2011-(04)apr-12: dag 22

Lite till

- Primtalitetstest
  - Fermattest
  - Pseudoprimtal, Carmichaeltal
  - Miller–Rabins test

Lite satslogik och boolesk algebra

- Satslogik
  - Atomära sentenser
  - Konnektiven ¬, ∧, ∨, →, ↔
  - Sanningsvärdestabeller
  - Logisk ekvivalens
- Boolesk algebra
  - Räkneregler
  - Booleska funktioner
  - Disjunktiv och konjunktiv normalform
  - Minimering, Karnaughdiagram

Primtalstest

Är (det stora) talet N ett primtal?

Fermattest (bas b, $1 < b < N$):

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N är sammansatt. Ja: Vet inte.

Pseudoprimtal, bas b:

Sammansatt, klarar Fermaltestet, bas b.

Exempel: $341 = 11 \cdot 31$, bas 2

Mer om primalitetstest

Problematiska för Fermattestet:

Carmichaeltal:

Klarar alla Fermattest med bas b med sgd(b, N) = 1.

Exempel:
$N = 561 = 3 \cdot 11 \cdot 17$, $560 = 2^4 \cdot 5 \cdot 7$

N är ett Carmichaeltal omm det är kvadratfritt och
$p \mid N \Rightarrow p^{-1} \mid N - 1$.

Det finns oändligt många sådana

1105, 1729, 2465, ...

Starkare test:

Miller–Rabins test (M–R) (1980)

Förfinning av Fermattestet:

$N - 1 = n \cdot 2^r$, n udda, $r \geq 1$ (N udda)

M–R:

$b^n \pmod N$

$\left(b^n\right)^2 \pmod N$

$\left(\left(b^n\right)^2\right)^2 = b^{n \cdot 2^2} \pmod N$

$\vdots$

$b^{n \cdot 2^r} \equiv 1 \pmod N$

Om N klarar Fermattestet, bas b.

Om N är ett primtal

$b^n \equiv 1 \pmod N$

eller

$\left(b^n\right)^{2^i} \equiv -1 \pmod N$, något i, $0 \leq i < r$.

Exempel: N = 561, bas = 2

$N - 1 = 560 = 35 \cdot 2^4$

$2^{35} \equiv 263 \pmod{561}$

$2^{70} \equiv 263^2 \equiv 166 \pmod{561}$

$2^{140} \equiv 116^2 \equiv 67 \pmod{561}$

$2^{280} \equiv 67^2 \equiv 1 \pmod{561}$

$2^{56} \equiv 1 \pmod{561}$

561 är inte ett primtal, ty detta är inte -1.

561 = 3·11·17 — Om −1 på alla rader så så primtal.

mod	3	11	17	Faktorer
	−1	−1	10	
	1	1	13	
	1	1	−1	
	1	1	1	Vi är klara

Lite om satslogik

Studerar påstående “matematiskt”.

Exempel:

“Lisa läser diskret matematik.” : A

“Det regnar.” : B

¬A: “Lisa läser inte diskret matematik.”

A ∧ ¬B: “Lisa läser diskret matematik och det regnar inte.”

C → A ∨ B: “Om det är onsdag så läser Lisa diskret matematik eller så regnar det (eller båda).”

Säger man “antingen A eller B” så menar man, men “eller”, “A, B, eller både A och B”.

Operationerna för sammansatta påståenden kallas konnektiv.

¬	negation	“inte”
∧	konjunktion	“och”, “men” (skillnaden får inte i den här analysen)
∨	disjunktion	“eller”, “minst en av”
→	implikation	“om … så …”, “bara om”
↔	dubbel implikation	“omm”

Deras betydelse ges av sanningsvärdestabeller:

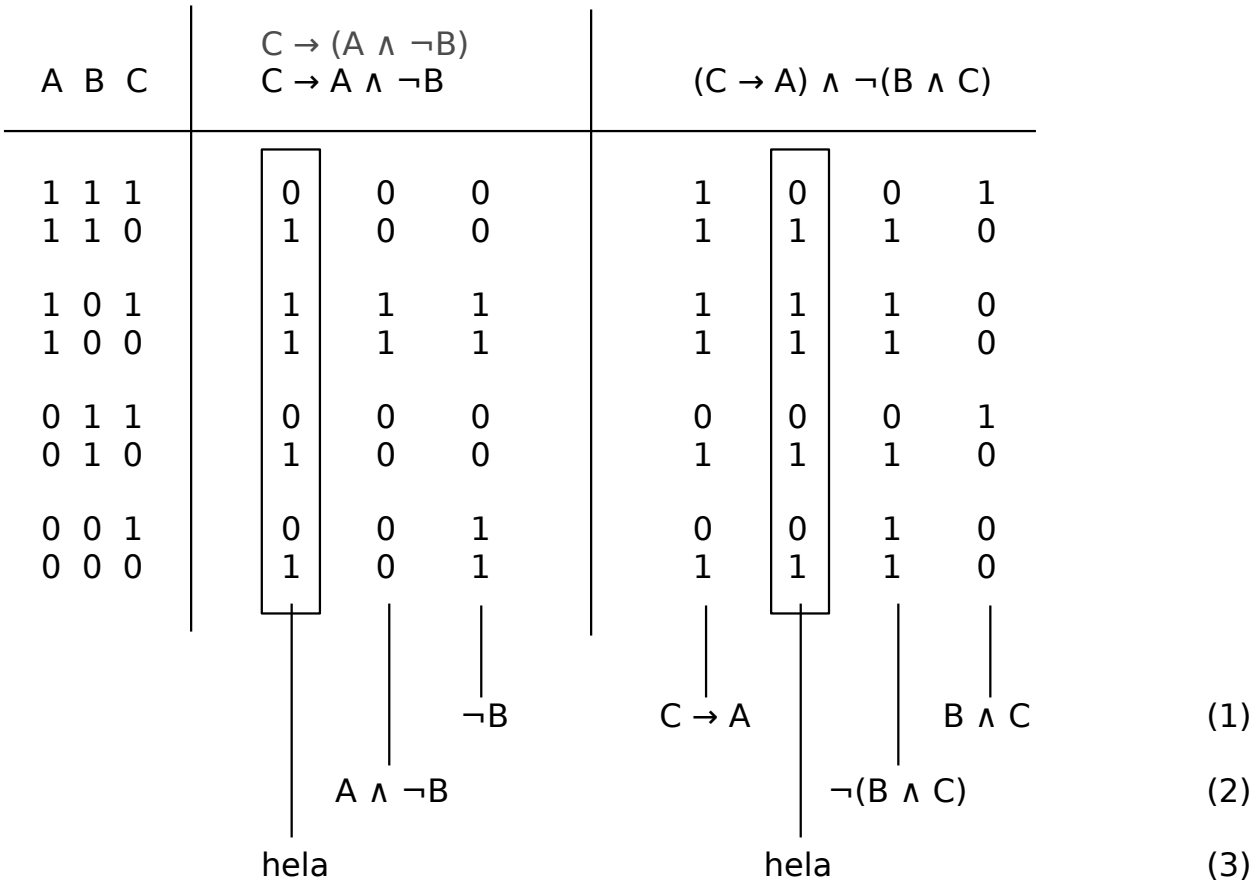
p	¬p
1	0
0	1

1 = sant
0 = falskt

p	q	p ∧ q	p ∨ q	p → q	p ↔ q
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

p ∧ q:	1 omm båda 1	»båda sanna»
p ∨ q:	0 omm båda 0	»någon sann»
p → q:	0 omm (1, 0)	»q minst lika sann som p»
p ↔ q:	1 omm lika	»p och q lika sanna»

Sanningsvärdestabeller för “större” sentenser



Observera att i exemplet får båda sentenserna samma sanningsvärden i alla tolkningar (alla rader). Vi säger att sentenserna är logiskt ekvivalenta.

$$C \to A \wedge \neg B \;\equiv\; (C \to A) \wedge \neg(B \wedge C)$$

(⇔ i boken)

Exempel:

$p \to q \;\equiv\; \neg p \to \neg q$ (kontraposition)

$p \to q \;\not\equiv\; q \to p$ (omvändning)

Alla logiska ekvivalenser kan fås med några enkla “tankelagar” (algebraiska).

Boolesk algebra, enkla logiska ekvivalenser

$p \wedge q$	$\equiv$	$q \wedge p$	$p \vee q$	$\equiv$	$q \vee p$	kommutativitet
$(p \wedge q) \wedge r$	$\equiv$	$p \wedge (q \wedge r)$	$(p \vee q) \vee r$	$\equiv$	$p \vee (q \vee r)$	associativitet
$p \wedge (q \vee r)$	$\equiv$	$(p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$	$\equiv$	$(p \vee q) \wedge (p \vee r)$	ditrivutivitet
$\neg(p \wedge q)$	$\equiv$	$\neg p \vee \neg q$	$\neg(p \vee q)$	$\equiv$	$\neg p \wedge \neg q$	De Morgan
$p \wedge p$	$\equiv$	p	$p \vee p$	$\equiv$	p	idempotens
$p \wedge (p \vee q)$	$\equiv$	p	$p \vee (p \wedge q)$	$\equiv$	p	absorption

$\neg\neg p$	$\equiv$	p	involution
$p \leftrightarrow q$	$\equiv$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$\leftrightarrow$ uttryckt
$p \rightarrow q$	$\equiv$	$\neg p \vee q$	$\rightarrow$ uttryckt
$\neg p$	$\equiv$	$p \rightarrow \bot$	$\neg$ uttryckt

$p \wedge \neg p$	$\equiv$	$\bot$	komplementaritet
$p \wedge \bot$	$\equiv$	$\bot$	Alltid falsk (falsum)
$p \wedge \top$	$\equiv$	p	Alltid sann (verum)

Annat skrivsätt (x·y skrivs oftast xy)

