INF1800 – Logikk og beregnbarhet

Forelesning 17: Førsteordens logikk

Roger Antonsen

Institutt for informatikk
Universitetet i Oslo

14. oktober 2008

(Sist oppdatert: 2008-10-14 16:29)

Før vi begynner

Repetisjon og kommentarer

- Vi skal nå kunne
  - Utsagnslogikk: syntaks og semantikk
  - Sekventkalkyle for utsagnslogikk
- Under den detaljert undervisningsplanen ligger det ekstramateriale om sunnhet av sekventkalkylen.
- Det er ikke pensum, men bør leses av alle.
- Alla skal være i stand til å forklare (intuitivt) hvorfor sekventkalkylen er sunn.
- Praktisk: Hvis dere ønsker å gi tilbakemeldinger til gruppelærerene, så kan skjemaet på nettsidene også brukes til dette.

Nytt tema

- Vi begynner nå med førsteordens logikk!
- Vi har satt av minst tre uker til dette.
- Følgende avsnitt i boken regnes som pensum.
  - Kapittel 7.1, side 397–416: *First-order Predicate Calculus*
  - Kapittel 7.2, side 416–432: *Equivalent Formulas*
- Forelesningsnotatene kan leses helt uavhengig av boken.
- Legg vekt på forelesningsnotatene, men les boken også.
- Boken er et godt supplement for å få bedre forståelse.
- På noen områder er forelesningsnotatene mer detaljerte.
  - Vi har f.eks. et skarpere skille mellom syntaks og semantikk.
- Det vi gjør i timene er mest relevant for eksamen.

Innledning til førsteordens logikk

Introduksjon

- I utsagnslogikk har vi kun konnektivene $\neg$, $\land$, $\lor$ og $\rightarrow$.
- Med disse kan vi representere, analysere og resonnere over *utsagn*.
- 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.
  - For utsagnslogikk fins det effektive metoder for å *avgjøre* om en formel er gyldig eller ikke.
  - Det fins ikke for førsteordens logikk; vi sier at førsteordens logikk er ikke *avgjørbar*.

Noen eksempler fra matematikk

Noen enkle matematisk 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 et annet brøktall."
- "Ethvert partall er summen av to primtall."
- "Hvis a er mindre enn b og b er mindre enn c, så er a mindre enn c."

Noen eksempler med naturlig språk

Her er noen ekempler 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.”

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.

Førsteordens logikk: Syntaks

Syntaks: Signaturer

Definisjon (Førsteordens språk: logiske symboler)

Alle førsteordens språk består av følgende logiske symboler:

- De logiske konnektivene $\wedge$, $\vee$, $\rightarrow$ og $\neg$.
- 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 som oftest x, y, z, $\ldots$, for variable).
- Vi skal også bruke parenteser og kommaer som hjelpesymboler.

Syntaks: Signaturer

Definisjon (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.

Syntaks: Signaturer

Merk

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

Definisjon (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.

Syntaks: Termer

Definisjon (Termer)

Mengden $\mathcal{T}$ av førsteordens 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 $f(t_1, ..., t_n)$ en term.

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, $\ldots$.

Eksempler på førsteordens språk

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: $=(x, x), ++, +0, \ldots$
- Når vi skriver $+xy$ bruker vi prefiks notasjon.
- Vi kan også bruke infiks notasjon og skrive: $(x + y), (0 + 0), (s0 + 0), (0 + s0), \ldots.$

Eksempler på førsteordens språk

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)

Termer: $\emptyset$, $x \cap \emptyset$, $y \cup (x \cap z)$,...

Eksempler på førsteordens språk

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, $\mathsf{Slektning}$ (alle med aritet 2)

Termer i språket for familierelasjoner:

- x, Ola og Kari er termer.
- $\mathsf{mor}(\mathsf{Ola})$, $\mathsf{mor}(\mathsf{Kari})$, $\mathsf{far}(\mathsf{Ola})$ og $\mathsf{far}(\mathsf{Kari})$ er termer.
- $\mathsf{mor}(x)$ og $\mathsf{far}(x)$ er termer.
- $\mathsf{mor}(\mathsf{mor}(x))$ og $\mathsf{mor}(\mathsf{far}(\mathsf{Kari}))$ er termer.

