Matematyka Dyskretna

Wykład 5
Metody zliczania

Wojciech Kordecki
wojciech.kordecki@collegiumwitelona.pl

Collegium Witelona
Wydział Nauk Technicznych i Ekonomicznych
Zakład Informatyki

Semestr letni 2023/24

Funkcja jako relacja

Funkcja

$$f : X \to Y$$

to relacja

$$\mathcal{R} \subseteq X \times Y$$

taka, że dla każdego $x \in X$ istnieje dokładnie jedna para

$$(x, y)\,,\ y = f\,(x)\,.$$

Zbiór X nazywamy dziedziną funkcji, a zbiór Y przeciwdziedziną funkcji.

Obraz i przeciwobraz

Obraz zbioru A to zbiór wszystkich wartości należących do przeciwdziedziny przyjmowanych przez funkcję dla każdego elementu danego podzbioru tej dziedziny, to znaczy

$$f(A) = \{y \in Y : \bigvee_{x \in A} y = f(x)\}.$$

Obraz i przeciwobraz

Obraz zbioru A to zbiór wszystkich wartości należących do przeciwdziedziny przyjmowanych przez funkcję dla każdego elementu danego podzbioru tej dziedziny, to znaczy

$$f(A) = \{y \in Y : \bigvee_{x \in A} y = f(x)\}.$$

Przeciwobraz zbioru B to zbiór wszystkich elementów dziedziny, które są odwzorowane na elementy danego zbioru, to znaczy

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

Klasyfikacja funkcji

Funkcja $f : X \to Y$ jest „na” (jest surjekcją), jeśli $f(X) = Y$.

Klasyfikacja funkcji

Funkcja $f : X \to Y$ jest „na” (jest surjekcją), jeśli $f(X) = Y$.

Funkcja $f : X \to Y$ jest *różnowartościowa* (jest wzajemnie jednoznaczna, jest iniekcją), jeśli

$$\bigwedge_{a,b \in X} a \neq b \Rightarrow f(a) \neq f(b).$$

Klasyfikacja funkcji

Funkcja $f : X \to Y$ jest „na” (jest surjekcją), jeśli $f(X) = Y$.

Funkcja $f : X \to Y$ jest *różnowartościowa* (jest wzajemnie jednoznaczna, jest iniekcją), jeśli

$$\bigwedge_{a,b \in X} a \neq b \Rightarrow f(a) \neq f(b).$$

Funkcja $f : X \to Y$ jest *bijekcją*, jeśli jest różnowartościowa i „na”.

Na ile sposobów?

Na ile sposobów można rozmieścić pewną liczbę obiektów w określonej liczbie pudełek, tak aby spełnione były zadane dodatkowe warunki?

Na ile sposobów?

Na ile sposobów można rozmieścić pewną liczbę obiektów w określonej liczbie pudełek, tak aby spełnione były zadane dodatkowe warunki?

Formalny opis tego problemu to klasyczne zadanie kombinatoryki, które brzmi: dane są dwa zbiory skończone X oraz Y o mocach, czyli liczbach elementów odpowiednio: $|X| = m$ i $|Y| = n$.

Ile jest funkcji $f : X \to Y$ spełniających zadane ograniczenia?

Interpretacje

1. X – zbiór obiektów, Y – zbiór pudełek; funkcja $f : X \to Y$ określa pewne rozmieszczenie obiektów w pudełkach przez wskazanie dla każdego obiektu $x \in X$ pudełka $f(x) \in Y$, w którym jest umieszczony;
2. X – zbiór obiektów, Y – zbiór kolorów; funkcja $f : X \to Y$ określa sposób kolorowania obiektów przez podanie dla każdego obiektu $x \in X$ koloru $f(x) \in Y$.

Interpretacje

1. X – zbiór obiektów, Y – zbiór pudełek; funkcja $f : X \to Y$ określa pewne rozmieszczenie obiektów w pudełkach przez wskazanie dla każdego obiektu $x \in X$ pudełka $f(x) \in Y$, w którym jest umieszczony;
2. X – zbiór obiektów, Y – zbiór kolorów; funkcja $f : X \to Y$ określa sposób kolorowania obiektów przez podanie dla każdego obiektu $x \in X$ koloru $f(x) \in Y$.

