-contained overview of this area. To state the main result in detail, we need to recall some notation.

The couple $(X, \|\cdot\|_X)$ is called a quasi-Banach space, if X is a real or complex vector space and the mapping $\|\cdot\|_X : X \rightarrow [0, \infty)$ satisfies

- (i) $\|x\|_X = 0$ if, and only if, $x = 0$,
- (ii) $\|\alpha x\|_X = |\alpha| \cdot \|x\|_X$ for all $\alpha \in \mathbb{R}$ (or in \mathbb{C}) and all $x \in X$,
- (iii) there exists a constant $C \geq 1$ such that $\|x + y\|_X \leq C(\|x\|_X + \|y\|_X)$ for all $x, y \in X$,
- (iv) X is complete with respect to $\|\cdot\|_X$.

If the constant C in (iii) can be chosen to be equal to one, X is actually a Banach space. If $\|\cdot\|_X$ satisfies the axioms above with (iii) replaced by

$$\|x + y\|_X^p \leq \|x\|_X^p + \|y\|_X^p, \quad x, y \in X$$

for some $0 < p \leq 1$, then $(X, \|\cdot\|_X)$ is called a p -Banach space and $\|\cdot\|_X$ is a p -norm. It follows that a Banach space X is also a p -Banach space for $p = 1$. It is easy to see that every p -norm is a quasi-norm with $C = 2^{1/p-1}$. On the other hand, by the Aoki-Rolewicz theorem [1, 33], every quasi-norm is equivalent to some p -norm for a suitably chosen p . We refer to [22] for a survey on quasi-Banach spaces.

If X is a vector space equipped with some (quasi-)norm or p -norm $\|\cdot\|_X$, we denote by B_X its unit ball, i.e. the set $B_X = \{x \in X : \|x\|_X \leq 1\}$. The symbol $\mathcal{L}(X, Y)$ stands for the set of all bounded linear operators from X to Y . For $0 < p \leq \infty$, we define $\ell_p^n(\mathbb{R})$ (or $\ell_p^n(\mathbb{C})$) to be the Euclidean space \mathbb{R}^n (or \mathbb{C}^n) equipped with the (quasi-)norm

$$\|x\|_p = \|(x_i)_{i=1}^n\|_p = \begin{cases} \left(\sum_{i=1}^n |x_i|^p\right)^{1/p}, & 0 < p < \infty; \\ \max_{1 \leq i \leq n} |x_i|, & p = \infty. \end{cases}$$

The unit ball of $\ell_p^n(\mathbb{R})$ will be denoted by B_p^n . It is easy to see, that $\ell_p^n(\mathbb{R})$ and $\ell_p^n(\mathbb{C})$ are Banach spaces if $p \geq 1$ and p -Banach spaces if $0 < p \leq 1$. Therefore, we will denote $\bar{p} = \min(1, p)$ and use the triangle inequality in $\ell_p^n(\mathbb{R})$ and $\ell_p^n(\mathbb{C})$ in the form

$$\|x + y\|_p^{\bar{p}} \leq \|x\|_p^{\bar{p}} + \|y\|_p^{\bar{p}}.$$

We define now the concept of entropy numbers of a bounded linear operator T between two (quasi-)Banach spaces X and Y . Essentially, we are allowed to use 2^{k-1} balls of radius r in Y to cover the image of the unit ball of X by T and $e_k(T)$ denotes the smallest r , for which this is still possible.

Definice 18.1. Let X and Y be Banach spaces, p -Banach spaces, or quasi-Banach spaces. Let $T : X \rightarrow Y$ be a bounded linear operator and let $k \geq 1$ be a positive integer. The k^{th} (dyadic) entropy number of T is defined as

$$e_k(T) := \inf \left\{ r > 0 : \exists y_1, \dots, y_{2^{k-1}} \in Y \text{ with } T(B_X) \subset \bigcup_{j=1}^{2^{k-1}} (y_j + rB_Y) \right\}. \quad (18.1)$$

The relation of the entropy numbers to the covering numbers of Kolmogorov is quite straightforward. If $K \subset Y$ and $r > 0$, then the covering number $N(K, Y, r)$ is the smallest number N such that there exist points y_1, \dots, y_N with $K \subset \bigcup_{j=1}^N (y_j + rB_Y)$. The entropy numbers $e_k(T)$ can then be equivalently defined as

$$e_n(T) = \inf \{ r > 0 : N(T(B_X), Y, r) \leq 2^{k-1} \}.$$

Although easy to define, the entropy numbers of some specific operator T are usually rather difficult to calculate, or estimate. One class of operators, where the upper and lower bounds on entropy numbers are known, are the identities between finite-dimensional vector spaces. The main aim of this note is to present a self-contained proof of the following result.

Věta 18.2. Let $0 < p, q \leq \infty$ and let $n \in \mathbb{N}$.

a) If $0 < p \leq q \leq \infty$ then for all $k \in \mathbb{N}$ it holds

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \sim \begin{cases} 1 & \text{if } 1 \leq k \leq \log_2 n, \\ \left(\frac{\log_2(1 + n/k)}{k} \right)^{\frac{1}{p} - \frac{1}{q}} & \text{if } \log_2 n \leq k \leq n, \\ 2^{-\frac{k-1}{n}} n^{\frac{1}{q} - \frac{1}{p}} & \text{if } n \leq k. \end{cases} \quad (18.2)$$

b) If $0 < q \leq p \leq \infty$ then for all $k \in \mathbb{N}$ it holds

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \sim 2^{-\frac{k-1}{n}} n^{\frac{1}{q} - \frac{1}{p}}. \quad (18.3)$$

The constants of equivalence in both (18.2) and (18.3) may depend on p and q , but are independent of k and n .

Theorem 18.2 was first proved for $1 \leq p < q \leq \infty$ by Schütt [34] with partial results given before by Höllig [21] and Pietsch [30, Section 12.2]. The case of quasi-Banach spaces (i.e. when p and/or q is smaller than one) was studied by Edmunds and Triebel in [13, Section 3.2.2], who provided the estimates from above in (18.2) including the intermediate k 's with $\log_2 n \leq k \leq n$. Finally, the corresponding lower bound was supplied by Kühn [26] and, independently, by Guédon and Litvak in [18]. Although all the estimates in Theorem 18.2 may be found in the literature since nearly two decades, there seems to be no place, were all the parts would appear together - the reader has to combine several sources, sometimes using different notations.

Interestingly enough, the proof of Theorem 18.2 requires a combination of several different techniques, which are of independent interest. The most natural are the so-called volume arguments. Quite intuitively, if we want to cover a body $K \subset \mathbb{R}^n$ by a number of other bodies $L_1, \dots, L_N \subset \mathbb{R}^n$, then their volume combined must be larger than the volume of K . Here, volume can be any positive measure on \mathbb{R}^n . As L_j 's are now different translates of a fixed dilation of one fixed body L , it is most convenient to work with a shift-invariant measure, which behaves well with respect to dilations. It is therefore most natural to work with the usual Lebesgue measure on \mathbb{R}^n and $\text{vol}(K)$ will be the usual Lebesgue volume of a measurable set $K \subset \mathbb{R}^n$. If $K = B_X$ and $L = B_Y$ are unit balls of some quasi-Banach spaces X and Y , and if the number N is fixed to be $N = 2^{k-1}$ for a positive integer k , this can be immediately translated into lower bounds of the entropy numbers $e_k(\text{id} : X \rightarrow Y)$.

With a bit of additional work, volume arguments can be also used to give upper bounds on entropy numbers. Indeed, if $r > 0$ is fixed, we take a maximal set $y_1, \dots, y_N \in B_X \subset Y$ with $\|y_i - y_j\|_Y \geq r$. Then, on one hand, the sets $y_j + c_1 r B_Y$ are disjoint and B_X is covered by the union of $y_j + c_2 r B_Y$ for suitably chosen constants $c_1, c_2 > 0$. On the other hand, the sets $y_j + c_1 r B_Y$ are included in a certain multiple of B_X , which must therefore have a larger volume than all the disjoint sets $y_j + c_1 r B_Y$ combined. This gives an upper bound on their number N , leading to an upper bound on the entropy numbers.

Although the volume arguments represent a powerful technique, which can in principle be applied to all the parameter settings in Theorem 18.2, the obtained bounds are not always optimal. Actually, it turns out that the volume arguments provide optimal bounds (up to a multiplicative constant) only when k is large or, equivalently, when r is small. For smaller k 's, direct combinatorial estimates are needed to provide both the lower and the upper bounds. Geometrically it means, that any good cover of $T(B_X)$ with a small number of sets $y_j + r B_Y$ needs to have big overlap and/or to cover also some large neighborhood of $T(B_X)$.

The structure of the paper is as follows. Section 18.1 gives basic properties of entropy numbers and Gamma function, presents the calculation of the volume of B_p^n , and provides a couple of lemmas used later. The proof of Theorem 18.2 comes in Section 18.2. Finally, Section 18.3 collects few additional remarks and topics, including the extension of Theorem 18.2 to the complex setting.

18.1 Preparations

We start by recalling few well-known basic facts about entropy numbers. Although the reader may find the proof, for instance, in [8] or [13], we include it for the sake of completeness.

Věta 18.3. *Let X, Y, Z be p -Banach spaces for some $0 < p \leq 1$. Let $S, T \in \mathcal{L}(X, Y)$ and $R \in \mathcal{L}(Y, Z)$. Then, for all $k, l \in \mathbb{N}$, it holds*

- (i) $\|T\| \geq e_1(T) \geq e_2(T) \geq \dots \geq 0$ (monotonicity);

- (ii) $e_{k+l-1}^p(S+T) \leq e_k^p(S) + e_l^p(T)$ (*subadditivity*);
 (iii) $e_{k+l-1}(R \circ T) \leq e_k(R) \cdot e_l(T)$ (*submultiplicativity*).

