# MAT1030 – Diskret Matematikk

## Forelesning 10: Mengdelære

Dag Normann

Matematisk Institutt, Universitetet i Oslo

17. februar 2010

(Sist oppdatert: 2010-02-17 12:41)

# Kapittel 5: Mengdelære



## Oversikt

- Tirsdag snakket vi først litt om mengder, og om hvordan vi beskriver en mengde.
- Vi har innført de Boolske operasjonene,
  - union $\cup$: $A \cup B = \{x : x \in A \vee x \in B\}$
  - snitt $\cap$: $A \cap B = \{x : x \in A \wedge x \in B\}$
  - komplement $\overline{A}$: $\overline{A} = \{x \in \mathcal{E} : x \notin A\}$
  - mengdedifferens $A - B$: $A - B = \{x : x \in A \wedge x \notin B\}$

  samt de faste mengdene $\emptyset$ og $\mathcal{E}$.
- Vi tegnet Venndiagrammet tilhørende de forskjellige Boolske operasjonene, og begynte på et eksempel på litt mer avansert bruk av Venndiagrammer.
- Vi fortsetter med flere eksempler (på tavlen).



## Mengdeteoretiske lover

**Eksempel**

- deMorgans lover
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (som vi så på i går).
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- De distributive lovene
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

**Eksempel**

- $A \cap \overline{(B \cup C)} = (A - B) \cap (A - C)$
- $(\overline{A} - B) \cap C = C - (A \cup B)$

## Mengdeteoretiske lover

### Oppgave

- Vi bruker bare Venndiagrammer for uttrykk med en, to eller tre mengder.
- Tegn et Venndiagram for tre mengder $A$, $B$ og $C$, og sett inn sannhetsverdiene for de tre basisutsagnene $x \in A$, $x \in B$ og $x \in C$ i de forskjellige feltene.
- Undersøk hvor mange deler det er mulig å dele planet inn i ved hjelp av fire sirkler.
- Forklar hvorfor dette viser at Venndiagrammer ikke er hensiktsmessige for Boolske uttrykk med mer enn tre mengder.



## Inklusjon

### Eksempel

- Det er selvfølgelig slik at alle tall som kan deles på 4 også er partall.

  Vi sier da at mengden av tall delelige med 4 er inneholdt i partallene, eller at den er en delmengde av partallene.
- Mengden av registrerte fødselsnummere er inneholdt i mengden av alle data registrert i skattedirektoratet.
- Mengden av hunder er en delmengde av mengden av dyr.



## Inklusjon

### Definisjon

Hvis $A$ og $B$ er mengder, sier vi at $A$ er inneholdt i $B$, eller at $A$ er en delmengde av $B$, hvis

$$\forall x(x \in A \to x \in B).$$

- Vi skriver

$$A \subseteq B$$

for at $A$ er inneholdt i $B$.



## Inklusjon

- Vi vil kunne skrive $A \subseteq B$ selv om $A = B$.
- Noen forfattere bruker $A \subset B$ slik vi bruker $A \subseteq B$ mens andre bruker det i betydningen

$$A \subseteq B \land A \neq B.$$

- I dette siste tilfellet vil vi si at $A$ er ekte inneholdt i $B$.

## Inklusjon

### Eksempel

- $\{2, 5, 6\} \subseteq \{1, 2, 5, 6, 7\}$ og inklusjonen er ekte.
- I følge læreboka vil
  $$\mathbb{N} \subseteq \mathbb{J} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$
  Når vi ser på disse mengdene som datatyper, vet vi at vi må bruke forskjellige måter å representere et tall i $\mathbb{J}$ på, avhengig av om vi ser på tallet som et element i $\mathbb{J}$ eller $\mathbb{R}$.

  Denne påstanden er derfor ikke helt uproblematisk, men dog akseptabel for våre formål.
- $\{x : x^2 > 4\} \subseteq \{x : x^2 > 4 \vee x < -1\}$.



## Inklusjon

Vi kan bruke Venndiagrammer til å vise at et Boolsk uttrykk alltid definerer en delmengde av mengden definert ved et annet Boolsk uttrykk.

Vi skal se et par eksempler på tavlen.

### Eksempel

- $A \cap B \subseteq A \cup B$
- $\overline{A} \cap (B - C) \subseteq B - (A \cap C)$



## Disjunkte mengder

### Definisjon

To mengder $A$ og $B$ er disjunkte hvis de ikke har noen felles elementer, det vil si, hvis
$$A \cap B = \emptyset.$$

### Eksempel

- $\{0, 4, 7, 9\}$ og $\{1, 2, 5, 10\}$ er disjunkte.
- $\{0, 4, 5, 7, 9\}$ og $\{0, 2, 5, 10\}$ er ikke disjunkte.

