Combinatorial Nullstellensatz

Tomasz Kochanek

Nazwa tytułowego twierdzenia, które można w zasadzie uznać za pewną metodę, czy nawet filozofię, dowodzenia twierdzeń z kombinatoryki algebraicznej, pochodzi od nazwy słynnego rezultatu Hilberta.

Nullstellensatz Hilberta. *Załóżmy, że $\mathbb{F}$ jest ciałem algebraicznie domkniętym. Niech $P, Q_1, \ldots, Q_k \in \mathbb{F}[x_1, \ldots, x_n]$ będą takimi wielomianami n zmiennych o współczynnikach z ciała $\mathbb{F}$, że $P(a_1, \ldots, a_n) = 0$ dla każdego $(a_1, \ldots, a_n) \in \mathbb{F}^n$ spełniającego równości $Q_j(a_1, \ldots, a_n) = 0$ dla $1 \leqslant j \leqslant n$. Wówczas istnieją: liczba naturalna ℓ oraz wielomiany $R_1, \ldots, R_k \in \mathbb{F}[x_1, \ldots, x_n]$, dla których zachodzi równość*

$$P^\ell = R_1 Q_1 + \ldots + R_k Q_k.$$

Jest to mocniejszy wariant tzw. słabej wersji Nullstellensatz, która mówi, że dla każdego **właściwego** ideału $\mathscr{I} \subset \mathbb{F}[x_1, \ldots, x_n]$ pierścienia wielomianów n zmiennych nad algebraicznie domkniętym ciałem $\mathbb{F}$ zbiór

$$V(\mathscr{I}) = \Big\{(a_1, \ldots, a_n) \in \mathbb{F}^n : P(a_1, \ldots, a_n) = 0 \text{ dla każdego } P \in \mathscr{I}\Big\}$$

(nazywany zbiorem zer ideału $\mathscr{I}$) jest niepusty. Równoważne jej sformułowanie brzmi: jeżeli $\mathscr{I} \subset \mathbb{F}[x_1, \ldots, x_n]$ jest ideałem oraz $V(\mathscr{I}) = \emptyset$, to $\mathscr{I} = \mathbb{F}[x_1, \ldots, x_n]$. Stwierdzenie to wynika bezpośrednio z zacytowanej mocnej wersji Nullstellensatz. Istotnie, każdy ideał $\mathscr{I} \subset \mathbb{F}[x_1, \ldots, x_n]$ jest skończenie generowany*– powiedzmy, że przez wielomiany $Q_1, \ldots, Q_k$ – więc wystarczy zastosować Nullstellensatz dla tych właśnie wielomianów oraz wielomianu $P = 1$. Jeżeli Q_i nie mają wspólnego zera (czyli $V(\mathscr{I}) = \emptyset$), to wielomian stale równy 1 należy do $\mathscr{I}$, a zatem $\mathscr{I} = \mathbb{F}[x_1, \ldots, x_n]$.

Kombinatoryczne wersje twierdzenia o zerach zawdzięczamy głównie pracom [4], [2], [3]. W pracy [1] Alon zaproponował następujące sformułowanie:

Combinatorial Nullstellensatz. *Niech $P \in \mathbb{F}[x_1, \ldots, x_n]$ będzie wielomianem n zmiennych o współczynnikach z ciała $\mathbb{F}$. Załóżmy, że stopień $\deg P = N \geqslant 1$, przy czym dla pewnych liczb całkowitych nieujemnych $k_1, \ldots, k_n$, spełniających $\sum_{i=1}^n k_i = N$, współczynnik stojący przy jednomianie $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ jest niezerowy. Jeżeli zbiory $A_1, \ldots, A_n \subset \mathbb{F}$ spełniają $|A_i| > k_i$ dla $1 \leqslant i \leqslant n$, to istnieje taki punkt $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$, że $P(a_1, \ldots, a_n) \neq 0$.*

Aby zobaczyć związek między kombinatoryczną wersją Nullstellensatz a jej wersją oryginalną, przyjmijmy w twierdzeniu Hilberta $k = n$ oraz zdefiniujmy wielomiany $Q_1, \ldots, Q_n$ jako wielomiany jednej zmiennej:

$$Q_j(x_1, \ldots, x_n) = \prod_{a \in A_j} (x_j - a) \text{ dla } 1 \leqslant j \leqslant n.$$

