Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z prednášky č. 1

Riešenie sústav lineárnych rovníc

Sústavu lineárnych rovníc prepíšeme do tabuľkovej formy tak, že v každom stĺpci budú koeficienty zodpovedajúce jednej premennej, pričom v poslednom stĺpci (oddelenom zvislou čiarou) budú hodnoty z pravých strán rovníc.

Na riadky tabuľky môžeme aplikovať nasledujúce elementárne operácie, ktoré nemenia množinu riešení sústavy rovníc.

ERO 1 - Výmena poradia ľubovoľných dvoch riadkov.
ERO 2 - Vynásobenie riadku nenulovou konštantou.
ERO 3 - Pripočítanie nenulového násobku jedného riadku k inému riadku.

Gaussova eliminačná metóda

Systém lineárnych rovníc riešime v tabuľkovej forme pomocou elementárnych riadkových operácií v dvoch hlavných etapách.

Etapa 1: Postupne identifikujeme pivotné prvky (prvé nenulové prvky v riadku) a pomocou ERO 2 z nich produkujeme pivotné jednotky, počnúc ľavým horným prvkom (jeho získanie môže vyžadovať použitie ERO 1) a pokračujúc postupne vpravo a nadol. Ihneď po získaní pivotnej jednotky vyprodukujeme pomocou ERO 3 nuly v stĺpci pod ňou. Prípadné nulové riadky umiestnime pod nenulovými riadkami pomocou ERO 1.

Etapa 2: Pomocou ERO 3 postupne produkujeme nuly nad pivotnými jednotkami, počnúc stĺpcom s poslednou pivotnou jednotkou vpravo dolu a pokračujúc smerom vľavo a nahor.

Výsledná tabuľka, kde v každom stĺpci s pivotnou jednotkou sú všetky ostatné prvky nulové, sa nazýva tabuľkou v **redukovanom tvare**.

Redukovaný tvar je pre každý systém rovníc jednoznačne určený.

Ak má lineárna sústava rovníc **aspoň toľko rovníc ako neznámych**, počet riešení bude jedna z možností

- žiadne
- jediné
- nekonečne veľa

Ak má lineárna sústava rovníc **menej rovníc ako neznámych**, počet riešení bude jedna z možností

- žiadne
- nekonečne veľa

Homogénna sústava lineárnych rovníc je sústava, ktorá má všetky konštantné členy (pravé strany) nulové.

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0 \\
\vdots \quad & \quad \vdots \quad \vdots \\
a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0
\end{aligned}$$

Pre homogénnu sústavu lineárnych rovníc platí jedna z nasledujúcich možností:

- Sústava má iba triviálne riešenie $x_1 = 0, x_2 = 0, \ldots, x_n = 0$.
- Sústava má nekonečne veľa riešení vrátane triviálneho.

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z prednášky č. 2

Matice, operácie s maticami, inverzná matica

Matica je usporiadaná obdĺžniková tabuľka čísel.

Ak matica pozostáva z m riadkov a n stĺpcov, hovoríme, že je **typu** $m \times n$.
Všeobecný zápis matice

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix} \quad \text{alebo} \quad A = (a_{ij})_{m\times n}$$

Štvorcová matica rádu n je matica s n riadkami a n stĺpcami.

Hlavná diagonála štvorcovej matice pozostáva z prvkov $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$.

Súčet prvkov na hlavnej diagonále je **stopa** matice a značujeme ju $\mathrm{tr}(A)$.

Diagonálna matica je štvorcová matica, ktorej všetky prvky nachádzajúce sa mimo hlavnej diagonály sú nulové.

Dve matice sa **rovnajú**, ak sú rovnakého typu a majú rovnaké prvky na všetkých príslušných miestach.

Súčtom matíc rovnakého typu je matica toho istého typu s prvkami získanými sčítaním prvkov daných matíc na príslušných pozíciách, t. j.

ak $A = (a_{ij})_{m\times n}$ a $B = (b_{ij})_{m\times n}$, tak $A + B = (a_{ij} + b_{ij})_{m\times n}$.

Rozdielom matíc $A = (a_{ij})_{m\times n}$ a $B = (b_{ij})_{m\times n}$ je matica

$$C = A - B = (a_{ij} - b_{ij})_{m\times n} = (c_{ij})_{m\times n}.$$

Nie je možné sčítať ani odčítať matice rôznych typov!

Sčítanie matíc je komutatívne aj asociatívne.

Nulová matica O je matica pozostávajúca zo samých núl.

Pre každú maticu platí: $A_{m\times n} + O_{m\times n} = O_{m\times n} + A_{m\times n} = A_{m\times n}$

Násobenie matice konštantou c znamená vynásobenie každého prvku danej matice číslom c, t. j. $c \cdot A = (c \cdot a_{ij})_{m\times n}$.

Súčin matíc $A = (a_{ik})_{m\times s}$ a $B = (b_{kj})_{s\times n}$ v poradí $A \cdot B$ je matica $C = (c_{ij})_{m\times n}$, kde $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{is}b_{sj}$.

Vo výslednej matici súčinu je prvok v i-tom riadku a j-tom stĺpci skalárnym súčinom vektora tvoreného i-tym riadkom ľavej matice s vektorom tvoreným j-tym stĺpcom pravej matice.

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1s} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2s} \\ \vdots & \vdots & & \vdots & \\ \boldsymbol{a}_{i1} & \boldsymbol{a}_{i2} & \boldsymbol{a}_{i3} & \dots & \boldsymbol{a}_{is} \\ \vdots & \vdots & & \vdots & \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{ms} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \dots & \boldsymbol{b}_{1j} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & \boldsymbol{b}_{2j} & \dots & b_{2n} \\ b_{31} & b_{32} & \dots & \boldsymbol{b}_{3j} & \dots & b_{3n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{s1} & b_{s2} & \dots & \boldsymbol{b}_{sj} & \dots & b_{sn} \end{pmatrix}$$

Násobenie matíc **nie je komutatívne**. $AB \neq BA$ (vo všeobecnosti)

Násobenie matíc **je asociatívne**. $(AB)C = A(BC)$

Jednotková matica I je štvorcová matica, ktorá má jednotky na hlavnej diagonále a inde nuly.

Pre každú maticu $A_{m\times n}$ platí: $A_{m\times n} \cdot I_{n\times n} = A_{m\times n}$ $\qquad$ $I_{m\times m} \cdot A_{m\times n} = A_{m\times n}$

Transponovaná matica A^T sa získa z matice A výmenou riadkov so stĺpcami, t. j. ak $A = (a_{ij})_{m\times n}$, potom $A^T = (a_{ji})_{n\times m}$.

Inverzná matica k štvorcovej matici A je matica A^{-1} (rovnakého typu), ktorá vyhovuje rovniciam

$A \cdot A^{-1} = I$ a $A^{-1} \cdot A = I$.

Ak inverzná matica k štvorcovej matici A existuje, je jednoznačne určená.

Inverzná matica existuje iba k štvorcovej matici, ktorá po úprave na redukovaný tvar (pomocou ERO 1 - 3) nemá nulové riadky.

Inverznú maticu k matici A hľadáme pomocou Gaussovej eliminačnej metódy aplikovanej na maticu A rozšírenú o jednotkovú maticu.

$$\left(A \mid I\right) \quad \sim \quad \text{(ERO 1 } - \text{ 3)} \quad \sim \quad \left(I \mid A^{-1}\right)$$

Sústavu lineárnych rovníc môžeme riešiť aj pomocou inverznej matice.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad\qquad &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= b_n \end{aligned}$$

Sústavu prepíšeme do maticovej formy

$$A \cdot X = B$$

Riešenie má potom tvar

$$X = A^{-1} \cdot B$$

Matice je tiež možné použiť na **šifrovanie správ**.

Najprv si želaný text prevedieme do číselného tvaru (podľa vopred zvoleného kľúča) a zapíšeme do maticovej formy $T_{m\times n}$. Text zašifrujeme tak, že ho vynásobíme nejakou štvorcovou maticou $S_{m\times m}$, t. j.

$$S \cdot T = Z.$$

Zašifrovanú správu potom rozšifrujeme výpočtom

$$T = S^{-1} \cdot Z.$$

Algebra a diskrétna matematika
Prehľad z 3. týždňa
Transformácie roviny pomocou matíc, determinanty, Cramerovo pravidlo

Pomocou matíc reprezentujeme transformácie v n-rozmerných priestoroch. Ak matica S je maticou súradníc bodov, ktoré zobrazujeme transformáciou pomocou matice T, tak maticu súradníc zobrazených bodov N zvyčajne vypočítame z rovnice

$$T \cdot S = N$$

Špeciálnym prípadom sú transformácie roviny. Medzi ne patria napríklad posunutie, škálovanie alebo otočenie (a iné).

Posunutie roviny
Body $(x_1, y_1), (x_2, y_2), \ldots (x_n, y_n)$ posunieme o vektor (a, b). Súradnice zobrazených bodov $(x'_1, y'_1), (x'_2, y'_2) \ldots (x'_n, y'_n)$ je možné získať dvomi spôsobmi:

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{pmatrix} + \begin{pmatrix} a & a & \ldots & a \\ b & b & \ldots & b \end{pmatrix} = \begin{pmatrix} x'_1 & x'_2 & \ldots & x'_n \\ y'_1 & y'_2 & \ldots & y'_n \end{pmatrix}$$

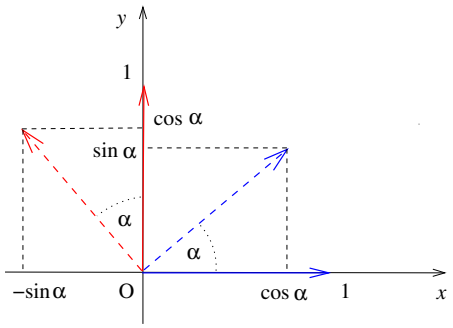
alebo

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \\ 1 & 1 & \ldots & 1 \end{pmatrix} = \begin{pmatrix} x'_1 & x'_2 & \ldots & x'_n \\ y'_1 & y'_2 & \ldots & y'_n \\ 1 & 1 & \ldots & 1 \end{pmatrix}$$

Škálovanie v smere súradnicových osí so stredom v $(0, 0)$
Ak škálovanie v smere x-ovej osi zmeníme faktorom c a v smere oxi y faktorom d, tak nové súradnice dostaneme z rovnice

$$\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{pmatrix} = \begin{pmatrix} x'_1 & x'_2 & \ldots & x'_n \\ y'_1 & y'_2 & \ldots & y'_n \end{pmatrix}$$

Otočenie roviny o uhol α okolo bodu $(0,0)$.



$$(1,0) \longrightarrow (\cos\alpha, \sin\alpha) \qquad (0,1) \longrightarrow (-\sin\alpha, \cos\alpha)$$

Matica otočenia o uhol α

$$O_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Determinant štvorcovej matice M, označovaný ako $|M|$ alebo $\det(M)$, je funkcia, ktorá matici M priradí reálne číslo, pričom platia nasledovné axiómy:

A1: Ak matica N vznikne z matice M **výmenou poradia** dvoch riadkov (stĺpcov), tak $|N| = -|M|$.

A2: Ak matica N vznikne z matice M **vynásobením** niektorého riadku (stĺpca) konštantou k, tak $|N| = k|M|$.

A3: Ak matica N vznikne z matice M **pripočítaním násobku** jedného riadku (stĺpca) k inému riadku (stĺpcu), tak $|N| = |M|$.

A4: Pre **jednotkovú** maticu platí $|I| = 1$.

Takto definovaný determinant je určený **jednoznačne**.

Z definície determinantu sa dajú odvodiť ďalšie vlastnosti:

V1: Ak sa v matici nachádza **nulový riadok** (stĺpec), tak jej determinant je **nulový**.

V2: Ak sa v matici nachádzajú dva **rovnaké riadky** (stĺpce), tak jej determinant je **nulový**.

V3: Determinant hornej (dolnej) **trojuholníkovej** matice sa rovná **súčinu prvkov na hlavnej diagonále**.

V4: Determinant **transponovanej** matice sa rovná determinantu **pôvodnej** matice, tj. $|A| = |A^T|$.

V5: Pre ľubovoľné dve štvorcové matice rovnakého typu platí, že determinant súčinu matíc je súčin ich determinantov, t. j.

$|M \cdot N| = |M| \cdot |N|$

Upozornenie: Determinant súčtu matíc sa nerovná súčtu determinantov!

$|M + N| \neq |M| + |N|$

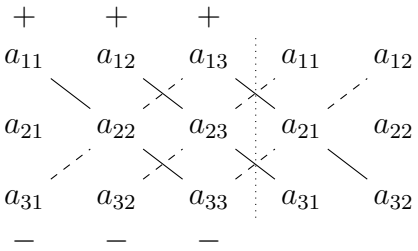
Vzorce na výpočet determinantov rádu $1, 2, 3$:

$$|A_{1\times 1}| = |a_{11}| = a_{11}$$

$$|A_{2\times 2}| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$|A_{3\times 3}| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

Sarrusovo pravidlo na výpočet determinantu matice $A_{3\times 3}$:



Aplikácie determinantov v geometrii

Obsah trojuholníka určeného bodmi (x_1, y_1), (x_2, y_2), (x_3, y_3) je

$$S = \pm\frac{1}{2}\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ 1 & 1 & 1 \end{vmatrix}$$

Objem štvorstena určeného bodmi (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), (x_4, y_4, z_4):

$$V = \pm\frac{1}{6}\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ 1 & 1 & 1 & 1 \end{vmatrix}$$

Rozvoj determinantu podľa riadku alebo stĺpca

Výrazom A_{ij} označujeme maticu typu $(n-1) \times (n-1)$, ktorú dostaneme z matice $A_{n\times n}$ vynechaním i-teho riadka a j-teho stĺpca.

Determinant matice A môžeme potom vypočítať aj pomocou

- rozvoja podľa i-teho riadku

$$|A| = (-1)^{i+1}a_{i1}|A_{i1}| + (-1)^{i+2}a_{i2}|A_{i2}| + \cdots + (-1)^{i+n}a_{in}|A_{in}|$$

- rozvoja podľa j-teho stĺpca

$$|A| = (-1)^{1+j}a_{1j}|A_{1j}| + (-1)^{2+j}a_{2j}|A_{2j}| + \cdots + (-1)^{n+j}a_{nj}|A_{nj}|$$

Determinant a inverzná matica

Štvorcovú maticu A nazývame **regulárnou**, ak $|A| \neq 0$.

K štvorcovej matici A existuje inverzná matica práve vtedy, keď $|A| \neq 0$.

Ak matica A je regulárna, tak

$$|A^{-1}| = \frac{1}{|A|}$$

Ak $|A| = 0$, maticu A nazývame **singulárnou.**

K singulárnej matici neexistuje inverzná matica.

Výpočet inverznej matice pomocou determinantu

Ak A je regulárna matica rádu n a A_{ij} vznikne z A vynechaním i-teho riadku a j-teho stĺpca, potom pre **inverznú** maticu platí

$$A^{-1} = \frac{1}{|A|}(b_{ij})_{n\times n}, \text{ kde} \quad b_{ij} = (-1)^{i+j}|A_{ji}|$$

Matica $(b_{ij})_{n\times n}$ sa nazýva **adjungovaná** a označuje sa adj(A);

$$A^{-1} = \frac{1}{|A|}\text{adj}(A)$$

$$\text{Ak} \quad A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{ tak} \quad A^{-1} = \frac{1}{|A|}\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Cramerovo pravidlo

Ak $AX = B$ je systém pozostávajúci z n lineárnych rovníc o n neznámych taký, že $|A| \neq 0$, potom systém má jediné riešenie.

Toto riešenie má tvar

$$x_1 = \frac{|A_1|}{|A|}, \; x_2 = \frac{|A_2|}{|A|}, \ldots, \; x_n = \frac{|A_n|}{|A|},$$

pričom maticu A_i získame z matice A náhradou i-teho stĺpca stĺpcom pravých strán $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$.

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad zo 4. týždňa

Teória grafov – základné pojmy

Graf je dvojica $G = (V, E)$, kde V je neprázdna množina **vrcholov** a E je nejaká množina dvojprvkových podmnožín V – **hrán**. Niekedy $V = V(G)$, $E = E(G)$.

