

Diskrétní matematika

Studijní materiál ke státnicím (M3)

Jakub Klesa

Pokryté předměty: NDMI002 (Diskrétní matematika), NDMI011 (Kombinatorika a grafy 1)

Obsah

Úvod	1
1 Relace, ekvivalence, rozkladové třídy	2
1.1 Ekvivalence a rozkladové třídy	3
2 Částečná uspořádání	4
3 Funkce: typy a počty	6
4 Permutace, kombinační čísla, binomická věta	8
4.1 Permutace	8
4.2 Kombinační čísla	8
4.3 Binomická věta	9
5 Princip inkluze a exkluze	9
5.1 Použití (1): problém šatnářky	10
5.2 Použití (2): Eulerova funkce	11
5.3 Použití (3): počet surjekcí	11
6 Hallova věta o SRR a párování v bipartitním grafu	11
Shrnutí	14
Zdroje	15

Úvod

Tento materiál pokrývá okruh **M3 – Diskrétní matematika** (předměty NDMI002 *Diskrétní matematika* a NDMI011 *Kombinatorika a grafy 1*). Výklad jádra okruhu (relace, uspořádání, funkce, kombinatorické počítání a princip inkluze a exkluze) stojí na zápiscích T. Slámy z přednášky doc. Martina Mareše a na učebnici J. Matouška a J. Nešetřila *Kapitoly z diskrétní matematiky* (v anglickém vydání *Invitation to Discrete Mathematics*), kterou jako literaturu k oběma předmětům doporučují jejich přednášející. Hallovu větu o systému různých reprezentantů uvádíme podle skript T. Vally a J. Matouška *Kombinatorika a grafy I* (NDMI011). Značení a hloubka odpovídají kurzu pro informatiky.

U *principu inkluze a exkluze* a *Hallově větě* požadavky okruhu výslovně uvádějí důkaz (resp. princip důkazu), proto je dokazujeme. Ostatní věty uvádíme *se zněním*, doplněné intuicí a krátkými odvozeními tam, kde pomáhají pochopení. Do výkladu jsou zařazeny řešené reálné otázky SZZ z let 2022–2026; všechny otázky k okruhu jsou pohromadě v samostatném dokumentu *Příklady otázek*. Použité zdroje jsou uvedeny na konci.

Značení. Množiny značíme velkými písmeny X, Y, A, B , jejich velikost $|X|$. Kartézský součin je $X \times Y = \{(x, y) : x \in X, y \in Y\}$, potenční množina (množina všech podmnožin) 2^X , množina všech k -prvkových podmnožin $\binom{X}{k}$. Binární relaci píšeme R a fakt $(x, y) \in R$ zkráceně xRy . Funkci (zobrazení) píšeme $f : X \rightarrow Y$. Symbolem $[n]$ míníme $\{1, 2, \dots, n\}$, faktoriál $n! = 1 \cdot 2 \cdots n$ ($0! = 1$) a kombinační číslo $\binom{n}{k}$. Uspořádání značíme $\leq$ (ostrou variantu $<$), částečně uspořádanou množinu (ČUM) dvojicí $(X, \leq)$.

1 Relace, ekvivalence, rozkladové třídy

Relace zachycuje vztah mezi prvky: kteří jsou „ve vztahu“ a kteří ne. Formálně je to prostě podmnožina kartézského součinu, tedy množina těch dvojic, které ve vztahu jsou.

Definice – Binární relace

Binární relace mezi množinami X a Y je libovolná podmnožina $R \subseteq X \times Y$. Je-li $X = Y$, mluvíme o *relaci na množině* X . Místo $(x, y) \in R$ píšeme xRy .

Poznámka. Speciální relace na X : *prázdná* $\emptyset$ (nic s ničím), *univerzální* $X \times X$ (vše se vším) a *diagonální (identická)* $\Delta_X = \{(x, x) : x \in X\}$ (každý prvek jen sám se sebou). K relaci R definujeme *inverzní* relaci $R^{-1} = \{(y, x) : (x, y) \in R\}$ a ke dvojici relací $R \subseteq X \times Y, S \subseteq Y \times Z$ jejich *složení* $R \circ S = \{(x, z) : \exists y \in Y, xRy \wedge ySz\}$.

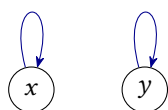
Intuice. Relaci na konečné X lze vidět dvěma způsoby. Jako *matici* $|X| \times |X|$ nul a jedniček (na pozici (x, y) je 1, právě když xRy): diagonální relaci pak odpovídají jedničky na hlavní diagonále. Nebo jako *orientovaný graf* na vrcholech X , kde šipka $x \rightarrow y$ vede právě pro xRy . Vlastnosti relací níže se hezky čtou na grafu.

Definice – Vlastnosti binární relace na X

Relace R na X je

- (1) *reflexivní*, pokud $\forall x \in X : xRx$;
- (2) *symetrická*, pokud $\forall x, y \in X : xRy \Rightarrow yRx$;
- (3) *antisymetrická*, pokud $\forall x, y \in X : (xRy \wedge yRx) \Rightarrow x = y$;
- (4) *tranzitivní*, pokud $\forall x, y, z \in X : (xRy \wedge yRz) \Rightarrow xRz$.

Intuice. Na grafu: *reflexivita* = u každého vrcholu smyčka; *symetrie* = každá šipka je obousměrná ($R^{-1} = R$); *antisymetrie* = mezi dvěma různými vrcholy nevedou šipky oběma směry; *tranzitivita* = vede-li cesta $x \rightarrow y \rightarrow z$, vede i přímá zkratka $x \rightarrow z$. Antisymetrie nezakazuje smyčky – omezuje jen dvojice *různých* prvků.



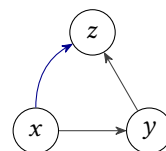
reflexivita
smyčka u každého



symetrie
obousměrné šipky



antisymetrie
jen jeden směr



tranzitivita
zkratka $x \rightarrow z$

Poznámka. Antisymetrie z definice výše je tzv. *slabá* antisymetrie: obousměrnou dvojici zakazuje jen pro *různé* prvky, smyčku xRx povoluje. Ekvivalentně $\forall x, y \in X, x \neq y : xRy \Rightarrow \neg yRx$. Vynecháme-li podmínku $x \neq y$, dostaneme *silnou* (ostrou) antisymetrii, též *asymetrii*: $\forall x, y \in X :$

$xRy \Rightarrow \neg yRx$ – ta navíc vylučuje i smyčky (je tedy ireflexivní). Slabou antisymetrii používá *neostré* uspořádání $\leq$ (reflexivní), asymetrie odpovídá *ostrému* uspořádání $<$ (ireflexivní). Označení „(slabě) antisymetrická“ v příkladech níže míní právě tuto slabou variantu.

1.1 Ekvivalence a rozkladové třídy

Některé relace vyjadřují „stejnost v nějakém ohledu“ (stejný zbytek po dělení, stejná barva). To jsou ekvivalence a my ukážeme, že přesně odpovídají rozkladům množiny na disjunktní části.

