INF4170 – Logikk
Forelesningsnotater

Arild Waaler
Martin Giese
Christian Mahesh Hansen (gjesteforeleser)
Espen Lian (gjesteforeleser)
Bjarne Holen (gjesteforeleser og gruppelærer)

Institutt for informatikk
Universitetet i Oslo
Våren 2007

Innhold:

Sist oppdatert: 23. mai 2008

Kompendiet er automatisk generert fra materialet som har blitt presentert i løpet av kurset og må leses med dette forbeholdet. Undervisningsmaterialet er i all hovedsak laget av Christian Mahesh Hansen og Roger Antonsen våren 2006, og justert av Christian Mahesh Hansen våren 2007. Flere små endringer av Martin Giese våren 2008.

Kommentarer, feil og forslag til forbedringer kan sendes til:
Martin Giese (martingi@ifi.uio.no)

Innhold

Forelesning 0: Mengdelære, Induksjon

Martin Giese - 23. januar 2008

1.1 Mengdelære

1.1.1 Mengder

Mengder

Definisjon 1.1.1.

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

Spørsmål: Hvor mange elementer har $\{a, b, c, d\}$?

Mengder

Antagelse: $a, b, c, d, 1, 2, \gamma, \Phi$ er alle forskellige

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 1.1.2 (Den tomme mengden)**.**

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

Definisjon 1.1.3 (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 1.1.4 (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 1.1.5 (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 1.1.6 (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 1.1.7 (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 1.1.8 (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 $\ldots$" *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:*

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

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

Mengder av mengder

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

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

Snitt av mengder av mengder

Definisjon 1.1.9. 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 1.1.10. 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.
- $\bigcup\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \mathbb{N}$
- $\bigcup\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\} = \mathbb{N}$

1.1.2 Relasjoner

Relasjoner

Definisjon 1.1.11 (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 1.1.12. *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 1.1.13 (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 1.1.14 (Symmetrisk)**.** *En binær relasjon R er* symmetrisk *hvis for alle x, y med $\langle x, y\rangle \in R$, også $\langle y, x\rangle \in R$.*

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 1.1.15 (Transitiv)**.** *En binær relasjon R er* transitiv *hvis for allex$, y, z$ med $\langle x, y\rangle \in R$ og $\langle y, z\rangle \in R$, også $\langle x, z\rangle \in R$.*

Definisjon 1.1.16 (Ekvivalensrelasjon)**.** *En binær relasjon over mengden S er en* ekvivalensrelasjon *hvis den er refleksiv, symmetrisk og transitiv.*

1.1.3 Funksjoner

Funksjoner

Definisjon 1.1.17 (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 $f(x) = y$.*

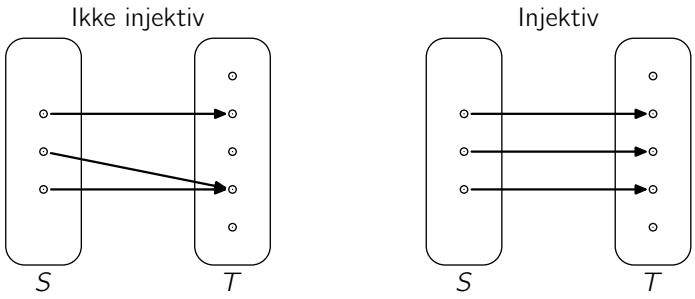
Funksjoner

Eksempel. *Funksjonen $Par : \mathbb{N} \to \{0, 1\}$ 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 1.1.18 (Injektiv)**.** *En funksjon $f : S \to T$ er* injektiv *hvis $f(x) \neq f(y)$ for alle $x, y \in S$ med $x \neq y$. Vi sier at f er en-til-en.*

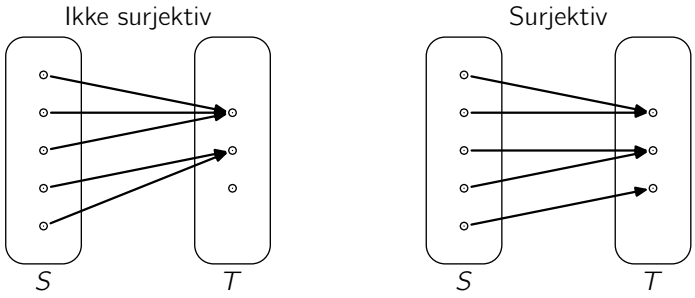
Eksempel.



Surjektive funksjoner

Definisjon 1.1.19 (Surjektiv)**.** *En funksjon $f : S \to T$ er* surjektiv *hvis for alle $y \in T$ så finnes $x \in S$ slik at $f(x) = y$. Vi sier at f er på.*

Eksempel.

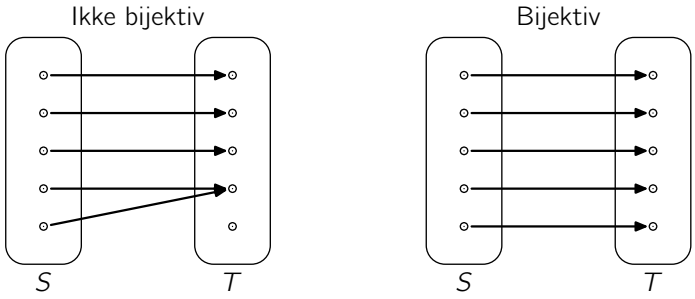


Bijektive funksjoner

Definisjon 1.1.20 (Bijektiv)**.** *En funksjon er* bijektiv *hvis den er injektiv og surjektiv.*

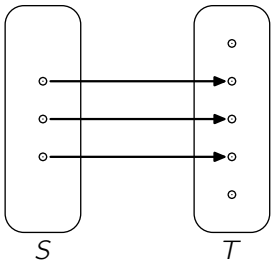
Vi sier at funksjonen er *en-til-en* og *på*, eller at vi har en *en-til-en korrespondanse*.

Eksempel.



Injektive og surjektive funksjoner

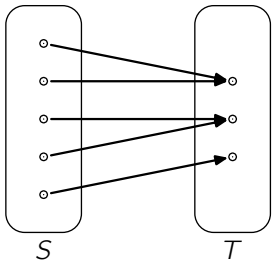
injektiv / en-til-en



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

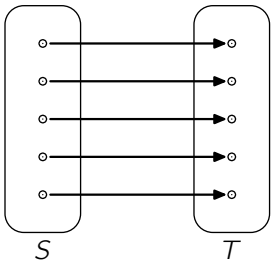


for alle $y \in T$:
det finnes $x \in S$ slik at $f(x) = y$

"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".*

1.1.4 Operatorer

Operatorer

Definisjon 1.1.21 (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 $\mathbb{Z}$.*

1.1.5 Multimengder

Multimengder

Mengder der antall forekomster av hvert element teller

Definisjon 1.1.22 (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.

- $\{a, a, b, c\} \cup \{a, c\} = \{a, a, a, b, c, c\}$ *d.v.s.* $m(x) = m_1(x) + m_2(x)$
- $\{a, a, a, b, c\} \cap \{a, a, d\} = \{a, a\}$ *d.v.s.* $m(x) = \min(m_1(x), m_2(x))$
- $\{a, a, a, b, c\} \setminus \{a, a, d\} = \{a, b, c\}$ *d.v.s.* $m(x) = \max(0, m_1(x) - m_2(x))$
- $\{a, a\} \subseteq \{a, a, b, c\}$*, men* $\{a, a, a\} \not\subseteq \{a, a, b, c\}$ *d.v.s.* $m_1(x) \leq m_2(x)$ *for alle* x*.*

- Vi bruker $\emptyset$ om den tomme multimengden.

1.1.6 Kardinalitet

Definisjon 1.1.23 (Kardinalitet)**.**

- *To mengder* S *og* T *har* lik kardinalitet *hvis det finnes en bijeksjon fra* S *til* T*.*
- *Mengden* S *har* kardinalitet mindre eller lik *T hvis det finnes 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*.*

Teorem 1.1.1 (Bernstein)**.** *Hvis det finnes en injektiv funksjon* $f : S \to T$ *og en injektiv funksjon* $g : T \to S$*, så finnes det også en bijeksjon* $h : S \to T$*.*

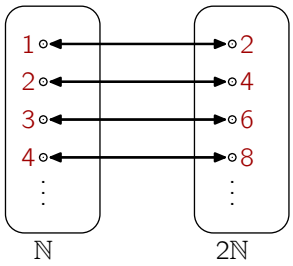
Eksempel. *Hva er kardinaliteten til*

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

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* $|\mathbb{N}| = |2\mathbb{N}|$.



1.1.7 Tellbart vs. overtellbart

Definisjon 1.1.24 (Tellbar)**.** *En uendelig mengde* S *er* tellbar *hvis det finnes 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 finnes 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.*

1.2 Induktive definisjoner og bevis

1.2.1 Induktivt definerte mengder

Induktive definisjoner

Definisjon 1.2.1 (Induktiv definisjon)**.** *Å definere en mengde induktivt betyr å konstruere den minste mengden som inneholder en gitt mengde* B*—kalt en* basismengde*—og som er lukket under gitte operasjoner.*

Eksempel. *Mengden* $\mathbb{N}$ *av naturlige tall kan defineres induktivt som minste mengde* $\mathbb{N}$ *med*

- $0 \in \mathbb{N}$*, og*
- *hvis* $x \in \mathbb{N}$*, så* $x + 1 \in \mathbb{N}$.

Her er basismengden $\{0\}$ *og* $\mathbb{N}$ *er lukket under suksessorfunksjonen (x+1).*

Eksempel. *Mengden* $\mathbb{B}$ *av binære tall kan defineres som minste mengde så at*

- 0 *og* 1 *er binære tall, og*
- *hvis* b *er et binært tall, så er* $b0$ *og* $b1$ *binære tall.*

steg 0:	0	1						
steg 1:	00	10	01	11				
steg 2:	000	100	010	110	001	101	011	111
⋮								

Eksempel. *Mengden* S *av symmetriske strenger over alfabetet* $\{a, b\}$ *kan defineres induktivt som minste mengde* S *slik at*

- $\epsilon \in S$ *(den tomme strengen),*
- *hvis* $x \in S$*, så* $axa \in S$ *og* $bxb \in S$*.*

steg 0:	ϵ			
steg 1:	aa	bb		
steg 2:	$aaaa$	$abba$	$baab$	$bbbb$
⋮				

Hvorfor den minste mengden?

Det er mange mengder som inkluderer B og som er lukket under gitte operasjoner.

Eksempel. *Hvilke mengder* N *oppfyller:*

- $0 \in N$*, og*
- *hvis* $x \in N$*, så* $x + 1 \in N$*?*

For eksempel:

- $\mathbb{N}$
- $\mathbb{Z}$
- $\{0, \frac{1}{2}, 1, \frac{3}{2}, \ldots\}$

Hva betyr egentlig 'minst'?

- La
$$\mathcal{M} := \{M \mid B \subseteq M \text{ og } M \text{ er lukket under operasjonene}\}$$
- $\mathcal{M}$ inneholder alle M som oppfyller kravene
- Ta snittet av alle sånne mengder:
$$M^* := \bigcap \mathcal{M}$$
- Da er $M^* \in \mathcal{M}$.
- Også er $M^* \subseteq M$ for alle $M \in \mathcal{M}$.
- Hvis $N \subseteq M$ for alle $M \in \mathcal{M}$ for noen mengde $N \in \mathcal{M}$, så er $N = M^*$.
- M^* er altså den entydige minste mengden i $\mathcal{M}$ med hensyn til $\subseteq$.

1.2.2 Induktivt definerte funksjoner

Induktiv definisjon av en funksjon

Hvis en mengde M er definert induktivt, så er det naturlig å definere funksjoner $M \to X$ induktivt.

Eksempel. *Definer funksjonen* $d : \mathbb{N} \to \mathbb{N}$ *induktivt ved*

- $d(0) := 0$
- $d(n+1) := d(n) + 1 + 1$ *for alle* $n \in \mathbb{N}$

Dette definerer d som minste relasjon $\subseteq \mathbb{N} \times \mathbb{N}$ som oppfyller

- $\langle 0, 0\rangle \in d$ og
- $\langle n+1, m+1+1\rangle \in d$ for alle $\langle n, m\rangle \in d$.

Eksempel (Naturlig tall representert av binær tall)**.**

- $v(0) = 0$
- $v(1) = 1$
- $v(b0) = 2v(b)$ *for alle* $b \in \mathbb{B}$
- $v(b1) = 2v(b) + 1$ *for alle* $b \in \mathbb{B}$

Eksempel (Lengden av symmetrisk streng)**.**

- $l(\epsilon) = 0$
- $l(axa) = l(x) + 2$ *for alle* $x \in S$
- $l(bxb) = l(x) + 2$ *for alle* $x \in S$

1.2.3 Induktive bevis

Strukturell induksjon

For å vise at alle naturlige tall $n \in \mathbb{N}$ har et egenskap $P(n)$

- Vis at egenskapet holder for 0, d.v.s. $P(0)$
- For alle $n \in \mathbb{N}$ med $P(n)$, vis at $P(n+1)$

Eksempel. *For å vise at $d(n) = 2n$ for alle $n \in \mathbb{N}$, definer:*

$$P(n) \quad \Leftrightarrow \quad d(n) = 2n$$

- $P(0)$*: $d(0) = 2 \cdot 0$, gjelder enligt def. av d*
- *Under antakelsen $P(n)$, d.v.s. $d(n) = 2n$, vis $P(n+1)$, d.v.s. $d(n+1) = 2(n+1)$.*

For å vise at alle binære tall $b \in \mathbb{B}$ har et egenskap $P(b)$

- Vis at egenskapet holder for 0, d.v.s. $P(0)$
- Vis at egenskapet holder for 1, d.v.s. $P(1)$
- For alle $b \in \mathbb{B}$ med $P(b)$, vis at $P(b0)$
- For alle $n \in \mathbb{B}$ med $P(b)$, vis at $P(b1)$

For å vise at alle symmetriske strenger $x \in S$ har et egenskap $P(x)$

- Vis at egenskapet holder for ϵ, d.v.s. $P(\epsilon)$
- For alle $x \in S$ med $P(x)$, vis at $P(axa)$
- For alle $x \in s$ med $P(x)$, vis at $P(bxb)$

Vis at $v(b) = v(0b)$ for alle $b \in \mathbb{B}$.

- $P(b) \quad :\Leftrightarrow \quad v(b) = v(0b)$
- $P(0)$: $\quad v(0) = 0 = 2 \cdot 0 = 2v(0) = v(00)$
- $P(1)$: $\quad v(1) = 1 = 2 \cdot 0 + 1 = 2v(0) + 1 = v(01)$
- Anta $P(b)$, d.v.s. $v(b) = v(0b)$.
  - $P(b0)$: $\quad v(b0) = 2v(b) = 2v(0b) = v(0b0)$
  - $P(b1)$: $\quad v(b1) = 2v(b) + 1 = 2v(0b) + 1 = v(0b1)$

Hvorfor er strukturell induksjon korrekt?

- La M være en induktivt definert mengde og P et egenskap
- Undersøk mengden N av alle $x \in M$ med $P(x)$.
- Se på induktivt bevis:
  - Basis: $P(b)$ for alle $b \in B \Rightarrow B \subseteq N$
  - Operasjoner: $P(x)$ og $P(y)$ impliserer $P(f(x,y))$ for alle $x, y \in M \Rightarrow f(x,y) \in N$ for alle $x, y \in N$.
- Derfor, $N \in \mathcal{M}$, som vi definert tidligere!
- $M \subseteq N$ fordi M er minst i $\mathcal{M}$.
- Med andre ord, $P(x)$ for alle $x \in M$.

Forelesning 1: Introduksjon, Semantikk, Sekventkalkyle

Arild Waaler - 21. januar 2008

2.1 Induktive definisjoner

Induktive definisjoner

Definisjon 2.1.1 (Induktiv definisjon)**.** *Å definere en mengde induktivt betyr å konstruere den minste mengden som inneholder en gitt mengde B—kalt en* basismengde*—og som er lukket under gitte operasjoner.*

Eksempel. *Mengden $\mathbb{N}$ av naturlige tall kan defineres induktivt ved*

- $0 \in \mathbb{N}$*, og*
- *hvis $x \in \mathbb{N}$, så $x + 1 \in \mathbb{N}$.*

Her er basismengden $\{0\}$ og $\mathbb{N}$ er lukket under suksessorfunksjonen (x+1).

Eksempel. *Mengden av binære tall kan defineres induktivt ved*

- *0 og 1 er binære tall, og*
- *hvis b er et binært tall, så er $b0$ og $b1$ binære tall.*

steg 0:	0	1						
steg 1:	00	10	01	11				
steg 2:	000	100	010	110	001	101	011	111
⋮								

Eksempel. *Menden S av symmetriske strenger kan defineres induktivt ved*

- *$\epsilon \in S$ (den tomme strengen),*
- *hvis $x \in S$, så $axa \in S$ og $bxb \in S$.*

steg 0:	ϵ			
steg 1:	aa	bb		
steg 2:	$aaaa$	$abba$	$baab$	$bbbb$
⋮				

2.2 Utsagnslogikk

2.2.1 Introduksjon

Utsagnslogikk

Studie av de *utsagnslogiske konnektivene*.

- Vi starter med en mengde *atomære* utsagn, f.eks.
  - *"parkeringsplassen er stengt"*
  - *"IFI2 bygges"*
- Den interne strukturen til atomære utsagn blir ikke analysert.
- Atomære utsagn er enten *sanne* eller *usanne*.

- Sammensatte utsagn bygges opp fra de atomære utsagnene ved hjelp av de logiske konnektivene: og, eller, ikke, hvis ... så ...
- Eksempel: *"IFI2 bygges og parkeringsplassen er stengt"*
- Hvordan avhenger sannhetsverdien til et sammensatt utsagn av sannhetsverdiene til de atomære utsagnene det er bygget opp av?
- Hvilke utsagn er sanne *uavhengig* av sannhetsverdiene til de atomære utsagnene?
- Slike utsagn kalles *tautologier*.
- Eksempel: *"IFI2 bygges eller IFI2 bygges ikke"*

- *Syntaks:* et presist definert symbolspråk for å representere utsagnslogiske utsagn.
- *Semantikk:* en presist definert tolkning av uttrykk i symbolspråket til sannhetsverdiene *sann* og *usann*.
- *Kalkyle:* syntaktisk manipulasjon av uttrykk i symbolspråket for å finne *bevisbare* uttrykk.
- *Sunnhet:* alle bevisbare uttrykk er tautologier — korrekthet av kalkylen.
- *Kompletthet:* alle tautologier er bevisbare — kalkylen sterk nok til å fange inn *alle* interessante uttrykk.

2.2.2 Syntaks

Syntaks

Definisjon 2.2.1 (Utsagnsvariable)**.** *Mengden av* utsagnsvariable *er en tellbart uendelig mengde* $\mathcal{V}_u = \{P_1, P_2, P_3, \ldots\}$.

- Utsagnsvariable representerer *atomære utsagn*, f.eks.
  - *"IFI2 bygges"*
  - *"Forskningsparken er yngre enn IFI1"*
  - *"logikk er gøy"*

Notasjon. *Vi skriver ofte utsagnsvariable som* $P, Q, R, \ldots$

For å fange inn sammensatte utsagn, f.eks.

"hvis IFI2 bygges, så er parkeringsplassen stengt,"

trengs flere symboler i språket:

Definisjon 2.2.2 (Utsagnslogisk alfabet)**.** *Det* utsagnslogiske alfabet *består av:*

- *Utsagnsvariablene i* $\mathcal{V}_u$*.*
- *De* logiske konnektivene $\wedge$, $\vee$, $\rightarrow$ *og* $\neg$*.*
- *Hjelpesymbolene '(' og ')'.*

Intuisjon: $\neg$ skal bety *"ikke"* $\wedge$ skal bety *"og"*
$\vee$ skal bety *"eller"* $\rightarrow$ skal bety *"impliserer"*

Utsagnslogiske formler

Definisjon 2.2.3 (Atomær formel)**.** *Enhver utsagnsvariabel er en* atomær formel*.*

Definisjon 2.2.4 (Utsagnslogisk formel)**.** *Mengden av* utsagnslogiske formler *er den minste mengden* $\mathcal{F}_u$ *slik at:*

1. $\mathcal{F}_u$ *inneholder alle atomære formler.*
2. *Hvis* $A \in \mathcal{F}_u$*, så er* $\neg A \in \mathcal{F}_u$*.*
3. *Hvis* $A, B \in \mathcal{F}_u$*, så er* $(A \wedge B)$*,* $(A \vee B)$ *og* $(A \rightarrow B)$ *med i* $\mathcal{F}_u$*.*

Eksempel (Utsagnslogiske formler)**.**

- P
- $(P \rightarrow Q)$
- $((P \vee Q) \wedge \neg(P \vee R))$

Notasjon. *Vi dropper ofte unødvendige parenteser:*

$$\begin{array}{lll} (P \rightarrow Q) & \textit{skrives} & P \rightarrow Q \\ ((P \vee Q) \wedge \neg(P \vee R)) & \textit{skrives} & (P \vee Q) \wedge \neg(P \vee R) \end{array}$$

Eksempel. *Ikke alle strenger over det utsagnslogiske alfabet er utsagnslogiske formler:*

- $P \rightarrow$
- $((Q \wedge P)$

Oppgave. *Vis at* $((Q \wedge P)$ ikke *er en utsagnslogisk formel.*

- Intuitivt, men
- hvordan *bevise* det?
- Ved *strukturell induksjon* kan vi vise noe *sterkere*:

Påstand 2.2.1. *Alle utsagnslogiske formler har like mange venstre- og høyreparenteser.*

2.2.3 Strukturell induksjon

Strukturell induksjon

- Mengden $\mathcal{F}_u$ av utsagnslogiske formler er definert *induktivt*.
- Ved *strukturell induksjon* kan man vise at en egenskap holder for *alle* formler i $\mathcal{F}_u$.

Teorem 2.2.1 (Strukturell induksjon)**.** *Alle formler i $\mathcal{F}_u$ har egenskapen* $\mathbf{Q}$ *hvis:*

Basissteg: Alle atomære formler har egenskapen $\mathbf{Q}$*.*

Induksjonssteg:

- *Hvis A har egenskapen* $\mathbf{Q}$*, så har også $\neg A$ egenskapen* $\mathbf{Q}$*.*
- *Hvis A og B har egenskapen* $\mathbf{Q}$*, så har også $(A \wedge B)$, $(A \vee B)$ og $(A \rightarrow B)$ egenskapen* $\mathbf{Q}$*.*

- Strukturell induksjon er en bevisteknikk vi kommer til å bruke *mye*!
- Derfor er det viktig å kunne den godt...

Påstand 2.2.2 (Balanserte parenteser)**.** *Alle formler $A \in \mathcal{F}_u$ har like mange venstre- og høyreparenteser.*

Bevis. Basissteg: Hvis A er atomær, inneholder den ikke parenteser. Dermed holder påstanden trivielt.

Induksjonssteg:

- Anta $A = \neg B$ og at påstanden holder for B. A har like mange parenteser som B. Dermed holder påstanden også for A.
- Anta $A = (B \circ C)$ for $\circ \in \{\wedge, \vee, \rightarrow\}$, og at påstanden holder for B og C. A har én venstre- og én høyreparentes i tillegg til de som finnes i B og C. Siden påstanden holder for B og C, holder den også for A.

□

Tilbake til uttrykket $((Q \wedge P)$:

Påstand 2.2.3. $((Q \wedge P)$ *er* ikke *en utsagnslogisk formel.*

Bevis.

1. Vi har vist at alle utsagnslogiske formler har like mange venstre- og høyreparenteser.
2. Det *kontrapositive* er at hvis et uttrykk *ikke* har like mange venstre- og høyreparenteser, så er det *ikke* en utsagnslogisk formel.
3. Uttrykket '$((Q \wedge P)$' har to venstre- og én høyreparentes, altså ulikt antall.
4. Derfor er det *ikke* en utsagnslogisk formel.

□

2.2.4 Semantikk

Semantikk

- Vi skal tolke utsagnslogiske formler som enten *sanne* eller *usanne*.

Definisjon 2.2.5. *La* $\mathbf{Bool} = \{\mathbf{1}, \mathbf{0}\}$.

Definisjon 2.2.6 (Operatorene $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$ og $\hat{\rightarrow}$)**.**

- *Vi definerer en unær operator* $\hat{\neg}$ *på* **Bool** *slik at* $\hat{\neg}\mathbf{1} = \mathbf{0}$ *og* $\hat{\neg}\mathbf{0} = \mathbf{1}$.
- *Vi definerer de binære operatorene* $\hat{\vee}$, $\hat{\wedge}$ *og* $\hat{\rightarrow}$ *på* **Bool** *som følger:*

x	y	$x \hat{\wedge} y$	$x \hat{\vee} y$	$x \hat{\rightarrow} y$
0	**0**	**0**	**0**	**1**
0	**1**	**0**	**1**	**1**
1	**0**	**0**	**1**	**0**
1	**1**	**1**	**1**	**1**

Tabellen over kalles en *sannhetsverditabell*.

Definisjon 2.2.7 (Boolsk valuasjon)**.** *En* boolsk valuasjon *er en funksjon* v *fra* $\mathcal{F}_u$ *til* **Bool** *slik at:*

- $v(\neg A) = \hat{\neg} v(A)$
- $v(A \wedge B) = v(A) \hat{\wedge} v(B)$
- $v(A \vee B) = v(A) \hat{\vee} v(B)$
- $v(A \rightarrow B) = v(A) \hat{\rightarrow} v(B)$

Merk.

- *Symbolene* $\neg$, $\wedge$, $\vee$ *og* $\rightarrow$ *på venstresiden er de utsagnslogiske konnektivene, som er en del av* syntaksen.
- *Symbolene* $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$ *og* $\hat{\rightarrow}$ *på høyresiden er operatorer på* **Bool**, *og en del av* semantikken.

Eksempel.

- *Se på formelen* $\neg P \rightarrow Q$.
- *La* v *være en valuasjon slik at* $v(P) = \mathbf{1}$ *og* $v(Q) = \mathbf{0}$.
- *Vi får:*

$$\begin{aligned} v(\neg P \rightarrow Q) &= v(\neg P) \hat{\rightarrow} v(Q) \\ &= (\hat{\neg}\, v(P)) \hat{\rightarrow} v(Q) \\ &= (\hat{\neg}\, \mathbf{1}) \hat{\rightarrow} v(Q) \\ &= (\hat{\neg}\, \mathbf{1}) \hat{\rightarrow} \mathbf{0} \\ &= \mathbf{0} \hat{\rightarrow} \mathbf{0} \\ &= \mathbf{1} \end{aligned}$$

Definisjon 2.2.8 (Oppfyllbar)**.**

- *En boolsk valuasjon v* oppfyller *en utsagnslogisk formel A hvis $v(A) = \mathbf{1}$. Skrives ofte $v \models A$.*
- *En utsagnslogisk formel er* oppfyllbar *hvis det finnes en boolsk valuasjon som oppfyller den.*

Eksempel.

- *Formelen $P \to Q$ er oppfyllbar: den oppfylles av alle valuasjoner v slik at $v(P) = \mathbf{0}$ eller $v(Q) = \mathbf{1}$.*
- *Formelen $\neg(P \to P)$ er* ikke *oppfyllbar. Hvorfor?*

Definisjon 2.2.9 (Falsifiserbar)**.**

- *En boolsk valuasjon v* falsifiserer *en utsagnslogisk formel A hvis $v(A) = \mathbf{0}$. Skrives ofte $v \not\models A$.*
- *En utsagnslogisk formel er* falsifiserbar *hvis det finnes en boolsk valuasjon som falsifiserer den.*

Eksempel.

- *Formelen $P \to Q$ er falsifiserbar: den falsifiseres av alle valuasjoner v slik at $v(P) = \mathbf{1}$ og $v(Q) = \mathbf{0}$.*
- *Formelen $P \to P$ er* ikke *falsifiserbar. Hvorfor?*

Definisjon 2.2.10 (Tautologi)**.** *En utsagnslogisk formel A er en* tautologi *hvis $v \models A$ for* alle *boolske valuasjoner v.*

Eksempel.

- *Er P en tautologi?*
- *Hva med $\neg(P \to P)$?*
- *Og $P \to P$?*

Definisjon 2.2.11 (Motsigelse)**.** *En utsagnslogisk formel A er en* motsigelse *hvis $v \not\models A$ for* alle *boolske valuasjoner v.*

Merk.

- *Det motsatte av en tautologi er den falsifiserbar formel.*
- *Det motsatte av en motsigelse er den oppfyllbar formel.*
- *En tautologi er ikke det motsatte av en motsigelse!*

Påstand 2.2.4. *En utsagnslogisk formel A er en tautologi hvis og bare hvis A* ikke *er falsifiserbar.*

Bevis. formelen A er en tautologi $\Leftrightarrow$ $v \models A$ for alle valuasjoner $v \Leftrightarrow$ det finnes ingen valuasjon v slik at $v \not\models A \Leftrightarrow$ A er ikke falsifiserbar

□

Hvis og bare hvis – $\Leftrightarrow$

Merk.

- *Begrepet* "hvis og bare hvis" *uttrykker toveis implikasjon.*
- *Skrives ofte* $\Leftrightarrow$.
- P "hvis og bare hvis" Q *kan uttrykkes i utsagnslogikk som*

$$(P \to Q) \wedge (Q \to P)$$

2.3 Sekventkalkyle

2.3.1 Motivasjon

Sekventkalkyle for utsagnslogikk

- Hvordan finne ut om en gitt formel er en *tautologi*?
- Fra semantikken: Hvis formelen *ikke* er falsifiserbar, så er den en tautologi.
- Idé: Å systematisk forsøke å falsifisere formelen.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg Q, P \vdash P}}{\neg Q \vdash \neg P, P}}{\vdash P, \neg Q \to \neg P} \qquad \dfrac{\dfrac{\dfrac{}{Q \vdash Q, \neg P}}{Q, \neg Q \vdash \neg P}}{Q \vdash \neg Q \to \neg P}}{P \to Q \vdash \neg Q \to \neg P}$$
$$\vdash (P \to Q) \to (\neg Q \to \neg P)$$

Eksempel

- Falsifisere formelen $(P \to Q) \to (\neg Q \to \neg P)$:
  - oppfylle $P \to Q$,
  - *og* falsifisere $\neg Q \to \neg P$.
- *Formler til* venstre *for* '$\vdash$' *skal* oppfylles.
- *Formler til* høyre *for* '$\vdash$' *skal* falsifiseres.

- Oppfylle $P \to Q$:
  - falsifisere P,
  - *eller* oppfylle Q.
- $\neg Q \to \neg P$ må kunne falsifiseres uavhengig av hvordan $P \to Q$ oppfylles.
- Formelen kopieres derfor inn i begge de nye løvnodene.

- Falsifisere $\neg Q \to \neg P$ i venstre løvnode:
  - oppfylle $\neg Q$,
  - *og* falsifisere $\neg P$.
- Tilsvarende, falsifisere $\neg Q \to \neg P$ i høyre løvnode:
  - oppfylle $\neg Q$,
  - *og* falsifisere $\neg P$.

- Falsifisere $\neg P$ i venstre løvnode:
  - oppfylle P.
- Oppfylle $\neg Q$ i høyre løvnode:
  - falsifisere Q.

- Venstre løvnode:
  - Oppfylle: $\neg Q$, P. Falsifisere: P.
  - Umulig, kan *ikke* både oppfylle og falsifisere P!
- Høyre løvnode:
  - Oppfylle: Q. Falsifisere: Q, $\neg P$.
  - Umulig, kan *ikke* både oppfylle og falsifisere Q!
- $(P \to Q) \to (\neg Q \to \neg P)$ kan ikke falsifiseres!

Kommentarer til det foregående eksempelet:

- Vi arbeidet med objekter av typen '$\ldots \vdash \ldots$'. Slike objekter kaller vi for *sekventer*.
- Ved å se på konnektivet til en bestemt formel i en sekvent konstruerte vi nedenfra og opp nye sekventer fra eksisterende. Hvilke nye sekventer vi får bestemmes av *regler*.
- Gjennom gjentatt anvendelse av regler konstruerte vi et tre-lignende objekt med en rotnode og løvnoder. Et slikt objekt kalles en *utledning*.
- Den utledningen vi konstruerte var slik at sekventene i løvnodene hadde noe likt på begge sier av '$\vdash$'. En utledning med denne egenskapen kalles et *bevis*.

Vi skal nå definere helt presist hva vi legger i disse begrepene!

2.3.2 Sekventer og aksiomer

Sekventkalkylen LK

Definisjon 2.3.1 (Sekvent)**.** *En sekvent er et objekt på formen* $\Gamma \vdash \Delta$ *slik at* Γ *og* Δ *er multimengder av utsagnslogiske formler.*

- Formlene som står til venstre for '$\vdash$' kalles *antecedent*.
- Formlene som står til høyre for '$\vdash$' kalles *succedent*.

Notasjon. *I sekventer leses '*,*' som union:*

- Γ, A *skal bety* $\Gamma \cup \{A\}$.

Eksempel. *Hvilke av uttrykkene nedenfor er sekventer?*

- $P \vdash Q$
- $P, P \vdash Q, P$
- $\vdash P \to Q$
- $\vdash P \vdash Q$
- $P, Q \to R \vdash Q \to R$
- $P, Q \to R \vdash Q \to R, P$
- $P, 1, P \to Q \vdash P \to 2$

Definisjon 2.3.2 (Aksiom)**.** *Et aksiom er en sekvent på formen* $\Gamma, A \vdash A, \Delta$ *slik at* A *er en* atomær *utsagnslogisk formel.*

Hvilke av sekventene i eksempelet over er aksiomer?

2.3.3 Sekventkalkylereglene

Sekventkalkyleregler

Definisjon 2.3.3 (α-regler)**.** *α-reglene i sekventkalkylen* LK *er:*

$$\frac{\Gamma, A\ ,\ B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \mathsf{L}\wedge \qquad \frac{\Gamma \vdash A\ ,\ B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \mathsf{R}\vee$$

$$\frac{\Gamma, A \vdash \quad B, \Delta}{\Gamma \quad \vdash A \to B, \Delta}\ \mathsf{R}\to$$

$$\frac{\Gamma \quad \vdash A, \Delta}{\Gamma, \neg A \vdash \quad \Delta}\ \mathsf{L}\neg \qquad \frac{\Gamma, A \vdash \quad \Delta}{\Gamma \quad \vdash \neg A, \Delta}\ \mathsf{R}\neg$$

α-reglene kalles ofte *ett-premissregler*.

Definisjon 2.3.4 (β-regler)**.** β-reglene *i sekventkalkylen* LK *er:*

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \mathsf{R}\wedge$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \mathsf{L}\vee$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \mathsf{L}\to$$

β-reglene kalles ofte *to-premissregler*.

Definisjon 2.3.5 (Slutningsreglene i LK)**.** Slutningsreglene *i sekventkalkylen* LK *er* α- *og* β*-reglene.*

Begreper knyttet til regler

Se på regelen

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \mathsf{L}\vee$$

- Sekventene *over* streken kalles *premisser*.
- Sekventen *under* streken kalles *konklusjon*.
- Teksten til høyre for streken er regelens *navn*.
- Formelen som forekommer eksplisitt i konklusjonen kalles *hovedformel*.
- Formlene som forekommer eksplisitt i premissene kalles *aktive formler*.
- Formlene som forekommer i Γ og Δ kalles *ekstraformler*.

2.3.4 Slutninger

Regler vs. slutninger

Definisjon 2.3.6 (LK-slutning)**.**

- *En* slutning *er en instans av en regel hvor*
  - A *og* B *er erstattet med utsagnslogiske formler*
  - Γ *og* Δ *er erstattet med multimengder av utsagnslogiske formler*
- *Slutninger av en regel med navn eller type* θ *kalles* θ-slutninger.

Eksempel. *En regel* $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \mathsf{R}\neg$ *definerer uendelig mange* $\mathsf{R}\neg$*-slutninger:*

$$\frac{P \vdash}{\vdash \neg P} \qquad \frac{Q, P \vdash}{Q \vdash \neg P} \qquad \frac{Q \to R, P \vdash P}{Q \to R \vdash \neg P, P} \qquad \cdots$$

Begrepene knyttet til regler anvendes om slutninger:

$$\frac{P \to Q, P \vdash Q \qquad P \to Q, R \vdash Q}{P \to Q, P \vee R \vdash Q}\,\mathsf{L}\vee$$

- Sekventene *over* streken kalles *premisser*.
- Sekventen *under* streken kalles *konklusjon*.
- Formelen $P \vee R$ i konklusjonen er *hovedformel*.
- Formlene P og R i premissene er *aktive formler*.
- De andre formlene er *ekstraformler*.

2.3.5 Utledninger

Utledninger

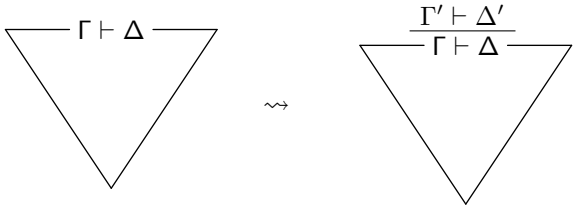
- En utledning er et tre der nodene er sekventer.
- Rotnoden er nederst og løvnodene er øverst.
- Rotnoden kalles *rotsekvent*.
- Løvnodene kalles *løvsekventer*.

Definisjon 2.3.7 (Mengden av LK-utledninger – basistilfelle)**.** *En sekvent* $\Gamma \vdash \Delta$ *er en* LK-utledning.

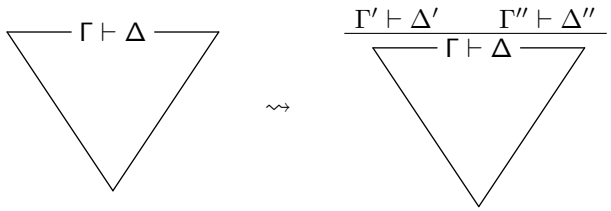
$$\Gamma \vdash \Delta$$

Her er $\Gamma \vdash \Delta$ *både rotsekvent og løvsekvent.*

Definisjon 2.3.8 (Mengden av LK-utledninger – α-utvidelse)**.** *Hvis det finnes en* LK*-utledning med en løvsekvent* $\Gamma \vdash \Delta$ *og en* α*-slutning med konklusjon* $\Gamma \vdash \Delta$ *og premiss* $\Gamma' \vdash \Delta'$*, så er objektet vi får ved å plassere* $\Gamma' \vdash \Delta'$ *over* $\Gamma \vdash \Delta$ *en* LK-utledning.