Príklad: $H = (V, E)$, $V = \{a, b, c, d, e\}$, $E = \{\{a, b\}, \{a, c\}, \{a, e\}, \{d, e\}\}$
Stručnejší zápis množiny hrán: $E = \{ab, ac, ae, de\}$

Grafy znázorňujeme obrázkami v rovine;
vrcholy = body roviny, **hrany** = jednoduché krivky (úsečky, ak je to výhodné) spájajúce príslušné vrcholy.

Grafy môžeme reprezentovať napr. ako vstupy rôznych algoritmov. Najčastejšie používame **zoznam susedov** vrcholov alebo **maticu susednosti**.

1. **Zoznam susedov** $S = S(H)$ pre graf $H = (V, E)$, $V = \{a, b, c, d, e\}$, $E = \{ab, ac, ae, de\}$:
   $a:\ b, c, e$
   $b:\ a$
   $c:\ a$
   $d:\ e$
   $e:\ a, d$

2. **Matica susednosti** $A = (a_{ij})_{n\times n}$ pre graf G s n vrcholmi $V(G) = \{v_1, v_2, \dots v_n\}$ a s hranami $E(G)$ má pre $i, j \in \{1, 2, \dots n\}$ definované prvky nasledovne

$$a_{ij} = \begin{cases} 1 & \text{ak } \{v_i v_j\} \in E(G) \\ 0 & \text{inak} \end{cases}$$

Niektoré jednoduché, ale dôležité príklady grafov:

P_n – **cesta** s n vrcholmi; jej *dĺžka* je $n - 1$ (počet jej hrán)
$V(P_n) = \{v_1, v_2, v_3, \dots, v_n\}$ a $E(P_n) = \{v_1v_2, v_2v_3, v_3v_4 \dots, v_{n-1}v_n\}$

Matica susednosti

$$A(P_n) = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

C_n – **kružnica** (niekedy aj cyklus) rádu n, $(n \geq 3)$

$V(C_n) = \{v_1, v_2, \dots, v_n\}$; $E(C_n) = \{v_1v_2, v_2v_3, v_3v_4 \dots, v_{n-1}v_n, v_nv_1\}$

Matica susednosti

$$A(C_n) = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

K_n – **úplný graf** rádu n (alebo: s n vrcholmi) je graf, v ktorom je každá dvojica vrcholov spojená práve jednou hranou. Matica susednosti má nuly na hlavnej diagonále a inde jednotky.

$K_{m,n}$ – **úplný bipartitný** graf rádu $m+n$ (alebo: s $m+n$ vrcholmi) je graf, v ktorom je množina vrcholov rozdelená do dvoch disjunktných partií, s m a n vrcholmi. Dvojica vrcholov je spojená hranou ak sa vrcholy nachádzajú v rôznych partiách.

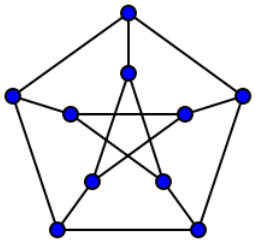
$V(K_{m,n}) = V_m \cup W_n$

$E(K_{m,n}) = \{v_iw_j; v_i \in V_m, i \in \{1, 2, \dots m\}, w_j \in W_n, j \in \{1, 2, \dots, n\}\}$

Matica susednosti je zložená z dvoch nulových blokov a dvoch blokov so samými jednotkami.

Koktailový graf rádu n (alebo: s $2n$ vrcholmi) pozostáva z n párov vrcholov, pričom každá dvojica vrcholov je spojená hranou okrem vrcholov tvoriacich páry.

Petersenov graf



Obyčajný graf je graf, ktorý nemá násobné hrany ani slučky. (Zatiaľ budeme pracovať len s nimi.)

Stupeň vrchola $v \in V(G)$ je počet hrán **incidentných** s vrcholom v. Označuje sa $\deg(v)$.

Pravidelný graf stupňa d je graf, ktorý má všetky stupne rovnaké (d).

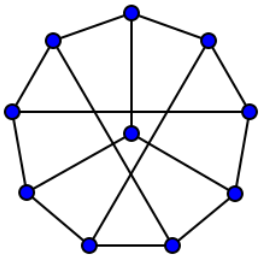
Známy fakt: V každom konečnom grafe platí:

$$\sum_{v \in V} \deg(v) = 2|E|$$

Tvrdenie: Každý konečný obyčajný graf má párny počet vrcholov nepárneho stupňa.

Izomorfizmus grafov: Dva grafy $G = (V, E)$ a $G' = (V', E')$ sú **izomorfné**, ak existuje vzájomne jednoznačné zobrazenie (bijekcia) $f : V \to V'$ také, že pre každú dvojicu vrcholov $u, v \in V$ platí: $\{u, v\} \in E$ práve vtedy, keď $\{f(u), f(v)\} \in E'$.

Nasledujúci graf je izomorfný Petersenovmu grafu:



Ak $G = (V, E)$, tak jeho **komplement** je graf $\overline{G} = (V, \overline{E})$, kde $\overline{E}$ je doplnok E v množine $V^{(2)}$ *všetkých* 2-prvkových podmnožín V.

Graf sa nazýva **samokomplementárny**, ak je izomorfný svojmu komplementu.

$G' = (V', E')$ je **podgraf** grafu $G = (V, E)$, ak $V' \subset V$ a $E' \subset E$. Tento podgraf je **indukovaný**, ak $E' = E \cap V'^{(2)}$.

Graf G je **súvislý**, ak každé jeho dva vrcholy sú spojené cestou v G.

Vzdialenosť $d(u, v)$ vrcholov $u, v \in V(G)$ v súvislom grafe G je dĺžka *najkratšej* cesty spájajúcej u a v.

Priemer $\mathrm{diam}(G)$ súvislého grafu G je *najväčšia* vzdialenosť "nameraná" v G: $\mathrm{diam}(G) = \max\{d(u, v);\ u, v \in V(G)\}$.

Obvod $g(G)$ grafu G je dĺžka najmenšej kružnice v grafe G.

Problém motivovaný navrhovaním sietí:
Máme navrhnúť sieť tak, aby jeden uzol bol pevnou linkou spojený s najviac 3 inými, ale aby ľubovoľná dvojica nespojených uzlov bola pevnými spojmi dosiahnuteľná len cez jeden uzol. Aký najväčší počet uzlov môže taká sieť mať?

Grafová formulácia: Aký najväčší rád má graf priemeru 2 s maximálnym stupňom vrchola $d \leq 3$?

Odpoveď po malom experimentovaní je Petersenov graf.

Aký **najväčší rád** n má graf priemeru 2 s maximálnym stupňom vrchola $d \geq 4$?

• Pre stupeň $d = 4$: $n = 15$

• Pre stupeň $d = 5$: $n = 24$ - ťažké !

• Pre stupeň $d = 6$: Odpoveď nepoznáme! Najlepšia známa hodnota je 32 vrcholov.

• Pre stupeň $d = 7$: $n = 50$ – veľmi slávny Hoffman-Singletonov graf.

• Pre stupne $d > 7$: Slávny otvorený problém – maximum nepoznáme pre žiadnu hodnotu $d > 7$.

Graf je **rovinný**, ak ho je možné znázorniť v rovine tak, aby žiadne 2 krivky reprezentujúce jeho hrany nemali spoločný bod, ktorý by bol vnútorným bodom jednej z nich.

Oblasti rovinnej realizácie $\mathcal{G}$ rovinného grafu G v R^2 sú súvislé komponenty množiny $R^2 \setminus \mathcal{G}$.

Eulerov vzorec: V súvislom rovinnom grafe s n vrcholmi, h hranami a o oblasťami platí $n - h + o = 2$.

Dôkaz: Indukciou* podľa počtu hrán h grafu G

Ak $h = 0$, potom $n = 1$, $o = 1$ a vzorec platí.

1. Veta platí pre súvislé grafy bez kružníc.

2. Uvažujme rovinný graf G, ktorý obsahuje kružnicu, napr. C. Nech e je hrana v C; potom $G - e$ vzniknutý z G odstránením e ostane súvislý, ale odstránenm hrany sa spoja dve oblasti do jednej. Teda pre rovinný graf $G-e$ s n vrcholmi, $h-1$ hranami a $o-1$ oblasťami podľa indukčného predpokladu platí $n - (h - 1) + (o - 1) = 2$. Ale potom triviálne $n - h + o = 2$.

Použitím Eulerovho vzorca sa dá ukázať, že grafy K_5 a $K_{3,3}$ nie sú rovinné. To isté platí pre Petersenov graf.

Graf H je **homeomorfný** grafu G, ak H vznikne z G nahradením ľubovoľnej podmnožiny hrán cestami (ľubovoľnej dĺžky).

Podgraf rovinného grafu je rovinný.

Kuratowského veta (1930): Graf je rovinný práve vtedy, keď neobsahuje podgraf homeomorfný grafu K_5 alebo $K_{3,3}$. (Slávny výsledok).

*** Dôkaz matematickou indukciou**

Matematickou indukciou dokazujeme tvrdenia, ktoré platia pre všetky *prirodzené čísla* alebo pre určitú *nekonečnú postupnosť*.

Tvrdenie: Pre každé prirodzené číslo $n \geq k_0$ platí $T(n)$.

Dôkaz sa skladá z dvoch krokov:

1. Báza:
Ukážeme, že tvrdenie platí pre najmenšie číslo z postupnosti, tj. dokazujeme platnosť $T(k_0)$.

2. Indukčný krok:
Ukážeme, že pre ľubovolné $k \geq k_0$ z platnosti $T(k)$ vyplýva platnosť $T(k+1)$.

Predpoklad platnosti $T(k)$ sa nazýva *indukčný predpoklad*.

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z 5. týždňa

Nerovinné grafy, ofarbenia grafov, stromy, kostry a ich konštruktívna enumerácia, ohodnotenia grafov

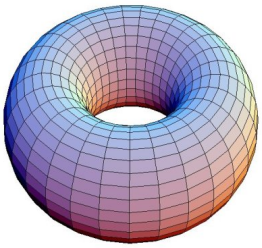
Graf je **rovinný**, ak ho je možné znázorniť v rovine tak, aby žiadne 2 krivky reprezentujúce jeho hrany nemali spoločný bod, ktorý by bol vnútorným bodom jednej z nich.

Graf, ktorý nie je rovinný sa nazýva **nerovinný (neplanárny)**.

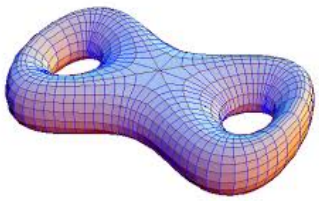
Z minula vieme, že grafy K_5, $K_{3,3}$ a Petersenov graf sú nerovinné.

Nerovinné grafy sa dajú nakresliť tak, aby sa ich hrany nepretínali vo svojich vnútorných bodoch v R^3 alebo na vhodných **plochách**.

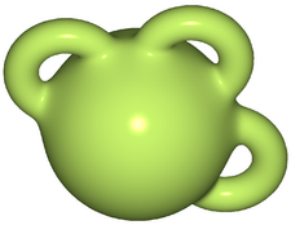
Príklady niektorých plôch:



Torus



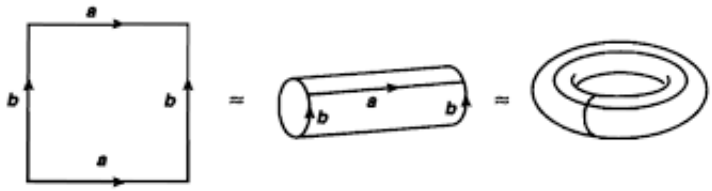
Dvojitý torus



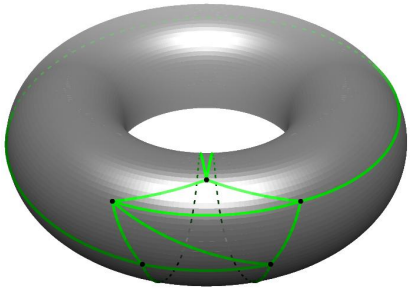
Trojitý torus

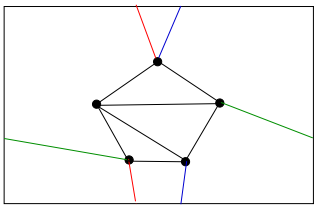
Tvrdenie: Každý graf je možné nakresliť bez priesečníkov na guľu s dostatočným počtom "uší".

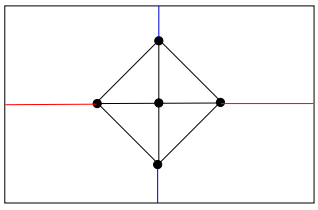
Zostrojenie torusu

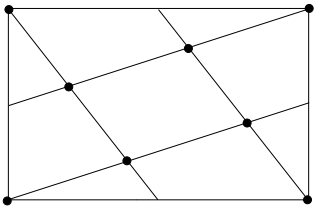


Príklad: Rôzne spôsoby umiestnenia úplného grafu K_5 na toruse.









Vrcholové ofarbenie grafu G je zobrazenie $f : V(G) \to \{1, 2, \ldots, k\}$ také, že pre každú $uv \in E(G)$ je $f(u) \neq f(v)$ (susedné vrcholy dostanú rôzne farby).

Najmenšie také k je **chromatické číslo** $\chi(G)$ grafu G.

Príklad: Chromatické číslo Petersenovho grafu je 3.

Hranové ofarbenie grafu je priradenie k farieb hranám grafu, pričom hrany incidentné s rovnakým vrcholom dostanú rôzne farby.

Najmenšie také k je **chromatický index** (hranové chromatické číslo) $\chi'(G)$ grafu G.

Príklad: Chromatický index Petersenovho grafu je 4.

Veta o 5 farbách: Pre každý konečný rovinný graf platí, že $\chi(G) \leq 5$.

Pomerne jednoduchý dôkaz indukciou podľa počtu vrcholov bol prezentovaný na prednáške (aj s ilustráciou). Využíva sa tam fakt, že v rovinnom grafe existuje vrchol stupňa nanajvýš 5.

Slávny problém – Formulovaný r. 1852 – Francis Guthrie

Problém 4 farieb Pre každý konečný rovinný graf platí, že $\chi(G) \leq 4$.

1976 – Appel a Haken - prvý dôkaz, nie všetkými matematikmi prijatý

1996 – Robertson, Sanders, Seymour, Thomas - všeobecne prijatý dôkaz

Významná aplikácia: Globálny systém mobilných aplikácií operuje iba na 4 rôznych frekvenciách.

Strom je súvislý graf neobsahujúci kružnicu.

Nesúvislý graf bez kružníc sa nazýva **les**.

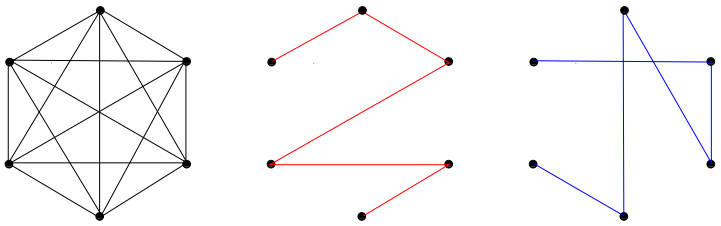
List grafu je vrchol stupňa jeden.

Hviezda je strom, ktorý má práve jeden vrchol stupňa aspoň 3 a všetky ostatné vrcholy majú stupeň 1.

Húsenica je strom, v ktorom po odstránení listov (vrcholov stupňa 1) ostane iba cesta.

Kostra grafu G je strom, ktorý je jeho podgrafom a obsahuje všetky vrcholy grafu G.

Príklad dvoch rôznych, ale izomorfných kostier grafu K_6



Cayleyho veta: Pre každé $n \geq 2$ je počet všetkých kostier úplného grafu K_n (počet stromov na daných n vrcholoch) rovný n^{n-2}.

Hlavné myšlienky dôkazu

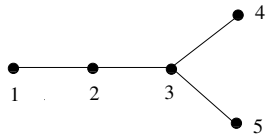
Ukážeme, že každú kostru K_n vieme zakódovať $(n-2)$-člennou postupnosťou čísel z množiny $\{1, 2, \ldots, n\}$. Také kódovanie definuje bijekciu medzi všetkými kostrami a všetkými postupnosťami tohto typu. Z toho vyplýva, že počet všetkých kostier je n^{n-2}.

