Nullstellensatz

Jakub Löwit

Abstrakt. Na přednášce se budeme zabývat takzvanými *větami o nulách*, které dávají do souvislosti množiny polynomů a množiny jejich společných řešení. Nejzajímavější pro nás bude takzvaná *Combinatorial Nullstellensatz*, s jejíž pomocí hravě zvítězíme nad mnoha netriviálními kombinatorickými úlohami.

Věty o nulách

Definice. *Těleso* je množina K obsahující přinejmenším dva význačné prvky 0 a 1, společně s binárními operacemi „plus" a „krát", které splňují vcelku intuitivní axiomy (obě operace jsou asociativní a komutativní; přičítání nuly nic nemění; násobení jedničkou nic nemění; násobení je distributivní vůči sčítání; pro každý prvek a existuje prvek $-a$, který se s ním sečte na 0; pro každý nenulový prvek b existuje prvek b^{-1}, který se s ním vynásobí na 1).

Ačkoli různých těles existuje spousta, my bude pracovat jenom s několika dobře známými[*)],[†)]:

- $\mathbb{C}$ – komplexní čísla
- $\mathbb{R}$ – reálná čísla
- $\mathbb{Q}$ – racionální čísla
- $\mathbb{Z}_p$ – zbytky modulo **prvočíslo** p

Značení.

- Pro dané těleso K můžeme uvažovat *polynomy s koeficienty v* K. Množinu všech takových polynomů značíme $K[x_1, \ldots, x_n]$.
- Dostaneme-li n-tici čísel $(s_1, \ldots, s_n) \in K^n$ a polynom $f \in K[x_1, \ldots, x_n]$, můžeme do něj naše čísla dosadit, čímž dostaneme číslo $f(s_1, \ldots, s_n) \in K$.
- Pro libovolnou množinu polynomů $F \subseteq K[x_1, \ldots, x_n]$ tak dostáváme množinu jejich společných nul $V(F)$, tj. množinu všech n-tic $(s_1, \ldots s_n)$, které pro každý polynom $f \in F$ splňují $f(s_1, \ldots, s_n) = 0$.
- Naopak pro libovolnou množinu $S \subseteq K^n$ takových n-tic můžeme uvažovat množinu $I(S)$ všech polynomů, které se na ní nulují.

Cvičení. Zamyslete se, jak se „hledání společných nul" a „hledání nulujících se polynomů" chová pro polynomy v jedné proměnné nad $\mathbb{C}$.

---

*) Takže pokud o tělesech nic nevíš, vůbec to nevadí a můžeš si místo obecného K po celou dobu představovat třeba reálná čísla $\mathbb{R}$. Pro jiná tělesa než $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ větu stejně používat nebudeme.

†) Naproti tomu $\mathbb{N}$, $\mathbb{Z}$ či $\mathbb{Z}_m$ pro složené číslo m tělesa nejsou – všem totiž chybí multiplikativní inverzy k některým nenulovým prvkům.

Obecně bychom rádi pochopili, jak spolu množiny polynomů a množiny jejich společných nul souvisí. Pro polynomy v jedné proměnné je situace vcelku přehledná – a přinejmenším jsme se už všichni s takovými příklady mnohokrát setkali. Naopak pro více proměnných se problém velmi rychle komplikuje. Přesto se v něm ale často dá najít jakýsi systém. A taková tvrzení se pak typicky nazývají *věty o nulách*.

No a proč nás zajímají? Důležitost souvislosti množin polynomů s jejich společnými nulami v rámci algebry je vcelku očividná. My si ale budeme chtít ilustrovat především důsledky pro řešení kombinatorických a teoriečíselných úloh. Pokud se nám takovou úlohu povede převést čistě do řeči polynomů a jejich hodnot, najednou se nám otevře silný a přehledný algebraický aparát, který můžeme použít. Ačkoli v této přednášce je náš arzenál představován „pouze" jednou větou (avizovanou *Combinatorial Nullstellensatz*), tento přístup funguje obecněji. Čím větší znalost polynomů získáme, tím lépe budeme umět „převádět úlohy do algebry".

