

Študijný poriadok, čl. 13, ods (3).

Preukázaná nečestnosť študenta pri hodnotení študijných výsledkov (zistenie opisovania, použitie nedovolených pomôcok a iných praktík, plagiátorstvo apod.) má za následok hodnotenie klasifikačným stupňom FX – nedostatočne (čl. 16 tohto študijného poriadku). Takéto konanie je porušenie zásad študijnej morálky a môže byť predmetom disciplinárneho konania.

Motivácia

- Cieľom predmetu Teoretické základy informatiky je poskytnúť informácie o teoretických (matematických) modeloch výpočtu, t.j. o tom, na čom je teoreticky informatika založená.
- Každý výpočtový stroj je totižto praktickou realizáciou nejakého teoretického formálneho konceptu.
- Na tomto predmete si vysvetlíme niekoľko formálnych modelov výpočtu, počnúc jednoduchými konečnými automatmi a končiac Turingovými strojmi, ktoré predstavujú matematický model bežného výpočtového zariadenia.



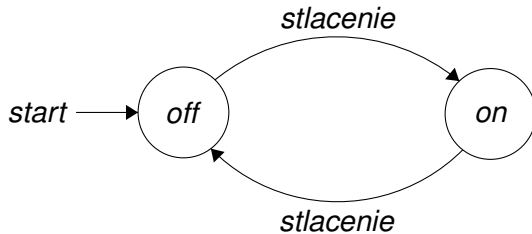
Motivácia

- Prvý koncept, s ktorým budeme pracovať, budú konečné automaty.
- Medzi jeho využitia patrí:
 - Návrh a overenie správania digitálnych obvodov.
 - Lexikálna analýza pri preklade programu.
 - Vyhľadávanie slov / fráz v textoch, resp. hľadanie postupnosti bajtov v dátach.
 - Overovanie systémov majúcich konečný počet stavov (komunikačné protokoly).
 - Formálny model správania sa systému.



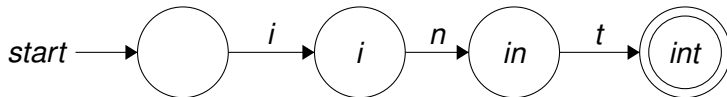
Motivačný príklad

Uvažujme nasledovný (formálny) model vypínača. Vždy si pamätá, či je vypínač vypnutý alebo zapnutý a modeluje, čo sa udeje, ak sa stlačí tlačidlo vypínača, t.j. ak je vypínač vypnutý a tlačidlo sa stlačí, tak sa vypínač zapne a naopak, ak je vypínač zapnutý a tlačidlo sa stlačí, tak sa vypínač vypne.



Motivačný príklad 2

Iným príkladom môže byť algoritmus, ktorý rozpoznáva v texte kľúčové slová - napríklad reťazec *int*. Jeho model pomocou konečného automatu by mohol vyzeráť nasledovne:



Automaty a zložitost'

Konečné automaty a najmä Turingové stroje poskytujú odpovede na 2 dôležité otázky:

- Čo vôbec počítače dokážu (a nedokážu) - s tým súvisí tzv. rozhodnuteľnosť (decidability) - táto problematika bude odprednášaná v rámci tohto predmetu.
- Čo dokážu počítače robiť efektívne - s tým súvisí tzv. zložitosť algoritmov (complexity) - táto problematika bude odprednášaná v rámci predmetu Analýza a zložitosť algoritmov.



Formálne dôkazy

- Existuje oblasť teoretickej informatiky, tzv. formálne metódy, ktorá sa o.i. zaoberá tým, že je človek schopný **formálne** dokázať korektnosť svojho algoritmu.
- To my robiť nebudeme, avšak počas tohto predmetu budeme často potrebovať dokázať nejaké vety / tvrdenia o automatoch, preto je dobré, aby sme si pripomenuli základné typy dôkazov rôznych tvrdení.
- Často budeme používať tzv. dôkaz indukciou, ktorý má svoju silnú oporu v programovaní v cykloch a rekurziách.
- Zopakujme si teraz tie časti dôkazov, ktoré budeme na tomto predmete potrebovať.



Príklad

Dokážeme, že platí veta: **Ak $x \geq 4$, potom $2^x \geq x^2$.**

- Veta má tvar implikácie, v ktorej predpokladom (hypotézou) je, že $x \geq 4$ a záverom je, že v takom prípade $2^x \geq x^2$.
- Vidíme, že aj hypotéza, aj záver, sú tvrdenia, ktoré môžu / nemusia byť pravdivé (podľa toho, akú hodnotu má x).
- Ak skúsime dosádzať za x čísla, tak vidíme, že pre $x = 3$ je $2^3 = 8$ a $3^2 = 9$. T.j. záver je nepravdivý - avšak aj predpoklad je nepravdivý.
- Ak dosadíme za $x = 4$, t.j. hypotéza bude pravdivá, dostaneme aj pravdivý záver, lebo $(2^4 = 16) \geq (4^2 = 16)$.
- Podobne pre $x = 5$ platí, že $(2^5 = 32) \geq (5^2 = 25)$



Príklad

- Samozrejme dosadiť do tvrdenia pár hodnôt a overiť platnosť je z hľadiska dôkazov absolútne nepostačujúce... maximálne získame väčšiu istotu (potenciálne falošnú) v platnosť tvrdenia.
- Reálny dôkaz musíme vykonať analyticky / pre všetky hodnoty.
- Uvažujme, čo sa stane, keď bude x rásť o 1, t.j. z x urobíme $x + 1$.

