Matematyka dyskretna

© Andrzej Łachwa, UJ, 2017
andrzej.lachwa@uj.edu.pl

1/15

Literatura obowiązkowa

[1] K.A.Ross, Ch.R.B.Wright: *Matematyka Dyskretna.* Wydawnictwo Naukowe PWN, Warszawa 1996

[2] R.L.Graham, D.E.Knuth, O.Patashnik: *Matematyka Konkretna*. Wydawnictwo Naukowe PWN, Warszawa 1996

[3] R.J.Wilson: *Wprowadzenie do teorii grafów*. Wydawnictwo Naukowe PWN, Warszawa 1998

[4] *Wykłady z matematyki dyskretnej dla informatyków*
http://wazniak.mimuw.edu.pl/index.php?title=Matematyka_dyskretna_1

Inne źródła będą podawane w trakcie wykładów.

Ważne informacje

Konsultacje: czwartki 9-10, pok. C-2-25

Slajdy z wykładów będą udostępniane po kolejnych wykładach na stronie Zakładu PiGK w zakładce Dydaktyka/Materiały.

Uwaga: materiały te nie zastępują wykładów, nie zawierają wszystkich treści i wyjaśnień. Są tylko skrótem, który ma być dla Państwa pomocny w przygotowywaniu się do ćwiczeń i do egzaminu.

Warunki zaliczenia modułu

- zaliczenie ćwiczeń i zdanie egzaminu.

Egzamin:

- ***po uzyskaniu zaliczenia ćwiczeń***
- ***pisemny, w zakresie wiedzy teoretycznej i umiejętności rozwiązywania zadań***
- ***egzamin poprawkowy we wrześniu***

Kryteria oceny dla efektów kształcenia w module: oceny 3/4/5 odpowiadają wiedzy, umiejętnościom i kompetencjom na poziomie co najmniej 40% / 60% / 80%.

Czym będziemy się zajmować?

Czego się nauczymy?

Ile rozwiązań w dziedzinie liczb naturalnych ma równanie
$s_1 + s_2 + s_3 = 10$?

Mamy 7 klocków z napisami 1,2,2,4,4,4,7.
Ile różnych 7-cyfrowych liczb możemy ułożyć z tych klocków?

Ile jest różnych podziałów zbioru 11 elementowego na 10 bloków?

Na ile sposobów można wybrać 7 cukierków o trzech smakach?

Czego jest więcej: (a) rozmieszczeń uporządkowanych 3 elementów w 4 pudełkach czy (b) 4 elementów w 3 pudełkach?

Matematyka dyskretna łączy i wykorzystuje różne działy matematyki aby dostarczyć informatykom podstaw teoretycznych oraz metod niezbędnych do konstruowania i analizy algorytmów.

W programie studiów mamy ponadto logikę i teorię mnogości, analizę matematyczną, algebrę i geometrię, rachunek prawdopodobieństwa oraz inne przedmioty z elementami matematyki. Niektóre z treści opisanych w literaturze naszego przedmiotu są wprowadzane w ramach tamtych przedmiotów. Mimo tego, niektóre tematy są na tyle ważne, że będą omawiane także na naszych zajęciach.

zbiory i relacje

Zbiory

Gdy mówię o zbiorze monet w portmonetce, to najlepszą strukturą danych może okazać się torba, czyli zbiór z powtórzeniami.

G*dy myślę o czasie, jaki upłynie od teraz do końca dzisiejszego dnia, to najlepszym modelem tego odcinka czasu wydaje mi się zbiór mereologiczny.*

Gdy słyszę o wysokiej opłacalności pewnej inwestycji, to właściwym modelem tej oceny będzie zbiór rozmyty (fuzzy set).

Gdy wybieram nowy komputer, to biorę pod uwagę zbiór komputerów, który pojmuję jako zbiór przybliżony (rough set).

Są jeszcze zbiory dystrybutywne ... i różne inne (intuicjonistyczne, bipolarne, aproksymowane, przedziałowe, probabilistyczne etc.).

