Kombinatorická a výpočetní geometrie

2. ledna 2013

Obsah

1 Úvod, pojmy

Často budeme pracovat v nějakém $\mathbb{R}^d$, což jsou d-tice reálných čísel – $(x_1, \ldots, x_d)$.

V lineární algebře se například používaly podprostory roviny (lineární) – přímky skrz počátek. V geometrii budeme mít i přímky, které neprocházejí počátkem – ***afinní podprostory***. Nějaký $(d-1)$ dimenzionální afinní podprostor $\mathbb{R}^d$ nazveme ***nadrovina***. Afinní podprostor lze definovat jako $L+x = \{l + x; l \in L\}$, kde L je nějaký podprostor.

Lineární obal množiny $X \subseteq \mathbb{R}^d$ je nejmenší podprostor R^d, který obsahuje X (což je průnik všech podprostorů, které jej obsahují). ***Afinní obal*** definujeme obdobně.

Afinní kombinace bodů $a_1, \ldots, a_n \in X$ je $\alpha_1 \cdot a_1 + \alpha_2 \cdot a_2 + \ldots + \alpha_n \cdot a_n$, $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ a $\sum_{i=1}^{n} \alpha_i = 1$. Pokud afinní prostor obsahuje počátek, pak je to podprostor. Tedy, když některé z a_i je počátek, pak je to podprostor. Jinak můžeme celou množinu posunout tak, aby jeden z nich nula byl, najít lineární obal a posunout zpět.

Body v $\mathbb{R}^d$ jsou ***afinně nezávislé***, když žádný není v afinním obalu ostatních, tedy neexistují čísla $\alpha_1, \ldots, \alpha_n$ taková, že $\exists i \in 1, \ldots, n; \alpha_i \neq 0 \wedge \alpha_1 \cdot a_1 + \ldots + \alpha_n \cdot a_n = 0 \wedge \alpha_1 + \ldots + \alpha_n = 0$.

V $\mathbb{R}^2$ je jeden bod vždy afinně nezávislý, dva jsou afinně nezávislé, pokud jsou různé. Tři pokud neleží na společné přímce. Čtyři už afinně nezávislé být nemohou.

Pokud máme v $\mathbb{R}^d$ nejvíce $d+1$ bodů, afinní nezávislost zjistíme pomocí determinantu. Když vezmeme vektory $(a_1 - a_{d+1}, \ldots, a_d - a_{d-1})$, tak jsou lineárně nezávislé právě když jsou původní afinně nezávislé. To odpovídá nenulovému determinantu. Je to opět trik s posunutím o jeden z bodů, tentokrát o a_d.

Nadrovina $\mathbb{R}^d$ se dá zapsat jako $h = \left\{x \in \mathbb{R}^d; a_1 \cdot x_1 + \ldots + a_n \cdot x_n = b\right\}$, neboli je to řešení jedné lineární rovnice. Lze psát také jako $\langle a, x \rangle = b$, kde $\langle , \rangle$ značí standardní skalární součin vektorů.

Poloprostor (uzavřený) v R^d je množina $\left\{x \in \mathbb{R}^d; \langle a, x \rangle \geq b\right\}$, $a \in \mathbb{R}^d \setminus \{0\}$, $b \in \mathbb{R}$. Nadrovina $\langle a, x \rangle = b$ tvoří jeho hranici.

2 Konvexní množiny

Konvexní množina je taková množina, která ke každým dvěma bodům obsahuje i úsečku, která je spojuje. Tedy:

$$\forall x, y \in C; \forall \lambda \in (0,1)\,; \lambda \cdot x + (1-\lambda) \cdot y \in C$$

Konvexní obal množiny $X \subseteq \mathbb{R}^d$ je nejmenší konvexní množina, která obsahuje tuto množinu, tedy průnik všech konvexních, které ji obsahují. V rovině jsou to konvexní mnohoúhelníky, v prostoru už vypadají zajímavě (jsou to konvexní mnohostěny).

Konvexní obal je také množina všech konvexních kombinací bodů z X.

Konvexní kombinace jsou všechny body x, které vypadají takto:

$$\begin{aligned} x &= t_1 \cdot a_1 + \ldots + t_n \cdot a_n \\ a_1, \ldots, a_n &\in X \\ t_1, \ldots, t_n &\in \mathbb{R} \\ \sum_{i=1}^{n} t_n &= 1 \\ t_1, \ldots, t_n &\geq 0 \end{aligned}$$

Lemma 1 *Konvexní obal $X \subseteq \mathbb{R}^d$ je rovna množině všech konvexních kombinací bodů z X.*

Tedy, že stavba zevnitř a zvenčí je stejná.

Důkaz:

$$C := conv(X) = \bigcap_{C' \text{konvexní}, X \subseteq C'} C'$$

Tedy, že každá konvexní kombinace leží v každé konvexní množině. No, kdyby v ní neležela, tak ta množina není konvexní, že....

$$\tilde{C} = \{\text{konvexní kombinace bodů z } X\}$$

Každá konvexní kombinace leží v C, tedy $\tilde{C} \subseteq C$.

$C \subseteq \tilde{C}$ – na to stačí, že $\tilde{C}$ je konvexní.

Když $n = 2$, tak to přímo odpovídá definici – úsečka.

Když $n > 2$ – lze přepočítat na úsečku, která má protějšek na vnější stěně.
TODO: Tohle je dost podezřelé a na zkoušce neprošlo, skripta, prosím.

☻

2.1 Základní výsledky o konvexních množinách $\mathbb{R}^d$

Věta 1 (Oddělovací) *Nechť $C, D \subseteq \mathbb{R}^d$ konvexní, $C \cap D = \emptyset \Rightarrow \exists$ nadrovina h oddělující C od D (neostře) – C je v jednom uzavřeném poloprostoru,*

D v druhém.

Pokud je C uzavřená a omezená, D uzavřená, pak je lze oddělit ostře.

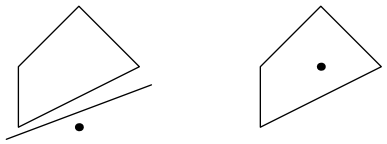
Důkaz:
Nejdříve se předpokládá, že obě jsou kompaktní. Pustím podprostor v polovině jejich vzdáleností, takže je pak opravdu oddělí.

TODO: Doplnit ze skript

☻

Lemma 2 (Farkasovo) *Máme matici s d řádky a m sloupci (nazveme ji A). Chceme najít takové x, aby* $Ax = 0$. *Toto má vždy minimálně triviální řešení. Buď má i nějaké další, nebo existuje nějaké y, že* $y^T A$ *má všechny složky záporné.*

Důkaz:
Plyne z věty o oddělování – přečteme matici A po sloupečcích, tím získáme množinu bodů, označme ji V. Mohou nastat dva případy – buď 0 je obsažéna v konvexní kombinaci, potom má netriviální řešení a nebo není. Tedy se dá oddělit nadrovinou $h = \{x : \langle y, x\rangle = b\}$. Poloprostor, kde je V bude $< b$ (kdyžtak přeznačíme znaménka u y). Potom $\langle y, 0\rangle > \langle y, x_i\rangle$.



Obrázek 1: Dva případy

☻

Věta 2 (Carathéodory) $X \subseteq \mathbb{R}^d \wedge x \in conv(X) \Rightarrow \exists Y \subseteq X \wedge |Y| \leq d + 1 \wedge x \in conv(Y)$.

Důkaz:
Nechť je a konvexní kombinace alespoň $d + 2$ bodů. Potom máme soustavu:

$$\begin{aligned} X \cdot \vec{t} &= a \\ \vec{t} \cdot \vec{1} &= 1 \end{aligned}$$

$\vec{t}$ jsou t_i z konvexní kombinace, X je množina $d+2$ bodů zapsaná za sebou jako sloupečky, $\vec{1}$ jsou samé jedničky.

Tato soustava má $d+1$ řádků, a alespoň $d+2$ sloupečků, máme slíbené nezáporné řešení, tedy nějaké má.

Pokud je už něco nulové, tak to jde jednoduše vyhodit.

Pokud ne, vybereme nějakou závislou proměnnou a začneme ji posouvat k nule. Co se stane první?

- Doleze až k nule. Můžeme ji vyhodit, ostatní jsou stále nezáporné.
- Něco jiného doleze k nule (v tu chvíli stop, aby nepřelezlo). No, vyhodíme to.

