INF2080 – Logikk og beregninger

Forelesning 24: Store tall og lange bevis

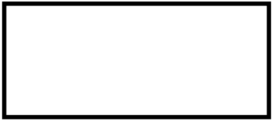
UiO : Institutt for informatikk

Sist oppdatert: 2012-04-16 20:34

24.1 Store tall og lange bevis

Operasjoner på tall

Addisjon 


Multiplikasjon

Eksponensiering Kan ikke visualiseres — må tenkes som en prosess

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \cdots \uparrow\uparrow m}_{n}$
- ...
- Assosiering — den vonde veien
- $$\begin{array}{rcl} 3 \uparrow (3 \uparrow 3) & = & 3^{27} = 7625597484987 \\ (3 \uparrow 3) \uparrow 3 & = & 27^{3} = 19683 \end{array}$$

Sekvensen $1 \uparrow 1$, $2 \uparrow\uparrow 2$, $3 \uparrow\uparrow\uparrow 3$, $\cdots$ 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 — $N0 \wedge \forall x(Nx \to Nsx)$
- 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
  - Komplett — 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
- $eeeeee0000000 = 2^{2^{16}}$ — større enn atomer i universet

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen $\mathtt{t}$
- Vis: $\mathrm{NUM} \wedge \mathcal{R} \rightarrow \mathtt{Nt}$
- Et analysetre bryter dette ned i
  - $\mathtt{N0}$
  - instanser av $\forall x.(\mathtt{N}x \rightarrow \mathtt{Ns}x)$
  - instanser av likningene $\mathcal{R}$
- Anta at vi har utledning av D av $\mathrm{NUM} \wedge \mathcal{R} \rightarrow \mathtt{Nt}$
- Denne utledningen må være lengre enn størrelsen på $\mathtt{t}$
- For $\mathtt{t} = eeeeee\mathtt{000000}$ er utledningen større enn universet

Indirekte bevis

- $$\begin{aligned} N_0 x &= Nx \\ N_{n+1} x &= \forall y : N_n \cdot exy : N_n \end{aligned}$$
- $\forall y : N_n \cdot exy : N_n$ forkorter $\forall y.(N_n y \to N_n exy)$
- For alle n : NUM $\wedge\, \mathcal{E} \to N_n 0$
  - 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 $\mathcal{E}$
- Fra $\mathsf{N}_6\mathsf{0}$ og $\mathsf{N}_5\mathsf{0}$: $\mathsf{N}_5\mathsf{e00}$
- Fra $\mathsf{N}_5\mathsf{e00}$ og $\mathsf{N}_4\mathsf{0}$: $\mathsf{N}_4\mathsf{ee000}$
- Fra $\mathsf{N}_4\mathsf{ee000}$ og $\mathsf{N}_3\mathsf{0}$: $\mathsf{N}_3\mathsf{eee0000}$
- Fra $\mathsf{N}_3\mathsf{eee0000}$ og $\mathsf{N}_2\mathsf{0}$: $\mathsf{N}_2\mathsf{eeee00000}$
- Fra $\mathsf{N}_2\mathsf{eeee00000}$ og $\mathsf{N}_1\mathsf{0}$: $\mathsf{N}_1\mathsf{eeeee000000}$
- Fra $\mathsf{N}_1\mathsf{eeeee000000}$ og $\mathsf{N}_0\mathsf{0}$: $\mathsf{N}_0\mathsf{eeeeee0000000}$
- Dermed NUM $\wedge\, \mathcal{E} \rightarrow \mathsf{Neeeeee0000000}$

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

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

Ødelegger automatisering av bevis — gjette på F

Fire viktige lærdommer

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