Důkaz. Monotonicity of entropy numbers follows directly from (18.1). Similarly, $e_1(T) \leq \|T\|$ is implied by $T(B_X) \subset \|T\| \cdot B_Y$.

For the proof of subadditivity, let k, l be positive integers and let $\varepsilon > 0$. Then there are $y_1, \dots, y_{2^{k-1}} \in Y$ and $z_1, \dots, z_{2^{l-1}} \in Y$ with

$$S(B_X) \subset \bigcup_{i=1}^{2^{k-1}} \left(y_i + (e_k(S) + \varepsilon)B_Y \right) \quad \text{and} \quad T(B_X) \subset \bigcup_{j=1}^{2^{l-1}} \left(z_j + (e_l(T) + \varepsilon)B_Y \right).$$

Then

$$\begin{aligned} (S+T)(B_X) &\subset S(B_X) + T(B_X) \\ &\subset \left[\bigcup_{i=1}^{2^{k-1}} \left(y_i + (e_k(S) + \varepsilon)B_Y \right) \right] + \left[\bigcup_{j=1}^{2^{l-1}} \left(z_j + (e_l(T) + \varepsilon)B_Y \right) \right] \\ &= \bigcup_{i,j} \left(y_i + z_j + (e_k(S) + \varepsilon)B_Y + (e_l(T) + \varepsilon)B_Y \right) \\ &\subset \bigcup_{i,j} \left(y_i + z_j + [(e_k(S) + \varepsilon)^p + (e_l(T) + \varepsilon)^p]^{1/p} B_Y \right) \end{aligned}$$

and taking the infimum over $\varepsilon > 0$ gives the result.

The proof of submultiplicativity follows in a similar way. Indeed, if k, l are positive integers and $\varepsilon > 0$, we find $y_1, \dots, y_{2^{l-1}} \in Y$ and $z_1, \dots, z_{2^{k-1}} \in Z$ with

$$T(B_X) \subset \bigcup_{i=1}^{2^{l-1}} \left(y_i + (e_l(T) + \varepsilon)B_Y \right) \quad \text{and} \quad R(B_Y) \subset \bigcup_{j=1}^{2^{k-1}} \left(z_j + (e_k(R) + \varepsilon)B_Z \right).$$

The proof then follows from

$$\begin{aligned} (R \circ T)(B_X) &= R(T(B_X)) \subset R \left(\bigcup_{i=1}^{2^{l-1}} \left(y_i + (e_l(T) + \varepsilon)B_Y \right) \right) \\ &= \bigcup_{i=1}^{2^{l-1}} \left(Ry_i + (e_l(T) + \varepsilon)R(B_Y) \right) \\ &\subset \bigcup_{i,j} \left(Ry_i + (e_l(T) + \varepsilon)z_j + (e_l(T) + \varepsilon)(e_k(R) + \varepsilon)B_Z \right). \quad \square \end{aligned}$$

We will also need few basic facts about the Gamma function, which is defined by $\Gamma(t) = \int_0^\infty x^{t-1} e^{-x} dx$ for every positive real number $t > 0$. By partial integration, we get

$$\Gamma(1+t) = t\Gamma(t) \quad \text{for every } t > 0 \quad (18.4)$$

and $\Gamma(n) = (n-1)!$ for every positive integer n . Furthermore, by standard calculus it follows that Γ is a continuous function on $(0, \infty)$.

Lemma 18.4. *Let $0 < p < \infty$. Then*

$$\Gamma(1 + x/p)^{1/x} \sim x^{1/p}, \quad x \geq 1, \quad (18.5)$$

where the constants of equivalence may depend on p .

Důkaz. The result is a corollary of Stirling's formula [35, Chapter A.2, Theorem 2.3], but we give also a simple proof for reader's convenience.

If $x = n$ is a positive integer and $p = 1$, the result follows from

$$n \log(n) - n \leq \log(n!) = \log(\Gamma(1 + n)) \leq n \log(n), \quad (18.6)$$

where the right-hand side of (18.6) comes from $n! \leq n^n$ and the left-hand side can be obtained by taking the Riemann sum of $\int_1^n \log(x) dx$ at right endpoints.

We modify this strategy also for $x \geq 1$ and $p > 0$. Let $k \in \mathbb{N}_0$ be the unique integer with

$$\frac{1}{p} + k \leq \frac{x}{p} < \frac{1}{p} + k + 1.$$

Iterative application of (18.4) leads to

$$\Gamma(1 + x/p) = \Gamma(x/p - k + 1) \prod_{j=0}^{k-1} (x/p - j) \leq C_p (x/p)^k, \quad (18.7)$$

where $C_p = \sup_{1/p+1 \leq t \leq 1/p+2} \Gamma(t)$. We conclude, that

$$\Gamma(1 + x/p)^{1/x} x^{-1/p} \leq C_p^{1/x} p^{-k/x} x^{k/x-1/p} \leq C_p^{1/x} \max(1, p^{-1/p}) x^{-1/px},$$

which is bounded (by a constant depending on p) for $x \in [1, \infty)$.

On the other hand, using the first identity in (18.7) and Riemann sums, we obtain

$$\begin{aligned} \log\left(\frac{\Gamma(1 + x/p)^{1/x}}{x^{1/p}}\right) &= \frac{1}{x} \log \Gamma(1 + x/p) - \frac{1}{p} \log(x) \\ &\geq \frac{1}{x} \log(c_p) + \frac{1}{x} \sum_{j=0}^{k-1} \log(x/p - j) - \frac{1}{p} \log(x) \\ &\geq \frac{1}{x} \log(c_p) + \frac{1}{x} \int_{x/p-k}^{x/p} \log(t) dt - \frac{1}{p} \log(x) \\ &= \frac{1}{x} \log(c_p) + \frac{1}{p} \log(1/p) - \frac{1}{p} - \frac{1}{x} f(x/p - k), \end{aligned}$$

where $c_p = \inf_{1/p+1 \leq t \leq 1/p+2} \Gamma(t) > 0$ and $f(t) = t \log(t) - t$. The last expression is bounded (by a constant depending on p) for $x \in [1, \infty)$, as $1/p \leq x/p - k < 1/p + 1$. \square

To apply the volume arguments, it is of course necessary to calculate (or at least to estimate) the volume of the unit ball B_p^n in $\ell_p^n(\mathbb{R})$. The exact value has been known (at least) since the work of Dirichlet, cf. [10]. We give a more modern proof, cf. [31].

Věta 18.5. *Let $0 < p \leq \infty$ and let $n \in \mathbb{N}$. Then it holds*

$$\text{vol}(B_p^n) = \frac{2^n \cdot \Gamma(1 + \frac{1}{p})^n}{\Gamma(1 + \frac{n}{p})}. \quad (18.8)$$

Důkaz. Let f be a smooth non-increasing positive function on $[0, \infty)$ quickly decaying to zero at infinity. Then, by Fubini's theorem and partial integration,

$$\begin{aligned} \int_{\mathbb{R}^n} f(\|x\|_p) dx &= - \int_{\mathbb{R}^n} \int_{\|x\|_p}^{\infty} f'(t) dt dx = - \int_0^{\infty} \left(\int_{x: \|x\|_p \leq t} 1 dx \right) f'(t) dt \\ &= - \int_0^{\infty} \text{vol}(tB_p^n) f'(t) dt = - \text{vol}(B_p^n) \int_0^{\infty} t^n f'(t) dt \\ &= \text{vol}(B_p^n) \cdot \int_0^{\infty} n t^{n-1} f(t) dt. \end{aligned}$$

For $f(t) = e^{-t^p}$, we get

$$\begin{aligned} \int_{\mathbb{R}^n} e^{-\|x\|_p^p} dx &= \text{vol}(B_p^n) \cdot \int_0^{\infty} n t^{n-1} e^{-t^p} dt = \text{vol}(B_p^n) \cdot \frac{n}{p} \cdot \int_0^{\infty} s^{n/p-1} e^{-s} ds \\ &= \frac{n \text{vol}(B_p^n) \Gamma(n/p)}{p} = \text{vol}(B_p^n) \Gamma(1 + n/p). \end{aligned} \quad (18.9)$$

The proof is then finished by Fubini's theorem

$$\begin{aligned} \text{vol}(B_p^n) \Gamma(1 + n/p) &= \int_{\mathbb{R}^n} e^{-\|x\|_p^p} dx = \int_{\mathbb{R}^n} e^{-|x_1|^p - \dots - |x_n|^p} dx = \left(2 \int_0^{\infty} e^{-t^p} dt \right)^n \\ &= 2^n \left(\frac{1}{p} \int_0^{\infty} s^{1/p-1} e^{-s} ds \right)^n = 2^n \left(\frac{\Gamma(1/p)}{p} \right)^n = 2^n \Gamma(1 + 1/p)^n. \end{aligned}$$

□

Theorem 18.5 combined with Lemma 18.4 gives

$$\text{vol}(B_p^n)^{1/n} = \frac{2\Gamma(1 + \frac{1}{p})}{\Gamma(1 + \frac{n}{p})^{1/n}} \sim n^{-1/p}, \quad n \geq 1, \quad (18.10)$$

where the constants of equivalence depend again on p .

Next, we collect two simple facts about the ℓ_p^n -(quasi-)norms. The easy proof is left to the reader.