Uvažujme kostru T grafu K_n s vrcholmi označenými číslami $1, 2, \ldots, n$.

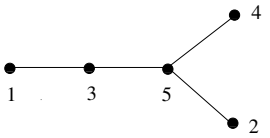
Kostre T priradíme **Prüferov kód** $P(T) = (p_1, p_2, \ldots, p_{n-2})$ nasledovne:

- Z kostry postupne odstraňujeme listy, až kým neostane jedna hrana.
- V každom kroku odstránime list s najmenším číslom.
- Do postupnosti pridáme číslo vrchola, ktorý je susedom odstráneného listu.

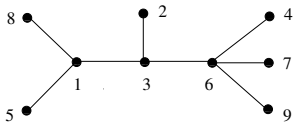
Príklad:



$P = (2, 3, 3)$



$P = (3, 5, 5)$



$P = (3, 6, 1, 6, 1, 3, 6)$

Spätná rekonštrukcia kostry

Uvedomme si najprv, že každý vrchol, ktorý nie je v P, je list.

Prvý vrchol bol odstránený list, ktorý susedil s prvým vstupom p_1 v P a mal najmenšie číslo ℓ_1 nevyskytujúce sa v P.

Ako druhý bol odstránený list susediaci s druhým vstupom p_2 v P a s najmenším číslom nevyskytujúcim sa v $P - \{p_1\}$ a rôznym od ℓ_1.

V ďalšom kroku budeme podobne vyšetrovať kód o dva vstupy kratší. Tak pokračujeme ďalej.

Po $n-2$ krokoch prejdeme celý kód. Ostáva určiť poslednú hranu. Jeden jej koniec je posledný vstup p_{n-2} v kóde P a druhý ten, ktorý sa nevyskytuje medzi odstránenými listami $\ell_1, \ldots \ell_{n-2}$ a je rôzny od p_{n-2}.

Algoritmus spätnej rekonštrukcie kostry

Vstup: Prüferov kód $P = (p_1, p_2, \ldots p_{n-2})$

Algoritmus

- Krok 1: Nakresli n vrcholov a označ číslami od 1 do n.
- Krok 2: Zostav **zoznam** čísel $Z = (1, 2, \ldots, n)$.
- Krok 3: Ak sú v zozname dve čísla, spoj vrcholy s týmito číslami hranou a ukonči, inak prejdi na Krok 4.
- Krok 4: Nájdi najmenšie číslo v zozname, ktoré nie je v kóde a prvé číslo v kóde. Spoj vrcholy s týmito číslami hranou.
- Krok 5: Vymaž čísla z Kroku 4 zo zoznamu aj z kódu. Choď na Krok 3.

Dá sa ukázať, že vzniknutý graf je vždy strom a že spätným prekódovaním dostaneme pôvodný kód.

Vrcholovo ohodnotený graf je graf, v ktorom sú vrcholom priradené čísla z nejakej množiny (tradične, $1, 2, ...$) .

Hranovo ohodnotený graf je graf, v ktorom sú hrany ohodnotené číslami $1, 2, ...$

Graciózne ohodnotenie (graceful labeling) stromu rádu n je ohodnotenie jeho vrcholov číslami $1, 2, \ldots, n$ tak, aby absolútne rozdiely ohodnotení susedných vrcholov vyčerpali celú množinu $\{1, 2, \ldots, n-1\}$.

Ringel-Kotzigova hypotéza: Každý strom má graciózne ohodnotenie.

Hypotéza je stále otvorená.

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad zo 6. týždňa

Prehľadávacie algoritmy, minimálna kostra, eulerovské grafy, hamiltonovské kružnice

Prehľadávanie grafov

Často v grafoch chceme zistiť určitú vlastnosť (napr. súvislosť, priemer, maximálny stupeň, existenciu kružníc, atď). Zo zoznamu susedov alebo matice susednosti to nie je ľahké hneď identifikovať. Mnohé takéto úlohy si preto vyžadujú efektívne a systematické preskúmanie grafu, kedy postupne navštevujeme všetky vrcholy a hrany grafu.

Uvedieme neformálny opis dvoch najviac používaných metód podľa spôsobu prehľadávania.

Prehľadávanie grafu do hĺbky (depth-first search DFS) Hlavná myšlienka tohto prehľadávania je, že postupujeme cez susedov vrcholov tak hlboko, ako je možné.
Začneme prehľadávanie vo zvolenom vrchole, navštívime jedného jeho suseda, potom suseda tohto suseda, atď. Ak sa ďalej takto nedá pokračovať a ešte existujú nenavštívené vrcholy, tak postupujúc naspäť nájdeme prvý vrchol s ešte nenavštíveným susedom a opakujeme postup, až kým nepreskúmame všetky vrcholy.

Prehľadávanie grafu do šírky (breadth-first search BFS) V tomto prípade najprv skúmame zvolený vrchol a potom všetkých jeho susedov, potom všetkých susedov týchto susedov, atď, kým nenavštívime všetky vrcholy grafu (prípadne komponentu). Algoritmus prechádza vrcholy podľa vzrastajúcej vzdialenosti od zvoleného vrchola. Je preto vhodný na nájdenie najkratšej cesty medzi zvoleným vrcholom a ľubovoľným iným vrcholom.

V oboch algoritmoch každá hrana dostane šípku označujúcu smer jej prvého prechodu. Hrany rozdeľujeme na stromové, ak nás dovedú k novým vrcholom, a inak na spätné.

Výstupom oboch algoritmov je (DFS alebo BFS) kostra v každom komponente súvislosti a usporiadanie vrcholov v poradí, v akom boli navštívené.

Problém minimálnej kostry: Pre súvislý graf $G = (V, E)$ s kladným ohodnotením hrán w nájdite kostru $T = (V, E')$ grafu G s najmenšou možnou hodnotou $w(T)$.

Kruskalov algoritmus: Minimálnu kostru v grafe konštruujeme postupným pridávaním hrán s najmenšou váhou tak, aby sme nevytvorili žiaden cyklus.
Vstup: Súvislý hranovo ohodnotený graf $G = (V, E)$ s n vrcholmi

Výstup: Podmnožina hrán $A \subseteq E$ taká, že graf (V, A) je minimálna kostra grafu G.

Algoritmus

• Krok 1: Polož $A = \emptyset$.

• Krok 2: Polož $F = E$.

• Krok 3: Ak F=$\emptyset$ alebo graf (V, A) je strom, ukonči, inak choď na Krok 4.

• Krok 4: Odstráň z množiny F hranu e s minimálnym ohodnotením (ak ich je viac, začni ľubovoľnou z nich). Ak graf $(V, A \cup \{e\})$ neobsahuje kružnicu, pridaj hranu e do množiny A. Choď na Krok 3.

Eulerovské grafy

Úloha: Nakreslite daný graf jedným uzavretým ťahom bez zdvihnutia tužky z papiera, pričom žiadna hrana sa neobkreslí viackrát.

Uzavretý eulerovský ťah v grafe je uzavretý sled hrán a vrcholov, v ktorom sa každá hrana vyskytuje práve raz a každý vrchol aspoň raz.

Graf je **eulerovský** práve vtedy, keď má aspoň jeden uzavretý eulerovský ťah.

Charakterizácia eulerovských grafov: Graf je eulerovský práve vtedy, keď je súvislý a všetky jeho vrcholy sú párneho stupňa.

Mostom grafu $G = (V, E)$ je taká hrana $e \in E$, pre ktorú platí, že graf $G - e$ má väčší počet komponentov ako graf G.

Tvrdenie: Ak má graf všetky vrcholy párneho stupňa, tak neobsahuje most.

Pred opisom algoritmu na generovanie eulerovských ťahov najprv opíšeme procedúru Proc(H, u), ktorá v súvislom eulerovskom grafe H vygeneruje *nejaký* uzavretý ťah T začínajúci a končiaci vo vrchole u grafu H:

Proc(H, u): Vyberieme ľubovoľnú hranu $e_1 = uv_1$ v H (taká musí existovať) a vytvoríme graf H_1 vynechaním hrany e_1 z grafu H; symbolicky, $H_1 = H - e_1$. Postup iterujeme, t.j. vyberieme ľubovoľnú hranu $e_2 = v_1v_2$ (taká musí existovať, pretože stupeň vrchola v_1 v novom grafe H_1 je nepárny – a zároveň $e_2 \neq e_1$, pretože e_1 už nie je v H_1) a vytvoríme graf $H_2 = H_1 - e_2$. Takto pokračujeme, až kým znova "narazíme" na vrchol u. To sa v niektorom kroku *musí* stať – t.j. niekde v i-tom kroku sa dostaneme do situácie, kedy v práve navštívenom vrchole v_{i-1} vyberieme hranu $e_i = v_{i-1}u$ "končiacu" vo vrchole u. Zostrojený *uzavretý* ťah $ue_1v_1e_2v_2 \dots v_{i-1}e_iu$ označíme symbolom T; ten bude tvorit' výstup našej procedúry.

Algoritmus vygenerovania eulerovského ťahu v eulerovskom grafe

Vstup: eulerovský graf $G = (V, E)$
Výstup: eulerovský ťah T
Algoritmus:

- Krok 1: Polož $H = G$.
- Krok 2: Polož $T = \emptyset$.
- Krok 3: Spusť Proc$(\tilde{H}, u)$ v nejakom súvislom komponente $\tilde{H}$ grafu H v nejakom vrchole $u \in H \cap T$ (ak $T = \emptyset$, $u \in H$), výstup označ T'
- Krok 4: Za T polož $T \cup T'$; t.j. ak $T = v_0e_1v_1 \dots e_rue_{r+1} \dots e_iv_0$ a $T' = uf_1 \dots f_su$, tak nové $T = v_0e_1v_1 \dots e_ruf_1 \dots f_sue_{r+1} \dots e_iv_0$.
- Krok 5: Za H polož $H - E(T')$.
- Krok 6: Ak $H = \emptyset$, ukonč, inak choď na Krok 3.

Hovoríme, že graf G s párnym počtom vrcholov $2n$ má **perfektné párovanie**, ak G obsahuje n nezávislých hrán (žiadne 2 nemajúce spoločný vrchol).

Veta (König, 1916): Každý pravidelný bipartitný graf s aspoň jednou hranou má perfektné párovanie.

Veta (Petersen, 1891) Každý pravidelný graf stupňa 3 bez mostov má perfektné párovanie. (Tu graf nemusí byť bipartitný!)

Problém obchodného cestujúceho
Nech v grafe G vrcholy reprezentujú mestá a hrany cesty medzi mestami. Problém obchodného cestujúceho spočíva v určení trasy začínajúcej a končiacej v tom istom meste, pričom cestujúci každé iné mesto navštívi práve raz a súčet prejdených vzdialeností (resp. nákladov, resp. časov) bude minimálny možný.

Kružnica v G je **hamiltonovská**, ak obsahuje všetky vrcholy grafu G.

Ekvivalentná formulácia problému obchodného cestujúceho: Nájsť v grafe G s kladne ohodnotenými hranami hamiltonovskú kružnicu s najmenším celkovým ohodnotením.

Algoritmy na hľadanie optimálnej hamiltonovskej kružnice sú veľmi komplikované. Nateraz sa uspokojíme s **heuristikou**, t.j. procedúrou, ktorá nájde hamiltonovskú kružnicu s "rozumne malým" ohodnotením.

Budeme uvažovať o ohodnotenom *úplnom* grafe G (aby sme sa vyhli problému existencie hamiltonovskej kružnice), pričom pre (kladné) ohodnotenie w hrán predpokladáme pre každú hranu uv **trojuholníkovú nerovnosť:**
$w(uv) \leq w(ux) + w(xv)$, pre každý vrchol x.

Heuristika zdvojenej kostry.

- Pomocou Kruskalovho algoritmu nájdeme v G najlacnejšiu kostru T.
- Na T vytvoríme uzavretý sled S, ktorý každú hranu T prejde 2-krát.
- Pomocou S budujeme kružnicu C z ľubovoľného vrchola u rekurzívne:

1. Vydáme sa z u v smere sledu S, až kým nie sme nútení prejsť nejakou hranou v opačnom smere, t.j. keď $S = u...vwv....$ Vezmeme dočasne $C = u...vw$.

2. Pokračujeme v traverzovaní sledu S, tentoraz z vrchola w, až po prvý výskyt nejakého vrchola x (čiže teraz $S = u...vwv...x...$), ktorý nie je v našej dočasnej C; do C pridáme vrchol x a hranu wx. Ak taký x nie je, tak bola prejdená celá trasa S; do C pridáme hranu wu a skončíme.

3. Ak $S = u...vwv...xy...$ a $y \notin C$, budujeme ďalej C ako v 1 (x preberie rolu vrchola u v bode 1); ak $y \in C$ (a teda xy je prejdená druhýkrát), pokračujeme ako v 2 (x preberie rolu vrchola w v bode 2).

Z trojuholníkovej nerovnosti máme $w(C) \leq 2 \cdot w(T)$, čo považujeme za "rozumne malé".

Algoritmická zložitosť – neformálny výklad

Príklady algoritmických riešení problémov: Zostrojiť kostru daného grafu, alebo rozhodnúť, či daný graf je súvislý, alebo či je hamiltonovský.

V prvom prípade žiadame, aby výstupom algoritmu bol *objekt* – tu graf (kostra), zatiaľ čo v ďalších dvoch prípadoch výstupom algoritmu je len jedna z 2 možných odpovedí: ÁNO – NIE. Takýmto problémom hovoríme *rozhodovacie*.

Uvedomte si, že graf, v ktorom potrebujeme niečo nájsť alebo o ňom urobiť nejaké rozhodnutie, môže mať tisíce vrcholov, je na vstupe algoritmu v podobe napr. zoznamu vrcholov a ich susedov, a najmä to, že počítač ho nevidí!

Odteraz budeme uvažovať len rozhodovacie problémy. Opíšeme základný pojem zložitosti rozhodovacieho problému; na podanie presnej definície zatiaľ nemáme vybudovaný matematický aparát a dozviete sa ju neskôr v špeciálnych predmetoch.

Neformálne, pod **zložitosťou** algoritmického problému budeme rozumieť počet "krokov" $f(n)$, ktoré algoritmus v najhoršom prípade vykoná, aby na výstupe dal odpoveď ÁNO alebo NIE, ak "dĺžka vstupu je n".

"Krok"? Napríklad, v opise algoritmu na prehľadávanie grafu to môže byť inštrukcia 'vezmi ďalší vrchol (hranu) zo zoznamu". V podrobnejšom opise (pseudokóde) to môže byť séria pokynov typu:

(1) Pozri, či vrchol číslo i už bol navštívený.

(2) Ak áno, zvýš honotu i na $i + 1$ a vráť sa na (1).

(3) Ak nie, pridaj i do zoznamu prejdených vrcholov a choď na (5).

Atď...

"Krok" v opise algoritmu: $\leq$ *konštantne veľa* "krokov" v pseudokóde.

"Krok" v pseudokóde: $\leq$ *konštantne veľa* "krokov" v program. jazyku.

"Krok" v program. jazyku: $\leq$ *konštantne veľa* inštrukcií v stroj. kóde.

Inštrukcia v strojovom kóde: $\leq$ *konštantne veľa* taktov procesora.

Ak máme prehľadať napr. n-vrcholovú cestu a prejsť každý vrchol, tak:

v opise algoritmu musíme urobiť n "krokov";

v pseudokóde to bude viac, ale nie viac ako napr. $5 \cdot n$ krokov,

v strojovom kóde nie viac ako (povedzme) $4 \cdot 5 \cdot n$ krokov,

a celkove (povedzme) nie viac ako $5 \cdot 4 \cdot 5 \cdot n$ taktov.

Či už počet krokov meriame pomocou opisu algoritmu alebo pomocou taktov procesora, dostávame síce rôzne čísla – n a $100n$ – ale stále je to konštanta krát n, kde konštanta závisí od mašiny a implementácie.

