

Uniwersytet Śląski w Katowicach
Wydział Matematyki, Fizyki i Chemii
Kierunek matematyka

Praca dyplomowa magisterska

Wielomiany dodatnie na zwartych zbiorach semialgebraicznych

Promotor:
dr Paweł Gładki

Autor:
inż. Edyta Swacha-Olender

Katowice 2011

Spis treści

Wstęp	2
I. Pojęcia wstępne.	5
I.1. Podstawowe definicje.	5
I.2. Teoria wykorzystana w dowodach.	6
II. Główny rezultat.	12
Skorowidz	15
Literatura	16

Wstęp

W niniejszej pracy zajmiemy się jednym z wariantów 17-tego Problemu Hilberta. Przypomnijmy, że w oryginale stawiał on następujące pytanie: czy jeżeli wielomian $f \in \mathbb{R}[X_1, \dots, X_n]$ przyjmuje wartości nieujemne, to jest sumą kwadratów funkcji wymiernych? Problem ten w 1927 roku pozytywnie rozwiązał Artin w klasycznej pracy [1], która dziś uważana jest za początek rozwoju rzeczywistej geometrii algebraicznej. Od tego czasu 17-ty Problem Hilberta znalazł wiele uogólnień. W szczególności można się zastanawiać, co się stanie, jeżeli warunek „ $f \geq 0$ ” zastąpimy „ $f \geq 0$ na zwartym zbiorze semialgebraicznym”.

Zdefiniujmy wersję 17-tego Problemu Hilberta, którą będziemy się zajmować, bardziej formalnie. W tym celu wprowadźmy kilka oznaczeń. Dla uproszczenia notacji w pracy tej będziemy pisać $\mathbb{R}[X]$ dla oznaczenia pierścienia $\mathbb{R}[X_1, \dots, X_n]$, $\mathbb{Q}[X]$ dla oznaczenia pierścienia $\mathbb{Q}[X_1, \dots, X_n]$ itp. Symbol X (odpowiednio x) będzie natomiast oznaczał uporządkowaną n -kę $(X_1, \dots, X_n)$ ($(x_1, \dots, x_n)$, odpowiednio). Niech S będzie skończonym podzbiorem $\mathbb{R}[X]$, natomiast $\sum \mathbb{R}[X]^2$ niech oznacza zbiór wszystkich sum kwadratów elementów pierścienia $\mathbb{R}[X]$ oraz $\sum \mathbb{Q}[X]^2$ oznacza zbiór wszystkich sum kwadratów elementów pierścienia $\mathbb{Q}[X]$. Niech

$$K_S = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \dots, g_m(x) \geq 0\}$$

będzie zbiorem semialgebraicznym wyznaczonym przez zbiór S oraz niech

$$T_S = \left\{ \sum \sigma_\epsilon \cdot g^\epsilon : \epsilon = (\epsilon_1, \dots, \epsilon_m) \in \{0, 1\}^m, \sigma_\epsilon \in \sum \mathbb{R}[X]^2 \right\}$$

będzie preporządkiem generowanym przez zbiór S , gdzie $g^\epsilon := g_1^{\epsilon_1}, \dots, g_m^{\epsilon_m}$. Ponadto, niech

$$M_S = \left\{ \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m : \sigma_i \in \sum \mathbb{R}[X]^2 \right\}$$

będzie modułem kwadratowym generowanym przez zbiór S . Przypomnijmy też, że zbiór $A \subseteq \mathbb{R}[X]$ nazywamy zbiorem archimedesowym jeżeli

$$\bigwedge_{b \in \mathbb{R}[X]} \bigvee_{n \in \mathbb{N}} b + n \in A.$$

Prawdziwe są dwa klasyczne twierdzenia:

Twierdzenie 1 (Schmüdgen). *Niech K_S będzie zbiorem zwartym. Jeżeli $f \in \mathbb{R}[X]$ oraz $f(x) > 0$ dla $x \in K_S$ to $f \in T_S$*

Twierdzenie 2 (Putinar). *Niech moduł kwadratowy M_S będzie zbiorem archimedesowym. Jeśli $f \in \mathbb{R}[X]$ oraz $f(x) > 0$ dla $x \in K_S$ to $f \in M_S$.*

Oczywiście $M_S \subset T_S$, tak więc twierdzenie Putinara jest rezultatem subtelniejszym, niż twierdzenie Schmüdgena, nie może jednak być traktowane jako jego uogólnienie: można skonstruować przykłady zwartych zbiorów K_S , dla których moduł kwadratowy M_S nie jest archimedesowy [4][Example 7.3.1]. Okazuje się, że prawdziwe są też twierdzenia odwrotne do powyższych. Tym samym twierdzenia Schmüdgena i Putinara dostarczają kryteriów potwierdzających, że dany wielomian jest dodatni na zbiorze K_S – kryteria te nazwane zostały przez Powers „certyfikatami dodatniości”.

