INF3170 – Forelesning 1

Introduksjon og mengdelære

Roger Antonsen - 26. januar 2010

(Sist oppdatert: 2010-01-26 14:58)

Dagens plan

Innhold

Velkommen til INF3710 – Logikk

Litt praktisk informasjon

- Forelesere
  - Roger Antonsen (`rantonse@ifi.uio.no`)
  - Kontor 2403, 2. etasje, Informatikkbygningen
  - Kurset gis på *dugnad* og det blir flere forelesere i løpet av semesteret.
- Forelesninger
  - Tirsdager 12:15–14:00
  - Lille auditorium
- Gruppeundervisning
  - Ingen gruppeundervisning.
- Nettside
  - `http://www.ifi.uio.no/inf3170/`

Obliger og eksamen

- Obligatoriske oppgaver
  - Sannsynligvis 2 obliger; mer informasjon kommer senere.
  - Se hjemmesiden for tidsfrister og regler.
  - Bedømmes til bestått/ikke bestått.
  - Alle obligene må bestås for å kunne gå opp til eksamen.
- Eksamen
  - Avsluttende eksamen: skriftlig *eller* muntlig.
  - Bokstavkarakterer – avsluttende eksamen teller 100%.

Pensum

- Pensum defineres av det som gjennomgås på forelesningene, samt det som deles ut av forelesningsnotater og oppgaver.
- Vi har ingen lærebok, men følgende kan være til nytte som støttelitteratur.
- *Dette er ikke pensum, men frivillig ekstralesing.*

Referanser

[Gallier, 2003] Jean 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.

Referanser

[Fitting, 1996] Melvin C. Fitting. *First-Order Logic and Automated Theorem Proving*

Hva skal vi lære?

Tenk deg en verden...

...der setninger er enten *sanne* eller *usanne*.

Eksempel.
Setning: "Ole liker logikk."

- Hvis Ole liker logikk, så er setningen *sann*.
- Hvis Ole *ikke* liker logikk, så er setningen *usann*.
- Setningens sannhetsverdi avhenger av hvorvidt det er sant at Ole liker logikk.

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”.

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.
- Andre emner fra logikkens verden (hvis vi får tid).

Oppgave.
Setning: “Det fins en person x slik at hvis x liker logikk så liker alle personer logikk.”

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

Mengdelære

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 $\{a, b, c, d\}$.

Eksempel.
(Antagelse: $a, b, c, d, 1, 2, \gamma$ og Φ er alle forskellige.)

- $a \in \{a, b, c\}$
- $d \notin \{a, b, c\}$
- $1 \in \{a, 1, \gamma, \Phi\}$
- $2 \notin \{a, 1, \gamma, \Phi\}$
- $\{a, b\} = \{b, a\}$
- $\{a, a, b\} = \{a, b\}$
- $\{a, b\} \neq \{b, c\}$ (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.

Mengder av mengder
Det er mulig å konstruere mengder som inneholder andre mengder (med visse restriksjoner).

Eksempel.

- $\{\emptyset\} \neq \emptyset$
- $\{\{0\}, \{1\}, \{2\}, \ldots\} = \{\{n\} \mid n \in \mathbb{N}\}$
- $\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \{\{m \mid 0 \leqslant m \leqslant n\} \mid n \in \mathbb{N}\}$
- $\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\}$

Snitt av mengder av mengder

Definisjon.
Snittet av en mengde $\mathcal{M}$ av mengder inneholder alle elementer som er element av alle $M \in \mathcal{M}$:

$$\bigcap \mathcal{M} := \{x \mid x \in M \text{ for alle } M \in \mathcal{M}\}$$

Eksempel.

- $\bigcap\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \{0\}$
- $\bigcap\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\} = \emptyset$

Union av mengder av mengder

Definisjon.
Unionen av en mengde $\mathcal{M}$ av mengder inneholder alle elementer som er element av minst en $M \in \mathcal{M}$:

$$\bigcup \mathcal{M} := \{x \mid x \in M \text{ for noen } M \in \mathcal{M}\}$$

Eksempel.

- $\bigcup\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \mathbb{N}$
- $\bigcup\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\} = \mathbb{N}$

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 $R_2 = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 1,3\rangle\}$?

