Invarianter og kombinatoriske beviser

Anders Nedergaard Jensen

Institut for Matematik,
Aarhus Universitet

Matematiklærerdag,
Aarhus, 24. Marts 2017

En invariant er

"en værdi/udsagn der forbliver konstant"

Eksempel:

Fysiker: " $\boxed{\text{Den totale energi}}$ er bevaret"

Anvendelsesområder i matematik:

- geometri
- algoritmer (induktionsbeviser)
- kombinatorik (induktionsbeviser)

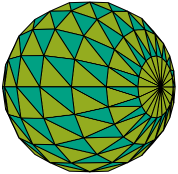
Eksempel: en geometrisk invariant: Euler karakteristik

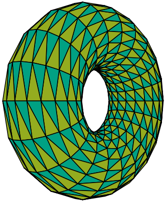
Betragt en flade S. En triangulering af S består af

- hjørner
- kanter
- trekanter

Euler karakteristik

$$\boxed{\chi(S) := \#\text{hjørner} - \#\text{kanter} + \#\text{trekanter}}$$

$\chi($  $) = 2$

$\chi($  $) = 0$

Eksempel på en datalogisk invariant: Bubble sort

Example

(4,3,2,1)

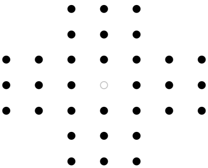
- (4,3,2,1)$\rightarrow$ (3,4,2,1) $\rightarrow$ (3,2,4,1) $\rightarrow$ (3,2,1,4)
- (3,2,1,4)$\rightarrow$ (2,3,1,4) $\rightarrow$ (2,1,3,4)
- (2,1,3,4)$\rightarrow$ (1,2,3,4)

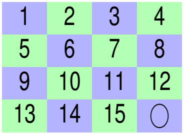
Algorithm

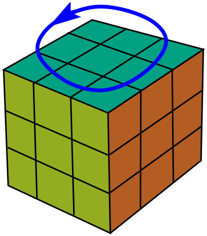
Input *En liste v af tal*
Output *En sorteret udgave af v*

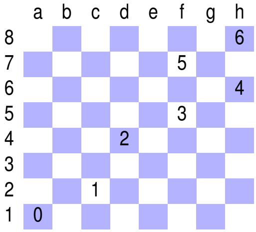
- *for* $i = 0$ *to* $|v|$ $\boxed{\text{/*Invariant: de sidste } i \text{ tal i } v \text{ er rigtige*/}}$
  - *for* $j = 1$ *to* $|v| - i - 1$
    - *if* $v[j] > v[j+1]$ *then swap(*$v[j], v[j+1]$*)*

Invarianter for velkendte puslespil



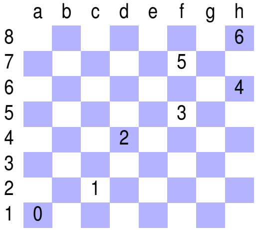






Et enkelt skakproblem

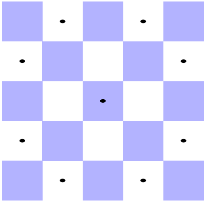
Hvormange træk kræver hesten for at komme fra a1 til h8?



Kan gøres med 6 træk.

Skakreglerne:

- Springeren rykker mellem to felter med afstand $\sqrt{5}$.



Et enkelt skakproblem

- Trekantsuligheden giver nu:

$$\boxed{\text{Efter } i\text{'te træk er } \mathit{dist}(a1, \mathit{hest}) \leq i\sqrt{5}}$$

- Efter 4 træk:

$$\mathit{dist}(a1, \mathit{hest}) \leq 4\sqrt{5} = \sqrt{80} < \sqrt{7^2 + 7^2} = \mathit{dist}(a1, h8).$$

- Efter 5 træk:

$$\mathit{dist}(a1, \mathit{hest}) \leq 5\sqrt{5} = \sqrt{125} > \sqrt{7^2 + 7^2} = \mathit{dist}(a1, h8).$$

