Matematyka dyskretna

© Andrzej Łachwa, UJ, 2019
andrzej.lachwa@uj.edu.pl

12B/14

Permutacje bez punktów stałych

Nieporządek na zbiorze *X* to permutacja $\alpha : X \to X$ taka, że $\alpha(x) \neq x$ dla dowolnego $x \in X$, czyli permutacja "bez punktów stałych".

Podsilnia liczby *n*, w skrócie !*n*, to liczba nieporządków zbioru *n*-elementowego. Przyjmujemy, że !0=1, jako że jedyna permutacja zbioru pustego - funkcja pusta - w oczywisty sposób nie ma punktów stałych. Przyjmujemy ponadto, że !1=0.

Liczba nieporządków

$$!n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}.$$

Liczby nieporządków zbioru *n*-elementowego wynoszą:

n	0	1	2	3	4	5	6	7	8	9	10
!n	1	0	1	2	9	44	265	1854	14833	133496	1334961

Reguła rekurencyjna:

$$! n = (n - 1) (! (n - 1) + ! (n - 2))$$ przy czym !0 = 1 i !1 = 0.

Podobnie dla silni:

$$n ! = (n - 1) ((n - 1) ! + (n - 2) !)$$ przy czym 0! = 1, 1! = 1.

Przykład

Zbiór $\mathbb{Z}_4 = \{0,1,2,3\}$ ma $4! = 24$ permutacje, ale tylko 9 z nich to nieporządki, bo !4 = 4! [1/0!−1/1!+1/2!−1/3!+1/4!] = $24-24+24\cdot\frac{1}{2}-24\cdot\frac{1}{6}+24\cdot\frac{1}{24} = 12-4+1 = 9$. Oto ich lista:

0	1	2	3	0	1	2	3	0	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	0	3	2	1	2	3	0	1	3	0	2
0	1	2	3	0	1	2	3	0	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
2	0	3	1	2	3	0	1	2	3	1	0
0	1	2	3	0	1	2	3	0	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
3	0	1	2	3	2	0	1	3	2	1	0

Dowód

Zauważmy najpierw, że liczba permutacji α zbioru *n*-elementowego takich, że $\alpha(x) \neq x$ dla dokładnie *i* elementów $x \in X$, wynosi $\binom{n}{i}\,!i$.

Stąd:
$$n! = \sum_{i=0}^{n} \binom{n}{i} !i = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^i (!i).$$

Stosując teraz regułę odwracania, dostajemy:

$$\begin{aligned} !n &= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i! \\ &= \sum_{i=0}^{n} (-1)^{n-i} \frac{n!}{(n-i)!} \\ &= n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \end{aligned}$$

Przykład

Cztery osoby przychodzą na plażę z własnymi leżakami. Po kąpieli mogą zająć leżaki na 4! = 24 sposobów. Jakie jest prawdopodobieństwo, że żadna osoba nie będzie leżeć na swoim leżaku?

Temu zdarzeniu sprzyjają permutacje bez punktów stałych, czyli nieporządki. Jest ich !4 = 9. Prawdopodobieństwo wynosi więc

!4 / 4! = 9 / 24

Współczynniki multimianowe

Współczynniki dwumianowe pojawiały się przy rozwinięciu dwumianu $(x+y)^n$. Odpowiadały one wyborom dwuwartościowym. Podobnie rozważając trójmian $(x+y+z)^n$, czy ogólnie $(x_1+\ldots+x_r)^n$, pojawią się współczynniki odpowiadające wyborom odpowiednio trójwartościowym i *r*-wartościowym.

Wybieranie podzbioru *k*-elementowego ze zbioru *n*-elementowego to podział zbioru na dwie części o odpowiednio *k* i *n*-*k* elementach. Naturalnym uogólnieniem będzie podział zbioru *n*-elementowego na *r* części o odpowiednio $k_1, k_2, \ldots, k_r$ elementach, przy czym oczywiście $k_1+\ldots k_r = n$.