Combinatorial Nullstellensatz

Zformulujme a dokažme tedy slíbenou větu, se kterou přišel v roce 1999 původem izraelský matematik Noga Alon. Sama o sobě tato věta není bůhvíjak „překvapivá", ale je nehorázně užitečná právě při převádění kombinatorických problémů do algebry.

Pozorování.

- Buď K těleso, $f \in K[x]$ polynom s k různými kořeny $s_1, \dots, s_k \in K$. Potom $f = h \cdot (x - s_1) \cdots (x - s_k)$ pro nějaký polynom $h \in K[x]$.
- Buď K těleso, $f \in K[x]$ nenulový polynom stupně d. Pak f má nejvýš d kořenů.

Důkaz. Má-li f kořen v $r \in K$, zkusme jej vydělit (se zbytkem) polynomem $(x - r)$, čímž dostaneme vyjádření $f = h \cdot (x - r) + c$ pro nějaké $h \in K[x]$ nižšího stupně a konstantu $c \in K$. Jenže $f(r) = 0$ z předpokladu, takže $c = 0$, pročež $f = h \cdot (x - r)$. Induktivně (dokud má h nějaký kořen) proto můžeme pokračovat a získat

$$f = h \cdot (x - r_1) \cdots (x - r_j),$$

kde $h \in K[x]$ je polynom bez kořene. Tedy $r_1, \dots, r_j$ jsou všechny kořeny f (i s násobnostmi).

V první části jsou nyní všechna $s_1, \dots, s_k$ obsažena mezi $r_1, \dots, r_j$, což dává hledaný tvar, tj. f je skutečně (polynomiálním) násobkem $(x - s_1) \cdots (x - s_k)$. V druhé části dostáváme díky $f \neq 0$ nerovnost stupňů $k \leq j \leq d$, čímž jsme hotovi. ■

Lemma (Rozklad na součet). Mějme těleso K a několik jeho konečných podmnožin $S_1, \dots, S_n$. Dále mějme polynom $f \in K[x_1, \dots, x_n]$, který se nuluje na celé množině $S_1 \times \cdots \times S_n$. Pro $i = 1, \dots, n$ označme $g_i = \prod_{j \in S_i} (x_i - s_j)$. Pak existují polynomy $h_1, \dots, h_n \in K[x_1, \dots, x_n]$ takové, že

$$f = h_1 g_1 + \cdots + h_n g_n.$$

Ty lze navíc zvolit tak, aby $\deg h_i + \deg g_i \leq \deg f$ pro všechna $i = 1, \dots, n$.

Poznámka. Rovnost z lemmatu lze vyjádřit slovy jako „f je lineární kombinace polynomů $g_1, \dots, g_n$ s koeficienty v $K[x_1, \dots, x_n]$“.

Poznámka. Všimněte si, že v případě $n = 1$ se lemma skutečně degeneruje na první část předchozího pozorování.

Důkaz. Nejprve zpozorujme, že postupným odečítáním polynomů tvaru $h_i' g_i$ jako ve znění lemmatu můžeme převést f na polynom f', ve kterém se každé x_i objevuje pouze v mocninách $0, 1, \dots, |S_i| - 1$. Vskutku, g_i je polynom v proměnné x_i tvaru

$$x_i^{|S_i|} + \sum_{j=0}^{|S_i|-1} c_j x_i^j$$

pro nějaké konstanty c_j. Pokud se tedy v f vyskytuje člen obsahující $x_i^{|S_i|}$, odečtením vhodného polynomu tvaru $h_i' g_i$ ho umíme nahradit součtem $h_i' c_i x_i^j$ pro $j = 0, \dots, |S_i| - 1$ (kde h_i' splňuje podmínku se stupni). Opakováním tohoto odečítání se tak skutečně zbavíme všech x_i s exponenty $\geq |S_i|$.

