Přehled přednášky

Kapitola 3. Důkazy v diskrétní matematice

- základní logické symboly
- pojem matematického důkazu
- princip matematické indukce
- důkazy vztahů pro kombinatorické výběry
- binomická věta
- několik důkazů „počítáním“

3. Důkazy v diskr. matematice

Matematika se jako vědní disciplína vyznačuje svou exaktností. Rozumíme tím schopnost dokázat tvrzení nade vší pochybnost.

Pojem matematického důkazu se vyvíjel několik století. K nejznámějším historicky doloženým důkazům patří:

- grafické důkazy Pythagorovy věty (tvrzení: Babylonská tabulka cca. 1900–1600 př.n.l., „Rhindův Papyrus“ z Egypta 1788–1580 př.n.l., důkaz: Pythagorejská škola cca. 560-480 př.n.l., v Číně cca. 500–200 před n.l.)
- Euklidovy „Základy“ cca 300 př.n.l.

V moderní matematice: pojem matematického důkazu je posloupnost elementárních ověřitelných kroků vedoucích od známých/předpokládaných faktů k novému/požadovanému tvrzení.

V diskrétní matematice jsou základní předpoklady tvořeny axiomy tzv. Peanovy aritmetiky (tj. dobře známá fakta o přirozených číslech společně s principem matematické indukce).

3.1. Základní logické symboly

Známé pojmy:

- *Výrok* je tvrzení, o kterém má smysl rozhodnout, zda je *pravdivé* či *nepravdivé*
- *Logické hodnoty*: 1/0, True/False, Pravda/Nepravda
- *Logické spojky*: „NOT“ $\neg X$, „AND“ $X \wedge Y$, „OR“ $X \vee Y$
- *Implikace*: „jestliže (je pravda) X, pak (musí být) Y“ $X \Rightarrow Y$
- *Ekvivalence*: „X (je pravda), právě když Y (je pravda)“ $X \Leftrightarrow Y$
- Kvantifikátory:
  všeobecný „Pro každé $x \in M$ platí tvrzení $P(x)$“
  píšeme: $\forall x \in M : P(x)$
  existenční „Existuje $x \in M$, pro které platí tvrzení $P(x)$“
  píšeme: $\exists x \in M : P(x)$
  Množinu M můžeme vynechat, pokud je zřejmé o jakou M se jedná.

Negace je *unární* operátor, $\wedge, \vee, \Rightarrow, \Leftrightarrow$ jsou *binární operátory*.

Další operátory jsou kombinací: $A \text{ XOR } B$ je totéž jako $\neg(A \Leftrightarrow B)$

3.2. Pojem matematického důkazu

Struktura *věty* (tvrzení) v matematice: $P \Rightarrow T$
Přesně formulované *předpoklady* P, za kterých platí *tvrzení věty* T.

Podrobný postup, jak z předpokladů odvodit tvrzení věty nazýváme *důkaz*.

Matematický důkaz nějakého tvrzení T je konečná posloupnost kroků/výroků, kde každý krok je:

- *axiom* – obecně platný či předpokládaný fakt
  (volba axiomů závisí na matematické teorii),
- *předpoklad* tvrzení T,
- *výrok odvozený* z předchozích kroků užitém některého z platných odvozovacích pravidel (závisí na použité logice).

Poslední krok obsahuje jako výrok tvrzení T.

Různá odvětví matematiky vychází z různých axiomů. Zatímco diskrétní matematika vychází z *Peanových axiomů*, například geometrie (nejstarší exaktně budovaná matematická disciplína) vychází z pěti *Euklidových axiomů*.

Příklad:

O inverzním prvku Dokážeme, že v libovolné (i nekomutativní!) algebraické grupě platí komutativita operace vzhledem k „násobení inverzním prvkem". Tj. jestliže $A \cdot B = E$, potom také $B \cdot A = E$

Vzpomeňte na násobení regulárních matic: jednotková matice má smysl pouze pro regulární matice, neboť existuje inverzní matice.