Definisjon 2.3.9 (Mengden av LK-utledninger – β-utvidelse)**.** *Hvis det finnes en* LK*-utledning med en løvsekvent* $\Gamma \vdash \Delta$ *og en* β*-slutning med konklusjon* $\Gamma \vdash \Delta$ *og premisser* $\Gamma' \vdash \Delta'$ *og* $\Gamma'' \vdash \Delta''$*, så er objektet vi får ved å plassere* $\Gamma' \vdash \Delta'$ *og* $\Gamma'' \vdash \Delta''$ *over* $\Gamma \vdash \Delta$ *en* LK-utledning.



β-utvidelse gir forgrening i utledningen!

Eksempel (LK-utledninger)**.**

$$\vdash R \vee Q \qquad\qquad P \to Q \vdash \neg Q \to \neg P$$

$$\frac{P \vdash Q}{\vdash P \to Q}\,\mathsf{R}\to \qquad \frac{\vdash P \qquad \vdash P}{\vdash P \wedge P}\,\mathsf{R}\wedge$$

$$\dfrac{\dfrac{P \vdash P \qquad P \vdash Q}{P \vdash P \wedge Q}\,\mathsf{R}\wedge \qquad \dfrac{Q \vdash P \qquad Q \vdash Q}{Q \vdash P \wedge Q}\,\mathsf{R}\wedge}{P \vee Q \vdash P \wedge Q}\,\mathsf{L}\vee$$

2.3.6 Bevis

LK-bevis

Definisjon 2.3.10 (LK-bevis)**.** *Et* LK-bevis *er en* LK*-utledning der alle løvsekventene er aksiomer.*

Definisjon 2.3.11 (LK-bevisbar)**.** *En sekvent* $\Gamma \vdash \Delta$ *er* LK-bevisbar *hvis det finnes et* LK*-bevis med* $\Gamma \vdash \Delta$ *som rotsekvent.*

Eksempel (LK-bevis)**.**

$$\dfrac{\overset{\times}{P \vdash P}}{\vdash P \to P}\,\mathsf{R}\to$$

$$\dfrac{\dfrac{\dfrac{\overset{\times}{\neg Q, P \vdash P}}{\neg Q \vdash \neg P, P}\,\mathsf{R}\neg}{\vdash P, \neg Q \to \neg P}\,\mathsf{R}\to \qquad \dfrac{\dfrac{\overset{\times}{Q \vdash Q, \neg P}}{Q, \neg Q \vdash \neg P}\,\mathsf{L}\neg}{Q \vdash \neg Q \to \neg P}\,\mathsf{R}\to}{P \to Q \vdash \neg Q \to \neg P}\,\mathsf{L}\to$$

- *Sekventene* $\vdash P \to P$ *og* $P \to Q \vdash \neg Q \to \neg P$ *er bevisbare, siden det finnes* LK*-bevis med disse sekventene som rotsekvent.*

Merk: symbolet '$\times$' er *ikke* en del av kalkylen, men et hjelpesymbol vi bruker for å markere at en gren er lukket.

2.4 Oppgaver

Husk at $\mathbb{N}$ er mengden av de naturlige tall (altså $\mathbb{N} = \{0, 1, 2, \ldots\}$), og at $\mathbb{Z}$ er mengden av heltall (altså $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$). La $d, n \in \mathbb{N}$. Vi sier at d *deler* n, og skriver $d \mid n$, hvis det finnes $m \in \mathbb{N}$ slik at $n = dm$.

Oppgave 2.1 La $A = \{2, 3, 4\}$ og $B = \{6, 8, 10\}$. Vi definerer en binær relasjon R fra A til B som følger:

$$\langle x, y \rangle \in R \text{ hvis og bare hvis } x \mid y$$

a. Er $\langle 4, 6 \rangle \in R$? Er $\langle 4, 8 \rangle \in R$? Er $\langle 3, 8 \rangle \in R$? Er $\langle 2, 10 \rangle \in R$?

b. Skriv R som en mengde ordnede par.

Oppgave 2.2 Vi definerer *kongruens modulo 2*-relasjonen K fra $\mathbb{Z}$ til $\mathbb{Z}$ slik:

$$\langle m, n \rangle \in K \text{ hvis og bare hvis } m - n \text{ er et partall}$$

a. Er $\langle 0, 0 \rangle \in K$? Er $\langle 5, 2 \rangle \in K$? Er $\langle 6, 6 \rangle \in K$? Er $\langle -1, 7 \rangle \in K$?

b. Vis at for alle partall $n \in \mathbb{Z}$ så er $\langle n, 0 \rangle \in K$.

Oppgave 2.3 Nedenfor listes åtte binære relasjoner over mengden $A = \{0, 1, 2, 3\}$. For hver relasjon, finn ut hvilke av egenskapene *refleksiv*, *symmetrisk* og *transitiv* den har. *Hint:* Det kan være lurt å tegne graphen til relasjonen som et hjelpemiddel.

a. $R_1 = \{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 0, 3 \rangle, \langle 1, 1 \rangle, \langle 1, 0 \rangle, \langle 2, 3 \rangle, \langle 3, 3 \rangle\}$

b. $R_2 = \{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle\}$

c. $R_3 = \{\langle 2, 3 \rangle, \langle 3, 2 \rangle\}$

d. $R_4 = \{\langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 1, 3 \rangle, \langle 3, 1 \rangle\}$

e. $R_5 = \{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 1, 2 \rangle\}$

f. $R_6 = \{\langle 0, 1 \rangle, \langle 0, 2 \rangle\}$

g. $R_7 = \{\langle 0, 3 \rangle, \langle 2, 3 \rangle\}$

h. $R_8 = \{\langle 0, 0 \rangle, \langle 1, 1 \rangle\}$

Oppgave 2.4 La A være en ikke-tom mengde, og la $\mathcal{P}(A)$ være potensmengden til A, dvs. mengden av alle delmengder av A. Finn ut hvorvidt relasjonene nedenfor har egenskapene *refleksiv*, *symmetrisk* eller *transitiv*. Begrunn svaret ditt.

a. Delmengde-relasjonen D på $\mathcal{P}(A)$:

$$\langle X, Y \rangle \in D \quad \Leftrightarrow \quad X \subseteq Y$$

b. Ulikhets-relasjonen U på $\mathcal{P}(A)$:

$$\langle X, Y \rangle \in U \quad \Leftrightarrow \quad X \neq Y$$

c. Relativ komplement-relasjonen K på $\mathcal{P}(A)$:

$$\langle X, Y \rangle \in K \quad \Leftrightarrow \quad Y = A \setminus X$$

Forelesning 2: Sunnhet og kompletthet av utsagnslogikk

Arild Waaler - 28. januar 2008

3.1 Sekventkalkyle

3.1.1 Semantikk for sekventer

Semantikk for sekventer

Definisjon 3.1.1 (Gyldig sekvent)**.** *En sekvent* $\Gamma \vdash \Delta$ *er* gyldig *hvis alle valuasjoner som oppfyller alle formlene i* Γ *også oppfyller minst én formel i* Δ*.*

Eksempel. *Følgende sekventer er gyldige:*

- $P \vdash P$
- $P \to Q \vdash P \to Q$
- $P, P \to Q \vdash Q$
- $P \to Q \vdash \neg Q \to \neg P$

Definisjon 3.1.2 (Motmodell/falsifiserbar sekvent)**.**

- *En valuasjon* v *er en* motmodell *til sekventen* $\Gamma \vdash \Delta$ *hvis* v *oppfyller alle formlene i* Γ *og falsifiserer alle formlene i* Δ*.*
- *Vi sier at en motmodell til en sekvent* falsifiserer *sekventen.*
- *En sekvent er* falsifiserbar *hvis den har en motmodell.*

Eksempel. *Følgende sekventer er falsifiserbare:*

- $P \vdash Q$ — *Motmodell:* $v(P) = \mathbf{1}, v(Q) = \mathbf{0}$
- $P \vee Q \vdash P \wedge Q$ — *Motmodell: som over eller* $v(P) = \mathbf{0}, v(Q) = \mathbf{1}$
- $\vdash P$ — *Motmodell:* $v(P) = \mathbf{0}$
- $P \vdash$ — *Motmodell:* $v(P) = \mathbf{1}$
- $\vdash$ — *Motmodell: alle modeller!*

3.1.2 Oppsummering

Gyldig

- $P, P \to Q \vdash Q$
- Hvis $v \models P$ og $v \models P \to Q$, så $v \models Q$.

Bevisbar

$$\dfrac{\dfrac{}{P \vdash P}\times \qquad \dfrac{}{Q \vdash Q}\times}{P, P \to Q \vdash Q}$$

Falsifiserbar

- $\neg P, P \to Q \vdash \neg Q$
- En valuasjon v slik at $v \not\models P$ og $v \models Q$.

Ikke bevisbar

$$\dfrac{\dfrac{\vdash P, P}{\neg P \vdash P} \qquad \dfrac{Q, Q \vdash}{Q \vdash \neg Q}}{\neg P, P \to Q \vdash \neg Q}$$

3.2 Sunnhet

3.2.1 Introduksjon

Sunnhet av LK

- Vi ønsker at alle LK-bevisbare sekventer skal være gyldige!
- Hvis ikke, så er LK *ukorrekt* eller *usunn* ...

Definisjon 3.2.1 (Sunnhet)**.** *Sekventkalkylen* LK *er* sunn *hvis enhver* LK*-bevisbar sekvent er gyldig.*

Teorem 3.2.1. *Sekventkalkylen* LK *er sunn.*

Sunnhetsteoremet sikrer oss at LK er en *korrekt* kalkyle.

Hvordan vise sunnhetsteoremet?

Vi viser følgende lemmaer:

1. Alle LK-reglene bevarer falsifiserbarhet oppover.
2. En LK-utledning med falsifiserbar rotsekvent har minst én falsifiserbar løvsekvent.
3. Alle aksiomer er gyldige.

Til slutt vises sunnhetsteoremet ved hjelp av lemmaene.

3.2.2 Bevaring av falsifiserbarhet

Definisjon 3.2.2. *En* LK*-regel* θ *er* falsifiserbarhetsbevarende *(oppover) hvis alle valuasjoner som falsifiserer konklusjonen i en* θ*-slutning også falsifiserer minst ett av premissene i slutningen.*

Lemma 3.2.1. *Alle* LK*-reglene er falsifiserbarhetsbevarende.*

- Vi får ett delbevis for hver LK-regel.
- Se på f.eks. L→-regelen:

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \mathsf{L}{\to}$$

- I delbeviset for L→ må vi vise at alle L→-slutninger bevarer falsifiserbarhet oppover.
- Regelen L→ generaliserer alle L→-slutninger.
- Vi lar Γ, Δ, A og B i regelen stå for vilkårlige (multimengder av) utsagnslogiske formler og viser på den måten at alle L→-slutninger bevarer falsifiserbarhet.

Bevis for R¬. $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \mathsf{R}{\neg}$

- Anta at v falsifiserer konklusjonen.
- Det betyr at $v \models \Gamma$, $v \not\models \neg A$ og v *falsifiserer alle formlene i* Δ.
- Pr. definisjon av v har vi at $v \models A$.
- *Vi har da at* $v \models \Gamma \cup \{A\}$ *og* v *falsifiserer alle formlene i* Δ.
- Da falsifiserer v premisset.

□

Bevis for L→. $\dfrac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \mathsf{L}{\to}$

- Anta at v falsifiserer konklusjonen.
- Det betyr at v *oppfyller* $\Gamma \cup \{A \to B\}$ og falsifiserer alle formlene i Δ.
- Siden v oppfyller $A \to B$, så har vi pr. definisjon av v at

  (1) $v \not\models A$, eller
  (2) $v \models B$.

- Hvis (1), så falsifiserer v venstre premiss.
- Hvis (2), så falsifiserer v høyre premiss.

□

Bevis for "for alle"-påstander

- Se på påstanden "for alle $x \in S$: $P(x)$".
- Vi kan vise påstanden ved å vise at $P(a)$ for hvert element $a \in S$.
- Hva hvis S er svært stor eller uendelig?
- Vi kan *generalisere fra et vilkårlig element*:
  - Velg et *vilkårlig* element $a \in S$.
  - Vis at $P(a)$ holder.
  - Siden a var tilfeldig valgt må påstanden i første linje holde.

3.2.3 Eksistens av falsifiserbar løvsekvent

Lemma 3.2.2. *Hvis en valuasjon v falsifiserer rotsekventen i en* LK*-utledning δ, så falsifiserer v minst én av løvsekventene i δ.*

Bevis. Ved strukturell induksjon på LK-utledningen δ.

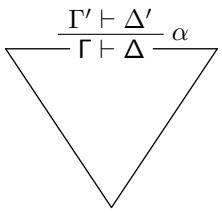
Basissteg: δ er en sekvent $\Gamma \vdash \Delta$:

$$\Gamma \vdash \Delta$$

- Her er $\Gamma \vdash \Delta$ både rotsekvent og (eneste) løvsekvent.
- Anta at v falsifiserer $\Gamma \vdash \Delta$.
- Da falsifiserer v én løvsekvent i δ, nemlig $\Gamma \vdash \Delta$.

□

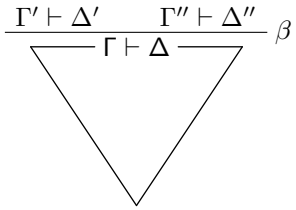
Bevis (induksjonssteg – α-utvidelse). Induksjonssteg: δ er en utledning på formen



- Anta at v falsifiserer rotsekventen i δ, og anta at v falsifiserer en løvsekvent i utledningen *før* α-utvidelsen.
- Hvis den falsifiserte løvsekventen *ikke* er $\Gamma \vdash \Delta$, så er den også løvsekvent i δ. Dermed falsifiserer v en løvsekvent i δ.
- Hvis den falsifiserte løvsekventen *er* $\Gamma \vdash \Delta$, så falsifiserer v også $\Gamma' \vdash \Delta'$ siden α-reglene bevarer falsifiserbarhet.

□

Bevis (induksjonssteg – β-utvidelse). Induksjonssteg: δ er en utledning på formen



- Anta at v falsifiserer rotsekventen i δ, og anta at v falsifiserer en løvsekvent i utledningen *før* β-utvidelsen.
- Hvis den falsifiserte løvsekventen *ikke* er $\Gamma \vdash \Delta$, så er den også løvsekvent i δ. Dermed falsifiserer v en løvsekvent i δ.
- Hvis den falsifiserte løvsekventen *er* $\Gamma \vdash \Delta$, så falsifiserer v også $\Gamma' \vdash \Delta'$ eller $\Gamma'' \vdash \Delta''$ siden β-reglene bevarer falsifiserbarhet.

□

3.2.4 Alle aksiomer er gyldige

Lemma 3.2.3. *Alle aksiomer er gyldige.*

Bevis. $\Gamma, A \vdash A, \Delta$

- Vi skal vise at alle valuasjoner som oppfyller antecedenten også oppfyller én formel i succedenten.
- La v være en tilfeldig valgt valuasjon som oppfyller antecedenten.
- Da oppfyller v formelen A i succedenten.

□

3.2.5 Bevis for sunnhetsteoremet

Bevis for sunnhet.

- Anta at π er et LK-bevis for sekventen $\Gamma \vdash \Delta$.
- Anta for motsigelse at $\Gamma \vdash \Delta$ *ikke* er gyldig.
- Da har den en motmodell v som falsifiserer $\Gamma \vdash \Delta$.
- Vi har da fra tidligere lemma at v falsifiserer minst én løvsekvent i π.

- Da har π en løvsekvent som ikke er et aksiom, siden ingen aksiomer er falsifiserbare.
- Men da er ikke π et LK-bevis.

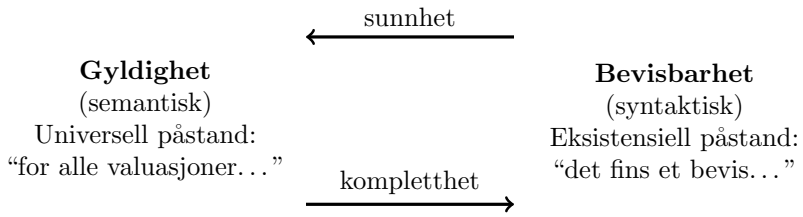
□

3.3 Kompletthet

3.3.1 Introduksjon

Definisjon 3.3.1 (Sunnhet)**.** *Sekventkalkylen* LK *er sunn hvis enhver* LK*-bevisbar sekvent er gyldig.*

Definisjon 3.3.2 (Kompletthet)**.** *Sekventkalkylen* LK *er* komplett *hvis enhver gyldig sekvent er* LK*-bevisbar.*



Sunnhet: $\Gamma \vdash \Delta$ bevisbar $\Rightarrow$ $\Gamma \vdash \Delta$ gyldig
Kompletthet: $\Gamma \vdash \Delta$ gyldig $\Rightarrow$ $\Gamma \vdash \Delta$ bevisbar

- Sunnhet og kompletthet er duale begreper.
- Sunnhet gir at vi ikke kan bevise noe *mer* enn de gyldige sekventene.
- Kompletthet gir at vi kan bevise *alle* gyldige sekventer.
- Husk at vi introduserte LK som et systematisk forsøk på å falsifisere.
- En sekvent er gyldig hvis og bare hvis den ikke er falsifiserbar.
- Vi kan dermed uttrykke sunnhet og kompletthet slik:

Sunnhet: $\Gamma \vdash \Delta$ falsifiserbar $\Rightarrow$ $\Gamma \vdash \Delta$ ikke bevisbar
Kompletthet: $\Gamma \vdash \Delta$ ikke bevisbar $\Rightarrow$ $\Gamma \vdash \Delta$ falsifiserbar

- Noe kan være sunt uten å være komplett.
  - Da vises for lite.
  - Eksempel med primtall: 2, 5, 7, 11, 17, 19, ...
- Noe kan være komplett uten å være sunt.
  - Da vises for mye.
  - Eksempel med primtall: 2, 3, 5, 7, *9*, 11, 13, *15* ...
- Vi ønsker begge deler
  - Hverken for mye eller for lite.
  - Eksempel med primtall: 2, 3, 5, 7, 11, 13, 17, 19 ...

3.3.2 Kompletthetsteoremet

Teorem 3.3.1 (Kompletthet)**.** *Hvis* $\Gamma \vdash \Delta$ *er gyldig, så er den bevisbar i* LK*.*

For å vise *kompletthet* av sekventkalkylen, viser vi den ekvivalente påstanden:

Lemma 3.3.1 (Eksistens av valuasjon)**.** *Hvis* $\Gamma \vdash \Delta$ ikke *er bevisbar i LK, så er den falsifiserbar*

Dvs. det finnes en valuasjon som gjør samtlige formler i Γ sanne og samtlige formler i Δ usanne.

3.3.3 Bevis for kompletthetsteoremet

Anta at $\Gamma \vdash \Delta$ ikke er bevisbar.

- Konstruer en utledning π av $\Gamma \vdash \Delta$ slik at ingen regel lenger kan anvendes. "En maksimal utledning".
- Da fins (minst) en gren G som ikke er lukket. Vi har da at:
  - løvsekventen i G inneholder kun atomære formler, og
  - løvsekventen i G er uten aksiom.
- Vi konstruerer nå en valuasjon som falsifiserer $\Gamma \vdash \Delta$. La

$G^\top$ være mengden av alle formler som forekommer i en antecedent i G, og

$G^\perp$ være mengden av alle formler som forekommer i en succedent i G, og

v være valuasjonen som gjør alle alle atomære formler i $G^\top$ sanne og alle andre atomære formler (spesielt de i $G^\perp$) usanne.

Eksempel

$$\dfrac{\dfrac{\dfrac{\overset{\times}{P \vdash Q, P} \qquad \overset{\times}{Q, P \vdash Q}}{P \to Q, P \vdash Q} \qquad \dfrac{R \vdash Q, P \qquad \overset{\times}{Q, R \vdash Q}}{P \to Q, R \vdash Q}}{P \to Q, P \vee R \vdash Q}}{P \to Q \vdash (P \vee R) \to Q}$$

Vi får at grenen G med løvsekvent $R \vdash Q, P$ ikke er lukket.

$G^\top = \{R, P \to Q, P \vee R\}$

$G^\perp = \{Q, P, (P \vee R) \to Q\}$

$v =$ valuasjonen definert ved $v(R) = 1$ og $v(Q) = v(P) = 0$

Denne valuasjonen falsifiserer rotsekventen.

- Vi viser ved strukturell induksjon på utsagnslogiske formler at valuasjonen v gjør *alle* formler i $G^\top$ sanne og alle formler i $G^\perp$ usanne.

- Påstandene som vi viser for utsagnslogiske formler er:

  Hvis $A \in G^{\top}$, så $v(A) = 1$.
  Hvis $A \in G^{\perp}$, så $v(A) = 0$.

Basissteg: A er en atomær formel i $G^{\top}/G^{\perp}$.

- Påstanden holder, fordi det var slik vi konstruerte $G^{\top}/G^{\perp}$.

Induksjonssteg: Fra antakelsen om at påstanden holder for A og B, så må vi vise at den holder for $\neg A$, $(A \wedge B)$, $(A \vee B)$ og $(A \rightarrow B)$. Dette gir fire forskjellige tilfeller. (Vi viser tre av dem her.)

Anta at $\neg A \in G^{\top}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\perp}$.
- Ved IH har vi $v(A) = 0$.
- Ved definisjonen av valuasjoner har vi $v(\neg A) = 1$.

Anta at $\neg A \in G^{\perp}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\top}$.
- Ved IH har vi $v(A) = 1$.
- Ved definisjonen av valuasjoner har vi $v(\neg A) = 0$.

Anta at $(A \wedge B) \in G^{\top}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\top}$ *og* $B \in G^{\top}$.
- Ved IH har vi $v(A) = 1$ *og* $v(B) = 1$.
- Ved definisjonen av valuasjoner har vi $v(A \wedge B) = 1$.

Anta at $(A \wedge B) \in G^{\perp}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\perp}$ *eller* $B \in G^{\perp}$.
- Ved IH har vi $v(A) = 0$ *eller* $v(B) = 0$.
- Ved definisjonen av valuasjoner har vi $v(A \wedge B) = 0$.

Anta at $(A \rightarrow B) \in G^{\top}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\perp}$ *eller* $B \in G^{\top}$.
- Ved IH har vi $v(A) = 0$ *eller* $v(B) = 1$.

- Ved definisjonen av valuasjoner har vi $v(A \to B) = 1$.

Anta at $(A \to B) \in G^{\perp}$.

- Siden utledningen er "maksimal", har vi $A \in G^{\top}$ *og* $B \in G^{\perp}$.
- Ved IH har vi $v(A) = 1$ *og* $v(B) = 0$.
- Ved definisjonen av valuasjoner har vi $v(A \to B) = 0$.

3.4 Egenskaper ved utsagnslogikk

3.4.1 Uttrykkskraft

Noe av det sterkeste vi kan uttrykke med utsagnslogikk er duehullprinsippet:

Duehullprinsippet / Dirichlets boksprinsipp

Gitt n bokser og $m > n$ objekter, så må minst en boks inneholde mer enn ett objekt.

- Anta at vi har n bokser og $n + 1$ objekter.
- Vi uttrykke duehullprinsippet i utsagnslogikk ved å la P_j^i være en utsagnsvariabel som tolkes som "objekt nr i ligger i boks nr j".
- Hvis vi har 2 bokser og 3 objekter får vi f.eks.
  - Objekt 1 ligger i en av boksene: $P_1^1 \vee P_2^1$.
  - Objekt 3 ligger i en av boksene: $P_1^3 \vee P_2^3$.
  - Boks 1 inneholder både objekt 1 og 2: $P_1^1 \wedge P_1^2$.
  - Boks 2 inneholder både objekt 1 og 3: $P_2^1 \wedge P_2^3$.

3.4.2 Avgjørbarhet

Teorem 3.4.1. *Utsagnslogikk er avgjørbart, dvs. det fins en algoritme som er i stand til etter endelig mange steg å avgjøre hvorvidt en utsagnslogisk formel er gyldig eller ikke.*

- Vår sekventkalkyle gir opphav til en slik algoritme.

3.4.3 Kompleksitet

Teorem 3.4.2. *Oppfyllbarhetsproblemet for utsagnslogikk - å finne ut hvorvidt en formel/sekvent er oppfyllbar eller ikke - er NP-komplett. (Avgjørbart i ikke-deterministisk polynomiell tid.)*

Teorem 3.4.3. *Gyldighetsproblemet for utsagnslogikk er coNP-komplett.*

3.5 Oppgaver

Oppgave 3.1 Skriv opp fem utsagnslogiske formler som har mer enn tre utsagnslogiske konnektiver.

Oppgave 3.2 Hvilke av de følgende uttrykkene er utsagnslogiske formler?

a. P

b. $(P$

c. $(((P \to Q) \vee (R \vee P) \wedge \neg Q)$

d. $(((P \to Q) \vee (R \vee P)) \wedge \neg Q)$

e. $((P \to Q)$

f. "parkeringsplassen er stengt"

Oppgave 3.3 Finn for hver av formlene nedenfor én valuasjon som falsifiserer formelen og én valuasjon som oppfyller den.

a. P

b. $\neg P$

c. $P \wedge Q$

d. $P \vee Q$

e. $P \to Q$

f. $((P \to Q) \vee (R \vee P)) \wedge \neg Q$

Oppgave 3.4 Sett opp en sannhetsverditabell som viser at

a. $P \to Q$ er sann hvis og bare hvis $\neg P \vee Q$ er sann.

b. $(P \to Q) \to (\neg Q \to \neg P)$ er en tautologi.

Oppgave 3.5 La S være en delmengde av utsagnsvariablene, og la v_1 og v_2 være boolske valuasjoner slik at $v_1(P) = v_2(P)$ for alle $P \in S$. Vis ved strukturell induksjon på $\mathcal{F}_u$ at $v_1(A) = v_2(A)$ for alle utsagnslogiske formler A som bare inneholder utsagnsvariable fra S.

Oppgave 3.6 La v_1 og v_2 være boolske valuasjoner slik at hvis $v_1(P) = \mathbf{1}$, så er $v_2(P) = \mathbf{1}$ for alle utsagnsvariable P.

a. Vis at hvis A er en utsagnslogisk formel som *ikke* inneholder noen andre konnektiver enn $\wedge$ og $\vee$, og $v_1(A) = \mathbf{1}$, så er $v_2(A) = \mathbf{1}$.

b. Holder det at hvis A ikke inneholder andre konnektiver enn $\wedge$ og $\vee$, og $v_2(A) = \mathbf{1}$, så er $v_1(A) = \mathbf{1}$? Begrunn svaret ditt.

Merk i de påfølgende oppgaver at Gallier bruker litt andre symboler og begreper enn i kurset. Ekvivalens skrives '$\equiv$': $A \equiv B$ er sann hvis og bare hvis $(A \to B) \wedge (B \to A)$ er sann. Konstanten $\bot$ falsifiseres av alle valuasjoner. Konstanten $\top$ oppfylles av alle valuasjoner. Gallier skriver "proposition" om utsagnslogisk formel, "propositional letter" om utsagnsvariabel og '$\to$' som '$\supset$'.

Oppgave 3.7 Gjør oppgave 3.3.1 på side 54/55 i Gallier.

Merk at hvis Γ[1] er en mengde utsagnslogiske formler og A er en utsagnslogisk formel, så holder $\Gamma \models A$ hvis alle valuasjoner som oppfyller alle formlene i Γ også oppfyller A.

Oppgave 3.8 Gjør oppgave 3.3.11 på side 57 i Gallier.

Oppgave 3.9 Gjør oppgave 3.3.12 b) på side 57 i Gallier.

Oppgave 3.10 La A og B være utsagnslogiske formler. Se på følgende påstander:

(1) A er sann hvis og bare hvis B er sann.

(2) A er en tautologi hvis og bare hvis B er en tautologi.

Lag et bevis eller finn et moteksempel til hver av påstandene nedenfor.

a. Påstand (1) følger fra påstand (2).

b. Påstand (2) følger fra påstand (1).

Hvis F er en utsagnslogisk formel og P en utsagnsvariabel, så betyr notasjonen $F(P)$ at eventuelle forekomster av P i F har en spesiell betydning. Hvis vi senere skriver $F(A)$ der A er en utsagnslogisk formel, så betegner $F(A)$ formelen F der alle forekomster av P er erstattet med A. Merk at P ikke trenger å forekomme i $F(P)$. Hvis $F(Q) = P \wedge Q$ så blir $F(\neg R) = P \wedge \neg R$. Hvis $F(Q) = P \wedge \neg P$ så er $F(\neg R) = P \wedge \neg P$.

Oppgave 3.11 La $F(P)$, A og B være utsagnslogiske formler.

a. Vis at hvis A er ekvivalent med B, så er $F(A)$ ekvivalent med $F(B)$. *Hint: Vis ved induksjon på $F(P)$ at $v(A) = v(B)$ impliserer $v(F(A)) = v(F(B))$ for alle utsagnslogiske formler A, B og alle boolske valuasjoner v.*

b. Anta nå at $A \to B$ er en tautologi. Ta stilling til om $F(A) \to F(B)$ er en tautologi. Finn et bevis eller et moteksempel. *Hint: $P \to R$ impliserer* ikke $(P \vee Q) \to R$.

[1] Uttales "gamma".

Forelesning 3: SAT og DPLL

Espen Lian - 4. februar 2008

4.1 DPLL prosedyren

Notatene passer ikke sammen med formatet av kompendiet, beklager

Se foilene på kurs websiden!

4.2 Oppgaver

Oppgave 4.1 Gi sekventkalkylebevis for følgende sekventer:

a. $\neg\neg P \vdash P$

b. $P, P \to Q \vdash Q$

c. $P \to Q \vdash \neg P \vee Q$

d. $P \vee (Q \wedge R) \vdash (P \vee Q) \wedge (P \vee R)$

e. $\neg(P \vee Q) \vdash \neg P \wedge \neg Q$

Oppgave 4.2 Vi minner om at en sekventkalkyleregel er *falsifikasjonsbevarende* (oppover) hvis minst ett av premissene er falsifiserbare hver gang konklusjonen er falsifiserbar. Vis at følgende LK-regler er falsifikasjonsbevarende: L$\neg$, R$\vee$, R$\to$, L$\wedge$ og R$\wedge$.

Oppgave 4.3 Vi definerer de *strukturelle* LK*-reglene* som følger:

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\,\mathsf{LW} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\,\mathsf{RW}$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,\mathsf{LC} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\,\mathsf{RC}$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,\mathsf{Cut}$$

Reglene LW og RW kalles *tynningsregler* (fra engelsk "weakening"). Navnet er motivert fra å lese regelen ovenfra og ned. Da ser vi at sekventen tynnes ved å legge til formler på henholdsvis venstre og høyre side av sekventtegnet. Reglene LC og RC kalles *kontraksjonsregler* (fra engelsk "contraction"). Lest ovenfra og ned ser vi at vi slår sammen to forekomster av en formel i premisset til én forekomst i konklusjonen. Regelen Cut kalles *snittregel*. Den fanger inn det å bruke lemmaer, eller hjelpesetninger, i matematiske bevis.

Legg merke til at både kontraksjonsreglene og snittregelen gjør at premissene blir mer komplekse enn konklusjonen. Hvis vi skal bruke disse formlene i automatisk bevissøk, så vil søke ikke terminere (med mindre vi lager strategier for hvordan vi bruker kontraksjon og snitt).

a. Vis at de strukturelle reglene er falsifikasjonsbevarende oppover.

b. Sekventkalkylen LK er *komplett* hvis enhver gyldig sekvent er bevisbar. Gjør deg opp noen tanker om hvorvidt vi trenger å ha med de strukturelle reglene for å få en komplett sekventkalkyle for utsagnslogikk.

Oppgave 4.4 Lag en regel slik at LK blir usunn når denne regelen legges til.

Oppgave 4.5 (Induktiv definisjon av utledninger)

- Vi har definert mengden av LK-utledninger induktivt ved å begynne med rotsekventer og anvende reglene "nedenfra og opp". Dette svarer til en *analytisk* måte å tenke på. (Ordet *analyse* betyr å dele opp/ta fra hverandre.)
- En annen måte å definere mengden av utledninger på, er å starte med løvsekventer og anvende reglene "ovenfra og ned". Dette svarer til en *syntetisk* måte å tenke på. (Ordet *syntetisk* betyr å sette sammen.)

1. Gi en induktiv definisjon av mengden av utledninger som svarer til den syntetiske måten å tenke på.
2. Forklar hvordan vi kan definere mengden av *bevis* induktivt på denne måten.
3. Gjør greie for hvordan sunnhetsbeviset går med denne definisjonen av utledninger.

Forelesning 4: Intuisjonistisk utsagnslogikk

Arild Waaler - 11. februar 2008

5.1 Intuisjonistisk logikk

5.1.1 Innledning

Til nå i kurset

- Det utsagnslogiske språket: konnektiver og formler
- Bevissystem: sekventkalkylen LK for *klassisk* utsagnslogikk
- Semantikk: Definisjon av sannhet og gyldighet
- Bevis for sunnhet av bevissystemet med hensyn på semantikken
- Vi skal nå gjøre det samme for en ny logikk!
- Språket til *intuisjonistisk* logikk er likt som for klassisk logikk, mens bevissystemet og semantikken er forskjellig!

Negasjon som bakgrunn for intuisjonistisk logikk

Aristoteles identifiserte to ulike prinsipper for negasjon:

- Kontradiksjonsprinsippet: En påstand og dens negasjon kan ikke begge være sanne samtidig og i samme henseende: $\neg(P \wedge \neg P)$
- Loven om det utelukkede tredje: En påstand er enten sann eller usann: $P \vee \neg P$
- I klassisk logikk holder begge disse prinsippene. I intuisjonistisk logikk holder bare kontradiksjonsprinsippet
- En hovedidé ved matematisk intuisjonisme: sannhet betyr at vi kan verifisere. Siden det er mange påstander som vi idag hverken er istand til å bevise eller motbevise, holder ikke $P \vee \neg P$.
- Intuisjonistisk logikk er en hovedretning innen matematikkens filosofi, og er idag også et viktig grunnlag for teoretisk databehandling.

5.1.2 Sekventkalkyle for intuisjonistisk logikk

Syntaks

- En *intuisjonistisk sekvent* er på formen $\Gamma \vdash A$ eller $\Gamma \vdash$
- $\Gamma \vdash A$ uttrykker at "A følger logisk fra Γ". I intuisjonistisk logikk kan vi tolke dette på to måter:
  - Vi kan konstruere et bevis for A gitt bevis for hvert utsagn i Γ
  - Hvis vi vet at Γ holder, så vet vi også at A holder

- $\Gamma \vdash$ uttrykker at "Γ er *inkonsistent*" (inneholder en selvmotsigelse)
- Sekventkalkylen LJ er essensielt LK begrenset til intuisjonistiske sekventer
- Reglene er inndelt i 3 grupper: Identitetsregler, strukturelle regler og logiske regler

Definisjon 5.1.1 (Identitetsregler)**.** Identitetsreglene *i* LJ *er:*

$$\Gamma, A \vdash A \qquad \frac{\Gamma \vdash A \qquad \Gamma, A \vdash C}{\Gamma \vdash C}\,\mathsf{Snitt}$$

Snitt-regelen holder også i LK, da med en Δ i succedenten.

- Regelen er kalkylens "resonneringsregel" og kan brukes til å representere matematiske resonnement: hvis vi ser på venstre premiss som et lemma, vil høyre premiss fange inn at vi anvender lemmaet.
- Bevislengden til bevis med snitt kan være dramatisk kortere enn for snittfrie bevis.
- Merk at *snittformelen* A ikke er en delformel av sekventen i konklusjonen til regelen. Dette gjør snitt-regelen vanskelig å implementere i bevissøk.
- Regelen er ikke nødvendig hverken i LJ eller LK. Kompletthetsbeviset for LK bruker ikke snitt-regelen.

Definisjon 5.1.2 (Strukturelle regler)**.** *De* strukturelle reglene *i* LJ *er:*

$$\frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}\,\mathsf{LC} \qquad \frac{\Gamma \vdash C}{\Gamma, A \vdash C}\,\mathsf{LT} \qquad \frac{\Gamma \vdash}{\Gamma \vdash C}\,\mathsf{RT}$$

- *Kopieringsregelen* uttrykker at vi kan bruke en antagelse i et bevis flere ganger. Denne regelen er unødvendig i utsagnslogisk LK, men er nødvendig i de fleste andre logikker.
- Den *venstre tynningsregelen* uttrykker at vi kan fjerne en antagelse i et resonnement som vi ikke bruker. Denne interpretasjonen bygger på at en tom succedent uttrykker "den usanne påstanden".
- Den *høyre tynningsregelen* reflekterer at "fra det usanne følger alt" (*ex falsum quodlibet*).

Definisjon 5.1.3 (Logiske regler)**.** *De* logiske reglene *i* LJ *er:*

$$\frac{\Gamma, A\ ,\ B \vdash C}{\Gamma, A \wedge B \vdash C}\,\mathsf{L}\wedge \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\mathsf{R}\wedge$$

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\,\mathsf{L}\vee \qquad \frac{\Gamma \vdash \quad A_i}{\Gamma \vdash A_1 \vee A_2}\,\mathsf{R}\vee_i$$

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}\,\mathsf{L}\to \qquad \frac{\Gamma, A \vdash \qquad B}{\Gamma \quad \vdash A \to B}\,\mathsf{R}\to$$

$$\frac{\Gamma \qquad \vdash A}{\Gamma, \neg A \vdash C}\,\mathsf{L}\neg \qquad \frac{\Gamma, A \vdash}{\Gamma \quad \vdash \neg A}\,\mathsf{R}\neg$$

Merk:

- C kan være fraværende.
- C forsvinner fra succendenten i venstre premiss til $\mathsf{L}\to$ og $\mathsf{L}\neg$.

Vi kan ikke bevise $\vdash P \vee \neg P$

$$\dfrac{\vdash P}{\vdash P \vee \neg P}\,\mathsf{R}\vee_1$$

$$\dfrac{\dfrac{P \vdash}{\vdash \neg P}\,\mathsf{R}\neg}{\vdash P \vee \neg P}\,\mathsf{R}\vee_2$$

- Vi kunne også prøvd å bruke Snitt. Det ville ikke ført frem, men det er ikke trivielt å vise dette! Vi skal senere i forelesningen se at det ikke kan føre frem.
- Vi kan vise at i LJ er $\Gamma \vdash A \vee B$ bevisbar hvis og bare hvis enten $\Gamma \vdash A$ er bevisbar eller $\Gamma \vdash B$ er bevisbar.

