Sammanfattning av modul 4

S_n ($n \geq 2$) har hälften jämna och hälften udda permutationer.
De jämna permutationerna utgör en normal delgrupp till S_n,
denna delgrupp kallas A_n.

För en $n \times n$-matris $\mathbf{A}$:

$$\det \mathbf{A} = \sum_{\pi \in S_n} = \operatorname{sgn} \pi \; a_{1\pi(1)} a_{2\pi(2)} \ldots a_{n\pi(n)} = \sum_{\pi \in S_n} \operatorname{sgn} \pi \; a_{\pi(1)1} a_{\pi(2)2} \ldots a_{\pi(n)n}$$

$\det \mathbf{M}_\pi = \operatorname{sgn} \pi$

Koden C är en mängd n-tuper av 1:or och 0:or, alltså $C \subseteq \mathbb{Z}_2^n$, n är kodens längd.

Minimala avståndet, δ, för C:

$$\delta = \min\{\partial(a, b) \mid a, b \in C, a \neq b\}, \qquad \partial(a, b) = \text{antalet } i \text{ med } a_i \neq b_i$$

C är felrättande och kan upptäcka upp till $\delta - 1$ fel,
men rätta upp till $\left\lfloor \frac{\delta - 1}{2} \right\rfloor$ fel (alltså avrundat nedåt).

Sfärpackningssatsen:

Om koden C har längden n och rättar upp till e fel:

$$|\mathcal{C}|\left(\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{e}\right) \leq 2^n \; \left(= \left|\mathbb{Z}_2^n\right|\right)$$

$|C| = 2^k$, k är C:s dimension.

C är en linjär kod om a, b $\in$ C $\Rightarrow$ a + b $\in$ C.
Det vill säga C är ett delrum till $\mathbb{Z}_2^n$, en delgrupp till $\left(\mathbb{Z}_2^n, +\right)$.

Då är minimala avståndet = minimala (nollskilda) vikten, det vill säga

$\delta = w_{min} = \min\{w(c) \mid c \in C, c \neq 0\}$

w(c), vikten för c, är antalet 1:or i c.

Om H är en m × n-matris är $C = \{x \in \mathbb{Z}_2^n \mid Hx = 0\}$ är en linjär kod av dimension n − rank H. H allas kodens (paritets)kontrollmatris.

Om H:s alla kolonner är $\neq \vec{0}$ så rättar C minst ett fel.

z är ett kodord med fel i position i $\Rightarrow$ Hz = H:s i:e kolonn.

Hammingkoder ges av en kontrollmatris H med r rader och $2^r - 1$ kolonner, alla olika och $\neq \vec{0}$ (alla som finns).

Längd:	$n = 2^r - 1$
Minimiavstånd:	$\delta = 3$
Dimension:	$k = 2^r - r - 1$

Hammingkoder ger likhet i sfärpackningstatsen, de är perfekta koder.

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

Carmichaeltal:

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

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

Starkare test:

Miller–Rabins test (M–R)

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, $0 \leq i < r$.

Satslogik

En sentens är en symbolsträng som kan stå för olika utsagor (påståenden).
Sentener byggs upp av atomära sentenser, konnektiv och parenteser.

1 = T, t, s = Sant
0 = F, f, f = Falskt

Sanningsvärdestabeller:

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

$p \wedge q$: 1 omm båda 1 »båda sanna»

$p \vee q$: 0 omm båda 0 »någon sann»

$p \to q$: 0 omm (1, 0) »q minst lika sann som p»

$p \leftrightarrow q$: 1 omm lika »p och q lika sanna»

Kontraposition: $p \to q \equiv \neg p \to \neg q$
Omvändning: $p \to q \not\equiv q \to p$

Sanningsvärdestabeller för “större” sentenser

A	B	C	$C \to (A \land \neg B)$ $C \to A \land \neg B$			$(C \to A) \land \neg(B \land C)$				
1	1	1	0	0	0	1	0	0	1	
1	1	0	1	0	0	1	1	1	0	
1	0	1	1	1	1	1	1	1	0	
1	0	0	1	1	1	1	1	1	0	
0	1	1	0	0	0	0	0	0	1	
0	1	0	1	0	0	1	1	1	0	
0	0	1	0	0	1	0	0	1	0	
0	0	0	1	0	1	1	1	1	0	
					$\neg B$	$C \to A$			$B \land C$	(1)
				$A \land \neg B$				$\neg(B \land C)$		(2)
			hela				hela			(3)

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

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

($\Leftrightarrow$ i boken; = för +, $\cdot$, $\bar{\ }$ -notationen)

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

$p \wedge \bot \equiv \bot$

$p \wedge \top \equiv p$

Alltid falsk (falsum)

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
$\overline{p \cdot q} = \bar{p} \cdot \bar{q}$	$\overline{p+q} = \bar{p}+\bar{q}$	De Morgan
$p \cdot p = p$	$p+p = p$	idempotens
$p \cdot (p+q) = p$	$p+(p \cdot q) = p$	absorption

$\bar{\bar{p}} = p$ involution

$p \cdot \bar{p} = \mathbf{0}$ komplementaritet

$p \cdot \mathbf{0} = \mathbf{0}$

$p \cdot \mathbf{1} = p$

Notera att $\overline{x\,\bar{y}} \neq \bar{x}\,\bar{\bar{y}}$ och $\bar{x}\,\bar{y} \neq \overline{xy}$ + är inte likadan som i $\mathbb{Z}_2$.