Takto upravený f' se stále nuluje na celém $S_1 \times \cdots \times S_n$. Tvrdíme, že $f' = 0$. To snadno ověříme indukcí na n, přičemž případ $n = 1$ plyne z předchozího pozorování. Pro $n \geq 2$ rozepišme f' jako součet členů podle exponentu u x_n, tj.

$$f' = \sum_{j=0}^{|S_n|-1} f_j' x_n^j,$$

kde $f_j' \in K[x_1, \dots, x_{n-1}]$ jsou polynomy ve zbylých proměnných. Pokud se některý z f_j' nenuluje na některém $(s_1, \dots, s_{n-1}) \in K^{n-1}$, částečným dosazením získáme nenulový polynom jedné proměnné $f'(s_1, \dots, s_{n-1}, x_n)$ stupně nejvýše $|S_n| - 1$, který se nuluje na celém $|S_n|$, což je spor s předchozím pozorováním. Tedy všechny f_j se nulují na celém $S_1 \times \cdots \times S_{n-1}$, z indukčního předpokladu se tedy jedná o nulové polynomy, pročež také $f' = 0$.

Tím jsme hotovi: z konstrukce f' je jasné, že $f = f' + h_1 g_1 + \cdots + h_n g_n$ pro polynomy h_i, g_i jako ve znění lemmatu, ale zároveň jsme ukázali $f' = 0$. ■

Nyní můžeme zajásat, protože naše napjatě očekávaná věta je pouze elegantním důsledkem předchozího explicitního lemmatu.

Věta (Combinatorial Nullstellensatz). Mějme těleso K, několik jeho konečných podmnožin $S_1, \dots, S_n$, a polynom $f \in K[x_1, \dots, x_n]$. Předpokládejme, že platí $\deg f = t_1 + \cdots + t_n$ pro $t_1, \dots, t_n \in \mathbb{N}_0$ splňující

(i) $t_i < |S_i|$ pro všechna $i = 1, \dots, n$,
(ii) koeficient u $x_1^{t_1} \cdots x_n^{t_n}$ v polynomu f je nenulový.

Potom existují $s_i \in S_i$ pro $i = 1, \dots, n$ taková, že $f(s_1, \dots, s_n) \neq 0$.

Poznámka. Všimněte si, že v případě $n = 1$ věta říká: Je-li $S \subseteq K$ konečná podmnožina a $f \in K[x]$ polynom stupně $\deg f = t < |S|$, pak existuje $s \in S$ splňující $f(s) \neq 0$.

Důkaz. Věta je důsledkem předchozího lemmatu – kdyby se f nuloval na celé množině $S_1 \times \cdots \times S_n$, mohli bychom jej přepsat jako

$$f = \sum_{i=1}^{n} h_i g_i,$$

kde $g_i = \prod_{j \in S_i} (x_i - s_j)$ a zároveň $\deg h_i + \deg g_i \leq \deg f$ pro všechna $i = 1, \ldots, n$. Součet členů maximálního stupně v f proto tvaru

$$\sum_{i=1}^{n} h_i' \cdot x_i^{|S_i|},$$

kde h_i' značí součet členů maximálního stupně v h_i. Má-li tedy nějaký člen polynomu f maximálního stupně nenulový koeficient, musí obsahovat některé x_i v mocnině $\geq |S_i|$. Jenže díky bodu (i) máme pro všechna i nerovnost $|S_i| > t_i$, takže člen (maximálního stupně) $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ musí mít nulový koeficient, což je ve sporu s bodem (ii). Polynom f se tedy na celé množině $S_1 \times \cdots \times S_n$ nulovat nesmí. ∎

Úlohy

Konečně nadchází čas si použití naší teorie pořádně procvičit. Při tom uvidíme důsledky *Combinatorial Nullstellensatz* zasahující do kombinatoriky a teorie grafů, kombinatorické geometrie, algebry, i teorie čísel.

Ačkoli následující úlohy nezřídka mají i pěkná elementární řešení, často je velmi neelementární na ně přijít. *Combinatorial Nullstellensatz* je skutečně silná, takže se není třeba divit, že ji často opravdu stačí přímočaře použít, a občas tak získat i obecnější výsledek. K její aplikaci nám stačí chytře zvolený polynom, jehož stupeň a vhodný „vedoucí koeficient“ máme pod kontrolou.