Grupa $(G, \cdot)$ je množina prvků s jednou operací, pro kterou platí nějaké vlastnosti, tzv. *axiomy grupy*. Nás zajímají tři

1. operace je asociativní:
2. v grupě existuje „jednička":
3. ke každému prvku existuje prvek inverzní:

Poznámka: Při psaní důkazů můžeme některé elementární kroky vynechat, případně zkrátit. Nesmí však být porušena korektnost tvrzení (vynechat některý předpoklad). Míra „zkratky" závisí i na očekávaném „průměrném čtenáři".

Grupa $(G, \cdot)$ je množina prvků s jednou operací, pro kterou platí tzv. *axiomy grupy*. Využijeme následující tři axiomy

1. operace je asociativní:
   $\forall A, B, C \in G : (A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. v grupě existuje „jednička“:
   $\exists E \in G : E \cdot A = A \cdot E = A$ pro $\forall A \in G$
3. ke každému prvku existuje prvek inverzní:
   $\forall A \in G \; \exists A^{-1} : A \cdot A^{-1} = E \;\wedge\; A^{-1} \cdot A = E.$

Důkaz tvrzení:

$$
\begin{array}{rcll}
A \cdot B & = & E & \text{předpoklad} \\
A^{-1} \cdot (A \cdot B) & = & A^{-1} \cdot E & \text{z axiomu 3. existuje } A^{-1} \\
(A^{-1} \cdot A) \cdot B & = & A^{-1} & \text{z axiomu 1. a axiomu 2.} \\
E \cdot B & = & A^{-1} & \text{z axiomu 3.} \\
B & = & A^{-1} & \text{z axiomu 2.} \\
B \cdot A & = & A^{-1} \cdot A & \\
B \cdot A & = & E & \text{z axiomu 3.}
\end{array}
$$

Základní důkazové techniky

- přímý důkaz $A \Rightarrow B$
- nepřímý důkaz $\neg B \Rightarrow \neg A$
- důkaz sporem $A \wedge \neg B \Rightarrow spor$ ($spor$ je současná platnost T a $\neg T$)
- důkaz matematickou indukcí ($slabá$ a $silná$)

Příklad:
Každé liché číslo je možno napsat jako rozdíl dvou čtverců.
Ukážeme přímo.
Mějme liché číslo $2k+1$, potom $2k+1 = k^2 + 2k + 1 - k^2 = (k+1)^2 - k^2$.

Příklad:
Prvočísel je nekonečně mnoho.
Víme, že každé číslo je možno napsat jako součin prvočísel. Sporem:
Předpokládáme, že prvočísel je konečně mnoho, označíme je $p_1, p_2, \ldots, p_n$ (*jsou všechna*). Ale číslo $x = p_1 \cdot p_2 \cdots p_n + 1$ není dělitelné ani jedním z prvočísel! Máme spor (= má současně platit nějaké tvrzení i jeho negace), proto předpoklad nepravdivý, tj. prvočísel je nekonečně mnoho.

3.3. Princip matematické indukce

Princip matematické indukce je jedna z nejčastěji používaných důkazových technik pro tvrzení závislá na parametru $n \in \mathbb{N}$ (označujeme $P(n)$).

Matematická indukce

Mějme tvrzení $P(n)$ s celočíselným parametrem n. Nechť platí:

- Tvrzení $P(n_0)$ je pravdivé, kde $n_0 = 0$ nebo 1, nebo obecné celé n_0. Číslo n_0 nazýváme *základ indukce*.
- Pro libovolné $n \in \mathbb{N}$ z platnosti $P(n)$ plyne platnost tvrzení $P(n+1)$. Tvrzení $P(n)$ nazýváme v tomto kroku *indukční předpoklad*.

Pak $P(n)$ platí pro všechna přirozená $n \geq n_0$.

