MATEMATYKA DYSKRETNA

doc. dr hab. inż. Marek Libura

Instytut Badań Systemowych PAN
01-447 Warszawa, Newelska 6, pok. 324

Marek.Libura@ibspan.waw.pl
tel.(48)(22)8373578 w.193

NOTACJA

Dla dowolnego zdania $\mathcal{Q}$

$$\lfloor \mathcal{Q} \rceil = \begin{cases} 1 & \text{jeśli zdanie } \mathcal{Q} \text{ jest prawdziwe,} \\ 0 & \text{jeśli zdanie } \mathcal{Q} \text{ jest fałszywe.} \end{cases}$$

Funktory zdaniotwórcze:

$\vee$ – **lub** (alternatywa, suma logiczna)

$\wedge$ – **i** (koniunkcja, iloczyn logiczny)

$\neg$ – **nie** (negacja)

$\Rightarrow$ – **jeśli . . . , to . . .** (implikacja),

$\Leftrightarrow$ – **wtedy i tylko wtedy, gdy** (równoważność).

Rachunek zdań

p, q – **zdania**

$\lfloor p \rceil$	$\lfloor q \rceil$	$\lfloor \neg q \rceil$	$\lfloor p \vee q \rceil$	$\lfloor p \wedge q \rceil$	$\lfloor p \Rightarrow q \rceil$	$\lfloor p \Leftrightarrow q \rceil$
0	0	1	0	0	1	1
0	1	0	1	0	1	0
1	0	1	1	0	0	0
1	1	0	1	1	1	1

FUNKCJE *podłoga* i *sufit*

Dla dowolnej liczby rzeczywistej x:

$\lfloor x \rfloor = \max\{y \in \mathbb{Z} : \ y \leqslant x\}$, – **podłoga** x

$\lceil x \rceil = \min\{y \in \mathbb{Z} : \ y \geqslant x\}$. – **sufit** x

Dla $x, y \in \mathbb{R}$, $y \neq 0$, **symbol** $x \bmod y$ **oznacza resztę z dzielenia** x **przez** y**:**

$$x \bmod y = x - y \cdot \lfloor x/y \rfloor .$$

Zbiory:

$\mathbb{N} = \{0, 1, 2, \ldots\}$ – **zbiór liczb naturalnych**

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ – **zbiór liczb całkowitych**

$\mathbb{B} = \{0, 1\}$

$\mathbb{R}$ – **zbiór liczb rzeczywistych**

$\mathbb{C}$ – **zbiór liczb zespolonych**

Dla dowolnego zbioru A, zapis $x \in A$ oznacza, że x jest elementem tego zbioru.

Dla zbiorów A, B, zapis $A \subseteq B$ oznacza, że A jest podzbiorem zbioru B.

Zapis $A \subset B$ oznacza, że A jest podzbiorem właściwym zbioru B, tzn.

$$A \subset B \quad \Leftrightarrow \quad (A \subseteq B) \wedge (B \setminus A \neq \emptyset).$$

Zbiory:

$\emptyset$ – **zbiór pusty**

$\{a\}$ – **zbiór jednoelementowy, zawierający tylko element** a

$\{a_1, a_2, \ldots, a_n\}$ – **zbiór, którego elementami są** $a_1, a_2, \ldots, a_n$

$\{x \in X : W(x)\}$ – **zbiór tych elementów zbioru** X**, dla których funkcja zdaniowa** $W(x)$**,** $x \in X$**, staje się zdaniem prawdziwym**

$|X|$ – **liczność (moc) zbioru skończonego** X

$\mathcal{P}(X)$ – **rodzina wszystkich podzbiorów zbioru** X

Operacje na zbiorach:

$\cup$ – **suma (mnogościowa) zbiorów**

$\cap$ – **przecięcie zbiorów**

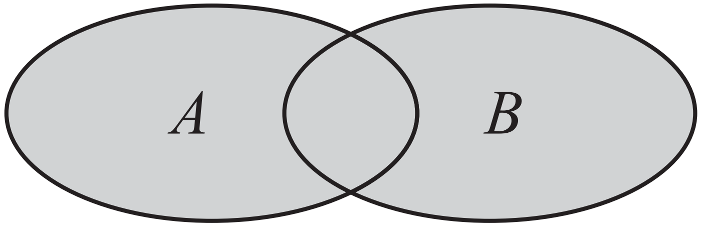
$\setminus$ – **różnica zbiorów**

$\otimes$ – **różnica symetryczna zbiorów**

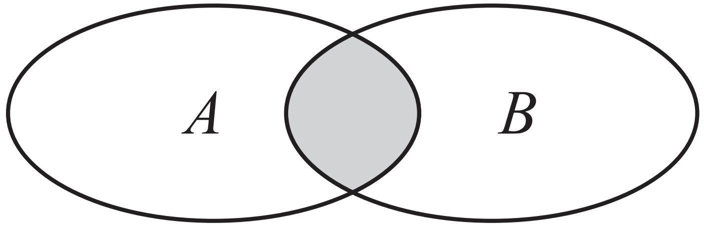
$\times$ – **iloczyn kartezjański zbiorów**

Diagramy Venna

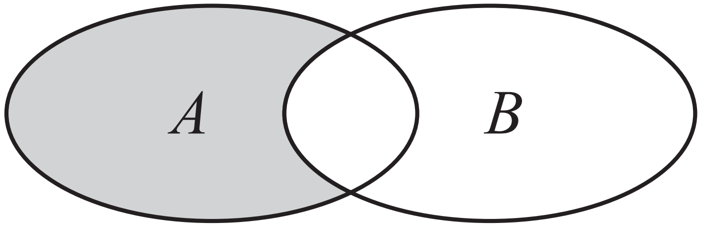
$C = A \cup B$



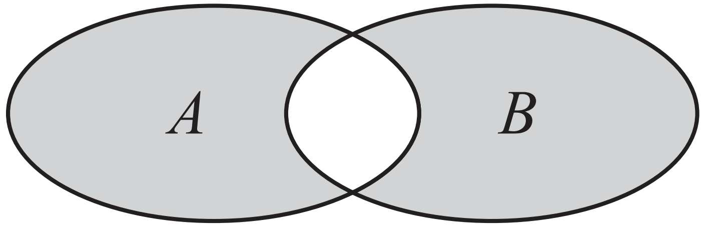
$C = A \cap B$



$C = A \setminus B$



$C = A \otimes B$



Dla $a, b \in E$, gdzie E jest dowolnym zbiorem, symbol (a, b) oznacza parę uporządkowaną o poprzedniku a i następniku b.

Iloczyn kartezjański zbiorów A i B

$$A \times B = \{(a, b) : \ a \in A, \ b \in B\}.$$

RELACJE BINARNE

Definicja

Relacją binarną w iloczynie kartezjańskim zbiorów A i B nazywamy dowolny podzbiór zbioru $A \times B$.

W przypadku, gdy oba zbiory są identyczne, tzn. $A = X$ oraz $B = X$, mówimy o relacji binarnej w zbiorze X.

Jeśli $R \subseteq A \times B$ jest relacją binarną w iloczynie kartezjańskim zbiorów A i B, to dla zaznaczenia faktu, że para (a, b) jest elementem relacji R piszemy:

$$(a, b) \in R$$

albo

$$aRb$$

Zbiór wszystkich poprzedników par należących do relacji R nazywamy dziedziną relacji R.

Zbiór wszystkich następników par należących do relacji R nazywamy przeciwdziedziną relacji R.

W iloczynie kartezjańskim zbiorów A i B możemy zdefiniować co najwyżej $2^{m \cdot n}$ różnych relacji binarnych, gdzie $m = |A|$ oraz $n = |B|$, bowiem dokładnie tyle elementów liczy rodzina wszystkich podzbiorów zbioru $A \times B$.

$R = \emptyset$ – **relacja pusta w** $A \times B$

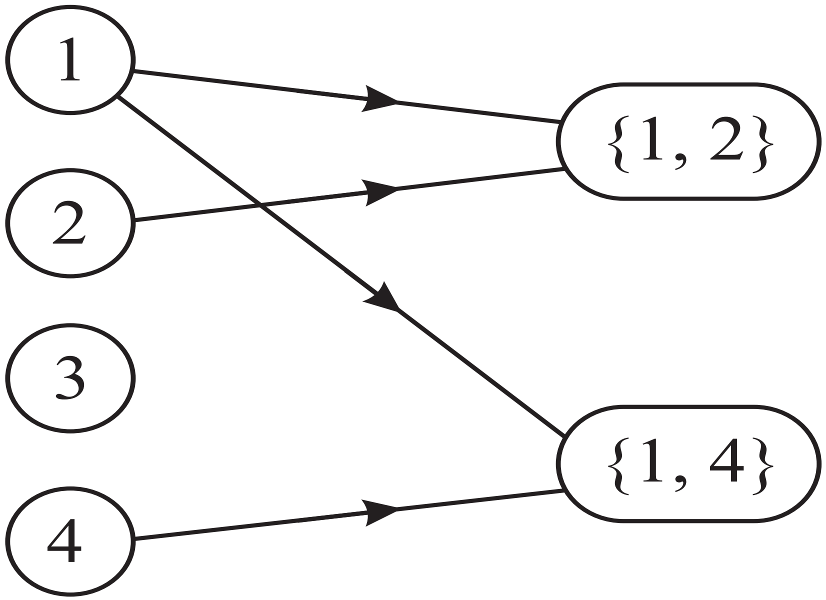
$R = A \times B$ – **relacja pełna w** $A \times B$

