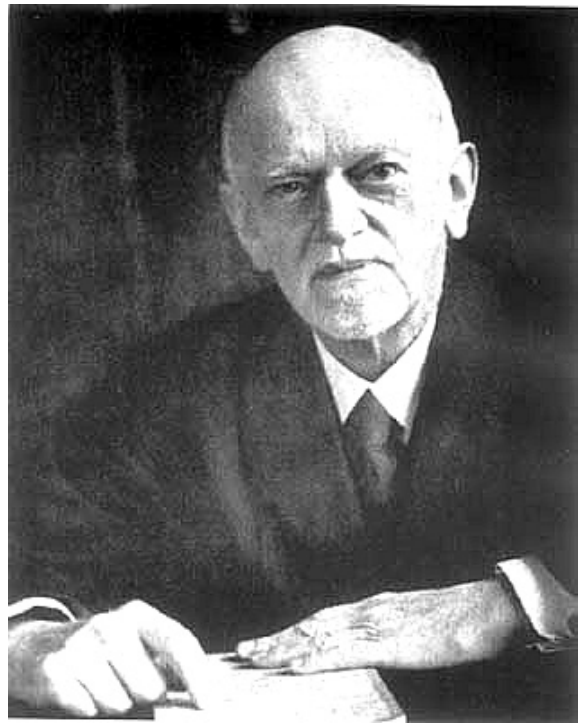
Teoretisk beregnelighed og Churchs tese

Klaus Frovin Jørgensen

Afdelingen for Filosofi og Videnskabsteori, RUC

Den 1. november 2011

David Hilbert
(23. jan., 1862 – 14. feb., 1943)



Hilberts foredrag i Paris år 1900

Hilbert udpegede 23 centrale uløste problemer i matematikken i foredraget *Matematiske problemer*:

1. Kontinuums hypotesen.
2. Konsistensen af de reelle tal.

⋮ ⋮

10. Eksistensen af en algoritme som afgører enhver diophantisk ligning.

⋮ ⋮

Diophantiske ligninger

En diophantisk ligning er en ligning med heltallige koefficienter. Løsningen skal også være heltallig. De diophantiske ligninger er opkaldt efter den græske matematiker Diophantus (levede omkring år 300 i Alexandria).

Eksempler på diophantiske ligninger:

$$ax + by = 1$$

$$x^n + y^n = z^n$$

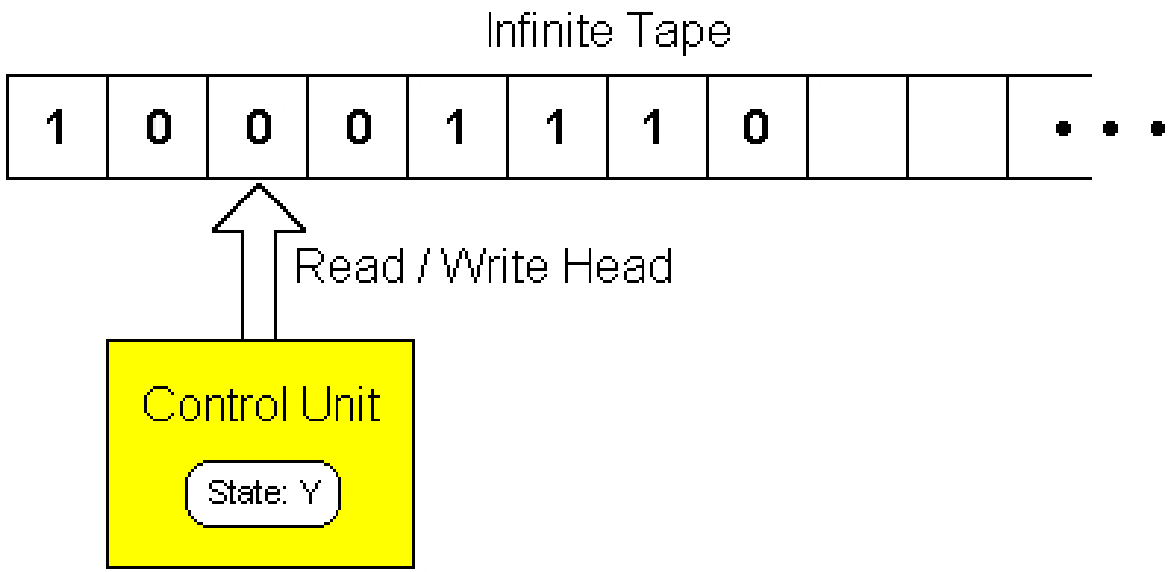
Så hvad er en algoritme?

