Ile jest podprzestrzeni?

Zofia MIECHOWICZ, Tomasz BARTNICKI**

* Wydział Matematyki, Informatyki i Ekonometrii, Uniwersytet Zielonogórski

Jaka jest liczba różnych k-elementowych podzbiorów zbioru n-elementowego? Jest to jedno z pierwszych pytań, które zadajemy sobie, zaczynając zajmować się elementarną kombinatoryką. Wkrótce dowiadujemy się, że liczbę tę oznacza się przez $\binom{n}{k}$ (symbol Newtona), a następnie poznajemy różne metody jej wyznaczania.

Niestety, w „matematyce szkolnej" równość $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ często podaje się jako definicję symbolu Newtona, a dopiero później przedstawia jej interpretację kombinatoryczną.

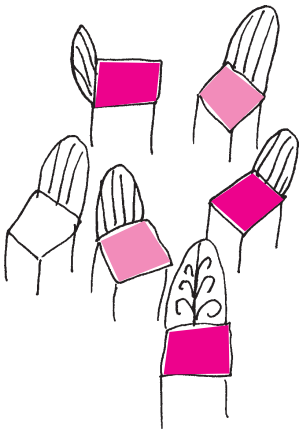
Wyjściowe pytanie o liczbę podzbiorów przeniesiemy na nieco wyższy poziom abstrakcji, zmieniając w nim kilka pojęć. Słowo *zbiór* zamienimy na *przestrzeń liniowa nad ciałem skończonym*, *podzbiór* na *podprzestrzeń*. Zamiast *mocy zbioru* (w tym przypadku liczby elementów) będziemy rozważać *wymiar przestrzeni*. Możemy teraz zadać analogiczne pytanie w świecie przestrzeni liniowych. *Jaka jest liczba różnych k-wymiarowych podprzestrzeni liniowych przestrzeni n-wymiarowej nad q-elementowym ciałem?* Zanim poznamy odpowiedź na to pytanie, przybliżymy pojęcia, których ono dotyczy.

Rozważmy zbiór reszt z dzielenia przez liczbę pierwszą p z dodawaniem i mnożeniem modulo p. Dla przykładu, przy $p = 11$ mamy $7 \oplus 8 = 4$ oraz $4 \odot 5 = 9$. Działania te mają, przedstawione na marginesie, naturalne własności, dzięki czemu zaprezentowaną strukturę możemy nazywać *ciałem* (które, rzecz jasna, jest *skończone*). Przedstawiony sposób nie jest jedynym, w jaki można otrzymać skończone ciało – na potrzeby naszych rozważań istotny jest jednak tylko fakt, że takie struktury istnieją.

Dla każdego z działań $\oplus$ i $\odot$ ich wynik nie zależy od kolejności argumentów (symetria) oraz kolejności ich wykonywania (łączność). Dodanie reszty 0 oraz pomnożenie przez resztę 1 nic nie zmienia, a dla każdej reszty niezerowej istnieje reszta do niej przeciwna i reszta do niej odwrotna. Ponadto, resztowe mnożenie jest rozdzielne względem resztowego dodawania.
Istnieją ciała, których liczba elementów jest potęgą liczby pierwszej, ale ich konstrukcja jest nieco bardziej skomplikowana. Warto jednak zaznaczyć, że dla zadanej liczby $q = p^k$ istnieje dokładnie jedno ciało q-elementowe, z dokładnością do izomorfizmu, czyli „nazewnictwa" elementów. Podobnie jest dla n-wymiarowych przestrzeni liniowych nad zadanym ciałem skończonym. Zawsze mają one $q^n = p^{kn}$ wektorów i są izomorficzne.

Niech $\mathbb{F}$ będzie ciałem skończonym. Rozważmy zbiór wszystkich n-elementowych ciągów liczb z $\mathbb{F}$, czyli $\mathbb{F}^n$. Takie ciągi można w naturalny sposób dodawać i mnożyć przez liczby z $\mathbb{F}$, na przykład (wracając do opisanego wcześniej ciała reszt z dzielenia przez 11 oraz biorąc $n = 2$) mamy $(7, 3) + (8, 10) = (4, 2)$ oraz $5 \cdot (7, 3) = (2, 4)$. Działania te są „porządne", to znaczy spełniają prawa łączności, przemienności i rozdzielności. Sprawia to, że $\mathbb{F}^n$ możemy traktować jako *przestrzeń liniową* nad ciałem $\mathbb{F}$; jej elementy będziemy nazywać *wektorami*.