Definice – Ekvivalence a třída ekvivalence

Relace R na X je *ekvivalence*, je-li reflexivní, symetrická a tranzitivní. Pro $x \in X$ je *třída ekvivalence* prvku x množina $[x]_R = \{y \in X : xRy\}$.

Definice – Rozklad množiny

Rozklad množiny X je systém neprázdných, navzájem disjunktních podmnožin X , jejichž sjednocením je celé X . Jednotlivé podmnožiny se nazývají *třídy rozkladu*.

★ Věta – Ekvivalence a rozklady si odpovídají

Nechť R je ekvivalence na X . Pak třídy $[x]_R$ tvoří rozklad množiny X , tj.

- (1) každá třída je neprázdná a $x \in [x]_R$;
- (2) pro libovolná x, y je buď $[x]_R = [y]_R$, nebo $[x]_R \cap [y]_R = \emptyset$.

Naopak každý rozklad X definuje ekvivalenci („být ve stejné třídě“) a tato dvě přiřazení jsou navzájem inverzní. Ekvivalence na X tedy odpovídají jedna ku jedné rozkladům X .

 **Intuice.** Bod (1) je reflexivita. Klíčový bod (2) říká, že třídy se nepřekrývají „napůl“: buď splynou, nebo jsou disjunktní. Důvod: leží-li z ve dvou třídách $[x]$ i $[y]$, pak xRz a zRy , takže ze symetrie a tranzitivity xRy , a obě třídy jsou stejné. Ekvivalence a rozklad jsou tedy jen dva pohledy na totéž.

Příklad – Typické ekvivalence

Kongruence modulo n : $x \sim y \iff n \mid (x - y)$ na $\mathbb{Z}$ má n tříd (zbytkové třídy $0, 1, \dots, n - 1$). Relace „mít stejnou velikost“ na podmnožinách dané množiny. Naopak „být nesoudělný“ ekvivalence není (není tranzitivní: 2 a 3, 3 a 4, ale 2 a 4 ne).

Následující reálná otázka kombinuje definici ekvivalence, počítání ekvivalencí a konstrukci relace s předepsanými vlastnostmi. Počet ekvivalencí spočteme rozбором tvarů rozkladu (díky předchozí větě ekvivalence = rozklady).

Příklad – SZZ podzim 2025 č. 4: Binární relace

(Reálná otázka SZZ: podzim 2025, č. 4 – Binární relace)

Zadání.

- (1) Definujte podmínky, které musí splňovat binární relace R na neprázdné množině X , aby byla ekvivalencí (pomocí kvantifikátorů a logických spojek).
- (2) Pro $X = \{a, b, c, d\}$ určete, kolik různých ekvivalencí na X existuje.
- (3) Pro $X = \{a, b, c, d\}$ najděte relaci, která je tranzitivní, ale není symetrická ani (slabě) antisymetrická, a zdůvodněte to. (Antisymetrii se zde míní $\forall x, y \in X : (xRy \wedge yRx) \Rightarrow x = y$.)

Řešení.

- (1) R je ekvivalence, právě když je
 - reflexivní: $\forall x \in X : (x, x) \in R$,

- symetrická: $\forall x, y \in X : (x, y) \in R \Rightarrow (y, x) \in R$,
- tranzitivní: $\forall x, y, z \in X : ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$.

(2) **Rozklady po tvarech.** Ekvivalence na X odpovídají rozkladům X , počítáme tedy rozklady 4-prvkové množiny podle tvaru (velikostí tříd):

tvar 4 :	1 blok,	1 rozklad,
tvar 3 + 1 :	vybíráme samotný prvek $\binom{4}{1}$,	4,
tvar 2 + 2 :	rozdělení na dvojice $\frac{1}{2}\binom{4}{2}$,	3,
tvar 2 + 1 + 1 :	vybíráme dvojici $\binom{4}{2}$,	6,
tvar 1 + 1 + 1 + 1 :	samé singletony,	1.

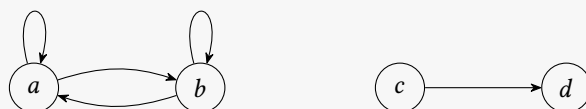
Celkem $1 + 4 + 3 + 6 + 1 = 15$ ekvivalencí. (U tvaru 2 + 2 dělíme dvěma, protože $\binom{4}{2} = 6$ započítává každou dvojici dvojic dvakrát.)

(3) Například $R = \{(a, a), (a, b), (b, a), (b, b), (c, d)\}$.

Tranzitivita. Jediné dvojice, které na sebe navazují, jsou uvnitř bloku $\{a, b\}$ (ten je úplný, takže každá zkratka už v R je) a u (c, d) žádná navazující dvojice $(d, \cdot)$ neexistuje.

Symetrie. $(c, d) \in R$, ale $(d, c) \notin R$ – není symetrická.

Antisymetrie. $(a, b), (b, a) \in R$, přitom $a \neq b$ – není (slabě) antisymetrická.



Graf relace z bodu (3): blok $\{a, b\}$ je úplný (uvnitř tranzitivní), osamocená šipka $c \rightarrow d$ porušuje symetrii a obousměrná dvojice $a \leftrightarrow b$ porušuje antisymetrii.

2 Částečná uspořádání

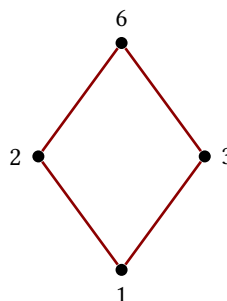
Uspořádání zachycuje vztah „být menší nebo roven“ – ne nutně mezi všemi dvojicemi. Formálně se liší od ekvivalence jen tím, že symetrii nahradíme antisymetrií.

Definice – Uspořádání

Relace $\leq$ na X je (*částečné*) *uspořádání*, je-li reflexivní, antisymetrická a tranzitivní; $(X, \leq)$ pak nazýváme *částečně uspořádaná množina* (ČUM). Uspořádání je *lineární* (úplné), pokud jsou navíc každé dva prvky *porovnatelné*: $\forall x, y \in X : x \leq y \vee y \leq x$. K uspořádání $\leq$ patří jeho *ostrá* varianta $x < y \iff (x \leq y \wedge x \neq y)$.



lineární uspořádání
 $1 < 2 < 3 < 4$



částečné uspořádání
 $(\{1, 2, 3, 6\}, |)$

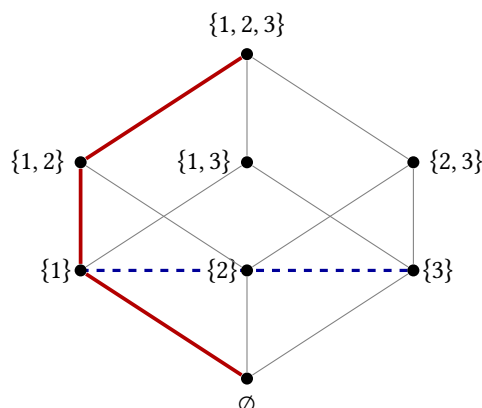
Haseovy diagramy. *Lineární* (vlevo, řetězec $1 < 2 < 3 < 4$): každé dva prvky jsou porovnatelné, body leží svisle nad sebou. *Částečné* (vpravo, dělitelnost na $\{1, 2, 3, 6\}$): prvky 2 a 3 nejsou porovnatelné (ani $2 \mid 3$, ani $3 \mid 2$), diagram má tvar kosočtverce.

