INF2080 – Logikk og beregninger

Forelesning 24: Store tall og lange bevis

UiO : Institutt for informatikk

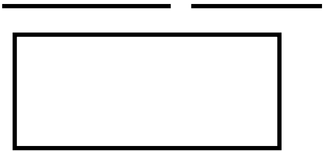
Sist oppdatert: 2012-04-16 20:33

24.1 Store tall og lange bevis

Operasjoner på tall

Operasjoner på tall

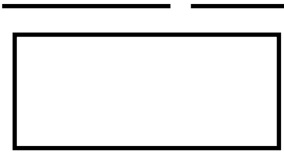
Addisjon



Multiplikasjon

Operasjoner på tall

Addisjon



Multiplikasjon

Eksponensiering Kan ikke visualiseres — må tenkes som en prosess

Knuths pil-notasjon

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \cdots \uparrow\uparrow m}_{n}$

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \cdots \uparrow\uparrow m}_{n}$
- $\ldots$

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \cdots \uparrow\uparrow m}_{n}$
- $\ldots$
- Assosiering — den vonde veien

Knuths pil-notasjon

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

Knuths pil-notasjon

- $m \times n = \underbrace{m + m + \cdots + m}_{n}$
- $m \uparrow n = \underbrace{m \times m \times \cdots \times m}_{n}$
- $m \uparrow\uparrow n = \underbrace{m \uparrow m \uparrow \cdots \uparrow m}_{n}$
- $m \uparrow\uparrow\uparrow n = \underbrace{m \uparrow\uparrow m \uparrow\uparrow \cdots \uparrow\uparrow m}_{n}$
- $\ldots$
- 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

Unære tall

- Null 0

Unære tall

- Null 0
- Etterfølger s

Unære tall

- Null 0
- Etterfølger s
- Funksjonsymboler

Unære tall

- Null 0
- Etterfølger s
- Funksjonsymboler
- Predikat Nx — x er et tall

Unære tall

- Null 0
- Etterfølger s
- Funksjonsymboler
- Predikat Nx — x er et tall
- Første ordens logikk med likhet

Unære tall

- Null 0
- Etterfølger s
- Funksjonsymboler
- Predikat Nx — x er et tall
- Første ordens logikk med likhet
- Aksiom NUM — $N0 \land \forall x(Nx \to Nsx)$

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

Notasjoner over unære tall

- Polsk skrivemåte — prefiks uten parenteser

Notasjoner over unære tall

- Polsk skrivemåte — prefiks uten parenteser
- Notasjon — samling med likninger

Notasjoner over unære tall

- Polsk skrivemåte — prefiks uten parenteser
- Notasjon — samling med likninger
  - Sunn — om den kan tolkes i vanlige tall

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

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

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

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 $\mathcal{E}$:

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

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 $2^x + y$

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

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

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: $\mathrm{NUM} \land \mathcal{R} \to \mathrm{N}\,\mathrm{t}$

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen $\mathtt{t}$
- Vis: $\mathrm{NUM} \wedge \mathcal{R} \to \mathrm{N}\mathtt{t}$
- Et analysetre bryter dette ned i

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: NUM $\wedge\, \mathcal{R} \to \mathsf{Nt}$
- Et analysetre bryter dette ned i
    - $\mathsf{N0}$

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: $\mathrm{NUM} \wedge \mathcal{R} \to \mathrm{N}t$
- Et analysetre bryter dette ned i
  - $\mathrm{N}0$
  - instanser av $\forall x.(\mathrm{N}x \to \mathrm{N}sx)$

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: $\mathsf{NUM} \wedge \mathcal{R} \to Nt$
- Et analysetre bryter dette ned i
  - $N0$
  - instanser av $\forall x.(Nx \to Nsx)$
  - instanser av likningene $\mathcal{R}$

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: $\mathrm{NUM} \land \mathcal{R} \to \mathsf{N}t$
- Et analysetre bryter dette ned i
  - $\mathsf{N}0$
  - instanser av $\forall x.(\mathsf{N}x \to \mathsf{N}sx)$
  - instanser av likningene $\mathcal{R}$
- Anta at vi har utledning av D av $\mathrm{NUM} \land \mathcal{R} \to \mathsf{N}t$

Lange bevis

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

Lange bevis

- La $\mathcal{R}$ være notasjonslikninger for symbolene i termen t
- Vis: $\mathsf{NUM} \wedge \mathcal{R} \rightarrow Nt$
- 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 $\mathsf{NUM} \wedge \mathcal{R} \rightarrow Nt$
- Denne utledningen må være lengre enn størrelsen på t
- For $t = eeeeee0000000$ er utledningen større enn universet

Indirekte bevis

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 $\forall y.(N_n y \rightarrow N_n exy)$

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 $\forall y.(N_n y \rightarrow N_n exy)$
- For alle n : NUM $\wedge\ \mathcal{E} \rightarrow N_n 0$

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 $n = 1$

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 : $\mathrm{NUM} \wedge \mathcal{E} \to N_n 0$
  - Opplagt for $n = 0$ og $n = 1$
  - Anta NUM og $\mathcal{E}$