Głównym celem niniejszej pracy będzie sformułowanie i udowodnienie tak zwanego „wymiernego certyfikatu dodatniości” dla twierdzenia Putinara. Będziemy rozważali sytuację, gdy w założeniu twierdzenia Putinara warunek „ $f \in \mathbb{R}[X]$ ” zastąpimy warunkiem „ $f \in \mathbb{Q}[X]$ ” i spróbujemy odpowiedzieć na pytanie czy w takiej sytuacji można pokazać, że f jest elementem pewnego modułu kwadratowego M w pierścieniu $\mathbb{Q}[X]$, a więc czy wielomian f można przedstawić jako kombinację liniową

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m$$

dla pewnych $g_1, \dots, g_m \in \mathbb{Q}[X]$ oraz $\sigma_0, \dots, \sigma_m \in \sum \mathbb{Q}[X]^2$. W istocie tak jest, o ile dla pewnego $N \in \mathbb{N}$ wielomian $N - \sum x_i^2$ jest elementem modułu kwadratowego M . Dokładniej, udowodnimy następujące twierdzenie:

Twierdzenie 3. *Niech $S \subseteq \mathbb{Q}[X]$ oraz niech $N \in \mathbb{N}$ będzie takie, że $N - \sum x_i^2 \in M_S$. Jeśli $f(x) \in \mathbb{Q}[X]$ oraz $f(x) > 0$, dla wszystkich $x \in K_S$, to istnieją $\sigma_0, \dots, \sigma_m, \sigma \in \sum \mathbb{Q}[X]^2$ takie, że:*

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m + \sigma(N - \sum x_i^2).$$

Dowód twierdzenia 3 zaczerpnięty został z pracy Powers [5] i opiera się w znacznym stopniu na lemacie Schweighofera z pracy [7]. Z kolei sam lemat Schweighofera jest wersją klasycznego twierdzenia Póyla, którego dowód został zapożyczony z książki Hardy’ego, Littlewooda i Pólya [2]. Definicje i notacje preporządku, zbioru

archimedesowego itp. zostały przedstawione tak, jak w książce Marshalla [4], zaś wykorzystane twierdzenia z analizy, matematyki dyskretniej oraz teorii liczb tak, jak w podręcznikach Kołodzieja [3], Rossa i Wrighta [6] oraz Sierpińskiego [8].

W pierwszym rozdziale znajdziemy podstawowe definicje i twierdzenia potrzebne do zrozumienia rozważań zawartych w głównej części niniejszej pracy. Przede wszystkim skoncentrowaliśmy się w nim na szczegółowym omówieniu lematu Schweighofera i twierdzenia Póyla. Z kolei drugi rozdział poświęcony jest dowodowi Twierdzenia 3.

Rozdział I

Pojęcia wstępne.

W rozdziale tym zawarta została cała teoria, dzięki której będziemy mogli zrozumieć późniejsze rozważania.

I.1. Podstawowe definicje.

W tym miejscu, raz jeszcze zgromadzimy wszystkie potrzebne definicje i oznaczenia, niezbędne dla niniejszego opracowania. Niech:

1. $\mathbb{R}[X]$ oznacza pierścień wielomianów $\mathbb{R}[X_1, \dots, X_n]$, podobnie niech $\mathbb{Q}[X]$ oznacza pierścień wielomianów $\mathbb{Q}[X_1, \dots, X_n]$,
2. $\sum \mathbb{R}[X]^2$ będzie zbiorem wszystkich sum kwadratów w $\mathbb{R}[X]$ oraz $\sum \mathbb{Q}[X]^2$ będzie zbiorem wszystkich sum kwadratów w $\mathbb{Q}[X]$,
3. $S = \{g_1, \dots, g_m\} \subseteq \mathbb{Q}[X]$ będzie ustalonym zbiorem wielomianów o współczynnikach wymiernych,
4. $K_S = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \dots, g_m(x) \geq 0\}$ będzie zbiorem semialgebraicznym wyznaczonym przez zbiór S ,
5. $M_S = \{\sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m : \sigma_i \in \sum \mathbb{R}[X]^2\}$ będzie modulem kwadrato-
wym wyznaczonym przez zbiór S ,
6. $T_S = \{\sum \sigma_\epsilon \cdot g^\epsilon : \epsilon = (\epsilon_1, \dots, \epsilon_m) \in \{0, 1\}^m, \sigma_\epsilon \in \sum \mathbb{R}[X]^2\}$ będzie preporząd-
kiem generowanym przez zbiór S , gdzie $g^\epsilon := g_1^{\epsilon_1}, \dots, g_m^{\epsilon_m}$.

