

# Matematyka dyskretna

Andrzej M. Borzyszkowski

Instytut Informatyki  
Uniwersytet Gdański

sem. zimowy 2025/26

inf.ug.edu.pl/~amb/MaD

Andrzej M. Borzyszkowski (Instytut Informatyki) Matematyka dyskretna sem. zimowy 2025/26 1 / 21

Zasady zliczania Sumy

## Zasady zliczania – sumy

- jeśli  $A \cap B = \emptyset$  to  $|A \cup B| = |A| + |B|$   
dw.: jeśli  $|A| = n$ ,  $|B| = m$ , to bijekcję  $f : n \rightarrow A$  przedłużamy wzorem  $f(i) = g(i - n)$  gdzie  $g : m \rightarrow B$
- jeśli zbiory  $A_1, \dots, A_n$  są parami rozłączne, to  $|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$
- $|A \cup B| = |A| + |B| - |A \cap B|$   
dw.:  $|A| = |A \setminus B| + |A \cap B|$ , podobnie dla  $B$ ,  
 $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B|$   
elementy z przekroju liczone są podwójnie
- dla trzech zbiorów  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$
- czyli odejmujemy elementy liczone podwójnie, ale elementy liczone potrójnie zostały trzy razy odliczone, więc trzeba dodać te elementy

Andrzej M. Borzyszkowski (Instytut Informatyki) Matematyka dyskretna sem. zimowy 2025/26 3 / 21

# Zasady zliczania

Andrzej M. Borzyszkowski (Instytut Informatyki) Matematyka dyskretna sem. zimowy 2025/26 2 / 21

Zasady zliczania Zasada włączania i wyłączania

## Zasada włączania i wyłączania

- $|\bigcup_{j=1}^n A_j| = \sum_{J \subseteq \{1, \dots, n\}, J \neq \emptyset} (-1)^{|J|-1} |\bigcap_{j \in J} A_j|$
- dw.: dla  $n = 1$  jest tylko jeden zbiór i oczywista równość  $|A_1| = |A_1|$   
dla  $n = 2$  sprawdziliśmy wcześniej  
krok indukcyjny: dodajemy zbiór  $A_{n+1}$  do rodziny  $\{A_1, \dots, A_n\}$   

$$|\bigcup_{j=1}^n A_j \cup A_{n+1}| =$$

$$|\bigcup_{j=1}^n A_j| + |A_{n+1}| - |(\bigcup_{j=1}^n A_j) \cap A_{n+1}| =$$

$$\sum_{J \subseteq \{1, \dots, n\}, J \neq \emptyset} (-1)^{|J|-1} |\bigcap_{j \in J} A_j| + |A_{n+1}| -$$

$$- \sum_{J \subseteq \{1, \dots, n\}, J \neq \emptyset} (-1)^{|J|-1} |\bigcap_{j \in J} A_j \cap A_{n+1}| =$$

$$\sum_{I \subseteq \{1, \dots, n+1\}, I \neq \emptyset} (-1)^{|I|-1} |\bigcap_{i \in I} A_i|$$
- zbiory indeksów  $J \subseteq \{1, \dots, n+1\}$ ,  $J \neq \emptyset$  albo zawierają  $n+1$  i wówczas odnoszą się do przekrojów z  $A_{n+1}$  albo nie zawierają i wówczas odnoszą się do  $\bigcup_{i=1}^n A_i$

Andrzej M. Borzyszkowski (Instytut Informatyki) Matematyka dyskretna sem. zimowy 2025/26 4 / 21