Niech $X = \{1, 2, \ldots, m\}$ i $Y = \{1, 2, \ldots, n\}$. W najprostszej sytuacji nie nakładamy żadnych dodatkowych warunków, rozmieszczenie obiektów w pudełkach może być opisane funkcją ze zbioru wszystkich funkcji z X w Y.

Zbiory w pudełkach

Zbiory w pudełkach

Twierdzenie

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

Zbiory w pudełkach

Twierdzenie

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

Dowód

Oznaczmy $X = \{1, 2, \ldots, m\}$*. Funkcje* $f : X \to Y$ *są ciągami długości* m *o wyrazach ze zbioru* Y*. Każdy wyraz można wybrać na* n *sposobów, wszystkich ciągów jest więc* n^m.

Zbiory w pudełkach c.d.

Co najwyżej jeden element w pudełku.

Twierdzenie

Jeśli $|X| = m$ *oraz* $|Y| = n$, *to liczba funkcji różnowartościowych* $f : X \to Y$ *jest dla* $m \leq n$ *równa* $\frac{n!}{(n-m)!}$

Zbiory w pudełkach c.d.

Co najwyżej jeden element w pudełku.

Twierdzenie

Jeśli $|X| = m$ *oraz* $|Y| = n$*, to liczba funkcji różnowartościowych* $f : X \to Y$ *jest dla* $m \leq n$ *równa* $\frac{n!}{(n-m)!}$

Dowód

Niech $X = \{1, 2, \ldots, m\}$ *oraz* $m \leq n$*. Pierwszy wyraz ciągu można wybrać na* n *sposobów, drugi na* $n - 1$*, a ogólnie* i*-ty wyraz można wybrać na* $m - (i - 1) = m - i + 1$ *sposobów, co dowodzi twierdzenia dla* $m \leq n$*.*
Dla $m > n$ *nie ma funkcji* $f : X \to Y$ *różnowartościowych.*

Liczba funkcji różnowartościowych

Twierdzenie

Jeśli $|X| = m$ *oraz* $|Y| = n$*, to liczba funkcji różnowartościowych* $f : X \to Y$ *jest dla* $m \leq n$ *równa* $\frac{n!}{(n-m)!}$.

Dowód

Niech $X = \{1, 2, \ldots, m\}$ *oraz* $m \leq n$*. Pierwszy wyraz ciągu można wybrać na* n *sposobów, drugi na* $n-1$*, a ogólnie* i*-ty wyraz można wybrać na* $m-(i-1) = m-i+1$ *sposobów, co dowodzi twierdzenia dla* $m \leq n$*. Dla* $m > n$ *nie ma funkcji* $f : X \to Y$ *różnowartościowych.*

Powyższe twierdzenie opisuje zadanie znalezienia liczby rozmieszczeń m elementów w n pudełkach, gdy w każdym pudełku można umieścić co najwyżej jeden element.

Rozmieszczenia ciągów w pudełkach

Zagadnieniem podobnym jest rozmieszczenie m elementów w n pudełkach, przy czym każde pudełko zawiera ciąg elementów (pudełka mogą być też puste). Dwa rozmieszczenia są identyczne, gdy te same pudełka mają te same ciągi elementów. Rozmieszczenia tego typu nazywa się rozmieszczeniami uporządkowanymi m elementów w n pudełkach.

Rozmieszczenia ciągów w pudełkach c.d.

Twierdzenie

Liczba rozmieszczeń uporządkowanych m elementów w n pudełkach jest równa $\frac{(n+m-1)!}{(n-1)!}$.

Rozmieszczenia ciągów w pudełkach c.d.

Twierdzenie

Liczba rozmieszczeń uporządkowanych m elementów w n pudełkach jest równa $\frac{(n+m-1)!}{(n-1)!}$.

Zamiast dowodu – przykład.

