MAT1030 – Diskret matematikk

Forelesning 10: Mengdelære

Dag Normann

Matematisk Institutt, Universitetet i Oslo

13. februar 2008

Venn-diagrammer

- Mandag innførte vi de Booleske operasjonene
  - Union $\cup$
  - Snitt $\cap$
  - Komplement $\overline{A}$
  - Mengdedifferens $A - B$

  samt de faste mengdene $\emptyset$ og $\mathcal{E}$.

Venn-diagrammer

- Vi tegnet Venn-diagrammet tilhørende de forskjellige Booleske operasjonene, og begynte på eksempler på litt mer avansert bruk av Venn-diagrammer.
- Dette skal vi fortsette med nå, fortsatt på tavlen.

Venn-diagrammer

Eksempel

- deMorgans lover
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- De distributive lovene
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Venn-diagrammer

Eksempel (Fortsatt)

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

Venn-diagrammer

Oppgave

Vi definerer ofte symmetrisk differens ved

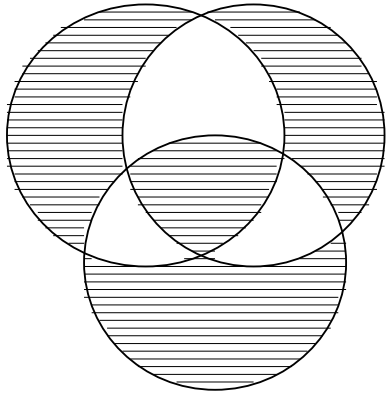
$$A \triangle B = (A - B) \cup (B - A).$$

a) Illustrer $A \triangle B$ ved et Venn-diagram.

b) Vis at $(A \triangle B) \triangle C$ kan illustreres ved Venn-diagrammet på neste side.

c) Drøft hvorfor dette viser at vi kunne skrevet $A \triangle B \triangle C$ uten bruk av parenteser.

Oppgaveillustrasjon



Venn-diagrammer

Oppgave

- Vi bruker bare Venn-diagrammer for uttrykk med en, to eller tre mengder.
- Tegn et Venn-diagram 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 Venn-diagrammer ikke er hensiktsmessige for Booleske 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 forsikret i et forsikringselskap er en delmengde av mengden av dyr forsikret i selskapet.

  Dette er igjen en delmengde av mengden av objekter (dyr, boliger, biler m.m.) som er forsikret i selskapet.

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

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

- Vi skriver

  $$A \subseteq B$$

  for 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

  $$A \subseteq B \wedge A \neq B.$$
- 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 Venn-diagrammer til å vise at et Boolesk uttrykk alltid definerer en delmengde av mengden definert ved et annet Boolesk uttrykk:

Eksempel

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

- I en konkret situasjon kan vi ha inklusjon selv om ikke Venn-diagrammet viser det.

Boolesk algebra

- Det er en nær sammenheng mellom Boolesk 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 vil alltid være like nøyaktig når oversettelsene er logisk ekvivalente.

Boolesk algebra

- Tabell 5.1 på side 79 i læreboka lister noen Booleske identiteter.
- De har sine paralleller i tabellen på side 55 over logikkens lover.
- Vi skal ikke drille regning med dissse Booleske identitetene, men noen av dere vil kunne møte dem igjen i senere emner.

En digresjon

- 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 finnes en mengde som har alle mengder som elementer, leder imidlertid til en motsigelse som kalles Russels Paradoks.
- Vi gir beviset for Russels Paradoks som en oppgave med hint.

Russels 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 $Z \in Z$ vil $Z \notin Z$.
- Vis at hvis $Z \notin Z$ 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 bits 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 Booleske operasjonene.
- Snitt svarer til punktvis multiplikasjon, union svarer til det å ta maksimumsverdien punktvis og komplement svarer til å skifte verdi i alle bits.
- Vi kommer ikke til å jobbe med digital representasjon av mengder på senere forelesninger.
- Digital representasjon av mengder inngår imidlertid i en av oppgavene i første oblig. sett.

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 bits.
- For å kunne følge med på hvor store mengder vi opererer med, og for å kunne resonere 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.

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 finnes det like mange rasjonale tall og hele tall som naturlige tall, mens det finnes 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.

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 finnes 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 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 pr. i dag om det finnes en vesentlig raskere metode til 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 Cartesiske 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 René Descartes, eller Renatus Cartesius som var det latinske navnet han tok seg.

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 antall 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

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

Ordnede par

Eksempel (Fortsatt fra side 34)

- Hvis A er mengden av norske statsborgere, vil $A \times A$ være mengden av par av norske statsborgere.

  Det finnes mange interessante undermengder av $A \times A$ bestemt av de forskjellige forhold det kan være mellom to personer, eksempelvis
  - kollega av
  - søster til
  - nabo av
  - misunnelig på
  - ...

  Dette vil lede oss over til avsnittet om relasjoner.

