

Mohutnost množin a počet dvojic

Definice: Počet prvků konečné množiny X nazýváme *mohutnost* X a značíme ji $|X|$.

Pozorování: Když existuje bijekce mezi množinami X a Y , pak $|X| = |Y|$.

Definice: *Kartézský součin* množin X a Y je množina $X \times Y = \{(x, y) : x \in X, y \in Y\}$, čili množina *všech uspořádaných* dvojic.

Pozorování: Mají-li konečné množiny X a Y mohutnosti n a m , potom jejich kartézský součin $X \times Y$ má mohutnost nm .

Důkaz: $X \times Y$ je množina dvojic, první prvek má n možností, druhý m . Každý výběr prvního prvku lze nezávisle rozšířit o druhý, proto je celkový počet možností dán součinem nm .

Ukázka: Má-li si 200 studentů zapsat 5 přednášek, dostaneme $200 \cdot 5 = 1\,000$ záznamů (p, s) o zápisu přednášky p studentem s .



René Descartes
1596 – 1650

[Obr. Wikipedie]

Počet n -tic

Věta: Z prvků konečné množiny X lze vytvořit $|X|^3$ různých uspořádaných trojic. Pro $n \in \mathbb{N}$ máme $|X|^n$ uspořádaných n -tic.

... intuitivně: pro trojice jde o mohutnost kartézského součinu $X \times X \times X$ a pro n -tice $|X|^n = \underbrace{|X \times X \times \dots \times X|}_{n\text{-krát}}$

Ukázka: IP adresu tvoří uspořádaná čtveřice čísel v rozsahu 0–255, proto různých IP adres je $256^4 = 4\,294\,967\,296$.

Na této větě si předvedeme princip důkazu *matematickou indukcí*:

Důkaz: $P(n)$: „Na konečné X je $|X|^n$ uspořádaných n -tic.“

I. $P(1)$: konečná X má $|X|$ prvků — „uspořádaných 1-tic“,

II. $P(n) \Rightarrow P(n+1)$: Uspořádaných n -tic je podle indukčního předpokladu $|X|^n$. Každou n -tici lze rozšířit $|X|$ způsoby na $(n+1)$ -tici přidáním prvku z X na poslední, $(n+1)$. místo.

Vytvoříme celkem $|X|^n \cdot |X| = |X|^{n+1}$ různých $(n+1)$ -tic, protože se liší buď v prvních n nebo v posledním prvku.

Každou $(n+1)$ -tici $(x_1, \dots, x_{n+1})$ lze takto vytvořit z n -tice $(x_1, \dots, x_n)$ a prvku x_{n+1} , a tak žádná nechybí, ani nepřebývá.

Matematická indukce



[Foto: Pixabay]

Výrok typu: „Pro každé $n \in \mathbb{N}$ platí $P(n)$ “, například $P(n)$: „Na konečné X je $|X|^n$ uspořádaných n -tic.“ lze dokázat ve dvou krocích:

- I. platí $P(1)$ — *první krok* indukce,
- II. pro každé n lze z *indukčního předpokladu* $P(n)$ odvodit $P(n+1)$ — *indukční krok*: $P(n) \Rightarrow P(n+1)$.

Když od $P(1)$ použijeme II. krok $(n-1)$ -krát za sebou, dostaneme posloupnost implikací: $P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \dots \Rightarrow P(n)$.

Začátek posloupnosti platí díky I., a proto platí i její ostatní členy.

Číslo n může být libovolné, proto $P(n)$ platí pro všechna $n \in \mathbb{N}$.

Varianty: Když místo $P(1)$ dokážeme $P(0)$, platí $P(n)$ pro všechna nezáporná celá n ; když místo $P(n) \Rightarrow P(n+1)$ dokážeme $P(n) \Rightarrow P(n+2)$, platí $P(n)$ pro všechna lichá $n \in \mathbb{N}$, atd.

Indukční krok lze provést i pomocí implikace se silnějšími předpoklady: $(P(1) \wedge P(2) \wedge \dots \wedge P(n-1)) \Rightarrow P(n)$

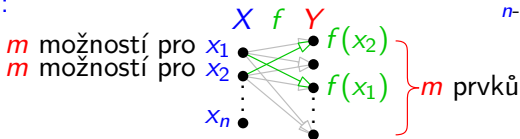
Počet zobrazení

Věta: Mají-li konečné množiny X a Y mohutnosti n a m , potom existuje m^n různých zobrazení $f: X \rightarrow Y$.