GRAF RELACJI

$A = \{1, 2, 3, 4\}$, $B = \{\{1, 2\}, \{1, 4\}\}$
$R \subseteq A \times B$ – **relacja przynależności do zbioru w** $A \times B$

$$R = \{(1, \{1, 2\}), (1, \{1, 4\}), (2, \{1, 2\}), (4, \{1, 4\})\}$$

Dziedzina relacji R**:** $\{1, 2, 4\}$
Przeciwdziedzina relacji R**:** $\{\{1, 2\}, \{1, 4\}\}$



TABLICA RELACJI

$A = \{1, 2, 3, 4\}$, $B = \{\{1, 2\}, \{1, 4\}\}$

$R \subseteq A \times B$ – **relacja przynależności do zbioru w** $A \times B$

$$R = \{(1, \{1, 2\}), (1, \{1, 4\}), (2, \{1, 2\}), (4, \{1, 4\})\}$$

Dziedzina relacji R**:** $\{1, 2, 4\}$

Przeciwdziedzina relacji R**:** $\{\{1, 2\}, \{1, 4\}\}$

	{1, 2}	{1, 4}
1	1	1
2	1	0
3	0	0
4	0	1

$R \subseteq X \times X$ – **relacja w zbiorze** X

O relacji R **mówimy, że jest:**

zwrotna – **jeśli** xRx **dla każdego** $x \in X$

przechodnia – **jeśli** $(xRy \wedge yRz) \Rightarrow xRz$ **dla dowolnych** $x, y, z \in X$

symetryczna – **jeśli** $xRy \Rightarrow yRx$ **dla dowolnych** $x, y \in X$

antysymetryczna – **jeśli** $(xRy \wedge yRx) \Rightarrow x = y$ **dla dowolnych** $x, y \in X$

Definicja

Relacją równoważności w zbiorze X nazywamy relację, która jest zwrotna, przechodnia i symetryczna.

Relacja równoważności R w zbiorze X dzieli ten zbiór na podzbiory, nazywane klasami równoważności (albo – klasami abstrakcji) relacji R w zbiorze X.

Dla $x \in X$ definiujemy zbiór oznaczany symbolem x/R, gdzie

$$x/R = \{y \in X : \ xRy\}.$$

Zbiór taki nazywamy klasą abstrakcji relacji R wyznaczoną przez element x.

Zbiór wszystkich klas abstrakcji relacji R w zbiorze X oznaczamy symbolem X/R.

Przykład

Rozważmy relację oznaczoną symbolem $\simeq$, zdefiniowaną w zbiorze $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geqslant 0\}$ w sposób następujący:

$x \simeq y$ **wtedy i tylko wtedy, gdy** $x - y \in \mathbb{Z}$**.**

Relacja $\simeq$ jest symetryczna, zwrotna i przechodnia, a zatem jest relacją równoważności.

Klasą abstrakcji tej relacji, wyznaczoną przez element $x \in \mathbb{R}_+$, jest zbiór liczb rzeczywistych, które mają tę samą część ułamkową co x.

Definicja

Relacją częściowego porządku w zbiorze X nazywamy relację, która jest zwrotna, przechodnia i antysymetryczna.

Parę uporządkowaną $(X, \preceq)$, gdzie X jest dowolnym zbiorem, a $\preceq$ jest relacją częściowego porządku w X, nazywamy zbiorem (częściowo) uporządkowanym.

Przykład

Rozważmy relację podzielności, oznaczaną symbolem $|$, którą definiujemy w zbiorze liczb naturalnych w sposób następujący:

$a \,|\, b$ **dla** $a, b \in \mathbb{N}$ **wtedy i tylko wtedy,**
gdy istnieje $k \in \mathbb{N}$**, dla którego** $b = k \cdot a$**.**

Relacja podzielności w $\mathbb{N}$ jest zwrotna, przechodnia i antysymetryczna, a zatem jest relacją częściowego porządku.

FUNKCJE

Definicja

Funkcją ze zbioru X w zbiór Y nazywamy dowolną relację $f \subseteq X \times Y$, mającą tę właściwość, że dla każdego $x \in X$ istnieje dokładnie jeden element $y \in Y$, taki że $(x, y) \in f$.

Dziedziną relacji $f \subseteq X \times Y$, będącej funkcją, jest więc cały zbiór X. Ponieważ dla danego elementu x, należącego do dziedziny funkcji f, istnieje dokładnie jedna para $(x, y) \in f$, zwykle piszemy $y = f(x)$ na oznaczenie faktu, że $(x, y) \in f$. Taki element $y \in Y$ nazywamy wartością funkcji f dla argumentu x.

Dla zaznaczenia, że relacja $f \subseteq X \times Y$ jest funkcją, stosujemy zapis:

$$f : X \to Y$$

Zbiór wszystkich funkcji $f : X \to Y$ oznaczamy symbolem $Fun(X, Y)$.

Dla dowolnego zbioru $A \subseteq X$ oraz funkcji $f \in Fun(X, Y)$, zbiór $f(A) \subseteq Y$, gdzie

$$f(A) = \{y \in Y : \text{ istnieje } x \in A, \text{ taki że } y = f(x)\},$$

nazywamy obrazem zbioru A przez funkcję f.

Dla podzbioru $B \subseteq Y$, zbiór

$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$

nazywamy przeciwobrazem zbioru B przez funkcję f.

Rodzinę przeciwobrazów wszystkich jednoelementowych podzbiorów zbioru Y, to znaczy rodzinę

$$N(f) = \{f^{-1}(\{y\}),\ y \in Y\},$$

nazywamy jądrem funkcji f.

SURJEKCJE

Jeśli dla funkcji $f \in Fun(X, Y)$ zachodzi warunek $f(X) = Y$, to mówimy, że jest to funkcja ze zbioru X na zbiór Y.

Funkcja o tej własności nazywana jest też surjekcją.

Podzbiór wszystkich surjekcji w zbiorze $Fun(X, Y)$ oznaczamy symbolem $Sur(X, Y)$.

INJEKCJE

Jeśli $f \in Fun(X, Y)$ **oraz dla dowolnych elementów** $a, b \in X$ **zachodzi warunek**

$$a \neq b \;\Rightarrow\; f(a) \neq f(b),$$

to funkcję f **nazywamy funkcją różnowartościową lub injekcją.**

Podzbiór wszystkich injekcji w zbiorze $Fun(X, Y)$ **oznaczamy symbolem** $Inj(X, Y)$**.**

BIJEKCJE

Funkcja, która jest jednocześnie surjekcją i injekcją, jest nazywana bijekcją.

Podzbiór wszystkich bijekcji w zbiorze $Fun(X, Y)$ oznaczamy symbolem $Bij(X, Y)$.

CIĄGI

Funkcję $f \in Fun(X, Y)$, której dziedziną jest k-elementowy zbiór liczb naturalnych $X = \{0, 1, 2, \ldots, k-1\}$ (albo $X = \{1, 2, \ldots, k\}$), nazywamy k-elementowym ciągiem o wyrazach ze zbioru Y i oznaczamy symbolem $(a_0, a_1, \ldots, a_{k-1})$ (albo $(a_1, \ldots, a_k)$).

Jeśli dla dowolnych dwóch różnych argumentów, wartości tej funkcji są różne, to wówczas mówimy o ciągu różnowartościowym.

ZAGADNIENIA ZLICZANIA

- **Na ile sposobów można przydzielić n programów do m procesorów?**
- **Ile nazw plików można utworzyć przy zadanym alfabecie i zadanych ograniczeniach na długość nazwy?**
- **Na ile sposobów można rozmieścić n obiektów w m pudełkach, jeśli istotna jest kolejność obiektów?**
- **Na ile sposobów można skonstruować system wieloprocesorowy typu *hypercube* mając do dyspozycji zadany zestaw procesorów?**
- **Ile jest różnych łańcuchów DNA, zawierających dane liczby nukleotydów C, G, T, A ?**

ZLICZANIE FUNKCJI

Dane są zbiory skończone X, Y

Ile elementów ma zbiór $Fun(X,Y)$?

Twierdzenie

Jeśli $|X| = n$ oraz $|Y| = m$, to liczba wszystkich funkcji $f : X \to Y$ jest równa m^n.

$$\boxed{|Fun(X,Y)| = |Y|^{|X|} = m^n}$$

$$X = \{x_1, x_2, x_3\}, \quad Y = \{y_1, y_2, y_3, y_4\}$$

$$X \times Y = \left\{ \begin{array}{cccc} (x_1, y_1), & (x_1, y_2), & (x_1, y_3), & (x_1, y_4), \\ (x_2, y_1), & (x_2, y_2), & (x_2, y_3), & (x_2, y_4), \\ (x_3, y_1), & (x_3, y_2), & (x_3, y_3), & (x_3, y_4) \end{array} \right\}$$

Przykład funkcji w $X \times Y$:

$$\color{red}{f} = \left\{ \begin{array}{cccc} & & (x_1, y_3), & \\ (x_2, y_1), & & & \\ (x_3, y_1), & & & \end{array} \right\}$$

Ile elementów ma zbiór $Inj(X,Y)$?

Twierdzenie

Jeśli $|X| = n$ **oraz** $|Y| = m$**, to liczba wszystkich funkcji różnowartościowych** $f : X \to Y$ **jest równa**

$$m \cdot (m-1) \cdot \ldots \cdot (m-n+1).$$

Oznaczenie **(**n**-ta potęga ubywająca liczby** m**):**

Dla $m, n \in \mathbb{N}$**,** $0 < n \leqslant m$**,**

$$m^{\underline{n}} = m \cdot (m-1) \cdot \ldots \cdot (m-n+1)$$

Dla $m < n$**,** $m^{\underline{n}} = 0$

Dla $m \in \mathbb{N}$ **przyjmujemy, że** $m^{\underline{0}} = 1$

$$\boxed{|Inj(X,Y)| = m^{\underline{n}}}$$

Ile elementów ma zbiór $Bij(X, Y)$?