Něco k nule dolézt musí.

☻

Lemma 3 (Radonovo) *$A \subseteq \mathbb{R}^d, |A| = d+2$. Potom existují disjunktní množiny $A_1, A_2 \subseteq A$ takové, že $conv(A_1) \cap conv(A_2) \neq \emptyset$.*

*Bod $x \in conv(A_1) \cap conv(A_2)$ se nazývá **Radonův bod** a množiny A_1, A_2 **Radonův rozklad**.*

Důkaz:
Nechť $A = \{a_1, a_2, \ldots, a_{d+2}\}$. Ty jsou affinně závislé. Takže existují koeficienty $\alpha_1, \alpha_2, \ldots, \alpha_{d+2}$, ne všechny 0, $\sum \alpha_i = 0$, $\sum \alpha_i \cdot a_i = 0$. Potom vezmeme $A_1 := \{a_i; \alpha_i > 0\}, A_2 := \{a_i; \alpha_i < 0\}$. Vyrobíme x, který bude ležet v konvexním obalu obou. Nechť $S := \sum_{\alpha_i > 0} \alpha_i = -\sum_{\alpha_i < 0} \alpha_i$. Vezměme $x := \frac{1}{S} \sum_{\alpha_i > 0} \alpha_i \cdot a_i = -\frac{1}{S} \sum_{\alpha_i < 0} \alpha_i \cdot a_i$. To jsou ale konvexní kombinace bodů.

☻

Věta 3 (Hellyho) *Nechť $C_1, C_2, \ldots, C_n$ jsou konvexní množiny v $\mathbb{R}^d$ a $n \geq d+1$. Předpokládejme, že každých $d+1$ z těchto množin má neprázdný průnik. Potom všechny C_i mají neprázdný průnik.*

Důkaz:
Indukcí z Lemmatu 3. Klíčový je krok pro $n \geq d+2$.

Předpokaládáme, že $C_1, \ldots, Cn$ jako ve větě. Když libovolnou z nich vynecháme, tak existuje bod, který mají společný. Označme jej a_i (při vynechání C_i). Uvažme $a_1, \ldots, a_{d+2}$. Aplikujeme Radonovo lemma a dostaneme nějaké x. Nyní dokážeme, že takové x leží ve všech.

Radon nám rozdělil (viz důkaz) původní body na dvě disjunktní množiny (neprázdné) – A_1, A_2. Doplňky k těmto mají tedy méně množin, pro ně věta platí. Navíc, x je konvexní kombinací vybraných bodů, musí tedy být i v těch průnicích.

TODO: Raději zkontrolovat podle skript

☻

Věta 4 (Hellyho nekonečná) *Pokud je $\mathcal{C}$ systém kompaktních konvexních množin, a dále stejné jako věta 3.*

Důkaz:
Za daných předpokladů dle věty 3 má každý konečný podsystém $\mathcal{C}$ neprázdný průnik. Základní vlastnost kompaktních množin je, že $\forall \mathcal{F}$ systém kompaktních množin platí, že pokud má $\forall$ konečný podsystém neprázdný průnik, pak i celé $\mathcal{F}$ má neprázdný průnik.

☻

Nechť X je n-bodová množina v $\mathbb{R}^d$. Potom $x \in \mathbb{R}^d$ se nazývá ***centrem*** X, pokud každý uzavřený poloprostor obsahující x obsahuje alespoň $\frac{n}{d+1}$.

Medián je hodnota taková, že polopřímka „nalevo“ obsahuje alespoň půlku bodů a „napravo“ také.

Věta 5 *Každá konečná $X \subseteq \mathbb{R}^d$ má alespoň jedno centrum.*

Důkaz:
x je centrum $X \Leftrightarrow \forall H$ otevřený poloprostor takový, že $x \in H$ platí $|H \cap X| > \frac{n}{d+1}$. Místo H budeme brát konvexní C_H, která bude konvexní obal všech bodů z průniku X a H.

Každých nejvýše $d+1$ množin C_H má neprázdný průnik. Vynechá málo bodů na to, aby to vyšlo.

TODO: Tohle je hodně podezřelé. Nemám dokonce i protipříklad? Jak se použije toho, že je to $\mathbb{R}^d$? Skripta.

☻

Věta 6 (O sandwichi) *Pro d-dimenzionální sandwich složený z d ingrediencí, potom existuje přímý řez, který všechny ingredience rozpůlí. Půlení znamená, že žádný otevřený poloprostor neobsahuje více než polovinu bodů.*

3 Mřížky a Minkovského věta

Uvažujeme standardní čísla, tedy $\mathbb{Z}^d$ – tedy, mřížové body.

Věta 7 (Minkovského) *$C \subseteq \mathbb{R}^d$ konvexní, omezená a symetrická podle počátku. Její objem $vol\,(C) > 2^d$. Potom C obsahuje alespoň jeden mřížový bod různý od počátku.*

Důkaz:
Uvážíme množinu C', což je $\{0.5 \cdot c; c \in C\}$.

Tvrzení 1 *Existuje nenulový celočíselný vektor v takový, že $C' \cap (C' + v) \neq \emptyset$.*

Důkaz:
Sporem. Nechť se žádné dvě neprotínají. Vezmeme R dostatečně velké přirozené číslo a vezmeme $\mathcal{C} = \left\{c' + v; v \in \{-R, -R+1, \ldots R\}^d\right\}$. Žádné z těchto se neprotínají (protože se neprotíná C' s žádnou $C'' \in \mathcal{C}$). Ke krychli přidáme nějaký okraj, aby se tam všechny tyto vešly, tedy jsou uzavřené v $\langle -R - D, R + D\rangle^d$, kde D je poloměr C'. Potom součet objemů těchto musí být menší než objem krychle. Ale to vyjde příliš málo vzhledem k objemu C.

Objem okraje roste s R^{d-1} (má konstantní tloušťku), objem vnitřku s R^d, to, co chybělo, musí někdy dorůst, pokud $vol(C') > 1$. Ale pokud se neprotínají, tak se to tam nemá kam vejít.

☻

Máme v jako v tvrzení 1. Tedy existuje $\exists x \in C'; x \in C' + v$, ze symetrie dostaneme, že jak $x - v$, tak $v - x \in C'$. Tedy, $2x \in C, 2(v - x) \in C$. Proto (z konvexity) $x + (v - x) \in C$, tedy $v \in C$ a v je mřížový bod.

☻

Příklad 1:

Les (kruhový) o poloměru $26m$, ve všech mřížových bodech kromě počátku stromy o průměru $16cm$, my stojíme v počátku. Je třeba dokázat, že nikde není vidět ven. Tedy, vezme se to sporem, tedy že pás o šířce $16cm$ je prázdný až ven – nemůže, moc velký objem.

☺

Příklad 2:

$\alpha \in \mathbb{R}$, chceme aproximovat číslem $z \in \mathbb{Z}$. Jak dobře to jde? Jde to libovolně. Když si zvolíme nějakou přesnost jako 10^k, tak zvolíme čitatel a je hotovo.

Nechť $\alpha \in (0,1)$, N přirozené číslo, potom $\exists$ dvojice m, n celých čísel, $1 \leq n \leq N$, potom $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n \cdot N}$.

☺

Důsledek 1 *Existuje nekonečně mnoho dvojic (m,n) tak že $\left|\alpha - \frac{m}{n}\right| \leq \frac{1}{n^2}$.*

4 Incidence bodů a přímek

Máme P množinu m bodů v rovině a L množina n přímek v rovině. Chceme $I(P,L) := |\{(p,l)\,; p \in P, l \in L, p \in l\}|$. Chceme vědět, jaká největší množina to může být.

- $I(1,n) = n$
- $I(m,1) = m$

Věta 8 (Szemerédi-Trotter) $\forall m, n \geq 1 : I(m,n) = O\left(m^{\frac{2}{3}} \cdot n^{\frac{2}{3}} + m + n\right)$ *a tento odhad je nejlepší možný až na hodnotu konstanty (a ta konstanta je „rozumná“).*

5 Problém jednotkových vzdáleností

Chceme nakreslit několik bodů do roviny tak, aby tam bylo co nejvíc jednotkových vzdáleností. Toto se zatím neví, ale ví se, že $U(n) = O(n^{\frac{4}{3}})$, na druhé straně $U(n) \geq n^{1+\frac{c}{\log\log n}}$. Máme graf G a definujeme průsečíkové číslo $Cr(G)$ jako minimální počet křížení hran v nakreslení grafu G. Pokud se kříží více než dvě hrany, potom to počítáme, jako kdyby se neprotínaly v jednom bodě. Je to NP těžký problém.