I.2. Teoria wykorzystana w dowodach.

Poniższy lemat wykorzystamy później do udowodnienia lematu Schweighofera.

Lemat I.1. [7, Lemma 7]

Dla $y \in [0, 1]$ oraz $k \in \mathbb{N}$,

$$(y - 1)^{2k} y \leq \left(\frac{1}{2k + 1} - 1 \right)^{2k} \frac{1}{2k + 1}.$$

Dowód. Niech $F(y) = (y - 1)^{2k} y$. Wówczas:

$$F(y)' = 2k(y - 1)^{2k-1} y + (y - 1)^{2k} = (y - 1)^{2k-1} [2ky + y - 1].$$

Wobec tego $F(y)' = 0$ wtedy i tylko wtedy, gdy $y = 1$ lub $2ky + y - 1 = 0$, to znaczy $y = \frac{1}{2k+1}$. Jeżeli $y = 1$, to $F(y) = 0$. Jeżeli $y = \frac{1}{2k+1}$, to

$$F(y) = \left(\frac{1}{2k + 1} - 1 \right)^{2k} \frac{1}{2k + 1}.$$

Zatem $F(y)$ przyjmuje maksimum w punkcie $\frac{1}{2k+1}$ i tym samym nierówność jest udowodniona. $\square$

Następnie szczegółowo omówimy lemat Schweighofera, który znalazł zastosowanie w głównym twierdzeniu niniejszej pracy.

Lemat I.2 (Schweighofer). [7, Lemma 8]

Niech $D \subseteq \mathbb{R}^n$ będzie zbiorem zwartym, niech, dla każdego $i \in \{1, \dots, m\}$, $g_i \in \mathbb{R}[X]$ będą ustalonymi wielomianami takimi, że $g_i(x) \leq 1$ dla $x \in D$. Niech $p \in \mathbb{R}[X]$ oraz $p(x) > 0$ dla $x \in K_S$. Wtedy istnieje $\lambda \in \mathbb{N}$ takie, że, dla każdego $k \in \mathbb{N}$, spełniona jest następująca nierówność:

$$p(x) - \lambda \sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) > 0, \text{ dla } x \in D.$$

Dowód. Skoro K_S jest zbiorem zwartym, to na mocy twierdzenia Weierstrassa [3, Rozdział 17 Twierdzenie 8] możemy wybrać $\varepsilon > 0$ takie, że $p(x) > \varepsilon$ dla $x \in K_S$.

Zauważmy, że $A := \{x \in D : p(x) \leq \varepsilon\}$ jest domkniętym¹ podzbiorem zbioru zwartego D i jest rozłączny ze zbiorem K_S . Wobec tego co najmniej jeden $g_i(x)$ jest ujemny dla pewnego $x \in A$. Ustalamy $\delta > 0$ taką, że

$$(1) \quad \min\{g_1(x), \dots, g_m(x)\} \leq -\delta, \text{ dla każdego } x \in A.$$

Wielomian p przyjmuje minimum na zbiorze zwartym D , możemy więc wybrać liczbę naturalną $\lambda \in \mathbb{N}$ taką, że:

$$(2) \quad p(x) + \frac{\lambda\delta}{2} > 0.$$

Ponadto, możemy wybrać liczbę $k \in \mathbb{N}$ na tyle dużą, aby

$$(3) \quad \frac{\delta}{2} \geq \frac{m-1}{2k+1}$$

oraz

$$(4) \quad \varepsilon \geq \frac{\lambda m}{2k+1}.$$

Wykażemy, że spełniona jest nierówność:

$$p(x) - \lambda \sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) > 0 \text{ dla } x \in D.$$

Skoro $A \cap K_S = \emptyset$, więc, dla $x \in A$, w sumie $\sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x)$ jest najwyżej $m-1$ składników nieujemnych. Jeżeli, dla $x \in D$, $g_i(x) \in [0, 1]$, to wobec

Lematu I.1

$$(5) \quad (1 - g_i(x))^{2k} g_i(x) \leq \left(\frac{1}{2k+1} - 1 \right)^{2k} \frac{1}{2k+1} \leq \frac{1}{2k+1}.$$

Zatem składniki nieujemne sumują się do co najwyżej $\frac{m-1}{2k+1}$. Jednocześnie, dla $x \in D$, co najmniej jeden składnik w sumie $\sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x)$ jest nieujemny, a nawet, wobec (1), mniejszy bądź równy $(1 - g_i(x))^{2k}(-\delta) \leq -\delta$ gdzie $(1 - g_i(x)) \geq 1$. Zatem składniki ujemne sumują się do co najwyżej $-\delta$.