Příklad – Uspořádání

$(\mathbb{R}, \leq)$ je lineární. $(2^X, \subseteq)$ (podmnožiny uspořádané inkluzí) a $(\mathbb{N}, |)$ (dělitelnost) jsou jen částečné: $\{1\}$ a $\{2\}$ nejsou inkluzí porovnatelné, stejně jako 2 a 3 dělitelností.

Definice – Hasseův diagram

Hasseův diagram ČUM $(X, \leq)$ je náčrt, v němž x leží níž než y , kdykoli $x < y$, a hranou spojujeme jen *bezprostřední* dvojice: $x < y$ takové, že neexistuje t s $x < t < y$. Ostatní vztahy doplní tranzitivita (čteme je „po cestě vzhůru“).



Hasseův diagram $(2^{\{1,2,3\}}, \subseteq)$. Červeně řetězec $\emptyset \subset \{1\} \subset \{1,2\} \subset \{1,2,3\}$ (délka 4). Modře vyznačená vrstva $\{1\}, \{2\}, \{3\}$ je antiřetězec. Nejmenší prvek je $\emptyset$, největší $\{1,2,3\}$.

Definice – Význačné prvky

V ČUM $(X, \leq)$ je prvek a

- *minimální*, neexistuje-li x s $x < a$; *maximální*, neexistuje-li x s $a < x$;
- *nejmenší*, je-li $\forall x \in X : a \leq x$; *největší*, je-li $\forall x \in X : x \leq a$.

 **Intuice.** Rozdíl „minimální“ vs. „nejmenší“ je zásadní. *Nejmenší* musí být porovnatelný se *všemi* a být pod nimi – proto je nejvýše jeden. *Minimální* jen nesmí mít nic pod sebou, ale nemusí být s ostatními vůbec porovnatelný. V antiřetězci dvou prvků (žádné dva porovnatelné) jsou *oba* minimální i maximální, a přitom není ani nejmenší, ani největší. Nejmenší prvek je vždy i minimální, opačně to neplatí.

Definice – Řetězec, antiřetězec, výška, šířka

Podmnožina $C \subseteq X$ je *řetězec*, jsou-li každé dva její prvky porovnatelné; je *antiřetězec*, nejsou-li žádné dva její různé prvky porovnatelné. *Výška* $v(X, \leq)$ je velikost nejdelšího řetězce, *šířka* $s(X, \leq)$ je velikost nejdelšího antiřetězce.

★ Věta – O dlouhém a širokém

Pro každou konečnou ČUM $(X, \leq)$ platí

$$|X| \leq v(X, \leq) \cdot s(X, \leq),$$

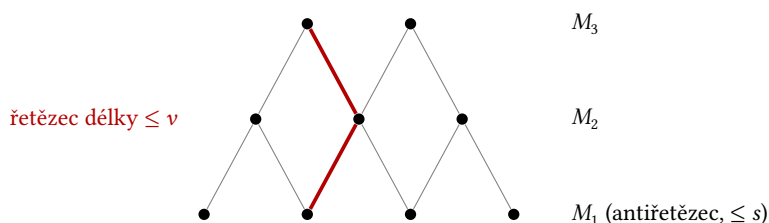
tj. počet prvků nepřevyší součin výšky a šířky.

Intuice. „Buď je něco dlouhé (vysoký řetězec), nebo široké (velký antiřetězec) – jinak se tolik prvků nevejde.“ Myšlenka důkazu: množinu rozvrstvíme na patra minimálních prvků. Každé patro je antiřetězec (nejvýše s prvků) a pater je nejvýše tolik, kolik měří nejdelší řetězec (v), protože každý prvek z k -tého patra je vrcholem řetězce délky k jdoucího skrz všechna nižší patra.

Důkaz (nepovinný – princip). Položme $M_1 = \{\text{minimální prvky } X\}$, $X_1 = X \setminus M_1$, dále $M_2 = \{\text{minimální prvky } X_1\}$ atd., dokud něco zbývá; vznikne rozklad $X = M_1 \cup \dots \cup M_t$. Každé M_i je antiřetězec (dva minimální prvky téže úrovně nemohou být porovnatelné), tedy $|M_i| \leq s$. Je-li $a \in M_k$ pro $k \geq 2$, pak a leží v X_{k-2} (kde $X_0 = X$), ale nebyl v ní minimální (jinak by patřil do M_{k-1}). Pod a tedy v X_{k-2} leží nějaký prvek, a protože je X konečná, i nějaký minimální prvek $a_{k-1} \in M_{k-1}$ s $a_{k-1} < a$; pokračováním dolů dostaneme řetězec $a_1 < a_2 < \dots < a_k = a$ délky k , proto $k \leq v$. Tedy pater je nejvýše v a

$$|X| = \sum_{i=1}^t |M_i| \leq t \cdot s \leq v \cdot s.$$

□



Rozvrstvení na patra minimálních prvků: každé patro je antiřetězec (vodorovně, $\leq s$ prvků), červený řetězec protíná každé patro nejvýše jednou (proto $\leq v$ pater), odtud $|X| \leq v \cdot s$.

Poznámka. Kontrola na obrázku výše: v $(2^{\{1,2,3\}}, \subseteq)$ je výška $v = 4$ (řetězec $\emptyset \subset \{1\} \subset \{1, 2\} \subset \{1, 2, 3\}$) a šířka $s = 3$ (největší antiřetězec, např. trojice jednoprvkových), takže $8 = |X| \leq v \cdot s = 12$.

Příklad – Aplikace: Erdős–Szekeres

Zadání. Z věty o dlouhém a širokém odvoďte: každá posloupnost $n^2 + 1$ navzájem různých reálných čísel obsahuje rostoucí nebo klesající podposloupnost délky alespoň $n + 1$.

Řešení. Na indexech $\{1, \dots, n^2 + 1\}$ definujeme uspořádání $i \preceq j \iff (i \leq j \wedge x_i \leq x_j)$. (Reflexivita, antisymetrie i tranzitivita plynou z téhož pro $\leq$ na obou složkách.) Řetězec v $\preceq$ je rostoucí podposloupnost, antiřetězec je klesající podposloupnost (rostoucí v indexu, ale klesající v hodnotě). Podle věty o dlouhém a širokém je $n^2 + 1 = |X| \leq v \cdot s$, takže $v \geq n + 1$ nebo $s \geq n + 1$ (jinak by $v \cdot s \leq n^2$). To je hledaná podposloupnost délky $n + 1$.

