Teoretične osnove računalništva - zapiski iz vaj 2010/2011

Miha Zidar

February 3, 2011

Contents

1 Dokazovaje

1.1 Dokaz s konstrukcijo

Kadar nas zanima obstoj nekega objekta, ga včasih lahko preprosto skonstruiramo.

Primer:

- Ali za vsako število elementov, večje od 4, obstaja graf ki ima natanko 3 liste?
- $|\mathbb{R}| = |[0, 1)|$

1.2 Dokaz z indukcijo

Velja za množice ki so zapisljive kot induktivni razred[1]
Induktivni razred I sestavlja:

- baza - najbolj osnovna množica elementov (osnovni razred)
- pravila generiranja - pravila kako iz elementov baze gradimo nove elemente (množico)

Primer:

- Induktivni razred naravnih števil ($\mathbb{N}$)
  1. Baza: $1 \in \mathbb{N}$
  2. Pravila generiranja: $n \in \mathbb{N} \Longrightarrow n + 1 \in \mathbb{N}$
- Hilbertove krivulje[2]

1.3 Dokaz s protislovjem

Vzamemo trditev in poskušamo najti primer v katerem trditev ne drži.

Primer:

- Praštevil je končno mnogo
  1. Predpostavimo, da poznamo vsa praštevila:
     $P = \{2, 3, 5, ..., p\}$, kjer je p zadnje praštevilo
  2. Po definiciji obstajajo le praštevila in sestavljena števila (to so taka, ki jih lahko razstavimo na prafaktorje).
  3. Če pomnožimo vsa znana praštevila iz P in prištejemo 1 dobimo število, ki se ga ne da razstaviti na prafaktorje iz množice P:
     $q = 2 * 3 * 5 * ... * p + 1$

[1] Glej slovarček na koncu.
[2] http://en.wikipedia.org/wiki/Hilbert_curve

4. Torej je q ali praštevilo (ker ni sestavljeno), ali pa število, sestavljeno iz prafaktorjev, ki jih ni v množici P.
5. Oboje kaže na to, da v množici P nimamo vseh praštevil in da to velja za vsako končno množico praštevil.

- $\sqrt[3]{2}$ je racionalno število

1. $\sqrt[3]{2} = \frac{a}{b}$ ker je $\frac{a}{b}$ racionalen ulomek ga lahko okrajšamo in si ga od sedaj predstavljamo okrajšanega $GCD(a, b) = 1$
2. $2 = \left(\frac{a}{b}\right)^3$
3. $2b^3 = a^3$ tukaj vidimo da je a sodo število, torej lahko pišemo $a = 2k$
4. $2b = (2k)^3$
5. $2b = 8k$
6. $b = 4k$ ker je b tudi sodo število, vidimo da $GCD(a, b) = 1$ ne drži, torej smo prišli do pizdarije.

2 Teorija jezikov

Oznake

- Σ - abeceda - končna neprazna množica simbolov oz. vseh besed dolžine 1
- w - besede ali nizi - poljubno končno zaporedje simbolov $w_1 w_2 \ldots w_n$. Prazen niz $w = \varepsilon$
- $|w|$ - dolžina niza - je 0 za $w = \varepsilon$

Operacije

1. Stik

   - Nizov:

$$
\begin{aligned}
w &= w_1 w_2 \ldots w_n \\
x &= x_1 x_2 \ldots x_m \\
wx &= w_1 w_2 \ldots w_n x_1 x_2 \ldots x_m
\end{aligned}
$$

   - Množic:

$$
\begin{aligned}
A &= \{w_1,\ w_2,\ \ldots,\ w_n\} \\
B &= \{x_1,\ x_2,\ \ldots,\ x_m\} \\
A \circ B &= \{w_i x_j \mid w_i \in A\ \wedge\ x_i \in B\}
\end{aligned}
$$

2. Potenciranje

$$
\begin{aligned}
A^k &= A \circ A \circ \cdots \circ A = \bigcirc_k A^k \\
A^0 &= \{\varepsilon\}
\end{aligned}
$$

3. Iteracija

$$
\begin{aligned}
A^* &= A^0 \bigcup A^1 \bigcup A^2 \cdots = \bigcup_{i=0}^{\infty} A^i \\
\Sigma^* &= \text{množica vseh možnih besed}
\end{aligned}
$$

