INF3170 – Logikk

Forelesning 6: Løse tråder og repetisjon av førsteordens logikk.

Christian Mahesh Hansen

Institutt for informatikk, Universitetet i Oslo

26. februar 2007

Dagens plan

1. Noen løse tråder
2. Førsteordens logikk – repetisjon

Bevisbarhet

Definisjon

Et bevis for en formel φ er et bevis for sekventen $\vdash \varphi$.

Eksempel

Et bevis for formelen $P \lor \neg P$ er

$$\cfrac{\cfrac{\cfrac{\times}{P \vdash P}}{\vdash P, \neg P}}{\vdash P \lor \neg P}$$

Notasjon

Formelen φ er (LK-)bevisbar:	$\vdash \varphi$	$\vdash_{\mathrm{LK}} \varphi$
Sekventen $\Gamma \vdash \Delta$ er (LK-)bevisbar:	$\vdash \Gamma \vdash \Delta$	$\vdash_{\mathrm{LK}} \Gamma \vdash \Delta$

Hva $\vdash \varphi$ betyr må være tydelig i konteksten!

Oppfyllbarhet og konsistens

Definisjon

En mengde Γ av formler er oppfyllbar hvis det fins en modell som oppfyller alle formlene i mengden.

Eksempel

Mengden $\{P \lor Q, \neg P\}$ er oppfyllbar. La f.eks. v være en valuasjon som gjør Q sann og P usann.

Definisjon

En mengde Γ er konsistent hvis sekventen $\Gamma \vdash$ ikke er bevisbar.

Eksempel

Mengden $\{P \lor Q, \neg P\}$ er konsistent.

$$\cfrac{\cfrac{\cfrac{\times}{P \vdash P} \qquad Q \vdash P}{P \lor Q \vdash P}}{P \lor Q, \neg P \vdash}$$

Oppfyllbarhet og konsistens

Sunnhet og kompletthet - andre formuleringer

Sunnhet:	enhver oppfyllbar mengde er konsistent.
Kompletthet:	enhver konsistent mengde er oppfyllbar.

Oppgave

Vis at disse formuleringene er ekvivalente med de vanlige formuleringene.

Notasjon

Notasjon

Formelen φ er gyldig:	$\models \varphi$
Sekventen $\Gamma \vdash \Delta$ er gyldig:	$\models \Gamma \vdash \Delta$

Notasjon

Hvis Γ og Δ er mengder eller multimengder av formler, har vi også følgende.

- *$\Gamma \models \Delta$: enhver modell som gjør alle formlene i Γ sanne, gjør også minst en av formlene i Δ sann.*
- *$\Gamma \models \varphi$: enhver modell som gjør alle formlene i Γ sanne, gjør også φ sann.*

Bevisteknikker

- Siden noe av det viktigste vi gjør i dette kurset er å bevise påstander, kan det være greit å si noe om hvordan vi gjør det.

Oppgave

Vis at hvis $\boxed{1}$, så $\boxed{2}$.

1. Et direkte bevis. Forsøk alltid dette først.
   - Anta $\boxed{1}$ og vis klart og tydelig hvorfor denne antakelsen fører til $\boxed{2}$.
2. Et motsigelsesbevis. Hvis et direkte bevis ikke er mulig.
   - Anta for motsigelse at påstanden ikke holder, dvs. at $\boxed{1}$ og ikke $\boxed{2}$.
   - Vis klart og tydelig hvorfor denne antakelsen fører til en motsigelse.
   - Konkluder med at påstanden må holde.
3. Et bevis for den kontrapositive påstanden: hvis ikke $\boxed{2}$, så ikke $\boxed{1}$.
   - Dette er essensielt det samme som et motsigelsesbevis.

Bevisteknikker

Noen fordeler med direkte bevis:

- Er som regel enklere å lese.
- Kan inneholde mer informasjon.
- Er mer konstruktivt.
- Kan gi mer intuisjon om grunnene for at noe holder.

Noen fordeler med motsigelsesbevis:

- Kan være enklere å gjennomføre.
- Kan være kortere enn direkte bevis.

Bevisteknikker

Oppgave

Vis at ikke $\boxed{X}$.

