INF3170 – Logikk

Forelesning 1: Introduksjon og mengdelære

Christian Mahesh Hansen

Institutt for informatikk, Universitetet i Oslo

22. januar 2007

Dagens plan

- Foreleser:
  - Christian Mahesh Hansen (chrisha@ifi.uio.no)
  - Kontor 2403, 2. etasje, Ifi
  - Gjesteforelesere i løpet av semesteret?
- Nettside:
  - http://www.ifi.uio.no/inf3170
- Forelesning:
  - Mandag 14:15 – 16:00
  - Lille auditorium
- Gruppeundervisning:
  - Onsdag 12:15 – 14:00, 3A, Ifi
  - Første gruppetime: onsdag 31. januar
  - Gruppelærere:
    - Bjarne Holen (bjarneh@ifi.uio.no)
    - Arild Waaler (arild@ifi.uio.no)

Obliger og eksamen

Obliger

- Planlagt 3 obliger.
- Se hjemmesiden for tidsfrister og regler.
- Bedømmes til bestått/ikke bestått.
- Alle obligene må bestås for å kunne gå opp til eksamen.

Eksamen

- Ingen midttermineksamen.
- Avsluttende eksamen: muntlig *eller* skriftlig.
- Bokstavkarakterer – avsluttende eksamen teller 100%

Pensum

- Definert av det som gjennomgås på forelesning og gruppeundervisning, samt obliger.
- Foiler deles ut på forelesning og legges ut på nettsiden.
- Ingen lærebok, men...

Støttelitteratur

Ikke pensum i seg selv, frivillig ekstralesing!

J. Gallier.
Logic for Computer Science - Foundations of Automated Theorem Proving

- Ligger tett opptil forelest pensum i kurset.
- Oppdatert versjon fra 2003 tilgjengelig for gratis nedlasting.
- Kun kapitlene 3, 4, 5 og 8 er aktuelle.

M. C. Fitting.
First-Order Logic and Automated Theorem Proving

Tenk deg en verden...

...der setninger er enten sanne eller usanne.

Eksempel

Setning: "Ole liker logikk."

- *Hvis "Ole liker logikk" er sann, så er setningen sann.*
- *Hvis "Ole liker logikk" er usann, så er setningen usann.*
- *Setningens sannhetsverdi avhenger av hvorvidt "Ole liker logikk" er sann eller usann.*

Sann-eller-usann-verden

Eksempel

Setning: "Ole liker logikk og Ole liker programmering."

- *Hvis både "Ole liker logikk" og "Ole liker programmering" er sanne, så er setningen sann.*
- *Hvis "Ole liker logikk" eller "Ole liker programmering" er usann, så er setningen usann.*
- *Setningens sannhetsverdi avhenger av sannhetsverdien til "Ole liker logikk" og "Ole liker programmering".*

Sann-eller-usann-verden

Eksempel

Setning: "Ole liker logikk eller Ole liker ikke logikk."

- *Hvis "Ole liker logikk" er usann, så er "Ole liker ikke logikk" sann.*
- *Hvis "Ole liker logikk" er sann, så er "Ole liker ikke logikk" usann.*
- *Setningens sannhetsverdi er helt uavhengig av sannhetverdien til "Ole liker logikk"!*
- *Det er umulig å gjøre setningen usann, den er sann på grunn av måten den er konstruert på.*

Oversikt over kurset

- Logisk symbolspråk – bygge opp formelle setninger.
- Semantikk – en presis måte å tolke formelle setninger på.
- Logisk kalkyle – regneregler for å finne ut om en formell setning alltid er sann uavhengig av tolkning.
- Sunnhet og kompletthet av logiske kalkyler.
- Nyttige teknikker for å lage søkealgoritmer for logiske kalkyler.

Oppgave

Setning: "Det finnes en person x slik at hvis x liker logikk så liker alle personer logikk."

- *Er det mulig å gjøre denne setningen usann. . . ?*

Mengder

Definisjon

- *En* mengde *er en endelig eller uendelig samling objekter der innbyrdes rekkefølge og antall forekomster av hvert objekt ignoreres.*
- *Objektene i en mengde kalles* elementer.
- *Hvis a er element i mengden S, skriver vi $a \in S$. Hvis a ikke er element i S, skriver vi $a \notin S$.*
- *To mengder S og T er* like, *$S = T$, hvis de inneholder de samme elementene.*

Notasjon

Mengden med elementene a, b, c og d skrives ofte $\{a, b, c, d\}$.