Můžeme požadovat třeba nakreslení jen úsečkami.

Věta 9 (O průsečíkovém čísle) *Nechť je G graf, který má n vrcholů a m hran, hrany nejsou násobné. Potom $Cr(G) \geq \frac{1}{64} \cdot \frac{m^3}{n^2} - n$.*

Důkaz:

Lemma 4 *G graf, $Cr(G) \geq m - 3 \cdot n$.*

Důkaz:
Plyne z eulerovy formule ($n + f \geq m + 2$) – je třeba hrany štípnout.

☻

Uvažme libovolné nakreslení grafu G, má x křížení. Budeme předpokládat, že $m \geq 4n$ (jinak ta věta stejně nic neříká). Vybereme nějaké $p \in (0, 1)$ a vybereme náhodnou podmnožinu $V' \subseteq V$, každý vrchol s pravděpodobností p vezmeme, nezávisle na ostatních.

Velikost V' označíme jako n'. Tím také vybereme i nějaké hrany (hrany, které nemají oba vrcholy, umřou), takže máme nějaké E' a m'. Máme ho také nakreslený, má nějaký počet průsečíků (x'). Dle lemmatu 4 $x' \geq m' - 3n'$.

Podíváme se na střední hodnoty, takže $Ex' \geq Em' - 3En'$. $En' = p \cdot n$, $Em' = p^2 \cdot m$. Počet křížení je $Ex' = p^4 x$ (musím vybrat obě hrany). Poté je jasné, že $xp^4 \geq mp^2 - 3np$.

Potom vybereme p tak, abychom maximalizovali pravou stranu. Můžeme vzít $p = \frac{4n}{m}$. A po zjednodušení to vyjde.

☻

Nyní můžeme dokázat větu 8.

Důkaz:
Definujeme nakreslení grafu tak, že z každé úsečky odebereme přímky „do nekonečna“ a necháme to jen mezi body.

TODO: Trochu vágní

☻

6 Konvexní mnohostěny

Máme systém množin $F \subseteq 2^X$, lze jim přiřadit charakteristické vektory. Potom vezmeme konvexní obal těchto charakteristických vektorů. Patří do polyedrální kombinatoriky.

6.1 Geometrická dualita

Mějme konvexní mnohostěn. Dále vezmeme množinu všech přímek, které protínají tento mnohostěn. Můžeme definovat dualitu D_0 – když máme bod

$a \in \mathbb{R}^d \setminus \{0\}$, tak mu přiřadíme nadrovinu $D_0(a) = \left\{x \in \mathbb{R}^d; \langle a, x\rangle = 1\right\}$. Když mám nadrovinu $h \subseteq \mathbb{R}^d$, která neprochází počátkem, tak přiřadíme bod $D_0(h) = a$ takové, že pro a platí výše zmíněná rovnice. Toto je jednoznačné přiřazení.

Například když máme v rovině bod a, tak její přímka bude kolmá na spojnici a s počátkem ve vzdálenosti $\frac{1}{|a|}$.

Potom ta množina přímek může být reprezentovaná množinou bodů, vznikne něco jako doplněk k mnohoúhelníku (vnějšek). *TODO: Tohle platí?*

Věta 10 (Vlastnosti duality D_0) *Platí následující věci:*

- $p \in \mathbb{R}^d \setminus \{0\}$, *$h$ nadrovina neprocházející počátkem. Potom* $p \in h \Rightarrow D_0(h) \in D_0(p)$.
- *p, h jako v předchozím.* $h^- = \left\{x \in \mathbb{R}^d : \langle a, x\rangle \leq 1\right\}$, *tedy poloprostor obsahující počátek. Potom* $p \in h' \Leftrightarrow D_0(h) \in D_0(p)^-$.

Důkaz:
Oboje je jen dosazení. *TODO: Dosadit*

☻

Mějme $X \subseteq \mathbb{R}^d$, potom $X^* := \left\{y \in \mathbb{R}^d; \forall x \in X; \langle x, y\rangle \leq 1\right\}$ je ***duální množina*** (nebo také polární množina). Tedy je to průnik poloprostorů, pro každý bod jeden poloprostor, tedy je konvexní, obsahuje počátek a je uzavřená.

Pokud X je konvexní, uzavřená a obsahuje počátek, potom $(X^*)^* = X$.

Pokud budeme mnohostěn reprezentovat rovinným grafem, pak duál k tomu grafu odpovídá duálu mnohostěnu jako množiny.

TODO: Nějaký obrázek? Proč to platí?

Poznámka 1 (Jiná dualita) *Máme nadrovinu h, která není svislá, pak ji lze jednoznačně napsat jako* $h = \left\{x \in \mathbb{R}^d; x_d = \left(\sum_{i=1}^{d-1} a_i \cdot x_i\right) - a_d\right\}$.

Toto dává vztah mezi body a nadrovinami.

TODO: Je to opravdu jiná dualita, nebo stejná jinak napsaná?

V-mnohostěn je definován jako konvexní obal konečné množiny $\mathbb{R}^d$.

H-polyedr je průnik konečně mnoha uzavřených poloprostorů v R^d.

H-mnohostěn je H-polyedr, který je ještě k tomu omezený.

Věta 11 *H-mnohostěny definují stejnou třídu objektů, jako V-mnohostěny.*

Důkaz:
Indukcí dle d. Pro $d = 1$ triviální, nechť je d větší. Máme neprázdný omezený průnik. Máme i hranici. Každé F z hranice je H-mnohostěn dimenze $\leq d-1$. Pro ně to platí a můžeme zkombinovat body.

Zpět pomocí duality.

TODO: Natáhnout ze skript

☻

Lineární programování využívá toho, že toto je stejné.

Když se řekne Konvexní mnohostěn, tak se myslí libovolný z těchto popisů. U neomezeného se používá polyedr.

Dimenze mnohostěnu je dimenze jeho afinního obalu.

Příklady: Platonská tělesa (krychle).

Někdy se za n-dimenzionální krychli považuje $\langle -1, 1\rangle^n$.

Křížové mnohostěny – vezmu několik os, na nich vezmu úsečky a obalím (tedy, $conv\,\{e_1, -e_1, e_2, \ldots, e_d, -e_d\}$).

6.2 Simplexy

Simplex lze definovat jako lineární obal afinně nezávislé množiny bodů. ***Stěna*** mnohostěnu P je buď P samotný, nebo $P \cap h$, kde h je nadrovina taková, že celý P leží v jednom poloprostoru ohraničeném h.

Stěna dimenze j je ***j-stěna***.

Pozorování 1 *Stěna P je mnohostěn.*

Pozorování 2 *Když je P omezené, potom P je konvexní obal svých vrcholů.*

Tvrzení 2 *Relace inkluze na množině stěn P je svaz.*

Tvrzení 3 *Svaz P^* je převrácený svaz P.*

Graf mnohostěnu P je graf určený stěnami dimenze $0, 1$.

Věta 12 (Steinitz) *Graf je grafem mnohostěnu právě když je rovinný a vrcholově* 3*-souvislý.*

TODO: Důkaz?

Stěna dimenze 0 je vrchol, 1 je hrana, 2 je mnohoúhelník, $d-1$ faseta.

Mnohostěn P je ***simpliciální***, pokud každá jeho vlastní stěna je simplex.

Pozorování 3 *Pokud vrcholy P jsou v obecné poloze, potom P je simpliciální.*

P je ***jednoduchý***, pokud každá j-stěna je obsažena v právě $d - j$ fasetách (pro $j = 0, \ldots, d - 2$).

Poznámka 2 *Krychle je jednoduchá.*

Poznámka 3 *V jednoduchém mnohostěnu v okolí vrcholu vypadá kombinatoricky jako okolí d-dimenzionální krychle nebo simplexu (tedy, vždy má d sousedů).*

Tvrzení 4 *P je jednoduchý $\Leftrightarrow$ P^* je simpliciální.*

TODO: Důkaz?