Przykład

$m = 3$ (elementy x, y, z), $n = 2$ (pudełka A i B),
$\frac{(n+m-1)!}{(n-1)!} = \frac{4!}{1!} = 24.$

A	B
xy	z
yx	z
xz	y
zx	y
yz	x
zy	x
z	xy
z	yx
y	xz
y	zx
x	yz
x	zy

A	B
xyz	
xzy	
yxz	
yzx	
zxy	
zyx	
	xyz
	xzy
	yxz
	yzx
	zxy
	zyx

Permutacje ponownie

Jeśli $m = n$, to każda funkcja różnowartościowa $f : X \to Y$ jest wzajemnie jednoznacznym odwzorowaniem zbioru X na zbiór Y.

Permutacje ponownie

Jeśli $m = n$, to każda funkcja różnowartościowa $f : X \to Y$ jest wzajemnie jednoznacznym odwzorowaniem zbioru X na zbiór Y.

Jest permutacją zbioru X.
Oczywiście liczba tych funkcji jest równa $n!$.

Przykład. Cztery elementy, cztery pudełka:

$$\begin{array}{lcc} \text{numer elementu} & \to & \multirow{2}{*}{$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$} \\ \text{numer pudełka} & \to & \end{array}$$

Permutacje ponownie

Jeśli $m = n$, to każda funkcja różnowartościowa $f : X \to Y$ jest wzajemnie jednoznacznym odwzorowaniem zbioru X na zbiór Y.

Jest permutacją zbioru X.
Oczywiście liczba tych funkcji jest równa $n!$.

Przykład. Cztery elementy, cztery pudełka:

$$\begin{array}{lcc} \text{numer elementu} & \rightarrow & \multirow{2}{*}{$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$} \\ \text{numer pudełka} & \rightarrow & \end{array}$$

$$f(1) = 2, \; f(2) = 1, \; f(3), = 4 \; f(4) = 3.$$

– bijekcja.

Złożenie permutacji

Złożeniem permutacji f oraz g nazywamy permutację $f \circ g$ taką, że $(f \circ g)(i) = f(g(i))$.
Jest to superpozycja funkcji, gdzie g jest funkcją wewnętrzną.

Złożenie permutacji

Złożeniem permutacji f oraz g nazywamy permutację $f \circ g$ taką, że $(f \circ g)(i) = f(g(i))$.
Jest to superpozycja funkcji, gdzie g jest funkcją wewnętrzną.

Prosty przykład: niech $X = \{1, 2, 3\}$ oraz $f_1 = (1, 3, 2)$, $f_2 = (3, 2, 1)$. Wtedy $f_1 \circ f_2 = (2, 3, 1)$.

Przykład złożenia permutacji

Niech:

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

Wtedy złożenie permutacji f oraz g to:

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

Permutacja identycznościowa i odwrotna

Permutacja identycznościowa I:

$$f \circ I = I \circ f = f,$$

czyli

$$I : \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Permutacja identycznościowa i odwrotna

Permutacja identycznościowa I:

$$f \circ I = I \circ f = f,$$

czyli

$$I : \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Permutacja f^{-1} odwrotna do f:

$$f^{-1} \circ f = I.$$

Permutacja identycznościowa i odwrotna

Permutacja identycznościowa I:

$$f \circ I = I \circ f = f,$$

czyli

$$I : \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Permutacja f^{-1} odwrotna do f:

$$f^{-1} \circ f = I.$$

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

Permutacja odwrotna f^{-1} – przykład

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

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

Złożenie:

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

Grupa (1)

Grupa:

$$G = (E, \circ),$$

gdzie E jest zbiorem elementów, a $\circ$ jest działaniem grupowym:

1. $\bigwedge_{a,b,c \in E} (a \circ b) \circ c = a \circ (b \circ c)$ – działanie jest łączne,
2. $\bigvee_{e \in E} \bigwedge_{a \in E} e \circ a = a \circ e = a$ – istnieje element neutralny e,
3. $\bigwedge_{a \in E} \bigvee_{b \in E} a \circ b = e$.

Działanie $\circ$ jest zwykle oznaczane jako $\cdot$ (notacja multiplikatywna i wtedy może być pominięte) lub jako $+$ (notacja addytywna).