Úloha 1. V každém vrcholu pravidelného 100-úhelníku jsou napsaná dvě přirozené čísla. Ukažte, že lze z každého vrcholu smazat jedno číslo tak, aby v žádných dvou sousedních vrcholech nezbyla stejná čísla. (ARO 2007)

Úloha 2. Pro přirozené číslo n označme

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, (x, y, z) \neq (0, 0, 0)\}.$$

Určete nejmenší přirozené číslo m, pro které může být S pokryta m rovinami, které neprochází počátkem. (IMO 2007, 6)

Úloha 3. Mějme prvočíslo p a dvě množiny A, B některých zbytků modulo p. Označme $A + B$ množinu těch zbytků, které lze získat jako $a + b$ pro $a \in A$, $b \in B$. Dokažte nerovnost $|A + B| \geq \min\{p, |A| + |B| - 1\}$. (Cauchy-Davenport)

Úloha♮ 4. Mějme prvočíslo p a polynomy $f_1, \ldots, f_m \in \mathbb{Z}_p[x_1, \ldots, x_n]$ splňující

$$\sum_{i=1}^{m} \deg f_i < n.$$

Ukažte, že pokud má soustava $f_1 = \cdots = f_m = 0$ řešení nad $\mathbb{Z}_p$, pak má nějaké další řešení nad $\mathbb{Z}_p$. (Chevalley-Warning)

Úloha 5. Nadroviny $H_1, \ldots, H_m$ v $\mathbb{R}^n$ pokrývají všechny vrcholy jednotkové hyperkrychle $\{0,1\}^n$ kromě jednoho. Dokažte $m \geq n$.

Úloha♮ 6. Mějme prvočíslo p a graf*) G, jehož vrcholy mají stupeň nejvýše $2p-1$ a průměrný stupeň ostře větší než $2p-2$. Dokažte, že z G můžeme smazáním některých hran a vrcholů vyrobit neprázdný graf G', ve kterém má každý vrchol stupeň p.

Úloha 7. Buď p prvočíslo a A podmnožina $\mathbb{Z}_p$. Ukažte nerovnost

$$\bigl|\{x + y \mid x, y \in A, x \neq y\}\bigr| \geq \min\{p, 2|A| - 3\}.$$

Úloha 8. Buď p prvočíslo a d přirozené číslo. Dokažte, že pro libovolné celé číslo k existují celá čísla $x_1, \ldots, x_d$ splňující $x_1^d + \cdots + x_d^d \equiv k \pmod{p}$.

Úloha♮ 9. Buď p prvočíslo a A množina přirozených čísel splňující, že

(i) prvky množiny A mají dohromady $p-1$ prvočíselných dělitelů,
(ii) součin prvků jakékoli neprázdné podmnožiny $X \subseteq A$ není roven p-té mocnině přirozeného čísla.

Kolik nejvýše prvků může obsahovat množina A? (IMO Shortlist 2003)

Úloha 10. Mějme prvočíslo p a množiny $S_1, \ldots, S_k$ zbytků modulo p, jež všechny obsahují 0. Předpokládejme $\sum_{i=1}^{k}(|S_i|-1) \geq p$. Ukažte, že pro libovolná $a_1, \ldots, a_k \in \mathbb{Z}_p$ má rovnice $a_1x_1 + \cdots + a_kx_k = 0$ nenulové řešení $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_k$.

Úloha 11. Mějme množiny $S_1, \ldots, S_n$ zbytků modulo prvočíslo p, dále mějme polynomy $f_1, \ldots, f_k \in \mathbb{Z}_p[x_1, \ldots, x_n]$ splňující

$$(p-1)\sum_{i=1}^{k} \deg f_i < \sum_{j=1}^{n}(|S_i| - 1).$$

Ukažte, že pokud má rovnice $f_1 = \cdots = f_k = 0$ řešení z $S_1 \times \cdots \times S_n$, pak má další takové řešení.

Úloha♮ 12. Mějme prvočíslo p, přirozené číslo n a vektory $x_1, \ldots, x_{(p-1)n+1}$ nad $\mathbb{Z}_p$. Dokažte existenci neprázdné podmnožiny $I \subseteq \{1, \ldots, (p-1)n+1\}$ splňující $\sum_{i \in I} x_i = 0$.

---

*) V grafu G dokonce můžeme povolit existenci násobných hran.