Powołując się na (2), (3) oraz (4) otrzymamy:

$$\begin{aligned} p(x) - \lambda \sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) &\geq p(x) - \lambda \left(\frac{m-1}{2k+1} - \delta \right) \\ (6) \quad &\geq p(x) - \lambda \frac{m-1}{2k+1} + \lambda\delta \geq p(x) - \lambda \frac{m-1}{2k+1} + \frac{\lambda\delta}{2} + \frac{\lambda\delta}{2} \\ &\geq p(x) + \frac{\lambda\delta}{2} + \lambda \left(\frac{\delta}{2} - \frac{m-1}{2k+1} \right) > 0, \text{ dla } x \in A. \end{aligned}$$

¹Niech $(x_n) \in A$ oraz $x_n \rightarrow x$. Wówczas $p(x_n) \leq \varepsilon$ dla każdego $n \in \mathbb{N}$, a więc $p(x) \leq \varepsilon$ co oznacza, że $x \in A$.

W przypadku gdy $x \in D \setminus A$ wszystkie wyrażenia w sumie $\sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x)$ mogą być nieujemne, a więc wobec (5)

$$\sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) < \frac{m}{2k+1}.$$

Jednocześnie $p(x) > 0$, dla $x \in D \setminus A$, a zatem:

$$(7) \quad p(x) - \lambda \sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) > \epsilon - \lambda \frac{m}{2k+1} \geq 0 \text{ dla } x \in D \setminus A$$

na mocy (4).

W rezultacie, dla wszystkich $x \in D$, otrzymujemy:

$$p(x) - \lambda \sum_{i=1}^m (1 - g_i(x))^{2k} g_i(x) \geq 0.$$

□

Również ważnym twierdzeniem, które zostało zastosowane w dowodzie głównego twierdzenia niniejszej pracy, jest twierdzenie Pólya.

Twierdzenie I.4. (*Pólya*) [2, Theorem 56]

Niech $F \in \mathbb{R}[X]$ będzie wielomianem jednorodnym stopnia m i niech

$$U = \{(x_1, \dots, x_m) \in \mathbb{R}^m : x_i \geq 0, i \in \{1, \dots, m\}, \sum_{i=1}^m x_i > 0\}.$$

Jeżeli $F(x) > 0$, dla $x \in U$, to istnieją wielomiany jednorodne $G, H \in \mathbb{R}[X]$ o dodatnich współczynnikach takie, że

$$F \cdot H = G.$$

Dowód. Twierdzenie udowodnimy w przypadku $m = 3$. Idea dowodu dla wyższych m jest taka sama.

Funkcja $F(x_1, x_2, x_3)$ jest dodatnia i ciągła na zbiorze W , gdzie

$$W = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 \geq 0, x_2 \geq 0, x_3 \geq 0, x_1 + x_2 + x_3 = 1\}.$$

Zauważmy, że W jest zbiorem domkniętym² i ograniczonym³, a więc jest zbiorem zwartym. Zatem F przyjmuje minimum μ dla pewnego $x \in W$. Ponadto $W \subset U$, a więc $\mu > 0$.

²Niech funkcja $g : \mathbb{R}^3 \rightarrow \mathbb{R}$ będzie dana wzorem $g((x_1, x_2, x_3)) = x_1 + x_2 + x_3$. Jest to funkcja ciągła, $\{(x_1, x_2, x_3) : x_i \in [0, \infty), x_1 + x_2 + x_3 = 1\} = g^{-1}(\{1\})$, a więc zbiór W jest zbiorem domkniętym jako przeciwobraz zbioru domkniętego $\{1\}$.

³Zbiór W jest zawarty w kuli $\bar{K}((0, 0), 1)$, a więc jest zbiorem ograniczonym.