Zaprzeczenie tezy Combinatorial Nullstellensatz to stwierdzenie, że wielomian P zeruje się w każdym wspólnym zerze wielomianów $Q_1, \ldots, Q_n$, czyli – w zbiorze $A_1 \times \ldots \times A_n$. Twierdzenie Hilberta nie pozwala jednak na proste wyprowadzenie wersji kombinatorycznej. Z dwóch powodów: po pierwsze – zakładamy w nim, że ciało $\mathbb{F}$ jest algebraicznie

*Z twierdzenia Hilberta o bazie wynika, że jeżeli $\mathbb{F}$ jest dowolnym ciałem, to pierścień wielomianów $\mathbb{F}[x_1, \ldots, x_n]$ jest *noetherowski*, tzn. każdy jego ideał jest skończenie generowany (zobacz np. §2.4 w książce: J. Browkin, *Teoria ciał*, PWN Warszawa 1977).

domknięte*; po drugie – daje ono reprezentację $P^\ell = \sum_{j=1}^n R_j Q_j$ z pewnym wykładnikiem $\ell \in \mathbb{N}$, potencjalnie większym od 1. Gdyby wiedzieć, że można przyjąć $\ell = 1$, dostalibyśmy sprzeczność niemal natychmiast: jeżeli w wielomianie P ma się pojawić jednomian $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$, to któryś z wielomianów R_j musi go zawierać, ewentualnie bez czynnika $x_j^{k_j}$; wtedy jednak w wielomianie P pojawiłby się jednomian zbyt wysokiego stopnia. Okazuje się, że w przypadku wielomianów Q_j o tej specjalnej postaci, zdefiniowanej wyżej, można opuścić zarówno założenie o algebraicznej domkniętości ciała $\mathbb{F}$, jak i pominąc wykładnik ℓ (zobacz [1, Theorem 1.1]).

My zajmiemy się zacytowaną powyżej wersją Combinatorial Nullstellensatz i zaprezentujemy elegancki, zwięzły dowód, pochodzący z pracy [6]. Dowód czysto algebraiczny, wykorzystujący elementy teorii ideałów, i przypominający standardowy dowód twierdzenia Hilberta o zerach, można znaleźć w artykule [10].

Dowód. Zastosujmy indukcję względem stopnia $\deg P = N$. Dla $N = 1$ teza jest (niemal) oczywista, więc załóżmy, że $N > 1$ i że teza zachodzi pod stosownymi założeniami dla wszelkich wielomianów P o stopniu mniejszym od N.

Bez straty ogólności przyjmijmy, że $k_1 \geqslant 1$, a zatem $|A_1| \geqslant 2$. Wybierzmy dowolnie $a_0 \in A_1$. Stosując zwykły algorytm dzielenia wielomianów**, dzielimy $P(x_1, \ldots, x_n)$ przez $x_1 - a_0$, otrzymując takie wielomiany Q i R, że

$$P(x_1, \ldots, x_n) = (x_1 - a_0)Q(x_1, \ldots, x_n) + R(x_2, \ldots, x_n).$$

Wielomian R, jak zaznaczono w powyższej równości, nie zależy od zmiennej x_1, jako że – zgodnie z procedurą dzielenia wielomianów – jego stopień, jako wielomianu zmiennej x_1, jest mniejszy od stopnia dzielnika $x_1 - a_0$, a zatem – równy zeru.

Przypuśćmy, wbrew tezie, że dla dowolnego $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$ mamy $P(a_1, \ldots, a_n) = 0$. Teraz prosty i efektowny trick. Podstawiając do powyższej równości punkt $(a_0, a_2, \ldots, a_n)$, otrzymamy równość $R(a_2, \ldots, a_n) = 0$, prawdziwą dla dowolnego $(a_2, \ldots, a_n) \in A_2 \times \ldots \times A_n$. Teraz zaś podstawmy $(a_1, a_2, \ldots, a_n) \in A_1 \setminus \{a_0\} \times A_2 \times \ldots \times A_n$; otrzymamy:

$$0 = P(a_1, a_2, \ldots, a_n) = \underbrace{(a_1 - a_0)}_{\neq 0} Q(a_1, a_2, \ldots, a_n) + 0.$$

