Jest to zapis odczytu wygłoszonego na XX Ogólnopolskim Sejmiku Matematycznym, czerwiec 2008.

O metodzie probabilistycznej Paula Erdősa

Tomasz KOCHANEK, Katowice

Artykuł poświęcony jest tzw. metodzie probabilistycznej dowodzenia istnienia obiektów kombinatorycznych o zadanych własnościach, za której twórcę uznaje się węgierskiego matematyka Paula Erdősa.

Wiele ciekawych problemów matematyki dyskretnej dotyczy istnienia pewnych obiektów kombinatorycznych. Choć naturalną i często przyjmowaną metodą postępowania jest próba ich konstrukcji, to zdarza się, że w pewnych sytuacjach żądanego obiektu skonstruować ani wskazać nie potrafimy. Niemniej, poprzez pewne rozumowania natury probabilistycznej, umiemy czasami wykazać ich istnienie. Za pioniera i głównego twórcę *metody probabilistycznej* uznaje się wybitnego węgierskiego matematyka Paula Erdősa, który po raz pierwszy użył jej w 1947 roku w celu uzyskania oszacowań od dołu tzw. liczb Ramseya. Dziś można stwierdzić, że metoda ta aplikuje się w takich dziedzinach matematyki jak m.in. teoria liczb, teoria grafów, geometria kombinatoryczna czy nawet teoria miar wektorowych. W celu dobrego zrozumienia prostej, bądź co bądź, idei stojącej u jej podstaw przeanalizujemy na początek dwa nietrudne problemy. Pierwszy z nich pochodzi z 15. Międzynarodowego Konkursu Matematycznego dla studentów im. Vojtěcha Jarníka (Ostrawa, 2005), natomiast drugi można nazwać „problemem równoważących się wektorów" i jest on szczególnym przypadkiem lematu Steinitza, o którym w dalszej części tekstu wspomnimy.

Zadanie 1. *Niech $(a_{ij})_{i,j=1}^n$ będzie taką macierzą o elementach będących liczbami rzeczywistymi, że $a_{ii} = 0$ dla każdego $i \in \{1, \ldots, n\}$. Wykazać, że istnieje taki zbiór indeksów $J \subset \{1, \ldots, n\}$, że*

$$\sum_{\substack{i \in J \\ j \notin J}} a_{ij} + \sum_{\substack{i \notin J \\ j \in J}} a_{ij} \geqslant \frac{1}{2} \sum_{i,j=1}^{n} a_{ij}. \tag{1}$$

Rozwiązanie. Rozważmy rodzinę $\mathcal{R}$ wszystkich podzbiorów zbioru $\{1, \ldots, n\}$ i dla każdego $J \in \mathcal{R}$ oznaczmy przez $s(J)$ lewą stronę nierówności (1) (umawiając się przy tym, że $s(\emptyset) = s(\{1, \ldots, n\}) = 0$). Rozważmy średnią tych liczb $\overline{s} = \frac{1}{2^n} \sum_{J \in \mathcal{R}} s(J)$. Zauważmy, że każdy element postaci a_{ij}, dla $i \neq j$, wystąpi tyle razy w powyższej sumie, na ile sposobów można dobrać zbiór $J \in \mathcal{R}$ spełniający warunki: $i \in J$, $j \notin J$ lub $i \notin J$, $j \in J$. Można to zrobić przez wybór dowolnego podzbioru zbioru $\{1, \ldots, n\} \setminus \{i, j\}$ i doklejeniu do niego jednego z elementów i, j, a zatem możliwości jest $2 \cdot 2^{n-2} = 2^{n-1}$. W konsekwencji

$$\overline{s} = \frac{2^{n-1}}{2^n} \sum_{i \neq j} a_{ij} = \frac{1}{2} \sum_{i,j=1}^{n} a_{ij}.$$

Wykazaliśmy przeto, że arytmetyczna średnia wszystkich możliwych wartości lewej strony nierówności (1) równa jest jej prawej stronie. To zaś oznacza, że dla przynajmniej jednego konkretnego wyboru zbioru $J \in \mathcal{R}$ nierówność (1) zachodzi. □

