

Sidste gang:

Indledende kvantorer (afsnit 1.5)

Kvantorenes orden

$$\Downarrow \begin{array}{l} \exists x : \forall y : P(x, y) \\ \forall y : \exists x : P(x, y) \end{array}$$

$$\Uparrow \forall x \in \mathbb{Z} : \forall y \in \mathbb{Z} : (x > y \Rightarrow 2x > 2y)$$

$$\Uparrow \forall y \in \mathbb{Z} : \forall x \in \mathbb{Z} : (x > y \Rightarrow 2x > 2y)$$

$$\Uparrow \forall x, y \in \mathbb{Z} : (x > y \Rightarrow 2x > 2y)$$

Sidste omskrivning er gyldig, da x og y har samme univers.

$$\forall x : \exists y : \forall z : P(x, y, z)$$

$$\times \forall z : \exists y : \forall x : P(x, y, z)$$

Negering

$$\neg \exists x \in \mathbb{Z} : \forall y \in \mathbb{Z} : x + y = 0$$

$$\Uparrow \forall x \in \mathbb{Z} : \neg \forall y \in \mathbb{Z} : x + y = 0, \text{ ifølge De Morgan}$$

$$\Uparrow \forall x \in \mathbb{Z} : \exists y \in \mathbb{Z} : x + y \neq 0, \text{ ifølge De Morgan}$$

Bevismetoder (afsnit 1.7)

Direkte bevis

Benyt, at $(p \Rightarrow p_1 \Rightarrow p_2 \dots \Rightarrow p_n \Rightarrow q) \Rightarrow (p \Rightarrow q)$

n ulige $\nearrow$ $\exists k \in \mathbb{Z}: n = 2k+1$ $\nearrow$ $\exists k \in \mathbb{Z}: n^2 = 4k^2 + 4k + 1$ $\nearrow$ $\exists k \in \mathbb{Z}: n^2 = 2(2k^2 + 2k) + 1$ $\nearrow$ n^2 ulige

Kontrapositions bevis

Benyt, at $p \Rightarrow q \Leftrightarrow \neg q \Rightarrow \neg p$

n^2 ulige $\nearrow$ p $\nwarrow$ n ulige $\nwarrow$ q $\nwarrow$ n lige $\nwarrow$ $\neg q$ $\nwarrow$ n^2 lige $\nwarrow$ $\neg p$

Modstridsbevis

Benyt, at $(\neg p \Rightarrow F) \Rightarrow p$

$\exists$  : $c > a+b$ $\nearrow$ $\neg p$ $\nwarrow$ $\exists$  : $c^2 > a^2 + b^2$ $\nwarrow$ F $\nwarrow$ $\neg p \Rightarrow F$ $\nwarrow$ p

$\neg \exists$ uge med ≥ 2 fødselsdage ≤ 52 personer $\nwarrow$ $\exists$ uge med ≥ 2 fødselsdage $\nwarrow$ p

$\forall$  : $c \leq a+b$ $\nwarrow$ p

Bevis-strategier (afsnit 1.8)

Split op i delresultater / specialtilfælde

1 dag

Flere bevis-strategier

Bla.a.: Lær af simple special-tilfælde

Induktionsbeviser (afsnit 5.1)

"Eks 1.8.18":

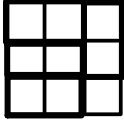
Lad $n \in \{2, 3, 4, \dots\}$

Kan et $n \times n$ skakbræt dækkes af dominobrikker,
som hver dækker to felter?

Ingen brikker må overlappe eller stikke ud over kanten.

Start evt. med simple specialtilfælde for at opnå
forståelse:

$n=2$:  ja

$n=3$:  Nej

Generelt:

n lige: ja, for man kan dække hver række
med $n/2$ brikker.

n ulige: Nej, fordi:

- Brikkerne dækker tilsammen et lige #felter
- Der er n^2 felter.

D.v.s. et ulige #felter, ifølge Eks 1.7.1.

Konstruktiv eksistensbevis:

Vi beviser at der findes en gyldig dækning af
brættet ved at beskrive en konkret dækning.

