Forelesning 4: Repetisjon og førsteordens logikk

Christian Mahesh Hansen - 12. februar 2007

1 Repetisjon

Motivasjon

"Hvis Ole følger inf3170, så liker Ole logikk."
"Ole følger inf3170, og Ole følger ikke inf3170."
"Ole følger inf3170, eller Ole følger ikke inf3170."

- Er utsagnene *sanne*?
- Avhengig av hvordan vi *tolker* utsagnene!
- Finnes det utsagn som alltid er sanne?
- Vi ønsker å en måte å finne slike utsagn på!
- Vi ønsker *matematisk presisjon*, så vi må *formalisere* utsagn og tolkninger.

Formalisering

- Utsagn formaliseres som utsagnslogiske formler.
- Tolkning formaliseres med sannhetsverdier og valuasjoner.

Syntaks: Utsagnslogiske formler

Alfabet

- Utsagnsvariable: $P_1, P_2, P_3, \ldots$
  - Står for *atomære* utsagn, f.eks. *"Ole liker logikk"*.
  - Skrives ofte $P, Q, R, \ldots$ pga. lesbarhet.
- Logiske konnektiver: $\neg$, $\wedge$, $\vee$, $\rightarrow$
  - Brukes til å bygge opp sammensatte utsagn.
- Hjelpesymboler: '(', ')'
  - Brukes for å gi entydig parsing av formler.

- Vi kan lage mange uttrykk med disse symbolene:
  - $((\neg \rightarrow \wedge(($
  - $\rightarrow P \wedge ((PP$
  - $\neg(P \wedge (\neg Q \rightarrow P))$
- Vi er kun interessert i uttrykk som samsvarer med de utsagn vi vil analysere!

Induktiv definisjon – stegvis bygge opp en uendelig mengde

Mengden av utsagnslogiske formler – $\mathcal{F}_u$

Basismengde: Enhver utsagnsvariabel er en utsagnslogisk formel.
Induksjonssteg: Hvis A og B er utsagnslogiske formler, så er

- $\neg A$ en utsagnslogisk formel
- $(A \wedge B)$, $(A \vee B)$ og $(A \to B)$ utsagnslogiske formler.

Basismengde:	$P, Q, R, \ldots$
Steg 1:	$\neg P, \neg Q, \neg R, \ldots$
	$(P \wedge P), (P \wedge Q), (P \wedge R), \ldots$
	$(P \vee P), (P \vee Q), (P \vee R), \ldots$
	$(P \to P), (P \to Q), (P \to R), \ldots$
Steg 2:	$\neg\neg P, \neg\neg Q, \neg\neg R$
	$(P \wedge \neg P), (\neg P \wedge P), (\neg P \wedge \neg P), (P \wedge \neg Q), \ldots$
	$\vdots$

Semantikk: Tolke utsagn – valuasjoner

- Vi skal gi sannhetsverdier, $\mathbf{1}$ eller $\mathbf{0}$, til formler: $(P \to Q) \vee \neg P$
- *Valuasjoner* er funksjoner fra $\mathcal{F}_u$ til $Bool = \{\mathbf{1}, \mathbf{0}\}$ som overholder bestemte regler m.h.p. konnektivene $\neg$, $\wedge$, $\vee$, $\to$.
- Hvorfor overholde konnektivregler?
- La $v(P) = f(P) = \mathbf{1}$ og $v(Q) = f(Q) = \mathbf{0}$, men la $v(P \to Q) = \mathbf{0}$ og $f(P \to Q) = \mathbf{1}$.
  - Begge er funksjoner fra $\mathcal{F}_u$ til **Bool**, men kun v er en valuasjon!
  - f overholder ikke regelen for $\to$: Hvis P tolkes som $\mathbf{1}$ og Q tolkes som $\mathbf{0}$, så skal $P \to Q$ tolkes som $\mathbf{0}$.

Konnektivreglene

Konnektivreglene uttrykkes v.h.a. de boolske operatorene $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$ og $\hat{\to}$.