6.3 Maximální počet stěn mnohostěnu

Věta 13 (Upper bound theorem) *Maximální počet stěn v d-dimenzionálním mnohostěnu s n vrcholy je $\Theta(n^{\lfloor \frac{d}{2} \rfloor})$.*

Poznámka 4 *Maximum je známo přesně.*

Dolní odhad je pomocí cyklických mnohostěnů.

Máme momentovou křivku v $\mathbb{R}^d$, tedy $\left\{t, t^2, \ldots, t^d\right\}$ $t \in \mathbb{R}$. Tedy, v rovině je to parabola.

Lemma 5 *Každá nadrovina protíná momentovou křivku v nejvýše d bodech.*

Důkaz:
Dosazením nadroviny do křivky, vyjde polynom.

☻

Důsledek 2 *Každých d bodů na momentové křivce je afinně nezávislých.*

Cyklický mnohostěn je konvexní obal libovolné konečné množiny bodů momentové křivky.

Lemma 6 (Gale) *d vrcholů cyklického mnohostěnu tvoří stěnu právě když jsou na momentové křivce rozdělené na dvojice (lichý nebo sudý počáteční úsek, potom souvislé sudě dlouhé úseky, zase libovolný uzavírací úsek).*

TODO: Tohle by fakt chtělo obrázek či něco, co je tím myšlené?

Důsledek 3 *Cyklický mnohostě má* $\Omega(n^{\lfloor \frac{d}{2} \rfloor})$ *faset.*

Důkaz:
Každá faceta leží na nějaké nadrovině, nevyšly by nadroviny.

☻

Důkaz:
Vybereme taková čísla, že tvoří dvojice, to máme dostatek možností.

$$\begin{pmatrix} n - \frac{d}{2} \\ \frac{d}{2} \end{pmatrix}$$

☻

Toto nám dalo dolní odhad, chtěli bychom i horní odhad.

Tvrzení 5 *Simpliciální mnohostěn* P *má nejvýše* $O(f_{\lfloor \frac{d}{2} \rfloor} - 1)$ *stěn, kde* f_i *je počet* i*-stěn.*

Tvrzení 6 *Maximum nabývá pro některý simpliciální mnohostěn.*

Důkaz:
Náznak: když máme něco, co není simpliciální mnohostěn, tak uděláme perturbaci vrcholů (malinko jimi hneme) a každá stěna se rozpadne na simplexy.

☻

Důkaz:
V simpliciálním mnohostěnu máme nejvýše $\begin{pmatrix} n \\ \lfloor \frac{d}{2} \rfloor \end{pmatrix}$ $(\lfloor \frac{d}{2} \rfloor - 1)$-stěn (každá stěna je simplex, potřebuji vybrat tolik vrcholů).

Poté posčítáme počet stěn – sečteme.

☻

Dualita: Simpliciální mnohostěn lze převést na jednoduchý mnohostěn. Máme zafixovanou dimenzi, počet všech stěn je tedy také omezen $O\left(f_{\lfloor \frac{d}{2} \rfloor}\right)$. Zvolme směr takový, že žádné 2 vrcholy neleží na stejné úrovni. Každý z těchto vrcholů vypadá lokálně jako na d-dimenzionální krychli, má tedy d hran.

Každý vrchol je nejvyšší nebo nejnižší nejvýše v $\lceil \frac{d}{2} \rceil$ stěnách.

TODO: Jakých stěnách? Libovolných?

6.4 Voroného diagramy

Je to množina regionů, které mají vždy k nějakému bodu nejblíž. Tedy, $reg(p \in P) := \{x \in \mathbb{R}^d; \forall q \in P; |x-p| \leq |x-q|\}$.

Pozorování 4 *Lze zapsat jako průnik poloprostorů, tedy je to mnohostěn.*

Jednotkový paraboloid je $U := \{x \in \mathbb{R}^{d+1}; x_{d+1} = x_1^2 + x_2^2 + \ldots + x_d^2\}$.

Přímku, která prochází bodem p v $\mathbb{R}^d$ (podstavci) a je k němu kolmá, nazveme $e(p)$ a bod, kde protíná U $\pi(p)$.

Tečnou nadrovinu nazveme l_x, pokud protíná podstavec v x.

Tvrzení 7 $p, x \in \mathbb{R}^d \Rightarrow |l_x \cap e(p), l_x \cap U| = |x,p|^2$

Tedy, čím dál je bod v podstavci od roviny, tím výš nadruhou protíná parabolu. `TODO: Vždyť je to parabola, ne? Tak co tvrzení? Něco jsem nepostřehnul? Obrázek?`

Důsledek 4 *Voroného diagram vznikne kolmou projekcí nějakého mnohostěnu P, který je průsečíkem poloprostorů $e(p)$.*

6.5 Arrangmenty nadrovin

Máme $H_1, \ldots, H_n$ nadroviny. Ty se budou protínat.

Stěna v $\mathbb{R}^d$ je uzávěr maximální souvislé části $\bigcap_{i \in I} H_i \setminus \bigcup_{i \notin I} H_i$.

Buňka je stěna dimenze d.

Tvrzení 8 *Máme $\mathcal{H} = \{H_1, \ldots, H_n\}$ v obecné poloze v $\mathbb{R}^d$, potom počet buněk je $\sum_{i=0}^{d} \binom{n}{i}$.*

Důkaz:
Důkaz indukcí podle d i n, rozdělí se některé buňky na dvě – ty protnuté.

Když přidám n-tou nadrovinu, rozdělím na dvě tolik, kolik na nadrovině zbylých $n-1$ nadrovin nakreslí buněk.

`TODO: Skoro by to chtělo obrázek?`

6.6 Hladiny

$\mathcal{H}$ je konečná hladina nadrovin v $\mathbb{R}^d$, mějme bod o (nazveme jej počátek), který není součástí žádné nadrovinu.

Úroveň bodu x z $x \in \mathbb{R}^d$ je počet nadrovin mezi o a x (protínající otevřenou úsečku mezi o a x). Úroveň stěny jako úroveň libovolného bodu vnitřku té stěny.

Hladina k je množina všech stěn úrovně k.

Věta 14 *Počet stěn hladin $\leq k$ je $O\left(n^{\lfloor \frac{d}{2} \rfloor}(k+1)^{\lceil \frac{d}{2} \rceil}\right)$, konstanta nezávisí na d.*

Důkaz:
Pro $k = 0$ jsou to mnohostěny, na ně máme upper bounds theorem. Vyšší: budeme předpokládat, že máme obecnou polohu. Počítá se pravděpodobnostně.

TODO: Jak?

☻

Věta 15 (O zóně) *Máme nějaké přímky. Vybereme si nějakou přímku g a vezmeme všechny body, které vidí tuto přímku g. Toto nazveme **zóna**.*

Budeme předpokládat, že $g \notin \mathcal{H}$ a i g je v obecné poloze.

Maximální počet stěn zóny nadroviny v arrangmentu nadrovin v $\mathbb{R}^d$ je $O(n^{d-1})$ pro pevné d (konstanta závisí na d).

TODO: Neplyne to přímočaře z upper bounds theorem? Nebo z toho, kolik buněk má g?

Důkaz:
Indukcí podle d, případ $d = 2$ vezmeme jako základ. Počet buněk v zóně je řádově $O(n^{d-1})$. To odpovídá buňkám uvnitř g, které nařežeme těmi zbylými nadrovinami (pokaždé, co krosneme přímku, máme buňku).

Libovolných n vrcholů v arrangmentů přímek v R^2 může mít celkem až $n^{\frac{4}{3}}$, takže počet buněk nám nestačí.

U roviny stačí pracovat s hranami (dvoudimenzionální buňky už jsme vyřešili, vrcholů je řádově stejně jako hran). Budeme počítat jen ty nad (potom můžeme násobit dvěma). Jsou dvou typů – buď ukotvené v g (stojej jedním bodem na ní), nebo létající. Ukotvených bude stejně jako úseček na g, tedy lineárně. Létajícím přiřadíme přímky, na kterých žijí. Podíváme se na ten bližší vrchol na této úsečce (ten je definovaný dvěma přímkami, ta

„nová“ bude ležet na l). Bude to pravá, když bude doprava od ní (tedy, jak jsou uspořádané paty těch přímek). Naopak bude levá. Nyní je třeba dokázat, že každá přímka l má nejvýše jednu pravou a jednu levou hranu. Předpokládejme tedy, že má dvě pravé hrany. Vezmeme tu, která nemá bod na této přímce nejblíž k g. Potom ji tato přímka nevidí. l zastíní vše nalevo od sebe. Ale ta „bližší“ přímka zakrývá vše od paty až doprava. U levé obdobně.