Úloha 13. Buď $G = (V, E)$ graf. Pro každý vrchol $v \in V$ máme množinu *zakázaných stupňů* $B(v)$. Dokažte:

(i) Pokud $B(v)$ obsahuje pouze kladná čísla a zároveň $\sum_{v\in V} |B(v)| < |E|$, pak lze smazáním některých hran získat podgraf H (s alespoň jednou hranou), jehož všechny vrcholy mají povolené stupně.
(ii) Pokud $B(v)$ může obsahovat i nulu a pro všechny $v \in V$ platí $|B(v)| \leq \frac{1}{2} \deg v$, tak lze smazáním některých hran získat podgraf H (klidně bez hran), jehož všechny vrcholy mají povolené stupně.

Úloha$^\natural$ **14.** Buď n přirozené číslo. Ukažte, že z každých $2n - 1$ celých čísel lze vybrat n, jejichž součet je dělitelný n.

Úloha 15. Buď p prvočíslo, d přirozené číslo a $G = (V, E)$ graf s $|V| > d(p - 1)$ vrcholy. Ukažte, že potom existuje neprázdná podmnožina vrcholů U taková, že počet klik na d vrcholech *protínajících* U je kongruentní 0 modulo p.

Úloha 16. Buď p prvočíslo a d přirozené číslo. Kolik nejméně prvků musí mít podmnožina $Y \subseteq \mathbb{Z}_p^d$, která protíná každou nadrovinu? (Brouwer-Schrijver)

Úloha 17. Buď $G = (V, E)$ **bipartitní** graf. Pro každý vrchol $v \in V$ máme dánu množinu *povolených barev* $L(v)$. Rádi bychom obarvili každý vrchol v některou barvou z $L(v)$ tak, aby sousedící vrcholy dostaly různé barvy. Předpokládejme, že hrany G lze orientovat tak, aby každý vrchol v měl vstupní stupeň $\deg_{\text{in}}(v) < |L(v)|$. Dokažte, že G lze korektně obarvit.

Úloha 18. Buď p prvočíslo, $k \leq p - 1$, a $a_1, \ldots, a_k \in \mathbb{Z}_p$ ne nutně různé zbytky. Dokažte, že pro jakékoli po dvou různé zbytky $b_1, \ldots, b_k \in \mathbb{Z}_p$ existuje permutace σ taková, že $a_1 + b_{\sigma(1)}, \ldots, a_k + b_{\sigma(k)}$ jsou také po dvou různé.

Úloha 19. Je dáno **sudé** přirozené číslo n. Mějme přirozené číslo k a vektory $v_1, \ldots, v_k \in \{\pm 1\}^n$ takové, že každý vektor $v \in \{\pm 1\}^n$ je kolmý na některý z nich. Ukažte, že nejmenší možná hodnota k je právě n.

Chevalley-Warning Theorem

Zdůrazněme nyní jednu z předchozích úloh, jejíž řešení dalo v minulém století pár matematikům celkem zabrat.

Věta (Chevalley-Warning). Mějme prvočíslo p spolu s polynomy $f_1, \ldots, f_m \in \mathbb{Z}_p[x_1, \ldots, x_n]$ splňujícími

$$\sum_{i=1}^{m} \deg f_i < n.$$

Pokud má soustava $f_1 = \cdots = f_m = 0$ nějaké řešení v $\mathbb{Z}_p^n$, pak má ještě další takové řešení. Přesněji, počet řešení této soustavy nad $\mathbb{Z}_p^n$ je násobkem p.

My většinu *Chevalley-Warningovy věty* dokázali jako důsledek *Nullstellensatz*. Mírně obecnější verze zmíněná výše ale z *Nullstellensatz* přímo nevyplývá. Přesto její důkaz není nijak přehnaně komplikovaný – jen celkem trikový.

