

Kombinatoryka & teoria grafów

by a fish

21.03.2137

SYLABUS – MDM:

A. ELEMENTY ALGEBRY I TEORII LICZB

- Funkcje całkowitoliczbowe, arytmetyka modularna, operacje sufit i podłoga zaokrąglania liczb rzeczywistych, algorytm mergesort
- Asymptotyka funkcji liczbowych z uwzględnieniem zastosować w szacowaniu złożoności czasowej algorytmów
- Podzielność liczb, algorytm Euklidiesza
- Liczby Fibonacciego
- Liczby pierwsze i względnie pierwsze. Rozkład na czynniki. Funkcja Eulera. Chińskie twierdzenie o resztach. Twierdzenie Eulera.

B. KOMBINATORYKA

- Rozmieszczenia, permutacje, kombinacje, podziały (zbioru, liczb), Lemat Burnside'a
- Metody generowania prostych obiektów kombinatorycznych
- Przykłady prostych problemów definiowanych rekurencyjnie
- Rozwiązanie równań rekurencyjnych, funkcje tworzące
- Liczby Catalana
- Zasada włączania i wyłączania

C. TEORIA GRAFÓW

- Definicja i przykłady grafów, grafy pełne, dwudzielne skierowane, stopień wierzchołka
- Drogi i cykle w grafach: grafy spójne i dwudzielne
- Drzewa – równoważność różnych definicji
- Komputerowa reprezentacja grafów
- Metody BFS i DFS przeszukiwania grafów
- Minimalne drzewa rozpinające – algorytmy Kruskala i Prima-Dijkstry
- Przechodzenie domknięcie: algorytmy Dijkstry i Warshalla. Złożoność problemu
- Cykle i drogi Eulera
- Cykle i drogi Hamiltona, twierdzenie Ore i wielomianowa redukcja problemu drogi do cyklu i odwrotnie
- Przepływy w sieciach
- Kolorowanie grafów: zastosowanie – planowanie sesji egzaminacyjnej. Algorytm sekwencyjny i twierdzenie o 5-kolorowaniu grafów planarnych.

SYLABUS – teoria grafów:

1. Basic concepts: graphs, paths and cycles, complete and bipartite graphs
2. Matchings: Hall's Marriage theorem and its variations
3. Forbidden subgraphs: complete bipartite and r -partite subgraphs, chromatic numbers, Turán's theorem, asymptotic behaviour of edge density, Erdős-Stone theorem
4. Hamiltonian cycles (Dirac's Theorem), Eulerian circuits
5. Connectivity: connected and k -connected graphs, Menger's theorem
6. Ramsey theory: edge colourings of graphs, Ramsey's theorem and its variations, asymptotic bounds on Ramsey numbers
7. Planar graphs and colourings: statements of Kuratowski's and Four Colour theorems, proof of Five Colour theorem, graphs on other surfaces and Euler characteristics, chromatic polynomial, edge colourings and Vizing's theorem
8. Random graphs: further asymptotic bounds on Ramsey numbers, Zarankiewicz numbers and their bounds, graphs of large first and high chromatic number, complete subgraphs in random graphs.
9. Algebraic methods: adjacency matrix and its eigenvalues, strongly regular graphs, Moore graphs and their existence.

Spis treści

1	Elementy algebry i teorii liczb	5
1.1	Podłoga i sufit	5
1.2	Operacja mod	6
1.3	Hierarchia – asymptotyka	7
1.4	Big O notation	7
1.5	Notacja Duże Ω	7
1.6	Notacja Dużego Θ	8
1.7	Notacja małego o	8
1.8	Reguły notacji dużego O	8
2	Podzielność liczb	9
2.1	NWD & NWW	9
2.2	Liczby pierwsze	9
3	Basic concepts of graph theory	11
3.1	Graphs	11
3.2	Paths	11
3.3	Cycles	12

1 Elementy algebry i teorii liczb

1.1 Podłoga i sufit

Reguły funkcji podłoga i sufit:

1. $\lfloor x \rfloor = n \iff n \leq x < n+1$
2. $\lfloor x \rfloor = n \iff x-1 < n \leq x$
2. $\lceil x \rceil = n \iff n-1 < x \leq n$
3. $\lceil x \rceil = n \iff x \leq n < x+1$

Więcej hardcorowych własności:

$$\lfloor x+n \rfloor = \lfloor x \rfloor + n$$

ale dla mnożenia to już nie zadziała.

