Řešení příkladu s mříží

Alexandr Kazda

Celý tento text je nepovinný a určený pro otrlejší čtenáře.

Zadání 1 *Buď $n \in \mathbb{N}$ a mějme prvky $u_1, \dots, u_n \in \mathbb{Z}^n$ takové, že když napíšeme souřadnice u_i do řádků, je*

$$V = \left| \det \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \right| \neq 0.$$

Potom platí, že $[\mathbb{Z}^n : \langle u_1, \dots, u_n \rangle] = V$ (tj. $|\mathbb{Z}^n / \langle u_1, \dots, u_n \rangle| = V$).

Řešení: Zkuste si situaci představovat pro $n = 1, 2$. Pokud nějakou část důkazu nechápete, zkuste ji přeskočit a vrátit se k ní později.

První pozorování je, že V přesně udává objem rovnoběžnostěnu určeného vektory $u_1, \dots, u_n$. Druhé pozorování, které dává do souvislosti index $[\mathbb{Z}^n : \langle u_1, \dots, u_n \rangle]$ a počty mřížových bodů, zformulujeme jako lemma:

Lemma 1.1 *Číslo $[\mathbb{Z}^n : \langle u_1, \dots, u_n \rangle]$ je rovno počtu bodů $\mathbb{Z}^n$ uvnitř množiny*

$$F = \{\alpha_1 u_1 + \cdots + \alpha_n u_n : \forall i, \alpha_i \in [0, 1)\}$$

Důkaz: Opět doporučuji si nakreslit obrázek, ta složitá množina F je vlastně maličko uříznutý rovnoběžnostěn.

Všimněte si, že pokud $V \neq 0$, můžeme pomocí F vydláždit $\mathbb{R}^n$. Přesněji pro $k_1, \dots, k_n \in \mathbb{Z}$ položme $F_{k_1,\dots,k_n} = F + k_1 u_1 + \cdots + k_n u_n$. Pak každá množina $F_{k_1,\dots,k_n}$ je trochu posunuté F, pro různé n-tice $k_1, \dots, k_n$ dostaneme disjunktní množiny a

$$\mathbb{R} = \bigcup_{k_1,\dots,k_n \in \mathbb{Z}} F_{k_1,\dots,k_n}.$$

Rozmyslete si, že toto vše plyne z toho, že $\{u_1, \dots, u_n\}$ je báze $\mathbb{R}^n$.

Víme přitom, že $[\mathbb{Z}^n : \langle u_1, \dots, u_n \rangle]$ je rovno počtu různých bodů $\mathbb{Z}^n$ modulo přičítání celočíselných násobků vektorů $u_1, \dots, u_n$. Protože F lze vydláždit rovinu, bude nutně $[\mathbb{Z}^n : \langle u_1, \dots, u_n \rangle]$ nejvýše rovno počtu mřížových bodů uvnitř F. Buď naopak $t \in \mathbb{Z}^n \cap F$ a předpokládejme, že $s \in (t + \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n) \cap F$. Pak vektor $s - t$ má jednoznačné vyjádření ve tvaru $\gamma_1 u_1 + \cdots + \gamma_n u_n$, kde (protože s, t leží v F) je $\gamma_i \in (-1, 1)$. Navíc s, t jsou mřížové body, takže

$s - t \in \mathbb{Z}^n$ a nutně $\gamma_i = 0$ pro všechna i. Tedy $s = t$. Z tohoto faktu už snadno plyne, že $[\mathbb{Z}^n : \langle u_1, \ldots, u_n \rangle]$ je rovno velikosti $\mathbb{Z}^n \cap F$.

Zbývá dokázat, že v F leží přesně V bodů. Půjdeme na to pomocí limit, takže nás čeká trocha technických výpočtů.