- Anta $\boxed{X}$ og vis klart og tydelig hvorfor denne antakelsen fører til en motsigelse.
- Dette er ikke et motsigelsesbevis, men et direkte bevis.

$$\frac{\begin{array}{c}\neg A\\ \vdots\\ \bot\end{array}}{A} \qquad\qquad \frac{\begin{array}{c}A\\ \vdots\\ \bot\end{array}}{\neg A}$$

Oppgave: bruk logikk til å uttrykke *sanne* utsagn om tall

- "2 er et partall"
- "2 pluss 2 er lik 4"
- "2 ganger 4 er lik 8"
- "hvis n og k er partall, så er n pluss k et partall"
- "hvis n er et partall, så finnes k slik at n er lik k ganger 2"
- Hva slags logisk språk skal vi bruke?

Forsøk 1: utsagnslogikk

- Uttrykk av typen "n er et partall":
  - P_2 står for "2 er et partall"
  - P_4 står for "4 er et partall"
  - ...
- Uttrykk av typen "n pluss k er lik l":
  - Q_1 står for "0 pluss 0 er lik 0"
  - Q_2 står for "0 pluss 1 er lik 1"
  - ...
- Tilsvarende for uttrykk av typen "n ganger k er lik l".
- Mulig, siden vi har uendelig mange utsagnsvariable.

Forsøk 1: utsagnslogikk

- Hva med "hvis n og k er partall, så er n pluss k et partall"?
- Vi kan lage atomære utsagn av typen
  - R_1 står for "2 pluss 2 er et partall"
  - R_2 står for "2 pluss 4 er et partall"
  - R_3 står for "2 pluss 6 er et partall"
  - ...
- For $n = 2$ og $k = 4$ får vi $(P_2 \wedge P_4) \rightarrow R_2$
- For $n = 2$ og $k = 6$ får vi $(P_2 \wedge P_6) \rightarrow R_3$
- Vi får en uendelig konjunksjon:

$$((P_2 \wedge P_4) \rightarrow R_2) \wedge ((P_2 \wedge P_6) \rightarrow R_3) \wedge \ldots$$

- Umulig! Utsagnslogiske formler er endelige...
- Utsagnslogikk er ikke uttrykkskraftig nok til å løse oppgaven!

Forsøk 2: førsteordens logikk

- Vi representerer de naturlige tallene med konstantsymboler: $\bar{0}, \bar{1}, \bar{2}, \ldots$
- Vi representerer "pluss" og "gange" med de binære funksjonssymbolene $\dot{+}$ og $\dot{\times}$.
- Vi innfører et unært predikatsymbol Par for partall og et binært predikatsymbol $\equiv$ for likhet.
- Vi bruker *innfiks* notasjon for $\dot{+}$, $\dot{\times}$ og $\equiv$, dvs. $\bar{2}\dot{+}\bar{2}$, $\bar{2}\dot{\times}\bar{2}$ og $\bar{2} \equiv \bar{2}$ i stedet for $\dot{+}(\bar{2},\bar{2})$, $\dot{\times}(\bar{2},\bar{2})$ og $\equiv(\bar{2},\bar{2})$.
- Vi får følgende signatur:

$$\langle \bar{0}, \bar{1}, \bar{2}, \ldots ; \dot{+}, \dot{\times} ; \mathrm{Par}, \equiv \rangle$$

Forsøk 2: førsteordens logikk

- "2 er et partall":

$$\mathrm{Par}(\bar{2})$$

- "2 pluss 2 er lik 4":

$$(\bar{2}\dot{+}\bar{2}) \equiv \bar{4}$$

- "2 ganger 4 er lik 8":

$$(\bar{2}\dot{\times}\bar{4}) \equiv \bar{8}$$

- "hvis n og k er partall, så er n pluss k et partall":

$$\forall x \forall y((\mathrm{Par}(x) \wedge \mathrm{Par}(y)) \rightarrow \mathrm{Par}(x\dot{+}y))$$

- "hvis n er et partall, så finnes k slik at n er lik k ganger 2":

$$\forall x(\mathrm{Par}(x) \rightarrow \exists y(x \equiv (y\dot{\times}\bar{2})))$$