Zbiory dystrybutywne

Według G. Cantora (1883) zbiór, to *każda wielość, która da się pomyśleć jako jedność, tzn. każdy ogół określonych elementów, który można za pomocą jakiegoś prawa powiązać w całość*.

Tak rozumianym zbiorem jest na przykład ogół liczb pierwszych, a prawem, które wiąże w całość te liczby, jest definicja liczby pierwszej.

Liczby pierwsze, to 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 itd. Rozstrzygnięcie, czy dana liczba jest pierwsza może być jednak trudne, np. 4 294 967 297. Nie zmienia to faktu, że albo jest ona albo nie jest liczbą pierwszą.

Dwa zbiory <u>są równe</u> jeśli mają te same elementy.

$\{n \in N$: n jest liczba parzystą$\} = \{0, 2, 4, 6, 8, \ldots\}$

$\{1, 2, 3\} = \{2, 2, 2, 1, 3, 3\}$

$\{(-1)^n: n \in N\} = \{-1, 1\}$

$\{\{1\}, \{1,2\}\} \neq \{1, 2\}$

$(1, 2) \mathbf{=} \{\{1\}, \{1,2\}\}$

Używamy symboli $=$, $\subset$ (czasami $\subseteq$), $\in$ (litera alfabetu greckiego), $\varnothing$ (litera alfabetu norweskiego).

UWAGA: dla operacji definiowania nie powinniśmy używać tego samego symbolu, co dla relacji równości.

Często wygodnie jest ustalić pewien zbiór U, zwany uniwersum, i rozpatrywać jego elementy i jego podzbiory.

Wtedy zbiór A elementów uniwersum U ma dopełnienie A' do uniwersum U, równe $U \backslash A$ (gdzie symbol \ oznacza różnicę zbiorów).

W tych wykładach zajmować się będziemy zbiorami co najwyżej przeliczalnymi, tzn. albo skończonymi albo nieskończonymi, ale równolicznymi ze zbiorem liczb naturalnych.

I często będziemy starać się najpierw określić uniwersum, a potem mówić o zbiorze elementów tego uniwersum. Dlaczego? Dlatego, żeby wiedzieć, o czym mówimy: o liczbach, przedmiotach, kolorach czy zwierzętach?

Rodzina wszystkich podzbiorów zbioru U z operacjami sumy, iloczynu i dopełnienia, oraz z wyróżnionym zbiorem pustym i zbiorem pełnym jest algebrą Boole'a.

Różnicą symetryczną zbiorów A i B nazywamy zbiór tych elementów wymienionych zbiorów, które nie należą do nich jednocześnie. Operator ten oznaczamy przez $\oplus$.

Jeżeli A_1, A_2, … są zbiorami, to przez $\bigcup_{i=1,2,\ldots} A_i$ oznaczamy sumę tych zbiorów. Indeksy mogą być wyrażone inaczej, np. „$i \in I$" albo „$5<i<12$". Podobnie dla iloczynu.

Produkt kartezjański zbiorów A i B oznaczamy przez $A \times B$, produkt $A \times A$ oznaczamy przez A^2 i podobnie dla większej liczby zbiorów, np. $A \times A \times A$ oznaczamy przez A^3.

Dla każdego zbioru skończonego A liczbę jego elementów oznaczamy przez $|A|$.

Jak wiemy:

$|A \times B| = |A| \cdot |B|$

$|\mathscr{P}(A)| = 2^{|A|}$ (i dlatego czasami $\mathscr{P}(A)$ oznacza się przez 2^A)

Na oznaczenie przedziałów liczbowych używamy nawiasów okrągłych i kwadratowych, ale (7, 9) może oznaczać przedział i może oznaczać parę liczb!

Jeśli mówimy o przedziale liczbowym to musimy wskazać jaki zbiór liczb stanowi nasze uniwersum. Możemy np. mówić o przedziale liczb naturalnych, przedziale liczb wymiernych itd.