Grupa (2)

Element neutralny w notacji addytywnej oznaczany jest zwykle jako 0 lub $\mathbb{0}$, a w notacji multiplikatywnej jako 1 lub $\mathbb{1}$. Element b określony w punkcie 3 jest elementem przeciwnym w notacji addytywnej i oznaczany jest jako $-a$, a w notacji multiplikatywnej jest elementem odwrotnym i oznaczany jest jako a^{-1}.

$$a + (-a) = a - a = \mathbb{0},$$
$$a \cdot a^{-1} = aa^{-1} = \mathbb{1}.$$

Definicja

Grupa G jest przemienna lub abelowa (od nazwiska: Niels Abel), gdy

$$\bigwedge_{a,b \in G} a + b = b + a.$$

Grupa permutacji (1)

Niech S_n oznacza zbiór permutacji na elementach wraz działaniem $\circ$.

Grupa permutacji (1)

Niech S_n oznacza zbiór permutacji na elementach wraz działaniem $\circ$.

S_n jest *grupą permutacji*.

Grupa permutacji (1)

Niech S_n oznacza zbiór permutacji na elementach wraz działaniem $\circ$.

S_n jest *grupą permutacji*.

Obszerne informacje o teorii grup i grupach permutacji można znaleźć w książce [RR], pkt. 6.4 i 6.5.

Grupa permutacji (2)

Grupy permutacji okazały się szczególnie ważne przy badaniu rozwiązywalności równań algebraicznych.
M. Rejewski, J. Różycki i H. Zygalski wykorzystali teorię permutacji do złamania szyfru Enigmy (1932).
Ich badania kontynuowała grupa kryptologów brytyjskich z istotnym udziałem A. Turinga w Bletchley Park.

Ciekawa książka o Enigmie: M. Grajek. *Enigma. Bliżej prawdy*. Rebis 2007.

W 2014 roku Morten Tyldum nakręcił film o pracy Turinga nad łamaniem kodu Enigmy, „Gra tajemnic". Film utworzył na podstawie adaptacji biografii Andrewa Hodgesa: „Alan Turing. Enigma".

Grupa permutacji (3)

Grupa permutacji nie jest przemienna.
Niech:

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

Wtedy:

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

Grupa permutacji (3)

Grupa permutacji nie jest przemienna.
Niech:

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

Wtedy:

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

$$f \circ g \neq g \circ f.$$

Podział zbioru

Niech $f : X \to X$ będzie permutacją zbioru X.
Podział zbioru X na rozłączne części $X_1, X_2, \ldots, X_k$

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

taki, że w każdym zbiorze X_j, $x \in X_j \implies f(x) \in X_j$. Żadnego z X_j nie można już podzielić na dwie niepuste części o powyższej własności. Wtedy X można uporządkować w taki sposób, że każdy X_j składa się z kolejnych elementów, $X_j = \{x_{j_1}, \ldots, x_{j_{m_j}}\}$ oraz

$$f(x_{j_1}) = x_{j_2}, f(x_{j_2}) = x_{j_3}, \ldots, f\left(x_{j_{m_j-1}}\right)$$
$$= x_{j+m_j}, f(x_{j+m_j}) = x_{j_1} .$$

Podział zbioru c.d.

Funkcja f ograniczona do zbioru X_j też jest permutacją.
Podział zbioru X na rozłączne części $X_1, X_2, \ldots, X_k$, to znaczy:

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

taki, że w każdym zbiorze X_j, $x \in X_j \implies f(x) \in X_j$. Żadnego z X_j nie można już podzielić na dwie niepuste części o powyższej własności. Wtedy X można uporządkować w taki sposób, że każdy X_j składa się z kolejnych elementów, $X_j = \{x_{j_1}, \ldots, x_{j_{m_j}}\}$ oraz

$$f\left(x_{j_1}\right) = x_{j_2}, f\left(x_{j_2}\right) = x_{j_3}, \ldots, f\left(x_{j_{m_j-1}}\right) = x_{j+m_j}, f\left(x_{j+m_j}\right) = x_{j_1}.$$

Oczywiście funkcja f ograniczona do zbioru X_j też jest permutacją.

