IN2505-II Berekenbaarheidstheorie

College 4

Hans Tonino

Algoritmiekgroep
Faculteit EWI – TU Delft

20 april 2009

Vorig college

- Vervolg NDTM's
- Vergelijking rekenkracht TM's en NDTM's
- Voorbeelden NDTM's

Opsommers

Een TM M is een opsommer (enumerator) van taal L als deze, gegeven het lege woord op de invoertape, alle woorden van L op een uitvoertape (mogelijkerwijs dezelfde tape als de invoertape) print, gescheiden door spaties en in een door de machine bepaalde volgorde.

Opsommers versus herkenners (Th. 3.21)

Een taal is Turing-herkenbaar d.e.s.d.a. er een opsommer voor de taal bestaat.

Idee bewijs 1

Opsommer $\Rightarrow$ herkenner: draai de opsommer en wacht op het te herkennen woord; als het voorbij komt: accepteer.

Idee bewijs 2a

Herkenner $\Rightarrow$ opsommer: zwaluwstaarttechniek, time-slicing

Laat de herkenner een steeds toenemende tijd rekenen op een tegelijkertijd toenemend aantal eerste woorden uit een opsomming van Σ^*. Print ieder woord dat daarbij herkend wordt op de tape.

Idee bewijs 2b

Zij gegeven de opsomming (bijv. alfabetisch)
$w_0, w_1, w_2, \ldots, w_n, \ldots$

Reken (en print bij acceptatie):
0 tijdseenheden op w_0.
1 tijdseenheid op w_0, w_1.
2 tijdseenheden op w_0, w_1, w_2.
...
n tijdseenheden op $w_0, w_1, w_2, \ldots, w_n$.
...

Opgave

Onder welke aanvullende voorwaarde zou het bestaan van een opsommer van een taal impliceren dat deze taal beslisbaar is?

Opgave Sipser 3.6

Zij L een Turing-herkenbare taal en zij M een herkenner van L. Is de volgende TM dan een opsommer van L? Neem aan dat $s_1, s_2, \ldots$ een lijst is van alle elementen van Σ^*.

M' = "Op lege invoer:

1. Herhaal voor $i = 1, 2, 3, \ldots$
2. Draai M op s_i.
3. Als M accepteert, print s_i."

Opgave Sipser 3.18 en 3.19

- Laat zien dat een taal L Turing-beslisbaar is d.e.s.d.a. er een opsommer voor L bestaat die L in alfabetische volgorde opsomt.
- Laat zien dat iedere oneindige Turing-herkenbare taal een oneindige beslisbare deelverzameling bezit.

Hilbert's 10^{e} probleem

In 1900 publiceerde David Hilbert (1862-1943) een lijst met 23 problemen waaronder het 10^{e} probleem:

> *Bestaat er een procedure waarmee in een eindig aantal stappen kan worden bepaald of een polynoom met geheeltallige coëfficiënten een geheeltallige wortel bezit (een toekenning van gehele getallen aan de variabelen die het polynoom de waarde 0 geeft).*

Overigens...

Het probleem (de taal)

$$\{p \mid p \text{ is een polynoom met een geheeltallige wortel}\}$$

is niet beslisbaar (Yuri Matiyasevich, 1970).

$$\{p \mid p \text{ is een polynoom in } x \text{ met een geheeltallige wortel}\}$$

is wel beslisbaar (zie ook opgave Sipser 3.21)!

Opgave Sipser 3.7

Leg uit waarom de volgende beschrijving geen legitieme TM is ter oplossing van Hilbert's 10^e probleem:

M = "Op invoer van een polynoom p met variabelen $x_1, \ldots, x_k$:

1. Probeer alle geheeltallige waardetoekenningen aan $x_1, \ldots, x_k$.
2. Bereken p voor al deze waardetoekenningen.
3. Als $p(x_1, \ldots, x_k) = 0$ voor een van deze toekenningen accepteer anders verwerp."

Opgave Sipser 3.7 (variant)

Leg uit waarom de volgende beschrijving van een NDTM geen beslisser is van Hilbert's 10^e probleem:

M = "Op invoer van een polynoom p met variabelen $x_1, \ldots, x_k$:

1. Gok een geheeltallige waardetoekenning aan $x_1, \ldots, x_k$.
2. Bereken p voor deze waardetoekenning.
3. Accepteer als $p(x_1, \ldots, x_k) = 0$, anders verwerp."

Het Entscheidungsproblem

In 1928 formuleerde Hilbert het zogenaamde Entscheidungsproblem:

> *Bestaat er een procedure waarmee in een eindig aantal stappen kan worden bepaald of een willekeurige wiskundige uitspraak (geformuleerd in formele taal) waar of onwaar is.*

Het 10^e probleem is een speciaal geval van het Entscheidungsproblem.

N.a.v. dit probleem bedachten Turing en Church in 1936 onafhankelijk van elkaar hun berekeningsmodellen. Deze bleken equivalent te zijn.

Church-Turing These

Alle tot nu toe bedachte berekeningsmodellen zijn equivalent gebleken. Dit rechtvaardigt in zekere zin:

Intuïtieve notie van algoritme
=
Algoritme als Turingmachine (of als λ-term)

Anders gezegd: iets is berekenbaar als er een TM voor gevonden kan worden.

Intelligent leven elders in het heelal?

Beschouw het volgende getal:

$$p = \begin{cases} 1 & \text{als er elders intelligent leven bestaat in het heelal;} \\ 0 & \text{anders} \end{cases}$$

Vraag: Is de verzameling $\{p\}$ beslisbaar?

Coderen van objecten

Een programma P in programmeertaal X^{++} wordt gecompileerd naar een bitreeks. Deze reeks kun je opvatten als de codering van P naar een woord uit $\{0,1\}^*$. De codering bewaart de belangrijkste eigenschap van P: zijn operationele 'betekenis'. Het programma als bitreeks kan worden gezien als een getal in binaire code:

Een programma is een getal!

In het boek wordt de codering van een object P (programma of data) weergegeven als $\langle P \rangle$. Daarbij wordt in het midden gelaten welke codering wordt gebruikt.

Voorbeeld codering

Context: grafentheorie.

Beschouw het volgende probleem (taal):

$$\{\langle G \rangle \mid G \text{ is een verbonden, ongerichte graaf}\}.$$

Er zijn verschillende zinvolle coderingen van grafen te bedenken.

Aanbevolen opgaven

Sipser p. 163 e.v.: 3.15, 3.16, 3.17.