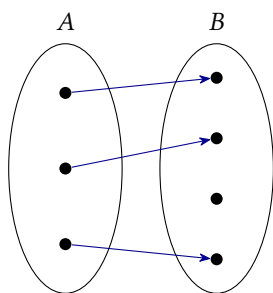
3 Funkce: typy a počty

Funkce je speciální relace, ve které jde z každého prvku právě jedna šipka. Spočítáme, kolik je různých typů funkcí mezi konečnými množinami – základní cvičení „kombinatorického počítání“.

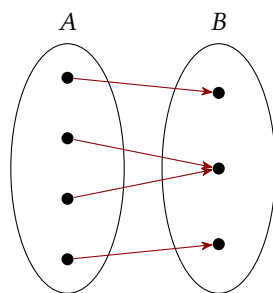
Definice – Funkce a její typy

Relace $f \subseteq X \times Y$ je *funkce* (zobrazení) $f : X \rightarrow Y$, pokud ke každému $x \in X$ existuje právě jedno y s $(x, y) \in f$; píšeme $f(x) = y$. Funkce je

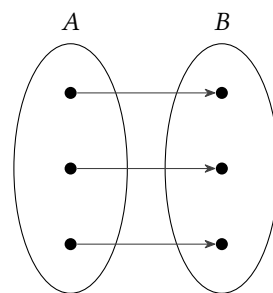
- *prostá* (injektivní): $\forall x, x' \in X : x \neq x' \Rightarrow f(x) \neq f(x')$;
- *na* (surjektivní): $\forall y \in Y \exists x \in X : f(x) = y$;
- *bijekce*: zároveň prostá a na ($\forall y \in Y$ existuje právě jedno x s $f(x) = y$).



injekce (prostá)



surjekce (na)



bijekce (vzájemně jednoznačná)

Tři typy funkcí. *Injekce* (prostá): různé vzory mají různé obrazy, v B smí zůstat nepokrytý prvek. *Surjekce* (na): každý prvek B je pokryt, ale dva prvky A mohou mířit na týž. *Bijekce* (vzájemně jednoznačná): prostá i na zároveň, prvky se párují 1 : 1.

★ Věta – Počty funkcí mezi konečnými množinami

Nechť $|A| = a$ a $|B| = b$. Pak počet

- (1) všech funkcí $A \rightarrow B$ je b^a ;
- (2) prostých funkcí $A \rightarrow B$ je $b(b-1)\dots(b-a+1) = \frac{b!}{(b-a)!}$ (pro $a \leq b$, jinak 0);
- (3) bijekcí $A \rightarrow B$ je $a!$ (jen je-li $a = b$, jinak 0);
- (4) surjekcí $A \rightarrow B$ je $\sum_{k=0}^b (-1)^k \binom{b}{k} (b-k)^a$ (odvodíme v sekci 5 principem inkluze a exkluze).

Intuice. (1) Každý z a prvků poslat nezávisle na kterýkoli z b – $b \cdot b \cdot \dots \cdot b = b^a$. (2) Aby byla prostá, ubývají možnosti: první prvek má b cílů, druhý $b-1$ (jeden je obsazený) atd. (3) Bijekce $A \rightarrow A$ je právě prostá funkce $A \rightarrow A$, tedy $a(a-1)\dots 1 = a!$. Speciálně počet podmnožin X je $|2^X| = 2^{|X|}$ – podmnožiny odpovídají funkcím $X \rightarrow \{0, 1\}$ (charakteristická funkce: 1 pro prvky uvnitř).

✎ Příklad – Počty funkcí

Zadání. Kolik je funkcí, prostých funkcí a bijekcí z $A = \{1, 2, 3\}$ do $B = \{1, 2, 3, 4\}$?

Řešení. Všech: $b^a = 4^3 = 64$. Prostých: $4 \cdot 3 \cdot 2 = 24$. Bijekcí: 0 (je $|A| \neq |B|$, bijekce neexistuje). Naopak prostých funkcí z B do A je 0 (nelze 4 různé prvky injektivně uložit do 3).

✎ Příklad – SZZ léto 2022 č. 4: Injekce a surjekce – definice a počty

(Reálná otázka SZZ: léto 2022, č. 4 – Zobrazení (injekce, surjekce, počty))

Zadání.

- (1) Definujte, kdy je zobrazení $f : X \rightarrow Y$ prosté (injektivní) a kdy „na“ (surjektivní).
- (2) Pro $n \in \mathbb{N}$ určete, kolik existuje prostých zobrazení z $\{1, \dots, n\}$ do $\{1, \dots, 2n\}$.
- (3) Pro $n \in \mathbb{N}$ určete, kolik existuje zobrazení $\{1, \dots, 2n\}$ na $\{1, \dots, n\}$ takových, že pro každé $k \in \{1, \dots, n\}$ existují právě dvě hodnoty i, j s $f(i) = f(j) = k$.

Řešení.

- (1) f je prosté: $\forall a, b \in X : f(a) = f(b) \Rightarrow a = b$ (různé vzory mají různé obrazy). f je na: $\forall y \in Y \exists x \in X : f(x) = y$ (každý prvek Y je obrazem).
- (2) Po prvcích: první obraz má $2n$ možností, druhý $2n-1, \dots, n$ -tý $n+1$, celkem $2n \cdot (2n-1) \cdot \dots \cdot (n+1) = \frac{(2n)!}{n!}$.
- (3) Jde o rozdělení $2n$ prvků do n označených dvojic; uspořádaných $2n$ -tic je $(2n)!$, v každé z n dvojic nezáleží na pořadí, tedy $\frac{(2n)!}{(2!)^n} = \frac{(2n)!}{2^n}$. (Kontrola $n = 2$: prostých $4 \cdot 3 = 12 = \frac{4!}{2!}$, takových surjekcí $\frac{4!}{2^2} = 6$.)

4 Permutace, kombinační čísla, binomická věta

4.1 Permutace

Definice – Permutace, pevný bod

Permutace množiny X je bijekce $p : X \rightarrow X$. Na $[n]$ značíme množinu všech permutací S_n . Pevný bod permutace p je prvek x s $p(x) = x$.

★ Věta – Počet permutací

Permutací n -prvkové množiny je $n! = n(n-1) \cdots 1$.

 **Intuice.** Permutace je prostá funkce $[n] \rightarrow [n]$, takže podle předchozí věty jich je $n(n-1) \cdots 1 = n!$ (první prvek má n obrazů, druhý $n-1$, ...). Permutaci lze rozložit na nezávislé cykly; pevné body jsou právě cykly délky 1. Počet permutací bez pevného bodu spočteme v sekci 5 (problém šatnářky).

4.2 Kombinační čísla

Definice – Kombinační číslo

Pro celá $0 \leq k \leq n$ je kombinační číslo

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1) \cdots (n-k+1)}{k!}.$$

★ Věta – Kombinační číslo počítá podmnožiny

$\binom{n}{k}$ je počet k -prvkových podmnožin n -prvkové množiny, tj. $|\binom{X}{k}| = \binom{|X|}{k}$.