Relacje

Relacja $E = \{(x, x): x \in S\}$ jest **relacją równości** w zbiorze S.

Piszemy xEx lub $x=x$ lub $(x, x) \in E$.

Relację odwrotną do relacji A oznaczamy A^{-1}.

Złożeniem relacji A w zbiorze S i relacji B w zbiorze S nazywamy relację C w zbiorze S taką, że

xCy wtw gdy istnieje $z \in S$ takie, że xAz i zBy.

Piszemy wtedy $xABy$.

Dla wielokrotnych złożeń jednej relacji stosujemy notację „potęgi", np.
$xAAy = xA^2 y$, $xAAAy = xA^3 y$ ...

Domknięciem relacji A w zbiorze S **z uwagi na operację składania relacj**i nazywamy relację A^d w zbiorze S taką, że $xA^d y$ jeśli istnieje ciąg $z_0=x$, z_1, z_2, … z_{n-1}, $z_n=y$ taki, że $z_0\ A\ z_1\ A\ z_2\ A \dots A\ z_{n-1}\ A\ z_n$.

Zatem $xA^d y$ wtw gdy istnieje n takie, że $xA^n y$.

Jest to jedno z wielu możliwych domknięć relacji A. Nazywamy je również przechodnim domknięciem A. Inne to np. zwrotne domknięcie A czy symetryczne domknięcie A. W każdym przypadku chodzi o najmniejszą relację przechodnią (zwrotną, symetryczną czy jeszcze inną) zawierającą relację A.

Lemat

Przechodnie domknięcie relacji A jest sumą wszystkich potęg tej relacji:

$A^d = A \cup A^2 \cup A^3 \cup \dots \cup A^n \cup \dots$

Formalne określenie domknięcia

Niech α będzie rodziną relacji w zbiorze *S, A* dowolną relacją w *S*.

Relacja A^{d} jest domknięciem *A* w zbiorze relacji α gdy:

(1) $A \subset A^{d}$

(2) $A^{d} \in \alpha$

(3) dla każdej relacji *B* jeżeli $A \subset B$ i $B \in \alpha$ to $A^{d} \subset B$

A zatem domknięciem relacji *A* z uwagi na własność α jest najmniejsza relacja zawierająca *A* i posiadająca własność α.

Reprezentacja macierzowa

Niech S będzie zbiorem n-elementowym i A relacją w S.

Ponumerujmy elementy zbioru S i zbudujmy tablicę kwadratową o wymiarze n. Na przecięciu i-tego wiersza i j-tej kolumny wpisujemy 1 jeśli $x_i A x_j$, w przeciwnym wypadku 0. Elementy takiej macierzy oznaczać będziemy przez a_{ij}, a całą macierz przez $[a_{ij}]$.

Oczywiście istnieje n! różnych numeracji zbioru S, czyli n! różnych macierzy opisujących relację A w S.

Macierz, której wszystkie elementy są zerami określa **relację pustą**.

Macierz, której wszystkie elementy są jedynkami określa **relację pełną** (uniwersalną).

Macierz $[\delta_{ij}]$, gdzie $\delta_{ij}=1$ dla $i=j$ oraz $\delta_{ij}=0$ dla $i\neq j$, określa relację **równości**.

Symbol δ_{ij} nazywamy **deltą Kroneckera**. Macierz $[\delta_{ij}]$ zawiera jedynki na przekątnej i zera poza przekątną. Nazywamy ja macierzą Kroneckera.

Macierz $[a_{ij}] = [1-\delta_{ij}]$ określa relację **nierówności**.

Lemat

Tylko dla tych czterech relacji (pustej, pełnej, równości i nierówności) ich macierze pozostają niezmienione dla różnych numeracji zbioru S.

Niech R relacja w zbiorze S. Wprowadza się następujące własności relacji:

- **zwrotność**

  $(x, x) \in R$ dla wszystkich $x \in S$

- **symetria**

  $(x, y) \in R \Rightarrow (y, x) \in R$ dla wszystkich $x \in S, y \in S$

- **przechodniość**

  $(x, y) \in R$ i $(y, z) \in R \Rightarrow (x, z) \in R$ dla wszystkich $x \in S, y \in S, z \in S$

Lematy

Relacja R jest przechodnia wtw gdy $R^2 \subseteq R$.