Wniosek

Jeśli $|X| = |Y| = n$, to liczba wszystkich bijekcji w zbiorze $Fun(X, Y)$ jest równa

$$n^{\underline{n}} = n \cdot (n-1) \cdot \ldots \cdot 1$$

Oznaczenie **(n silnia)**

Dla $0 < n \in \mathbb{N}$

$$n! = n^{\underline{n}} = n \cdot (n-1) \cdot \ldots \cdot 1$$

$0! = 0^{\underline{0}} = 1$

$$\boxed{|Bij(X, Y)| = n!}$$

Permutacje

Definicja

Permutacją zbioru X nazywamy dowolną funkcję różnowartościową $f \in Fun(X, X)$.

Wniosek

Liczba wszystkich permutacji zbioru n-elementowego jest równa $n!$.

Dla $n \in \mathbb{N}, \quad n > 0$

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n,$$

gdzie e jest podstawą logarytmów naturalnych, $e \approx 2,7182\ldots$.

Rozmieszczenia uporządkowane

Dane: n obiektów, m pudełek

1.	1 a b	2	3
2.	1 b a	2	3
3.	1 a	2 b	3
4.	1 b	2 a	3
5.	1 a	2	3 b
6.	1 b	2	3 a
7.	1	2 a	3 b
8.	1	2 b	3 a
9.	1	2 a b	3
10.	1	2 b a	3
11.	1	2	3 a b
12.	1	2	3 b a

Wszystkie rozmieszczenia uporządkowane obiektów ze zbioru $\{a, b\}$ w trzech pudełkach.

Oznaczenie (n**-ta potęga przyrastająca liczby** m)

Dla $m, n \in \mathbb{N},\ n > 0$**:**

$$m^{\overline{n}} = m \cdot (m+1) \cdot \ldots \cdot (m+n-1).$$

Dla $m \in \mathbb{N}$ **przyjmiemy, że** $m^{\overline{0}} = 1$**.**

Twierdzenie

Liczba wszystkich rozmieszczeń uporządkowanych n **obiektów w** m **pudełkach jest równa** $m^{\overline{n}}$**.**

Twierdzenie

Dla $m, n \in \mathbb{N}$, dla których wyrażenia poniższe są dobrze określone, zachodzą następujące tożsamości:

$$1^{\overline{n}} = n! \tag{1}$$

$$m^{\overline{n}} = (m+n-1)^{\underline{n}} \tag{2}$$

$$m^{\underline{n}} = m^{\underline{n-1}} \cdot (m-n+1) \tag{3}$$

$$m^{\underline{n}} = (m-1)^{\underline{n-1}} \cdot m \tag{4}$$

$$m^{\underline{n}} = m^{\underline{m-n}} \cdot \frac{n!}{(m-n)!} \tag{5}$$

$$m^{\underline{n}} = (m-1)^{\underline{n}} \cdot \frac{m}{m-n} \tag{6}$$

$$m^{\underline{n}} = \frac{m!}{(m-n)!} \tag{7}$$

PERMUTACJE

Permutacją zbioru X nazywamy dowolną funkcję różnowartościową $f : X \to X$.

Zapis permutacji f w postaci tablicy:

– w górnym wierszu umieszczamy elementy zbioru X,
– pod nimi w dolnym wierszu – odpowiednie wartości funkcji f dla tych argumentów.

Przykład $X = \{a, b, c, d\}$ $f(a) = d$, $f(b) = a$, $f(c) = c$, $f(d) = b$.

Zapis permutacji f w postaci tablicy jest następujący:

$$f = \begin{pmatrix} a & b & c & d \\ d & a & c & b \end{pmatrix}.$$

Jeśli $X = \{1, \ldots, n\}$, to permutacje zbioru X są ciągami różnowartościowymi o wyrazach ze zbioru X.

Permutację $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ identyfikujemy z wektorem

$$(a_1, \ldots, a_n),$$

gdzie $a_i = f(i), \quad i = 1, \ldots, n$.

<u>Oznaczenie</u>

Zbiór wszystkich permutacji zbioru $\{1, \ldots, n\}$ oznaczamy symbolem S_n.

Składanie permutacji

Wynikiem złożenia dwóch permutacji f i g ze zbioru S_n jest również permutacja należąca do tego zbioru, którą oznaczamy symbolem fg.

Zgodnie z zasadą składania funkcji mamy:

$$fg(i) = f(g(i)) \quad \text{dla } i = 1, \ldots, n$$

Permutację f nazywamy permutacją zewnętrzną, natomiast permutację g – permutacją wewnętrzną.

Przy składaniu permutacji *istotna* jest ich kolejność. W ogólnym przypadku permutacja fg jest *różna* od permutacji gf.

Przykład

Rozważmy dwie permutacje f oraz g zbioru $\{1, \ldots, n\}$, gdzie

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}.$$

Złożeniem permutacji f i g jest następująca permutacja fg:

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}.$$

Natomiast złożeniem permutacji g i f jest permutacja gf:

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

Permutacja identycznościowa $e \in S_n$

$$e(i) = i \quad \textbf{dla} \quad i = 1, \ldots, n$$

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Dla każdego $f \in S_n$ mamy zależności

$$ef = fe = f$$

Permutacja odwrotna

Permutacją odwrotną do permutacji $f \in S_n$ nazywamy permutację $f^{-1} \in S_n$, spełniającą warunek $f^{-1}f = e$.

Dla każdej permutacji $f \in S_n$ permutacja odwrotna istnieje i jeśli

$$f = \begin{pmatrix} \ldots & i & \ldots \\ \ldots & j & \ldots \end{pmatrix},$$

to

$$f^{-1} = \begin{pmatrix} \ldots & j & \ldots \\ \ldots & i & \ldots \end{pmatrix}.$$

Działanie dwuargumentowe (operacja binarna)

S, T – zbiory

Definicja

Działaniem dwuargumentowym w zbiorze S nazywamy dowolną funkcję ze zbioru $S \times S$ w zbiór T.

Zwykle dla oznaczenia działania dwuargumentowego stosujemy specjalny symbol (na przykład $*, +, -$ itp.). Na oznaczenie faktu, że element $c \in T$ jest wartością funkcji $*$ dla argumentu, będącego parą uporządkowaną $(a, b) \in S \times S$, piszemy $a * b = c$.

W przypadku złożenia permutacji symbol działania jest zwykle pomijany dla uproszczenia zapisu.

Grupa

Definicja

Parę uporządkowaną $(S, *)$, gdzie S jest zbiorem, a $*$ jest działaniem dwuargumentowym w S, nazywamy grupą, jeśli:

- **dla dowolnych $a, b \in S$, $a * b \in S$;**
- **dla dowolnych $a, b, c \in S$, $(a * b) * c = a * (b * c)$;**
- **istnieje taki element $e \in S$, że dla każdego $a \in S$, $a * e = a$;**
- **dla każdego $a \in S$ istnieje taki element $a^{-1} \in S$, dla którego $a * a^{-1} = e$.**

Liczność zbioru S nazywamy rzędem grupy $(S, *)$.

Element e w definicji grupy nazywamy elementem neutralnym grupy.

Element a^{-1}, dla którego $a * a^{-1} = e$, nazywamy elementem odwrotnym dla elementu a.

Jeśli rząd grupy spełnia warunek $|S| < \infty$, to grupę taką nazywamy grupą skończoną.

Grupa symetryczna stopnia n

Zbiór permutacji S_n z działaniem złożenia spełnia wszystkie warunki definicji grupy; grupa ta jest nazywana grupą symetryczną stopnia n.

- **Wynikiem złożenia permutacji $f, g \in S_n$ jest permutacja $fg \in S_n$.**
- **Dla dowolnych permutacji $f, g, h \in S_n$ mamy $(fg)h = f(gh)$.**
- **Elementem neutralnym grupy S_n jest permutacja e.**
- **Elementem odwrotnym dla elementu $f \in S_n$ jest permutacja odwrotna $f^{-1} \in S_n$.**

Grupa permutacji stopnia n

Definicja

Grupą permutacji stopnia n nazywamy dowolny podzbiór $G \subseteq S_n$, spełniający następujące warunki:

- $f \in G \wedge g \in G \Rightarrow fg \in G$ **dla wszystkich** $f, g \in G$;
- $f \in G \Rightarrow f^{-1} \in G$ **dla każdego** $f \in G$.

Przykład

Rozważmy zbiór $S_4 = \{\pi_1, \ldots, \pi_{24}\}$, składający się ze wszystkich permutacji zbioru $\{1, 2, 3, 4\}$.

