

Bachelorprojekt  
Standsningsproblemet og Gödels  
ufuldstændighedssætninger

Bodil Biering

juni 2000

# Contents

<b>Indledning</b>	<b>2</b>
<b>1 Rekursivitet</b>	<b>3</b>
1.1 Rekursive funktioner . . . . .	3
1.2 Turingmaskiner . . . . .	5
<b>2 Standsningsproblemet</b>	<b>11</b>
2.1 Reduktioner . . . . .	13
<b>3 Gödels ufuldstændighedssætninger</b>	<b>17</b>
3.1 Peano's aksiomer . . . . .	18
3.2 Repræsentation . . . . .	21
3.3 Gödelnumre . . . . .	22
3.4 Gödels ufuldstændighedssætninger . . . . .	26
<b>Konklusion</b>	<b>31</b>
<b>Bibliografi</b>	<b>32</b>

# Indledning

Udviklingen af matematikken førte i begyndelsen af 1900-tallet til en komplet formalisering, forstået på den måde, at man havde fået konstrueret et formelt system hvori alle kendte matematiske bevismetoder er reduceret til nogle få mekaniske regler. Et formelt matematisk bevis består dermed af et sæt af aksiomer, hvorpå man har anvendt de førnævnte regler. Store dele af matematikken blev bevist i dette formelle eller logiske system, og der var i 1920'erne en udbredt tro på, at disse aksiomer og regler var tilstrækkelige til at afgøre ethvert matematisk spørgsmål, som man kunne udtrykke i systemet. Gödels ufuldstændighedssætninger (1931) viste imidlertid, at dette ikke var tilfældet.

En computer er et eksempel på et logisk system, da den i princippet handler efter de regler, den er programmeret til. En Turingmaskine er en simpel matematisk model for en computer. Ikke desto mindre kan den i princippet simulere enhver anden computer.

Standsningsproblemet, eller Turings standsningsproblem, som det også bliver kaldt (efter Alan Turing) er Turingmaskinens pendant til Gödels ufuldstændighedssætninger. Standsningsproblemet er umiddelbart et relativt simpelt problem, som Turingmaskinen dog ikke kan afgøre. Standsningsproblemet er i sin natur tæt knyttet til Gödels ufuldstændighedssætninger. Begge dele udtaler sig om nogle af de begrænsninger, der kan være i formelle systemer: Turings standsningsproblem om programmer til maskiner og Gödels ufuldstændighedssætninger om systemer til formalisering af matematikken.

Rekursivitet og formelle systemer (deriblandt Turingmaskiner) hænger uløseligt sammen, det første kapitel handler derfor om rekursivitet. Andet kapitel handler om standsningsproblemet for Turingmaskiner og er altså et eksempel på et formelt system med et uafgørligt problem. Tredje og sidste kapitel handler om Gödels ufuldstændighedssætninger.

Projektet bygger hovedsagligt på Cori & Lascars bog [Las94], og i tredje kapitel forudsætter jeg, at læseren har kendskab til modelteori svarende til de første to kapitler af Mendelsons bog [Men97].

# Chapter 1

## Rekursivitet

Klassen af rekursive funktioner spiller en central rolle i studiet af beregnelighed. Intuitivt er de rekursive funktioner netop de funktioner, som kan beregnes algoritmisk, altså ved hjælp af en mekanisk procedure (Church's tese). Turingmaskinen er et bud på en præcis definition af begrebet algoritme, og det skal vise sig, at en funktion er rekursiv netop når der findes en Turing maskine, der beregner den. Under Church's tese kan Turing maskinen altså beregne præcis de funktioner, som er beregnelige i intuitiv forstand.

### 1.1 Rekursive funktioner

**Definition 1.1** Lad  $\mathcal{F}_p$  være mængden af afbildninger fra  $\mathbb{N}^p$  ind i  $\mathbb{N}$ , og  $\mathcal{F} = \bigcup_{p \in \mathbb{N}} \mathcal{F}_p$ . Mængden af primitive rekursive funktioner er den mindste delmængde  $\mathcal{E}$  af  $\mathcal{F}$ , som opfylder:

1. De konstante funktioner tilhører  $\mathcal{E}$ .
2. Projektionerne  $P_i^k(x_1, \dots, x_k) = x_i$  ligger i  $\mathcal{E}$  for alle  $k \in \mathbb{N}$  og for alle  $i \in 1, \dots, k$ .
3. Succesor-funktionen  $S(x) = x + 1$  tilhører  $\mathcal{E}$ .
4.  $\mathcal{E}$  er stabil under substitution, dvs. hvis  $f_1, \dots, f_n \in \mathcal{F}_k \cap \mathcal{E}$  og  $g \in \mathcal{F}_n \cap \mathcal{E}$ , så er  $g(f_1, \dots, f_n) \in \mathcal{E}$ .
5.  $\mathcal{E}$  er stabil under rekursion, dvs. hvis  $g \in \mathcal{F}_k \cap \mathcal{E}$  og  $h \in \mathcal{F}_{k+2} \cap \mathcal{E}$  og
  - $f(x_1, \dots, x_k, 0) = g(x_1, \dots, x_k)$
  - $f(x_1, \dots, x_k, y + 1) = h(x_1, \dots, x_k, y, f(x_1, \dots, x_k, y))$

da er  $f \in \mathcal{E}$ .

#### Eksempel 1.2

$f(x, y) = x + y$  er primitiv rekursiv idet

- $f(x, 0) = x = P_1^1(x)$
- $f(x, y + 1) = h(x, y, f(x, y))$ , hvor  $h(x, y, z) = S(z) = S(P_3^3(x, y, z))$

Resultatet følger nu af punkterne 2-5 i definitionen. Følgende funktioner er ligeledes primitive rekursive:

$$\delta(x) = \begin{cases} x - 1 & \text{hvis } x > 0 \\ 0 & \text{hvis } x = 0 \end{cases}$$
$$x \dot{-} y = \begin{cases} x - y & \text{hvis } x \geq y \\ 0 & \text{ellers} \end{cases}$$

$$sg(x) = \begin{cases} 0 & \text{hvis } x = 0 \\ 1 & \text{ellers} \end{cases}$$

Beviset er nemt:  $\delta(0) = 0$  og  $\delta(y + 1) = y$  (rekursion)  
 $x - 0 = x$  og  $x - (y + 1) = \delta(x - y)$  (rekursion)  
 $sg(x) = x - \delta(x)$  (substitution).

### Definition 1.3

$\mu$ -operatoren,  $\mu : \mathcal{E} \rightarrow \mathbb{N}$  noteres  $\mu y(g(x_1, \dots, x_k, y) = 0)$  og er det mindste  $y$  således at  $(g(x_1, \dots, x_k, y) = 0)$ . Bemærk, at  $\mu$ -operatoren ikke altid er defineret. Mere præcist gælder der, at  $\mu y(g(x_1, \dots, x_k, y) = 0) = k$ , hvis  $(g(x_1, \dots, x_k, y) = 0)$ , og hvis for alle  $y' < y$ ,  $(g(x_1, \dots, x_k, y'))$  er defineret og forskellig fra nul.

Mængden af *rekursive funktioner*  $\mathcal{E}^*$  er foreningen af de primitive rekursive funktioner  $\mathcal{E}$  og funktionerne opnået fra  $\mathcal{E}$  ved anvendelse af  $\mu$ -operatoren. En rekursiv funktion er ikke nødvendigvis total (i.e. overalt defineret), idet  $\mu$ -operatoren ikke altid er defineret.

### Eksempel 1.4

Lad  $g(x, y) = x - 2$  og  $f(x) = \mu y(g(x, y) = 0)$ ,  $f$  er da den partielle rekursive funktion, som antager værdien 0 for  $x = 2$ , og som ikke er defineret for  $x \neq 2$ .

$h(x) = \mu y(y > x)$  er en total rekursiv funktion, som specielt er primitiv rekursiv, idet den er identisk med successor-funktionen. Der findes totale rekursive funktioner, som ikke er primitive rekursive, for eksempel Ackermann's funktion  $A(x) = A_x(x)$ , hvor  $A_x(x)$  er defineret ved dobbelt rekursion:

- $A_0(x) = 2^x$
- $A_n(0) = 1$
- $A_{n+1}(x + 1) = A_n(A_{n+1}(x))$

se [Las94] p.18 for bevis.

**Definition 1.5** En mængde  $A$  er (primitiv) rekursiv hvis og kun hvis dens indikatorfunktion  $1_A$  er (primitiv) rekursiv.

### Eksempel 1.6

Enhver endelig mængde er primitiv rekursiv. Lad  $A = \{x_1, \dots, x_n\}$  så er

$$1_A = 1 - sg(|x - x_1||x - x_2| \cdots |x - x_n|)$$

som er primitiv rekursiv idet  $|x - y|$  og  $xy$  oplagt er det.

Hvis  $A \subseteq \mathbb{N}^{p+1}$  er primitiv rekursiv, så gælder det samme for mængderne

$$\begin{aligned} B &= \{(x_1, \dots, x_p, y); \exists t \leq y (x_1, \dots, x_p, t) \in A\} \\ C &= \{(x_1, \dots, x_p, y); \forall t \leq y (x_1, \dots, x_p, t) \in A\} \quad \text{thi} \\ 1_B(x_1, \dots, x_p, y) &= sg(\sum_{t=0}^y 1_A(x_1, \dots, x_p, t)) \quad \text{og} \\ 1_C(x_1, \dots, x_p, y) &= sg(\prod_{t=0}^y 1_A(x_1, \dots, x_p, t)) \end{aligned}$$

**Sætning 1.7** For ethvert  $p \in \mathbb{N}$  findes rekursive funktioner  $\alpha_p \in \mathcal{F}_p$  og  $\beta_p^1, \beta_p^2, \dots, \beta_p^p \in \mathcal{F}_1$ , som opfylder at  $\alpha_p$  er en bijektion mellem  $\mathbb{N}^p$  og  $\mathbb{N}$  og  $\lambda x. (\beta_p^1(x), \beta_p^2(x), \dots, \beta_p^p(x))$  er dens reciproke.

#### Bevis:

Sætningen vises ved induktion efter  $p$ . For  $p = 1$  er resultatet oplagt  $\alpha_1 = \beta_1^1 = Id$ . For  $p = 2$  nummereres parrene i  $\mathbb{N}^2$  diagonalt, dvs efter ordenen  $(0,0)$   $(1,0)$   $(0,1)$   $(2,0)$   $(1,1)$   $(0,2)$   $(3,0)$   $(2,1)$   $(1,2)$   $(0,3)$  ... hvor  $(0,0)$  får nummer 0. Så er  $\alpha_2(x, y)$  lig antallet af par der kommer før  $(x, y)$  i ovenstående liste. Den  $n$ 'te diagonal starter med  $(n, 0)$  og har  $n + 1$  elementer, så

$\alpha_2(x, 0) = (x - 1) + 1 + (x - 2) + 1 + (x - 3) + 1 + \dots + 2 + 1 = \frac{1}{2}x(x + 1)$  og  $\alpha_2(x, y)$  er det y'te par efter parret  $(x + y, 0)$ , altså  $\alpha_2(x, y) = \alpha_2(x + y, 0) + y = \frac{1}{2}(x + y)(x + y + 1) + y$ . Bemærk, at  $\alpha_2(x, y) \geq x$  og  $\alpha_2(x, y) \geq y$  så man kan definere

$$\beta_2^1(x) = \mu z \leq x (\exists t \leq x : \alpha_2(z, t) = x) \text{ og } \beta_2^2(x) = \mu z \leq x (\exists t \leq x : \alpha_2(t, z) = x)$$

Lad  $A_x = \{z; \exists t \leq x : \alpha_2(z, t) \in \{x\}\}$  I følge eksempel 1.6 er  $A_x$  primitiv rekursiv, og det følger at  $\beta_2^1(x) = \mu z \leq x (z \in A_x)$  er rekursiv. Tilsvarende for  $\beta_2^2$ .

Antag, at  $\alpha_n$  og  $\beta_n^i$   $1 \leq i \leq n$  eksisterer. Så kan man definere

$$\alpha_{n+1}(x_1, x_2, \dots, x_{n+1}) = \alpha_n(x_1, \dots, x_{n-1}, \alpha_2(x_n, x_{n+1})),$$

som da er rekursiv, og for  $1 \leq i \leq n - 1$  har man da  $\beta_{n+1}^i = \beta_n^i$  mens  $\beta_{n+1}^n = \beta_2^1 \circ \beta_n^n$  og  $\beta_{n+1}^{n+1} = \beta_2^2 \circ \beta_n^n$ , som således også er rekursive.  $\square$

## 1.2 Turingmaskiner

En Turingmaskine (i det følgende forkortet TM) er en matematisk model for det intuitive begreb algoritme. En TM er givet ved:

- $n$  bånd, som hver er delt op i nummererede celler startende fra venstre med cellerne nr 1.
- En endelig mængde af tilstande  $E$
- En afbildning  $M : S^n \times E \rightarrow S^n \times E \times \{-1, 0, 1\}$ , hvor  $S = \{d, b, |\}$ .  $M$  kaldes transitions-tabellen.

d	celle nr.2	celle nr.3	bånd nr.1
d	celle nr.2	celle nr.3	bånd nr.2
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
d	celle nr.2	celle nr.3	bånd nr. $n$

↑  
cursor

Der findes forskellige måder at definere Turingmaskinen på, nogle bruger fx kun et bånd, men de er essentielt ens forstået på den måde, at de beregner de samme funktioner.

TM's bånd er afgrænsede til venstre og uendelige mod højre. TM har desuden en cursor, som kan læse, skrive, slette og flytte sig alt efter instruktionerne givet ved  $M$ .  $E$  indeholder som minimum den initiale tilstand  $e_i$  og en (eller flere) slut-tilstande  $e_f$ . Maskinen befinder sig til ethvert tidspunkt i netop en tilstand.  $S$  er maskinens alfabet bestående af d (for debut) b (blank) og |. Den tredje variabel i  $M$ 's billede angiver, hvilken vej cursoren skal flytte sig (1: en celle til højre, -1: en celle til venstre og 0: blive stående) *efter* at have foretaget eventuelle ændringer i de celler, hvor den står. Maskinen standser når den når en slut-tilstand  $e_f$ . Cellerne med nr 1 indeholder altid symbolet d. Maskinen kan ikke slette symbolet d, og cursoren kan ikke gå længere til venstre når den står ved d. Til tiden  $t = 0$  står cursoren ved cellerne med nr 1 (se figur). Maskinen skriver aldrig på de bånd, som indeholder input. TM's arbejde illustreres bedst ved et par eksempler:

### Eksempel 1.8

**Successor-funktionen:** TM skal bruge 2 bånd og 2 tilstande.  $E = \{e_i, e_f\}$

$$\begin{aligned} M(d, d, e_i) &= (d, d, e_i, +1) \\ M(|, b, e_i) &= (|, |, e_i, +1) \\ M(b, b, e_i) &= (b, |, e_f, 0) \end{aligned}$$

Inputtet  $x$  står på øverste bånd når maskinen starter, dvs. celle nr 2 til og med nr  $x+1$  indeholder en streg. Maskinen sætter streger på bånd 2 indtil den når celle  $x+1$ , hvor den sætter en streg og stopper. Nu står input  $x$  på bånd 1 og resultatet  $x+1$  på bånd 2.