Oppfylle og falsifisere

- En valuasjon *oppfyller* en utsagnslogisk formel A, $v \models A$, hvis $v(A) = \mathbf{1}$.
- En valuasjon *falsifiserer* en utsagnslogisk formel A, $v \not\models A$, hvis $v(A) = \mathbf{0}$.
- Formelen A er en *tautologi* hvis *alle* valuasjoner oppfyller den.
- Det er det samme som at *ingen* valuasjoner falsifiserer den.

Sekventer og sekventkalkyle

- En *sekvent* er på formen $\Gamma \vdash \Delta$ der Γ og Δ er multimengder av formler.
- En sekvent er *gyldig* hvis enhver valuasjon som oppfyller alle formlene i Γ også oppfyller en formel i Δ.
- En valuasjon v er en *motmodell* til en sekvent $\Gamma \vdash \Delta$ hvis v oppfyller alle formlene i Γ og falsifiserer alle formlene i Δ.
- En sekvent er *falsifiserbar* hvis den har en motmodell.
- En sekventkalkyle er *sunn* hvis enhver bevisbar sekvent er gyldig.
- En sekventkalkyle er *usunn* hvis det finnes en bevisbar sekvent som er falsifiserbar.
- En sekventkalkyle er *komplett* hvis enhver gyldig sekvent er bevisbar.
- En sekventkalkyle er *ukomplett* hvis det finnes en gyldig sekvent som *ikke* er bevisbar.

2 Innledning til førsteordens logikk

2.1 Introduksjon

- I utsagnslogikk kan vi analysere de logiske konnektivene $\neg$, $\wedge$, $\vee$ og $\rightarrow$, og resonnering som gjøres med slike.
- Førsteordens logikk (også kalt predikatlogikk) utvider utsagnslogikk med *kvantorer*:
  - $\exists$ (eksistenskvantoren) og
  - $\forall$ (allkvantoren).
- Vi kan med disse uttrykke påstander om at det finnes et objekt med en bestemt egenskap eller at alle objekter har en bestemt egenskap.
- Førsteordens logikk er langt rikere enn utsagnslogikk.
- Førsteordens logikk er ikke avgjørbart.

Noen eksempler

Noen påstander som vi kan representere og analysere ved førsteordens logikk er følgende:

- "Ethvert heltall er enten partall eller oddetall."
- "Det fins uendelig mange primtall."
- "Mellom to brøktall fins det annet brøktall."
- "Hvis a er mindre enn b og b er mindre enn c, så er a mindre enn c."

Flere eksempler

Av mindre matematisk art:

- "Alle Ifi-studenter er late."
- "Ingen Ifi-studenter er late."
- "Noen Ifi-studenter er late."
- "Alle Ifi-studenter som er late, får problemer på eksamen."
- "Noen Ifi-studenter som er late, får ingen problemer på eksamen."
- "Enhver Ifi-student er enten lat eller ikke lat."
- "Alle bevisbare formler er gyldige."
- "Det fins to sheriffer i byen."

2.2 Overblikk

Syntaks: førsteordens språk og formler – en utvidelse av utsagnslogikk.

Semantikk: tolkninger av førsteordens formler – modeller, sannhet, oppfyllbarhet, gyldighet.

Kalkyle: tillegg av regler.

Sunnhet: alle bevisbare sekventer er gyldige.

Kompletthet: alle gyldige sekventer er bevisbare.

2.3 Syntaks

Definisjon 2.1 (Førsteordens språk - logiske symboler)**.** *Alle førsteordens språk består av følgende logiske symboler:*

- *De logiske konnektivene* $\wedge$, $\vee$, $\rightarrow$ *og* $\neg$.
- *Hjelpesymbolene '(' og ')' og ',' .*
- Kvantorene $\exists$ *(det fins) og* $\forall$ *(for alle).*
- *En tellbart uendelig mengde* $\mathcal{V}$ *av variable* $x_1, x_2, x_3, \ldots$ *(vi skriver* x, y, z, $\ldots$, *for variable).*

Definisjon 2.2 (Førsteordens språk - ikke-logiske symboler)**.** *I tillegg består et førsteordens språk av følgende mengder av ikke-logiske symboler:*

- *En tellbar mengde av konstantsymboler* $c_1, c_2, c_3, \ldots$.
- *En tellbar mengde av funksjonssymboler* $f_1, f_2, f_3, \ldots$.
- *En tellbar mengde av relasjonssymboler* $R_1, R_2, R_3, \ldots$.