Lemma 18.6. *(i) Let $0 < p, q \leq \infty$ and $n \in \mathbb{N}$. Then*

$$\|id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})\| = \max(1, n^{1/q-1/p}).$$

(ii) Let $0 < p < q < \infty$. Then $\|x\|_q \leq \|x\|_p^{p/q} \cdot \|x\|_{\infty}^{1-p/q}$.

The following lemma is the analogue of [30, Proposition 12.1.13] for quasi-Banach spaces and appeared already in [19]. Although it uses the volume arguments, no calculation of $\text{vol}(B_X)$ is necessary, because two such terms cancel each other out. The estimate obtained is optimal up to the constant $4^{1/p}$, cf. Section 18.4 for details.

Lemma 18.7. *Let $0 < p \leq 1$, $n \in \mathbb{N}$, and let X be a real n -dimensional p -Banach space. Then, for all $k \in \mathbb{N}$,*

$$e_k(id : X \rightarrow X) \leq 4^{1/p} \cdot 2^{-\frac{k-1}{n}}. \quad (18.11)$$

Důkaz. If $k - 1 \leq 2n/p$, the result is trivial as the right-hand side of (18.11) is larger than or equal to 1. We will therefore assume that $k - 1 > 2n/p$ or, equivalently, $2^{(k-1)p/n} > 4$.

Let x_1, \dots, x_N be a maximal family of elements of B_X with $\|x_i - x_j\|_X > \tau$ for $i \neq j$, where $\tau > 0$ is given by $\frac{1+\tau^p/2}{\tau^p/2} = 2^{p(k-1)/n}$. Then, by triangle inequality, the sets $x_i + 2^{-1/p}\tau B_X$ are mutually disjoint, they are all included in $(1 + \tau^p/2)^{1/p}B_X$ and B_X is covered by the union of $x_i + \tau B_X$ over $i = 1, \dots, N$. By volume comparison, we get

$$N \operatorname{vol}(2^{-1/p}\tau B_X) \leq \operatorname{vol}[(1 + \tau^p/2)^{1/p}B_X]$$

and, therefore,

$$N \leq \frac{(1 + \tau^p/2)^{n/p}}{2^{-n/p}\tau^n} = \left(\frac{1 + \tau^p/2}{\tau^p/2}\right)^{n/p} = 2^{k-1}.$$

We conclude that

$$e_k(id : X \rightarrow X) \leq \tau = \left[\frac{2}{2^{(k-1)p/n} - 1}\right]^{1/p} \leq \left[\frac{4}{2^{(k-1)p/n}}\right]^{1/p} = 4^{1/p} 2^{-\frac{k-1}{n}}. \quad \square$$

The behavior of entropy numbers with respect to interpolation of Banach spaces was studied intensively. It is rather easy to show, that they behave well if one of the endpoints is fixed and we refer to [13] for details. Surprisingly, it was shown only recently in [12], that a general interpolation formula for entropy numbers with both endpoints interpolated is out of reach. We give only a simplified version in a form, which shall be needed later on.

Lemma 18.8. *Let $0 < p \leq q < \infty$ and let k, l, n be positive integers. Then*

$$e_{k+l-1}(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \leq 2^{1/\bar{p}} e_k^{p/q}(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{R})) \cdot e_l^{1-p/q}(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R})),$$

where $\bar{p} = \min(1, p)$.

Důkaz. Let $\varepsilon > 0$ be arbitrary. We put

$$e^0 := (1 + \varepsilon)e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{R})) \quad \text{and} \quad e^1 := (1 + \varepsilon)e_l(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R})).$$

Then B_p^n can be covered by 2^{k-1} balls in $\ell_p^n(\mathbb{R})$ with radius e^0 and by 2^{l-1} balls in $\ell_\infty^n(\mathbb{R})$ with radius e^1 . We can therefore decompose

$$B_p^n = \bigcup_i A_i,$$

where this union contains at most 2^{k-1} components A_i , and each A_i lies in some ball in $\ell_p^n(\mathbb{R})$ with radius e^0 . Similarly we can write

$$B_p^n = \bigcup_j B_j,$$

with at most 2^{l-1} components B_j , each of them lying in some ball in $\ell_\infty^n(\mathbb{R})$ with radius e^1 .

Finally, we denote $C_{i,j} = A_i \cap B_j$ and choose $z_{i,j} \in C_{i,j}$ arbitrarily any time $C_{i,j}$ is non-empty. Let now $x \in C_{i,j}$. Then both x and $z_{i,j}$ are in $C_{i,j} \subset A_i$. Therefore $\|x - z_{i,j}\|_p \leq 2^{1/\bar{p}}e^0$. Using $C_{i,j} \subset B_j$, we get in the same way also $\|x - z_{i,j}\|_\infty \leq 2e^1 \leq 2^{1/\bar{p}}e^1$. Hence, by Lemma 18.6,

$$\|x - z_{i,j}\|_q \leq 2^{1/\bar{p}}(e^0)^{p/q}(e^1)^{1-p/q},$$

and balls with centers in $z_{i,j}$'s with this radius in $\ell_q^n(\mathbb{R})$ cover B_p^n . Finally, there is at most 2^{k+l-2} such points. \square

Some of the arguments used in the proof of Theorem 18.2 are of combinatorial nature. As a preparation, we present the following lemma from [26], another variant is discussed in the last section.

Lemma 18.9. *Let $m, n \in \mathbb{N}$ with $m \leq \frac{n}{4}$ and define*

$$H_m = \{x \in \{-1, 0, 1\}^n : \|x\|_1 = 2m\}.$$

Furthermore, for $x, y \in H_m$, define their Hamming distance as $h(x, y) = \#\{i : x_i \neq y_i\}$. Then there is a set $A_m \subset H_m$ with $\#A_m \geq [n/(2m)]^m$, such that any two distinct $x, y \in A_m$ satisfy $h(x, y) > m$.

Důkaz. First note, that

$$\#H_m = \binom{n}{2m} 2^{2m}. \quad (18.12)$$

Second, if $x \in H_m$ is arbitrary, then the set $\{y \in H_m : h(x, y) \leq m\}$ has cardinality at most

$$\binom{n}{m} 3^m. \quad (18.13)$$

Indeed, there is $\binom{n}{m}$ ways to choose m coordinates, where x and y may differ, and three possible values for each of the coordinates for y .

The set A_m can be constructed by the following greedy algorithm. First, choose $x^1 \in H_m$ arbitrarily. If x^1, \dots, x^l were already selected and if there is some $y \in H_m$, which has the Hamming distance from all these points at least equal to $m + 1$, put $x^{l+1} := y$. Otherwise, the algorithm stops and A_m is the collection of all x^1, \dots, x^N , which were selected so far. This ensures, that $h(x, y) \geq m + 1$ for any two distinct $x, y \in A_m$.

Finally, from (18.12) and (18.13) it follows that

$$\#A_m = N \geq \frac{\binom{n}{2m} 2^{2m}}{\binom{n}{m} 3^m} = \frac{4^m}{3^m} \cdot \frac{(n-m) \dots (n-2m+1)}{(2m) \dots (m+1)} \geq \frac{4^m}{3^m} \left(\frac{n-m}{2m}\right)^m \geq \left(\frac{n}{2m}\right)^m.$$

We have used that $t \rightarrow \frac{n-2m+t}{m+t}$ is decreasing on $(0, \infty)$ and $n \geq 4m$. \square

18.2 Proof of Theorem 18.2

This section is devoted to the proof of the main result, Theorem 18.2. For reader's convenience, we repeat its statement and then prove step-by-step all the upper and lower bounds of $e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R}))$ for all possible values of p, q, k and n .

Věta 18.2. *Let $0 < p, q \leq \infty$ and let $n \in \mathbb{N}$.*

a) *If $0 < p \leq q \leq \infty$ then for all $k \in \mathbb{N}$ it holds*

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \sim \begin{cases} 1 & \text{if } 1 \leq k \leq \log_2 n, \\ \left(\frac{\log_2(1 + n/k)}{k} \right)^{\frac{1}{p} - \frac{1}{q}} & \text{if } \log_2 n \leq k \leq n, \\ 2^{-\frac{k-1}{n}} n^{\frac{1}{q} - \frac{1}{p}} & \text{if } n \leq k. \end{cases} \quad (18.2)$$

b) *If $0 < q \leq p \leq \infty$ then for all $k \in \mathbb{N}$ it holds*

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \sim 2^{-\frac{k-1}{n}} n^{\frac{1}{q} - \frac{1}{p}}. \quad (18.3)$$

The constants of equivalence in both (18.2) and (18.3) may depend on p and q , but are independent of k and n .

Důkaz. We split the proof of the different estimates in Theorem 18.2 by the used technique. Furthermore, we denote throughout the proof $\bar{p} = \min(1, p)$ and $\bar{q} = \min(1, q)$.

Step 1: Elementary estimates

(i) If $0 < p \leq q \leq \infty$, we have by Theorem 18.3 and Lemma 18.6

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \leq \|id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})\| = 1$$

or, equivalently, we can always cover B_p^n with B_q^n . This gives the optimal upper bound for $1 \leq k \leq \log_2 n$.

(ii) On the other side, the canonical vectors e^1, \dots, e^n defined by

$$(e^i)_l = \delta_{il}, \quad i, l = 1, \dots, n,$$

satisfy $e^i \in B_p^n$ and $\|e^i - e^j\|_q = 2^{1/q}$ for $i, j \in \{1, \dots, n\}$ and $i \neq j$. Therefore, if we cover B_p^n with $2^{k-1} < n$ balls in $\ell_q^n(\mathbb{R})$ of radius $r > 0$, at least one of these balls must contain two different e^i, e^j with $i \neq j$, simply by the pigeonhole principle. We denote the center of such a ball by $z \in \mathbb{R}^n$ and obtain by triangle inequality

$$2^{\bar{q}/q} = \|e^i - e^j\|_q^{\bar{q}} \leq \|e^i - z\|_q^{\bar{q}} + \|z - e^j\|_q^{\bar{q}} \leq 2r^{\bar{q}}.$$

Therefore,

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \geq 2^{1/q - 1/\bar{q}}$$

for $1 \leq k \leq \log_2 n$. Together with (i), this finishes the proof of the equivalence in (18.2) for this range of k 's.