Współczynnik multimianowy $\binom{n}{k_1, k_2 \ldots, k_r}$, dla $n \in \mathbb{Z}$, $r \geqslant 2$ oraz całkowitych $k_1, \ldots, k_r$ takich, że $k_1 + \ldots k_r = n$, to liczba sposobów umieszczenia *n* obiektów w *r* pudełkach z odpowiednio k_1 obiektami w pierwszym pudełku, k_2 w drugim, itd. oraz k_r w *r*-tym.

Jeśli którakolwiek z liczb k_i jest ujemna to współczynnik jest równy 0.

Kolejność dolnych indeksów nie jest istotna.

Oczywiście $\binom{n}{k}$ to w nowej notacji $\binom{n}{k, n-k}$.

Następne obserwacje wynikają wprost z definicji współczynników multimianowych:

dla $n \in \mathbb{Z}$, $k, l, k_1, \ldots, k_r \in \mathbb{Z}$ takich, że $k_1 + \ldots k_r = n = k + l$ zachodzi:

$$\binom{n}{n,0,\ldots,0} = 1$$

$$\binom{n}{1,1,\ldots 1} = n!$$

$$\binom{n}{0,k_1,\ldots,k_r} = \binom{n}{k_1,\ldots,k_r}$$

$$\binom{n}{l,k,0,0,\ldots 0} = \binom{n}{l} = \binom{n}{k}$$

$\binom{n}{k_1,\ldots,k_r} = \binom{n}{k_{\sigma(1)},\ldots,k_{\sigma(r)}}$, dla dowolnej permutacji α zbioru $\{1, 2, \ldots, r\}$.

Obserwacja

Dla $n, k_1, \ldots, k_r \geqslant 0$ takich, że $k_1 + \ldots + k_r = n$

$$\binom{n}{k_1,\ldots,k_r} = \binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-(k_1+k_2)}{k_3} \cdot \ldots \cdot \binom{n-(k_1+\ldots+k_{r-1})}{k_r}.$$

Dowód

Rozmieszczenie *n*-obiektów w *r* pudełkach po k_i w każdym, polega na:

- wyborze k_1 obiektów spośród wszystkich *n* i umieszczeniu ich w pierwszym pudełku - możemy to uczynić na $\binom{n}{k_1}$ sposobów,
- wyborze k_2 obiektów spośród pozostałych $n - k_1$ i umieszczeniu ich w drugim pudełku - możemy to uczynić na $\binom{n-k_1}{k_2}$ sposobów,

- wyborze k_3 obiektów spośród pozostałych $n-(k_1+k_2)$ i umieszczeniu ich w trzecim pudełku - możemy to uczynić na $\binom{n-(k_1+k_2)}{k_3}$ sposobów,

...

- wyborze k_r obiektów spośród pozostałych $n-(k_1+\ldots+k_{r-1})=k_r$ i umieszczeniu ich w ostatnim pudełku - możemy to uczynić na $\binom{n-(k_1+\ldots+k_{r-1})}{k_r}=\binom{k_r}{k_r}=1$ sposobów.

Zatem wszystkich możliwych rozmieszczeń zgodnie z zasadą mnożenia i z wymogami z definicji współczynnika multimianowego jest dokładnie

$$\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-(k_1+k_2)}{k_3}\cdot\ldots\cdot\binom{n-(k_1+\ldots+k_{r-1})}{k_r}.$$

Wniosek

Dla $n, k_1, \ldots, k_r \geqslant 0$ takich, że $k_1 + \ldots + k_r = n$ mamy

$\binom{n}{k_1, \ldots, k_r} = \frac{n!}{k_1! \cdot \ldots \cdot k_r!}$.