Silná matematická indukce

- Tvrzení $P(n_0)$ je pravdivé (základ indukce).
- Z platnosti tvrzení $P(n)$ pro $\forall n_0 \leq n < k$ plyne platnost tvrzení $P(k)$.

Pak $P(n)$ platí pro všechna přirozená $n \geq n_0$.

Matematickou indukci lze dobře využít i při dokazování správnosti algoritmů.

Věta 3.4.
Všech zobrazení libovolné b-prvkové množiny do a-prvkové množiny je a^b.
Důkaz matematickou indukcí podle b:

- Pro $b = 0$ máme jedinou možnost (jak nic nepřiřadit: $a^b = a^0 = 1$).
- Pro $b = 1$ máme a možných obrazů pro jediný prvek ($a^b = a^1 = a$).
- Nechť nyní tvrzení platí pro $b \geq 0$.
  Mějme libovolnou množinu B o $b + 1 > 0$ prvcích. Zvolme nějaký prvek $x \in B$ a označme $B' = B \setminus \{x\}$, $|B'| = b$. Všech zobrazení z B' do A je podle indukčního předpokladu a^b. Pro prvek x máme navíc nezávislý výběr z a možných obrazů. Celkem je dle principu nezávislých výběrů $a \cdot a^b = a^{b+1}$ různých zobrazení z B do A.

Podle principu matematické indukce je důkaz dokončen. □

Věta 3.3. (o počtu podmnožin konečné množiny)
Každá n-prvková množina má právě 2^n podmnožin.

$$\left|2^X\right| = 2^{|X|}$$

Příklad:
Pro nalámání čokolády rozměru $p \times r$ dílků je vždy potřeba $pr - 1$ zlomů.

Důkaz silnou matematickou indukcí podle $n = pr$:

- Pro $n_0 = 1$ máme jeden dílek a je třeba $pr - 1 = 0$ zlomů.
- Nechť nyní tvrzení platí pro všechny čokolády o méně než k dílcích. Mějme libovolnou tabulku o k dílcích. Tabulku rozlomíme a dostaneme dvě menší tabulky o s, t dílcích, kde $1 \leq s, t < k$ a $s + t = k$. Každou z nich umíme podle předpokladu nalámat pomocí $s-1$ resp. $t-1$ zlomů. Celkem je třeba $(s - 1) + (t - 1) + 1 = s + t - 1 = k - 1$ zlomů.

Podle principu silné matematické indukce je důkaz dokončen. $\square$

3.4. Důkazy vztahů pro kombinatorické výběry

Při důkazech využijeme matematickou indukci a metodu dvojího počítání.

Věta 3.5. Počet všech permutací n-prvkové množiny je $n!$, pro každé $n \geq 0$.

Důkaz indukcí podle n:
Tvrzení platí pro $n = 0$, protože žádné prvky lze uspořádat jen jedním způsobem (stejně jednoprvkové množiny).

Mějme nyní $n \geq 0$ a množinu P o $n+1$ prvcích, předpokládejme pro jednoduchost $P = \{1, 2, \ldots, n+1\}$. Zvolme první prvek $p \in P$ naší permutace jedním z $n+1$ způsobů. Nemůžeme přímo říci, že potom je volba zbytku permutace $P \setminus \{p\}$ nezávislá na volbě prvního p, neboť formálně to není pravda. Jedná se o permutaci *jiné množiny*. Nejprve musíme zbylé prvky $P \setminus \{p\}$ „přečíslovat“ na $\{1, 2, \ldots, n\}$, což počet voleb neovlivní.

Pak už plyne jasně – n-prvková množina $\{1, 2, \ldots, n\}$ má podle indukčního předpokladu $n!$ permutací, proto P má celkem $(n+1) \cdot n! = (n+1)!$ permutací. To je požadované tvrzení. $\square$

Věta 3.6. Počet všech k-prvkových variací z n-prvkové množiny je $\frac{n!}{(n-k)!}$, pro každé $n \geq k \geq 0$.

