Algebra liniowa i matematyka

Edmund PUCZYŁOWSKI, Białystok

Przedstawię tu kilka raczej trudnych, choć elementarnie formułujących się zagadnień, które rozwiązuje się dość prosto stosując metody algebry liniowej.

1. Wykażę, że każdy wielomian o współczynnikach rzeczywistych jest różnicą dwóch wielomianów rosnących.

Zauważmy w tym celu, że zbiór P wielomianów postaci $f - g$, gdzie f, g są rosnącymi wielomianami o współczynnikach rzeczywistych, jest podprzestrzenią liniową przestrzeni liniowej wszystkich wielomianów o współczynnikach rzeczywistych. Wykażemy przez indukcję ze względu na n, że zbiór W_n wielomianów stopnia co najwyżej n jest zawarty w P.

Ponieważ $1 = (x+1) - x$ oraz $x+1$ i x są wielomianami rosnącymi, $1 \in P$, w konsekwencji, $W_0 \subseteq P$.

Zauważmy, że (dla $n \geq 1$) ciąg $1, x, \ldots, x^n$ jest bazą W_n. Jeśli więc $W_{n-1} \subseteq P$, to dla wykazania, że $W_n \subseteq P$ wystarczy stwierdzić, że $x^n \in P$. Jest to oczywiste w przypadku, gdy n jest liczbą nieparzystą, gdyż wówczas x^n jest wielomianem rosnącym i $x^n = 2x^n - x^n$. Jeśli n jest liczbą parzystą, to przedstawiamy x^n w postaci $x^n = \frac{1}{n+1}\left((x+1)^{n+1} - x^{n+1}\right) + h(x)$. Oczywiście, $h(x) \in W_{n-1} \subseteq P$ oraz $\frac{1}{n+1}\left((x+1)^{n+1} - x^{n+1}\right) \in P$, więc $x^n \in P$.

2. Rozważane w szkole ciągi geometryczny i arytmetyczny są przykładami tzw. ciągów rekurencyjnych, tj. ciągów, które są określone przez podanie wartości początkowych wyrazów i wzorów pozwalających wyznaczyć kolejne wyrazy w zależności od wyrazów poprzednich. I tak ciąg geometryczny jest określony przez warunki

$$a_0 = a\,, \quad a_{n+1} = a_n q \quad \text{dla} \quad n \geq 0\,,$$

ciąg arytmetyczny zaś przez warunki

$$a_0 = a\,, \quad a_1 = b\,, \quad 2a_{n+1} = a_n + a_{n+2} \quad \text{dla} \quad n \geq 0\,,$$

gdzie a, b i $q \neq 0$ są pewnymi ustalonymi liczbami.

Innym przykładem ciągu rekurencyjnego jest tzw. ciąg Fibonacciego określony przez warunki

$$f_0 = f_1\,, \quad f_{n+2} = f_{n+1} + f_n \quad \text{dla} \quad n \geq 0\,.$$

W przypadku ciągów geometrycznego i arytmetycznego łatwo wyznacza się wzory na dowolny wyraz (odpowiednio: $a_n = aq^n$ i $a_n = a + n(b-a)$.) Znalezienie podobnego wzoru dla ciągu Fibonacciego jest już znacznie trudniejsze. Przedstawię tu dwa sposoby (są również inne) rozwiązania tego zadania.

a. Rozważmy zbiór $\mathcal{F}$ wszystkich ciągów (a_n) o wyrazach rzeczywistych spełniających zależność

$$a_{n+2} = a_{n+1} + a_n\,, \quad n = 0, 1, 2, \ldots$$

Zbiór $\mathcal{F}$ z naturalnymi działaniami dodawania i mnożenia ciągów przez liczby rzeczywiste jest rzeczywistą przestrzenią liniową. Jest to przestrzeń dwuwymiarowa, gdyż, jak łatwo się przekonać, jej bazę tworzą ciągi

$$1,\ 0,\ 1,\ 1,\ 2,\ 3,\ \ldots$$
$$0,\ 1,\ 1,\ 1,\ 2,\ 3,\ \ldots$$

Idea polega teraz na znalezieniu w $\mathcal{F}$ bazy złożonej z ciągów, dla których łatwo wyznacza się wzór na wyraz ogólny, a następnie przedstawienie ciągu Fibonacciego jako kombinacji liniowej elementów tej bazy. Okazuje się, że taką wygodną bazę można znaleźć wśród ciągów geometrycznych należących do $\mathcal{F}$.