Príklad

- Teda vidíme, že pre rastúce x rastie 2^x **rýchlejšie (viac)** než x^2 .
- Teda ak začneme s hodnotou $x = 4$, kde sa oba výrazy rovnajú a x bude rásť, tak potom keďže 2^x rastie rýchlejšie než x^2 , tak musí platiť, že **ak** $x \geq 4$, **tak potom** $2^x \geq x^2$.
- Teda sme z hypotézy pomocou postupnosti logických krokov vyvodili požadovaný záver.
- Samotný dôkaz nebol úplne formálne korektný, avšak mal slúžiť na demonštráciu toho, ako z nejakého tvrdenia môžeme dokázať platnosť iného tvrdenia postupnosťou logických krokov.

Príklad 2

Dokážme tvrdenie: **Ak x je súčet druhých mocnín 4 prirodzených čísel, potom $2^x \geq x^2$**

- Intuitívne toto tvrdenie platí, pretože súčet 4 prirodzených čísiel je minimálne 4, t.j. $x \geq 4$.
- A v predchádzajúcom príklade sme ukázali, že platí, že ak $x \geq 4$, tak potom $2^x \geq x^2$, čo je práve to, čo chceme dokázať v tomto tvrdení.
- Platí totiž logické pravidlo *modus ponens*, ktoré hovorí, že ak platí tvrdenie "Ak platí H, potom platí C" a zároveň ak H je pravdivé, tak potom môžeme z toho odvodiť, že aj C pravdivé.



Príklad

Dôkaz ($\Rightarrow$) "Nech $\lceil x \rceil = |x|$. Potom platí, že x je celé číslo."

- Predpokladáme, že $\lceil x \rceil = \lfloor x \rfloor$ a chceme ukázať, že v takom prípade je x celé číslo.
- Z definície $\lceil x \rceil$ a $\lfloor x \rfloor$ vidíme, že $\lceil x \rceil \geq x$ a $\lfloor x \rfloor \leq x$.
- Zároveň z predpokladu máme, že $\lceil x \rceil = \lfloor x \rfloor$.
- Teda musí v tomto prípade platiť aj že $\lceil x \rceil \leq x$.
- Keďže v tomto prípade platí, že $\lceil x \rceil \leq x$ a zároveň $\lceil x \rceil \geq x$, tak podľa matematických pravidiel logicky $\lceil x \rceil = x$.
- A keďže $\lceil x \rceil$ je **vždy** celé číslo, tak aj x je tým pádom celé číslo.
- Dokázali sme teda, že ak platí, že $\lceil x \rceil = \lfloor x \rfloor$, tak potom je x celé číslo.



Príklad

Dôkaz ($\Leftarrow$) "Nech x je celé číslo. Potom $\lceil x \rceil = \lfloor x \rfloor$.

- Predpokladáme, že x je celé číslo a chceme ukázať, že v tomto prípade $\lceil x \rceil = \lfloor x \rfloor$.
- Z definície operácií $\lceil x \rceil$, resp. $\lfloor x \rfloor$ vyplýva, že ak x je celé číslo, tak potom $x = \lceil x \rceil$, resp. $x = \lfloor x \rfloor$.
- A teda, ak x je celé číslo, tak v tom prípade $|x| = \lceil x \rceil$.

Dôkazy o množinách

- Dôkaz rovnosti 2 množín E a F bude preto vždy pozostávať z 2 častí:
 1. Dôkaz, že platí, že **ak x je prvkom E , tak potom x je prvkom F**
 2. Dôkaz, že platí, že **ak x je prvkom F , tak potom x je prvkom E**

Príklad

Dôkaz (1.) že ak x je prvkom $R \cup (S \cap T)$, tak potom x je prvkom $(R \cup S) \cap (R \cup T)$.

1. Z hypotézy: $x \in R \cup (S \cap T)$
2. Z kroku 1 a definície zjednotenia: $x \in R$ alebo $x \in S \cap T$.
3. Z kroku 2 a definície prieniku: $x \in R$ alebo x je v oboch S aj T .
4. Z kroku 3 a definície zjednotenia: $x \in R \cup S$.
5. Z kroku 3 a definície zjednotenia: $x \in R \cup T$.
6. Z krokov 4,5 a definície prieniku: $x \in (R \cup S) \cap (R \cup T)$.

Príklad

- Dokázali sme teda, že súčasne platia tieto 2 tvrdenia:
 1. ak x je prvkom $R \cup (S \cap T)$, tak potom x je prvkom $(R \cup S) \cap (R \cup T)$
 2. ak x je prvkom $(R \cup S) \cap (R \cup T)$, tak potom x je prvkom $R \cup (S \cap T)$
- Z toho logicky vyplýva, že obe množiny sú totožné a teda
$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T).$$

Príklad 2

Dokážte, že pre 2 množiny A, B platí: $A \cup (B \setminus A) = A \cup B$.