  Snittet av disse to mengdene er $\{0, 5\} \neq \emptyset$.



## Boolsk algebra

- Det er en nær sammenheng mellom Boolsk mengdealgebra og utsagnslogikk.
- Ved å erstatte $A$ med $x \in A$ oppfattet som en utsagnsvariabel, kan vi spisse $\cup$ til $\vee$, $\cap$ til $\wedge$ og erstatte komplement $\overline{A}$ med $\neg(x \in A)$, og vi får en utsagnslogisk formel.
- Det er da naturlig å erstatte $\emptyset$ med **F** og $\mathcal{E}$ med **T**.
- To mengder, definert fra mengdevariable $A$, $B$ og liknende ved hjelp av union, snitt og komplement vil alltid være like nøyaktig når oversettelsene er logisk ekvivalente.

## Boolsk algebra

- Tabell 5.1 på side 80 (79 i Utgave 2) i læreboka lister noen Boolske identiteter.
- De har sine paralleller i tabellen på side 56 (55) over logikkens lover.
- Vi skal ikke drille regning med disse Boolske identitetene.



## En digresjon: Russells Paradoks

- Hvis vi hadde kunnet snakke om mengden av alle mengder, hadde vi hatt en grunn mindre til å bringe inn den universelle mengden $\mathcal{E}$.
- Antagelsen om at det fins en mengde som har alle mengder som elementer, leder imidlertid til en motsigelse som kalles Russells Paradoks.
- Vi gir beviset for Russells Paradoks som en oppgave med hint.



## En digresjon: Russells Paradoks

**Oppgave**

- Anta at $X$ er en mengde, og at for alle mengder $Y$ vil $Y \in X$.
- La $Z = \{Y \in X \ : \ Y \notin Y\}$.
- Da er $Z \in X$.
- Vis at hvis $Z \in Z$ så vil $Z \notin Z$.
- Vis at hvis $Z \notin Z$ så vil $Z \in Z$.
- Forklar hvorfor dette viser at mengden $X$ ikke kan finnes.



## Digital representasjon av mengder

- I utgangspunktet skal det ikke spille noen rolle i hvilken rekkefølge man skriver opp elementene i en mengde.
- Hvis man imidlertid har behov for å representere visse mengder digitalt, må man velge seg en rekkefølge på elementene i den universelle mengden $\mathcal{E}$.
- Vi skal nå se på en metode for digital representasjon av mengder som virker når $\mathcal{E}$ er endelig.
- Hvis $\mathcal{E}$ er en uendelig mengde, må man enten velge en annen metode eller gi opp.

## Digital representasjon av mengder

### Definisjon

- Anta at $\mathcal{E}$ har $k$ elementer i rekkefølge

$$\{a_1, \ldots, a_k\}.$$

- La $A \subseteq \mathcal{E}$
- Vi representerer $A$ som informasjon på $k$ bit i rekkefølge, ved at bit nummer $i$ får verdien 1 hvis og bare hvis $a_i \in A$.



## Digital representasjon av mengder

- Ved denne måten å representere mengder på blir det svært enkelt å etterlikne de Boolske operasjonene.
- Snitt svarer til punktvis multiplikasjon, union svarer til det å ta maksimumsverdien punktvis og komplement svarer til å skifte verdi i alle bit.
- Vi kommer ikke til å jobbe så mye med digital representasjon av mengder.
- Når vi kommer til kompleksitetsteori, og vi spør om kompleksiteten til et problem som involverer mengder, trenger vi å vite hvordan mengder representeres digitalt.



## Kardinaltall

- Hvis vi i noen sammenhenger ønsker å bruke digitale representasjoner av mengder, er det viktig at $\mathcal{E}$ ikke får lov til å være for stor.
- $10^{10^{10}}$ er lett å skrive, men foreløpig har vi ingen datamaskin med så mange bit.
- For å kunne følge med på hvor store mengder vi opererer med, og for å kunne resonnere omkring størrelse på mengder, er det en fordel med en notasjon for størrelsen av mengder.
- Det er dette vi vil fange opp i begrepet kardinaltall.



## Kardinaltall

### Definisjon

- La $A$ være en endelig mengde.
- Med kardinaltallet til $A$ mener vi antall elementer i $A$.
- Vi skriver $|A|$ for kardinaltallet til $A$.

### Eksempel

- Hvis $A = \{2, 3, 17, 5, 23, 12, 15\}$ er $|A| = 7$.
- Hvis $B = \{n \in \mathbb{N} : 2n + 1 < 17\}$ er $|B| = 7$.
- Hvis $C = \{x \in \mathbb{R} : x^3 - 6x^2 + 11x - 6 = 0\}$ er $|C| = 3$.
- Hvis $D = \{x \in \mathbb{J} : x^2 = 64\}$ er $|D| = 2$.