Uvažme velké $m \in \mathbb{N}$ a hyperkrychli $\{-m, \ldots, m\}^n$. V té leží přesně $(2m+1)^n$ mřížových bodů a má objem $(2m)^n$. Označme r počet množin $F_{k_1,\ldots,k_n}$ zcela uvnitř hyperkrychle a p počet množin $F_{k_1,\ldots,k_n}$, které mají neprázdný průnik s povrchem hyperkrychle (tj. kus jich trčí ven). Všimněme si, že v každé množině $F_{k_1,\ldots,k_n}$ leží stejný počet b mřížových bodů.

Jistě platí nerovnosti pro počet bodů

$$
\begin{aligned}
(r+p) \cdot b \geq (2m+1)^n &\geq r \cdot b \\
\frac{(2m+1)^n}{r} \geq b &\geq \frac{(2m+1)^n}{r+p}
\end{aligned}
$$

a pro objemy (nakreslete si obrázek)

$$
\begin{aligned}
(r+p) \cdot V \geq (2m)^n &\geq r \cdot V \\
\frac{(2m)^n}{V} \geq r &\geq \frac{(2m)^n - p}{V}
\end{aligned}
$$

Pokud ukážeme, že počet p špatných množin je malý, konkrétně $p \leq c \cdot m^{n-1}$ pro nějakou konstantu c, tak jsme vyhráli, protože pak ze druhé sady nerovností dostaneme

$$
\frac{(2m)^n}{V} \geq r \geq \frac{(2m)^n - cm^{n-1}}{V},
$$

což po dosazení do nerovností pro počet bodů dá:

$$
\begin{aligned}
\frac{(2m+1)^n}{\frac{(2m)^n - cm^{n-1}}{V}} \geq b &\geq \frac{(2m+1)^n}{\frac{(2m)^n}{V} + cm^{n-1}} \\
\frac{V(2m+1)^n}{(2m)^n - cm^{n-1}} \geq b &\geq \frac{(2m+1)^n V}{(2m)^n + Vcm^{n-1}} \\
\left(1 + \frac{1}{2m}\right)^n \frac{V}{1 - c\frac{1}{2^n m}} \geq b &\geq \left(1 + \frac{1}{2m}\right)^n \frac{V}{1 + Vc\frac{1}{2^n m}}
\end{aligned}
$$

Nyní pro $m \to \infty$ je limita $\left(1 + \frac{1}{2m}\right)^n$ rovna 1 a limity výrazů $\frac{V}{1-c\frac{1}{2^n m}}$ a $\frac{V}{1+Vc\frac{1}{2^n m}}$ jsou obě rovny V. Nutně tedy $b = V$.

Zbývá ukázat, že špatných rovnoběžnostěnů $F_{k_1,\ldots,k_n}$ (takových, že jich kus trčí ven z hyperkrychle) je málo. Hyperkrychle má $2n$ nadstěn $S_1, \ldots, S_{2n}$. Stačí nám dokázat, že každá S_i má neprázdný průnik jen s $O(m^{n-1})$ rovnoběžnostěny $F_{k_1,\ldots,k_n}$. Bez újmy na obecnosti uvažme S_1 stěnu, pro jejíž všechny body platí $x_1 = 1$ (první souřadnice). Položme $l = |u_1| + \cdots + |u_n|$.

Pak uvažme množinu bodů (nafouknutou stěnu)

$$
R_1 = \{(x_1, \ldots, x_n) : \exists (y_1, \ldots, y_n) \in S_1, \forall i, |y_i - x_i| \leq l\}.
$$

Objem R_1 je roven $l \cdot (2(m+l))^{n-1} = O(m^{n-1})$ a pokud má nějaký rovnoběžnostěn $F_{k_1,\ldots,k_n}$ neprázdný průnik s S_1, tak nutně celý leží v R_1 (rozmyslete si; komu nepomůže obrázek, pomůže trojúhelníková nerovnost). Nutně tedy s S_1 může mít neprázdný průnik nejvýše $O(m^{n-1})/V = O(m^{n-1})$ rovnoběžnostěnů $F_{k_1,\ldots,k_n}$, čímž je důkaz ukončen.