- Dôkaz bude pozostávať teda z 2 častí:
 1. Dôkaz, že platí, že **ak x je prvkom $A \cup (B \setminus A)$, tak potom x je prvkom $A \cup B$**
 2. Dôkaz, že platí, že **ak x je prvkom $A \cup B$, tak potom x je prvkom $A \cup (B \setminus A)$**

Nepriamy dôkaz

- Pre ilustráciu, obmenou tvrdenia **Ak** $x \geq 4$, **tak potom** $2^x \geq x^2$ je tvrdenie **Ak** $2^x < x^2$, **tak potom** $x < 4$.
- Dôkaz obmenou môže byť užitočný pri dôkazoch rovnosti množín E a F , keďže tvrdenie $E = F$ je možné dokazovať tak, že namiesto dôkazu tvrdenia "Ak $x \in E$ tak potom $x \in F$ a zároveň ak $x \in F$ tak potom $x \in E$ "
- je možné dokazovať tvrdenie "Ak $x \in E$ tak potom $x \in F$ a zároveň ak $x \notin E$ tak potom $x \notin F$ "

Nepriamy dôkaz - Príklad

Dokážte tvrdenie: Nech n je celé číslo. Ak 3 delí n^2 , potom 3 delí n . (formálne $3 \mid n^2 \Rightarrow 3 \mid n$).

- Toto tvrdenie dokážeme nepriamo, t.j. dokážeme obmenu tohto výroku.
- Obmena výroku je: $3 \nmid n \Rightarrow 3 \nmid n^2$, t.j. ak 3 nedelí n , potom 3 nedelí n^2 .
- Túto obmenu dokážeme priamo.

Nepriamy dôkaz - Príklad

Dokazujeme tvrdenie, že ak 3 nedelí n , potom 3 nedelí n^2 . Predpoklad "3 nedelí n " znamená, že číslo n po delení číslom 3 dáva zvyšok 1 alebo 2. Tieto 2 prípady vyšetríme samostatne:

- Ak n po delení 3 dáva zvyšok 1:

$$n = 3q + 1 \Rightarrow n^2 = (3q + 1)^2 \Rightarrow n^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 \Rightarrow n^2 \text{ po delení 3 dáva tiež zvyšok 1.}$$

- Ak n po delení 3 dáva zvyšok 2:

$$n = 3q + 2 \Rightarrow n^2 = (3q + 2)^2 \Rightarrow n^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1 \Rightarrow n^2 \text{ po delení 3 dáva zvyšok 1.}$$

Nepriamy dôkaz - Príklad

- Vidíme teda, že v prípade, že ak 3 nedelí n , čo znamená, že n po delení 3 dáva zvyšok 1 alebo 2, tak v oboch prípadoch 3 nedelí ani n^2 .
- Priamo sme teda dokázali tvrdenie, že $3 \nmid n \Rightarrow 3 \nmid n^2$.
- Keďže platí toto tvrdenie, platí teda aj jeho obmena, ktorú sme tým pádom dokázali, t.j. že platí $3 \mid n^2 \Rightarrow 3 \mid n$.

Dôkaz sporom - Príklad

Sporom dokážeme, že platí, že $\sqrt{3}$ je iracionálne číslo.

- Predpokladáme, že platí negácia, t.j. že $\sqrt{3}$ je racionálne číslo.
- To znamená, že $\sqrt{3} = \frac{p}{q}$, kde p, q sú celé čísla a $GCD(p, q) = 1$ (sú nesúdeliteľné).
- $\sqrt{3} = \frac{p}{q} \Rightarrow 3 = \frac{p^2}{q^2} \Rightarrow p^2 = 3q^2 \Rightarrow 3 \mid p^2$.
- Podľa už dokázanej vety: $3 \mid p \Rightarrow p = 3k$, k je celé číslo.
- Dosadíme do $p^2 = 3q^2$ za $p = 3k$:
 $(3k)^2 = 3q^2 \Rightarrow 9k^2 = 3q^2 \Rightarrow 3k^2 = q^2 \Rightarrow 3 \mid q^2 \Rightarrow 3 \mid q$.
- Dostali sme teda, že v tomto prípade musí platiť, že $3 \mid p$ a súčasne $3 \mid q$.

Dôkaz sporom

Ak chceme dokázať tvrdenie v tvare implikácie, t.j. $H \Rightarrow C$ pomocou dôkazu sporom:

- Náš predpoklad bude, že platí negácia daného tvrdenia, t.j. že platí $H \wedge \neg C$ (lebo je to negácia implikácie $H \Rightarrow C$).
- Následne z tejto negácie začneme odvodzovať logické dôsledky, až narazíme na tvrdenie, o ktorom vieme s istotou povedať, že určite neplatí.
- Napríklad je v rozpore s nejakým skôr dokázaným tvrdením, alebo s nejakou axiómou, či predpokladmi dokazovaného tvrdenia.
- Keďže sme pomocou korektného usudzovania dospeli k niečomu, čo nemôže byť pravda, znamená to, že pravdou nemohol byť už náš predpoklad!
- Preto musí byť pravdou opak nášho predpokladu - t.j. $\neg(H \wedge \neg C)$, čiže implikácia $H \Rightarrow C$.