(iii) Lemma 18.7 together with Lemma 18.6 can be used to prove the upper bound in (18.3). Let $0 < q \leq p \leq \infty$ and let k and n be positive integers. Then

$$\begin{aligned} e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) &\leq e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{R})) \cdot \|id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})\| \\ &\leq 4^{1/p} \cdot 2^{-\frac{k-1}{n}} \cdot n^{1/q - 1/p}. \end{aligned}$$

Step 2: Volume arguments, estimates from below

If B_p^n is covered by 2^{k-1} balls in $\ell_q^n(\mathbb{R})$ of radius $r > 0$, then their volume must be larger than the volume of B_p^n . This simple observation can be turned into the estimate

$$\text{vol}(B_p^n) \leq 2^{k-1} \text{vol}(rB_q^n) = 2^{k-1} r^n \text{vol}(B_q^n)$$

and, by (18.10),

$$e_k(\text{id} : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \geq 2^{-\frac{k-1}{n}} \left(\frac{\text{vol}(B_p^n)}{\text{vol}(B_q^n)} \right)^{1/n} \sim 2^{-\frac{k-1}{n}} n^{1/q-1/p}.$$

This proves the lower bound in (18.3) for all k 's and in (18.2) for $k \geq n$. Together with Step 1, the proof of (18.3) is therefore finished.

Step 3: Volume arguments, estimates from above

Let $0 < p \leq q \leq \infty$ and let $\tau > 0$. Similarly to the proof of Lemma 18.7, we let $\{y_1, \dots, y_N\} \subset B_p^n$ be any maximal τ -distant set in the ℓ_q^n - (quasi)-norm. In detail, this means that we assume that $\|y_i - y_j\|_q > \tau$ for $i, j \in \{1, \dots, N\}$ with $i \neq j$ and that for every $y \in B_p^n$, there is $i \in \{1, \dots, N\}$ with $\|y - y_i\|_q \leq \tau$.

Then we observe a couple of simple facts

- (i) If $z \in (y_i + 2^{-1/\bar{q}}\tau B_q^n) \cap (y_j + 2^{-1/\bar{q}}\tau B_q^n)$ for $i \neq j$, then

$$\tau^{\bar{q}} < \|y_i - y_j\|_q^{\bar{q}} \leq \|y_i - z\|_q^{\bar{q}} + \|z - y_j\|_q^{\bar{q}} \leq 2(2^{-1/\bar{q}}\tau)^{\bar{q}},$$

gives a contradiction. Hence, the sets $y_j + 2^{-1/\bar{q}}\tau B_q^n, j = 1, \dots, N$, are disjoint.

- (ii) If $z \in y_j + 2^{-1/\bar{q}}\tau B_q^n$, we obtain for $\nu = \|\text{id} : \ell_q^n(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{R})\| = n^{1/p-1/q}$

$$\|z\|_p^{\bar{p}} \leq \|y_j\|_p^{\bar{p}} + \|z - y_j\|_p^{\bar{p}} \leq 1 + \nu^{\bar{p}} \|z - y_j\|_q^{\bar{p}} \leq 1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}}.$$

It follows that all the sets $y_j + 2^{-1/\bar{q}}\tau B_q^n, j = 1, \dots, N$ are included in $(1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}})^{1/\bar{p}} B_p^n$.

By volume comparison, we conclude

$$N \text{vol}(2^{-1/\bar{q}}\tau B_q^n) \leq \text{vol}[(1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}})^{1/\bar{p}} B_p^n]$$

and

$$N \leq \frac{(1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}})^{n/\bar{p}} \text{vol}(B_p^n)}{2^{-n/\bar{q}}\tau^n \text{vol}(B_q^n)} = \left[\frac{1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}}}{2^{-\bar{p}/\bar{q}}\tau^{\bar{p}}} \right]^{n/\bar{p}} V_n(p, q), \quad (18.14)$$

where we denoted $V_n(p, q) = \frac{\text{vol}(B_p^n)}{\text{vol}(B_q^n)}$. For a positive integer k , we define τ by putting the right-hand side of (18.14) equal to 2^{k-1} . We obtain

$$\left[\frac{1 + (2^{-1/\bar{q}}\tau\nu)^{\bar{p}}}{2^{-\bar{p}/\bar{q}}\tau^{\bar{p}}} \right]^{n/\bar{p}} V_n(p, q) = 2^{k-1} \quad \text{and} \quad \tau = \frac{2^{1/\bar{q}}}{[2^{(k-1)\bar{p}/n} V_n(p, q)^{-\bar{p}/n} - \nu^{\bar{p}}]^{1/\bar{p}}}.$$

Observe, that this is always possible if the denominator is positive. This is the case if

$$2^{\frac{k-1}{n}} > 2\nu V_n(p, q)^{1/n} = 2n^{1/p-1/q} \left(\frac{\text{vol}(B_p^n)}{\text{vol}(B_q^n)} \right)^{1/n}. \quad (18.15)$$

By (18.10), the right-hand side of (18.15) is equivalent to a constant, and (18.15) is satisfied if $k \geq \gamma_{p,q}n$ for some $\gamma_{p,q} > 0$ depending only on p and q .

We conclude that, for $k \geq \gamma_{p,q}n$,

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \leq \tau \leq \frac{C_{p,q}}{[2^{(k-1)\bar{p}/n} V_n(p, q)^{-\bar{p}/n}]^{1/\bar{p}}} \leq C'_{p,q} 2^{-\frac{k-1}{n}} n^{1/q-1/p},$$

where we used (18.15) in the last but one inequality with $C_{p,q} = 2^{1+1/\bar{q}}/(2^{\bar{p}} - 1)^{1/\bar{p}}$.

Step 4: Combinatorial part - estimate from below

Let $0 < p \leq q \leq \infty$. Let $m, n \in \mathbb{N}$ with $m \leq n/4$ and let A_m be the set from Lemma 18.9. Then $\tilde{A}_m := (2m)^{-1/p} A_m \subset B_p^n$ and for two distinct $x, y \in \tilde{A}_m$ it holds $\|x - y\|_q \geq 2^{-1/p} m^{1/q-1/p}$. As a consequence, two different points from \tilde{A}_m cannot be covered by an ℓ_q^n -ball, unless its radius is at least $2^{-1/p-1/\bar{q}} m^{1/q-1/p}$.

We summarize, that if for some $k \in \mathbb{N}$, there is $m \in \mathbb{N}$ with

$$m \leq n/4 \quad \text{and} \quad 2^{k-1} < \left(\frac{n}{2m}\right)^m, \quad (18.16)$$

then $e_k(id : \ell_p^n \rightarrow \ell_q^n) \geq 2^{-1/p-1/\bar{q}} m^{1/q-1/p}$.

Let us therefore fix $k, n \in \mathbb{N}$ with $n \geq 64$ and $\log_2 n \leq k \leq n/8$. Then $k \geq \log_2 n \geq \log_2(n/k + 1)$ and we may choose m to be any integer with

$$\frac{k}{\log_2(n/k + 1)} \leq m \leq \frac{2k}{\log_2(n/k + 1)}.$$

Then $m \leq 2k/\log_2(8) = 2k/3 \leq n/12$. The function $f : t \rightarrow t \log_2(n/(2t))$ is increasing on $(0, \frac{n}{2e})$ and therefore

$$\begin{aligned} m \log_2\left(\frac{n}{2m}\right) &= f(m) \geq f\left(\frac{k}{\log_2(n/k + 1)}\right) \\ &= \frac{k}{\log_2(n/k + 1)} \log_2\left(\frac{n \log_2(n/k + 1)}{2k}\right) \geq k, \end{aligned}$$

where in the last inequality we used that

$$\frac{n}{2k} \log_2(n/k + 1) \geq \frac{3n}{2k} \geq \frac{n}{k} + 1.$$

We therefore get also

$$2^k \leq \left(\frac{n}{2m}\right)^m.$$

This finishes the proof of (18.16). It follows that

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \geq 2^{-1/p-1/\bar{q}} m^{1/q-1/p} \geq c_{p,q} \left(\frac{\log_2(n/k + 1)}{k}\right)^{1/p-1/q}$$

for $n \geq 64$ and $\log_2 n \leq k \leq n/8$. Furthermore, by Step 2, we know that $e_n(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \gtrsim n^{1/q-1/p}$. This allows to use the monotonicity of entropy numbers and to obtain the lower bound in (18.2) for all $n \geq 64$ and all positive integers k . The (finitely many) remaining values of n can then also be incorporated at the cost of possibly larger constants.

Step 5: Combinatorial part - estimate from above

We first prove the result for $0 < p < q = \infty$, the general case then follows by interpolation, i.e. by Lemma 18.8. Let $1 \leq m \leq n$ be two natural numbers. Then every $x \in B_p^n$ can be approximated in the ℓ_∞^n -norm by a vector \tilde{x} with at most m non-zero components and $\|x - \tilde{x}\|_\infty \leq r^0 := m^{-1/p}$. Indeed, we can take \tilde{x} equal to x on the indices of the m largest (in the absolute value) components of x , and zero elsewhere.

