INF3170 – Logikk

Forelesning 2: Mengdelære, induktive definisjoner og utsagnslogikk

Roger Antonsen

Institutt for informatikk, Universitetet i Oslo

2. februar 2010

(Sist oppdatert: 2010-02-02 14:26)

Litt mer mengdelære

Litt mer mengdelære

- Multimengder
- Kardinalitet
- Tellbart versus overtellbart

Induktive definisjoner og bevis

Utsagnslogikk

Multimengder

Mengder der antall forekomster av hvert element teller

Definisjon (Multimengde)

En multimengde er et par $\langle S, m \rangle$ der S er en mengde og $m : S \to \mathbb{N}$. For hver $x \in S$ sier vi at $m(x)$ er multiplisiteten til x, eller antall forekomster av x i S.

Eksempel

Vi skriver multimengder som mengder:

- I multimengden $\{a, a, a, b, b\}$ er multiplisiteten til a og b henholdsvis 3 og 2.
- I multimengden $\{a, b, a, c, a, b\}$ er multiplisiteten til a, b og c henholdsvis 3, 2 og 1.

$\cup$, $\cap$, $\setminus$ og $\subseteq$ på multimengder

- Vi bruker union ($\cup$), snitt ($\cap$), mengdedifferans ($\setminus$) og delmengderelasjonen ($\subseteq$) også på multimengder.

Eksempel

- $\{a, a, b, c\} \cup \{a, c\} = \{a, a, a, b, c, c\}$
  dvs. $m(x) = m_1(x) + m_2(x)$
- $\{a, a, a, b, c\} \cap \{a, a, d\} = \{a, a\}$
  dvs. $m(x) = \min(m_1(x), m_2(x))$
- $\{a, a, a, b, c\} \setminus \{a, a, d\} = \{a, b, c\}$
  dvs. $m(x) = \max(0, m_1(x) - m_2(x))$
- $\{a, a\} \subseteq \{a, a, b, c\}$, men $\{a, a, a\} \not\subseteq \{a, a, b, c\}$
  dvs. $m_1(x) \leqslant m_2(x)$ for alle x.

- Vi bruker $\emptyset$ om den tomme multimengden.

Kardinalitet

Definisjon (Kardinalitet)

- To mengder S og T har lik kardinalitet hvis det fins en bijeksjon fra S til T.
- Mengden S har kardinalitet mindre eller lik T hvis det fins en injektiv funksjon fra S til T.
- Hvis S er en endelig mengde, så er kardinaliteten til S lik antall elementer i S.
- Vi bruker notasjonen $|S|$ for kardinaliteten til S.

Teorem (Bernstein)

Hvis det finnes en injektiv funksjon $f : S \to T$ og en injektiv funksjon $g : T \to S$, så fins det også en bijeksjon $h : S \to T$.

Kardinalitet

Eksempel

Hva er kardinaliteten til

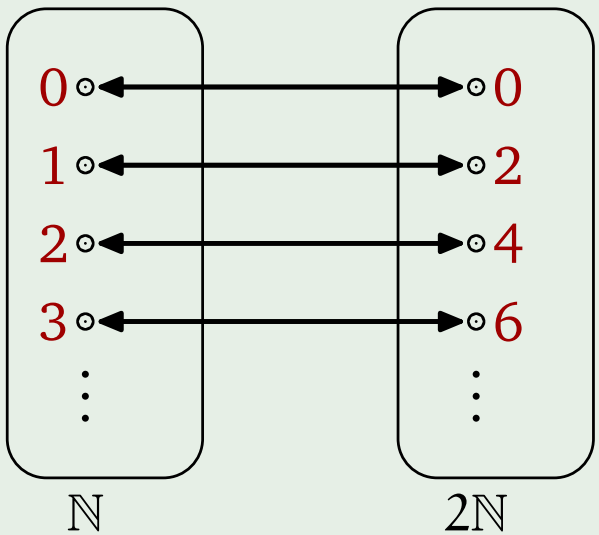
- $\{a, b, c\}$?
- $\{a, b, a\}$?
- $\{a\}$?
- $\emptyset$?

Kardinalitet

Eksempel

- $\mathbb{N}$ = mengden av alle naturlige tall $\{0, 1, 2, 3, 4, \ldots\}$
- $2\mathbb{N}$ = mengden av alle partall $\{0, 2, 4, 6, 8, \ldots\}$

$f(x) = 2x$ er en bijeksjon fra $\mathbb{N}$ til $2\mathbb{N}$, så $\mathbb{N}$ og $2\mathbb{N}$ har samme kardinalitet. Vi skriver $|\mathbb{N}| = |2\mathbb{N}|$.