Dôkaz sporom - Príklad

Chceme dokázať tvrdenie: **Nech S je konečná podmnožina nekonečnej množiny U . Nech T je doplnok množiny S vzhľadom na množinu U . Potom T je nekonečná množina.**

- Dokazované tvrdenie má tvar implikácie $H \Rightarrow C$.
- Hypotéza H tohto tvrdenia je: U je nekonečná množina, S je konečná podmnožina U , T je doplnok množiny S vzhľadom na množinu U .
- Záver C tohto tvrdenia je: T je nekonečná množina.
- Dôkaz sporom vykonáme tak, že predpokladáme negáciu implikácie $H \Rightarrow C$, t.j. tvrdenie $H \wedge \neg C$, čiže:
- **S je konečná podmnožina nekonečnej množiny U . T je doplnok množiny S vzhľadom na množinu U a zároveň T je konečná množina.**



Dôkazy indukciou

- Dôkazy matematickou indukciou sú vhodný nástroj, keď je potrebné dokázať tvrdenie o rekurzívne definovaných objektoch.
- Typické príklady zo strednej školy zahŕňajú matematické vzťahy, avšak my ich budeme používať na dôkazy tvrdení o automatoch, regulárnych výrazoch, atď.

Dôkazy indukciou o celých číslach

Predpokladajme, že je dané nejaké tvrdenie $S(n)$ o prirodzenej premennej n , ktoré je potrebné dokázať. Dôkaz indukciou má 2 kroky:

- **Základný krok** kde ukážeme, že $S(i)$ platí pre konkrétnu hodnotu i . To sa robí pre najmenšie vhodné i - štandardne $i = 0, i = 1$, prípadne podľa potreby.
- **Indukčný krok** kde predpokladáme, že $n \geq i$ a ukážeme, že platí tvrdenie "Ak platí $S(n)$, tak platí $S(n + 1)$ ". Inými slovami, predpokladáme, že platí tvrdenie $S(n)$ a ukážeme, že z toho vyplýva, že platí tvrdenie $S(n + 1)$. Predpoklad, že platí $S(n)$ nazývame aj **indukčný predpoklad**.

Príklad

Dokážte: Pre $\forall n \geq 0, n \in \mathbb{Z}$ platí, že $3 \mid n(n+1)(n+2)$.

Toto tvrdenie sa dá dokázať aj tým, že si uvedomíme, že je to súčin 3 po sebe idúcich čísiel a v nich sa určite nachádza práve jedno deliteľné 3. My však ukážeme aj dôkaz matematickou indukciou.

- Zistujeme, či $3 \mid (n+1)(n+2)(n+3)$
- To je to isté, ako otázka, či $3 \mid (n+1)(n+2)n + (n+1)(n+2)3$, t.j. roznásobili sme poslednú zátvorku $(n+3)$
- Z indukčného prepokladu vieme, že $3 \mid (n+1)(n+2)n$
- Taktiež platí, že $3 \mid (n+1)(n+2)3$
- A keďže 3 delí oba sčítance, teda $(n+1)(n+2)n + (n+1)(n+2)3$, tak delí aj celý výraz $(n+1)(n+2)(n+3)$.

V indukčnom kroku predpokladáme, že tvrdenie platí pre hodnotu n , t.j. indukčný predpoklad je, že platí

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$$

a chceme dokázať, že platí pre hodnotu $n+1$, t.j. že platí rovnosť

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

Hlavným trikom je znovu použiť v dôkaze tejto rovnosti indukčný predpoklad.

L'avú stranu dokazovanej rovnosti, t.j.

$$\sum_{i=1}^{n+1} i^2$$

si rozpíšeme ako

$$(\sum_{j=1}^n i^2) + (n + 1)$$

Ak za $(\sum_{i=1}^n i^2)$ dosadíme pravú stranu z indukčného predpokladu, dostaneme výraz:

$$\frac{n(n+1)(2n+1)}{6} + (n+1) = \frac{2n^3 + 9n^2 + 13n + 6}{6}$$



Pravú stranu dokazovanej rovnosti, t.j.

$$\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

vieme po roznásobení upraviť na

$$\frac{2n^3 + 9n^2 + 13n + 6}{6}$$

- Z posledných dvoch bodov predchádzajúceho slajdu teda vyplýva, že daná rovnosť

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$$

naozaj platí pre všetky $n \geq 0$, čím sme dokázali požadované tvrdenie.

- Pretože ak vieme, že platí toto tvrdenie pre $n = 0$, t.j. $S(0)$ a platí implikácia $S(n) \Rightarrow S(n + 1)$, tak ich kombináciou zistíme, že to platí aj pre $S(1)$. Z neho $S(2)$. Z neho $S(3)$. Z neho $S(4)$. Atd'.
- Často sa to popisuje aj ako efekt padajúcich domino kociek :).