Relacja R jest przechodnia wtw gdy $R = R^d$.

Relacja **niezwrotna**, to relacja, która nie jest zwrotna,

tzn. $(x, x) \notin R$ dla pewnego $x \in S$

Relacja **przeciwzwrotna** (antyzwrotna), to nowa własność:

$(x, x) \notin R$ dla wszystkich $x \in S$

Lematy

Relacja zwrotna zawiera relację równości.

Relacja pełna i relacja równości są zwrotne.

Relacja przeciwzwrotna jest relacją niezwrotną.

Macierz relacji przeciwzwrotnej ma zera na przekątnej.

Relacja pusta jest przeciwzwrotna.

Relacja asymetryczna, to relacja która nie jest symetryczna:

$(x, y) \in R$ i $(y, x) \notin R$ dla pewnych $x \in S, y \in S.$

Relacja R w zbiorze S jest zwana **przeciwsymetryczną**, gdy z dwóch zależności xRy, yRx co najmniej jedna jest nieprawdziwa:

$(x, y) \in R \Rightarrow (y, x) \notin R$ dla wszystkich $x \in S, y \in S$.

Relacja R w zbiorze S jest zwana **antysymetryczną**, gdy prawdziwość dwu zależności xRy, yRx jest równoważna równości x i y:

$(x, y) \in R$ i $(y, x) \in R$ wtw $x=y$.

Lematy

Macierz relacji symetrycznej jest symetryczna względem przekątnej.

Relacja A jest symetryczna wtw gdy $A=A^{-1}$.

Relacja A jest przeciwsymetryczna wtw gdy $A \cap A^{-1}=\emptyset$.

Relacje pusta, pełna, równości i nierówności są symetryczne.

Relacja pusta jest również przeciwsymetryczna.

Relacja przeciwsymetryczna jest przeciwzwrotna.

Relacja równości nie jest przeciwsymetryczna!

Relacja A jest antysymetryczna wtw gdy $A \cap A^{-1} \subseteq$ E (gdzie E to relacja równości).

Relacje pusta i równości są antysymetryczne.

Niech R relacja w zbiorze S. Wprowadza się kolejne własności relacji:

- **spójność**

  $(x, y) \in R$ lub $(y, x) \in R$ dla wszystkich $x \in S$

- **słaba spójność**

  $(x, z) \in R$ i $(y, z) \in R$ dla pewnego $z \in S \Rightarrow (x, y) \in R$ lub $(y, x) \in R$

Lematy

Relacja $<$ w zbiorze liczb rzeczywistych jest …

Relacja $\leq$ w zbiorze liczb rzeczywistych jest …

Własności relacji a działania na relacjach

Jeśli A, B są zwrotne to $A \cup B$, $A \cap B$, AB, A^{-1}, A^{d} są zwrotne.

Jeśli A, B są przeciwzwrotne to $A \cup B$, $A \cap B$, A^{-1} są przeciwzwrotne.

Jeśli A, B są symetryczne to $A \cup B$, $A \cap B$, A^{-1} są symetryczne.

Domknięcie relacji symetrycznej jest symetryczne.

Jeśli A jest przeciwsymetryczna to A^{-1} jest przeciwsymetryczna.

Jeśli A jest przeciwsymetryczna to dla dowolnej B relacja $A \cap B$ jest przeciwsymetryczna.

Jeśli A, B są antysymetryczne to $A \cap B$, A^{-1} są antysymetryczne.

Jeśli A, B są przechodnie to $A \cap B$, A^{-1} i A^{d} są przechodnie.