Vi kan bevise $\vdash \neg\neg(P \vee \neg P)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P \vdash P}{P \vdash P \vee \neg P}\,\mathsf{L}\vee_1}{\neg(P \vee \neg P), P \vdash}\,\mathsf{L}\neg}{\neg(P \vee \neg P) \vdash \neg P}\,\mathsf{R}\neg}{\neg(P \vee \neg P) \vdash P \vee \neg P}\,\mathsf{L}\vee_2}{\neg(P \vee \neg P), \neg(P \vee \neg P) \vdash}\,\mathsf{L}\neg}{\neg(P \vee \neg P) \vdash}\,\mathsf{LC}}{\vdash \neg\neg(P \vee \neg P)}\,\mathsf{R}\neg$$

- Generelt kan vi i intuisjonistisk utsagnslogikk alltid vise dobbeltnegasjonen til en formel som kan bevises i klassisk logikk.
- Merk bruken av kontraksjon! Vi trenger kontraksjon fordi kalkylen inneholder tre *destruktive* regler: $\mathsf{L}\neg$, $\mathsf{L}\to$ og $\mathsf{R}\vee_i$. I disse reglene mistes informasjon når vi går fra konklusjon til premiss.

Lemma 5.1.1. *En sekvent som er bevisbar i* LJ *er også bevisbar i* $\mathsf{LK}^{+\mathsf{LC}}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P \vdash P, \neg P, P}{P \vdash P \vee \neg P, P}\,\mathsf{L}\vee_1}{\neg(P \vee \neg P), P \vdash P}\,\mathsf{L}\neg}{\neg(P \vee \neg P) \vdash P, \neg P}\,\mathsf{R}\neg}{\neg(P \vee \neg P) \vdash P \vee \neg P}\,\mathsf{L}\vee_2}{\neg(P \vee \neg P), \neg(P \vee \neg P) \vdash}\,\mathsf{L}\neg}{\neg(P \vee \neg P) \vdash}\,\mathsf{LC}}{\vdash \neg\neg(P \vee \neg P)}\,\mathsf{R}\neg$$

Bevisskisse. Hvis δ er en LJ-utledning av rotsekventen $\Gamma \vdash C$, så konstruer vi en LK-utledning δ' induktivt ved å

1. la $\Gamma \vdash C$ være rotsekventen i δ, og

2. erstatte enhver LJ-slutning med den tilsvarende LK-slutingen.

Hvis δ er et LJ-bevis, så må δ' være et $\mathsf{LK}^{+\mathsf{LC}}$-bevis.

- Vi kan da få flere formler i succedenten i sekventene i δ' enn i de tilsvarende sekventer i δ.
- De logiske reglene kan da brukes i nøyaktig samme rekkefølge i δ' som i δ.
- Siden vi ikke har innført strukturelle regler i LK, kan vi simpelthen ignorere tynningsreglene. Kontraksjon beholder vi pr. antagelse.

□

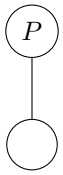
5.1.3 Kripke-semantikk

Idéen bak intuisjonistisk semantikk

Semantikken til intuisjonistisk logikk er nøye knyttet opp til en modell av kunnskap til en ideell resonnerer, dvs. et subjekt som er istand til å trekke alle konsekvenser av sin egen kunnskap.

- Et punkt x er assosiert med en mengde atomære formler, dvs. de formler som subjektet har bevis for/evidens for/vet på x.
- $\neg A$ holder på x dersom A ikke holder på noe punkt y der subjektet vet minst like mye som på x.

Moteksempel til $P \vee \neg P$:



- På det nederste punktet vet ikke subjektet at P, selv om det vet det på et "bedre" punkt lenger opp i treet. Subjektet vet heller ikke $\neg P$, siden det forutsetter at P ikke holder på noe "bedre" punkt.

- Idéen er at vi gir en mengde kunnskapstilstander (kalt *punkter*) som typisk er ordnet i en trestruktur. Hvis x er et punkt og y er et punkt lenger opp i treet enn x (en "etterkommer" til x), så er y et punkt der subjektet vet minst like mye som det vet på x.
- Hva som er *grunnen* til at subjektet vet mer på et punkt enn et annet, tar vi ikke stilling til i modellen. Det er vanlig å tenke at ny kunnskap er knyttet til ny evidens. Vi kan tenke oss punktene utstrakt i tid, men det er ingenting i modellene som krever denne tolkningen.

Partiell ordning

Definisjon 5.1.4 (Partiell ordning)**.** *Et par* $(S, \leq)$ *er en* partiell ordning *hvis* $\leq$ *er en binær relasjon på* S *slik at for alle* $x, y, z \in S$*,*

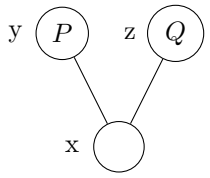
1. $x \leq x$ *(refleksivitet),*
2. *hvis* $x \leq y$ *og* $y \leq z$*, så* $x \leq z$ *(transitivitet),*
3. *hvis* $x \leq y$ *og* $y \leq x$*, så* $x = y$ *(anti-symmetri).*

Kripke-modeller

Definisjon 5.1.5. *En* Kripke-modell *er et trippel* $(S, \leq, \Vdash')$ *der*

1. S *er en ikke-tom mengde av punkter,*
2. $(S, \leq)$ *er en partiell ordning,*
3. $\Vdash'$ *er en relasjon fra* S *til* $\mathcal{V}_u$ *(mengden av alle atomære formler),* $x \Vdash' P$ *betyr at* x *tvinger* P*, og*
4. $\Vdash'$ *tilfredsstiller* monotoni*: hvis* $x \Vdash' P$ *og* $x \leq y$*, så* $y \Vdash' P$*.*
5. $\Vdash'$ *utvides så til* $\Vdash$*, som er definert over hele språket:*
   - $x \Vdash P$ *hviss* $x \Vdash' P$
   - $x \Vdash A \wedge B$ *hviss* $x \Vdash A$ *og* $x \Vdash B$
   - $x \Vdash A \vee B$ *hviss* $x \Vdash A$ *eller* $x \Vdash B$
   - $x \Vdash A \to B$ *hviss vi for enhver* y *slik at* $x \leq y$ *har at:* *hvis* $y \Vdash A$ *så* $y \Vdash B$*.*
   - $x \Vdash \neg A$ *hviss for enhver* y *slik at* $x \leq y$*:* $y \nVdash A$

Motmodell til $\vdash (P \to Q) \vee (Q \to P)$



- Toppnodene y og z er klassiske valuasjoner. Vi har at
  - $y \Vdash P$. Siden $y \nVdash Q$ og ingen andre punkter er over y har vi $y \Vdash \neg Q$.
  - $z \Vdash Q$. Tilsvarende har vi $z \Vdash \neg P$.
- $x \nVdash P \to Q$ siden $x \leq y$ og $y \Vdash P$ og $y \nVdash Q$.
- $x \nVdash Q \to P$ siden $x \leq z$ og $z \Vdash Q$ og $z \nVdash P$.

Sammenheng mellom klassisk og intuisjonistisk semantikk

- Kripke-modeller som kun består av ett punkt kollapser til valuasjoner, dvs. modeller for klassisk logikk.
- Merk at dette gir et *semantisk* bevis for at alt som er gyldig intuisjonistisk, også er klassisk gyldig. For anta at en formel A ikke er klassisk gyldig. Da finnes en valuasjon v som gjør den usann. Men siden alle valuasjoner også er intuisjonistiske modeller, er A heller ikke intuisjonistisk gyldig.

- Merk hvordan de intuisjonistiske modellene generaliserer semantikken for klassisk logikk. Når vi nå skal evaluere en formel, ser vi i det generelle tilfellet ikke bare på én valuasjon: Vi ser på en mengde valuasjoner som er ordnet!

Lemma 5.1.2. *Monotoni gjelder for enhver formel i enhver modell, dvs.* $x \Vdash A$ *og* $x \leq y$*, så* $y \Vdash A$*.*

Bevis. Ved strukturell induksjon over oppbyggingen av formelen A:

Basissteg: A er atomær formel. Påstanden i lemmaet følger fra definisjonen av Kripke-modeller og monotoni-egenskapen.

Induksjonssteg: Vi viser påstanden i lemmaet for tilfellet at A er $B \to C$. De andre tilfellene er lignende.

- Anta $x \Vdash B \to C$ og at $x \leq y$. (Må vise at $y \Vdash B \to C$.)
- Ta en vilkårlig z slik at $y \leq z$. Ved transitivitet av $\leq$ har vi at $x \leq z$.
- Ved modellbetingelsen følger at hvis $z \Vdash B$, så $z \Vdash C$.
- Siden z er et vilkårlig punkt slik at $y \leq z$, gir modellbetingelsen at $y \Vdash B \to C$.

□

Intuisjonistiske generaliseringer av semantiske begreper

- En punkt i en modell tvinger Γ hvis den tvinger hver formel i Γ. Intet punkt tvinger $\emptyset$.
- Et punkt x i en Kripke-modell er en *motmodell* til en sekvent $\Gamma \vdash C$ hvis $x \Vdash \Gamma$ og $x \nVdash C$. Hvis det finnes et slikt punkt x i modellen sier vi at *Kripke-modellen* er en motmodell til sekventen.
- Merk at hvis C ikke finnes, dvs. at succedenten er tom, vil trivielt x ikke tvinge succedenten. Hvis Γ er tom, vil x være motmodell til $\Gamma \vdash C$ dersom den ikke tvinger C.
- Et punkt x i en Kripke-modell er en *modell for* en sekvent hvis den ikke er en motmodell til sekventen.
- En sekvent er *gyldig* i en Kripke-modell hvis alle punkter i Kripke-modellen er en modell for sekventen.
- En sekvent er *gyldig* mhp. klassen av Kripke-modeller hvis den ikke har noen motmodell, dvs. at den er gyldig i enhver modell.

5.1.4 Sunnhet

Sunnhetsteoremet

Sekventkalkylen LJ er *sunn* hvis enhver LJ-bevisbar sekvent er gyldig mhp. klassen av Kripke-modeller.

Teorem 5.1.1. *Sekventkalkylen* LJ *er sunn.*

1. Alle LJ-reglene bevarer falsifiserbarhet nedenfra og opp, evt. gyldighet ovenfra og ned.
2. En LJ-utledning med falsifiserbar rotsekvent har minst én falsifiserbar løvsekvent. Dette viser vi ved induksjon over utledningen.
3. Alle aksiomer er gyldige.

Vi viser bare det første punktet siden argumentet ellers er helt identisk til sunnhetsargumentet for LK.

Snitt-regelen bevarer falsifiserbarhet

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash C}{\Gamma \vdash C}\ \mathsf{Snitt}$$

- Anta at det finnes en Kripke-modell og et punkt x slik at x tvinger Γ og at x ikke tvinger C.
- Enten tvinger x A eller så tvinger ikke x A.
- Hvis x ikke tvinger A, så vil Kripke-modellen være en motmodell til venstre premiss.
- Ellers vil Kripke-modellen være en motmodell til høyre premiss.

$\mathsf{L}\vee$ bevarer falsifiserbarhet

Husk: $x \Vdash A \vee B$ hviss $x \Vdash A$ eller $x \Vdash B$.

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \mathsf{L}\vee$$

- Anta at det finnes en Kripke-modell og et punkt x slik at x tvinger $\Gamma, A \vee B$ og at x ikke tvinger C.
- Ved modellbetingelsen for *eller* vil x enten tvinge A eller tvinge B.
- Hvis x tvinger A, så vil Kripke-modellen være en motmodell til venstre premiss.
- Ellers vil Kripke-modellen være en motmodell til høyre premiss.

$\mathsf{R}\vee_i$ bevarer falsifiserbarhet:

Husk: $x \Vdash A \vee B$ hviss $x \Vdash A$ eller $x \Vdash B$.

$$\frac{\Gamma \vdash \quad A_i}{\Gamma \vdash A_1 \vee A_2}\ \mathsf{R}\vee_i$$

- Anta at det finnes en Kripke-modell og et punkt x slik at x tvinger Γ og at x ikke tvinger $A_1 \vee A_2$.
- Ved modellbetingelsen for $\vee$ vil x hverken tvinge A_1 eller tvinge A_2.
- Derfor vil Kripke-modellen være en motmodell til premisset både i tilfellet $\mathsf{R}\vee_1$ og i tilfellet $\mathsf{R}\vee_2$.

$\mathsf{L}\to$ bevarer falsifiserbarhet:

Husk: $x \Vdash A \to B$ hviss for enhver y slik at $x \leq y$: hvis $y \Vdash A$, så $y \Vdash B$.

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}\ \mathsf{L}\to$$

- Anta at det finnes en Kripke-modell og et punkt x slik at x tvinger $\Gamma, A \to B$ og at x ikke tvinger C.
- Enten tvinger x A eller så tvinger ikke x A.

- Hvis x ikke tvinger A, så vil Kripke-modellen være en motmodell til venstre premiss.
- Ellers vil Kripke-modellen være en motmodell til høyre premiss.

Merk likheten med resonnementet om Snitt! Dette er ikke tilfeldig: Snitt er en generalisert L→.

R→ bevarer falsifiserbarhet:

Husk: $x \Vdash A \to B$ hviss for enhver y slik at $x \leq y$: hvis $y \Vdash A$, så $y \Vdash B$.

$$\frac{\Gamma, A \vdash \quad B}{\Gamma \quad \vdash A \to B}\ \mathsf{R}{\to}$$

- Anta at det finnes en Kripke-modell og et punkt x slik at x tvinger Γ og at x ikke tvinger $A \to B$.
- Ved modellbetingelsen for *implikasjon* vil det finnes et punkt y der $x \leq y$ slik at y tvinger A og y ikke tvinger B.
- Ved Lemmaet vil y tvinge Γ.
- Dermed vil y tvinge Γ, A og ikke tvinge B, dvs. at Kripke-modellen er en motmodell til premisset.

5.2 Konsistens

5.2.1 Definisjoner

To betydninger av konsistens

Definisjon 5.2.1 (Konsistens av sekventkalkyle)**.** *Sekventkalkylen* LJ *er* konsistent *hvis den tomme* LJ*-sekventen* $\vdash$ *ikke er bevisbar.*

- Dette gjenspeiler tolkningen av den tomme sekventen som et uttrykk for en absurditet. Ved hjelp av tynning kan vi utlede hva som helst fra den tomme sekventen.

Definisjon 5.2.2 (Konsistens av formelmengde)**.** *En mengde formler* Γ *er* LJ-konsistent *hvis sekventen* $\Gamma \vdash$ *ikke er bevisbar.*

- Merk at et utsagn om konsistens av en mengde Γ er en påstand om *ikke-bevisbarhet*. Dette er en kompleks påstand om en uendelig stor mengde av utledninger: Av alle LJ-utledninger er ingen av dem bevis for sekventen $\Gamma \vdash$.

5.2.2 Konsistens følger fra sunnhet

Teorem 5.2.1. *Hvis det finnes et punkt i en Kripke-modell som tvinger alle formlene i en mengde* Γ*, så er ikke sekventen* $\Gamma \vdash$ *bevisbar i* LJ*.*

Bevis. Anta at $x \Vdash \Gamma$. Anta for motsigelse at $\Gamma \vdash$ er LJ-bevisbar.

- Ved Sunnhetsteoremet er $\Gamma \vdash$ gyldig.
- Siden $x \Vdash \Gamma$, må $x \Vdash \bot$, der $\bot$ står for en formel som alltid er usann. Dette er umulig.

□

Eksistensen av en enkelt Kripke-modell er nok til å konkludere at intet bevis finnes. Derfor vet vi at vi ikke kan utlede $P \vee \neg P$ i LJ selv om vi bruker snitt.

5.3 Oppgaver

Førsteordens logikk

Oppgave 5.1 (Rekursive definisjoner)

1. Skriv ut hele den rekursive definisjonen av mengden av frie variable i en formel.
2. Definer rekursivt mengden $\mathsf{BV}(\varphi)$ av *bundne* variable i en formel φ.
3. Skriv ut hele den rekursive definisjonen av tolkningen av en lukket term.

Oppgave 5.2 (Førsteordens formler)

Finn førsteordens formler i språket $\langle -; -; \mathsf{Lat}, \mathsf{IfiStud}, \mathsf{Problemer}\rangle$ for følgende setninger.

1. Alle Ifi-studenter er late.
2. Ingen Ifi-studenter er late.
3. Noen Ifi-studenter er late.
4. Alle Ifi-studenter som er late, får problemer på eksamen.
5. Noen Ifi-studenter som er late, får ingen problemer på eksamen.

Finn førsteordens formler i språket $\langle \mathsf{Ola}, \mathsf{Kari}; -; \mathsf{Mor}, \mathsf{Far}\rangle$ for følgende setninger.

1. Ola er far til Kari
2. Kari er mor til noen
3. Ola har ingen mor
4. Alle har en mor og en far
5. Alle har en mormor
6. Ingen er både mor og far

Andre oppgaver

Oppgave 5.3 (Konger, damer og tigre) En konge gir sin fange valget mellom to rom. I hvert rom er det enten en dame eller en tiger, men ikke begge deler. På utsiden av dørene står det følgende:

(1)	(2)
I MINST ETT AV DISSE ROMMENE ER DET EN DAME	I DET ANDRE ROMMET ER DET EN TIGER

Kongen sier så: "Enten så er begge påstandene sanne, eller så er begge usanne!"

Hvilken dør bør fangen velge?

(Oppgaven er hentet fra *The lady or the tiger?*, Raymond Smullyan, 1982)

Oppgave 5.4 (Tre søsken) Tre søsken, A, B og C, er i et hus, og må rette seg etter følgende regler:

i) Hvis A går ut, så må B gå ut.

ii) Hvis C går ut, så, hvis A går ut, så må B være inne.

(1) Formaliser påstandene ved hjelp av utsagnslogikk.

(2) Sjekk om det er mulig at C kan gå ut. Begrunn svaret.

(3) Gitt et språk med bare tre atomære utsagn; hvor mange ikke-ekvivalente utsagn kan du lage fra disse? Begrunn svaret skikkelig eller lag en liste over alle mulige slike utsagn.

(4) Hva er det mulig for A, B og C å gjøre?

Forelesning 6: Førsteordens logikk – syntaks og semantikk

Martin Giese - 25. februar 2008

6.1 Innledning til førsteordens logikk

6.1.1 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 et 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."

6.1.2 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.

6.2 Førsteordens logikk – syntaks

6.2.1 Syntaks – Signaturer

Definisjon 6.2.1 (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 6.2.2 (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 6.2.3 (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.*

6.2.2 Syntaks – Termer

Definisjon 6.2.4 (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 $f(t_1, ..., t_n)$ en term.*

6.2.3 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, ..., $f(a)$, $f(x)$, $f(y)$, ...
- $g(a,a)$, $g(a,x)$, $g(a,y)$, $g(x,x)$, $g(x,y)$, $g(y,y)$, ...
- $f(f(a))$, $f(f(x))$, $f(f(y))$, ...

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

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)

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

6.2.4 Syntaks – Formler

Definisjon 6.2.5 (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 6.2.6 (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.

6.2.5 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:

1:	Alice er et idol:	$\mathsf{Idol}(a)$
2:	Alice liker Bob:	$\mathsf{Liker}(a, b)$
3:	x liker Alice:	$\mathsf{Liker}(x, a)$

Signatur: $\langle a, b; -; \mathsf{Idol}, \mathsf{Liker}\rangle$

Ikke atomære formler:

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:	$\neg\exists x(\mathsf{Liker}(x, a) \wedge \mathsf{Liker}(x, b))$
10:	Noen liker ikke seg selv:	$\exists x\neg\mathsf{Liker}(x, x)$
11:	Bob liker noen som liker Alice:	$\exists x(\mathsf{Liker}(b, x) \wedge \mathsf{Liker}(x, a))$
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:	$\forall x(\mathsf{Idol}(x) \to \forall y\mathsf{Liker}(y, x))$

I språket for aritmetikk $\langle 0; s, +; =\rangle$, 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"

6.2.6 Frie variable i termer

Definisjon 6.2.7 (Frie variable i en term)**.** $\mathsf{FV}(t)$ *betegner mengden av* frie variable *i termen* t*.*

Definisjon 6.2.8 (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.*

6.2.7 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 6.2.9 (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.*

Frie variable i formler

Definisjon 6.2.10 (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 $\mathsf{FV}(\varphi)$ for mengden av frie variable i φ.*

Eksempel $(\forall x Rxy \wedge Pz)$**.**

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

Eksempel $(\forall x Pxy \rightarrow \forall z Pzx)$**.**

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

Oppgave. *Gi den presise, rekursive, definisjonen av frie variable i en formel.*

6.2.8 Substitusjoner

Definisjon 6.2.11 (Substitusjon for termer)**.** *La s og t være termer og x en variabel. Da er $s[t/x]$, det vi får ved å erstatte alle forekomster av x i s med t, definert rekursivt ved:*

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

Eksempel.

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

Definisjon 6.2.12 (Substitusjon for formler)**.** *$\varphi[t/x]$ er definert rekursivt ved:*

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

Eksempel.

- $(Pxy \wedge \forall x Pxy)[a/x] = (Pay \wedge \forall x Pxy)$
- $(Pxy \wedge \forall x Pxy)[a/y] = (Pxa \wedge \forall x Pxa)$
- Vi ser at substitusjon ikke blir gjort for bundne variable.
- Vi har enda et tilfelle hvor vi ønsker å forhindre substitusjon.

Eksempel.

- $\exists x \mathsf{Liker}(x,y)[f(x)/y] = \exists x \mathsf{Liker}(x, f(x))$
- Her blir en variabel bundet *etter* substitusjon.
- Dette kan endre meningen til en formel på en måte som vi ikke ønsker.

Definisjon 6.2.13. *Vi sier at t er fri for x i φ hvis ingen variabel i t blir bundet som følge av å substitutere t for x i φ.*

Eksempel. *Termen $f(x)$ er ikke fri for y i formelen $\exists x \mathsf{Liker}(x,y)$.*

- En måte å unngå dette på er å omdøpe bundne variable først.
- F.eks. se på $\exists z \mathsf{Liker}(z,y)$ i stedet for $\exists x \mathsf{Liker}(x,y)$.
- Fra nå av antar vi at alle substitusjoner er "fri for", dvs. at ingen variable blir bundet som følge av en substitusjon.

6.2.9 Lukkede og åpne formler

Definisjon 6.2.14 (Lukket/åpen formel)**.** *En formel φ er* lukket *hvis* $\mathsf{FV}(\varphi) = \emptyset$*, dvs. φ inneholder ingen frie variable. En formel er* åpen *hvis den ikke inneholder noen kvantorer.*

Eksempel.

- $\forall x Pxa$ *er lukket*
- $\forall x Pxy$ *er* ikke *lukket*
- Pxy *er* ikke *lukket, men åpen*
- Pab *er åpen* og *lukket*

6.3 Førsteordens logikk – semantikk

6.3.1 Introduksjon

- Hvordan skal vi *tolke* førsteordens formler?
- Hva skal $\forall x\varphi$ og $\exists x\varphi$ bety?
- 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.

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 først 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 $n \geq 0$.

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

6.3.2 Modeller

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

Definisjon 6.3.1 (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*.*

1

- *Hvis* R *er et relasjonssymbol med aritet* n*,så er* $R^{\mathcal{M}}$ *en relasjon på* $D^n = \underbrace{D \times \cdots \times D}_{n}$*.*

2

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

Noen kommentarer

1. Et funksjonssymbol f med aritet 0 kan betraktes som en konstant.
   - Da er $f^{\mathcal{M}}$ en funksjon fra D^0 til D.
   - 3 Siden D^0 består av kun ett element $\langle\rangle$ – det tomme tuppelet – så består $f^{\mathcal{M}}$ også av kun ett element $\langle\langle\rangle, e\rangle$, hvor $e \in D$.
   - Vi kan derfor identifisere $f^{\mathcal{M}}$ med e.
2. Et relasjonssymbol R med aritet 0 kan betraktes som en utsagnsvariabel.
   - Da er $R^{\mathcal{M}}$ en delmengde av D^0.
   - 4 Siden D^0 består av kun ett element $\langle\rangle$ – det tomme tuppelet -så fins det nøyaktig to muligheter for $R^{\mathcal{M}}$.
   - Enten så er $R^{\mathcal{M}}$ tom eller så er $\langle\rangle \in R^{\mathcal{M}}$.
   - Vi kan derfor tenke på mengden $\{\emptyset, \{\langle\rangle\}\}$ av delmengder av D^0 som **Bool**.
3. Et tuppel $\langle e\rangle$, hvor $e \in D$, kan vi identifisere med elementet e.
   - 5 Når et relasjonssymbol R har aritet 1,så skriver vi derfor $\{e_1, \ldots, e_n\}$ i stedet for $\{\langle e_1\rangle, \ldots, \langle e_n\rangle\}$.
   - Vi antar derfor også at $R^{\mathcal{M}} \subseteq D$.

6.3.3 Hovedeksempel – et figurspråk

Relasjonssymbol	aritet
Sirkel	1
Firkant	1
Trekant	1
Stor	1
Liten	1
Mindre	2

- Konstantsymboler: a, b, c, d, e, f.
- Funksjonssymboler: ingen.
- Vi leser på denne måten:

  $\mathsf{Sirkel}(x)$: "x er en sirkel"

  $\mathsf{Firkant}(x)$: "x er en firkant"

  $\mathsf{Trekant}(x)$: "x er en trekant"

  $\mathsf{Stor}(x)$: "x er stor"

  $\mathsf{Liten}(x)$: "x er liten"

  $\mathsf{Mindre}(x, y)$: "x er mindre enn y"

La oss nå lage en modell for dette språket!

En tolkning av figurspråket

La $\mathcal{M}$ være en modell med domene $D = \{$  $\}$.

$a^{\mathcal{M}} =$  $\quad \mathsf{Sirkel}^{\mathcal{M}} = \{$  $\}$

$b^{\mathcal{M}} =$  $\quad \mathsf{Firkant}^{\mathcal{M}} = \{$  $\}$

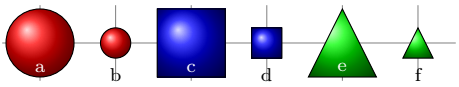
$c^{\mathcal{M}} =$  $\quad \mathsf{Trekant}^{\mathcal{M}} = \{$  $\}$

$d^{\mathcal{M}} =$  $\quad \mathsf{Stor}^{\mathcal{M}} = \{$  $\}$

$e^{\mathcal{M}} =$  $\quad \mathsf{Liten}^{\mathcal{M}} = \{$  $\}$

$f^{\mathcal{M}} =$  $\quad \mathsf{Mindre}^{\mathcal{M}} = \{$ $\}$

Vi foregriper begivenhetene og ser på hvilke atomære formler som er sanne og usanne i modellen $\mathcal{M}$.



Sant	Usant
• Sirkel(a)	• Trekant(a)
• Firkant(c)	• Stor(b)
• Liten(b)	• Mindre(a, b)
• Mindre(b, e)	• Mindre(a, a)

Variabeltilordninger

- En modell tolker konstantsymboler, funksjonssymboler, og relasjonssymboler, men...
- ...ikke variable. Derfor definerer vi...

Definisjon 6.3.2 (Variabeltilordning)**.** *La $\mathcal{M}$ være en modell. En variabeltilordning for $\mathcal{M}$ er en funksjon $\mu : \mathcal{V} \to |\mathcal{M}|$ fra mengen av variable til domenet.*

- En variabeltilordning er alltid gitt relativ til en modell $\mathcal{M}$ siden den tolker variable som elementer i domenet til $\mathcal{M}$.
- For en gitt modell kan vi ha mange variabeltilordninger.
- Hvis $|\mathcal{M}| = \{1, 2, 3\}$, så kan vi ha
  - μ_1 slik at $\mu_1(x_1) = 1$, $\mu_1(x_2) = 1$, $\mu_1(x_3) = 1$, ...
  - μ_2 slik at $\mu_2(x_1) = 2$, $\mu_2(x_2) = 2$, $\mu_2(x_3) = 2$, ...
  - μ_3 slik at $\mu_3(x_1) = 1$, $\mu_3(x_2) = 2$, $\mu_3(x_3) = 3$, ...
  - ...

Modifikasjon av variabeltilordninger

Definisjon 6.3.3. *La μ være en variabeltilordning for en modell $\mathcal{M}$, $x \in \mathcal{V}$ en variabel, og $a \in |\mathcal{M}|$ et element av domenet. Vi definerer modifikasjonen av μ på x til a, skrevet $\mu\{x \mapsto a\}$, gjennom:*

$$\mu\{x \mapsto a\}(y) := \begin{cases} a & \text{hvis } x{=}y \\ \mu(y) & \text{ellers} \end{cases}$$

for alle variabler $y \in \mathcal{V}$.

La μ være slik at $\mu(x_1) = 1$, $\mu(x_2) = 1$, $\mu(x_3) = 1$, ...

Hvis $\mu' = \mu\{x_2 \mapsto 2\}$, så er $\mu'(x_1) = 1$, $\mu'(x_2) = 2$, $\mu'(x_3) = 1$, ...

6.3.4 Tolkning av termer og formler

Tolkning av termer

- Vi bruker tolkningsfunksjonen i modellen til å tolke konstant- og funksjonssymboler
- Tolkningen av variable overlates til variabeltilordningen.

Definisjon 6.3.4 (Tolkning av termer)**.** *La $\mathcal{L}$ være et førsteordens språk og $\mathcal{M}$ en modell for $\mathcal{L}$. La μ være en variabeltilordning for $\mathcal{M}$. Tolkningen av en term t i $\mathcal{M}$ under μ, skrevet $t^{\mathcal{M},\mu}$, defineres induktivt.*

- $x^{\mathcal{M},\mu} = \mu(x)$ *for en variabel* x
- $c^{\mathcal{M},\mu} = c^{\mathcal{M}}$ *for et konstantsymbol* c
- $f(t_1, \ldots, t_n)^{\mathcal{M},\mu} = f^{\mathcal{M}}(t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu})$ *for en funksjonsterm*

Tolkning av formler

Definisjon 6.3.5 (Tolkning av formler)**.** *La $\mathcal{L}$ være et førsteordens språk og $\mathcal{M}$ en modell for $\mathcal{L}$. La μ være en variabeltilordning for $\mathcal{M}$. Vi definerer ved induksjon hva det vil si at en formel φ er* sann *i $\mathcal{M}$ under μ; vi skriver $\mathcal{M}, \mu \models \varphi$ når φ er sann i $\mathcal{M}$ under μ.*

- *Atomære fml:* $\mathcal{M}, \mu \models R(t_1, \ldots, t_n)$ *hvis* $\langle t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M}, \mu \models \neg\varphi$ *hvis det ikke er tilfelle at* $\mathcal{M}, \mu \models \varphi$.
- $\mathcal{M}, \mu \models \varphi \wedge \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *og* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \varphi \vee \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *eller* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \varphi \to \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *impliserer* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \forall x\varphi$ *hvis* $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for alle* a *i* $|\mathcal{M}|$.
- $\mathcal{M}, \mu \models \exists x\varphi$ *hvis* $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for minst en* a *i* $|\mathcal{M}|$.

Koinsidenslemma

- $t^{\mathcal{M},\mu}$ er uavhengig av μ for variabler som ikke forekommer i t.
- $\mathcal{M}, \mu \models \varphi$ er uavhengig av μ for variabler som ikke forekommer *fritt* i φ.

Lemma 6.3.1 (Koinsidenslemma)**.** *La t være en term, $\mathcal{M}$ en modell, og μ og ν to variabeltilordninger med $\mu(x) = \nu(x)$ for alle $x \in \mathsf{FV}(t)$. Da er $t^{\mathcal{M},\mu} = t^{\mathcal{M},\nu}$.*

La φ være en formel, $\mathcal{M}$ en modell, og μ og ν to variabeltilordninger med $\mu(x) = \nu(x)$ for alle $x \in \mathsf{FV}(\varphi)$. Da gjelder $\mathcal{M}, \mu \models \varphi$ hviss $\mathcal{M}, \nu \models \varphi$.

For lukkede termer t og formler φ: skriv $t^{\mathcal{M}}$ og $\mathcal{M} \models \varphi$.

Definisjon 6.3.6 (Oppfyllbarhet)**.** *En lukket formel φ er* oppfyllbar *hvis det fins en modell $\mathcal{M}$ som gjør φ sann. Vi sier også at $\mathcal{M}$ oppfyller φ og at $\mathcal{M}$ er en modell for φ.*

Oppfyllbar

- $\exists x \mathsf{Liten}(x)$
- $\exists x(\mathsf{Liten}(x) \wedge \mathsf{Stor}(x))$
- $\exists x Px \rightarrow \forall x Px$

Ikke oppfyllbar

- $Pa \wedge \neg Pa$
- $\exists x(\mathsf{Liten}(x) \wedge \neg\mathsf{Liten}(x))$
- $\neg\mathsf{Stor}(a) \wedge \forall x \mathsf{Stor}(x)$

Definisjon 6.3.7 (Gyldighet)**.** *En lukket formel φ er* gyldig *hvis den er sann i alle modeller $\mathcal{M}$, ellers så er den* falsifiserbar*.*

Gyldig

- $\forall x Pxa \rightarrow \forall z Pza$
- $(\forall x Px \wedge \forall y Qy) \rightarrow \forall x Px$
- $\exists x \mathsf{Liten}(x) \vee \exists x \neg \mathsf{Liten}(x)$

Ikke gyldig (falsfiserbar)

- $\forall x Px$
- $\exists x \mathsf{Stor}(x) \rightarrow \forall x \mathsf{Stor}(x)$
- $\exists x Px \rightarrow \exists x(Px \wedge Qx)$

6.3.5 Oppsummering

En modell $\mathcal{M}$ for et språk $\mathcal{L}$ består av

1. en ikke-tom mengde $|\mathcal{M}|$, kalt domenet til $\mathcal{M}$, og
2. en tolkning av alle ikke-logiske symboler i språket.

For eksempel, hvis $\mathcal{L}$ er språket $\langle$ 🕴 , 🧍 , ☕ ; 🏭 ; ♀ , ♂ $\rangle$, så må en modell $\mathcal{M}$ gi et domene og en tolkning til alle symbolene.

- 🕴$^{\mathcal{M}}$, 🧍$^{\mathcal{M}}$ og ☕$^{\mathcal{M}}$ må være elementer i domenet.
- 🏭$^{\mathcal{M}}$ må være en funksjon på domenet
- ♀$^{\mathcal{M}}$ og ♂$^{\mathcal{M}}$ må være relasjoner på domenet.
- Husk på ariteten til symbolene. (🏭 har aritet 2; ♀ og ♂ har aritet 1.)

Hvis $\mathcal{M}$ er en modell og φ er en lukket formel, så definerte vi $\mathcal{M} \models \varphi$.

- For atomære formler: $\mathcal{M}, \mu \models R(t_1, \ldots, t_n)$ hvis $\langle t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M}, \mu \models \neg\varphi$ hvis det *ikke* er tilfelle at $\mathcal{M}, \mu \models \varphi$.
- $\mathcal{M}, \mu \models \varphi \wedge \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *og* $\mathcal{M}, \mu \models \psi$.

- $\mathcal{M}, \mu \models \varphi \vee \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *eller* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \varphi \rightarrow \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *impliserer* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \forall x \varphi$ hvis $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for alle* $a \in |\mathcal{M}|$.
- $\mathcal{M}, \mu \models \exists x \varphi$ hvis $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for minst en* $a \in |\mathcal{M}|$.

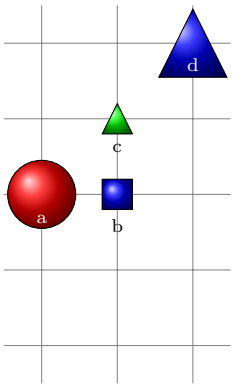
6.3.6 Språk og modeller – et komplekst forhold

- Ved førsteordens språk har vi fått betydelig større uttrykkskraft.
- Modeller kan være rike på struktur.
- Det er et ikke-trivielt forhold mellom språk og modeller.
- Noe av det vi er interessert i:
  - Sjekke om en formel er sann i en modell. (Modellsjekking)
  - Sjekke om en formel er oppfyllbar eller falsifiserbar.
  - Sjekke om en formel er gyldig.
  - Sjekke om formler er uavhengige av hverandre.
  - Bruke språket til å beskrive modeller, forsøke å "fange inn" og beskrive virkeligheten.