En modell for utsagnene om tall

- La oss se på hvordan vi tolker utsagnene om tall.
- Vi lager en modell $\mathcal{M}$ med $|\mathcal{M}| = \{0, 1, 2, 3, \ldots\}$.
- Vi tolker konstantsymbolene som følger:
  - $\bar{0}^{\mathcal{M}} = 0$
  - $\bar{1}^{\mathcal{M}} = 1$
  - $\bar{2}^{\mathcal{M}} = 2$
  - ...
- Vi tolker funksjonssymbolene som følger:
  - $\dot{+}^{\mathcal{M}}$ er addisjon (funksjon fra $|\mathcal{M}| \times |\mathcal{M}|$ til $|\mathcal{M}|$)
  - $\dot{\times}^{\mathcal{M}}$ er multiplikasjon (funksjon fra $|\mathcal{M}| \times |\mathcal{M}|$ til $|\mathcal{M}|$)
- Vi tolker relasjonssymbolene som følger:
  - $\mathrm{Par}^{\mathcal{M}}$ er mengden $\{0, 2, 4, 6, \ldots\}$ (delmengde av $|\mathcal{M}|$)
  - $\equiv^{\mathcal{M}}$ er mengden $\{\langle 0, 0\rangle, \langle 1, 1\rangle, \ldots\}$ (delmengde av $|\mathcal{M}| \times |\mathcal{M}|$)

Modellen oppfyller formlene

- $\mathcal{M} \models \mathrm{Par}(\bar{2})$ fordi
  - $\bar{2}^{\mathcal{M}} = 2$
  - $2 \in \mathrm{Par}^{\mathcal{M}}$
- $\mathcal{M} \models (\bar{2} \dot{+} \bar{2}) \equiv \bar{4}$ fordi
  - $\bar{2}^{\mathcal{M}} = 2$, og $\bar{4}^{\mathcal{M}} = 4$
  - $2 \dot{+}^{\mathcal{M}} 2 = 2 + 2 = 4$
  - $\langle 4, 4\rangle \in \equiv^{\mathcal{M}}$
- $\mathcal{M} \models (\bar{2} \dot{\times} \bar{4}) \equiv \bar{8}$ fordi
  - $\bar{2}^{\mathcal{M}} = 2$, $\bar{4}^{\mathcal{M}} = 4$ og $\bar{8}^{\mathcal{M}} = 8$
  - $2 \dot{\times}^{\mathcal{M}} 4 = 2 \cdot 4 = 8$
  - $\langle 8, 8\rangle \in \equiv^{\mathcal{M}}$

Oppfyllbarhet av ikke-aromære formler

- Hva med ikke-atomære formler?
- Nye konnektiver i førsteordens logikk er $\forall$ og $\exists$.
- De andre konnektivene tolkes likt som i utsagnslogikk.
- Vi har definert $\models$-relasjonen rekursivt, dvs. at vi definerer $\mathcal{M} \models \forall x\varphi$ som en funksjon av $\mathcal{M} \models \varphi$.
- Den bundne variabel x i $\forall x\varphi$ og $\exists x\varphi$ skal løpe over elementene i domenet til $\mathcal{M}$.

Oppfyllbarhet av ikke-aromære formler

- Intuitivt har vi at $\mathcal{M}$ oppfyller $\forall x\varphi$ hvis $\mathcal{M}$ oppfyller $\varphi[e/x]$ for *alle* elementer e i domenet til $\mathcal{M}$.
- Problem: $\varphi[e/x]$ er ikke en førsteordens formel!
- Derfor kan vi ikke si noe om hvorvidt $\mathcal{M}$ oppfyller $\varphi[e/x]$ ...
- Vi bruker spesielle *konstantsymboler* for å representere elementene i $|\mathcal{M}|$.
- I tallspråket vårt har vi allerede $\bar{0}, \bar{1}, \bar{2}, \ldots$ for elementene i $|\mathcal{M}|$.
- Generelt lager vi et utvidet språk fra modellen ved å legge til et konstantsymbol $\bar{e}$ for hvert element e i domenet til modellen.
- Vi krever at modellen skal tolke konstantsymbolet $\bar{e}$ som elementet e i domenet til modellen.

