Wielowymiarowe uogólnienie twierdzenia Bezouta

Tomasz OSMAN

(Niniejszy artykuł jest skróconą wersją pracy Autora nagrodzonej złotym medalem w Konkursie Uczniowskich Prac z Matematyki. Skrót został dokonany przez redakcję.)

Zdarza się, że rozmaite zależności (o charakterze geometrycznym) między wektorami lub innymi obiektami matematycznymi dają się zapisać w postaci $W(x_1,\ldots,x_n)=0$, gdzie W jest wielomianem n zmiennych rzeczywistych. Na przykład, aby dwie proste były prostopadłe, ich współczynniki kierunkowe muszą spełniać zależność $a_1a_2+1=0$. Często mamy do czynienia z sytuacją, że w postaci algebraicznej zapisane są dwa różne warunki:

$$W_1(x_1,\ldots,x_n)=0 \qquad \text{oraz} \qquad W_2(x_1,\ldots,x_n)=0,$$

i wiadomo skądinąd, że jeden z tych warunków implikuje drugi (tzn. jeśli $W_1(x_1,\ldots,x_n)=0$, to i $W_2(x_1,\ldots,x_n)=0$). Okazuje się, że wtedy, przy pewnych dodatkowych założeniach, zachodzi prosty związek między wielomianami W_1 i W_2.

Według przyjętej w artykule definicji wielomianu nierozkładalnego, każda stała jest takim wielomianem. Nie wpływa to źle na wyniki Autora, ale warto odnotować, że w ten sposób traci się jednoznaczność rozkładu wielomianu na wielomiany nierozkładalne.

Przez $\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ (odp. $\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_{n-1}}]$) oznaczymy pierścień wielomianów n zmiennych $x_1,\ldots,x_n$ (odp. $(n-1)$ zmiennych $x_1,\ldots,x_{n-1}$) o współczynnikach rzeczywistych. W dalszym ciągu będziemy wykorzystywać fakt, że wielomiany z każdego z tych pierścieni można jednoznacznie rozłożyć na czynniki „pierwsze”, tzn. przedstawić w postaci iloczynu wielomianów nierozkładalnych. Wielomian nierozkładalny to taki, który nie jest iloczynem dwóch innych niższego stopnia. Na przykład, dla $n=1$ nierozkładalny w pierścieniu $\mathbf{R}[\mathbf{x}]$ jest wielomian x^2+1, wielomian zaś x^4+1 jest iloczynem dwóch wielomianów nierozkładalnych:

$$x^4+1=(x^2-x\sqrt{2}+1)\cdot(x^2+x\sqrt{2}+1).$$

Twierdzenie. *Załóżmy, że wielomian $W_1\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ jest nierozkładalny i przyjmuje zarówno wartości dodatnie, jak i ujemne. Jeśli wielomian $W_2\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ ma tę własność, że dla wszystkich $(x_1,\ldots,x_n)$*

$$W_1(x_1,\ldots,x_n)=0 \implies W_2(x_1,\ldots,x_n)=0,$$

to istnieje taki wielomian $G\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$, że $W_2=G\cdot W_1$.

Dla wielomianów jednej zmiennej powyższe twierdzenie wynika łatwo z twierdzenia Bezouta.

W dowodzie twierdzenia potrzebny będzie następujący

Lemat 1. *Jeśli wielomiany $W_1,W_2\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ są względnie pierwsze (tzn. nie mają wspólnego dzielnika pierwszego różnego od stałej), to istnieją takie wielomiany $T_1,T_2\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ oraz $S\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_{n-1}}]$, że dla wszystkich $(x_1,\ldots,x_n)$ zachodzi równość*

$$T_1(x_1,\ldots,x_n)W_1(x_1,\ldots,x_n)+T_2(x_1,\ldots,x_n)W_2(x_1,\ldots,x_n)= \\ =S(x_1,\ldots,x_{n-1}).$$

Przy tym, $S\not\equiv 0$.