Eks: Har $f(x) = x^4 - x^2 - 1$ et nulpunkt?

Ja, fordi $f(0) = -1 < 0$ og $f(2) = 16 - 4 - 1 = 11 > 0$

Da f er kontinuert, må der dermed findes et x , $-1 < x < 2$, sådan at $f(x) = 0$.

Ikke-konstruktiv eksistensbevis:

Vi har ikke fundet 0-punktet, men vi har bevist, at det eksisterer.

Tilbage til skakbrætter, dominobrikker og "tricks"...

Eks: $n \times n$ skakbræt

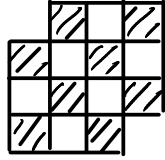
Fjern to modstående hjørner

Kan brættet dækkes af dominobrikker?

n ulige: **Nej**, da $n-2$ er ulige.

n lige: Først simple specialtilfælde:

$n=2$:  **Nej**

$n=4$:  **Nej**, for der er 8 sorte felter og 6 hvide, men dominobrikker dækker lige mange sorte og hvide felter

Generelt: **Nej**, for de to fjernede felter har samme farve, da alle felter på diagonalen har samme farve. D.v.s. der er **ikke lige mange hvide og sorte felter**. (Det gælder også for n ulige, så vi behøvede ikke at splitte op i to tilfælde, lige/ulige.)

Uden at have tegnet brættet havde vi måske ikke tænkt over, at de to fjernede felter havde samme farve.

Lidt terminologi:

Sætning (theorem): Vigtigt udsagn
(som er bevist at være sandt - ellers
er det bare en **påstand** (conjecture)).
D.v.s. et udsagn, man ofte refererer til.

Lemma: Hjælpesætning
Bruges til at strukturere et langt bevis

Korollar: Følgesætning
Udsagn, som følger umiddelbart af en sætning

Induktion

(Afsnit 5.1)

I denne uge i DMS34 kommer datalogerne til at se, hvordan induktion bruges til at bevise korrekthed af algoritmer. Både dataloger og SE-ingeniører kommer til at se det i foråret.

Først recap af potensregne regler:

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 2 \cdot 2 = 4$$

$$2^3 = 2 \cdot 2 \cdot 2 = 2 \cdot 2^2 = 8$$

$$2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 2 \cdot 2^3 = 2^2 \cdot 2^2 = 16$$

Generelt:

$$2^k \cdot 2^l = 2^{k+l}$$

Vi kommer til at bruge følgende special-tilfælde:

$$2 \cdot 2^n = 2^{n+1}$$

Induktionsbeviser bruges til at bevise
parametriserede udsagn:

Eks 3:

$$\underbrace{2^0 + 2^1 + \dots + 2^n}_{P(n)} = 2^{n+1} - 1, \text{ for alle } n \in \mathbb{N}$$

$$P(0): \underbrace{2^0}_{=1} = \underbrace{2^1 - 1}_{2-1=1} \quad S \quad \left. \vphantom{\begin{matrix} P(0) \\ P(1) \\ P(2) \end{matrix}} \right\} \text{Basis-tilfælde}$$

$$P(1): \underbrace{2^0 + 2^1}_{1+2=3} = \underbrace{2^2 - 1}_{4-1=3} \quad S$$

$$P(2): \underbrace{2^0 + 2^1 + 2^2}_{1+2+4=7} = \underbrace{2^3 - 1}_{8-1=7} \quad S$$

$$\underbrace{2^3 - 1}_{\text{ifølge } P(2)}$$

$$P(3): \underbrace{2^0 + 2^1 + 2^2 + 2^3}_{2^3 - 1 + 2^3} = 2^4 - 1 \quad S$$
$$2^3 - 1 + 2^3 = 2 \cdot 2^3 - 1 = 2^4 - 1$$

Vi kan bruge $P(k-1)$ til at verificere $P(k)$.