Dla liczb całkowitych zachodzi:

$$x < n \iff \lfloor x \rfloor < n$$

$$n < x \iff n < \lceil x \rceil$$

$$x \leq n \iff \lceil x \rceil \leq n$$

$$n \leq x \iff n \leq \lfloor x \rfloor$$

Część ułamkowa to różnica $x - \lfloor x \rfloor$. Oznaczamy $\{x\}$, chyba że gdzieś obok pojawiają się singletony. Wtedy nie oznaczamy. Simple.

$$\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$$

W pierwszej kolejności chcemy pozbyć się zewnętrznych nawiasów i pierwiastka kwadratowego, potem usunąć nawiasy wewnętrzne. Na koniec dodajemy z powrotem pierwiastek i nawiasy zewnętrzne:

$$\lfloor \sqrt{\lfloor x \rfloor} \rfloor \rightarrow \sqrt{\lfloor x \rfloor} \rightarrow \lfloor x \rfloor \rightarrow x \rightarrow \sqrt{x} \rightarrow \lfloor \sqrt{x} \rfloor$$

Niech $m = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$. Z wcześniej ustalonych reguł wynika, że

$$m \leq \sqrt{\lfloor x \rfloor} < m+1.$$

Ponieważ wszystkie trzy wyrażenia są nieujemne, możemy podnieść je do kwadratu:

$$m^2 \leq \lfloor x \rfloor < (m+1)^2.$$

Ponieważ zarówno m jak i $m+1$ są liczbami całkowitymi, to możemy pozbyć się nawiasów kwadratowych, otrzymując

$$m^2 \leq x < (m+1)^2.$$

Obie strony nadal są nieujemne, możemy je więc spierwiastkować, żeby otrzymać

$$m \leq \sqrt{x} < m+1$$

a więc

$$m = \lfloor \sqrt{x} \rfloor$$

i to jest to, co chcieliśmy otrzymać.

i śmiga



Możemy tę równość uogólnić dla dowolnej funkcji f takiej, że $f(x) \in \mathbb{Z} \implies x \in \mathbb{Z}$:

$$\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor \wedge \lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil.$$

Szczególnym przypadkiem tego twierdzenia jest

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor \wedge \left\lceil \frac{x+m}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil + m}{n} \right\rceil$$

Widmo liczby rzeczywistej α to nieskończony zbiór liczb całkowitych z powtórzeniami:

$$Spec(\alpha) = \{\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor, \dots\}.$$

Ilość elementów $Spec(\alpha)$ nie większych niż n wynosi:

$$N(\alpha, n) = \sum_{k>0} (\lfloor k\alpha \rfloor \leq n) = \sum_{k>0} (\lfloor k\alpha \rfloor < n+1) = \sum_{k>0} (k\alpha < n+1) = \left\lceil \frac{n+1}{\alpha} \right\rceil - 1$$

1.2 Operacja mod

Wzór na dzielenie liczby n przez m :

$$n = m \left\lfloor \frac{n}{m} \right\rfloor + n \bmod m,$$

czyli

$$n \bmod m = n - m \left\lfloor \frac{n}{m} \right\rfloor, \quad m \neq 0$$

Jest to definicja która działa też dla liczb ujemnych, na przykłady

$$5 \bmod 3 = 5 - 3 \left\lfloor \frac{5}{3} \right\rfloor = 2$$

$$5 \bmod -3 = 5 - (-3) \left\lfloor \frac{5}{-3} \right\rfloor = -1$$

$$-5 \bmod -3 = -5 - (-3) \left\lfloor \frac{-5}{-3} \right\rfloor = -2$$

Część ułamkową można zdefiniować jako operację modulo:

$$\{x\} = x \bmod 1.$$

Działania modulo:

$$c(x \bmod y) = cx \bmod cy$$

Jeśli rozmieścimy n przedmiotów do m grup tak, żeby różnica ich ilości między grupami była nie większa niż 1, a większe grupy były bliżej początku, to bez problemu możemy sprawdzić ilość przedmiotów w k -tej grupie:

$$\left\lceil \frac{n - k + 1}{m} \right\rceil.$$

A więc skoro mamy n przedmiotów w m grupach, to całość dostaniemy sumując wszystkie grupy:

$$n = \left\lceil \frac{n}{m} \right\rceil + \dots + \left\lceil \frac{n - m + 1}{m} \right\rceil.$$

Po prostu powoli odejmujemy coraz więcej od reszty z tego dzielenia.

