IN2505-II Berekenbaarheidstheorie

College 10

Hans Tonino

Algoritmiekgroep
Faculteit EWI – TU Delft

20 mei 2009

Opgave

Ga na of de volgende uitspraak waar of onwaar is:

Als A en B beide niet Turing-herkenbare talen zijn, dan geldt $A \leq_m B$.

Antwoord

NEEN !!!

Tegenvoorbeeld: Neem $A = \overline{EQ_{\mathsf{TM}}}$ en $B = \overline{A_{\mathsf{TM}}}$.

Zowel $\overline{EQ_{\mathsf{TM}}}$ als $\overline{A_{\mathsf{TM}}}$ zijn niet Turing-herkenbaar.

$\overline{EQ_{\mathsf{TM}}} \leq_m \overline{A_{\mathsf{TM}}}$ kan niet gelden. Immers, dit is equivalent met $EQ_{\mathsf{TM}} \leq_m A_{\mathsf{TM}}$. Omdat A_{TM} Turing-herkenbaar is, zou ook EQ_{TM} Turing-herkenbaar moeten zijn, maar dat is niet zo.

Stelling van Rice

Zij P een verzameling van Turing-machines die voldoet aan:

1. P is uitsluitend gedefinieerd in termen van input-output-gedrag van TM's, d.w.z. als $L(M_1) = L(M_2)$, dan $\langle M_1 \rangle \in P$ d.e.s.d.a. $\langle M_2 \rangle \in P$;
2. P is niet triviaal, d.w.z., $P \neq \emptyset$ en $\overline{P} \neq \emptyset$.

Dan is P niet beslisbaar.

Bewijs (1)

Zij $M_\emptyset$ een TM die op iedere invoer "loopt". Dit betekent dat $L(M_\emptyset) = \emptyset$.
Als $\langle M_\emptyset \rangle \notin P$, dan voeren we een reductie $HALT_{\mathsf{TM}} \leq_m P$ uit, en anders $HALT_{\mathsf{TM}} \leq_m \overline{P}$. De reductie loopt in beide gevallen op dezelfde wijze.
Neem aan dat $\langle M_\emptyset \rangle \notin P$. Zij verder $\langle M_P \rangle \in P$ (we weten dat $P \neq \emptyset$).

Bewijs (2)

De reductie f is als volgt gedefinieerd:

$$f(\langle M, w \rangle) = \langle M_1 \rangle,$$

met:

M_1 = "Op invoer x:

1. Draai M op invoer w.
2. Draai M_P op invoer x.
3. Geef als output de output van M_P op x."

Bewijs (3)

Nu geldt:

- Als $\langle M, w \rangle \in HALT_{\mathsf{TM}}$, dan $L(M_1) = L(M_P)$ (immers M_1 komt altijd aan de stappen 2 en 3 toe). Maar dan geldt $\langle M_1 \rangle \in P$, aangezien $\langle M_P \rangle \in P$.
- Als $\langle M, w \rangle \notin HALT_{\mathsf{TM}}$, dan zal M_1 bij het uitvoeren van stap 1 niet in een stoptoestand terecht komen, zodat $L(M_1) = \emptyset = L(M_\emptyset)$. Derhalve $\langle M_1 \rangle \notin P$, omdat $\langle M_\emptyset \rangle \notin P$.

Aangezien f een berekenbare functie is, hebben we hiermee een reductie gegeven. Het andere geval gaat net zo.

Reductie via berekeningsgeschiedenis

Deze techniek gebruikt berekeningsgeschiedenissen bij het construeren van een reductie.

(Sipser p. 196 e.v.)

Berekeningsgeschiedenissen (Def. 5.5)

Zij M een TM en w een invoerwoord. Een accepterende berekeningsgeschiedenis voor M op w is een reeks configuraties $C_1, C_2, \ldots, C_l$ waarbij C_1 de startconfiguratie van M op w is, C_l een accepterende configuratie van M is, en waarbij iedere C_i wordt opgeleverd door C_{i-1}.