Dowód

$$\begin{aligned}
\binom{n}{k_1, \ldots, k_r} &= \binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-(k_1+k_2)}{k_3} \cdot \ldots \cdot \binom{n-(k_1+\ldots+k_{r-1})}{k_r} \\
&= \frac{n!}{(n-k_1)!k_1!} \cdot \frac{(n-k_1)!}{(n-(k_1+k_2))!k_2!} \cdot \ldots \cdot \frac{(n-(k_1+\ldots+k_{r-1}))!}{(n-(k_1+\ldots+k_r))!k_r!} \\
&= \frac{n!}{k_1! \cdot \ldots \cdot k_r! \cdot (n-(k_1+\ldots+k_r))!} \\
&= \frac{n!}{k_1! \cdot \ldots \cdot k_r!}.
\end{aligned}$$

Przykład

Ile liczb możemy ułożyć zapisując w dowolnej kolejności 11 cyfr: $1,1,3,4,5,5,5,6,7,7,9$?

Zauważmy, że każda taka liczba powstaje przez wybór dwu pozycji dla cyfry 1, jednej dla cyfry 3, jednej dla cyfry 4, trzech dla cyfry 5, jednej dla cyfry 6, dwu dla cyfry 7 i wreszcie jednej pozycji dla cyfry 9. Zatem 11 pozycji to nasze obiekty, które rozmieszczamy w siedmiu pudełkach etykietowanych cyframi: $1,3,4,5,6,7,9$. Z definicji współczynnika multimianowego mamy:

$$\binom{11}{2,1,1,3,1,2,1} = \frac{11!}{2!\cdot 3!\cdot 2!} = 1663200.$$

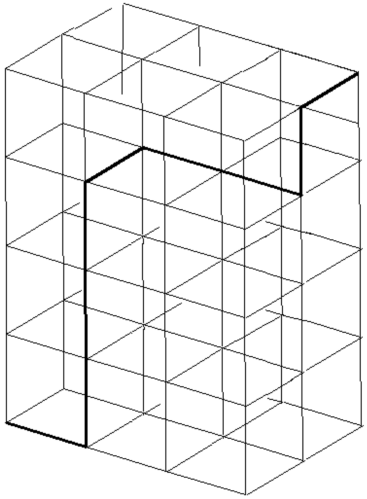
Przykład

Rozważmy raz jeszcze podróż w mieście o ulicach na planie siatki. Tym razem weźmy wersję 3-wymiarową. Mamy więc do dyspozycji trójwymiarową, prostopadłościenną kratownicę $a \times b \times c$. Na ile sposobów można połączyć przeciwległe wierzchołki prostopadłościanu najkrótszą możliwą łamaną?

Zauważmy, że każda najkrótsza możliwa łamana składa się z dokładnie $a+b+c$ odcinków jednostkowych. Przy czym dokładnie *a* z nich jest poziomych, *b* pionowych i *c* idzie w głąb. Zatem najkrótszych łamanych jest tyle co rozmieszczeń $a+b+c$ odcinków (obiekty) w 3 pudełkach: "poziomy", "pionowy", "w głąb" tak, by było ich odpowiednio *a*, *b* i *c*.

Z definicji współczynnika multimianowego mamy zatem $\binom{a+b+c}{a,b,c}=\frac{(a+b+c)!}{a!\,b!\,c!}$ łamanych.

Dla przykładu, kratka o wymiarach 3x4x2 ma $\binom{9}{3,4,2}=\frac{9!}{3!\ 4!\ 2!}=1260$ interesujących nas łamanych.



Współczynniki multimianowe zachowują **regułę dodawania**:

dla $n > 0$, całkowitych $k_1, \ldots, k_r$ takich, że $k_1 + \ldots + k_r = n$

$$\binom{n}{k_1 k_2 \cdots k_r} = \binom{n-1}{k_1 - 1, k_2, \ldots, k_r} + \binom{n-1}{k_1, k_2 - 1, \ldots, k_r} + \ldots + \binom{n-1}{k_1, k_2, \ldots, k_r - 1}.$$

Obserwacja

$$(x_1 + \ldots + x_r)^n = \sum_{k_1 + \ldots + k_r = n} \binom{n}{k_1, \ldots, k_r} x_1^{k_1} x_2^{k_2} \ldots x_r^{k_r}.$$

Zadania

Wyprowadzić wzór na $(x+y+z)^3$.