Uwaga: Kto wnikliwie prześledzi szkic dowodu poniżej, spostrzeże, iż można nieco osłabić założenia tego lematu. Mianowicie, prawdziwy jest następujący

Wniosek 1. Teza Lematu 1 zachodzi, jeśli największy wspólny dzielnik wielomianów W_1 i W_2 nie zależy od zmiennej x_n.

Szkic dowodu. Rozpatrujemy pierścień $\mathbf{R}(\mathbf{x_1},\ldots,\mathbf{x_{n-1}})[\mathbf{x_n}]$ wielomianów zmiennej x_n o współczynnikach będących funkcjami wymiernymi zmiennych $x_1,\ldots,x_{n-1}$. Czytelnik zechce sam udowodnić, że dowolny wielomian $Q\in\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ jest nierozkładalny w pierścieniu $\mathbf{R}[\mathbf{x_1},\ldots,\mathbf{x_n}]$ wtedy i tylko wtedy, gdy jest nierozkładalny w pierścieniu $\mathbf{R}(\mathbf{x_1},\ldots,\mathbf{x_{n-1}})[\mathbf{x_n}]$. (Dowodzi się tego niemal tak samo jak znanego faktu, że wielomian jednej zmiennej o współczynnikach całkowitych nierozkładalny w pierścieniu $\mathbf{Z}[\mathbf{x}]$ jest nierozkładalny także w $\mathbf{Q}[\mathbf{x}]$.)

Z tej własności wynika, że wielomiany W_1 i W_2 są względnie pierwsze w $\mathbf{R}(\mathbf{x_1},\ldots,\mathbf{x_{n-1}})[\mathbf{x_n}]$. Załóżmy bez ograniczenia ogólności, że stopień (ze względu na zmienną x_n) wielomianu W_1 jest nie mniejszy niż stopień W_2

Rozwiązanie zadania M 767.
Gdy $a=1$, nie ma czego dowodzić. Niech więc $a>1$.

Podzielmy duże pudło na $A\cdot B\cdot C$ sześcianików o krawędzi 1. Każdemu z sześcianików przypiszmy trzy współrzędne (i,j,k), gdzie $1\le i\le A$, $1\le j\le B$, $1\le k\le C$. W sześcianik o współrzędnych (i,j,k) wpisujemy liczbę ε_a^{i+j+k}, gdzie $\varepsilon_a=\cos\frac{2\pi}{a}+i\sin\frac{2\pi}{a}$.

Z poprzedniego zadania wynika, że suma liczb w każdym prostopadłościanie o wymiarach $a\times b\times c$ jest równa zeru, bowiem

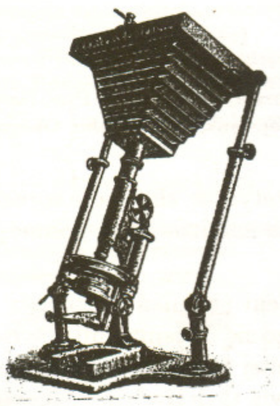
$$\sum_{i=i_p}^{i_\ell}\sum_{j=j_p}^{j_\ell}\sum_{k=k_p}^{k_\ell}\varepsilon_a^{i+j+k}= \left(\sum_{i=i_p}^{i_\ell}\varepsilon_a^i\right)\left(\sum_{j=j_p}^{j_\ell}\varepsilon_a^j\right)\left(\sum_{k=k_p}^{k_\ell}\varepsilon_a^k\right),$$

a jedna z sum po prawej stronie ma wartość a.