Niech $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ będzie podzbiorem zbioru S_4, przy czym

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

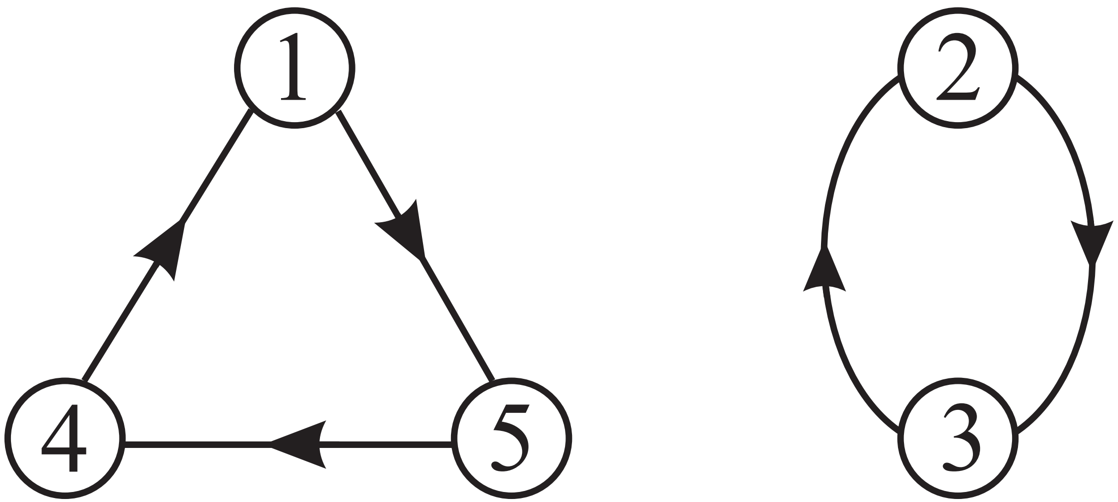
Zbiór G z działaniem złożenia jest grupą permutacji stopnia 4.
Rząd tej grupy jest równy 4.
Elementem neutralnym jest permutacja π_1.

Rozkład permutacji na cykle rozłączne

Przykład

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

Rysunek grafu permutacji f:



$(a_{i_1}, \ldots, a_{i_k})$ – **ciąg różnowartościowy o wyrazach w zbiorze** $\{1, \ldots, n\}$

Definicja

Permutację $\pi \in S_n$ **nazywamy cyklem wyznaczonym przez ciąg** $(a_{i_1}, \ldots, a_{i_k})$**, jeśli:**

$\pi(a_{i_j}) = a_{i_{j+1}}$ **dla** $j = 1, \ldots, k-1$**;**

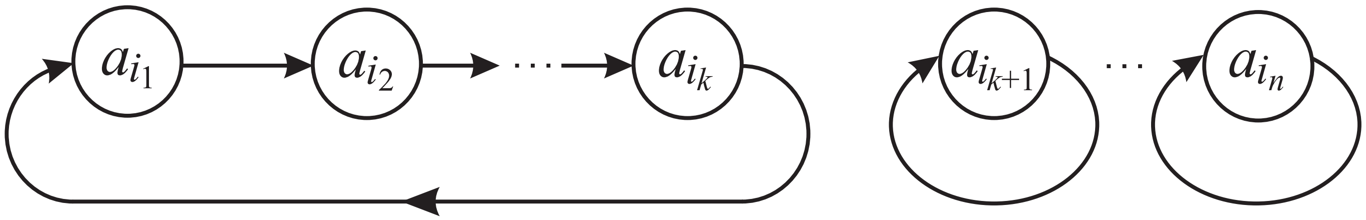
$\pi(a_{i_k}) = a_{i_1}$**;**

$\pi(a_l) = a_l$ **dla** $l \neq i_1, \ldots, i_k$.

Cykl wyznaczony przez ciąg $(a_{i_1}, \ldots, a_{i_k})$**, oznaczamy symbolem** $[a_{i_1}, \ldots, a_{i_k}]$**.**

Liczbę k **nazywamy długością cyklu.**

Rysunek grafu permutacji $\pi \in S_n$, będącej cyklem wyznaczonym przez ciąg $(a_{i_1}, \ldots, a_{i_k})$:



Cykle wyznaczone przez ciągi $(a'_{i_1}, \ldots, a'_{i_k})$ oraz $(a''_{i_1}, \ldots, a''_{i_l})$ nazywamy cyklami rozłącznymi, jeśli

$$\{a'_{i_1}, \ldots, a'_{i_k}\} \cap \{a''_{i_1}, \ldots, a''_{i_l}\} = \emptyset$$

Definicja

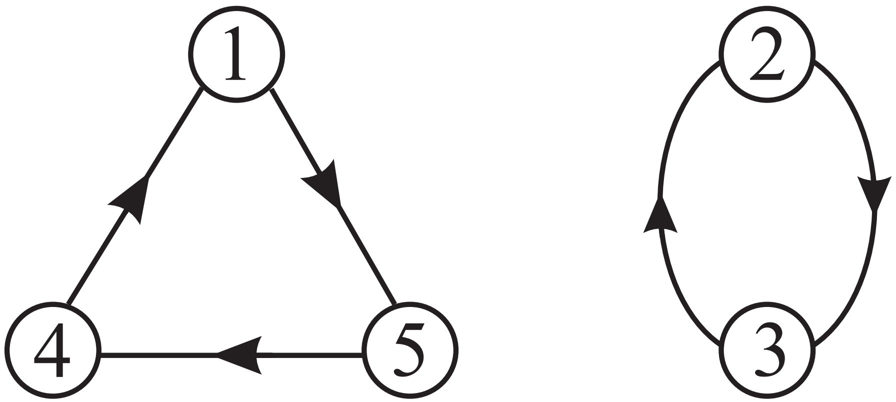
Rozkładem permutacji $f \in S_n$ na cykle rozłączne nazywamy zbiór cykli parami rozłącznych, których złożeniem jest permutacja f.

Rozkład permutacji na cykle *rozłączne* jest wyznaczony jednoznacznie.

Dla permutacji f ze zbioru S_n jej rozkład na cykle rozłączne zawiera od jednego do n elementów. Z pierwszą sytuacją mamy do czynienia w przypadku permutacji, która sama jest cyklem o długości n, natomiast druga dotyczy permutacji identycznościowej.

Przykład

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$



$$f' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} = [1, 5, 4], \qquad f'' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = [2, 3]$$

$$f = f'f'' = f''f' = [1, 5, 4][2, 3] = [2, 3][1, 5, 4]$$

Typ permutacji

Mówimy, że permutacja $f \in S_n$ jest typu $(\lambda_1, \ldots, \lambda_n)$, jeśli jej rozkład na cykle rozłączne zawiera dokładnie λ_i cykli o długości i dla $i = 1, \ldots, n$.

Typ permutacji będziemy również podawać w postaci następującego równoważnego zapisu:

$$1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}.$$

Często dla uproszczenia będziemy pomijać w takim zapisie elementy, dla których $\lambda_i = 0$.

Przykład

Rozważmy permutację $f \in S_9$, gdzie

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 4 & 2 & 3 & 6 & 9 & 8 \end{pmatrix}.$$

Rozkład tej permutacji na cykle rozłączne ma postać:

$$f = [1, 7, 6, 3][2, 5][4][8, 9].$$

Permutacja f jest więc typu

$$(1, 2, 0, 1, 0, 0, 0, 0, 0),$$

co możemy również zapisać w postaci

$$1^1 2^2 4^1.$$

Inwersje permutacji

Definicja

Inwersją permutacji $f = (a_1, \ldots, a_n) \in S_n$ **nazywamy parę** (a_i, a_j)**, dla której**

$$i < j \leqslant n \quad \textbf{oraz} \quad a_i > a_j.$$

Liczbę wszystkich inwersji permutacji f **oznaczamy symbolem** $I(f)$**.**

Znak permutacji

Definicja

Znakiem permutacji $f \in S_n$ nazywamy liczbę

$$sgn(f) = (-1)^{I(f)}.$$

Permutację f nazywamy:

permutacją parzystą, jeśli $sgn(f) = 1$,

permutacją nieparzystą, jeśli $sgn(f) = -1$.

Przykład

Rozważmy permutację $f \in S_5$, gdzie

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}.$$

Inwersjami tej permutacji są następujące pary:

$$(5,3), (5,2), (5,1), (5,4), (3,2), (3,1), (2,1).$$

Zatem $I(f) = 7$ **oraz** $sgn(f) = (-1)^7 = -1$**.**

Permutacja f jest więc permutacją *nieparzystą*.

Transpozycje

Definicja

Transpozycją nazywamy permutację, która jest cyklem o długości 2.

Permutacją odwrotną do dowolnej transpozycji jest ta sama permutacja.

Jeśli permutacja $t \in S_n$ jest transpozycją o postaci $[i, i+1]$ dla pewnego $i \in \{1, \ldots, n-1\}$, to taką permutację nazywamy transpozycją sąsiednich elementów.

Twierdzenie

Dowolną permutację $f \in S_n$ można przedstawić w postaci złożenia $I(f)$ transpozycji sąsiednich elementów.

Jeśli $f = (a_1, \ldots, a_n) \in S_n$ oraz $t = [i, i+1]$ dla pewnego $i = 1, \ldots, n-1$, to

$$ft = (a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n)$$

Przykład $f = (2, 4, 3, 5, 1) \in S_5$**,** $\quad I(f) = 5$

$$f\ [4,5][3,4][2,3][1,2][3,4] = e$$

$$f = (2,4,3,5,1) = ([4,5][3,4][2,3][1,2][3,4])^{-1} = [3,4][1,2][2,3][3,4][4,5]$$

M. Rejewski – *An application ot the theory of permutations in breaking the Enigma cipher*. Applicationes Mathematicae, (1980) nr 4.

Dla $f \in S_n$ i dowolnej transpozycji sąsiednich elementów $t \in S_n$ mamy $sgn(ft) = -sgn(f)$.

$$sgn(fg) = sgn(f\ t_1 \ldots t_{I(g)}) = sgn(f) \cdot (-1)^{I(g)} = sgn(f) \cdot sgn(g).$$

Twierdzenie **Dla dowolnych permutacji $f, g \in S_n$,**

$$sgn(fg) = sgn(f) \cdot sgn(g).$$

Wniosek **Dla dowolnej permutacji $f \in S_n$,**

$$sgn(f^{-1}) = sgn(f).$$

Twierdzenie

Każda transpozycja jest permutacją nieparzystą.