Důkaz metodou dvojího počítání:
Dvěma způsoby spočítáme počet permutací n-prvkové množiny. Jak víme, lze tyto permutace vybrat $n!$ různými způsoby. Na druhou stranu lze vzít některou k-prvkovou variaci, její prvky dát na začátek permutace (dodržíme pořadí) a *zbylých* $n-k$ *prvků seřadíme za nimi jedním z* $(n-k)!$ *různých způsobů*. Z různých variací tímto postupem zřejmě získáme různé výsledné permutace, a přitom každou permutaci lze získat z variace vybírající jejích prvních k prvků.

Označíme-li x neznámý počet všech k-prvkových variací z n-prvkové množiny, lze výše popsaným postupem vytvořit právě $x \cdot (n-k)!$ všech různých permutací n-prvkové množiny. Proto platí

$$\begin{aligned} x \cdot (n-k)! &= n! \\ x &= \frac{n!}{(n-k)!}. \end{aligned}$$

□

Věta 3.7. Počet všech k-prvkových kombinací z n-prvkové množiny je $\binom{n}{k}$, pro každé $n \geq k \geq 0$.

Důkaz metodou dvojího počítání:
Nyní budeme dvojím způsobem počítat všechny k-prvkové variace z n-prvkové množiny. Na jednu stranu už víme, že jich je $\frac{n!}{(n-k)!}$, na druhou stranu můžeme z *jedné k-prvkové kombinace vygenerovat celkem $k!$ různých variací* uspořádáním prvků této kombinace. Označíme-li tedy x neznámý počet všech k-prvkových kombinací z n-prvkové množiny, dostaneme, obdobně jako v předchozím důkazu,

$$\begin{aligned} x \cdot k! &= \frac{n!}{(n-k)!} \\ x &= \frac{n!}{k! \cdot (n-k)!} \\ x &= \binom{n}{k}. \end{aligned}$$

□

3.5. Důkazy vztahů s kombinačními čísly

Pro kombinační čísla můžeme dokázat celou řadu zajímavých vztahů. Zabývá se jimi dokonce celá samostatná část diskrétní matematiky.

Fakt (na první pohled zřejmé tvrzení) Pro všechna $n \geq 0$ platí

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Fakt Pro všechna $n \geq k \geq 0$ platí

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

Tvrzení, jejichž důkaz spočívá v dosazení do definice, případně, která vyžadují je jednu nebo dvě jednoduché úpravy považujeme za „zřejmá“ tvrzení a jejich důkaz se neuvádí.
Na druhou stranu tvrzení, jejichž důkaz vyžaduje nějaký „trik“, nebo neobvyklé úpravy (byť jen jednu jedinou úpravu), bývá zvykem stručně vysvětlit.

Lemma 3.8. (pomocné tvrzení) Pro všechna $n \geq k \geq 0$ platí
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Důkaz přímý (dosazením a úpravou)

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

□

Uvedené vztahy mohou sloužit jako *alternativní definice kombinačních čísel*.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n}{k} = \binom{n}{n-k} \qquad \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Pascalův trojúhelník

$$\binom{0}{0} = 1$$

$$\binom{1}{0} = 1 \quad \binom{1}{1} = 1$$

$$\binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1$$

$$\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1$$

$$\binom{5}{0} = 1 \quad \binom{5}{1} = 5 \quad \binom{5}{2} = 10 \quad \binom{5}{3} = 10 \quad \binom{5}{4} = 5 \quad \binom{5}{5} = 1$$

. . . .

Krajní členy mají hodnoty 1, každý vnitřní člen je součtem dvou členů bezprostředně nad ním.