Niech

$$(8) \quad F(x_1, x_2, x_3) = \sum A_{\alpha\beta\gamma} \frac{x_1^\alpha x_2^\beta x_3^\gamma}{\alpha! \beta! \gamma!},$$

gdzie sumowanie przebiega po wszystkich trójkach liczb naturalnych (α, β, γ) takich, że $\alpha + \beta + \gamma = n$. Niech

$$(9) \quad \phi(x_1, x_2, x_3, x_4) = x_4^n \sum A_{\alpha\beta\gamma} \binom{x_1 x_4^{-1}}{\alpha} \binom{x_2 x_4^{-1}}{\beta} \binom{x_3 x_4^{-1}}{\gamma},$$

gdzie $x_4 > 0$ i $\binom{x x_4^{-1}}{\delta}$ definiujemy następująco:

$$\binom{x x_4^{-1}}{\delta} = \begin{cases} 1, & \text{gdy } \delta = 0, \\ \frac{x(x-x_4)\dots(x-(x_4\delta-1))}{\delta!}, & \text{gdy } \delta \in \mathbb{N}, \ x_4 > 0 \text{ i } x \in \mathbb{R}. \end{cases}$$

Gdy $x_4 \rightarrow 0$, to $\phi(x_1, x_2, x_3, x_4) \rightarrow F(x_1, x_2, x_3)$. Możemy wobec tego przedłużyć ϕ do funkcji ciągłej na zbiorze Z zdefiniowanym wzorem:

$$Z = \{(x_1, x_2, x_3, x_4) : (x_1, x_2, x_3) \in W, x_4 \in [0, 1]\}$$

przyjmując $\phi(x_1, x_2, x_3, 0) = F(x_1, x_2, x_3)$. Funkcja ϕ jest wobec tego przedziałami monotoniczna [3, Rozdział 31 Lemat 2], a zatem możemy dobrać $\epsilon > 0$ takie, że dla $x_4 \in (0, \epsilon)$ zachodzi:

$$(10) \quad \phi(x_1, x_2, x_3, x_4) > \phi(x_1, x_2, x_3, 0) - \frac{1}{2}\mu = F(x_1, x_2, x_3) - \frac{1}{2}\mu \geq \frac{1}{2}\mu > 0$$

dla $(x_1, x_2, x_3) \in W$.

Zauważmy, że wobec uogólnionego wzoru dwumianowego Newtona [6]:

$$(11) \quad \begin{aligned} (x_1 + x_2 + x_3 + x_4)^{l-n} &= \sum \binom{l-n}{\kappa + \lambda + \eta} x_1^\kappa x_2^\lambda x_3^\eta \\ &= \sum \frac{(l-n)!}{\kappa! \lambda! \eta!} = (l-n)! \sum \frac{x_1^\kappa x_2^\lambda x_3^\eta}{\kappa! \lambda! \eta!}, \end{aligned}$$

gdzie sumowanie przebiega po wszystkich trójkach liczb naturalnych (κ, λ, η) takich, że $\kappa + \lambda + \eta = l - n$. Mnożąc (8) i (10) otrzymujemy:

$$(12) \quad (x_1 + x_2 + x_3)^{l-n} F = (l-n)! \sum \sum A_{\alpha\beta\gamma} \frac{x_1^{\alpha+\kappa} x_2^{\beta+\lambda} x_3^{\gamma+\eta}}{\alpha! \kappa! \beta! \lambda! \gamma! \eta!},$$

gdzie pierwsze sumowanie przebiega po wszystkich trójkach liczb naturalnych (α, β, γ) takich, że $\alpha + \beta + \gamma = n$ oraz drugie sumowanie przebiega po wszystkich trójkach liczb naturalnych (κ, λ, η) takich, że $\kappa + \lambda + \eta = l - n$.

Niech $a = \alpha + \kappa$, $b = \beta + \lambda$, $c = \gamma + \eta$. Wówczas $a \geq 0$, $b \geq 0$, $c \geq 0$ oraz $a + b + c = \alpha + \kappa + \beta + \lambda + \gamma + \eta = n + l - n = l$. Ponadto $a \geq \alpha \geq 0$, $b \geq \beta \geq 0$, $c \geq \gamma \geq 0$ oraz $\alpha + \beta + \gamma = n$ wzór (11) można przedstawić jako:

$$(x_1 + x_2 + x_3)^{l-n} F = (l-n)! \sum \frac{x_1^a x_2^b x_3^c}{a!b!c!} \sum' A_{\alpha\beta\gamma} \begin{pmatrix} a \\ \alpha \end{pmatrix} \begin{pmatrix} b \\ \beta \end{pmatrix} \begin{pmatrix} c \\ \gamma \end{pmatrix},$$

gdzie pierwsze sumowanie przebiega po trójkach liczb naturalnych (a, b, c) takich, że $a + b + c = l$, a suma $\sum'$ po trójkach liczb naturalnych (α, β, γ) takich, że $a \geq \alpha \geq 0$, $b \geq \beta \geq 0$, $c \geq \gamma \geq 0$ oraz $\alpha + \beta + \gamma = n$. Ponadto, ponieważ $\begin{pmatrix} a \\ \alpha \end{pmatrix} = 0$, $\begin{pmatrix} b \\ \beta \end{pmatrix} = 0$, $\begin{pmatrix} c \\ \gamma \end{pmatrix} = 0$, dla $\alpha \geq a$, $\beta \geq b$, $\gamma \geq c$, możemy po prostu zastąpić sumę $\sum'$ sumą $\sum'' A_{\alpha\beta\gamma} \begin{pmatrix} a \\ \alpha \end{pmatrix} \begin{pmatrix} b \\ \beta \end{pmatrix} \begin{pmatrix} c \\ \gamma \end{pmatrix}$, gdzie sumowanie przebiega po trójkach liczb naturalnych (α, β, γ) takich, że $\alpha + \beta + \gamma = n$.