Cykle

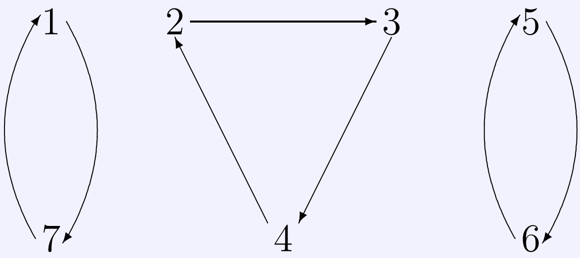
Każdy taki podzbiór (uporządkowany) $X_j \subseteq X$ nazywa się cyklem, a przedstawienie X w postaci sumy cykli nazywa się *rozkładem permutacji na cykle*.
Moc zbioru X_j nazywa się *długością* cyklu X_j.
Rozkład permutacji $(x_1, x_2, \dots, x_n)$ na cykle oznacza się:

$$[x_1, \dots, x_{m_1}]\,[x_{m_1+1}, \dots, x_{m_1+m_2}] \dots [x_{n-m_k}, \dots, x_n]\,,$$

gdzie m_j jest długością j-tego cyklu.

Cykle – rysunek

Rozkład permutacji $(7, 3, 4, 2, 6, 5, 1)$ na cykle $[1, 7][2, 3, 4][5, 6]$.



Definicja rekurencyjna

Liczby Stirlinga pierwszego rodzaju $s_{n,k}$ (lub $s(n,k)$):

$$s(n,k) = s(n-1,k-1) - (n-1)\,s(n-1,k)$$

dla $0 < k < n$ oraz $s(n,n) = 1$ dla $n \geq 0$ i $s(n,0) = 0$ dla $n > 0$.

Cykliczne liczby Stirlinga

Stirlinga pierwszego rodzaju $s\left(n,k\right)$ mogą być ujemne. Z tego powodu dodatkowo rozważa się ich wartość bezwzględną. Takie liczby nazywane są nieoznakowanymi liczbami Stirlinga pierwszego rodzaju i oznaczane $c\left(n,k\right)$ lub częściej cyklicznymi liczbami Stirlinga oznaczanymi $\left[{n \atop k}\right]$, to znaczy:

$$\left|s\left(n,k\right)\right| = c\left(n,k\right) = \left[{n \atop k}\right].$$

Liczbt Stirlinga a cykle

Twierdzenie

Wartość bezwzględna liczby Stirlinga pierwszego rodzaju $|s(n,k)| = \left[{n \atop k}\right]$ *jest równa liczbie permutacji zbioru n-elementowego, która ma rozkład na k cykli.*

Liczbt Stirlinga a cykle

Twierdzenie

Wartość bezwzględna liczby Stirlinga pierwszego rodzaju $|s(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}$ *jest równa liczbie permutacji zbioru n-elementowego, która ma rozkład na k cykli.*

Cykliczna liczba Stirlinga oznacza więc liczbę sposobów na rozmieszczenie n obiektów w k cyklach.

Inna definicja

Cykliczne liczby Stirlinga definiuje się też równoważnym wzorem rekurencyjnym:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}.$$

Własności (1)

Twierdzenie

Dla dowolnych k, n prawdziwe są własności:

- $\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!,$
- $\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2},$
- $\begin{bmatrix} n \\ k \end{bmatrix} = 0 \text{ dla } k > n.$

Własności (2)

Twierdzenie

Dla dowolnych $n \geq 0$ i $k \geq 0$:

$$\begin{bmatrix} n \\ k \end{bmatrix} = (-1)^{n+k} \, s\,(n, k)\,.$$

Zachodzi też związek:

$$s\,(n, k) = (-1)^{n+k} \begin{bmatrix} n \\ k \end{bmatrix} = (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}.$$

Liczby Stirlinga a liczby harmoniczne

Związek cyklicznych liczb Stirlinga z liczbami harmonicznymi

$$H_n = \sum_{k=1}^{n} \frac{1}{n} \, .$$

Liczby Stirlinga a liczby harmoniczne

Związek cyklicznych liczb Stirlinga z liczbami harmonicznymi

$$H_n = \sum_{k=1}^{n} \frac{1}{n} .$$

Twierdzenie

Dla $n \geq 1$ zachodzi:

$$\sum_{k=0}^{n} k \begin{bmatrix} n \\ k \end{bmatrix} = n! H_n ,$$

gdzie H_n jest n-tą liczbą harmoniczną.