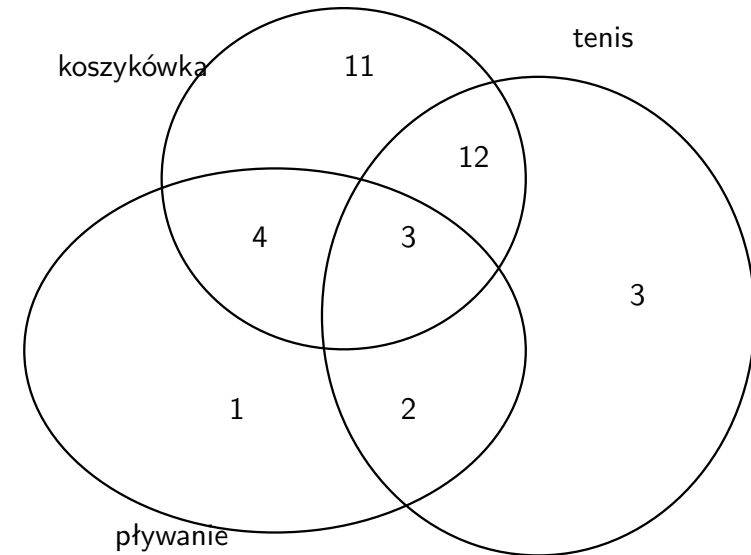
## Przykład liczbowy

- studenci zapisali się na zajęcia sportowe:
  - 30 na koszykówkę, 20 na tenisa, a 10 na pływanie
  - 15 studentów zapisało się na koszykówkę i tenisa
  - 7 na koszykówkę i pływanie
  - a 5 na tenisa i pływanie
  - 3 studentów zapisało się na wszystkie zajęcia sportowe
- pytanie: o ilu studentach jest mowa?
- odpowiedź:  $30+20+10-15-7-5+3=36$  studentów

## Przykład liczbowy inny

- hasło powinno składać się z 8 znaków alfanumerycznych i mieć co najmniej jedną literę dużą, małą i cyfrę
  - nieprawidłowe hasła to ciągi bez cyfr –  $52^8$ , bez małych liter –  $36^8$ , tyle samo bez dużych
  - trzeba odliczyć podwójne przekroje (potrójny jest pusty)
  - liczba haseł to  $62^8 - (52^8 + 36^8 + 36^8 - 26^8 - 26^8 - 10^8 + 0^8)$
  - czyli 159 655 911 367 680 zamiast 218 340 105 584 896
- żądanie konkretnej postaci haseł zmniejsza liczbę możliwych haseł o 27%.
- ale zwalcza pokusę stosowania haseł z małego słownika, dużo mniejszego niż 159 655 911 367 680.

## Przykład liczbowy, rysunek



## Zasady zliczania – iloczyn

- jeśli  $A$  i  $B$  są zbiorami skończonymi, to  $|A \times B| = |A| \cdot |B|$
- dw.: niech  $|A|=n$ ,  $|B|=m$ , istnieją bijekcje  $n \rightarrow A$ ,  $m \rightarrow B$  znajdujemy bijekcję  $n \times m \rightarrow n \cdot m$   
parze liczb  $(i, j)$ ,  $i < n$ ,  $j < m$  przypisujemy  $i \cdot m + j < n \cdot m$
- tablicę o dwóch indeksach umieszczamy w pamięci komputera: element  $(i, j)$  umieszczamy w miejscu  $i \cdot m + j + \text{adres początku}$
- w tej wersji konieczna jest znajomość rozmiaru względem  $j$  liczba  $i$  może pozostać nieokreślona i tablica może rosnąć
- przykład deklaracji w jęz. C

```
float tablica[][3]
```

nie jest określony jeden z rozmiarów tablicy, ale musi być określony drugi

## Iloczyny zbiorów nieskończonych

- jeśli choć jeden ze zbiorów  $A$  i  $B$  jest nieskończony i oba są niepuste, to ich iloczyn kartezjański też jest taki
- wzór  $f(i, j) = i \cdot m + j$ ,  $j < m$  jest dobry dla wszystkich  $i$  czyli określa bijekcję  $\mathbb{N} \times m \rightarrow \mathbb{N}$
- $f$  określona wzorem  $f(i, j) = i + \frac{1}{2} \cdot (i + j) \cdot (i + j + 1)$  jest bijekcją  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
- jednak język C nie dopuszcza deklaracji tablicy dwuwymiarowej bez określonych wymiarów