Policzyć $\binom{4}{2\ 1\ 1}$, $\binom{6}{3\ 1\ 2}$ i $\binom{7}{2\ 3\ 3}$.

Na ile sposobów można podzielić grupę 12 uczniów na 3 równoliczne ponumerowane grupy?

Na ile sposobów można podzielić grupę 6 uczniów na 3 ponumerowane grupy tak, aby w każdej następnej było więcej uczniów niż w poprzedniej?

Wracamy do permutacji

Przypomnijmy, że rozkład permutacji na cykle jest jednoznaczny z dokładnością do kolejności, tzn. jeśli $\sigma_1 \circ \ldots \circ \sigma_k = \pi_1 \circ \ldots \circ \pi_l$ są dwoma rozkładami tej samej permutacji na cykle to

$$k = l \quad \text{i} \quad \{\sigma_1, \ldots, \sigma_k\} = \{\pi_1, \ldots, \pi_k\}.$$

Pierwszym ważnym niezmiennikiem dla permutacji $\pi \in S_n$ jest zatem **liczba cykli *c*(π)**. Drugi ważny niezmiennik to **typ** permutacji.

Typ permutacji $\pi \in S_n$ to wektor $(\alpha_1, \ldots, \alpha_n)$, gdzie α_i jest liczbą i-elementowych cykli w rozkładzie π. Zazwyczaj typ permutacji zapisujemy jako $[1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}]$, przy czym często pomijamy te wartości, dla których $\alpha_i = 0$.

Przykład

Dla permutacji $\pi \in S_7$ zadanej przez

n	0	1	2	3	4	5	6
$\pi(n)$	3	6	2	4	0	5	1

mamy: $\pi = (0,3,4)(1,6)(2)(5) = (0,3,4)(1,6)$, π jest typu $[1^2 2^1 3^1]$ i $c(\pi)=4$.

Z samej definicji typu permutacji natychmiast wynika, że dla $\pi \in S_n$ typu $(\alpha_1, \ldots, \alpha_n)$ zachodzi:

- ✓ $\alpha_1 + \ldots + \alpha_n = c(\pi)$,
- ✓ $\alpha_1 + 2\alpha_2 + \ldots + n\alpha_n = n$.

Twierdzenie

Liczba permutacji w S_n typu $(\alpha_1, \ldots, \alpha_n)$ to

$$\frac{n!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \ldots \cdot n^{\alpha_n} \cdot \alpha_1! \cdot \alpha_2! \cdot \ldots \cdot \alpha_n!} .$$

Dowód

Potraktujmy permutację typu $(\alpha_1, \ldots, \alpha_n)$, jako uzupełnienie elementami z $\mathbb{Z}_n$ następującego wzorca:

$$\underbrace{(\bullet)\ldots(\bullet)}_{\alpha_1 \text{ razy}}\underbrace{(\bullet\bullet)\ldots(\bullet\bullet)}_{\alpha_2 \text{ razy}}\ldots\ldots\underbrace{(\bullet\ldots\bullet)}_{\alpha_n \text{ razy } (\alpha_n \leqslant 1)} .$$

W miejsce *k* kropek możemy wstawić *k*-elementów na *k*! sposobów. Jednak w ten sposób otrzymamy wielokrotnie te same permutacje.

Każdy cykl *i*-elementowy możemy zadać na *i* sposobów (rozpoczynając od różnych elementów). Dodatkowo, zwróćmy uwagę, że w naszym wzorcu dopuszczamy różną kolejność cykli o tej samej długości i że α_i takich samych cykli *i*-elementowych może być wybranych na $\alpha_i!$ sposobów.