F.eks.:

$k=1$:

$$\begin{aligned} 2^0 &= 2^1 - 1 && P(0) \\ \Downarrow \\ 2^0 + 2^1 &= 2^1 - 1 + 2^1 = 2 \cdot 2^1 - 1 = 2^2 - 1 && \Downarrow P(1) \end{aligned}$$

$k=2$:

$$\begin{aligned} 2^0 + 2^1 &= 2^2 - 1 && P(1) \\ \Downarrow \\ 2^0 + 2^1 + 2^2 &= 2^2 - 1 + 2^2 = 2 \cdot 2^2 - 1 = 2^3 - 1 && \Downarrow P(2) \end{aligned}$$

$k=3$:

$$\begin{aligned} 2^0 + 2^1 + 2^2 &= 2^3 - 1 && P(2) \\ \Downarrow \\ 2^0 + 2^1 + 2^2 + 2^3 &= 2^3 - 1 + 2^3 = 2 \cdot 2^3 - 1 = 2^4 - 1 && \Downarrow P(3) \end{aligned}$$

Mer generelt:

Induktionsantagelse ($P(k-1)$)

Hvis vi ved, at $2^0 + 2^1 + \dots + 2^{k-1} = 2^k - 1$,

kan vi udlede følgende:

$$\left. \begin{aligned} &2^0 + 2^1 + \dots + 2^{k-1} = 2^k - 1 \\ \Updownarrow \\ &2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2^k - 1 + 2^k \\ \Updownarrow \\ &2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2 \cdot 2^k - 1 \\ \Updownarrow \\ &2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2^{k+1} - 1 \end{aligned} \right\} \text{Induktionsstredt}$$

$P(k)$

Induktionsbevis:

Basistilfælde: Bevis $P(0)$

Ind. skridt: $\forall k \in \mathbb{Z}^+ : \underbrace{(P(k-1) \Rightarrow P(k))}_{\text{Ind. ant.}}$

Basis: $P(0)$

Ind. skridt:

$$k=1: P(0) \Rightarrow P(1)$$

$$k=2: P(1) \Rightarrow P(2)$$

$$k=3: P(2) \Rightarrow P(3)$$

$\vdots$

„Domino-effekt“:

$$P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \dots$$

$2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1, \text{ for alle } n \in \mathbb{N}$

Bevis:

Basis ($n=0$): $2^0 = 1 = 2^1 - 1.$

$P(0)$

Ind. ant.: $2^0 + 2^1 + \dots + 2^{k-1} = 2^k - 1$

Ind. skridt: For $k \geq 1$ gælder:

$$2^0 + 2^1 + \dots + 2^{k-1} = 2^k - 1 \quad (\text{ind. ant.})$$

$P(k-1)$

$$\Downarrow 2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2^k - 1 + 2^k$$

$$\Updownarrow 2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2 \cdot 2^k - 1$$

$\Downarrow$

$$\Updownarrow 2^0 + 2^1 + \dots + 2^{k-1} + 2^k = 2^{k+1} - 1$$

$P(k)$

□

Simpel induktion:

Bevis $P(n)$, for alle $n \geq m$

Basis: Bevis $P(m)$

Induktionsantagelse

Induktionsskridt: Bevis, at $P(k) \Rightarrow P(k+1)$,
for alle $k \geq m$

Eller bevis, at $P(k-1) \Rightarrow P(k)$, for alle $n \geq m+1$
Eller ...

O.v.s. vi beviser:

$$P(m)$$

$$P(m) \Rightarrow P(m+1)$$

$$P(m+1) \Rightarrow P(m+2)$$

$\vdots$

$$k=m \quad (\text{eller } k=m+1)$$

$$k=m+1 \quad (\text{eller } k=m+2)$$

Eks 2:

Prøve selv at bevise, at

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}, \text{ for alle } n \geq 1.$$

$$\text{D.v.s. } 1+2+3+\dots+n = \frac{n(n+1)}{2}, \text{ for alle } n \geq 1$$

Bevis: Ved induktion over n

Basis: ($n=1$)

$P(1)$

$$\frac{1 \cdot 2}{2} = 1$$

$$\text{Ind. ant: } 1+2+\dots+k-1 = \frac{(k-1)k}{2}$$

$P(k-1)$

Ind. skridt: ($P(k-1) \Rightarrow P(k)$)