Vi antar at mengdene av variable, konstant-, funksjons- og relasjonssymboler er disjunkte, og vi assosierer med ethvert funksjons- og relasjonssymbol et ikke-negativt heltall, kalt ariteten *til symbolet.*

Merk.

- *Det eneste som skiller to førsteordens språk fra hverandre er de ikke-logiske symbolene.*

Definisjon 2.3 (Signatur)**.**

- *De ikke-logiske symbolene utgjør det som kalles en* signatur*.*
- *En signatur angis ved et tuppel* $\langle c_1, c_2, c_3, \ldots; f_1, f_2, f_3, \ldots; R_1, R_2, R_3, \ldots \rangle$*, hvor konstant-, funksjons- og relasjonssymboler er adskilt med semikolon.*

Definisjon 2.4 (Termer)**.** *Mengden* $\mathcal{T}$ *av* første-ordens termer *er induktivt definert som den minste mengden slik at:*

- *Enhver variabel og konstant er en term.*
- *Hvis* f *er et funksjonssymbol med aritet* n *og* $t_1, \ldots, t_n$ *er termer, så er* $f(t_1, \ldots, t_n)$ *en term.*

2.4 Eksempler på førsteordens språk

Et enkelt språk: $\langle a; f, g; P, R \rangle$

- Konstantsymboler: a
- Funksjonssymboler: f (med aritet 1) og g (med aritet 2)
- Relasjonssymboler: P (med aritet 1) og R (med aritet 2)

Termer i dette språket:

- a, x, y, $\ldots$, $f(a)$, $f(x)$, $f(y)$, $\ldots$
- $g(a,a)$, $g(a,x)$, $g(a,y)$, $g(x,x)$, $g(x,y)$, $g(y,y)$, $\ldots$
- $f(f(a))$, $f(f(x))$, $f(f(y))$, $\ldots$

Notasjon. *Så lenge det er entydig og ariteten er kjent, kan vi droppe parentesene og skrive* fa*,* fx*,* fy*,* gaa*,* gax*,* $\ldots$*.*

Et språk for aritmetikk: $\langle 0; s, +; = \rangle$

- Konstantsymboler: 0
- Funksjonssymboler: s (med aritet 1) og $+$ (med aritet 2)
- Relasjonssymboler: $=$

Kommentarer:

- Termer: $x, y, 0, s0, ss0, sss0, +xy, +00, +(s0)0, +0s0, \ldots$
- *Ikke* termer: $= (\mathsf{x}, \mathsf{x}), ++, +0, \ldots$
- Når vi skriver $+xy$ bruker vi *prefiks notasjon*.
- Vi bruker også *infiks notasjon* og skriver: $(x + y), (0 + 0), (s0 + 0), (0 + s0), \ldots$.

Et annet språk for aritmetikk: $\langle 0, 1; +, \times; =, < \rangle$

- Konstantsymboler: $0, 1$
- Funksjonssymboler: $+$ og $\times$ (begge med aritet 2)
- Relasjonssymboler: $=$ og $<$ (begge med aritet 2)

Et språk for mengdelære: $\langle \emptyset; \cap, \cup; =, \in \rangle$

- Konstantsymboler: $\emptyset$
- Funksjonssymboler: $\cap$ og $\cup$ (begge med aritet 2)
- Relasjonssymboler: $=$ og $\in$ (begge med aritet 2)

Et språk for familierelasjoner: $\langle \mathsf{Ola}, \mathsf{Kari}; \mathsf{mor}, \mathsf{far}; \mathsf{Mor}, \mathsf{Far}, \mathsf{Slektning} \rangle$

- Konstantsymboler: Ola og Kari
- Funksjonssymboler: mor, far (begge med aritet 1)
- Relasjonssymboler: Mor, Far, Slektning (alle med aritet 2)

Termer i språket for familierelasjoner:

- x, Ola og Kari er termer.
- mor(Ola), mor(Kari), far(Ola) og far(Kari) er termer.
- mor(x) og far(x) er termer.
- mor(mor(x)) og mor(far(Kari)) er termer.