Zauważmy, że ciąg (g^n) gdzie $g \neq 0$ i $n = 0, 1, 2, \ldots$ należy do $\mathcal{F}$ wtedy i tylko wtedy, gdy

$$g^2 = g + 1\,.$$

Zatem ciągi (a^n) i (b^n), gdzie $a = \frac{1+\sqrt{5}}{2}$, $b = \frac{1-\sqrt{5}}{2}$ należą do $\mathcal{F}$. Łatwo się też zauważa, że $\{(a^n), (b^n)\}$ jest bazą tej przestrzeni. Istnieją więc liczby rzeczywiste A i B takie, że

(1) $$A(a^n) + B(b^n) = (f_n)\,.$$

Porównując pierwsze dwa wyrazy ciągów po lewej i prawej stronie (1) otrzymujemy układ równań

$$A + B = 1$$

$$A\frac{1+\sqrt{5}}{2} + B\frac{1-\sqrt{5}}{2} = 1$$

z którego wyliczamy, że $A = \frac{1+\sqrt{5}}{2\sqrt{5}}$ oraz $B = \frac{\sqrt{5}-1}{2\sqrt{5}}$. Wracając do (1) uzyskujemy wzór

(2) $$f_n = \frac{1+\sqrt{5}}{2\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1-\sqrt{5}}{2\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n =$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

b. Uzyskamy teraz wzór (2) wyliczając na dwa różne sposoby potęgi macierzy

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Zauważmy najpierw, że dla $n \geq 1$ jest

(3) $$M^{n+1} = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}.$$

Istotnie:

$$M^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} f_0 & f_1 \\ f_1 & f_2 \end{pmatrix};$$

zakładając dalej, że $M^{n+1} = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$ otrzymujemy

$$M^{n+2} = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_n & f_{n-1} + f_n \\ f_{n+1} & f_n + f_{n+1} \end{pmatrix} = \begin{pmatrix} f_n & f_{n+1} \\ f_{n+1} & f_{n+2} \end{pmatrix},$$

a więc wzór (3) jest prawdziwy na mocy zasady indukcji.

Zauważmy teraz, że jeśli

$$B = \begin{pmatrix} \lambda_2/\sqrt{5} & -1/\sqrt{5} \\ -\lambda_1/\sqrt{5} & 1/\sqrt{5} \end{pmatrix}, \quad \text{gdzie } \lambda_1 = \tfrac{1-\sqrt{5}}{2} \text{ i } \lambda_2 = \tfrac{1+\sqrt{5}}{2},$$

$$\text{to } B^{-1} = \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \quad \text{oraz} \quad M = B^{-1}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}B.$$

Zależności te łatwo się sprawdza wykonując bezpośrednie rachunki. Wynikają one także z ogólnych zależności między macierzami danego przekształcenia liniowego w różnych bazach. W naszym przypadku należy rozważyć przekształcenie dwuwymiarowej przestrzeni kartezjańskiej $\mathbf{R}^2$ w siebie określone wzorem

$$f(x_1, x_2) = (x_2, x_1 + x_2)\,.$$

Macierzą tego przekształcenia w bazie $\{(1,0), (0,1)\}$ jest M. Wektory $(1, \lambda_1)$, $(1, \lambda_2)$ są wektorami własnymi przekształcenia f, którym odpowiadają wartości własne, odpowiednio, λ_1 i λ_2. W bazie $\{(1, \lambda_1), (1, \lambda_2)\}$ przekształcenie f ma macierz $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. B oraz B^{-1} są odpowiednio macierzami przejścia z bazy $\{(1,0), (0,1)\}$ do bazy $\{(1, \lambda_1), (1, \lambda_2)\}$ i na odwrót. W efekcie

$$M = B^{-1}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}B.$$

Z powyższych zależności otrzymujemy, że dla $n \geq 1$

$$\begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix} = M^{n+1} = \left(B^{-1}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} B\right)^{n+1} =$$