Let now $l \geq \gamma_{p,\infty}m$ be an integer, where $\gamma_{p,\infty} > 0$ is the constant defined at the end of Step 3. Then we know that $e_l(\text{id} : \ell_p^m(\mathbb{R}) \rightarrow \ell_\infty^m(\mathbb{R})) \leq r^1 := C_{p,\infty}2^{-\frac{l-1}{m}}m^{-1/p}$. Therefore, for any $\varepsilon > 0$, there exist points $x_1, \dots, x_{2^{l-1}} \in \mathbb{R}^m$ with

$$B_p^m \subset \bigcup_{j=1}^{2^{l-1}} (x_j + (1 + \varepsilon)r^1 B_\infty^m).$$

we collect the points with support of the size at most m and equal to some of x_j 's on its support. In this way, we obtain at most $\binom{n}{m}2^{l-1}$ centers of ℓ_∞^n -balls of radius $r^0 + (1 + \varepsilon)r^1$, which cover B_p^n .

We conclude, that if $1 \leq m \leq n$ and $l \geq \gamma_{p,\infty}m$, then

$$2^{k-1} \geq \binom{n}{m}2^{l-1} \implies e_k(\text{id} : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R})) \leq m^{-1/p} \left(1 + C_{p,\infty}2^{-\frac{l-1}{m}}\right). \quad (18.17)$$

For $1 \leq m \leq n$, we choose any integer l with $\gamma_{p,\infty}m \leq l \leq (\gamma_{p,\infty} + 1)m$. Using the elementary estimate

$$\binom{n}{m} \leq \frac{n^m}{m!} \leq n^m \left(\frac{e}{m}\right)^m \leq \left(\frac{3n}{m}\right)^m \leq \left(\frac{n}{m} + 1\right)^{3m}$$

we obtain

$$\log_2 \left[\binom{n}{m} 2^{l-1} \right] = l - 1 + \log_2 \binom{n}{m} \leq (\gamma_{p,\infty} + 1)m - 1 + 3m \log_2 \left(\frac{n}{m} + 1\right).$$

Together with (18.17), we arrive at

$$k \geq \gamma_p m \log_2(n/m + 1) \implies e_k(\text{id} : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R})) \leq C_p m^{-1/p},$$

where $\gamma_p = \gamma_{p,\infty} + 4$ and $C_p = 1 + C_{p,\infty}$ depend only on p .

Next, we define $\alpha_p > 2$ to be a real number large enough to ensure

$$\gamma_p \alpha_p + 1 \leq 2^{\alpha_p - 2}. \quad (18.18)$$

Moreover, we assume that k and n are positive integers with $n \geq k \geq 2\alpha_p \gamma_p \log_2 n$. This allows us to choose m to be any integer with

$$\frac{k}{2\alpha_p \gamma_p \log_2(n/k + 1)} \leq m \leq \frac{k}{\alpha_p \gamma_p \log_2(n/k + 1)}. \quad (18.19)$$

From $\gamma_p > 4$ and $\alpha_p > 2$, it follows that $m \leq n$ and, by monotonicity of $f : t \rightarrow t \log_2(n/t + 1)$ on $(0, \infty)$, we get

$$\begin{aligned} \gamma_p f(m) &= \gamma_p m \log_2(n/m + 1) \leq \gamma_p f\left(\frac{k}{\gamma_p \alpha_p \log_2(n/k + 1)}\right) \\ &= \gamma_p \cdot \frac{k}{\gamma_p \alpha_p \log_2(n/k + 1)} \log_2\left(\frac{n}{k} \gamma_p \alpha_p \log_2\left(\frac{n}{k} + 1\right) + 1\right) \\ &\leq \frac{k}{\alpha_p \log_2(n/k + 1)} \left[\log_2\left(\frac{n}{k} + 1\right) + \log_2(\gamma_p \alpha_p + 1) + \log_2\left(\log_2\left(\frac{n}{k} + 1\right) + 1\right) \right] \\ &\leq \frac{2k}{\alpha_p} + \frac{k \log_2(\gamma_p \alpha_p + 1)}{\alpha_p \log_2(n/k + 1)} \leq \frac{k}{\alpha_p} \left[2 + \log_2(\gamma_p \alpha_p + 1) \right] \leq k, \end{aligned}$$

where we used (18.18) in the last step.

This finishes the proof of the upper bound in (18.2) for $q = \infty$ and $2\alpha_p \gamma_p \log_2 n \leq k \leq n$. The k 's between $\log_2 n$ and $2\alpha_p \gamma_p \log_2 n$ can be incorporated by monotonicity at the cost of larger constants.

Finally, the case $0 < p < q < \infty$ follows by interpolation. Indeed, Lemma 18.8 implies that

$$e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \leq 2^{1/\bar{p}} e_k^{1-\frac{p}{q}}(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R})),$$

and the result follows from the bound just proven for $e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_\infty^n(\mathbb{R}))$. \square

18.3 Extensions

We collect further facts about the entropy numbers of identities between finite-dimensional spaces, which seem to be very well known in the community. Several parts of Theorem 18.2 can be proved in different ways and we present some of these alternative approaches. Finally, we extend Theorem 18.2 also to the complex setting.

18.4 Alternative use of volume arguments

Without much work, one can show that Lemma 18.7 is optimal up to the constant $4^{1/\bar{p}}$. Indeed, if X is a n -dimensional real vector spaces equipped with a (quasi)-norm and B_X is covered by 2^{k-1} translations of rB_X , then

$$\text{vol}(B_X) \leq 2^{k-1} r^n \text{vol}(B_X).$$

This implies that $e_k(id : X \rightarrow X) \geq 2^{-\frac{k-1}{n}}$.

If $0 < p \leq q \leq \infty$, we can write

$$2^{-\frac{k-1}{n}} \leq e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \leq e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R})) \cdot \|id : \ell_q^n(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{R})\|.$$

By Lemma 18.6, the last norm is equal to $n^{1/p-1/q}$ and we obtain the lower bound in (18.2) for $k \geq n$.

The upper bound on $e_k(id : \ell_p^n(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{R}))$ for $0 < p < q \leq \infty$ and $\log_2 n \leq k \leq n$ was proven in Section 18.2 first for $q = \infty$ and, afterwards, for $p < q < \infty$ by interpolation. Actually, one can adapt the original proof for $q = \infty$ also to the general setting of $q \leq \infty$. Unfortunately, this comes at a price of further technical difficulties and we, together with [30], preferred to go through interpolation.

18.5 Alternative use of combinatorial arguments

Next comment considers the lower bound in (18.2) for $\log_2 n \leq k \leq n$. Lemma 18.9 constructs a large subset (namely $(2m)^{-1/p}A_m$) of B_p^n with the elements having large mutual distances in ℓ_q^n . There is, however, more ways to achieve a similar result. We present a statement, which is very well-known in coding theory, cf. [17, 29], and appeared also in [14, 15] and [2] in connection with Gelfand widths and optimality results of sparse recovery. There the reader can also find a short proof, which is very much in the spirit of the proof of Lemma 18.9.

Lemma 18.10. *Let $k \leq n$ be two positive integers. Then there are N subsets T_1, \dots, T_N of $\{1, \dots, n\}$, such that*

$$(i) \quad N \geq \left(\frac{n}{4k}\right)^{k/2},$$

$$(ii) \quad |T_i| = k \text{ for all } i = 1, \dots, N \text{ and}$$

$$(iii) \quad |T_i \cap T_j| < k/2 \text{ for all } i \neq j.$$

Similarly to Lemma 18.9, Lemma 18.10 can be used to produce a large set of points in B_p^n with large distance in ℓ_q^n . It is enough to take $x_j = k^{-1/p}\chi_{T_j}$, $j = 1, \dots, N$, where T_j 's are the sets from Lemma 18.10 and χ_{T_j} is the indicator vector of T_j .

18.6 Complex spaces

It is surprisingly easy to extend the estimates of Theorem 18.2 to the setting of complex spaces $\ell_p^n(\mathbb{C})$. The main result then reads as follows.

Věta 18.11. *Let $0 < p, q \leq \infty$ and let $n \in \mathbb{N}$.*

a) *If $0 < p \leq q \leq \infty$ then for all $k \in \mathbb{N}$ it holds*

$$e_k(id : \ell_p^n(\mathbb{C}) \rightarrow \ell_q^n(\mathbb{C})) \sim \begin{cases} 1 & \text{if } 1 \leq k \leq \log_2(2n), \\ \left(\frac{\log_2(1 + 2n/k)}{k}\right)^{\frac{1}{p} - \frac{1}{q}} & \text{if } \log_2(2n) \leq k \leq 2n, \\ 2^{-\frac{k-1}{2n}} n^{\frac{1}{q} - \frac{1}{p}} & \text{if } 2n \leq k. \end{cases} \quad (18.20)$$

b) *If $0 < q \leq p \leq \infty$ then for all $k \in \mathbb{N}$ it holds*

$$e_k(id : \ell_p^n(\mathbb{C}) \rightarrow \ell_q^n(\mathbb{C})) \sim 2^{-\frac{k-1}{2n}} n^{\frac{1}{q} - \frac{1}{p}}. \quad (18.21)$$

The constants of equivalence in both (18.20) and (18.21) may depend on p and q , but are independent of k and n .