V informatike túto situáciu zapíšeme symbolom $O(n)$. Ak teda $f(n)$ z opisu zložitosti je počet "krokov" nutných na prejdenie všetkých n vrcholov, tak by sme napísali $f(n) = O(n)$, čo formálne znamená, že $f(n) \leq cn$ pre nejakú konštantu c a pre všetky n. (V tej konštante je zahrnutá naša diskusia o počte krokov.)

Podobne budeme hľadieť na pojem "dĺžka vstupu". Či už je to zoznam vrcholov, ako ho máme na papieri, alebo prekódovaný na postupnosť núl a jednotiek, vždy v prípade napr. cesty na n vrcholoch môžme rovnako dobre povedať, že vstup má dĺžku $O(n)$.

Obvykle sa symbol O používa len na zložitosť, a nie na dĺžku vstupu (to je potom zahrnuté v "narábaní s multiplikatívnymi konštantami").

Matematika má na presné definície týchto pojmov prostriedky – tzv. Turingov stroj; opis jeho činnosti sa dozviete neskôr na špecializovaných prednáškach. Zatiaľ vystačíme s naznačenými intuitívnymi pojmami.

Príklad: Rozhodovací problém zistiť či graf s n vrcholmi a m hranami, zadaný na vstupe, je súvislý. Vzhľadom na našu diskusiu môžeme predpokladať, že dĺžka vstupu je $2m + n$. Počet krokov prehľadávacieho algoritmu je $O(2m + n)$, pretože každú hranu navštívime najviac dva razy.

Niekedy sa zložitosť udáva *len* v terminológii počtu vrcholov n grafu. Keďže $m \leq n(n-1)/2$, môžeme jednoducho povedať, že zložitosť prehľadávacieho algoritmu je nanajvýš $O(n^2)$. Podstatné je, že n^2 je *polynóm* v premennej n. Je to rastúca funkcia, ale nie "divoko" rastúca.

Algoritmy, ktoré na rozhodovacie problémy o grafoch s n vrcholmi dajú odpoveď ÁNO alebo NIE a spotrebujú pri tom najviac $O(n^k)$ krokov pre *konštantné* k, sa nazývajú **polynomiálne**, alebo **patriace do triedy** P.

Príklady: Určenie, či priemer grafu je $\leq d$ pre dané d, rozhodnutie, či graf má perfektné párovanie, alebo či daný graf je rovinný, atď.

Je však celý rad rozhodovacích problémov, na ktoré zatiaľ nepoznáme žiaden polynomiálny algoritmus.

Príklady: Rozhodnúť, či daný graf s n vrcholmi na vstupe je hamiltonovský, alebo či jeho chromatické číslo je $\leq \ell$ pre ľubovoľné *konštantné* $\ell \geq 3$.

Aj tie najlepšie známe algoritmy na tieto úlohy dokážu spracovať vstupný graf s n vrcholmi v najlepšom prípade až po $O(c^n)$ krokoch, kde $c > 1$

V informatike sa skúma celá trieda takýchto problémov, ktoré možno "rýchlo" – v polynomiálnom čase – pretransformovať jeden na druhý, a v konečnom dôsledku na rozhodnutie, či daný n-vrcholový graf na vstupe je hamiltonovský.

Tejto triede problémov sa hovorí **NP-úplné problémy**. Ich definícia vysoko presahuje túto prednášku (NP znamená *nedeterministické polynomiálne*).

Rozdiel medzi zložitosťou napr. $O(n^3)$ a $O(2^n)$: Ak napr. $n = 400$, tak (až na multiplikatívnu konštantu) porovnávame 400^3 s 2^{400}; to druhé je viac, ako fyzikmi odhadovaný počet elementárnych častíc vo vesmíre!

P-NP problém: Jeden z najslávnejších problémov v súčasnosti zo zoznamu 7 miléniových problémov Clayovho matematickéeho inštitútu, USA. Vyriešenie každého z nich je dotovaný miliónom USD! (Jeden z nich už je vyriešený.)

P-NP problém je otázka, či P=NP;
v ekvivalentnej formulácii, či existuje algoritmus polynomiálnej zložitosti na rozhodnutie, či ľubovoľný daný n-vrcholový graf je hamiltonovský. (Vzhľadom na ekvivalentnosť v triede NP-úplných problémov by kladná odpoveď znamenala existenciu polynomiálnych algoritmov pre *všetky* NP-úplné problémy.)

Verí sa, že P≠NP, ale nikto to nevie dokázať! Tu je významný problém *izomorfizmu* grafov: Rozhodnúť, či dva n-vrcholové grafy na vstupe sú izomorfné. Zatiaľ nepoznáme žiaden polynomiálny algoritmus na tento problém, ale na druhej strane ani nikto nevie dokázať, že je NP-úplný!

Predpokladá sa, že ide o problém, ktorý striktne medzi P a NP! Ak by to niekto dokázal, tak by zároveň vyriešil aj P-NP problém.

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad zo 7. prednášky

Kombinatorika

Kombinatorika sa zaoberá konečnými množinami, ich štruktúrami, usporiadaním, rozkladom na menšie objekty, zobrazeniami medzi nimi, usporiadanými n-ticami, atď.

Tvrdenie 1: Ľubovoľná n-prvková množina má práve 2^n podmnožín.

Odvodenie: Nech $A = \{a_1, a_2, a_3, \ldots, a_n\}$.

Každú podmnožinu B množniny A môžeme reprezentovať pomocou n-tice 0 a 1, pričom

na i-tej pozícii je $\begin{cases} 1 & \text{ak} \quad a_i \in B \\ 0 & \text{ak} \quad a_i \notin B \end{cases}$

Napr. $B = \{a_1, a_3, a_4\}$ reprezentujeme postupnosťou $(1, 0, 1, 1, 0 \ldots, 0)$

Každá podmnožina množiny A má jednoznačnú reprezentáciu pomocou n-tice núl a jednotiek. Celkový počet rôznych n-tíc núl a jednotiek je 2^n, čo je aj hľadaný počet všetkých podmnožín množiny veľkosti n. □

Tvrdenie 2: Každá n-prvková množina má práve 2^{n-1} podmnožín nepárnej veľkosti a 2^{n-1} podmnožín párnej veľkosti.

Odvodenie: Nech A je n-prvková množina a prvok $a \in A$.

Z predchádzajúceho tvrdenia vieme, že počet všetkých podmnožín množiny $A - \{a\}$ je 2^{n-1}.

Vyberme si ľubovoľnú z nich, $B \subseteq A - \{a\}$.

Ak B má nepárny počet prvkov, je to aj želaná podmnožina množiny A s nepárnym počtom prvkov.

Ak B má párny počet prvkov, pridáme k nej prvok a.
Potom $B \cup \{a\} \subseteq A$ a veľkosť $|B \cup \{a\}|$ je nepárna.

Našli sme bijekciu medzi množinou všetkých podmnožín $A - \{a\}$ a množinou všetkých podmnožín A nepárnej veľkosti. Je ich 2^{n-1}.

Doplnok k nim sú všetky podmnožiny párnej veľkosti: $2^n - 2^{n-1} = 2^{n-1}$. □

Príklad 1: Aký je počet podmnožín množiny $\{1, 2, \ldots, n\}$, ktoré obsahujú všetky nepárne čísla $\leq n$?

$$2^{\lceil \frac{n}{2} \rceil}$$

Príklad 2: Koľkými spôsobmi je možné rozdeliť množinu $\{1, 2, \ldots, n\}$ na 2 disjunktné podmnožiny, ak nezáleží na poradí podmnožín?

$$2^{n-1} - 1$$

Variácie k-tej triedy z n prvkov s opakovaním

- všetky možné usporiadané výbery k prvkov z n prvkov, pričom vo výberoch sa prvky *môžu opakovať*
- všetky zobrazenia z k-prvkovej množiny do n-prvkovej množiny
- počet slov dĺžky k nad abecedou z n písmen

Ich počet je

$$\mathbf{V^*(n, k) = n^k}$$

Na každú "pozíciu" 1, 2, ..., k možno vybrať ktorýkoľvek z n prvkov.

Príklad 3: Koľko rôznych PIN-kódov si môžete zvoliť pre bankovú kartu?

$$V^*(10, 4) = 10000$$

Príklad 4: Koľko rôznych kódov dĺžky 5 môžete vytvoriť z písmen A, E, I, O, U, Y?

$$V^*(6, 5) = 6^5 = 7776$$

Príklad 5: Koľko existuje rôznych ŠPZ vozidiel ku každému označeniu mesta? (Trojčíslie 000 sa nevyužíva.)

$$(V^*(10, 3) - 1) \cdot V^*(26, 2) = 999 \cdot 26^2 = 675324$$

Príklad 6: Koľko párnych 5-ciferných čísel môžeme napísať z cifier $0, 1, 2, 3, 4, 5, 6$?

$$6 \cdot 7 \cdot 7 \cdot 7 \cdot 4 = 8232$$

Variácie k-tej triedy z n prvkov bez opakovania

• všetky možné usporiadané výbery *navzájom rôznych* k prvkov z n prvkov

• všetky *prosté* zobrazenia z k-prvkovej množiny do n-prvkovej množiny

• počet slov dĺžky k z navzájom rôznych písmen nad abecedou z n písmen

Ich počet je

$$\mathbf{V(n,k) = n(n-1)...(n-(k-1)) = \frac{n!}{(n-k)!}}$$

Na "pozície" 1, 2, ..., k možno postupne vybrať ktorýkoľvek z n prvkov na pozíciu 1, ktorýkoľvek zo zvyšných $n-1$ prvkov na pozíciu 2, atď, až napokon (keď už aj $(k-1)$-vá pozícia je obsadená) ktorýkoľvek zo zvyšných $(n-(k-1))$ prvkov na pozíciu k.

Príklad 7: Koľko rôznych 5-písmenových slov sa dá zostaviť z písmen slova VYHRAŤ, ak sa žiadne neopakuje?

$$V(6,4) = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$$

Príklad 8: Koľko rôznych umiestnení na prvých troch miestach je možných v súťaži s 10 účastníkmi?

$$V(10,3) = 10 \cdot 9 \cdot 8 = 720$$

Príklad 9: Koľko je rôznych 4-ciferných párnych čísel, v ktorých sú všetky cifry rôzne?

$$8 \cdot 8 \cdot 7 \cdot 4 + 9 \cdot 8 \cdot 7 \cdot 1 = 2296$$

Permutácia n prvkov

• *variácia* n-tej triedy z n prvkov bez opakovania

• ľubovoľná *bijekcia* n-prvkovej množiny

• počet slov dĺžky n z navzájom rôznych písmen nad abecedou z n písmen

Ich počet je

$$\mathbf{P(n) = V(n,n) = n! = \prod_{i=1}^{n} i}$$

Príklad 10: Koľko rôznych slov dĺžky 6 je možné vytvoriť z písmen slova PIATOK?

$$6! = 720$$

Príklad 11: Koľkými rôznymi spôsobmi je možné usadiť do radu 10 ľudí?

$$10! = 3628800$$

Príklad 12: Aký je počet variácií k-tej triedy z množiny $\{1, 2, \ldots, n\}$ bez opakovania a permutácii z množiny $\{1, 2, \ldots, n\}$ takých, že 1 a 2 nie sú vedľa seba?

$$V(n, k) - 2(k-1)V(n-2, k-2);$$

pre permutácie $k = n$:

$$P(n) - 2(n-1)P(n-2) = n! - 2(n-1)(n-2)! = (n-2)(n-1)!$$

Príklad 13: Pre n=5 jedna možná premutácia je

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

$$p(1) = 3,\ p(2) = 1,\ p(3) = 5,\ p(4) = 2,\ p(5) = 4$$

Kratší zápis pomocou *cyklu*: $p = (13542)$

Príklad 14: Pomocou cyklov zapíšte permutáciu

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 6 & 8 & 9 & 4 & 2 & 3 & 5 \end{pmatrix} = (172)(3648)(59)$$

Kombinácie k-tej triedy z n prvkov

• všetky možné *neusporiadané* výbery *navzájom rôznych* k prvkov z n prvkov

• všetky možné k-prvkové *podmnožiny* n-prvkovej množiny

Ich počet dostaneme z variácií k-tej triedy bez opakovania vydelením $k!$, čo je počet všetkých usporiadaní konkrétnej variácie, t.j.

počet kombinácií k-tej triedy z n prvkov je

$$\mathbf{C(n,k)} = \frac{\mathbf{n(n-1)...(n-(k-1))}}{\mathbf{k!}} = \frac{\mathbf{n!}}{\mathbf{k!(n-k)!}} = \binom{\mathbf{n}}{\mathbf{k}}$$

Príklad 15: Koľko rôznych súčinov troch prvočísel možno vypočítať z prvočísel: $2, 3, 5, 7, 11, 13, 17, 19$?

$$\binom{8}{3} = 56$$

Príklad 16: Koľko priamok určuje 15 bodov v rovine, ak
a) žiadne tri neležia na jednej priamke?
b) práve 7 leží na jednej priamke?

$$\text{a)} \qquad \binom{15}{2} = 105$$

$$\text{b)} \qquad \binom{15}{2} - \binom{7}{2} + 1 = 85$$

Vlastnosť 1:

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

Vlastnosť 2 (Pascalova rovnosť):

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

Odvodenie: Pravá strana je počet k-prvkových podmnožín n-prvkovej množiny A. Zvoľme si $a \in A$. Podmnožiny množiny A si rozdeľme podľa toho, či obsahujú a alebo nie.

Každá k-prvková podmnožina množiny A neobsahujúca a je zároveň aj k-prvková podmnožina množiny $A - \{a\}$. Všetkých takých podmnožín je $\binom{n-1}{k}$.

Ak B je nejaká k-prvková podmnožina A obsahujúca a, môžeme jej bijektívne priradiť $(k-1)$-prvkovú podmnožinu množiny $B - \{a\}$.

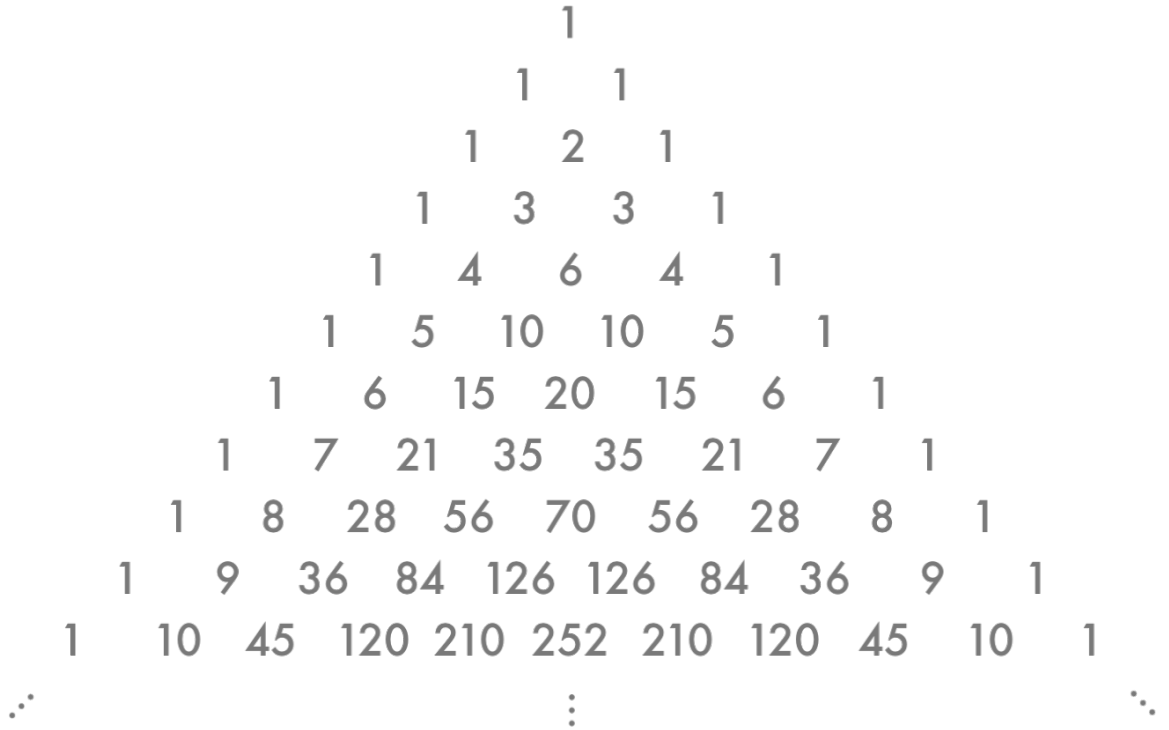
Ich počet je $\binom{n-1}{k-1}$. Sčítaním týchto dvoch kombinačných čísel dostaneme dokazovanú rovnosť.