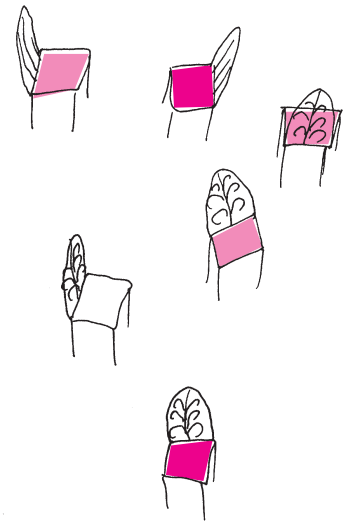
Niektóre podzbiory $\mathbb{F}^n$ są bardzo szczególne i nie można z nich „uciec", dodając dowolne dwa ich elementy oraz mnożąc je przez liczbę z $\mathbb{F}$. Takie zbiory nazywamy *podprzestrzeniami* wyjściowej przestrzeni – nazwa jest bardzo naturalna, gdyż podprzestrzenie same w sobie mogą być traktowane jako przestrzenie liniowe nad rozważanym ciałem. Przykładem jest zbiór ciągów stałych. Nieco ogólniej, wystarczy wziąć dowolny wektor v z naszej przestrzeni i rozpatrzeć zbiór jego wielokrotności, tzn. wektorów postaci $a \cdot v$ dla $a \in \mathbb{F}$. Podprzestrzenie tej postaci nazywamy *jednowymiarowymi*. Jak możemy zwiększyć ich wymiar? Wystarczy znaleźć wektor w spoza tej podprzestrzeni i rozważyć zbiór wektorów postaci $a \cdot v + b \cdot w$ (są to *kombinacje liniowe* wektorów v i w) – to też będzie podprzestrzeń, już dwuwymiarowa. Ogólnie, podprzestrzeń k-wymiarowa składa się z kombinacji liniowych układu k wektorów o tej własności, że żaden z nich nie jest kombinacją liniową pozostałych (o takim układzie mówimy, że jest *liniowo niezależny*).



Możemy już przejść do wyjściowego pytania. Przestrzeń $\mathbb{F}^n$ składa się z q^n wektorów (gdzie q to liczba elementów $\mathbb{F}$). Chcemy wyznaczyć liczbę jej różnych k-wymiarowych podprzestrzeni liniowych. Będziemy ją oznaczać przez $\binom{n}{k}_q$.

Do opisania podprzestrzeni k-wymiarowej wystarczy wskazać k liniowo niezależnych wektorów $v_1, \ldots, v_k$ z tej przestrzeni. Ponieważ poruszamy się po przestrzeni nad ciałem skończonym, to wyznaczenie liczby takich k-tek sprowadza się do prostego przeliczenia. Wybierzmy najpierw wektor v_1. Jedyne, o co musimy się zatroszczyć, to żeby był on różny od wektora zerowego. Ze wszystkich q^n wektorów, które są dostępne, musimy wykluczyć tylko ten jeden. Wektor v_1 możemy zatem wybrać na $q^n - 1$ sposobów.

Na wektor v_2 mamy już odrobinę mniej kandydatów. Nie może on należeć do podprzestrzeni rozpinanej przez wektor v_1. Elementów tej podprzestrzeni jest



tyle, na ile sposobów możemy pomnożyć ten wektor przez element ciała F (tych elementów jest q). Wektor v_2 wybieramy zatem na $q^n - q$ sposobów.

Wektor v_3 nie może należeć do podprzestrzeni rozpiętej przez oba wcześniej wybrane. Wykluczamy więc dokładnie q^2 wektorów.

Jeżeli wybraliśmy już l wektorów, to kolejny nie może być kombinacją liniową poprzednich, w związku z czym mamy już tylko $q^n - q^l$ możliwości. Różnych k-tek wektorów niezależnych mamy więc

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{k-1}).$$

Oczywiście, niektóre układy wektorów generują te same podprzestrzenie, nas interesują te generujące różne. Każdą podprzestrzeń wymiaru k możemy uzyskać na tyle sposobów, ile różnych k-tek wektorów niezależnych w niej znajdziemy. Wiemy dokładnie, ile jest takich k-tek (przed chwilą właśnie to policzyliśmy!):

$$(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1}).$$

Zatem ostatecznie szukana przez nas liczba wyraża się następująco:

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

Wzór ten nie jest nowy, a dobór oznaczenia nie jest przypadkowy. Formuła ta nazywana jest *współczynnikiem dwumianowym Gaussa*, a pierwszy raz została użyta przez tego słynnego matematyka do znalezienia wzoru na tak zwane sumy Gaussa. Ale czy ma ona, oprócz nazwy, jakiś bliższy związek ze współczynnikiem dwumianowym Newtona? Przyjrzyjmy się bliżej. Przypomnijmy, że zachodzi algebraiczna równość $q^s - 1 = (q-1)\sum_{i=0}^{s-1} q^i$, w związku z czym powyższy ułamek można „skrócić" przez $(q-1)^k$, otrzymując

$$(\star) \qquad \binom{n}{k}_q = \frac{\sum_{i=0}^{n-1} q^i \cdot \sum_{i=0}^{n-2} q^i \cdot \ldots \cdot \sum_{i=0}^{n-k} q^i}{\sum_{i=0}^{k-1} q^i \cdot \sum_{i=0}^{k-2} q^i \cdot \ldots \cdot \sum_{i=0}^{0} q^i}$$