Ostatecznie, wobec (9) otrzymujemy:

$$\begin{aligned} (x_1 + x_2 + x_3)^{l-n} F &= (l-n)! \sum \frac{x_1^a x_2^b x_3^c}{a!b!c!} \sum'' A_{\alpha\beta\gamma} \begin{pmatrix} a \\ \alpha \end{pmatrix} \begin{pmatrix} b \\ \beta \end{pmatrix} \begin{pmatrix} c \\ \gamma \end{pmatrix} \\ (13) \quad &= (l-n)! \sum \frac{x_1^a x_2^b x_3^c}{a!b!c!} \sum'' A_{\alpha\beta\gamma} \begin{pmatrix} \frac{a}{l} \cdot l \\ \alpha \end{pmatrix} \begin{pmatrix} \frac{b}{l} \cdot l \\ \beta \end{pmatrix} \begin{pmatrix} \frac{c}{l} \cdot l \\ \gamma \end{pmatrix} \\ &= (l-n)! \sum \frac{x_1^a x_2^b x_3^c}{a!b!c!} l^n \phi\left(\frac{a}{l}, \frac{b}{l}, \frac{c}{l}, \frac{1}{l}\right) = (l-n)! l^n \sum \phi\left(\frac{a}{l}, \frac{b}{l}, \frac{c}{l}, \frac{1}{l}\right) \frac{x_1^a x_2^b x_3^c}{a!b!c!} \end{aligned}$$

gdzie, dla $x_4 \in (0, \varepsilon)$, wobec (10) $\phi(x_1, x_2, x_3, x_4) > 0$. Zauważmy też, że dla l dostatecznie dużych (dokładniej takich, że $\frac{1}{l} < \epsilon$ oraz $l - n > 0$), wobec (9) i (10) wielomiany jednorodne

$$H(x_1, x_2, x_3) = (x_1 + x_2 + x_3)^{l-n}$$

oraz

$$G(x_1, x_2, x_3) = (k-n)! l^n \sum \phi\left(\frac{a}{l}, \frac{b}{l}, \frac{c}{l}, \frac{1}{l}\right) \frac{x_1^a x_2^b x_3^c}{a!b!c!},$$

gdzie suma w G przebiega po trójkach liczb naturalnych (a, b, c) takich, że $a + b + c = n$ mają dodatnie współczynniki i zachodzi

$$F \cdot H = G.$$

□

Z powyższego twierdzenia Pólya wynika następująca uwaga:

Uwaga I.1. *Zauważmy, że wielomian H skonstruowany w dowodzie twierdzenia Pólya jest w następującej postaci:*

$$H(x_1, \dots, x_m) = (x_1 + \dots + x_m)^k,$$

dla pewnego $k \in \mathbb{N}$.

Rozdział II

Główny rezultat.

Rozdział ten zawiera dowód twierdzenia, które stanowi uogólnienie 17-tego Problemu Hilberta na zwartych zbiorach semialgebraicznych.

Twierdzenie II.5. [5, Theorem 6]

Niech $S \subseteq \mathbb{Q}[X]$ oraz niech $N \in \mathbb{N}$ będzie takie, że $N - \sum x_i^2 \in M_S$.

Jeśli $f(x) \in \mathbb{Q}[X]$ oraz $f(x) > 0$, dla wszystkich $x \in K_S$, to istnieją

$\sigma_0, \dots, \sigma_m, \sigma \in \sum \mathbb{Q}[X]^2$ takie, że:

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m + \sigma(N - \sum x_i^2).$$

Dowód. Niech $l : \mathbb{R}^{2n} \rightarrow \mathbb{R}^n$ będzie funkcją określoną wzorem

$$l(y_1, \dots, y_{2n}) = \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right)$$

i niech zbiór $C \subseteq \mathbb{R}^n$ będzie zdefiniowane przez

$$C = l(\Delta)$$

gdzie:

$$\Delta := \left\{ (y_1, \dots, y_{2n}) : y_i \in [0, \infty), y_1 + \dots + y_{2n} = 2n \left(N + \frac{1}{4} \right) \right\} \subseteq \mathbb{R}^{2n}.$$

Zauważmy, że Δ jest zbiorem niepustym, gdyż dla dowolnego $n \in \mathbb{N}$ liczba $2n(N + \frac{1}{4})$ jest sumą $2n$ liczb rzeczywistych nieujemnych. Zauważmy również, że Δ jest zbiorem domkniętym⁴ i ograniczonym⁵, czyli jest zbiorem zwartym.