□

Príklad 17: Nech A je n-prvková množina. Určte, koľko rôznych aspoň $(n-3)$-prvkových podmnožín obsahuje.

$$\binom{n}{n-3} + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n} = \frac{(n+1)(n^2-n+6)}{6}$$

Pascalov trojuholník



Vlastnosť 3 (Binomická veta):

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

Vlastnosť 4:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Odvodenie: Matematickou indukciou vzhľadom na n.

1. Vzťah platí pre $n = 0$.

2. Predoklajme, že tvrdenie je splnená pre nejaké $n \geq 0$. Našou úlohou teraz je, dokázať, že rovnica platí aj pre $n+1$.

$$(1+x)^{(n+1)} = (1+x)(1+x)^n = (1+x)\sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k=0}^{n} \binom{n}{k} x^{(k+1)} =$$

$$= \binom{n}{0} x^0 + \sum_{k=1}^{n} \binom{n}{k} x^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{(k+1)} + \binom{n}{n} x^{n+1} =$$

$$= 1 + \sum_{k=1}^{n} \binom{n}{k} x^k + \sum_{k=1}^{n} \binom{n}{k-1} x^k + x^{n+1} =$$

$$= 1 + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) x^k + x^{n+1} =$$

$$= \binom{n+1}{0} x^0 + \sum_{k=1}^{n} \binom{n+1}{k} x^k + \binom{n+1}{n+1} x^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k$$

□

Vlastnosť 5:

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Vlastnost' 6:

$$\sum_{j=0}^{r} \binom{m}{j} \binom{n}{r-j} = \binom{m+n}{r}$$

Vlastnost' 7:

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

Algebra a diskrétna matematika
Prehľad z 8. týždňa
Kombinatorika, princíp zapojenia a vypojenia,
systémy rôznych reprezentantov, lineárne rekurencie

Kombinatorika

Variácie k-tej triedy z n prvkov s opakovaním: všetky možné usporiadané výbery k prvkov z n prvkov; prvky sa môžu opakovať

$$V^*(n,k) = n^k$$

Variácie k-tej triedy z n prvkov bez opakovania: všetky možné usporiadané výbery navzájom rôznych k prvkov z n prvkov

$$V(n,k) = n(n-1)...(n-(k-1)) = \frac{n!}{(n-k)!}$$

Permutácia n prvkov: variácia n-tej triedy z n prvkov bez opakovania

$$P(n) = V(n,n) = n! = \prod_{i=1}^{n} i$$

Kombinácie k-tej triedy z n prvkov: všetky možné neusporiadané výbery *navzájom rôznych* k prvkov z n prvkov

$$C(n,k) = \frac{n(n-1)...(n-(k-1))}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Príklad 1: Koľkými spôsobmi možno rozdeliť n identických objektov do k očíslovaných skupín?

Ekvivalentne, aký je počet nezáporných celočíselných riešení rovnice
$x_1 + x_2 + \cdots + x_k = n$.

Riešenie:
Predstavme si, že máme $n + k - 1$ vyhradených miest v jednom riadku.

Rozdeliť n identických objektov do k očíslovaných skupín je ekvivalentné umiestneniu $k-1$ priehradiek do našich $n+k-1$ vyhradených miest (a n nerozlíšiteľných objektov do zvyšných n miest).
Teda, hľadaný počet je počet kombinácii $k-1$ miest spomedzi vyhradených $n+k-1$ miest, čiže

$$C(n+k-1,k-1)=\binom{n+k-1}{k-1}=\binom{n+k-1}{n}$$

Kombinácie s opakovaním

Príklad 2: Aký je počet tzv. kombinácií k-tej triedy z n prvkov *s opakovaním*, t.j. počet všetkých *neusporiadaných* výberov k prvkov (nie nutne navzájom rôznych) z n prvkov?

Ekvivalentne, aký je počet k-prvkových postupností $(x_1,x_2,\ldots,x_k)$ prirodzených čísel takých, že $1\le x_1\le x_2\le\ldots\le x_k\le n$?

Riešenie:
Určenie počtu uvedených postupností je ekvivalentné určeniu počtu rastúcich postupností

$$1\le x_1<x_2+1<x_3+2<\ldots<x_k+(k-1)\le n+k-1,$$

a tých je toľko, koľko je neusporiadaných výberov k *navzájom rôznych* čísel z $\{1,2,\ldots,n+k-1\}$, čo sú kombinácie k prvkov z $n+k-1$ prvkov, čiže

$$C^*(n,k)=C(n+k-1,k)=\binom{n+k-1}{k}=\binom{n+k-1}{n-1}$$

Permutácie s opakovaním

Permutácie n objektov rozdelených na s skupiniek z k_i $(1\le i\le s)$ nerozlíšiteľných objektov v každej skupinke, t.j. $n=k_1+k_2+\ldots+k_s$: Ich počet je

$$P^*(n;k_1,k_2,\ldots,k_s)=\frac{n!}{k_1!k_2!\ldots k_s!}=\binom{n}{k_1,k_2,\ldots,k_s}$$

Multinomická veta Pre ľubovoľné čísla $x_1,x_2,\ldots,x_m\in R$ a celé n platí

$$(x_1+x_2+\cdots+x_m)^n=\sum_{k_1+k_2+\ldots k_m=n}\binom{n}{k_1,k_2,\ldots,k_m}x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}$$

Princíp zapojenia a vypojenia
(inclusion-exclusion principle)

Pre konečné množiny A_1 a A_2 platí:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Pre 3 konečné množiny platí:

$$|A_1 \cup A_2 \cup A_3| =$$

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Odvodenie je jednoduché, napr. pomocou Vennových diagramov.

Vo všeobecnosti máme tzv. **princíp zapojenia a vypojenia** pre konečné množiny $A_1, \ldots, A_n$:

$$|\cup_{i=1}^{n} A_i| = \sum_{1 \le i \le n} |A_i| \; - \sum_{1 \le i < j \le n} |A_i \cap A_j| \; + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| -$$

$$- \sum_{1 \le i < j < k < \ell \le n} |A_i \cap A_j \cap A_k \cap A_\ell| + \cdots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|$$

Kratší zápis:

$$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\ldots n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$$

Odvodenie princípu zapojenia a vypojenia

Každý prvok $x \in \cup_{i=1}^{n} A_i$ je na ľavej strane započítaný presne raz.
Stačí ukázať, že x je presne raz započítaný aj na pravej strane.

Nech x patrí do presne t množín spomedzi A_i. Bez ujmy na všeobecnosti (t.j. až na označenie) môžeme predpokladať, že x je v $A_1, ..., A_t$ a nie v $A_{t+1}, ..., A_n$. Uvedomme si, že x sa vyskytuje v prieniku každého výberu z množín $A_1, ..., A_t$.

Prepíšeme binomickú vetu pre $(1-1)^t$ do tvaru

$$1 = \binom{t}{1} - \binom{t}{2} + \ldots + (-1)^{t-1}\binom{t}{t} .$$

Číslo $\binom{t}{i}$ vyjadruje *počet* prienikov i množín z výberu $A_1, ..., A_t$, t.j. x sa celkovo započíta len raz na pravej strane v rovnosti zapojenia-vypojenia. Tento fakt je potrebné aplikovať pre *každé* $x \in \cup_{i=1}^{n} A_i$.

Príklad 3: Aký je počet usporiadaní n prvkov na očíslovaných miestach $1, 2, \ldots, n$ tak, aby sa žiaden prvok i neocitol na mieste s číslom i?

Iná formulácia: Koľkými spôsobmi si n pánov môže preusporiadať svoje klobúky, aby žiaden z nich nemal na hlave svoj vlastný klobúk?

Jedná sa o derangement = "rozhádzanie".

Riešenie:

Nech A_i je množina permutácií fixujúcich i.

$|A_i| = (n-1)!$ $\quad |A_1 \cap A_2| = (n-2)!$

$|A_1 \cap A_4 \cap A_7| = (n-3)!$ $\quad |A_{i_1} \cap A_{i_2} \ldots A_{i_k}| = (n-k)!,$

Podľa princípu zapojenia a vypojenia máme

$$|A_1 \cup A_2 \ldots A_n| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}$$

Odpoveď:

$$n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} = n! \left(\sum_{k=0}^{n} (-1)^{k} \frac{1}{k!} \right)$$

Príklad 4: S akou pravdepodobnosťou "chaos v šatni" skončí tak, že žiaden z n pánov nedostane svoj vlastný klobúk?

Riešenie:

Pravdepodobnosť chápeme intuitívne ako pomer počtu priaznivých možností (viď vyššie) ku počtu všetkých možností.

V našom prípade je všetkých možností $n!$.

$$P = n! \left(\sum_{k=0}^{n} (-1)^{k} \frac{1}{k!} \right) / n! = \sum_{k=0}^{n} (-1)^{k} \frac{1}{k!} \approx 1/e \approx 0.368 \quad \text{pre} \quad n \to \infty$$

Príklad 5: Aký je počet všetkých surjektívnych zobrazení $[k] \to [n]$?

Riešenie: Ak A značí všetky zobrazenia $[k] \to [n]$, tak $|A| = n^k$.
Nech $A_i = \{f : [k] \to [n];\ f(x) \neq i \text{ pre } x \in [k]\}$.
Potom $|A_i| = (n-1)^k, \quad |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}| = (n-j)^k$
Podľa princípu zapojenia a vypojenia

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \binom{n}{j} (n-j)^k$$

Počet všetkých surjekcií je

$$|S| = |A| - |A_1 \cup A_2 \cup \cdots \cup A_n| = n^k - \sum_{j=1}^{n} (-1)^{j-1} \binom{n}{j} (n-j)^k =$$

$$|S| = \sum_{i=0}^{n} (-1)^j \binom{n}{j} (n-j)^k$$

Systémy rôznych reprezentantov

Hovoríme, že sústava množín $A_1, A_2, \ldots, A_n$ má **systém rôznych reprezentantov**, alebo **transverzálu**, ak existuje n *navzájom rôznych* prvkov $a_1, a_2, \ldots, a_n$ takých, že $a_i \in A_i$ pre každé $i \in \{1, 2, \ldots, n\}$.

Príklad 6: Nájdite systém rôznych reprezentantov pre $A_1 = \{1, 3, 6\}$, $A_2 = \{1, 2, 3, 8\}$, $A_3 = \{3, 5\}$, $A_4 = \{4, 8\}$, $A_5 = \{1, 5\}$.
Odpoveď: $1, 2, 3, 4, 5$ alebo $3, 2, 5, 8, 1$, prípadne iné.

Príklad 7: Nájdite transverzálu pre
$A_1 = \{1, 3\}$, $A_2 = \{1, 2, 3, 8\}$, $A_3 = \{3, 5\}$, $A_4 = \{2, 3, 4, 5\}$, $A_5 = \{1, 5\}$, $A_6 = \{2, 5, 6, 7, 8\}$, $A_7 = \{2, 4, 6, 7\}$, $A_8 = \{1, 3, 5\}$.
Odpoveď: Nedá sa nájsť.

Veta (Ph. Hall, 1935) Sústava množín $A_1, A_2, \ldots, A_n$ má **systém rôznych reprezentantov** práve vtedy, keď pre každú $I \subset \{1, 2, \ldots, n\}$ platí:
$$|\cup_{i \in I} A_i| \geq |I| \quad \text{(Hallova podmienka)}$$

V našom príklade 7, kde
$A_1 = \{1,3\},\ A_2 = \{1,2,3,8\},\ A_3 = \{3,5\},\ A_4 = \{2,3,4,5\},\ A_5 = \{1,5\},$
$A_6 = \{2,5,6,7,8\},\ A_7 = \{2,4,6,7\},\ A_8 = \{1,3,5\},$

vezmime $I = \{1,3,5,8\}$,

vidíme, že $3 = |A_1 \cup A_3 \cup A_5 \cup A_8| < |I| = 4$,

t.j. nie je splnená Hallova podmienka, a teda v tomto prípade systém rôznych reprezentantov neexistuje.

Lineárne rekurencie

Uvažujme Fibonacciho postupnosť (r. 1202)

$$1,\ \ 1,\ \ 2,\ \ 3,\ \ 5,\ \ 8,\ \ 13,\ \ 21,\ \ 34, \ldots$$

Jej zápis je $F_n = F_{n-1} + F_{n-2}$ a $F_0 = 1, F_1 = 1$.

Uvedený vzťah nazývame **lineárna rekurencia**.
Hodnoty pre F_0, F_1 sú **počiatočné podmienky**.

Vedeli by sme vyriešiť

$$F_n = F_{n-1} + F_{n-2} \quad (*)$$

bez hodnôt $F_0 = 1, F_1 = 1$?

Riešenie skúsime hľadať v tvare r^n.

$$r^n = r^{n-1} + r^{n-2}$$
$$r^2 = r + 1$$

Máme kvadratickú rovnicu s koreňmi r_1, r_2.
Ak $b_n = r_1^n, c_n = r_2^n$ spĺňajú rovnicu $(*)$, potom aj $F_n = \alpha r_1^n + \beta r_2^n$ ju spĺňa.
Dôvod:

$$r_1^2 = r_1 + 1$$
$$r_1^n = r_1^{n-1} + r_1^{n-2}$$
$$\alpha r_1^n = \alpha r_1^{n-1} + \alpha r_1^{n-2}$$

Podobne $$\beta r_2^n = \beta r_2^{n-1} + \beta r_2^{n-2}$$

Z uvedeného vyplýva, že $F_n = \alpha r_1^n + \beta r_2^n$ spĺňa $(*)$.

Teraz chceme vypočítať α, β tak, aby $F_0 = 1, F_1 = 1$.

Pre $n = 0$ a $n = 1$ dostaneme

$$F_0 = \alpha + \beta = 1$$
$$F_1 = \alpha r_1 + \beta r_2 = 1$$

Pomocou Cramerovho pravidla nájdeme riešenie

$$\alpha = \frac{\begin{vmatrix} 1 & 1 \\ 1 & r_2 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ r_1 & r_2 \end{vmatrix}} = \frac{r_2 - 1}{r_2 - r_1} \qquad \beta = \frac{\begin{vmatrix} 1 & 1 \\ r_1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ r_1 & r_2 \end{vmatrix}} = \frac{1 - r_1}{r_2 - r_1}$$

$$F_n = \frac{r_2 - 1}{r_2 - r_1}\, r_1^n + \frac{1 - r_1}{r_2 - r_1}\, r_2^n$$

Aké hodnoty majú r_1, r_2?

Platí pre ne $r_i^2 = r_i + 1$.

Sú teda koreňmi **charakteristickej rovnice**

$$r^2 - r - 1 = 0$$

$$r_1 = \frac{1 - \sqrt{5}}{2},\ r_1 = \frac{1 + \sqrt{5}}{2}$$

$$F_n = \frac{-1 + \sqrt{5}}{2\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n + \frac{1 + \sqrt{5}}{2\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n$$

Príklad 8: Nájdite explicitné riešenie rekurentnej rovnice

$$a_n = 4a_{n-1} - 3a_{n-2}$$

s podmienkami $a_0 = 6, a_1 = -1$.

Riešenie (stručný postup):

$r^n = 4r^{n-1} - 3r^{n-2}$

$r^2 = 4r - 3$

$r^2 - 4r + 3 = 0$

$r_1 = 1, r_2 = 3$

$a_n = \alpha 1^n + \beta 3^n$

Do tohto riešenia dosadíme počiatočné podmienky a vypočítame α a β.

$6 = \alpha + \beta$

$-1 = \alpha + 3\beta$

$\alpha = 9,5; \beta = -3,5$

Riešenie je $a_n = 9,5 - 3,5 \cdot 3^n$.