**Projektionerne**  $P_k^i(x_1, \dots, x_k) = x_i$

Lad  $i, k$  være givet,  $i \leq k$ . TM skal have  $k + 1$  bånd og 2 tilstande.

$$\begin{aligned} M(d, \dots, d, e_i) &= (d, \dots, d, e_i, +1) \\ M(s_1, \dots, s_k, b, e_i) &= (s_1, \dots, s_k, |, e_i, +1), \text{ for } s_i = | \\ M(s_1, \dots, s_k, b, e_i) &= (s_1, \dots, s_k, b, e_f, 0), \text{ for } s_i = b \end{aligned}$$

Denne maskine kopierer simpelthen indholdet af det  $i$ 'te bånd til det nederste bånd.

**De konstante funktioner**  $f(x_1, \dots, x_p) = k$  for  $p, k \in \mathbb{N}$  kan beregnes af en TM med  $p + 1$  bånd og  $k + 2$  tilstande  $\{e_i, e_1, \dots, e_k, e_f\}$

$$\begin{aligned} M(d, \dots, d, e_i) &= (d, \dots, d, e_1, +1) \\ M(s_1, \dots, s_p, b, e_n) &= (s_1, \dots, s_p, |, e_{n+1}, +1) \\ &\text{for alle } s_1, \dots, s_p \text{ og } 1 \leq n \leq k - 1 \\ M(s_1, \dots, s_p, b, e_k) &= (s_1, \dots, s_p, |, e_f, 0) \\ &\text{for alle } s_1, \dots, s_p \end{aligned}$$

Man siger at TM beregner en funktion  $f : \mathbb{N}^p \rightarrow \mathbb{N}$ , hvis TM har  $p+1$  bånd og hvis der for  $(x_1, \dots, x_p) \in \text{dom}(f)$  gælder, at TM når en slut-tilstand med  $(x_1, \dots, x_p)$  på de  $p$  første bånd og  $f(x_1, \dots, x_p)$  på det sidste. Resten af båndene skal være tomme. Desuden skal der gælde, at for  $(x_1, \dots, x_p) \notin \text{dom}(f)$  standser maskinen ikke.  $f$  kaldes da *Turing-beregnelig*

**Sætning 1.9** *En funktion er Turing-beregnelig hvis og kun hvis den er rekursiv.*

**Bevis:**

For at vise at enhver rekursiv funktion er T-beregnelig, er det tilstrækkeligt at vise, at det gælder for projektionerne, de konstante funktioner og successor-funktionen (hvilket allerede er gjort i eksempel 1.8) samt at mængden af T-beregnelige funktioner er stabil mht. rekursion, substitution og  $\mu$ -operatoren.

Først **rekursionen**:

Lad  $f : \mathbb{N}^{p+1} \rightarrow \mathbb{N}$  være givet ved

$$\begin{aligned} f(x_1, \dots, x_p, 0) &= g(x_1, \dots, x_p) \\ f(x_1, \dots, x_p, y + 1) &= h(x_1, \dots, x_p, y, f(x_1, \dots, x_p, y)) \end{aligned}$$

hvor  $g$  og  $h$  er partielle funktioner, som beregnes med maskinerne  $M$  hhv.  $M'$ . Antag, at  $M$  har  $p+1+k$  bånd og  $M'$   $p+3+k'$ , samt at  $E$  er mængden af tilstande for  $M$  og  $E'$  mængden af tilstande for  $M'$ . Idet man altid kan give en tilstand et nyt navn, kan det antages, at  $E \cap E' = \emptyset$ . Maskinen  $N$ , som skal beregne  $f$  skal bruge  $p+4+k+k'$  bånd og mængden af tilstande er  $E \cup E' \cup \{e_0, \dots, e_7\}$ , hvor  $e_i$ 'erne er tilstande som ikke allerede findes i  $E \cup E'$ . Til at begynde med står  $x_1, \dots, x_{p+1}$  på de første  $p + 1$  bånd og når  $N$  standser (hvis den standser) skal  $f(x_1, \dots, x_{p+1})$  stå på bånd nr.  $p + 2$ . Ideen er at lade  $N$  beregne  $f(x_1, \dots, x_p, 1), f(x_1, \dots, x_p, 2), \dots, f(x_1, \dots, x_p, x_{p+1})$ , mens et af båndene ( $p+2$ ) bruges som tæller, der holder styr på, hvornår maskinen er nået til  $f(x_1, \dots, x_p, x_{p+1})$ .  $N$  starter som  $M$  på båndene  $1, \dots, p, p + 4$  (samt de  $k$  bånd  $M$  bruger til at arbejde på). Hvis  $M$  standser, står  $g(x_1, \dots, x_p)$  på bånd  $p + 4$  og  $N$  skifter til tilstand  $e_0$ . I denne tilstand kopieres indholdet af  $p + 4$  til  $p + 3$  samtidig med at  $p + 4$  slettes. Tilstanden  $e_1$  sammenligner  $p + 2$  med  $p + 1$ , dvs. sammenligner  $x_{p+1}$  med tælleren. Hvis indholdet er ens skiftes til  $e_6$  som sørger for at flytte indholdet af  $p + 3$  til  $p + 2$ , som jo var output-bånd for  $N$ , hvorefter den skifter til  $e_7$  som er slut-tilstanden for  $N$ . Ellers skiftes til  $e_2$ , som har til opgave at lægge én til tælleren, altså sætte en streg på  $p + 2$ . Nu skiftes til begyndelses-tilstanden for  $M'$ .  $M'$  bruger båndene  $1, \dots, p, p + 2, p + 3$  som input og skriver resultatet på bånd  $p + 4$ . Hvis  $M'$

standser skiftes til til  $e_0$  igen. Tilstandene  $e_3, e_4$ , og  $e_5$  har alle til opgave at flytte cursoren til venstre inden der skiftes til tilstandene hhv.  $e_1, e_2$  og  $e_6$ . Efter denne grundige beskrivelse, er det ingen sag at opskrive transitions-tabellen for  $N$ , så det vil jeg ikke bruge plads på.

**substitution:**

Lad  $f_1, \dots, f_n : \mathbb{N}^p \rightarrow \mathbb{N}$  og  $g : \mathbb{N}^n \rightarrow \mathbb{N}$  være T-beregnelige funktioner. Det drejer sig om at konstruere en Turing-maskine  $N$ , som beregner  $h = g(f_1, \dots, f_n)$ . Lad  $M_i$  være maskinen, som beregner  $f_i$  for  $i = 1, \dots, n$  og  $M$  maskinen, som beregner  $g$ . Antag for hvert  $i$ , at  $M_i$  har  $p_i$  bånd, hvor  $p_i \geq p + 1$  og at mængden af tilstande er  $E_i$ . Maskinen  $M$  har  $m$  bånd og  $E$  betegner mængden af tilstande. Som før antages det, at disse mængder er disjunkte.  $N$  har  $p' = p + \sum_{i=1}^n (p_i - p) + (m - n)$  bånd og mængden af tilstande er  $E \cup (\cup_{i=1}^n E_i) \cup \{e_N, e_f\}$ .

$N$  starter med at arbejde som  $M_1$  dog uden at bruge bånd  $p+1$ , hvor det endelige resultat skal stå. Resultatet  $f(x_1, \dots, x_p)$  skrives i stedet på et andet bånd  $B_1$ , hvis  $M_1$  vel at mærke stopper, og slut-tilstanden for  $M_1$  skal bringe cursoren hen til starten af båndene for derefter at skifte til begyndelses-tilstanden for  $M_2$ . Resultatet af  $M_2$ 's beregninger skrives på af bånd  $B_2$  (som er forskelligt fra bånd  $p+1$  og fra  $B_1$ ) og så fremdeles.  $M_n$ 's slut-tilstand bringer cursoren til start og skifter til  $M$ 's begyndelses-tilstand.  $N$  arbejder nu som  $M$ , men med båndene  $B_1, \dots, B_n$  som input og skriver resultatet  $h(x_1, \dots, x_p)$  på bånd nr.  $p+1$ . Derefter bringer slut-tilstanden for  $M$  cursoren tilbage til start og  $e_N$  sletter indholdet af  $B_1, B_2, \dots, B_n$  hvorefter  $N$  stopper i tilstanden  $e_f$ . Inputtet  $x_1, \dots, x_p$  står nu på båndene  $1, \dots, p$  og output  $h(x_1, \dots, x_p)$  på bånd  $p+1$ . Resten af båndene er tomme.

**$\mu$ -operatoren:**

Maskinen  $N$ , som beregner  $g(x_1, \dots, x_p) = \mu y (f(x_1, \dots, x_p, y) = 0)$ , hvor  $f$  er en funktion, som beregnes af maskinen  $M$ , konstrueres tilsvarende:

$N$  har  $p + 2$  bånd og mængden af tilstande er tilstandene for  $M$  forenet med  $\{e_0, \dots, e_5\}$  nye.  $N$  starter med at arbejde som  $M$  med  $x_1, \dots, x_p, 0$  som input. Hvis  $f$  er defineret for  $x_1, \dots, x_p, 0$  vil  $M$  stoppe og output stå på bånd  $p + 2$ .  $M$ 's slut-tilstand bringer cursoren til start og skifter til  $e_0$ .  $e_0$  checker, om der står noget på bånd  $p + 2$ . Hvis det første  $e_0$  møder er et  $b$  går  $N$  i slut-tilstanden  $e_5$ . Ellers skiftes til  $e_1$ , som skriver en streg på  $p + 1$  (således at input for  $M$  nu er  $x_1, \dots, x_p, 1$ ) og går over i  $e_2$ , som bringer cursoren til start.  $e_3$  sletter indholdet af  $p + 2$  og  $e_4$  har også til opgave at bringe cursoren til start.  $N$  bliver ved til den har fundet et  $y$  så  $f(x_1, \dots, x_p, y) = 0$ , hvis det eksisterer, ellers stopper maskinen ikke.

For at vise den anden implikation, altså at enhver funktion som er T-beregnelig er rekursiv, antages det, at  $M$  er en vilkårlig TM, som beregner en partiel funktion  $f : \mathbb{N}^p \rightarrow \mathbb{N}$ . Det skal vises, at  $f$  er rekursiv.  $M$  er givet ved:

- antallet af bånd:  $n$
- antallet af tilstande  $m + 1$ . Her antages det at tilstandene nummereres fra 0 til  $m$  og at 0 betegner begyndelsestilstanden, mens 1 betegner sluttilstanden.
- Transitionstabellen  $M : S^n \times E \rightarrow S^n \times E \times \{-1, 0, 1\}$

Lad tallene 0, 1 og 2 stå for henholdsvis b, d og |. Skriv indholdet af cellerne til tiden  $t$  op i en liste  $K(t) = (s_0, s_1, \dots, s_i, \dots)$ , hvor  $s_i \in \{0, 1, 2\}$  for alle  $i$ . Start med celle 1 bånd 1 derefter celle 1 bånd 2 indtil celle 1 bånd  $n$  dernæst cellerne med nr. 2 osv. Listen har et endeligt antal elementer forskellige fra nul, thi til tiden  $t = 0$  står input, som er endeligt på båndene og maskinen kan højst tilføje et symbol per tidsenhed. Bemærk, at  $s_{n(u-1)+(v-1)}$  svarer til symbolet i celle  $u$  bånd  $v \leq n$  (hvor  $n$  var antallet af bånd). Listen kodes på følgende måde:

$$\Gamma(K) = \sum_{i \geq 0} s_i 3^i$$

Det er klart, at  $\Gamma$  er injektiv da  $s_i \in \{0, 1, 2\}$  for alle  $i$ . Man genfinder tallet som svarer til symbolet i celle  $u$  bånd  $v$  ved:

$$r(q(\Gamma(K), 3^{n(u-1)+(v-1)}), 3)$$

hvor  $r(x, y)$  er resten ved heltalsdivision af  $x$  med  $y$  og  $q(x, y)$  kvotienten. Antag nemlig, at  $n(u - 1) + (v - 1) = k$ , da er

$$\Gamma(K) = s_0 + s_1\mathfrak{3} + \cdots + s_{k-1}\mathfrak{3}^{k-1} + s_k\mathfrak{3}^k + s_{k+1}\mathfrak{3}^{k+1} + \cdots$$

og

$$\sum_{i=0}^{k-1} s_i\mathfrak{3}^i < \mathfrak{3}^k$$

så

$$\begin{aligned} q(\Gamma(K), \mathfrak{3}^k) &= s_k + s_{k+1}\mathfrak{3} + s_{k+2}\mathfrak{3}^2 + \cdots \\ &= s_k + \mathfrak{3}(s_{k+1} + s_{k+2}\mathfrak{3} + \cdots) \\ &\equiv s_k \pmod{\mathfrak{3}} \end{aligned}$$

det vil sige  $r(q(\Gamma(K), \mathfrak{3}^k), \mathfrak{3}) = s_k$  som ønsket.

Maskinens *situation* til tiden  $t$  er  $S(t) = (e, k, K(t))$ , hvor  $e \in \{0, \dots, m\}$  er tilstanden og  $k$  nummeret på de celler cursoren befinder sig ved.

$$\Gamma(S) = \alpha_3(e, k, \Gamma(K))$$

Funktionen  $Sit(t, x_1, \dots, x_p) = \Gamma(S(t))$  er primitiv rekursiv<sup>1</sup>.  $Sit(t, x_1, \dots, x_p)$  er situation til tiden  $t$  for maskinen startet på input  $x_1, \dots, x_p$ . Man kan nu definere en rekursiv funktion, som finder beregningstiden for et givet input  $x_1, \dots, x_p$ .

$$T(x_1, \dots, x_p) = \mu t (\beta_3^1(Sit(t, x_1, \dots, x_p)) = 1)$$

altså  $T$  finder det mindste  $t$  således at  $M$  med inputtet  $x_1, \dots, x_p$  befinder sig i sluttstanden. Hvis  $f(x_1, \dots, x_p)$  ikke er defineret, standser  $M$  ikke og  $T$  er da heller ikke defineret. Hvis  $f(x_1, \dots, x_p)$  er defineret, vil resultatet stå på bånd  $p + 1$  til tiden  $t$ . Det drejer sig altså om at tælle antallet af streger på  $p + 1$  til dette tidspunkt. Betragt dertil

$$\alpha(x) = \mu y (r(q(\beta_3^3(x), \mathfrak{3}^{n(y+1)+p}), \mathfrak{3}) = 0)$$

Hvis  $x = Sit(t, x_1, \dots, x_p)$  så er  $\beta_3^3(x) = \Gamma(K(t))$  og  $\alpha$  finder da det mindste  $y$  således at symbolet i celle  $y + 2$ , bånd  $p + 1$  er et b. Idet første symbol på et bånd altid er d, svarer  $\alpha(x)$  præcis til antallet af streger på bånd  $p + 1$ . Man finder nu

$$f(x_1, \dots, x_p) = \alpha(Sit(T(x_1, \dots, x_p), x_1, \dots, x_p)).$$

Da  $f$  er sammensat af rekursive funktioner, ses det som ønsket, at  $f$  selv er rekursiv.