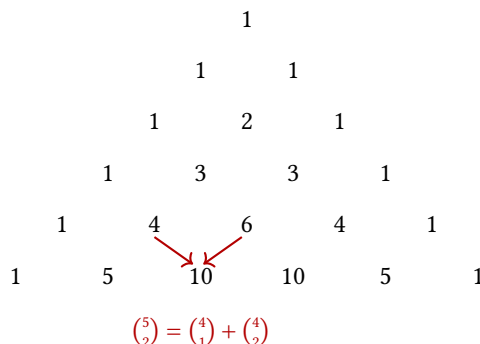
 **Intuice.** Uspořádaných k -tic různých prvků z n -prvkové X je $n(n-1) \cdots (n-k+1)$ (prostá funkce $[k] \rightarrow X$). Každá k -prvková podmnožina dá $k!$ takových k -tic (jejím přerovnáním). Proto počet podmnožin je podíl $\frac{n(n-1) \cdots (n-k+1)}{k!} = \binom{n}{k}$.

★ Věta – Vztahy mezi kombinačními čísly

Pro $0 \leq k \leq n$ platí

- (1) symetrie: $\binom{n}{k} = \binom{n}{n-k}$;
- (2) Pascalův vztah: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$;
- (3) součet řádku: $\sum_{k=0}^n \binom{n}{k} = 2^n$;
- (4) alternující součet: $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ (pro $n \geq 1$).

Intuice. (1) Vybrat k prvků „dovnitř“ je totéž jako vybrat $n - k$ „ven“. (2) Zafixujeme jeden prvek: k -prvkové podmnožiny ho buď neobsahují ($\binom{n-1}{k}$ způsobů), nebo obsahují a zbytek vybíráme z ostatních ($\binom{n-1}{k-1}$). To je pravidlo „sčítání dvou čísel nad sebou“ v Pascalově trojúhelníku. (3) Součet počtů podmnožin všech velikostí je počet všech podmnožin 2^n . (4) Plyne dosazením $a = 1, b = -1$ do binomické věty níže – podmnožin sudé velikosti je stejně jako lichých.



Pascalův trojúhelník. Každé číslo je součtem dvou nad ním (Pascalův vztah); součet n -tého řádku je 2^n .

4.3 Binomická věta

★ Věta – Binomická věta

Pro $n \in \mathbb{N}_0$ a libovolná a, b (z komutativního okruhu, např. $\mathbb{R}$) platí

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Intuice. Roznásobujeme n závorek $(a + b)$. Z každé vybereme buď a , nebo b ; výsledný člen s právě k vybranými b je $a^{n-k} b^k$ a počet způsobů, jak vybrat oněch k závorek dávajících b , je $\binom{n}{k}$. Sečtením přes k dostaneme vzorec.

🔧 Příklad – Aplikace binomické věty

Zadání. Odvoďte $\sum_{k=0}^n \binom{n}{k} = 2^n$ a $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.

Řešení. Dosazením $a = b = 1$: $(1 + 1)^n = \sum_k \binom{n}{k} 1^{n-k} 1^k = \sum_k \binom{n}{k}$, tedy 2^n . Dosazením $a = 1, b = -1$: $(1 - 1)^n = 0 = \sum_k \binom{n}{k} (-1)^k$ (pro $n \geq 1$). Druhý vztah říká, že podmnožin sudé velikosti je stejně jako lichých.

5 Princip inkluze a exkluze

Chceme spočítat velikost sjednocení množin, které se mohou překrývat. Sečíst velikosti nestačí (průniky se započtou víckrát); princip inkluze a exkluze je systematicky „přičítá a odečítá“.

★ Věta – Princip inkluze a exkluze

Pro konečné množiny $A_1, \dots, A_n$ platí

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} \sum_{\substack{I \subseteq [n] \\ |I|=k}} \left| \bigcap_{i \in I} A_i \right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

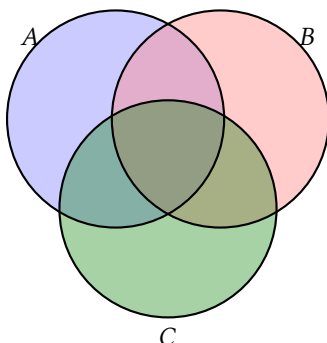
Pro $n = 2$ je to známé $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

Intuice. „Přičti jednotlivé, odečti dvojnásobně započtené průniky dvojic, přičti zpět trojic, ...“
Sudé průniky se odečítají, liché přičítají, aby každý prvek byl nakonec započten přesně jednou.

Důkaz (počítací). Ukážeme, že každý prvek $x \in \bigcup A_i$ je na obou stranách započten právě jednou. Vlevo jednou (je ve sjednocení). Vpravo: leží-li x v právě j množinách ($j \geq 1$), pak $x \in \bigcap_{i \in I} A_i$ právě pro ty I , které jsou podmnožinami oněch j množin; takových I velikosti k je $\binom{j}{k}$. Příspěvek x vpravo je tedy

$$\sum_{k=1}^j (-1)^{k-1} \binom{j}{k} = - \sum_{k=1}^j (-1)^k \binom{j}{k} = - \left(\underbrace{\sum_{k=0}^j (-1)^k \binom{j}{k}}_{=(1-1)^j=0} - \binom{j}{0} \right) = -(0 - 1) = 1.$$

Obě strany tedy počítají každý prvek jednou. □



Vennův diagram tří množin: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.
Překryvy se nejdřív odečtou (jsou započteny dvakrát) a trojitý průnik se zpět přičte.

5.1 Použití (1): problém šatnářky

Příklad – Problém šatnářky – permutace bez pevného bodu

Zadání. n pánů odevzdá v šatně klobouky a šatnářka jim je vrátí náhodně, každému jeden. Jaká je pravděpodobnost, že *nikdo* nedostane svůj klobouk? Ekvivalentně: kolik je permutací $D(n)$ na $[n]$ bez pevného bodu?

Řešení. Vrácení klobouků je náhodná permutace π ; „pán i dostal svůj“ znamená pevný bod $\pi(i) = i$. Spočteme „špatné“ permutace (alespoň jeden pevný bod). Pro $i \in [n]$ nechť $A_i = \{\pi \in S_n : \pi(i) = i\}$. Pak $|A_i| = (n-1)!$ (ostatních $n-1$ prvků libovolně) a obecně pro $i_1 < \dots < i_k$ je $|\bigcap_j A_{i_j}| = (n-k)!$ (zafixujeme k bodů).

Inkluze–exkluze.

$$\left| \bigcup_i A_i \right| = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^n (-1)^{k-1} \frac{n!}{k!},$$

takže permutací bez pevného bodu je

$$D(n) = n! - \left| \bigcup_i A_i \right| = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

Limita. Hledaná pravděpodobnost je $\frac{D(n)}{n!} = \sum_{k=0}^n \frac{(-1)^k}{k!} \xrightarrow{n \rightarrow \infty} \boxed{e^{-1} \approx 0,368}$. Pozoruhodné je, že na počtu pánů skoro nezáleží.