Zadanie 2. *Niech $\|\boldsymbol{x}\|$ oznacza długość euklidesową wektora $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, tj. $\|\boldsymbol{x}\| = (x_1^2 + \ldots + x_n^2)^{1/2}$. Załóżmy, że $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^n$ oraz $\|\boldsymbol{x}_i\| \leqslant 1$ dla każdego $i \in \{1, \ldots, n\}$. Wykazać, że istnieją takie liczby $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$, że*

$$\Big\| \sum_{i=1}^{n} \varepsilon_i \boldsymbol{x}_i \Big\| \leqslant \sqrt{n}. \tag{2}$$

Rozwiązanie. Rozważmy rodzinę $\mathcal{R}$ wszystkich n-elementowych ciągów o wyrazach ze zbioru $\{-1, 1\}$ i dla każdego $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \mathcal{R}$ oznaczmy przez $s(\boldsymbol{\varepsilon})$ lewą stronę nierówności (2). Korzystając z własności iloczynu skalarnego $(\cdot|\cdot)$

w przestrzeni $\mathbb{R}^n$ możemy napisać

$$s(\boldsymbol{\varepsilon})^2 = \Big(\sum_{i=1}^n \varepsilon_i \boldsymbol{x}_i \Big| \sum_{i=1}^n \varepsilon_i \boldsymbol{x}_i\Big) = \sum_{i=1}^n \|\boldsymbol{x}_i\|^2 + \sum_{i\neq j} \varepsilon_i\varepsilon_j(\boldsymbol{x}_i|\boldsymbol{x}_j)$$
$$\leqslant n + \sum_{i\neq j} \varepsilon_i\varepsilon_j(\boldsymbol{x}_i|\boldsymbol{x}_j).$$

Zatem, biorąc pod uwagę średnią kwadratów $\overline{s^2} = \frac{1}{2^n}\sum_{\boldsymbol{\varepsilon}\in\mathcal{R}} s(\boldsymbol{\varepsilon})^2$, otrzymujemy

$$\overline{s^2} \leqslant n + \frac{1}{2^n}\sum_{\boldsymbol{\varepsilon}\in\mathcal{R}}\sum_{i\neq j} \varepsilon_i\varepsilon_j(\boldsymbol{x}_i|\boldsymbol{x}_j).$$

Zauważmy jednak, że występująca powyżej suma podwójna jest równa 0. Istotnie, dla dowolnej takiej pary indeksów i, j, że $i \neq j$, ilość tych ciągów $\boldsymbol{\varepsilon} \in \mathcal{R}$, dla których $\varepsilon_i\varepsilon_j = 1$, wynosi 2^{n-1} – podobnie jak ilość tych, dla których $\varepsilon_i\varepsilon_j = -1$. Wynika stąd, że współczynniki stojące przy każdym z iloczynów $(\boldsymbol{x}_i|\boldsymbol{x}_j)$ sumują się do 0. W konsekwencji $\overline{s^2} \leqslant n$, a więc dla pewnego ciągu $\boldsymbol{\varepsilon} \in \mathcal{R}$ musi być $s(\boldsymbol{\varepsilon}) \leqslant \sqrt{n}$. □

Przedstawiona tutaj prosta argumentacja działa tylko w przypadku, gdy ilość danych wektorów nie przekracza wymiaru przestrzeni. Okazuje się jednak, że teza zadania 2 pozostaje w mocy również dla dowolnej skończonej ilości wektorów $\boldsymbol{x}_i$, dla których $\|\boldsymbol{x}_i\| \leqslant 1$. Stanowi to treść lematu Steinitza. Jego dowód jest nieco trudniejszy od zaprezentowanego powyżej, choć używa tylko elementarnych faktów z algebry liniowej. Czytelnik jest gorąco zachęcany do samodzielnej próby jego znalezienia.