Relasjoner

Definisjon

La A være en mengde.

En binær relasjon på A er en delmengde R av $A^2 = A \times A$.

Merk

- I senere studier kan dere komme borti relasjoner mellom tre eller flere objekter.

  Disse er da ikke binære.
- Siden vi bare skal studere binære relasjoner, gjør vi som boken, og dropper ordet "binær".

Relasjoner

Eksempel

- La A være mengden av hele tall vi representerer som tidligere beskrevet i en datamaskin.

  La $(a, b) \in R$ hvis $a < b$ mens $(a, b) \in S$ om representasjonen av a er et mindre binært tall enn representasjonen av b.

  Begge relasjonene kan brukes hvis vi skal søke etter et eksempel eller et moteksempel, men søkene kan gi forskjellige resultater.

  Det er lettest å programmere en gjennomsøkning av mengden hvis vi bruker ordningen S.

Relasjoner

Eksempel (Fortsatt)

- I kryptografi er moduloregning viktig.

  Hvis p er et primtall og a og b er hele tall, sier vi at $a \equiv_p b$ om p er en faktor i $a - b$.

  Vi kunne like gjerne skrevet

  $$(a, b) \in \equiv_p .$$

  Relasjonene $\equiv_p$ og beslektede relasjoner (hvor eksempelvis p ikke er et primtall, men i praksis umulig å faktorisere) spiller en stor rolle i arbeidet for sikker overføring av sensitive data.

Relasjoner

Eksempel

- Kompliserte prosesser kan gjerne beskrives ved hjelp av et flyt-diagram.
- Hvert ledd i prosessen blir beskrevet ved en node, og de mulige utviklingene i prosessen blir beskrevet ved piler.
- Vi skal ikke gi noen innføring i flytdiagrammer men se på et enkelt eksempel:
- En sjokoladeautomat kan ta imot 20-kroner, kan gi ut sjokolader til verdier av 10 kroner og 20 kroner, og kan gi vekslepenger.
- Automaten illustreres på tavlen
- Den relevante relasjonen er den som markeres med pilene.

Relasjoner

- Noen lærebøker vil definere en relasjon fra A til B som en mengde

$$R \subseteq A \times B.$$

- Det kan finnes pedagogiske grunner for å gjøre det slik, men enhver relasjon fra A til B vil samtidig være en relasjon på $A \cup B$.

Relasjoner

- Det å beskrive en relasjon som en mengde av ordnede par gir ikke mye innsikt i hvordan relasjonen ser ut.
- Det å skrive $(a, b) \in R$ representerer også en uvant måte å skrive ting på.
- Ingen av oss har lyst til å begynne å skrive $(2, 3) \in <$ i stedenfor $2 < 3$ eller $(3, 3) \in =$ i stedenfor $3 = 3$,
  for ikke å snakke om $(\emptyset, \{\emptyset\}) \in \in$ i stedenfor $\emptyset \in \{\emptyset\}$.
  (Skulle vi finne på noe slikt, ville vi rote oss bort i grunnlagsproblemer som langt overstiger det vi skal ta opp i MAT1030, samt gjøre noe helt unyttig.)
- Den første forenklingen vi skal gøre er å skrive aRb når vi mener $(a, b) \in R$.

Relasjoner

- Hvis A er en relativt liten mengde, finnes det to måter å beskrive R på,
  - Ved hjelp av en matrise
  - Ved hjelp av en graf
- Vi skal se på noen eksempler.
- For begge måter å beskrive relasjoner på spiller det en stor rolle hvordan man organiserer elementene i mengden A,
  - i rekkefølge som koordinater
  - som punkter på en tavle eller et ark

Relasjoner

- La $A = \{1, 2, 3, 4, 5\}$
- La $R = \{(1, 3), (2, 4), (3, 5), (4, 1), (5, 2)\}$
- Vi vil illustrere R ved hjelp av en 5×5-matrise.
- Radene, regnet ovenfra, vil representere 1. koordinat.
- Søylene, regnet fra venstre, vil representere 2. koordinat.
- Vi markerer elementene i R med T og de parene som ikke er med i R med F.
- Det er like vanlig, og av forskjellige grunner bedre, å bruke 1 og 0.

Relasjoner

$$\begin{bmatrix} \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{F} \\ \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \end{bmatrix}$$

Det hadde vært lettere om man hadde brukt farver, eller 1 og 0 for å se hvor "pen" denne relasjonen er.

Den grafiske fremstillingen tar vi på tavlen.

Relasjoner

La $A = \{1, 2, 3, 4\}$ og
$R = \{(1, 2), (1, 3), (1, 4), (4, 1), (3, 1), (2, 1), (3, 3)\}$

Matriseformen blir

$$\begin{bmatrix} \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{T} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \end{bmatrix}$$

- Den grafiske fremstillingen tar vi på tavlen.