Twierdzenie

Znak cyklu o długości k **jest równy** $(-1)^{k-1}$**.**

$$[a_1, \ldots, a_k] = [a_1, a_2][a_2, a_3] \ldots [a_{k-1}, a_k].$$

Twierdzenie

Znak dowolnej permutacji f **typu** $1^{\lambda_1} \ldots n^{\lambda_n}$ **wyraża się wzorem**

$$sgn(f) = (-1)^{\sum_{j=1}^{\lfloor n/2 \rfloor} \lambda_{2j}}.$$

Przykład **Rozważmy permutację**

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 4 & 2 & 3 & 6 & 9 & 8 \end{pmatrix}.$$

Rozkładając f na cykle rozłączne otrzymujemy:

$$f = [1\ 7\ 6\ 3][2\ 5\ ][4][8\ 9].$$

Permutacja f jest więc typu

$$1^1 2^2 4^1.$$

Z twierdzenia o znaku mamy:

$$sgn(f) = (-1)^{\Sigma_{j=1}^{4} \lambda_{2j}} = (-1)^{\lambda_2+\lambda_4+\lambda_6+\lambda_8} = (-1)^{2+1} = -1.$$

Permutacja f jest zatem permutacją *nieparzystą*.

PODZBIORY ZBIORÓW SKOŃCZONYCH

$$X = \{x_1, \ldots, x_n\}$$

$\mathcal{P}(X)$ – **rodzina wszystkich podzbiorów zbioru** X

Ile jest wszystkich podzbiorów zbioru X?

$$\boxed{|\mathcal{P}(X)| = 2^{|X|}}$$

Wektory charakterystyczne podzbiorów

Istnieje wzajemnie jednoznaczna odpowiedniość między elementami zbioru $\mathcal{P}(X)$ dla $|X| = n$ a elementami zbioru $\mathbb{B}^n$.

Każdemu podzbiorowi $Y \subseteq X = \{x_1, \ldots, x_n\}$ odpowiada jednoznacznie wektor

$$\xi(Y) = (b_1, \ldots, b_n) \in \mathbb{B}^n$$

nazywany wektorem charakterystycznym zbioru Y, gdzie

$$b_i = \lfloor x_i \in Y \rceil \quad \text{dla } i = 1, \ldots, n.$$

Podobnie, wektorowi $b = (b_1, \ldots, b_n) \in \mathbb{B}^n$ możemy jednoznacznie przyporządkować podzbiór Y zbioru $X = \{x_1, \ldots, x_n\}$, biorąc $Y = \{x_i \in X : \ b_i = 1, \ \ i = 1, \ldots, n\}$.

Generowanie wszystkich podzbiorów zbioru X

Wektory charakterystyczne $\xi(Y) \in \mathbb{B}^n$ dla $Y \subseteq X$, można traktować jako zapisy w dwójkowym systemie pozycyjnym wszystkich 2^n liczb naturalnych z przedziału domkniętego $[0, 2^n - 1]$.

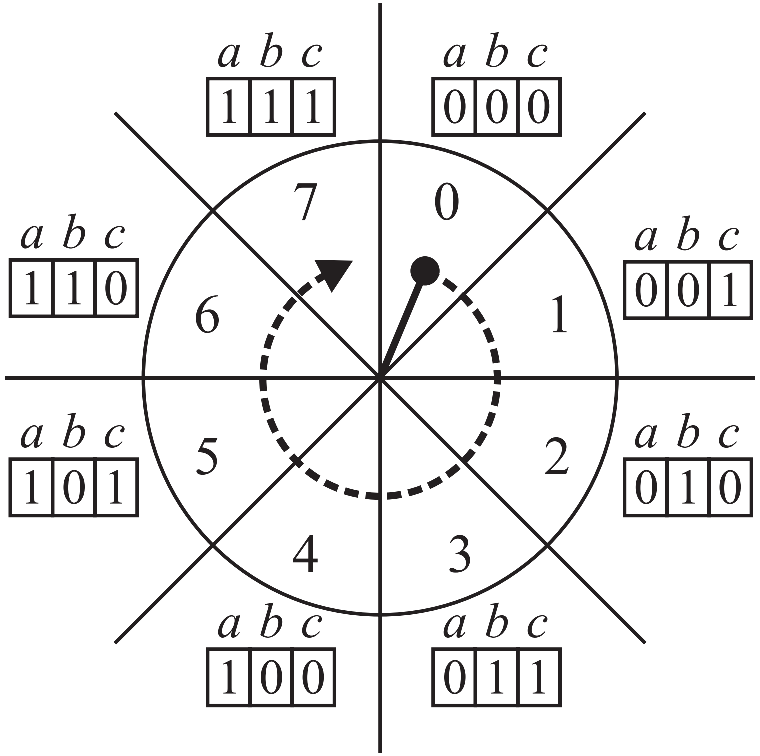
<u>**Metoda wyznaczenia elementów rodziny $\mathcal{P}(X)$:**</u>

Wypisz kolejno podzbiory zbioru X, których wektory charakterystyczne są reprezentacjami dwójkowymi kolejnych liczb naturalnych z przedziału $[0, 2^{|X|} - 1]$.

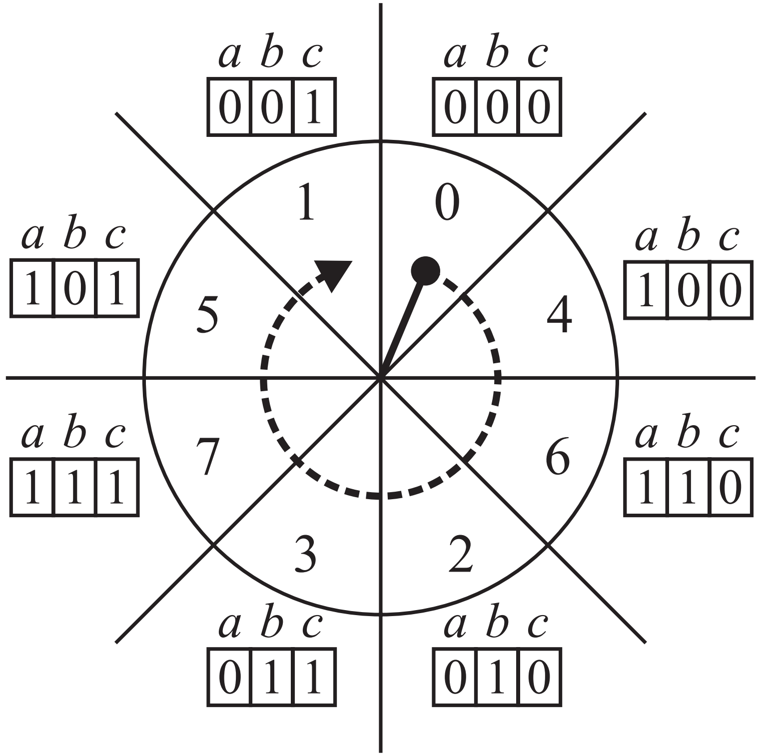
Przykład **Dany jest zbiór $X = \{a, b, c\}$**

W kolejnych wierszach tabeli wypisane są: podzbiór Y zbioru X, jego wektor charakterystyczny $\xi(Y)$ i liczba naturalna $\eta(Y)$, dla której ten wektor jest reprezentacją w systemie dwójkowym.

Y	$\xi(Y)$	$\eta(Y)$
$\emptyset$	$(0,0,0)$	**0**
$\{c\}$	$(0,0,1)$	**1**
$\{b\}$	$(0,1,0)$	**2**
$\{b,c\}$	$(0,1,1)$	**3**
$\{a\}$	$(1,0,0)$	**4**
$\{a,c\}$	$(1,0,1)$	**5**
$\{a,b\}$	$(1,1,0)$	**6**
$\{a,b,c\}$	$(1,1,1)$	**7**



$$(\ \emptyset,\ \{c\},\ \{b\},\ \{b,c\},\ \{a\},\ \{a,c\},\ \{a,b\},\ \{a,b,c\}\ )$$



$$(\ \emptyset,\ \{a\},\ \{a,b\},\ \{b\},\ \{b,c\},\ \{a,b,c\},\ \{a,c\},\ \{c\}\ )$$

Kod Graya rzędu n:

Ciąg wszystkich wektorów należących do zbioru $\mathbb{B}^n$, uporządkowanych w taki sposób, aby sąsiednie wektory ciągu oraz wektory pierwszy i ostatni różniły się dokładnie na jednej pozycji.

Taki ciąg wektorów ze zbioru $\mathbb{B}^n$ istnieje dla dowolnego $n \geqslant 1$ i nosi nazwę kodu Graya rzędu n.