## Zasady zliczania – ciągi i funkcje

- dany zbiór  $A$
- ciągi długości 1 to elementy zbioru  $A$ , czyli  $A^1 = A$
- ciągi długości dwa to elementy iloczynu kartezjańskiego  $(a_1, a_2) \in A \times A$ ,  $A^2 = A \times A$  więc  $|A^2| = |A|^2$
- definiujemy  $A^{n+1} = A^n \times A$ , wówczas  $|A^{n+1}| = |A|^{n+1}$
- niech  $B = \{b_1, \dots, b_k\}$
- funkcja  $f : B \rightarrow A$  określa ciąg w  $A$  długości  $k$ :  $(f(b_1), \dots, f(b_k))$
- na odwrót, ciąg elementów z  $A$  długości  $k$  określa funkcję  $f : B \rightarrow A$  wzorem  $f(b_i) = a_i$
- wniosek:  $|B \rightarrow A| = |A|^{|B|}$
- uwaga: czasem zbiór funkcji  $B \rightarrow A$  zapisuje się jako  $A^B$
- ciągi długości zero to funkcja  $\emptyset : \emptyset \rightarrow A$ ,  $A^0 = \{()\}$ ,  $|A^0| = 1$ .

## Paradoks Hilberta

- hotel ma nieskończenie wiele pokoi, wszystkie są zajęte
- przybywa dodatkowy gość, co robić?  
odp.  $f(i) = i + 1$  określa sposób przesunięcia dotychczasowych gości i zwolnienia pokoju nr 0
- przybywa nieskończenie wiele nowych gości, co teraz?  
 $f(i) = 2 \cdot i$  daje sposób zwolnienia nieparzystych pokoi
- przybywa nieskończenie wiele autokarów, każdy z nieskończoną liczbą gości, jak ich rozmieścić?  
bijekcja  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  wskaże numer pokoju  $f(i, j)$  dla gościa z autokaru numer  $i$  zajmującego miejsce numer  $j$  (obecni goście hotelowi są traktowani jak autokar zerowy)
- do portu wpływa nieskończenie wiele promów, każdy ma nieskończenie wiele autokarów z nieskończoną liczbą gości itd. itp.

## Iloczyn kartezjański uogólniony

- dana rodzina zbiorów  $\{A_i\}_{i \in I}$   
iloczyn kartezjański (ozn.  $\times_{i \in I} A_i$  albo  $\prod_{i \in I} A_i$ )  
to zbiór funkcji  $f$  takich, że  $f(i) \in A_i$  dla  $i \in I$   
czyli zbiorów par  $f = \{(i, a_i) \mid i \in I, a_i \in A_i\}$
- $Atrybut = \{Imie, Nazwisko, Pesel, DataUr, Adres\}$
- $\Pi Atrybut = \{s \mid s(Imie) \in Imie, s(Nazwisko) \in Nazwisko, \dots\}$
- $Student \subseteq \Pi Atrybut$  jest zbiorem pewnych zestawów (krotek), których atrybuty mają sensowne wartości

Student.ods — LibreOffice Calc

|   | A         | B           | C           | D          | E                                |
|---|-----------|-------------|-------------|------------|----------------------------------|
|   | Imie      | Nazwisko    | Pesel       | DataUr     | Adres                            |
| 1 |           |             |             |            |                                  |
| 2 | Gerard    | Bazior      | 05251394633 | 13.05.2005 | 87-109 Kwidzyn Odrowskiego 3     |
| 3 | Jan       | Chodkiewicz | 05231854733 | 18.03.2005 | 81-737 Gdynia Chwarznieńska 33/5 |
| 4 | Agnieszka | Kolak       | 04230184784 | 1.03.2004  | 81-234 Kielno 4                  |
| 5 | Bernard   | Łukowski    | 05222829631 | 28.02.2005 | 81-620 Gdynia Górnicza 29        |
| 6 | Wojciech  | Miszke      | 06282009477 | 20.08.2006 | 81-831 Sopot Mazowiecka 73/44    |
| 7 | Marzena   | Songin      | 04311284947 | 12.11.2004 | 80-619 Gdańsk Focha 39-41 m.66   |
| 8 | Marcin    | Zaorski     | 04222938230 | 29.02.2004 | 89-534 Dziewięć Włók             |

## Iloczyn kartezjański uogólniony

- $|\prod_{i \in I} A_i| = \prod_{i \in I} |A_i|$  – moc iloczynu kartezjańskiego jest iloczynem mocy zbiorów
- tablica rejestracyjna ma dwie litery (z 26) i pięć cyfr, ile istnieje różnych tablic rejestracyjnych?
  - $26 \cdot 26 \cdot 10^5 = 67\,600\,000$
- a trzy litery i cztery cyfry?
  - $26^3 \cdot 10^4 = 175\,760\,000$
- a dwie litery, cztery cyfry i na końcu litera?
  - również  $26^3 \cdot 10^4 = 175\,760\,000$
- założmy  $|Imie| = 10^4$ ,  $|Nazwisko| = 10^7$ ,  $|Pesel| = 100 \cdot 365 \cdot 10^4$ ,  $|DataUr| = 100 \cdot 365$ ,  $|Adres| = 10^8$ 
  - wówczas  $|\prod A_{trybut}| = 1,33225 \cdot 10^{32} \approx 2^{106}$