Tellbart versus overtellbart

Definisjon (Tellbar)

En uendelig mengde S er tellbar hvis det fins en en-til-en korrespondanse mellom elementene i S og de naturlige tallene. Hvis ikke, er S overtellbar.

- Alle endelige mengder er tellbare.
- Når en uendelig mengde S er tellbar fins det en bijektiv funksjon fra S til $\mathbb{N}$.

Eksempel

- Mengden $2\mathbb{N}$ av alle partall er tellbar.
- Mengden $\mathbb{B}$ av binære tall er tellbar.
- Mengden $\mathbb{Q}$ av brøktall er tellbar.
- Mengden av nålevende mennesker er tellbar.
- Mengden $\mathbb{R}$ av reelle tall er ikke tellbar.

Induktive definisjoner og bevis

Litt mer mengdelære

Induktive definisjoner og bevis

- Induktive definisjoner
- Rekursive funksjoner
- Induktive bevis

Utsagnslogikk

Induktive definisjoner

Definisjon (Induktiv definisjon)

Å definere en mengde induktivt betyr å konstruere den minste mengden som inneholder en gitt mengde B—kalt en basismengde—og som er lukket under gitte operasjoner.

Eksempel

Mengden $\mathbb{N}$ av naturlige tall kan defineres induktivt som den minste mengden $\mathbb{N}$ som er slik at

- $0 \in \mathbb{N}$, og
- hvis $x \in \mathbb{N}$, så $x + 1 \in \mathbb{N}$.

Her er basismengden $\{0\}$ og $\mathbb{N}$ er lukket under suksessorfunksjonen $(x+1)$.

Eksempel

Mengden $\mathbb{B}$ av binære tall kan defineres induktivt som den minste mengden $\mathbb{B}$ som er slik at

- 0 og 1 er binære tall, og
- hvis b er et binært tall, så er b0 og b1 binære tall.

steg 0: 0 1

steg 1: 00 10 01 11

steg 2: 000 100 010 110 001 101 011 111

⋮

Eksempel

Mengden S av symmetriske strenger over alfabetet $\{a, b\}$ kan defineres induktivt som den minste mengden S som er slik at

- $\epsilon \in S$ (den tomme strengen),
- hvis $x \in S$, så $axa \in S$ og $bxb \in S$.

steg 0: ϵ
steg 1: aa bb
steg 2: $aaaa$ $abba$ $baab$ $bbbb$
$\vdots$

Hvorfor den minste mengden?

Det er mange mengder som inkluderer basismengden B og som er lukket under gitte operasjoner.

Eksempel

Hvilke mengder N oppfyller:

- $0 \in N$, og
- hvis $x \in N$, så $x + 1 \in N$?

For eksempel:

- $\mathbb{N}$
- $\mathbb{Z}$
- $\{0, \frac{1}{2}, 1, \frac{3}{2}, \ldots\}$

Hva betyr egentlig 'minst'?

- La
$$S := \{M \mid B \subseteq M \text{ og } M \text{ er lukket under operasjonene}\}$$
- S inneholder alle M som oppfyller kravene
- Ta snittet av alle sånne mengder:
$$M^* := \bigcap S$$
- Da er $M^* \in S$.
- Også er $M^* \subseteq M$ for alle $M \in S$.
- Hvis det fins en mengde $N \in S$ som er slik at $N \subseteq M$ for alle $M \in S$, så er $N = M^*$.
- M^* er altså den entydig minste mengden i S med hensyn til $\subseteq$.

Rekursive funksjoner

Hvis en mengde M er definert induktivt, så er det naturlig å definere rekursive funksjoner fra M til en mengde X på følgende måte.

Eksempel

Definer funksjonen $d : \mathbb{N} \to \mathbb{N}$ rekursivt ved

- $d(0) = 0$, og
- $d(n+1) = d(n) + 1 + 1$, for alle $n \in \mathbb{N}$.

Eksempel (Verdien til et binært tall)

- $\nu(0) = 0$
- $\nu(1) = 1$
- $\nu(b0) = 2\nu(b)$, for alle $b \in \mathbb{B}$
- $\nu(b1) = 2\nu(b) + 1$, for alle $b \in \mathbb{B}$

Eksempel (Lengden av symmetrisk streng)

- $l(\epsilon) = 0$
- $l(axa) = l(x) + 2$, for alle $x \in S$
- $l(bxb) = l(x) + 2$, for alle $x \in S$

Induktive bevis

For å vise at alle naturlige tall $n \in \mathbb{N}$ har en egenskap P:

- Vis at egenskapen holder for 0, dvs. at $P(0)$ er sann.
- For alle $n \in \mathbb{N}$ som er slik at $P(n)$ er sann, vis at $P(n+1)$ er sann.

