invarianter

bevisteknik

datavetenskap

Visdomens källa

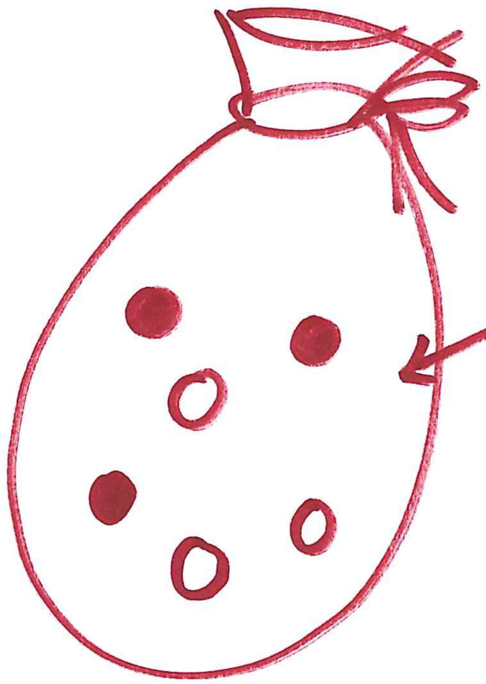
evigt liv?

|

2 saker:

1. aldrig mer ljuga
2. säg: "jag upprepar den här meningen imorgon"

gåta



påse med kulor

röda vita

från början: 50 50

gör steg

① ta ut 2 kulor

② om samma färg, lägg tillbaka en röd

om olika färger, lägg tillbaka en vit

... tills det finns 1 kula kvar

vilken färg?

det **måste** vara en röd

○ ○ → ●

○ ● → ○

● ● → ●

(x, y)

vita ○ — röda ●

$(x,y) \to (x-2, y+1)$

$(x,y) \to (x, y-1)$

$((x,y) \to (x, y-1))$

vita kulor: 50 ... 48 .... 46 .... 44 ....

verkar alltid vara jämn

alltså kan den sista kulan inte vara vit!

$\boxed{\text{måste vara röd}}$

eg~~g~~enskap som påsen alltid har: "antalet vita kulor är jamt"

$\boxed{\text{invariant}}$

steg-system

påse met kulor

(x, y)

- systemet beskrivs med hjälp av "tillstånd"

  s

- det finns ett tillstånd där vi börjar

  "initial tillstånd"

  (50,50)

- det finns "steg" vi kan ta från ett tillstånd till ett annat

  s s'

  $(x,y) \to (x-2, y+1)$

  $(x,y) \to (x, y-1)$

<u>invariant</u> givet ett steg-system

ett predikat $P(s)$ — sant / falskt

$P(x,y) =$ "x är jämn"

① <u>sant</u> för initialtillståndet

$P(50,50)$ sant

② <u>bevaras</u> i steg: för alla tillstånd s och s', där vi kan ta ett steg från s till s',