Na przykład w przypadku $n = 3$ jeden z możliwych kodów Graya rzędu 3 ma postać następującego ciągu:

$$((0,0,0), (1,0,0), (1,1,0), (0,1,0), (0,1,1), (1,1,1), (1,0,1), (0,0,1))$$

Zwierciadlany kod Graya

Jeśli mamy kod Graya rzędu k dla pewnego $k \in \mathbb{N}$, $k \geqslant 1$, zapisany w postaci ciągu:

$$((C_1), (C_2), \ldots, (C_{m-1}), (C_m)),$$

gdzie $m = 2^k$, $(C_i) \in \mathbb{B}^k$, to następujący ciąg wektorów należących do $\mathbb{B}^{k+1}$ jest kodem Graya rzędu $k+1$:

$$((C_1, 0), (C_2, 0), \ldots, (C_{m-1}, 0), (C_m, 0),$$
$$(C_m, 1), (C_{m-1}, 1), \ldots, (C_2, 1), (C_1, 1)).$$

Zapisy $(C_i, 0)$ oraz $(C_i, 1)$ oznaczają dla k-elementowego wektora (C_i), gdzie $i = 1, \ldots, m$, odpowiednio $(k+1)$-elementowe wektory, otrzymywane przez uzupełnienie wektora (C_i) przez zero albo jedynkę na ostatniej pozycji.

Przykład

Kody Graya rzędu n dla $n = 1, 2, 3, 4$

(dla uproszczenia zapisu pominięte są nawiasy i przecinki w oznaczeniach wektorów):

$n = 1$	0	1						
$n = 2$	00	10	11	01				
$n = 3$	000	100	110	010	011	111	101	001
$n = 4$	0000	1000	1100	0100	0110	1110	1010	0010
	0011	1011	1111	0111	0101	1101	1001	0001

Podzbiory k-elementowe zbiorów skończonych

$X = \{x_1, \ldots, x_n\}$ – **zbiór**, k – **liczba naturalna**

Ile jest wszystkich różnych podzbiorów zbioru X, mających dokładnie k elementów?

Liczbę k-elementowych podzbiorów zbioru n-elementowego będziemy oznaczać symbolem

$$\binom{n}{k}$$

i nazywać współczynnikiem dwumianowym.

Symbol n w tym zapisie nazywamy indeksem górnym, natomiast symbol k – indeksem dolnym.

Wzór dwumianowy Newtona

Dla $x, y \in \mathbb{R}$ oraz $n \in \mathbb{N}$ zachodzi następująca równość:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \, y^{n-i}.$$

Twierdzenie

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\cdot\ldots\cdot k} = \frac{n!}{k!\,(n-k)!}$$

Dowód **Dowolna injekcja $f \in Fun(A, X)$, gdzie $|A| = k$ oraz $|X| = n$, wyznacza dokładnie jeden k-elementowy podzbiór $f(A)$ n-elementowego zbioru X. Liczba wszystkich takich funkcji jest równa $n^{\underline{k}}$.**

Ale jednocześnie dla $f \in Fun(A, X)$ oraz dowolnej permutacji π zbioru A również funkcja $f\pi \in Fun(A, X)$ wyznacza ten sam podzbiór.

Oznacza to, że liczba wszystkich różnych podzbiorów k-elementowych zbioru n-elementowego jest dokładnie $k!$ razy mniejsza niż liczba injekcji w zbiorze $Fun(A, X)$, to znaczy jest równa $\frac{n^{\underline{k}}}{k!}$.

Pozostałe zależności otrzymuje się w wyniku prostych przekształceń algebraicznych. $\square$

Współczynniki dwumianowe – tożsamości

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

$$\sum_{i=0}^{n} i \cdot \binom{n}{i} = n \cdot 2^{n-1}$$

$$\binom{m+n}{k} = \sum_{s=0}^{k} \binom{m}{s} \cdot \binom{n}{k-s}$$

Trójkąt Pascala

$$\binom{n}{k}$$

	$k=0$	1	2	3	4	5	6	7	8	9	10	11	12	…
$n=0$	1	0	0	0	0	0	0	0	0	0	0	0	0	
1	1	1	0	0	0	0	0	0	0	0	0	0	0	
2	1	2	1	0	0	0	0	0	0	0	0	0	0	
3	1	3	3	1	0	0	0	0	0	0	0	0	0	
4	1	4	6	4	1	0	0	0	0	0	0	0	0	
5	1	5	10	10	5	1	0	0	0	0	0	0	0	
6	1	6	15	20	15	6	1	0	0	0	0	0	0	
7	1	7	21	35	35	21	7	1	0	0	0	0	0	
8	1	8	28	56	70	56	28	8	1	0	0	0	0	
9	1	9	36	84	126	126	84	36	9	1	0	0	0	
10	1	10	45	120	210	252	210	120	45	10	1	0	0	
11	1	11	55	165	330	462	462	330	165	55	11	1	0	
12	1	12	66	220	495	792	924	792	495	220	66	12	1	
…														…

Współczynniki wielomianowe

Ile jest wszystkich funkcji $f \in Fun(X, Y)$, gdzie $|X| = n$, $Y = \{1, \ldots, m\}$, dla których $|f^{-1}(\{i\})| = k_i$, $i = 1, \ldots, m$?

Liczbę takich funkcji oznaczamy symbolem

$$\binom{n}{k_1\ k_2 \ldots k_m}$$

i nazywamy współczynnikiem wielomianowym.

Symbol n w tym zapisie nazywamy indeksem górnym, natomiast symbole $k_1, \ldots, k_m$ – indeksami dolnymi.

Twierdzenie

Dla $n \in \mathbb{N}$ **oraz liczb naturalnych** $k_1,\ k_2, \ldots, k_m$**, spełniających warunek** $k_1 + k_2 + \ldots + k_m = n$**, zachodzi równość**

$$\binom{n}{k_1\ k_2 \ldots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_m!}\ .$$

Dla $m = 2$ **oraz** $k_1 = k$ **i** $k_2 = n - k$**, gdzie** $k, n \in \mathbb{N}$**,** $k \leqslant n$**, mamy:**

$$\binom{n}{k \quad n-k} = \frac{n!}{k!\,(n-k)!} = \binom{n}{k} = \binom{n}{n-k \quad k}.$$

Przykład Sekwencjonowanie RNA

Interesuje nas struktura fragmentu łańcucha RNA, o którym wiemy, że składa się z dziesięciu nukleotydów. Wiemy ponadto, że w łańcuchu występuje czterokrotnie adenina (A), trzykrotnie guanina (G), dwukrotnie cytozyna (C) i jeden raz uracyl (U). Dodatkowo wiemy, że na początku łańcucha znajduje się guanina.

Chcemy policzyć, ile jest wszystkich różnych łańcuchów RNA zgodnych z taką analizą.

Mamy tutaj $m = |\{A, G, C, U\}| = 4$**,** $k_1 = 4,\ k_2 = 2,\ k_3 = 2,\ k_4 = 1$**,** $n = 9$**.**

Liczba wszystkich możliwych łańcuchów RNA, odpowiadających powyższym warunkom jest równa:

$$\binom{n}{k_1\ k_2\ k_3\ k_4} = \binom{9}{4\ 2\ 2\ 1} = \frac{9!}{4! \cdot 2! \cdot 2! \cdot 1!} = 3780\ .$$

Wzór wielomianowy

Twierdzenie

Dla $m, n \in \mathbb{N}$ **oraz** $x_1, \ldots, x_m \in \mathbb{R}$ **zachodzi następująca równość:**

$$(x_1 + \ldots + x_m)^n = \sum_{\substack{k_1, \ldots, k_m \in \mathbb{N} \\ k_1 + \ldots + k_m = n}} \binom{n}{k_1 \ldots k_m} \cdot x_1^{k_1} \cdot \ldots \cdot x_m^{k_m} .$$

Tożsamości dla współczynników wielomianowych

$$\sum_{\substack{k_1,\ldots,k_m \in \mathbb{N} \\ k_1+\ldots+k_m=n}} \binom{n}{k_1 \ldots k_m} = m^n$$

$$\binom{n}{k_1 \;\; k_2 \;\; k_3 \;\; \ldots \;\; k_m} = \binom{n-1}{k_1-1 \;\; k_2 \;\; k_3 \;\; \ldots \;\; k_m} + \binom{n-1}{k_1 \;\; k_2-1 \;\; k_3 \;\; \ldots \;\; k_m} + \ldots + \binom{n-1}{k_1 \;\; k_2 \;\; k_3 \;\; \ldots \;\; k_m-1}$$

Dla zbioru z powtórzeniami $Q = (X, (k_1, \ldots, k_n))$ stosujemy następujące oznaczenie:

$$Q = \langle k_1 * x_1, \ldots, k_n * x_n \rangle \ .$$

Liczność zbioru z powtórzeniami $Q = \langle k_1 * x_1, \ldots, k_n * x_n \rangle$ oznaczamy symbolem $|Q|$ i definiujemy jako sumę krotności wszystkich jego elementów, tzn.

$$|Q| = k_1 + \ldots + k_n.$$

Podzbiory zbioru z powtórzeniami

Zbiór z powtórzeniami $S = \langle m_1 * x_1, \ldots, m_n * x_n \rangle$ **jest podzbiorem zbioru z powtórzeniami** $Q = \langle k_1 * x_1, \ldots, k_n * x_n \rangle$ **wtedy i tylko wtedy, gdy**

$$0 \leqslant m_i \leqslant k_i \text{ dla każdego } i = 1, \ldots, n.$$

Dla zaznaczenia faktu, że S **jest podzbiorem zbioru z powtórzeniami** Q**, używamy zapisu:**

$$S \subseteq Q.$$

Rodzinę wszystkich podzbiorów zbioru z powtórzeniami Q oznaczamy symbolem

$$\mathcal{P}(Q).$$

Liczba wszystkich podzbiorów zbioru z powtórzeniami $Q = \langle k_1 * x_1, \ldots, k_n * x_n \rangle$ jest równa

$$|\mathcal{P}(Q)| = (1 + k_1) \cdot (1 + k_2) \cdot \ldots \cdot (1 + k_n).$$

Podzbiory k-elementowe zbioru z powtórzeniami

Twierdzenie

Liczba wszystkich k-elementowych podzbiorów zbioru z powtórzeniami $\langle k_1 * x_1, \ldots, k_n * x_n \rangle$, gdzie $k_i \geqslant k$ dla $i = 1, \ldots, n$, jest równa

$$\frac{n^{\overline{k}}}{k!} = \binom{n+k-1}{k}.$$

Przykład **Rozważmy liniowe równanie diofantyczne:**

$$x_1 + x_2 + \ldots + x_n = k. \qquad (*)$$

Chcemy wyznaczyć liczbę wszystkich nieujemnych rozwiązań równania (*), czyli liczbę wektorów $(x_1, \ldots, x_n) \in \mathbb{N}^n$, spełniających powyższą równość.