2.5 Syntaks

Definisjon 2.5 (Atomær formel - førsteordens)**.** *Hvis R er et relasjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer, så er $R(t_1, \ldots, t_n)$ en* atomær formel*.*

Merk.

- *Hvis R har aritet 0, så er R en atomær formel. Dette svarer til utsagnsvariable i utsagnslogikk.*
- *Så lenge det er entydig og ariteten er kjent skriver vi Rx, Rfa, $Rafa$, etc. for $R(x)$, $R(f(a))$ og $R(a, f(a))$.*

Definisjon 2.6 (Førsteordens formler)**.** *Mengden $\mathcal{F}$ av* førsteordens formler *er den minste mengden slik at:*

1. *Alle atomære formler er formler.*
2. *Hvis φ og ψ er formler, så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \to \psi)$ formler.*
3. *Hvis φ er en formel og x er en variabel, så er $\forall x\varphi$ og $\exists x\varphi$ formler.*

Alle forekomster av en variabel x i φ sies å være bundet *i formlene $\forall x\varphi$ og $\exists x\varphi$ og innenfor* skopet *til den gjeldende kvantoren.*

2.6 Eksempler på førsteordens formler

Et språk for beundring: $\langle a, b; ; \mathsf{Idol}, \mathsf{Liker}\rangle$

- Konstantsymboler: a og b
- Funksjonssymboler: (ingen)
- Relasjonssymboler: **Idol** (med aritet 1) og **Liker** (med aritet 2)

Formler i språket:

- Atomære formler: $\mathsf{Idol}(x), \mathsf{Idol}(a), \mathsf{Liker}(a, a), \mathsf{Liker}(a, b)$
- $\exists x\mathsf{Idol}(x)$ - "det fins et Idol"
- $\forall x\exists y\mathsf{Liker}(x, y)$ - "alle liker noen"
- $\forall x\mathsf{Liker}(x, a)$ - "alle liker a"
- $\neg\exists x\mathsf{Liker}(x, b)$ - "ingen liker b"
- $\forall x(\mathsf{Idol}(x) \to \mathsf{Liker}(x, x))$ - "alle idoler liker seg selv"

I språket for aritmetikk $\langle 0; s, +; =\rangle$, så har vi formlene

- $s0 + s0 = ss0$ - "en pluss en er to"

- $\forall x \forall y(x + y = y + x)$ - "addisjon er kommutativt"
- $\forall x \exists y(y = sx)$ - "alle tall har en etterfølger"
- $\neg \exists x(0 = sx)$ - "0 er ikke etterfølgeren til noe"
- $\exists x \exists y \neg(x = y)$ - "det fins to forskjellige objekter"

3 Førsteordens logikk - syntaks

3.1 Repetisjon og presiseringer

Et førsteordens språk $\mathcal{L}$ består av:

1. Logiske symboler
   - konnektiver: $\wedge$, $\vee$, $\rightarrow$ og $\neg$
   - hjelpesymboler: '(' og ')' og ','
   - kvantorer: $\exists$ og $\forall$
   - variable: $\mathcal{V} = \{x_1, x_2, x_3, \ldots\}$
2. Ikke-logiske symboler:
   - en tellbar mengde konstantsymboler
   - en tellbar mengde funksjonssymboler (med aritet)
   - en tellbar mengde relasjonssymboler (med aritet)

- De ikke-logiske symbolene utgjør en *signatur*

  $\langle \underbrace{c_1, c_2, c_3, \ldots}_{konstantsymboler} ; \underbrace{f_1, f_2, f_3, \ldots}_{funksjonssymboler} ; \underbrace{R_1, R_2, R_3, \ldots}_{relasjonssymboler} \rangle$.

Vi så følgende signaturer sist:

enkelt språk:	$\langle$	a	; f, g	;	P, R	$\rangle$
aritmetikk 1:	$\langle$	0	; $s, +$	;	$=$	$\rangle$
aritmetikk 2:	$\langle$	$0, 1$	; $+, \times$	;	$=, <$	$\rangle$
mengdelære:	$\langle$	$\emptyset$	; $\cap, \cup$	;	$=, \in$	$\rangle$
familierelasjoner:	$\langle$	Ola, Kari	; mor, far	;	Mor, Far, Slektning	$\rangle$
beundring:	$\langle$	a, b	;	;	Idol, Liker	$\rangle$

Hvis et førsteordens språk $\mathcal{L}$ er gitt, så får vi (definert induktivt):

1. Mengden $\mathcal{T}$ av termer i $\mathcal{L}$:
   - Enhver variabel og konstant er en term.
   - Hvis f er et funksjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer,så er $f(t_1, ..., t_n)$ en term.