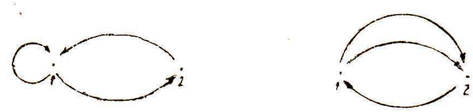
$$= B^{-1}\begin{pmatrix} \lambda_1^{n+1} & 0 \\ 0 & \lambda_2^{n+1} \end{pmatrix} B =$$

$$= \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix}\begin{pmatrix} \lambda_1^{n+1} & 0 \\ 0 & \lambda_2^{n+1} \end{pmatrix}\begin{pmatrix} \lambda_2/\sqrt{5} & -1/\sqrt{5} \\ -\lambda_1/\sqrt{5} & 1/\sqrt{5} \end{pmatrix},$$

skąd wyliczamy, że

$$f_n = \frac{1}{\sqrt{5}}(\lambda_2^{n+1} - \lambda_1^{n+1}) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

3. Załóżmy, że G jest grafem zorientowanym o wierzchołkach ponumerowanych liczbami $1, 2, \ldots, m$, w którym z i-tego wierzchołka prowadzi a_{ij} krawędzi do wierzchołka j-tego (a_{ij} są liczbami całkowitymi nieujemnymi, na ogół $a_{ij} \neq a_{ji}$). Szczególnym przykładem są następujące grafy o dwóch wierzchołkach:



w pierwszym przypadku $a_{11} = a_{12} = a_{21} = 1$ i $a_{22} = 0$, w drugim zaś $a_{11} = a_{22} = 0$, $a_{12} = 2$ i $a_{21} = 1$.

Drogą o długości n w grafie G nazywamy ciąg $k_1 \ldots k_n$, gdzie k_i jest krawędzią prowadzącą z wierzchołka p_1 do wierzchołka q_i, przy czym $q_l = p_{l+1}$ dla $l = 1, 2, \ldots, n-1$.

Oznaczmy przez d_n liczbę wszystkich dróg długości n w grafie G. W naszych przykładach $d_n = d_n^{(1)} + d_n^{(2)}$, gdzie $d_n^{(i)}$ oznacza liczbę dróg długości n kończących się w i-tym wierzchołku. Łatwo zauważyć, że w pierwszym z tych przykładów $d_{n+1}^{(1)} = d_n^{(1)} + d_n^{(2)}$ oraz $d_{n+1}^{(2)} = d_n^{(1)}$, skąd otrzymujemy, że $d_{n+2} = d_{n+1} + d_n$. Podobnie można stwierdzić, że dla dowolnego z tych grafów $d_{n+2} = 2d_n$. W obu więc przypadkach d_n jest ciągiem rekurencyjnym. Wykażę, że jest tak dla dowolnego grafu G. Dokładniej: dla dowolnego grafu G istnieją takie liczby rzeczywiste $a_0, \ldots, a_k$, że dla dowolnego $n \geq 1$

$$d_{n+k+1} = a_k d_{n+k} + a_{k-1}d_{n+k-1} + \ldots + a_0 d_n.$$

Zauważmy, że liczba b_{ij} dróg o długości 2 w grafie G, które zaczynają się w i-tym, a kończą w j-tym wierzchołku, jest równa $\sum_{l=1}^{m} a_{il}a_{lj}$. Oznacza to, że jeśli $A = (a_{ij})$ jest macierzą utworzoną z liczb a_{ij} i jeśli $B = (b_{ij})$ jest macierzą utworzoną z liczb b_{ij}, to $B = A^2$. Ogólniej, wyrazy d_{ij} macierzy A^n są równe liczbie dróg długości n zaczynających się w i-tym i kończących w j-tym wierzchołku. Oczywiście d_n jest sumą wszystkich d_{ij}.