Idea rozwiązań obu zadań była ta sama. Zamiast konstrukcji konkretnego zbioru czy też ciągu, rozważyliśmy rodzinę wszelkich możliwych do uzyskania wartości danego wyrażenia dowodząc, że ich średnia spełnia odpowiedni warunek. Na tym właśnie polega metoda probabilistyczna. Chcąc udowodnić istnienie pewnego obiektu pokazujemy, że prawdopodobieństwo jego wyboru jest dodatnie (przy odpowiednio zbudowanej przestrzeni probabilistycznej), bądź też – że wartość oczekiwana pewnej zmiennej losowej spełnia odpowiedni warunek. I choć często tego typu rozwiązania dają się zapisać bez użycia terminologii probabilistycznej (o czym świadczą chociażby powyższe przykłady), to już samo podejście do problemu w sposób „probabilistyczny" często ułatwia sprawę.

Pokażemy teraz znacznie mniej trywialne zastosowanie omawianej metody. Zbiór $A \subset \mathbb{Z} \setminus \{0\}$ nazwiemy *wolnym od sum*, jeżeli dla dowolnych $a, b \in A$ mamy $a + b \notin A$. Dowód następującego rezultatu stanowi piękne połączenie metody probabilistycznej z metodami algebry i teorii liczb.

Twierdzenie (P. Erdős, 1965). *Każdy n-elementowy zbiór niezerowych liczb całkowitych zawiera wolny od sum podzbiór posiadający więcej niż $\frac{n}{3}$ elementów.*

Pomysł Erdősa polegał na tym, by w pierwszym kroku „przerzucić" nasze rozważania na lepiej zbadany grunt. Niech $A = \{a_1, \ldots, a_n\}$ będzie dowolnym n-elementowym zbiorem niezerowych liczb całkowitych. Zamiast operować na zbiorze A (o którym właściwie nic nie wiemy) zajmiemy się strukturą, z której bardzo łatwo wybrać pewien „spory" podzbiór wolny od sum. Strukturą tą jest grupa $\mathbb{Z}_l = \{0, 1, \ldots, l-1\}$ (gdzie $l \in \mathbb{N}$) z działaniem dodawania modulo l, tzn. dla $a, b \in \mathbb{Z}_l$ sumę $a \oplus b$ określamy jako resztę z dzielenia zwykłej sumy $a + b$ przez liczbę l. Zauważmy, że jeżeli l jest liczbą postaci $l = 3k + 2$ dla pewnego $k \in \mathbb{N}$, to zbiór

$$C = \{k + 1, k + 2, \ldots, 2k + 1\} \subset \mathbb{Z}_l$$

jest zbiorem wolnym od sum (modulo l). Rzeczywiście, dwie „skrajne" możliwości dają bowiem

$$(k + 1) \oplus (k + 1) = 2k + 2 \notin C \quad \text{oraz} \quad (2k + 1) \oplus (2k + 1) = k \notin C.$$

Zauważmy dalej, że zbiór C stanowi więcej niż trzecią część całego zbioru $\mathbb{Z}_l$, a więc wydaje się być dla nas dobrym kandydatem. Dokonajmy zatem „zanurzenia" naszego zbioru A w grupę $\mathbb{Z}_l$ patrząc na każdy element $a_i \in A$ jak na jego resztę z dzielenia przez l.

Niestety nie widać żadnego powodu, dla którego jakiekolwiek elementy zbioru A miałyby zostać zanurzone w wyselekcjonowany przez nas zbiór C. Aby wybrnąć z tego problemu, posłużymy się działaniem mnożenia modulo l, tzn. dla dowolnych $a, b \in \mathbb{Z}_l$ iloczyn $a \odot b$ określamy jako resztę z dzielenia zwykłego iloczynu ab przez liczbę l. Zamiast patrzeć na pojedyncze elementy $a_i \in A$ spróbujmy „przefiltrować" je przez cały zbiór $\mathbb{Z}_l \setminus \{0\}$ rozważając iloczyny $a_i \odot x$ dla $x \in \mathbb{Z}_l \setminus \{0\}$. Aby iloczyny te faktycznie przebiegały zbiór $\mathbb{Z}_l \setminus \{0\}$, musimy rzecz jasna zagwarantować, by $a_i \neq 0 \pmod{l}$. Da się to łatwo zrobić dobierając liczbę l tak, aby $l > \max_{1 \leqslant i \leqslant n} |a_i|$. Czy to jednak wystarcza? Powołamy się w tym miejscu na następujący fakt (nieznający go Czytelnik może sięgnąć np. po książkę W. Narkiewicza [1, Rozdział 2]). Mianowicie, jeżeli l jest liczbą *pierwszą*, to dla każdego $y \in \mathbb{Z}_l \setminus \{0\}$ funkcja $x \mapsto y \odot x$ jest bijekcją zbioru $\mathbb{Z}_l \setminus \{0\}$. Czy można jednak znaleźć liczbę pierwszą $l = 3k + 2$ większą od $\max_{1 \leqslant i \leqslant n} |a_i|$? Z pomocą przychodzi nam tu *twierdzenie Dirichleta*: dla dowolnych względnie pierwszych liczb $q, r \in \mathbb{N}$ istnieje nieskończenie wiele liczb pierwszych postaci $qk + r$. Dowód tego rezultatu jest trudny; można znaleźć go np. w [1, Rozdział 5]. Przejdźmy w końcu do sformalizowania naszych rozważań.