Pokazuje to, że

$$Q(a_1, a_2 \ldots, a_n) = 0 \text{ dla } (a_1, a_2, \ldots, a_n) \in A_1 \setminus \{a_0\} \times A_2 \times \ldots \times A_n.$$

Jednak wielomian Q ma stopień równy $N-1$ i niezerowy współczynnik przy jednomianie $x_1^{k_1-1} x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}$. Sprzeczność z założeniem indukcyjnym. ■

*Nullstellensatz Hilberta nie zachodzi dla ciał, które nie są algebraicznie domknięte, na co wskazuje banalny przykład ideału $\mathscr{I} = (x^2 + 1) \subset \mathbb{R}[x]$, generowanego przez wielomian $x^2 + 1$. W tym przypadku $V(\mathscr{I}) = \emptyset$, ale oczywiście $\mathscr{I} \subsetneq \mathbb{R}[x]$. Założenie algebraicznej domkniętości przy Combinatorial Nullstellensatz byłoby bolesną restrykcją, często bowiem stosujemy je w przypadku ciał $\mathbb{Z}_p$, które algebraicznie domknięte nie są (ciało algebraicznie domknięte musi być nieskończone).

**Wielomiany z $\mathbb{F}[x_1, \ldots, x_n]$ traktujemy tu jak wielomiany jednej zmiennej x_1, ale o współczynnikach z pierścienia $\mathbb{F}[x_2, \ldots, x_n]$, który to jest pierścieniem całkowitym. Zwykły algorytm dzielenia wielomianów daje się przeprowadzić, o ile tylko najstarszy współczynnik dzielnika jest odwracalny w tym pierścieniu, a tak w naszej sytuacji jest, gdyż dzielnikiem jest wielomian $x_1 - a_0$. Formalny dowód poprawności takiego algorytmu można znaleźć np. w §5.2 książki: A.I. Kostrykin, *Wstęp do algebry*, tom 1 (*Podstawy algebry*), PWN Warszawa 2004.

Poniższa lista zadań stanowi ilustrację efektownych zastosowań kombinatorycznej wersji twierdzenia o zerach. Niektóre są dokładnie omówione w [7] i [8]. O związkach Combinatorial Nullstellensatz z teorią grafów można poczytać w [5]. Szerokie omówienie zagadnień addytywnej teorii liczb, związanych z zadaniami 2a i 2b, można znaleźć w książce [9] (rozdziały 5 i 9).

Zadanie 1 (IMO 2007). Niech n będzie liczbą naturalną. Rozważmy zbiór

$$S = \Big\{(x, y, z) : x, y, z \in \{0, 1, \ldots, n\} \text{ oraz } x + y + z > 0\Big\}$$

złożony z $(n + 1)^3 - 1$ punktów w przestrzeni trójwymiarowej. Wyznaczyć najmniejszą możliwą liczbę płaszczyzn, których suma pokrywa zbiór S, ale nie zawiera punktu $(0, 0, 0)$.

Wskazówka. Łatwo podać ograniczenie górne. Jeżeli zaś płaszczyzny $a_i x + b_i y + c_i z = d_i$ (dla $1 \leqslant i \leqslant k$) pokrywają zbiór S, to narzucający się wielomian $P(x, y, z) = \prod_{i=1}^{k}(a_i x + b_i y + c_i z - d_i)$ nie jest dobry z dwóch powodów: nie „koduje" w żaden sposób tego, że punkt $(0, 0, 0)$ ma nie należeć do sumy płaszczyzn oraz nie ma gwarancji, że znajdziemy jednomian najwyższego stopnia o odpowiedniej postaci. Należy naprawić tę sytuację, dodając do $P(x, y, z)$ stosowny wielomian.

Zadanie 2a (twierdzenie Cauchy'ego – Davenporta). Niech p będzie liczbą pierwszą oraz $A, B \subset \mathbb{Z}_p$. Pokazać, że

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}.$$

Wskazówka. Rozważyć dwa przypadki: gdy prawa strona nierówności wynosi p oraz gdy wynosi $|A| + |B| - 1$. W drugim przypadku rozumować nie wprost i rozważyć wielomian $P(x, y) \in \mathbb{Z}_p[x, y]$ dany wzorem $P(x, y) = \prod_{d \in D}(x + y - d)$, gdzie $D \subset \mathbb{Z}_p$ jest takim zbiorem (hipotetycznie istniejącym), że $A + B \subset D$ oraz $|D| = |A| + |B| - 2$.