Podsumowując, aby otrzymać liczbę permutacji typu $(\alpha_1, \ldots, \alpha_n)$ musimy dla wszystkich $i \in \{1, \ldots, n\}$ podzielić *n*! przez długość każdego cyklu z osobna, tzn. dla każdego cyklu długości *i* podzielić przez *i*, oraz przez silnię liczby *i*-elementowych cykli. Zatem szukana liczba to $\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n} \alpha_1! \ldots \alpha_n!}$.

Przykład

Lista typów wszystkich permutacji z S_3:

n	0	1	2	rozkład na cykle	typ
π_0	0	1	2	$(0)(1)(2)$	$[1^3]$
π_1	1	0	2	$(0,1)(2)$	$[1^1 2^1]$
π_2	0	2	1	$(0)(12)$	$[1^1 2^1]$
π_3	1	2	0	$(0,1,2)$	$[3^1]$
π_4	2	0	1	$(0,2,1)$	$[3^1]$
π_5	2	1	0	$(0,2)(1)$	$[1^1 2^1]$

Liczba permutacji z S_3 o kolejnych typach:

typ	liczba permutacji
1^3	$\frac{3!}{1^3 \cdot 3!} = 1$
$1^1 2^1$	$\frac{3!}{1^1 \cdot 2^1 \cdot 1! \cdot 1!} = 3$
3^1	$\frac{3!}{3^1 \cdot 1!} = 2$

Permutacja sprzężona do permutacji $\pi \in S_n$ to każda permutacja postaci $\sigma\pi\sigma^{-1}$, gdzie $\sigma \in S_n$.

Oczywiście, jeśli $\sigma\pi\sigma^{-1} = \rho$ to $\pi = \sigma^{-1}\rho\sigma$.

Zatem dwuargumentowa relacja sprzężenia jest symetryczna. Łatwo udowodnić, że relacja ta jest również zwrotna i przechodnia oraz, że jedyną permutacją sprzężoną do permutacji identycznościowej id jest ona sama.

Twierdzenie

Permutacje $\pi, \rho \in S_n$ mają ten sam typ wtedy i tylko wtedy, gdy są sprzężone.

Dowód

Załóżmy najpierw, że π i ρ są sprzężone, czyli że $\sigma\pi\sigma^{-1} = \rho$ dla pewnego σ. Rozważmy jakiś cykl $(x_0, \ldots, x_{k-1})$ permutacji π.

Wtedy $(\sigma(x_0), \ldots, \sigma(x_{k-1}))$ jest cyklem permutacji ρ. Istotnie, dla $i = 0, \ldots, k-1$ mamy:

$$\rho(\sigma(x_i)) = \sigma\pi\sigma^{-1}\sigma(x_i) = \sigma\pi(x_i) = \sigma(x_{i+1}),$$

i podobnie:

$$\rho(\sigma(x_{k-1}) = \sigma\pi\sigma^{-1}\sigma(x_{k-1}) = \sigma\pi(x_{k-1}) = \sigma(x_0).$$

Każdy zatem cykl permutacji π wyznacza jednoznacznie cykl permutacji ρ o tej samej liczności. Tym samym π i ρ są tego samego typu.

Dla dowodu w drugą stronę załóżmy, że π i ρ mają ten sam typ. Wtedy możemy określić bijekcję przyporządkowującą każdemu cyklowi permutacji π pewien cykl ρ o tej samej długości.

Po rozkładzie obu permutacji π, ρ na rozłączne cykle nasza bijekcja między cyklami przyporządkowuje cyklowi $(x_0, \ldots, x_{k-1})$ cykl $(y_0, \ldots, y_{k-1})$.
Definiujemy $\sigma \in S_n$ kładąc $\sigma(x_i) = y_i$.

Łatwo sprawdzić, że wtedy $\sigma\pi\sigma^{-1} = \rho$.

Transpozycja to permutacja w S_n (dla n≥2) typu $[1^{n-2}2^1]$. Innymi słowy, transpozycja dokonuje tylko jednego przestawienia dwóch elementów ze zbioru *n*-elementowego.

