

Sidste gang:

Indløjrede kvantorer

Eks (næring)

$$\begin{aligned} & \neg \exists x \in \mathbb{Z} : \forall y \in \mathbb{Z} : x \geq y \\ \Leftrightarrow & \forall x \in \mathbb{Z} : \exists y \in \mathbb{Z} : x < y \end{aligned}$$

Eks (Ens kvantorer)

$$\begin{aligned} & \forall x \in \mathbb{Z} : \forall y \in \mathbb{Z} : (x \leq y \vee x > y) \\ \Leftrightarrow & \forall y \in \mathbb{Z} : \forall x \in \mathbb{Z} : (x \leq y \vee x > y) \\ \Leftrightarrow & \forall x, y \in \mathbb{Z} : (x \leq y \vee x > y) \end{aligned}$$

Eks

$$\begin{aligned} & \forall x \in \mathbb{Z}^+ : \exists y \in \mathbb{Z}^+ : \forall z \in \mathbb{Z}^+ : \frac{x}{y} \leq z \\ \Leftrightarrow & \forall z \in \mathbb{Z}^+ : \exists y \in \mathbb{Z}^+ : \forall x \in \mathbb{Z}^+ : \frac{x}{y} \leq z \end{aligned}$$

Bevismetoder

- Direkte bevis

$$n^2 = 2(2k^2 + 2k) + 1$$
$$(p \Rightarrow p_1 \Rightarrow \dots \Rightarrow p_n \Rightarrow q) \Rightarrow \boxed{p \Rightarrow q}$$

n er ulige
 $n = 2k+1, k \in \mathbb{Z}$
 n^2 er ulige
 n ulige
 n^2 ulige

- Kontrapositionsbevis

$$(\neg q \Rightarrow \neg p) \Leftrightarrow \boxed{p \Rightarrow q}$$

n lige
 n^2 lige
 n^2 ulige
 n ulige

- Modstridsbevis

$$(\neg p \Rightarrow F) \Rightarrow \boxed{p}$$

Ingen uge med 2 fødselsdage
Højest 52 i lokalet
Mindst 2 med fødselsdag i samme uge

$$c \geq a+b \quad c^2 > a^2 + b^2 \quad c < a+b$$

$a > 0$
 $b > 0$

„Tricks“ : Split op i delresultater

1 dag:

Flere „tricks“, f.eks.: Se først på simple specieltilfælde
Induktionsbeviser (Afsnit 5.1)

"Eks 18": Lad $n \in \{2, 3, 4, \dots\}$

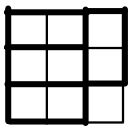
Kan et $n \times n$ skakbræt dækkes af dominobrikker?

Dominobrik: dækker præcis to felter

Ingen brikker må overlappe eller stikke ud over brættet.

Start evt. med simple special-tilfælde for at opnå forståelse:

$n=2$:  Ja

$n=3$:  Nej, vi får brug for en halv brik

n ulige: Nej, fordi:

Hver brik dækker to felter. D.v.s. tilsammen dækker brikkerne et lige #felter

Men ifølge Eks 1 er n^2 ulige

n lige: Ja:

Dæk hver række med $n/2$ brikker

Konstruktiv eksistensbevis:

Vi viser, 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
 $f(2) = 16 - 4 - 1 = 11 > 0$

Ikke-konstruktiv eksistensbevis:

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

Eksisterer der en unik løsning til $f(x) = 0$?

Nej, der er også et nulpunkt ml. -2 og 0 .

Lidt sjovere eksempel: Eks 12

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

Eks: $n \times n$ skakbræt

Fjern to modstående hjørner.

Kan brættet dækkes af domino-brikker?

n ulige: Nej, da $n-2$ ulige

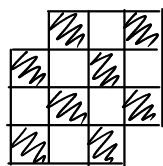
n lige: Først simple specialtilfælde:

$n=2$:



Nej

$n=4$:



Nej

Generelt:

Antag til modstrid, at brættet kan dækkes af dominobrikker.

Da har brættet lige mange sorte og hvide felter.

Men vi startede med et bræt, hvor hver række havde lige mange sorte og hvide felter, og fjernede to sorte eller to hvide felter. D.v.s. der er ikke lige mange sorte og hvide felter ↴

Uden at tegne brættet havde vi måske ikke tænkt over, at de to manglende felter har 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, som man ofte
refererer til.

Lemma: Hjælpe-sætning
Bruges til at strukturere et langt bevis.

Korollar: Følge-sætning.
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:

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

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

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

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

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

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

F. eks. :

$$2^0 = 2^1 - 1$$

$$\Downarrow \begin{matrix} p(0) \\ p(1) \end{matrix}$$

$$2^0 + 2^1 = 2^2 - 1$$

$$\begin{matrix} P(1) \\ \cup \\ P(2) \end{matrix}$$

$$2^0 + 2^1 + 2^2 = 2^3 - 1$$

$$\begin{array}{c} P(2) \\ \Downarrow \\ P(3) \end{array}$$

$P(k-1)$ Induktions-annahme

Kan vi udlede følgende:

Induktions- schritt

$$P(k)$$

Induktionsbevis:

Basistilfælde: Bevis $P(0)$

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

$$\begin{aligned} & P(0) \\ k=1: & P(0) \Rightarrow P(1) \\ k=2: & P(1) \Rightarrow P(2) \\ k=3: & P(2) \Rightarrow P(3) \\ & \vdots \end{aligned}$$

„Domino-effekt“:

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

Bevis ved induktion over n .

Basis: ($n=0$)

$$2^0 = 1 = 2^1 - 1$$

$P(0)$

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

$P(k-1)$

Ind. skridt: For $k \geq 1$ gælder:

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

$P(k-1)$

$$\begin{aligned} 2^0 + 2^1 + \dots + 2^{k-1} + 2^k &= 2^k - 1 + 2^k \\ &= 2 \cdot 2^k - 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

$\Downarrow$

$P(k)$

□

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 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:

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

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

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

□