Zatem, suma wszystkich liczb w całym pudle także znika. Skoro jednak

$$0=\sum_{i=1}^{A}\sum_{j=1}^{B}\sum_{k=1}^{C}\varepsilon_a^{i+j+k}= \left(\sum_{i=1}^{A}\varepsilon_a^i\right)\left(\sum_{j=1}^{B}\varepsilon_a^j\right)\left(\sum_{k=1}^{C}\varepsilon_a^k\right),$$

to musi być np. (bez zmniejszenia ogólności) $\sum_{i=1}^{A}\varepsilon_a^i=0$. Stąd, ponownie na mocy poprzedniego zadania, a jest dzielnikiem A.



i zastosujmy algorytm Euklidesa poszukiwania największego wspólnego dzielnika. Otrzymamy ciąg równości

$$W_1 = Q_1 W_2 + W_3, \quad W_2 = Q_2 W_3 + W_4, \quad \ldots \quad W_{k-2} = Q_{k-2} W_{k-1} + W_k\,,$$

gdzie wszystkie wielomiany W_j oraz Q_j należą do pierścienia $\mathbf{R}(\mathbf{x_1}, \ldots, \mathbf{x_{n-1}})[\mathbf{x_n}]$ oraz

$$\operatorname{st} W_1 \geq \operatorname{st} W_2 > \operatorname{st} W_3 > \ldots > \operatorname{st} W_k = 0\,.$$

Przy tym musi być $W_k \not\equiv 0$, bo w przeciwnym razie wielomian niezerowego stopnia W_{k-1} byłby wspólnym dzielnikiem względnie pierwszych wielomianów W_1 i W_2. Zatem $W_k \equiv c$, $c \neq 0$.

Stąd już do tezy Lematu niedaleko: z równań $W_j = Q_j W_{j+1} + W_{j+2}$ (spełnionych dla $j = 1, \ldots, k-2$) dostaniemy zależność

$$P_1 W_1 + P_2 W_2 = c\,,$$

gdzie $P_i \in \mathbf{R}(\mathbf{x_1}, \ldots, \mathbf{x_{n-1}})[\mathbf{x_n}]$. By otrzymać tezę Lematu, wystarczy teraz pomnożyć obie strony tej równości przez najmniejszą wspólną wielokrotność wielomianów znajdujących się w mianownikach współczynników wielomianów P_1 i P_2.

Przejdźmy teraz do dowodu twierdzenia.

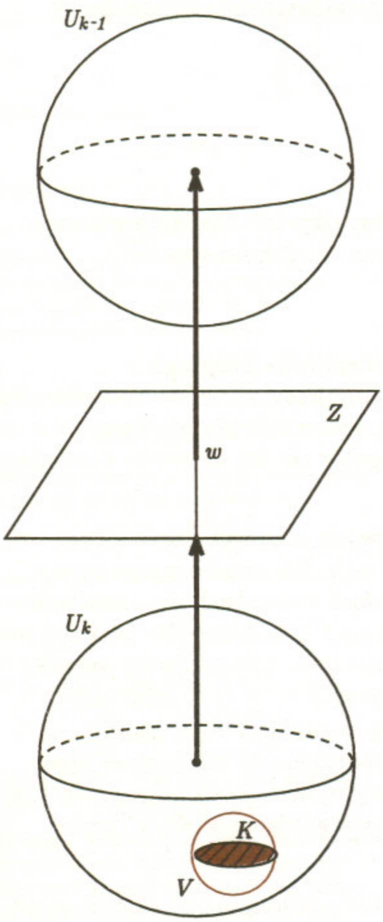
Załóżmy, że teza jest fałszywa. Z założenia o nierozkładalności W_1 wynika wówczas, że wielomiany W_1 i W_2 są względnie pierwsze. Z Wniosku 1 wynika, że dla dowolnego $k \in \{1, 2, \ldots, n\}$ istnieje (nie znikający tożsamościowo) taki wielomian S_k zależny od $(n-1)$ zmiennych, że

$$T_1(x_1, \ldots, x_n) W_1(x_1, \ldots, x_n) + T_2(x_1, \ldots, x_n) W_2(x_1, \ldots, x_n) = \\ = S_k(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n)\,.$$

Aby otrzymać sprzeczność, wykażemy, że wielomian W_1 ma dostatecznie dużo miejsc zerowych. Dokładniej, zachodzi następujący