Równość, równoważność, podobieństwo, tolerancja

Pojęcie podobieństwa wykorzystujemy głównie do budowania zbiorów (zbiór składa się z elementów podobnych!). I choć termin „zbiór” może być pojmowany na wiele sposobów oraz często zastępujemy go terminami „typ encji” czy „klasa obiektów”, nie zmienia to istoty sprawy. Łącząc elementy w zbiór podejmujemy decyzję, na czym ma polegać ich podobieństwo.

Najwyższym stopniem podobieństwa jest **nierozróżnialność**, a nie równość.

Równość jest szczególnym przypadkiem nierozróżnialności i szczególnym przypadkiem podobieństwa. Równość (identyczność) to także zastępowalność jednego obiektu drugim w określonej sytuacji. Podobieństwo oznacza tylko częściową zastępowalność, możliwość zastąpienia jednego obiektu drugim, ale z pewnym ryzykiem czy pewną stratą.

Podobieństwo obiektów danego uniwersum jest w matematyce zwane **tolerancją** (relacją zwrotną i zarazem symetryczną). Nie jest zaś wymagana przechodniość, a to dlatego, że obiekty podobne nie są identyczne: nieznacznie różnią się od siebie i te drobne różnice między kolejnymi podobnymi obiektami mogą doprowadzić do obiektów całkowicie różnych od tych początkowych.

Przykładem podobieństwa jest znana zabawa ze słowami polegająca na przekształceniu słowa początkowego w słowo końcowe poprzez kolejne słowa różniące się tylko jedną literą, np. możemy w taki sposób przekształcić słowo „kot” w słowo „lew”:

kot – kos – los – lis – lin – len – lew.

Zbiór *U* z określoną na nim relacją tolerancji *T* nazywa się **przestrzenią tolerancji**. Struktura tej przestrzeni jest bardzo ciekawa. W szczególności okazuje się, że dowolną tolerancję można określić przy pomocy zbioru cech elementów uniwersum *U* w taki sposób, że elementami podobnymi są te, które mają co najmniej jedną wspólną cechę.

Lematy

Jeśli *A* i *B* są tolerancjami, to $A \cup B$, $A \cap B$, A^{-1}, A^{d} są tolerancjami.

Domknięcie tolerancji *A* jest najmniejszą relacją równoważności zawierającą *A*.

Jeśli A jest zwrotna, to $A \cup A^{-1}$, $A \cap A^{-1}$, $A\,A^{-1}$ są tolerancjami.

W matematyce **podobieństwo** często definiuje się nie jako relację tolerancji, lecz jako szczególną relację równoważności – równokształtność.

Na przykład w geometrii dwa wielokąty uznaje się za podobne, gdy mają te same kąty i proporcje: mają taki sam kształt, ale mogą mieć różną wielkość. Podobnie w algebrze: dwa wyrażenia nazywa się podobnymi, gdy mają ten sam kształt z dokładnością do współczynników liczbowych. Przykłady takie można mnożyć.

Funkcje

Funkcja o dziedzinie *X* i przeciwdziedzinie *Y* to dowolna relacja $f \subset X \times Y$ taka, że $\forall x \in X \; \exists! y \in Y: (x,y) \in f$.

Dziedzinę i przeciwdziedzinę funkcji oznaczamy przez Dom(f) i Im(f).

Przykłady

$$h : \mathbb{R} \ni x \mapsto \sin\frac{\pi}{x} \in \mathbb{R}$$

$$\{0,1\}^* \ni w \mapsto w1 \in \{0,1\}^*$$

$d : \{0,1\}^* \longrightarrow \mathbb{N},\ d(w) =$ długość słowa w

$X^* \times X^* \ni (v,w) \mapsto vw \in X^*$, **gdzie vw słowo powstałe z doklejenia słowa w za v.**

Surjekcja to funkcja *f*: *X*→*Y* spełniająca warunek $\forall y \in Y \ \exists x \in X \quad f(x) = y$
Piszemy wtedy $f : X \twoheadrightarrow Y$, czytamy „X na Y”.

Injekcja to funkcja *f*: *X*→*Y* spełniająca warunek
$\forall x_1, x_2 \in X \quad x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$. Piszemy $f : X \hookrightarrow Y$.

