IN2505-II Berekenbaarheidstheorie

College 5

Hans Tonino

Algoritmiekgroep
Faculteit EWI – TU Delft

23 april 2009

Vorig college

- Opsommers vs. Herkenners
- Church-Turing These
- Codering van problemen

Aanbevolen opgaven

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

Wat is oneindigheid?

- Natuurlijke getallen $\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$
- Hotel Hilbert
- Aftelbaarheid
- Aftelbaar oneindig

(Sipser p. 176)

Functies (Def. 4.12)

Een functie $f : A \to B$ is:

- surjectief (onto): er bestaat voor iedere $b \in B$ een $a \in A$ met $f(a) = b$.
- injectief (one-to-one): als $a \neq b$, dan $f(a) \neq f(b)$.
- bijectief (correspondence): f is zowel surjectief als injectief.

Gelijkmachtigheid (eindige geval)

Twee eindige verzamelingen A en B zijn gelijkmachtig (even groot, same size) als deze evenveel elementen bezitten, ofwel als er een bijectie $f : A \to B$ bestaat.

(Sipser, Def. 4.12)

Gelijkmachtigheid (oneindige geval)

Voor oneindige verzamelingen kunnen we dit als volgt generaliseren:

Twee oneindige verzamelingen A en B zijn gelijkmachtig (even groot) als er een bijectie $f : A \to B$ bestaat.

(Sipser, Def. 4.12)

Aftelbaarheid (Def. 4.14)

- Een verzameling A is *oneindig aftelbaar* (countably infinite, at most countable) als er een bijectie bestaat tussen A en $\mathbb{N}$.
- Een verzameling A is *aftelbaar* (countable) als A eindig is, of als A aftelbaar oneindig is.
- Alternatieve definitie: Een verzameling A is *aftelbaar* als $A = \emptyset$ of als er een surjectie bestaat van $\mathbb{N}$ naar A.
- Een verzameling is *overaftelbaar* (uncountable) als deze niet aftelbaar is.

Aftelbare verzamelingen

- $\mathbb{Z}$
- $\mathbb{N} \times \mathbb{N}$
- $\mathbb{Q}$
- De verzameling programma's in taal X^{++}

Voorbeeld $\mathbb{N} \times \mathbb{N}$

Aftelling:

$(0,0),(1,0),(0,1),(2,0),(1,1),(0,2),(3,0),(2,1),(1,2),(0,3),\ldots$

Definieer $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$:

$$f(m,n) = \frac{(m+n)(m+n+1)}{2} + n.$$

Bijvoorbeeld: $(2,3) \mapsto 18$.

f is een injectie.

Opgave

Bedenk een aftelling voor alle rationale getallen die groter dan of gelijk zijn aan 0, met andere woorden, bedenk een aftelling voor de verzameling:

$$\{q \in \mathbb{Q} \mid q \geq 0\}.$$

Alephs

De $\aleph$ is de eerste letter uit het Hebreeuwse alfabet. Met $\aleph_0$ wordt de eerste graad van oneindigheid aangeduid: het aantal natuurlijke getallen. Men kan met $\aleph$'s rekenen (denk aan Hotel Hilbert):

- $\aleph_0 + 1 = \aleph_0$
- $\aleph_0 + \aleph_0 = \aleph_0$
- $\aleph_0 \cdot \aleph_0 = \aleph_0$

Slimme constructie gevraagd

Gegeven een tabel met rijen getallen:

$$\begin{array}{ccccc} 8 & 13 & 99 & 71 & \dots \\ 101 & 94 & 99 & 34 & \dots \\ 37 & 94 & 49 & 85 & \dots \\ 20 & 54 & 67 & 12 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Hoe construeer je op systematische wijze een rij die niet in de tabel voorkomt?

Diagonaal

Doe 'iets' met de diagonaal, bijvoorbeeld:

$$\begin{array}{ccccc} 8+1 & 13 & 99 & 71 & \dots \\ 101 & 94+1 & 99 & 34 & \dots \\ 37 & 94 & 49+1 & 85 & \dots \\ 20 & 54 & 67 & 12+1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Dit geeft de rij:
9, 95, 50, 13, ...
Deze kan niet voorkomen in de tabel!

$\mathbb{R}$ is overaftelbaar! (Th. 4.17)

Bewijs:
Standaardbewijs is dat aangetoond wordt dat $(0,1)$ niet aftelbaar is. Als $(0,1)$ niet aftelbaar is, dan is $\mathbb{R}$ dat ook niet.

Stel dat $(0,1)$ aftelbaar is, leidt hier dan m.b.v. diagonalisatie een tegenspraak uit af.