Een verwerpende berekeningsgeschiedenis is evenzo gedefinieerd, behalve dat C_l een verwerpende configuratie is.

Lineair begrensde automaten (Def. 5.6)

Een Lineair Begrensde Automaat (LBA) is een TM waarbij de lees/schrijfkop niet het deel van de tape mag/kan verlaten waarop de invoer staat (stond).

Opgave

Leg uit waarom voor een LBA geldt (en dit verklaart haar naam):

Omdat het tape-alfabet groter mag zijn dan het invoeralfabet, is het beschikbare geheugen van een LBA in feite gelijk aan een constante factor maal de lengte van de invoer.

Aantal configuraties LBA's (Lem. 5.8)

Zij M een LBA met q toestanden en g symbolen in het tape-alfabet. Dan zijn er precies qng^n verschillende configuraties van M voor een tape van lengte n.

Het acceptatieprobleem voor LBA's (Th. 5.9)

Het acceptatieprobleem A_{LBA} voor LBA's gedefinieerd door

$$A_{\mathsf{LBA}} = \{\langle M, w\rangle \mid M \text{ is een LBA die invoer } w \text{ accepteert}\}$$

is beslisbaar.

Onbeslisbaarheid van E_{LBA} (Th. 5.10)

Het probleem E_{LBA} gedefinieerd door:

$$E_{\mathsf{LBA}} = \{\langle M\rangle \mid M \text{ is een LBA met } L(M) = \emptyset\}$$

is niet beslisbaar.

Bewijs: reductie via berekeningsgeschiedenis:

$$A_{\mathsf{TM}} \leq E_{\mathsf{LBA}}.$$

Neem aan dat R een beslisser is die E_{LBA} beslist.

Hulpconstructie

We construeren een LBA B die voor een specifieke TM M en invoer w de taal bestaande uit alle accepterende berekeningsgeschiedenissen van M op w herkent. Deze B is zodanig dat:

$$L(B) \neq \emptyset \qquad \Leftrightarrow \qquad M \text{ accepteert } w.$$

Merk op dat $L(B)$ één string bevat als M invoer w accepteert.

Deze B kunnen we "voeren" aan de beslisser R.

Het Post-correspondentieprobleem

Zij gegeven een verzameling "dominostenen" van de vorm:

$$\left[\frac{t}{b}\right],$$

waarbij $t, b \in \Sigma^+$ voor een zeker alfabet Σ.

Kun je een rij dominostenen leggen waarbij herhaling van stenen is toegestaan,

$$\left[\frac{t_1}{b_1}\right]\left[\frac{t_2}{b_2}\right]\ldots\left[\frac{t_n}{b_n}\right]$$

zodanig dat $t_1t_2\ldots t_n = b_1b_2\ldots b_n$?

Dit probleem staat bekend als PCP, het Post-correspondentieprobleem (Sipser p. 203 e.v.).

Voorbeeld dominostenen

Zij bijvoorbeeld de volgende verzameling dominostenen gegeven:

$$\left\{ \left[\frac{\mathsf{b}}{\mathsf{ca}}\right], \left[\frac{\mathsf{a}}{\mathsf{ab}}\right], \left[\frac{\mathsf{ca}}{\mathsf{a}}\right], \left[\frac{\mathsf{abc}}{\mathsf{c}}\right] \right\}.$$

Een "match" is bijvoorbeeld:

$$\left[\frac{\mathsf{a}}{\mathsf{ab}}\right] \left[\frac{\mathsf{b}}{\mathsf{ca}}\right] \left[\frac{\mathsf{ca}}{\mathsf{a}}\right] \left[\frac{\mathsf{a}}{\mathsf{ab}}\right] \left[\frac{\mathsf{abc}}{\mathsf{c}}\right].$$

Onbeslisbaarheid PCP (Th. 5.15)

PCP is niet beslisbaar.