Lineárne rekurencie - zovšeobecnenie

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_k a_{n-k} = 0$$

Riešenie hľadáme v tvare r^n.

$$r^n - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_k r^{n-k} = 0$$

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0$$

Vo všeobecnosti dostenme k riešení $r_1, r_2, \ldots, r_k$. Ak sú všety rôzne, tak **všeobecné riešenie** má tvar

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

Hodnoty $\alpha_1, \ldots, \alpha_k$ dopočítame z počiatočných podmienok pre $a_0, a_1, \ldots, a_{k-1}$.

Algebra a diskrétna matematika
Prehľad z 9. prednášky
Algebraické štruktúry - Úvod

Binárna relácia

Nech M je neprázdna množina a nech $M \times M$ je **kartézsky súčin** množiny M samej so sebou, t.j. $M \times M = \{(x, y); x, y \in M\}$.

Pod **binárnou reláciou** na množine M rozumieme ľubovoľnú podmnožinu súčinu $M \times M$. Formálne, $\mathcal{R}$ je binárna relácia na M, ak $\mathcal{R} \subseteq M \times M$.

Vzťah medzi x a y v relácii $\mathcal{R}$ zapisujeme $(x, y) \in \mathcal{R}$ alebo $x\mathcal{R}y$.

Ak M má veľkosť n, body v relácii môžeme znázorniť vyznačením zodpovedajúcich bodov na mriežke $n \times n$ alebo pomocou orientovaného grafu s n vrcholmi, v ktorom je dvojica bodov $x\mathcal{R}y$ reprezetovaná šípkou z x do y. Reláciu na n prvkovej množine $M = \{x_1, x_2, \ldots, x_n\}$ je tiež možné popísať pomocou *matice susednosti* A relácie $\mathcal{R}$, pričom $A_{n\times n} = (a_{ij})$, kde $a_{ij} = 1$, ak $x_i\mathcal{R}x_j$, inak $a_{ij} = 0$.

Príklad 1: Ilustrácia binárnych relácií na daných množinách.

a) $M = \{0, 1, 2\}$, $\mathcal{R} = \{(0, 0), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2)\}$.
b) $M = \{a, b, c, d, e\}$, $\mathcal{R} = \{(a, b), (a, c), (b, b), (c, d), (e, b), (e, e)\}$
c) $M = \mathbb{Z}$, $\mathcal{R} = \{(z, z + 9); z \in \mathbb{Z}\}$.
d) $\mathcal{R}$ na $\mathbb{R}$: $\quad x\mathcal{R}y \Leftrightarrow y = x^3 - x$

Poznámka: Funkcia je špeciálnym typom relácie.

Vlastnosti binárnej relácie

Hovoríme, že relácia $\mathcal{R}$ je na množine M

(R) **reflexívna**, ak pre každé $x \in M$ platí $x\mathcal{R}x$

(S) **symetrická**, ak $x\mathcal{R}y$ implikuje $y\mathcal{R}x$ pre každé $x, y \in M$

(A) **antisymetrická**, ak $x\mathcal{R}y$ a $y\mathcal{R}x$ implikuje $x = y$ pre každé $x, y \in M$

(T) **tranzitívna**, ak $x\mathcal{R}y$ a $y\mathcal{R}$z implikuje $x\mathcal{R}z$ pre každé $x, y, z \in M$

Príklad 2: Overte vlastnosti relácií na daných množinách

a) $M = \{0, 1, 2\}$, $\mathcal{R} = \{(0,0), (1,0), (1,1), (1,2), (2,0), (2,2)\}$

b) $\mathcal{R}$ na $\mathbb{R}$: $x\mathcal{R}y \Leftrightarrow |x - y| \geq 6$

c) $\mathcal{R}$ na $\mathbb{Z}$: $x\mathcal{R}y \Leftrightarrow x \leq y$

d) M je množina všetkých priamok v rovine a $\mathcal{R}$ je relácia rovnobežnosti priamok, t. j. $\forall\, p, q \in M;\ p\mathcal{R}q \ \Leftrightarrow\ p \parallel q$

Odpoveď:

a) (R), (A), (T)
b) (S)
c) (R), (A), (T)
d) (R), (S), (T)

Čiastočne usporiadaná množina (poset)

Binárna relácia $\mathcal{R} \subseteq M \times M$ sa nazýva **čiastočným usporiadaním** na M, ak je na M *reflexívna, antisymetrická* a *tranzitívna.*

Ak $\mathcal{R}$ je čiastočné usporiadanie na M, tak namiesto $x\mathcal{R}y$ používame označenie $x \preceq_{\mathcal{R}} y$ alebo sa index $\mathcal{R}$ vynecháva.

Často sa jednoducho píše $x \leq y$.

Vlastnosti z definície čiastočného usporiadania potom majú tvar

(R) $x \leq x$ (reflexívnosť)

(A) ak $x \leq y$ a $y \leq x$, tak $x = y$ (antisymetria)

(T) ak $x \leq y$ a $y \leq z$, tak $x \leq z$ (tranzitívnosť)

pre každé $x, y, z \in M$.

Dvojicu $(M, \leq)$, kde $\leq$ je binárna relácia čiastočného usporiadania, nazývame **čiastočne usporiadaná množina**.

Príklad 3: Nech S je neprázdna množina a nech M je ľubovoľná množina *podmnožín* množiny S. Nech $\leq$ je binárna relácia inklúzie, t.j. ak $X, Y \in M$, tak $X \leq Y$, ak X je podmnožinou množiny Y. Potom $(M, \leq)$ je čiastočne usporiadaná množina.

Príklad 4: Nech M je ľubovoľná neprázdna podmnožina množiny $\mathbb{N}$ a nech pre každé $x, y \in M$ symbol $x \leq y$ označuje fakt, že číslo x je deliteľom čísla y. Potom $(M, \leq)$ je opäť čiastočne usporiadaná množina.

Ak $(M, \leq)$ je čiastočne usporiadaná množina, tak dva rôzne prvky $x, y \in M$ sú **porovnateľné**, ak buď $x \leq y$, alebo $y \leq x$.
(Oba vzťahy nemôžu platiť súčasne pre $x \neq y$.)
Budeme písať $x < y$, ak $x \leq y$ a $x \neq y$.

- Prvok $a \in M$ sa nazýva **najmenší**, ak $a \leq x$ pre každé $x \in M$.
- Prvok $b \in M$ sa nazýva **najväčší**, ak $x \leq b$ pre *každé* $x \in M$.
- Prvok $a \in M$ je **minimálny**, ak neexistuje žiadne $x \in M$, že $x < a$.
- Prvok $b \in M$ je **maximálny**, ak neexistuje žiadne $x \in M$, že $b < x$.

Ak v $(M, \leq)$ existuje najmenší (najväčší) prvok, tak tento je určený *jednoznačne*.
Najmenší (najväčší) prvok v $(M, \leq)$ je zároveň minimálnym (maximálnym) prvkom; vo všeobecnosti to neplatí obrátene.
Ak $(M, \leq)$ obsahuje viac ako jeden minimálny (maximálny) prvok, tak žiadne dva minimálne (maximálne) prvky nemôžu byť porovnateľné.

Príklad 5: Pre čiastočne usporiadanú množinu $(\{1, 2, \ldots, 10\}, |)$, kde $x \mid y$ označuje fakt, že x delí y, nájdite všetky minimálne a maximálne prvky, najmenší a najväčší prvok.
Odpoveď: Najmenší a zároveň minimálny prvok je 1, maximálne prvky sú $6, 7, 8, 9, 10$ a najväčší prvok neexistuje.

Čiastočne usporiadané množiny znázorňuje pomocou **Hasseho diagramu**.

V Hasseho diagrame čiastočne usporiadanej množiny $(M, \leq)$:

- sa nevyskytujú slučky,
- spojnica je medzi x, y iba ak x je bezprostredným predchodcom prvku y, t.j. $x < y$ a neexistuje žiadne $z \in M$, že $x < z < y$,
- ak $x < y$, tak x sa umiestňuje pod y.

Z Hasseho diagramu je možné jednoznačne zrekonštruovať reláciu $\leq$ čiastočného uporiadania na množine M.

Zväzy

Nech $(M, \leq)$ je čiastočne usporiadaná množina a nech $x, y \in M$.

- Prvok $z \in M$ je **dolným ohraničením** prvkov x a y, ak $z \leq x$ a $z \leq y$.
- Prvok $c \in M$ je **najväčším dolným ohraničením** prvkov x a y, ak $c \leq x$, $c \leq y$, a ak $z \leq c$ pre každé dolné ohraničenie z prvkov x, y.

  Označenie: $c = \inf(x, y)$, alebo $c = x \wedge y$, *priesek* x a y.

- Prvok $z \in M$ je **horným ohraničením** prvkov x a y, ak $x \leq z$ a $y \leq z$.
- Prvok $d \in M$ je **najmenším horným ohraničením** prvkov x a y, ak $x \leq d$, $y \leq d$, a ak $d \leq z$ pre každé horné ohraničenie z prvkov x, y.

  Označenie: $d = \sup(x, y)$, alebo $d = x \vee y$, *spojenie* prvkov x a y.

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **zväz**, ak pre každé $x, y \in M$ existuje ich priesek $x \wedge y$ a aj ich spojenie $x \vee y$.

Príklad 6: Nech $M = \{0, 1, 2\} \times \{0, 1\}$ a relácia usporiadania $\leq$ je daná predpisom $(a, b) \leq (c, d) \Leftrightarrow a \leq c$ a $b \leq d$. Dvojica $(M, \leq)$ tvorí zväz.

Príklad 7: Nech $(\mathbb{N}, |)$ je čiastočne usporiadaná množina, kde $\mathbb{N}$ je množina prirodzených čísiel a $x \mid y$ označuje fakt, že x delí y. Potom $x \wedge y$ je najväčší spoločný deliteľ a $x \vee y$ je najmenší spoločný násobok čísel x a y; čiastočne usporiadaná množina $(\mathbb{N}, |)$ je tiež zväz.

Príklad 8: Nech S je neprázdna množina a nech 2^S označuje množinu *všetkých* podmnožín množiny S. V čiastočne usporiadanej množine $(2^S, \subseteq)$ je priesek dvoch prvkov rovný prieniku a spojenie je rovné zjednoteniu príslušných množín a teda $(2^S, \subseteq)$ je zväz.

Takéto zväzy sa nazývajú **boolovské**.

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **ret'azec**, ak pre každé $x, y \in M$ platí, že $x \leq y$ alebo $y \leq x$; skrátene, ak každé dva prvky v M sú *porovnateľné*.

Príslušné čiastočné usporiadanie $\leq$ sa nazýva aj **lineárne**.

Tvrdenie 1: Každý reťazec je zväz.

Príklad 9: Dané čiastočne usporiadané množiny sú reťazce.

a) $(\{1,2,3,4,5,6\}, \leq)$

b) $M = \{1,2,3,4\}$, $\mathcal{R} = \{(2,3),(2,1),(1,4),(1,3),(2,4),(4,3)\}$

Binárna operácia a algebraická štruktúra

Binárna operácia je "dvojčlenná" operácia, ktorá každej usporiadanej dvojici prvkov z nejakej množiny priraďuje jediný tretí prvok z tej istej množiny; t. j. binárna operácia φ na množine M je zobrazenie $\varphi : M \times M \to M$.

Z faktu, že φ je zobrazenie vyplýva, že

- každá binárna operácia je *uzavretá*; t. j. $\forall x, y \in M : \varphi(x, y) \in M$,
- výsledok operácie je definovaný pre *každú* usporiadanú dvojicu z $M \times M$, t. j. $\forall x, y \in M \; \exists z \in M : \varphi(x, y) = z$.

Známe príklady:

Číselné operácie: sčítanie, odčítanie, násobenie, max, min.

Množinové operácie: prienik, zjednotenie, rozdiel.

Označenie: Ak sa nejedná o známe operácie, najčastejšie používané označenie binárnej operácie je $*$, $\circ, \oplus$ alebo $\otimes$; píšeme $x * y, x \circ y$ atď.

Vlastnosti binárnych operácií

Nech $*$ je binárna operácia na množine M. Hovoríme, že operácia $*$ je

- **komutatívna**, ak $\forall x, y \in M : x * y = y * x$
- **asociatívna**, ak $\forall x, y, z \in M : (x * y) * z = x * (y * z)$

Nech $*, \circ$ sú dve binárne operácie na M. Hovoríme, že

- operácia $*$ je **zľava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x, y, z \in M : x * (y \circ z) = (x * y) \circ (x * z)$,

- operácia $*$ je **sprava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x, y, z \in M : (x \circ y) * z = (x * z) \circ (y * z)$,
- operácia $*$ je **distributívna** vzhľadom na operáciu $\circ$, ak je vzhľadom na $\circ$ distributívna zľava aj sprava.

Neprázdna množina M spolu s jednou alebo viacerými binárnymi operáciami tvorí **algebraickú štruktúru**.

Rozoznávame veľa rôznych algebraických štruktúr podľa toho, aké vlastnosti spĺňajú ich binárne operácie.

Zväz ako algebraická štruktúra

V každom zväze $(M, \leq)$ pre všetky $x, y, z \in M$ platia nasledujúce vzťahy:

(1)	$x \wedge x$	$=$	x	$x \vee x$	$=$	x
(2)	$x \wedge y$	$=$	$y \wedge x$	$x \vee y$	$=$	$y \vee x$
(3)	$(x \wedge y) \wedge z$	$=$	$x \wedge (y \wedge z)$	$(x \vee y) \vee z$	$=$	$x \vee (y \vee z)$
(4)	$(x \wedge y) \vee y$	$=$	y	$(x \vee y) \wedge y$	$=$	y
(5)	$x \leq y$	$\Leftrightarrow$	$x \wedge y = x$	$x \leq y$	$\Leftrightarrow$	$x \vee y = y$

Dá sa ukázať, že na zväz $(M, \leq)$ je ekvivalentne možné hľadieť aj ako na *algebraickú štruktúru* $(M, \wedge, \vee)$ s dvoma binárnymi operáciami $\wedge$ a $\vee$: $M \times M \to M$, ktoré majú vlastnosti (1) – (4).

Príslušné čiastočné usporiadanie je potom definované vzťahom (5).

Načrtneme fakt, že ak $(M, \wedge, \vee)$ je algebraická štruktúra spĺňajúca (1) – (4), tak predpisom (5) je naozaj definované čiastočné usporiadanie.

- Na odvodenie (R) treba ukázať, že $x \leq x$, čiže treba overiť, že $x \wedge x = x$, ale to je vzťah (1).
- Na odvodenie (A) predpokladajme, že $x \leq y$ a $y \leq x$, teda $x \wedge y = x$ a $y \wedge x = y$; potom ale z (2) máme $x = y$, čím dostávame (A).
- Na odvodenie (T) predpokladajme, že $x \leq y$ a $y \leq z$, teda $x \wedge y = x$ a $y \wedge z = y$. Z vlastnosti (3) máme $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, ale $x \wedge z = x$ znamená, že $x \leq z$, z čoho vyplýva (T).

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z 10. týždňa

Algebraické štruktúry s jednou binárnou operáciou

Binárna operácia φ na množine M je zobrazenie $\varphi : M \times M \to M$.

Poznámka: Binárna operácia je vždy *uzavretá*; $\forall x, y \in M : \varphi(x, y) \in M$.

Neprázdna množina M spolu s jednou alebo viacerými binárnymi operáciami tvorí **algebraickú štruktúru**.

Grupoid

Nech M je neprázdna množina a $*$ binárna operácia na M. Potom dvojicu $(M, *)$ nazývame **grupoid**.

Ak M je konečná, jedná sa o *konečný grupoid*; inak *nekonečný*.

Rád grupoidu je veľkosť množiny M; označujeme ho $|M|$.

V prípade, že je operácia $*$ komutatívna, tak hovoríme, že grupoid je **komutatívny**, alebo **abelovský**.

Pologrupa

Pologrupa je grupoid $(M, *)$, v ktorom je binárna operácia $*$ asociatívna.

