1. Logikk

Logiske operatorer

Symbol	Mening
$\sim p$	ikke p
$p \wedge q$	p og q
$p \vee q$	p eller q
$P \equiv Q$	P er ekvivalent med Q
$p \rightarrow q$	p impliserer q
$p \leftrightarrow q$	p hvis og bare hvis q
$\therefore$	Derfor

NB! $\neg$ og $\sim$ betyr det samme.

Logiske operatorer

Symbol	Mening
$P(x)$	Predikat i x: parametrisert utsagn med x som parameter
$P(x) \Rightarrow Q(x)$	Sannhetsmengden til $P(x)$ er inneholdt i sannhetsmengden til $Q(x)$.
$P(x) \Leftrightarrow Q(x)$	Sannhetsmengden til $P(x)$ er lik sannhetsmengden til $Q(x)$.
$\forall$	For alle
$\exists$	Det eksisterer

Logikklovene

Kommutative lover:	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Assosiative lover:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive lover:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identitetslover:	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negasjonslover:	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
Dobbel negativ-lov:	$\sim (\sim p) \equiv p$	
Idempotente lover:	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universalgrenselover:	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
DeMorgans lover:	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorpsjonslover:	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negasjon av $\mathbf{t}$ og $\mathbf{c}$:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$
	$\mathbf{t} = 1 =$ tautologi	$\mathbf{c} = 0 =$ selvmotsigelse

Inferens-regler

Modus Ponens	$p \rightarrow q$ p $\therefore \quad q$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \quad \sim p$
Generalisering	p $\therefore \quad p \vee q$
Spesialisering	$p \wedge q$ $\quad\quad$ $p \wedge q$ $\therefore \quad p$ $\quad\quad$ $\therefore \quad q$
Konjunksjon	p q $\therefore \quad p \wedge q$

Eliminasjon	$p \vee q$ $\quad\quad$ $p \vee q$ $\sim q$ $\quad\quad$ $\sim p$ $\therefore \quad p$ $\quad\quad$ $\therefore \quad q$
Transitivitet	$p \rightarrow q$ $q \rightarrow r$ $\therefore \quad p \rightarrow r$
Oppdeling i tilfeller	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore \quad r$
Motsigelse	$\sim p \rightarrow \mathbf{c}$ $\therefore \quad p$

2. Kombinatorikk

Formler for kombinatorikk

	Ordnet utvalg	Uordnet utvalg
Med tilbakelegging	n^r	$\binom{n+r-1}{r}$
Uten tilbakelegging	$\frac{n!}{(n-r)!}$	$\binom{n}{r}$

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Antall elementer i en union

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

3. Mengdelære

Mengdelovene

Alle mengder er inneholdt i en universalmengde U.

Kommutative lover:	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Assosiative lover:	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
Distributive lover:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identitetslover:	$A \cap U = A$	$A \cup \emptyset = A$
Negasjonslover:	$A \cup A^c = U$	$A \cap A^c = \emptyset$
Dobbel negativ-lov:	$(A^c)^c = A$	
Idempotente lover:	$A \cap A = A$	$A \cup A = A$
Universalgrenselover:	$A \cup U = U$	$A \cap \emptyset = \emptyset$
DeMorgans lover:	$(A \cap B)^c = A^c \cup B^c$	$(A \cup B)^c = A^c \cap B^c$
Absorpsjonslover:	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Komplement av U og $\emptyset$:	$U^c = \emptyset$	$\emptyset^c = U$
Mengdedifferensloven:	$A - B = A \cap B^c$	

4. Tallteori

Symboler

Symbol	**Mening**
$d \mid n$	Det finnes et heltall k slik at $n = dk$.
$d \nmid n$	d deler ikke n
$\gcd(a, b)$	Største felles divisor av a og b
$a \equiv b \pmod{n}$	$n \mid (a - b)$

Aritmetikkens fundamentalteorem

Gitt et heltall n eksisterer det et positivt heltall k, forskjellige primtall $p_1, p_2, p_3, \ldots, p_k$ og positive heltall $e_1, e_2, e_3, \ldots, e_k$ slik at

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_k^{e_k}.$$

Videre er denne måten å skrive n som et produkt av primtall på unik bortsett fra rekkefølgen på faktorene.

Euklids algoritme

Euklids algoritme brukes til å bestemme $\gcd(A, B)$ for to heltall A og B, der vi antar at $A > B \geq 0$.

1. Hvis $B = 0$, er $\gcd(A, B) = A$.
2. Hvis ikke, finn q og r slik at
$$A = Bq + r \text{ slik at } 0 \leq r < B.$$
Da er $gcd(A, B) = gcd(B, r)$.
3. Sett $A := B$ og $B := r$ og gå tilbake til trinn 1.

Tips for å regne ut a%n

Tips for å regne ut $a\%n$.

(1) Tast inn a inn på kalkulator.
(2) Tast minustast.
(3) Tast inn n
(4) Trykk =-tasten inntil tallet er mindre enn n.

Regneregler for kongruenser

La a, b, c, d, n være heltall slik at $n > 1$, og anta at $a \equiv c \pmod{n}$ og $b \equiv d \pmod{n}$. Da har vi at

a) $(a + b) \equiv (c + d) \pmod{n}$
b) $(a - b) \equiv (c - d) \pmod{n}$
c) $ab \equiv cd \pmod{n}$
d) $a^m \equiv c^m \pmod{n}$ for alle positive heltall m.

5. RSA

RSA er offentlig nøkkel-kryptografi. Et RSA-kryptosystem er basert på to (helst veldig store) primtall p og q.