Bewijs: reductie via berekeningsgeschiedenis:

$$A_{\mathsf{TM}} \leq PCP.$$

Eigenlijk reductie $A_{\mathsf{TM}} \leq MPCP$, waarbij MPCP een gemodificeerde versie van PCP is: een match begint altijd met een gegeven dominosteen.

Idee reductie

We laten zien dat er voor iedere TM M met invoer w een instantie P van MPCP kan worden geconstrueerd met de eigenschap:

$$P \text{ bezit een match} \quad \Leftrightarrow \quad M \text{ accepteert } w.$$

Een matching string is daarbij steeds zodanig dat deze de berekeningsgeschiedenis van een accepterende berekening van M op w voorstelt.

Gegeven een beslisser R van MPCP, kan deze P aan R worden "gevoerd".

Constructie P

Gegeven $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$ en $w = w_1 w_2 \dots w_n$, bevat P de volgende dominostenen:

1. $\left[\frac{\#}{\# q_0 w_1 w_2 \dots w_n \#}\right]$ (startconfiguratie is startsteen),
2. $\left[\frac{qa}{br}\right]$ voor iedere $a, b \in \Gamma$ en $q, r \in Q$ waarvoor $q \neq q_{reject}$ en $\delta(q, a) = (r, b, R)$ (δ-regels rechts),
3. $\left[\frac{cqa}{rcb}\right]$ voor iedere $a, b, c \in \Gamma$ en $q, r \in Q$ waarvoor $q \neq q_{reject}$ en $\delta(q, a) = (r, b, L)$, (δ-regels links),
4. $\left[\frac{a}{a}\right]$ voor iedere $a \in \Gamma$ (symbolen die niet gewijzigd worden),
5. $\left[\frac{\#}{\#}\right]$ en $\left[\frac{\#}{\sqcup \#}\right]$ (copiëren $\#$ en tape rechts verlengen),

Vervolg constructie P

6. $\left[\frac{a q_{accept}}{q_{accept}}\right]$ en $\left[\frac{q_{accept} a}{q_{accept}}\right]$ (de eindconfiguratie "opeten"), en
7. $\left[\frac{q_{accept}\#\#}{\#}\right]$ (afsluitende steen).

Let op: Het symbool $\#$ is zo gekozen dat het niet in Γ voorkomt.

Van MPCP naar PCP

Ieder MPCP-probleem A kan worden omgezet in een daarmee equivalent PCP-probleem B, dat wil zeggen

$$A \text{ bezit een match} \quad \Leftrightarrow \quad B \text{ bezit een match}$$

De truc...

Zij $u = u_1 u_2 u_3 \cdots u_n$ met $u_i \in \Sigma$ $(1 \leq i \leq n)$, definieer:

$$\begin{aligned} \star u &= * u_1 * u_2 * u_3 * \cdots * u_n, \\ u\star &= u_1 * u_2 * u_3 * \cdots * u_n *, \\ \star u \star &= * u_1 * u_2 * u_3 * \cdots * u_n *. \end{aligned}$$

De omzetting

De volgende instantie van MPCP

$$\left\{\left[\frac{t_1}{b_1}\right], \left[\frac{t_2}{b_2}\right], \left[\frac{t_3}{b_3}\right], \ldots, \left[\frac{t_k}{b_k}\right]\right\}.$$

kan worden omgezet in de volgende instantie van PCP

$$\left\{\left[\frac{\star t_1}{\star b_1 \star}\right], \left[\frac{\star t_1}{b_1 \star}\right], \left[\frac{\star t_2}{b_2 \star}\right], \left[\frac{\star t_3}{b_3 \star}\right], \ldots, \left[\frac{\star t_k}{b_k \star}\right], \left[\frac{* \diamond}{\diamond}\right]\right\}.$$