4. Jezik - jezik L nad Σ je poljubna podmnožica Σ^*

$$
\begin{aligned}
L &\subseteq \Sigma^* \\
L_1 &= \{\} \ \rightarrow \text{ prazen jezik} \\
L_2 &= \{\varepsilon\} \ \rightarrow \text{ ni prazen jezik}
\end{aligned}
$$

3 Regularni Izrazi

- $\underline{\phi}$ opisuje prazen jezik $L(\underline{\phi}) = \{\}$
- $\underline{\varepsilon}$ opisuje jezik $L(\underline{\varepsilon}) = \{\varepsilon\}$
- $\underline{a}$, $a \in \Sigma$ opisuje $L(\underline{a}) = \{a\}$
- $(r_1 + r_2)$ opisuje $L(r_1 + r_2) = L(r_1) \bigcup L(r_2)$
- $(r_1 r_2)$ opisuje $L(r_1 r_2) = L(r_1)L(r_2)$
- (r^*) opisuje $(L(r))^*$

Jezik ki ga opisuje poljubni Regularni izraz (RI) se imenuje Regularni jezik.

- Σ^* je regularni izraz
- $\{\}$ je regularni izraz
- $\{0^n 1^n \mid n \geqslant 0$ <u>ni</u> regularni izraz

primeri

1. abeceda $\Sigma = \{0, 1\}$
   Opiši vse nize, ki se končajo z nizom 00.
   $$r = (0 + 1)^* 00$$
2. abeceda $\Sigma = \{a, b, c\}$
   Opiši vse nize, pri katerih so vsi a-ji pred b-ji in vsi b-ji pred c-ji.
   $$a^* b^* c^*$$
3. abeceda $\Sigma = \{a, b, c\}$
   Opiši vse nize, ki vsebujejo vsaj dva niza 'aa', ki se ne prekrivata.
   $$(a + b + c)^* aa(a + b + c)^* aa(a + b + c)^*$$
4. abeceda $\Sigma = \{a, b, c\}$
   Opiši vse nize, ki vsebuje vsaj dva niza 'aa' ki se lahko prekrivata
   $$(a + b + c)^* aa(a + b + c)^* aa(a + b + c)^* + (a + b + c)^* aaa(a + b + c)^*$$
5. abeceda $\Sigma = \{0, 1\}$
   Opiši vse nize, ki ne vsebujejo niza 11
   $$(\varepsilon + 1)(0^* 01)^* 0^*$$
   $$(\varepsilon + 1)(0^* + 01)^*$$

6. S slovensko abecedo napisi besedo "ljubljana" v vseh sklonih (case insensitive)

   $(L+l)(J+j)(U+u)(B+b)(L+l)(J+j)(A+a)(N+n)\,((A+a)(O+o)(E+e)(I+i))$

   Koliko nizov opišemo s tem regularnim izrazom?

   $$2^8 \cdot 2^3 = 2^{11} \text{ nizov}$$

4 Končni avtomati

4.1 Nedeterministični končni avtomat z epsilon prehodi

$\varepsilon - NKA$ je $M = < Q, \Sigma, \delta, q_0, F >$

- Q - končna množica stanj
- Σ - abeceda, ki vsebuje tudi ε
- δ - funkcija prehodov ($\delta : Q \times \Sigma \to 2^Q$)
- q_0 - začetno stanje
- F - množica končnih stanj

4.2 Nedeterministični končni avtomat

NKA je $M = < Q, \Sigma, \delta, q_0, F >$

- Q - končna množica stanj
- Σ - abeceda
- δ - funkcija prehodov ($\delta : Q \times \Sigma \to 2^Q$)
- q_0 - začetno stanje
- F - množica končnih stanj

4.3 Deterministični končni avtomat

DKA je $M = < Q, \Sigma, \delta, q_0, F >$

- Q - končna množica stanj
- Σ - abeceda
- δ - funkcija prehodov ($\delta : Q \times \Sigma \to Q$)
- q_0 - začetno stanje
- F - množica končnih stanj

primeri

1.

4.4 Regularne gramatike

Desno linearne, levo linearne, ...

4.5 Pretvarjanje med regularnimi ...

Regularni izrazi, regularne gramatike in vsi do sedaj omenjeni avtomati so enako močni in je možno poljubnega pretvarjati med njimi.

5 Slovar

- Razred - razred je množica elementov, ki ga lahko podamo z naštevanjem elementov ali z opisom lastnosti (opisni ali konceptualni razredi)