6.3.7 En utvidelse av figurspråket

Atomær formel	Intendert tolkning
$\mathsf{Sirkel}(x)$	x er en sirkel
$\mathsf{Firkant}(x)$	x er en firkant
$\mathsf{Trekant}(x)$	x er en trekant
$\mathsf{Stor}(x)$	x er stor
$\mathsf{Liten}(x)$	x er liten
$\mathsf{Mindre}(x, y)$	x er mindre enn y
$\mathsf{Over}(x, y)$	x er nærmere toppen enn y
$\mathsf{Under}(x, y)$	x er nærmere bunnen enn y
$\mathsf{VenstreFor}(x, y)$	x er lenger til venstre enn y
$\mathsf{HoyreFor}(x, y)$	x er lenger til høyre enn y
$\mathsf{Inntil}(x, y)$	x er rett ved siden av, rett over eller rett under y
$\mathsf{Mellom}(x, y, z)$	x, y og z er i samme kolonne, rad eller diagonal, og x er mellom y og z

-3.6cm-



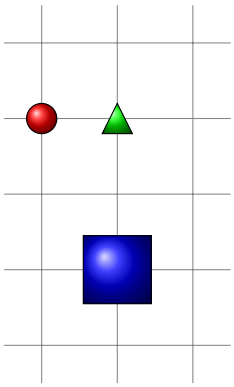
3.6cm

Forklarende eksempler til semantikken:

- $a^{\mathcal{M}} =$  , $b^{\mathcal{M}} =$  , $c^{\mathcal{M}} =$, $d^{\mathcal{M}} =$  (vi antar at dette er alle konstantene)
- $\mathsf{Trekant}^{\mathcal{M}} = \{$,  $\}$
- $\mathsf{Stor}^{\mathcal{M}} = \{$  ,  $\}$
- $\mathsf{Liten}^{\mathcal{M}} = \{$  ,  $\}$
- $\mathcal{M} \models \mathsf{Under}(a, c)$ fordi $\langle a^{\mathcal{M}}, c^{\mathcal{M}} \rangle = \langle$  ,  $\rangle \in \mathsf{Under}^{\mathcal{M}}$
- $\mathcal{M} \models \neg\mathsf{Under}(a, b)$
- $\mathcal{M} \models \mathsf{VenstreFor}(a, c) \wedge \neg\mathsf{VenstreFor}(b, c)$
- $\mathcal{M} \models \mathsf{Inntil}(a, b) \wedge \neg\mathsf{Inntil}(a, c)$
- $\mathcal{M} \models \mathsf{Mellom}(c, a, d) \wedge \neg\mathsf{Mellom}(c, b, d)$

6.3.8 Oppfyllbarhet av førsteordens formler

-3.6cm-



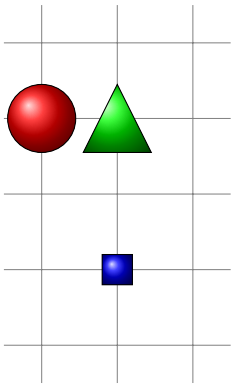
3.6cm

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

$$
\begin{array}{c}
\mathcal{M}, \mu \models \exists x \mathsf{Liten}(x) \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at} \\
\mathcal{M}, \mu\{x \mapsto a\} \models \mathsf{Liten}(x) \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } x^{\mathcal{M}, \mu\{x \mapsto a\}} \in \mathsf{Liten}^{\mathcal{M}} \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \mu\{x \mapsto a\}(x) \in \mathsf{Liten}^{\mathcal{M}} \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } a \in \mathsf{Liten}^{\mathcal{M}}
\end{array}
$$

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

-3.6cm-



3.6cm

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

$$
\begin{array}{c}
\mathcal{M}, \mu \models \forall x \mathsf{Stor}(x) \\
\Updownarrow \\
\text{for alle } a \in |\mathcal{M}| \text{ så } \mathcal{M}, \mu\{x \mapsto a\} \models \mathsf{Stor}(x) \\
\Updownarrow \\
\text{for alle } a \in |\mathcal{M}| \text{ så } x^{\mathcal{M}, \mu\{x \mapsto a\}} \in \mathsf{Stor}^{\mathcal{M}} \\
\Updownarrow \\
\text{for alle } a \in |\mathcal{M}| \text{ så } \mu\{x \mapsto a\}(x) \in \mathsf{Stor}^{\mathcal{M}} \\
\Updownarrow \\
\text{for alle } a \in |\mathcal{M}| \text{ så } a \in \mathsf{Stor}^{\mathcal{M}}
\end{array}
$$

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

6.4 Oppgaver

Normalformer

Negasjons normalform

I dette oppgavesettet skal vi se nærmere på *normalformer*. Formelen $\neg(P \wedge Q)$ kan også skrives som $\neg P \vee \neg Q$. Formlene er *ekvivalente*, dvs. at $\neg(P \wedge Q)$ sann hvis og bare hvis $\neg P \vee \neg Q$ er sann. I formelen $\neg P \vee \neg Q$ forekommer negasjonstegnet ($\neg$) kun foran atomære formler. Vi sier at formler med denne egenskapen er på *negasjons normalform*. Merk at definisjonene nedenfor gjelder både for utsagnslogiske og førsteordens formler.

Definisjon 6.4.1 (Negasjons normalform – NNF)**.** *En formel er på* negasjons normalform *(NNF) hvis negasjonstegnet kun forekommer foran atomære delformler.*

Teorem 6.4.1. *Enhver formel kan skrives om til en ekvivalent formel på negasjons normalform.*

Vi skal ikke se på beviset for teoremet, men nøye oss med å liste opp følgende ekvivalenser, som lett kan verifiseres med f.eks. sannhetsverditabeller når formlene er utsagnslogiske.

(1) $\neg\neg\varphi \Leftrightarrow \varphi$

(2) $\varphi \rightarrow \psi \Leftrightarrow \neg\varphi \vee \psi$

(3) $\neg(\varphi \wedge \psi) \Leftrightarrow \neg\varphi \vee \neg\psi$

(4) $\neg(\varphi \vee \psi) \Leftrightarrow \neg\varphi \wedge \neg\psi$

I tillegg har vi følgende ekvivalenser for kvantorer.

(5) $\neg\forall x\varphi \Leftrightarrow \exists x\neg\varphi$

(6) $\neg\exists x\varphi \Leftrightarrow \forall x\neg\varphi$

Lest fra venstre mot høyre kan ekvivalensene 1–6 sees på som omskrivingsregler. La oss se på et eksempel der vi illustrerer hva vi mener. Formelen $\neg\forall x(Px \to \exists yQy)$ kan omskrives på følgende måte:

$$\begin{aligned}
\neg\forall x(Px \to \exists yQy) &\rightsquigarrow \exists x\neg(Px \to \exists yQy)\\
&\rightsquigarrow \exists x\neg(\neg Px \vee \exists yQy)\\
&\rightsquigarrow \exists x(\neg\neg Px \wedge \neg\exists yQy)\\
&\rightsquigarrow \exists x(Px \wedge \neg\exists yQy)\\
&\rightsquigarrow \exists x(Px \wedge \forall y\neg Qy)
\end{aligned}$$

Her brukes ekvivalensene 5, 2, 4, 1 og deretter 6 som omskrivingsregler for å komme fram til resultatformelen på negasjons normalform.

Oppgave 6.1 (Negasjons normalform) Skriv om følgende formler til negasjons normalform.

a. $\neg(P \to Q)$

b. $\neg\forall xPx$

c. $\neg\exists x(Px \to Qx)$

d. $\neg\exists x(Px \to (Qx \wedge \neg Rx))$

Gjør bevis for at

e. ekvivalens 5 holder.

f. ekvivalens 6 holder.

Preneks normalform

I formelen $\forall xPx \vee \forall xQx$ er variabelen x bundet av to forskjellige kvantorer. Hvis vi døper om x til y i høyre delformel får vi formelen $\forall xPx \vee \forall yQy$, der hver kvantor binder en unik variabel. Generelt kan vi alltid omforme en formel til en ekvivalent formel der alle kvantorene binder unike variable. La oss i det følgende anta at alle formler har denne egenskapen.

Definisjon 6.4.2 (Preneks normalform – PNF)**.** *En formel φ er på preneks normalform (PNF) hvis φ er på formen*

$$\mathcal{Q}_1x_1 \dots \mathcal{Q}_nx_n\psi$$

der hver $\mathcal{Q}_i$ er en kvantor ($\forall$ eller $\exists$), hver x_i er en variabel og ψ er en åpen (kvantorfri) formel.

Merk at listen med kvantorer kan være tom, dvs. at enhver kvantorfri formel er på preneks normalform. Enhver formel kan transformeres til en ekvivalent formel på preneks normalform på følgende måte.

1. Døp om bundne variable som beskrevet ovenfor slik at hver kvantor binder en unik variabel.

2. Transformer formelen til negasjons normalform.
3. Bruk ekvivalensene 7–10 nedenfor til å flytte kvantorene "ytterst".

(7) $\forall x\varphi \wedge \psi \Leftrightarrow \forall x(\varphi \wedge \psi)$

(8) $\exists x\varphi \wedge \psi \Leftrightarrow \exists x(\varphi \wedge \psi)$

(9) $\forall x\varphi \vee \psi \Leftrightarrow \forall x(\varphi \vee \psi)$

(10) $\exists x\varphi \vee \psi \Leftrightarrow \exists x(\varphi \vee \psi)$

Oppgave 6.2 (Preneks normalform) Skriv om følgende formler til preneks normalform.

a. $\neg\forall xPx$

b. $\forall xPx \vee \forall xQx$

c. $\neg\forall x(Px \rightarrow \exists xQx)$

d. $(\forall xPx \vee \forall xQx) \rightarrow \forall x(Px \vee Qx)$

Bevis at

e. ekvivalens 7 holder.

f. ekvivalens 8 holder.

Hvis vi ikke sørger for at hver kvantor binder en unik variabel, så holder ikke ekvivalensene 7–10 over.

g. Er $\forall xPx \vee \forall xQx$ ekvivalent med $\forall x(Px \vee Qx)$? Lag et bevis eller finn et moteksempel.

Disjunktiv og konjunktiv normalform - for utsagnslogikk

Vi har til nå i kurset sett på disjunksjoner ($\varphi \vee \psi$) og konjunksjoner ($\varphi \wedge \psi$) med *to* argumenter. Konnektivene $\vee$ og $\wedge$ kan imidlertid generaliseres til å ta mer enn to argumenter.

Definisjon 6.4.3.

- *En* generalisert disjunksjon *er en formel på formen* $(\varphi_1 \vee \ldots \vee \varphi_n)$ *der hver* φ_i $(1 \leq i \leq n)$ *er en formel.*
- *En* generalisert konjunksjon *er en formel på formen* $(\varphi_1 \wedge \ldots \wedge \varphi_n)$ *der hver* φ_i $(1 \leq i \leq n)$ *er en formel.*

Ved å bruke de generaliserte konnektivene kan vi f.eks. skrive $P \vee Q \vee R$ der vi tidligere måtte skrive $P \vee (Q \vee R)$ (eller $(P \vee Q) \vee R$). Legg merke til at P både er en generalisert disjunksjon og konjunksjon. Fra nå av bruker vi kun de generaliserte konnektivene. For å definere disjunktiv og konjunktiv normalform trenger vi i tillegg begrepet *literal*.

Definisjon 6.4.4.

- *En* literal *er en atomær formel eller negasjonen av en atomær formel.*
- *En formel er på* disjunktiv normalform *(DNF) hvis den er en disjunksjon av en eller flere konjunksjoner av en eller flere literaler.*
- *En formel er på* konjunktiv normalform *(KNF) hvis den er en konjunksjon av en eller flere disjunksjoner av en eller flere literaler.*

Det følger fra definisjonene at envher formel på DNF eller KNF også er på NNF. Noen eksempler:

- $\neg P$ er både på DNF og KNF.
- $(P \wedge \neg Q) \vee (\neg R \wedge S)$ er på DNF.
- $(P \vee \neg Q) \wedge (\neg R \vee S)$ er på KNF.
- $P \vee Q$ er både på DNF og KNF.
- $P \wedge Q$ er både på DNF og KNF.
- $\neg(P \vee Q)$ er hverken på KNF, DNF eller NNF.
- $P \vee (Q \wedge (R \vee S))$ er hverken på KNF eller DNF, men er på NNF.

De *distributive lover* er følgende ekvivalenser (for alle utsagnslogiske formler A, B eller C):

(11) $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

(12) $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$

(13) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

(14) $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$

Lest fra venstre mot høyre kan disse også leses som omskrivingsregler. Eksempel på overføring til DNF:

$$\begin{aligned}(A \vee B) \wedge (C \vee D) &\rightsquigarrow ((A \vee B) \wedge C) \vee ((A \vee B) \wedge D) \\ &\rightsquigarrow (A \wedge C) \vee (B \wedge C) \vee ((A \vee B) \wedge D) \\ &\rightsquigarrow (A \wedge C) \vee (B \wedge C) \vee (A \wedge D) \vee (B \wedge D)\end{aligned}$$

Oppgave 6.3 Overfør hver av følgende formler til ekvivalente formler på DNF og KNF.

1. $P \to Q$
2. $(P \to Q) \to (Q \to R)$
3. $(P \vee Q) \wedge (R \wedge S)$
4. $(\neg P \wedge Q) \to R$

Forklar hva som er sammenhengen mellom DNF, KNF og sannhetsverditabeller.

Andre oppgaver

Oppgave 6.4 La $\mathcal{M}$ være en modell. Omformuler definisjonen av semantikken for førsteordens logikk ved å definere (rekursivt) en funksjon $v_{\mathcal{M}} : \mathcal{F} \to \mathbf{Bool}$ slik at $v_{\mathcal{M}}(\varphi) = \mathbf{1}$ hvis og bare hvis $\mathcal{M} \models \varphi$. Hint 1: $v_{\mathcal{M}}$ er helt lik en boolsk valuasjon, bortsett fra på formler som har en kvantor ytterst. Hint 2: En boolsk valuasjon v *kunne ha vært definert* slik: $v(A \wedge B) = \mathsf{min}\{v(A), v(B)\}$ og $v(A \vee B) = \mathsf{max}\{v(A), v(B)\}$. Hint 3: Kvantorene kan ses på som en form for uendelige konnektiver.

Oppgave 6.5 (Konger, damer og tigre III) Kongen var misfornøyd, for alle fangene klarte oppgavene. Derfor bestemte han seg for å gjøre oppgavene litt vanskeligere. Kongen forklarer: "I det venstre rommet (rom 1), så er det slik at hvis det er en dame der, så er det som står på utsiden sant, men hvis det er en tiger der, så er det som står på utsiden usant. I det andre rommet (rom 2), så er det omvendt: Hvis det er en dame der, så er det som står på utsiden usant, og hvis det er en tiger der, så er det som står på utsiden sant. Det er mulig at begge rommene inneholder en tigre eller at begge rommene inneholder damer, eller at det er en tiger og en dame."

(1)	(2)
Begge rommene inneholder damer	Begge rommene inneholder damer

Hvilket rom velger du?

(Oppgaven er hentet fra *The lady or the tiger?*, Raymond Smullyan, 1982)

Forelesning 7: Førsteordens logikk – sekventkalkyle og sunnhet

Christian Mahesh Hansen - 3. mars 2007

7.1 Repetisjon: 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*

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

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.
6 - 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 $\mathcal{L}$:
7 - 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.
8 - Hvis φ og ψ er formler,så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \rightarrow \psi)$ formler.
9 - 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.

Hvis $\mathcal{M}$ er en modell, μ en variabeltilordning for $\mathcal{M}$, og φ er en formel, så definerte vi $\mathcal{M}, \mu \models \varphi$.

- For atomære formler: $\mathcal{M}, \mu \models R(t_1, \ldots, t_n)$ hvis $\langle t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu} \rangle \in R^{\mathcal{M},\mu}$.
- $\mathcal{M}, \mu \models \neg\varphi$ hvis det *ikke* er tilfelle at $\mathcal{M}, \mu \models \varphi$.
- $\mathcal{M}, \mu \models \varphi \wedge \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *og* $\mathcal{M}, \mu \models \psi$.

- $\mathcal{M}, \mu \models \varphi \vee \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *eller* $\mathcal{M}, \mu \models \psi$.

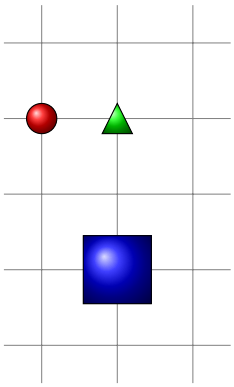
- $\mathcal{M}, \mu \models \varphi \rightarrow \psi$ hvis $\mathcal{M}, \mu \models \varphi$ *impliserer* $\mathcal{M}, \mu \models \psi$.

- $\mathcal{M}, \mu \models \forall x \varphi$ hvis $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for alle* a i $|\mathcal{M}|$.

- $\mathcal{M}, \mu \models \exists x \varphi$ hvis $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for minst en* a i $|\mathcal{M}|$.

7.1.1 Oppfyllbarhet

-3.6cm-



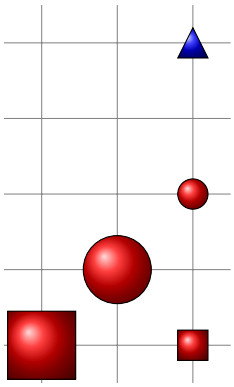
3.6cm

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

$$
\begin{array}{c}
\mathcal{M}, \mu \models \exists x \mathsf{Liten}(x) \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at} \\
\mathcal{M}, \mu\{x \mapsto a\} \models \mathsf{Liten}(x) \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } x^{\mathcal{M}, \mu\{x \mapsto a\}} \in \mathsf{Liten}^{\mathcal{M}} \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \mu\{x \mapsto a\}(x) \in \mathsf{Liten}^{\mathcal{M}} \\
\Updownarrow \\
\text{det fins en } a \in |\mathcal{M}| \text{ slik at } a \in \mathsf{Liten}^{\mathcal{M}}
\end{array}
$$

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

-3.6cm-

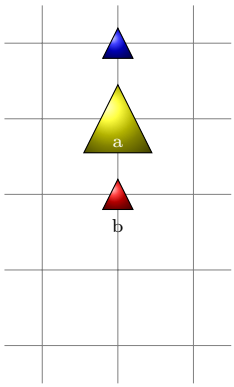


3.6cm

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

Påstanden holder, fordi
$\langle$  $\rangle \in \mathsf{Mellom}^{\mathcal{M}}$ og
$\langle$  $\rangle \in \mathsf{Mellom}^{\mathcal{M}}$.

-3.6cm-



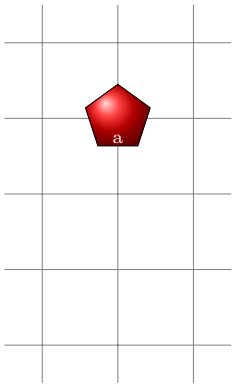
3.6cm

Er følgende formler oppfyllbare samtidig?

1. $\mathsf{Stor}(a) \wedge \mathsf{Liten}(b)$
2. $\forall x(\mathsf{Trekant}(x))$
3. $\forall x(\mathsf{Inntil}(x, a) \vee \mathsf{Inntil}(x, b))$
4. $\neg\exists x(\mathsf{VenstreFor}(x, a) \vee \mathsf{HoyreFor}(x, a))$
5. $\forall x(\mathsf{Stor}(x) \rightarrow \exists y\mathsf{Over}(y, x))$

Svaret er JA!

-3.6cm-



3.6cm

Er følgende formler oppfyllbare?

1. $\neg\mathsf{Sirkel}(a) \wedge \neg\mathsf{Trekant}(a) \wedge \neg\mathsf{Firkant}(a))$

   Svaret er JA!

   La $|\mathcal{M}| = \{$  $\}$ og $a^{\mathcal{M}} =$  .

2. $\mathsf{Liten}(a) \wedge \mathsf{Stor}(a)$

   Svaret er JA!

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

7.2 Førsteordens sekventkalkyle

7.2.1 Introduksjon

- Vi har til nå sett sekventkalkyle for utsagnslogikk.
- Vi har bevist sunnhet og kompletthet av denne kalkylen.
- Nå skal vi gjøre det samme for førsteordens logikk!
- Gitt en førsteordens formel φ, er φ gyldig?
- Husk: vi introduserte LK som et systematisk forsøk på å falsifisere.
- La oss se på et eksempel.

$$\dfrac{\dfrac{\dfrac{\dfrac{\times}{\neg Qa, Pa \vdash Pa}}{\neg Qa \vdash \neg Pa, Pa}}{\vdash Pa, \neg Qa \to \neg Pa} \qquad \dfrac{\dfrac{\dfrac{\times}{Qa \vdash Qa, \neg Pa}}{Qa, \neg Qa \vdash \neg Pa}}{Qa \vdash \neg Qa \to \neg Pa}}{\dfrac{\dfrac{Pa \to Qa \vdash \neg Qa \to \neg Pa}{\forall x(Px \to Qx) \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx) \vdash \forall x(\neg Qx \to \neg Px)}}$$

Eksempel

- Falsifisere formelen $\forall x(\neg Qx \to \neg Px)$:
  - Introdusere et *vitne* som gjør formelen usann.
  - Sette inn et *nytt* konstantsymbol a for x.
- Oppfylle formelen $\forall x(Px \to Qx)$:
  - Da må delformelen være sann uansett hva vi setter inn for x.
  - Spesielt må delformelen være sann når vi setter inn a for x.

- Vi kan nå anvende α- og β-reglene og lukke.

La oss forsøke med en annen regel-rekkefølge:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\times}{\forall x(Px \to Qx), \neg Qa, Pa, Po \to Qo \vdash Pa}}{\forall x(Px \to Qx), \neg Qa, Po \to Qo \vdash \neg Pa, Pa}}{\forall x(Px \to Qx), Po \to Qo \vdash Pa, \neg Qa \to \neg Pa} \qquad \dfrac{\dfrac{\dfrac{\times}{\forall x(Px \to Qx), Qa, Po \to Qo \vdash Qa, \neg Pa}}{\forall x(Px \to Qx), Qa, \neg Qa, Po \to Qo \vdash \neg Pa}}{\forall x(Px \to Qx), Qa, Po \to Qo \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx), Pa \to Qa, Po \to Qo \vdash \quad \neg Qa \to \neg Pa}}{\dfrac{\forall x(Px \to Qx), Po \to Qo \vdash \quad \neg Qa \to \neg Pa}{\dfrac{\forall x(Px \to Qx), Po \to Qo \vdash \forall x(\neg Qx \to \neg Px)}{\forall x(Px \to Qx) \vdash \forall x(\neg Qx \to \neg Px)}}}$$

Eksempel

- Oppfylle $\forall x(Px \to Qx)$:
  - Hva skal vi sette inn for x? Vi bruker en *dummykonstant* o.
- Falsifisere $\forall x(\neg Qx \to \neg Px)$:
  - Vitnet må være *ubrukt*. Kan derfor ikke sette inn o. Setter inn a.
- Oppfylle $\forall x(Px \to Qx)$. Da må vi kunne sette inn a for x!
  - Vi må ta kopi av $\forall$-formelen når vi setter inn for x.
  - Setter inn a for x.
- Vi kan nå anvende α- og β-reglene og lukke.

Motivasjon

- Vi skal nå definere sekventkalkylen LK for førsteordens logikk.
- Vi trenger slutningsregler for formler med kvantorene $\forall/\exists$.
- Fra de foregående eksemplene har vi:
  - Hvis vi skal oppfylle en formel $\forall x\varphi$ så må vi oppfylle $\varphi[t/x]$ for alle valg av term t.
  - I tillegg trenger vi en ekstra kopi av $\forall x\varphi$.
  - Hvis vi skal falsifisere $\forall x\varphi$ må vi velge et *vitne* – et ubrukt konstantsymbol a – slik at $\varphi[a/x]$ er usann.
  - Å oppfylle/falsifisere $\exists$-formler blir dualt.
- Vi skal nå definere begreper som *sekvent*, *aksiom*, *utledning* og *bevis* for førsteordens språk.

7.2.2 Sekventer og aksiomer

Definisjon 7.2.1 (Parameter)**.** *La $\mathcal{L}$ være et førsteordens språk og la* par *være en tellbart uendelig mengde av konstantsymboler, kalt* parametre*, forskjellige fra symbolene i $\mathcal{L}$. La $\mathcal{L}^{\mathsf{par}}$ være førsteordens språket man får ved å ta med disse som konstantsymboler.*

Definisjon 7.2.2 (Sekvent)**.** *En* sekvent *er et objekt på formen $\Gamma \vdash \Delta$ slik at Γ og Δ er multimengder av lukkede førsteordens formler i $\mathcal{L}^{\mathsf{par}}$.*

Definisjon 7.2.3 (Aksiom)**.** *Et* aksiom *er en sekvent på formen $\Gamma, A \vdash A, \Delta$ slik at A er en atomær formel.*

Oppgave. *Hvilke av uttrykkene nedenfor er sekventer?*

- $Px \vdash Qx$
- $\forall x Px \vdash \exists x Qx$
- $Pa, \forall x(Qx \to Rx) \vdash Qb \to Rb$
- $\forall x Px, Pa \vdash Pa, \exists x Pa$

Hvilke av sekventene over er aksiomer?

7.2.3 Sekventkalkyleregler

Definisjon 7.2.4 (γ-regler)**.** *γ-reglene i sekventkalkylen* LK *er:*

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall \qquad \frac{\Gamma \vdash \Delta, \exists x\varphi, \varphi[t/x]}{\Gamma \vdash \Delta, \exists x\varphi}\,\mathsf{R}\exists$$

t er en lukket term

Merk: kopieringen av hovedformelen i γ-reglene medfører at bevissøk i førsteordens logikk ikke nødvendigvis behøver å terminere!

Definisjon 7.2.5 (δ-regler)**.** *δ-reglene i sekventkalkylen* LK *er:*

$$\frac{\Gamma, \varphi[a/x] \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}\,\mathsf{L}\exists \qquad \frac{\Gamma \vdash \Delta, \varphi[a/x]}{\Gamma \vdash \Delta, \forall x\varphi}\,\mathsf{R}\forall$$

a er en parameter som ikke forekommer i konklusjonen.

- γ-reglene erstatter den bundne variabelen med en lukket term.
- δ-reglene erstatter den bundne variabelen med et konstantsymbol.
- Det betyr at hvis hovedformelen er lukket, så er også de aktive formlene lukkede.
- γ- og δ-reglene er derfor *veldefinerte* i den forstand at alle sekventer forblir lukket.

Definisjon 7.2.6 (Slutningsreglene i førsteordens LK)**.** Slutningsreglene *i førsteordens* LK *er α- og β-reglene fra utsagnslogisk* LK *og γ- og δ-reglene.*

7.2.4 Slutninger

- Som i utsagnslogikk definerer reglene *slutninger* ved at vi erstatter symbolene i reglene med lukkede førsteordens formler:

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall \quad \Bigg| \quad \frac{Pa, \forall x(Px \to Qx), Pa \to Qa \vdash Qa}{Pa, \forall x(Px \to Qx) \vdash Qa}\,\mathsf{L}\forall$$

- Begrepene innført i tilknytning til regler/slutninger i utsagnslogisk LK gjelder også i førsteordens LK:
- Sekventene *over* streken kalles *premisser*.
- Sekventen *under* streken kalles *konklusjon*.
- Teksten til høyre for streken er regelens *navn*.
- Formelen som forekommer eksplisitt i konklusjonen kalles *hovedformel*.
- Formlene som forekommer eksplisitt i premissene kalles *aktive formler*.
- Formlene som forekommer i Γ og Δ kalles *ekstraformler*.

7.2.5 Utledninger

- *Ett-premissregler*: α-, γ- og δ-reglene.
- *To-premissregler*: β-reglene.

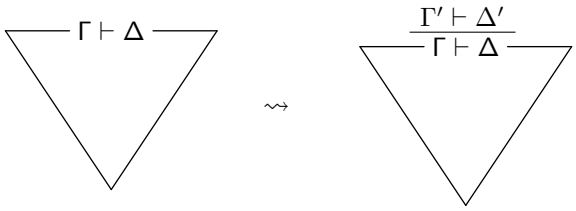
Definisjon 7.2.7 (LK-utledninger – basistilfelle)**.** *En sekvent $\Gamma \vdash \Delta$, hvor Γ og Δ er multimengder av lukkede førsteordens formler i $\mathcal{L}$, er en* LK-utledning.

$$\Gamma \vdash \Delta$$

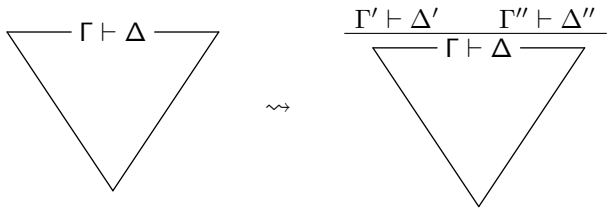
Her er $\Gamma \vdash \Delta$ både rotsekvent og løvsekvent.

- Merk: språket $\mathcal{L}^{\mathsf{par}}$ brukes ikke i rotsekventen, men kun for å introdusere nye parametre i δ-reglene.

Definisjon 7.2.8 (LK-utledninger – ett-premissutvidelse)**.** *Hvis det finnes en* LK*-utledning med en løvsekvent $\Gamma \vdash \Delta$ og en ett-premisslutning med konklusjon $\Gamma \vdash \Delta$ og premiss $\Gamma' \vdash \Delta'$, så er objektet vi får ved å plassere $\Gamma' \vdash \Delta'$ over $\Gamma \vdash \Delta$ en* LK-utledning.



Definisjon 7.2.9 (LK-utledninger – to-premissutvidelse)**.** *Hvis det finnes en* LK*-utledning med en løvsekvent $\Gamma \vdash \Delta$ og en to-premisslutning med konklusjon $\Gamma \vdash \Delta$ og premisser $\Gamma' \vdash \Delta'$ og $\Gamma'' \vdash \Delta''$, så er objektet vi får ved å plassere $\Gamma' \vdash \Delta'$ og $\Gamma'' \vdash \Delta''$ over $\Gamma \vdash \Delta$ en* LK-utledning.



7.2.6 Bevis

Definisjon 7.2.10 (LK-bevis)**.** *Et* LK-bevis *er en* LK*-utledning der alle løvsekventene er aksiomer.*

Definisjon 7.2.11 (LK-bevisbar)**.** *En sekvent* $\Gamma \vdash \Delta$ *er* LK-bevisbar *hvis det finnes et* LK*-bevis med* $\Gamma \vdash \Delta$ *som rotsekvent.*

7.2.7 Eksempler

Eksempel 1

$$\dfrac{\dfrac{\dfrac{}{\forall xPx, Pa \vdash Pa}\times}{\forall xPx \vdash Pa}}{\forall xPx \vdash \forall xPx}$$

- Dette viser at sekventen $\forall xPx \vdash \forall xPx$ er bevisbar.
- Sekventen er også gyldig, noe som er lett å se:
  - Envher modell som oppfyller antecedenten, må oppfylle succedenten.
- At sekventen er gyldig følger også fra sunnhetsteoremet.

Eksempel 2

$$\dfrac{\dfrac{\dfrac{}{\forall xPx, Po \vdash \exists xPx, Po}\times}{\forall xPx \vdash \exists xPx, Po}}{\forall xPx \vdash \exists xPx}$$

- Dette viser at sekventen $\forall xPx \vdash \exists xPx$ er bevisbar.
- Sekventen er også gyldig:
  - Anta at modellen $\mathcal{M}$ gjør $\forall xPx$ sann.
  - Domenet må bestå av minst ett element e.
  - Siden $\mathcal{M} \models \forall xPx$ sann, gjelder også $\mathcal{M}, \{x \mapsto e\} \models Px$.
  - Siden $\mathcal{M}, \{x \mapsto e\} \models Px$, gjelder også $\mathcal{M} \models \exists xPx$.
- At sekventen er gyldig følger også fra sunnhetsteoremet.

Eksempel 3

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(Px \wedge Qx), Pa, Qa \vdash Pa}\times}{\forall x(Px \wedge Qx), Pa \wedge Qa \vdash Pa}}{\forall x(Px \wedge Qx) \vdash Pa} \quad \dfrac{\dfrac{\dfrac{}{\forall x(Px \wedge Qx), Pa, Qa \vdash Qa}\times}{\forall x(Px \wedge Qx), Pa \wedge Qa \vdash Qa}}{\forall x(Px \wedge Qx) \vdash Qa}}{\forall x(Px \wedge Qx) \vdash \forall xPx} \quad \dfrac{}{\forall x(Px \wedge Qx) \vdash \forall xQx}}{\forall x(Px \wedge Qx) \vdash \forall xPx \wedge \forall xQx}$$

- Dette viser at sekventen $\forall x(Px \wedge Qx) \vdash \forall xPx \wedge \forall xQx$ er bevisbar.
- Sekventen er også gyldig:
  - Anta at modellen $\mathcal{M}$ gjør $\forall x(Px \wedge Qx)$ sann.
  - Velg et vilkårlig element e i domenet til $\mathcal{M}$.
  - Ved antakelsen gjelder $\mathcal{M}, \{x \mapsto e\} \models Px \wedge Qx$.
  - Da må også $\mathcal{M}, \{x \mapsto e\} \models Px$ og $\mathcal{M}, \{x \mapsto e\} \models Qx$ gjelde.
  - Siden e var vilkårlig valgt, må $\mathcal{M}$ også gjøre $\forall xPx$ og $\forall xQx$ sanne.
- At sekventen er gyldig følger også fra sunnhetsteoremet.

Eksempel 4

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall xLxa, Lba \vdash Lba, \exists yLby}\times}{\forall xLxa, Lba \vdash \exists yLby}}{\forall xLxa \vdash \exists yLby}}{\forall xLxa \vdash \forall x\exists yLxy}}{\exists y\forall xLxy \vdash \forall x\exists yLxy}$$

- Dette viser at sekventen $\exists y\forall xLxy \vdash \forall x\exists yLxy$ er bevisbar.
- Sekventen er også gyldig:
  - Anta at modellen $\mathcal{M}$ gjør $\exists y\forall xLxy$ sann.
  - Da fins det et element a slik at $\mathcal{M}, \{y \mapsto a\} \models \forall xLxy$.
  - For å vise at $\forall x\exists yLxy$ er sann i $\mathcal{M}$, velg et vilkårlig element b.
  - Det er nok å vise at $\mathcal{M}, \{x \mapsto b\} \models \exists yLxy$.
  - Vi har at $\mathcal{M}, \{y \mapsto a, x \mapsto b\} \models Lxy$ er sann i $\mathcal{M}$, siden $\mathcal{M}, \{y \mapsto a\} \models \forall xLxy$.
  - "Hvis det fins en som blir likt av alle, så har alle noen de liker."
- At sekventen er gyldig følger også fra sunnhetsteoremet.

Eksempel 5

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\forall x\exists yLxy, Lbc, Loa \vdash Lba, Ldc, \exists y\forall xLxy}}{\forall x\exists yLxy, Lbc, Loa \vdash Lba, \forall xLxc, \exists y\forall xLxy}}{\forall x\exists yLxy, Lbc, Loa \vdash Lba, \exists y\forall xLxy\exists y\forall xLxy}}{\forall x\exists yLxy, \exists yLby, Loa \vdash Lba, \exists y\forall xLxy}}{\forall x\exists yLxy\forall x\exists yLxy, Loa \vdash Lba, \exists y\forall xLxy}}{\forall x\exists yLxy, Loa \vdash \forall xLxa, \exists y\forall xLxy}}{\forall x\exists yLxy, Loa \vdash \exists y\forall xLxy}}{\forall x\exists yLxy, \exists yLoy \vdash \exists y\forall xLxy}}{\forall x\exists yLxy \vdash \exists y\forall xLxy}
$$

- Vi klarte ikke å bevise sekventen $\forall x\exists yLxy \vdash \exists y\forall xLxy$.
- Kan vi klare å lage en motmodell?
  - Når vi kommer til kompletthet, så skal vi se at det *alltid* fins en motmodell for ikke-bevisbare sekventer.
- **JA**, la $\mathcal{M} = \{a, b\}$ og la $L^{\mathcal{M}} = \{\langle a, a\rangle, \langle b, b\rangle\}$.
- "Alle liker seg selv og ingen andre."
- Da vil $\mathcal{M} \models \forall x\exists yLxy$.
  - $\mathcal{M}, \{x \mapsto a\} \models \exists yLxy$, siden $\mathcal{M}, \{x \mapsto a, y \mapsto a\} \models Lxy$.
  - $\mathcal{M}, \{x \mapsto b\} \models \exists yLxy$, siden $\mathcal{M}, \{x \mapsto b, y \mapsto b\} \models Lxy$.
- Og $\mathcal{M} \not\models \exists y\forall xLyx$.
  - $\mathcal{M}, \{y \mapsto a\} \not\models \forall xLxy$, siden $\mathcal{M}, \{x \mapsto b, y \mapsto a\} \not\models Lxy$.
  - $\mathcal{M}, \{y \mapsto b\} \not\models \forall xLxy$, siden $\mathcal{M}, \{x \mapsto a, y \mapsto b\} \not\models Lxy$.

Eksempel 6

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\times}{Po, Pa \vdash \forall xPx, Pa, \exists x(Px \to \forall xPx)}}{Po \vdash Pa, Pa \to \forall xPx, \exists x(Px \to \forall xPx)}}{Po \vdash Pa, \exists x(Px \to \forall xPx)\exists x(Px \to \forall xPx)}}{Po \vdash \forall xPx, \exists x(Px \to \forall xPx)}}{\vdash Po \to \forall xPx, \exists x(Px \to \forall xPx)}}{\vdash \exists x(Px \to \forall xPx)}
$$

- Dette viser at sekventen $\vdash \exists x(Px \to \forall xPx)$ er bevisbar.
- "Det fins en x slik at hvis x liker fotball, så liker alle fotball."
- Dette er ikke den samme påstanden som: "Hvis det fins en x som liker fotball, så liker alle fotball."
- Oppgave: vis at formelen er gyldig. Argumenter for at formelen er sann i enhver modell.

7.3 Sunnhet av førsteordens sekventkalkyle

7.3.1 Overblikk

- Vi skal nå vise at enhver sekvent som kan bevises ved å bruke LK-reglene er gyldig.
- Hvis vi kunne bevise noe som *ikke* var gyldig, så ville LK ha vært *ukorrekt* eller *usunn...*

Definisjon 7.3.1 (Sunnhet)**.** *En sekventkalkyle er* sunn *hvis enhver sekvent som er bevisbar i kalkylen, er gyldig.*

Teorem 7.3.1 (Sunnhet)**.** *Sekventkalkylen* LK *for førsteordens logikk er sunn.*

7.3.2 Antakelser om førsteordens språk

- Vi antar i beviset at et førsteordens språk $\mathcal{L}$ er gitt.
- En rotsekvent $\Gamma \vdash \Delta$ består altså av lukkede $\mathcal{L}$-formler.
- Fra antakelsen om at $\Gamma \vdash \Delta$ er bevisbar, skal vi vise at $\Gamma \vdash \Delta$ er gyldig.
- Med *gyldig* mener vi *gyldig i alle $\mathcal{L}$-modeller.*
- I en utledning av $\Gamma \vdash \Delta$ brukes det utvidete språket $\mathcal{L}^{\mathsf{par}}$.
- Vi antar derfor i sunnhetsbeviset at alle modeller er $\mathcal{L}^{\mathsf{par}}$-modeller.
- Når vi har vist at $\Gamma \vdash \Delta$ er gyldig i alle $\mathcal{L}^{\mathsf{par}}$-modeller, så må $\Gamma \vdash \Delta$ også være gyldig i alle $\mathcal{L}$-modeller, siden $\Gamma \vdash \Delta$ kun består av $\mathcal{L}$-formler.

7.3.3 Substitusjonslemma

- Sunnhet og fullstendighet gir sammenheng mellom
  - syntaks (= kalkyle)
  - semantikk ($\mathcal{M}, \mu \models \varphi$)
- Kvantorreglene bruker substitusjoner
- Semantikk av kvantorer bruker variabeltilordninger
- Vi trenger derfor en sammenheng mellom
  - substitusjoner (= syntaktiske operasjoner)
  - variabeltilordninger (= semantiske objekter)
- Substitusjonslemmaet beskriver denne sammenhengen

Lemma 7.3.1 (Substitusjonslemma)**.** *La $\mathcal{M}$ være en modell og μ en variabeltilordning for $\mathcal{M}$. La s, t være termer og x en variabel. Da gjelder:*

$$(t[s/x])^{\mathcal{M},\mu} = t^{\mathcal{M},\mu\{x \mapsto s^{\mathcal{M},\mu}\}}$$

La φ være en formel. Hvis s er fri for x i φ, så gjelder:

$$\mathcal{M}, \mu \models \varphi[s/x] \quad \textit{hviss} \quad \mathcal{M}, \mu\{x \mapsto s^{\mathcal{M},\mu}\} \models \varphi$$

Eksempel: $a^{\mathcal{M}} = ▲$. Så gjelder:

$$(x[a/x])^{\mathcal{M},\mu} = x^{\mathcal{M},\mu\{x\mapsto ▲\}}$$

$$\mathcal{M},\mu \models (\exists y.\mathsf{Inntil}(x,y))[x/a] \quad \text{hviss} \quad \mathcal{M},\mu\{x \mapsto ▲\} \models \exists y.\mathsf{Inntil}(x,y)$$

7.3.4 Bevisstruktur

Strukturen i beviset for sunnhet

Vi viser følgende lemmaer:

1. Alle LK-reglene bevarer falsifiserbarhet oppover.
2. En LK-utledning med falsifiserbar rotsekvent har minst én falsifiserbar løvsekvent.
3. Alle aksiomer er gyldige.