Podobna zależność działa też dla liczb rzeczywistych:

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor \dots + \left\lfloor x + \frac{m-1}{m} \right\rfloor$$

WYPADAŁOBY TUTAJ WRÓCIĆ, ALE CHWILOWO MAM DOŚĆ OPERACJI NA PODŁOGACH I INNYCH SUFITACH

1.3 Hierarchia – asymptotyka

$$f(n) \prec g(n) \iff \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$$

Czyli $f(n)$ rośnie wolniej niż $g(n)$. Na przykład $n \prec n^2$. Podstawowa hierarchia to dla $0 < \varepsilon < 1 \leq c$:

$$1 \prec \log \log n \prec \log n \prec n^\varepsilon \prec n^c \prec n^{\log n} \prec c^n \prec n^n \prec c^{c^n}.$$

Wszystkie te funkcje przy $n \rightarrow \infty$ dążą do nieskończoności, kluczowe więc nie jest określenie czy to robią, a raczej **jak szybko do ∞ dążą**. Alternatywnie, możemy porównywać odwrotności funkcji i jak szybko one dążą do zera, nigdy go nie osiągając.

$$e^{f(n)} \prec e^{g(n)} \iff \lim_{n \rightarrow \infty} (f(n) - g(n)) = -\infty$$

Dwie funkcje są do siebie **asymptotyczne**, jeżeli mają **ten sam współczynnik**. Piszemy wtedy $f(n) \asymp g(n)$, czyli

$$f(n) \asymp g(n) \iff |f(n)| \leq C \cdot |g(n)| \wedge |g(n)| \leq C \cdot |f(n)|,$$

dla pewnej stałej C oraz dostatecznie dużych n . Zachodzi to na przykład dla wielomianów tego samego stopnia.

Klasa funkcji logarytmiczno-wykładniczych jest zdefiniowana rekurencyjnie jako najmniejsza rodzina L (to powinno być gotyckie L , ale coś nie działa) spełniająca

1. dla każdego $\alpha \in \mathbb{R}$ funkcja $f(n) = \alpha$ należy do L
2. funkcja tożsamościowa $f(n) = n$ należy do L
3. jeżeli $f(n)$ i $g(n)$ należą do L , to również $f(n) - g(n)$ należy do L
4. jeżeli $f(n)$ należy do L oraz jest dodatnia od pewnego momentu, to również $\ln(f(n))$ należy do L .

Główne twierdzenie Hardy’ego mówi, że jeżeli $f(n), g(n) \in L$ to zachodzi jedna z możliwości:

1. $f(n) \prec g(n)$
2. $g(n) \prec f(n)$
3. $f(n) \asymp g(n)$.

1.4 Big O notation

Zapis $f(n) = O(g(n))$ oznacza, że $|f(n)| \leq C|g(n)|$ dla wszystkich n . Czyli oznacza, że $O(5)$ jest liczbą której wartość bezwzględna po pomnożeniu przez jakąś stałą jest nie większa niż 5.

Bardzo często narzucamy na notację O pewne ograniczenia, na przykład powiedzenie, że

$$f(n) = O(g(n)), \quad n \rightarrow \infty$$

oznacza, że warunek jest spełniony dla n bardzo bliskich ∞ , a o inne n nie dbamy. Czyli tak naprawdę nakładamy dwie stałe: C do mnożenia i n_0 od którego warunek zaczyna być spełniany.

Uwaga, znak $=$ w kontekście notacji dużego O to lekkie nadużycie. Notacja $f(n) = O(g(n))$ oznacza tylko, że $f(n)$ należy do pewnego zbioru funkcji takich, że istnieje C takie, że $f(n) \leq C|g(n)|$. Dlatego też piszemy O po prawej stronie równania nie po lewej – znak $=$ to tak naprawdę leniwe \subseteq .

1.5 Notacja Duże Ω

Używana jest do dolnych ograniczeń funkcji, tzn

$$f(n) = \Omega(g(n)) \iff |f(n)| \geq C|g(n)|$$

dla pewnego $C > 0$. Mamy więc

$$f(n) = \Omega(g(n)) \iff g(n) = O(f(n)).$$

Czyli na przykład algorytm sortujący w czasie $\Omega(n^2)$ jest o wiele bardziej nieefektywny niż $O(n \log n)$.