Príklad 1: Rozhodnite, či sú nasledujúce štruktúry pologrupy.

a) $(\mathbb{N}, +)$
b) $(\mathbb{N}, \cdot)$
c) $(\mathbb{Z}, -)$
d) $(\mathbb{Q}, +)$
e) $(\mathbb{Q}, \cdot)$
f) $(\mathbb{R} - \{0\}, \cdot)$
g) $(\mathbb{R} - \{0\}, /)$
h) $(\mathbb{C}, +)$

Odpoveď: a) áno, b) áno, c) nie d) áno e) áno, f) áno, g) nie, h) áno

Príklad 2:
a) Štruktúra $(\mathbb{N}, *)$, kde $\forall m, n \in \mathbb{N} : m * n = \max\{m, n\}$, je abelovská pologrupa.

b) Príklad nekomutatívnej pologrupy je štruktúra $(M_X, \circ)$, kde M_X je množina všetkých funkcií $f : X \to X$ a operácia $\circ$ je skladanie funkcií.

Príklad 3:
Nech množina $M = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{N} \right\}$ a operácia $*$ je násobenie matíc.

Dvojica $(M, *)$ je komutatívna pologrupa, pretože násobenie matíc je asociatívna operácia a navyše pre tento typ matíc platí aj komutativita.

Monoid

Nech $(M, *)$ je pologrupa.
Prvok $e \in M$ sa nazýva **neutrálny** (jednotkový), ak

$$\forall x \in M : \; x * e = e * x = x$$

Pologrupa $(M, *)$, ktorá má neutrálny prvok, sa nazýva **monoid**.

Príklad 4: Overte, či sa jedná o monoidy.
a) $(\mathbb{N}, +)$
b) $(\mathbb{N}, \cdot)$
c) $(2^{\mathbb{N}}, \bigcup)$
d) $(2^{\mathbb{N}}, \bigcap)$

Odpoveď: a) nie, b) áno, c) áno, d) áno

Príklad 5: Zistite, či sú nasledujúce štruktúry monoidy a overte ich komutativitu.
a) $(\{0, 1, 2, 3\}, *)$, kde $m * n = \max\{m + n, 3\}$
b) $(\{0, 1, 2, 3\}, *)$, kde $m * n = \min\{m + n, 3\}$
c) $(M, \cdot)$, kde $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z} \right\}$

Odpoveď: a) nie je algebraická štruktúra, b) komutatívny monoid c) nekomutatívny monoid

Tvrdenie 1: Ak v monoide existujú neutrálne prvky e_1 a e_2, potom $e_1 = e_2$.

Dôkaz:

Predokladajme, že monoid $(M, *)$ má dva neutrálne prvky e_1, e_2.

Platí, že $e_1 * e_2 = e_2$, lebo e_1 je neutrálny prvok.

Taktiež $e_1 * e_2 = e_1$, lebo e_2 je neutrálny prvok.

Dostali sme, že $e_1 = e_2$. □

Dôsledok: Každý monoid má práve jeden neutrálny prvok.

Grupa

Nech $(M, *)$ je monoid s neutrálnym prvkom e.

Nech $x \in M$. Prvok $y \in M$ sa nazýva **inverzný** k prvku x, ak platí

$$x * y = y * x = e$$

Monoid $(M, *)$, v ktorom ku každému prvku existuje inverzný prvok, sa nazýva **grupa**.

Príklad 6: Overte, či sa jedná o grupy.

a) $(\mathbb{Z}, +)$

b) $(\mathbb{Z} - \{0\}, \cdot)$

c) $(\mathbb{Q}^+, \cdot)$

d) $(\mathbb{R} - \{0\}, \cdot)$

Odpoveď: a) áno, b) nie, c) áno, d) áno

Tvrdenie 2: Ak v grupe $(M, *)$ existujú k prvku $x \in M$ inverzné prvky y_1 a y_2, potom $y_1 = y_2$.

Dôkaz:

Predokladajme, že prvok $x \in M$ má v grupe $(M, *)$ dva inverzné prvky $y_1, y_2 \in M$, t. j. $x * y_1 = y_1 * x = e$ a $x * y_2 = y_2 * x = e$.
Potom platia nasledujúce rovnosti

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$$

Dostali sme teda, že $y_1 = y_2$. □

Dôsledok: Každý prvok grupy má práve jeden inverzný prvok.

Inverzný prvok k prvku x označujeme x^{-1}.

Príklad 7: Množinu celých čísel si rozdeľme do dvoch množín podľa parity.

$P =$ množina všetkých celých párnych čísel

$N =$ množina všetkých celých nepárnych čísel

Uvažujme množinu $M = \{P, N\}$ s operáciou sčítania (aplikovanou medzi každou dvojicou čísel z daných množín). Dvojica $(M, +)$ tvorí grupu. Neutrálny prvok je P a inverzný prvok k N je N.

Príklad 8: Uvažujme nasledujúce množiny

$A = \{\ldots, -15, -12, -9, -6, -3,\ 0,\ 3,\ 6,\ 9,\ 12,\ 15, \ldots\}$

$B = \{\ldots, -14, -11, -8, -5, -2,\ 1,\ 4,\ 7,\ 10,\ 13,\ 16, \ldots\}$

$C = \{\ldots, -13, -10, -7, -4, -1,\ 2,\ 5,\ 8,\ 11,\ 14,\ 17, \ldots\}$

Dvojica $(\{A, B, C\}, +)$ tvorí grupu. Jej neutrálnym prvkom je A a platí, že $B^{-1} = C$, teda aj $C^{-1} = B$.

Pre každé prirodzené čislo k označme

$$\mathbb{Z}_k = \{n \in \mathbb{Z}_0^+, n < k\} = \{0, 1, 2, \ldots, k-1\}$$

Množinu $\mathbb{Z}_k$ nazývame **množinou zvyškových tried modulo** k, alebo triedami reziduí.

Definujme operáciu $\oplus$ na množine $\mathbb{Z}_k$ nasledovne:
$\forall a, b \in \mathbb{Z}_k :\quad a \oplus b$ je zvyšok po delení $(a + b) : k$.

Operácia $\oplus$ je na $\mathbb{Z}_k$ asociatívna.

Neutrálny prvok vzľadom na $\oplus$ je $e = 0$.

Pre každé $a \in \mathbb{Z}_k, a \neq 0$ je inverzný prvok $a^{-1} = k - a$, lebo $a \oplus a^{-1} = a \oplus (k - a) \equiv 0 \pmod{k}$.

Dvojica $(Z_k, \oplus)$ tvorí **abelovskú grupu**.

Zapisujeme ju jednoducho $(Z_k, +)$.
V tejto grupe sa namiesto a^{-1} zvykne písať $-a$, pretože $k - a$ je v rovnakej zvyškovej triede ako $-a$.

Príklad 9: Inverzné prvky v grupe $(\mathbb{Z}_{11}, \oplus)$ sú nasledovné:
$-1 = 10,\ -10 = 1$
$-2 = 9,\ -9 = 2$
$-3 = 8,\ -8 = 3$
$-4 = 7,\ -7 = 4$
$-5 = 6,\ -6 = 5$

Príklad 10: Nájdite všetky riešenia každej z daných rovníc.
a) $7 + x = 5 \pmod{9}$
b) $x + x + x = 4 \pmod{8}$
c) $x + x + x + x = 6 \pmod{7}$

Odpoveď: a) $x = 7 + 9k, k \in \mathbb{Z}$; b) $x = 4 + 8k, k \in \mathbb{Z}$, c) $x = 5 + 7k, k \in \mathbb{Z}$

Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z 11. prednášky

Dihedrálna, symetrická grupa, izmorfizmus grúp

Algebraické štruktúry s jednou binárnou operáciou

Nech M je neprázdna množina a nech platí

(1) $*$ je binárna operácia na M

(2) $*$ je asocitívna na M

(3) $\exists\, e \in M\ \forall x \in M:\ x * e = e * x = x$

(4) $\forall\, x \in M\ \exists x^{-1} \in M:\ x * x^{-1} = x^{-1} * x = e$

Potom dvojicu $(M, *)$ nazývame **grupa**.

Ak sú na M splné iba vlastnosti $(1), (2), (3)$, jedná sa o **monoid**.

Ak na M platí len $(1), (2)$, hovoríme, že $(M, *)$ je **pologrupa**.

Ak na M požadujeme iba platnosť (1), štruktúra $(M, *)$ je **grupoid**.

Rád prvku a grupy $(M, *)$ je najmenšie kladné celé číslo n také, že

$$a^n = e,$$

$$(a * a * a \ldots a * a = e)$$

.

Označuje sa $|a|$.

Ak také n neexistuje, hovoríme, že a má **nekonečný rád**.

Príklad 1: Určte rády daných prvkov v zodpovedajúcich grupách.

a) všetkých prvkov v $(\mathbb{Z}_6, +)$

b) prvku 4 v $(\mathbb{Z}, +)$

c) komplexnej jednotky i v $(\mathbb{C} - \{(0,0)\}, \cdot)$

Odpoveď: a) rád 0 je 1 (jedná sa o neutrálny prvok), rády prvkov $1, 2, 3, 4, 5$ sú $6, 3, 2, 3, 6$ v zodpovedajúcom poradí; b) ∞, c) 4

Množina **generátorov** grupy je taká podmnožina grupy, že každý prvok grupy sa dá vyjadriť ako "súčin" mocnín týchto generátorov.

Prezentácia grupy pomocou generátorov: $\langle$ generátory$|$ relácie $\rangle$

Cyklická grupa je grupa, ktorá je generovaná jedným prvkom g, t. j. je to množina všetkých mocnín prvku g.
Zapisuje sa $\langle g|g^n = e\rangle$, skrátene $\langle g\rangle$.

Grupa z príkladu 7 je cyklická grupa $(\mathbb{Z}_2, +)$ a grupa z príkladu 8 je $(\mathbb{Z}_3, +)$.

Príklad 2: Nájdite generátory grúp $(\mathbb{Z}_5, +), (\mathbb{Z}_6, +), (\mathbb{Z}_5 - \{0\}, \odot)$.

Odpoveď:
$(\mathbb{Z}_5, +) = \langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle$
$(\mathbb{Z}_6, +) = \langle 1\rangle = \langle 5\rangle$
$(\mathbb{Z}_5 - \{0\}, \odot) = \langle 2\rangle = \langle 3\rangle$

Dihedrálna grupa

Grupa symetrií pravidelného n-uholníka sa nazýva **dihedrálna grupa**.

Označuje sa D_n

Jej rád je $|D_n| = 2n$ (n osových symetrií a n otočení)

Neutrálny prvok e je identita.

Prezentácia: $D_n = \langle r, s|r^n = e, s^2 = e, rs = sr^{-1}\rangle$
r – rotácia o $360°/n$
s – symetria podľa pevnej osi symetrie

Priamy súčin grúp

Priamy súčin dvoch grúp $(S, *)$ a $(T, \circ)$ je definovaný ako operácia $\bullet$ na $S \times T$, kde $\forall s_1, s_2 \in S, t_1, t_2 \in T : (s_1, t_1) \bullet (s_2, t_2) = (s_1 * s_2, t_1 \circ t_2)$

Dá sa ukázať, že operácia $\bullet$ je *asociatívna*.
Neutrálny prvok v $(S \times T, \bullet)$ je (e_1, e_2), kde e_1 je neutrálny prvok v S a e_2 je neutrálny prvok v T.

Inverzný prvok k prvku (s,t) je prvok (s^{-1},t^{-1}), pričom s^{-1} je inverzný k s v $(S,*)$ a t^{-1} je inverzný k t v $(T,\circ)$.

Dvojica $(S\times T,\bullet)$ tvorí *grupu*.

Príklad 3: Priamy súčin grúp $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_2,+)$ je množina
$\mathbb{Z}_2\times\mathbb{Z}_2=\{(0,0),(0,1),(1,0),(1,1)\}$
s operáciou súčtu modulo 2 v oboch súradniciach.
Napr. $(0,1)\oplus(1,0)=(1,1),(1,1)\oplus(1,0)=(0,1),(1,0)\oplus(1,1)=(0,1)$ atď.

Príklad 4: Priamy súčin grúp $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_3,+)$ je množina
$\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$
s operáciou $\oplus$, ktorá vykoná súčet modulo 2 v prvej súradnici a súčet modulo 3 v druhej súradnici.
Napr. $(1,2)\oplus(0,2)=(1,1),\quad(1,1)\oplus(1,2)=(0,0)$.

Izomorfizmus grúp

Nech $(M_1,*)$ a $(M_2,\circ)$ sú dve grupy. Ak existuje bijekcia φ medzi M_1 a M_2 taká, že $\forall x,y\in M_1$ platí

$$\varphi(x*y)=\varphi(x)\circ\varphi(y),$$

potom grupy $(M_1,*)$ a $(M_2,\circ)$ sú **izomorfné**, píšeme $M_1\cong M_2$.
Zobrazenie φ sa nazýva **izomorfizmus**.

Neformálne: Dve grupy sú izomorfné, ak majú "takú istú štruktúru".

Izomorfné grupy majú rovnaký rád a rovnaký počet prvkov určitého rádu.

Tvrdenie 1: Všetky grupy s jedným prvkom sú izomorfné.

Tvrdenie 2: Existuje konečne veľa grúp daného konečného rádu (až na izomorfizmus).

Príklad 5: Grupy $(\mathbb{Z}_4,+)$ a $\mathbb{Z}_2\times\mathbb{Z}_2$ nie sú izomorfné, pretože grupa $(\mathbb{Z}_4,+)$ má dva prvky rádu 4 a také sa v $\mathbb{Z}_2\times\mathbb{Z}_2$ nenachádzajú. Všetky jej prvky majú rád 2.

Príklad 6: Rozhodnite, či sú niektoré z grúp $\mathbb{Z}_6, D_3$ a $\mathbb{Z}_2\times\mathbb{Z}_3$ izomorfné.

Odpoveď: Overením rádov prvkov zistíme, že D_3 nemôže byť izomorfná ani

s $\mathbb{Z}_6$ ani s $\mathbb{Z}_2 \times \mathbb{Z}_3$.
V grupách $\mathbb{Z}_6$ a $\mathbb{Z}_2 \times \mathbb{Z}_3$ má rovnaký počet prvkov zhodné rády. Príslušný izomorfizmus je $\varphi(0) = (0,0), \varphi(1) = (1,1), \varphi(2) = (0,2), \varphi(3) = (1,0), \varphi(4) = (0,1), \varphi(5) = (1,2)$.

Príklad 7: Sú grupy $(\mathbb{Z}_4, +)$ a $(\mathbb{Z}_5 - \{0\}, \cdot)$ izomorfné?

Odpoveď: Áno

Symetrická grupa

Skladanie permutácií vykonávame *zľava doprava.*

Príklad 8: Zložte dané permutácie

$(12)(34) \circ (13)(24) = (14)(23)$

$(13)(24) \circ (12)(34) = (14)(23)$

$(134)(258) \circ (2456)(78) = (135784)(26)$

$(2456)(78) \circ (134)(258) = (134872)(56)$

Vo všeobecnosti je skladanie permutácií nekomutatívne, ale máme výnimky.

Nech $X = \{1, 2, \ldots, n\}$ a nech S_n je množina všetkých bijekcií (čiže permutácií) $\sigma : X \to X$. Potom platí

- zloženie dvoch bijekcií je bijekcia
- skladanie bijekcií je asociatívne
$(\sigma \circ \tau) \circ \pi(x) = (\sigma \circ \tau)(\pi(x)) = \sigma(\tau(\pi(x)) = \sigma(\tau \circ \pi)(x) = \sigma \circ (\tau \circ \pi)(x)$
- identické zobrazenie je bijekcia na X
- inverzné zobrazenie bijekcie v S_n je tiež bijekcia v S_n

Množina S_n všetkých permutácií n objektov spolu s operáciou skladania permutácií tvorí grupu rádu $n!$ a nazýva sa **symetrická grupa** stupňa n.

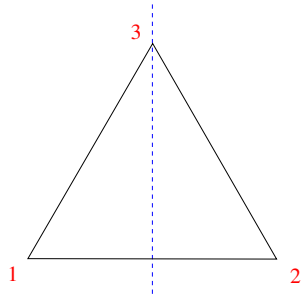
Inverzný prvok sa počíta nasledujúcim spôsobom
$(a_1 a_2 a_3 a_4 \ldots a_{n-1} a_n)^{-1} = (a_1 a_n a_{n-1} \ldots a_4 a_3 a_2)$
$((a_1 a_2 a_3 \ldots a_{i-1} a_i)(b_1 b_2 \ldots b_j))^{-1} = (a_1 a_i a_{i-1} \ldots a_3 a_2)(b_1 b_j \ldots b_2)$

Príklad 9: Vypíšte všetky prvky symetrickej grupy S_3 a overte komutatívnosť. Zistite, či je izomorfná s niektorou známou grupou rovnakého rádu.