Każdy taki wektor $(x_1, \ldots, x_n) \in \mathbb{N}^n$ jednoznacznie odpowiada k-elementowemu podzbiorowi $\langle x_1{*}z_1, \ldots, x_n{*}z_n\rangle$ zbioru z powtórzeniami $Q = \langle k * z_1, \ldots, k * z_n\rangle$.

Liczba wszystkich nieujemnych całkowitoliczbowych rozwiązań równania (*) jest więc równa liczbie wszystkich k-elementowych podzbiorów zbioru Q, tzn. $\binom{n+k-1}{k}$.

PODZIAŁY ZBIORU NA BLOKI

X – **zbiór skończony**

k – **liczba naturalna**

Definicja

Podziałem zbioru skończonego X na k bloków nazywamy rodzinę zbiorów $\mathcal{A} = \{A_1, \ldots, A_k\}$, spełniającą następujące warunki:

(i) $A_i \neq \emptyset$ **dla** $1 \leqslant i \leqslant k$**;**

(ii) $A_1 \cup \ldots \cup A_k = X$**;**

(iii) $A_i \cap A_j = \emptyset$ **dla** $1 \leqslant i < j \leqslant k$**.**

Podzbiory $A_1, \ldots, A_k$, nazywamy blokami podziału $\mathcal{A}$.

Przykład

$$X = \{a, b, c, d\}, \quad k = 3$$

Istnieje dokładnie sześć podziałów zbioru X na trzy bloki:

$$\begin{aligned}
\mathcal{A}_1 &= \{\ \{a\}, \{b\}, \{c, d\}\ \},\\
\mathcal{A}_2 &= \{\ \{a\}, \{b, c\}, \{d\}\ \},\\
\mathcal{A}_3 &= \{\ \{a, b\}, \{c\}, \{d\}\ \},\\
\mathcal{A}_4 &= \{\ \{a, c\}, \{b\}, \{d\}\ \},\\
\mathcal{A}_5 &= \{\ \{a\}, \{b, d\}, \{c\}\ \},\\
\mathcal{A}_6 &= \{\ \{a, d\}, \{b\}, \{c\}\ \}.
\end{aligned}$$

Oznaczenia:

$\Pi_k(X)$ – zbiór wszystkich podziałów zbioru X na k bloków;
$\Pi(X)$ – zbiór wszystkich podziałów zbioru X.

$$\Pi(X) = \Pi_1(X) \cup \ldots \cup \Pi_n(X).$$

$$\left\{ {n \atop k} \right\} = |\Pi_k(X)|, \quad \text{gdzie } |X| = n.$$

Wielkości $\left\{ {n \atop k} \right\}$ noszą nazwę liczb Stirlinga drugiego rodzaju albo liczb podzbiorowych Stirlinga.

Liczby Stirlinga drugiego rodzaju

Przyjmiemy, że istnieje dokładnie jeden podział zbioru pustego na 0 **bloków, tzn.** $\left\{ {0 \atop 0} \right\} = 1$.

$$\left\{ {n \atop k} \right\} = 0 \quad \text{dla } k > n$$

$$\left\{ {n \atop n} \right\} = 1 \quad \text{dla } n \geqslant 0$$

$$\left\{ {n \atop 0} \right\} = 0 \quad \text{dla } n > 0$$

$$\left\{ {n \atop 1} \right\} = 1 \quad \text{dla } n > 0$$

Wyznaczanie liczby podziałów zbioru na bloki

Twierdzenie

Dla $n \in \mathbb{N}$ **oraz** $k \in \mathbb{N}$**, gdzie** $0 < k < n$**, zachodzi następująca równość:**

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}.$$

Liczby Bella

Liczności zbioru $|\Pi(X)|$, gdy $|X| = n$, $n \in \mathbb{N}$ nazywamy n-tą liczbą Bella i oznaczamy symbolem B_n.

Zachodzi następująca równość:

$$B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$$

	B_n	$\left\{ n \atop k \right\}$											
		$k=0$	1	2	3	4	5	6	7	8	9	10	...
$n=0$	**1**	1	0	0	0	0	0	0	0	0	0	0	
1	**1**	0	1	0	0	0	0	0	0	0	0	0	
2	**2**	0	1	1	0	0	0	0	0	0	0	0	
3	**5**	0	1	3	1	0	0	0	0	0	0	0	
4	**15**	0	1	7	6	1	0	0	0	0	0	0	
5	**52**	0	1	15	25	10	1	0	0	0	0	0	
6	**203**	0	1	31	90	65	15	1	0	0	0	0	
7	**877**	0	1	63	301	350	140	21	1	0	0	0	
8	**4140**	0	1	127	966	1701	1050	266	28	1	0	0	
9	**21147**	0	1	255	3025	7770	6951	2646	462	36	1	0	
10	**115975**	0	1	511	9330	34105	42525	22827	5880	750	45	1	
...	...												...

Tabela liczb Stirlinga drugiego rodzaju $\left\{ n \atop k \right\}$ i liczb Bella B_n dla $k, n = 0, 1, \ldots, 10$.

Wyznaczanie wszystkich podziałów zbioru na bloki

Załóżmy, że dla pewnego k, gdzie $1 \leqslant k < n$, mamy rodzinę zbiorów $\mathcal{A} = \{A_1, \ldots, A_l\}$, będącą podziałem zbioru $\{1, \ldots, k-1\}$ na bloki.

Wówczas następujące rodziny zbiorów są podziałami zbioru $\{1, \ldots, k\}$:

$\{A_1 \cup \{k\},\ A_2, \ldots, A_l\}$,

$\{A_1,\ A_2 \cup \{k\}, \ldots, A_l\}$,

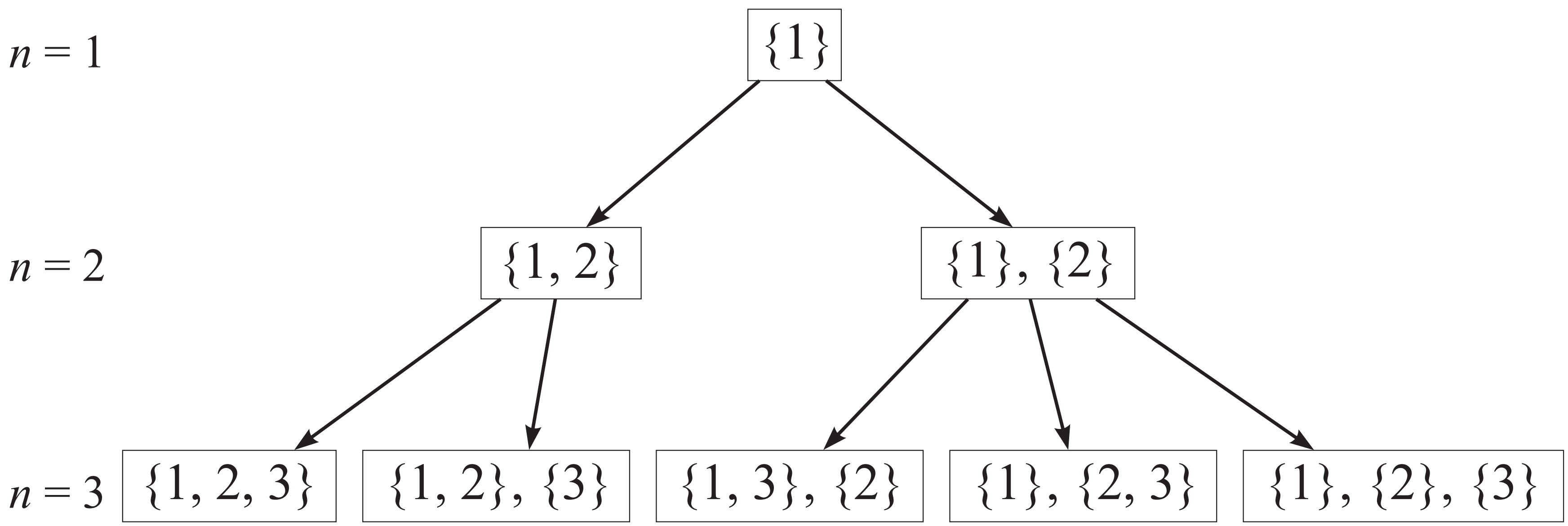
$\vdots$

$\{A_1,\ A_2, \ldots, A_l \cup \{k\}\}$,

$\{A_1,\ A_2, \ldots, A_l,\ \{k\}\ \}$.

Zaczynając od rodziny, która zawiera tylko jednoelementowy zbiór $\{1\}$, i powtarzając opisany wyżej krok procedury rekurencyjnej $n-1$ razy, otrzymamy drzewo, którego liście odpowiadają wszystkim możliwym podziałom zbioru $\{1, \ldots, n\}$.