$$P(s) \Rightarrow P(s')$$

$P(x,y) \Rightarrow P(x-2, y+$

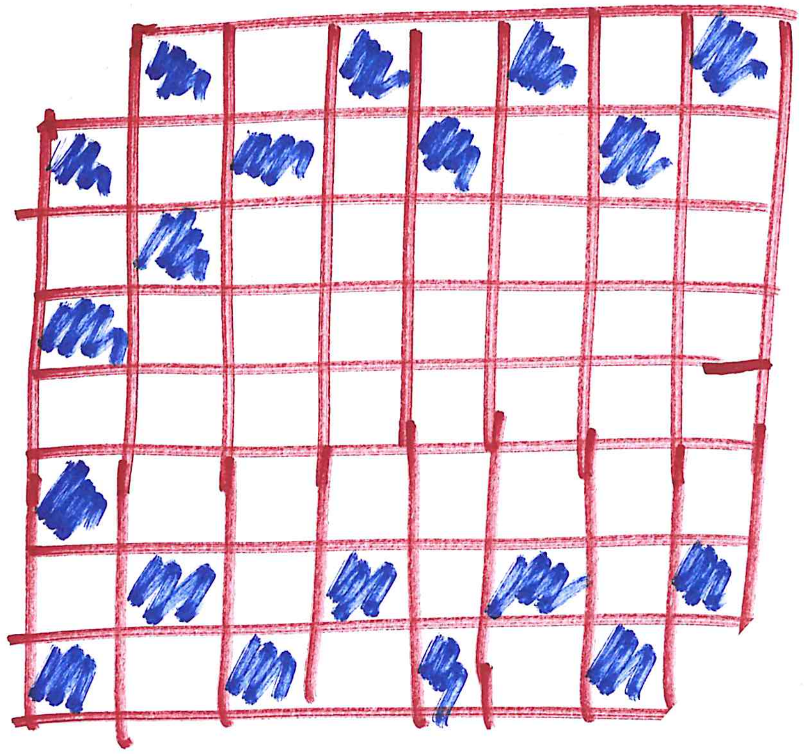
$P(x,y) \Rightarrow P(x, y-1)$

invarianten måste gälla i alla tillstånd nåbara från initialtillståndet

specifikt i sluttillståndet

exempel 2

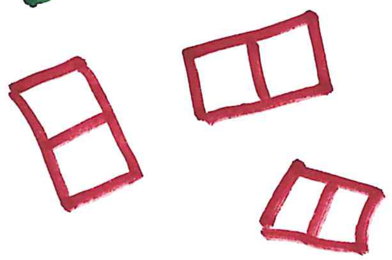
schachbräda
8×8



62
rutor
kvar

32 blå
30 vita

domino-
brickor



(2 rutor)

1 blå 1 vit

täck alla 62 rutor
ovan med 31
brickor

möjligt? ja
nej

Steg-system

· tillstånd : (a, b)

a: antalet otäckta blå rutor

b: antalet otäckta vita rutor

initialtillstånd: $(32, 30)$

· steg: $(a,b) \to (a-1, b-1)$

alt: $P(a,b) =$ "$a \geq b$"

invariant : $P(a,b) =$ " $a = b+2$ "

initialtillstånd: OK

bevaras av steget:

$P(a,b) \Rightarrow P(a-1, b-1)$

$a = b+2 \Rightarrow a-1 = b-1+2$

$a = b+2$

OK

undrar: kan vi nå $(0,0)$?

NEJ

P är falsk

$0 \neq 0+2$

övning:

vilka $n \times m$ brädor går att täcka om man tar bort motsatta hörn?

rysk bondemultiplikation

dela med 2 — gångra med 2 — addition — $a \cdot b$

~~42~~	~~31~~
21	62
~~10~~	~~124~~
5	248
~~2~~	~~496~~
1	992 +
~~0~~	~~1984~~
	1302

tillstånd : (x, y, s)

- initialtillstånd : $(a, b, 0)$
- steg:

$$(x,y,s) \rightarrow \begin{cases} \left(\frac{x}{2}, 2\cdot y, s\right), & \underline{x \text{ jämn}} \\ \left(\frac{x-1}{2}, 2\cdot y, s+y\right), & \underline{x \text{ udda}} \end{cases}$$

invariant : $P(x,y,s) =$ "$x \cdot y + s = a \cdot b$"

- P gäller initialt: $a \cdot b + 0 = a \cdot b$

  ok

$P(x,y,s) = \text{"}x \cdot y + s = a \cdot b\text{"}$

<u>P bevaras</u> :

<u>x jämn</u>: $P(x,y,s) \Rightarrow P\left(\frac{x}{2}, 2 \cdot y, s\right)$

$$x \cdot y + s = a \cdot b \Rightarrow \frac{x}{2} \cdot 2 \cdot y + s = a \cdot b$$

$$= x \cdot y + s = a \cdot b \quad \underline{\text{ok}}$$

<u>x udda</u>: $P(x,y,s) \Rightarrow P\left(\frac{x-1}{2}, 2 \cdot y, s+y\right)$

$$x \cdot y + s = a \cdot b \Rightarrow \frac{x-1}{2} \cdot 2 \cdot y + s + y = a \cdot b$$

$$(x-1) \cdot y + s + y =$$

$$x \cdot y \cancel{-y} + s \cancel{+y} =$$

$$x \cdot y + s = a \cdot b \quad \underline{\text{ok}}$$