5.2 Použití (2): Eulerova funkce

Příklad — Eulerova funkce $\varphi(n)$

Zadání. $\varphi(n)$ je počet čísel $m \in [n]$ nesoudělných s n (tj. $\gcd(n, m) = 1$). Odvoďte vzorec pomocí prvočíselného rozkladu $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Řešení. „Špatná“ $m \leq n$ (soudělná s n) jsou právě násobky některého z prvočísel p_i . Nechť $A_i = \{m \in [n] : p_i \mid m\}$; pak $|A_i| = \frac{n}{p_i}$ a obecně $|\bigcap_j A_{i_j}| = \frac{n}{p_{i_1} \cdots p_{i_k}}$ (násobky součinu příslušných prvočísel). Je $\varphi(n) = n - |\bigcup_i A_i|$, tedy principem inkluze a exkluze

$$\varphi(n) = n \sum_{I \subseteq \{1, \dots, r\}} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i} = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Například $\varphi(12) = \varphi(2^2 \cdot 3) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$ (čísla 1, 5, 7, 11).

 **Intuice.** Roznásobením součinu $n \prod_i (1 - \frac{1}{p_i})$ dá přesně střídavou sumu inkluze a exkluze: člen $\frac{(-1)^{|I|} n}{\prod_{i \in I} p_i}$ pro každou podmnožinu prvočísel I . (Požadavky M3 tuto funkci zmiňují slovy „Eulerova funkce pro počet dělitelů“; míní se jí právě φ , tj. počet zbytkových tříd nesoudělných s n .)

5.3 Použití (3): počet surjekcí

Příklad — Počet surjekcí

Zadání. Spočítejte počet surjekcí (funkcí „na“) z a -prvkové množiny A na b -prvkovou množinu B .

Řešení. Spočteme „špatné“ funkce (nejsou na, tedy nějaký prvek B vynechají). Pro $y \in B$ nechť $A_y = \{f : A \rightarrow B : y \notin f(A)\}$ (funkce vynechávající y). Pak $|A_y| = (b-1)^a$ (cíľ je jen $b-1$) a obecně průnik k takových množin (vynechání k daných prvků) má velikost $(b-k)^a$; množin velikosti k je $\binom{b}{k}$. Funkcí, které vynechají aspoň jeden prvek, je $|\bigcup_y A_y|$, takže surjekcí je

$$b^a - \left| \bigcup_y A_y \right| = \sum_{k=0}^b (-1)^k \binom{b}{k} (b-k)^a.$$

(Tím je doplněn bod (4) věty o počtech funkcí. Např. surjekcí $[3] \rightarrow [2]$ je $2^3 - 2 = 6$.)

6 Hallova věta o SRR a párování v bipartitním grafu

Máme rodinu množin a chceme z každé vybrat jednoho „reprezentanta“ tak, aby byli navzájem různí. Kdy to jde? Odpověď dává Hallova věta, která tento výběr převádí na párování v bipartitním grafu.

Definice — Systém různých reprezentantů

Množinový systém nad X je rodina $\mathcal{M} = (M_i : i \in I)$ podmnožin X (množiny se mohou opakovat). Systém různých reprezentantů (SRR) je prostá funkce $f : I \rightarrow X$ taková, že $f(i) \in M_i$ pro každé $i \in I$ – z každé množiny vybere jeden prvek a vybrané prvky jsou navzájem různé.

Definice — Párování, bipartitní a incidenční graf

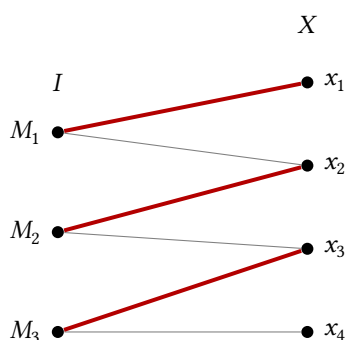
Bipartitní graf je graf s vrcholy rozdělenými na dvě části V_1, V_2 tak, že každá hrana spojuje vrchol z V_1 s vrcholem z V_2 . Párování je množina hran, z nichž žádné dvě nesdílejí vrchol. Incidenční graf

systému $\mathcal{M}$ je bipartitní graf $B_{\mathcal{M}} = (I \cup X, \{ \{i, x\} : x \in M_i \})$.

★ Lemma – SRR jako párování

SRR v $\mathcal{M}$ existuje, právě když v $B_{\mathcal{M}}$ existuje párování velikosti $|I|$ (párování „nasycující“ celé I).

💡 **Intuice.** Hrana $\{i, x\}$ párování znamená „reprezentantem M_i je x “. Že se hrany párování nedotýkají, znamená přesně, že každé i má svého reprezentanta a žádné dva nesdílejí tentýž prvek x – to je definice SRR.



Incidenční graf systému $M_1 = \{x_1, x_2\}$, $M_2 = \{x_2, x_3\}$, $M_3 = \{x_3, x_4\}$. Červené párování velikosti 3 dává SRR $f(1) = x_1$, $f(2) = x_2$, $f(3) = x_3$.

★ Věta – Hallova věta

SRR v konečném systému $\mathcal{M} = (M_i : i \in I)$ existuje, právě když platí *Hallova podmínka*

$$\forall J \subseteq I : \left| \bigcup_{j \in J} M_j \right| \geq |J|.$$

📺 **Video:** *Wrath of Math, Hall's Theorem and Condition for Bipartite Matchings (Hallova věta a Hallova podmínka pro párování v bipartitním grafu).*

💡 **Intuice.** Podmínka je zjevně *nutná*: každých $|J|$ množin musí dohromady obsahovat aspoň $|J|$ různých prvků, jinak z nich nelze vybrat $|J|$ různých reprezentantů. Hallova věta říká, že tato samozřejmá nutná podmínka je i *postačující* – to je její netriviální obsah. Postačitelnost dokážeme elegantně *přes toky*: hledání SRR převedeme na hledání maximálního toku v síti. Párování velikosti $|I|$ odpovídá toku velikosti $|I|$ ze zdroje do stoku, a Hallova podmínka přesně zaručí, že *každý* řez je velký (alespoň $|I|$) – takže i maximální tok je velký a celé I nasytí.

Princip důkazu. Nutnost. Je-li f SRR, pak $\bigcup_{j \in J} M_j \supseteq \{f(j) : j \in J\}$ a prvky $f(j)$ jsou navzájem různé, takže $|\bigcup_{j \in J} M_j| \geq |J|$.