Anti-symmetriske relasjoner

Definisjon (Anti-symmetrisk).
En binær relasjon R over mengden S er *anti-symmetrisk* hvis $\langle x,y\rangle \in R$ og $\langle y,x\rangle \in R$ impliserer at $x = y$.

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

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

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

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 $f(x) = y$.

Eksempel.
Funksjonen $\mathrm{Par} : \mathbb{N} \to \{0, 1\}$ definert ved

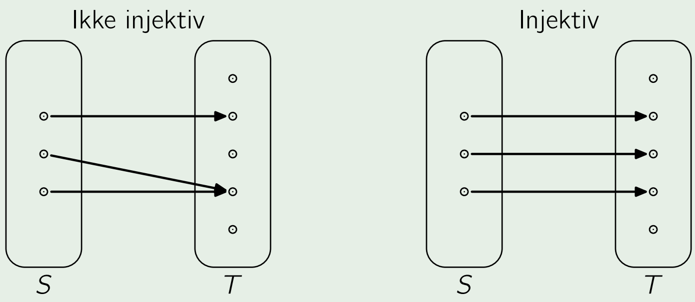
$$\mathrm{Par}(x) = \begin{cases} 1 \text{ hvis } x \text{ er et partall} \\ 0 \text{ hvis } x \text{ er et oddetall} \end{cases}$$

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

Injektive funksjoner

Definisjon (Injektiv).
En funksjon $f : S \to T$ 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*.

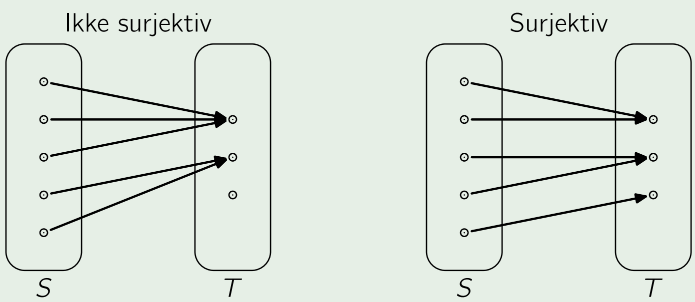
Eksempel.



Surjektive funksjoner

Definisjon (Surjektiv).
En funksjon $f : S \to T$ 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.

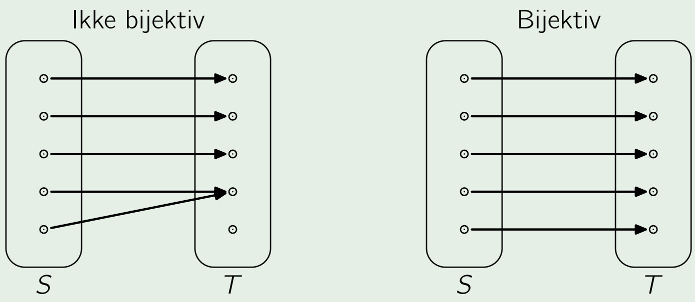


Bijektive funksjoner

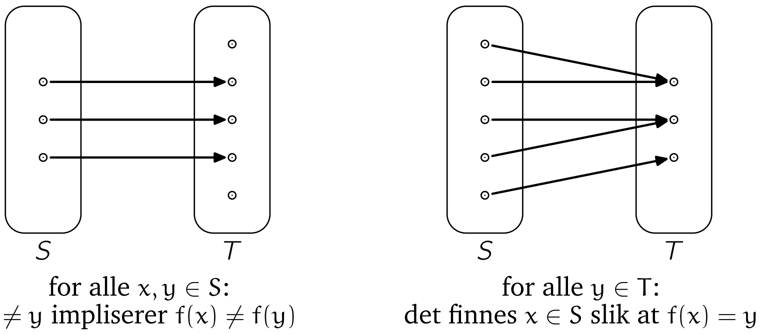
Definisjon (Bijektiv).
En funksjon er *bijektiv* hvis den er injektiv og surjektiv.

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

Eksempel.



Injektive og surjektive funksjoner

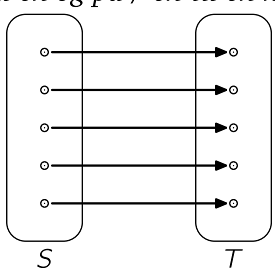


hvert element i definisjonsmengden sendes til et unikt element i verdimengden

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 $\mathbb{Z}$.