Zadanie 2b (hipoteza Erdösa – Heilbronna). Niech p będzie liczbą pierwszą oraz $A, B \subset \mathbb{Z}_p$. Oznaczmy $C = \{a + b \in \mathbb{Z}_p : a \in A, b \in B, a \neq b\}$. Pokazać, że

$$|C| \geqslant \min\{p, |A| + |B| - 3\}.$$

Wskazówka. Postępować podobnie jak w poprzednim zadaniu; z uwagi na warunek $a \neq b$ pojawiający się w definicji zbioru C, należy zmienić definicję wielomianu $P(x, y)$, wprowadzając czynnik $x - y$.

Uwaga. Była to hipoteza sformułowana przez Erdösa i Heilbronna w Acta Arithmetica w 1964 roku (oryginalnie dla $A = B$), którą udowodnili pierwsi da Silva i Hamidoune w 1994 roku, stosując teorię reprezentacji grup. Zadziwiające jest to jak bardzo wzrasta stopień trudności (w stosunku do twierdzenia Cauchy'ego–Davenporta, którego dowód znany był już od publikacji Cauchy'ego z roku 1813) po dołożeniu w definicji zbioru C warunku $a \neq b$. Zbiory tego typu nazywane są w addytywnej teorii liczb *restricted sum sets*. W pracach Alona, Nathansona i Ruzsy [2], [3] pokazano skuteczność metody wielomianowej w dowodzie hipotezy Erdősa–Heilbronna, jak i w dowodach szeregu twierdzeń pokrewnych.

Zadanie 3 (twierdzenie Erdösa – Ginzburga – Ziva). Niech n będzie liczbą naturalną. Udowodnić, że spośród dowolnych $2n - 1$ liczb całkowitych można wybrać n, których suma jest podzielna przez n.

Wskazówka. Udowodnić twierdzenie najpierw dla liczb pierwszych, a dalej przez indukcję. Niech $a_1 \leqslant \ldots \leqslant a_{2p-1}$. Jeżeli $a_i = a_{i+p-1}$ dla pewnego $1 \leqslant i \leqslant p$, to teza zachodzi (dlaczego?); jeżeli nie – zastosować wielokrotnie twierdzenie Cauchy'ego–Davenporta dla zbiorów $A_i = \{a_i, a_{i+p-1}\}$.

Zadanie 4 (twierdzenie Chevalleya – Warninga). Niech p będzie liczbą pierwszą, $k, n \in \mathbb{N}$ i niech $P_1, \ldots, P_k \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Załóżmy, że $\sum_{i=1}^{k} \deg(P_i) < n$. Pokazać, że jeżeli wielomiany $P_1, \ldots, P_k$ mają choć jeden wspólny pierwiastek, to mają przynajmniej dwa wspólne pierwiastki.

Wskazówka. Niech $(c_1, \ldots, c_n) \in \mathbb{Z}_p^n$ będzie wspólnym zerem wielomianów P_j. Rozważyć wielomian

$$Q(x_1, \ldots, x_n) = \prod_{j=1}^{k} \Big(1 - P_j(x_1, \ldots, x_n)^{p-1}\Big) - \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}_p, c \neq c_j} (x_j - c),$$

gdzie $\delta \in \mathbb{Z}_p$ jest dobrane tak, aby $Q(c_1, \ldots, c_n) = 0$. Pamiętać o małym twierdzeniu Fermata.

Uwaga. Sugerowany dowód pochodzi z [1] (Theorem 3.1). Oryginalne brzmienie twierdzenia Chevalleya–Warninga jest silniejsze: jeżeli V jest zbiorem wszystkich wspólnych zer wielomianów P_i (takich, jak wyżej), to $|V| \equiv 0 \,(\mathrm{mod}\, p)$. Jeszcze ogólniejsza wersja funkcjonuje dla dowolnego ciała skończonego $\mathbb{F}$ w miejscu $\mathbb{Z}_p$, przy czym ostatnia kongruencja zmieniona jest wtedy na $|V| \equiv 0 \,(\mathrm{mod}\, \mathrm{char}\mathbb{F})$; zobacz: [9, Theorem 9.24].