## Kardinaltall

Vi skal se på en enkel setning om kardinalitet som kan bli nyttig i avsnittet om kombinatorikk.
Det er en setning som har sin parallell i sannsynlighetsteori, og i mange andre sammenhenger hvor man på en eller annen måte måler størrelse på mengder.

### Teorem

La $A$ og $B$ være to endelige mengder.

Da er

$$|A| + |B| = |A \cup B| + |A \cap B|.$$



## Kardinaltall

### Bevis

Først observerer vi at hvis $C$, $D$ og $E$ er vilkårlige disjunkte mengder, så vil

$$|C \cup D \cup E| = |C| + |D| + |E|.$$

Så lar vi $C = A - B$, $D = A \cap B$ og $E = B - A$.

Fra Venn-diagrammet ser vi at disse er disjunkte.

Da er

- $|A \cup B| = |C| + |D| + |E|$
- $|A| = |C| + |D|$
- $|B| = |D| + |E|$

Teoremet følger da ved enkel regning.

Til de som ikke kom til forelesningen: Noe ble forklart ved Venn-diagrammer på tavlen.



## Kardinaltall

### Eksempel

- Hvis alle 16 spillerne på et håndball-lag må kunne brukes i angrep eller forsvar, og vi vet at 7 av spillerne kan brukes i begge posisjoner og at 12 av spillerne kan brukes i forsvar, setter vi opp en likning for antall spillere som kan brukes i angrep:
- $$16 + 7 = x + 12.$$
- Det gir at 11 spillere kan brukes i angrepsspillet.
- Fra Venn-diagrammet ser vi at det vil være fire spillere som bare kan brukes i angrep, og fem spillere som bare kan brukes i forsvar.



## Kardinaltall

- Den tyske matematikeren *Georg Cantor* utviklet en teori for kardinaltallet til en uendelig mengde også.
- Dette skjedde i siste halvdel av 1800-tallet.
- Ut fra Cantors definisjon fins det like mange rasjonale tall og hele tall som naturlige tall, mens det fins ekte flere reelle tall.
- Vi skal begrense oss til kardinalitet av endelige mengder.
- Selv om datamaskiner av natur bare kan håndtere endelig mye informasjon, har imidlertid studiet av uendelige mengder også en plass i informatikken.
- Dette faller ofte utenfor rammen til diskret matematikk og derfor utenfor pensum i MAT1030.

## Kardinaltall

### Eksempel

a) La $A = \{0, 1, 2\}$.
Da har $A$ 8 delmengder: $\emptyset$, $\{0\}$, $\{1\}$, $\{2\}$, $\{0, 2\}$, $\{0, 1\}$, $\{1, 2\}$ og $\{0, 1, 2\}$.
Disse er skrevet opp i en usystematisk rekkefølge.
En mer systematisk måte vil være først å skrive den ene delmengden av $\emptyset$: $\emptyset$,
så resten av delmengdene av $\{0\}$: $\{0\}$
så resten av delmengdene av $\{0, 1\}$: $\{1\}$ og $\{0, 1\}$
og til slutt resten av delmengdene av $\{0, 1, 2\}$: $\{2\}$, $\{0, 2\}$, $\{1, 2\}$ og $\{0, 1, 2\}$



## Kardinaltall

### Eksempel (Fortsatt)

Den naturlige rekkefølgen blir da

$$\{\emptyset, \{0\}, \{1\}, \{0, 1\}, \{2\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

b) For å liste opp alle delmengder av $\{0, 1, 2, 3\}$ lister vi først opp alle delmengder av $\{0, 1, 2\}$ og deretter alle nye delmengder, ved å legge 3 til en av de åtte første.
Det gir
$\{\emptyset, \{0\}, \{1\}, \{0, 1\}, \{2\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\},$
$\{3\}, \{0, 3\}, \{1, 3\}, \{0, 1, 3\}, \{2, 3\}, \{0, 2, 3\}, \{1, 2, 3\}, \{0, 1, 2, 3\}\}$



## Potensmengder

### Definisjon

- La $A$ være en mengde.
- Med potensmengden til $A$ mener vi mengden av alle delmengder av $A$.

### Merk

- Hvis $A$ er en mengde og $B \subseteq A$ er en vilkårlig delmengde, vil vi for hver $x \in A$ ha to muligheter, $x \in B$ og $x \notin B$.
- En konsekvens er at hvis $A$ er endelig vil potensmengden til $A$ ha $2^{|A|}$ elementer.
- Dette vil ofte bety at det vil ta alt for lang tid å gjennomføre naive algoritmer.



