NTNU
Norwegian University of Science and Technology
Department of Mathematical Sciences
N-7491 Trondheim
Norway

Relasjon $R \subseteq A \times B$ | **symmetrisk** | **Anti-sym** $\langle x,y\rangle \wedge \langle y,x\rangle \Rightarrow x=y$ | **Ekvivalent:** Refle + Symm + transitiv

Refleksiv  | **transitiv**  | **Irref** ingen $\langle x,x\rangle$ | **Partial-order** refl + transitiv + anti-sym

Logic

distr. $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ V.V.

abs. $p \wedge (p \vee q) \equiv p$ V.V.

DM $\neg(A \wedge B) \equiv \neg A \vee \neg B$ V.V.

asso. $A \vee (B \vee C) \equiv (A \vee B) \vee C$ V.V.

Ident. $p \vee 0 \equiv p$ $p \wedge 1 \equiv p$

Negeti $p \vee \neg p \equiv 1$ $p \wedge \neg p \equiv 0$

Idem. $p \vee p \equiv p \wedge p \equiv p$

$p \rightarrow q \equiv \neg p \vee q$

Set

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

—"—

—"—

—"—

~~$A \cap \emptyset = A$ $A \cup U = U$~~

$A \cup \emptyset = A$ $A \cap U = A$

Compliment

$A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$

—"—

$A \times B = \{\langle x_1, x_2\rangle \mid x_1 \in A, x_2 \in B\}$

Powerset $M = \{1,2\}$, $P(M) = \{\emptyset, \{1\}, \ldots\}$

CNF

ledd m/ $\wedge$ og $\neg$ knyttet av $\vee$

DNF

ledd m/ $\vee$ og $\neg$ knyttet av $\wedge$

Språk:

Konkatinering: $a^3b^2 = aaabb$

A-alfabet, A^*-språk

Funksjoner

Injektiv (unik):

Surjektiv (hele codomene):

Bijektiv (1 til 1)

Induktivt definert:

Minste mengden

språk - $\Lambda \in S$

Eks: hvis $x \in S$, så er $axa \in S$

Partisjon "kamper av S"

- Union lik S
- snitt lik $\emptyset$

Boolean

krav:

Kommutativ: $XY = YX$, $X+Y = Y+X$

Identitet: $X+0 = X$, $X \cdot 1 = X$

kompli: $X+\bar{X} = 1$, $X \cdot \bar{X} = 0$

distrib: $X(Y+Z) = XY + XZ$

$X + (YZ) = (X+Y)(X+Z)$

B følger:

absorp: $X \cdot 0 = 0$, $X+1 = 1$

DM: $\overline{XY} = \bar{X} + \bar{Y}$, $\overline{X+Y} = \bar{X} \cdot \bar{Y}$

Idem: $X \cdot X = X$, $X+X = X$

Første ordens logikk

Predikat: $P(x)$ U-univers

kvantor: $\forall$ og $\exists$

to lover:

- $\neg \forall x (P(x)) \equiv \exists x (\neg P(x))$
- $\neg \exists x (P(x)) \equiv \forall x (\neg P(x))$

- tilfredsstillende
- U-"—"
- Valid
- Motsigende

Kombinatorikk

- Permut - ant. endringer
- ordnet - rekkefølge viktig
- n-elementer, trekk k

	ordnet	uordnet
m/rep	n^k	$\binom{n+k-1}{k}$
u/rep	${}_nP_k = \frac{n!}{(n-k)!}$	$nCk = \binom{n}{k}$

Overtelling

dele m/ n! per n like elementer

Eks: pappa, 3p 2a $\frac{5!}{3!2!} = 10$perm

$nCk = \frac{n!}{(n-k)!\,k!}$ | $\binom{n}{k} = \binom{n}{n-k}$

Binomialko:

$(x+y)^n \rightarrow \binom{n}{k} x^{n-k} y^k$

Tilstandsmaskin

$M = (S, I, O, \nu, S_0, F)$

S = tilstander

I - input

O - output

ν - $S \times I \rightarrow S \times O$

ν	S_0	S_1
0	S_1, a	S_0, b
1	S_0, b	S_1, a

S_0 - start

F - godkjente S

Graf

- Multi 
- reflet
- kompliment - ingen like nabopar

deg(v): løkke teller 2

ant. oddegrad er partall

Trær

- n-noder → n-1 kanter
- -1 kant → ¬sammenheng.
- Nøyaktig 1 sti mellom noder

Sti:

ingen node >1 gang

lukket: start = slutt v

krets: ingen E >1 gang

sykel: lukket sti

Eulervei

- sammenheng.
- Hver E nøyaktig 1 gang

Eulerkrets

- eulervei m/ start v = slutt v
- * grad $\forall$v partall $\Rightarrow$ G har eulerkrets
- * Nøyaktig to oddegrader $\Rightarrow$ eulervei mellan de to nodene
- * >2 oddegrad $\Rightarrow$ ingen eulervei

n+k-1 kan tenkes:

$\binom{n+k-1}{k}$ n+k-1 = ant * + ant 1

k = ant *

***|*|**

Isomorfi:

- Lik grad ?
- Ant. E ?
- Naborelasjoner

Først ord. Bonus

$\forall x \exists y$ - flere y per x

$\exists y \forall x$ - en y for alle x

Hamilton sti

- Sammenheng.
- $\forall$v i G nøyak. 1 gang

Hamilton sykel

Sykel m/ $\forall$v i G nøyaktig 1 gang

Diofantisk:
$\gcd(a,b) \mid c \Rightarrow$ løsning.

Eratos s.i:
- Skriv 2 til n
- Ring minste, kryss multi
- $p^2 > n \Rightarrow$ ring rest

Krypto
Fermat faktor:
$n = (a-b)(a+b)$
$a^2 - n = b^2$
- sett $a = \sqrt{n}$ rundet opp
- Er $a^2 - n$ kvadrat?

RSA
krav: $e \perp \varphi(n)$ og $0 < e < \varphi(n)$
$0 < d < \varphi(n)$
krypt: $C = m^e \bmod n$, $n = p \cdot q$
dekrypt: $m = C^d \bmod n$, d er invers emod $\varphi(n)$

Euclids algoritme:
$\gcd(a,b) = \gcd(b, a \bmod b)$
repeat-algoritme

Modulær invers
$a \cdot c \equiv 1 \bmod n$
$a^{-1} \bmod b = a^{\varphi(b)-1} \bmod b$

Fermats lille
$a^{p-1} \bmod p = 1$
og $a^{p-1} \equiv 1 \bmod p$

Dekryptering oppskrift
- Finn p og q (fermats)
- finn $d = e^{-1} \bmod \varphi(n)$
- $m = c^d \bmod n$

Euclids-utvidede:
Euclids, så bakleng:
EKS $321x + 78y = 3$
Fra euclids:
$3 = 9 - 1 \cdot 6$, $6 = 78 - 8 \cdot 9$
$\Rightarrow 3 = 9 - 1 \cdot (78 - 8 \cdot 9)$
$\Rightarrow = (-1)(78) + 9 \cdot 9$
$= -78 + 9(321 - 4 \cdot 78)$
$= 9 \cdot 321 - 37 \cdot 78$
$\Rightarrow x = 9 \wedge y = -37$

Eulers teorem
$a^{\varphi(n)} \equiv 1 \bmod n$

Modulær potens
Regn 2-er potenser og del opp
$5^{22} = 5^{16+4+2}$

$b \mid a \Rightarrow q \cdot b = a$

φ-funk:
$\varphi(1) = 1$, $\varphi(p) = p-1$
$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$
$\varphi(24) = (2^3 - 2^2)(3^1 - 3^0) = 8$

Flere likninger:
* konflikt? $\Rightarrow$ ingen løs
* utvid og forenkle
EKS $X \equiv 11 \bmod 12$
$X \equiv 11 \bmod 4$ og $X \equiv 11 \bmod 3$
* Fjern duplikat
OBS! Fjern minste

deling:
$15x \equiv a \bmod n$
Finn invers til 15:
$15 \cdot 15^{-1} x \equiv a \cdot 15^{-1} \bmod n$
$x \equiv a \cdot 15^{-1} \bmod n$

Kinesisk rest
u invers m mod n
v invers n mod m
$x \equiv a \bmod m$
$x \equiv b \bmod n$
løs: $x \equiv anv + bmu \bmod mn$

Oppskrift
$M = m_1 \cdot m_2 \cdots m_n$
$M_1 = M \div m_1$
$k_1 = \text{invers } M_1 \bmod m_1$
$x \equiv aM_1k_1 + bM_2k_2 \bmod M$

Tjen. prim
anta endelig ant. prim
La $p_1, p_2 \ldots p_n$ være prim
$P = p_1 \cdot p_2 \cdots p_n + 1$
Da er $P \bmod p_i = 1$
$\Rightarrow P$ prim motsigelse

Bevis oppg 3 $f: X_1 \to X_2$ $g: X_2 \to X_3$
f, g injek
for $\forall x_3 \in g(x_2)$ $\exists$ unik $x_2 \in X_2$
for $\forall x_2 \in f(x_1)$ $\exists$ unik $x_1 \in X_1$
$\Rightarrow g \circ f$ injek

f, g surjek.
$\forall x_3 \in X_3$ $\exists x_2 \in X_2$ s.a. $g(x_2) = x_3$
$\forall x_2 \in X_2$ $\exists x_1 \in X_1$ s.a $f(x_1) = x_2$
$\Rightarrow g \circ f$ sur