Teoretične osnove računalništva - zapiski iz vaj 2010/2011

Miha Zidar

24. februar 2011

Kazalo

Poglavje 1

Uvod

1.1 Dokazovaje

1.1.1 Dokaz s konstrukcijo

Dokaz obstoja nekega objekta je to, da nam objekt uspe skonstruirati.

Primer 1: Ali za vsako število elementov, večje od 4, obstaja graf ki ima natanko 3 liste?
Primer 2: $|\mathbb{R}| = |[0,1)|$

1.1.2 Dokaz z indukcijo

Če je množica induktivni razred[1], lahko z matematično indukcijo dokazujemo neko lastnost članov množice.

Induktivni razred I sestavlja:

- Baza indukcije - najbolj osnovna množica elementov (osnovni razred)
- Pravila generiranja - kako iz elementov baze gradimo nove elemente (množico)

Primer 1: Induktivni razred naravnih števil ($\mathbb{N}$)

- Baza: $1 \in \mathbb{N}$
- Pravila generiranja: $n \in \mathbb{N} \Longrightarrow n + 1 \in \mathbb{N}$

Primer 2: Hilbertove krivulje[2]

1.1.3 Dokaz s protislovjem

Vzamemo nasprotno trditev, od tiste, ki jo želimo preveriti in pokažemo, da to vodi v protislovje.

Primer 1: Praštevil je končno mnogo

- Predpostavimo, da poznamo vsa praštevila:
  $P = \{2, 3, 5, ..., p\}$, kjer je p zadnje praštevilo
- Po definiciji obstajajo le praštevila in sestavljena števila (to so taka, ki jih lahko razstavimo na prafaktorje).
- Če pomnožimo vsa znana praštevila iz P in prištejemo 1 dobimo število, ki se ga ne da razstaviti na prafaktorje iz množice P:
  $q = 2 * 3 * 5 * ... * p + 1$
- Torej je q ali praštevilo (ker ni sestavljeno), ali pa število, sestavljeno iz prafaktorjev, ki jih ni v množici P.
- Oboje kaže na to, da v množici P nimamo vseh praštevil in da to velja za vsako končno množico praštevil.

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

Primer 2: $\sqrt[3]{2}$ je racionalno število

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

Poglavje 2

Regularni jeziki

2.1 Uvod

Oznake

- a - simbol oz. beseda dolžine 1
- Σ - abeceda oz. končna neprazna množica simbolov
- w - besede, nizi oz. poljubno končno zaporedje simbolov $w_1 w_2 \dots w_n$.
- $|w|$ - dolžina niza - je 0 za $w = \varepsilon$
- ε - prazen niz oz. niz dolžine 0

Operacije

- Stik
  - Nizov:

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

  - Množic:

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

- Potenciranje

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

- Iteracija

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

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

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

2.2 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
- $\{0^n 1^n \mid n \geqslant 0$ ni regularni izraz

Primer:

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?

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

2.3 Končni avtomati

2.3.1 Nedeterministični končni avtomati z ε-prehodi

Def.: εNKA je definiran kot peterka $M = \langle Q, \Sigma, \delta, q_0, F \rangle$, kjer je:

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

2.3.2 Nedeterministični končni avtomati

Def.: NKA je definiran kot peterka $M = \langle Q, \Sigma, \delta, q_0, F \rangle$, kjer je:

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

2.3.3 Deterministični končni avtomat

Def.: DKA je definiran kot petorka $M = \langle Q, \Sigma, \delta, q_0, F \rangle$, kjer je:

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

Primer:

2.3.4 Regularne gramatike

Desno linearne, levo linearne, ...

2.3.5 Pretvarjanje med regularnimi ...

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

Poglavje 3

Slovar

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