0-ställiga (en. nullary) konnektiv: $\bot$ $\top$

1-ställiga (en. unary) konnektiv: $\neg$

2-ställiga (en. binary) konnektiv: $\wedge$ $\vee$ $\rightarrow$ $\leftrightarrow$

$$\mathbb{B}_n = \{0, 1\}^n = \{00\ldots0,\ 00\ldots1,\ \ldots,\ \underbrace{11\ldots1}_{\times n}\}$$

En boolesk funktion beskrivs fullständigt av en sanningsvärdestabell.

Exempel:

x	y	z	ƒ(x, y, z)		
1	1	1	1	xyz	1 på denna rad, 0 för övriga
1	1	0	1	$xy\bar{z}$	1 på denna rad, 0 för övriga
1	0	1	1	$x\bar{y}z$	1 på denna rad, 0 för övriga
1	0	0	0		
0	1	1	0		
0	1	0	0		
0	0	1	1	$\bar{x}\bar{y}z$	1 på denna rad, 0 för övriga
0	0	0	0		

“Så” $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$

På samma sätt kan varje boolesk funktion skrivas på disjunktiv normalform (dnf).

Dualt: konjunktiv normalform (knf)

$$f(x, y, z) = (\bar{x} + y + z)(x + \bar{y} + \bar{z})(x + \bar{y} + z)(x + y + z)$$

Karnaugh-diagram

xy \ z	z 0	$\bar{z}$ 1
0 0 ($\bar{x}$)	0	1
0 1 (y)	0	0
1 1 (x)	1	1
1 0 ($\bar{y}$)	0	1

Här är $f(x, y, z) = xy + \bar{y}\bar{z}$

För ihop 1:orna i rektanglar med sida 1, 2 eller 4 (2^n). Rektanglarna ska vara Så stora som möjligr som får vara överlappande.

Endast en skillnad per rad i xy, gäller även i kolonnerna.

I diagrammet till vänster finns, det två ihopförningar, de heldragna bilder en rektangel.

Dualitet: Om varken p eller q innehåller → eller ↔ och p = q, så också d(p) ≡ d(q), där d(p) fås av att i p byta alla ∧ ⇄ ∨ och ⊤ ⇄ ⊥.

Kryptering

$\mathcal{M}$ — Meddelande i klartext
$\mathcal{C}$ — Chiffer (Meddelandet krypterat)

$E(M) = C$, $D(C) = M$, $D = E^{-1}$

E — Krypteringsalgroitm (nyckel inbyggd)
D — Dekrypteringsalgroitm (nyckel inbyggd)

Traditionellt: E och D bara kända av behöriga, E och D kan fås ur varanda.
(symmetriskt krypto)

Modernt (1976): Offentlig nyckel, E kan inte (lätt) fås ur D och är offentlig.

(till exempel RSA, asymmetriskt krypto)
Asymmetriska krypton är söliga, och kan användas för att komma överrens om ett symmetriskt krypto.

Elektronisk signatur:

1. Offentliggör $D(x)$. Alla kan läsa (med E), ingen utan D kunde ha skrivit.

2. B änder $E_A(D_B(x))$ (eller $D_B(E_A(x))$) till A. Bara någon med D_A kan läsa, bara någon med D_B kunde ha skrivit.

Fermats lilla sats:

Om p är ett primtal och $p \nmid a$ så $a^{p-1} \equiv 1 \pmod{p}$.

Sats:

Låt p och q vara olika primtal, $n - pq$, $m - (p-1)(q-1)$.
$s \equiv 1 \pmod{m} \;\Rightarrow\; x^s \equiv x \pmod{n}$, alla $x \in \mathbb{Z}$.

RSA-algoritmen:

Tag två stora primtal ($\approx 10^{150}$), p och q.

Välj e med $\mathrm{sgd}(e, m) = 1$.

Finn d så att $ed \equiv 1 \pmod{m}$. (Euklides)

Offentliggör n och e och hemlighåll d.

$E, D : \mathbb{Z}_n \to \mathbb{Z}_n$

$E(x) = x^e$, $D(x) = x^d$

$D = E^{-1}$

$E(x)$ och $D(x)$ kan beräknas med upprepad kvadrering (mod n) av x och multiplication (mod n) av rätt x^{2^i} (mod n).