1.6 Notacja Dużego Θ

Określa dokładny porządek przyrostu:

$$f(n) = \Theta(g(n)) \iff \begin{matrix} f(n) = O(g(n)) \\ f(n) = \Omega(n) \end{matrix}.$$

Czyli $f(n) = \Theta(g(n)) \iff f(n) \asymp g(n)$.

1.7 Notacja małego o

Odpowiada relacji $f(n) \prec g(n)$. Dodatkowo, mamy

$$f(n) \sim g(n) \iff f(n) = g(n) + o(g(n)).$$

1.8 Reguły notacji dużego O

Ciąg bardzo fajnych i przyjemnych wzorków które trzeba się nauczyć c:

$$n^a = O(n^b) \quad a \leq b$$

$$O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$$

$$f(n) = O(f(n))$$

$$c \cdot O(f(n)) = O(f(n))$$

$$O(O(f(n))) = O(f(n))$$

$$O(f(n))O(g(n)) = O(f(n)g(n))$$

$$O(f(n)g(n)) = f(n)O(g(n))$$

Jeżeli suma

$$S(z) = \sum_{n \geq 0} a_n z^n$$

jest bezwzględnie zbieżna dla pewnego $z_0 \in \mathbb{Z}$, to

$$S(z) = O(1) \quad (\forall z) \quad |z| \leq |z_0|,$$

bo

$$S(z) = \sum_{n \geq 0} a_n z^n \leq \sum_{n \geq 0} a_n z_0^n = C < \infty$$

Przybliżenie asymptotyczne ma **błąd bezwzględny** równy $O(g(n))$ jeżeli jest ono postaci $f(n) + O(g(n))$, gdzie $f(n)$ nie zawiera O . **Błąd względny** jest równy $O(g(n))$ gdy jest ono z kolei postaci $f(n)(1 + O(g(n)))$.

2 Podzielność liczb

2.1 NWD & NWW

NWW – najmniejsza wspólna wielokrotność

NWD – największy wspólny dzielnik

Algorytm Euklidesa – do liczenia $NWD(n, m)$:

$$NWD(0, n) = n$$

$$NWD(m, n) = NWD(n \bmod m, m) \quad m > 0$$

Można go rozszerzyć do stwierdzenia, które tak naprawdę potwierdza poprawność algorytmu Euklidesa, które znajduje liczby całkowite n' i m' takie, że $m'm + n'n = NWD(m, n)$

Śmieszne sumowanie względem wszystkich dzielników liczby n :

$$\sum_{m|n} a_m = \sum_{n|m} a_{\frac{n}{m}}$$

2.2 Liczby pierwsze

Liczba pierwsza to liczba naturalna, która ma dokładnie dwa dzielniki – siebie samą i 1. Liczby naturalne mające 3 i więcej dzielników są nazywane liczbami złożonymi.

Każdą liczbę naturalną większą niż 1 można jednoznacznie przedstawić jako iloczyn liczb pierwszych. Istnieje tylko jeden sposób, w jaki liczbę n można zapisać jako iloczyn liczb pierwszych w niemalejącym porządku (podstawowe twierdzenie arytmetyki).

DOWÓD:

Indukcją po n można pokazać jednoznaczność rozkładu dowolnej liczby naturalnej $n > 1$

$$n = \prod_{k=1}^m p_k \quad p_1 \leq \dots \leq p_m$$

1° $n = 1$ wtedy jednoznaczność jest trywialna, bo iloczyn musi być pusty

2° zakładamy, że zachodzi dla wszystkich liczb poniżej n .

Przypuśćmy, nie wprost, że istnieją dwa rozkłady:

$$n = p_1 \dots p_m = q_1 \dots q_k,$$

gdzie wszystkie liczby p_r i q_r są pierwsze.