⁴Niech funkcja $h : \mathbb{R}^{2n} \rightarrow \mathbb{R}$ będzie dana wzorem $h((y_1, \dots, y_{2n})) = y_1 + \dots + y_{2n}$. Jest to funkcja ciągła, $\{(y_1, \dots, y_{2n}) : y_i \in [0, \infty), y_1 + \dots + y_{2n} = 2n(N + \frac{1}{4})\} = h^{-1}(\{2n(N + \frac{1}{4})\})$ a więc zbiór Δ jest zbiorem domkniętym jako przeciwobraz zbioru domkniętego $\{2n(N + \frac{1}{4})\}$.

⁵Zbiór $\Delta = \{(y_1, \dots, y_{2n}) : y_i \in [0, \infty), y_1 + \dots + y_{2n} = 2n(N + \frac{1}{4})\} \subseteq \mathbb{R}^{2n}$ jest zawarty w kuli domkniętej $\bar{K} = ((0, 0), 2n(N + \frac{1}{4}))$, a więc jest zbiorem ograniczonym.

Zbiór C również jest zbiorem zwartym, gdyż jest ciągłym obrazem zbioru zwartego. Na mocy twierdzenia Weierstrassa [3, Rozdział 17 Twierdzenie 8] wiemy, że każdy z wielomianów g_i , $i \in \{1, 2, \dots, m\}$, jest ograniczony i przyjmuje swoje kresy w zbiorze C . Zatem mnożąc $g_i(x)$ przez odpowiednią liczbę wymierną możemy założyć, że $g_i(x) \leq 1$ dla $x \in C$.

Na podstawie Lematu Schweighofera I.2 wiemy, że istnieje $\lambda \in \mathbb{Q}_+$ takie, że

$$q(x) := f(x) - \lambda \sum_{i=1}^n (g_i(x) - 1)^{2k} g_i(x) > 0 \text{ dla } x \in C.$$

Ponieważ wielomian stopnia d możemy zapisać jako sumę d wielomianów jednorodnych stopni $1, \dots, d$, odpowiednio, to wielomian q przedstawiamy jako $q = \sum_{i=1}^d Q_i$, gdzie $d = st(q)$ oraz Q_i jest wielomianem jednorodnym stopnia i .

Niech $Y = (y_1, \dots, y_{2n})$. Zdefiniujmy następujący wielomian w $\mathbb{Q}[Y]$:

$$F(y_1, \dots, y_{2n}) = \sum_{i=1}^d Q_i \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) \left(\frac{y_1 + \dots + y_{2n}}{2n \left(N + \frac{1}{4} \right)} \right)^{d-i}.$$

F jest wielomianem jednorodnym stopnia d . Zauważmy, że $F(Y) > 0$ dla $Y \in \Delta \setminus \{0\}$.⁶ Korzystając z twierdzenia Pólya (a dokładniej z Twierdzenia I.4 i Uwagi I.1) wiemy, że istnieje $k \in \mathbb{N}$ takie, że wszystkie współczynniki wielomianu $(y_1 + \dots + y_{2n})^k \cdot F(Y)$ są dodatnie.

Niech $G(Y) = \left[\frac{y_1 + \dots + y_{2n}}{2n \left(N + \frac{1}{4} \right)} \right]^k \cdot F(Y)$. Wielomian G ma wszystkie współczynniki dodatnie i wymierne. Zdefiniujmy homomorfizm pierścieni $\psi : \mathbb{Q}[Y] \rightarrow \mathbb{Q}[X]$ warunkami:

$$\begin{aligned} \psi(r) &= r, \text{ dla } r \in \mathbb{Q}, \\ \psi(Y_i) &= \left(N + \frac{1}{4} \right) + X_i \text{ jeżeli } i \in 1, \dots, n \end{aligned}$$

oraz

$$\psi(Y_{n+i}) = \left(N + \frac{1}{4} \right) - X_i \text{ jeżeli } i \in 1, \dots, n.$$

⁶Jeżeli $(y_1, \dots, y_{2n}) \in \Delta$, to $\left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) \in C$, z czego wynika, że $q \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) > 0$ oraz, że suma wielomianów $Q_1 + \dots + Q_d > 0$ a więc $F(Y) > 0$. Z drugiej strony otrzymujemy $q \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) = \sum_{i=1}^d Q_i \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right)$. Ponadto $(y_1, \dots, y_{2n}) \in \Delta \setminus \{0\}$, co oznacza że $\left(\frac{y_1 + \dots + y_{2n}}{2n \left(N + \frac{1}{4} \right)} \right) > 0$.