Dôkazy indukciou - verzia 2

Menej známou, ale rovnako účinnou formou dôkazu indukciou je všeobecnejšia verzia, ktorá oproti klasickej ponúka 2 "vylepšenia":

1. Väčší počet základných krokov. T.j. explicitne dokážeme, že platí $S(i), S(i+1), \dots, S(j)$ pre nejaké $j > i$, t.j. dokážeme platnosť pre väčší počet konkrétnych hodnôt.
2. Pri dokazovaní platnosti $S(n+1)$ nevyužívame len predpoklad, že platí $S(n)$, ale aj

$$S(i), S(i+1), \dots, S(n)$$

Navyše kroky 1 a 2 môžeme skombinovať a ak dokážeme platnosť pre prípady po $S(j)$, tak môžeme predpokladať, že $n \geq j$ namiesto $n \geq i$.



Príklad

V indukčnom kroku teraz budeme predpokladať, že $n \geq 10$ a že platia všetky:

$$S(8), S(9), \dots, S(n)$$

a budeme dokazovať, že platí $S(n+1)$.

Uvedomme si, že číslo $n+1 = 3 + (n-2)$. T.j. ak je $S(n-2)$ pravdivé, tak potom aj $S(n+1)$ je pravdivé. Ak by sa číslo $n-2$ dalo vyjadriť ako súčet trojok a pätiok, tak potom musí platiť, že $n-2 = 3a + 5b$. Potom však $n+1 = 3 + 3a + 5b = 3(a+1) + 5b$, teda aj $S(n+1)$ je pravdivé.



Príklad

Všimnite si, ako teraz zafunguje indukcia pre 3 základné prípady:

- Keďže sme dokázali, že platí $S(8)$, tak potom bude platiť aj $S(11)$.
- Keďže sme dokázali, že platí $S(9)$, tak potom bude platiť aj $S(12)$.
- Keďže sme dokázali, že platí $S(10)$, tak potom bude platiť aj $S(13)$.

A teraz ako z už novo dokázaných prípadov ideme ďalej...

- Keďže sme dokázali, že platí $S(11)$, tak potom bude platiť aj $S(14)$.
- Keďže sme dokázali, že platí $S(12)$, tak potom bude platiť aj $S(15)$.
- Keďže sme dokázali, že platí $S(13)$, tak potom bude platiť aj $S(16)$.

a tak d'alej...



Príklad 2

Indukčným predpokladom teraz bude, že predpokladáme, že **všetky** čísla od 2 po n sa dajú napísať ako súčin prvočísiel, t.j. že $S(n)$ je pravdivé pre $S(i)$, $2 \leq i \leq n$.

A tento predpoklad využijeme pri dôkaze tvrdenia pre $S(n + 1)$.

- Ak $n + 1$ je prvočíslo, tak potom je $S(n + 1)$ určite pravdivé.
- Ak $n + 1$ je zložené číslo, tak potom má určite deliteľ p , $1 < p < n + 1$, t.j.
 $n + 1 = pN$
- Keďže $N < n + 1$, podľa indukčného predpokladu N má rozklad na súčin prvočísiel, teda aj $n + 1$ má rozklad na súčin prvočísiel.



Dôkaz štruktúrnou indukciou

Ak máme nejakú rekurzívne definovanú štruktúru X a chceme dokázať nejaké tvrdenie $S(X)$ o nej, môžeme postupovať nasledovne:

Základný krok: Dokážeme platnosť $S(X)$ pre základné štruktúry X .
(štruktúry zo základnej časti definície)

Indukčný krok: Ak je v indukčnej časti definovaná štruktúra X rekurzívne pomocou štruktúr $Y_1, Y_2, \dots, Y_k$, tak v tomto kroku predpokladáme, že tvrdenia $S(Y_1), S(Y_2), \dots, S(Y_k)$ sú pravdivé a dokazujeme, že platí $S(X)$.

Dôkaz štruktúrnou indukciou - Príklad

- **Základný krok:** Základná štruktúra definície stromu je 1 vrchol. V takom prípade je $n = 1$ a $e = 0$, takže vzťah $n = e + 1$ platí.
- **Indukčný krok:** Nech T je strom vytvorený podľa rekurzívnej definície zo stromov T_i a koreňa N . Ak predpokladáme, že $S(T_i)$ platí pre jednotlivé stromy $T_1, T_2, \dots, T_k$, tak potom v každom strome platí $n_i = e_i + 1, 1 \leq i \leq k$.

Vrcholov v strome T je spolu $1 + n_1 + n_2 + \dots + n_k$

Hrán v strome T je spolu $k + e_1 + e_2 + \dots + e_k$

Ak v počte vrcholov dosadíme za každé $n_i = e_i + 1$, dostaneme

$$1 + e_1 + 1 + e_2 + 1 \dots e_k + 1 = 1 + k + e_1 + e_2 + \dots e_k$$

Tento výraz je o 1 väčší než $k + e_1 + e_2 + \dots e_k$, t.j. strom T má počet vrcholov o 1 väčší než hrán.