Důkaz. We observe, that the mapping

$$\mathcal{J}(z) = \mathcal{J}(z_1, \dots, z_n) = (\mathbb{R}(z_1), \text{Im}(z_1), \dots, \mathbb{R}(z_n), \text{Im}(z_n))$$

is bounded from $\ell_p^n(\mathbb{C})$ to $\ell_p^{2n}(\mathbb{R})$ with the norm bounded by a quantity independent of n . The same is true about

$$\mathcal{J}'(x) = \mathcal{J}'(x_1, \dots, x_{2n}) = (x_1 + ix_2, \dots, x_{2n-1} + ix_{2n})$$

as a mapping from $\ell_p^{2n}(\mathbb{R})$ to $\ell_p^n(\mathbb{C})$.

Using the submultiplicativity of entropy numbers, we get

$$e_k(\text{id} : \ell_p^n(\mathbb{C}) \rightarrow \ell_q^n(\mathbb{C})) \leq \|\mathcal{J} : \ell_p^n(\mathbb{C}) \rightarrow \ell_p^{2n}(\mathbb{R})\| \\ \cdot e_k(\text{id} : \ell_p^{2n}(\mathbb{R}) \rightarrow \ell_q^{2n}(\mathbb{R})) \cdot \|\mathcal{J}' : \ell_q^{2n}(\mathbb{R}) \rightarrow \ell_q^n(\mathbb{C})\|$$

and

$$e_k(\text{id} : \ell_p^{2n}(\mathbb{R}) \rightarrow \ell_q^{2n}(\mathbb{R})) \leq \|\mathcal{J}' : \ell_p^{2n}(\mathbb{R}) \rightarrow \ell_p^n(\mathbb{C})\| \\ \cdot e_k(\text{id} : \ell_p^n(\mathbb{C}) \rightarrow \ell_q^n(\mathbb{C})) \cdot \|\mathcal{J} : \ell_q^n(\mathbb{C}) \rightarrow \ell_q^{2n}(\mathbb{R})\|.$$

This can be summarized into

$$e_k(\text{id} : \ell_p^n(\mathbb{C}) \rightarrow \ell_q^n(\mathbb{C})) \sim e_k(\text{id} : \ell_p^{2n}(\mathbb{R}) \rightarrow \ell_q^{2n}(\mathbb{R}))$$

with constants of equivalence independent on k and n . The result then follows from Theorem 18.2. \square

Reference

- [1] T. Aoki, *Locally bounded linear topological spaces*, Proc. Imp. Acad. Tokyo 18 (10) (1942), 588–594
- [2] H. Boche, R. Calderbank, G. Kutyniok, and J. Vybíral, *A survey of compressed sensing*, in: Compressed Sensing and its Applications, Birkhäuser, Boston, 2015
- [3] J. Bourgain, J. Lindenstrauss, and V. Milman, *Approximation of zonoids by zonotopes*, Acta Math. 162 (1) (1989), 73–141
- [4] J. Bourgain, A. Pajor, S.J. Szarek, and N. Tomczak-Jaegermann, *On the duality problem for entropy numbers of operators*, in: Geometric aspects of functional analysis, Springer, Berlin, Heidelberg, 1989
- [5] E.J. Candès, J. Romberg, and T. Tao, *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information*, IEEE Trans. Inform. Theory 52 (2) (2006), 489–509
- [6] B. Carl, *Entropy numbers, s -numbers, and eigenvalue problems*, J. Funct. Anal. 41 (3) (1981), 290–306
- [7] B. Carl, *Entropy numbers of diagonal operators with an application to eigenvalue problems*, J. Approx. Theory 32 (1981), 135–150
- [8] B. Carl and I. Stephani, *Entropy, compactness and the approximation of operators*, Cambridge University Press, Cambridge, 1990

- [9] B. Carl and H. Triebel, *Inequalities between eigenvalues, entropy numbers, and related quantities of compact operators in Banach spaces*, Math. Ann. 251 (2) (1980), 129–133
- [10] P.G.L. Dirichlet, *Sur une nouvelle méthode pour la détermination des intégrales multiples*, J. Math. Pures Appl. 4 (1839), 164–168
- [11] D.L. Donoho, *Compressed sensing*, IEEE Trans. Inform. Theory 52 (4) (2006), 1289–1306
- [12] D.E. Edmunds and Yu. Netrusov, *Entropy numbers and interpolation*, Math. Ann. 351 (4) (2011), 963–977
- [13] D.E. Edmunds and H. Triebel, *Function spaces, entropy numbers and differential operators*, Cambridge University Press, Cambridge, 1996
- [14] S. Foucart, A. Pajor, H. Rauhut, and T. Ullrich, *The Gelfand widths of ℓ_p -balls for $0 < p \leq 1$* , J. Compl. 26 (6) (2010), 629–640
- [15] S. Foucart and H. Rauhut, *A mathematical introduction to compressive sensing*, Birkhäuser, Boston, 2013
- [16] Y. Gordon, H. König, and C. Schütt, *Geometric and probabilistic estimates for entropy and approximation numbers of operators*, J. Approx. Theory 49 (3) (1987), 219–239
- [17] R. Graham and N. Sloane, *Lower bounds for constant weight codes*, IEEE Trans. Inform. Theor. 26 (1) (1980), 37–43
- [18] O. Guédon and A.E. Litvak, *Euclidean projections of a p -convex body*, in: Geometric aspects of functional analysis, Springer, Berlin, Heidelberg, 2000
- [19] A. Hinrichs, A. Kolleck, and J. Vybírál, *Carl’s inequality for quasi-Banach spaces*, J. Funct. Anal. 271 (8) (2016), 2293–2307
- [20] Y. Guo, P.L. Bartlett, J. Shawe-Taylor, and R.C. Williamson, *Covering numbers for support vector machines*, in: Proceedings of the twelfth annual conference on Computational learning theory (pp. 267-277), ACM (1999)
- [21] K. Höllig, *Diameters of classes of smooth functions*, in: Quantitative Approximation (pp. 163–175), Academic Press, New York, London, 1980
- [22] N. Kalton, *Quasi-Banach spaces*, in: Handbook of the geometry of Banach spaces, Vol. 2 (pp. 1099–1130), North-Holland, Amsterdam, 2003
- [23] A. Kolmogorov, *On certain asymptotic characteristics of some completely bounded metric spaces*, Dokl. Akad. Nauk. SSSR 108 (1956), 385–389
- [24] A. Kolmogorov and B. Tikhomirov, *ε -entropy and ε -capacity of sets in functional space*, Uspekhi Mat. Nauk 14 (2) (86) (1959), 3–86
- [25] H. König, *Eigenvalue distribution of compact operators*, Birkhäuser, Basel, 1986
- [26] T. Kühn, *A lower estimate for entropy numbers*, J. Approx. Theory 110 (1) (2001), 120–124

- [27] M. Ledoux and M. Talagrand, *Probability in Banach spaces: isoperimetry and processes*, Springer, Berlin, 1991
- [28] M.A. Lifshits and W. Linde, *Approximation and entropy numbers of Volterra operators with application to Brownian motion*, *Memoirs Amer. Math. Soc.* 157 (2002)
- [29] N. Noam and W. Avi, *Hardness vs randomness*, *J. Comput. Syst. Sci.* 49 (2) (1994), 149–167
- [30] A. Pietsch, *Operator ideals*, North-Holland, Amsterdam, 1980
- [31] G. Pisier, *The volume of convex bodies and Banach space geometry*, Cambridge University Press, Cambridge, 1999
- [32] G. Raskutti, M.J. Wainwright, and B. Yu, *Minimax rates of estimation for high-dimensional linear regression over ℓ_q -balls*. *IEEE Trans. Inform. Theory* 57 (10) (2011), 6976–6994
- [33] S. Rolewicz, *On a certain class of linear metric spaces*, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astrono. Phys.* 5 (1957), 471–473
- [34] C. Schütt, *Entropy numbers of diagonal operators between symmetric Banach spaces*, *J. Approx. Theory* 40 (2) (1984), 121–128
- [35] E.M. Stein and R. Shakarchi, *Complex analysis*, Princeton Lectures in Analysis II, Princeton University Press, Princeton, NJ, 2003
- [36] R. Williamson, A.J. Smola, and B. Schölkopf, *Entropy numbers, operators and support vector kernels*, in: *Computational Learning Theory*, Springer, Berlin, Heidelberg, 1999
- [37] R.C. Williamson, A.J. Smola, and B. Schölkopf, *Generalization performance of regularization networks and support vector machines via entropy numbers of compact operators*, *IEEE Trans. Inform. Theory* 47 (6) (2001), 2516–2532
- [38] D.-X. Zhou, *The covering number in learning theory*, *J. Compl.* 18 (3) (2002), 739–767

19 Carl-Triebelova nerovnost

We restrict ourselves to the Banach space setting in this section. The generalisation to the quasi-Banach spaces may be found in the book [13].

Let X be a complex Banach space and let $T \in \mathcal{K}(X, X) = \mathcal{K}(X)$. Then the *spectrum* of T is defined as

$$\sigma(T) = \{\lambda \in \mathbb{C} : (T - \lambda I) \text{ is not boundedly invertible}\}.$$

Here, I is the identity mapping $I : X \rightarrow X$ and we say, that $(T - \lambda I)$ is boundedly invertible if

- $(T - \lambda I)^{-1}$ exists, i.e. $(T - \lambda I)$ must be injective and surjective, and
- $(T - \lambda I)^{-1}$ is bounded, i.e. $(T - \lambda I)^{-1} \in (X, X)$.

If for some $\lambda \in \mathbb{C}$, there is a $0 \neq x \in X$, such that $Tx = \lambda x$, then $(T - \lambda I)$ is not injective and hence $\lambda \in \sigma(T)$. Such a λ is called *eigenvalue* and the corresponding x is called *eigenvector*. But in general, not all the elements of $\sigma(T)$ are eigenvalues, cf. Exercise 21.