Zbiór wszystkich $(m \times m)$-macierzy o wyrazach rzeczywistych jest rzeczywistą przestrzenią liniową wymiaru m^2. Wynika stąd w szczególności, że zbiór $\{A^0, A^1, A^2, \ldots\}$ jest liniowo zależny. Oznacza to, że istnieją takie liczby rzeczywiste $a_0, a_1, \ldots, a_k$, że

W tym miejscu można by wykorzystać twierdzenie Cayleya–Hamiltona, które mówi, że każda macierz kwadratowa spełnia swój wielomian charakterystyczny. Korzystając z tego twierdzenia uzyskalibyśmy dodatkowo, że a_i są liczbami całkowitymi oraz $k \leq m-1$.

$$A^{k+1} = a_k A^k + a_{k-1}A^{k-1} + \ldots + a_0 A^0. \tag{4}$$

Mnożąc równość (4) przez A^n otrzymujemy

$$A^{n+k+1} = a_k A^{n+k} + \ldots + a_0 A^n,$$

skąd wynika, że

$$d_{n+k+1} = a_k d_{n+k} + \ldots + a_0 d_n.$$

4. Dany jest ciąg liczb całkowitych $a_1, a_2, \dots, a_{2n+1}$ o następującej własności: po odrzuceniu dowolnego wyrazu pozostałe można podzielić na takie dwie grupy po n wyrazów, że suma wyrazów w pierwszej grupie jest równa sumie wyrazów w drugiej. Wykażę, że $a_1 = a_2 = \dots = a_{2n+1}$.

Gdyby bowiem tak nie było, to wśród różnic $a_i - a_j$ moglibyśmy wybrać tę, która dzieli się przez najniższą potęgę dwójki. Bez zmniejszenia ogólności możemy założyć, że tą wybraną jest różnica $a_1 - a_2$. Z warunków zadania wynika, że jeśli

$$s = a_1 + a_2 + \dots + a_{2n+1},$$

to dla pewnych $a_{i_1}, \dots, a_{i_n}, a_{j_1}, \dots, a_{j_n}$ jest

$$s - a_1 = 2(a_{i_1} + \dots + a_{i_n}) \quad \text{oraz} \quad s - a_2 = 2(a_{j_1} + \dots + a_{j_n}).$$

Wynika stąd, że

$$a_1 - a_2 = 2\big((a_{j_1} - a_{i_1}) + (a_{j_2} - a_{i_2}) + \dots + (a_{j_n} - a_{i_n})\big).$$

To jednak przeczy uczynionemu założeniu o minimalności $a_1 - a_2$.

Powyższe rozumowanie jest zupełnie elementarne i opiera się na prostym pomyśle dotyczącym podzielności przez potęgi dwójki. Może wydać się to nieprawdopodobne, ale to samo rozumowanie można zastosować również w przypadku, gdy a_i są liczbami rzeczywistymi.

Tutaj jednak trzeba posłużyć się tzw. normą dwuadyczną. Przytoczę teraz to rozumowanie (jego autorem jest dr P. Grzeszczuk), a później wykażę, jak to zadanie (dla liczb rzeczywistych) można rozwiązać stosując metody algebry liniowej.

Norma dwuadyczna jest to funkcja f określona na liczbach rzeczywistych, przyjmująca wartości rzeczywiste nieujemne i spełniająca warunki

1. $f(a) = 0$ wtedy i tylko wtedy, gdy $a = 0$;
2. $f(ab) = f(a)f(b)$;
3. $f(a+b) \leq \max(f(a), f(b))$;
4. $f(2) = \frac{1}{2}$.