Věta 3.9. Binomická věta Pro všechna $n > 0$ platí

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Důkaz Tvrzení je možno dokázat indukcí. Avšak možný je i důkaz jednoduchou úvahou (s využitím Věty 3.7.):
Algebraickém rozvoji součinu používáme pravidlo „vynásobit každý člen s každým". Proto se v rozvoji vztahu $\underbrace{(1+x)(1+x)\dots(1+x)}_{n}$ člen x^k objeví tolikrát, kolik je možností (neuspořádaně) vybrat k z n činitelů – závorek. To je právě $\binom{n}{k}$ krát = počet k prvkových podmnožin z n prvků. □

Z binomické věty ihned plyne (pro přirozená $n \geq 0$ a druhé pro $n > 0$)

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n\,,$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots - (-1)^n\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0\,.$$

3.6. Důkazy „metodou počítání“

Někdy máme ukázat existenci nějakého objektu nebo vlastnosti, aniž jsme schopni objekt zkonstruovat nebo jinak specifikovat. Takovým důkazům říkáme *nekonstruktivní*, někdy také *existenční*.

Místo abychom řešení „zkonstruovali“, tak se nám podaří „spočítat“, že řešení musí existovat.

Metoda 3.11. Dirichletův princip (the pigeon-hole principle)

Rozmístíme-li $\ell + 1$ (nebo více) objektů do ℓ přihrádek, v některé přihrádce musí být alespoň dva objekty.

Důkazy počítáním možností

Existenci konkrétní možnosti ze známé množiny ukážeme, jestliže spočítáme, že případů, kdy možnost nemůže nastat je menší než celkový počet případů.

Příklad:

Vidíme, jak do tunelu vjedou tři auta a jen dvě vidíme vyjet ven. To znamená, že jedno auto v tunelu zůstalo (přestože ho nyní nevidíme).

Příklad:

8 kamarádů jelo na 9 dní dovolené. Každý den některá (jedna) trojice z nich šla na výlet. Dokažte, že někteří dva z nich ani jednou nebyli spolu na výletě.

Důkaz rozebírání možností by asi k ničemu nevedlo...

Důkaz počítáním je však snadný: Jedna trojice má celkem 3 dvojice, proto po 9 dnech se mohlo vystřídat *nejvýše různých* $9 \cdot 3$ *dvojic*, ale $9 \cdot 3 = 27 < \binom{8}{2} = 28$, jedna dvojice nám zde schází.

Otázka:

Žijí na Zemi dva lidé, kteří mají stejný počet vlasů?

Příklad:
V šuplíku je (poházeno) 30 párů černých ponožek, 10 párů hnědých ponožek a 3 páry bílých ponožek. Kolik musíme potmě vytáhnout ponožek, abychom měli jistotu, že máme alespoň jeden pár stejné barvy?

„Přihrádky“ Dirichletova principu budou odpovídat třem různým barvám. Vytáhneme-li čtyři ponožky (nerozlišujeme pravou a levou ponožku), musí být alespoň dvě ponožky stejné barvy.

Příklad:
Máme 4 přirozená čísla. Ukažte, že mezi nimi vždy najdete dvě čísla tak, aby jejich rozdíl dělitelný číslem 3.

Příklad:
Máme 3 přirozená čísla. Ukažte, že mezi nimi vždy najdete dvě čísla tak, aby jejich součet byl dělitelný nějakým prvočíslem.

Příklad:
Máme 5 přirozených čísel. Ukažte, že mezi nimi vždy najdeme dvě čísla tak, že jejich součet je dělitelný 9.

Důkaz (chybný!) Celkem máme 9 různých zbytkových tříd po dělení číslem 9. Z pěti čísel můžeme získat 10 různých součtů. Jistě bude v každé zbytkové třídě alespoň jeden součet, v některé budou dokonce dva součty. Proto dvojice čísel, jejichž součet odpovídá zbytkové třídě 0, má rozdíl čísel dělitelný devíti. □

Otázka:
Co je špatně na uvedeném důkazu předchozího tvrzení?
nápověda: zkuste úlohu rozebrat pro množinu pěti čísel $\{0, 2, 4, 6, 8\}$

Příště

Kapitola 4. Relace

- motivace
- pojem relace
- uspořádání a ekvivalence
- funkce a zobrazení
- skládání zobrazení
- princip inkluze a exkluze