Mengder

Eksempel

- $a \in \{a, b, c\}$
- $d \notin \{a, b, c\}$
- $1 \in \{a, 1, \gamma, \Phi\}$
- $2 \notin \{a, 1, \gamma, \Phi\}$
- $\{a, b\} = \{b, a\}$
- $\{a, a, b\} = \{a, b\}$
- $\{a, b\} \neq \{b, c\}$ *(mengdene er* ulike*)*

Noen spesielle mengder

Definisjon (Den tomme mengden)

- *Den* tomme mengden *er mengden som ikke inneholder noen elementer.*
- *Skrives ofte $\{\}$ eller $\emptyset$.*

Definisjon (Singletonmengde)

En singletonmengde *er en mengde som har nøyaktig ett element.*

Eksempel

Både $\{a\}$, $\{b\}$ og $\{b, b\}$ er singletonmengder.

Union – slå sammen mengder

Definisjon (Union)

- Unionen *av to mengder S og T er den mengden som inneholder alle objekter som er element i S eller T.*
- *Unionen av S og T skrives ofte $S \cup T$.*

Eksempel

- $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$
- $\{a, b\} \cup \{b, c\} = \{a, b, c\}$
- $\{1, 2, 3\} \cup \emptyset = \{1, 2, 3\}$

Snitt – felles elementer

Definisjon (Snitt)

- *Hvis S og T er mengder, så er snittet mellom S og T, eller S snittet med T, mengden som inneholder alle objekter som er element i både S og T.*
- *S snittet med T skrives ofte $S \cap T$.*

Eksempel

- $\{a, b\} \cap \{c, d\} = \emptyset$
- $\{a, b\} \cap \{b, c\} = \{b\}$
- $\{1, 2, 3\} \cap \emptyset = \emptyset$

Mengdedifferanse – fjerne elementer

Definisjon (Mengdedifferanse)

- *Hvis S og T er mengder, så er mengdedifferansen mellom S og T, eller S minus T, mengden som inneholder alle objekter som er element i S men ikke element i T.*
- *S minus T skrives ofte $S \setminus T$.*

Eksempel

- $\{a, b\} \setminus \{c, d\} = \{a, b\}$
- $\{a, b\} \setminus \{b, c\} = \{a\}$
- $\{1, 2, 3\} \setminus \emptyset = \{1, 2, 3\}$
- $\emptyset \setminus \{a, b, c\} = \emptyset$

Delmengde

Definisjon (Delmengde)

- *En mengde S er en delmengde av en mengde T hvis alle elementer i S også er elementer i T.*
- *Skrives ofte $S \subseteq T$.*

Eksempel

- $\{a, b\} \subseteq \{a, b, c\}$
- $\{a, b\} \subseteq \{a, b\}$ *(enhver mengde er en delmengde av seg selv)*
- $\{a, b, c\} \not\subseteq \{a, b\}$
- $\emptyset \subseteq \{a, b\}$ *(den tomme mengden er en delmengde av alle mengder)*
- $\{a, b\} \not\subseteq \emptyset$

Kryssprodukt

Definisjon (Kryssprodukt)

- *Hvis S og T er mengder, så er kryssproduktet av S og T mengden av alle par $\langle s, t\rangle$ slik at $s \in S$ og $t \in T$.*
- *Kryssproduktet av S og T skrives ofte $S \times T$.*

Eksempel

- $\{a, b\} \times \{c, d\} = \{\langle a, c\rangle, \langle a, d\rangle, \langle b, c\rangle, \langle b, d\rangle\}$
- $\{a, b\} \times \{b, c\} = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, b\rangle, \langle b, c\rangle\}$
- $\{a\} \times \{1, 2\} = \{\langle a, 1\rangle, \langle a, 2\rangle\}$

Kryssprodukt

Notasjon

- *En mengde kan krysses med seg selv:* $S \times S$
- $\{a, b\} \times \{a, b\} = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle\}$
- $S \times S \times S$ *skrives ofte* S^3.
- *Generalisert:* $\underbrace{S \times S \times \ldots \times S}_{n}$ *skrives* S^n.

Mengdebygger

Notasjon

En definisjon på formen "mengden av alle elementer $x \in S$ *slik at ..." kan skrives på formen*

$$\{x \mid x \in S \text{ og betingelse på } x\}.$$

En slik konstruksjon kalles en mengdebygger.

Eksempel

- *Definisjonen av kryssprodukt av* S *og* T *kunne vært skrevet slik:*

$$S \times T = \{\langle s, t\rangle \mid s \in S \text{ og } t \in T\}$$

- $\{n \mid n \in \mathbb{N} \text{ og } n \text{ er partall }\}$ *definerer mengden av alle partall.*
- $\{n \mid n \in \mathbb{N} \text{ og } n \text{ er oddetall }\}$ *definerer mengden av alle oddetall.*

Relasjoner

Definisjon (Relasjon)

- *En unær relasjon over* S *er en delmengde av* S.
- *En binær relasjon fra* S *til* T *er en delmengde av* $S \times T$.
- *En n-ær relasjon over mengdene* $S_1, S_2, \ldots, S_n$ *er en delmengde av kryssproduktet* $S_1 \times S_2 \times \ldots \times S_n$.