Jeżeli zatem potraktujemy $\binom{n}{k}_q$ jak funkcję zmiennej rzeczywistej q, dostaniemy $\binom{n}{k}_1 = \binom{n}{k}$. Widzimy więc wyraźnie, że coś jest na rzeczy. Tylko, że po analitycznym podejściu do sprawy trudno nam powiedzieć coś oprócz tego, iż zależność (której zresztą się spodziewaliśmy) istnieje. A gdybyśmy chcieli poczuć jej istotę? Zrozumieć charakter? W tym celu musimy się udać po pomoc do Donalda Knutha, który podszedł do sprawy z zupełnie innej strony.

Donald Ervin Knuth (ur. 10 stycznia 1938 r.) – amerykański matematyk i informatyk. Jeden z pionierów informatyki, jest znany m.in. z wielotomowego dzieła *Sztuka programowania*. Jest też autorem systemu składu drukarskiego TEX.

Spróbujmy jeszcze raz zliczyć podprzestrzenie wymiaru k, tym razem innym sposobem. Po pierwsze, umieśćmy wektory $v_1, \ldots, v_k$ w macierzy, jako jej wiersze. Taką macierz możemy, poprzez elementarne operacje na wierszach, sprowadzić do tak zwanej zredukowanej postaci schodkowej

$$\begin{pmatrix} v_1 \\ \vdots \\ v_2 \end{pmatrix} \xrightarrow{\text{elementarne operacje na wierszach}} \begin{pmatrix} 0\ldots1*\cdots*0*\cdots*0*\cdots* \\ 0\ldots0\,0\ldots0\,1*\cdots*0*\cdots* \\ 0\ldots0\,0\ldots0\,\underset{\cdots}{0\,0}\ldots0\,1*\cdots* \end{pmatrix}$$

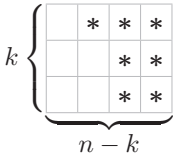
Operacje elementarne to: dodawanie wierszy, mnożenie wiersza przez niezerowy skalar oraz zamiana kolejności wierszy.
Zredukowana postać schodkowa ma następujące cechy:

- pierwszy niezerowy element od lewej w każdym wierszu to 1 (tę jedynkę będziemy nazywać wiodącą),
- wszystkie pozostałe elementy w kolumnie, w której jest jedynka wiodąca, to zera,
- w każdym wierszu jedynka wiodąca pojawia się na prawo od jedynki wiodącej w poprzednim wierszu.

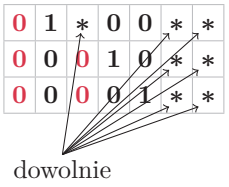
Można udowodnić, że jeżeli wiersze dwóch takich macierzy generują tę samą przestrzeń, to macierze te są równe. Zliczenie wszystkich interesujących nas podprzestrzeni sprowadza się więc do policzenia, ile jest różnych zredukowanych macierzy schodkowych. Żeby je policzyć, spróbujmy usunąć z takiej macierzy wszystko, co „zbędne". Z pewnością zbędne są wszystkie zera, na lewo od jedynek wiodących. Możemy je więc bezkarnie usunąć. Kolumny zawierające wiodące jedynki również nie będą miały dla nas znaczenia, więc je też usuńmy

$$\begin{array}{|ccccccc|} \hline \mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{2} \\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{2}&\mathbf{0} \\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1} \\ \hline \end{array} \Rightarrow \begin{array}{|ccccccc|} \hline & \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{2} \\ & & & \mathbf{1}&\mathbf{0}&\mathbf{2}&\mathbf{0} \\ & & & &\mathbf{1}&\mathbf{0}&\mathbf{1} \\ \hline \end{array} \Rightarrow \begin{array}{|cccc|} \hline & \mathbf{1}&\mathbf{1}&\mathbf{2} \\ & & \mathbf{2}&\mathbf{0} \\ & & \mathbf{0}&\mathbf{1} \\ \hline \end{array}$$

Otrzymaliśmy macierz zawierającą puste pola oraz pewne liczby. Tak naprawdę nie interesuje nas, jakie to są liczby, więc możemy każdą z nich zastąpić gwiazdką.