## Potensmengder

### Eksempel

- La $A$ være en endelig mengde av naturlige tall.
- Vi lar $\sum A$ bety summen av alle tallene i $A$.
- Partisjonsproblemet er om det fins delmengder $B$ og $C$ av $A$ som er slik at
  1. $A = B \cup C$
  2. $\emptyset = B \cap C$ ( de er disjunkte)
  3. $\sum B = \sum C$
- Den første strategien for å løse dette problemet kan være å liste opp alle par $B \subseteq A$ og $C = A - B$, og sjekke, men hvis $A$ har 1000 elementer, er ikke dette praktisk gjennomførbart.
- Ingen vet per i dag om det fins en vesentlig raskere metode for å løse partisjonsproblemet generelt.
- Partisjonsproblemet er et eksempel på et NP-komplett problem.

## Potensmengder

### Merk

- Potensmengden til $A$ er definert selv om $A$ er uendelig.
- I det tilfellet er ikke alle egenskapene ved potensmengder fullstendig klarlagt ennå.
- Vi ledes langt ut over rammene for diskret matematikk om vi prøver å forstå potensmengden til en uendelig mengde.
- Cantor viste at i en viss forstand er potensmengden til $A$ alltid ekte større enn $A$.



## Ordnede par

- Vi har brukt mengden $\mathbb{R}^2$ av tallpar i tidligere eksempler.
- Alle vet at det er forskjell på tallparene $(2, 3)$ og $(3, 2)$ i $\mathbb{R}^2$.
- Det betyr at rekkefølgen på tallene i paret spiller en rolle.
- Et slikt par kaller vi et ordnet par.



## Ordnede par

- Det er ikke bare tall som kan opptre i par.
- Vi kan for eksempel skrive at

  Per og Kari er ektefeller

  og vi mener så absolutt at de utgjør et par.
- I dette tilfellet betyr ikke rekkefølgen noe, men skriver vi

  Kari er kona til Per

  kan vi ikke erstatte det med

  Per er kona til Kari.



## Ordnede par

- Vi trenger begrepet ordnet par for å kunne snakke presist og generelt om visse former for sammenhenger vi kan finne mellom to objekter.
- Disse objektene kan være tall i en tallmengde.
- De kan imidlertid også være data i en base, data som representerer personer, hendelser, adresser, yrker og mye annet det kan være behov for å registrere.
- Derfor vil vi legge en helt generell definisjon til grunn, når vi definerer hva som menes med et ordnet par.

## Ordnede par

### Definisjon

La $a$ og $b$ være to objekter.

Det ordnede paret $(a, b)$ av $a$ og $b$ er $a$ og $b$ skrevet i rekkefølge.

To ordnede par $(a, b)$ og $(c, d)$ er like hvis $a = c$ og $b = d$.

### Merk

- Vi har egentlig ikke sagt hva et ordnet par er for noe, bare knyttet det til at objektene settes i rekkefølge.
- Det er definisjonen av når to ordnede par er like som gir oss den ønskede matematiske presisjonen. Det knytter den abstrakte definisjonen opp til skrivemåten vi benytter.



## Ordnede par

### Definisjon

La $A$ og $B$ være to mengder.

Med det kartesiske produktet $A \times B$ av $A$ og $B$ mener vi

$$A \times B = \{(a, b) \ : \ a \in A \wedge b \in B\}.$$

Betegnelsen henter sitt navn fra den franske matematikeren og filosofen René Descartes.



## Ordnede par

### Eksempel

- La $A$ være mengden av registrerte norske skøyteløpere og $B$ være mengden av tider mellom 1.30.00 og 2.30.00.

  Da vil registreringer av personlige rekorder på 1500m oppfattes som par i $A \times B$
- Hvis $A$ er mengden av ord skrevet med latinske bokstaver og $B$ er mengden av sider på nettet, leter vi i prinsippet gjennom $A \times B$ når vi søker etter nettsider hvor et bestemt ord forekommer.

  I dette tilfellet er det klart at vi trenger å utvikle spesielle teknikker for å kunne gjøre dette på en effektiv måte, men utviklingen av slike teknikker starter med å forstå kompleksiteten av $A \times B$.



## Ordnede par

Hvis $A$ og $B$ er endelige mengder, vil

$$|A \times B| = |A| \cdot |B|.$$

For de som har lært om matriser, ser vi sammenhengen med en $n \times m$-matrise.

La $A = \{a_1, \cdots, a_n\}$ og $B = \{b_1, \cdots, b_m\}$.

Da kan vi skrive $A \times B$ som:

# Ordnede par

$$\left\{ \begin{array}{ccc} (a_1, b_1) & \cdots\cdots & (a_1, b_m) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ (a_n, b_1) & \cdots\cdots & (a_n, b_m) \end{array} \right\}$$