Možná se počítá jen to, co není úplně přímo nalepené?

Dále tedy indukční krok: Předpokládáme, že počet stěn v zóně $d-1$ je nejvýše $O(n^{d-2})$. Indukce podle n, bohužel, nefunguje. Chceme dokázat, že v průměrném případě se to nezhorší příliš. Napřed odvodíme, že maximální počet facet v zóně je $O(n^{d-1})$. Označme $f(n)$ jako maximální možný počet facet pro n nadrovin. Uvažme nějaké $\mathcal{H}, g$, kde se $f(n)$ nabývá. Vezmeme náhodný pokus – obarvíme náhodně zvolenou $h \in H$ červeně, ostatní modře. Každá faceta má tedy barvu. Zkoumáme počet modrých facet v zóně. Každá má pravděpodobnost, že bude modrá, $\frac{n-1}{n}$. Tedy modrých bude $\frac{n-1}{n} \cdot f(n)$. Když se podíváme na jen modré nadroviny, tak máme $f(n-1)$. Kolik jich přibude, když přidáme tu červenou (ale počítáme jen modré). Ty vznikají jen tak, že nějaká modrá stará je rozpůlená na dvě části. Počet vzroste jen, když jsou obě části v zóně. Podíváme se tedy na arrangment uvnitř červené. Potom ten řez modré facety musí být v zóně v červené kolem g. Tedy, celkový počet facet je $O(n^{d-1})$.

TODO: Mírně dlouhé a nepřehledné. Co s tím?

Počet stěn dimenze $d-k$, kde k je mezi 1 a $d-1$ (nezahrnuje hrany a vrcholy). Označíme $f_{d-k}(n)$ maximální počet $d-k$ dimenzionálních stěn zóny s n nadrovinami. Vezememe náhodnou $h \in \mathcal{H}$, obarvíme červeně, zbytek modře. Stěna bude modrá, pokud její vnitřek bude disjunktní s červenou. Jaký je střední počet modrých stěn v zóře, zase dva způsoby. Že zůstane modrá je, že žádná z k protínajících není modrá, takže $\frac{n-k}{n} \cdot f_{d-k}(n)$. Druhým způsobem, máme $f_{d-k}(n-1)$ starých modrých stěn po odebrání červené, přibude – zase rozdělujeme. Každý vrchol leží v nějaké 3-dimenzionální stěně arrangmentu, což je polyedr. Je to tedy rovinný graf a podle eulerova formule není počet vrcholů více, než lineárně s počtem stěn. Každá 2-dimenzionální stěna může sousedit s konstantně mnoha 3-dimenzionálních (závislé na dimenzi prostoru).

☻

Arrangmenty obecnějších geometrických objektů

Kdybych měl třeba úsečky v rovině, tak to dělá složité věci. Vrcholy budou průsečíky úseček, hrany jsou části po odebrání bodů, stěny jsou souvislé

části roviny, kde to nepřerušují úsečky.

Mám $O(n^2)$ vrcholů i hran. Složitost jedné stěny je řádu $\alpha(n)$.

Kdybychom měl libovolné množiny v $\mathbb{R}^d$, tak arrangement bude rozklad na jednotlivé stěny, které jsou souvislé podmnožiny a nezalézají do žádné z množin.

Řekneme že x je ekvivalentní s y pokud jsou ve stejných množinách. Stěny budou takové části, které jsou ekvivalentní.

Arrangment algebraických ploch

Vezmou se mnohočleny a beru nulové množiny (množiny, kde jsou nulové). Předpokládáme, že stupeň všech polynomů je menší než nějaké D (budeme uvažovat především malé). Tímto se dá udělat spoustu útvarů (kužele, koule...).

Vezmeme D a d konstanty. Potom arrangement bude mít $O(n^d)$ stěn.

Slabší verze je znaménková posloupnost. Vezmeme posloupnost čísel $\in \{0, -1, 1\}$. Tato posloupnost je znaménková, pokud existuje bod, kde polynomy nabývají takových znamének v tomto bodě.

Věta 16 (Müllerova-Thorova) *Nechť $p_1, p_2, \ldots, p_n$ jsou polynomy d proměnných maximálního stupně D. Potom maximální počet stěn arrangmentu nulových množin těchto polynomů (tedy i znaménkových posloupností) je:*

$$\left(\frac{50D \cdot n}{d}^d\right)$$

Arrangement pseudopřímek

Je to arrangement konečného souboru křivek v rovině, které splňují následující:

- Každá křivka je x-monotónní a neomezená v obou směrech (tedy, protíná každou svislou přímku v právě jednom bodě).
- Každé dvě křivky se protínají přesně v jednom bodě, tam se kříží.

Vylučuje rovnoběžné a svislé. Je to technicky těžší.

Dva arrangementy pseudopřímek jsou isomorfní, pokud se kříží „ve stejném pořadí“.

Pro každý arrangement nejvýše 8 pseudopřímek k němu existuje ekvivalentní arrangement přímek, pro víc už to neplatí. Máme afinní arrangment a žádné

tři pseudopřímky nemají společný průsečík. Dá se překreslit do wiring diagramu. Lze si všimnout, že protože se každé dvě protínají právě jednou, tak musí skončit v opačném pořadí, než začaly.

Arrangmentů pseudopřímek je mnoho (dolní odhad se dá udělat něco jako 2^{n^2} přes mřížku, další sada každý průsečík obchází zezdola nebo zezhora). U přímek to bude jen něco jako $2^{n \log n}$. `TODO: Proč?`

6.7 Půlící přímky

Nechť P je množina bodů v obecné poloze. Přímka je ***půlící***, pokud protíná dva body a na každé straně leží právě $\frac{n-2}{2}$ bodů. Budeme předpokládat, že n bude sudé.

Nechť $h(P)$ je počet půlících přímek v P. $h(n)$ bude maximum přes všechny P velikosti n z $h(P)$ ($h(n) = \max_{P;|P|=n} h(P)$).

Půlící úsečka je taková, která leží na půlící přímce.

Je jich alespoň $\frac{n}{2}$ – vezmu jeden bod a seřadím si ostatní podle úhlu. Větší najít nejde (příklad na takle malý).

Věta 17

$$n \cdot e^{\Omega(\sqrt{logn})} \leq h(n) \leq O(n^{\frac{4}{3}})$$

`TODO: Proč?`

Lemma 7 *Půlící úsečky v libovolném bodě $p \in P$ a jejich prodloužení se pravidelně střídají.*

Důsledek 5 *Z každého $p \in P$ vychází lichý počet půlících úseček.*

Nechť G je geometrický graf (vrcholy budou body množiny P, hrany jsou půlící úsečky). Lze počítat přes počty průsečíků úseček.

Tvrzení 9

$$cr(G) + \sum_{v \in V} \left(\begin{pmatrix} \frac{1}{2} \cdot (deg(v) + 1) \\ 2 \end{pmatrix} \right) = \begin{pmatrix} \frac{n}{2} \\ 2 \end{pmatrix}$$

`TODO: Je to určitě dobře?`

Napřed ověříme pro konvexní polohu. To je vidět (můžeme jimi otáčet).

Když nejsou konvexní, body můžu šoupat, pokud je to uvnitř jedné stěny. Pokud přelezeme přes půlící úsečku (vnitřkem, mezi těmi konci), tak jedna

zmizí (ta původní) a nahradí se dvěma novýma. Průsečíkové číslo se zmenší (tam, kde bydlel původně, bylo méně vrcholů a protože část vede do něj a ne přes něj). A postupně se to popřehází.

Opačně, když není půlící, ale ty dvě jsou půlící, tak je situace opačná. Tedy, levá strana se opět nemění.

Pokud prochází vnějškem. Potom ale můžeme koukat jako že přelejzá prostřední a to už je rozebrané.

Důsledek 6

$$cr(G) \leq n^2$$

TODO: Proč?

Zapojíme větu 9. Z toho plyne, že $h(n) = O\left(n^{\frac{4}{3}}\right)$.

6.8 Kovnexní nezávislost

Lemma 8 *Máme množinu $X \subseteq \mathbb{R}^2$ velikosti alespoň 5. Potom obsahuje konvexní čtyřúhelník.*

Důkaz:
Vezmeme konvexní obal X. Pokud má 4 vrcholy, pak jsme vyhráli, pokud jen 3, pak jeden zahodíme a tyto 4 jsou konvexní čtyřúhelník.