□

En TM er som bekendt givet ved antallet af bånd  $n$ , antallet af tilstande  $m + 1$  og transitionstabellen. Man kan afbilde transitionstabellen ind i  $\mathbb{N}$  på følgende måde: For  $(s_1, \dots, s_n, e) \in S^n \times E$  sæt

$$\begin{aligned} r_1 &= \alpha_2(\Gamma(s_1, \dots, s_n), e) \\ r_2 &= \alpha_3(\Gamma(t_1, \dots, t_n), e', \varepsilon + 1) \text{ hvor } \varepsilon \in \{-1, 0, 1\} \text{ og} \\ t_1, \dots, t_n, e' &= M(s_1, \dots, s_n, e) \\ n(s_1, \dots, s_n, e) &= (\pi(r_1))^{r_2}, \text{ hvor } \pi(i) \text{ er det } i + 1 \text{'te primtal} \end{aligned}$$

Koden for transitionstabellen er da

$$u = \prod_{(s_1, \dots, s_n, e) \in S^n \times E} n((s_1, \dots, s_n, e))$$

**Definition 1.10** *Et indeks for en TM er tallet  $\alpha_3(n, m + 1, u)$ .*

<sup>1</sup>Se [Las94] p 35 for bevis

## Den universelle Turingmaskine

-er en TM, som for et naturligt tal  $p$ , kan beregne enhver rekursiv funktion af  $p$  variable. Man ved allerede, at til enhver rekursiv funktion findes en TM, som beregner denne. Ideen er, at knytte et indeks til hver TM og derefter vise, at den partielle funktion  $\varphi : \mathbb{N}^{p+1} \rightarrow \mathbb{N}$ , som er defineret ved:

$$\varphi^p(i, x_1, \dots, x_p) = \begin{cases} \text{ikke defineret} & \text{hvis } i \text{ ikke er indeks for en TM med mindst} \\ & p + 1 \text{ bånd} \\ \text{indholdet af det } p + 1\text{'te bånd} & \text{hvis TM med indeks } i \text{ standser} \\ & \text{på input } x_1, \dots, x_p \\ \text{ikke defineret} & \text{hvis TM med indeks } i \text{ ikke standser} \\ & \text{på input } x_1, \dots, x_p \end{cases}$$

er rekursiv. Dette betyder nemlig, at der findes en TM, som beregner  $\varphi^p(i, x_1, \dots, x_p)$  dvs. givet et  $i \in \mathbb{N}$ , opfører den sig som maskinen med indeks  $i$ , hvis  $i$  altså er et indeks for en maskine som tager  $p$  variable. Afbildning fra mængden af TM ind i  $\mathbb{N}$  er ikke surjektiv, så der er også tal i  $\mathbb{N}$  som ikke er indeks for nogensomhelst maskine.

**Sætning 1.11** For hvert  $p > 0$ , er  $\varphi^p$  rekursiv og hvis  $f$  er en rekursiv funktion af  $p$  variable, findes et naturligt tal  $i$  således at  $f = \lambda x_1, \dots, x_p. \varphi^p(i, x_1, \dots, x_p) = \varphi_i^p$

Hvis  $f$  er en rekursiv funktion af  $p$  variable, så findes der i følge sætning 1.9 en TM, som beregner  $f$ . Denne TM har et indeks  $i_0$ , så per definition af  $\varphi$ , er  $f = \varphi_{i_0}^p$ , og  $i_0$  kaldes da indeks for  $f$ . Man for brug for følgende:

$$I_p = \{i; i \text{ er indeks for en TM med mindst } p + 1 \text{ bånd}\}$$

$$ST^p(i, t, x_1, \dots, x_p) = \begin{cases} \text{hvis } i \in I_p : & \Gamma(S(t)) \text{ dvs} \\ & Sit(t, x_1, \dots, x_p) \text{ for maskinen med indeks } i \\ \text{ellers:} & 0 \end{cases}$$

$ST^p$  er primitiv rekursiv<sup>2</sup>. På samme måde som tidligere defineres en funktion, som finder beregningstiden:

$$T^p(i, x_1, \dots, x_p) = \mu t(\beta_3^1(ST^p(i, t, x_1, \dots, x_p)) = 1)$$

desuden defineres mængderne

$$B^p = \{(i, t, x_1, \dots, x_p); \beta_3^1(ST^p(i, t, x_1, \dots, x_p)) = 1\}$$

$$C^p = \{(i, y, t, x_1, \dots, x_p); i \in I_p, (i, t, x_1, \dots, x_p) \in B^p, y = \alpha(ST^p(i, t, x_1, \dots, x_p))\}$$

Det ses at  $B^p$  og  $C^p$  er primitive rekursive. At  $y = \alpha(ST^p(i, t, x_1, \dots, x_p))$  betyder at maskinen med indeks  $i$  startet på  $x_1, \dots, x_p$  har  $y$  streger på bånd  $p + 1$  til tiden  $t$ . Det følger nu, at

$$\varphi^p(i, x_1, \dots, x_p) = \mu y((i, y, T^p(i, x_1, \dots, x_p), x_1, \dots, x_p) \in C^p)$$

□

### Church's tese:

En talteoretisk funktion er beregnelig i intuitiv forstand hvis og kun hvis den er rekursiv.

Church's tese kan selvfølgelig ikke bevises, da man ikke kan give nogen præcis definition af det at være "beregnelig i intuitiv forstand", på den anden side findes der ingen modeksempler på Church's tese. At en funktion er beregnelig i intuitiv forstand er det samme som at der findes en opskrift eller en algoritme til at beregne den. Algoritme er også et intuitivt begreb, og Turingmaskinen et forsøg på at indfange det. De Turing-beregnelige funktioner er netop de rekursive, så Church's

<sup>2</sup>se [Las94] p.38 for bevis

tese kan også formuleres: *En talteoretisk funktion er beregnelig i intuitiv forstand hvis og kun hvis den er Turing-beregnelig hvis og kun hvis der findes en algoritme til at beregne den.* Turingmaskinen er langt fra den eneste definition af begrebet algoritme, men samtlige definitioner har vist sig at være ækvivalente<sup>3</sup> forstået på den måde, at de beregner de samme funktioner nemlig de rekursive, hvilket understøtter Church's tese.

---

<sup>3</sup> [Men97] p.345

## Chapter 2

# Standsningsproblemet

Standsningsproblemet for en TM  $M$  drejer sig om at afgøre, hvorvidt  $M$  standser når maskinen startes på et input  $x$ .

Man siger, at et problem er afgørligt hvis der findes en algoritme, som løser det. Under Church's tese er det det samme som at sige, at der findes en rekursiv funktion eller en TM som løser problemet. Hvis det ikke er tilfældet, siges problemet at være uafgørligt. Der findes både Turingmaskiner med afgørlige og med uafgørlige standsningsproblemer.

### Eksempel 2.1

Betragt en TM  $M$  med 2 bånd og 3 tilstande og transitionstabellen

$$\begin{aligned}M(d, d, e_i) &= (d, d, e_i, +1) \\M(|, b, e_i) &= (|, b, e_1, -1) \\M(b, b, e_i) &= (b, b, e_f, 0) \\M(b, |, e_i) &= (b, |, e_1, -1) \\M(s_1, s_2, e_1) &= (s_1, s_2, e_1, +1) \text{ hvor } s_1, s_2 \in \{d, b, |\}\end{aligned}$$

$M$  er et simpelt eksempel på en maskine med et afgørligt standsningsproblem.  $M$  standser hvis og kun hvis  $x = 0$ .

**Definition 2.2** Lad  $A \subseteq \mathbb{N}^p$ , man siger at mængden  $A$  er rekursivt numerabel (forkortes r.n.) hvis den er domænet af en rekursiv funktion.

Betragt den rekursive funktion  $\varphi_i^p$ , som er defineret under afsnittet om den universelle Turing-maskine.

Man noterer  $\text{dom}\varphi_i^p = W_i^p$ . Bemærk, at enhver rekursiv mængde er rekursivt numerabel. Thi hvis  $A$  er rekursiv, så er  $1_A$  rekursiv. Og funktionen  $f(x) = \mu y(y + 1 = x)$  er rekursiv og defineret for alle  $x \neq 0$ .  $f \circ 1_A$  er rekursiv og domænet er netop  $A$ , hvilket viser, at  $A$  er r.n.

**Lemma 2.3**  $A \subseteq \mathbb{N}^p$  er rekursiv hvis og kun hvis  $A$  og  $\bar{A}$  (hvor  $\bar{A} = \mathbb{N}^p \setminus A$ ) begge er rekursivt numerable.

Hvis  $A$  er rekursiv, så er  $\bar{A}$  det også, idet  $1_{\bar{A}} = 1 - 1_A$ , og de er da begge r.n. På den anden side, hvis både  $A$  og  $\bar{A}$  er r.n. findes indeks  $j, k$  så  $A = W_j^p$  og  $\bar{A} = W_k^p$ . Man ved desuden at

$$B^p = \{(i, t, x_1, \dots, x_p); \beta_3^1(ST^p(i, t, x_1, \dots, x_p)) = 1\}$$

er rekursiv,

$$B^p(i) = \{(t, x_1, \dots, x_p); (i, t, x_1, \dots, x_p) \in B^p\}$$

er det derfor også. Lad

$$h(x_1, \dots, x_p) = \mu t((t, x_1, \dots, x_p) \in B^p(j) \cup B^p(k))$$

h er rekursiv og total.  $B^p(j)$  er netop de  $(t, x_1, \dots, x_p)$  sådan at maskinen med indeks  $j$  standser til tiden  $t$  på input  $x_1, \dots, x_p$ . Det vil sige, hvis der findes et  $t$  så  $(t, x_1, \dots, x_p) \in B^p(j)$  så er

$$x_1, \dots, x_p \in \text{dom}\varphi_j^p = A$$

. Altså  $(x_1, \dots, x_p) \in A$  hvis og kun hvis  $(h(x_1, \dots, x_p), x_1, \dots, x_p) \in B^p(j)$ . Da  $B^p(j)$  er rekursiv, er  $A$  det også.  $\square$

**Sætning 2.4 (s-m-n)** For ethvert par  $m, n \in \mathbb{N}$ , findes der en primitiv rekursiv funktion  $s_n^m$  af  $n+1$  variable således at man for alle  $i, x_1, \dots, x_n, y_1, \dots, y_m$  har

$$\varphi^{n+m}(i, x_1, \dots, x_n, y_1, \dots, y_m) = \varphi^m(s_n^m(i, x_1, \dots, x_n), y_1, \dots, y_m)$$

**Bevis:**

Hvis man fastholder de  $n$  første variable i funktionen  $\varphi_i^{n+m}$  fås en funktion

$$g = \lambda y_1, \dots, y_m. \varphi_i^{n+m}(x_1, \dots, x_n, y_1, \dots, y_m)$$

som også er rekursiv.  $g$  har derfor et indeks, og resten af beviset drejer sig om at vise, at dette indeks kan beregnes ved hjælp af en primitiv rekursiv funktion  $s_n^m(i, x_1, \dots, x_n)$ , men det vil jeg ikke gå i detaljer med.  $\square$

**Sætning 2.5 (fixpunktssætningen) Bevis:**

Hvis  $h(x)$  er en total rekursiv funktion og  $p \in \mathbb{N}$  så findes der et  $n \in \mathbb{N}$  så  $\varphi_n^p = \varphi_{h(n)}^p$ .

$\varphi^p(h(s_1^p(i, i)), x_1, \dots, x_p)$  er per substitution en rekursiv funktion af  $p+1$  variable. lad  $d$  være et indeks for denne, så er  $\varphi^p(h(s_1^p(i, i)), x_1, \dots, x_p) = \varphi_d^{p+1}(i, x_1, \dots, x_p) = \varphi^{p+1}(d, i, x_1, \dots, x_p)$ . I følge s-m-n sætningen er da  $\varphi^{p+1}(d, i, x_1, \dots, x_p) = \varphi^p(s_1^p(d, i), x_1, \dots, x_p)$ , lad  $n = s_1^p(d, d)$  så fås  $\varphi_n^p = \varphi_{h(n)}^p$  som ønsket.  $\square$

**Korollar 2.6 (Rice's sætning)** Lad  $\mathcal{F} \neq \emptyset$  være en ægte delmængde af de rekursive funktioner af en variabel, så er mængden  $A = \{u, \varphi_u^1 \in \mathcal{F}\}$  ikke rekursiv.

**Bevis:**

Antag, at  $A$  er rekursiv. Der findes per definition  $u_1$  og  $u_2$  således at  $u_1 \in A$  og  $u_2 \notin A$ . Definer

$$h(x) = \begin{cases} u_1 & \text{hvis } x \notin A \\ u_2 & \text{hvis } x \in A \end{cases}$$

$h(x) = u_1(1 - 1_A(x)) + u_2 1_A(x)$  så da  $A$  var rekursiv, er  $h$  det også. I følge fixpunktssætningen findes der et  $n$  så  $\varphi_n^1 = \varphi_{h(n)}^1$ , det vil sige

$$\begin{aligned} n \in A &\Leftrightarrow h(n) = u_2 \\ &\Leftrightarrow h(n) \notin A \\ &\Leftrightarrow \varphi_{h(n)}^1 = \varphi_n^1 \notin \mathcal{F} \\ &\Leftrightarrow n \notin A \end{aligned}$$

hvilket er en modstrid,  $A$  er derfor ikke rekursiv.  $\square$

**Lemma 2.7** Selvstandsningsproblemet er uafgørligt.

**Bevis:**

Selvstandsningsproblemet handler om at afgøre, hvorvidt en TM med indeks  $x$  standser på input  $x$ . At vise at det er uafgørligt kommer ud på at vise, at mængden  $K = \{x, \varphi_x^1(x) \downarrow\}$  ikke er rekursiv. Definer derfor  $\mathcal{F} = \{\varphi_x^1, x \in W_x^1\}$   $\mathcal{F} \neq \emptyset$  da  $Id \in \mathcal{F}$  og funktionen

$$f(x) = \begin{cases} 0 & \text{hvis } x = 0 \\ \uparrow & \text{ellers} \end{cases}$$

er en rekursiv funktion, som ikke ligger i  $\mathcal{F}$  da  $f$ 's indeks ellers skulle være 0, hvilket ikke kan lade sig gøre, idet men nemt ser, at der ikke findes en TM med indeks 0 (en sådan ville have 0 bånd). Betingelserne i Rice's sætning er opfyldt, så mængden  $A = \{x; \varphi_x^1 \in \mathcal{F}\}$  er ikke rekursiv.  $A = \{x; x \in W_x^1\} = \{x; \varphi_x^1(x) \downarrow\} = K \square$

**Sætning 2.8** *Det specielle standsningsproblem er uafgørligt.*

**Bevis:**

Givet et indeks  $i$  og et input  $x$  at afgøre om  $\varphi^1(i, x)$  er defineret, eller med andre ord om TM med indeks  $i$  standser på  $x$ , kaldes det specielle standsningsproblem. Det skal vises, at  $W = \{(i, x); \varphi^1(i, x) \downarrow\} = \{(i, x); x \in W_x^1\}$  ikke er rekursiv. Betragt mængden  $B = \{(x, x); x \in \mathbb{N}\}$ .  $B$  er rekursiv da  $1_B(x, y) = 1 - |x - y|$ .  $K' = \{(x, x); x \in K\}$  er til gengæld ikke rekursiv i følge ovenstående lemma, idet  $1_{K'}(x, x) = 1_K(x)$ . Det ses at  $K' = B \cap W$ , så hvis  $W$  var rekursiv ville  $K'$  også være det. Konklusion:  $W$  er ikke rekursiv.  $\square$

**bemærkning:**  $K$  og  $W$  er rekursivt numerable:  $K$  er domænet af den rekursive funktion  $g(x) = \varphi^1(x, x)$ , og  $W$  er domænet af  $h(i, x) = \mu t((i, t, x) \in B^1)$  som ligeledes er rekursiv.

At det specielle standsningsproblem er uafgørligt betyder (under Church's tese) at der ikke nogen algoritme som kan løse det. Med andre ord findes der ingen algoritme (eller TM) som givet et vilkårligt computerprogram og et vilkårligt input til dette program, kan afgøre hvorvidt programmet vil standse på dette input.