Førsteordens syntaks og semantikk

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

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

Førsteordens syntaks og semantikk

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 $(\varphi \rightarrow \psi)$ formler.
   - Hvis φ er en formel og x er en variabel,så er $\forall x\varphi$ og $\exists x\varphi$ formler.

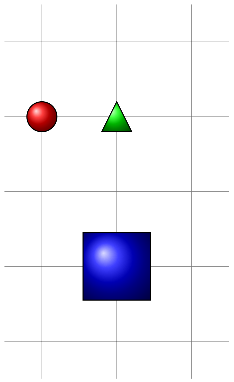
   Alle forekomster av en variabel x i φ sies å være bundet i formlene $\forall x\varphi$ og $\exists x\varphi$ og innenfor skopet til den gjeldende kvantoren.

Førsteordens syntaks og semantikk

Hvis $\mathcal{M}$ er en modell og φ er en lukket formel, så definerte vi $\mathcal{M} \models \varphi$. Vi brukte det utvidete språket - med konstanter for hvert element i domenet - for å gjøre dette.

- For atomære formler: $\mathcal{M} \models R(t_1, \ldots, t_n)$ hvis $\langle t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M} \models \neg\varphi$ hvis det ikke er tilfelle at $\mathcal{M} \models \varphi$.
- $\mathcal{M} \models \varphi \wedge \psi$ hvis $\mathcal{M} \models \varphi$ og $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \vee \psi$ hvis $\mathcal{M} \models \varphi$ eller $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \rightarrow \psi$ hvis $\mathcal{M} \models \varphi$ impliserer $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \forall x\varphi$ hvis $\mathcal{M} \models \varphi[\bar{a}/x]$ for alle a i $|\mathcal{M}|$.
- $\mathcal{M} \models \exists x\varphi$ hvis $\mathcal{M} \models \varphi[\bar{a}/x]$ for minst en a i $|\mathcal{M}|$.

Oppfyllbarhet

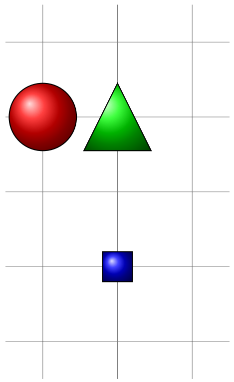


- Er det slik at $\mathcal{M} \models \exists x\text{Liten}(x)$?
- For å svare, må vi se på definisjonen av $\models$.

$$\mathcal{M} \models \exists x\text{Liten}(x)$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \mathcal{M} \models \text{Liten}(\bar{a})$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \bar{a}^{\mathcal{M}} \in \text{Liten}^{\mathcal{M}}$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } a \in \text{Liten}^{\mathcal{M}}$$

- Siden $\text{Liten}^{\mathcal{M}} = \{ , \}$, kan vi konkludere med **JA**.

Oppfyllbarhet

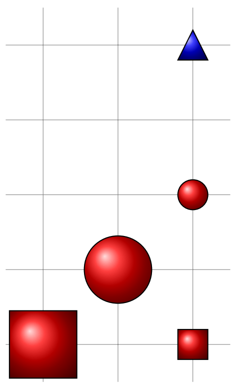


- Er det slik at $\mathcal{M} \models \forall x\text{Stor}(x)$?
- For å svare, må vi se på definisjonen av $\models$.

$$\mathcal{M} \models \forall x\text{Stor}(x)$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } \mathcal{M} \models \text{Stor}(\bar{a})$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } \bar{a}^{\mathcal{M}} \in \text{Stor}^{\mathcal{M}}$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } a \in \text{Stor}^{\mathcal{M}}$$

- Siden $|\mathcal{M}| = \{ , , \}$ og $\text{Stor}^{\mathcal{M}} = \{ , \}$, så kan vi konkludere med **NEI**.