## Funkcje charakterystyczne

- dw. 2: budujemy bijekcję pomiędzy  $\mathcal{P}(A)$  a  $A \rightarrow 2$
- każdy podzbiór  $B \in \mathcal{P}(A)$  definiuje funkcję  $\chi_B : A \rightarrow 2$  wzorem
 
$$\chi_B(x) = \begin{cases} 0 & x \notin B \\ 1 & x \in B \end{cases}$$
- każda funkcja  $f : A \rightarrow 2$  określa podzbiór  $\text{supp}(f) \in \mathcal{P}(A)$  wzorem  $\text{supp}(f) = \{x \in A \mid f(x)=1\}$  (nośnik funkcji)
- te definicje określają bijekcję, stąd  $|\mathcal{P}(A)| = |A \rightarrow 2| = 2^{|A|}$
- jeśli elementy z  $A$  ponumerujemy, to funkcja  $A \rightarrow 2$  jest ciągiem zer i jedynek długości  $|A|$  (mapa bitowa)
- np. zamiast  $\{2, 3, 7\} \subseteq \{1, \dots, 8\}$  można pisać 01100010  
 $\emptyset$  to 00000000, ciąg samych jedynek to cały zbiór  $\{1, \dots, 8\}$

## Zasady zliczania – zbiory potęgowe

- liczba podzbiorów zbioru  $n$ -elementowego  $A$  wynosi  $2^n$
- dw. 1: indukcja względem liczby elementów:
  - zbiór pusty ma  $2^0 = 1$  podzbiór –  $\mathcal{P}(\emptyset) = \{\emptyset\}$ ,  $|\mathcal{P}(\emptyset)| = 1$
  - jeśli do zbioru dodamy nowy element  $x$ , to liczba jego podzbiorów podwoi się –  
 każdy podzbiór  $B \in \mathcal{P}(A)$  określa dwa podzbiory  $B \in \mathcal{P}(A \cup \{x\})$  oraz  $B \cup \{x\} \in \mathcal{P}(A \cup \{x\})$
  - czyli  $|\mathcal{P}(A \cup \{x\})| = 2 \cdot |\mathcal{P}(A)| = 2 \cdot 2^{|A|} = 2^{|A|+1}$

## Zasady zliczania – ciągi bez powtórzeń

- niech  $|A| = n$ , liczba ciągów długości  $k$  to  $n^k$   
 $k$  krotnie wybieramy element z  $A$ , elementy te mogą się powtarzać
- w ciągu bez powtórzeń elementy *nie mogą* się powtarzać  
 pierwszy można wybrać na  $n$  sposobów  
 drugi już tylko na  $n - 1$  sposobów  
 jeśli  $k > n$  to nie da się wybrać  $n + 1$  nowego elementu
- jeśli  $k \leq n$  to liczba ciągów elementów z  $A$  bez powtórzeń wynosi  $n \cdot (n - 1) \cdot \dots \cdot (n - k + 1)$
- ciąg bez powtórzeń długości  $n$  jest bijekcją  $n \rightarrow A$   
 liczba tych bijekcji to  $n \cdot (n - 1) \cdot \dots \cdot 1 = n!$  (silnia)

$$n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n - k)!}$$

## Permutacje

- permutacja w zbiorze  $A = \{a_1, \dots, a_n\}$  – bijekcja zbioru  $A$  w siebie  
 $\pi : A \rightarrow A$
- określa ona ciąg elementów z  $A : (\pi(a_1), \dots, \pi(a_n))$   
jest to ciąg bez powtórzeń  
na odwrót, każdy ciąg bez powtórzeń  $(b_1, \dots, b_n)$  definiuje permutację  $\pi(a_i) = b_i$
- permutację może zapisać tablicą  $\begin{pmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{pmatrix}$
- funkcja  $id(a_i) = a_i$  dla  $i = 1, \dots, n$  jest też permutacją  
permutacje można składać  $(\sigma \circ \pi)(a) = \sigma(\pi(a))$   
dla każdej permutacji istnieje odwrotna  $\pi^{-1}(b_i) = a_i$  gdzie  $\pi(a_i) = b_i, i = 1, \dots, n$ 
  - zbiór permutacji stanowi *grupę*