Gdyby istniało j takie, że $p_j \neq q_j$, to ponieważ obie liczby są pierwsze, to ich NWD jest równe 1. Ponadto, z algorytmu Euklidesa możemy znaleźć liczby a, b takie, że

$$ap_j + bq_j = 1.$$

W takim razie

$$p_1 \dots p_{j-1} p_{j+1} \dots p_m = p_1 \dots p_{j-1} p_{j+1} \dots p_m (ap_j + bq_j) = p_1 \dots ap_j \dots p_m + p_1 \dots bq_j \dots p_m.$$

Zauważmy, że liczba q_j dzieli oba składniki sumy po prawej stronie. Podzielność drugiego jest trywialna, natomiast pierwszy jest dzielony ponieważ $p_1 \dots p_m = n$ a $q_j | n$. W takim razie liczba

$$\frac{p_1 \dots p_{j-1} p_{j+1} \dots p_m}{q_j}$$

jest liczbą całkowitą mniejsza od n , a więc ma jednoznaczny rozkład na iloczyn liczb pierwszych:

$$\frac{p_1 \dots p_{j-1} p_{j+1} \dots p_m}{q_j} = t_1 \dots t_r$$

w takim razie możemy napisać

$$p_1 \dots p_{j-1} p_{j+1} \dots p_m = q_j t_1 \dots t_r$$

3 Basic concepts of graph theory

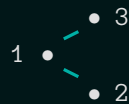
3.1 Graphs

Graph ($G = (V, E)$) - a structure made up of **vertices** (V) that are connected in pairs with **edges** (E).

Multigraph - a graph where two vertices are allowed to have more than one edge connecting them.

If a vertex is allowed to be connected to itself, then the graph is called a **graph with loops** and the edge that connects the vertex to itself is known as a **loop**.

Adjacency relation - is the symmetric relation of pairings between vertices of an undirected graph. It is used to construct an **adjacency matrix** that is another form of representing graphs.



$$\begin{matrix} & 1 & 2 & 3 \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

Directed graph is a graph in which edges have orientation. Here, the set of edges contains ordered pairs of vertices. However, this definition does not allow multiple edges between two vertices. To fix this problem, we introduce another object, ϕ , that is a mapping of edges to ordered pairs of vertices. To avoid confusion, we call such graph a **directed multigraph** ($G = (V, E, \phi)$).

Mixed graph is a graph that allows both directed and undirected edges.

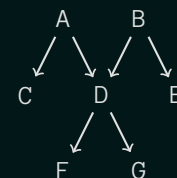
Weighted graph is a graph in which each edge has a value assigned to it.

Oriented graph is a directed graph where each edge has a set orientation, that is if an edge $\langle x, y \rangle$ exists, there cannot be an edge $\langle y, x \rangle$.

Regular graph is a graph in which each vertex has the same number of neighbours (**degree**).

Complete graph is a graph where every pair of vertices is connected with an edge.

Tree is a graph in which any two vertices are connected by exactly one path.



Polytree is a graph whose underlying graph is a tree. For example on the right is a polytree in which subgraph (A, D, F, G) is a tree.

3.2 Paths

A pair of vertices x, y is **connected** if there can be found a collection of edges so that they are have connected ends and going through them leads from x to y and vice versa. Such a collection is called a **path**.

A graph is **connected** if each two vertices are connected. A stronger condition, each two vertices are connected with directed edges, makes a graph **strongly connected**.

.....
Chromatic number - the smallest number of colors needed to color a graph so that every two vertices of an edge have different colors. For example the following graph has chromatic number 3:



.....
Bipartite graph is a simple graph where vertex set can be partitioned into two sets. Alternatively, it is a graph with chromatic number 2.

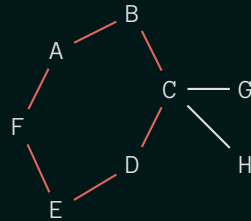
Planar graph is a graph that can be drawn on a plane so that no two edges intersect.

3.3 Cycles

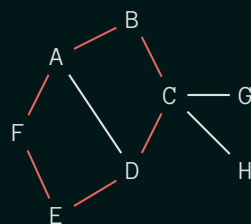
Cycle – non-empty trail in which only the first and last vertices are equal. If more than just the first and last vertices repeat in a cycle, then it is called a **circuit**.

Cycle graph of order n is a graph where n vertices create a cycle. They are connected graphs with vertices of degree 2. If no cycles exist in a graph, then it is called an **acyclic graph**.

Chordless cycle is a cycle in which no two vertices are connected by an edge that itself does not belong in the cycle, for example (A, B, C, D, E, F) form an chordless cycle



Whereas in the next example, (A, B, C, D, E, F) do not form a chordless cycle – edge $\{A, D\}$ is a **chord**.



Girth of a graph is the length of its shortest chordless cycle. **Cages** are regular graphs with as few vertices as possible for its girth.