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 : $\mathrm{NUM} \wedge \mathcal{E} \to N_n 0$
  - Opplagt for $n = 0$ og $n = 1$
  - Anta NUM og $\mathcal{E}$
  - Anta at vi har y med $N_{n+1} y$ — dvs $\forall z : N_n \cdot eyz : N_n$

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 $\forall y.(N_n y \rightarrow N_n exy)$
- For alle $n : \mathrm{NUM} \wedge \mathcal{E} \rightarrow N_n 0$
    - 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

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 $\forall z : N_n \cdot eyeyz : N_n$

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 $\forall y.(N_n y \rightarrow N_n exy)$
- For alle n : 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 $N_{n+1} sy$

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 $n : \mathrm{NUM} \wedge \mathcal{E} \to N_n 0$
  - 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 $\forall y : N_{n+1}.sy : N_{n+1}$

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 : $\mathrm{NUM} \wedge \mathcal{E} \to N_n 0$
    - 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

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $\mathsf{N}_6 0$ og $\mathsf{N}_5 0$: $\mathsf{N}_5 e00$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$
- Fra $N_4 ee000$ og $N_3 0$: $N_3 eee0000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$
- Fra $N_4 ee000$ og $N_3 0$: $N_3 eee0000$
- Fra $N_3 eee0000$ og $N_2 0$: $N_2 eeee00000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$
- Fra $N_4 ee000$ og $N_3 0$: $N_3 eee0000$
- Fra $N_3 eee0000$ og $N_2 0$: $N_2 eeee00000$
- Fra $N_2 eeee00000$ og $N_1 0$: $N_1 eeeee000000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$
- Fra $N_4 ee000$ og $N_3 0$: $N_3 eee0000$
- Fra $N_3 eee0000$ og $N_2 0$: $N_2 eeee00000$
- Fra $N_2 eeee00000$ og $N_1 0$: $N_1 eeeee000000$
- Fra $N_1 eeeee000000$ og $N_0 0$: $N_0 eeeeee0000000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $\mathrm{N}_6 0$ og $\mathrm{N}_5 0$: $\mathrm{N}_5 e00$
- Fra $\mathrm{N}_5 e00$ og $\mathrm{N}_4 0$: $\mathrm{N}_4 ee000$
- Fra $\mathrm{N}_4 ee000$ og $\mathrm{N}_3 0$: $\mathrm{N}_3 eee0000$
- Fra $\mathrm{N}_3 eee0000$ og $\mathrm{N}_2 0$: $\mathrm{N}_2 eeee00000$
- Fra $\mathrm{N}_2 eeee00000$ og $\mathrm{N}_1 0$: $\mathrm{N}_1 eeeee000000$
- Fra $\mathrm{N}_1 eeeee000000$ og $\mathrm{N}_0 0$: $\mathrm{N}_0 eeeeee0000000$
- Dermed NUM $\wedge\, \mathcal{E} \rightarrow \mathrm{N} eeeeee0000000$

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $N_6 0$ og $N_5 0$: $N_5 e00$
- Fra $N_5 e00$ og $N_4 0$: $N_4 ee000$
- Fra $N_4 ee000$ og $N_3 0$: $N_3 eee0000$
- Fra $N_3 eee0000$ og $N_2 0$: $N_2 eeee00000$
- Fra $N_2 eeee00000$ og $N_1 0$: $N_1 eeeee000000$
- Fra $N_1 eeeee000000$ og $N_0 0$: $N_0 eeeeee0000000$
- Dermed $\mathrm{NUM} \wedge \mathcal{E} \rightarrow Neeeeee0000000$

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

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

Kort indirekte bevis

- Anta NUM og $\mathcal{E}$
- Fra $\mathsf{N}_6 0$ og $\mathsf{N}_5 0$: $\mathsf{N}_5 e00$
- Fra $\mathsf{N}_5 e00$ og $\mathsf{N}_4 0$: $\mathsf{N}_4 ee000$
- Fra $\mathsf{N}_4 ee000$ og $\mathsf{N}_3 0$: $\mathsf{N}_3 eee0000$
- Fra $\mathsf{N}_3 eee0000$ og $\mathsf{N}_2 0$: $\mathsf{N}_2 eeee00000$
- Fra $\mathsf{N}_2 eeee00000$ og $\mathsf{N}_1 0$: $\mathsf{N}_1 eeeee000000$
- Fra $\mathsf{N}_1 eeeee000000$ og $\mathsf{N}_0 0$: $\mathsf{N}_0 eeeeee0000000$
- Dermed NUM $\wedge\, \mathcal{E} \to \mathsf{N}eeeeee0000000$

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

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

Ødelegger automatisering av bevis — gjette på F

Fire viktige lærdommer

Fire viktige lærdommer

- Signatur
- Syntaks maskiner

Fire viktige lærdommer

- Signatur
- Syntaks maskiner
- Ikke determinisme og beslutningstrær

Fire viktige lærdommer

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