Załóżmy teraz, że $a_1, \dots, a_{2n+1}$ są liczbami rzeczywistymi spełniającymi warunki twierdzenia. Bez zmniejszenia ogólności możemy założyć, że

$$f(a_1 - a_2) = \max_{1 \leq i < j < 2n+1} f(a_i - a_j).$$

Tak jak wyżej wykazujemy, że

$$a_1 - a_2 = 2\big((a_{j_1} - a_{i_1}) + \dots + (a_{j_n} - a_{i_n})\big).$$

Teraz

$$0 \leq f(a_1 - a_2) \leq \frac{1}{2}\max\big(f(a_{j_1} - a_{i_1}, \dots, f(a_{j_n} - a_{i_n})\big) \leq \frac{1}{2} f(a_1 - a_2).$$

Zatem $f(a_1 - a_2) = 0$ i w konsekwencji $f(a_i - a_j) = 0$ dla $i < j$. To dowodzi, że $a_i = a_j$ dla dowolnych i, j.

Udowodnię teraz powyższe twierdzenie (dla liczb rzeczywistych) stosując metody algebry liniowej. Ten dowód jest w gruncie rzeczy dużo prostszy od poprzedniego (mimo, że wydaje się być bardziej skomplikowany), gdyż nie używa się w nim normy dwuadycznej, a dowód istnienia normy dwuadycznej na zbiorze liczb rzeczywistych wymaga użycia zaawansowanych technik algebraicznych.

Zauważmy, że jeśli liczby rzeczywiste $a_1, \dots, a_{2n+1}$ spełniają warunki twierdzenia, to również liczby $b_1 = a_1 - a_{2n+1}$, $b_2 = a_2 - a_{2n+1}$, …, $b_{2n+1} = a_{2n+1} - a_{2n+1} = 0$ też spełniają te warunki. Mamy wykazać, że $b_1 = \dots = b_{2n+1} = 0$. Z warunków twierdzenia zastosowanych do ciągu $b_1, b_2, \dots, b_{2n}, b_{2n+1} = 0$, w którym pomijamy kolejno wyrazy $b_1, \dots, b_{2n}$ wynika, że istnieją takie liczby $e_{i,j}$, $1 \leq i, j \leq 2n$, że

Warunki twierdzenia niosą więcej informacji, te jednak już nam wystarczą.

i) $e_{i,i} = 0$,

ii) $e_{i,j} = \pm 1$ dla $i \neq j$,

iii) $$\begin{cases} e_{1,1}b_1 + e_{1,2}b_2 + \dots + a_{1,2n}b_{2n} = 0 \\ \dots \\ e_{2n,1}b_1 + e_{2n,2}b_2 + \dots + a_{2n,2n}b_{2n} = 0 \end{cases}$$

Korzystając ze wzorów Cramera wystarczy wykazać, że wyznacznik macierzy

$$\begin{bmatrix} e_{1,1} & \dots & e_{1,2n} \\ \vdots & \ddots & \vdots \\ e_{2n,1} & \dots & e_{2n,2n} \end{bmatrix}$$

jest różny od zera. Zauważmy, że reszta z dzielenia tego wyznacznika przez 2 jest równa reszcie z dzielenia przez 2 wyznacznika macierzy stopnia $2n$

$$M = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 0 \end{bmatrix}.$$

Ta ostatnia reszta jest równa zero wtedy i tylko wtedy, gdy reszta z dzielenia przez 2 wyznacznika macierzy M^2 jest równa zero (korzystamy tu z twierdzenia, że wyznacznik iloczynu dwóch macierzy tego samego stopnia jest równy iloczynowi ich wyznaczników). Zobaczmy jednak, że

$$M^2 = \begin{bmatrix} 2n-1 & 2n-2 & \dots & 2n-2 \\ 2n-2 & 2n-1 & \dots & 2n-2 \\ \vdots & \vdots & \ddots & \vdots \\ 2n-2 & 2n-2 & \dots & 2n-1 \end{bmatrix},$$

czyli interesująca nas reszta jest równa 1. To kończy dowód.