Eksempel

- *Hvis* $S = \{a, b, c\}$, *så er* $\{a, b\}$ *en unær relasjon over* S.
- *Hvis* $S = \{a, b\}$ *og* $T = \{1, 2\}$, *så er* $\{\langle a, 1\rangle, \langle b, 2\rangle\}$ *en binær relasjon fra* S *til* T.

Relasjoner over én mengde

Definisjon

En n-ær relasjon over mengden S *er en delmengde av* S^n.

Eksempel

La $S = \{1, 2, 3\}$.

- $\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$ *er en binær relasjon over* S.
- $\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$ *er også en binær relasjon over* S.

Refleksive relasjoner

Definisjon (Refleksiv)

En binær relasjon R over mengden S er refleksiv *hvis $\langle x, x\rangle \in R$ for alle $x \in S$.*

Eksempel

La $S = \{1, 2, 3\}$.

- *Er $R_1 = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle\}$ refleksiv?*
- *Hva med $R_2 = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$?*

Symmetriske relasjoner

Definisjon (Symmetrisk)

En binær relasjon R er symmetrisk *hvis $\langle x, y\rangle \in R$ impliserer at $\langle y, x\rangle \in R$.*

Eksempel

La $S = \{1, 2, 3\}$.

- *Er $R_1 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle, \langle 2, 3\rangle\}$ symmetrisk?*
- *Hva med $R_2 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 1, 3\rangle\}$?*

Transitive relasjoner

Definisjon (Transitiv)

En binær relasjon R er transitiv *hvis $\langle x, y\rangle \in R$ og $\langle y, z\rangle \in R$ impliserer at $\langle x, z\rangle \in R$.*

Definisjon (Ekvivalensrelasjon)

En binær relasjon over mengden S er en ekvivalensrelasjon *hvis den er refleksiv, symmetrisk og transitiv.*

Funksjoner

Definisjon (Funksjon)

La S og T være mengder. En funksjon *f fra S til T er en binær relasjon fra S til T med følgende egenskaper:*

- *For alle $x \in S$ så finnes en $y \in T$ slik at $\langle x, y\rangle \in f$.*
- *Hvis $\langle x, y\rangle \in f$ og $\langle x, z\rangle \in f$, så er $y = z$.*

Vi kaller S for definisjonsmengden *til f og T for* verdimengden *til f.*

Notasjon

Hvis $\langle x, y\rangle \in f$, så skriver vi ofte $f(x) = y$.

Funksjoner

Eksempel

Funksjonen Par $: \mathbb{N} \rightarrow \{0, 1\}$ *definert ved*

$$Par(x) = \begin{cases} 1 \text{ hvis } x \text{ er et partall} \\ 0 \text{ hvis } x \text{ er et oddetall} \end{cases}$$

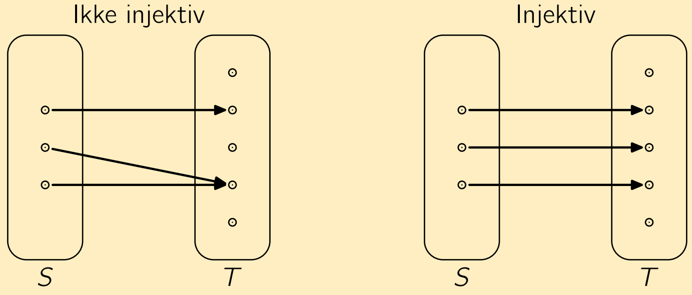
har $\mathbb{N}$ *som definisjonsmengde og* $\{0, 1\}$ *som verdimengde.*

Injektive funksjoner

Definisjon (Injektiv)

En funksjon $f : S \rightarrow T$ *er injektiv hvis for alle* $x, y \in S$ *så impliserer* $x \neq y$ *at* $f(x) \neq f(y)$. *Vi sier at* f *er en-til-en.*

Eksempel

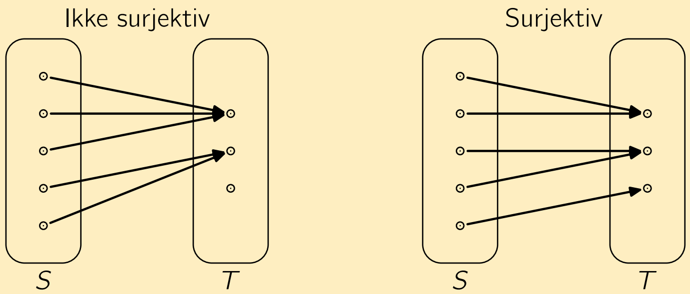


Surjektive funksjoner

Definisjon (Surjektiv)