Dowód twierdzenia Erdősa. Niech l będzie dowolną liczbą pierwszą postaci $l = 3k + 2$, większą od $\max_{1 \leqslant i \leqslant n} |a_i|$. Potraktujmy $\mathbb{Z}_l \setminus \{0\}$ jako przestrzeń probabilistyczną, w której wybór każdego z jej elementów jest tak samo prawdopodobny. Dla każdego $i \in \{1, \ldots, n\}$ wzór $f_i(x) = a_i \odot x$ określa zmienną losową odwzorowującą zbiór $\mathbb{Z}_l \setminus \{0\}$ na siebie. Prawdopodobieństwo tego, że jej wartość wpada do zbioru C wynosi:

$$\boldsymbol{P}(f_i(x) \in C) = \frac{\#C}{l-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Rozważmy zmienną losową daną wzorem $\nu(x) = \#\{i : f_i(x) \in C\}$. Oszacujemy jej wartość średnią (oczekiwaną) $\boldsymbol{E}\nu$. Wygodnie w tym celu będzie posłużyć się funkcją charakterystyczną χ_C zbioru C określoną jako

$$\chi_C(x) = \begin{cases} 1, \text{ gdy } x \in C, \\ 0, \text{ gdy } x \notin C. \end{cases}$$

Mamy mianowicie:

$$\begin{aligned} \boldsymbol{E}\nu &= \frac{1}{l-1} \sum_{x \in \mathbb{Z}_l \setminus \{0\}} \nu(x) = \frac{1}{l-1} \sum_{x \in \mathbb{Z}_l \setminus \{0\}} \sum_{i=1}^{n} \chi_C(f_i(x)) \\ &= \sum_{i=1}^{n} \frac{1}{l-1} \sum_{x \in \mathbb{Z}_l \setminus \{0\}} \chi_C(f_i(x)) = \sum_{i=1}^{n} \boldsymbol{P}(f_i(x) \in C) > \frac{1}{3} n. \end{aligned}$$

Dowodzi to, że dla choć jednego $x \in \mathbb{Z}_l \setminus \{0\}$ mamy $\nu(x) > \frac{1}{3}n$, czyli $a_i \odot x \in C$ dla wszystkich $i \in J$, przy czym $\#J > \frac{1}{3}n$. Dla żadnych $i, j, k \in J$ nie może zachodzić równość $a_i + a_j = a_k$. Implikowałaby bowiem ona, że $(a_i \odot x) \oplus (a_j \odot x) = a_k \odot x$, co jest niemożliwe, gdyż wszystkie te składniki należą do zbioru C. □

Rozwinięcie metody probabilistycznej uznawane jest za jedno z największych osiągnięć w imponującym dorobku naukowym Paula Erdősa. Wiele dalszych różnorodnych jej zastosowań można znaleźć w książce Z. Palki i A. Rucińskiego [2], do sięgnięcia po którą Czytelnik jest gorąco zachęcany.

Literatura

[1] W. Narkiewicz, *Teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2003.

[2] Z. Palka, A. Ruciński, *Niekonstruktywne metody matematyki dyskretnej*, Wydawnictwa Naukowo-Techniczne, Warszawa 1996.