☻

TODO: Proč a který?

Věta 18 (Erdös-Szekeres) *$\forall k \exists n$ pro n bodů v rovině $\exists$ konvexní k-úhelník.*

Důkaz:
BÚNO žádné dva body neleží na svislé přímce. Potom k-miska je konvexní množina k bodů které jdou „dolů a potom nahoru“ (leží na grafu konvexní funkce). k-čepice je opačně.

Označíme $f(k,l)$ jako maximální počet bodů v obecné poloze v $\mathbb{R}^2$ bez k-misky a l-čepice. Dokážeme, že toto číslo je konečné, indukcí a je to $\begin{pmatrix} k+l-4 \\ k-2 \end{pmatrix}$.

$f(k,2) = f(2,l) = 1$. Další krok je, že jak k, tak l jsou alespoň 3 a pro menší součet to platí. Tedy, $f(k,l-1) = \begin{pmatrix} k+l-5 \\ k-2 \end{pmatrix}, f(k-1,l) =$

$\binom{k+l-5}{k-3}$. Určitě je to alespoň součet těchto dvou čísel, tedy $f(k,l) \geq f(k-1,l)+f(k,l-1)$. Dám je za sebe, první nahoru $f(k,l-1)$, druhý dolů $f(k-1,l)$ (když vlevo proložíme libovolné 2 body, tak vpravo leží všechno pod tím, vlevo opačně).

Když vezmeme $f(k-1,l)+f(l-1,k)+1$, tak to už buď k-misku nebo l-čepici musí obsahovat. Předpokládejme, že ne. Vezmeme všechny koncové body $k-1$-misek, označíme jako množinu A. Vezmeme zbytek, to musí být dostatečně malé, protože je to bez $k-1$ misky a bez l-čepice, A musí být dostatečně velké. Kdyby obsahovalo k-misku, tak spor, obsahuje tedy $l-1$ čepici c. Ty jsou někde spojené, ty 3 body (jeden, který je spojuje) tvoří buď 3-misku nebo 3-čepici. Tedy jde něco z toho prodloužit.

TODO: Upřesnit?

☻

Označme $ES(k)$ jako nejmenší číslo, pro které platí věta 18. Potom $ES(k)$ určitě obsahuje konvexní k-úhelník v obecné poloze. Je doměnka, že $ES(k) = 2^{k-1}+1$. Dolní odhad na to existuje, horní je dokázán na $\binom{2k-5}{k-2}+1$ pro $k \geq 5$.

7 Geometrické incidence

Navazuje na incidence bodů a přímek.

7.1 Dolní odhady

Na větu 8 byla mřížka široká k, vysoká $4k^2$, přímky jsou s celočíselnými souřadnicemi. Celkem tedy zhruba k^3 přímek i bodů, k^4 průsečíků.

Původní byl jiný: mřížka $\sqrt{n} \times \sqrt{n}$, přímky které jsou ve tvaru $y = \frac{a}{b}x + c$, kde $a, b \in 0 \ldots t$, t volíme tak, aby bylo zhruba n přímek, tedy to vyjde asi $n^{\frac{1}{6}}$, každý bod bude mít zhruba $n^{\frac{1}{3}}$ incidencí.

Na jednotkové vzdálenosti – $\exists$ mnoho jednotkových vzdáleností pro vhodnou normu v rovině (autor: Valtr). Norma – máme jednotkový kruh, ptáme se, kolikrát je potřeba ho zvětšit, aby se bod ocitl uvnitř. Obecná norma je nějaká množina, která obsahuje počátek a je dle něj symetrická (např. elipsa).

Z normy uděláme metriku tak, že hledáme normu rozdílu bodů.

Známé důkazy horního odhadu $O(n^{\frac{4}{3}}$ vrací stejný odhad i pro libovolnou normu v $\mathbb{R}^2$, pokud je striktně konvexní. (tedy, nevyužívají „kulatosti“ kružnice).

Existuje norma že $\forall n \exists$ množina n bodů v $\mathbb{R}^2$ s $\geq c \cdot n^{\frac{4}{3}}$ jednotkových vzdáleností. Máme dvě paraboly „nad sebou“ (horní prochází $[-1,0],[0,1],[1,0]$, tedy $|y| \leq 1 - x^2$. Potom vezmeme mřížku s k body na šířku a k^2 na výšku tak, aby se to „vešlo“ do paraboly (tedy, výška i šířka mřížky bude vždy 2).

Některé body mají vzdálenost 1 od počátku, to jsou ty na hranici, tedy body o souřadnici $\left(\frac{i}{k}, 1 - \frac{i^2}{k}\right)$. Tedy, v každém sloupečku bude alespoň jeden nahoře a jeden dole. Pro počátek tedy je řádově k bodů o jednotkové vzdálenosti. Mám k^3 bodů, každý má řádově k bodů v jednotkové vzdálenosti (kvůli posunutí počátku), celkem tedy k^4 jednotkových vzdáleností, což je $n^{\frac{4}{3}}$.

Věta 19 *$\forall n > 2 \exists n$ bodů v $\mathbb{R}^2$, které mají alespoň $n^{1+\frac{c}{\log\log n}}$ jednotkových vzdáleností (zde se už mluví zase o euklidovské vzdálenosti).*

Důkaz:
Vezmeme mřížku $\sqrt{n} \times \sqrt{n}$ bodů, ale dobře škálovaná (řádově tak velká jednotka jako velikost mřížky, ale trochu menší).

Hledáme body takové a a b počty mezer, že $a^2 + b^2 = c$.

Lemma 9 *Nechť $p_1 < p_2 < \ldots < p_r$ prvočísla tvaru $4k+1$ a $M := \prod p_i$. Potom $M = a^2 + b^2$ má $\geq 2^r$ celočíselných řešení pro (a,b).*

Důkaz:
Prvočíslo $p > 3$ se dá napsat jako $a^2 + b^2, a, b \in \mathbb{Z} \Leftrightarrow p \cong 1 (\mathrm{mod} 4)$. Bereme jako fakt z teorie čísel (doprava jednoduché, ale my potřebujeme doleva, vyplývá z věty 7).

Víme, že každé prvočíslo p_j lze zapsat jako $a_j^2 + b_j^2, a_j, b_j \in \mathbb{Z}$. Uděláme gaussova celá čísle $\mathbb{Z}[i]$ (to jsou komplexní celá čísla). Toto je okruh s jednoznačným rozkladem na prvočinitele. Tedy, je to euklidovský okruh.

Definujeme $\alpha_j := a_j + i \cdot b_j, \overline{\alpha_j} := a_j - i \cdot b_j, \left|\alpha_j^2\right| = \alpha_j \cdot \overline{\alpha_j} = a_j^2 + b_j^2 = p_j$.
$\forall J \subseteq I := \{1,2,\ldots,r\}\, A_J + i \cdot B_j := \left(\prod_{j \in J} \alpha_j\right)\left(\prod_{j \in I \setminus J} \overline{\alpha_j}\right)$. Tyto A_J a B_J jsou různá. $A_J^2 + B_J^2 = |A_J + i \cdot B_J|^2 = (A_J + i \cdot B_J)(A_J - i \cdot B_j) = (\prod_{j \in J} \alpha_j)(\prod_{j \notin J} \overline{\alpha_j})(\prod_{j \in J} \overline{\alpha_j})(\prod_{j \notin J} \alpha_j) = \prod p_j = M$.

Čísla A_J, B_J jsou řešení naší rovnice. Pokud mají různé rozklady na prvočinitele, pak musejí být různé. Na to stačí ověřit, že $\alpha_{1\ldots r}, \overline{\alpha_{1\ldots r}}$ jsou prvočinitele v $\mathbb{Z}[i]$ a žádné se nedostane z jiného vynásobení jednotkou (žádnou jednotkou – $1, -1, i, -i$). $\alpha_j \neq -1, i, -i\overline{\alpha_j}$. Když porovnávám $\alpha_j, \alpha_{j'}$, tak mají různou absolutní hodnotu.

Prvočinitele se dokážou z toho, že p_i jsou prvočísla. Předpokládejme, že $\alpha_i = \gamma_1\gamma_2 \Rightarrow |\alpha_i|^2 = p_i = |\gamma_1|^2 \cdot |\gamma_2|^2$, obě celá čísla, jedno z toho musí být jednotka.