“The father of computer science”?

Alan Turing
(1912-1954)

Turing-maskine (Turing, 1936)

- Et endeligt alfabet
- Et vilkårligt langt bånd, der kan læses og skrives på.
- Et endeligt antal instruktioner



Kleenes partielt rekursive funktioner

De partielt rekursive funktioner er funktioner fra natulige tal til naturlige tal. De kan beregnes ud fra følgende skemaer og sammensætninger heraf. Anvendelser

1. Der er initialfunktioner for 0, efterfølger og projektion.
2. Primitiv rekursion: Givet ψ, γ så har vi også:

$$\begin{aligned} \varphi(x,0) &\simeq \psi(x) \\ \varphi(x,y+1) &\simeq \gamma(x,y,\varphi(x,y)) \end{aligned}$$

3. μ-rekursion: Givet ψ we have

$$\varphi(x) \simeq \mu y(\forall z \leq y(\psi(x,z)\downarrow) \wedge \psi(x,y) \simeq 0).$$

Ackermann-funktionen

Antag $\varphi_1(a,b) = a + b$ og $\varphi_2(a,b) = a \cdot b$ samt at $\varphi_3(a,b) = a^b$. Lad ligeledes $\varphi_4(a,b)$ være det b-te element af følgen:

$$a, \quad a^a, \quad a^{(a^a)}, \quad a^{(a^{(a^a)})}, \ldots$$

Fortsæt en sådan iteration af φ_n. Derved får vi, at $\varphi_{n+1}(a,b)$ er en iteration af $\varphi_n(a,a)$ b gange.

Ackermann-funktionen $\varphi : \mathbf{N} \to \mathbf{N}$ er givet ved $\varphi_n(n,n)$.

$$\varphi(1) = 2, \qquad \varphi(2) = 4, \qquad \varphi(3) = 27, \qquad \varphi(4) = 4^{4294967296}.$$

Funktionen er ikke primitivt rekursiv (da den majoriserer alle primitivt rekursive funktioner), men den er generelt rekursiv.

Churchs tese

Der er givet forskellige forsøg på at karakterisere klassen af algoritmer (dvs. beregnelige funktioner). Ved:

- Turing-maskiner
- Kleene-skemaer
- Register-maskiner
- Lambda-kalkyle
- Post-algortimer
- Programmeringssprog (C, f.eks.)

Der kan gives et matematisk bevis for, at disse klasser af funktioner er sammenfaldende.

Churchs tese – som ikke er en matematisk sætning – siger, at vi med eksempelvis de Turing-beregnelige funktioner har *alle* beregnelige funktioner. Altså, at begrebet om en generel rekursiv funktion karakteriserer begrebet om algoritme.

Hilberts tiende problem

"10. Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers." (Hilbert, 1900)

I 1973 viser Yuri Matiyasevich, at der ikke findes nogen algoritme, som løser Hilbert's tiende problem

Hilbert ville være blevet overrasket!

Mod videre anvendelser af algoritme-begrebet

Logiske teorier

En logisk teori består almindeligvist af

1. Fastlæggelsen af et formelt sprog,
2. En mængde af aksiomer/grundantagelser,
3. En samling af slutningsregler.

På baggrund heraf kan man *bevise* udsagn i et sprog.

En simpel logisk teori T

Som et eksempel på en *logisk teori* kan vi tage teorien T bestående af følgende grundantagelser:

1. $A \to (B \to A)$.
2. $(\neg A \to B) \to ((\neg A \to \neg B) \to A)$

T har en slutningsregel, som hedder modus ponens:

$$\frac{A \qquad A \to B}{B}$$

Et eksempel på et bevis i T

I T kan vi bevise forskellige ting, eksempelvis at fra A og $A \to B$ og $B \to C$, følger C:

$$\dfrac{\dfrac{A \quad A \to B}{B} \qquad B \to C}{C}$$

Det vil sige,

$$A, A \to B, B \to C \text{ beviser } C.$$

Et andet eksempel

$$\dfrac{\dfrac{\neg B \quad \neg B \to (\neg A \to \neg B)}{\neg A \to \neg B} \qquad \dfrac{\dfrac{B \quad B \to (\neg A \to B)}{\neg A \to B} \qquad (\neg A \to B) \to \Big((\neg A \to \neg B) \to A\Big)}{(\neg A \to \neg B) \to A}}{A}$$

Vores teori siger altså at, hvis vi har en modstrid, det vil sige både B og $\neg B$, så følger hvad som helst, A. Det vil sige:

$B, \neg B$ beviser A.

