

INF2080 – Logikk og beregninger

Forelesning 24: Store tall og lange bevis



UiO **I**nstitut for informatikk

Sist oppdatert: 2012-04-16 20:34

24.1 Store tall og lange bevis

Operasjoner på tall

Addisjon



Multiplikasjon

Eksponasiering Kan ikke visualiseres — må tenkes som en prosess

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \dots + m}_n$
- $m \uparrow n = \underbrace{m \times m \times \dots \times m}_n$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \dots \uparrow m}_n$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \dots \uparrow\uparrow m}_n$
- ...
- Assosiering — den vonde veien
- $3 \uparrow (3 \uparrow 3) = 3^{27} = 7625597484987$
- $(3 \uparrow 3) \uparrow 3 = 27^3 = 19683$

Sekvensen $1 \uparrow 1$, $2 \uparrow\uparrow 2$, $3 \uparrow\uparrow\uparrow 3$, ... kalles Ackermann sekvensen. Den vokser raskere enn en hvilken som helst funksjon definert ved iterasjon (primitiv rekursiv funksjon) — men beverfunksjonen vokser mye raskere.

Unære tall

- Null 0
- Etterfølger s
- Funksjonsymboler
- Predikat Nx — x er et tall
- Første ordens logikk med likhet
- Aksiom NUM — $N0 \wedge \forall x(Nx \rightarrow Nsx)$
- Addisjon og multiplikasjon

$$\begin{aligned} +0y &= y \\ +sxy &= s + xy \\ *0y &= 0 \\ *sxy &= +y * xy \end{aligned}$$

Notasjoner over unære tall

- Polsk skrivemåte — prefiks uten parenteser
- Notasjon — samling med likninger
 - Sunn — om den kan tolkes i vanlige tall
 - Komplette — om vi kan utlede alle atomære setninger
- Notasjon for eksponensiering
 - Binært funksjonssymbol e
 - Likninger \mathcal{E} :

$$\begin{aligned} e0y &= sy \\ esxy &= exexy \end{aligned}$$

- Kan tolke exy som $2^x + y$
- \mathcal{E} er sunn og komplett
- $eeeeee000000 = 2^{2^{16}}$ — større enn atomer i universet

Lange bevis

- La \mathcal{R} være notasjonslikninger for symbolene i termen t
- Vis: $\text{NUM} \wedge \mathcal{R} \rightarrow Nt$
- Et analysetre bryter dette ned i
 - $N0$
 - instanser av $\forall x.(Nx \rightarrow Nsx)$
 - instanser av likningene \mathcal{R}
- Anta at vi har utledning av D av $\text{NUM} \wedge \mathcal{R} \rightarrow Nt$
- Denne utledningen må være lengre enn størrelsen på t
- For $t = eeeeeee0000000$ er utledningen større enn universet

Indirekte bevis

•

$$\begin{aligned} N_0x &= Nx \\ N_{n+1}x &= \forall y : N_n \cdot exy : N_n \end{aligned}$$

- $\forall y : N_n \cdot exy : N_n$ forkorter $\forall y.(N_n y \rightarrow N_n exy)$
- For alle $n : \text{NUM} \wedge \mathcal{E} \rightarrow N_n 0$
 - Opplagt for $n = 0$ og $n = 1$
 - Anta NUM og \mathcal{E}
 - Anta at vi har y med $N_{n+1}y$ — dvs $\forall z : N_n \cdot eyz : N_n$
 - Sett inn eyz for z og anvend utsagnet to ganger
 - Vi får $\forall z : N_n \cdot eyeyz : N_n$
 - Dvs $N_{n+1}sy$
 - Og $\forall y : N_{n+1}.sy : N_{n+1}$
 - Dette gir $N_{n+2}0$

Kort indirekte bevis

- Anta NUM og ε
- Fra N_60 og N_50 : N_5e00
- Fra N_5e00 og N_40 : N_4ee000
- Fra N_4ee000 og N_30 : $N_3eee0000$
- Fra $N_3eee0000$ og N_20 : $N_2eeee00000$
- Fra $N_2eeee00000$ og N_10 : $N_1eeeeee000000$
- Fra $N_1eeeeee000000$ og N_00 : $N_0eeeeeee0000000$
- Dermed $\text{NUM} \wedge \varepsilon \rightarrow \text{Neeeeee0000000}$

Selve beviset kan formuleres kort i vårt system om vi tillater følgende (overflødige) regel — kalt snitt

$$\frac{\Gamma, F \quad \Gamma, \neg F}{\Gamma}$$

Ødelegger automatisering av bevis — gjette på F

Fire viktige lærdommer

- Signatur
- Syntaks maskiner
- Ikke determinisme og beslutningstrær
- Dybde først søk i trær