Zauważmy, że $\psi(G) = q$:

$$\begin{aligned}
\psi(G(Y)) &= \psi \left(\left[\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right]^k \cdot F(Y) \right) = \psi \left(\left[\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right]^k \right) \cdot \psi(F(Y)) \\
&= \left[\psi \left(\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right) \right]^k \cdot \psi \left(\sum_{i=1}^d Q_i \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) \left(\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right)^{d-i} \right) \\
&= \left[\psi \left(\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right) \right]^k \cdot \sum_{i=1}^d \left[\psi \left(Q_i \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right) \right) \cdot \psi \left(\left(\frac{y_1 + \dots + y_{2n}}{2n(N + \frac{1}{4})} \right)^{d-i} \right) \right] \\
&= \left[\frac{(N + \frac{1}{4}) + x_1 + \dots + (N + \frac{1}{4}) + x_n + (N + \frac{1}{4}) - x_1 + \dots + (N + \frac{1}{4}) - x_n}{2n(N + \frac{1}{4})} \right]^k \\
&\quad \cdot \sum_{i=1}^d \left[Q_i \left(\frac{(N + \frac{1}{4}) + x_1 - (N + \frac{1}{4}) + x_1}{2}, \dots, \frac{(N + \frac{1}{4}) + x_n - (N + \frac{1}{4}) + x_n}{2} \right) \right. \\
&\quad \cdot \left. \left(\frac{(N + \frac{1}{4}) + x_1 + \dots + (N + \frac{1}{4}) + x_n + (N + \frac{1}{4}) - x_1 + \dots + (N + \frac{1}{4}) - x_n}{2n(N + \frac{1}{4})} \right)^{d-i} \right] \\
&= \sum_{i=1}^d Q_i(x_1, \dots, x_n) = q.
\end{aligned}$$

Jako że każdy współczynnik wielomianu G jest dodatni i wymierny, jest sumą kwadratów liczb wymiernych wobec twierdzenia Lagrange'a [8, Theorem 4]. Ponadto iloczyn wyrażeń postaci $\sum \mathbb{Q}[X]^2 + r(N - \sum x_j^2)$, gdzie r jest sumą kwadratów liczb wymiernych, jest tej samej postaci. Wobec tego

$$\psi(G) = f(x) - \lambda \sum_{i=1}^n (g_i(x) - 1)^{2k} g_i(x)$$

możemy zapisać jako

$$\delta_o + \delta(N - \sum x_j^2), \text{ gdzie } \delta_o, \delta \in \sum \mathbb{Q}[X]^2,$$

a zatem

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m + \sigma(N - \sum x_i^2)$$

jest żądanej postaci. □

Skorowidz

Lemat, 6

lemat Schweighofera, 6

moduł kwadratowy, 5

preporządek, 2,5

TWIERDZENIE, 3, 12

twierdzenie Pólya, 8

twierdzenie Putinara, 3

twierdzenie Schmüdgen, 3

zbiór archimedesowy, 2

zbiór semialgebraiczny, 2, 5

zbiór sum kwadratów, 5

zbiór wielomianów, 5

Uwaga, 11

Literatura

- [1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, **5**, Abh. math. Sem. Hamburg (1927), 110–115.
- [2] G.H. Hardy, J.E. Littlewood, E. Pólya, *Inequalities*, Cambridge University (1934), 57–60.
- [3] W. Kołodziej, *Analiza matematyczna*, PWN, Warszawa (1978), 76, 87–88, 178.
- [4] M. Marshall, *Positive polynomials and sums of squares*, AMS Math, Surveys and Monographs 146 (2008).
- [5] V. Powers, *Rational certificates of positivity on compact semialgebraic sets*, preprint (2009).
- [6] A. Ross, R.B. Wright, *Matematyka dyskretna*, **4**, PWN, Warszawa (2003), 298–299.
- [7] M. Schweighofer, *Optimization of polynomials on compact semialgebraic sets*, SIAM, Universität Konstanz, Fachbereich Mathematik und Statistik (2006), 7–8.
- [8] W. Sierpiński, *Elementary theory of numbers*, PWN, Warszawa (1964), 368.