Důkaz: Pokud si označíme $X = \{x_1, \dots, x_n\}$, potom každé zobrazení f odpovídá jednoznačně uspořádané n -tici prvků z Y , jmenovitě $(f(x_1), f(x_2), \dots, f(x_n))$ a těchto n -tic je m^n .

Jde o bijekci mezi množinou všech zobrazení, tj. $\{f: X \rightarrow Y\}$ a množinou všech možných n -tic prvků z Y , tj. $\underbrace{Y \times Y \times \dots \times Y}_{n\text{-krát}}$.

Jiný pohled:



Ukázky: Pokud 5 dětem rozdáváme po jednom kusu ze čtyř možných druhů ovoce (jablko, hruška, meruňka a švestka), lze to provést $4^5 = \underbrace{4 \cdot 4 \cdot \dots \cdot 4}_{5 \times} = 1\,024$ způsoby.

Počet slov s k písmeny z n -prvkové abecedy je n^k .

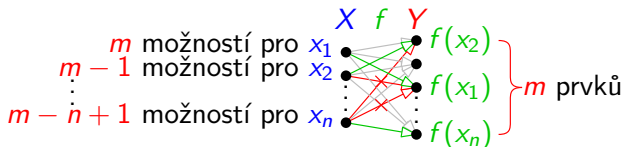
Počet prostých zobrazení

Věta: Mají-li konečné množiny X a Y mohutnosti n a m , potom existuje $m(m-1)(m-2)\cdots(m-n+1)$ různých **prostých** zobrazení $f: X \rightarrow Y$.

... pro $n > m$ je jeden činitel nulový a žádné prosté f neexistuje.

Značení: **Klesající mocnina** je $m^n = m(m-1)\cdots(m-n+1)$.

Důkaz:



Ukázka: Pokud si 5 dětí vybere po jedné z 8 různých hraček, mohou si je vybrat $8^5 = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6\,720$ způsoby.

Zobrazení odpovídají uspořádaným výběrům s opakováním (úloha o rozdávání ovoce), zatímco prostá zobrazení odpovídají uspořádaným výběrům bez opakování (úloha o rozdávání hraček).

Důsledek: **Uspořádaných** výběrů k prvků z n -prvkové množiny je n^k pro výběry **bez opakování**, a n^k pro výběry **s opakováním**.

Faktoriál



Definice: Součin $1 \cdot 2 \cdot 3 \cdots n = \prod_{i=1}^n i$

se nazývá *n faktoriál* a značí se $n!$.

... počet prostých zobrazení pak lze vyjádřit:

$$m^n = m(m-1)(m-2) \cdots (m-n+1) = \frac{m!}{(m-n)!}$$

Poznámka: $0! = 1$ (odpovídá prázdnému součinu).

Důsledek: Na n -prvkové množině je $n!$ permutací.

Seřazení prvků množiny X lze reprezentovat jako bijekci mezi množinou pozic $\{1, \dots, n\}$ a množinou X .

Důsledek: Různých seřazení prvků n -prvkové množiny je také $n!$.

Ukázky: Na 26 písmenech je $26!$ různých substitučních šifer.

Odhad faktoriálu



Otázka: Jak rychle roste faktoriál?

Přímočarý odhad: $n! \leq n^n$

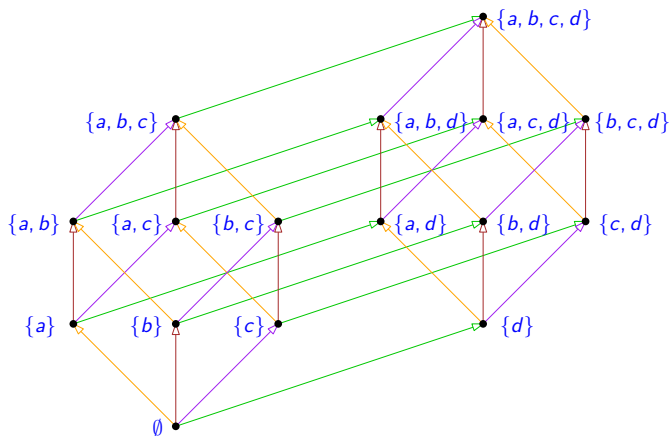
$$(n!)^2 = (\underset{\text{green}}{1} \cdots \underset{\text{red}}{n})(\underset{\text{red}}{1} \cdots \underset{\text{green}}{n}) = \prod_{k=1}^n k(n+1-k) \Rightarrow n! = \sqrt{\prod_{k=1}^n k(n+1-k)}$$

Z nerovností $n \leq k(n+1-k) \leq \left(\frac{n+1}{2}\right)^2$ plyne: $n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$

Přesnější odhad dává tzv. *Stirlingova formule*: $n! \simeq \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

Počet podmnožin

Věta: Konečná množina X mohutnosti n ,
má 2^n různých podmnožin, neboli $|\mathcal{P}(X)| = 2^{|X|}$.