Syntaks: Formler

Definisjon (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, kan vi skrive Rx, Rfa, $Rafa$, etc. for $R(x)$, $R(f(a))$ og $R(a, f(a))$.

Syntaks: Formler

Definisjon (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 $\neg\varphi$, $(\varphi \land \psi)$, $(\varphi \lor \psi)$ 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.

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)

- Signaturen er $\langle a, b; -; \mathsf{Idol}, \mathsf{Liker} \rangle$
- Atomære formler i språket:

1 Alice er et idol: $\mathsf{Idol}(a)$

2 Alice liker Bob: $\mathsf{Liker}(a, b)$

3 x liker Alice: $\mathsf{Liker}(x, a)$

Eksempler på førsteordens formler

- Ikke-atomære formler i språket:

4	Alice liker alle:	$\forall x \mathsf{Liker}(a, x)$
5	Det finnes et idol:	$\exists x \mathsf{Idol}(x)$
6	Alice liker alle som Bob liker:	$\forall x(\mathsf{Liker}(b, x) \to \mathsf{Liker}(a, x))$
7	Noen liker seg selv:	$\exists x \mathsf{Liker}(x, x)$
8	Bob liker alle som liker seg selv:	$\forall x(\mathsf{Liker}(x, x) \to \mathsf{Liker}(b, x))$
9	Ingen liker både Alice og Bob:	$\neg \exists x(\mathsf{Liker}(x, a) \land \mathsf{Liker}(x, b))$
10	Noen liker ikke seg selv:	$\exists x \neg \mathsf{Liker}(x, x)$
11	Bob liker noen som liker Alice:	$\exists x(\mathsf{Liker}(b, x) \land \mathsf{Liker}(x, a))$
12	Alle liker noen:	$\forall x(\exists y \mathsf{Liker}(x, y))$
13	En som blir likt av alle er et idol:	$\forall x(\forall y \mathsf{Liker}(y, x) \to \mathsf{Idol}(x))$
14	Et idol blir likt av alle:	$\forall x(\mathsf{Idol}(x) \to \forall y \mathsf{Liker}(y, x))$

Flere eksempler

I språket for aritmetikk, $\langle 0; s, +; =\rangle$, har vi følgende formler.

- $s0 + s0 = ss0$ – "en pluss en er to"
- $\forall x \forall y (x + y = y + x)$ – "addisjon er kommutativt"
- $\neg \exists x (0 = sx)$ – "0 er ikke etterfølgeren til noe"
- $\exists x \exists y \neg (x = y)$ – "det fins to forskjellige objekter"

Frie variable i termer

Definisjon (Frie variable i en term)

$\mathsf{FV}(t)$ betegner mengden av frie variable i termen t.

Definisjon (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.

Frie variable i formler

Definisjon (Frie variable i en formel)

En variabelforekomst i en førsteordens formel er fri hvis den ikke er bundet, dvs. hvis den ikke er innenfor skopet til en kvantor. Vi skriver $\mathrm{FV}(\varphi)$ for mengden av frie variable i φ.

Eksempel ($\forall x Rxy \land Pz$)

- x er bundet
- y er fri
- z er fri

Eksempel ($\forall x Pxy \to \forall z Pzx$)

- x er bundet
- x er fri
- y er fri
- z er bundet

Substitusjoner

Definisjon (Substitusjon for termer)

La s og t være termer og x en variabel. Da er $s[x/t]$ resultatet av å erstatte alle forekomster av x i s med t. Det kan defineres helt presist slik:

1. $y[x/t] = \begin{cases} t & \text{hvis } x = y \\ y & \text{ellers} \end{cases}$ (når s er en variabel y).
2. $c[x/t] = c$ (når s er en konstant c).
3. $f(t_1[x/t], \ldots, t_n[x/t])$ (når s er en funksjonsterm $f(t_1, \ldots, t_n)$).