Przykład

Dla permutacji $\pi \in S_7$ zadanej przez

n	0	1	2	3	4	5	6
$\pi(n)$	0	1	5	3	4	2	6

mamy: $\pi = (0)(1)(25)(3)(4)(6) = (25)$,

π ma typ $[1^5 2^1]$,

π jest transpozycją.

Obserwacja

Dowolna permutacja jest złożeniem transpozycji.

Ponieważ dowolna permutacja jest rozkładalna na cykle wystarczy pokazać, że każdy cykl jest złożeniem transpozycji. Dokładniej: pokażemy, że dowolny cykl z S_n jest złożeniem $n-1$ transpozycji.

Dowód

Cykl $\pi = (x_0, \ldots, x_{n-1})$ można przedstawić tabelką:

n	x_0	x_1	x_2	$\ldots$	x_{n-2}	x_{n-1}
$\pi(n)$	x_1	x_2	x_3	$\ldots$	x_{n-1}	x_0

Zauważmy, że π jest następującym złożeniem transpozycji

$$(x_0, x_{n-1})(x_0, x_{n-2}) \ldots (x_0, x_2)(x_0, x_1).$$

Rzeczywiście x_0 przejdzie w pierwszej transpozycji (x_0, x_1) w x_1,
a następne transpozycje już go nie przesuną.

Podobnie x_1 przejdzie pierwszą transpozycją (x_0, x_1) w x_0, drugą (x_0, x_2) w x_2, a następne transpozycje już go nie przesuną.

Ogólnie, x_i (dla $i \in \{1, \ldots, n-2\}$) pozostanie na swoim miejscu przez pierwsze $i-1$ transpozycji $(x_0, x_1), (x_0, x_2), \ldots, (x_0, x_{i-1})$, przejdzie i-tą transpozycją w x_0, przejdzie $(i+1)$-szą transpozycją w x_{i+1}, po czym zostanie już nienaruszone.

Natomiast x_{n-1} zostanie przesunięte dopiero ostatnią transpozycją i przyjmie wartość x_0.

Wniosek

Dowolna permutacja typu $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ ma rozkład na co najwyżej $\alpha_2 + 2\alpha_3 + \dots (n-1)\alpha_n$ transpozycji.

Przykład

Dla permutacji $\pi \in S_7$ zadanej przez

n	0	1	2	3	4	5	6
$\pi(n)$	2	3	5	4	6	0	1

mamy

$$\pi = (0,2,5)(1,3,4,6)$$
$$(1,3,4,6) = (1,6)(1,4)(1,3)$$
$$(0,2,5) = (0,5)(0,2)$$
$$\pi = (0,5)(0,2)(1,6)(1,4)(1,3) = (1,6)(1,4)(1,3)(0,5)(0,2)$$

Zauważmy, że składanie transpozycji na rozłącznych zbiorach dwu-elementowych jest przemienne. Na ogół jednak, ponieważ transpozycje nie działają na zbiorach rozłącznych, to nie możemy ich dowolnie przestawiać. W naszym przykładzie transpozycje generujące dwa różne cykle są parami rozłączne, więc ich kolejność jest bez znaczenia. Między innymi dlatego istnieje wiele rozkładów na transpozycje. Ale nie tylko dlatego, mamy bowiem również $\pi = (1,6)(2,5)(0,2)(3,6)(0,5)(4,6)(2,5)$.

Nie mamy zatem jednoznaczności rozkładu na transpozycje, tak jak to miało miejsce przy rozkładzie na cykle. Nawet liczba transpozycji nie musi być ta sama w różnych rozkładach na transpozycje. Zobaczymy jednak, że nie zmienia się parzystość liczby transpozycji w rozkładzie.

Obserwacja

Jeśli $\pi, \tau \in S_n$ i τ jest transpozycją, to $c(\tau\pi) = c(\pi) \pm 1 = c(\pi\tau)$.