Przykład **Drzewo podziałów zbioru $\{1, 2, 3\}$.**



Tożsamości dla liczb Stirlinga i liczb Bella

Dla $k, n, x \in \mathbb{N}$ zachodzą następujące równości:

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \cdot x^{\underline{n}} = \sum_{k=0}^{n} (-1)^{n-k} \cdot \left\{ {n \atop k} \right\} \cdot x^{\overline{n}}.$$

Dla $n \in \mathbb{N}$ zachodzi zależność:

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i.$$

Podziały zbiorów a relacje

Z dowolnynm podziałem $\mathcal{A}$ zbioru X na bloki można związać pewną relację, którą oznaczymy symbolem $R_{\mathcal{A}}$ i zdefiniujemy następująco:

$$R_{\mathcal{A}} = \bigcup_{A \in \mathcal{A}} A \times A.$$

Powyższy zapis oznacza, że dwa elementy x oraz y zbioru X są w relacji $R_{\mathcal{A}}$ wtedy i tylko wtedy, gdy należą do tego samego bloku podziału. Jeśli na przykład $X = \{a, b, c, d\}$ i $\mathcal{A} = \{\{a\}, \{b, d\}, \{c\}\}$, to:

$$R_{\mathcal{A}} = \{(a, a), (b, b), (b, d), (d, b), (d, d), (c, c)\}.$$

Podziały zbiorów a relacje

Z dowolnyn podziałem $\mathcal{A}$ zbioru X na bloki można związać pewną relację, którą oznaczymy symbolem $R_{\mathcal{A}}$ i zdefiniujemy następująco:

$$R_{\mathcal{A}} = \bigcup_{A \in \mathcal{A}} A \times A.$$

Dla dowolnego podziału $\mathcal{A}$ zbioru X relacja $R_{\mathcal{A}}$ jest symetryczna, zwrotna i przechodnia, a zatem jest relacją równoważności w zbiorze X.

Dowolnej relacji równoważności R w zbiorze X można przyporządkować jednoznacznie podział

$$\mathcal{A}_R = X/R$$

zbioru X na bloki, będący zbiorem wszystkich klas abstrakcji relacji równoważności R w X.

Przykład

Jeśli $X = \{x \in \mathbb{N} : \ x \leqslant 10\}$ i jako relację równoważności weźmiemy relację R zdefiniowaną następująco:

$$xRy \Leftrightarrow x \bmod 3 = y \bmod 3,$$

to otrzymamy podział $\mathcal{A}_R$ zbioru X na bloki, gdzie:

$$\mathcal{A}_R = X/R = \{\{0, 3, 6, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8\}\}.$$

Wniosek

Liczba wszystkich różnych relacji równoważności w zbiorze n-elementowym jest równa n-tej liczbie Bella B_n.

Zatem na przykład liczba wszystkich możliwych relacji równoważności, które można zdefiniować w zbiorze pięcioelementowym, jest równa 52.

Podziały zbioru na bloki i relacja rozdrobnienia

$\mathcal{A}$, $\mathcal{A}'$ – podziały zbioru X na bloki.

Podział $\mathcal{A}'$ zbioru X jest rozdrobnieniem podziału $\mathcal{A}$ wtedy i tylko wtedy, gdy każdy blok podziału $\mathcal{A}$ jest sumą pewnej liczby bloków podziału $\mathcal{A}'$.

Fakt ten zapisujemy następująco:

$$\mathcal{A}' \preceq \mathcal{A}$$

i mówimy, że podział $\mathcal{A}'$ jest w relacji rozdrobnienia z podziałem $\mathcal{A}$.

Przykład

Podział zbioru $X = \{x \in \mathbb{N} : \ x \leqslant 10\}$ na bloki

$$\mathcal{A}' = \{\{0,3\},\{6,9\},\{1,4,7\},\{10\},\{2,5,8\}\}$$

jest rozdrobnieniem podziału

$$\mathcal{A}_R = X/R = \{\{0,3,6,9\},\{1,4,7,10\},\{2,5,8\}\}.$$

Relacja rozdrobnienia $\preceq$ jest zwrotna, przechodnia i antysymetryczna, a zatem jest relacją częściowego porządku w zbiorze podziałów danego zbioru na bloki.

Podziały zbiorów a zliczanie surjekcji

Przykład

Mamy do dyspozycji m ponumerowanych procesorów i $n \geqslant m$ programów, z których każdy może być wykonany na dowolnym z tych procesorów. Chcemy przydzielić wszystkie programy do procesorów w taki sposób, by każdy procesor otrzymał co najmniej jeden program. (Zakładamy przy tym, że każdy program jest wykonywany w całości przez jeden procesor.) Należy policzyć, na ile sposobów można dokonać takiego przydziału.

Każdy przydział programów do procesorów może być opisany przez pewną funkcję z n-elementowego zbioru programów X w m-elementowy zbiór procesorów Y. Z warunku, że każdy procesor ma dostać do wykonania co najmniej jeden program wynika, że funkcja ta musi być surjekcją.

Zliczanie surjekcji

Niech X, Y będą dowolnymi zbiorami i niech $|X| = n$ oraz $|Y| = m$. Chcemy policzyć:

Ile jest wszystkich surjekcji w zbiorze $Fun(X, Y)$?

Liczbę wszystkich surjekcji w zbiorze $Fun(X, Y)$, gdzie $|X| = n$ oraz $|Y| = m$, będziemy oznaczać symbolem $s_{n,m}$, tzn.

$$s_{n,m} = |Sur(X, Y)| \quad \text{dla } |X| = n, \ |Y| = m.$$

Twierdzenie

Liczba $s_{n,m}$ surjekcji w zbiorze $Fun(X, Y)$, gdzie $|X| = n$, $|Y| = m$, spełnia zależność

$$s_{n,m} = m! \cdot \left\{ {n \atop m} \right\}.$$

Dowód **Jądro każdej surjekcji f ze zbioru $Fun(X, Y)$ wyznacza podział $N(f)$ zbioru X na m bloków:**

$$N(f) = \{f^{-1}(\{y\}) : \ y \in Y\}.$$

Dla dowolnej permutacji π zbioru Y jądra funkcji f i πf są identyczne, a zatem dokładnie $m!$ surjekcji ze zbioru $Fun(X, Y)$ ma to samo jądro $\mathcal{A} \in \Pi_m(X)$. Liczba wszystkich surjekcji w zbiorze $Fun(X, Y)$ jest więc $m!$ razy większa niż liczba wszystkich podziałów n-elementowego zbioru X na m bloków. $\square$

PODZIAŁY LICZBY

n, k – **liczby naturalne**

Definicja

Podziałem liczby n **na** k **składników nazywamy ciąg liczb naturalnych** $(a_1, \dots, a_k)$**, spełniający warunki**

$$a_1 + \ldots + a_k = n \quad \text{oraz} \quad a_1 \geqslant \ldots \geqslant a_k > 0.$$

Liczbę wszystkich podziałów liczby $n \in \mathbb{N}$ **na** $k \in \mathbb{N}$ **składników oznaczamy symbolem**

$$P(n, k),$$

a liczbę wszystkich podziałów liczby n **– symbolem**

$$P(n).$$

Podziały liczby na składniki

Zachodzi zależność:

$$P(n) = \sum_{k=1}^{n} P(n,k)$$

Przyjmiemy, że $P(0,0) = P(0) = 1$**.**

Dla n, $t \in \mathbb{N}$**, liczność zbioru wszystkich podziałów** $(a_1, \ldots, a_k)$ **liczby** n**, dla których spełniony jest warunek**

$$a_i \leqslant t, \quad i = 1, \ldots, k,$$

będziemy oznaczać symbolem $P_t(n)$**.**

Twierdzenie

Dla $n, k \in \mathbb{N}$**, gdzie** $n \geqslant k > 0$**, zachodzi zależność**

$$P(n,k) = P(n-1,k-1) + P(n-k,k)$$

Twierdzenie powyższe pozwala na rekurencyjne obliczanie wartości $P(n,k)$ **dla dowolnych parametrów** $n \geqslant k > 0$**, korzystając z faktu, że**

$$P(0,k) = P(k,0) = \lfloor k = 0 \rceil.$$

	$P(n)$	$P(n, k)$													
		$k = 0$	1	2	3	4	5	6	7	8	9	10	11	12	...
$n = 0$	**1**	1	0	0	0	0	0	0	0	0	0	0	0	0	
1	**1**	0	1	0	0	0	0	0	0	0	0	0	0	0	
2	**2**	0	1	1	0	0	0	0	0	0	0	0	0	0	
3	**3**	0	1	1	1	0	0	0	0	0	0	0	0	0	
4	**5**	0	1	2	1	1	0	0	0	0	0	0	0	0	
5	**7**	0	1	2	2	1	1	0	0	0	0	0	0	0	
6	**11**	0	1	3	3	2	1	1	0	0	0	0	0	0	
7	**15**	0	1	3	4	3	2	1	1	0	0	0	0	0	
8	**22**	0	1	4	5	5	3	2	1	1	0	0	0	0	
9	**30**	0	1	4	7	6	5	3	2	1	1	0	0	0	
10	**42**	0	1	5	8	9	7	5	3	2	1	1	0	0	
11	**56**	0	1	5	10	11	10	7	5	3	2	1	1	0	
12	**77**	0	1	6	12	15	13	11	7	5	3	2	1	1	
...	...														...

Liczność podziałów liczby naturalnej n na składniki dla $n, k = 0, \ldots, 12$.

Diagramy Ferrersa i podziały sprzężone

$$10 = 5 + 3 + 2 \qquad\qquad 10 = 3 + 3 + 2 + 1 + 1$$