Zadanie 5 (Alon [1, Theorem 6.1]). Niech p będzie liczbą pierwszą i niech $X = (V, E)$ będzie grafem*, dla którego średni stopień wierzchołka jest większy niż $2p - 2$, a maksymalny stopień wierzchołka wynosi $2p - 1$, tzn.

$$\frac{1}{|V|} \sum_{v \in V} \deg(v) > 2p - 2 \quad \text{oraz} \quad \max_{v \in V} \deg(v) = 2p - 1,$$

gdzie $\deg(v) = |\{e \in E : e \sim v\}|$, a symbol $e \sim v$ oznacza, że jednym z końców krawędzi e jest wierzchołek v. Wykazać, że X zawiera p-regularny podgraf, tzn. podgraf, w którym stopień każdego wierzchołka jest jednakowy i wynosi p.

Wskazówka. Dla każdej krawędzi $e \in E$ niech x_e będzie zmienną z nią stowarzyszoną. Rozważyć następujący wielomian $P \in \mathbb{Z}_p[(x_e)_{e \in E}]$ o $|E|$ zmiennych:

$$P((x_e)_{e \in E}) = \prod_{v \in V} \Big(1 - \Big(\sum_{e \sim v} x_e\Big)^{p-1}\Big) - \prod_{e \in E} (1 - x_e).$$

Zadanie 6 (Alon [1, Lemma 8.1]). Niech $A = (a_{ij})$ będzie macierzą wymiaru $n \times n$ o elementach z ciała $\mathbb{F}$. *Permanent* macierzy A definiujemy wzorem

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)},$$

gdzie S_n oznacza zbiór wszystkich permutacji zbioru $\{1, \ldots, n\}$. Załóżmy, że $\mathrm{Per}(A) \neq 0$. Pokazać, że dla każdego wektora $\boldsymbol{y} \in \mathbb{F}^n$ oraz dowolnej rodziny zbiorów $S_1, \ldots, S_n \subset \mathbb{F}$, z których każdy ma dokładnie 2 elementy, istnieje taki wektor $\boldsymbol{x} \in S_1 \times \ldots \times S_n$, że $A\boldsymbol{x}$ różni się od $\boldsymbol{y}$ na każdej współrzędnej.

Wskazówka. Odpowiednio dobrany wielomian powinien być stopnia n ze współczynnikiem przy $x_1 \cdot \ldots \cdot x_n$ równym $\mathrm{Per}(A) \neq 0$.

*Rozważamy tu grafy nieskierowane i bez pętli.

Literatura

[1] N. Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing **8** (1999), 7–29.

[2] N. Alon, M.B. Nathanson, I. Ruzsa, *Adding distinct congruence classes modulo a prime*, American Mathematical Monthly **102** (1995), 250–255.

[3] N. Alon, M.B. Nathanson, I. Ruzsa, *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory **56** (1996), 404–417.

[4] N. Alon, M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica **9** (1989), 393–395.

[5] T. Bartnicki, *Combinatorial Nullstellensatz, czyli o algebrze w kombinatoryce*, Matematyka, Społeczeństwo, Nauczanie **38** (2007), 14–18.

[6] M. Michałek, *A short proof of Combinatorial Nullstellensatz*, American Mathematical Monthly **117** (2010), 821–823.

[7] T.J. Mildorf, *Olympiad number theory: An abstract perspective*, online: `http://www.artofproblemsolving.com/Resources/Papers/MildorfNT.pdf`

[8] J. Steinhardt, *Algebraic combinatorics*, online: `http://activities.tjhsst.edu/vmt/wiki/images/a/ad/AlgebraicCombo.pdf`

[9] T. Tao, V.H. Vu, *Additive combinatorics*, Cambridge Studies in Advance Mathematics, vol. **105**, Cambridge University Press 2006.

[10] N.K. Vishnoi, *An algebraic proof of Alon's Combinatorial Nullstellensatz*, Congressus Numerantium **152** (2001), 89–91.