Dowód

Udowodnimy tylko pierwszą równość. Załóżmy, że $\tau = (a, b)$ tzn., $\tau(a) = b$, $\tau(b) = a$ i $\tau(x) = x$ dla wszystkich pozostałych elementów $x \in \mathbb{Z}_n$.
Rozumowanie dzielimy na dwa przypadki:

1. *a* i *b* są w tym samym cyklu $(a, x, \ldots, y, b, w, \ldots, z)$ permutacji π.

Wtedy $\tau\pi = (a, x, \ldots, y)(b, w, \ldots, z)\cdots$, gdzie ostatni wielokropek oznacza pozostałe cykle permutacji π. Zatem w tym przypadku mamy $c(\tau\pi) = c(\pi) + 1$.

2. *a* i *b* są w różnych cyklach permutacji $\pi = (a, x \ldots, y)(b, \ldots, z)\ldots$.

Wtedy $\tau\pi = (a, x, \ldots, y, b, \ldots, z)\ldots$. Mamy więc $c(\tau\pi) = c(\pi) - 1$.

Obserwacja

Jeśli permutacja jest przedstawialna jako złożenia r i r' transpozycji, to liczby r i r' albo są obie parzyste albo obie nieparzyste.

Dowód

Niech $\tau_{r-1}\dots\tau_0 = \tau'_{r'-1}\dots\tau'_0$ będą dwoma rozkładami tej samej permutacji $\pi \in S_n$ na transpozycje. Na mocy wcześniejszej obserwacji mamy:

$$c(\tau_{r-1}\dots\tau_0) = c(\tau_{r-2}\dots\tau_0)\pm 1 = c(\tau_{r-3}\dots\tau_0)\pm 1\pm 1 = \dots = c(\tau_0)\underbrace{\pm 1 \pm 1 \dots \pm 1}_{r-1 \text{ razy}}$$

Niech *t* opisuje ilość dodawań jedynki w powyższej formule. Wtedy $r-1-t$ to liczba odejmowań jedynki. Transpozycja τ_0 ma 1 cykl 2-elementowy i *n*–2 cykli 1-elementowych, czyli $c(\tau_0) = 1 + (n-2) = n-1$.

Zatem $c(\pi) = c(\tau_{r-1}\dots\tau_0) = n - 1 + t - (r-1-t) = n - r + 2t$ dla pewnego *t*.

Analogicznie $c(\pi) = c(\tau'_{r'-1} \dots \tau'_0) = n - 1 + t' - (r' - 1 - t') = n - r' + 2t'$

dla pewnego t'. Porównując obydwa wyniki otrzymujemy $r–r'=2t–2t'$, czyli różnica $r–r'$ jest zawsze parzysta.

Definicje

Permutacja parzysta to permutacja będąca złożeniem parzystej liczby transpozycji.

Permutacja nieparzysta to permutacja będąca złożeniem nieparzystej liczby transpozycji.

Znak permutacji π to $\mathrm{sgn}(\pi) = (-1)^r$, gdzie r jest liczbą transpozycji, na które można rozłożyć π.

Obserwacja

Dla dowolnych $\pi, \sigma \in S_n$

- $\mathbf{sgn}(id_{\mathbb{Z}_n}) = 1$,
- $\mathbf{sgn}(\sigma\pi) = \mathbf{sgn}(\pi) \cdot \mathbf{sgn}(\sigma)$,
- $\mathbf{sgn}(\pi) = \mathbf{sgn}(\pi^{-1})$,
- transpozycja ma znak -1

Dowód

Identyczność jest złożeniem zera transpozycji (albo dwóch takich samych).

Drugi punkt wynika natychmiast z wcześniejszej obserwacji.

Dla dowodu trzeciego odnotujmy tylko, że
$\mathbf{sgn}(\pi) \cdot \mathbf{sgn}(\pi^{-1}) = \mathbf{sgn}(\pi\pi^{-1}) = \mathbf{sgn}(id_{\mathbb{Z}_n}) = 1$.