Czyli mamy diagram o wymiarach k na $n-k$. Oznaczmy pojedynczy diagram przez λ, a liczbę gwiazdek w nim przez $|\lambda|$. Zauważmy, że z diagramu λ możemy „odzyskać” postać macierzy, z której powstał. Kolumny z jedynkami wiodącymi wstawiamy w sposób jednoznaczny, podobnie jak zera po ich lewej stronie. Natomiast gwiazdki możemy zastąpić elementami ciała F na wszystkie możliwe sposoby, których jest dokładnie $q^{|\lambda|}$



I tak oto dochodzimy do wniosku, że różnych zredukowanych macierzy schodkowych, a więc również podprzestrzeni k-wymiarowych przestrzeni n-wymiarowej jest:

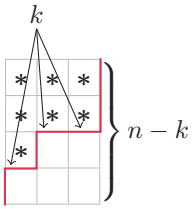
$$(**) \qquad \binom{n}{k}_q = \sum_{\lambda \subset k\times(n-k)} q^{|\lambda|},$$

gdzie zapis $\lambda \subset k \times (n-k)$ oznacza, że diagram λ „mieści” się w macierzy o k wierszach i $n-k$ kolumnach. Z powyższej formuły widać ponadto, że $\binom{n}{k}_q$ wyraża się zawsze jako wielomian stopnia $(n-k)k$ zmiennej q o całkowitych dodatnich współczynnikach. To nie było od razu widoczne z formuły $(\star)$, gdyż na pozór nie wydaje się, aby występujący tam ułamek mógł zostać skrócony. Warto również podkreślić, że równość pomiędzy prawymi stronami równań $(\star)$ i $(**)$ zachodzi dla dowolnej liczby rzeczywistej q; na mocy naszych rozważań jest bowiem prawdziwa dla dowolnego q będącego licznością pewnego ciała skończonego (w szczególności dla liczb pierwszych), a jeśli funkcje wymierne (tzn. ilorazy wielomianów) przyjmują te same wartości dla nieskończenie wielu argumentów, to są równe wszędzie tam, gdzie są określone.

Pozostało nam jeszcze policzyć, ile jest różnych diagramów o $|\lambda|$ gwiazdkach. Jeżeli przyjrzymy się dokładnie pojedynczemu diagramowi i obrócimy go o 90°, to zobaczymy, że w istocie jest on tym samym, co tak zwany *diagram Ferrersa* (znany matematykom od dawna i dokładnie zbadany).

Diagramy Ferrersa reprezentują podziały liczby naturalnej na skończoną liczbę dodatnich składników, przy czym ich kolejność jest nieistotna. Zliczanie takich diagramów jest równoważne zliczaniu różnych podziałów.

Łatwo policzyć, ile jest takich diagramów. Możemy każdy z nich utożsamić z linią łamaną stanowiącą jego prawostronny obrys (na rysunku diagram Ferrersa dla $n=7$ i $k=3$). Żeby otrzymać taką linię, złożoną z n kresek, musimy wybrać dokładnie k miejsc, na których postawimy kreski poziome, a możemy to zrobić na $\binom{n}{k}$ sposobów. Dzięki temu, że policzyliśmy, ile jest różnych diagramów o mocy $|\lambda|$, możemy ponownie stwierdzić słuszność interesującej nas zależności; wystarczy zauważyć, że dla $q=1$ prawa strona $(**)$ jest liczbą wszystkich możliwych diagramów Ferrersa, czyli wynosi $\binom{n}{k}$.



Zagnieżdżone pierwiastki

*Jarosław GÓRNICKI**

* Wydział Matematyki i Fizyki Stosowanej, Politechnika Rzeszowska

W 1911 roku Srinivasa Ramanujan (1887–1920) zaproponował czytelnikom *Journal of the Indian Mathematical Society* (JIMS 3 (1911), Question 289, p. 90) wyznaczenie wartości:

$$\text{(a)}\ \sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{\cdots}}}}, \qquad \text{(b)}\ \sqrt{6+2\sqrt{7+3\sqrt{8+\cdots}}}.$$

Ponieważ pytania te w 1911 r. nie doczekały się odpowiedzi, więc Ramanujan podał je w kolejnym tomie JIMS 4 (1912), p. 226. Zadania Ramanujana można rozwiązać prosto i elegancko.

(a) Zauważmy, że

$$n(n+2) = n\sqrt{1+(n+1)(n+3)}, \quad n=1,2,\ldots.$$

Niech $f(n)=n(n+2)$, wtedy

$$f(n) = n\sqrt{1+f(n+1)} = n\sqrt{1+(n+1)f(n+2)} = \ldots,$$

zatem

$$n(n+2) = n\sqrt{1+(n+1)\sqrt{1+(n+2)\sqrt{1+\cdots}}}.$$

O innych wzorach Ramanujana pisaliśmy w Δ^3_{18}.