## Permutacje c.d.

- liczba permutacji jest b. duża (wzór Strilinga)

$$n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \quad \pi \approx 3.14, \quad e \approx 2.71$$

- permutacja zbioru  $A$  rozkłada się na rozłączne cykle  
 $a \in A, a \mapsto \pi(a) \mapsto \pi^2(a) \mapsto \dots \mapsto \pi^\ell(a) = a$   
każdy z elementów  $\pi^i(a)$  ma własność  $\pi^\ell(\pi^i(a)) = \pi^i(a)$   
jeśli  $a' \in A$  nie występuje na powyższej liście, to ma swój własny cykl, rozłączny z powyższym, być może innej długości  
każdy element należy do jakiegoś cyklu długości  $\geq 1$
- np.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (12)(3)(456)$$

pojedynczą permutację zapisuje się w ten sposób wygodniej, złożenie wielu liczy się w sposób mniej oczywisty

## Permutacje, przykład

$$\begin{aligned} \sigma &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 0 & 5 & 2 \end{pmatrix} & \pi &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 & 0 \end{pmatrix} \\ \sigma^{-1} &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 0 & 1 & 4 \end{pmatrix} & \pi^{-1} &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 0 & 2 \end{pmatrix} \\ \pi \circ \sigma &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 0 & 5 \end{pmatrix} & \sigma \circ \pi &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 0 & 3 \end{pmatrix} \\ (\pi \circ \sigma)^{-1} &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 0 & 1 & 3 & 5 \end{pmatrix} & (\sigma \circ \pi)^{-1} &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 & 0 \end{pmatrix} \end{aligned}$$

- zachodzi równość  $(\sigma \circ \pi)^{-1} = \pi^{-1} \circ \sigma^{-1}$   
dw.: jeśli  $(\pi^{-1} \circ \sigma^{-1})(a) = b$ , to  $\pi^{-1}(\sigma^{-1}(a)) = b$   
czyli  $\sigma^{-1}(a) = \pi(b)$  i dalej  $a = \sigma(\pi(b)) = (\sigma \circ \pi)(b)$ , stąd  
 $(\sigma \circ \pi)^{-1}(a) = b$

## Zliczanie na dwa sposoby

- jeśli elementy zbioru dadzą się policzyć na dwa sposoby, to wynik musi być identyczny
- przykład: uczestnicy przyjęcia witają się ze sobą (niekoniecznie wszyscy), tych, którzy przywitali się z nieparzystą liczbą uczestników jest parzysta liczba
  - dw.: tworzymy graf – uczestnicy są wierzchołkami, przywitania krawędziami, liczymy liczbę krawędzi:  
 $\sum_u \text{witaj}(u)$  jest podwojoną liczbą krawędzi (każdą krawędź liczymy dwa razy)  
parzysta suma musi mieć parzystą liczbę nieparzystych składników

## Wielokrotne zliczanie tego samego elementu

- załóżmy, że  $\varphi : X \rightarrow Y$  ma tę własność, że wszystkie przeciwobrazy  $\varphi^{\leftarrow}(y) = \{x \in X \mid \varphi(x) = y\}$ ,  $y \in Y$  mają tyle samo  $\ell$  elementów, wówczas  $|Y| = \frac{|X|}{\ell}$
- dw.:  $X = \bigcup_{y \in Y} \{x \in X \mid \varphi(x) = y\} \quad |X| = |Y| \cdot \ell$

Już z tego korzystaliśmy:

- ciągi bez powtórzeń:  $X =$  zbiór permutacji zbioru  $A$ ,  
 $Y =$  zbiór ciągów bez powtórzeń długości  $k$ ,  
 $\varphi =$  obcięcie permutacji  $A$  do pierwszych  $k$  elementów  
 każdy ciąg liczony był  $(n - k)!$  razy permutując pozostałe elementy  
 liczba ciągów bez powtórzeń:  $\frac{n!}{(n-k)!}$