Teoretične osnove računalništva

Zapiski predavanj 2010/2011

23. februar 2011

Kazalo

Poglavje 1

Turingov Stroj

1.1 Zgodovina

Eden izmed Hilbertovih problemov (deseti po vrsti), je vprašanje, ali obstaja postopek, ki pove, če je neka poljubna diofantska enačba rešljiva - torej ali lahko ugotovimo, če ima polinom $P(x_1, x_2, \ldots, x_n) = 0$ celoštevilsko rešitev.

Matematiki so se precej ukvarjali s tem problemom in kmalu ugotovili, da pojem postopka oz. algoritma ni bil dovolj dobro definiran.

Osnovna intuitivna definicija se glasi nekako tako:

Def.: Algoritem je zaporedje ukazov, s katerimi se v končnem številu korakov opravi neka naloga.

Ostaja pa še kar nekaj odprtih vprašanj, npr.:

- Kakšni naj bodo ukazi?
  - Osnovni - algoritem ima veliko korakov
  - Kompleksni - algoritem nalogo reši v enem koraku
- Koliko ukazov naj bo?
  - Končno - ali je s tako množico res mogoče rešiti vsako nalogo?
  - Neskončno - kakšen izvajalec je sposoben uporabljati neskončno ukazov?
- So ukazi zvezni ali diskretni?
- V kakšnem pomnilniku so ukazi shranjeni?
  - Končnem
  - Neskončnem

Nekateri zgodnji poskusi formalizacije pojma algoritma:

- GK (Kurt Gödel, Stephen Kleene)
- HG (Jacques Herbrand, Kurt Gödel)
- (Andrey Markov),
- Produkcijski sistem (Emil Post),
- Lambda račun (Alonso Church, 1936)
- Turingov stroj (Alan Turing, 1936)

1.2 Definicija Turingovega stroja

Def.: Turingov stroj je sedmerka $M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$ kjer je:

- Q končna množica stanj
- Σ končna množica vhodnih simbolov, $Q \cap \Sigma = \emptyset$
- Γ končna množica tračnih simbolov, $\Sigma \subset \Gamma$
- δ funkcija prehodov: $Q \times \Gamma \to Q \times \Gamma \times \{L, D\}$, kjer L in D označujeta premik levo ali desno
- q_0 začetno stanje, $q_0 \in Q$
- B prazen simbol, $B \in \Gamma$
- F množica končnih stanj, $F \subseteq Q$

1.2.1 Trenutni opis

Def.: $TO = \Gamma^* \times Q \times \Gamma^*$ je množica vseh trenutnih opisov.
Nek trenutni opis (α_1, q, α_2), ali krajše $\alpha_1\ q\ \alpha_2$ opisuje konfiguracijo Turingovega stroja.

Iz α_1 in α_2, lahko razberemo:

- če je $\alpha_1 = \varepsilon$, je okno skrajno levo
- če je $\alpha_2 = \varepsilon$, je okno nad B in so naprej sami B-ji

1.2.2 Relacija $\vdash$

Def.: Če sta u, v trenutna opisa, ter v neposredno sledi iz u v enem koraku Turingovega stroja, tedaj pišemo $u \vdash v$.

Naj bo $x_1 \dots x_{i-1}\ q\ x_i \dots x_n$ trenutni opis:

- če je $\delta(q, x_i) = (p, Y, D)$:
  $x_1 \dots x_{i-1}\ q\ x_i \dots x_n \vdash x_1 \dots x_{i-1}\ Y\ p\ x_{i+1} \dots x_n$
- če je $\delta(q, x_i) = (p, Y, L)$:
  - če je okno na robu ($i = 1$), se Turingov stroj ustavi, ker je trak na levi omejen.
  - če okno ni na robu ($i > 1$), potem: $x_1 \dots x_{i-1}\ q\ x_i \dots x_n \vdash x_1 \dots\ p\ x_{i-1}\ Y\ x_{i+1} \dots x_n$

1.2.3 Tranzitivna ovojnica $\vdash^*$ relacije $\vdash$

Def.: $u \vdash^* v$, če obstaja tako zaporedje $x_i, (i \in [0, 1, \dots, k], k \geq 0)$, da velja $u = x_0, v = x_k$ in $x_0 \vdash x_1 \wedge x_1 \vdash x_2 \wedge \dots \wedge x_{k-1} \vdash x_k$

Torej, trenutni opis v sledi iz u, v k korakih Turingovega stroja.

1.3 Jezik Turingovega stroja

Def.: Jezik Turingovega stroja je definiran kot:

$$L(M) = \{w \mid w \in \Sigma^* \wedge q_0 w \vdash^* w_1\ q\ w_2 \wedge w_1, w_2 \in \Gamma^* \wedge q \in F\}$$

Z besedami to pomeni, da je $L(M)$ množica besed $w \in \Sigma^*$, ki če jih damo na vhod stroju M, povzročijo, da se stroj M v končno mnogo korakih znajde v končnem stanju.

Def.: Jezik L je Turingov jezik, če obstaja Turingov stroj M, tak, da je $L = L(M)$.

1.3.1 Ugotavljanje pripadnosti besed Turingovemu jeziku

Pri vprašanju ali je neka beseda v jeziku, Turingove jezike ločimo na:

- Odločljive - obstaja algoritem, s katerim se lahko za poljubno besedo odločimo, ali pripada jeziku.
- Neodločljive - v splošnem ni algoritma, ki bi za poljubno vhodno besedo z DA ali NE odgovoril na vprašanje pripadnosti.
  - če je odgovor DA, to ugotovimo v nekem končnem številu korakov.
  - če je odgovor NE, pa ni nujno, da se bo stroj kdaj ustavil.