☻

☻

Věta 20 (Prvočíselná) *Nechť $\pi(n) = |\{p \leq n, p \text{ prvočíslo}\}|$. Potom*

$$\pi(n) = (1 + o(1)) \cdot \frac{n}{|n|}$$

Když máme aritmetickou posloupnost (tedy, $a+kd$), některé žádná prvočísla neobsahují.

Věta 21 (Dirichletova) *Nechť $\pi_{a,d}(n)$ je počet prvočísel v aritmetické posloupnosti $a+k\cdot d$, potom pokud jsou a, d nesoudělná (pak by to neobsahovalo žádná prvočísla), tak je:*

$$\pi_{a,d}(n) = (1 + o(1)) \cdot \frac{n}{\varphi(d) \cdot \log n}$$

Důsledek 7

$$\pi_{1,4}(n) \in \Omega\left(\frac{n}{\ln n}\right)$$

Máme tedy mřížku $\sqrt{n} \times \sqrt{n}$ mřížka. M je součin prvních $r-1$ prvočísel tvaru $4k+1$, r největší takové, že $M \leq \frac{n}{4}$. Mřížku naškálujeme na $\frac{1}{\sqrt{M}}$.

Každý bod se podílí alespoň na tolika jednotkových vzdálenostech, kolik je reprezentací $M = a^2 + b^2$, kde a, b jsou nezáporná celá čísla (beru jen čísla v levém dolním půlkruhu). Máme alespoň 2^{r-1} reprezentací. Z toho alespoň $\frac{2^{r-1}}{4}$ jsou nezáporná celá.

Z volby n plyne, že $4 \cdot \prod_{i=1}^{r-1} p_i \leq n < 4 \prod_{i=1}^{r} p_i$, $2^r \leq n$, $pr \geq \left(\frac{n}{4}\right)^{\frac{1}{r}}$.

$$r = \pi_{1,4}(p_r) \geq \left(\frac{1}{2} - o(1)\right) \cdot \frac{p_r}{\ln p_r} > \sqrt{p_r} \geq n^{\frac{1}{3}r}$$

(ta třetina je v exponentu kvůli tomu dělení 4).

$$\begin{aligned} r^{3r} &\geq n \\ 3r \ln r &\geq lnn \end{aligned}$$

$$\begin{aligned} r &\geq \frac{\log n}{3 \log r} \\ r &\geq \frac{\log n}{3 \log \log n} \\ \log r &< \log \log n \end{aligned}$$

Celkem tedy alespoň $n \cdot \frac{2^\pi}{16} \geq n^{1+\frac{c}{\log \log n}}$.

8 Věty o součtech a součinech

Budeme uvažovat konečné množiny reálných čísel $A \subseteq \mathbb{R}$. Budeme značit:

- $A + A = \{a + b; a, b \in A\}$
- $A \cdot A = AA = \{a \cdot b; a, b \in A\}$

Pokud je A generická (nejsou mezi nimi lineární závislosti) a $|A| = n$, potom $|A + A| = \binom{n}{2} + n$.

Naopak, pokud bude $A = \{1, 2, \ldots, n\}$, potom $A + A = \{2, 3, \ldots, 2n\}$, což je $2n - 1$ členů. Toto platí pro libovolnou aritmetickou posloupnost. Dá se ukázat, že je to nejmenší možné.

Věta 22 (Freiman) *$\forall C \exists d, C_1$ taková, že $A \subseteq \mathbb{R}, |A| = n; |A + A| \leq C \cdot n$, potom existuje d-dimensionální aritmetická posloupnost A' taková, že $A \subseteq A' \wedge |A1| \leq C_1 \cdot n$.*

d-dimensionální aritmetická posloupnost *jsou čísla ve tvaru $\left\{a_0 + \sum_{i=1}^{d} k_i \cdot b_i\right\}$, $k_i \in n_i$, kde n_i, b_i jsou parametry.*

Podobně to bude fungovat pro $A \cdot A$ a geometrickou posloupnost.

Dá se najít nějaká množina A, kde $A + A$ je malé a i $A \cdot A$ malé? Hypotéza je, že $\forall \epsilon \in \mathbb{R}^+ \max |A + A|, |A \cdot A| \geq c \cdot n^{2-\epsilon}$.

Rekord je $\max(|A + A|, |A \cdot A|) > n^{\frac{4}{3}}$.

Věta 23 (Elekes)

$$\max(|A + A|, |A \cdot A|) \geq c \cdot |A|^{\frac{5}{4}}$$

.

Důkaz:
Dokážeme pomocí věty 8, že $|A+A| \cdot |A \cdot A| \geq c' \cdot n^{\frac{5}{2}}$.

Na jednu osu si nakreslíme $A+A$, na druhou $A \cdot A$, vezmeme jejich kartézský součin – tím získáme body.

Nechť $A = \{a_1, \ldots, a_n\}$, přímky $l_{i,j} = \{y = a_i \cdot (x - a_j)\}$, $i, j \in 1 \ldots n$

Máme n^2 bodů a n^2 přímek.

$\forall k$ uvážíme bod $a_j + a_k$ a bod $a_i \cdot a_k$. To náleží do $l_{i,j}$. Tedy, každá přímka z L má alespoň n incidencí. Dosadíme do věty 8, vyjde, že $I(P, L) \geq 3$. $\leq C\left(|P|^{\frac{2}{3}} \cdot |L|^{\frac{2}{3}} + |P| + |L|\right) = C\left(n^{\frac{4}{3}}|P|^{\frac{4}{3}} + |P| + n^2\right) \geq n^3$.

Z toho už vyjde, že $|P| \geq c \cdot n^{\frac{5}{2}}$.

☻

Věta 24 (Solymosi) *Nechť $A \subseteq \mathbb{R}^+$ je množina kladných čísel. Potom* $\max(|A+A|, |A \cdot A|) \geq c \cdot \frac{|A|^{\frac{4}{3}}}{(\log |A|)^{\frac{1}{3}}}$.

Důkaz:
Dokážeme, že $|A+A|^2 \cdot |A \cdot A| \geq c \cdot \frac{|A|^4}{\log A}$. Zavedeme veličinu $E(A)$, říká se jí multiplikativní energie množiny. To je $|\{(a, b, c, d)\,; a, b, c, d \in A; a \cdot d = b \cdot c\}|$.

Lemma 10

$$E(A) \geq \frac{|A|^4}{|A \cdot A|}$$

Důkaz:
Počítání dvěma způsoby, Cauchy-Swartzova nerovnost:

Budeme brát dvojice podle toho, jaké mají součiny (tedy, zafixuji ad, k nim vybírám bc tak, aby měly stejný součin). Tedy, $n_p := |\{(x, y)\,; x, y \in A; xy = p\}|$.

$$E(A) = \sum_{p \in A \cdot A} n_p^2$$

$$|A|^4 = \sum_{p \in A \cdot A} \sum_{q \in A \cdot A} n_p \cdot n_q = \left(\sum_{p \in A \cdot A} n_p\right)^2$$

Pak vezmeme cauchy-swartzovu nerovnost:

$$\left(\sum x_i y_i\right)^2 \leq \left(\sum x_i^2\right) \cdot \left(\sum y_i^2\right)$$

(za y_i dáme 1, za x_i dáme n_p).

Tedy, máme:

$$|A|^4 \leq (\sum n_p^2) \cdot |A \cdot A| = E(A) \cdot |A \cdot A|$$

☻

Lemma 11

$$\frac{E(A)}{\log |A|} = O(|A + A|^2)$$

Budeme z těch čtveřic energie dělat prvky $(A + A) \times (A + A)$. Na prvky $(A + A) \times (A + A)$ se můžeme dívat jako na $(A \times A) + (A \times A)$.

Když bude multiplikativní energie veliká, bude těch součtů hodně.

Definujeme $m_q := \left|\left\{(a, b) \in A^2; \frac{a}{b} = q\right\}\right|$. $E(A) = \sum_{q \in A/A} m_q^2$. Toto říká, že na přímce se směrnicí q je tolikle bodů.

