Combinatorial Nullstellensatz

Jędrzej Kula

08 kwietnia 2021

Theoretical Computer Science
Jagiellonian University

Spis treści

Twierdzenie

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

$$P^l = R_1 Q_1 + \cdots + R_k Q_k$$

Twierdzenie

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

Wielomiany P w obu twierdzeniach odpowiadają sobie, przyjmujemy, że $k = n$ i wielomiany $Q_1, \dots, Q_n$ z twierdzenia 1 definiujemy jako wielomiany jednej zmiennej:

$$Q_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Następnie zakładamy, że wielomian $P \neq 0$ zeruje się na zbiorze $S_1 \dots S_n$, który jest tutaj jednocześnie zbiorem wszystkich wspólnych zer wielomianów $Q_1, \dots, Q_n$, co jednak prowadzi do konkluzji, że $P = 0$ i w efekcie do sprzeczności. Warto również zauważyć, że w twierdzeniu 2 nie trzeba zakładać algebraicznej domkniętości ciała F.

Spis treści

Induckcja po stopniu wielomianu P.

Induckcja po stopniu wielomianu P.

1. Dla $deg(P) = 1$ trywialne.

Induckcja po stopniu wielomianu P.

1. Dla $deg(P) = 1$ trywialne,
2. Dla $deg(P) > 1$ dowód nie wprost - wielomian zeruje się w każdym punkcie.

Dowód dla $deg(P) > 1.$
Bez strat ogólności możemy założyć, że potęga $k_1 > 0$. Wybierzmy zatem $a \in A_1$ oraz zapiszmy:

$$P = (x_1 - a)Q + R.$$

Możemy zauważyć, że R nie jest zależny zmiennej x_1. Z założen wynika więc, że Q posiada jednomian $x_1^{k_1} \dots x_n^{k_n}$ o niezerowym współczynniku oraz $deg(Q) = deg(P) - 1.$

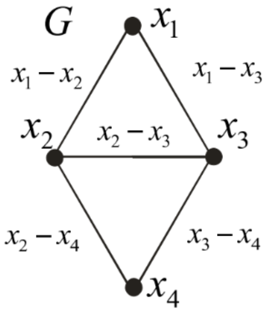
Dowód dla $deg(P) > 1$.
Weźmy więc teraz dowolny $x \in a \times A_2 \times \cdots \times A_n$ oraz podstawmy do naszego równania. Z założenia, że $P(x) = 0$, wynika że $R(x)$ również musi być równe 0. Jednakże R nie jest zależne od x_1 z czego wynika, że zeruje się również na każdym elemencie $(A_1 - \{a\}) \times A_2 \times \cdots \times A_n$. Podstawmy zatem do równania dowolne $x \in (A_1 - \{a\}) \times A_2 \times \cdots \times A_n$. Skoro $x_1 - a$ ma wartość różną od 0, to $Q(x) = 0$. Jest to sprzeczność z założeniem indukcyjnym dla Q.

Spis treści

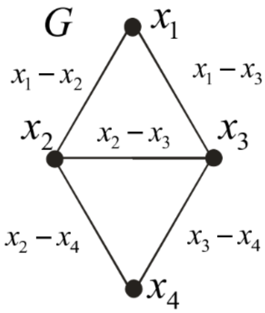
Definicja wielomianu f_G dla grafu G:
Każdemu wierzchołkowi v_i możemy przypisać zmienną x_i,a następnie stworzyć iloczyn różnic zmiennych na końcach każdej krawędzi:

$$f_G(x_1, \dots, x_n) = \prod_{i<j, \{v_i, v_j\} \in E} (x_i - x_j).$$

$$f_G(x_1, \dots, x_n) = \prod_{i<j, \{v_i, v_j\} \in E} (x_i - x_j)$$



$$f_G(x_1, \dots, x_n) = \prod_{i<j, \{v_i, v_j\} \in E} (x_i - x_j)$$



$$f_G(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

$$f_G(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

Możemy zauważyc, że w f_G istnieje jednomian $-x_1 x_2 x_3^2 x_4$. Dzięki tej obserwacji i aplikacji Combinatorial Nullstellensatz możemy zauważyć, że graf ten można pokolorować trzema kolorami.

Spis treści

Twierdzenie

Niech p będzie liczbą pierwszą, A oraz B niepustymi podzbiorami $\mathbb{Z}_p$. Niech

$$C = \{x \in \mathbb{Z}_p\colon x = a + b dla pewnych a \in A, b \in B, a \neq b\},$$

wtedy

$$|C| \geq min(p, |A| + |B| - 3)$$

Możemy założyć, że $p > 2$.
Jeżeli $min(p, |A| + |B| - 3) = p$ to dla dowolnego $g \in \mathbb{Z}_p$ zbiory A i $g - B$ mają co najmniej dwa wspólne elementy. Weźmy teraz $a \in A, a \neq \frac{g}{2}$. Wtedy $g = a + b$ dla pewnego $b \in B$. Z tego wynika, że $g \in C$, więc $C = \mathbb{Z}_p$.

Jeżeli $min(p, |A| + |B| - 3) < p$ oraz twierdzenie nie jest prawdziwe, istnieje wtedy zbiór $D \subseteq C$ oraz $|D| = |A| + |B| - 4$. Zdefiniujmy następująco dwa wielomiany

$$P(x, y) = \prod_{d \in D} (x + y - d) \text{ i } Q(x, y) = P(x, y)(x - y).$$

Zauważmy, że $P(a, b) = 0$ dla dowolnego $a \in A, b \in B, a \neq b$, zatem $Q(a, b) = 0$ dla dowolnego $a \in A, b \in B$. Zauważmy, że współczynnik przy $x^i y^j$ w $P(x, y)$ jest równy $\binom{|D|}{i}$ jeżeli $i + j = |D|$. Jeżeli więc $i + j = |D| + 1$, to współczynnik przy $x^i y^j$ w $Q(x, y)$ jest równy $\binom{|D|}{i-1} - \binom{|D|}{i}$, co natomiast jest równe 0 wtedy i tylko wtedy, gdy $i = \frac{|D|+1}{2}$ w $\mathbb{Z}_p$. Jednakże skoro $|D| + 1 = |A| + |B| - 3$ to jeden z współczynników przy $x^{|A|-1} y^{|B|-2}$ lub $x^{|A|-2} y^{|B|-1}$ jest niezerowy. Używając więc Twierdzenia 1 oraz faktu, że $deg(Q) = |A| + |B| - 3$ otrzymujemy sprzeczność.