Vzájomná indukcia

- Niekedy potrebujeme dokázať súčasnú platnosť hneď niekoľkých tvrdení $S_1(n), S_2(n), \dots, S_k(n)$, indukciou na n .
- Takáto situácia nastáva obzvlášť pri štúdiu konečných automatov :).
- Ak chceme dokázať, že súčasne platí viacero tvrdení $S_1(n), S_2(n), \dots, S_k(n)$, znamená to, že chceme vlastne dokázať 1 zložený výrok $S_1(n) \wedge S_2(n) \wedge \dots \wedge S_k(n)$
- Dokazujeme to tak, že samostatne dokážeme platnosť jednotlivých výrokov $S_1(n)$, potom $S_2(n)$, atď., pomocou klasickej indukcie.



Obe časti $S_1(n)$ a $S_2(n)$ budeme dokazovať matematickou indukciou pre n , t.j. v 2 častiach - základnej a indukčnej.

Navyše, keďže obe tvrdenia majú tvar **ekvivalencie** $A \Leftrightarrow B$ (t.j. obsahujú logickú spojku "vtedy a len vtedy"), budeme ich dokazovať "v oboch smeroch", t.j. ako implikácie $B \Rightarrow A$ a $A \Rightarrow B$.

Základná časť: ako základ zvolíme $n = 0$, t.j. dokazujeme platnosť tvrdení $S_1(0)$ a $S_2(0)$.

- $(S_1, \Rightarrow)$ Dokazujeme, že platí výrok: "Ak automat je v stave *off* po 0 stlačeniach, potom 0 je párne.

Predpoklad je splnený, keďže automat je naozaj v stave *off* po 0 stlačeniach (lebo je na začiatku a vtedy je v stave *off*). A dôsledok taktiež, pretože 0 je párne číslo. Teda toto platí.

- $(S_1, \Leftarrow)$ Dokazujeme, že platí výrok: "Ak 0 je párne, potom automat je v stave *off* po 0 stlačeniach.

Predpoklad je splnený, pretože 0 je párne číslo. A dôsledok taktiež, po 0 stlačeniach bude automat v stave na začiatku, teda v stave *off*. Teda aj toto platí.



Základná časť: ako základ zvolíme $n = 0$, t.j. dokazujeme platnosť tvrdení $S_1(0)$ a $S_2(0)$.

- $(S_2, \Rightarrow)$ Dokazujeme, že platí výrok: "Ak automat je v stave *on* po 0 stlačeniach, potom 0 je nepárne."

Predpoklad **nie je** splnený, keďže automat **nie je** stave *on* po 0 stlačeniach (lebo na začiatku je v stave *off*, nie v stave *on*). Ak nie je splnený predpoklad nejakej implikácie, tak potom podľa pravidiel implikácie je celková implikácia pravdivá, takže daný výrok platí.

- $(S_2, \Leftarrow)$ Dokazujeme, že platí výrok: "Ak 0 je nepárne, potom automat je v stave *on* po 0 stlačeniach."

Predpoklad znovu **nie je** splnený, pretože 0 nie je nepárne číslo. Znovu teda platí, že celú implikáciu budeme považovať za pravdivú a teda aj tento výrok platí.



Dokázali sme teda, že výroky $S_1(0)$ a $S_2(0)$ sú oba pravdivé, čím sme dokázali platnosť základnej časti matematickej indukcie.

Teraz sa pokúsime dokázať platnosť indukčnej časti. Ako indukčný predpoklad budeme predpokladať platnosť výrokov $S_1(n)$ a $S_2(n)$ a pokúsime sa dokázať platnosť výrokov $S_1(n+1)$ a $S_2(n+1)$.

Indukčná časť:

- $(S_1(n+1), \Rightarrow)$ Dokazujeme, že platí výrok: "Ak automat je v stave *off* po $n+1$ stlačeniach, potom $n+1$ je párne.

Ak sa automat po $n + 1$ stlačeniach nachádza v stave *off*, tak potom to musí znamenať, že v predchádzajúcom stave (pred posledným stlačením) sa nachádzal v stave *on*. Z **indukčného predpokladu** vyplýva, že sa však v stave *on* môže nachádzať po n stlačeniach len vtedy, ak n bolo nepárne. Z toho však teda vyplýva, že $n + 1$ musí byť párne. Príslušný výrok sme dokázali.



Indukčná časť:

- $(S_1(n+1), \Leftarrow)$ Dokazujeme, že platí výrok: "Ak $n+1$ je párne, potom je automat v stave *off* po $n+1$ stlačeniach.

Ak $n+1$ je párne číslo, tak potom n musí byť nepárne číslo. Z indukčného predpokladu vyplýva, že n je nepárne číslo vtedy a len vtedy, ak sa automat po n stlačeniach nachádza v stave *on*. Čiže po n stlačeniach vieme, že bude v stave *on* ak n bolo nepárne a po ďalšom, $n+1$ stlačení sa zo stavu *on* dostane do stavu *off*. Príslušný výrok sme dokázali.