Postačitelnost (přes toky v sítích), ve čtyřech krocích:

- (1) **Síť.** Z incidenčního grafu $B_{\mathcal{M}}$ uděláme síť (viz obrázek níže): přidáme zdroj z s hranami $z \rightarrow i$ pro každé $i \in I$, ponecháme hrany $i \rightarrow x$ pro $x \in M_i$ a přidáme hrany $x \rightarrow s$ do stoku s pro každé $x \in X$. Všem hranám dáme kapacitu 1.
- (2) **Tok = párování.** Celočíslný tok velikosti t odpovídá párování velikosti t v $B_{\mathcal{M}}$: hrana $i \rightarrow x$, po níž teče jednotka, je párovací hrana, a jednotkové kapacity zaručí, že každé i i každé x je nejvýše v jedné. Maximální (celočíslný) tok najde Fordův–Fulkersonův algoritmus.
- (3) **Každý řez má velikost $\geq |I|$.** U minimálního řezu lze předpokládat, že přetíná jen hrany $z \rightarrow i$ a $x \rightarrow s$ (kdyby přetínal nějakou hranu $i \rightarrow x$, lze ji nahradit hranou $z \rightarrow i$ na téže cestě, aniž se řez

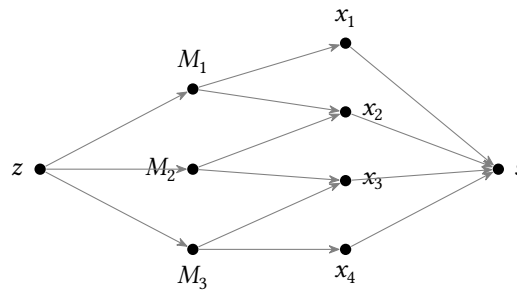
zvětší). Označme $A \subseteq I$ vrcholy, jejichž hrana $z \rightarrow i$ přefatá *není*. Pak řez obsahuje $|I| - |A|$ hran $z \rightarrow i$ (pro $i \notin A$) a – aby z A nic neproteklo do stoku – všechny hrany $x \rightarrow s$ pro $x \in \bigcup_{i \in A} M_i$. Proto

$$\text{velikost řezu} \geq (|I| - |A|) + \left| \bigcup_{i \in A} M_i \right| \geq (|I| - |A|) + |A| = |I|,$$

kde prostřední nerovnost je právě Hallova podmínka pro $J = A$.

- (4) **Závěr.** Podle věty o maximálním toku a minimálním řezu je maximální tok roven nejmenšímu řezu, tedy $\geq |I|$ (a zároveň $\leq |I|$, víc ze zdroje nevyteče). Maximální tok má tak velikost $|I|$ – to je párování nasycující celé I , a podle lemmatu výše je to hledaný SRR.

□



Síť pro důkaz Hallovy věty (systém $M_1 = \{x_1, x_2\}$, $M_2 = \{x_2, x_3\}$, $M_3 = \{x_3, x_4\}$ z obrázku výše): $z \rightarrow I \rightarrow X \rightarrow s$, všechny kapacity 1. Celočíselný tok velikosti $|I|$ je párování nasycující I , tj. SRR.

i Poznámka. Předvedený důkaz je zároveň *algoritmem*: SRR (resp. maximální párování) najde Fordův–Fulkersonův algoritmus v **polynomiálním** čase. Síť má jednotkové kapacity, takže každé hledání zlepšující cesty zvětší tok o 1; cest je nejvýše $|I|$ a každá se najde prohledáním grafu (BFS/DFS) v čase $O(|E|)$. Celkem $O(|I| \cdot |E|)$ – polynom ve velikosti vstupu. (Konstrukci sítě i větu o maximálním toku a minimálním řezu podrobně rozebírá okruh M4 – toky v sítích; Hallovu větu lze dokázat i přímo indukcí nebo z Tutteovy věty, tok ale navíc dává konstruktivní algoritmus.)

Příklad – Použití Hallovy věty

Zadání.

- (1) Pro systém $M_1 = \{1, 2\}$, $M_2 = \{2, 3\}$, $M_3 = \{1, 3\}$ ověřte Hallovu podmínku a najděte SRR.
- (2) Ukažte, že systém $M_1 = M_2 = M_3 = \{1, 2\}$ žádný SRR nemá.

Řešení.

- (1) Stačí ověřit sjednocení pro všechny $J \subseteq I$: jednoprvkové dají $|M_i| = 2 \geq 1$; každá dvojice dá $M_i \cup M_j = \{1, 2, 3\}$, tj. $3 \geq 2$; celé $M_1 \cup M_2 \cup M_3 = \{1, 2, 3\}$ má velikost $3 \geq 3$. Hallova podmínka platí, SRR tedy existuje – například $f(1) = 1$, $f(2) = 2$, $f(3) = 3$ (různí reprezentanti, $f(i) \in M_i$).
- (2) Pro $J = \{1, 2, 3\}$ je $|\bigcup_{j \in J} M_j| = |\{1, 2\}| = 2 < 3 = |J|$. Hallova podmínka neplatí, takže SRR neexistuje: tři množiny by potřebovaly tři navzájem různé reprezentanty, ale dohromady nabízejí jen dva prvky.

★ Důsledek – Postačující podmínka přes stupně

Je-li v bipartitním grafu $B = (V_1 \cup V_2, E)$ s neprázdnou množinou hran pro každé dva vrcholy $x \in V_1$, $y \in V_2$ splněno $\deg_B x \geq \deg_B y$, pak existuje párování nasycující V_1 .

💡 Intuice. Položíme $M_i =$ sousedé vrcholu $i \in V_1$. Pro $J \subseteq V_1$ a $B(J) = \bigcup_{i \in J} M_i$ je počet hran mezi J a $B(J)$ alespoň $|J| \cdot \min \deg$ a nejvýše $|B(J)| \cdot \max \deg$; z předpokladu $\min_{V_1} \deg \geq \max_{V_2} \deg$ pak plyne $|J| \leq |B(J)|$, tedy Hallova podmínka. (Důsledkem je např. tvrzení, že každý *latinský obdélník* $k \times n$ s $k < n$ lze doplnit na latinský čtverec $n \times n$.)

Shrnutí

i Poznámka. Klíčové vlastnosti a vzorce (přehled k SZZ). Stručný výčet klíčových definic, vět a vzorců okruhu M3. Zkratky: ČUM = částečně uspořádaná množina, SRR = systém různých reprezentantů.

Vlastnosti binárních relací.

- Relace R na X : *reflexivní* $\forall x : xRx$; *symetrická* $xRy \Rightarrow yRx$; *antisymetrická* $(xRy \wedge yRx) \Rightarrow x = y$; *tranzitivní* $(xRy \wedge yRz) \Rightarrow xRz$.
- Antisymetrie (slabá) povoluje smyčky – zakazuje jen obousměrné hrany mezi *různými* vrcholy. Asymetrie (ostrá) zakáže navíc smyčky (je ireflexivní).
- Složení $R \circ S = \{(x, z) : \exists y, xRy \wedge ySz\}$; inverzní $R^{-1} = \{(y, x) : (x, y) \in R\}$.

Ekvivalence a rozklady.