Til slutt vises sunnhetsteoremet ved hjelp av lemmaene.

7.3.5 Reglene bevarer falsifiserbarhet

Definisjon 7.3.2. *En* LK*-regel θ er* falsifiserbarhetsbevarende *(oppover) hvis hver gang konklusjonen i en θ-slutning er falsifiserbar, så er også minst ett av premissene i slutningen falsifiserbart.*

Lemma 7.3.2. *Alle* LK*-reglene er falsifiserbarhetsbevarende.*

- Vi har vist at α- og β-reglene har egenskapen.
- Gjenstår å vise at γ- og δ-reglene har egenskapen.

Bevis for at L$\forall$ bevarer falsifiserbarhet

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \ \vdash \Delta}{\Gamma, \forall x\varphi \ \vdash \Delta}\,\mathsf{L}\forall \qquad t \text{ er en lukket term}$$

- Anta at modellen $\mathcal{M}$ falsifiserer konklusjonen $\Gamma, \forall x\varphi \vdash \Delta$.
- $\mathcal{M}$ gjør alle formlene i $\Gamma \cup \{\forall x\varphi\}$ sanne og alle formlene i Δ usanne.
- Det holder å vise at $\mathcal{M} \models \varphi[t/x]$. Da er premisset falsifisert av $\mathcal{M}$.
- Siden $\mathcal{M} \models \forall x\varphi$ har vi at $\mathcal{M}, \{x \mapsto d\} \models \varphi$ for alle $d \in |\mathcal{M}|$. (Her bruker vi semantikken av $\forall$.)
- Spesielt har vi at $\mathcal{M}, \{x \mapsto t^{\mathcal{M}}\} \models \varphi$.
- Med Substitusjonslemmaet får vi: $\mathcal{M} \models \varphi[t/x]$.

Bevis for at $\vdash\exists$ bevarer falsifiserbarhet

$$\frac{\Gamma, \varphi[a/x] \ \vdash \Delta}{\Gamma, \exists x\varphi \ \vdash \Delta}\ \vdash\exists \qquad \begin{array}{l} a \text{ er en parameter som ikke} \\ \text{forekommer i konklusjonen} \end{array}$$

- Anta at modellen $\mathcal{M}$ falsifiserer konklusjonen $\Gamma, \exists x\varphi \vdash \Delta$.
- $\mathcal{M}$ gjør alle formlene i $\Gamma \cup \{\exists x\varphi\}$ sanne og alle formlene i Δ usanne.
- Vi må finne en modell som falsifiserer premisset.
- Men, vi kan *ikke* uten videre anta at $\mathcal{M} \models \varphi[a/x]$.
- Siden $\mathcal{M} \models \exists x\varphi$ har vi at $\mathcal{M}, \{x \mapsto d\} \models \varphi$ for en $d \in |\mathcal{M}|$.
- Fra modellen $\mathcal{M}$ lager vi en ny modell $\mathcal{M}'$ på følgende måte:
  - $\mathcal{M}'$ skal være helt lik $\mathcal{M}$ bortsett fra når det gjelder tolkningen av a.
  - Parameteren a skal tolkes som elemenet d, dvs. $a^{\mathcal{M}'} = d$.
- Vi konkluderer med at $\mathcal{M}'$ falsifiserer premisset:
  - Siden a ikke forekommer i konklusjonen, så må $\mathcal{M}'$ og $\mathcal{M}$ tolke formlene i Γ og Δ likt. $\mathcal{M}'$ gjør derfor alle formlene i Γ sanne og alle formlene i Δ usanne.
  - $\mathcal{M}', \{x \mapsto d\} \models \varphi$, og med substitusjonslemmaet $\mathcal{M}' \models \varphi[a/x]$.

Et eksempel

- Anta at $\mathcal{M}$ er en modell med domene $\{1, 2\}$ slik at $P^{\mathcal{M}} = \{2\}$.
- Anta at a og b er parametre slik at $a^{\mathcal{M}} = b^{\mathcal{M}} = 1$.
- Da vil $\mathcal{M} \not\models Pa$ og $\mathcal{M} \not\models Pb$.

$$\frac{Pb \vdash Pa}{\exists xPx \vdash Pa}$$

- Vi har at $\mathcal{M}$ falsifiserer konklusjonen:

  $\mathcal{M} \models \exists xPx$, siden $\mathcal{M}, \{x \mapsto 2\} \models Px$.
  $\mathcal{M} \not\models Pa$.

- Men, $\mathcal{M}$ falsifiserer ikke premisset, siden $\mathcal{M} \not\models Pb$.
- Vi lager en ny modell $\mathcal{M}'$ som er slik at $b^{\mathcal{M}'} = 2$.
- Da vil $\mathcal{M}'$ falsifiserer premisset.

Bevis for at R∃ og R∀ bevarer falsifiserbarhet

- beviset for R∃ er dualt til det for L∀
- beviset for R∀ er dualt til det for L∃

Lemma 7.3.3. *Hvis rotsekventen i en* LK*-utledning* π *er falsifiserbar, så er minst én av løvsekventene i* π *falsifiserbar.*

- Beviset går likt som for utsagnslogikk ved strukturell induksjon på LK-utledningen π.
- Basissteget (π er en sekvent $\Gamma \vdash \Delta$) er trivielt, siden eneste sekvent $\Gamma \vdash \Delta$ er både rot- og løvsekvent.
- To induksjonssteg: ettpremiss- og topremissutvidelse.
- Begge bruker lemmaet om falsifiserbarhetsbevaring (oppover).

7.3.6 Alle aksiomer er gyldige

Lemma 7.3.4. *Alle aksiomer er gyldige.*

- Beviset går likt som for utsagnslogikk.
- Et aksiom er på formen:
$$\Gamma, P(t_1, \ldots, t_n) \vdash P(t_1, \ldots, t_n), \Delta$$
- Enhver modell som oppfyller antecedenten må oppfylle $P(t_1, \ldots, t_n)$.
- Dermed oppfylles den samme formelen $P(t_1, \ldots, t_n)$ i succedenten.

7.3.7 Sunnhetsbeviset

Teorem 7.3.2 (Sunnhet)**.** *Sekventkalkylen* LK *for førsteordens logikk er sunn.*

Bevis.

- Anta at $\Gamma \vdash \Delta$ er LK-bevisbar.
- La π være et LK-bevis med rotsekvent $\Gamma \vdash \Delta$.
- Anta for motsigelse at $\Gamma \vdash \Delta$ *ikke* er gyldig, men er falsifiserbar.
- Ved Lemma fins det minst én løvsekvent i π som er falsifiserbar.
- Siden π er et bevis, må løvsekventen være et aksiom.
- Ved Lemma må løvsekventen være gyldig. Det gir en motsigelse.
- Da må $\Gamma \vdash \Delta$ være gyldig.

□

7.4 Oppgaver

Oppgave 7.1 Bevis eller finn motmodeller for følgende sekventer

1. $\forall x(Px \to Pfx) \vdash Pa \to Pffa$
2. $\forall x(Px \to \exists xPx)$
3. $\exists x(Px \to \exists xPx)$
4. $\forall x(Px \to \forall xPx)$
5. $\exists x(Px \to \forall xPx)$
6. $P \vee \forall x \neg Qx \vdash \forall x(P \vee \neg Qx)$
7. $\forall x \forall y(Pxy \to Pyx), \forall x \exists y Pxy \vdash \forall x \exists y(Pxy \wedge Pyx)$
8. $\exists x(Px \vee Qx) \vdash \exists xPx \vee \exists xQx$
9. $\exists x(Px \wedge Qx) \vdash \exists xPx \wedge \exists xQx$
10. $\vdash \forall x \exists y \forall z \exists w(Rxy \to Rwz)$
11. $\forall x((Px \wedge Qx) \to Rx) \vdash \forall x(Px \to Rx) \vee \forall x(Qx \to Rx)$

Oppgave 7.2 Vis at LK er **sunn** hvis og bare hvis enhver oppfyllbar mengde Γ er konsistent.

Oppgave 7.3 La Γ være en mengde formler. La $\varphi \in \Gamma$. Vi sier at φ er *uavhengig* av de andre formlene i Γ, hvis det er slik at $\Gamma \setminus \{\varphi\} \nvdash \varphi$.

(1) $\forall x \forall y \forall z(Rxy \wedge Rxz \to Rxz)$

(2) $\forall x \forall y(Rxy \to Ryx)$

(3) $\forall xRxx$

(1), **(2)** og **(3)** aksiomatiserer en ekvivalensrelasjon. Vis at alle tre er uavgengig av hverandre. (Hint: bruk sunnhetsteoremet.)

Forelesning 8: Førsteordens logikk – kompletthet

Martin Giese - 10. mars 2008

8.1 Repetisjon: Kalkyle og Sunnhet av LK

8.1.1 Sekventkalkyleregler

Definisjon 8.1.1 (γ-regler)**.** γ-reglene *i sekventkalkylen* LK *er:*

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall \qquad \frac{\Gamma \vdash \Delta, \exists x\varphi, \varphi[t/x]}{\Gamma \vdash \Delta, \exists x\varphi}\,\mathsf{R}\exists$$

t er en lukket term

Merk: kopieringen av hovedformelen i γ-reglene medfører at bevissøk i førsteordens logikk ikke nødvendigvis behøver å terminere!

Definisjon 8.1.2 (δ-regler)**.** δ-reglene *i sekventkalkylen* LK *er:*

$$\frac{\Gamma, \varphi[a/x] \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}\,\mathsf{L}\exists \qquad \frac{\Gamma \vdash \Delta, \varphi[a/x]}{\Gamma \vdash \Delta, \forall x\varphi}\,\mathsf{R}\forall$$

a er en parameter som ikke forekommer i konklusjonen.

8.1.2 Bevisstruktur

Strukturen i beviset for sunnhet

Vi viser følgende lemmaer:

1. Alle LK-reglene bevarer falsifiserbarhet oppover.
2. En LK-utledning med falsifiserbar rotsekvent har minst én falsifiserbar løvsekvent.
3. Alle aksiomer er gyldige.

Til slutt vises sunnhetsteoremet ved hjelp av lemmaene.

Bevis for at L$\forall$ bevarer falsifiserbarhet

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \;\vdash \Delta}{\Gamma, \forall x\varphi \;\vdash \Delta}\,\mathsf{L}\forall \qquad t \text{ er en lukket term}$$

- Anta at modellen $\mathcal{M}$ falsifiserer konklusjonen $\Gamma, \forall x\varphi \vdash \Delta$.
- $\mathcal{M}$ gjør alle formlene i $\Gamma \cup \{\forall x\varphi\}$ sanne og alle formlene i Δ usanne.

- Det holder å vise at $\mathcal{M} \models \varphi[t/x]$. Da er premisset falsifisert av $\mathcal{M}$.
- Siden $\mathcal{M} \models \forall x\varphi$ har vi at $\mathcal{M}, \{x \mapsto d\} \models \varphi$ for alle $d \in |\mathcal{M}|$. (Her bruker vi semantikken av $\forall$.)
- Spesielt har vi at $\mathcal{M}, \{x \mapsto t^{\mathcal{M}}\} \models \varphi$.
- Med Substitusjonslemmaet får vi: $\mathcal{M} \models \varphi[t/x]$.

Bevis for at $\mathsf{L}\exists$ bevarer falsifiserbarhet

$$\frac{\Gamma, \varphi[a/x] \ \vdash \Delta}{\Gamma, \exists x\varphi \ \vdash \Delta}\ \mathsf{L}\exists \qquad \begin{array}{l} a \text{ er en parameter som ikke} \\ \text{forekommer i konklusjonen} \end{array}$$

- Anta at modellen $\mathcal{M}$ falsifiserer konklusjonen $\Gamma, \exists x\varphi \vdash \Delta$.
- $\mathcal{M}$ gjør alle formlene i $\Gamma \cup \{\exists x\varphi\}$ sanne og alle formlene i Δ usanne.
- Vi må finne en modell som falsifiserer premisset.
- Men, vi kan *ikke* uten videre anta at $\mathcal{M} \models \varphi[a/x]$.
- Siden $\mathcal{M} \models \exists x\varphi$ har vi at $\mathcal{M}, \{x \mapsto d\} \models \varphi$ for en $d \in |\mathcal{M}|$.
- Fra modellen $\mathcal{M}$ lager vi en ny modell $\mathcal{M}'$ på følgende måte:
  - $\mathcal{M}'$ skal være helt lik $\mathcal{M}$ bortsett fra når det gjelder tolkningen av a.
  - Parameteren a skal tolkes som elemenet d, dvs. $a^{\mathcal{M}'} = d$.
- Vi konkluderer med at $\mathcal{M}'$ falsifiserer premisset:
  - Siden a ikke forekommer i konklusjonen, så må $\mathcal{M}'$ og $\mathcal{M}$ tolke formlene i Γ og Δ likt. $\mathcal{M}'$ gjør derfor alle formlene i Γ sanne og alle formlene i Δ usanne.
  - $\mathcal{M}', \{x \mapsto d\} \models \varphi$, og med substitusjonslemmaet $\mathcal{M}' \models \varphi[a/x]$.

8.2 Kompletthet av LK

8.2.1 Kompletthet – Overblikk

- Vi skal nå bevise at LK er komplett.
- Ikke bare er LK sunn, den kan også vise *alle* gyldige sekventer.
- Det er ingen "hull" i mengden av LK-bevisbare formler.
- Det er to måter å forstå "fra φ følger ψ" på:
  1. Semantisk: $\varphi \vDash \psi$, hvis φ er sann, så er ψ sann.
  2. Syntaktisk: $\varphi \vdash \psi$, det fins et bevis for sekventen $\varphi \vdash \psi$ / fra antakelsen φ, så kan ψ bevises.
- Med sunnhet og kompletthet, så blir disse ekvivalente.

Kurt Gödel (1906-1978)


Kurt Gödel (1906-1978)

- En av de mest betydningsfulle logikere noensinne.
- Har hatt enorm innflytelse på logikk, matematikk og filosofi.
- Det er han som først viste kompletthet av førsteordens logikk (1929).
- Er mest kjent for ufullstendighetsteoremene (1931) og at kontinuumshypotesen er konsistent med mengdelæren (1937).

Teorem 8.2.1 (Kompletthet)**.** *Hvis* $\Gamma \vdash \Delta$ *er gyldig, så er den bevisbar i* LK*.*

For å vise *kompletthet*, viser vi den ekvivalente påstanden:

Lemma 8.2.1 (Modelleksistens)**.** *Hvis* $\Gamma \vdash \Delta$ ikke *er bevisbar i LK, så er den falsifiserbar.*

Dvs. det finnes en modell som gjør alle formler i Γ sanne og alle formler i Δ usanne.

Merk at vi uansett går fra en universell påstand ("for alle modeller") til en eksistensiell påstand ("det fins et bevis").

8.2.2 Strategier

- Hvis en formel eller sekvent er gyldig, kan vi ha en *garanti* for at vi finner et bevis ved å begynne med en rotsekvent og anvende LK-reglene gjentatte ganger?
- For å gjøre dette litt mer presist, innfører vi begrepet *strategi.*

Definisjon 8.2.1 (Strategi)**.** *En* strategi *for* LK *er en angivelse av hvordan* LK*-reglene systematisk skal anvendes på formler i* LK*-utledninger.*

- Med vilje litt vagt. Mye kan være en strategi.
- Vi er interessert i strategier som garanterer at vi får et bevis til slutt hvis det er slik at bevis fins. La oss kalle slike strategier for "gode".

Definisjon 8.2.2 (Formeltype)**.** *La* φ *være en formel i en utledning. Vi sier at* φ *er av* type θ *hvis* φ *kan være hovedformelen i en* θ*-slutning.*

Eksempel.

$$Pa \wedge Pb, Qa \vee Qb \vdash \exists x Px, \forall x Px$$

- $Pa \wedge Pb$ *er en* α*-formel*

- $Qa \vee Qb$ *er en* β*-formel*
- $\exists x Px$ *er en* γ*-formel*
- $\forall x Px$ *er en* δ*-formel*

En enkel strategi

1. Anvend α-regler så mange ganger som mulig, dvs. helt til ingen løvsekvent lenger inneholder en formel av type α. Gå til 2.
2. Anvend β-regler så mange ganger som mulig.

$$\dfrac{\dfrac{\overset{\times}{P, Q \vdash P} \qquad \overset{\times}{P, Q \vdash Q}}{P, Q \vdash P \wedge Q}\, 2}{P \wedge Q \vdash P \wedge Q}\, 1$$

- Denne strategien er ikke "god". Det kan hende at 1 må anvendes etter at 2 er anvendt.

En "god" strategi for utsagnslogikk.

1. Anvend α-regler så mange ganger som mulig. Gå til 2.
2. Anvend β-regler så mange ganger som mulig. Gå til 3.
3. Hvis det er mulig å anvende en α-regel, gå til 1.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{\times}{P, Q \vdash P, R, R} \qquad \overset{\times}{P, Q \vdash Q, R, R}}{P, Q \vdash P \wedge Q, R, R}\, 2}{\neg(P \wedge Q), P, Q \vdash R, R}\, 1 \qquad \overset{\times}{R, P, Q \vdash R, R}}{\neg(P \wedge Q) \vee R, P, Q \vdash R, R}\, 2}{\neg(P \wedge Q) \vee R, P \vdash R, Q \to R}\, 1}{\neg(P \wedge Q) \vee R \vdash P \to R, Q \to R}\, 1}{\neg(P \wedge Q) \vee R \vdash (P \to R) \vee (Q \to R)}\, 1$$

- Hva skal til for at en strategi skal være "god"?

1. Alle formler må analyseres før eller senere.

$$\dfrac{\dfrac{\dfrac{Pffa, Pfa, Pa, \forall x Px, Qfa \wedge Qfa \vdash Qfa}{Pfa, Pa, \forall x Px, Qfa \wedge Qfa \vdash Qfa}}{Pa, \forall x Px, Qfa \wedge Qfa \vdash Qfa}}{\forall x Px, Qfa \wedge Qfa \vdash Qfa}$$

2. Vi må forsøke å sette inn "alle termer" for γ-formler.

$$\dfrac{\dfrac{\dfrac{Pgga, Pga, Pa, \forall xPx \vdash Qga, Pfffb}{Pga, Pa, \forall xPx \vdash Qga, Pfffb}}{Pa, \forall xPx \vdash Qga, Pfffb}}{\forall xPx \vdash Qga, Pfffb}$$

- Vi må kunne snakke om "alle termer" på en presis måte...

8.2.3 Herbranduniverset

Definisjon 8.2.3 (Herbranduniverset)**.** *La T være en mengde termer. Da er $\mathcal{H}(T)$, Herbranduniverset til T, den minste mengden slik at:*

- *$\mathcal{H}(T)$ inneholder alle konstanter fra T. Hvis det ikke er noen konstanter i T, så er en parameter o fra* par *(kalt en dummykonstant) med i $\mathcal{H}(T)$.*
- *Hvis f er et funksjonssymbol i T med aritet n og $t_1, \ldots, t_n$ er termer i $\mathcal{H}(T)$, så er $f(t_1, \ldots, t_n)$ i $\mathcal{H}(T)$.*

Herbranduniverset til en mengde formler er Herbranduniverset til mengden av termer som forekommer i formlene. Herbranduniverset til en gren er Herbranduniverset til mengden av formler som forekommer i grenen.

- Intuitivt, så er Herbranduniverset til T mengden av alle *lukkede* termer som kan genereres fra termer i T.

Eksempel. *La $T = \{f(x)\}$.Da er Herbranduniverset til Tmengden*

$$\{o, fo, ffo, fffo, \ldots\}$$

Eksempel. *La $T = \{a, f(x)\}$.Da er Herbranduniverset til Tmengden*

$$\{a, fa, ffa, fffa, \ldots\}$$

Eksempel. *La $F = \{\forall xH(f(g(x)))\}$.Da er Herbranduniverset til F mengden*

$$\{o, fo, go, fgo, gfo, ffo, ggo, , \ldots\}$$

8.2.4 Rettferdige strategier

- Enhver rettferdig strategi må gjøre at
  - alle formler blir analysert før eller senere, og
  - alle γ-formler blir instansiert med alle termer før eller senere.
- Hvis vi følger en rettferdig strategi, så skal én av to ting skje:
  1. Enten så klarer vi å lukke alle grener og får et bevis,
  2. eller så fins en åpen gren som vi kan lage en motmodell fra.
- For at dette skal gi mening må vi godta at utledninger kan være uendelig store, dvs. ha uendelig lange grener.

- Vi kan tenke at vi går til *grensen* i konstruksjonen av en utledning, enten ved at ingen regler lenger kan anvendes eller ved å fortsette med regelanvendelser i det uendelige. Vi kaller slike for *grenseutledninger*.
- Vi inkluderer altså uendelige trær når vi snakker om grenseutledninger.
- Merk: hvis alle grener i en utledning kan lukkes, så er utledningen endelig.
- Vi skal nå abstrahere over alle "gode" strategier.

Definisjon 8.2.4 (Rettferdig strategi)**.** *En strategi er* rettferdig *hvis enhver grenseutledning som fås ved å følge strategien har følgende egenskaper:*

1. *Hvis φ er en α-, β- eller δ-formel i en gren som ikke er lukket, så er φ hovedformel i en slutning i grenen.*
2. *Hvis φ er en γ-formel på formen $\mathsf{Q}x\psi$ i en gren som ikke er lukket, så er $\psi[t/x]$ aktiv formel i en slutning i grenen, for alle termer t i Herbranduniverset til grenen.*

8.2.5 Königs lemma

Lemma 8.2.2 (Königs lemma)**.** *Hvis T er et uendelig tre, men hvor enhver forgrening er endelig, så fins det en uendelig lang gren.*

Bevis. *Vi definerer en uendelig lang gren induktivt. La u_0 være rotnoden i treet T. Siden T er uendelig og u_0 har endelig mange etterkommere, så må ett av de umiddelbare deltrærne fra u_0 være uendelig. (Ellers ville T ha vært et endelig tre.) La u_1 være rotnoden i et slikt deltre. Hvis grenen $u_0, u_1, \ldots, u_n$ er generert, så finner man neste node u_{n+1} ved samme type resonnering. Denne prosessen gir en uendelig gren.*

Korollar 8.2.1. *Hvis T er et tre hvor enhver forgrening er endelig, og hvor alle grener er endelig lange, så er T endelig.*

8.2.6 Bevis for modelleksistensteoremet

- Anta at $\Gamma \vdash \Delta$ ikke er bevisbar.
- La π være en utledning (muligens uendelig) av $\Gamma \vdash \Delta$ som fremkommer ved å følge en rettferdig strategi. "En maksimal utledning".
- Siden $\Gamma \vdash \Delta$ ikke er bevisbar, så må det finnes minst en gren som ikke er lukket. (Her bruker vi Königs lemma.) La G være en slik gren. La

$G^\top$ være mengden av alle formler som forekommer i en antecedent i G,

$G^\perp$ være mengden av alle formler som forekommer i en succedent i G, og

A være mengden av alle atomære formler som forekommer i $G^\top$.

- Vi konstruerer nå en motmodell $\mathcal{M}$ for $\Gamma \vdash \Delta$.
- La domenet til $\mathcal{M}$ være Herbranduniverset til grenen (dvs. mengden av alle lukkede termer som kan genereres fra termer som forekommer i grenen).

- La $a^{\mathcal{M}} = a$ for alle konstantsymboler a.
- Hvis f er et funksjonssymbol med aritet n, la $f^{\mathcal{M}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.
  - Da vil $t^{\mathcal{M}} = t$ for alle lukkede termer t.
  - Alle termer tolkes som seg selv.
- Hvis R er et relasjonssymbol med aritet n, la $\langle t_1, \ldots, t_n \rangle \in R^{\mathcal{M}}$ hvis og bare hvis $R(t_1, \ldots, t_n) \in A$.
- En slik modell kalles ofte for en *Herbrandmodell* eller en *termmodell*.

- Vi viser ved induksjon på førsteordens formler (i språket $\mathcal{L}^{\mathsf{par}}$) at modellen $\mathcal{M}$ gjør *alle* formler i $G^{\top}$ sanne og alle formler i $G^{\bot}$ usanne.
- Påstandene som vi viser for førsteordens formler er:

  Hvis $\varphi \in G^{\top}$, så $\mathcal{M} \models \varphi$.
  Hvis $\varphi \in G^{\bot}$, så $\mathcal{M} \not\models \varphi$.

Basissteg 1: φ er en atomær formel $R(t_1, \ldots, t_n)$ i $G^{\top}$.

- Da må $R(t_1, \ldots, t_n) \in A$ og $\langle t_1, \ldots, t_n \rangle \in R^{\mathcal{M}}$ ved konstruksjon.
- Da må $\mathcal{M} \models R(t_1, \ldots, t_n)$.

Basissteg 2: φ er en atomær formel $R(t_1, \ldots, t_n)$ i $G^{\bot}$.

- Siden G ikke er lukket, må $R(t_1, \ldots, t_n) \notin A$ og $\langle t_1, \ldots, t_n \rangle \notin R^{\mathcal{M}}$.
- Da vil $\mathcal{M} \not\models R(t_1, \ldots, t_n)$.

Induksjonssteg: Fra antakelsen om at påstandene holder for mindre formler, så må vi vise at de holder for $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $\forall x\varphi$ og $\exists x\varphi$.

I beviset for kompletthet av utsagnslogisk LK gjorde vi mesteparten.

F.eks. anta at $\varphi \wedge \psi \in G^{\top}$.

- Ved antakelsen om at strategien var rettferdig, så har $\varphi \wedge \psi$ vært hovedformel i en slutning i grenen G.
- Da vil $\varphi \in G^{\top}$ *og* $\psi \in G^{\top}$.
- Ved induksjonshypotesen vil $\mathcal{M} \models \varphi$ *og* $\mathcal{M} \models \psi$.
- Ved definisjonen av oppfyllbarhet har vi $\mathcal{M} \models \varphi \wedge \psi$.

Formler med kvantorer gjenstår.

Anta at $\exists x\varphi \in G^{\top}$.

- Ved antakelsen om at strategien var rettferdig, så har $\exists x\varphi$ vært hovedformel i en slutning i grenen.
- Da fins en parameter a slik at $\varphi[a/x] \in G^{\top}$.

- Ved induksjonshypotesen vil $\mathcal{M} \models \varphi[a/x]$.
- Med substitusjonslemmaet: $\mathcal{M}, \{x \mapsto a^{\mathcal{M}}\} \models \varphi$.
- Ved definisjonen av oppfyllbarhet vil $\mathcal{M} \models \exists x\varphi$.

Anta at $\exists x\varphi \in G^{\perp}$.

- Vi må vise at $\mathcal{M} \not\models \exists x\varphi$. Anta at det ikke holder.
- Da gjelder $\mathcal{M}, \{x \mapsto t\} \models \varphi$ for en term $t \in |\mathcal{M}|$.
- Ved antakelsen om at strategien var rettferdig, så har $\varphi[t/x]$ vært aktiv formel på grenen.
- Vi har dermed følgende:
  - $\varphi[t/x] \in G^{\perp}$
  - $\mathcal{M} \not\models \varphi[t/x]$ (fra induksjonshypotesen)
  - $\mathcal{M}, \{x \mapsto t^{\mathcal{M}}\} \not\models \varphi$ (substitusjonslemmaet)
  - $\mathcal{M}, \{x \mapsto t\} \not\models \varphi$ (siden $t^{\mathcal{M}} = t$)
- Dermed har vi en motsigelse.

Anta at $\forall x\varphi \in G^{\perp}$.

- Ved antakelsen om at strategien var rettferdig, så har $\forall x\varphi$ vært hovedformel i en slutning i grenen.
- Da fins en parameter a slik at $\varphi[a/x] \in G^{\perp}$.
- Ved induksjonshypotesen vil $\mathcal{M} \not\models \varphi[a/x]$.
- Med substitusjonslemmaet: $\mathcal{M}, \{x \mapsto a^{\mathcal{M}}\} \not\models \varphi$.
- Ved definisjonen av oppfyllbarhet vil $\mathcal{M} \not\models \forall x\varphi$.

Anta at $\forall x\varphi \in G^{\top}$.

- Vi må vise at $\mathcal{M} \models \forall x\varphi$. Anta at det ikke holder.
- Da gjelder $\mathcal{M}, \{x \mapsto t\} \not\models \varphi$ for en term $t \in |\mathcal{M}|$.
- Ved antakelsen om at strategien var rettferdig, så har $\varphi[t/x]$ vært aktiv formel på grenen.
- Vi har dermed følgende:
  - $\varphi[t/x] \in G^{\top}$
  - $\mathcal{M} \models \varphi[t/x]$ (fra induksjonshypotesen)
  - $\mathcal{M}, \{x \mapsto t^{\mathcal{M}}\} \models \varphi$ (substitusjonslemmaet)
  - $\mathcal{M}, \{x \mapsto t\} \models \varphi$ (siden $t^{\mathcal{M}} = t$)
- Dermed har vi en motsigelse.

Noen kommentarer

- Vi kan se på konstruksjonen av en utledning som en tilnærming/approksimasjon til en motmodell for $\Gamma \vdash \Delta$.
- Jo flere ganger vi anvender regler (ved å følge en rettferdig strategi), jo nærmere kommer vi en eventuell motmodell.
- For å lage en motmodell på denne måten, kan det være nødvendig å anvende reglene uendelig mange ganger.
- Ofte fins det endelige motmodeller der hvor denne metoden gir en uendelig motmodell. Å finne endelige motmodeller der hvor det fins er ikke lett. Dette er noe det forskes på.
- Idéen i kompletthetsbeviset er viktig. Konstruksjonen av modeller fra noe rent syntaktisk. Et filosofisk spørsmål: Er det egentlig et skille mellom syntaks og semantikk?

8.2.7 Eksempler på eksistens av motmodell

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi, Pa \vdash \forall x Qx, Pa}\times \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{Qa, \varphi, Pa \vdash Qb, Pb}G \qquad \dfrac{}{Qb, Qa, \varphi, Pa \vdash Qb}\times}{Qa, \varphi, Pb \to Qb, Pa \vdash Qb}}{Qa, \varphi, Pa \vdash Qb}}{Qa, \varphi, Pa \vdash \forall x Qx}}{\varphi, Pa \to Qa, Pa \vdash \forall x Qx}}{\underbrace{\forall x(Px \to Qx)}_{\varphi}, Pa \vdash \forall x Qx}$$

- Herbranduniverset til grenen G, og domenet til $\mathcal{M}$, er $\{a, b\}$.
- Siden $Pa \in G^{\top}$ vil $a \in P^{\mathcal{M}}$ og $\mathcal{M} \models Pa$.
- Siden $Qa \in G^{\top}$ vil $a \in Q^{\mathcal{M}}$ og $\mathcal{M} \models Qa$ og $\mathcal{M} \models Pa \to Qa$.
- Siden $Qb \in G^{\perp}$ vil $b \notin Q^{\mathcal{M}}$ og $\mathcal{M} \not\models Qb$ og $\mathcal{M} \not\models \forall x Qx$.
- Siden $Pb \in G^{\perp}$ vil $b \notin P^{\mathcal{M}}$ og $\mathcal{M} \not\models Pb$ og $\mathcal{M} \models Pb \to Qb$.
- Dermed har vi også $\mathcal{M} \models \forall x(Px \to Qx)$.
- $\mathcal{M}$ oppfyller alle formlene i $G^{\top}$ og falsifiserer alle formlene i $G^{\perp}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi, Paa \to Pab, Paa \vdash Pab}}{\varphi, Paa \vdash Pab}\text{(Greit. Begge grener lukkes.)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\varphi, Pba \vdash Pab, Paa, Pba}\times \qquad \dfrac{}{Pbb, \varphi, Pba \vdash Pab, Paa}G}{\varphi, Pba \to Pbb, Pba \vdash Pab, Paa}}{\varphi, Pba \vdash Pab, Paa} \qquad \dfrac{}{Pab, \varphi, Pba \vdash Pab}\times}{\varphi, Paa \to Pab, Pba \vdash Pab}}{\varphi, Pba \vdash Pab}}{\underbrace{\forall x(Pxa \to Pxb)}_{\varphi}, Paa \vee Pba \vdash Pab}$$

- Herbranduniverset til grenen G - og domenet til $\mathcal{M}$ - er $\{a, b\}$.

- Siden $Pab \in G^{\bot}$ vil $\langle a, b\rangle \notin P^{\mathcal{M}}$ og $\mathcal{M} \not\models Pab$.
- Siden $Pba \in G^{\top}$ vil $\langle b, a\rangle \in P^{\mathcal{M}}$ og $\mathcal{M} \models Pba$ og $\mathcal{M} \models Paa \vee Pba$.
- Siden $Paa \in G^{\bot}$ vil $\langle a, a\rangle \notin P^{\mathcal{M}}$ og $\mathcal{M} \not\models Paa$ og $\mathcal{M} \models Paa \rightarrow Pab$.
- Siden $Pbb \in G^{\top}$ vil $\langle b, b\rangle \in P^{\mathcal{M}}$ og $\mathcal{M} \models Pbb$ og $\mathcal{M} \models Pba \rightarrow Pbb$.
- Dermed har vi også $\mathcal{M} \models \forall x(Pxa \rightarrow Pxb)$.
- $\mathcal{M}$ oppfyller alle formlene i $G^{\top}$ og falsifiserer alle formlene i $G^{\bot}$.

8.3 Oppgaver

Oppgave 8.1 Strategier kan ha mye å si for størrelsen på bevis. Lag to strategier for utsagnslogisk LK som viser at det er slik. Finn eksempler på bevisbare sekventer hvor den ene strategien gir små bevis og den andre strategien gir store bevis. Hint: er det lurt å forgrene så for som mulig i et bevissøk, eller er det ikke det? Se på sekventen:

$$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$$

Oppgave 8.2 Anta at vi har en lukket formel $\forall x\varphi$ og at a er en parameter som ikke forkommer i $\forall x\varphi$.

- Vis at $\forall x\varphi$ er falsifiserbar hvis og bare hvis $\varphi[a/x]$ er falsifiserbar.
- Vis at $\forall x\varphi$ er gyldig hvis og bare hvis $\varphi[a/x]$ er gyldig.

Oppgave 8.3 Bruk en rettferdig strategi for LK til å undersøke gyldigheten av følgende sekventer:

- $\forall x\exists yLxy \vdash \exists y\forall xLxy$
- $\exists x\forall yLxy \vdash \forall y\exists xLxy$

Vis hvordan søkestrategien gir et bevis eller hvordan søkestrategien genererer et objekt utfra hvilket man kan konstruere en motmodell.

Oppgave 8.4 La $\forall x\varphi$ være en formel og la $\mathcal{M}$ være en Herbrandmodell med domene lik Herbranduniverset til formelen. Vis at

- $\mathcal{M} \models \forall x\varphi$ hvis og bare hvis $\mathcal{M} \models \varphi[t/x]$ for alle termer $t \in |\mathcal{M}|$, og
- $\mathcal{M} \models \exists x\varphi$ hvis og bare hvis $\mathcal{M} \models \varphi[t/x]$ for minst en term $t \in |\mathcal{M}|$.

Oppgave 8.5 Vis at en endelig mengde formler Γ er oppfyllbar hvis og bare hvis den er konsistent.

Forelesning 9: Automatisk bevissøk – introduksjon, substitusjoner og unifisering

Martin Giese - 7. april 2008

9.1 Automatisk bevissøk

9.1.1 Introduksjon

Automatisk bevissøk i førsteordens logikk

- Sekventkalkylen LK tilbyr
  - et sett med regler for å bygge opp utledninger, og
  - en egenskap som skiller bevis fra utledninger.
- *Sunnhet* sikrer oss at enhver bevisbar sekvent er gyldig.
- *Kompletthet* sikrer oss at det *finnes* et bevis for enhver gyldig sekvent.
- Kalkylen sier imidlertid ingenting om *hvordan* man finner bevis for gyldige sekventer!
- Kompletthetsbeviset for LK gir hint om hvordan vi kan lage en søkealgoritme.
- La oss forsøke!

Noen begreper

- En utledning er *lukket* hvis alle grenene er lukket.
- En utledning er *utvidbar* hvis det er mulig å anvende en regel på en formel i en løvsekvent i utledningen.
- En søkealgoritme er *komplett* hvis den *finner* et bevis for enhver gyldig sekvent.

Algoritme: gyldig?($\Gamma \vdash \Delta$)

$\pi := \Gamma \vdash \Delta$;
while *(π ikke er lukket)* **do**
  if *(π ikke er utvidbar)* **then**
    return *"ikke gyldig"*
  else
    φ := ikke-atomær formel i løvsekvent i π;
    utvid π ved å anvende riktig LK-regel på φ
  end
end
return *"gyldig"*;

- Algoritmen er komplett hvis utvelgelsen av φ er *rettferdig*.

Effektivitet

- Effektiviteten til algoritmen avhenger av tre ting:
  1. Hvor effektivt er det å sjekke om utledningen er lukket?
  2. Strategi for valg av utvidelse av utledningen.
  3. Hvor effektiv er selve utvidelsen, dvs. regelanvendelsen?
- I første runde ser vi på punkt 1 og 3.
- Senere introduseres *koblingskalkylen*, som gir oppgav til en strategi for valg av utvidelser av utledningene.
- La oss starte med punkt 3 – effektiviteten til regelanvendelsene.

Hvor kostbare er regelanvendelsene?

- α- og β-reglene henter ut delformler fra en sammensatt formel:

$$\frac{\Gamma, A\ ,\ B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\,\mathsf{L}\wedge \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\,\mathsf{R}\wedge$$

- All nødvendig informasjon tilgjengelig i hovedformelen: kan utføres i konstant tid.
- Riktignok får vi en del formelkopiering i β-regelen, men dette kan optimaliseres med f.eks. pekere i en objektorientert implementasjon.
- δ-regelen setter inn en ny parameter for den bundne variabelen:

$$\frac{\Gamma, \varphi[a/x] \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}\,\mathsf{L}\exists$$

- Parametrene kan nummereres: utføres i lineær tid.