Eksempel

For å vise at $d(n) = 2n$ for alle $n \in \mathbb{N}$, la $P(n)$ stå for "$d(n) = 2n$".

- Vis først at $P(0)$ er sann: $d(0) = 2 \cdot 0$ ved defininsjonen av d.
- Anta at $P(n)$ er sann, dvs. at $d(n) = 2n$, og vis at $P(n+1)$ er sann, dvs. at $d(n+1) = 2(n+1)$.

Induktive bevis

For å vise at alle binære tall $b \in \mathbb{B}$ har en egenskap P:

- Vis at egenskapen holder for 0, dvs. at $P(0)$.
- Vis at egenskapen holder for 1, dvs. at $P(1)$.
- For alle $b \in \mathbb{B}$ med $P(b)$, vis at $P(b0)$.
- For alle $n \in \mathbb{B}$ med $P(b)$, vis at $P(b1)$.

For å vise at alle symmetriske strenger $x \in S$ har en egenskap P.

- Vis at egenskapen holder for ϵ, dvs. at $P(\epsilon)$.
- For alle $x \in S$ med $P(x)$, vis at $P(axa)$.
- For alle $x \in s$ med $P(x)$, vis at $P(bxb)$.

Induktive bevis

Eksempel

Vis at $\nu(b) = \nu(0b)$ for alle $b \in \mathbb{B}$.

- La $P(b)$ stå for "$\nu(b) = \nu(0b)$".
- $P(0)$ er sann: $\nu(0) = 0 = 2 \cdot 0 = 2\nu(0) = \nu(00)$
- $P(1)$ er sann: $\nu(1) = 1 = 2 \cdot 0 + 1 = 2\nu(0) + 1 = \nu(01)$
- Anta at $P(b)$ er sann, dvs. at $\nu(b) = \nu(0b)$.
  - $P(b0)$ er sann: $\nu(b0) = 2\nu(b) = 2\nu(0b) = \nu(0b0)$
  - $P(b1)$ er sann: $\nu(b1) = 2\nu(b) + 1 = 2\nu(0b) + 1 = \nu(0b1)$

Hvorfor er strukturell induksjon korrekt?

- La M være en induktivt definert mengde og P en egenskap.
- Undersøk mengden N av alle x i M som er slik at $P(x)$ er sann.
- Se på et induktivt bevis.
  - Basissteg: $P(b)$ for alle $b \in B$, og det betyr at $B \subseteq N$.
  - Induksjonssteg: $P(x)$ og $P(y)$ impliserer $P(f(x, y))$ for alle $x, y \in M$, og det betyr at $f(x, y) \in N$ for alle $x, y \in N$.
- Men, da må $N \in S$, som vi definerte tidligere.
- Siden M er minst i S, må $M \subseteq N$.
- Med andre ord, $P(x)$ for alle $x \in M$.

Utsagnslogikk

Litt mer mengdelære

Induktive definisjoner og bevis

Utsagnslogikk
- Utsagnslogikk
- Syntaks
- Strukturell induksjon

Utsagnslogikk

Utsagnslogikk er studiet av de utsagnslogiske konnektivene.

- Vi starter med en mengde atomære utsagn, f.eks.
  - *"broen er stengt"*, og
  - *"IFI2 bygges"*.
- Den interne strukturen til atomære utsagn blir ikke analysert.
- Atomære utsagn er enten sanne eller usanne.

Utsagnslogikk

- Sammensatte utsagn bygges opp fra de atomære utsagnene ved hjelp av de logiske konnektivene: *og*, *eller*, *ikke*, *hvis . . . så . . .*
- Eksempel: *"IFI2 bygges og broen er stengt"*
- Hvordan avhenger sannhetsverdien til et sammensatt utsagn av sannhetsverdiene til de atomære utsagnene det er bygget opp av?
- Hvilke utsagn er sanne *uavhengig* av sannhetsverdiene til de atomære utsagnene?
- Slike utsagn kalles tautologier.
- Eksempel: *"IFI2 bygges eller IFI2 bygges ikke"*

Utsagnslogikk

- Syntaks: et presist definert symbolspråk for å representere utsagnslogiske utsagn.
- Semantikk: en presist definert tolkning av uttrykk i symbolspråket til sannhetsverdiene *sann* og *usann*.
- Kalkyle: syntaktisk manipulasjon av uttrykk i symbolspråket for å finne bevisbare uttrykk.
- Sunnhet: alle bevisbare uttrykk er tautologier — korrekthet av kalkylen.
- Kompletthet: alle tautologier er bevisbare — kalkylen sterk nok til å fange inn *alle* interessante uttrykk.

Syntaks

Definisjon (Utsagnsvariable)

Mengden av utsagnsvariable er en tellbart uendelig mengde $\mathcal{V}_u = \{P_1, P_2, P_3, \ldots\}$.