- Ekvivalence = refl. + sym. + trans. Třída prvku x : $[x]_R = \{y : xRy\}$.
- Ekvivalence na $X \iff$ rozklady X (třídy disjunktní, pokrývají X) – 1:1 korespondence.
- Počet ekvivalencí na n -prvkové X = počet rozkladů n -prvkové množiny. Pro $n=4$: rozbor tvarů 4; 3+1; 2+2; 2+1+1; 1+1+1+1 dá $1 + 4 + 3 + 6 + 1 = 15$.

Částečná uspořádání.

- *Uspořádání* = refl. + antisym. + trans.; *lineární* (úplné): navíc každé dva porovnatelné. Příklady: $(\mathbb{R}, \leq)$ lineární; $(2^X, \subseteq)$, $(\mathbb{N}, |)$ jen částečná.
- *Minimální* prvek: nic pod ním (neexistuje t s $t < a$). *Nejmenší*: menší nebo roven všem ($\forall x : a \leq x$). *Nejmenší* $\Rightarrow$ *minimální*; opačně ne. *Nejmenší* je nejvýše jeden; *minimálních* může být více.
- *Řetězec*: každé dva prvky porovnatelné. *Antiřetězec*: žádné dva různé porovnatelné. *Výška* v = délka nejdelšího řetězce; *šířka* s = velikost největšího antiřetězce.
- **Věta o dlouhém a širokém**: $|X| \leq v \cdot s$. Důkaz: rozvrstvit na patra minimálních prvků – každé patro je antiřetězec ($\leq s$ prvků), pater je $\leq v$ (prvek k -tého patra leží v řetězci délky k).
- Erdős–Szekeres: v posloupnosti n^2+1 různých čísel existuje rostoucí nebo klesající podposloupnost délky $\geq n+1$ (ČUM na indexech: řetězec = rostoucí, antiřetězec = klesající, $n^2+1 \leq v \cdot s$).

Funkce: typy a počty.

- *Prostá* (injekce): $f(a) = f(b) \Rightarrow a = b$. *Na* (surjekce): $\forall y \in Y \exists x \in X : f(x) = y$. *Bijekce*: prostá i na.
- Počty $f : A \rightarrow B$, $|A| = a$, $|B| = b$: všech b^a ; *prostých* $\frac{b!}{(b-a)!}$ (pro $a \leq b$, jinak 0); *bijekcí* $a!$ (jen $a = b$, jinak 0); *surjekcí* viz inkluze-exkluze níže.
- Speciálně: k -prvkových podmnožin n -prvkové X je $\binom{n}{k}$; všech podmnožin 2^n ; permutací $n!$.

Permutace a pevný bod.

- Permutace $[n] =$ bijekce $[n] \rightarrow [n]$; celkem $n! = n(n-1) \cdots 1$ permutací. *Pevný bod*: $p(x) = x$.
- Permutace bez pevného bodu (šatnářka): $D(n) = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$; pravděpodobnost $\frac{D(n)}{n!} \rightarrow e^{-1} \approx 0,368$ pro $n \rightarrow \infty$, skoro nezávislá na n .

Kombinační čísla a binomická věta.

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ = počet k -prvkových podmnožin n -prvkové X . Symetrie: $\binom{n}{k} = \binom{n}{n-k}$. Pascal: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
- Součty: $\sum_{k=0}^n \binom{n}{k} = 2^n$; $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ (pro $n \geq 1$; sudých podmnožin je stejně jako lichých).
- *Binomická věta*: $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$. Dosazením $a=b=1$ dostaneme 2^n ; $a=1, b=-1$ dostaneme 0.

Princip inkluze a exkluze.

- Obecná formulace: $|\bigcup_{i=1}^n A_i| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |\bigcap_{i \in I} A_i|$.
- Počítací důkaz: prvek v právě j množinách přispěje $\sum_{k=1}^j (-1)^{k-1} \binom{j}{k} = 1$.
- Šatnářka: $D(n) = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$ (permutace bez pevného bodu; $A_i = \{\pi : \pi(i) = i\}$, $|A_i| = (n-1)!$).
- Eulerova funkce: $\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ = počet $m \leq n$ s $\gcd(m, n) = 1$; pro $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ a

$$A_i = \{m \leq n : p_i \mid m\}.$$

- Počet surjekcí $A \rightarrow B$: $\sum_{k=0}^b (-1)^k \binom{b}{k} (b-k)^a$ (pro b^a všech funkcí odečteme ty, co vynechají aspoň jeden prvek B).

Hallova věta a SRR.

- SRR systému $\mathcal{M} = (M_i : i \in I)$: prostá $f : I \rightarrow X$ s $f(i) \in M_i$ pro všechna i ; ekvivalentní párování velikosti $|I|$ v incidenčním bipartitním grafu.
- **Hallova věta**: SRR existuje $\iff$ *Hallova podmínka*: $\forall J \subseteq I : |\bigcup_{j \in J} M_j| \geq |J|$ (každých $|J|$ množin má dohromady $\geq |J|$ prvků).
- Princip důkazu (postačitelnost): síť $z \rightarrow I \rightarrow X \rightarrow s$, kapacity 1; tok velikosti $|I| = \text{SRR}$; každý řez $\geq |I|$ z Hallovy podmínky; max-tok = min-řez $\Rightarrow$ tok velikosti $|I|$ existuje.
- Polynomiální algoritmus: Ford–Fulkerson v síti s jednotkovými kapacitami, čas $O(|I| \cdot |E|)$.

Zdroje

- T. Sláma: *Diskrétní matematika*, zápisky z přednášky NDMI002 (přednášející M. Mareš), MFF UK, 2019/20 (primární zdroj výkladu relací, uspořádání, počítání a inkluze a exkluze).
<https://slama.dev/poznamky/diskretni-matematika/>
- J. Matoušek, J. Nešetřil: *Kapitoly z diskrétní matematiky*, Karolinum; anglicky *Invitation to Discrete Mathematics*, 2. vydání, Oxford University Press, 2008 (učebnice k oběma předmětům; aplikace inkluze a exkluze, SRR).
- T. Valla, J. Matoušek: *Kombinatorika a grafy I*, skripty, MFF UK, 2008 (kap. 4: systémy různých reprezentantů a Hallova věta).
<https://iuuk.mff.cuni.cz/~valla/kg.html>
- M. Mareš: *Kombinatorika do kapsy*, MFF UK, 2022 (kombinační čísla a binomická věta).
<https://mj.ucw.cz/papers/komb-tahak.pdf>
- Wrath of Math: *Hall's Theorem and Condition for Bipartite Matchings* (video odkazované v textu).
<https://www.youtube.com/watch?v=Ihr6gMx7b9c>
- MFF UK: požadavky ke státní závěrečné zkoušce (Informatika, Bc.) a zadání otázek z minulých termínů.
<https://www.mff.cuni.cz/cs/studenti/bakalarske-studium/statni-zaverecne-zkousky/bakalarske-statni-zkousky-studijniho-programu-informatika>