Eksempel

- $f(x, y, a)[x/y] = f(x[x/y], y[x/y], a[x/y]) = f(y, y, a)$
- $f(y, y, a)[y/b] = f(y[y/b], y[y/b], a[y/b]) = f(b, b, a)$

Substitusjoner

Definisjon (Substitusjon for formler)

$\varphi[x/t]$ er definert (rekursivt) ved:

1. $R(t_1, \ldots, t_n)[x/t] = R(t_1[x/t], \ldots, t_n[x/t])$
2. $\neg\psi[x/t] = \neg(\psi[x/t])$
3. $(\varphi_1 \circ \varphi_2)[x/t] = (\varphi_1[x/t] \circ \varphi_2[x/t])$, hvor $\circ \in \{\land, \lor, \rightarrow\}$
4. $Qy\psi[x/t] = \begin{cases} Qy(\psi[x/t]) & \text{hvis } x \neq y \\ Qy\psi & \text{ellers} \end{cases}$, hvor $Q \in \{\forall, \exists\}$

Eksempel

- $(Pxy \land \forall x Pxy)[x/a] = (Pay \land \forall x Pxy)$
- $(Pxy \land \forall x Pxy)[y/a] = (Pxa \land \forall x Pxa)$

Førsteordens logikk: Semantikk

Introduksjon

- Hvordan skal vi tolke førsteordens formler?
- Hva skal $\forall x \varphi$ og $\exists x \varphi$ bety?
- Hva kan vi bruke førsteordens formler til å uttrykke?

  (Hva er det førsteordens formler *ikke* kan uttrykke?)
- Hva gjør en formel sann / gyldig / oppfyllbar?
- Å gi en semantikk er å si noe om forholdet mellom språk og virkelighet.
  - Valuasjoner gir en semantikk for klassisk utsagnslogikk.
- I førsteordens logikk vil modeller gi oss en semantikk.

Introduksjon

En modell består intuitivt av

1. en mengde, og
2. en tolkning av alle ikke-logiske symboler slik at
    - et konstantsymbol tolkes som et element i mengden,
    - et funksjonssymbol tolkes som en funksjon på mengden, og
    - et relasjonssymbol tolkes som en relasjon på mengden.

Vi skal definere modeller helt presist, også skal vi definere hva det vil si at en formel er sann i en modell.

Husk

Hvis D er en mengde, så består D^n av alle n-tupler av elementer fra D, for $n \geqslant 0$.

$$D^n = \{\langle d_1, \ldots, d_n \rangle \mid d_1, \ldots, d_n \in D\}$$

Modeller – Intuisjon

- Se på formelen
$$\forall x \exists y Rxy.$$
- Vi leser den som: *For alle* x, så *fins* det en y slik at Rxy.
- Hvorvidt denne formelen er sann eller usann avhenger av tolkningen eller modellen.
    - Hvis R tolkes som *ekte mindre enn*-relasjonen over de naturlige tallene, så er den sann.
    - Grunnen er at for alle tall så fins det ett som er større.
    - Hvis R tolkes som *ekte mindre enn*-relasjonen over mengden $\{1, 2, 3, 4, 5, 6, 7\}$, så er den usann.
    - Grunnen er at det fins et tall, nemlig 7, slik at det *ikke* fins noe større tall.
- Vi må definere hva vi mener med en *modell*.

Modeller

La et førsteordens språk $\mathcal{L}$ være gitt.

Definisjon (Modell)

En modell $\mathcal{M}$ for $\mathcal{L}$ består av en ikke-tom mengde D, kalt domenet til $\mathcal{M}$, og en funksjon $(\cdot)^{\mathcal{M}}$ som tolker alle ikke-logiske symboler på følgende måte:

- Hvis c er et konstantsymbol, så er $c^{\mathcal{M}} \in D$.
- Hvis f er et funksjonsymbol med aritet n, så er $f^{\mathcal{M}}$ en funksjon fra $D^n = \underbrace{D \times \cdots \times D}_{n}$ til D.
- Hvis R er et relasjonssymbol med aritet n, så er $R^{\mathcal{M}}$ en relasjon på $D^n = \underbrace{D \times \cdots \times D}_{n}$.

Vi skriver $|\mathcal{M}|$ for domenet D til modellen $\mathcal{M}$.