We recall briefly the *Riesz-Schauder theory* of compact operators.

If $T \in \mathcal{K}(X)$, then

- $\sigma(T)$ is countable,
- for all $\varepsilon > 0$, there are only finitely many $\lambda \in \sigma(T)$ with $|\lambda| \geq \varepsilon$,
- $0 \in \sigma(T)$,
- if $\lambda \in \sigma(T) \setminus \{0\}$, then λ is an eigenvalue and
- it has *finite multiplicity*.

We discuss in a bigger detail the notion of *multiplicity* of an eigenvalue. The *geometrical multiplicity* is defined as

$$\dim \ker (T - \lambda I)$$

and denotes the dimension of the space of eigenvectors associated to λ . The so-called *algebraic multiplicity* is defined as

$$\dim \bigcup_{k=1}^{\infty} \ker (T - \lambda I)^k$$

and is always bigger than (or equal to) the geometrical multiplicity. We refer to Exercise 24b.

According to the Riesz-Schauder theory, we may assign to each $T \in \mathcal{K}(X)$ a sequence of all its eigenvalues

$$|\lambda_1(T)| \geq |\lambda_2(T)| \geq \dots \geq 0,$$

where each eigenvalue is repeated with its algebraic multiplicity. If T has only finitely many eigenvalues, fill the rest of the sequence with zeros.

Věta 19.1. *Let X be a complex Banach space and let $T \in \mathcal{K}(X)$. We re-order the eigenvalues, as described above. Then*

$$|\lambda_n(T)| \leq \left(\prod_{j=1}^n |\lambda_j(T)| \right)^{1/n} \leq \inf_{k \in \mathbb{N}} 2^{\frac{k}{2n}} e_k(T) \leq \sqrt{2} e_n(T). \quad (19.1)$$

Důkaz. We give the proof in the most significant case, when all the eigenvalues are simple. The full proof may be found for example in the book [?].

So, take $n \in \mathbb{N}$ and $|\lambda_1(T)| \geq |\lambda_2(T)| \geq \dots \geq |\lambda_n(T)| \geq 0$. Then there are linearly independent $x_1, \dots, x_n \in X$ such that $Tx_j = \lambda_j x_j, j = 1, \dots, n$. We define $M = \text{span}(x_1, \dots, x_n)$. Then $\dim M = n$ and $T(M) = M$.

Let us take $x \in M$, i.e. $x = \sum_{j=1}^n \gamma_j x_j$ with $\gamma_j \in \mathbb{C}, j = 1, \dots, n$ and $Tx = \sum_{j=1}^n \gamma_j \lambda_j x_j$.

We define an operator $J : M \rightarrow \mathbb{C}^n$, which assigns to each $x \in M$ the coefficients $\gamma_1, \dots, \gamma_n$, i.e.

$$Jx = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \quad \text{and} \quad J^{-1} : \mathbb{C}^n \rightarrow M, \quad J^{-1} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = \sum_{j=1}^n \gamma_j x_j.$$

Then $Tx = J^{-1}T_n Jx$ for every $x \in M$, where

$$T_n = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}.$$

Unfortunately, we wish to apply volume arguments and in this context, \mathbb{R}^{2n} seems to be more suitable space than \mathbb{C}^n .

Hence, we define $\mathbb{J} : M \rightarrow \mathbb{R}^{2n}$ and $\mathbb{J}^{-1} : \mathbb{R}^{2n} \rightarrow M$ by

$$\mathbb{J}x = \begin{pmatrix} \text{Re}(\gamma_1) \\ \text{Im}(\gamma_1) \\ \vdots \\ \text{Re}(\gamma_n) \\ \text{Im}(\gamma_n) \end{pmatrix} \quad \text{and} \quad \mathbb{J}^{-1} \begin{pmatrix} \alpha_1 \\ \beta_1 \\ \vdots \\ \alpha_n \\ \beta_n \end{pmatrix} = \sum_{j=1}^n (\alpha_j + i\beta_j)x_j,$$

where $\text{Re}(z)$ denotes the real part of a complex number $z \in \mathbb{C}$ and $\text{Im}(z)$ its imaginary part. Then $Tx = \mathbb{J}^{-1}\mathbb{T}_n \mathbb{J}x$ for all $x \in M$, where

$$\mathbb{T}_n = \begin{pmatrix} \text{Re}(\lambda_1) & -\text{Im}(\lambda_1) & 0 & 0 & \dots & 0 & 0 \\ \text{Im}(\lambda_1) & \text{Re}(\lambda_1) & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \text{Re}(\lambda_2) & -\text{Im}(\lambda_2) & \dots & 0 & 0 \\ 0 & 0 & \text{Im}(\lambda_2) & \text{Re}(\lambda_2) & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \text{Re}(\lambda_n) & -\text{Im}(\lambda_n) \\ 0 & 0 & 0 & 0 & \dots & \text{Im}(\lambda_n) & \text{Re}(\lambda_n) \end{pmatrix},$$

while

$$\begin{aligned} Tx &= \sum_{j=1}^n (\text{Re}(\lambda_j) + i\text{Im}(\lambda_j))(\text{Re}(\gamma_j) + i\text{Im}(\gamma_j))x_j \\ &= \sum_{j=1}^n \{ \text{Re}(\lambda_j)\text{Re}(\gamma_j) - \text{Im}(\lambda_j)\text{Im}(\gamma_j) + i(\text{Re}(\lambda_j)\text{Im}(\gamma_j) + \text{Im}(\lambda_j)\text{Re}(\gamma_j)) \} x_j. \end{aligned}$$

We define a measure μ on M by

$$\mu(K) = \text{vol} \left(\mathbb{J}(K) \right)$$

for all $K \subset M$, for which $\mathbb{J}(K) \subset \mathbb{R}^{2n}$ is Lebesgue-measurable. ³⁰

With the help of the notation introduced so far, the proof becomes simple.

For every $K \subset M$, we get

$$\mathbb{J}T(K) = \mathbb{J}\mathbb{J}^{-1}\mathbb{T}_n\mathbb{J}(K) = \mathbb{T}_n(\mathbb{J}(K)),$$

hence

$$\begin{aligned} \mu(T(K)) &= \text{vol} (\mathbb{J}T(K)) = \text{vol} (\mathbb{T}_n(\mathbb{J}(K))) \\ &= \det (\mathbb{T}_n) \cdot \text{vol} (\mathbb{J}(K)) \\ &= \begin{vmatrix} \text{Re}(\lambda_1) & -\text{Im}(\lambda_1) \\ \text{Im}(\lambda_1) & \text{Re}(\lambda_1) \end{vmatrix} \cdot \begin{vmatrix} \text{Re}(\lambda_2) & -\text{Im}(\lambda_2) \\ \text{Im}(\lambda_2) & \text{Re}(\lambda_2) \end{vmatrix} \cdots \begin{vmatrix} \text{Re}(\lambda_n) & -\text{Im}(\lambda_n) \\ \text{Im}(\lambda_n) & \text{Re}(\lambda_n) \end{vmatrix} \cdot \mu(K) \\ &= \left(\prod_{j=1}^n |\lambda_j|^2 \right) \cdot \mu(K). \end{aligned}$$

Let us mention, that this formula (with a slightly more technical proof, which uses the Jordan canonical form of T) holds also for eigenvalues with higher multiplicity.

Let $k \in \mathbb{N}$ and let

$$T(B_X) \subset \bigcup_{j=1}^{2^{k-1}} y_j + \varepsilon B_X,$$

where $\varepsilon > e_k(T)$ is arbitrary. Then

$$T(B_X \cap M) \subset \bigcup_{j=1}^{2^{k-1}} (y_j + \varepsilon B_X) \cap M.$$

If $(y_j + \varepsilon B_X) \cap M = \emptyset$, then we may leave out this j . Otherwise, we find $z_j \in M$, such that $y_j + \varepsilon B_X \subset z_j + 2\varepsilon B_X$. Then

$$T(B_X \cap M) \subset \bigcup_{j=1}^{2^{k-1}} (z_j + 2\varepsilon B_X) \cap M = \bigcup_{j=1}^{2^{k-1}} z_j + 2\varepsilon(B_X \cap M).$$

Comparing the μ -volumes, we obtain

$$\left(\prod_{j=1}^n |\lambda_j|^2 \right) \cdot \mu(B_X \cap M) = \mu(T(B_X \cap M)) \leq 2^{k-1} \mu(2\varepsilon(B_X \cap M)) = 2^{k-1} \cdot (2\varepsilon)^{2n} \cdot \mu(B_X \cap M).$$

Dividing by $\mu(B_X \cap M)$ and taking the $2n$ -root, we get

$$\sqrt[n]{\prod_{j=1}^n |\lambda_j|^2} = \sqrt[2n]{\prod_{j=1}^n |\lambda_j|^{2n}} \leq 2^{\frac{k-1}{2n}} \cdot 2\varepsilon \leq 2 \cdot 2^{\frac{k}{2n}} \cdot \varepsilon.$$

³⁰Of course, vol denotes the Lebesgue measure on \mathbb{R}^{2n} .