Prosedyre for å finne nøkler

1. Finn et tall e som er relativt primisk med $(p - 1)(q - 1)$ og finn så en positiv invers d til dette tallet modulo $(p - 1)(q - 1)$.
2. La $n = pq$. Da blir (n, e) *offentlig nøkkel* og
3. (n, d) *privat nøkkel*.

Kryptering og dekryptering

Du ønsker å sende en melding M. Du må da kjenne mottakerens offentlige nøkkel (n, e).

- Den krypterte meldingen C er gitt ved
$$C \equiv M^e \pmod{n}.$$
- C dekrypteres av mottakerenved å beregne
$$M \equiv C^d \pmod{n}.$$

6. Lineær algebra

Matriseoperasjoner

Gitt matrisene $A = [a_{ij}]$ og $B = [b_{ij}]$.

Sum:	$A + B$	$=$	$[a_{ij} + b_{ij}]$
Multipli kasjon med skalar:	kA	$=$	$\left[k\, a_{ij}\right]$
Produkt	AB	$=$	$\left[\sum_{k=1}^{n} a_{ik} b_{kj}\right]$
Transponert	A^T	$=$	$[a_{ji}]$
	$(AB)^T$	$=$	$B^T A^T$

Gauss-eliminering

Gauss-eliminering har som mår å omforme en matrise A til en trappematrise U. Til det brukes tre operasjoner

(1) Addere multiplum av rad i til rad j.
(2) Bytte om på radene i og j.
(3) Multiplisere rad i med ikke-negativ skalar.

Invers matrise / Rank

rank A = antall pivotelementer i en trappematrise for A.

$$\text{rank}(A^T) = \text{rank}(A)$$

Invers matrise:

$$A^{-1}A = AA^{-1} = I$$
$$(AB)^{-1} = B^{-1}A^{-1}$$
$$(A^T)^{-1} = (A^{-1})^T$$

Gauss Jordan:

$$[A|I] \sim [I|A^{-1}]$$

Følgende er ekivalent for kvadratiske matriser:

(1) A er inverterbar (A^{-1} eksisterer.)
(2) $\det A \neq 0$.
(3) A har maksimal rang.

Lineære transformasjoner

rank A = antall pivotelementer i en trappematrise for A.
En transformasjon T fra $\mathbb{R}^n$ til $\mathbb{R}^m$ kalles lineær hvis og bare hvis

(1) $T(c\mathbf{x}) = cT(\mathbf{x})$, for alle $\mathbf{x} \in \mathbb{R}^n$ og alle $c \in \mathbb{R}$.
(2) $T(\mathbf{x}+\mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y})$, for alle $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Transformasjonsmatrisen til T er matrisen

$$\begin{bmatrix} T(\mathbf{e}_1) & T(\mathbf{e}_2) & \cdots & T(\mathbf{e}_n) \end{bmatrix}$$

Speiling om 1. akse	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Speiling om 2. akse	$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$
Speiling om linjen $x_1 = x_2$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Rotasjon om origo	$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$
Skalering	$\begin{bmatrix} k_1 & 0 \\ 0 & k_2 \end{bmatrix}$

Normallikningen

Normallikningen $A^TA = A^Tb$.

Lineær avhengig/uavhengig vektormengde / Basis

Rangmetoden: Innfør matrisen $A = \begin{bmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_k \end{bmatrix}$ så er $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ l.a. hvis $\text{rank}(A) < k$ og l.u. hvis $\text{rank}(A) = k$.

Alternativ metode: $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ er l.u. hvis og bare hvis $x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_k\mathbf{a}_k = 0$ kun har løsningen $x_1 = x_2 = \ldots = x_k = 0$.

Indreprodukt

- For $\mathbb{R}^n$:

$$\langle u, v\rangle = u^Tv = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

Ortonormalitet

- To vektorer u og v er ortogonale hvis
$$\langle u, v\rangle = 0$$
- En vektor-mengde S er **ortogonal** hvis elementene er parvis ortogonale.
- En vektor-mengde S er **ortonormal** hvis elementene er parvis ortogonale og hver vektor i S har lengde 1. ($\langle u, u\rangle = 1, \forall u \in S$)

systemer

Et system kalles
konsistent: hvis det har en eller flere løsninger.
inkonsistent: hvis det har ingen løsninger.

7. Grafer

Veier

vei: Sekvens av kanter $(v_1v_2), (v_2v_3), (v_3v_4), \ldots, (v_{n-1}v_n)$.
lukket: En vei er lukket om den starter og stopper i samme hjørne. $(v_1 = v_n)$
rundtur: En lukket vei.
sti: Vei som ikke gjentar hjørner.
spor: Vei som ikke gjentar kanter.
krets: Et lukket spor.
simpel krets: En krets som ikke gjentar noe hjørne bortsett fra start og slutt
Eulerspor: Er et spor som inneholder alle hjørner og kanter i G.
Eulerkrets: Er et Eulerspor som også er en krets.
Hamiltonkrets: Er en simpel krets som inneholder alle hjørner i G.

Begreper

sammenhengende: En graf er sammenhengende hvis det for hvert par av hjørner a og b finnes en vei som forbinder a med b.
komponent: en ikke-sammenhengende graf består av noen sammenhengende komponenter. Enhver komponent er da en maksimal sammenhengende delgraf (delgraf hvor det ikke er mulig å legge til flere noder slik at den forblir sammenhengende)
isomorfi: En 1-1 avbilding av hjørnene i en graf G_1 til hjørnene i en annen graf G_2 er en isomorfi hvis den er 1-1 på kantene også.
isomorfi-invariant: En egenskap som ikke endres ved isomorfier.

- Antall hjørner
- Antall kanter
- Ei rekke med gradene til alle hjørnene
- Antall komponenter
- $\vdots$