Pozorování 5 *Kdykoliv vezmeme součet dvou vektorů, tak výsledek padne mezi ně. Když tedy jsou* 3 *vektory, tak součet prvního s druhým a druhého s třetím, tak nikdy nesplynou (nebudou ve stejném kvadrantu). Tedy, kdykoliv* $\alpha u + \alpha' u' = \beta u + \beta' u'$*, pak taky* $\alpha = \beta$ *a* $\alpha' = b'$*. Pro takové* 3 *přímky dostaneme alespoň* $m_q m'_q + m'_q m''_q$*.*

Pokud to vezmeme abstraktně, $m_1, m_2, \ldots, m_s$ přirozená čísla. Potom $\sum m_i^2 = E(A)$. Chceme vybrat indexy $i_1, i_2, \ldots, i_t$ tak, aby $m_{i_1} m_{i_2} + m_{i_2} m_{i_3} + \ldots + m_{i_{t-1}} m_{i_t}$ byly co největší (ideálně $E(A)$).

Samozřejmě, jsou menší, než n.

Na to použijeme trik. Rozdělíme je do škatulek podle velikosti (od 1 do 2, od 2 do 4, etc, až $2^k, 2^{k+1}$). Těch je řádově $\log n$. Existuje nějaká, která obsahuje alespoň taková m_i, aby $\sum_{i \in I} m_i^2 \geq \frac{E(A)}{\log n}$. t bude počet indexů v této škatulce. Z toho se odvodí, že $tm^2 \geq \frac{E(A)}{4 \log n}$.

$$\sum_{j=1} t - 1 m_{i_j} m_{i_{j+1}} \geq (t-1)m^2 \geq \frac{t-1}{t} \frac{E(A)}{4 \log n}$$

Ošetření, že $t = 1$, je, že příspěvek téhle šaktulky je nejvíc n^2. Vezmu první řádek a první sloupec, sečtu nějaký z jeho vektorů.

☻

8.1 Sumy a součiny v konečných tělesech

Máme těleso $\mathbb{F}_q$, $A \subseteq \mathbb{F}_g$. Opět se ptáme, kolik je $\max(|A+A|, |A \cdot A|)$.

Pro incidence v konečné afinní/projektivní rovině platí jen slabší odhady pro $Szemereni - Trotter$.

Konečná projektivní rovina řádu q má $n = q^2 + q + 1$ bodů, má také n přímek, každá přímka má $q+1$ incidencí. Počet incidencí $I(n,n) \geq n^{\frac{3}{2}}$.

Když $q = p^\alpha$ je mocnina prvočísla, $\beta|\alpha$, pak $\mathbb{F}_{p^\beta}$ je podtěleso $\mathbb{F}_{p^\alpha}$.

Tedy, pokud q není prvočíslo, potom netriviální podtěleso, $A = A + A, A = A \cdot A$.

Nicméně platí:

Tvrzení 10 $\forall \delta > 0 \exists \epsilon > 0$, *p prvočíslo,* $A \subseteq \mathbb{F}_p, 1 \leq |A| \leq p^{1-\delta}$. *Potom* $\max(|A+A|, |A \cdot A|) \geq c \cdot \delta \cdot |A|^{1+\epsilon}$.

Tvrzení 11 *Když qje obecné (tedy, i mocnina prvočísla), potom když* $\sqrt{q}^{1+\delta} \leq |A| \leq q^{1-\delta}$, *potom platí totéž, jako v minulém.*

Dají se s tím vytvářet pseudonáhodné objekty (ramseoyvské grafy, expandery), používá se ve výpočetní složitosti, kryptografii, teorie grup.

Věta 25 $A \subseteq \mathbb{F}_q$. *Potom* $\max(|A+A|, |A \cdot A|) \geq c \cdot \min\left(\sqrt{q \cdot |A|}, \frac{|A|^2}{q}\right)$.

Důkaz:
Nejdříve zapomeneme na A a budeme si všímat tělese $\mathbb{F}_q$. Za pomoci něj definujeme multigraf G, jehož vrcholy budou dvojice $\mathbb{F}_q^* \times \mathbb{F}_q$ (tedy, první není nula). Hrany budou $E := \{\{(a,b),(c,d)\}, ac = b + d\}$.

Má $q \cdot (q-1)$ vrcholů. Budeme tomu říkat n. Každý vrchol (a,b) má stupeň $q-1$. Pro každé c nenulové existuje právě jedno d tak, aby to vyšlo.

Vlastní čísla G: definujeme matici sousednosti M ($n \times n$, jedničky odpovídají hranám).

M je reálná symetrická matice. Ta má n reálných vlastních čísel $\lambda_1, \lambda_2, \ldots, _n$ (nemusí být všechna různá). Existuje ortogonální báze $\mathbb{R}^n$ z vlastních vektorů.

V každém řádku je $q-1$ jedniček. To znamená, že když ji vynásobím vektorem samých jedniček (vyjdou mi řádkové součty), tak dostanu vektor samých $(q-1)$-ček. Toto je první vlastní číslo, tedy λ_1 je $q-1$. $|\lambda_i| \leq q-1$ (protože součet maximálně $q-1$ prvků).

Lemma 12 *Všechny ostatní jsou menší (v absolutní hodnotě) než* $\sqrt{3q}$.

☻

9 Purdyho doměnka

Máme dvě přímky, na každé je n bodů. Ptáme se, kolik minimálně vzdáleností je specifikovaných body různých přímek (tedy, mezi p_i, q_j a ne mezi p_i, p_j).

Dá se sestavit $O(n)$ na dvou rovnoběžných, když jsou pravidelně. Druhá možnost je dvě kolmé, vzdálenosti jsou $\sqrt{1}, \sqrt{2}, \sqrt{3} \ldots$.

Domněnka je, že pokud přímky nesvírají úhel 0, $\frac{\pi}{2}$ je počet vzdáleností $\omega(n)$.

Máme souřadnice tak, že měříme vzdálenost od jejich průsečíku v nějakých jednotkových vektorech jejich směru. $\lambda = \cos\alpha$, chceme, aby nebyl ani 0, ani ± 1. Vzdálenost budeme měřit jako $p(x, y) = x^2 + y^2 - 2\lambda xy$.

Řekneme, že polynom $p(x, y)$ je ***speciální***, pokud existují polynomy $f(x), g(x), h(x)$ takové, že $p(x, y)$ jde zapsat buď jako $f(g(x) + h(y))$ nebo $f(g(x) \cdot h(y))$.

Věta 26 *Pokud p není speciální, potom nabývá na množině parametrů velikosti n $\omega(n)$ výsledků.*

10 Dolní obálky, Davenport-Schinzelovy posloupnosti

Máme množinu úseček a pozorovatele v ploše, přes úsečky není vidět. Vidí nějaké úseky, z některé úsečky může vidět i více částí. Otázkou je, kolik úseků vidí.

Máme množinu úseček, koukáme na ni zespodu (tedy, jakoby v $-\infty$).

Máme funkce $\mathbb{R} \to \mathbb{R}$, každé dvě se protínají v max řekněme 3, nebo v s bodech, kolik kousků vidí pozorovatel zespodu?

Davenport-Schinzelova posloupnost rádu s nad abecedou $1 \ldots n$ je posloupnost délky m:

- $\forall i; a_i \in \{1, \ldots, n\}$
- $\forall i < m; a_i \neq a_{i+1}$
- Daná posloupnost neobsahuje střídavou podposloupnost délky $s + 2$.

Maximální délka této posloupnosti se označuje $\lambda_s(n)$.

- $\lambda_1(n) = n$

- $\lambda_2(n) = 2n - 1$ indukcí podle n.
- $\lambda_3(n) = 2n \cdot \ln n + 4n$

Existuje i zobecnění, zakazujeme i jiné vzory, než střídavé podposloupnosti.

Nechť $w = a_1 a_2 a_3 \dots a_l$. w je m-***rozložitelná***, pokud w lze rozložit na m řetězců takových, že se v žádném nic neopakuje.

Nechť $\psi(m, n)$ je max. délka m-rozložitelné posloupnosti řádu 3 nad $1 \dots n$.

Lemma 13 $\lambda_3(n) = \psi(2n, n)$

Uděláme uspořádání na abecedě, $a < b$, pokud první výskyt a je dříve, než b. Inverzní ackermanova funkce $\alpha(n) = \min\{k \geq 1; A(k) \geq n\}$.

Snažíme se dokázat, že $\lambda_3(n) \in O(n \cdot \alpha(n))$.

$m, n \geq 1$, $m = m_1 + m_2 + \ldots + m_p$, $m_i \geq 1$.