## 2.1 Reduktioner

**Definition 2.9** *Lad  $A$  og  $B$  være delmængder af  $\mathbb{N}$ . Men siger, at  $A$  kan reduceres til  $B$ , og man skriver  $A \leq B$ , hvis der findes en total, rekursiv funktion  $f$  således at*

$$x \in A \Leftrightarrow f(x) \in B \text{ altså hvis } f^{-1}(B) = A$$

$B$  er komplet hvis  $B$  er r.n. og hvis alle mængder, som er r.n. kan reduceres til  $B$ . Hvis  $f$  også er injektiv, skriver man  $A \leq_1 B$

**Sætning 2.10** 1.  $\leq$  er reflektiv og transitiv

2. Hvis  $A \leq B$  og  $B$  er r.n. henholdsvis rekursiv, så er  $A$  også r.n henholdsvis rekursiv.

3.  $K = \{x; \varphi^1(x, x) \downarrow\}$  er komplet.

4. En mængde er r.n. hvis og kun hvis den kan reduceres til  $K$ .

**Bevis:**

1.  $A \leq A$ : Lad  $f = Id$  da er  $f$  total og rekursiv og  $x \in A \Leftrightarrow f(x) \in A$   
Antag  $A \leq B$  via  $g$  og  $B \leq C$  via  $h$  så er  $x \in A \Leftrightarrow g(x) \in B \Leftrightarrow h(g(x)) \in C$  altså  $A \leq C$  via  $h \circ g$ .

2. Antag først at  $A \leq B$  via en rekursiv, total funktion  $f$  og  $B$  r.n. Da  $B$  er r.n. findes der et  $i \in \mathbb{N}$  så  $\text{dom} \varphi^1(i, x) = W_i^1 = B$  dvs.  $x \in A \Leftrightarrow f(x) \in \text{dom} \varphi_i^1 \Leftrightarrow x \in \text{dom}(\varphi_i^1 \circ f)$ .  $\varphi_i^1 \circ f$  er en rekursiv funktion og  $A$  er domænet for denne, ergo er  $A$  r.n.

Antag nu at  $B$  er rekursiv.  $x \in A \Leftrightarrow f(x) \in B \Leftrightarrow 1_B(f(x)) = 1$ , så

$$1_A = \begin{cases} 1 & \text{hvis } 1_B \circ f(x) = 1 \\ 0 & \text{hvis } 1_B \circ f(x) = 0 \end{cases}$$

altså  $1_A = 1_B \circ f$  hvilket viser, at  $A$  er rekursiv.

3. Det er allerede blevet bemærket, at  $K$  er r.n. Lad  $A$  være en vilkårlig rekursivt numerabel mængde  $A = \text{dom}\varphi_i^1$ . Definer funktionen

$$\psi(x, y) = \begin{cases} 0 & \text{hvis } x \in A \\ \uparrow & \text{ellers} \end{cases}$$

$\psi$  er rekursiv, fordi  $x \in A \Leftrightarrow \varphi_i^1 = 0$  så faktisk er  $\psi(x, y) = \varphi_i^1(x) - \varphi_i^1(x)$  (hvis  $\varphi_i^1(x)$  ikke er defineret er  $\psi(x, y)$  det heller ikke). Da  $\psi$  er rekursiv findes der et  $j_0 \in \mathbb{N}$  så  $\psi(x, y) = \varphi_{j_0}^2(x, y) = \varphi^2(j_0, x, y) = \varphi^1(s_1^1(j_0, x), y)$  i følge s-m-n sætningen. Sæt  $h(x) = s_1^1(j_0, x)$  så er  $\psi(x, y) = \varphi_{h(x)}^1(y)$  Man finder nu, at

$x \in A \Rightarrow \psi(x, y) = 0$  for alle  $y \Rightarrow \psi(x, h(x)) = 0 \Rightarrow \varphi_{h(x)}^1(h(x)) \downarrow \Rightarrow h(x) \in K$  og på den anden side

$h(x) \in K \Rightarrow \varphi_{h(x)}^1(h(x)) \downarrow \Rightarrow \psi(x, h(x)) \downarrow \Rightarrow x \in A$  Altså  $A \leq K$  via  $h$  som ønsket.

4. Hvis  $A \leq K$  så er  $A$  r.n. i følge punkt 2. Hvis  $A$  er r.n. så følger det af punkt 3, at  $A \leq K$ .  
□

**Definition 2.11 (Det aritmetiske hierarki)** lad  $R(x_1, \dots, x_n, y_1, \dots, y_m)$  være en rekursiv relation. Betragt følgende opstilling:

$$\begin{array}{ll} R(x_1, \dots, x_n) & R(x_1, \dots, x_n) \\ \exists y_1 R(x_1, \dots, x_n, y_1) & \forall y_1 R(x_1, \dots, x_n, y_1) \\ \exists y_1 \forall y_2 R(x_1, \dots, x_n, y_1, y_2) & \forall y_1 \exists y_2 R(x_1, \dots, x_n, y_1, y_2) \\ \exists y_1 \forall y_2 \exists y_3 R(x_1, \dots, x_n, y_1, y_2, y_3) & \forall y_1 \exists y_2 \forall y_3 R(x_1, \dots, x_n, y_1, y_2, y_3) \\ \vdots & \vdots \end{array}$$

Lad  $\Sigma_0^n = \Pi_0^n =$  mængden af alle relationer af  $n$  variable. For  $k > 0$  lad  $\Sigma_k^n$  være mængden af alle relationer af  $n$  variable som kan udtrykkes på formen

$$\exists y_1 \forall y_2 \cdots Q y_k R(x_1, \dots, x_n, y_1, \dots, y_k)$$

bestående af  $k$  alternerende kvantifikatorer efterfulgt af en rekursiv relation.  $Q = \exists$  eller  $Q = \forall$  afhængigt af om  $k$  er lige eller ulige. Lad  $\Pi_k^n$  være den tilsvarende mængde, men hvor rækken af kvantifikatorer starter med  $\forall$ . Man kan opskrive mængderne i et hierarki, hvor hver række af mængder er indeholdt de efterfølgende rækker af mængder.

$$\begin{array}{ll} \Sigma_0^n & = \Pi_0^n \\ \Sigma_1^n & \Pi_1^n \\ \Sigma_2^n & \Pi_2^n \\ \vdots & \vdots \end{array}$$

**Sætning 2.12** Lad  $A \subseteq \mathbb{N}^n$  og lad  $n, k \in \mathbb{N}$  da gælder

1.  $A \in \Sigma_1^n$  hvis og kun hvis  $A$  er r.n.
2.  $A \in \Pi_k^n$  hvis og kun hvis  $\bar{A} \in \Sigma_k^n$
3.  $A \in \Pi_1^n$  hvis og kun hvis  $\bar{A}$  er r.n.
4.  $\Sigma_k^n$  og  $\Pi_k^n$  er stabile mht. forening og fællesmængde-dannelse.
5. Hvis  $Q_1 y_1 Q_2 y_2 \cdots Q_k y_k R(\bar{x}, \bar{y}) \in \Sigma_k^n$  eller  $\Pi_k^n$  så gælder det samme for relationerne

$$\forall x_i < a Q_1 y_1 Q_2 y_2 \cdots Q_k y_k R(\bar{x}, \bar{y})$$

og

$$\exists x_i < a Q_1 y_1 Q_2 y_2 \cdots Q_k y_k R(\bar{x}, \bar{y})$$

hvor  $a \in \mathbb{N}$  og  $1 \leq i \leq n$ .

**Bevis:**

1.  $A \in \Sigma_1^n$  hvis og kun hvis der findes en rekursiv relation  $R$  sådan at

$$(x_1, \dots, x_n) \in A \Leftrightarrow \exists y R(x_1, \dots, x_n, y).$$

$R(x_1, \dots, x_n, y)$  definerer en rekursiv mængde  $B$ . Lad  $i$  være indekset for en TM, som beregner  $B$ , så er  $(x_1, \dots, x_n, y) \in B$  hvis og kun hvis der findes et  $t$  så  $(t, x_1, \dots, x_n, y) \in B^{n+1}(i)$ , og  $(x_1, \dots, x_n) \in A$  hvis og kun hvis der findes  $t$  og  $y$  så  $(t, x_1, \dots, x_n, y) \in B^{n+1}(i)$ .  $A$  er altså domænet for funktionen

$$g(x_1, \dots, x_n) = \mu z((\beta_2^1(z), x_1, \dots, x_n, \beta_2^2(z)) \in B^{n+1}(i))$$

så  $A$  er r.n.

Antag på den anden side at  $A$  er r.n. dvs. der findes et  $i$  så  $A = W_i^n$ . Men så gælder

$$(x_1, \dots, x_n) \in A \Leftrightarrow \exists t : (t, x_1, \dots, x_n) \in B^n(i)$$

$B^n(i)$  er rekursiv, der findes derfor en rekursiv relation  $R_B$ , som definerer  $B^n(i)$  sådan at  $(t, x_1, \dots, x_n) \in B^n(i) \Leftrightarrow R_B(x_1, \dots, x_n, t)$  og dermed er  $(x_1, \dots, x_n) \in A \Leftrightarrow \exists t R_B(x_1, \dots, x_n, t)$ .

2. Antag at  $A \in \Pi_k^n$

$$\begin{aligned} (x_1, \dots, x_n) \in A &\Leftrightarrow \forall y_1 \exists y_2 \cdots Q y_k R(x_1, \dots, x_n) \\ (x_1, \dots, x_n) \notin A &\Leftrightarrow \neg(\forall y_1 \exists y_2 \cdots Q y_k R(x_1, \dots, x_n)) \text{ altså} \\ (x_1, \dots, x_n) \in \bar{A} &\Leftrightarrow \exists y_1 \forall y_2 \cdots \neg Q y_k \neg R(x_1, \dots, x_n) \end{aligned}$$

Det vil sige  $\bar{A} \in \Sigma_k^n$  som ønsket.

3. følger af 1 og 2.  
4. Lad  $A, B \in \Sigma_k^n$

$$\begin{aligned} (x_1, \dots, x_n) \in A &\Leftrightarrow \exists t R_A(x_1, \dots, x_n, t) \\ (x_1, \dots, x_n) \in B &\Leftrightarrow \exists s R_B(x_1, \dots, x_n, s) \end{aligned}$$

hvoraf

$$(x_1, \dots, x_n) \in A \cup B \Leftrightarrow \exists z (R_A(x_1, \dots, x_n, z) \vee R_B(x_1, \dots, x_n, z))$$

og

$$(x_1, \dots, x_n) \in A \cap B \Leftrightarrow \exists z (R_A(x_1, \dots, x_n, \beta_2^1(z)) \wedge R_B(x_1, \dots, x_n, \beta_2^2(z))).$$

Tilsvarende for  $\Pi_k^n$ .

5. Lad  $A \in \Sigma_k^n$  og lad  $a \in \mathbb{N}$  antag for nemheds skyld, at  $i = n$  (generaliseringen er oplagt). Da gælder:

$$\begin{aligned} \exists x_n < a \exists y_1 \forall y_2 \cdots Q y_k R_A(x_1, \dots, x_n, y_1, \dots, y_k) \\ \Updownarrow \\ \exists z \forall y_2 \cdots Q y_k (R_A(x_1, \dots, x_{n-1}, \beta_2^1(z), \beta_2^2(z), y_2, \dots, y_k) \wedge \beta_2^1(z) < a) \end{aligned}$$

hvilket viser, at udtrykket øverst er  $\Sigma_k^n$ . Tilsvarende er

$$\begin{aligned} \forall x_n < a \exists y_1 \forall y_2 \cdots Q y_k R_A(x_1, \dots, x_n, y_1, \dots, y_k) \\ \Updownarrow \\ \exists y_1 \forall z \exists y_3 \cdots Q y_k (R_A(x_1, \dots, x_{n-1}, \beta_2^1(z), y_1, \beta_2^2(z), y_3, \dots, y_k) \wedge \beta_2^1(z) < a) \end{aligned}$$

Resultatet for  $\Pi_k^n$  følger nu af 2.  $\square$

**Definition 2.13** En mængde  $A \in \Sigma_k^n$  (eller  $\Pi_k^n$ ) er  $\Sigma_k^n$ -komplet (eller  $\Pi_k^n$ -komplet) hvis og kun hvis der for alle  $B \in \Sigma_k^n$  (eller  $\Pi_k^n$ ) gælder  $B \leq_1 A$

### Eksempel 2.14

$K$  er  $\Sigma_1^1$ -komplet.

Relationen  $T(i, x, y) \Leftrightarrow \varphi^1(i, x) = y$  er rekursiv og  $K = \{x; \exists y T(x, x, y)\}$  så  $K \in \Sigma_1^1$ . Lad  $B \in \Sigma_1^1$  så er  $B$  r.n. i følge sætning 2.12 punkt 1, og dermed er  $B \leq K$  via  $h$  fra sætning 2.10 punkt 4. Hvis  $h$  ikke allerede er injektiv, kan man konstruere  $h^*$  som er det, og så at  $B \leq_1 K$  via  $h^*$ . Dette gøres ved succesivt at konstruere højere og højere indeks for den samme funktion ( $h(x)$  er jo et indeks), hvilket er muligt da alle funktioner har uendeligt mange forskellige indeks, men kan fx bare tilføje et bånd til den TM, som beregner funktionen, så har man et nyt indeks til samme funktion<sup>1</sup>

$Tot = \{x; \varphi_x^1 \text{ er total}\}$  er  $\Pi_2^1$ -komplet.

$$Tot = \{x; \forall y \exists z T(x, y, z)\} \in \Pi_2^1$$

Lad  $A \in \Pi_2^1$  dvs. der findes en rekursiv relation  $R$  så  $x \in A \Leftrightarrow \forall y \exists z R(x, y, z)$ . Sæt

$$\psi(x, a) = \begin{cases} 0 & \text{hvis } \forall y < a \exists z R(x, y, z) \\ \uparrow & \text{ellers} \end{cases}$$

Relationen  $\forall y < a \exists z R(x, y, z)$  er  $\Sigma_1^1$  så den er r.n. og dermed er  $\psi$  rekursiv (se bevis for sætning 2.10 punkt 3). Lad  $i$  være et indeks for  $\psi$ .  $\psi(x, a) = \varphi^2(i, x, a) = \varphi^1(s_1^1(i, x), a)$  per s-m-n sætningen. Sæt  $h(x) = s_1^1(i, x)$  så er  $\psi(x, a) = \varphi_{h(x)}^1(a)$ . Man har altså

$x \in A \Leftrightarrow \forall y \exists z R(x, y, z) \Leftrightarrow \forall a (\forall y < a \exists z R(x, y, z)) \Leftrightarrow \forall a \psi(x, a) = 0 \Leftrightarrow \forall a \varphi_{h(x)}^1(a) = 0 \Leftrightarrow \varphi_{h(x)}^1 \text{ er total} \Leftrightarrow h(x) \in Tot$ . Konklusion:  $A \leq Tot$  via  $h$  og jævnfør bemærkningen fra forrige eksempel kan man konstruere en injektiv funktion  $h^*$  således at  $A \leq_1 Tot$  via  $h^*$ .

**Definition 2.15**  $A \equiv B$  hvis  $A \leq B$  og  $B \leq A$

Det er nemt at se, at  $\equiv$  definerer en ækvivalensrelation da  $\leq$  er reflexiv og transitiv. Klasserne kaldes grader af uafgørlighed. En komplet mængde har altså den størst mulige grad af uafgørlighed blandt de rekursivt numerable mængder.

Da der gælder  $[A \leq B \text{ og } B \text{ rekursiv hhv r.n.}] \Rightarrow [A \text{ rekursiv hhv r.n.}]$ , kan man slutte, at hvis en klasse indeholder en rekursiv (eller r.n.) mængde, består den udelukkende af rekursive (eller r.n.) mængder.