γ-reglene

- La oss se på γ-reglene:

$$\frac{\Gamma, \forall x\varphi, \varphi[t/x] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall \qquad \frac{\Gamma \vdash \Delta, \exists x\varphi, \varphi[t/x]}{\Gamma \vdash \Delta, \exists x\varphi}\,\mathsf{R}\exists$$

- Vi kan sette inn en vilkårlig lukket term t for x.
- For å få en komplett algoritme, må vi (før eller senere) instansiere hver γ-formel med *alle* termene i Herbranduniverset.
- Vi kan nummerere termene i Herbranduniverset og instansiere γ-formlene i denne rekkefølgen.
- Hvilken rekkefølge er gunstig med tanke på å *finne bevis så tidlig som mulig*?

$$\dfrac{\dfrac{\dfrac{\forall xPx, Pa, \ldots, Pfffa \vdash Pfffa, Qga}{\vdots}}{\forall xPx, Pa \vdash Pfffa, Qga}}{\forall xPx \vdash Pfffa, Qga} \qquad \underset{1}{a}, \underset{2}{fa}, \underset{3}{ga}, \underset{4}{ffa}, \underset{5}{fga}, \ldots, \underset{i}{fffa}, \ldots$$

Utsette valg av γ-term

- En bedre idé: Utsette valg av term i γ-reglene til et senere tidspunkt.
- La γ-reglene sette inn *frie variable*:

$$\dfrac{\dfrac{\dfrac{}{\forall xPx, Pu \vdash Pa}\,a/u}{\forall xPx \vdash Pa} \qquad \dfrac{\dfrac{}{\forall xPx, Pv \vdash Pb}\,b/v}{\forall xPx \vdash Pb}}{\forall xPx \vdash Pa \wedge Pb}$$

- Substituere termer for variable slik at løvnodene blir aksiomer.
- Hvilke substitusjoner vi kan anvende på løvnoder med frie variable slik at de blir aksiomer?
- Problemet kan løses med *unifiseringsalgoritmer*.

δ-reglene

- Når vi setter inn variable i γ-reglene får vi imidlertid problemer med δ-reglene.
- Hvordan sikre at parameteren vi setter inn er *ny* når vi ennå ikke har satt inn termer for de frie variablene?

$$\cancel{\dfrac{\dfrac{\dfrac{}{Lua \vdash Lbv}\,b/u, a/v}{\exists yLuy \vdash \forall xLxv}}{\forall x\exists yLxy \vdash \exists y\forall xLxy}}$$

kan ikke lukkes

$$\dfrac{\dfrac{}{Luf(u) \vdash Lg(v)v}}{\exists yLuy \vdash \forall xLxv}$$
$$\forall x\exists yLxy \vdash \exists y\forall xLxy$$

- Vi lar δ-reglene introdusere en *Skolemterm*:

$$f(u_1, \ldots, u_n),$$

der f er et nytt funksjonssymbol, kalt en *Skolemfunksjon*, og $u_1, \ldots, u_n$ er alle variablene som forekommer fritt i δ-formelen.

- På den måten sikrer vi at termen introdusert av δ-regelen er *ny* uansett hva slags verdi vi velger å instansiere de frie variablene med.

Oppsummering

- Vi skal introdusere en *fri-variabel sekventkalkyle* og vise at den er *sunn* og *komplett*.
- γ-reglene introduserer nye *frie variable* og δ-reglene introduserer *Skolemtermer*.
- Ved hjelp av *unifiseringsalgoritmer* finner vi *substitusjoner* som *lukker* utledningen.

9.1.2 Substitusjoner

- Vi har tidligere definert $\varphi[s/x]$ som formelen vi får ved å erstatte alle frie forekomster av x i φ med s.
- I fri-variabel sekventkalkyle har vi behov for å erstatte flere forskjellige variable med termer *samtidig*.
- Vi skal nå definere en bestemt type funksjoner – *substitusjoner* – som generaliserer én-variabel substitusjon til flere variable.
- Notasjon: Når vi anvender en substitusjon σ på en formel φ eller en term t skriver vi $\varphi\sigma$ eller $t\sigma$ istedenfor $\sigma(\varphi)/\sigma(t)$.

Definisjon 9.1.1 (Substitusjon)**.** *En* substitusjon *er en funksjon σ fra mengden variable $\mathcal{V}$ til mengden av termer $\mathcal{T}$ i et gitt førsteordens språk.*

- Støtten *(support) eller* støttemengden *(support set) til σ er mengden av variable x slik at $x\sigma \neq x$.*
- *σ er* grunn *dersom $x\sigma$ er en lukket term for alle variable x i støttemengden til σ.*

Notasjon. *En substitusjon σ med endelig støtte $\{x_1, \ldots, x_n\}$ slik at $x_1\sigma = t_1, \ldots, x_n\sigma = t_n$ skriver vi ofte slik:*

$$\sigma = \{t_1/x_1, \ldots, t_n/x_n\}$$

- Substitusjonen ϵ slik at $x\epsilon = x$ for alle variable x kalles *identitetssubstitusjonen*.
- Identitetssubstitusjonen kan skrives $\{\}$ siden den har tom støttemengde.

$$\sigma = \{a/x, fa/y\}$$

- er en substitusjon slik at
  - $x\sigma = a$
  - $y\sigma = fa$
  - $z\sigma = z$ for alle andre variable
- er en grunn substitusjon

$$\tau = \{a/y, fx/z\}$$

- er en substitusjon slik at
  - $y\sigma = a$
  - $z\sigma = fx$
  - $v\sigma = v$ for alle andre variable
- er *ikke* en grunn substitusjon

Substitusjon på termer

- Vi definerer substitusjon på termer som tidligere.

Definisjon 9.1.2 (Substitusjon på termer)**.** *Vi definerer resultatet av å anvende en substitusjon σ på vilkårlige termer rekursivt ved:*

- *$c\sigma = c$ for et konstantsymbol c.*
- *$f(t_1, \ldots, t_n)\sigma = f(t_1\sigma, \ldots, t_n\sigma)$ for en funksjonsterm $f(t_1, \ldots, t_n)$.*

La $\sigma = \{gy/x, y/z\}$**.**

- $f(x,a)\sigma = f(gy,a)$
- $h(y,z)\sigma = h(y,y)$
- $x\sigma = gy$

La $\tau = \{y/x, x/y\}$**.**

- $x\tau = y$
- $f(x,y)\tau = f(y,x)$

Substitusjon på formler

- Som tidligere, ønsker vi at substitusjoner *ikke* skal endre *bundne* variable.
- Eksempel: for $\sigma = \{a/x, b/y\}$ så vil $\forall x(Px \to Qy)\sigma = \forall xPx \to Qb$.
- Vi begrenser substitusjonen på den bundne variabelen:

Definisjon 9.1.3 (Begrenset substitusjon)**.** *La σ være en substitusjon. Substitusjonen σ begrenset på x, skrevet σ_x, er definert slik at*

$$y\sigma_x = \begin{cases} y & \text{hvis } y = x \\ y\sigma & \text{ellers} \end{cases}$$

for enhver variabel y.

Definisjon 9.1.4 (Substitusjon på formler)**.** *$\varphi\sigma$ er definert rekursivt ved:*

1. $R(t_1, \ldots, t_n)\sigma = R(t_1\sigma, \ldots, t_n\sigma)$
2. $\neg\psi\sigma = \neg(\psi\sigma)$
3. $(\varphi_1 \circ \varphi_2)\sigma = (\varphi_1\sigma \circ \varphi_2\sigma)$, *hvor* $\circ \in \{\wedge, \vee, \to\}$
4. $(\mathsf{Q}x\psi)\sigma = \mathsf{Q}x(\psi\sigma_x)$, *hvor* $\mathsf{Q} \in \{\forall, \exists\}$

- Vi antar, som tidligere, at ingen variable blir bundet som resultat av å anvende en substitusjon.
- Dette kan vi unngå ved å omdøpe bundne variable.

La $\sigma = \{fx/x, a/y, y/z\}$

- $\sigma_x = \{ \cancel{fx/x} \, , a/y, y/z\}$
- $\sigma_y = \{fx/x, \, \cancel{a/y} \, , y/z\}$
- $\sigma_z = \{fx/x, a/y, \, \cancel{y/z} \, \}$
- $P(x,y)\sigma = P(fx,a)$
- $\forall xP(x,y)\sigma = \forall x(P(x,y)\sigma_x) = \forall xP(x,a)$
- $\exists z(Px \to Qz)\sigma = \exists z((Px \to Qz)\sigma_z) = \exists z(Pfx \to Qz)$

Komposisjon av substitusjoner

- La σ og τ være substitusjoner.
- Anta at vi først anvender σ og så τ på en formel φ: $(\varphi\sigma)\tau$.
- Vi har av og til bruk for å snakke om den substitusjonen som tilsvarer å anvende σ etterfulgt av τ.

Definisjon 9.1.5 (Komposisjon av substitusjoner)**.** *La σ og τ være substitusjoner.* Komposisjonen *av σ og τ er en substitusjon skrevet $\sigma\tau$ slik at $x(\sigma\tau) = (x\sigma)\tau$ for hver variabel x.*

- Oppgave: vis at $\varphi(\sigma\tau) = (\varphi\sigma)\tau$ for alle formler φ og alle substitusjoner σ og τ.

Komposisjon av substitusjoner med endelig støtte

Påstand 9.1.1. *La $\sigma_1 = \{s_1/x_1, \ldots, s_n/x_n\}$ og $\sigma_2 = \{t_1/y_1, \ldots, t_k/y_k\}$. Da er*

$$\sigma_1\sigma_2 = \{(s_1\sigma_2)/x_1, \ldots, (s_n\sigma_2)/x_n, (z_1\sigma_2)/z_1, \ldots, (z_m\sigma_2)/z_m\}$$

der $z_1, \ldots, z_m$ er de variablene blant $y_1, \ldots, y_k$ som ikke er blant $x_1, \ldots, x_n$.

La $\sigma = \{z/x, a/y\}$ og $\tau = \{b/y, a/z\}$.

Da er $\sigma\tau = \{(z\tau)/x, (a\tau)/y, (z\tau)/z\} = \{a/x, a/y, a/z\}$.

La $\sigma = \{y/x\}$ og $\tau = \{x/y\}$.

Da er $\sigma\tau = \{(y\tau)/x, (y\tau)/y\} = \{x/x, x/y\} = \{x/y\}$.

9.1.3 Unifisering

- I fri-variabel sekventkalkyle kan vi ha løvsekventer på formen

$$\Gamma, P(s_1, \ldots, s_n) \vdash P(t_1, \ldots, t_n), \Delta$$

  der hver s_i og t_i er termer som kan inneholde variable.
- For å lukke løvsekventen må vi finne en substitusjon σ slik at $s_i\sigma = t_i\sigma$ for hver i.
- *Det er ikke sikkert at noen slik substitusjon finnes!*

Unifiseringsproblemet
La s og t være termer. Finn *alle* substitusjoner som gjør s og t syntaktisk like, dvs. alle σ slik at $s\sigma = t\sigma$.

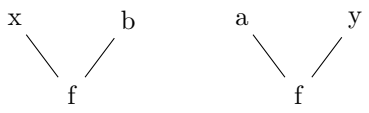
- En substitusjon som gjør termene s og t syntaktisk like, kalles en *unifikator* for s og t.
- To termer er *unifiserbare* hvis de har en unifikator.

Er $f(x)$ og $f(a)$ unifiserbare?

Ja. Vi ser at $\sigma = \{a/x\}$ er en *unifikator*: $f(x)\sigma = f(a)$

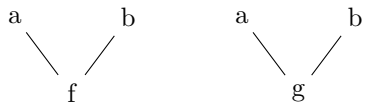
Er $f(x, b)$ og $f(a, y)$ unifiserbare?

Kan være lettere å se hvis vi skriver termene som *trær*:



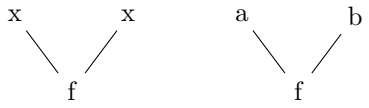
- Symbolene i posisjon 0 (rotposisjonen) er like.
- Symbolene i venstre barn er ulike, men kan unifiseres med $\{a/x\}$.
- Symbolene i høyre barn er ulike, men kan unifiseres med $\{b/y\}$.

Er $f(a, b)$ og $g(a, b)$ unifiserbare?



- Symbolene i posisjon 0 er ulike, og kan *ikke* unifiseres!

Er $f(x, x)$ og $f(a, b)$ unifiserbare?



- Symbolene i posisjon 0 er like.
- Symbolene i venstre barn er ulike, men kan unifiseres med $\{a/x\}$.
- Vi må anvende $\{a/x\}$ på x i både venstre og høyre barn.
- Symbolene i høyre barn er nå ulike, og kan *ikke* unifiseres!

Er x og $f(x)$ unifiserbare?

- Symbolene i posisjon 0 er ulike, men kan unifiseres med $\{f(x)/x\}$.
- Vi må samtidig anvende $\{f(x)/x\}$ på x i høyre tre.
- På posisjon 1 ser vi nå at symbolene x og f er ulike.
- Hvis vi unifiserer med $\{f(x)/x\}$, må vi igjen erstatte x i høyre tre.
- Sånn kan vi holde på en stund...

Generelt har vi:

- To *ulike* konstantsymboler eller funksjonssymboler er *ikke* unifiserbare.
- En variabel x er *ikke* unifiserbar med en term som *inneholder* x.

- Vi skal lage en *unifiseringsalgoritme*, som finner *alle* unifikatorer for to termer.
- Problem: To termer har potensielt uendelig mange unifikatorer! Vi kan ikke returnere alle...
- Løsning: Finne en *representant* σ for mengden av unifikatorer slik at alle andre unifikatorer kan konstrueres fra σ.
- En slik unifikator kalles en *mest generell unifikator*.

Definisjon 9.1.6 (Mer generell substitusjon)**.** *La σ_1 og σ_2 være substitusjoner. Vi sier at σ_2 er* mer generell *enn σ_1 hvis det finnes en substitusjon τ slik at $\sigma_1 = \sigma_2\tau$.*

Er $\{f(y)/x\}$ mer generell enn $\{f(a)/x\}$?

Ja, siden $\{f(a)/x\} = \{f(y)/x\}\{a/y\}$.

Er $\{f(a)/x\}$ mer generell enn $\{f(y)/x\}$?

Nei, for det finnes ingen substitusjon σ slik at $\{f(y)/x\} = \{f(a)/x\}\sigma$.

Er $\{f(y)/x\}$ mer generell enn $\{f(y)/x\}$?

Ja, siden $\{f(y)/x\} = \{f(y)/x\}\epsilon$. (Husk: ϵ er identitetssubstitusjonen.)

Definisjon 9.1.7 (Unifikator)**.** *La s og t være termer. En substitusjon σ er*

- *en unifikator for s og t hvis $s\sigma = t\sigma$.*
- *en mest generell unifikator (mgu) for s og t hvis*
  - *den er en unifikator for s og t, og*
  - *den er mer generell enn alle andre unifikatorer for s og t.*

Vi sier at s og t er unifiserbare hvis de har en unifikator.

La $s = f(x)$ og $t = f(y)$.

- $\sigma_1 = \{a/x, a/y\}$ er en unifikator for s og t
- $\sigma_2 = \{y/x\}$ og $\sigma_3 = \{x/y\}$ er også unifikatorer for s og t
- σ_2 og σ_3 er de mest generelle unifikatorene for s og t

Variabelomdøping

- Fra det foregående eksempelet ser vi at to termer kan ha flere forskjellige mest generelle unifikatorer.
- Disse mgu-ene er imidlertid like *opp til omdøping av variable.*

Definisjon 9.1.8 (Variabelomdøping)**.** *En substitusjon η er en variabelomdøping hvis*

1. *$x\eta$ er en variabel for alle $x \in \mathcal{V}$, og*
2. *$x\eta \neq y\eta$ for alle $x, y \in \mathcal{V}$ slik at $x \neq y$.*

Er disse substitusjonene variabelomdøpinger?

- $\sigma_1 = \{z/x, x/y, y/z\}$ Ja.
- $\sigma_2 = \{z/x, y/z\}$ Nei, siden $y\sigma_2 = z\sigma_2$.
- $\sigma_3 = \{z/x, x/y, y/z, a/u\}$ Nei, siden $u\sigma_3$ ikke er en variabel.

Unikhet "opp til omdøping av variable"

Påstand 9.1.2. *Hvis σ_1 og σ_2 er mest generelle unifikatorer for to termer s og t, så finnes en variable-omdøping η slik at $\sigma_1\eta = \sigma_2$.*

- Bevis som oppgave?

Deltermer

Definisjon 9.1.9 (Deltermer)**.** *Mengden av* deltermer *av en term t er den minste mengden T slik at*

- *$t \in T$, og*
- *hvis $f(t_1, \ldots, t_n) \in T$, så er hver $t_i \in T$.*

Alle termer i T utenom t er ekte deltermer *av t.*

La $s = gx$.

- Deltermer er: x, gx
- Ekte deltermer er: x

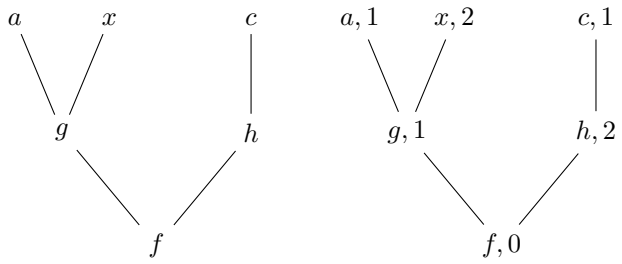
La $t = f(x, a)$.

- Deltermer er: x, a, $f(x, a)$
- Ekte deltermer er: x, a

- En term er altså en delterm av seg selv.

Nummererte termtrær

- Vi har sett at termer kan representeres med trær.
- Når vi unifiserer er det gunstig å nummerere barna til noder i termtreet:



- Slike trær kalles *nummererte termtrær*.
- Vi referer til roten til det nummererte termtreet til en term t som $\text{rot}(t)$.

Kritisk par

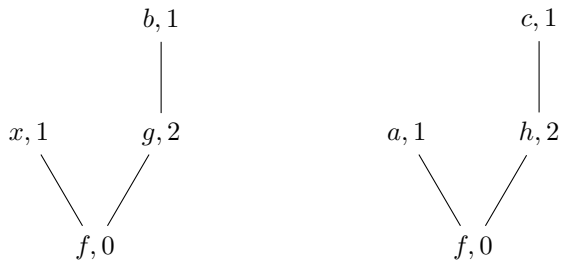
- Når vi skal unifisere to termer t_1 og t_2 er vi interessert i å finne par av deltermer som er *ulike*.
- Samtidig er det ønskelig å se på ulike deltermer så nærme roten som mulig.

Definisjon 9.1.10 (Kritisk par)**.** *Et* kritisk par *for to termer t_1 og t_2 er et par $\langle k_1, k_2 \rangle$ slik at*

- *k_1 er en delterm av t_1*

- *k_2 er en delterm av t_2*
- *når vi tenker på termer som nummererte termtrær så er*
  - *rot(k_1) forskjellig fra rot(k_2)*
  - *stien fra rot(t_1) til rot(k_1) er lik stien fra rot(t_2) til rot(k_2)*
- Merk: stiene kan være tomme, dvs. at termene er ulike allerede i rotsymbolet. Tomme stier er trivielt like...

Eksempel. *La $s = f(x, gb)$ og $t = f(a, hc)$. Vi får følgende nummererte termtrær:*



- *Er $\langle b, c\rangle$ kritisk par for s og t?*
  - *Nei, stien fra rot(s) til rot(b) er ulik stien fra rot(t) til rot(c).*
- *Er $\langle x, a\rangle$ kritisk par for s og t? Ja.*
- *Er $\langle gb, hc\rangle$ kritisk par for s og t? Ja.*

Algoritme: unifiser(t_1, t_2)

$\sigma := \epsilon$;
while *($t_1\sigma \neq t_2\sigma$)* **do**
  velg et kritisk par $\langle k_1, k_2\rangle$ for $t_1\sigma, t_2\sigma$;
  if *(hverken k_1 eller k_2 er en variabel)* **then**
    return *"ikke unifiserbare"*;
  end
  $x :=$ den av k_1, k_2 som er variabel (hvis begge er, så velg én);
  $t :=$ den av k_1, k_2 som ikke er x;
  if *(x forekommer i t)* **then**
    return *"ikke unifiserbare"*;
  end
  $\sigma := \sigma\{t/x\}$;
end
return σ;

Egenskaper ved unifiseringsalgoritmen

- Hvis termene t_1 og t_2 er unifiserbare, så returnerer algoritmen en mest generell unifikator for t_1 og t_2.
- Denne mgu-en er en representant for alle andre unifikatorer for t_1 og t_2.
- Hvis t_1 og t_2 *ikke* er unifiserbare, så returnerer algoritmen *"ikke unifiserbare"*.

9.2 Oppgaver

Oppgave 9.1 (LJ-bevis) Gi LJ-bevis for følgede sekventer.

1. $\neg P \land \neg Q \vdash \neg(P \lor Q)$
2. $\neg(P \lor Q) \vdash \neg P \land \neg Q$
3. $\neg P \lor \neg Q \vdash \neg(P \land Q)$
4. $P \to Q \vdash (P \to (Q \to R)) \to (P \to R)$
5. $P \to Q \vdash (P \to \neg Q) \to \neg P$
6. $P \to R \vdash (Q \to R) \to ((P \lor Q) \to R)$
7. $\neg\neg(P \land Q) \vdash \neg\neg P \land \neg\neg Q$
8. $\neg\neg P \land \neg\neg Q \vdash \neg\neg(P \land Q)$

Oppgave 9.2 (Motmodeller) Gi Kripke-modeller som er motmodeller for følgende sekventer:

1. $P \vdash \neg P$
2. $\neg P \vdash P$
3. $\neg Q \to \neg P \vdash P \to Q$
4. $\neg(P \land Q) \vdash \neg P \lor \neg Q$
5. $P \to Q \vdash \neg P \lor Q$

Oppgave 9.3 (Peirce's lov) La φ være $((P \to Q) \to P) \to P$. Formelen φ kalles "Peirce's lov".

1. Gi et LJ-bevis for $\vdash \neg\neg\varphi$.
2. Fins et LJ-bevis for $\vdash \varphi$? Hvis ja, gi beviset. Hvis nei, finn en motmodell.

Oppgave 9.4 Vis at $x \Vdash \neg\neg A$ hvis og bare hvis for alle y slik at $x \leq y$ det fins en z slik at $y \leq z$ og $z \Vdash A$.

Forelesning 10: Automatisk bevissøk II – fri-variabel sekventkalkyle og sunnhet

Martin Giese - 14. april 2008

10.1 Automatisk bevissøk II

10.1.1 Fri-variabel sekventkalkyle

- Valg av term i γ-slutninger utsettes ved å sette inn en *fri* variabel.
- Introduksjon av frie variable i γ-slutninger gjør at vi må la δ-slutninger introdusere *Skolemtermer*.
- Ved unifisering finner vi en substitusjon som erstatter frie variable med termer slik at utledningen lukkes.

$$\dfrac{\dfrac{\dfrac{}{Lufu \vdash Lav}\,u/a, v/fa}{\exists y Luy \vdash Lav}}{\forall x \exists y Lxy \vdash \exists x Lax}$$

Utvidet språk

- δ-slutningene introduserer *Skolemkonstanter* og *Skolemfunksjoner*.
- Disse symbolene er *nye* symboler som ikke forekommer i det språket som defineres av rotsekventen i en utledning.
- Språket som brukes i utledningene er *utvidet* med slike Skolemsymboler.

Definisjon 10.1.1 (Utvidet språk)**.** *La $\mathcal{L}$ være et førsteordens språk. La $\mathcal{S}$ være en mengde som består av*

- *tellbart uendelig mange* Skolemkonstanter*, og*
- *tellbart uendelig mange* Skolemfunksjoner *av hver aritet,*

slik at symbolene i $\mathcal{S}$ er forskjellig fra symbolene i $\mathcal{L}$. La $\mathcal{L}^{\mathsf{sko}}$ være språket vi får ved å utvide $\mathcal{L}$ med konstant- og funksjonssymbolene i $\mathcal{S}$.

Sekventer

Definisjon 10.1.2 (Sekvent)**.** *La $\mathcal{L}$ være et førsteordens språk.*

- *En* sekvent *er et objekt på formen $\Gamma \vdash \Delta$ slik at Γ og Δ er multimengder av førsteordens formler i $\mathcal{L}^{\mathsf{sko}}$.*
- *En sekvent $\Gamma \vdash \Delta$ er* lukket *hvis formlene i Γ og Δ er lukkede.*

Sekventer

1. $\forall x Px \vdash Pa$
2. $\forall x \exists y Lxy \vdash \exists x \forall y Lyx$
3. $\forall x Pxy \vdash Pufu$
4. $Pu \vdash Pa$
5. $Pu \vdash Pu, \exists x Px$

Lukkede sekventer

Nr. 1 og 2 er *lukkede* sekventer.

γ-reglene

Definisjon 10.1.3 (γ-regler i fri-variabel LK)**.** γ-reglene *i fri-variabel* LK *er:*

$$\frac{\Gamma, \forall x\varphi, \varphi[u/x] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall \qquad \frac{\Gamma \vdash \Delta, \exists x\varphi, \varphi[u/x]}{\Gamma \vdash \Delta, \exists x\varphi}\,\mathsf{R}\exists$$

u er en ny fri variabel

- Med *ny* mener vi her at u ikke må forekomme fritt i utledningen fra før.

δ-reglene

Definisjon 10.1.4 (δ-regler i fri-variabel LK)**.** δ-reglene *i fri-variabel* LK *er:*

$$\frac{\Gamma, \varphi[f(\vec{u})/x] \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}\,\mathsf{L}\exists \qquad \frac{\Gamma \vdash \Delta, \varphi[f(\vec{u})/x]}{\Gamma \vdash \Delta, \forall x\varphi}\,\mathsf{R}\forall$$

f er en ny Skolemfunksjon
$\vec{u} = u_1, \ldots, u_n$ er de frie variablene i hovedformelen

- Med *ny* mener vi her at f ikke må forekomme i utledningen fra før.

Slutningsregler og utledninger

Definisjon 10.1.5 (Slutningsreglene i fri-variabel LK)**.** Slutningsreglene *i fri-variabel* LK *er*

- *γ- og δ-reglene for frie variable, og*
- *α- og β-reglene fra utsagnslogisk* LK*.*

- Mengden av *fri-variabel utledninger* defineres induktivt:
  - *Basismengden* er mengden av lukkede sekventer.
  - Mengden er lukket under slutningsreglene i fri-variabel LK.
- Vi krever altså at rotsekventen i en utledning *kun* inneholder lukkede formler!
- Formlene i de andre sekventene i en utledning behøver imidlertid ikke være lukkede.

Eksempler på fri-variabel utledninger

$$\dfrac{\dfrac{\dfrac{\forall xPx, Pu \vdash \exists xPx, Pv}{\forall xPx, Pu \vdash \exists xPx}\,\mathsf{R}\exists}{\forall xPx \vdash \exists xPx}\,\mathsf{L}\forall$$

$\mathsf{R}\exists$ kan *ikke* introdusere u, siden denne allerede forekommer fri i utledningen.

$$\dfrac{\dfrac{\forall xPx, Pu \vdash Pa}{\forall xPx \vdash Pa}\,\mathsf{L}\forall \qquad \dfrac{\forall xPx, Pv \vdash Pb}{\forall xPx \vdash Pb}\,\mathsf{L}\forall}{\forall xPx \vdash Pa \wedge Pb}\,\mathsf{R}\wedge$$

$\mathsf{L}\forall$ i høyre og venstre gren kan *ikke* introdusere den samme variabelen, av samme grunn som over.

Eksempler på fri-variabel utledninger

$$\dfrac{\dfrac{\dfrac{\forall x(Px \vee Qx), Pu \vdash Pa, \forall xQx}{\forall x(Px \vee Qx), Pu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall \qquad \dfrac{\forall x(Px \vee Qx), Qu \vdash \forall xPx, Qb}{\forall x(Px \vee Qx), Qu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall}{\forall x(Px \vee Qx), Pu \vee Qu \vdash \forall xPx, \forall xQx}\,\mathsf{L}\vee}{\forall x(Px \vee Qx) \vdash \forall xPx, \forall xQx}\,\mathsf{L}\forall$$

- Vi krever at hver δ-slutning introduserer et *nytt* Skolemsymbol, dvs. et som *ikke* forekommer i utledningen fra før.
- Derfor kan $\mathsf{R}\forall$ i høyre gren *ikke* introdusere den samme Skolemkonstanten som $\mathsf{R}\forall$ i venstre gren.
- Dette er et *strengere* krav enn for δ-reglene i LK uten frie variable, der den introduserte parameteren ikke må forekomme i *konklusjonen*.
- I utledningen over vet vi ikke hvilke symboler som forekommer i konklusjonen før vi har instansiert u!

Eksempel på objekter som *ikke* er utledninger

$$\dfrac{\dfrac{Px \vdash Pa}{Px \vdash \forall xPx}\,\mathsf{R}\forall}{\vdash Px \to \forall xPx}\,\mathsf{R}\to$$

Rotsekventen er ikke lukket.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x\exists yPxy, Puf(u) \vdash Pf(v)v, \exists x\forall yPyx}{\forall x\exists yPxy, Puf(u) \vdash \forall yPyv, \exists x\forall yPyx}\,\mathsf{R}\forall}{\forall x\exists yPxy, Puf(u) \vdash \exists x\forall yPyx}\,\mathsf{R}\exists}{\forall x\exists yPxy, \exists yPuy \vdash \exists x\forall yPyx}\,\mathsf{L}\exists}{\forall x\exists yPxy \vdash \exists x\forall yPyx}\,\mathsf{L}\forall$$

De to δ-slutningene introduserer det samme Skolemfunksjonssymbolet.

Lukkede utledninger

- For at en fri-variabel LK-utledning skal være et bevis, må vi instansiere de frie variablene i utledningen slik at løvsekventene blir aksiomer.
- Dette kalles å *lukke* en utledning.

Definisjon 10.1.6 (Lukking)**.** *La π være en fri-variabel utledning, og la σ være en substitusjon.*

- *σ lukker en løvsekvent $\Gamma \vdash \Delta$ i π hvis det finnes* atomære *formler $\varphi \in \Gamma$ og $\psi \in \Delta$ slik at $\varphi\sigma = \psi\sigma$.*
- *σ lukker π hvis σ lukker alle løvsekventene i π.*

Bevis

Definisjon 10.1.7 (Bevis)**.** *Et fri-variabel LK-bevis for en sekvent $\Gamma \vdash \Delta$ er et par $\langle \pi, \sigma \rangle$ der*

- *π er en utledning med $\Gamma \vdash \Delta$ som rotsekvent, og*
- *σ er en grunn substitusjon som lukker π.*

- Vi krever at den lukkende substitusjonen skal være *grunn*, siden dette gjør sunnhetsbeviset *litt* lettere.
- Senere skal vi se at vi kan lempe på dette kravet og tillate lukkende substitusjoner som ikke er grunne.

Eksempel (1)**.** *La π være utledningen*

$$\dfrac{\dfrac{\forall xPx, Pu \vdash \exists xPx, Pv}{\forall xPx, Pu \vdash \exists xPx}\,\mathsf{R}\exists}{\forall xPx \vdash \exists xPx}\,\mathsf{L}\forall$$

og la $\sigma = \{a/u, a/v\}$.

- *σ lukker løvsekventen: $(Pu)\sigma = Pa = (Pv)\sigma$.*
- *σ lukker π, siden den lukker den eneste løvsekventen.*
- *Da er $\langle \pi, \sigma \rangle$ et bevis for sekventen $\forall xPx \vdash \exists xPx$.*

Merk:

Slik vi har definert fri-variabel LK vil f.eks. $\langle \pi, \sigma' \rangle$ der $\sigma' = \{v/u\}$ *ikke* være et bevis, siden σ' ikke er grunn.

Eksempel (2)**.** *La π være utledningen*

$$\dfrac{\dfrac{\forall xPx, Pu \vdash Pa}{\forall xPx \vdash Pa}\,\mathsf{L}\forall \qquad \dfrac{\forall xPx, Pv \vdash Pb}{\forall xPx \vdash Pb}\,\mathsf{L}\forall}{\forall xPx \vdash Pa \wedge Pb}\,\mathsf{R}\wedge$$

og la $\sigma = \{a/u, b/v\}$.

- *σ lukker venstre løvsekvent: $(Pu)\sigma = Pa$.*
- *σ lukker høyre løvsekvent: $(Pv)\sigma = Pb$.*
- *σ lukker π, siden den lukker begge løvsekventene.*
- *Da er $\langle \pi, \sigma \rangle$ et bevis for sekventen $\forall xPx \vdash Pa \wedge Pb$.*

Eksempel (3)**.** *La π være utledningen*

$$\dfrac{\dfrac{\dfrac{\forall x(Px \vee Qx), Pu \vdash Pa, \forall xQx}{\forall x(Px \vee Qx), Pu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall \qquad \dfrac{\forall x(Px \vee Qx), Qu \vdash \forall xPx, Qb}{\forall x(Px \vee Qx), Qu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall}{\forall x(Px \vee Qx), Pu \vee Qu \vdash \forall xPx, \forall xQx}\,\mathsf{L}\vee}{\forall x(Px \vee Qx) \vdash \forall xPx, \forall xQx}\,\mathsf{L}\forall$$

- *Det finnes ingen substitusjon som lukker begge løvsekventene, siden u ikke kan instansieres med både a og b* samtidig*.*
- *Derfor finnes ikke noe bevis for sekventen $\forall x(Px \vee Qx) \vdash \forall xPx, \forall xQx$ basert på utledningen π.*
- *Er rotsekventen gyldig...?*

10.1.2 Semantikk

- For å kunne vise at kalkylen er sunn må vi ha klart for oss hvordan vi tolker formlene i utledningene.
- Tidligere inneholdt våre sekventer bare *lukkede* formler.
- Vi har imidlertid definert semantikken av formler med frie variabler gjennom *variabeltilordninger*.
- Vi gir nå en repetisjon av definisjonene.

Variabeltilordninger

Definisjon 10.1.8 (Variabeltilordning)**.** *La $\mathcal{M}$ være en modell. En* variabeltilordning *for $\mathcal{M}$ er en funksjon fra mengen av variable til $|\mathcal{M}|$.*

- En variabeltilordning er alltid gitt relativ til en modell $\mathcal{M}$ siden den tolker variable som elementer i domenet til $\mathcal{M}$.
- For en gitt modell kan vi ha mange variabeltilordninger.
- Hvis $|\mathcal{M}| = \{1, 2, 3\}$, så kan vi ha
  - μ_1 slik at $\mu_1(x_1) = 1$, $\mu_1(x_2) = 1$, $\mu_1(x_3) = 1$, ...
  - μ_2 slik at $\mu_2(x_1) = 2$, $\mu_2(x_2) = 2$, $\mu_2(x_3) = 2$, ...
  - μ_3 slik at $\mu_3(x_1) = 1$, $\mu_3(x_2) = 2$, $\mu_3(x_3) = 3$, ...
  - ...

Tolkning av termer med frie variable

- Tolkningsfunksjonen i modellen tolker konstant- og funksjonssymboler.
- Tolkningen av frie variable overlates til variabeltilordningen.

Definisjon 10.1.9 (Tolkning av termer med frie variable)**.** *La $\mathcal{L}$ være et førsteordens språk og $\mathcal{M}$ en modell for $\mathcal{L}$. La μ være en variabeltilordning for $\mathcal{M}$. Tolkningen av en term t i $\mathcal{M}$ under μ, skrevet $t^{\mathcal{M},\mu}$, defineres rekursivt.*

- $x^{\mathcal{M},\mu} = \mu(x)$ *for en variabel* x
- $c^{\mathcal{M},\mu} = c^{\mathcal{M}}$ *for et konstantsymbol* c
- $f(t_1, \ldots, t_n)^{\mathcal{M},\mu} = f^{\mathcal{M}}(t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu})$ *for en funksjonsterm*

Tolkning av formler med frie variable

Definisjon 10.1.10 (Tolkning av formler med frie variable)**.** *La $\mathcal{L}$ være et førsteordens språk og $\mathcal{M}$ en modell for $\mathcal{L}$. La μ være en variabeltilordning for $\mathcal{M}$. Vi definerer ved rekursjon hva det vil si at en formel φ er* sann *i $\mathcal{M}$ under μ; vi skriver $\mathcal{M}, \mu \models \varphi$ når φ er sann i $\mathcal{M}$ under μ.*

- *Atomære fml:* $\mathcal{M}, \mu \models R(t_1, \ldots, t_n)$ *hvis* $\langle t_1^{\mathcal{M},\mu}, \ldots, t_n^{\mathcal{M},\mu} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M}, \mu \models \neg\varphi$ *hvis det ikke er tilfelle at* $\mathcal{M}, \mu \models \varphi$.
- $\mathcal{M}, \mu \models \varphi \wedge \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *og* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \varphi \vee \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *eller* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \varphi \to \psi$ *hvis* $\mathcal{M}, \mu \models \varphi$ *impliserer* $\mathcal{M}, \mu \models \psi$.
- $\mathcal{M}, \mu \models \forall x\varphi$ *hvis* $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for alle* a *i* $|\mathcal{M}|$.
- $\mathcal{M}, \mu \models \exists x\varphi$ *hvis* $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ *for minst en* a *i* $|\mathcal{M}|$.

Eksempel I

Modellen $\mathcal{M}$

$|\mathcal{M}| = \{$  $\}$

$\mathsf{Liker}^{\mathcal{M}} =$

$\{\langle$  $\rangle, \langle$  $\rangle,$

$\langle$  $\rangle, \langle$  $\rangle\}$

Variabeltilordningen μ_1

$\mu_1(x) =$ 

- *Er det slik at* $\mathcal{M}, \mu_1 \models \exists y \mathsf{Liker}(y, x)$*?*
- Fra semantikken:

$$\begin{gathered}
\mathcal{M}, \mu_1 \models \exists y \mathsf{Liker}(y, x) \\
\Updownarrow \\
\text{finnes } e \in |\mathcal{M}| \text{ slik at } \mathcal{M}, \mu_1\{y \mapsto e\} \models \mathsf{Liker}(y, x) \\
\Updownarrow \\
\text{finnes } e \in |\mathcal{M}| \text{ slik at } \langle y^{\mathcal{M}, \mu_1\{y \mapsto e\}}, x^{\mathcal{M}, \mu_1\{y \mapsto e\}} \rangle \in \mathsf{Liker}^{\mathcal{M}} \\
\Updownarrow \\
\text{finnes } e \in |\mathcal{M}| \text{ slik at } \langle e, \mu_1(x) \rangle \in \mathsf{Liker}^{\mathcal{M}} \\
\Updownarrow \\
\text{finnes } e \in |\mathcal{M}| \text{ slik at } \langle e, \text{  } \rangle \in \mathsf{Liker}^{\mathcal{M}}
\end{gathered}$$

- **Ja**, både $e =$  og $e =$  .