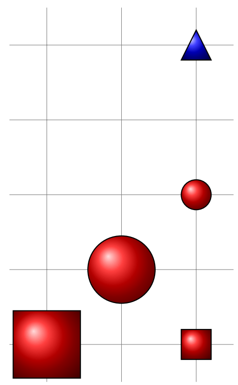
Oppfyllbarhet



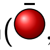
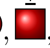
$$\mathcal{M} \models \forall x(\text{Stor}(x) \to \text{Sirkel}(x))$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \text{Stor}(\bar{a}) \to \text{Sirkel}(\bar{a})$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$\mathcal{M} \models \text{Stor}(\bar{a})$ impliserer $\mathcal{M} \models \text{Sirkel}(\bar{a})$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
hvis $a \in \text{Stor}^{\mathcal{M}}$, så $a \in \text{Sirkel}^{\mathcal{M}}$
$$\Updownarrow$$
"alle store objekter er sirkler"

Påstander holder ikke.

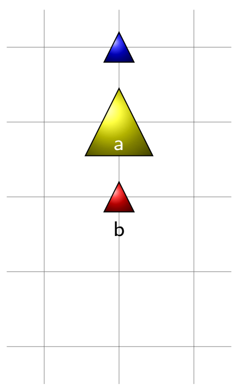
Oppfyllbarhet



$$\mathcal{M} \models \forall x(\text{Sirkel}(x) \to \exists y \exists z \text{Mellom}(x, y, z))$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \text{Sirkel}(\bar{a}) \to \exists y \exists z \text{Mellom}(\bar{a}, y, z)$$
$$\Updownarrow$$
for alle sirkler $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \exists y \exists z \text{Mellom}(\bar{a}, y, z)$$
$$\Updownarrow$$
for alle sirkler $a \in |\mathcal{M}|$ så
fins $b, c \in \mathcal{M}$ slik at $\mathcal{M} \models \text{Mellom}(\bar{a}, \bar{b}, \bar{c})$

Påstanden holder, fordi
$\mathcal{M} \models$ Mellom(, , ) og
$\mathcal{M} \models$ Mellom(, , ).

Oppfyllbarhet

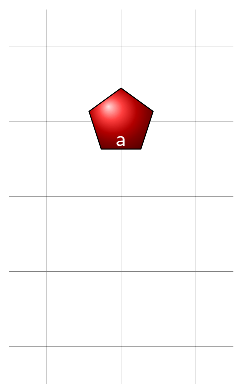


Er følgende formler oppfyllbare samtidig?

1. $\text{Stor}(a) \land \text{Liten}(b)$
2. $\forall x(\text{Trekant}(x))$
3. $\forall x(\text{Inntil}(x, a) \lor \text{Inntil}(x, b))$
4. $\neg \exists x(\text{VenstreFor}(x, a) \lor \text{HoyreFor}(x, a))$
5. $\forall x(\text{Stor}(x) \to \exists y \text{Over}(y, x))$

Svaret er JA!

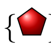
Oppfyllbarhet



Er følgende formler oppfyllbare?

1. $\neg\text{Sirkel}(a) \land \neg\text{Trekant}(a) \land \neg\text{Firkant}(a))$

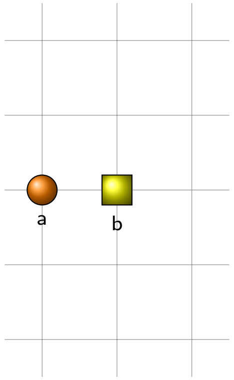
   Svaret er JA!

   La $|\mathcal{M}| = \{$$\}$ og $a^{\mathcal{M}} =$ .
2. $\text{Liten}(a) \land \text{Stor}(a)$

   Svaret er JA!

   La $|\mathcal{M}| = \{$🚲$\}$, $a^{\mathcal{M}} =$ 🚲 og
   $\text{Liten}^{\mathcal{M}} = \text{Stor}^{\mathcal{M}} = \{$🚲$\}$

Bruke språket til å beskrive modeller



Gi en mengde formler som beskriver denne modellen nøyaktig, dvs. som har denne og (essensielt) ingen andre modeller.

1. $\text{Sirkel}(a) \land \text{Firkant}(b)$
2. $\forall x \text{Liten}(x)$
3. $\text{VenstreFor}(a, b)$
4. $\forall x(\text{Inntil}(x, a) \lor \text{Inntil}(x, b))$
5. $\forall x(\neg\text{Over}(x, a) \land \neg\text{Under}(x, a))$
6. $\forall x(\neg\text{VenstreFor}(x, a) \land \neg\text{HoyreFor}(x, b))$

Ganske vanskelig...