Ønsker man at vise, at et problem  $A$  er uafgørligt, er den mest oplagte måde at reducere standsningsproblemet til  $A$  dvs. vise, at  $K \leq A$ . Hvis  $A$  også er r.n. har man samtidig vist, at  $A$  er komplet.

Indeholder alle uafgørlige problemer standsningsproblemet? Spørgsmålet er kendt som Post's problem, og kan også formuleres: Findes der en klasse, som ikke er rekursiv, og som har lavere grad end klassen, der indeholder  $K$ . Eller: er enhver rekursivt numerabel mængde, som ikke er rekursiv, komplet.

Svaret er nej, der findes rekursivt numerable mængder som ikke er komplette.<sup>2</sup> Man har altså ikke den modsatte implikation ( $A$  uafgørlig  $\Rightarrow K \leq A$ ).

<sup>1</sup>se [HR67] p.83 for den præcise konstruktion af  $h^*$ .

<sup>2</sup>se [HR67] p.106

## Chapter 3

# Gödels ufuldstændighedssætninger

I 1910 udkom Whitehead & Russells omfattende værk Principia Mathematica. Et af målene var en fuldstændig formalisering af aritmetikken forstået på den måde, at man ved udelukkende at arbejde i et symbolsprog og med ganske få interaktions- (eller deduktions-) regler kunne fjerne al semantik fra den matematiske bevisførelse. Et sådan symbolsprog med deduktionsregler kaldes et *logisk system*.

Hypotesen var, at man i det logiske system, på grundlag af Peano's aksiomer for aritmetikken, kunne vise alle teoremer indenfor denne. Man troede med andre ord, at systemet var *komplet* det vil sige, at for ethvert udsagn  $F$  skulle man enten kunne udlede  $F$  eller  $\neg F$  i systemet.

Mange matematikere troede at en sådan aksiomatisering var mulig, ikke blot for aritmetikken, men for hele matematikken, og flere arbejdede på at bevise det. I 1931 udkom imidlertid Gödels artikel "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme", som en gang for alle fastslog projektets umulighed. Gödel viser nemlig i sin første ufuldstændighedssætning, at ethvert aksiomssystem (også kaldet *teori*) for aritmetikken, som opfylder, at men effektivt (i.e. rekursivt) kan afgøre, om et givet udsagn er et aksiom eller ej, ikke kan være komplet. I sin anden sætning giver han et eksempel på et uafgørligt udsagn, altså et udsagn, som opfylder at hverken det selv eller dets negation kan vises i systemet.

Jeg har i dette afsnit forudsat, at læseren kender til modelteori og førsteordens logik, men for en ordens skyld vil jeg alligevel definere de begreber, der bliver brugt, da der kan være forskel på, hvad forskellige lærebøger kalder tingene. Dog vil jeg ikke give ret mange eksempler.

**Definition 3.1** *Et førsteordens sprog er en mængde bestående af*

- en numerabel mængde af variable  $\{v_0, v_1, v_2, \dots\}$
- parenteserne  $)$  og  $($  og de logiske konnektiver  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$  og kvantorerne  $\forall, \exists$
- En mængde af symboler for konstanter.
- En mængde af symboler for funktioner  $\{f_{n_1}^1, f_{n_2}^2, f_{n_3}^3, \dots\}$ , hvor  $n_i \geq 1$  angiver hvor mange variable funktionen tager.
- En mængde af symboler for relationer  $\{R_{n_1}^1, R_{n_2}^2, R_{n_3}^3, \dots\}$ , hvor  $n_i \geq 1$  angiver hvor mange argumenter relationen har.

De to første punkter er fælles for alle førsteordens sprog, mens de tre sidste varierer og kan være den tomme mængde.

**Definition 3.2** *Mængden af led i et sprog  $L$  er den mindste mængde, som opfylder*

- Den indeholder mængden af variable og symbolerne for konstanter

- For hvert symbol for en funktion er den stabil overfor operationen:

$$(x_1, x_2, \dots, x_{n_i}) \mapsto f_{n_i}^i(x_1, x_2, \dots, x_{n_i})$$

**Definition 3.3** Lad  $t_1, \dots, t_{n_i}$  være led og  $R_{n_i}^i$  være et symbol for en relation, da er  $R_{n_i}^i t_1, \dots, t_{n_i}$  en atomisk wf.

**Definition 3.4** Mængden af wf'er (wellformed formula) er den mindste mængde, som opfylder

- den indeholder alle de atomiske wf'er
- den er stabil overfor  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$
- for ethvert naturligt tal  $n$  og enhver wf  $F$  er  $\forall v_n F$  og  $\exists v_n F$  også wf'er.

**Definition 3.5** En fri variabel er en variabel som hverken er bundet af en alkvantor eller af en eksistenskvantor.

**Definition 3.6** En lukket wf er en wf uden frie variable.

**Definition 3.7** En teori er en mængde af lukkede wf'er.

### 3.1 Peano's aksiomer

Til det logiske system hører først og fremmest de logiske aksiomer og deduktionsreglerne, som er fælles for alle førsteordenssprog og alle teorier.

**Definition 3.8** Lad  $\mathcal{L}$  være et førsteordenssprog og  $B, C, D$  wf'er i  $\mathcal{L}$ . De logiske aksiomer er følgende:

$L_1$   $\forall v_0 B(v_0) \Rightarrow B(t)$ , hvor  $t$  er et led og ingen variabel i  $t$  i forvejen er bundet, der hvor  $t$  indsættes.

$L_2$   $\forall v_0 (B \Rightarrow C) \Rightarrow (B \Rightarrow \forall v_0 C)$  hvis  $v_0$  ikke optræder frit i  $B$ .

$L_3$  Alle wf'er, som opnåes ved at erstatte variable med wf'er i en tautologi fra propositional kalkyle.

For at forstå meningen med  $L_1$ , hjælper det nok at se dette eksempel:

#### Eksempel 3.9

Betragt følgende wf:

$$\forall v_0 \exists v_1 (v_1^2 = v_0 \vee v_1^2 + v_0 = 0)$$

Denne wf er sand i de reelle tal, men hvis man fandt på at sætte  $v_0 = v_1^2 + 1$  kunne man udlede

$$\exists v_1 (v_1^2 = v_1^2 + 1 \vee v_1^2 + v_1^2 + 1 = 0)$$

hvilket ikke gælder i de reelle tal. Derfor forbeholdene i aksiomet  $L_1$ .

**Definition 3.10** Deduktionsreglerne er følgende

**MP** Modus ponens: Af  $B$  og  $B \Rightarrow C$  får man  $C$

**GEN** Generalisation: Af  $B$  får man  $\forall v_n B$ , hvor  $n \in \mathbb{N}$

**Definition 3.11** Et formelt bevis ud fra en teori  $T$  for en wf  $F$  i det logiske system er en endelig følge  $G_1, G_2, \dots, G_n$  sådan at  $G_n = F$  og for hvert  $i < n$  er  $G_i$  enten

1. et logisk aksiom
2. en wf i  $T$

3. udledt af  $G_j, G_k$   $j, k < i$  ved hjælp af en af deduktionsreglerne

Hvis der findes et bevis for  $F$  ud fra en teori  $T$  skriver man  $T \vdash F$  og  $F$  kaldes da et teorem i  $T$ .

**Definition 3.12** En teori  $T$  siges at være komplet hvis der for enhver wf  $F$  gælder enten  $T \vdash F$  eller  $T \vdash \neg F$

**Definition 3.13** En teori  $T$  siges at være konsistent, hvis der for alle wf'er gælder enten  $T \not\vdash F$  eller  $T \not\vdash \neg F$

Desuden er deduktionslemmet overordentligt nyttigt

**Lemma 3.14 (Deduktionslemmet)** Lad  $T$  være en teori og  $B$  en lukket wf, da gælder  $T \vdash B \Rightarrow C$  hvis og kun hvis  $T \cup \{B\} \vdash C$

Se [Men97] p.74 for bevis.

### Eksempel 3.15

Hvis  $T$  er inkonsistent vil  $T \vdash G$  for alle wf'er  $G$ . Der findes nemlig en wf  $F$  så  $T \vdash F$  og  $T \vdash \neg F$  dermed også  $T \vdash F \wedge \neg F$ . Lad  $G$  være en vilkårlig wf.  $F \wedge \neg F \Rightarrow G$  er en tautologi, så ved modus ponens fås  $T \vdash G$ .

Peano's aksiomer er en teori i sproget  $\mathcal{L}_{\mathcal{A}} = \{\bar{0}, \bar{s}, \bar{+}, \bar{\times}, =\}$ . Her er  $\bar{0}$  et symbol for en konstant,  $\bar{s}$  et symbol for en funktion af en variabel og  $\bar{+}, \bar{\times}$  symboler for funktioner af to variable. Disse symboler har ikke noget af gøre med det sædvanlige nul, plus eller gange-tegn, men det er klart at symbolerne er valgt på denne måde, fordi de, når de tolkes som de "rigtige" nul, plus og gange i  $\mathbb{N}$  og når  $\bar{s}$  tolkes som successorfunktionen, giver en model for Peano's aksiomer. Lighedstegnet er underlagt nogle faste normer og kan kun tolkes som det sædvanlige lighedstegn.

#### Peano's aksiomer

- (A<sub>1</sub>)  $\forall v_0 \neg \bar{s}v_0 = \bar{0}$
- (A<sub>2</sub>)  $\forall v_0 \exists v_1 (\neg v_0 = \bar{0} \Rightarrow \bar{s}v_1 = v_0)$
- (A<sub>3</sub>)  $\forall v_0 \forall v_1 (\bar{s}v_0 = \bar{s}v_1 \Rightarrow v_0 = v_1)$
- (A<sub>4</sub>)  $\forall v_0 v_0 \bar{+} \bar{0} = v_0$
- (A<sub>5</sub>)  $\forall v_0 \forall v_1 v_0 \bar{+} \bar{s}v_1 = \bar{s}(v_0 \bar{+} v_1)$
- (A<sub>6</sub>)  $\forall v_0 v_0 \bar{\times} \bar{0} = \bar{0}$
- (A<sub>7</sub>)  $\forall v_0 \forall v_1 v_0 \bar{\times} \bar{s}v_1 = (v_0 \bar{\times} v_1) \bar{+} v_1$
- (IS)  $[F(\bar{0}) \wedge \forall v_0 (F(v_0) \Rightarrow F(\bar{s}v_0))] \Rightarrow \forall v_0 F(v_0)$ ,  
hvor  $F(v_0)$  er en vilkårlig wf i  $\mathcal{L}_{\mathcal{A}}$  med  $v_0$  som fri variabel

Lad  $\{A_1, \dots, A_7, IS\} = P$  IS står for induktionsskema. Da man i IS kan indsætte en vilkårlig wf er Peano's aksiomer en uendelig teori. På den anden side er det nemt at afgøre, hvorvidt en wf er et aksiom eller ej, ved at undersøge om det enten er et af aksiomerne  $A_1 - A_7$  eller om den har formen IS. Det virker klart, at der må findes en algoritme som svarer på dette spørgsmål, og det skal da også vise sig, at der findes en rekursiv funktion, som afgør, om en wf tilhører  $P$  eller ej. Som allerede nævnt er  $\langle \mathbb{N}, 0, s, +, \times \rangle$ , hvor  $s$  er successorfunktionen og  $0$  er det rigtige nul og  $+, \times$  de sædvanlige funktioner "plus" og "gange" en model for  $P$ . Jeg vil i det følgende nøjes med at skrive  $\mathbb{N} \models P$  for at udtrykke dette.

Man får brug for endnu et resultat fra modelteorien, nemlig Gödels fuldstændighedssætning

**Sætning 3.16 (fuldstændighedssætningen)** Lad  $F$  være en lukket wf og  $T$  en teori i et sprog  $\mathcal{L}$  så gælder:  $T \vdash F$  hvis og kun hvis, der for enhver model  $\mathcal{M}$  for  $T$  gælder  $\mathcal{M} \models F$

**Bevis:** Se [Men97] p. 91.

Og her kommer et eksempel på, hvordan systemet fungerer:

**Eksempel 3.17**  $P \vdash \forall v_0 \bar{0} \bar{+} v_0 = v_0$

1.) $\forall v_0 v_0 \bar{+} \bar{0} = v_0$	$A_4$
2.) $\bar{0} \bar{+} \bar{0} = \bar{0}$	$L_1$
3.) $\forall v_0 \forall v_1 v_0 \bar{+} \bar{s} v_1 = \bar{s}(v_0 \bar{+} v_1)$	$A_5$
4.) $\bar{0} \bar{+} v_0 = v_0$	$HYP$
5.) $\bar{0} \bar{+} \bar{s} v_0 = \bar{s}(\bar{0} \bar{+} v_0)$	$A_5, L_1$
6.) $\bar{0} \bar{+} \bar{s} v_0 = \bar{s} v_0$	4., 5. linie
7.) $A \Rightarrow (B \Rightarrow A \wedge B)$	
8.) $\forall v_0 (\bar{0} \bar{+} v_0 = v_0 \Rightarrow \bar{0} \bar{+} \bar{s} v_0 = \bar{s} v_0)$	4., 6., deduktionslemma, GEN
9.) $\bar{0} \bar{+} \bar{0} = \bar{0} \Rightarrow ((\forall v_0 (\bar{0} \bar{+} v_0 = v_0) \Rightarrow \bar{0} \bar{+} \bar{s} v_0 = \bar{s} v_0) \Rightarrow (\bar{0} \bar{+} \bar{0} = \bar{0} \wedge \forall v_0 (\bar{0} \bar{+} v_0 = v_0 \Rightarrow \bar{0} \bar{+} \bar{s} v_0 = \bar{s} v_0)))$	7., $L_3$
10.) $\bar{0} \bar{+} \bar{0} = \bar{0} \wedge \forall v_0 (\bar{0} \bar{+} v_0 = v_0 \Rightarrow \bar{0} \bar{+} \bar{s} v_0 = \bar{s} v_0)$	2., 8., $MP, MP$
11.) $\forall v_0 \bar{0} \bar{+} v_0 = v_0$	10., $IS$

I dette eksempel beskrives hvert skridt i beviset, denne form for bevisførelse bliver de fleste nok hurtigt trætte af. Pointen med ovenstående eksempel er at demonstrere, at bevisførelsen rent faktisk foregår fuldstændigt automatisk, og uden videre ville kunne udføres af en maskine. Hvis man tillader sig at være lidt mindre stringent, kan man rimeligt hurtigt vise, at  $\bar{+}$  er kommutativ og andre lidt mere interessante resultater. Man kan i princippet vise alle kendte sætninger i aritmetikken på denne måde, selv om det nok ville tage lang tid at vise Fermat-Wiles sætning.

Lad  $P_0$  være teorien som består af aksiomerne  $A_1, A_2, \dots, A_7$ .  $P_0$  har den fordel frem for  $P$ , at det er en endelig teori, men bortset fra det, er den meget "svag", man kan ikke engang vise at  $\bar{+}$  er kommutativ.

**Definition 3.18** initial segment

Lad  $\mathcal{M}$  og  $\mathcal{N}$  være to modeller for  $P_0$  og antag, at  $\mathcal{N}$  er en delstruktur af  $\mathcal{M}$ . Man kalder  $\mathcal{N}$  et initial segment af  $\mathcal{M}$ , hvis der gælder for alle  $a \in \mathcal{N}$  og  $b \in \mathcal{M}$ :

1. hvis  $\mathcal{M} \models b \leq a$  da er  $b \in \mathcal{N}$
2. hvis  $b \notin \mathcal{N}$  så gælder der  $\mathcal{M} \models a \leq b$

Her er  $a \leq b$  en forkortelse for  $\exists c (c \bar{+} a = b)$

**Lemma 3.19** Lad  $\mathcal{M}$  være en model for  $P_0$ , så er  $\langle \mathbb{N}, +, \times, 0 \rangle$  et initial segment for  $\mathcal{M}$ .

se [Las94] p.74 for bevis.