Injekcje często są nazywane funkcjami różnowartościowymi.

Bijekcja to funkcja, która jest jednocześnie surjekcją i injekcją. Nazywamy ją również przekształceniem wzajemnie jednoznacznym.

Wykresem funkcji liczbowo-liczbowej nazywamy zbiór punktów na układzie współrzędnych, gdzie argument jest odciętą punktu, a wartość funkcji jest rzędną. Na rysunkach pokazuje się zwykle fragment wykresu (najbardziej interesujący).

Funkcja charakterystyczna zbioru *A* w przestrzeni *S* to

$\chi_A\colon S \to \{0, 1\}$; $\chi_A(x)=1$ dla $x \in A$, 0 wpp

Funkcja dwóch zmiennych to funkcja, której dziedziną jest zbiór par (wciąż jednak zbiór!). Piszemy np. $f\colon XGY \to Z$. Podobnie można zdefiniować funkcje trzech i większej liczby zmiennych.

Obcięciem funkcji f: $A \to B$ do zbioru C nazywamy funkcję

$f|_C: C \to B$; $f|_C(x) = f(x)$ dla $x \in C$.

Traktując funkcję f: $X \to Y$ jako relację $f \subset X \times Y$ (zbiór par), możemy rozważać **relację f^{-1} odwrotną do f**. Kiedy ta relacja jest funkcją?

Funkcja posiada funkcję odwrotną, wtedy i tylko wtedy, gdy jest bijekcją.
W takim przypadku funkcja odwrotna to relacja odwrotna.
Przykład konstrukcji funkcji odwrotnej:

$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R},$$

$$f : \mathbb{R} \ni x \mapsto x^2 \in [0, +\infty).$$

$$f|_{[0,+\infty)} : [0, +\infty) \ni x \mapsto x^2 \in [0, +\infty),$$

$$[0, +\infty) \ni x \mapsto \sqrt{x} \in [0, +\infty).$$

Wartość bezwzględna to funkcja $|\,|$: $R \to R$; $|x|=x$ dla $x \geq 0$, $-x$ wpp

Własności: $|x \cdot y| = |x| \cdot |y|$, $|x+y| \leq |x| + |y|$

Oznaczenia niektórych funkcji:

1. **log *x*** to logarytm z liczby x przy podstawie 10,
2. **lg *x*** to logarytm z liczby x przy podstawie 2,
3. **ln *x*** to logarytm z liczby x przy podstawie e.

Złożenie $f \circ g$ funkcji f: $X \to Y$ i funkcji g: $Y \to Z$ to funkcja h: $X \to Z$ określona dla wszystkich argumentów jako $h(x)=g(f(x))$.

<u>Złożenie $f \circ g$ bywa oznaczane jako gf</u>.

Czy dziedzina funkcji g może być większa niż przeciwdziedzina funkcji f w złożeniu $f \circ g$?

Przemienność: zwykle nie zachodzi równość $f \circ g = g \circ f$.

Łączność: dla funkcji $X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} W$ zachodzi $(h \circ g) \circ f = h \circ (g \circ f)$.
Zapis uproszczony: $f(gh) = (fg)h$.

Dla $X \xrightarrow{f} Y \xrightarrow{g} Z$ mamy lematy:

- ✓ jeśli f, g są surjekcjami, to gf jest surjekcją,
- ✓ jeśli f, g są injekcjami to gf jest injekcją,
- ✓ jeśli f, g są bijekcjami to gf jest bijekcją.

Niech $f: X \to Y$, $A \subset X$, $B \subset Y$. Wtedy:

- $f(A)$ nazywamy **obrazem** zbioru A.
- $f^{-}(B)$ nazywamy **przeciwobrazem zbioru** B względem f.
- $f^{-}(y)$ nazywamy **przeciwobrazem elementu** y wzg. f i jest to $f^{-}(\{y\})$

Czy $f^{-}(y)$ to $f^{-1}(y)$?