Indukčná časť:

- $(S_2(n+1), \Leftarrow)$ Dokazujeme, že platí výrok: "Ak $n+1$ je nepárne, potom je automat v stave *on* po $n+1$ stlačeniach.

Ak $n+1$ je nepárne číslo, tak potom n musí byť párne číslo. Z indukčného predpokladu vyplýva, že n je párne číslo vtedy a len vtedy, ak sa automat po n stlačeniach nachádza v stave *off*. Čiže po n stlačeniach vieme, že bude v stave *off* ak n bolo párne a po ďalšom, $n+1$ stlačení sa zo stavu *off* dostane do stavu *on*. Príslušný výrok sme dokázali.

Podarilo sa nám teda dokázať indukciou aj výrok $S_1(n)$, aj výrok $S_2(n)$ o správaní sa daného automatu.

Zhrnutie vzájomnej indukcie

Vzájomnú indukciu teda dokazujeme nasledovne:

- Každý výrok zo sústavy výrokov dokážeme samostatne indukciou, t.j. ak základnú, aj indukčnú časť.
- Ak sú výroky v tvare ekvivalencií (vtedy-a-len-vtedy, $A \Leftrightarrow B$), potom musíme indukciami dokázať oba smery (t.j. obe implikácie, $A \Leftarrow B$, $A \Rightarrow B$)



Abeceda

Definição

Abecedou nazývame konečnú neprázdnu množinu symbolov.

- Pre označenie nejakej abecedy budeme štandardne používať symbol Σ .
- Príklady rôznych abecied:
 1. $\Sigma = \{0, 1\}$, t.j. *binárna* abeceda.
 2. $\Sigma = \{a, b, c, \dots, z\}$, t.j. malé písmená anglickej abecedy.
 3. Množina všetkých ASCII znakov, prípadne všetkých tlačiteľných znakov.



Ret'azce

Definição

Reťazcom, prípadne **slovom**, **vetou** nad abecedou Σ nazývame konečnú postupnosť symbolov z abecedy Σ .

- **Príklady rôznych reťazcov:**
 1. 11011 je reťazec nad binárnou abecedou $\Sigma = \{0, 1\}$.
 2. *TZI* je reťazec nad abecedou veľkých písmen.
 3. *TZI* je reťazec nad abecedou všetkých ASCII znakov.

Prázdný reťazec

Definição

Prázdny reťazcom nazývame konečnú postupnosť nula symbolov, t.j. reťazec, ktorý nie je tvorený žiadnymi symbolmi.

- Budeme ho označovať symbolom ε .
- Prázdny reťazec môžeme vždy uvažovať nad ľubovoľnou abecedou.

Prázdný reťazec

Definição

Prázdny reťazcom nazývame konečnú postupnosť nula symbolov, t.j. reťazec, ktorý nie je tvorený žiadnymi symbolmi.

- Budeme ho označovať symbolom ε .
- Prázdny reťazec môžeme vždy uvažovať nad ľubovoľnou abecedou.

Dôležité mocniny abecedy

- Σ^* je množina **všetkých** reťazcov nad abecedou Σ .
- Napríklad $\{0, 1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$
- T.j. $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \dots$
- Σ^+ je množina **všetkých neprázdnych** reťazcov nad abecedou Σ , t.j. $\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$, resp. $\Sigma^* = \Sigma^+ \cup \{\varepsilon\}$.
- T.j. $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \dots$

Zreťazenie

Definição

Nech x je reťazec pozostávajúci z i symbolov, t.j. $x = a_1 a_2 \dots a_i$, $|x| = i$. Nech y je reťazec pozostávajúci z j symbolov, t.j. $y = b_1 b_2 \dots b_j$, $|y| = j$. Potom reťazec $xy = a_1 a_2 \dots a_i b_1 b_2 \dots b_j$ dĺžky $|xy| = i + j$, nazývame **zreťazením** reťazcov x a y .

- Pre každý reťazec w platí $w\varepsilon = \varepsilon w = w$, t.j. prázdny reťazec je jednotkovým prvkom vzhľadom na operáciu zreťazenia.

Jazyky

Definição

Nech Σ je abeceda. Nech L je množina reťazcov, ktoré sú vybrané z množiny Σ^* , t.j. $L \subseteq \Sigma^*$. Potom túto množinu L nazývame **jazykom** nad abecedou Σ .

- Jazyk L nad abecedou Σ nemusí obsahovať reťazce zo všetkých symbolov Σ .
- To znamená, že jazyk L nad abecedou Σ je zároveň jazykom nad každou abecedou, ktorá je nadmnožinou Σ .

Jazyky

Príklady jazykov

- (Keď to DOSŤ zjednodušíme) *slovenský jazyk* je množina platných zrozumiteľných slov nad písmenami slovenskej abecedy.
- Uvažujme množinu všetkých platných programov nad programovacím jazykom C (platný program = taký, ktorý kompilátor preloží do strojového kódu). Potom aj táto množina je jazyk nad abecedou, ktorú tvoria prípustné symboly v jazyku C (zároveň je táto abeceda podmnožinou ASCII symbolov).
- T.j. množina všetkých *skompilovateľných programov* v jazyku C tvorí jazyk, pretože každý skompilovateľný program je v podstate jeden veľmi veľký reťazec :).