Důkaz. Označíme-li $h = \prod_{i=1}^{m}(1 - f_i^{p-1})$, počet řešení soustavy $f_1 = \cdots = f_m = 0$ lze díky Malé Fermatově větě vyjádřit jako

$$\sum_{(a_1,\dots,a_n)\in\mathbb{Z}_p^n} h(a_1,\dots,a_n) = \sum_{(a_1,\dots,a_n)\in\mathbb{Z}_p^n} \prod_{i=1}^{m} \left(1 - f_i(a_1,\dots,a_n)^{p-1}\right).$$

Každý člen $x_1^{t_1}\cdots x_n^{t_n}$ polynomu h do výsledné sumy přispívá hodnotou

$$\sum_{(a_1,\dots,a_n)\in\mathbb{Z}_p^n} x_1^{t_1}\cdots x_n^{t_n} = \prod_{i=1}^{n} \sum_{a\in\mathbb{Z}_p} a^{t_i}.$$

Ukážeme, že ve skutečnosti každý takový člen přispívá nulou. Z podmínky ze zadání je $\deg h < n(p-1)$, takže každý člen $x_1^{t_1}\cdots x_n^{t_n}$ polynomu h obsahuje některé x_j pouze v mocnině $0 \le t_j \le p-2$. Potom ale modulo p (například z existence primitivního prvku) platí

$$\sum_{a\in\mathbb{Z}_p} a^{t_i} = 0.$$

Dle předchozí rovnosti tedy každý člen h do sumy přispívá nulou, čímž jsme hotovi. ■

Chevalley-Warningova věta je sama o sobě velmi praktickým nástrojem – a oproti *Combinatorial Nullstellensatz* je na první pohled trochu přehlednější. Ve skutečnosti už jsme mnohé její aplikace viděli – například úlohy z předešlé sekce označené symbolem ♮ (a určitě i lecjaké další) se dají alternativně přímočaře nahlédnout z naší „slabší verze“ *Chevalley-Warningovy věty.* Ukažme si nyní úlohu, ve které tuto větu použijeme v plné síle.

Úloha 20. Buď p prvočíslo a $a_1,\dots,a_{2p-1}$ zbytky modulo p. Buď b libovolný zbytek modulo p. Nahlédněte, že počet p-prvkových podmnožin $I \subset \{1,\dots 2p-1\}$, součet jejichž prvků je kongruentní číslu b modulo p, je kongruentní 0 nebo 1 modulo p.

Hilbert's Nullstellensatz

Pro dodání jistého kontextu na závěr uveďme jinou (mnohem slavnější) nullstellensatz – tu Hilbertovu, která byla zformulována přibližně o sto let dřív. Ačkoli spolu obě věty souvisí, ani jedna není přímým důsledkem druhé. *Hilbertova Nullstellensatz* sice popisuje „množiny nulujících se polynomů“ pro libovolné $S \subseteq K^n$ (tj. ne nutně hyperkrychli), ale na druhou stranu funguje pouze nad extra pěknými tělesy K (těmi algebraicky uzavřenými).

Definice. Těleso K se nazývá algebraicky uzavřené, má-li každý nekonstantní polynom v jedná proměnné $f \in K[x]$ nějaký kořen.

Věta (Základní věta algebry*)). Komplexní čísla $\mathbb{C}$ jsou algebraicky uzavřená.

*) „…která není ani základní, ani algebry“, jak říká známá anekdota.

Cvičení. Rozmyslete si, že tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$ pro prvočíslo p **nejsou** algebraicky uzavřená .

Z našich známých příkladů je tedy algebraicky uzavřené pouze $\mathbb{C}$. Ačkoli je tento fakt obecně známý, důkaz vyžaduje netriviální práci.

Věta (Hilbert's Nullstellensatz). Buď K algebraicky uzavřené těleso, $G \subseteq K[x_1, \ldots, x_n]$ množina polynomů. Označme $V(G) \subseteq K^n$ množinu jejich společných nul. Pro libovolný polynom $f \in K[x_1, \ldots, x_n]$ je potom ekvivalentní:

(i) f se nuluje na celé množině $V(G)$,).
(ii) Existují $m, k \in \mathbb{N}$, pro které se dá f^m zapsat jako $f^m = f_1 g_1 + \cdots + f_k g_k$ pro vhodné $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ a $g_1, \ldots, g_n \in G$.