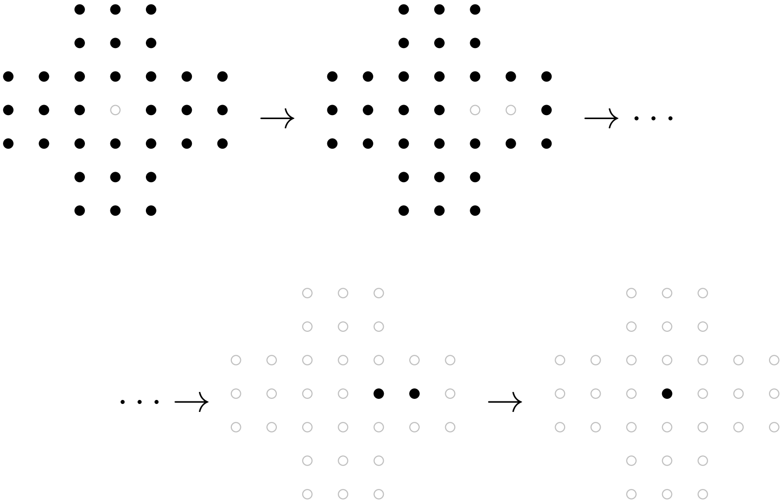
$\{\text{hvid}, \text{blå}\} := \{-1, 1\}$.

Invariant:

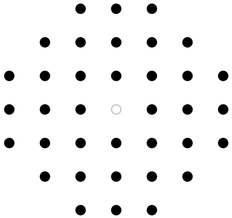
$$\boxed{\text{Efter } i \text{ træk er hesten på felt af farve } (-1)^i.}$$

$\Rightarrow$ Kan ikke gøres på 5 træk.

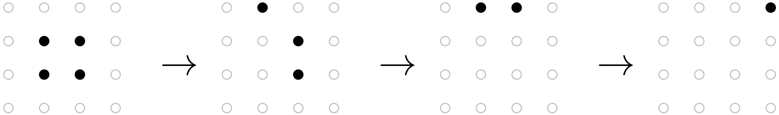
Solitaire kan løses



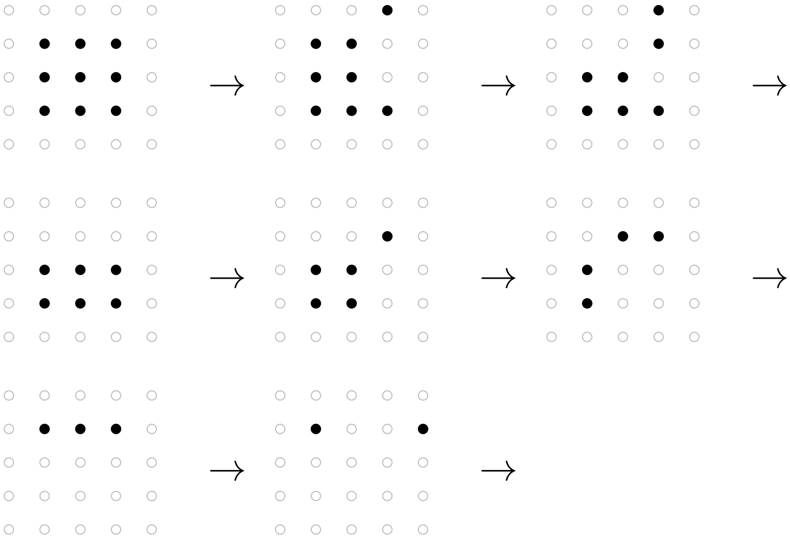
Hvad med den franske version?



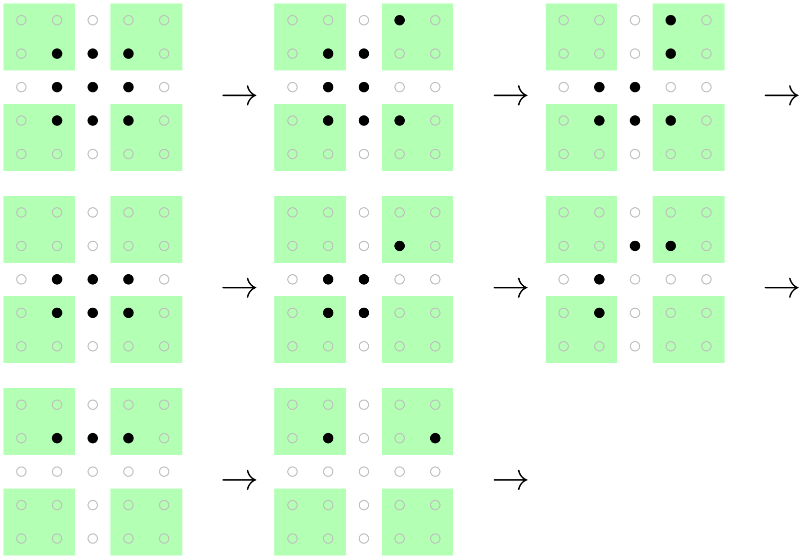
Simplere versioner?