2. Mengden $\mathcal{F}$ av formler i $\mathcal{L}$:

   - Hvis R er et relasjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer,så er $R(t_1, \ldots, t_n)$ en (atomær) formel.
   - Hvis φ og ψ er formler,så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \to \psi)$ formler.
   - Hvis φ er en formel og x er en variabel,så er $\forall x\varphi$ og $\exists x\varphi$ formler.

   Alle forekomster av en variabel x i φ sies å være bundet i formlene $\forall x\varphi$ og $\exists x\varphi$ og innenfor skopet til den gjeldende kvantoren.

I språket for beundring $\langle a, b; -; \mathsf{Idol}, \mathsf{Liker}\rangle$ kan vi uttrykke:

1:	Alice liker Bob:	$\mathsf{Liker}(a, b)$
2:	Alice liker alle:	$\forall x\mathsf{Liker}(a, x)$
3:	Alice liker alle som Bob liker:	$\forall x(\mathsf{Liker}(b, x) \to \mathsf{Liker}(a, x))$
4:	Noen liker seg selv:	$\exists x\mathsf{Liker}(x, x)$
5:	Bob liker alle som liker seg selv:	$\forall x(\mathsf{Liker}(x, x) \to \mathsf{Liker}(b, x))$
6:	Ingen liker både Alice og Bob:	$\neg\exists x(\mathsf{Liker}(x, a) \wedge \mathsf{Liker}(x, b))$
		$\forall x(\mathsf{Liker}(x, a) \to \neg\mathsf{Liker}(x, b))$
7:	Noen liker ikke seg selv:	$\exists x\neg\mathsf{Liker}(x, x)$
8:	Bob liker noen som liker Alice:	$\exists x(\mathsf{Liker}(b, x) \wedge \mathsf{Liker}(x, a))$
9:	En som blir likt av alle er et idol:	$\forall x(\forall y\mathsf{Liker}(y, x) \to \mathsf{Idol}(x))$
10:	Et idol blir likt av alle:	$\forall x(\mathsf{Idol}(x) \to \forall y\mathsf{Liker}(y, x))$

3.2 Frie variable i termer

Definisjon 3.1 (Frie variable i en term)**.** $\mathsf{FV}(t)$ *betegner mengden av frie variable i termen* t*.*

Definisjon 3.2 (Lukket term)**.** *En term* t *er lukket hvis* $\mathsf{FV}(t) = \emptyset$*, dvs.* t *inneholder ingen frie variable.*

Eksempel. *I språket* $\langle a, b; f; -\rangle$ *har vi:*

- *Termen* $f(x, a)$ *har en fri variabel* x*.*
- *Termen* $f(a, b)$ *har ingen frie variable og er en lukket term.*

3.3 Rekursive definisjoner

Når mengder er definert *induktivt*, så kan vi definere funksjoner over denne mengden *rekursivt* ved å

1. gi verdi til de "atomære" elementene (i basismengden), og
2. gi verdi til "sammensatte" elementene (fra induksjonssteget) ved å bruke verdiene som ble gitt til komponentene.

Den presise, rekursive definisjonen av FV er følgende.

Definisjon 3.3 (Frie variable - definert rekursivt)**.** *Gitt en term t, la mengden* $\mathsf{FV}(t)$ *av* frie variable *i t være definert rekursivt ved:*

- $\mathsf{FV}(x_i) = \{x_i\}$*, for en variabel* x_i*, og*
- $\mathsf{FV}(c_i) = \emptyset$*, for en konstant* c_i*, og*
- $\mathsf{FV}(f(t_1, \ldots, t_n)) = \mathsf{FV}(t_1) \cup \cdots \cup \mathsf{FV}(t_n)$*, for et funksjonssymbol f med aritet n.*