Lemat 2. *Dla pewnego $k \in \{1, 2, \ldots, n\}$ istnieje kula $(n-1)$-wymiarowa K o środku $(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n)$ i promieniu ε o tej własności, że dla dowolnego $(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n) \in K$ istnieje taka liczba rzeczywista x_k, że $W_1(x_1, \ldots, x_n) = 0$.*

Z tego Lematu twierdzenie wynika natychmiast: ponieważ z założenia W_2 zeruje się wszędzie tam, gdzie zeruje się W_1, to równość (2) implikuje, że wielomian S_k znika na całej kuli K, a więc $S_k \equiv 0$, sprzeczność.



Mała kula V jest zawarta w zbiorze B, na którym wielomian W_1 przyjmuje wartości ujemne, natomiast duża kula U_{k-1} – w zbiorze $\mathbf{R}^n \backslash B = A \cup Z$. Zatem (ponieważ wielomian W_1 jest ciągły na każdej prostej w $\mathbf{R}^n$) przesuwając każdy punkt „koła wielkiego" K o wektory $t \cdot \mathbf{w}$, $t \in [0,1]$, trafimy dla pewnej wartości t w punkt należący do zbioru Z, na którym wielomian W_1 się zeruje.

Szkic dowodu Lematu 2. Niech A (odp. B) oznacza zbiór tych punktów $x \in \mathbf{R^n}$, dla których $W_1(x) > 0$ (odp. $W_1(x) < 0$). Ponadto, oznaczmy przez Z zbiór wszystkich miejsc zerowych wielomianu W_1. Oczywiście, zbiory A i B są otwarte oraz $A \cup B \cup Z = \mathbf{R^n}$.

Wybierzmy punkty $a = (a_1, \ldots, a_n) \in A$ oraz $b = (b_1, \ldots b_n) \in B$. Z otwartości zbioru A wynika, że istnieje takie $r > 0$, iż kula otwarta U_0 o środku a i promieniu r jest zawarta w A. Rozważmy kule otwarte $U_1, \ldots, U_n$ o tym samym promieniu r i o środkach odpowiednio w punktach $(b_1, a_2, a_3, a_4, \ldots, a_n)$, $(b_1, b_2, a_3, a_4, \ldots, a_n)$, $(b_1, b_2, b_3, a_4, \ldots, a_n)$, $\ldots$ $(b_1, b_2, b_3, b_4, \ldots, b_n)$. Niech k będzie najmniejszą liczbą o tej własności, że kula U_k przecina zbiór B. Z otwartości B wnosimy, że istnieje punkt $c = (c_1, \ldots, c_n)$ i liczba $\varepsilon > 0$, takie, że kula V o środku w c i promieniu ε jest zawarta w $U_k \cap B$. Poszukiwaną kulą $(n-1)$-wymiarową jest zbiór

$$K := \Big\{(x_1, \ldots, x_{k-1}, c_k, x_{k+1}, \ldots, x_n) \;:\; \sum_{j \neq k} (x_j - c_j)^2 < \varepsilon^2\Big\}\,.$$

Istotnie, wprost z definicji $K \subset V \subset B$. Obraz zbioru K w przesunięciu o wektor $\mathbf{w} = (0, \ldots, 0, a_k - b_k, 0, \ldots, 0)$ zawiera się w kuli U_{k-1}, a ta z kolei zawiera się w zbiorze $A \cup Z$ (bo nie ma punktów wspólnych z B). Wystarczy teraz przypomnieć sobie własność Darboux, by stwierdzić, że przesuwając dowolny punkt z K o wektory $t \cdot \mathbf{w}$, $t \in [0,1]$, musimy natrafić na punkt zbioru Z (patrz rysunek). Ponieważ przesuwanie o wektor $t \cdot \mathbf{w}$ to nic innego, jak odpowiedni dobór k-tej współrzędnej punktu, dowód Lematu 2, a więc i całego twierdzenia, jest tym samym zakończony.