Cvičení. Všimněte si, že z předchozí věty třeba vyplývá:
Jsou-li $g_1, \ldots, g_k \in \mathbb{C}[x_1, \ldots, x_n]$ takové komplexní polynomy, že soustava rovnic $g_1 = \cdots = g_k = 0$ nemá řešení v $\mathbb{C}$, tak už nutně existují polynomy $h_1, \ldots, h_k \in \mathbb{C}[x_1, \ldots, x_n]$ splňující

$$h_1 g_1 + \cdots + h_n g_n = 1.$$

Literatura a zdroje

Úlohy z příspěvku jsou poměrně standardní a provařené (a upřímně je celkem těžké najít víc „olympiádních“ použití této metody). Většina příspěvku je převzatá z přehledné kapitolky v [1]. Pro další aplikace se dá podívat na původní článek [2]. Pro širší algebraický kontext lze použít článek [3].

[1] Titu Andreescu, Gabriel Dospinescu; *Problems from the Book*, XYZ Press
[2] Noga Alon; *Combinatorial Nullstellensatz*, 1999
[3] Terence Tao; *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, 2014
[4] Evan Chen; *Combinatorial Nullstellensatz*, Berkley Math Circle, 2013
[5] Robert Šámal; *Kombinatorika a grafy III*, přednáška, 2018
[6] Štěpán Šimsa; *Combinatorial Nullstellensatz*, Sborník *i*KS, 2013

Hinty

Hint 1. Použijte Nullstellensatz na polynom $\prod_{i=1}^{100}(x_i - x_{i+1}) \in \mathbb{Q}[x_1, \ldots, x_{100}]$, kde do každého S_i dosazujeme dvě různá čísla. Využijte sudost čísla 100.

Hint 2. Vyjde $m = 3n$. Kdyby $m < 3n$, vynásobte lineární rovnice všech příslušných rovin a nakonec odečtěte vhodný skalární násobek $\prod_{j=1}^{n}(x-j) \cdot \prod_{j=1}^{n}(y-j) \cdot \prod_{j=1}^{n}(z-j)$.

Hint 3. Kdyby platila opačná nerovnost, vezměte polynom $\prod_{c \in A+B}(x+y-c)$, který se nuluje na $A \times B$.

Hint 4. Při vybírání polynomu použijte Malý Fermatův fígl – pro všechna $x \in \mathbb{Z}_p$ platí: $x = 0$, právě když $\left(x^{p-1} - 1\right) \neq 0$. Použijte fígl, vynásobte všech m věcí dohromady, nakonec opravte triviální nenulu přičtením vhodného polynomu vyššího stupně $(p-1)n$.

Hint 5. Kdyby $m < n$, vynásobte rovnice rovin dohromady a přičtením polynomu stupně n opravte zbylou nenulu.

Hint 6. Každé hraně e přiřaďte jednu proměnnou x_e, do které budeme chtít dosazovat $\{0, 1\}$; pro každý vrchol pak s pomocí Malého Fermata napište jednu rovnici. Všimněte si nulového (ne)řešení.

Hint 7. Vynásobte $(x+y-c)$ přes všechna c jako na levé straně nerovnosti. Kde všude se nuluje polynom $(x-y)$? Buďte opatrní při ověřování předpokladů Nullstellensatz.

Hint 8. S pomocí řádů búno mějmte $d \mid p-1$. Polynom $\left(x_1^d + \cdots + x_d^d - k\right)^{p-1} - 1$ společně s Malým Fermatovým fíglem pak postačí.

Hint 9. Vyjde $(p-1)^2$, konstrukce je jasná. Čísla z A odpovídají vektorům délky $p-1$. Kdyby $|A| \geq (p-1)^2 + 1$, uvažte $|A|$ proměnných s hodnotami v $\{0, 1\}$. Napište s Malým Fermatem pro každé z daných prvočísel rovnici stupně $p-1$, jejichž součin se nuluje právě když platí druhá podmínka. Přičtením vhodného polynomu stupně $|A|$ opravte triviální nenulu.

Ve skutečnosti lze zapomenout na první podmínku a číslo $p-1$ nahradit obecným d. Stejný postup pak dává výsledek $d(p-1)$.

Hint 10. Vezměte $(a_1x_1 + \cdots + a_kx_k)^{p-1} - 1$ a odečtěte polynom stupně $\sum_{i=1}^{k}(|S_i| - 1)$ tak, aby se výsledek nuloval na celém $S_1 \times \cdots \times S_k$.