$\mathbb{R}$ is overaftelbaar (2)

Stel $r_0, r_1, r_2, \dots, r_m, \dots$ is een aftelling van $(0,1)$.
Ieder element $r_m \in (0,1)$ kan worden weergegeven als:

$$r_m = 0.r_{m_0} r_{m_1} r_{m_2} \dots r_{m_n} \dots$$

Definieer:

$$d = 0.d_0 d_1 d_2 \dots d_n \dots$$

met

$$d_n = \begin{cases} 8 & \text{als } r_{nn} = 7, \\ 7 & \text{anders.} \end{cases}$$

Dan hebben we een tegenspraak afgeleid, want

1. $d \in (0,1)$, maar
2. wegens constructie geldt $d \neq r_m$ voor alle $m = 0, 1, 2, \dots$ ofwel d komt niet in de aftelling voor.

Opgave

Waarom kunnen we niet op dezelfde wijze als we de overaftelbaarheid van $\mathbb{R}$ hebben aangetoond, bewijzen dat $\mathbb{Q}$ overaftelbaar is. Immers, elementen uit $\mathbb{Q}$ kunnen ook in decimale representatie worden voorgesteld. Met andere woorden, wat gaat er dan fout in dat bewijs?

Karakteristieke functie

Beschouw een deelverzameling $A \subseteq \mathbb{N}$. We kunnen A op tenminste twee manieren representeren:

1. als verzameling, bijvoorbeeld $A = \{0, 1, 4, 9, 16, 25, \ldots\} = \{n^2 \mid n \in \mathbb{N}\}$.
2. als karakteristieke functie $\chi_A : \mathbb{N} \to \{0, 1\}$:

$$\chi_A(x) = \begin{cases} 1 & \text{als } x \in A, \\ 0 & \text{als } x \notin A. \end{cases}$$

Bijvoorbeeld $\chi_A(0) = 1, \chi_A(1) = 1, \chi_A(2) = 0, \ldots$.

Karakteristieke functie van een taal

Ook voor een taal $L \subseteq \Sigma^*$ kunnen we een karakteristieke functie $\chi_L : \Sigma^* \to \{0, 1\}$ definiëren:

$$\chi_L(x) = \begin{cases} 1 & \text{als } x \in L, \\ 0 & \text{als } x \notin L. \end{cases}$$

Karakteristieke reeks van een taal

In plaats van karatkteristieke functie gebruikt Sipser het begrip karakteristieke reeks. Hierbij wordt uitgegaan van een standaard aftelling van $\Sigma^* = \{s_0, s_1, s_2, \ldots, s_i, \ldots\}$. Nu is χ_L een oneindige reeks van 0-en en 1-en: $\chi_L = b_0 b_1 b_2 \ldots b_i \ldots$ waarbij:

$$b_i = \begin{cases} 1 & \text{als } s_i \in L, \\ 0 & \text{als } s_i \notin L. \end{cases}$$

(Sipser, p. 180)

Andere overaftelbare verzamelingen

- De verzameling $\mathscr{P}(\mathbb{N}) = \{V \mid V \subseteq \mathbb{N}\}$ van alle deelverzamelingen van $\mathbb{N}$ is overaftelbaar.
- De verzameling van alle functies $f : \mathbb{N} \to \mathbb{N}$ is overaftelbaar.

Diagonalisatiemethode: samenvatting

Als je moet bewijzen dat een verzameling V niet aftelbaar is, ga je als volgt te werk:

1. Stel dat V (of een geschikte deelverzameling $W \subseteq V$) wel aftelbaar is.
2. Representeer V (of W) als een oneindige tabel.
3. Construeer uitgaande van de diagonaal van deze tabel een element $s \in V$ (of $s \in W$) dat niet in de tabel kan voorkomen, maar er wel in zou moeten voorkomen. (Diagonaalelementen + 1 werkt niet altijd!)
4. Tegenspraak, derhalve is V niet aftelbaar.

Niet-herkenbare talen (Cor. 4.18)

Er bestaan talen die niet Turing-herkenbaar zijn.

Waarom?

1. Σ^* is oneindig-aftelbaar.
2. Voor een taal L over Σ geldt: $L \subseteq \Sigma^*$.
3. De collectie van alle talen over Σ is gelijk aan $\mathscr{P}(\Sigma^*)$.
4. De verzameling $\mathscr{P}(\Sigma^*)$ is overaftelbaar.
5. Er bestaan aftelbaar veel Turingmachines met Σ als invoeralfabet omdat deze gecodeerd kunnen worden als een string over een of ander alfabet.
6. Ergo!