Aksiomer for Peano-aritmetik

Teorien formuleret i førsteordenssproget med symbolerne $0, S, +, \cdot$ vil vi kalde for PA. Den baserer sig på aksiomerne for den klassiske førsteordenslogik samt følgende aksiomer:

1. $\forall x(0 \neq Sx)$.
2. $\forall x \forall y((Sx = Sy) \rightarrow (x = y))$.
3. $\forall x(x + 0 = x)$.
4. $\forall x \forall y(x + Sy = S(x + y))$.
5. $\forall x(x \cdot 0 = 0)$.
6. $\forall x \forall y(x \cdot Sy = (x \cdot y) + x)$.
7. *For enhver formel* $A(x)$ *formuleret i sproget* $\mathcal{L}(+, \cdot, S, 0)$ *gælder*

$$A(0) \wedge \forall x(A(x) \rightarrow A(Sx)) \rightarrow \forall x A(x).$$

Selvreference; uafgørbarhed (1/2)

Lad PA være den formelle teori for Peano artimetikken, som vi *antager* er konsistent; De primitive rekursive funktioner (det vil sige, de funktioner som kan beregnes ud fra en simpel algoritme) kan repræsenteres i PA. Og da PAs sprog er tælleligt kan vi nummerere PAs formler: $A_1, \ldots, A_n, \ldots$. Hvis en formel A_i kan bevises i PA skriver vi dette på følgende måde:

$$\mathrm{PA} \vdash A_i.$$

Sætning (Church 1936). Bevisbarhed i PA er uafgørbart.

Antag, at der findes en rekursiv funktion ψ, som afgører for en hvilken som helst formel i PA uden frie variable, om den er beviselig eller ej:

$$\begin{aligned} \mathrm{PA} \vdash A_x &\quad\Rightarrow\quad \mathrm{PA} \vdash \psi(\bar{x}) = 0 \\ \mathrm{PA} \nvdash A_x &\quad\Rightarrow\quad \mathrm{PA} \vdash \psi(\bar{x}) = 1 \end{aligned}$$

Selvreference; uafgørbarhed (2/2)

Lad A_x antage sin egen ubeviselighed, det vil sige

$$\mathsf{PA} \vdash A_x \leftrightarrow \psi(\bar{x}) = 1.$$

Heraf følger

$$\mathsf{PA} \vdash A_x \Rightarrow \mathsf{PA} \vdash \psi(\bar{x}) = 0 \Rightarrow \mathsf{PA} \nvdash A_x$$

På den anden side har vi:

$$\mathsf{PA} \nvdash A_x \Rightarrow \mathsf{PA} \vdash \psi(\bar{x}) = 1 \Rightarrow \mathsf{PA} \vdash A_x.$$

Det følger altså, at der ikke kan eksistere en sådan ψ.

Hermed en negativ løsning til Hilberts såkaldte *Entscheidungsproblem*.

Hvad skal vi mene om disse resultater?

1. Church's Sætning. Logisk bevisbarhed er ikke afgørbart.
2. Tarskis Sætning. Sprog der bla. omhandler de naturlige tal besidder ikke et prædikat for sandhed.
3. Gödels Ufuldstændighedssætninger. Ovenstående sprog er også syntaktisk ufuldstændige og kan ikke bevise, at de er konsistente.
4. Löwenheim-Skolems Sætning. Hvis et sprog har en uendelig model, så har den modeller i alle mulige uendelige størrelser.

Var bevisteorien færdig?

Hilberts program

Den aksiomatiske metode har flere funktioner. En meget vigtig er at give en garanti for rimeligheden af indførte ideal-elementer.

Program (David Hilbert):

- Angiv *formelle* systemer, som modsvarer matematiske teorier indeholdende ideal-elementer.
- Vis, at *repræsentationen* er korrekt.
- Bevis konsistens af de formelle systemer ved brug af helt elementære metoder fra matematikkens endelige kerne.

Gerhard Gentzen (1909-1945)

På trods af Gödels ufuldstændigheds-sætninger beviste Gentzen – elev af Bernays og assistent til Hilbert – konsistensen af PA i 1936.