Jazyky

Príklady jazykov

- Jazyk pozostávajúci zo všetkých reťazcov obsahujúcich n -krát symbol 0, za ktorým ide n -krát symbol 1 pre nejaké celé číslo $n \geq 0$, t.j. $\{\epsilon, 01, 0011, 000111, \dots\}$
- Množinu reťazcov zo symbolov 0, 1, v ktorých je počet núl a jednotiek rovnaký: $\{\epsilon, 01, 10, 0011, 0101, 1100, \dots\}$.
- Množina binárnych reťazcov predstavujúcich prvočísla: $\{10, 11, 101, 111, 1011, \dots\}$
- Σ^* je jazykom nad Σ .
- $\emptyset$ je jazykom nad ľubovoľnou abecedou.
- $\{\epsilon\}$ je taktiež jazykom nad ľubovoľnou abecedou. POZOR! $\{\epsilon\} \neq \emptyset$.



Jazyky

Jazyky budeme často popisovať nasledovnou notáciou: $\{w \mid \text{tvrdenie o } w\}$

1. $\{w \mid w \text{ pozostáva z rovnakého počtu } 0 \text{ a } 1\}$
2. $\{w \mid w \text{ je binárny zápis prvočísla}\}$
3. $\{w \mid w \text{ je syntakticky korektný C program}\}$
4. $\{0^n 1^n \mid n \geq 1\}$ - podobne ako pri abecedách, mocninný zápis 0^n znamená n -krát zopakovaný symbol 0 (podobne s inými symbolmi). T.j. toto je jazyk obsahujúci reťazce pozostávajúce z kladného počtu núl, za ktorými je rovnaký počet jednotiek.
5. $\{0^i 1^j \mid 0 \leq i \leq j\}$ - jazyk pozostávajúci z nejakého nezáporného (t.j. prípadne nulového) počtu núl, za ktorými ide aspoň toľko isto jednotiek.



Jazyky a problémy

- Na tomto predmete budeme často riešiť problém, či nejaký reťazec patrí do nejakého jazyka.
- Tento na prvý pohľad umelý problém má ďalekosiahle implikácie v informatike samotnej, keďže v podstate čokoľvek, čo môžeme nazvať "problémom" v informatike, sa dá vyjadriť ako problém príslušnosti do nejakého jazyka.
- Presnejšie:

Ak Σ je abeceda a L je jazyk nad abecedou Σ , potom problém L je:

- Pre daný reťazec $w \in \Sigma^*$ rozhodnite, či $w \in L$ alebo $w \notin L$.



Jazyky a problémy

- Napríklad štandardný problém v informatike - testovanie prvočíselnosti - sa dá vyjadriť ako jazyk L_p všetkých binárnych postupností, ktoré reprezentujú prvočíslo. A následne otázka, či je nejaké číslo prvočíslo znamená, či jeho binárna reprezentácia patrí do jazyka L_p alebo nie.
- Pre niektoré reťazce, ako napr. 0011101 je odpoveď jednoduchá, keďže platné binárne reprezentácie čísiel musia začínať jednotkou.
- Vo všeobecnosti však riešenie takéhoto problému (t.j. odpoveď na otázku, či patrí/nepatrí binárny reťazec do L_p) jednoduché byť nemusí.

Jazyky a problémy

- Napríklad, ak L_X je množina všetkých syntakticky korektných programov v programovacom jazyku X , tak ak riešiť problém, či je program syntakticky korektný, je ťažká úloha, tak samotný preklad programu do cieľového jazyka nemôže byť ľahší.
- Keďže ak by bolo ťažké rozhodnúť, či je program syntakticky korektný, ale zároveň by samotný preklad bol ľahký, tak keďže počas prekladov programov sa robí aj syntaktická analýza, tak potom by stačilo len spustiť samotný preklad a počkať si na (ľahké) vygenerovanie výstupu. V takom prípade by teda program musel byť syntakticky korektný a máme spor s tým, že rozhodnúť o korektnosti je ťažká úloha.
- Čiže v tomto prípade by platilo: "Ak testovanie príslušnosti do L_X je ťažké, potom aj kompilácia programov v jazyku X je ťažká."



Zhrnutie

- Z tejto prednášky sú najdôležitejšie nové pojmy ako abeceda, reťazce, zreženie, jazyk.
- Taktiež je dobré mať na pamäti, že existujú rôzne formy dôkazov, ako priamy/nepriamy dôkaz, dôkaz sporom, či dôkaz indukciou (či už na číslach alebo rekurzívne definovaných štruktúrach), keďže ich počas semestra budeme používať.



Použitá literatura

- Hopcroft, Motwani, Ullman - Introduction to Automata Theory, Languages and Computations, 3rd Ed.
- Králiková, Jana - Druhy dôkazov,
https://www.galeje.sk/web_object/9440.pdf
- Kollár, Jozef - Polakovič, Marcel - Diskrétna matematika pre študentov aplikovanej informatiky FEI STU
<http://matika.elf.stuba.sk/KMAT/DiskretnaMatematika>