- Utsagnsvariable representerer atomære utsagn, f.eks.:
  - *"IFI2 bygges"*
  - *"Forskningsparken er yngre enn IFI1"*
  - *"logikk er gøy"*

Notasjon

Vi skriver ofte utsagnsvariable som $P, Q, R, \ldots$

Syntaks

For å fange inn sammensatte utsagn, f.eks.

"hvis IFI2 bygges, så er broen stengt,"

trengs flere symboler i språket:

Definisjon (Utsagnslogisk alfabet)

Det utsagnslogiske alfabet består av:

- Utsagnsvariablene i $\mathcal{V}_u$.
- De logiske konnektivene $\wedge$, $\vee$, $\rightarrow$ og $\neg$.
- Hjelpesymbolene '(' og ')'.

Intuisjon: $\neg$ skal bety *"ikke"* $\wedge$ skal bety *"og"*
$\vee$ skal bety *"eller"* $\rightarrow$ skal bety *"impliserer"*

Utsagnslogiske formler

Definisjon (Atomær formel)

Enhver utsagnsvariabel er en atomær formel.

Definisjon (Utsagnslogisk formel)

Mengden av utsagnslogiske formler er den minste mengden $\mathfrak{F}_u$ slik at:

1. $\mathfrak{F}_u$ inneholder alle atomære formler.
2. Hvis $A \in \mathfrak{F}_u$, så er $\neg A \in \mathfrak{F}_u$.
3. Hvis $A, B \in \mathfrak{F}_u$, så er $(A \wedge B)$, $(A \vee B)$ og $(A \rightarrow B)$ med i $\mathfrak{F}_u$.

Eksempel (Utsagnslogiske formler)

- P
- $(P \rightarrow Q)$
- $((P \vee Q) \wedge \neg(P \vee R))$

Notasjon

Vi dropper ofte unødvendige parenteser:

$(P \rightarrow Q)$	skrives	$P \rightarrow Q$
$((P \vee Q) \wedge \neg(P \vee R))$	skrives	$(P \vee Q) \wedge \neg(P \vee R)$

Eksempel

Ikke alle strenger over det utsagnslogiske alfabet er utsagnslogiske formler:

- $P \rightarrow$
- $((Q \wedge P)$

Oppgave

Vis at $((Q \wedge P)$ *ikke* er en utsagnslogisk formel.

- Intuitivt, men hvordan bevise det?
- Ved såkalt strukturell induksjon kan vi vise noe sterkere:

Påstand

Alle utsagnslogiske formler har like mange venstre- og høyreparenteser.

Strukturell induksjon

- Mengden $\mathcal{F}_u$ av utsagnslogiske formler er definert induktivt.
- Ved strukturell induksjon kan man da vise at en egenskap holder for alle formler i $\mathcal{F}_u$.

Teorem (Strukturell induksjon)

Alle formler i $\mathcal{F}_u$ har egenskapen **P** hvis:
Basissteg: Alle atomære formler har egenskapen **P**.
Induksjonssteg:

- Hvis A har egenskapen **P**, så har også $\neg A$ egenskapen **P**.
- Hvis A og B har egenskapen **P**, så har også $(A \wedge B)$, $(A \vee B)$ og $(A \rightarrow B)$ egenskapen **P**.

- Strukturell induksjon er en bevisteknikk vi kommer til å bruke mye!
- Derfor er det viktig å kunne den godt...

Påstand (Balanserte parenteser)

Alle formler $A \in \mathcal{F}_u$ har like mange venstre- og høyreparenteser.

Bevis.

Basissteg: Hvis A er atomær, inneholder den ikke parenteser. Dermed holder påstanden trivielt.

Induksjonssteg:

- Anta $A = \neg B$ og at påstanden holder for B. A har like mange parenteser som B. Dermed holder påstanden også for A.
- Anta $A = (B \circ C)$ for $\circ \in \{\wedge, \vee, \rightarrow\}$, og at påstanden holder for B og C. A har én venstre- og én høyreparentes i tillegg til de som finnes i B og C. Siden påstanden holder for B og C, holder den også for A.

□

Tilbake til uttrykket $((Q \wedge P)$:

Påstand

$((Q \wedge P)$ er *ikke* en utsagnslogisk formel.

Bevis.

1. Vi har vist at alle utsagnslogiske formler har like mange venstre- og høyreparenteser.
2. Det kontrapositive er at hvis et uttrykk *ikke* har like mange venstre- og høyreparenteser, så er det *ikke* en utsagnslogisk formel.
3. Uttrykket '$((Q \wedge P)$' har to venstre- og én høyreparentes, altså ulikt antall.
4. Derfor er det ikke en utsagnslogisk formel.

□