As we may take ε arbitrarily close to $e_k(T)$, we get

$$\sqrt[n]{\prod_{j=1}^n |\lambda_j|} \leq 2 \cdot 2^{\frac{k}{2n}} \cdot e_k(T).$$

We use the so-called *Carl's trick* to improve the constant, namely we apply the obtained result to T^r and $k' = kr$ and take $r \rightarrow \infty$. This leads to

$$\sqrt[n]{\prod_{j=1}^n |\lambda_j(T)|^r} = \sqrt[n]{\prod_{j=1}^n |\lambda_j(T^r)|} \leq 2 \cdot 2^{\frac{kr}{2n}} e_{rk}(T^r) \leq 2 \cdot 2^{\frac{kr}{2n}} e_k^r(T).$$

Taking the $1/r$ power gives

$$\sqrt[n]{\prod_{j=1}^n |\lambda_j(T)|} \leq 2^{1/r} \cdot 2^{\frac{k}{2n}} \cdot e_k(T)$$

and we let $r \rightarrow \infty$ to finish the proof. □

20 =====

21 Cauchy-Schwartz pro Riemannův integrál

Věta 21.1. *Nechť $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ a $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ jsou dvě n -tice reálných čísel a necht' $1 \leq p \leq \infty$. Položme $p' = p/(p-1)$ pokud $1 < p < \infty$, $p' = 1$ pokud $p = \infty$ a $p' = \infty$ pro $p = 1$. Pak platí*

$$\langle x, y \rangle \leq \|x\|_p \cdot \|y\|_{p'}. \quad (21.1)$$

Předchozí větu lze snadno přenést ze sumací na integrály.

Věta 21.2. *Bud' $f, g : [a, b] \rightarrow \mathbb{R}$ dvě reálné funkce na intervalu $[a, b] \subset \mathbb{R}$. Pak³¹*

$$\int_a^b f(x)g(x)dx \leq \left(\int_a^b |f(x)|^p dx \right)^{1/p} \cdot \left(\int_a^b |g(x)|^{p'} dx \right)^{1/p'}. \quad (21.2)$$

Důkaz. Necht' $\mathcal{D} \subset [a, b]$ je dělení intervalu $[a, b]$ s dělicími body $a = x_0 < x_1 < \dots < x_n = b$. Pak pro horní součty platí

$$\begin{aligned} S(fg, \mathcal{D}) &= \sum_{j=1}^n (x_j - x_{j-1}) \sup_{t \in [x_{j-1}, x_j]} f(t)g(t) \leq \sum_{j=1}^n (x_j - x_{j-1}) \sup_{t \in [x_{j-1}, x_j]} |f(t)g(t)| \\ &\leq \sum_{j=1}^n (x_j - x_{j-1}) \sup_{t \in [x_{j-1}, x_j]} |f(t)| \sup_{t \in [x_{j-1}, x_j]} |g(t)| \\ &\leq \left(\sum_{j=1}^n (x_j - x_{j-1}) \sup_{t \in [x_{j-1}, x_j]} |f(t)|^p \right)^{1/p} \cdot \left(\sum_{j=1}^n (x_j - x_{j-1}) \sup_{t \in [x_{j-1}, x_j]} |g(t)|^{p'} \right)^{1/p'} \\ &= S(|f|^p, \mathcal{D})^{1/p} \cdot S(|g|^{p'}, \mathcal{D})^{1/p'}. \end{aligned}$$

Vezmeme-li supremum přes všechna dělení \mathcal{D} intervalu $[a, b]$, je důkaz hotov. □

³¹Modifikace nutné pro $p = \infty$ nebo $p' = \infty$ přenecháváme čtenáři.

22 Bochnerova věta - jednoduchá část

We say, that a complex-valued function $\Phi : \mathbb{R}^n \rightarrow \mathbb{C}$ is *positive-definite* if the matrix $(\Phi(x_j - x_k))_{j,k=1}^N$ is positive semi-definite for every $N \in \mathbb{N}$ and every choice of points $x_1, \dots, x_N \in \mathbb{R}^n$, i.e. if

$$\sum_{j,k=1}^N c_j \overline{c_k} \Phi(x_j - x_k) \geq 0$$

for every $N \in \mathbb{N}$, every $x_1, \dots, x_N \in \mathbb{R}^n$ and every $c = (c_1, \dots, c_N) \in \mathbb{C}^N$.

Let Φ be a Fourier transform of a finite positive Borel measure ν , i.e.

$$\Phi(\xi) = \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{-i\langle x, \xi \rangle} d\nu(x), \quad \xi \in \mathbb{R}^n.$$

We observe, that each such function is positive-definite by

$$\begin{aligned} \sum_{j,k=1}^N c_j \overline{c_k} \Phi(x_j - x_k) &= \sum_{j,k=1}^N c_j \overline{c_k} \cdot \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{-i\langle x_j - x_k, \xi \rangle} d\nu(\xi) \\ &= \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} \left(\sum_{j,k=1}^N c_j \overline{c_k} e^{-i\langle x_j - x_k, \xi \rangle} \right) d\nu(\xi) \\ &= \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} \left(\sum_{j,k=1}^N c_j e^{-i\langle x_j, \xi \rangle} \overline{c_k e^{-i\langle x_k, \xi \rangle}} \right) d\nu(\xi) \\ &= \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} \left| \sum_{j=1}^N c_j e^{-i\langle x_j, \xi \rangle} \right|^2 d\nu(\xi) \geq 0. \end{aligned}$$

This gives immediately the easy part of the following theorem.

Věta 22.1. *The Fourier transform of every positive Borel measure on \mathbb{R}^n is a positive-definite function. On the other hand, if $\Phi : \mathbb{R}^n \rightarrow \mathbb{C}$ is continuous and positive-definite, then Φ is a Fourier transform of a finite positive Borel measure.*

Bochnerova věta (ovšem její těžší část) se často používá ve strojovém učení. Řada metod strojového učení je lineárních, jinak řečeno, při jejich implementaci vystačíme se skalárními součiny vstupních dat $x_1, \dots, x_N \in \mathbb{R}^d$. Nelineární zobecnění takové metody je pak možno dostat tím, že nejprve zobrazíme vstupní data nelineárně do prostoru vyšší dimenze, tedy pomocí $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^D, D \gg d$. Například

$$\Phi : (x_1, \dots, x_d) \rightarrow (x_1^2, \dots, x_d^2, \sqrt{2}x_1x_2, \dots, \sqrt{2}x_{d-1}x_d) \in \mathbb{R}^D, \quad D = d(d+1)/2.$$

Pokud je D mnohem větší než d , vede toto zobrazení k enormnímu zpomalení výpočtu skalárních součinů a celého algoritmu. V některých případech se tomuto efektu dá vyhnout pomocí obratu

zvaném *kernel trick*. Například pro Φ uvedené výše platí:

$$\langle \Phi(x), \Phi(y) \rangle = \sum_{j=1}^d x_j^2 y_j^2 + 2 \sum_{i < j} x_i x_j y_i y_j = \left(\sum_{j=1}^d x_j y_j \right)^2 = \langle x, y \rangle^2.$$

Zatímco naivní výpočet $\langle \Phi(x), \Phi(y) \rangle$ by tedy vyžadoval $O(D) = O(d^2)$ operací, pravou stranu předchozí rovnice lze vypočítat pomocí $O(d)$ kroků. Nabízí se tedy otázka, pro která $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^D$ platí $\langle \Phi(x), \Phi(y) \rangle = k(\langle x, y \rangle)$ pro vhodně zvolené $k : \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}$? Bochnerova věta umožňuje odpovědět na tuto otázku pro translačně invariantní jádra $k(x, y) = K(x - y)$.

Nechť je opravdu $\langle \Phi(x), \Phi(y) \rangle = K(x - y)$ pro všechna $x, y \in \mathbb{R}^d$. Pak je pro libovolná $x_1, \dots, x_N \in \mathbb{R}^d$ a libovolná $c_1, \dots, c_N \in \mathbb{R}$

$$0 \leq \left\langle \sum_{l=1}^N c_l \Phi(x_l), \sum_{m=1}^N c_m \Phi(x_m) \right\rangle = \sum_{l,m=1}^N c_l c_m \langle \Phi(x_l), \Phi(x_m) \rangle = \sum_{l,m=1}^N c_l c_m K(x_l - x_m).$$

Jinými slovy, matice $(K(x_l - x_m))_{l,m=1}^N$ je pozitivně semidefinitní, nebo-li K je pozitivně definitní funkce, a je tedy Fourierovou transformací nějaké nezáporné míry μ na \mathbb{R}^d . Tato podmínka je i postačující...³²

Open problem: If $f : \mathbb{R}^n \rightarrow \mathbb{C}$ is a positive and positive-definite continuous function (i.e. $f(x)$ is real, $f(x) \geq 0$ for all $x \in \mathbb{R}^n$ and $f = \mathcal{F}\mu$ for some positive finite Borel measure μ) with $f(0) = 1$, then

$$\sum_{j,k=1}^N c_j \overline{c_k} f(x_j - x_k) \geq \frac{|c_1 + \dots + c_N|^2}{N}$$

for all $x_1, \dots, x_N \in \mathbb{R}^n$ and all $c = (c_1, \dots, c_N) \in \mathbb{C}^N$.

23 =====

³²Kernel Methods in Machine Learning, Thomas Hofmann, Bernhard Schölkopf and Alexander J. Smola

24 Fourierova transformace - 0/5

1. Definice nevlastním integrálem
2. Modulace, translace
3. Jednoduché příklady ($e^{-|x|}, \dots$)
4. $e^{-x^2/2}$ - diff. rovnice?

25 Approximační a další čísla - 0/5

- Definice, interpretace...
- Jednoduché odhady
- Jeden složitější???
- Carlova nerovnost

26 Other topics:

- Grothendick?
- Komplexka???
- Mumford-Shah
- Level-set methods

27 PageRank

28 Shannon's theorem

Podle J.H. van Lint

29 Monte Carlo - 4. semestr (?) - 0/5

1. t.b.a.???

30 Numerická integrace - u Riemannova integrálu - 2.-3. semestr - 0/5

1. Jednoduchý odhad konvergence některých numerických metod