**Lemma 3.20** Lad  $T$  være en teori med  $P_0 \subseteq T$ , da er  $\mathbb{N}$  initial segment for enhver model  $\mathcal{M}$  for  $T$ .

**Bevis** Antag, at  $\mathcal{M} \models T$ . Da  $P_0 \subseteq T$  er  $\mathcal{M}$  specielt model for  $P_0$ . I følge lemma 3.19 er  $\mathbb{N}$  initial segment for enhver model for  $P_0$ , altså  $\mathbb{N}$  er initial segment for  $\mathcal{M}$  som ønsket.  $\square$

**Definition 3.21** En wf  $F$  siges at være  $\Sigma_1$  (jævnfør det aritmetiske hierarki) hvis  $F$  er på formen  $\exists v_0 G$ , hvor  $G$  er en wf uden kvantifikatorer.

**Lemma 3.22** Lad  $F$  være en wf som er  $\Sigma_1$  og lad  $\mathcal{N}$  være et initial segment af  $\mathcal{M}$ , da gælder

$$(\mathcal{N} \models F) \Rightarrow (\mathcal{M} \models F)$$

**Bevis**  $F$  er på formen  $\exists v_0 G$ , det vil sige, der findes  $a \in \mathcal{N}$  så  $\mathcal{N} \models G[a/v_0]$ . Da  $\mathcal{N}$  er et initial segment af  $\mathcal{M}$ , er  $\mathcal{N}$  specielt en delstruktur, dvs  $a \in \mathcal{M}$ , og dermed har man  $\mathcal{M} \models G[a/v_0]$  altså  $\mathcal{M} \models F$ .  $\square$

**Sætning 3.23** Lad  $T$  være en teori og  $F$  en wf som er  $\Sigma_1$ . Hvis  $\mathbb{N}$  er initial segment for enhver model for  $T$  gælder der:

$$(\mathbb{N} \models F) \Rightarrow (T \vdash F)$$

**Bevis** I følge fuldstændighedssætningen er det nok at vise, at  $\mathcal{M} \models F$  for alle modeller  $\mathcal{M}$  for  $T$ . Lad der være givet en model  $\mathcal{M}$  for  $T$ . Per antagelse er  $\mathbb{N}$  initial segment for  $\mathcal{M}$ , så i følge lemma 3.22 er  $\mathcal{M} \models F$ .  $\square$

**Korollar 3.24** Lad  $F$  være en wf, som er  $\Sigma_1$ , da gælder

$$\mathbb{N} \models F \Leftrightarrow P_0 \vdash F$$

**Bevis** Implikationen fra venstre følger af sætningen ovenfor, da  $\mathbb{N}$  er initial segment for enhver model for  $P_0$  (lemma 3.19). Den anden implikation følger af fuldstændighedssætningen da  $\mathbb{N}$  jo er model for  $P_0$ .  $\square$

## 3.2 Repræsentation

**Definition 3.25** Lad  $f$  være en funktion fra  $\mathbb{N}^p \rightarrow \mathbb{N}$  og  $F[v_0, v_1, \dots, v_p]$  en wf. Men siger, at  $F[v_0, v_1, \dots, v_p]$  repræsenterer  $f$  i en teori  $T \subseteq P_0$ , hvis der for alle  $(n_1, n_2, \dots, n_p) \in \mathbb{N}^p$  gælder:

$$T \vdash \forall v_0 (F[v_0, \underline{n}_1, \dots, \underline{n}_p] \Leftrightarrow v_0 = \underline{f(n_1, \dots, n_p)})$$

Hvor  $\underline{n}$  er en forkortelse for leddet  $\underbrace{\bar{s}\bar{s} \dots \bar{s}\bar{0}}_n$ .

Det vil sige, hvis  $\mathcal{M}$  er en model for  $T$  og  $v_0$  et element, som opfylder  $F$ , så er  $v_0$  fortolkningen af leddet  $\underline{f(n_1, \dots, n_p)}$ , altså der er netop et element, som opfylder  $F$ .

**Eksempel 3.26** • Successor-funktionen kan repræsenteres af  $v_0 = \bar{s}v_1$ .

$$P_0 \vdash \forall v_0 (v_0 = \bar{s}\underline{n}_1 \Leftrightarrow \underline{sn}_1)$$

skal være opfyldt. Per definition er

$$\bar{s}\underline{n}_1 = \underbrace{\bar{s}\bar{s} \dots \bar{s}\bar{0}}_{n_1+1} \text{ og } \underline{sn}_1 = \underline{n_1 + 1} = \underbrace{\bar{s}\bar{s} \dots \bar{s}\bar{0}}_{n_1+1}$$

så resultatet er trivielt.

- Den konstante funktion kan repræsenteres ved  $v_0 = \underline{n}$ .
- Projektionerne  $P_p^i(n_1, \dots, n_p) = n_i$  kan repræsenteres ved  $v_0 = v_i$

Faktisk gælder der:

**Sætning 3.27 (Repræsentationssætningen)** Alle totale, rekursive funktioner kan repræsenteres i  $T$  af en wf som er  $\Sigma_1$ , hvor  $T$  er en vilkårlig teori, som indeholder  $P_0$ .

**Bevis** Se [Las94] p.77 og 96

**Definition 3.28** En mængde  $A \subseteq \mathbb{N}^p$  siges at være repræsenteret i  $T \supseteq P_0$  af en wf  $F[v_1, \dots, v_p]$  hvis der for alle  $(n_1, \dots, n_p) \in \mathbb{N}^p$  gælder

- $(n_1, \dots, n_p) \in A \Rightarrow T \vdash F[\underline{n}_1, \dots, \underline{n}_p]$
- $(n_1, \dots, n_p) \notin A \Rightarrow T \vdash \neg F[\underline{n}_1, \dots, \underline{n}_p]$

Bemærk, at det ikke er ækvivalent med  $(n_1, \dots, n_p) \in A \Leftrightarrow T \vdash F[\underline{n}_1, \dots, \underline{n}_p]$  idet negationen af  $T \vdash F[\underline{n}_1, \dots, \underline{n}_p]$  er  $T \not\vdash F[\underline{n}_1, \dots, \underline{n}_p]$ .

**Lemma 3.29** *En mængde  $A \subseteq \mathbb{N}^p$  kan repræsenteres hvis og kun hvis dens indikatorfunktion kan repræsenteres.*

**Bevis:** Hvis  $F$  repræsenterer  $A$ , vil denne wf

$$(F[v_1, \dots, v_p] \wedge v_0 = 1) \vee (\neg F[v_1, \dots, v_p] \wedge v_0 = 0)$$

repræsenterer  $1_A$ . Omvendt, hvis  $G[v_0, v_1, \dots, v_p]$  repræsenterer  $1_A$ , så vil  $G[\underline{1}, v_1, \dots, v_p]$  repræsenterer  $A$ , fordi,

$$P_0 \vdash \forall v_0 (G[v_0 \underline{n}_1, \dots, \underline{n}_p] \Leftrightarrow v_0 = \underline{1}_A(n_1, \dots, n_p))$$

Substituer  $v_0$  med  $\underline{1}$  så fås

$$P_0 \vdash (G[\underline{1} \underline{n}_1, \dots, \underline{n}_p] \Leftrightarrow \underline{1}_A(n_1, \dots, n_p) = \underline{1})$$

Så hvis  $(n_1, \dots, n_p) \in A$  da er  $\underline{1}_A(n_1, \dots, n_p) = \underline{1}$  så da

$$P_0 \vdash \underline{1} = \underline{1}$$

følger ved modus ponens at

$$P_0 \vdash G[\underline{1}, \underline{n}_1, \dots, \underline{n}_p].$$

Hvis  $(m_1, \dots, m_p) \notin A$  er  $\underline{1}_A(m_1, \dots, m_p) = \bar{0}$  og da

$$P_0 \vdash \underline{1} \neq \bar{0}$$

følger ved modus ponens, at

$$P_0 \vdash \neg G[\underline{1}, \underline{m}_1, \dots, \underline{m}_p].$$

□

Da en mængde er rekursiv netop når dens indikatorfunktion (som altid er total) er rekursiv, gælder altså:

**Sætning 3.30** *Hvis  $A \subseteq \mathbb{N}^p$  er rekursiv, da kan  $A$  repræsenteres i  $T \supseteq P_0$ .*

### 3.3 Gödelnumre

Ligesom Turingmaskinen blev kodet ved hjælp af de naturlige tal, kan man også kode hele syntaxen for det logiske system. Disse koder kaldes Gödelnumre. Der findes mange forskellige måder at kode syntaxen på, men dette har ikke den store betydning, det interessante er, at det kan lade sig gøre, og at man på denne måde får en mængde af naturlige tal, som svarer til fx mængden af wf'er i  $\mathcal{L}_A$ . Hvis denne mængde er rekursiv, så har man en algoritme til at afgøre, om en følge af symboler er en wf eller ej.

Et af hovedresultaterne i dette afsnit er netop at vise, at mængden af wf'er som kan bevises i en teori  $T$ , er rekursiv. Kun Gödelnumrene for sproget  $\mathcal{L}_A$  vil blive defineret her. Man får brug for funktionerne  $\alpha_n$  og  $\beta_n^i$ , som blev defineret i 1.7.

**Definition 3.31** *Gödelnummeret for et led  $t$  noteres  $\#t$  og er defineret ved*

$$\begin{aligned} \text{hvis } t = \bar{0} & \quad \#t = \alpha_3(0, 0, 0) \\ \text{hvis } t = v_n & \quad \#t = \alpha_3(n + 1, 0, 0) \\ \text{hvis } t = \bar{s}t_1 & \quad \#t = \alpha_3(\#t_1, 0, 1) \\ \text{hvis } t = t_1 \bar{+} t_2 & \quad \#t = \alpha_3(\#t_1, \#t_2, 2) \\ \text{hvis } t = t_1 \bar{\times} t_2 & \quad \#t = \alpha_3(\#t_1, \#t_2, 3) \end{aligned}$$

**Lemma 3.32** Mængden  $Led = \{\#t; t \text{ er et led i } \mathcal{L}_A\}$  er rekursiv

**Bevis** Det skal vises, at indikatorfunktionen  $f$  for mængden  $Led$  er rekursiv.  $f$  kan defineres ved

$$\begin{array}{ll} f(0) = f(1) = 1 & \\ \text{hvis } \beta_3^3(x) = \beta_3^2(x) = 0 & f(x) = 1 \\ \text{hvis } \beta_3^3(x) = 0 \text{ og } \beta_3^2(x) \neq 0 & f(x) = 0 \\ \text{hvis } \beta_3^3(x) = 1 \text{ og } \beta_3^2(x) \neq 0 & f(x) = 0 \\ \text{hvis } \beta_3^3(x) = 0 \text{ og } \beta_3^2(x) = 1 & f(x) = f(\beta_3^1(x)) \\ \text{hvis } \beta_3^3(x) \in \{2, 3\} & f(\beta_3^1(x))f(\beta_3^2(x)) \\ \text{hvis } \beta_3^3(x) > 3 & f(x) = 0 \end{array}$$

Bemærk, at for  $x > 1$  er  $\beta_3^i(x) < x$  thi per induktion:

$$\text{for } x = 2 \text{ er } \beta_3^1(x) = \beta_3^2(x) = 1 \text{ og } \beta_3^3(x) = 0$$

Antag nu, at  $\beta_3^i(n) < n$  for  $i = 1, 2, 3$ . Per konstruktion af  $\beta$ -funktionerne gælder der  $\beta_3^i(x) = x$  eller  $\beta_3^i(x) = x + 1$  for alle  $x$ , så

$$\beta_3^i(n+1) \leq \beta_3^i(n) + 1 < n + 1$$

$f$  er derfor veldefineret, og da  $\beta$ -funktionerne er rekursive, er  $f$  rekursiv.  $\square$

**Definition 3.33** Lad  $t_1, t_2$  være led. For en wf  $F$  er Gödelnummeret:

$$\begin{array}{ll} \text{hvis } F \equiv t_1 = t_2 & \#F = \alpha_3(\#t_1, \#t_2, 0) \\ \text{hvis } F \equiv \neg F_1 & \#F = \alpha_3(\#F_1, 0, 1) \\ \text{hvis } F \equiv F_1 \wedge F_2 & \#F = \alpha_3(\#F_1, \#F_2, 2) \\ \text{hvis } F \equiv F_1 \vee F_2 & \#F = \alpha_3(\#F_1, \#F_2, 3) \\ \text{hvis } F \equiv F_1 \Rightarrow F_2 & \#F = \alpha_3(\#F_1, \#F_2, 4) \\ \text{hvis } F \equiv F_1 \Leftrightarrow F_2 & \#F = \alpha_3(\#F_1, \#F_2, 5) \\ \text{hvis } F \equiv \forall v_n F_1 & \#F = \alpha_3(\#F_1, n, 6) \\ \text{hvis } F \equiv \exists v_n F_1 & \#F = \alpha_3(\#F_1, n, 7) \end{array}$$

**Lemma 3.34**

$$WF = \{\#F; F \text{ er en wf i } \mathcal{L}_A\}$$

og

$$AX = \{\#F; F \text{ er et logisk axiom } \}$$

er rekursive.

Beviset er fuldstændigt magen til før, hvor man deler op efter tilfælde.

**Lemma 3.35** Der findes to rekursive funktioner  $Subs_t$  og  $Subs_f$  sådan at hvis  $t$  og  $u$  er led og  $F$  er en wf da gælder for alle  $n$

$$Subs_t(n, \#t, \#u) = \#u_{t/v_n}$$

og

$$Subs_f(n, \#t, \#F) = \#F_{t/v_n}$$

Givet et  $n$  og givet Gödelnumrene for  $t$  og  $F$  beregner  $Subs_f$  altså Gödelnummeret for wf  $F$ , hvor alle frie forekomster (hvis der er nogen) af  $v_n$  er erstattet med  $t$ .  $Subs_t$  gør det tilsvarende for et led, her er alle forekomster for  $v_n$  dog automatisk frie.

**Bevis:**

Jeg vil nøjes med at vise resultatet for  $Subs_t$ , da beviset for  $Subs_f$  næsten er magen til. Definer

$$\begin{array}{ll} \text{hvis } \beta_3^3(x) = 0 \text{ og } x \neq \alpha_3(n+1, 0, 0) & Subs_t(n, y, x) = x \\ \text{hvis } \beta_3^3(x) = 0 \text{ og } x = \alpha_3(n+1, 0, 0) & Subs_t(n, y, x) = y \\ \text{hvis } \beta_3^3(x) = 1 \text{ og } \beta_3^2(x) = 0 & Subs_t(n, y, x) = \alpha_3(Subs_t(n, y, \beta_3^1(x)), 0, 1) \\ \text{hvis } \beta_3^3(x) \in \{2, 3\} & Subs_t(n, y, x) = \alpha_3(Subs_t(n, y, \beta_3^1(x)), Subs_t(n, y, \beta_3^2(x)), \beta_3^3(x)) \\ \text{ellers sættes} & Subs_t(n, y, x) = x \end{array}$$

$Subs_t$  er veldefineret, for hvis  $x = 0$  er  $x = \alpha_3(0, 0, 0)$  og hvis  $x = 1$  er  $x = \alpha_3(1, 0, 0)$  i begge tilfælde er  $\beta_3^3(x) = 0$ , og i dette tilfælde er givet definitionen af  $Subs_t$  ingen problemer. Da man ved, at  $\beta_3^i(x) < x$  for  $x > 1$  er de andre tilfælde også veldefinerede, og da  $Subs_t$  består af rekursive elementer, er funktionen rekursiv.  $\square$

**Definition 3.36** Lad  $T$  være en teori og lad  $Th(T) = \{\#F; F \text{ er en lukket wf og } T \vdash F\}$ . Man siger da at

- $T$  er rekursiv, hvis mængden  $\#T = \{\#F; F \in T\}$  er rekursiv.
- $T$  er afgørlig, hvis  $Th(T)$  er rekursiv.