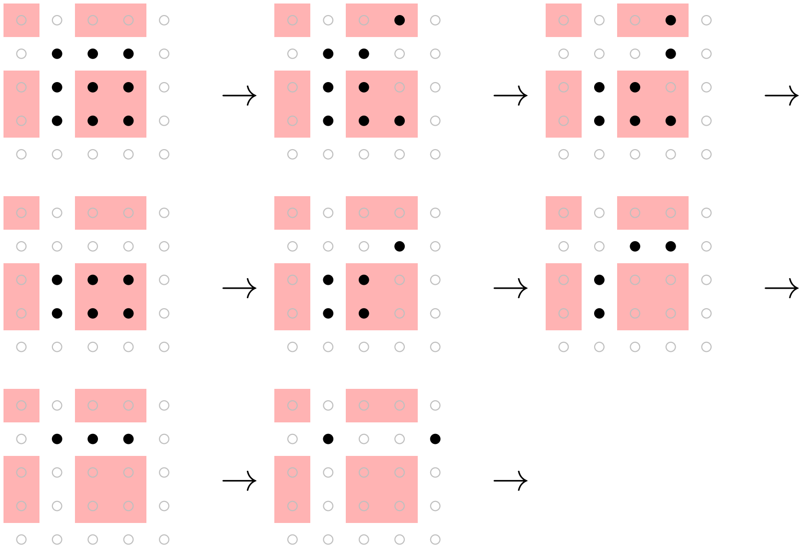
Simplere versioner?



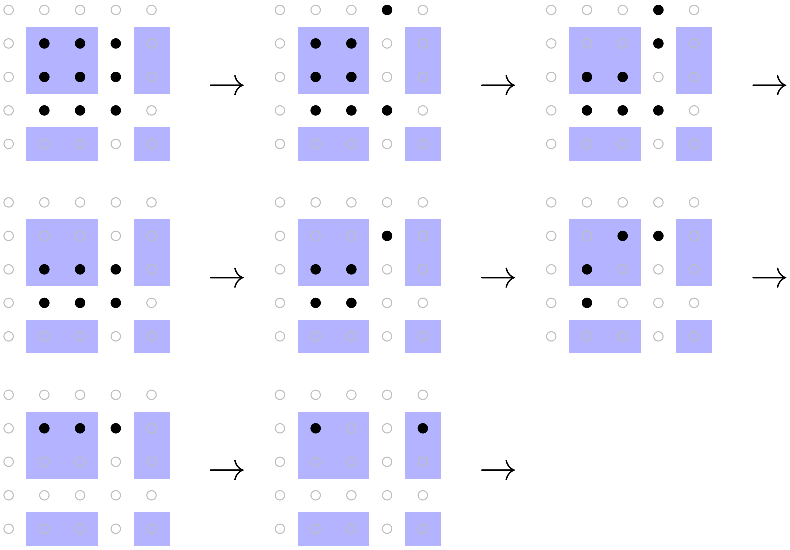
Invariant: “Antal pinde i grønne huller er lige”



Invariant: “Antal pinde i røde huller er lige”



Invariant: “Antal pinde i blå huller er lige”



Bevis

Invariant:

- Antal pinde i grønne huller er lige
- Antal pinde i blå huller er lige
- Antal pinde i røde huller er lige

Bevis:

Induktionsbasis: Vi starter med 4 pinde i grønne huller.

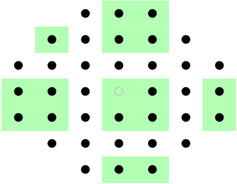
Induktionsskridt: Ændring afhænger af farver for brugte pinde:

- • • ○ $\rightarrow$ ○ ○ • +0
- • • ○ $\rightarrow$ ○ ○ • +0
- • • ○ $\rightarrow$ ○ ○ • +0
- • • ○ $\rightarrow$ ○ ○ • -2

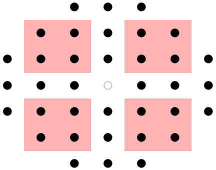
Tilsvarende med røde og blå.

Altså, hvis vi slutter med netop een pind, skal den hverken være grøn, rød eller blå. Modstrid.