Odpoveď: $S_3 = \{e, (12), (13), (23), (123), (132)\}$

Komutatívnosť neplatí; napr. $(12)(123) \neq (123)(12)$.

S_3 je izomorfná s dihedrálnou grupou $D_3 = \{e, r, r^2, s, rs, r^2s\}$, kde r je rotácia okolo stredu o $120°$ proti smeru hodinových ručičiek a s je osová symetria podľa zvislej osi.



Zodpovedajúci izomorfizmus $\varphi : S_3 \to D_3$ je
$\varphi(e) = e, \varphi((123)) = r, \varphi((132)) = r^2,$
$\varphi((12)) = s, \varphi((23)) = rs, \varphi((13)) = r^2s$

Príklad 10: Aké rôzne rády majú prvky grupy S_5?

Odpoveď: Rád 1 má identita,
rád 2 majú prvky typu (ij), $i, j \in \{1, 2, 3, 4, 5\}$, $i < j$
rád 2 majú tiež prvky typu $(ij)(k\ell)$, $i, j, k, \ell \in \{1, 2, 3, 4, 5\}, i < j, k < \ell$,
rád 3 majú prvky tvaru (ijk), $i, j, k \in \{1, 2, 3, 4, 5\}$, $i < j, k$
rád 4 majú prvky $(ijk\ell)$, $i, j, k, \ell \in \{1, 2, 3, 4, 5\}$, $i < j, k, \ell$,
rád 5 majú prvky $(1ijk\ell)$, $i, j, k, \ell \in \{2, 3, 4, 5\}$,
rád 6 majú prvky tvaru $(1i)(jk\ell)$, $i, j, \ell \in \{2, 3, 4, 5\}$, $j < k, \ell$,
pričom prvky i, j, k, ℓ sú vždy navzájom rôzne.

Permutácia zamieňajúca dva prvky a fixujúca všetky ostatné sa nazýva **transpozícia**.

Každú permutáciu je možné napísať vo forme súčinu transpozícií.

$$(a_1a_2a_3a_4 \dots a_n) = (a_1a_2)(a_1a_3)(a_1a_4) \dots (a_1a_n)$$

Permutácia je **párna**, ak je súčinom párneho počtu transpozícií.

Permutácia je **nepárna**, ak je súčinom nepárneho počtu transpozícií.

Príklad 11: Určte paritu daných permutácií

a) (13587)

b) (245398)

c) (142)(3875)

Odpoveď: a) párna permutácia, lebo (13587) = (13)(15)(18)(17)
b) nepárna permutácia; (245398) = (24)(25)(23)(29)(28)
c) nepárna permutácia; (142)(3875) = (14)(12)(38)(37)(35)

Množina všetkých párnych premutácií n prvkovej množiny spolu s operáciou skladania permutácií tvorí grupu, ktorá sa nazýva **alternujúca grupa** stupňa n a označuje sa A_n.

Počet prvkov A_n je $\frac{n!}{2}$.

Príklad 12: Vypíšte všetky prvky grupy A_3 a grupy A_4.

Odpoveď: $A_3 = \{e, (123), (132)\}$
$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

Algebra a diskrétna matematika

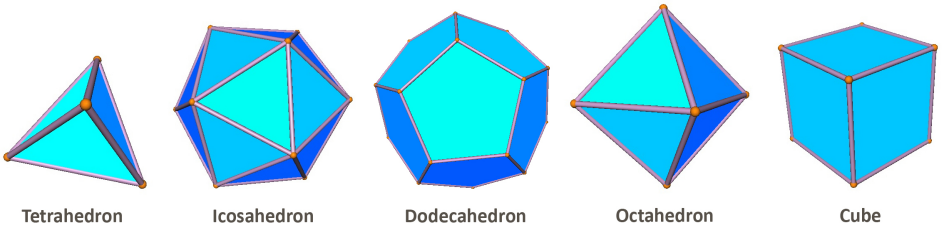
doc. RNDr. Jana Šiagiová, PhD.

Prehľad z 12. prednášky

Platónske telesá, polia

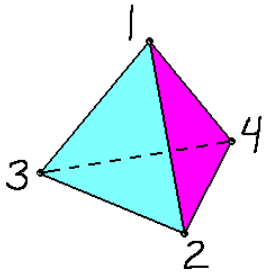
Platónske teleso je pravidelný mnohosten tvorený pravidelnými zhodnými mnohouholníkmi.

Existuje len 5 nasledujúcich platónskych telies.



štvorsten dvadsať sten dvanásť sten osemsten kocka

Príklad 1: Určte grupu rotácií pravidelného štvorstena.



Odpoveď: Prvky grupy sú:
- identita,
- 8 prvkov rádu 3 – otočenia okolo 4 osí prechádzajúcich cez vrchol a stred protiľahlej steny o 120° a 240°,
- 3 prvky rádu 2 – otočenia okolo 3 osí prchádzajúcich stredmi protiľahlých hrán o 180°.

Grupa rotácií pravidelného štvorstena je izomorfná s grupou A_4.

Príklad 2: Určte grupu rotácií kocky.

Odpoveď: Prvky grupy sú:
- identita,
- 8 prvkov rádu 3 – otočenia okolo 4 telesových uhlopriečok o 120° a 240°,
- 9 prvkov, 6 z nich rádu 4 a 3 prvky rádu 2 – otočenia okolo 3 osí prechádzajúcich stredmi protiľahlých stien o $90°, 180°$ (rád 2) a 270°
- 6 prvkov rádu 2 – otočenia okolo 6 osí prechádzajúcich stredmi protiľahlých hrán o 180°.

Grupa rotácií kocky je izomorfná s grupou S_4.

Medzi slávne antické problémy, ktoré sa viac ako dvetisíc rokov nedarilo vyriešiť patria:

• *Problém trisekcie uhla* – Pomocou pravítka a kružidla zostrojte uhol, ktorý je tretinou daného uhla.

• *Problém kvadratúry kruhu* – Pomocou pravítka a kružidla zostrojte štvorec, ktorý má rovnaký obsah ako daný kruh.

• *Problém zdvojenia kocky* – Pomocou pravítka a kružidla zostrojte kocku, ktorá má dvojnásobný objem ako daná kocka.

Odpoveď o ich neriešiteľnosti priniesla až moderná algebra v 19. storočí. Pomocou prostriedkov algebry sa dá dokázať, že pomocou pravítka a kružidla nedokážeme žiadnou konštrukciou
– rozdeliť daný uhol na tri rovnaké časti,
– zostrojiť z úsečky dĺžky 1 úsečku dĺžky π,
– zostrojiť z úsečky dĺžky a úsečku dĺžky $a\sqrt[3]{2}$.

Dôležitá algebraická štruktúra v tomto dôkaze je **pole**.

Pole je množina F s dvoma binárnymi operáciami $\oplus, \otimes$, pričom sú splnené nasledujúce podmienky

- $(F, \oplus)$ a $(F - \{0\}, \otimes)$ tvoria komutatívne grupy,
- Na F platí distributívny zákon

$$\forall\ a, b, c \in F: \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

Operácie $\oplus, \otimes$ zvyčajne nazývame *sčitovanie* a *násobenie*.

Pole potom jednoducho zapisujeme $(F, +, \cdot)$.
Grupa $(F, +)$ sa nazýva *aditívnou* grupou poľa, skrátene F^+.
Grupa $(F - \{0\}, \cdot)$ sa nazýva *multiplikatívnou* grupou poľa, skrátene $F^\times$.

Príklad 3: Najznámejšie nekonečné polia sú $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$.

Príklad 4: Príklad konečného poľa je $(\mathbb{Z}_5, +, \cdot)$.
Jeho aditívny neutrálny prvok je 0 a inverzné prvky v aditínej grupe sú $-1 = 4, -2 = 3, -3 = 2, -4 = 1$.
Multiplikatívny neutrálny prvok je 1 a inverzné prvky v multiplikatívnej grupe sú $2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$.
Rovnicu $3x + 4 \equiv 1$ v $\mathbb{Z}_5$ riešime nasledovne

$$\begin{aligned} 3x + 4 + 1 &= 1 + 1 \\ 3x &= 2 \\ 3^{-1} \cdot 3x &= 3^{-1} \cdot 2 \\ 2 \cdot 3x &= 2 \cdot 2 \\ x &= 4 \end{aligned}$$

Príklad 5: V poli $(\mathbb{Z}_5, +, \cdot)$ riešte rovnicu

$$x^2 + 4x + 3 = 0$$

Odpoveď: $x_1 = 2, x_2 = 4$

Príklad 6: V poli $\mathbb{Z}_5$ riešte sústavu rovníc

$$\begin{aligned} 3x + y &= 3 \\ x + 3y &= 2 \end{aligned}$$

Odpoveď: $x = 4, y = 1$

Príklad 7: V $\mathbb{Z}_6$ rovnica $3x + 4 = 2$ nemá riešenie, lebo k 3 neexistuje multiplikatívny inverz. $\mathbb{Z}_6$ nie je pole!

Tvrdenie 1: Ak p je prvočíslo, tak pre každé $x \in \mathbb{Z}_p - \{0\}$ existuje $y \in \mathbb{Z}_p - \{0\}$ také, že $x \cdot y \equiv 1 \pmod{p}$.

Rád poľa je počet prvkov poľa.

Tvrdenie 2: Rád konečného poľa je mocnina prvočísla.

Tvrdenie 3: Pre každé prvočíslo p a prirodzené číslo n existuje práve jedno (až na izomorfizmus) pole rádu $p^n = q$.
Toto pole sa nazýva **Galoisove pole** a označuje sa $GF(q)$.

Aditívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $n \cdot x = 0$; ak také n neexistuje, rádom prvku x je ∞.

Tvrdenie 4: V každom poli majú všetky prvky ($\neq 0$) rovnaký aditívny rád.

Multiplikatívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $x^n = 1$; ak také n neexistuje, rádom prvku x je ∞.

Príklad 8: Vypočítajte aditívne a mutliplikatívne rády prvkov $2, 3$ v poli $\mathbb{Z}_{11}$.

Odpoveď: Aditívny rád prvku 2 je 11, pretože najmenšie n, ktoré vyhovuje rovnici $n \cdot 2 \equiv 0 \pmod{11}$, je $n = 11$. To isté platí pre prvok 3.
Multiplikatívny rád prvku 2 je 10, pretože $2^{10} \equiv 1 \pmod{11}$ a 10 je najmenšia taká kladná mocnina.
Prvok 3 má multiplikatívny rád 5, lebo $3^5 \equiv 1 \pmod{11}$ a 5 je najmenšia taká kladná mocnina.

Príklad 9: Ktorý prvok generuje pole $\mathbb{Z}_{17}$?

Odpoveď: Ak prvok x je generátor v $\mathbb{Z}_{17}$, potom platí
$x^{16} \equiv 1$ a $x^8 \equiv -1 \pmod{16}$.
Postupne ideme overovať mocniny prvkov v $\mathbb{Z}_{17}$.
$2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16 \equiv -1, 2^8 \equiv 1$, teda 2 nie je generátor $\mathbb{Z}_{17}$.
$3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13, 3^5 \equiv 5, 3^6 \equiv 15, 3^7 \equiv 11, 3^8 \equiv 16 \equiv -1$,
$3^9 \equiv 3 \cdot 3^8 \equiv -3 \equiv 14, 3^{10} \equiv -3 \cdot 3 \equiv 8, 3^{11} \equiv 7, 3^{12} \equiv 4, 3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1$.
Prvok 3 je generátor poľa $\mathbb{Z}_{17}$.

Grupa je cyklická, ak je generovaná jedným prvkom.

Veta: Multiplikatívna grupa každého *konečného* poľa je **cyklická**.

Každý generátor multiplikatívnej grupy poľa nazývame **primitívny prvok**.

Nájsť primitívny prvok v poli nie je triviálne, ak ide o pole veľkého rádu.

Príklad 10: V poli $\mathbb{Z}_{23}$ nájdite primitívny prvok.

Odpoveď: Hľadáme prvok x v $\mathbb{Z}_{23}$, pre ktorý $x^{22} \equiv 1 \pmod{23}$ a tiež $x^{11} \equiv -1 \equiv 22 \pmod{23}$.

$2^{11} \equiv 1 \pmod{23}$, 2 nie je generátor. To isté platí pre 4.

Overíme prvok 3.

$3^3 \equiv 4$, takže $3^{33} \equiv (3^3)^{11} \equiv 4^{11} \equiv 1 \pmod{23}$ (*)

Ale potom ak by 3 bol primitívny prvok, tak 3^{11} by musel byť $-1 \pmod{23}$, a teda

$3^{33} = 3^{22} \cdot 3^{11} \equiv 1.(-1) \equiv -1 \bmod 23$, čo je v rozpore s (*).

Ani 3 nie je primitívnym prvkom v $\mathbb{Z}_{23}$.

Overme prvok 5.

$5^2 \equiv 2, 5^{10} \equiv 2^5 \equiv 9, 5^{11} \equiv 9 \cdot 5 \equiv -1 \pmod{23}$.

Prvok 5 je primitívny v poli $\mathbb{Z}_{23}$.

Počet primitívnych prvkov

Pole rádu p má $\varphi(p-1)$ primitívnych prvkov, kde φ je Eulerova funkcia (počet kladných čísel menších ako $p-1$ a nesúdeliteľných s $p-1$).

Ak prirodzené číslo n má prvočíselný rozklad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, potom

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

Príklad 11: Určte počet primitívnych prvkov v poliach $\mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$.

Odpoveď:

$\varphi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$

$\varphi(16) = 16(1 - \frac{1}{2}) = 8$

$\varphi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6$

V poli $\mathbb{Z}_{11}$ sú 4 primitívne prvky, v poli $\mathbb{Z}_{17}$ je ich 8 a pole $\mathbb{Z}_{19}$ ich má 6.

Príklad 12: Určte, ktoré prvky majú v poli $\mathbb{Z}_{19}$ druhé odmocniny.

Odpoveď: Najprv je potrebné nájsť primitívny prvok v $\mathbb{Z}_{19}$. Sú nimi napríklad prvky 2 a 3. Potom všetky prvky, ktoré sú párne mocniny primitívneho prvku, majú v $\mathbb{Z}_{19}$ druhú odmocninu.
Túto množinu tvoria prvky $1, 4, 5, 6, 7, 9, 11, 16, 17$.

Príklad 13: Riešte rovnicu $x^3 = 1$ v poli $\mathbb{Z}_7$ a v poli $\mathbb{Z}_{11}$.

Odpoveď: V $\mathbb{Z}_7$ sú korene $x_1 = 1, x_2 = 2, x_3 = 4$.
V poli $\mathbb{Z}_{11}$ je iba jeden koreň $x = 1$, pretože $11 - 1$ nie je deliteľné číslom 3.

Malá Fermatova veta: Nech p je prvočíslo a nech a je celé číslo nesúdeliteľné s p. Potom platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Príklad 14: Bez použitia kalkulačky vypočítajte

a) $19669^{28} \pmod{29}$

b) $3321^{3323} \pmod{3323}$

c) $11^{209458} \pmod{104729}$

Odpoveď: Keďže každé z čísel $29, 3323, 104729$ je prvočíslo, je možné aplikovať Malú Fermatovu vetu.

a) $19669^{28} \equiv 1 \pmod{29}$

b) $3321^{3323} \equiv 3321 \pmod{3323}$

c) $11^{209458} = (11^{104728})^2 \cdot 11^2 \equiv 121 \pmod{104729}$

Veľká Fermatova veta: Pre žiadne nenulové celé čísla a, b, c a $n > 2$ *neplatí*

$$a^n + b^n = c^n$$

Považuje sa za jeden z najťažších matematických problémov.
V roku 1637 Fermat napísal toto tvrdenie na okraj jedného listu Diofantovej Aritmetiky (3. st. pnl) s tým, ze údajný dôkaz sa mu tam už nezmestil.
Prvý dôkaz publikoval v roku 1995 anglický matematik Andrew Wiles.
V tom istom roku s Richardom Taylorom odstránili medzeru v dôkaze.