**Eksempel 3.37** Enhver endelig teori er rekursiv.

Lad  $T = \{F_1, F_2, \dots, F_n\}$  være en endelig teori.  $\#T$  er da en endelig delmængde af  $\mathbb{N}$  og i følge eksempel 1.6 er enhver endelig mængde rekursiv.

**Sætning 3.38**  $P$  er en rekursiv teori.

**Bevis:** Ligesom ved mængderne  $Led$  og  $WF$  kan man ved opdeling i tilfælde se, at mængden  $\Phi = \{(\#F, n); F \text{ er en wf hvori } v_n \text{ har en fri forekomst}\}$  er rekursiv. Desuden bemærkes det, at  $P_0$  er rekursiv da det er en endelig teori. Man mangler altså kun at vise, at det kan afgøres rekursivt, om et givet naturligt tal er Gödelnummeret for en wf er på formen IS. Lad derfor  $n \in \mathbb{N}$  være givet. Der skal først og fremmest gælde, at

$$\exists k, j < n (k \in WF \wedge (k, j) \in \Phi)$$

lad

$$\begin{array}{l} Subs_f(j, \#0, k) = Subs_f(j, 0, k) = n_1 \\ Subs_f(j, \#\bar{s}v_j, k) = Subs_f(j, \alpha_3(\alpha_3(j+1, 0, 0), 0, 1), k) = n_2 \\ Subs_f(k, j, 6) = n_3 \end{array}$$

Man kan nu nemt opskrive hvad det vil sige at være på formen IS:

$$is(k) = \alpha_3(\alpha_3(n_1, \alpha_3(\alpha_3(k, n_2, 4), j, 6), 2), n_3, 4)$$

For at opsummere har man altså:  $n \in P$  hvis og kun hvis  $n \in P_0$  eller  $\exists k, j < n (k \in WF \wedge (k, j) \in \Phi \wedge n = is(k))$   $\square$

Alle de teorier man sædvanligvis arbejder i er rekursive, for hvis en teori ikke er rekursiv, betyder det (under Church's tese) at man ikke har en effektiv måde til at afgøre, hvorvidt en wf er et aksiom. Men hvis man ikke kan afgøre dette, kan man heller afgøre, hvornår man har et bevis! De ikke-rekursive teorier er med andre ord ikke særligt interessante i praksis. Derimod er der mange "naturlige" eksempler på *uafgørlige* teorier.

**Eksempel 3.39** Lad  $T$  være en konsistent teori som indeholder  $P_0$ , da er  $T$  uafgørlig.

At  $T$  er uafgørlig vil sige at  $Th(T) = \{\#F; F \text{ er en wf og } T \vdash F\}$  ikke er rekursiv. Antag at  $T$  er afgørlig, så er mængden

$$\Theta = \{(m, n); m = \#F[v_0] \wedge T \vdash F[\underline{n}] \text{ for en wf } F\}$$

rekursiv.

$$B = \{n \in \mathbb{N}; (n, n) \notin \Theta\}$$

er derfor også rekursiv, og da  $T \supseteq P_0$  findes der en wf  $G[v_0]$  som repræsenterer  $B$  dvs

$$n \in B \Rightarrow T \vdash G[\underline{n}] \text{ og } n \notin B \Rightarrow T \vdash \neg G[\underline{n}]$$

Lad  $\#G[v_0] = a$  så får man

$$a \in B \Rightarrow T \vdash G[\underline{a}] \Rightarrow (a, a) \in \Theta$$

hvilket er i modstrid med ovenstående da

$$a \in B \Rightarrow (a, a) \notin \Theta$$

,og

$$a \notin B \Rightarrow T \vdash \neg G[\underline{a}]$$

hvilket betyder at  $T$  er inkonsistent, da

$$a \notin A \Rightarrow (a, a) \in \Theta \Rightarrow T \vdash G[\underline{a}].$$

Konklusion:  $Th(T)$  er ikke rekursiv.  $\square$

**Definition 3.40** Lad  $\mathcal{S}$  betegne mængden af endelige følger af naturlige tal. Definer  $\Omega : \mathcal{S} \rightarrow \mathbb{N}$  ved

$$\Omega(x_1, x_2, \dots, x_p) = \pi(0)^{x_1} \pi(1)^{x_2} \dots \pi(p)^{x_p}$$

(hvor  $\pi(i)$  er det  $i + 1$ 'te primtal). For den tomme følge  $()$  sættes

$$\Omega() = 0$$

Endvidere defineres  $\delta : \mathbb{N}^2 \rightarrow \mathbb{N}$  ved

$$\delta(i, x) = \mu z \leq x (x \text{ er ikke delelig med } \pi(i)^{z+1})$$

$\delta(i, x)$  giver altså eksponenten til  $\pi(i)$  i primopløsningen af  $x$ . Det ses, at  $\delta$  er rekursiv, da  $\pi$  er rekursiv og euklidisk division er rekursiv (se [Men97] p. 177 og 179).

Man kan nu definere Gödelnummereringen for beviser:

Lad  $d = (F_1, \dots, F_n)$  være en følge af wf'er i  $\mathcal{L}_A$ . Man noterer  $\#\#d = \Omega(\#F_1, \dots, \#F_n)$ . Hvis  $d$  er et bevis for  $F_n$  (se definition 3.11) er  $\#\#d$  altså Gödelnummeret for beviset.

**Sætning 3.41** Lad  $T$  være en rekursiv teori, da er mængden

$$Bev(T) = \{(n, m); n = \#F \text{ hvor } F \text{ er en wf } m = \#\#d \text{ hvor } d \text{ er et bevis for } f \text{ i } T\}$$

rekursiv.

**Bevis:** Lad  $lg(m)$  være defineret ved

$$lg(m) = \mu k \leq m (\pi(k) \text{ ikke går op i } m)$$

$lg$  er rekursiv og giver længden af følgen  $d$ . ( $\pi(i)$  er det  $i + 1$ 'te primtal)

$(n, m) \in Bev(T)$  hvis og kun hvis følgende tre betingelser er opfyldt:

1. For alle  $i \leq lg(m)$  er  $\delta(i, m) \in WF$
2.  $\delta(lg(m), m) = n$
3.  $\forall i \leq lg(m)$  skal der gælde en af følgende:
  - $\delta(i, m) \in Ax \cup \#T$
  - $\exists j < i \exists p < m : \delta(i, m) = \alpha_3(\delta(j, m), p, 6)$  [GEN]
  - $\exists j, k < i : \delta(j, m) = \alpha_3(\delta(k, m), \delta(i, j), 4)$  [MP]

Betingelse nr 1 sikrer, at  $m$  er Gödelnummeret for en følge af wf'er. Betingelse 2 sikrer, at det sidste led i følgen er  $F$  (hvor  $\#F = n$ ). Betingelse 3 sikrer, at følgen opfylder definitionen på et formelt bevis (se definition 3.11).

Betingelserne består af rekursive elementer, så  $Bev(T)$  er rekursiv.  $\square$

### 3.4 Gödels ufuldstændighedssætninger

Der findes mange forskellige udgaver af ufuldstændighedssætningerne. Nogle udgaver (heriblandt Gödels oprindelige) bruger begrebet  $\omega$ -konsistens. Jeg vil her vise to udgaver; dels Gödels oprindelige og dels en udgave som også kaldes Gödel-Rossers sætning og som kun kræver at teorierne er konsistente, hvilket er en svagere betingelse end  $\omega$ -konsistens. Det er en mere generel udgave, end Gödels oprindelige sætning, idet den omhandler en større klasse af teorier.

Først et par lemmaer.

**Lemma 3.42** *Lad  $T \supseteq P_0$  være en rekursiv teori og  $F$  en wf da gælder*

$$T \vdash F \text{ hvis og kun hvis } \mathbb{N} \models \exists y \mathcal{B}ev_T[\#F, y]$$

hvor  $\mathcal{B}ev_T$  er en wf som repræsenterer  $Bev(T)$

**Bevis:** Antag  $T \vdash F$ , dvs der findes et bevis for  $f$  i  $T$ . Antag  $\#d = n$  så har man  $(\#F, n) \in Bev(T)$  så per repræsentation har man  $T \vdash \mathcal{B}ev_T[\#F, \underline{n}]$ .  $\mathcal{B}ev_T$  er rekursiv og dermed specielt repræsenteret i  $P_0$  så  $\mathbb{N} \models \exists y \mathcal{B}ev_T[\#F, y]$ . Antag omvendt, at  $\mathbb{N} \models \exists y \mathcal{B}ev_T[\#F, y]$ . Da  $\exists y \mathcal{B}ev_T[\#F, y]$  er  $\Sigma_1$  følger det af sætning 3.23, da  $\mathbb{N}$  er initial segment for enhver model for  $T$  at  $T \vdash \exists y \mathcal{B}ev_T[\#F, y]$   $\square$

**Lemma 3.43** *Lad  $A \subseteq \mathbb{N}^p$  og lad  $T \supseteq P_0$  være en rekursiv og konsistent teori.  $A$  kan da repræsenteres i  $T$  hvis og kun hvis  $A$  er rekursiv.*

**Bevis:** Hvis  $A$  er rekursiv, findes der i følge repræsentationssætningen en wf  $F[v_1, \dots, v_n]$  som repræsenterer  $A$  i  $T$ .

Antag på den anden side, at  $A$  er repræsenteret af  $F[v_1, \dots, v_n]$  dvs

$$\begin{aligned} (n_1, \dots, n_p) \in A &\Rightarrow T \vdash F[\underline{n}_1, \dots, \underline{n}_p] \\ (n_1, \dots, n_p) \notin A &\Rightarrow T \vdash \neg F[\underline{n}_1, \dots, \underline{n}_p] \end{aligned}$$

Så af det forgående lemma fås

$$\begin{aligned} (n_1, \dots, n_p) \in A &\Leftrightarrow \mathbb{N} \models \exists y \mathcal{B}ev_T[\#F[\underline{n}_1, \dots, \underline{n}_p], y] \\ (n_1, \dots, n_p) \notin A &\Leftrightarrow \mathbb{N} \models \exists y \mathcal{B}ev_T[\#\neg F[\underline{n}_1, \dots, \underline{n}_p], y] \end{aligned}$$

Altså hvis

$$(n_1, \dots, n_p) \in A \text{ findes der et } m \in \mathbb{N} \text{ så } (\#F[\underline{n}_1, \dots, \underline{n}_p], m) \in Bev(T)$$

og hvis

$$(n_1, \dots, n_p) \notin A \text{ findes der et } m \in \mathbb{N} \text{ så } (\#\neg F[\underline{n}_1, \dots, \underline{n}_p], m) \in Bev(T)$$

$Bev(T)$  er rekursiv, så mængderne

$$B = \{(n_1, \dots, n_p); \exists m (\#F[\underline{n}_1, \dots, \underline{n}_p], m) \in Bev(T)\}$$

og

$$C = \{(n_1, \dots, n_p); \exists m (\#\neg F[\underline{n}_1, \dots, \underline{n}_p], m) \in Bev(T)\}$$

er rekursivt numerable (sætning 2.12 punkt 1). Det fremgår, at  $B = A$  og  $C = \bar{A}$ .  $A$  og  $\bar{A}$  er altså begge r.n. så  $A$  er rekursiv (lemma 2.3)  $\square$

**Definition 3.44**  *$A \subseteq \mathbb{N}^p$  siges at være svagt repræsenteret i  $T$ , hvis der findes en wf  $F[v_1, \dots, v_p]$  så*

$$(n_1, \dots, n_p) \in A \Leftrightarrow T \vdash F[\underline{n}_1, \dots, \underline{n}_p]$$

I modsætning til når  $A$  er repræsenteret, har man altså ikke

$$(n_1, \dots, n_p) \notin A \Rightarrow T \vdash \neg F[\underline{n}_1, \dots, \underline{n}_p]$$

**Definition 3.45** En teori  $T$  siges at være  $\omega$ -konsistent hvis der for enhver wf  $F[v_0]$  gælder: For alle  $n \in \mathbb{N}$   $T \vdash \neg F[\underline{n}]$  medfører  $T \not\vdash \exists y F[y]$

Bemærk, at hvis  $\mathbb{N}$  er model for  $T$  så er  $T$   $\omega$ -konsistent.

**Lemma 3.46** Lad  $T \supseteq P_0$  være en rekursiv og  $\omega$ -konsistent teori og lad  $A \subseteq \mathbb{N}^p$ , da gælder:  $A$  er r.n. hvis og kun hvis  $A$  er svagt repræsenteret i  $T$ .

**Bevis** Antag at  $A$  er svagt repræsenteret af  $F[v_1, \dots, v_p]$  altså

$$(n_1, \dots, n_p) \in A \Leftrightarrow T \vdash F[\underline{n}_1, \dots, \underline{n}_p]$$

hvilket i følge lemma 3.42 er ensbetydende med

$$\mathbb{N} \models \exists y \text{Bev}_T[\#F[\underline{n}_1, \dots, \underline{n}_p], y]$$

altså der findes  $m \in \mathbb{N}$  så  $(\#F[\underline{n}_1, \dots, \underline{n}_p], m) \in \text{Bev}(T)$ , dvs

$$A = \{(n_1, \dots, n_p); \exists m (\#F[\underline{n}_1, \dots, \underline{n}_p], m) \in \text{Bev}(T)\}$$

som ses at være r.n.

Antag på den anden side, at  $A$  er r.n. så findes der en rekursiv relation  $R$  så

$$(n_1, \dots, n_p) \in A \Leftrightarrow \exists t R(n_1, \dots, n_p, t).$$

Lad  $\mathcal{R}[v_1, \dots, v_p, y]$  repræsentere  $R$  i  $T$ , altså

$$\begin{aligned} R(n_1, \dots, n_p, t) &\Rightarrow T \vdash \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, \underline{t}] \\ \neg R(n_1, \dots, n_p, t) &\Rightarrow T \vdash \neg \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, \underline{t}] \end{aligned}$$

Målet er at vise, at wf  $\exists y \mathcal{R}(v_1, \dots, v_p, t)$  svagt repræsenterer  $A$  i  $T$ . Man har

$$(n_1, \dots, n_p) \in A \Leftrightarrow \exists t R(n_1, \dots, n_p, t)$$

dvs der findes  $t \in \mathbb{N}$  så  $\mathbb{N} \models \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, \underline{t}]$  og dermed  $\mathbb{N} \models \exists y \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, y]$  som i følge lemma 3.23 betyder at  $T \vdash \exists y \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, y]$  Altså

$$(n_1, \dots, n_p) \in A \Rightarrow T \vdash \exists y \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, y]$$

Hvis omvendt  $(n_1, \dots, n_p) \notin A$  så gælder for alle  $t \in \mathbb{N}$  at  $T \vdash \neg \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, \underline{t}]$ , så da  $T$  er  $\omega$ -konsistent har man som ønsket  $T \not\vdash \exists y \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, y]$ . Altså

$$(n_1, \dots, n_p) \in A \Leftrightarrow T \vdash \exists y \mathcal{R}[\underline{n}_1, \dots, \underline{n}_p, y]$$

□

**Sætning 3.47 (Gödels første ufuldstændighedssætning)** Lad  $T$  være en rekursiv,  $\omega$ -konsistent teori som indeholder  $P_0$ .  $T$  er da ikke komplet, specielt er  $P$  ikke komplet.