$p \cdot q$	$=$	$q \cdot p$	$p + q$	$=$	$q + p$	kommutativitet
$(p \cdot q) \cdot r$	$=$	$p \cdot (q \cdot r)$	$(p + q) + r$	$=$	$p + (q + r)$	associativitet
$p \cdot (q + r)$	$=$	$(p \cdot q) + (p \cdot r)$	$p + (q \cdot r)$	$=$	$(p + q) \cdot (p + r)$	ditrivutivitet
$\overline{p \cdot q}$	$=$	$\overline{p} \cdot \overline{q}$	$\overline{p + q}$	$=$	$\overline{p} + \overline{q}$	De Morgan
$p \cdot p$	$=$	p	$p + p$	$=$	p	idempotens
$p \cdot (p + q)$	$=$	p	$p + (p \cdot q)$	$=$	p	absorption

$\overline{\overline{p}} = p$ involution

$p \cdot \overline{p}$	$=$	$\mathbf{0}$	komplementaritet
$p \cdot \mathbf{0}$	$=$	$\mathbf{0}$	
$p \cdot \mathbf{1}$	$=$	p	

Notera att $\overline{x\,\overline{y}} \neq \bar{x}\,\bar{\bar{y}}$ och $\bar{x}\,\bar{y} \neq \overline{xy}$

(Det som stod på förra sidan)

$p \wedge q$	$\equiv$	$q \wedge p$	$p \vee q$	$\equiv$	$q \vee p$	kommutativitet
$(p \wedge q) \wedge r$	$\equiv$	$p \wedge (q \wedge r)$	$(p \vee q) \vee r$	$\equiv$	$p \vee (q \vee r)$	associativitet
$p \wedge (q \vee r)$	$\equiv$	$(p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$	$\equiv$	$(p \vee q) \wedge (p \vee r)$	ditrivutivitet
$\neg(p \wedge q)$	$\equiv$	$\neg p \vee \neg q$	$\neg(p \vee q)$	$\equiv$	$\neg p \wedge \neg q$	De Morgan
$p \wedge p$	$\equiv$	p	$p \vee p$	$\equiv$	p	idempotens
$p \wedge (p \vee q)$	$\equiv$	p	$p \vee (p \wedge q)$	$\equiv$	p	absorption

$\neg \neg p \equiv p$ involution

$p \wedge \neg p$	$\equiv$	$\bot$	komplementaritet
$p \wedge \bot$	$\equiv$	$\bot$	
$p \wedge \top$	$\equiv$	p	

Motsvarande i mängdlära

$A \cap B$	$\equiv$	$B \cap A$	$p \cup q$	$\equiv$	$q \cup p$	kommutativitet
$(A \cap B) \cap C$	$\equiv$	$A \cap (B \cap C)$	$(p \cup q) \cup r$	$\equiv$	$p \cup (q \cup r)$	associativitet
$A \cap (B \cup C)$	$\equiv$	$(A \cap B) \cup (A \cap C)$	$p \cup (q \cap r)$	$\equiv$	$(p \cup q) \cap (p \cup r)$	ditrivutivitet
$(A \cap B)^c$	$\equiv$	$A^c \cup B^c$	$(p \cup q)^c$	$\equiv$	$p^c \cap q^c$	De Morgan
$A \cap A$	$\equiv$	A	$p \cup p$	$\equiv$	p	idempotens
$A \cap (A \cup B)$	$\equiv$	A	$p \cup (p \cap q)$	$\equiv$	p	absorption

$A^{c\,c} \equiv A$ involution

$A \cap A^c$	$\equiv$	$\varnothing$	komplementaritet
$A \cap \varnothing$	$\equiv$	$\varnothing$	
$A \cap \mathcal{U}$	$\equiv$	A	

[5.3] (Text om ett hypotetiskt reglemente finns nog i en av böckerna)

Exempel med “resonemang” (att förenkla logiska uttryck) med boolesk algebra.

Militärt reglement: $x \rightarrow y = \bar{x} + y$

a: slips skall bäras
b: vapenrock skall bäras
c: ytterrock skall bäras

Reglementet:

$$
\begin{aligned}
& (\bar{a} \rightarrow \bar{b})(a\bar{b} \rightarrow c)((c+\bar{a}) \rightarrow b) && = \\
= \quad & (\bar{\bar{a}}+\bar{b})(\overline{a\bar{b}}+c)(\overline{c+\bar{a}}+b) && = \\
= \quad & (\bar{\bar{a}}+\bar{b})(\bar{a}+\bar{\bar{b}}+c)(\overline{c+\bar{a}}+b) && = \\
= \quad & (a+\bar{b})(\bar{a}+b+\bar{c})(a\bar{c}+b) && = \\
= \quad & (a+\bar{b})(b+(\bar{a}+\bar{c})a\bar{c}) && = \\
= \quad & (a+\bar{b})(b+\mathbf{0}c+a\bar{c}) && = \\
= \quad & (a+\bar{b})(b+a\bar{c}) && = \\
= \quad & ab+a\bar{c}+\mathbf{0}+a\bar{b}\bar{c} && = \\
= \quad & a(b+\bar{c}+\bar{b}\bar{c}) && = \\
= \quad & a(b+\bar{c}) && = \\
= \quad & a(c \rightarrow b)
\end{aligned}
$$

Så förenklingen:

1) Slips skall bäras.

2) Om ytterrock bäres, skall vapenrock bäras.