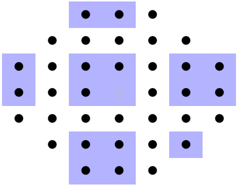
Hvad med den franske version?



grønne lige



røde lige



blå lige.

$\Rightarrow$ Sidste pind er hverken grøn, rød eller blå. Modstrid.

Nim

- 3 stakke S_1, S_2, S_3 med i alt $6 + 7 + 8$ brikker stables
- A og B skiftes til at fjerne mindst en brik fra selvvalgt stak
- **~~Taberen~~ Vinderen er den, der fjerner sidst brik**

Vindende strategi for A:
Opretthold invarianten:

$$\boxed{\text{Efter A's ryk er } |S_1|\,\mathbf{xor}\,|S_2|\,\mathbf{xor}\,|S_3| = 0}$$

Eksempel

$$\begin{aligned}
|S_1| &= 6 & &= 110_2 \\
|S_2| &= 7 & &= 111_2 \\
|S_3| &= 8 & &= 1000_2 \\
|S_1|\,\mathbf{xor}\,|S_2|\,\mathbf{xor}\,|S_3| & & &= 1001_2
\end{aligned}$$

$|S_1|\,\mathbf{xor}\,|S_2|\,\mathbf{xor}\,|S_3| = 0 \Rightarrow$

to stakke er ikke tomme $\Rightarrow$ B kan ikke vinde.

Nim - hvordan opretholdes invarianten?

$$\begin{aligned}
|S_1| = 6 & \qquad = 110_2 \\
|S_2| = 7 & \qquad = 111_2 \\
|S_3| = 8 & \qquad = 1000_2 \\
|S_1| \mathbf{xor} |S_2| \mathbf{xor} |S_3| & \qquad = 1001_2
\end{aligned}$$

Ønsker at justere med 1001_2 f.eks. ved at ændre $|S_3|$ til $1000_2 \mathbf{xor} 1001_2 = 1_2$

$$\begin{aligned}
|S_1| = 6 & \qquad = 110_2 \\
|S_2| = 7 & \qquad = 111_2 \\
|S_3| = 1 & \qquad = 1_2 \\
|S_1| \mathbf{xor} |S_2| \mathbf{xor} |S_3| & \qquad = 0_2
\end{aligned}$$

Generelt tvinges B til at gøre $|S_1| \mathbf{xor} |S_2| \mathbf{xor} |S_3| \neq 0$

Hvad er en permutation?

Lad A være en mængde ("grundmængden").
En permutation af A er en funktion $\sigma : A \to A$ så

- σ er <u>surjektiv</u>
- σ er <u>injektiv</u>

Altså σ er blot en <u>bijektion</u> mellem A og A.

Normalt giver vi elementerne i A navne:

$$A = \{1, \ldots, n\}$$

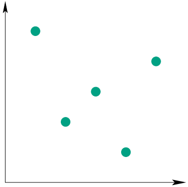
Mængden af alle permutation af $\{1, \ldots, n\}$ kaldes S_n.

Hvordan ser grafen for σ ud?

Eksempel:
$A = (1, 2, 3, 4, 5)$

F.eks. kunne vi have sildebenet:

x	1	2	3	4	5
$\sigma(X)$	5	2	3	1	4



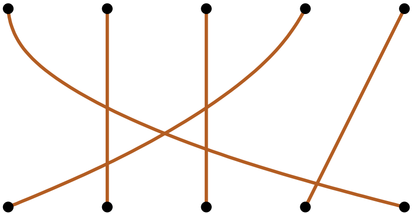
Grafen til højre giver ikke meget mening!

Lad os blot benytte sildebenet til at skrive bijektionen op.

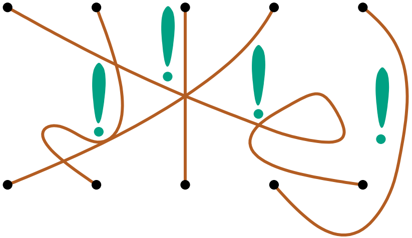
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$$

Hvilken tegning giver så mening?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$$

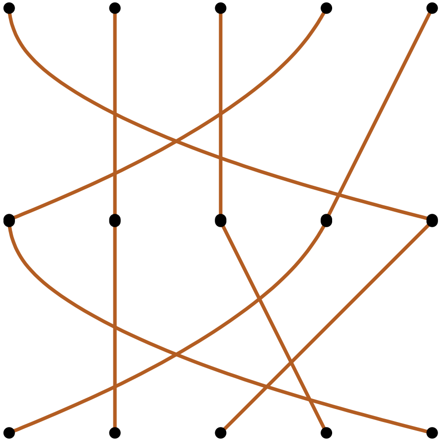


Ikke tilladt:



Sammensætning af permutationer

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$$



$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$$

Fortegnet for en permutation

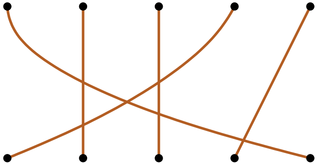
Definition

Fortegnet af $\sigma \in S_n$ defineres som

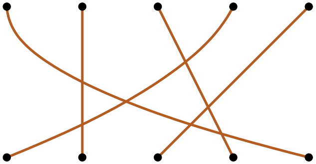
$$sgn(\sigma) := (-1)^k$$

hvor k er antallet af kryds i tegningen af σ.

$$sgn(\sigma) = (-1)^6 = 1$$

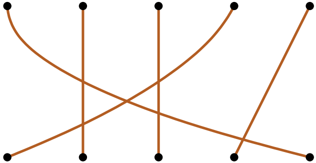


$$sgn(\tau) = (-1)^7 = -1$$

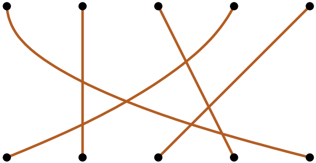


Fortegn af sammensætninger

$$sgn(\sigma) = (-1)^6 = 1$$



$$sgn(\tau) = (-1)^7 = -1$$



$$sgn(\tau \circ \sigma) = (-1)^{13} = (-1)^7(-1)^6 = sgn(\tau)sgn(\sigma)$$

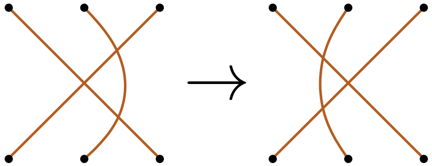
Lemma

$sgn : S_n \to \{-1, 1\}$ er en gruppehomomorfi!

Er fortegnet veldefineret?

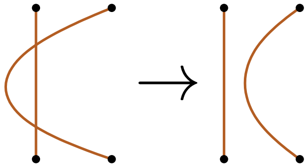
..... vi kunne jo tegne en permutation på flere måder.
Lad os prøve at deformere tegningen til en anden med samme permutation.

Eksempel 1



+0

Eksempel 2



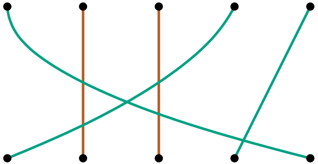
-2

"Lokalt" er det alt hvad der kan ske.
Bemærk: fortegnet er bevaret fordi $(-1)^{-2} = 1$.

Specielle permutationer: cykler

Eksempel:

3-cykel:



Lemma

Fortegnet af en k-cykel er $(-1)^{k-1}$.

Bevis?

Eksempel:
En 2-cykel (kaldes også en transposition) har fortegn -1.

15-spillet

1	2	3	4
5	6	7	8
9	10	$\bigcirc$	12
13	14	11	15

$\mapsto$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	$\bigcirc$	15

$\mapsto$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	$\bigcirc$

Kan

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	$\bigcirc$

løses?

- Den nødvendige permutation i S_{16} har fortegn -1.
- Hvert af vores tilladte ryk har har fortegn -1.

$\Rightarrow$ Et ulige antal ryk kræves.

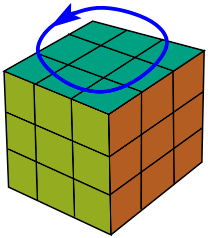
Invariant efter i'te ryk: -1, +1

$$\boxed{(-1)^i \cdot \text{farve}(\text{tomt felt}) = 1}$$

$\Rightarrow$ efter ulige antal ryk er det tomme felt grønt. **Modstrid**

Rubiks terning

- består af $3^3 = 27$ delterninger, hvor af 20 kan flyttes



- hvert træk er en permutation med fortegn (-1)(-1)=+1

En Rubiks terning med to ombyttede delterninger kan ikke løses.
Invariant:

$$\boxed{\text{Fortegnet for den manglende permutationen er altid -1}}$$

Hvad vi ellers kunne have set på

- Tetris med skiftevis Z og S brikker
- Rubiks terning
- Mere om grupper
- Sandsynlighedsteori