For $k \geq 2$ gælder:

$$\Downarrow \quad 1+2+\dots+k-1 = \frac{(k-1)k}{2} \quad (\text{ind. ant.})$$

$$\underline{1+2+\dots+k-1 + k} = \frac{(k-1)k}{2} + k$$

$$= \frac{(k-1)k + 2k}{2}$$

$$= \underline{\frac{(k+1)k}{2}}$$

□

Vi har vist:

$P(1)$

$\forall k \geq 2: P(k-1) \Rightarrow P(k)$

Äquivalent basis:

Basis: $(n=1)$

$$1 = \frac{1 \cdot 2}{2}$$

$P(1)$

Ind. anl.:

$$1+2+\dots+k = \frac{k(k+1)}{2}$$

$P(k)$

Ind. Schritt: $(P(k) \Rightarrow P(k+1))$

For $k \geq 1$ gælder:

$$1+2+\dots+k = \frac{k(k+1)}{2} \quad (\text{ind. anl.})$$

$\Downarrow$

$$\begin{aligned} 1+2+\dots+k+k+1 &= \frac{k(k+1)}{2} + k+1 \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+2)(k+1)}{2} \end{aligned}$$

□

$\forall$ har vist:

$P(1)$

$\forall k \geq 1 : P(k) \Rightarrow P(k+1)$

Eks 6: $2^n < n!$, for $n \geq 4$

Lad os starte med at se på små n -værdier, ligesom i Afsnit 1.8, hvor vi så på simple specialtilfælde for at få en forståelse af, hvad der foregår:

$$n=4: \left. \begin{array}{l} 2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 16 \\ 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \end{array} \right\} \Rightarrow 2^4 < 4!$$

$$n=5: \left. \begin{array}{l} 2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2 \cdot 16 = 32 \\ 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5 \cdot 24 = 120 \end{array} \right\} \Rightarrow 2^5 < 5!$$

$$n=6: \left. \begin{array}{l} 2^6 = 2 \cdot 2^5 = 64 \\ 6! = 6 \cdot 5! = 720 \end{array} \right\} \Rightarrow 2^6 < 6!$$

Vi ganger hele tiden 2 på venstre-siden og større og større tal på højre-siden.

D.v.s. når n vokser, bliver uligheden „mere og mere sand“.

Basis ved induktion over n :

Basis: $n=4$

$$2^4 = 16 < 24 = 4!$$

Ind.ant.: $2^{k-1} < (k-1)!$, for $k \geq 5$

Ind.skridt: For $k \geq 5$ gælder:

$$\Downarrow 2^{k-1} < (k-1)! \quad (\text{ind. ant.})$$

$$\Updownarrow 2 \cdot 2^{k-1} < k \cdot (k-1)!, \text{ da } 2 < k$$

$$\Updownarrow 2^k < k!$$

□

„Eks 15“: Alle æbler har samme farve.

„Bevis“: Induktion over $n = \# \text{æbler}$

Basis: ($n=1$)

Ethvert æble har samme farve som sig selv.

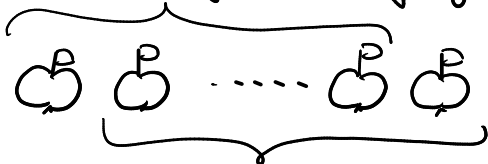
Ind. ant.: ($k \geq 2$)

I enhver skål med $k-1$ æbler har alle æblerne samme farve.

Ind. skridt: $k \geq 3$

Stil k æbler op på række:

Samme farve ifølge ind. ant.

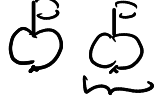


Samme farve ifølge ind. ant.

D.v.s. det første æble har samme farve som de næste $k-2$ æbler, som igen har samme farve som det sidste æble.

Altså har alle k æbler samme farve. $\square$

Bemærk: Argumentet i ind. skridtet fungerer ikke for $k=2$:

samme farve

samme farve

D.v.s. vi har vist

$P(1)$ og

$P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \dots$

men ikke

$P(1) \Rightarrow P(2)$

Da $P(2)$ (selvfølgelig) ikke er sand, har vi ikke meget glæde af at vide, at $P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \dots$