En funksjon $f : S \rightarrow T$ *er surjektiv hvis for alle* $y \in T$ *så fins* $x \in S$ *slik at* $f(x) = y$. *Vi sier at* f *er på.*

Eksempel



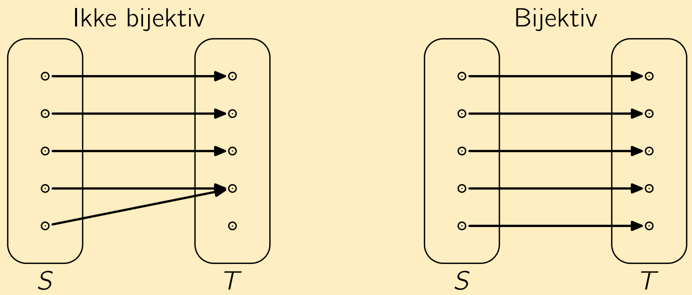
Bijektive funksjoner

Definisjon (Bijektiv)

En funksjon er bijektiv hvis den er injektiv og surjektiv.

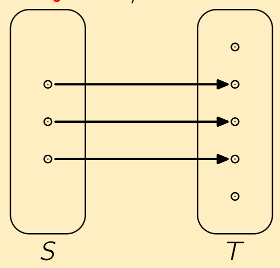
Vi sier at funksjonen er en-til-en og på, eller at vi har en en-til-en korrespondanse.

Eksempel



Injektive og surjektive funksjoner

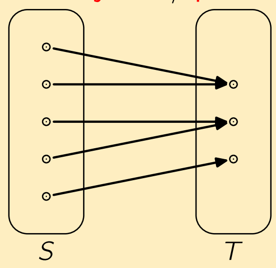
injektiv / en-til-en



for alle $x, y \in S$:
$x \neq y$ impliserer $f(x) \neq f(y)$

"hvert element i definisjonsmengden sendes til et unikt element i verdimengden"

surjektiv / på

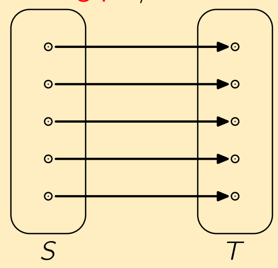


for alle $y \in T$:
det finnes $x \in S$ slik at $f(x) = y$

"alle elementer i verdimengden blir truffet"

Bijektive funksjoner

bijektiv / en-til-en og på / en-til-en korrespondanse



- En bijektiv funksjon er en funksjon som er både *injektiv* og *surjektiv*:
- *"Ethvert element i verdimengden blir truffet av et unikt element i definisjonsmengden"*.

Operatorer

Definisjon (Operator)

La S være en mengde.

- *En unær operator på S er en funksjon fra S til S.*
- *En binær operator på S er en funksjon fra $S \times S$ til S.*

Eksempel

- *Suksessorfunksjonen $(n+1)$ er en unær operator på $\mathbb{N}$.*
- *Addisjonsfunksjonen $(+)$ er en binær operator på $\mathbb{N}$.*
- *Subtraksjonsfunksjonen $(-)$ er en binær operator på $\mathbb{Z}$.*

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

- $\{a, a, b, c\} \cup \{a, c\} = \{a, a, a, b, c, c\}$
- $\{a, a, a, b, c\} \cap \{a, a, d\} = \{a, a\}$
- $\{a, a, a, b, c\} \setminus \{a, a, d\} = \{a, b, c\}$
- $\{a, a\} \subseteq \{a, a, b, c\}$, *men* $\{a, a, a\} \not\subseteq \{a, a, b, c\}$

- 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.*

Eksempel

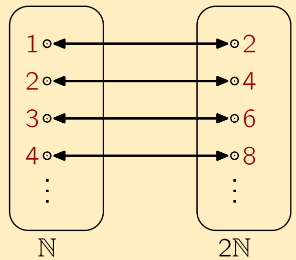
Hva er kardinaliteten til

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

Eksempel

- $\mathbb{N}$ = *mengden av alle naturlige tall* $\{1, 2, 3, 4, 5, \ldots\}$
- $2\mathbb{N}$ = *mengden av alle partall* $\{2, 4, 6, 8, 10, \ldots\}$

$f(x) = 2x$ 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 vs. 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.*