Falsifiserbarhet

- Vi har tidligere definert gyldighet av en *lukket* sekvent $\Gamma \vdash \Delta$ slik:
  - Enhver modell som oppfyller alle formlene i Γ må oppfylle minst én formel i Δ.
- Vi kan også definere en gyldig sekvent som en sekvent som *ikke* er falsifiserbar.
- En sekvent $\Gamma \vdash \Delta$ er falsifiserbar hvis den har en *motmodell*, dvs. en modell som oppfyller alle formlene i Γ og gjør alle formlene i Δ usanne.
- I fri-variabel LK kan Γ og Δ inneholde formler som *ikke* er lukket.
- Vi ønsker at en motmodell til en sekvent skal være en motmodell *uavhengig* av hvordan vi tolker de frie variablene.

Falsifiserbarhet II

Se på sekventen $Qx \vdash Px$

- En motmodell vil f.eks. være modellen $\mathcal{M}$ slik at $|\mathcal{M}| = \{a, b\}$, $Q^{\mathcal{M}} = \{a, b\}$ og $P^{\mathcal{M}} = \emptyset$.
- Her finnes to aktuelle variabeltilordninger: $\mu_1(x) = a$ og $\mu_2(x) = b$.
- Uansett hvilken av disse vi bruker til å tolke de frie variablene, så vil $\mathcal{M}$ være en motmodell til sekventen.

Se på sekventen $Px \vdash Pa$

- Et forsøk på å lage en motmodell kan være $\mathcal{M}'$ slik at $|\mathcal{M}'| = \{a, b\}$ og $P^{\mathcal{M}'} = \{b\}$.

- Hvis vi tolker x som b, ser vi at $\mathcal{M}'$ oppfyller Px og falsifiserer Pa.
- Men hvis vi tolker x som a, ser vi at $\mathcal{M}'$ ikke lenger er en motmodell.
- Her finnes en variabeltilordning som gjør at $\mathcal{M}'$ ikke er en motmodell til sekventen.

Falsifiserbarhet III

- Hvorvidt en modell $\mathcal{M}$ er en motmodell til en sekvent $\Gamma \vdash \Delta$ avhenger altså av hvilke sannhetsverdier formlene i Γ og Δ får for *hver enkelt* variabeltilordning for $\mathcal{M}$.
- Det leder til følgende definisjon.

Definisjon 10.1.11 (Falsifiserbar sekvent)**.** *En modell $\mathcal{M}$ er en* motmodell *til en sekvent $\Gamma \vdash \Delta$ hvis følgende holder for* alle *variabeltilordninger μ for $\mathcal{M}$:*

- *$\mathcal{M}, \mu$ gjør alle formlene i Γ sanne, og*
- *$\mathcal{M}, \mu$ gjør alle formlene i Δ usanne.*

En sekvent er

- falsifiserbar *hvis den har en motmodell*
- gyldig *hvis den ikke er falsifiserbar*

10.1.3 Sunnhet

Definisjon 10.1.12 (Sunnhet)**.** *En sekventkalkyle er* sunn *dersom enhver bevisbar sekvent er gyldig.*

- Kjernen i sunnhetsbeviset for utsagnslogisk LK og grunn LK er at slutningsreglene bevarer falsifiserbarhet oppover.
- Reglene i fri-variabel LK har *ikke* denne egenskapen!

β-regelen bevarer ikke falsifiserbarhet oppover

- Se på slutningen

$$\frac{Pu \vdash Pa, Qb \qquad Qu \vdash Pa, Qb}{Pu \vee Qu \vdash Pa, Qb}$$

- La $\mathcal{M}$ være en modell slik at $|\mathcal{M}| = \{a, b\}$, $a^{\mathcal{M}} = a$, $b^{\mathcal{M}} = b$, $P^{\mathcal{M}} = \{b\}$ og $Q^{\mathcal{M}} = \{a\}$.
- Vi har to aktuelle variabeltilordninger for $\mathcal{M}$: $\mu_1(u) = a$ og $\mu_2(u) = b$.
- $\mathcal{M}$ falsifiserer konklusjonen:
  - $\mathcal{M}$ falsifiserer begge formlene i succedenten.
  - $\mathcal{M}, \mu_1 \models Qu$ og $\mathcal{M}, \mu_2 \models Pu$, så $\mathcal{M}$ gjør formelen i antecedenten sann uavhengig av variabeltilordning.
- Premissene er *ikke* falsifiserbare. (Prøv!)
- Konklusjonen er falsifiserbar, mens premissene *ikke* er det!

Sunnhet – alternativ framgangsmåte

- På grunn av β-slutningene vil en fri variabel kunne forekomme i flere *forskjellige* grener i en utledning.
- De forskjellige forekomstene er *avhengige* av hverandre i den forstand at de må tildeles den samme verdien av en variabeltilordning.
- Vi skal definere hva det vil si at en utledning er *falsifiserbar*.
- Vi skal så vise at alle utledninger med falsifiserbar rotsekvent er falsifiserbare.
- Når vi har denne egenskapen, er resten av sunnhetsbeviset for fri-variabel LK tilsvarende beviset for den grunne kalkylen.

Falsifiserbarhet

- Husk at hvis G er en gren i en utledning, så er
  - $\mathsf{G}^\top$ alle formler som forekommer i en antecedent på G, og
  - $\mathsf{G}^\bot$ alle formler som forekommer i en succedent på G.

Definisjon 10.1.13 (Falsifiserbarhet)**.** *La π være en fri-variabel utledning, og la $\mathcal{M}$ være en modell.*

- *Anta at μ er en variabeltilordning for $\mathcal{M}$. En gren G i π er* falsifisert *av $\mathcal{M}$ under μ hvis*
  - *$\mathcal{M}, \mu$ gjør alle formlene i $\mathsf{G}^\top$ sanne, og*
  - *$\mathcal{M}, \mu$ gjør alle formlene i $\mathsf{G}^\bot$ usanne.*
- *$\mathcal{M}$* falsifiserer *π hvis for alle variabeltilordninger μ for $\mathcal{M}$ så finnes en gren i π som er falsifisert av $\mathcal{M}$ under μ.*

En utledning er falsifiserbar hvis det finnes en modell som falsifiserer den.

Falsifisert gren avhenger av variabeltilordningen

La π være følgende utledning (der γ-kopiene ikke vises):

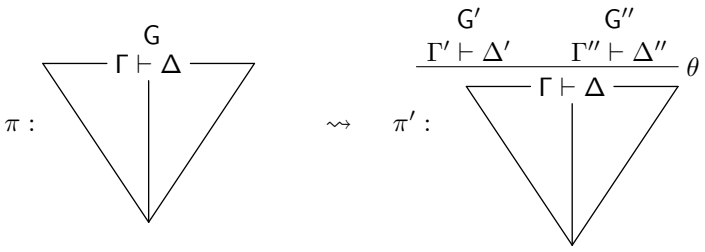
$$\dfrac{\dfrac{Pu \vdash Pa, Qb \qquad Qu \vdash Pa, Qb}{Pu \vee Qu \vdash Pa, Qb}}{\forall x(Px \vee Qx) \vdash Pa, Qb}$$

- La $\mathcal{M}$ være en modell slik at $|\mathcal{M}| = \{a, b\}$, $a^\mathcal{M} = a$, $b^\mathcal{M} = b$, $P^\mathcal{M} = \{b\}$ og $Q^\mathcal{M} = \{a\}$.
- $\mathcal{M}$ falsifiserer π:
  - Hvis $\mu_1(u) = a$, så har vi at den høyre grenen er falsifisert av $\mathcal{M}$ under μ_1.
  - Hvis $\mu_2(u) = b$, så har vi at den venstre grenen er falsifisert av $\mathcal{M}$ under μ_2.

Lemma 10.1.1. *Hvis en slutningsregel fra fri-variabel LK anvendes på en falsifiserbar utledning, så får vi en ny falsifiserbar utledning.*

- Vi skal med andre ord vise at reglene *bevarer falsifiserbarhet.*
- Vi får ett tilfelle for hver regel.
- Alle tilfellene bortsett fra δ-reglene ($\mathsf{L}\exists$ og $\mathsf{R}\forall$) går på samme måte.
- Vi viser først hvordan beviset går for disse og tar δ-reglene til slutt.

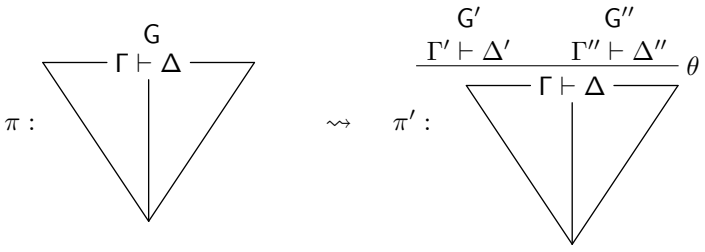
Bevis. Overblikk:



- Anta at π er falsifiserbar.
- Skal vise at π' er falsifiserbar.
- La $\mathcal{M}$ være en modell som falsifiserer π.
- Velg en vilkårlig variabeltilordning μ for $\mathcal{M}$.
- Vi får to tilfeller:
  1. Den grenen i π som er falsifisert av $\mathcal{M}$ under μ er en annen enn G.
  2. Den falsifiserte grenen er G.

□

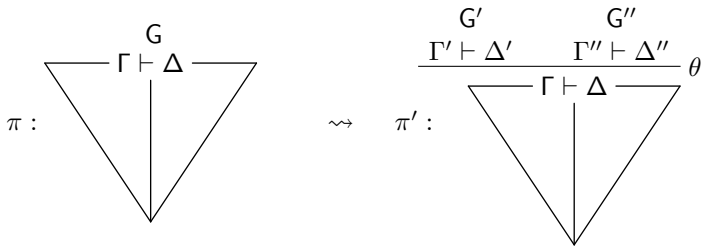
Bevis (tilfelle 1).



- Har antatt at π er falsifiserbar.
- Har valgt en modell $\mathcal{M}$ som falsifiserer π og en variabeltilordning μ for $\mathcal{M}$.
- Har antatt at grenen i π som er falsifisert av $\mathcal{M}$ under μ *ikke* er G.
- Da er den falsifiserte grenen i π også en gren i π'.

□

Bevis (tilfelle 2).



- Har antatt at π er falsifiserbar.
- Har en modell $\mathcal{M}$ som falsifiserer π og en variabeltilordning μ for $\mathcal{M}$.
- Har antatt at G i π er falsifisert av $\mathcal{M}$ under μ.
- Må vise at enten G' eller G'' er falsifisert i π'.
- Vi får ett tilfelle for hver LK-regel.
- Vi viser argumentet for $\mathsf{L}\vee$ og $\mathsf{L}\forall$.

□

Bevis (tilfelle 2 – $\mathsf{L}\vee$).

$$\dfrac{\dfrac{\mathsf{G}'}{\Gamma, A \vdash \Delta} \qquad \dfrac{\mathsf{G}''}{\Gamma, B \vdash \Delta}}{\Gamma, A \vee B \vdash \Delta}\,\mathsf{L}\vee$$

$$\Big|\ \mathsf{G}$$

- Siden konklusjonen er på G og G er falsifisert av $\mathcal{M}$ under μ, så har vi at $\mathcal{M}, \mu \models \Gamma \cup \{A \vee B\}$ og at $\mathcal{M}, \mu$ gjør alle i Δ usanne.
- Fra semantikken har vi at $\mathcal{M}, \mu \models A$ *eller* $\mathcal{M}, \mu \models B$.
- Hvis $\mathcal{M}, \mu \models A$, så er G' falsifisert av $\mathcal{M}$ under μ.
- Hvis $\mathcal{M}, \mu \models B$, så er G'' falsifisert av $\mathcal{M}$ under μ.

□

Bevis (tilfelle 2 – $\mathsf{L}\forall$).

$$\dfrac{\dfrac{\mathsf{G}'}{\Gamma, \forall x\varphi, \varphi[u/x] \vdash \Delta}}{\Gamma, \forall x\varphi \vdash \Delta}\,\mathsf{L}\forall$$

$$\Big|\ \mathsf{G}$$

- Siden konklusjonen er på G og G er falsifisert av $\mathcal{M}$ under μ, så har vi at $\mathcal{M}, \mu \models \Gamma \cup \{\forall x\varphi\}$ og at $\mathcal{M}, \mu$ gjør alle formler i Δ usanne.
- Anta at $\mu(u) = e$ (der $e \in |\mathcal{M}|$).

- Siden $\mathcal{M}, \mu \models \forall x \varphi$ har vi fra semantikken at $\mathcal{M}, \mu\{x \mapsto a\} \models \varphi$ for *alle* $a \in |\mathcal{M}|$.
- Spesielt vil $\mathcal{M}, \mu\{x \mapsto e\} \models \varphi$, men da vil $\mathcal{M}, \mu \models \varphi[u/x]$, på grunn av substitusjonslemmaet.
- Da er G' falsifisert av $\mathcal{M}$ under μ.

□

Bevis (δ-regler). Når en δ-regel anvendes, må vi vise lemmaet på en annen måte. Vi gjør tilfellet for $\mathsf{L}\exists$.

$$\dfrac{\begin{array}{c}\mathsf{G}' \\ \Gamma, \varphi[f(u_1, \ldots, u_n)/x] \vdash \Delta\end{array}}{\Gamma, \exists x \varphi \vdash \Delta}\, \mathsf{L}\exists \qquad \Big|\ \mathsf{G}$$

- La $\mathcal{M}'$ være en modell som er *lik* $\mathcal{M}$ bortsett fra tolkningen av f, som defineres som følger:
  - La $a_1, \ldots, a_n \in |\mathcal{M}'|$ og la μ' være en variabeltilordning slik at $\mu'(u_i) = a_i$ for $1 \leq i \leq n$.
  - Hvis $\mathcal{M}, \mu' \models \exists x \varphi$, så finnes $e \in |\mathcal{M}|$ slik at $\mathcal{M}, \mu'\{x \mapsto e\} \models \varphi$. La $f^{\mathcal{M}'}(a_1, \ldots, a_n) = e$.
  - Hvis $\mathcal{M}, \mu' \not\models \exists x \varphi$, så la $f^{\mathcal{M}'}(a_1, \ldots, a_n)$ være et vilkårlig element i $|\mathcal{M}'|$.
- Påstand: $\mathcal{M}'$ falsifiserer π'. Oppgave!

□

Lemma 10.1.2. *Enhver utledning med falsifiserbar rotsekvent er falsifiserbar.*

Bevis. Ved strukturell induksjon på utledninger.

- Basistilfellet: rotsekventen er falsifiserbar.
- Induksjonssteget: følger fra Lemma.

□

En variant av substitusjonslemmaet, for flere variabler, men bare for grunn substittusjoner:

Lemma 10.1.3. *La $\mathcal{M}$ være en modell, og la σ være en grunn substitusjon. La μ være en variabeltilordning slik at $\mu(x) = (x\sigma)^{\mathcal{M}}$ for hver variabel x i støtten til σ. Hvis φ er en formel slik at de frie variablene i φ er med i støtten til σ, så holder $\mathcal{M}, \mu \models \varphi$ hvis og bare hvis $\mathcal{M} \models \varphi\sigma$.*

Bevis. Ukeoppgave. □

Teorem 10.1.1 (Sunnhet)**.** *Sekventkalkylen fri-variabel LK er sunn.*

Bevis.
- Anta at $\langle \pi, \sigma \rangle$ er et bevis for $\Gamma \vdash \Delta$.
- Anta for motsigelse at $\Gamma \vdash \Delta$ *ikke* er gyldig, men er falsifiserbar.
- Ved Lemma finnes en modell $\mathcal{M}$ som falsifiserer π.
- La μ være en variabeltilordning slik at $\mu(x) = (x\sigma)^{\mathcal{M}}$ for hver variabel x i støtten til σ.

- Da finnes en gren G i π som er falsifisert av $\mathcal{M}$ under μ.
- Siden σ lukker løvsekventen på G, så finnes atomære formler $\varphi \in \mathsf{G}^{\top}$ og $\psi \in \mathsf{G}^{\bot}$ slik at $\varphi\sigma = \psi\sigma$.
- Siden G er falsifisert av $\mathcal{M}$ under μ, så $\mathcal{M}, \mu \models \varphi$ og $\mathcal{M}, \mu \not\models \psi$.
- Fra Lemma har vi $\mathcal{M} \models \varphi\sigma$ og $\mathcal{M} \not\models \psi\sigma$. Men $\varphi\sigma = \psi\sigma$, motsigelse.

□

10.2 Oppgaver

I forelesning 10 så vi på en unifiseringsalgoritme som finner en mest generell unifikator for *to* termer. I automatisk bevissøk har vi imidlertid bruk for å sjekke om *flere* par av termer er unifiserbare *samtidig*. Se på sekventen

$$P(k(x,z), f(y, q(v,a))) \vdash P(k(g(y), j(v)), f(h(z,a), w)),$$

der x, y, z, v, w er variable, f, g, h, j, k, q er funksjonssymboler og P er et relasjonssymbol. For å gjøre de to atomære formlene like, må vi finne en substitusjon σ slik at

$$k(x,z) =_\sigma k(g(y), j(v)) \quad \textit{og} \quad f(y, q(v,a)) =_\sigma f(h(z,a), w)$$

samtidig. (Notasjon: $s =_\sigma t$ betyr $s\sigma = t\sigma$.) Vi kan bruke unifiseringsalgoritmen fra forelesningen til også å løse slike problemer. Hvis vi betrakter relasjonssymbolet P som et funksjonssymbol, kan vi la de to atomære formlene være de to termene som skal unifiseres. Generelt kan vi bruke algoritmen til å løse unifiseringsproblemer på formen

$$s_1 =^? t_1, \ldots, s_n =^? t_n$$

ved å unifisere termene $\circ(s_1, \ldots, s_n)$ og $\circ(t_1, \ldots, t_n)$, der $\circ$ er et vilkårlig funksjomssymbol med aritet n. (Notasjon: $s =^? t$ uttrykker at vi ønsker å unifisere termene s og t.) Vi sier at en *unifikator* for et slikt unifiseringsproblem er en substitusjon σ slik at

$$s_1 =_\sigma t_1, \ldots, s_n =_\sigma t_n.$$

Oppgave 10.1 Finn en mest generell unifikator (hvis noen finnes) for følgende unifiseringsproblemer.

a. $k(x,z) =^? k(g(y), j(v))$ og $f(y, q(v,a)) =^? f(h(z,a), w)$

b. $x =^? f(y)$ og $y =^? g(x)$

Oppgave 10.2 Vis at for alle substitusjoner σ og τ, og for alle førsteordens formler φ så er $\varphi(\sigma\tau) = (\varphi\sigma)\tau$. (Hint: strukturell induksjon.)

Forelesning 11: Automatisk bevissøk III – fri-variabel kompletthet og repetisjon av sunnhet

Martin Giese - 31. april 2008

11.1 Kompletthet av fri-variabel LK

Teorem 11.1.1 (Kompletthet)**.** *Hvis* $\Gamma \vdash \Delta$ *er gyldig, så er den bevisbar i fri-variabel* LK*.*

For å vise *kompletthet*, viser vi den ekvivalente påstanden:

Lemma 11.1.1 (Modelleksistens)**.** *Hvis* $\Gamma \vdash \Delta$ ikke *er bevisbar i LK, så er den falsifiserbar.*

Husk:

- En modell $\mathcal{M}$ *falsifiserer* $\Gamma \vdash \Delta$ hvis ethvert valg av variabeltilordning for $\mathcal{M}$ gjør alle formler i Γ sanne og alle formler i Δ usanne.
- Hvis formlene i Γ og Δ er *lukkede*, vil sannhetsverdiene til formlene under $\mathcal{M}$ være *uavhengig av variabeltilordning.*

Modelleksistens for grunn LK – repetisjon

Beviset for modelleksistens for fri-variabel LK bygger på beviset for grunn LK. Hovedtrekkene i beviset for grunn LK:

- Vi antar at en sekvent $\Gamma \vdash \Delta$ *ikke* er bevisbar i grunn LK.
  - Det betyr at alle utledninger med rotsekvent $\Gamma \vdash \Delta$ har en åpen gren.
- Vi bruker en *rettferdig strategi* til å konstruere en *grenseutledning* for $\Gamma \vdash \Delta$ der hver åpen gren G har følgende egenskaper:
  - enhver α-, β- og δ-formel på G er hovedformel i en slutning på G, og
  - hvis G inneholder en γ-formel på formen $\mathsf{Q}x\varphi$, så er $\varphi[t/x]$ aktiv formel i en slutning på G for hver term t i Herbrand-universet til G.
  - *"Alle mulige regelanvendelser er forsøkt på alle åpne grener."*
- Siden $\Gamma \vdash \Delta$ ikke er bevisbar, så må grenseutledningen inneholde en *åpen* gren G (ved Königs lemma).

Modelleksistens for grunn LK – repetisjon II

- Vi benytter informasjonen i G til å konstruere en Herbrand-modell $\mathcal{M}$ på følgende måte:
  - Domenet til $\mathcal{M}$ er Herbrand-universet til G.
  - For lukkede termer t på G: $t^{\mathcal{M}} = t$
  - For n-ære relasjonssymboler P på G: $\langle t_1, \ldots, t_n \rangle \in P^{\mathcal{M}} \Leftrightarrow P(t_1, \ldots, t_n) \in \mathsf{G}^{\top}$
- *Husk: Herbrand-universet til en gren er mengden av alle grunne termer som kan konstrueres fra konstant- og funksjonssymboler på grenen.*

- Vi viser så ved strukturell induksjon på formler i G at $\mathcal{M}$ oppfyller alle formler i $\mathsf{G}^\top$ og falsifiserer alle formler i $\mathsf{G}^\bot$.
  - Basissteget har to tilfeller: $P(t_1, \ldots, t_n) \in \mathsf{G}^\top$ og $P(t_1, \ldots, t_n) \in \mathsf{G}^\bot$.
  - I induksjonssteget får vi ett hovedtilfelle for hvert konnektiv.
  - I hvert hovedtilfelle må vi se på om formelen forekommer i $\mathsf{G}^\top$ eller $\mathsf{G}^\bot$.
- Det følger at $\mathcal{M}$ falsifiserer $\Gamma \vdash \Delta$, siden $\Gamma \subseteq \mathsf{G}^\top$ og $\Delta \subseteq \mathsf{G}^\bot$.

Modelleksistens for grunn LK – repetisjon III

- I argumentet for at $\mathcal{M}$ oppfyller alle formler i $\mathsf{G}^\top$ og falsifiserer alle formler i $\mathsf{G}^\bot$ gjør vi strukturell induksjon på formlene i G.
- Basissteget følger pr. definisjon av Herbrand-modellen $\mathcal{M}$.
- I induksjonssteget antar vi at en formel φ forekommer på den åpne grenen G og benytter oss av at grenseutledningen er konstruert med en rettferdig strategi:
  - For α-, β- og δ-formler bruker vi at φ er hovedformel i en slutning på G, og at de umiddelbare delformlene til φ derfor må være i G.
  - For γ-formler bruker vi at den umiddelbare delformelen til φ er instansiert med alle termer i Herbrand-universet til G.
- Siden delformlene er av enklere struktur enn φ, kan vi anta at påstanden holder for disse, og bruke semantikken til å slutte at påstanden holder for φ.

Modelleksistens for fri-variabel LK

- I beviset for modelleksistens for fri-variabel LK skal vi
  - bruke en *rettferdig strategi* til å konstruere en grenseutledning med en åpen gren for en ikke-bevisbar sekvent, og
  - anvende en *grunn* substitusjon på alle formlene i den åpne grenen slik at alle frie variable blir instansiert med grunne termer.
- Vi kan så konstruere en Herbrand-modell fra den *grunnede* åpne grenen på samme måte som for grunn LK, og bruke det samme induksjonsargumentet.
- I fri-variabel LK introduserer γ-reglene imidlertid *frie variable* istedenfor termer, så vi trenger en ny definisjon av *rettferdig strategi*.
- Vi må også velge den grunnende substitusjonen slik at den grunnede åpne grenen får samme egenskaper m.h.p. γ-formler som i grenseutledningen i grunn LK.

Rettferdig strategi for fri-variabel LK

- En rettferdig strategi vil før eller senere anvende en regel på enhver ikke-atomær formel i en løvsekvent i utledningen.

- Siden hovedformelen i en γ-slutning kopieres, vil vi (hvis vi fortsetter å anvende regler i det uendelige) måtte introdusere uendelig mange frie variable for hver γ-formel på en gren.

Definisjon 11.1.1 (Rettferdig strategi)**.** *En strategi er* rettferdig *hvis enhver grenseutledning som fås ved å følge strategien har følgende egenskaper:*

1. *Hvis φ er en α-, β- eller δ-formel i en gren, så er φ hovedformel i en slutning i grenen.*
2. *Hvis φ er en γ-formel på formen $\mathsf{Q}x\psi$ i en gren, så er $\psi[u/x]$ aktiv formel i en slutning i grenen, for uendelig mange variable u.*

Rettferdig substitusjon

- Grenseutledningen til høyre er generert med en rettferdig strategi.
- Formelen $\forall xPx$ introduserer uendelig mange frie variable u_i.
- La substitusjonen σ være slik at $\sigma(u_i) = a$ for alle u_i.

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\forall xPx, Pu_1, Pu_2, Pu_3 \vdash Qfa}}{\forall xPx, Pu_1, Pu_2 \vdash Qfa}}{\forall xPx, Pu_1 \vdash Qfa}}{\forall xPx \vdash Qfa}$$

- Utledningen har kun én gren, kall den G. Hvis vi anvender σ på formlene i G, så vil alle Pu_i-formlene bli til Pa.
- Vi ser at Herbrand-universet til $\mathsf{G}\sigma$ er $a, fa, ffa, fffa, \ldots$ Det finnes nå termer t i Herbrand-universet slik at Pt *ikke* er i $\mathsf{G}\sigma$, f.eks. $t = fa$.
- Herbrand-modellen generert fra $\mathsf{G}\sigma$ vil derfor *ikke* gjøre $\forall xPx$ sann.

Rettferdig substitusjon II

- La substitusjonen τ være definert rekursivt slik at
  - $\tau(u_1) = a$, og
  - $\tau(u_{i+1}) = f\tau(u_i)$.
- Vi anvender τ på formlene i grenen G.

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\forall xPx, Pu_1, Pu_2, Pu_3 \vdash Qfa}}{\forall xPx, Pu_1, Pu_2 \vdash Qfa}}{\forall xPx, Pu_1 \vdash Qfa}}{\forall xPx \vdash Qfa}$$

- Vi har nå at $Pt \in \mathsf{G}\tau$ for alle termer t i Herbrand-universet til $\mathsf{G}\tau$.
- Derfor vil Herbrand-modellen generert fra $\mathsf{G}\tau$ oppfylle $\forall xPx$.
- Vi kaller τ en *rettferdig substitusjon*.

Rettferdig substitusjon III

Definisjon 11.1.2 (Rettferdig substitusjon)**.** *La π være en grenseutledning generert med en rettferdig strategi, og la G være en gren i π. La σ være en substitusjon.*

- σ *er* rettferdig m.h.p. en γ-formel $\mathsf{Q}x\varphi$ *i* G *hvis for alle termer* t *i Herbrand-universet til* G *så finnes en formel* $\varphi[u/x]$ *aktiv i en* γ*-slutning i* G *slik at* $\sigma(u) = t$.
- σ *er* rettferdig m.h.p. grenen G *hvis* σ *er rettferdig m.h.p. alle* γ*-formlene i* G.
- σ *er* rettferdig m.h.p. utledningen π *hvis* σ *er rettferdig m.h.p. hver gren i* π.

Modelleksistens for fri-variabel LK – bevis

- Anta at sekventen $\Gamma \vdash \Delta$ *ikke* er bevisbar i fri-variabel LK.
  - Det betyr at for alle utledninger med $\Gamma \vdash \Delta$ som rotsekvent, så finnes *ingen* substitusjon som lukker utledningen.
- Vi bruker en *rettferdig strategi* til å lage en *grenseutledning* med $\Gamma \vdash \Delta$ som rotsekvent.
- Vi velger en substitusjon σ som er *rettferdig* m.h.p. grenseutledningen og som instansierer alle frie variable i utledningen med grunne termer.
- Siden σ ikke lukker grenseutledningen, så vil det finnes en gren G i grenseutledningen som ikke er lukket av σ (ved Königs lemma).
- Vi anvender σ på alle formlene i G. Merk at $\mathsf{G}\sigma$ kun inneholder *lukkede* formler. Vi kan derfor gjøre resten av beviset på samme måte som for grunn LK.
- Merk at $\Gamma \vdash \Delta$ er *lukket*. Herbrand-modellen generert fra $\mathsf{G}\sigma$ vil derfor falsifisere $\Gamma \vdash \Delta$ uavhengig av variabeltilordning.

11.2 Repetisjon: sunnhet av fri-variabel LK

Sunnhet

Vi viste forrige gang at sekventkalkylen fri-variabel LK er *sunn*.

Teorem 11.2.1 (Sunnhet)**.** *Hvis en sekvent er bevisbar i fri-variabel* LK*, så er den gyldig.*

Sentralt i beviset står argumentet for at det å anvende en LK-regel på en falsifiserbar utledning gir en falsifiserbar utledning.

Lemma 11.2.1. *Enhver utledning med falsifiserbar rotsekvent er falsifiserbar.*

Vi skal ta en kort repetisjon av sunnhetsargumentet.

Falsifiserbarhet

- I sunnhetsbeviset for *grunn* LK viste vi at alle reglene bevarer falsifiserbarhet oppover.
- I fri-variabel LK utvidet vi semantikken med variabeltilordninger for å tolke formler med frie variable.
- Vi måtte også innføre et nytt falsifiseringsbegrep for sekventer med frie variable.
- β-reglene i fri-variabel LK bevarer *ikke* falsifiserbarhet oppover.

- Vi innførte derfor falsifiserbarhet for *utledninger*.
- En modell *falsifiserer* en utledning hvis ethvert valg av variabeltilordning for modellen gir en falsifisert gren.

β-regelen bevarer ikke falsifiserbarhet oppover

- Se på slutningen

$$\frac{Pu \vdash Pa, Qb \qquad Qu \vdash Pa, Qb}{Pu \vee Qu \vdash Pa, Qb}$$

- La $\mathcal{M}$ være en modell slik at $|\mathcal{M}| = \{a, b\}$, $a^{\mathcal{M}} = a$, $b^{\mathcal{M}} = b$, $P^{\mathcal{M}} = \{b\}$ og $Q^{\mathcal{M}} = \{a\}$.
- Vi har to aktuelle variabeltilordninger for $\mathcal{M}$: $\mu_1(u) = a$ og $\mu_2(u) = b$.
- $\mathcal{M}$ falsifiserer konklusjonen:
  - $\mathcal{M}$ falsifiserer begge formlene i succedenten.
  - $\mathcal{M}, \mu_1 \models Qu$ og $\mathcal{M}, \mu_2 \models Pu$, så $\mathcal{M}$ gjør formelen i antecedenten sann uavhengig av variabeltilordning.
- Premissene er *ikke* falsifiserbare. (Prøv!)
- Konklusjonen er falsifiserbar, mens premissene *ikke* er det!

Beviset for falsifiserbarhetslemmaet

- Beviset for falsifiserbarhetslemmaet går ved strukturell induksjon på utledninger.
- I induksjonssteget
  - antar vi at en utledning π er falsifiserbar, og
  - viser at utledningen vi får når vi utvider π med en fri-variabel LK-regel også er falsifiserbar.
- Vi får ett tilfelle for hver LK-regel.
- Antagelsen om at π er falsifiserbar gir oss en falsifiserende modell $\mathcal{M}$.
- For α-, β- og γ-reglene kan vi vise at $\mathcal{M}$ også falsifiserer den utvidete utledningen.
- Det holder ikke for δ-reglene. Her konstruerer vi en ny modell (basert på $\mathcal{M}$) som falsifiserer den utvidete utledningen.

Beviset for falsifiserbarhetslemmaet – δ-regelen

$$\frac{\Gamma, \varphi[f(u_1, \ldots, u_n)/x] \vdash \Delta}{\Gamma, \exists x \varphi \vdash \Delta}\ \mathsf{L}\exists$$

- Hvis vi utvider med en δ-slutning, så vil den nye løvsekventen inneholder Skolemtermen $f(u_1, \ldots, u_n)$.
- Vi lager en ny modell $\mathcal{M}'$ som er lik $\mathcal{M}$ bortsett fra tolkningen av f.

- For hver variabeltilordning μ for $\mathcal{M}'$ spesifiserer vi $\mathcal{M}', \mu$ sin tolkning av den introduserte Skolemtermen slik at $\mathcal{M}', \mu$ gjør $\varphi[f(u_1, \ldots, u_n)/x]$ sann dersom $\mathcal{M}, \mu$ gjør $\exists x \varphi$ sann.
- Siden f ikke forekommer i π *og* $\mathcal{M}$ er lik $\mathcal{M}'$ utenom f, så er π falsifisert av $\mathcal{M}'$.
- Ved å bruke de semantiske definisjonene, viser vi så at $\mathcal{M}'$ falsifiserer den utvidete utledningen.

Teorem 11.2.2 (Sunnhet)**.** *Hvis* $\Gamma \vdash \Delta$ *er bevisbar i fri-variabel* LK*, så er* $\Gamma \vdash \Delta$ *gyldig.*

Bevis.
- Anta at $\langle \pi, \sigma \rangle$ er et bevis for $\Gamma \vdash \Delta$.
- Anta for motsigelse at $\Gamma \vdash \Delta$ *ikke* er gyldig, men er falsifiserbar.
- Ved Lemma finnes en modell $\mathcal{M}$ som falsifiserer π.
- La μ være en variabeltilordning slik at $\mu(x) = (x\sigma)^{\mathcal{M}}$ for hver variabel x i støtten til σ.
- Da finnes en gren G i π som er falsifisert av $\mathcal{M}$ under μ.
- Siden σ lukker løvsekventen på G, så finnes atomære formler $\varphi \in \mathsf{G}^{\top}$ og $\psi \in \mathsf{G}^{\bot}$ slik at $\varphi\sigma = \psi\sigma$.
- Siden G er falsifisert av $\mathcal{M}$ under μ, så $\mathcal{M}, \mu \models \varphi$ og $\mathcal{M}, \mu \not\models \psi$.
- Fra Lemma har vi $\mathcal{M} \models \varphi\sigma$ og $\mathcal{M} \not\models \psi\sigma$. Men $\varphi\sigma = \psi\sigma$, motsigelse.

□

11.3 Oppgaver

Fri-variabel semantikk

La φ være formelen $\exists x \mathsf{Liker}(x, y)$. Vi ser at variabelen y forekommer fritt i φ. La modellen $\mathcal{M}$ være slik at $|\mathcal{M}| = \{\mathsf{Ola}, \mathsf{Kari}\}$, og $\mathsf{Liker}^{\mathcal{M}} = \{\langle \mathsf{Ola}, \mathsf{Kari} \rangle\}$. Anta videre at vi har konstantsymbolene a og b i signaturen vår, og at $a^{\mathcal{M}} = \mathsf{Ola}$ og $b^{\mathcal{M}} = \mathsf{Kari}$. La σ være en grunn substitusjon slik at $\sigma = \{b/y\}$. Vi lar μ være en variabeltilordning for $\mathcal{M}$ slik at $\mu(y) = (y\sigma)^{\mathcal{M}} = b^{\mathcal{M}} = \mathsf{Kari}$ (hvordan μ tolker andre variable enn y ser vi bort fra i denne sammenhengen). Vi ser at både

$$(1) \quad \mathcal{M}, \mu \models \varphi$$

og[2]

$$(2) \quad \mathcal{M} \models \varphi\sigma$$

holder. Vi har definert μ slik at μ tolker y – den eneste frie variabelen i φ – som det samme objektet som $(y\sigma)^{\mathcal{M}}$. Det er derfor ikke så overraskende at både (1) og (2) holder. Generelt kan vi definere følgende lemma.

Lemma 11.3.1. *La* $\mathcal{M}$ *være en modell, og la* σ *være en grunn substitusjon. La* μ *være en variabeltilordning slik at* $\mu(x) = (x\sigma)^{\mathcal{M}}$ *for hver variabel* x *i støtten til* σ*. Hvis* φ *er en formel slik at de frie variablene i* φ *er med i støtten til* σ*, så holder* $\mathcal{M}, \mu \models \varphi$ *hvis og bare hvis* $\mathcal{M} \models \varphi\sigma$*.*

Oppgave 11.1 Vis lemmaet over. (Hint: Strukturell induksjon på formler.)

[2] I det siste tilfellet behøver vi ikke μ for å tolke $\varphi\sigma$, siden $\varphi\sigma$ er en lukket formel.

Sunnhet av fri-variabel LK

I fri-variabel LK definerte vi δ-reglene som

$$\frac{\Gamma, \varphi[f(\vec{u})/x] \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}\,\mathsf{L}\exists \qquad \frac{\Gamma \vdash \Delta, \varphi[f(\vec{u})/x]}{\Gamma \vdash \Delta, \forall x\varphi}\,\mathsf{R}\forall$$

der symbolene f og $\vec{u}$ ble definert på følgende måte:

(I)
- f er ny for *utledningen*
- $\vec{u} = u_1, \ldots, u_n$ er de variablene som forekommer fritt i *hovedformelen*

I beviset for sunnhet av kalkylen står følgende lemma sentralt.

Lemma 11.3.2 (Falsifiserbarhet)**.** *Enhver utledning med falsifiserbar rotsekvent er falsifiserbar.*

Beviset går ved strukturell induksjon på utledninger. I induksjonssteget antar vi at lemmaet holder for en utledning π med falsifiserbar rotsekvent og viser at lemmaet holder for utledningen π', som vi får ved å anvende en LK-regel θ på en løvsekvent i π. Siden vi har antatt at lemmaet holder for π og at π har falsifiserbar rotsekvent, så finnes en modell $\mathcal{M}$ som falsifiserer π. Ved definisjonen av falsifiserbarhet så vet vi at for hver variabeltilordning μ for $\mathcal{M}$, så finnes en gren G i π som er falsifisert[3] av $\mathcal{M}$ under μ.

Vi må vise at π' er falsifiserbar. Dette gjør vi ved å finne en modell $\mathcal{M}'$ som *falsifiserer* den utvidete utledningen π'. Framgangsmåten avhenger av hvilken regel vi brukte for å utvide π til π'. Vi får ett tilfelle for hver av LK-reglene. Siden vi pr. antagelse allerede har en modell $\mathcal{M}$ som falsifiserer π så er det en god idé å forsøke å bruke denne som motmodell til π' også. Dette fungerer fint for α-, β- og γ-reglene. Beviset for f.eks. $\mathsf{L}\!\rightarrow$ kan gjøres på følgende måte.