Hint 11. Kdyby to tak nebylo, vezměte polynom $\prod_{i=1}^{k}(1 - f_i^{p-1})$ a opravte jeho jediné neřešení odečtením vhodného polynomu stupně $\sum_{j=1}^{n}(|S_i| - 1)$.

Hint 12. Kdyby to tak nebylo, v každé z n složek s pomocí Malého Fermata napište jednu rovnici, vynásobte, pak přičtením opravte triviální nenulu.

Hint 13.

(i) Pro každou hranu e vezměte jednu proměnnou x_e, pro každý vrchol v napište $|B(v)|$ lineárních rovnic, které se nemají nulovat. Opravte triviální (ne)řešení.

(ii) Vezměte polynom stupně $\sum_{v \in V} |B(v)|$ ze začátku předchozí části. Hledejte vhodný nenulový „vedoucí“ koeficient. Může se hodit buď Hallova věta, nebo vhodná orientace grafu.

Hint 14. Pro n prvočíslo použijte *Chevalley-Warningovu větu* společně s Malým Fermatem. Pak ukažte, že dokazovaná vlastnost se dědí z činitelů na součin.

Hint 15. Pro každý vrchol $v \in V$ představte proměnnou x_v, která bude nabývat hodnot z $\{0, 1\}$ podle toho, zda $x \in U$ nebo $x \notin U$. Pro každou d-kliku v G napište polynom stupně d, který se po dosazení dává 1 či 0 v závislosti na tom, zda klika protíná U či nikoli. Pak sečtěte tyto polynomy přes všechny d-kliky a pomocí Malého Fermata vyrobte polynom stupně $d(p-1)$, který je nenulový právě pro hledaná U. Opravte triviální (ne)řešení.

Hint 16. Odpověď je $d(p-1)+1$, pro konstrukci stačí vzít „souřadnicové přímky". Pro spor ať $|Y| = d(p-1)$, BÚNO obsahuje Y počátek o. Pak $Y' = Y \setminus \{o\}$ protíná každou nadrovinu s rovnicí $a_1y_1+\cdots+a_dy_d = 1$, kde $a_1,\ldots,a_d$ nejsou všechny nulové, tj. polynom $\prod_{(y_1,\ldots,y_n)\in Y'}(x_1y_1+\cdots+x_dy_d) \in \mathbb{Z}_p[x_1,\ldots,x_d]$ se nuluje všude kromě počátku.

Hint 17. Pro každý vrchol $v \in V$ vezměte jednu proměnnou nabývající hodnot z $L(v)$, graf zorientujte a uvažte $\prod_{(u,v)\text{ hrana}}(x_u - x_v)$. Pro použití *Nullstellensatz* teď stačí ukázat, že koeficient u $\prod_{v\in V} x_v^{\deg_{\mathrm{in}}(v)}$ je nenulový. Každá orientace grafu G se stejnými vstupními a výstupními stupni do tohoto koeficientu přispěje ±1, kde znaménko závisí na tom, kolik hran je třeba otočit. S pomocí Eulerovských tahů nahlédněte, že v případě bipartitního grafu je to vždy $+1$.

Hint 18. Vezměte $B = \{b_1,\ldots,b_k\}$ a proměnné $x_1,\ldots,x_k$. Kdyby tvrzení neplatilo, polynom

$$\prod_{1\le i<j\le k}(x_i - x_j)\cdot\prod_{1\le i<j\le k}(x_i - x_j + a_i - a_j)$$

by se nuloval na hyperkrychli $B^k \subseteq \mathbb{Z}_p^k$. Dokažte, že koeficient u $x_1^{k-1}\cdots x_k^{k-1}$ je $k!$.

Hint 19. Kdo to dořeší, dostane čokoládku.

Hint 20. Vezměte $2p-1$ proměnných, uvažte rovnice $\sum_{i=1}^{2p-1} x_i^{p-1} = 0$ a $\sum_{i=1}^{2p-1} x_i^{p-1}a_i$. Jak souvisí počet jejich společných řešení s hledaným počtem podmnožin I?