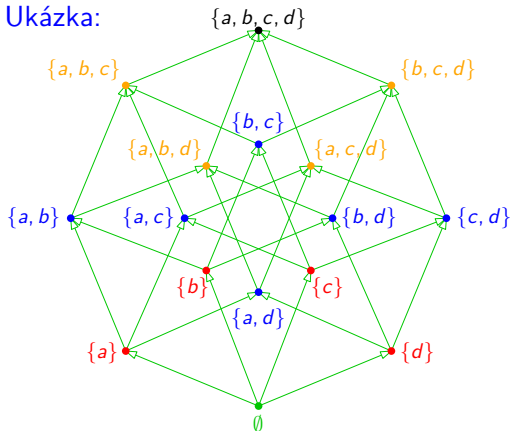


Počet podmnožin předepsané velikosti

Věta: Pro každou n -prvkovou množinu X a $k \in \{0, \dots, n\}$ platí, že X má $\frac{n^k}{k!} = \frac{n!}{(n-k)!k!}$ podmnožin velikosti k .

Definice: Číslo $\frac{n!}{(n-k)!k!}$ je *binomický koeficient* a značí se $\binom{n}{k}$.

Ukázka:



$$\binom{4}{4} = \frac{4!}{0! \cdot 4!} = \frac{24}{1 \cdot 24} = 1$$

$$\binom{4}{3} = \frac{4!}{1! \cdot 3!} = \frac{24}{1 \cdot 6} = 4$$

$$\binom{4}{2} = \frac{4!}{2! \cdot 2!} = \frac{24}{2 \cdot 2} = 6$$

$$\binom{4}{1} = \frac{4!}{3! \cdot 1!} = \frac{24}{6 \cdot 1} = 4$$

$$\binom{4}{0} = \frac{4!}{4! \cdot 0!} = \frac{24}{24 \cdot 1} = 1$$

Vlastnosti binomických koeficientů

Pascalův trojúhelník je uspořádání binomických koeficientů znázorňující vztah:

$$\underbrace{\binom{n-1}{k-1} + \binom{n-1}{k}}_{\binom{n}{k}}$$

Pro $k < 0$ a $k > n$ se definuje $\binom{n}{k} = 0$.

$$\begin{array}{ccccccc} & & 1 & = & \binom{0}{0} & & \\ & & 1 & = & \binom{1}{0} & 1 & = & \binom{1}{1} \\ & 1 & = & \binom{2}{0} & 2 & = & \binom{2}{1} & 1 & = & \binom{2}{2} \\ 1 & = & \binom{3}{0} & 3 & = & \binom{3}{1} & 3 & = & \binom{3}{2} & 1 & = & \binom{3}{3} \\ 1 & = & \binom{4}{0} & 4 & = & \binom{4}{1} & 6 & = & \binom{4}{2} & 4 & = & \binom{4}{3} & 1 & = & \binom{4}{4} \end{array}$$

$$\begin{array}{c} 1 \\ 1 + 1x \\ 1 + 2x + 1x^2 \\ 1 + 3x + 3x^2 + 1x^3 \\ 1 + 4x + 6x^2 + 4x^3 + 1x^4 \end{array}$$

Pozorování:

- ▶ $\binom{n}{k} = \binom{n}{n-k}$... každá množina má jednoznačný doplněk.
- ▶ $\sum_{k=0}^n \binom{n}{k} = 2^n$... odpovídá počtu všech podmnožin.

Binomická věta

Věta: Pro každé $n \in \mathbb{N}$ platí:

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

Důkaz 1: Rozepíšeme $(1+x)^n = \underbrace{(1+x)(1+x)\dots(1+x)}_{n \times}$.

Člen x^k lze při roznásobení získat tak, že z k dvoučlenů $(1+x)$ zvolíme x a z ostatních $n-k$ dvoučlenů zvolíme 1 . Koeficient $\binom{n}{k}$ u x^k je počet možností, kolikrát lze z n -prvkové množiny dvoučlenů vybrat k -prvkovou podmnožinu, tj. dvoučleny, z nichž volíme x .

Důkaz 2: Indukcí podle n : Pro $n=1$: $(1+x)^1 = 1x^0 + 1x^1$.