**Bevis** Betragt fra standsningsproblemet  $K = \{x; \varphi_x(x) \downarrow\}$ .  $K$  er r.n men ikke rekursiv. Der findes derfor en wf  $F[v_0]$  som svagt repræsenterer  $K$  i  $T$ .

$$n \in K \Leftrightarrow T \vdash F[\underline{n}]$$

Til gengæld findes der ikke nogen wf, som repræsenterer  $K$ , da  $K$  ikke er rekursiv. Man har med andre ord ikke  $n \notin K \Rightarrow T \vdash \neg F[\underline{n}]$  for alle  $n$ . Der findes altså et naturligt tal  $m$ , så  $m \notin K$  og  $T \not\vdash \neg F[\underline{m}]$  og da  $m \notin K$  har man samtidig  $T \not\vdash F[\underline{m}]$ .  $F[\underline{m}]$  er altså en uafgørlig wf i  $T$  □

Da der for en wf  $F$  altid gælder enten  $\mathbb{N} \models F$  eller  $\mathbb{N} \models \neg F$ , viser Gödels første ufuldstændighedssætning, at der findes gyldige sætninger i aritmetikken, som man ikke kan bevise

i det formelle system, i hvert fald ikke med de aksiomer man har defineret. Det er selvfølgelig nærliggende at spørge, om problemet kan løses ved at tilføje nye aksiomer. Og det kan det egentlig godt, man kan jo vælge teorien  $Th(\mathbb{N}) = \{\#F; F \text{ er en wf og } \mathbb{N} \models F\}$  som aksiomer, den er komplet, men den er imidlertid ikke rekursiv (i følge ufuldstændighedssætningen), og løser derfor ikke det oprindelige problem, nemlig at formalisere aritmetikken, sådan at det at lave beviser kan gøres helt mekanisk. De eneste teorier der dner til dette formål er de rekursive, og disse er inkomplette, hvis de er  $\omega$ -konsistente. Ikke bare findes der sætninger, som man ikke kan få en (Turing)-maskine til at vise; man kan heller ikke afgøre (rekursivt) om en given wf er uafgørlig, da  $Th(T)$  er uafgørlig (eksempel 3.39). Som med standsningsproblemet, kan man konkludere, at der ikke findes nogen (Turing)-maskine, som givet en teori og en wf, kan afgøre om denne wf er et teorem i den givne teori.

Faktisk gælder ufuldstændighedssætningen også med den svagere betingelse,  $T$  konsistent:

**Sætning 3.48 (Gödel-Rosser)** *Lad  $T$  være en rekursiv og konsistent teori, som indeholder  $P_0$ .  $T$  er da ikke komplet.*

**Bevis:** Først vises, at hvis  $T$  er rekursiv og komplet, så er  $T$  afgørlig, altså  $Th(T)$  er rekursiv. Bemærk, at  $Th(T)$  er r.n. fordi

$$n \in Th(T) \Leftrightarrow n \in \underbrace{WF \wedge \exists m((n, m) \in Bev(T))}_{\Sigma_1}.$$

Hvis komplementet til  $Th(T)$  også er r.n. følger det, at  $Th(T)$  er rekursiv. Da  $T$  var antaget komplet har man

$$n \notin Th(T) \Leftrightarrow n \notin WF \vee \alpha_3(n, 0, 1) \in Th(T)$$

hvor  $\alpha_3(\#F, 0, 1) = \# \neg F$ . Men da man allerede ved fra eksempel 3.39 at  $Th(T)$  er uafgørlig, kan  $T$  ikke være komplet.  $\square$

Betingelsen  $P_0 \subseteq T$  er nødvendig for at sikre, at teorien er tilstrækkelig stærk til, at de rekursive funktioner kan repræsenteres i den.

Gödels første ufuldstændighedssætning siger intet om, hvad det er for wf'er, man ikke kan afgøre, og om disse overhovedet har nogen betydning. Den anden ufuldstændighedssætning, som kommer om lidt, giver svaret på dette.

**Lemma 3.49** *Hvis  $F$  er en lukket wf, som er  $\Sigma_1$  og  $T \supseteq P_0$  en rekursiv teori, da gælder*

$$P \vdash F \Rightarrow \exists y Bev_T[\#F, y]$$

**Bevis:** Se [Las94] p98 ff.

**Definition 3.50** *Funktionen  $Neg: \mathbb{N} \rightarrow \mathbb{N}$  er givet ved*

- hvis  $n$  er Gödelnummeret for en lukket wf  $F$ , så er  $Neg(n) = \alpha_3(n, 0, 1)$  dvs Gödelnummeret for  $\neg F$
- ellers er  $Neg(n) = 0$

$Neg$  er oplagt rekursiv. Lad  $\mathcal{N}eg[v_0, v_1]$  være en wf, som repræsenterer  $Neg$ . Betragt nu for  $T \supseteq P_0$  rekursiv:

$$Kons(T) = \neg \exists v_0 \exists v_1 \exists v_2 \exists v_3 (Bev_T[v_0, v_2] \wedge Bev_T[v_1, v_3] \wedge Neg[v_0, v_1])$$

$Kons(T)$  er en wf, som i det logiske system udtrykker konsistensen af en teori  $T$ .  $Kons(T)$  er netop et eksempel på en uafgørlig wf i  $T$ , idet

**Sætning 3.51 (Gödels 2. ufuldstændighedssætning)** *Lad  $T$  være en konsistent, rekursiv teori som indeholder  $P$ , da gælder  $T \not\vdash Kons(T)$*

**Bevis:** Bemærk først, at  $T \not\vdash \neg \text{Kons}(T)$ , for hvis det var tilfældet, at  $T \vdash \neg \text{Kons}(T)$  ville det betyde, at der fandtes en wf  $F$ , så  $T \vdash \exists v_0 \mathcal{B}ev_T[\#F, v_0]$  og  $T \vdash \exists v_1 \mathcal{B}ev_T[\#\neg F, v_1]$  og dermed  $\mathbb{N} \models \exists v_0 \mathcal{B}ev_T[\#F, v_0]$  og  $\mathbb{N} \models \exists v_1 \mathcal{B}ev_T[\#\neg F, v_1]$ , der findes altså  $n_1$  og  $n_2$  så  $(\#F, n_1) \in \text{B}ev(T)$  og  $(\#\neg F, n_2) \in \overline{\text{B}ev}(T)$  dvs  $T \vdash F$  og  $T \vdash \neg F$ , så  $T$  er inkonsistent.

Definer nu  $g : \mathbb{N} \rightarrow \mathbb{N}$

$$g(n) = \begin{cases} \#F[\underline{n}] & \text{hvis } n = \#F[v_0] \text{ hvor } F \text{ er en wf} \\ 0 & \text{ellers} \end{cases}$$

$g$  er rekursiv, så  $g$  repræsenteres af en wf  $\psi(v_0, v_1)$ . Det vil sige for alle  $n \in \mathbb{N}$ :

$$T \vdash \forall v_1 (\psi(\underline{n}, v_1) \Leftrightarrow v_1 = \underline{g(n)})$$

Betragt nu

$$\varepsilon(v_0) = \exists v_1 \exists v_2 (\mathcal{B}ev_T(v_1, v_2) \wedge \psi(v_0, v_1))$$

Bemærk, at hvis  $\#G[v_0] = n$  for en wf  $G[v_0]$  har man  $\mathbb{N} \models \varepsilon[\underline{n}]$  hvis og kun hvis  $G[\underline{n}]$  kan bevises i  $T$ , fordi  $\mathbb{N} \models \varepsilon[\underline{n}]$  betyder, at

$$\mathbb{N} \models \psi(\underline{n}, \underline{g(n)}) \wedge \exists v_2 \mathcal{B}ev_T[\underline{g(n)}, v_2]$$

og  $g(n) = \#G(\underline{n})$  så  $\mathbb{N} \models \exists v_2 \mathcal{B}ev_T[\#G[\underline{n}], v_2]$ . Hvis på den anden side  $\mathbb{N} \models \neg \varepsilon[\underline{n}]$  dvs

$$\mathbb{N} \models \forall v_1 \forall v_2 (\neg \mathcal{B}ev_T[v_1, v_2] \vee \neg \psi[\underline{n}, v_1])$$

Altså enten er  $v_1 \neq \#G[\underline{n}]$  eller også gælder for alle  $d \in \mathbb{N}$  at  $(\#G[\underline{n}], d) \notin \text{B}ev(T)$ .

Sæt  $\#\neg \varepsilon[v_0] = a$  og  $g(a) = b$ , husk at  $g(a) = \#\neg \varepsilon[\underline{a}]$ . Jævnfør ovenstående bemærkning, er

$$\mathbb{N} \models \varepsilon[\underline{a}] \Leftrightarrow \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1]$$

og da denne wf er  $\Sigma_1$

$$T \vdash \varepsilon[\underline{a}] \Leftrightarrow \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1]$$

Hvis man kan vise, at

$$\begin{cases} T \vdash \neg \varepsilon[\underline{a}] & (1) \\ T \vdash \text{Kons}(T) \Rightarrow \neg \varepsilon[\underline{a}] & (2) \end{cases}$$

følger det, at  $T \not\vdash \text{Kons}(T)$  da man ellers ville have  $T \not\vdash \neg \varepsilon[\underline{a}]$  og  $T \vdash \neg \varepsilon[\underline{a}]$  samtidigt. (1) Antag  $T \vdash \neg \varepsilon[\underline{a}]$  og lad  $c$  være Gödelnummeret for et bevis i  $T$  for  $\neg \varepsilon[\underline{a}]$ . Man har da  $(b, c) \in \text{B}ev(T)$  så  $T \vdash \mathcal{B}ev_T[\underline{b}, \underline{c}]$  og dermed  $T \vdash \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1]$  så da

$$T \vdash \varepsilon[\underline{a}] \Leftrightarrow \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1]$$

har man  $T \vdash \varepsilon[\underline{a}]$  hvilket strider mod konsistensen af  $T$ . (2) Det skal vises, at  $T \vdash \varepsilon[\underline{a}] \Rightarrow \neg \text{Kons}(T)$  Lad  $P' = P \cup \{\varepsilon[\underline{a}]\}$ . Da

$$P_0 \vdash \varepsilon[\underline{a}] \Leftrightarrow \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1]$$

fås

$$P' \vdash \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1] \quad (*)$$

$\varepsilon[\underline{a}]$  er en lukket wf som er  $\Sigma_1$ , så i følge lemma 3.49 gælder:

$$P \vdash \varepsilon[\underline{a}] \Rightarrow \exists v_2 \mathcal{B}ev_T[\underline{b}, \#\varepsilon[\underline{a}]]$$

sæt  $\#\varepsilon[\underline{a}] = d$ .

$$P' \vdash \exists v_2 \mathcal{B}ev_T[\underline{d}, v_2]$$

som sammen med (\*) giver

$$P' \vdash \exists v_1 \mathcal{B}ev_T[\underline{b}, v_1] \wedge \exists v_2 \mathcal{B}ev_T[\underline{d}, v_2] \wedge \mathcal{N}eg[\underline{b}, \underline{d}]$$

Altså  $P' \vdash \neg \text{Kons}(T)$  så per modus ponens

$$P \vdash \varepsilon[\underline{a}] \Rightarrow \neg \text{Kons}(T)$$

□

Man kan altså konkludere, at der findes mindst en model  $\mathcal{M}$  for  $P$  som opfylder  $\mathcal{M} \models \neg \text{Kons}(P)$  (konsekvens af fuldstændighedssætningen). Man har dog trods alt  $\mathbb{N} \models \text{Kons}(P)$  fordi hvis  $\mathbb{N} \models \neg \text{Kons}(P)$  ville man i følge korollar 3.24 have  $P \vdash \neg \text{Kons}(P)$  da  $\neg \text{Kons}(P)$  er  $\Sigma_1$ .

# Konklusion

Gödels første ufuldstændighedssætning har afsløret, hvor en af grænserne går for formelle systemers formåen. Ved et formelt eller logisk system forstås et system som fungerer helt mekanisk efter et på forhånd defineret regelsæt. Hvis man har en rekursiv teori kan man altså sætte en Turingmaskine til at regne på, hvorvidt en given wf er et teorem eller ej, men som en konsekvens af at  $Th(T)$  er uafgørlig, er det ikke til at vide, om maskinen vil standse eller ej. Hvis den standser har man et positivt svar: der fandtes et bevis, hvis den ikke er standset efter et stykke tid kan man ikke vide, om det er fordi den aldrig vil standse eller om man blot er for utålmodig. Turingmaskinen som undersøger for beviselighed har med andre ord et uafgørligt standsningsproblem.

Hvis man betragter beviset for den første ufuldstændighedssætning, ser man, at ethvert uafgørligt standsningsproblem (i.e. mængde som er r.n.) har ufuldstændighedssætningen som konsekvens.

Det er også værd at bemærke, at både for Turingmaskinen og for det logiske system, som bruges til at formalisere matematikken, er det selvreferencen der afslører systemets grænser. Altså når man beder systemet om at besvare et spørgsmål der omhandler systemet selv, kommer det til kort. Specielt er den wf,  $\varepsilon[\underline{a}]$  som bruges i beviset for Gödels 2. ufuldstændighedssætning, egentlig en udgave af løgnerparadokset, idet  $\varepsilon[\underline{a}]$  udtrykker “der findes et bevis for min negation”. Denne form for paradokser skabt af selvreference støder man ofte på i forskellige forklædninger. Mest kendt er nok Russells paradoks:

Lad  $x$  være mængden af alle de mængder  $y$  som opfylder  $y \notin y$ , da har man

$$x \in x \Leftrightarrow x \notin x$$

I den mængdelæren, som er et andet område i matematikken man har forsøgt at aksiomatisere, arbejdede man i første omgang med en inkonsistent teori. Det var Russells paradoks, der viste denne inkonsistens og konsekvensen var, at man måtte ændre i aksiomerne, så de nu ikke tillader den type mængder, som fører til Russells paradoks. Men om den nye teori er konsistent er stadig uvist. Det samme gælder i princippet for  $P$ , altså at man ikke kan være sikker på, at  $P$  er konsistent, måske har man bare ikke fundet et paradoks – endnu. På den anden side, hvis  $P$  var inkonsistent, så ville alle modellerne for  $P$ , heriblandt  $\mathbb{N}$  også være inkonsistente (i følge fuldstændighedssætningen). Det eneste argument man har imod  $\mathbb{N}$ 's inkonsistens er, at matematikere har arbejdet med modellen  $\mathbb{N}$  i flere tusinde år; men det er altså næsten et spørgsmål om tro! Dog kan man sige, at hvis man accepterede inkonsistente modeller, ville det være meningsløst at lave matematik, for da ville man kunne vise alt.

Vil man for alvor være formalist, må man altså i begyndelsen af hvert bevis skrive “under antagelse af, at matematikken er konsistent”.

# Bibliography

- [HR67] Jr. Hartley Rogers. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, 1967.
- [Las94] René Cori & Daniel Lascar. *Logique mathématique II*. Masson, 1994.
- [Men97] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman & Hall, fourth edition, 1997.