Bevis (induksjonssteget for $\mathsf{L}\!\rightarrow$*).* La θ være en slutning på formen

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta}.$$

Legg merke til at konklusjonen i θ er løvsekvent i π, men ikke i den utvidete utledningen π'. Premissene i θ er begge løvsekventer i π', men ikke i π. La G være den grenen i π som har konklusjonen i θ som løvsekvent. La G' og G'' være grenene i π' som har henholdsvis venstre og høyre premiss i θ som løvsekventer.

Vi skal vise at π' er falsifiserbar, dvs. at det finnes en modell $\mathcal{M}'$ som falsifiserer π'. Vi setter $\mathcal{M}' = \mathcal{M}$ og viser at $\mathcal{M}$ falsifiserer π'. La μ' være en vilkårlig variabeltilordning for $\mathcal{M}$. Hvis vi kan vise at det finnes en gren i π' som er falsifisert av $\mathcal{M}$ under μ', så er vi i mål. Pr. antagelse så finnes det en gren i π som er falsifisert av $\mathcal{M}$ under μ'. Vi har to tilfeller:

1. Den falsifiserte grenen er en annen enn G.
2. Den falsifiserte grenen er G.

[3] Dvs. $\mathcal{M}, \mu \models \varphi$ for alle $\varphi \in \mathsf{G}^{\top}$ og $\mathcal{M}, \mu \not\models \psi$ for alle $\psi \in \mathsf{G}^{\bot}$

I tilfelle (1), så er den falsifiserte grenen også en gren i π', og vi er i mål. Anta derfor at vi har tilfelle (2), dvs. at G er falsifisert av $\mathcal{M}$ under μ'. Vi må vise at G' eller G'' er falsifisert av $\mathcal{M}$ under μ'. Siden G er falsifisert av $\mathcal{M}$ under μ' og $A \to B \in \mathsf{G}^{\top}$, så har vi at $\mathcal{M}, \mu' \models A \to B$. Ved definisjonen av tolkning av formler med frie variable så har vi at (2a) $\mathcal{M}, \mu' \not\models A$ eller (2b) $\mathcal{M}, \mu' \models B$. I tilfelle (2a) så er G' falsifisert av $\mathcal{M}$ under μ'. I tilfelle (2b) så er G'' falsifisert av $\mathcal{M}$ under μ'. □

De to første avsnittene i beviset kan også brukes i induksjonssteget for de andre α-, β- og γ-reglene. Det er det siste avsnittet i beviset som blir spesifikt for regelen. Den generelle framgangsmåten er imidlertid den samme:

1. Vi bruker antagelsen om at $\mathcal{M}, \mu'$ gjør hovedformelen sann eller usann (avhengig av om det er en ventre- eller høyreregel vi skal vise).
2. Vi bruker fri-variabel semantikken til å finne ut hvilke sannhetsverdier de aktive formlene får av $\mathcal{M}, \mu'$.
3. Vi konkluderer med at G' eller G'' er falsifisert av $\mathcal{M}$ under μ'.

Legg merke til at resonnementet er likt det vi brukte for å vise at reglene bevarer falsifiserbarhet oppover i utsagnslogisk LK og grunn førsteordens LK. Det er imidlertid en viktig forskjell: I fri-variabel LK viser vi at reglene *bevarer falsifiserbarhet av utledninger*.

Oppgave 11.2 Gjør induksjonssteget i beviset for falsifiserbarhetslemmaet for LK-reglene $\mathsf{L}\neg$, $\mathsf{R}\neg$, $\mathsf{R}\to$, $\mathsf{R}\vee$, $\mathsf{L}\wedge$, $\mathsf{R}\wedge$ og $\mathsf{R}\exists$.

For δ-reglene kan vi ikke bruke $\mathcal{M}$ som falsifiserende modell for π'. Vi må definere en ny modell $\mathcal{M}'$ som er lik $\mathcal{M}$ bortsett fra tolkningen av Skolemsymbolet f i den introduserte Skolemtermen $f(u_1, \ldots, u_n)$. Husk at $f^{\mathcal{M}'}$ er en funksjon fra $|\mathcal{M}'|^n$ til $|\mathcal{M}'|$. Vi må derfor spesifisere et element $e \in |\mathcal{M}'|$ som verdi for $f^{\mathcal{M}'}$ for alle elementer $\langle a_1, \ldots, a_n \rangle \in |\mathcal{M}'|^n$. Termen $f(u_1, \ldots, u_n)$ inneholder imidlertid frie variable, så vi må bruke variabeltilordninger for å kunne tolke den. For en variabeltilordning μ' for $\mathcal{M}'$ har vi at

$$\mu'(u_1), \ldots, \mu'(u_n) = a_1, \ldots, a_n,$$

der $\mu'(u_i) = a_i \in |\mathcal{M}'|$ for $1 \leq i \leq n$, altså et element i $|\mathcal{M}'|^n$. En annen variabeltilordning kan gi et annet element i $|\mathcal{M}'|^n$. Vi må derfor spesifisere tolkningen $f(u_1, \ldots, u_n)^{\mathcal{M}', \mu'}$ for hver variabeltilordning μ' for $\mathcal{M}'$. For $\mathsf{L}\exists$ med hovedformel $\exists x \varphi$ gjøres det på følgende måte:

- Anta at $\langle u_1, \ldots, u_n \rangle^{\mu'} = \langle a_1, \ldots, a_n \rangle$.
- Hvis $\exists x \varphi$ er sann i $\mathcal{M}$ under[4] μ', så finnes en $e \in |\mathcal{M}|$ slik at $\varphi[\bar{e}/x]$ er sann i $\mathcal{M}$ under μ'. Siden $|\mathcal{M}|$ og $|\mathcal{M}'|$ er like, så er e også med i $|\mathcal{M}'|$. La $f^{\mathcal{M}}(a_1, \ldots, a_n) = e$.
- Hvis $\exists x \varphi$ er usann i $\mathcal{M}$ under μ', la $f^{\mathcal{M}}(a_1, \ldots, a_n) = d$ for et vilkårlig element $d \in |\mathcal{M}'|$.

For $\mathsf{R}\forall$ blir definisjonen tilsvarende, bortsett fra at vi i det andre punktet setter $f^{\mathcal{M}}(a_1, \ldots, a_n) = e$ hvis hovedformelen er *usann* i $\mathcal{M}$ under μ'. Vi må så vise at modellen $\mathcal{M}'$ falsifiserer π'. For $\mathsf{L}\exists$ kan beviset gjøres slik.

Bevis ($\mathcal{M}'$ falsifiserer π' når θ er $\mathsf{L}\exists$). La μ' være en vilkårlig variabeltilordning for $\mathcal{M}'$. Vi må vise at det finnes en gren i π' som er falsifisert av $\mathcal{M}'$ under μ'. La G og G' være definert på samme måte som i beviset for $\mathsf{L}\to$. Siden $\mathcal{M}$ og $\mathcal{M}'$ er like bortsett fra tolkingen av f, *og siden f ikke forekommer i* π, så vil $\mathcal{M}$ og $\mathcal{M}'$ tolke alle symboler i π på samme måte. Siden $\mathcal{M}$ falsifiserer π, så vil også $\mathcal{M}'$ falsifisere π. Det finnes derfor en gren i π som er falsifisert av $\mathcal{M}'$ under μ'. Vi har to tilfeller:

[4]Siden $\mathcal{M}$ og $\mathcal{M}'$ har det samme domenet, så er alle variabeltilordninger for $\mathcal{M}$ også variabeltilordninger for $\mathcal{M}'$ og vice versa.

- Den falsifiserte grenen er en annen enn G.
- Den falsifiserte grenen er G.

I tilfelle (1) har vi at den falsifiserte grenen i π også er en gren i π', og vi er i mål. Anta derfor at vi har tilfelle (2), dvs. at G er falsifisert av $\mathcal{M}'$ under μ'. Vi må vise at G' er falsifisert av $\mathcal{M}'$ under μ'. □

Oppgave 11.3 Fullfør argumentet i beviset over. (Hint: Argumentet går tilsvarende som for $\mathsf{L}\rightarrow$ ved å bruke semantikken. Bruk definisjonen av $\mathcal{M}'$ sin tolkning av f for å komme i mål.)

Oppgave 11.4 Gjør induksjonssteget i beviset for falsifiserbarhetslemmaet for LK-regelen $\mathsf{R}\forall$.

Det er flere måter å definere δ-reglene på enn den vi har gitt over, men ikke alle er sunne. Se på følgene alternative definisjoner:

(II)
- f er ny for *utledningen*
- $\vec{u} = u_1, \ldots, u_n$ er de variablene som forekommer fritt i *konklusjonen*

(III)
- f er ny for *konklusjonen*
- $\vec{u} = u_1, \ldots, u_n$ er de variablene som forekommer fritt i *hovedformelen*

Oppgave 11.5 Hvilke av alternativene (II) og (III) er *sunne*? Hvis definisjonen er sunn, forklar hvorfor. Hvis ikke, finn et *moteksempel*, dvs. en utledning med falsifiserbar rotsekvent som kan lukkes hvis man bruker den alternative δ-regelen. (Hint: Se på beviset for $\mathsf{L}\exists$ over. Her bruker vi at f *ikke forekommer i* π til å "fiske fram" en falsifisert gren i π'. Vil dette by på problemer med (II) eller (III)?)

Vi skal til slutt se på en variant av δ-regelen der vi tillater en viss gjenbruk av Skolemsymboler.

Definisjon 11.3.1 (Funksjonen sko)**.** *La sko være en funksjon som tar en δ-formel som argument og returnerer en Skolemfunksjon. For to δ-formler φ og ψ så har vi at $sko(\varphi) = sko(\psi)$ hvis og bare hvis $\varphi = \psi$.*

Vi definerer δ-regelen som følger.

(IV)
- $f = \text{sko}(\psi)$ der ψ er hovedformelen
- $\vec{u} = u_1, \ldots, u_n$ er de variablene som forekommer fritt i *hovedformelen*

Vi vil nå få at like δ-formler i forskjellige grener introduserer det samme Skolemsymbolet. Se på følgende eksempel (der vi ikke viser γ-kopiene).

$$\dfrac{\dfrac{\dfrac{Pu \vdash Pa, \forall xQx}{Pu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall \qquad \dfrac{\dfrac{Qu \vdash Pa, Qb}{Qu \vdash \forall xPx, Qb}\,\mathsf{R}\forall}{Qu \vdash \forall xPx, \forall xQx}\,\mathsf{R}\forall}{Pu \vee Qu \vdash \forall xPx, \forall xQx}\,\mathsf{L}\vee}{\forall x(Px \vee Qx) \vdash \forall xPx, \forall xQx}\,\mathsf{L}\forall$$

Vi ser her at den øverste $\mathsf{R}\forall$-slutningen i høyre gren introduserer den *samme* Skolemkonstanten som $\mathsf{R}\forall$-slutningen i venstre gren, siden hovedformlene i de to slutningene er *like*. Sammenligner vi den nederste

R∀-slutningen i høyre gren med R∀-slutningen i venstre gren ser vi at de introduserte Skolemkonstantene er *ulike*, siden hovedformlene er *ulike*.

Oppgave 11.6 Er definisjon (IV) av δ-reglene *sunn*? Hvorfor/hvorfor ikke? (Hint: I definisjon (IV) legger vi en begrensning på gjenbruken av Skolemsymboler i forhold til definisjon (III). Hvordan påvirker dette sunnhetsbeviset? Kan vi bruke en egenskap ved funksjonen sko til å få sunnhetsbeviset til å gå gjennom?)

Definisjon 11.3.2 (Funksjonen sko*)**.** *La sko* være en funksjon fra δ-formler til Skolemsymboler slik at for to δ-formler φ og ψ så har vi sko$^*(\varphi) =$ sko$^*(\psi)$ hvis og bare hvis φ og ψ er like* opp til omdøping av frie og bundne variable.

Med omdøping av frie variable mener vi at vi kan endre navn på en eller flere bundne variable. Hvis vi f.eks. omdøper x til z i formelen (1) $\exists xPxy$ får vi formelen $\exists zPzy$. På samme måte kan vi omdøpe frie variable. Hvis vi omdøper y til z i formelen (1) over, så får vi formelen $\exists xPxz$. Vi krever imidlertid at ingen frie variable skal bli bundet som følge av en slik variabelomdøping. For formelen (1) over er derfor ikke en omdøping av x til y tillat, siden vi da får formelen $\exists yPyy$, som semantisk sett er *ulik* formelen vi startet med.

To formler φ og ψ defineres som like opp til omdøping av frie og bundne variable hvis vi kan omdøpe variablene i φ på en slik måte at resultatformelen blir syntaktisk lik ψ (eller tilsvarende, hvis vi kan omdøpe variablene ψ slik at resultatet blir syntaktisk likt φ). Formlene $\exists xPxy$ og $\exists yPyx$ er like opp til omdøping av frie og bundne variable, mens formlene $\exists xPxy$ og $\exists xPxx$ *ikke* er det.

Vi definerer så en variant av δ-betingelsen (IV) som følger.

(V)
- $f =$ sko$^*(\psi)$ der ψ er hovedformelen
- $\vec{u} = u_1, \ldots, u_n$ er de variablene som forekommer fritt i *hovedformelen*

Oppgave 11.7 Er definisjon (V) av δ-reglene *sunn*? Hvorfor/hvorfor ikke?

Forelesning 12: Automatisk bevissøk IV – matriser og koblingskalkyle

Bjarne Holen - 28. april 2008

12.1 Automatisk bevissøk IV

12.1.1 Introduksjon

Bevissøk med koblinger

- Vi har til nå sett på forskjellige varianter av sekventkalkyle:
  - LK for *klassisk utsagnslogikk*,
  - LJ for *intuisjonistisk utsagnslogikk*,
  - ensidig sekventkalkyle,
  - grunn LK og
  - fri-variabel LK for *klassisk førsteordens logikk*.
- Alle disse kalkylene har to svakheter når de skal implementeres med en automatisk søkealgoritme:
  - *Redundans* – gjennom formelkopiering kan vi få mange forekomster av én og samme formel.
  - *Ingen relevanssjekk* – siden det kun tas hensyn til toppkonnektiv ved formelanalyse kan vi risikere å utvide formler som ikke er relevante for å lukke utledningen.
- Vi skal i denne forelesningen se på koblingskalkylen, som ikke har disse problemene.

Redundans i LK-utledninger

$$\dfrac{\dfrac{\dfrac{}{Q_2 \to R_1, P_2 \vdash R_2, P_1}\times}{Q_2 \to R_1 \vdash P_1, P_2 \to R_2} \qquad \dfrac{\dfrac{}{Q_1 \vdash Q_2, P_2 \to R_2}\times \qquad \dfrac{\dfrac{}{Q_1, R_1, P_2 \vdash R_2}\times}{Q_1, R_1 \vdash P_2 \to R_2}}{Q_2 \to R_1, Q_1 \vdash P_2 \to R_2}}{P_1 \to Q_1, Q_2 \to R_1 \vdash P_2 \to R_2}$$

- I rotsekventen forekommer både P, Q og R to ganger. Vi bruker $_1$ og $_2$ til å skille forekomstene fra hverandre.
- Siden P_2 og P_1 i venstre løvsekvent er forekomster av P, kan vi lukke med disse. Tilsvarende for de andre løvsekventene.
- En LK-utledning kan inneholde mange kopier av en (del)formel i rotsekventen. I utledningen over: 3 kopier av $Q_2 \to R_1$, 4 kopier av $P_2 \to R_2$, 2 kopier av P_1, 6 kopier av P_2, osv.
- Vi har derfor *redundans* i LK-utledninger.

Ingen relevanssjekk

$$\dfrac{\overset{\times}{(Q \to R) \vee (R \to Q), P \vdash P} \qquad \overset{\times}{(Q \to R) \vee (R \to Q), P \vdash P}}{(Q \to R) \vee (R \to Q), P \vee P \vdash P}$$

- I rotsekventen over er det to muligheter for utvidelse: $(Q \to R) \vee (R \to Q)$ eller $P \vee P$
  - Hvis vi velger $(Q \to R) \vee (R \to Q)$, vil vi gjøre (en eller flere) utvidelser som ikke bidrar til å lukke løvsekventene.
  - Velger vi derimot $P \vee P$, vil vi kunne lukke direkte.
- Det er de *atomære delformlene* til en formel som er med på å lukke løvsekventene.
- I sekventkalkyle ser vi imidlertid kun på *toppkonnektivene* for å velge hvilken formel vi skal utvide.
- Vi kan derfor risikere å utvide formler som er *irrelevante* m.h.p. å lukke utledningen.

Matriser og koblingskalkyle

- Bevisbarhet av en formel kan defineres som en egenskap ved formelen direkte, istedenfor via utledninger som i sekventkalkyle.
  - Vi kan representere en formel todimensjonalt ved en *matrise* bestående av de atomære delformlene.
  - Gyldighet defineres så som en egenskap ved stiene gjennom matrisen.
  - Hver sti må inneholde et komplementært par av atomer – kalt en *kobling*.
- *Koblingskalkyle* er basert på matrisekarakteristikken av gyldighet og utnytter at samme kobling kan forekomme på flere stier gjennom en matrise.
- Vi skal begrense oss til å se på koblingskalkyle for utsagnslogikk i disjunktiv normalform.
- Koblingskalkyle er imidlertid ikke begrenset til normalform, og finnes for mange forskjellige logikker – inkludert de vi har sett på i kurset.

12.1.2 Matriser

Disjunktiv normalform

- I ukeoppgavene har vi sett på normalformer.
- En *literal* er en atomær formel eller negasjonen av en atomær formel:
  - $P, Q, R, \ldots$ er *positive* literaler og $\neg P, \neg Q, \neg R, \ldots$ er *negative* literaler.
- En *generalisert konjunksjon* er en formel på formen $(\varphi_1 \wedge \ldots \wedge \varphi_n)$ der hver φ_i er en formel.
- En *generalisert disjunksjon* er en formel på formen $(\varphi_1 \vee \ldots \vee \varphi_n)$ der hver φ_i er en formel.

Definisjon 12.1.1 (Disjunktiv normalform)**.** *En formel er på* disjunktiv normalform *(DNF) hvis den er en (generalisert) disjunksjon av en eller flere (generaliserte) konjunksjoner av en eller flere literaler.*

Disjunktiv normalform

Hvilke formler er på DNF?

- P $\surd$
- $P \vee Q$ $\surd$
- $(P \vee Q) \wedge R$ Nei, venstre konjunkt er en disjunksjon.
- $(\neg P \wedge Q) \vee (\neg Q \wedge P)$ $\surd$
- $(P \rightarrow Q) \vee Q \vee \neg P$ Nei, venstre konjunkt er en implikasjon.
- $(\neg P \wedge Q) \vee R \vee (\neg R \wedge P) \vee (\neg P \wedge Q \wedge \neg R)$ $\surd$
- $\neg P \wedge Q \wedge \neg R$ $\surd$
- Enhver literal er på DNF.
- Enhver disjunksjon av literaler er på DNF.
- Enhver konjunksjon av literaler er på DNF.

Transformasjon til DNF

- Vi har i ukeoppgavene sett at enhver utsagnslogisk formel kan transformeres til en *ekvivalent* formel på DNF.
- Husk: to formler er *ekvivalente* hvis de oppfylles av nøyaktig de samme valuasjonene/modellene.
- Eksempel:

$$\begin{aligned}(P \wedge (P \rightarrow Q)) \rightarrow Q &\Leftrightarrow \neg(P \wedge (P \rightarrow Q)) \vee Q \\ &\Leftrightarrow \neg P \vee \neg(P \rightarrow Q) \vee Q \\ &\Leftrightarrow \neg P \vee \neg(\neg P \vee Q) \vee Q \\ &\Leftrightarrow \neg P \vee (\neg\neg P \wedge \neg Q) \vee Q \\ &\Leftrightarrow \neg P \vee (P \wedge \neg Q) \vee Q\end{aligned}$$

Transformasjon fra DNF til KNF

- Vi har sett at alle DNF formler kan transformeres til *ekvivalente* KNF formler ved gjentagende bruk av

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

- Hva er problemet med en slik transformasjon?
- Hvorfor vil vi ha formler på KNF?

$$\begin{aligned}(P \wedge (P \rightarrow Q)) \rightarrow Q &\Leftrightarrow \neg P \vee (P \wedge \neg Q) \vee Q \\ &\Leftrightarrow (\neg P \vee (P \wedge \neg Q)) \vee Q \\ &\Leftrightarrow ((\neg P \vee P) \wedge (\neg P \vee \neg Q)) \vee Q \\ &\Leftrightarrow ((\neg P \vee P) \vee Q) \wedge ((\neg P \vee \neg Q) \vee Q) \\ &\Leftrightarrow (\neg P \vee P \vee Q) \wedge (\neg P \vee \neg Q \vee Q)\end{aligned}$$

- Falsifikasjon av 1 klausul falsifiserer formelen

Sammenheng mellom DNF og KNF

- Enkelt å konvertere formel til DNF
- Vi er mest interessert i KNF
- Finnes det en enkel måte å få KNF fra DNF representasjon?
- Anta at vi har en formel på DNF

$$(A_1 \wedge A_2 \ldots \wedge A_n) \vee (B_1 \wedge B_2 \ldots \wedge B_m) \cdots \vee (P_1 \wedge P_2 \ldots \wedge P_s)$$

- Ved gjentatte anvendelser av regelen

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

- ser vi at klausulene i KNF representasjonen blir slik

$$(A_i \vee B_j \ldots \vee P_k)$$

$$1 < i < n \quad 1 < j < m \quad \ldots \quad 1 < k < s$$

- Merk at KNF klausulene får 1 element fra hver DNF klausul!

Overblikk over Matrise-søk

- For å vise at en sekvent er gyldig

$$P, (P \rightarrow Q) \vdash Q$$

- Bytt ut meta-symbol med objekt-symbol

$$(P \wedge (P \rightarrow Q)) \rightarrow Q$$

- Konverter til DNF

$$\neg P \vee (P \wedge \neg Q) \vee Q$$

- Elementene i DNF klausulene utgjør søylene i matrisen

$$\left|\begin{array}{ccc} & P & Q \\ \neg P & \neg Q & \end{array}\right|$$

Overblikk over Matrise-søk

- Vi har sett at ved å plukke 1 element fra hver DNF klausul
- (søylene i matrisen) får vi KNF klausulene.
- Dersom enhver KNF klausul har en kobling (¬ A, A)
- vil matrisen representere enn IKKE-falsifiserbar formel (gyldig)

- En matrise er en kompakt representasjon av formelen
- Vi bruker denne til å søke igjennom alle KNF klausuler
- Vi søker målrettet og leter etter koblinger

Definisjon 12.1.2 (Matrise)**.**

- *En* klausul *er en endelig mengde literaler. (metasymbol , $:= \wedge$)*
- *En* matrise *er en endelig mengde klausuler. (metasymbol , $:= \vee$)*

Eksempel (klausuler):

- $\{P\}$
- $\{P, \neg P, Q\}$
- $\{\neg Q, R, P\}$
- $\{\}$

Eksempel (matriser):

- $\{\{P\}, \{\neg P\}\}$
- $\{\{Q\}, \{\neg P, R\}, \{\neg R, P, \neg Q\}\}$
- $\{\}$
- $\{\{\}\}$

- En klausul er
  - *positiv* hvis den bare inneholder positive literaler, og
  - *negativ* hvis den bare inneholder negative literaler.

Definisjon 12.1.3 (Semantikk for matriser)**.** *La v være en boolsk valuasjon.*

- *For klausuler: $v \models \{L_1, \ldots, L_n\}$ hvis og bare hvis $v \models L_i$ for alle L_i.*
- *For matriser: $v \models \{K_1, \ldots, K_n\}$ hvis og bare hvis $v \models K_i$ for en K_i.*

Eksempel. *La v være slik at $v \models P$, $v \not\models Q$ og $v \models R$.*

- $v \models \{\{P\}, \{\neg P\}\}$*?* $\surd$
- $v \models \{\{Q\}, \{\neg P, R\}, \{\neg R, P, \neg Q\}\}$*?* *Nei, v oppfyller ingen klausuler.*
- $v \models \{\}$ *der* $\{\}$ *er en tom matrise?* *Nei, v oppfyller ingen klausuler i* $\{\}$*.*
- $v \models \{\{\}\}$ *(matrisen som kun inneholder en tom klausul)?* $\surd$
  ($v \models \{\} \in \{\{\}\}$ siden alle valuasjon oppfyller en tom klausul.)

Falsifiserbarhet av matriser

v	$M = \{K_1, \ldots, K_n\}$	$K = \{L_1, \ldots, L_m\}$
oppfyller	$v \models K_i$ for *en* K_i	$v \models L_i$ for *alle* L_i
falsifiserer	$v \not\models K_i$ for *alle* K_i	$v \not\models L_i$ for *en* L_i

- En boolsk valuasjon v *falsifiserer*
  - en klausul i M hvis v falsifiserer en av literalene i klausulen
  - alle klausulene i M hvis v falsifiserer en literal i hver klausul
- For hver klausul K_i har vi $|K_i|$ valg av literaler å falsifisere.
- Vi får maksimalt $|K_1| \times \ldots \times |K_n|$ måter å falsifisere M på.

DNF-formler som matriser

- En formel på DNF kan sees på som en matrise der klausulene tilsvarer disjunktene i formelen.
- Eksempel: formelen
$$\neg P \vee (P \wedge \neg Q) \vee Q$$
tilsvarer matrisen
$$\{\{\neg P\}, \{P, \neg Q\}, \{Q\}\}$$
tilsvarer KNF representasjonen
$$(\neg P \vee P \vee Q) \wedge (\neg P \vee \neg Q \vee Q)$$

Stier

Definisjon 12.1.4 (Sti)**.** *La M være en matrise.*

- *En sti gjennom M er en mengde som inneholder nøyaktig én literal fra hver klausul i M.*
- *En sti gjennom M er partiell hvis den mangler literaler fra én eller flere klausuler i M.*

Eksempel.

	P	Q
$\neg P$	$\neg Q$	

- *Stier: $\{\neg P, P, Q\}$ og $\{\neg P, \neg Q, Q\}$.*
- *Partieller stier: $\{\neg P\}$, $\{\neg P, P\}$, $\{\neg P, \neg Q\}$, $\{P\}$, $\{P, Q\}$, $\{Q\}$, $\{Q, \neg Q\}$ og $\{Q, \neg P\}$.*

Hver sti gjennom en matrise representerer en mulig falsifikasjon!

Koblinger

Definisjon 12.1.5 (Koblinger)**.** *La M være en matrise. En kobling i M er en partiell sti gjennom M på formen $\{A, \neg A\}$ der A er en atomær formel.*

Eksempel.

	P	Q
$\neg P$	$\neg Q$	

- *Koblinger: $\{\neg P, P\}$ og $\{\neg Q, Q\}$.*
- *Vi markerer sammenkoblede literaler med en bue i den grafiske matrisenotasjonen.*

Åpne og lukkede stier

- En kobling $\{P, \neg P\}$ er *ikke* falsifiserbar:
  - en boolsk valuasjon kan ikke falsifisere både P og $\neg P$ samtidig!
- Derfor vil en sti som inneholder en kobling, *ikke* være falsifiserbar.
- Dersom alle stiene gjennom en matrise inneholder en kobling, vil matrisen ikke være falsifiserbar – og dermed må formelen den representerer være gyldig.
- Vi sier at en (partiell) sti i en matrise er
  - *åpen* hvis den *ikke* inneholder noen kobling, og
  - *lukket* hvis den inneholder en kobling.

Matriser vs. LK-utledninger

- Stiene gjennom matrisen til en formel F tilsvarer løvsekventene vi får hvis vi gjør en *maksimal* LK-utledning for sekventen $\vdash F$:
  - Negative literaler er antecedentformler, og
  - positive literaler er succedentformler.

$$\left|\begin{array}{ccc} & P & Q \\ \neg P & \neg Q & \end{array}\right|$$

$$\dfrac{\dfrac{P \vdash P, Q \qquad \dfrac{P, Q \vdash Q}{P \vdash \neg Q, Q}}{P \vdash P \wedge \neg Q, Q}}{\vdash \neg P, P \wedge \neg Q, Q}$$

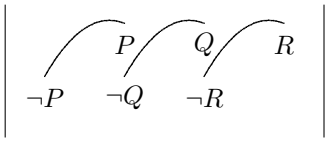
- Lukkede stier gjennom matriser tilsvarer aksiomer i LK-utledninger.

Matrisekarakterisering av gyldighet

Teorem 12.1.1. *En formel F på DNF er gyldig hvis og bare hvis enhver sti gjennom matrisen til F inneholder en kobling.*

Eksempel.

- *Formelen $(P \wedge (P \to Q) \wedge (Q \to R)) \to R$ er gyldig.*
- *På DNF får vi formelen $\neg P \vee (P \wedge \neg Q) \vee (Q \wedge \neg R) \vee R$.*



Koblinger: $\{\neg P, P\}$, $\{\neg Q, Q\}$ *og* $\{\neg R, R\}$.

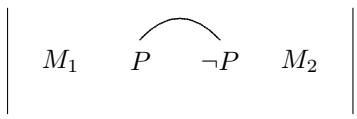
Stier: $\{\neg P, P, Q, R\}$, $\{\neg P, P, \neg R, R\}$, $\{\neg P, \neg Q, Q, R\}$ *og* $\{\neg P, \neg Q, \neg R, R\}$.

- *Alle stiene inneholder en kobling.*

12.1.3 Koblingskalkyle

- Matrisekarakteriseringen av gyldighet gir oss muligheten til å avgjøre bevisbarhet ved å sjekke at alle stier inneholder en kobling.
- En første tilnærming vil være å liste opp alle stiene gjennom en matrise og sjekke hver av dem for koblinger.
- Det er imidlertid slik at én kobling kan forekomme på flere stier gjennom en matrise.

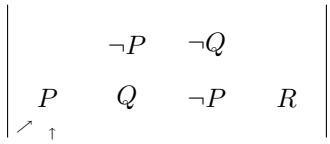
Eksempel.



Uansett hvordan M_1 og M_2 ser ut vil enhver sti gå gjennom koblingen $\{P, \neg P\}$.

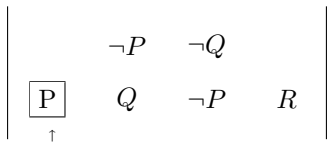
- Det er derfor en god idé å fokusere på koblinger istedenfor stier.
- Vi skal vise grunnidéene i koblingskalkylen ved et eksempel.

Startsteget



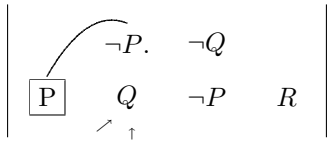
- Vi starter med å velge en *startklausul*.
- Vi velger $\{P\}$ og markerer denne med ↑ under klausulen, og markerer alle literalene i startklausulen med ↗.

Utvidelsessteget I



- Vi kaller klausulen som er markert med ↑, for *aktiv klausul*.
- Hvis en literal i aktiv klausul er markert med ↗ må vi sjekke alle stier som inneholder literalen.
- I dette tilfellet har vi bare ett valg: P.
- Vi markerer P med en ramme for å indikere at literalen er en del av den stien vi for øyeblikket undersøker – den *aktive stien*.
- Samtidig fjerner vi ↗-symbolet fra P.

Utvidelsessteget II



- Vi utvider den aktive stien ved å koble P med en komplementær literal i en av de andre klausulene.
- Vi har tre valg: $\{\neg P, Q\}$, $\{\neg Q, \neg P\}$ og $\{R\}$
- Vi velger den første klausulen og markerer de sammenkoblede literalene med en bue.
- Alle stier som springer ut fra den sammenkoblede $\neg P$ vil være lukkede på grunn av koblingen $\{P, \neg P\}$. Dette markeres med '.' etter $\neg P$.
- Den sammenkoblede klausulen settes aktiv og de resterende literalene på den markeres med ↗.

Utvidelsessteget – oppsummering

↑ markerer aktiv klausul
. markerer lukkede partielle stier
[L] markerer literaler på den aktive stien
↗ markerer literaler i åpne partielle stier

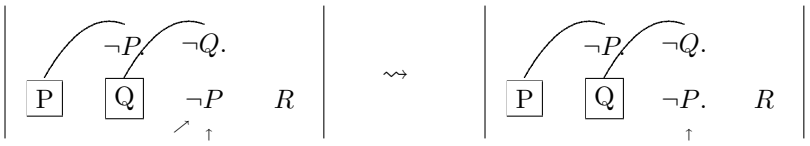
1. Velg en literal L markert med ↗ i den aktive klausulen.
2. Bytt ut ↗ med en boks rundt L. Velg en L-kobling.
   - Hvis det er flere alternativer, ta vare på dem.
3. Marker den koblede literalen med '.'
4. Marker de resterende literalene i den koblede klausulen med ↗.
5. Flytt ↑ til den sammenkoblede klausulen.

Vi foretar nok et utvidelsessteg

↑ markerer aktiv klausul
. markerer lukkede partielle stier
[L] markerer literaler på den aktive stien
↗ markerer literaler i åpne partielle stier

1. Vi velger literalen Q i den aktive klausulen.
2. Vi bytter ut ↗ med en boks rundt Q. Vi har bare ett alternativ til kobling: $\neg Q$.
3. Markerer den koblede literalen med '.'
4. Markerer de resterende literalene i den koblede klausulen med ↗.
5. Flytt ↑ til den sammenkoblede klausulen.

Reduksjonssteget

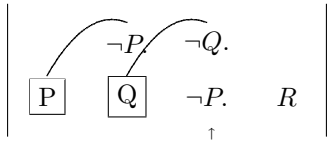


↑ markerer aktiv klausul
. markerer lukkede partielle stier
$\boxed{L}$ markerer literaler på den aktive stien
↗ markerer literaler i åpne partielle stier

- I situasjonen til venstre finnes det ingen literaler å koble $\neg P$ med.
- Det finnes imidlertid en komplementær literal i den aktive stien: P.
- Vi kan derfor foreta et *reduksjonssteg*:

1. Blant literalene som er merket med ↗ i den aktive klausulen, velg en L som er komplementær med en literal på den aktive stien.
2. Fjern ↗ fra L og marker den med '.'

Fullført søk – suksess

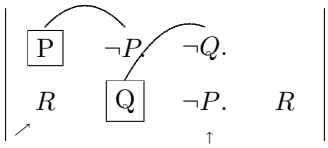


- I situasjonen over er alle literaler i aktiv klausul markert med '.', dvs. at alle stier som fortsetter ut fra denne klausulen inneholder koblinger.
- I tillegg er ingen literaler i klausuler på den aktive stien merket med ↗, dvs. at vi ikke har noen partielle åpne stier igjen å sjekke.
- Tilstanden er et vitne på at søket er *fullført med suksess* – alle stier gjennom matrisen inneholder koblinger.

Kalkyle vs. søkealgoritme

- Koblingskalkylen består av reglene *start*, *utvidelse* og *reduksjon*.
- Reglene definerer et sett *stisjekkingstilstander*.
- I tillegg har vi en beskrivelse av hvilke tilstander som representerer *suksess* i stisjekkingen.
- En søkealgoritme for koblingskalkylen må spesifisere en *rekkefølge* å gjøre reglene i.
- Vi skal nøye oss med å presentere noen viktige poenger m.h.p. implementasjon av en søkealgoritme.
- Til slutt skal vi ta en titt på en Prolog-implementasjon av koblingskalkylen.

Sjekke alle åpne partielle stier



- Vi ser på suksesstilstanden med matrisen fra eksempelet, men legger til R i første klausul. Den nye matrisen inneholder flere stier uten koblinger, f.eks. $\{R, Q, \neg P, R\}$.
- Tilstanden over er *ikke* en suksesstilstand, siden vi har en partiell åpen sti: den nye literalen R er merket med $\nearrow$.
- Vi må gå tilbake og se hva som skjer hvis vi velger R som del av den aktive stien istedenfor P i venstre klausul.
- Vi får en låst tilstand, siden R ikke kan kobles med noen literaler i matrisen.
- Vi må altså sjekke alle åpne partielle stier (literaler merket med $\nearrow$) før vi kan konludere med suksess.

Implementasjon i Prolog – leanCoP

```
prove(Mat) :-
  append(MatA,[Cla|MatB],Mat), append(MatA,MatB,Mat1),
  \+member(-_,Cla), prove(Cla,Mat1,[]).
prove([],_,_).
prove([Lit|Cla],Mat,Path) :-
  (-NegLit=Lit;-NegLit\=Lit,-Lit=NegLit),
   ( member(NegLit,Path); append(MatA,[Cla1|MatB],Mat),
     append(MatA,MatB,Mat1), append(ClaA,[NegLit|ClaB],Cla1),
     append(ClaA,ClaB,Cla3), prove(Cla3,Mat1,[Lit|Path])
   ), prove(Cla,Mat,Path).
```

- leanCoP er en elegant Prolog-implementasjon av koblingskalkylen for klassisk logikk i normalform.
- Utviklet av Jens Otten ved Universitetet i Potsdam utenfor Berlin.
- Utnytter Prologs innebygde unifikasjon og backtracking.
- For mer info: `http://www.leancop.de/`

Forelesning 13: Resolusjon

Martin Giese - 5. mai 2008

13.1 Resolusjonskalkyle

Foilene jeg viste i forelesningen var hentet fra

http://www.uni-koblenz.de/~beckert/Lehre/Logik/

Bildet av semantiske trær er i foilene til forelesning 13.

Kompletthetsbeviset med semantiske trær kan leses (i veldig kompakt form) på:

http://en.wikibooks.org/wiki/Logic_for_Computer_Scientists/Predicate_Logic/Resolution

13.2 Oppgaver

Oppgave 13.1 Vis at en formel F på DNF er gyldig hvis og bare hvis enhver sti gjennom matrisen til F inneholder en kobling.

Oppgave 13.2 Vis at en matrise for en gyldig formel inneholder minst én positiv og minst én negativ klausul.

Forelesning 14: Modallogikk og Beskrivelseslogikk

Martin Giese - 19. mai 2008

14.1 Modallogikk

Foilene var igjen hentet fra Berhard Beckert sine web sider, forelesning 6

http://www.uni-koblenz.de/~beckert/Lehre/Nicht-klassische-Logiken/

En masse om modallogikk kan leses her:

http://plato.stanford.edu/entries/logic-modal/

14.2 Beskrivelseslogikk

Det står litt i Wikipedia:

http://en.wikipedia.org/wiki/Description_logic

Register