Indukční krok: $(1+x)^n = (1+x)^{n-1}(1+x)$. Člen $(1+x)^{n-1}$

zapišeme podle indukčního předpokladu jako $\sum_{k=0}^{n-1} \binom{n-1}{k}x^k$,

jehož součin s $(1+x)$ pak algebraicky upravíme na $\sum_{k=0}^n \binom{n}{k}x^k$:

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

Důsledky a zobecnění binomické věty

$\sum_{k=0}^n \binom{n}{k} = 2^n$... dosazením $x = 1$ do binomické věty.

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

... anebo kombinatoricky stejně jako u binomické věty.

Multinomická věta:

$$(x_1 + x_2 + \dots + x_t)^n = \sum_{\substack{k_1, k_2, \dots, k_t \in \{0, 1, \dots, n\} \\ k_1 + k_2 + \dots + k_t = n}} \binom{n}{k_1, k_2, \dots, k_t} x_1^{k_1} x_2^{k_2} \dots x_t^{k_t}$$

kde $\binom{n}{k_1, k_2, \dots, k_t} = \frac{n!}{k_1! k_2! \dots k_t!}$ je **multinomický koeficient**.

Ukázka: $(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz$. Koeficient u xz je dán volbou $k_x = 1$, $k_y = 0$ a $k_z = 1$ a $\binom{2}{1, 0, 1} = \frac{2!}{1! 0! 1!} = 2$.

Multinomický koeficient $\binom{n}{k_1, \dots, k_t}$ udává počet rozdělení n -prvkové množiny na navzájem disjunktní¹ množiny o velikostech $k_1, \dots, k_t$.

Užití: Počet přesmyček slova MISSISSIPPI: $\binom{11}{1, 4, 4, 2} = \frac{11!}{1! 4! 4! 2!} = 34\,650$.

¹ **disjunktní** znamená „neprotínající se“: A a B jsou disjunktní $\Leftrightarrow A \cap B = \emptyset$.

Neuspořádané výběry s opakováním a bez opakování

Podobně znějící úlohy: Kolika způsoby lze rozdělit mezi 5 dětí

- ▶ 3 třešně, každé může mít nejvýše jednu?
- ▶ 7 malin, čili některé jich dostane i víc než jednu?

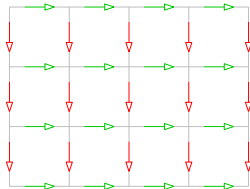
První úloha odpovídá výběru tříprvkové podmnožiny dětí, tj. těch, které dostanou třešně. To lze provést $\binom{5}{3} = 10$ způsoby. Jiný pohled: počítáme rozklady $3 = a_1 + \dots + a_5$, kde $a_i \in \{0, 1\}$.

Ve druhé rozkládáme $7 = a_1 + \dots + a_5$ bez dalších podmínek. Každý rozklad, např. $\boxed{0} + \boxed{4} + \boxed{1} + \boxed{0} + \boxed{2}$ lze zapsat v unární soustavě, čili $\boxed{} + \boxed{////} + \boxed{/} + \boxed{} + \boxed{//}$. Prázdná pozice na kraji a mezi dvěma sousedními $+$ odpovídají nulovému sčítanci. Jde o řetězce délky 11 se sedmi symboly $/$ a čtyřmi symboly $+$. Takových posloupností, a tedy i rozdělení malin je $\binom{11}{7} = 330$.

Důsledek: *Neuspořádaných* výběrů k prvků z n -prvkové množiny je $\binom{n}{k}$ pro výběry *bez opakování*, a $\binom{n+k-1}{k}$ pro výběry *s opakováním*.

Otázky k porozumění tématu přednášky

- ▶ Jaká je souvislost mezi asociativitou součinu a počtem k -tic?
- ▶ Jak se mění počet zobrazení vzhledem ke skládání, případně provedením množinových operací na nosných množinách?
- ▶ Jak souvisí Pascalův trojúhelník s počtem nejkratších cest mezi dvěma protilehlými body mřížky $m \times n$?



Otázka z úvodu o počtu vyhodnocení databázových dotazů i počtu některých turnajů souvisí s tzv. *Catalanovými čísly*. Ta mj. udávají počet cest ve čtvercové mřížce, které nevstoupí pod diagonálu.

Poznámky k pojmosloví a značení

Pojem „permutace“ někdy označuje *počet* permutací (coby vzájemně jednoznačných zobrazení). Počtu zobrazení se také říká „variace“, přičemž „variace s opakováním“ berou v potaz všechna zobrazení a „variace bez opakování“ jen prostá. Podobně termín „kombinace bez opakování“ je totéž co binomický koeficient.

Binomický koeficient se často nazývá *kombinační číslo*.

Množina *k*-prvkových podmnožin množiny *X* se může značit $\binom{X}{k}$.