Ostatnie polega na podstawieniu *r*=1 w definicji funkcji *sgn.*

Przykład

Rozważmy łamigłówkę logiczną rozgrywaną na kwadracie 3x3. Wszystkie pola, poza prawym dolnym, wypełnione są kwadratowymi klockami z różnymi literami B,O,R,L,Y,M,E,P. Prawe dolne pole jest puste - oznaczamy go przez "_". Celem gry jest ułożenie napisu "PROBLEMY_". Dopuszczalnym ruchem jest przesunięcie klocka sąsiadującego z pustym polem na to właśnie pole. Czy z pozycji "BORLYMEP_" można ułożyć napis "PROBLEMY_"?

Zauważmy, że pozycja startowa i końcowa mają puste pole "_" w tym samym miejscu. To oznacza, że wykonując roszadę bloków musimy wykonać tyle samo przesunięć do góry co w dół i tyle samo przesunięć w prawo co w lewo. To z kolei oznacza, że potencjalna ilość ruchów wiodących do rozwiązania musi być parzysta. Tłumacząc nasz problem na język permutacji odnotujmy, że:

mamy dokonać permutacji $\pi \in S_9$:

$$\begin{array}{cccccccccc} B & O & R & L & Y & M & E & P & \_ \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ P & R & O & B & L & E & M & Y & \_ \end{array}$$

każdy ruch zgodny z regułami gry to jakaś transpozycja wybranych klocków, przy czym nie wszystkie transpozycje są dopuszczalne.

Zauważmy, że rozwiązanie musi być wykonane przy pomocy parzystej liczby ruchów, zatem każda permutacja dokonująca żądanej rearanżacji klocków jest parzysta, a ponadto mamy rozkład

$\pi = (B,P,Y,L)(O,R)(M,E)(\_)$.

Z wcześniejszych wniosków mamy jednak, że π jest złożeniem $3+1+1=5$ transpozycji, czyli π jest permutacją nieparzystą.

Ponieważ nie można złożyć nieparzystej permutacji z parzystej liczby transpozycji, nasza łamigłówka nie jest możliwa do rozwiązania.

Obserwacja

Dla $n \geqslant 2$ w S_n jest dokładnie tyle samo permutacji parzystych co nieparzystych.

Dowód

Niech $n \geqslant 2$ i $\pi_0, \ldots, \pi_{k-1}$ będzie listą wszystkich parzystych permutacji w S_n. Ponadto, rozważmy transpozycję $\tau = (01)(2)\ldots(n)$. Wtedy oczywiście permutacje $\tau\pi_0, \tau\pi_1, \ldots, \tau\pi_{k-1}$ są parami różne, gdyż jeśli $\tau\pi_i = \tau\pi_j$ to $\pi_i = \tau^{-1}\tau\pi = \tau^{-1}\tau\pi_j = \pi_j$. Ponadto dowolna $\tau\pi$ jest nieparzysta, bo $\mathrm{sgn}(\tau\pi) = \mathrm{sgn}(\tau)\mathrm{sgn}(\pi) = (-1)\cdot 1 = -1$. Pozostaje pokazać, że dowolna nieparzysta permutacja ρ jest na liście $\tau\pi_0, \tau\pi_1, \ldots, \tau\pi_{k-1}$. Ponieważ $\mathrm{sgn}(\tau^{-1}\rho) = \mathrm{sgn}(\tau^{-1})\mathrm{sgn}(\rho) = (-1)\cdot(-1) = 1$, to $\tau^{-1}\rho$ jest permutacją parzystą, a zatem jest postaci π_i dla pewnego i. To zaś oznacza, że $\rho = \tau\tau^{-1}\rho = \tau\pi_i$, czyli ρ jest na liście $\tau\pi_0, \tau\pi_1, \ldots, \tau\pi_{k-1}$. Uzyskana bijekcja $\pi_i \mapsto \tau\pi_i$ dowodzi naszej obserwacji.