INF3170 – Forelesning 4

Sunnhet og kompletthet

- 16. februar 2010

(Sist oppdatert: 2010-02-09 17:43)

Dagens plan

Innhold

Sunnhet

Introduksjon

Sunnhet av LK

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

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

Teorem.
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.

Bevaring av falsifiserbarhet

Definisjon.
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.
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$\rightarrow$-slutninger bevarer falsifiserbarhet.

Bevis (Bevis for R$\neg$).
¡2-¿

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

- Anta at v falsifiserer konklusjonen.
- Det betyr at $v \models \Gamma$, $v \not\models \neg A$ og v *falsifiserer alle formlene i* Δ.
- Per 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 (Bevis for L$\rightarrow$).

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

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

Eksistens av falsifiserbar løvsekvent

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

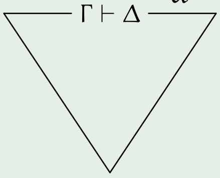
Bevis.
Ved strukturell induksjon på LK-utledningen δ.
Basissteg: δ er en sekvent $\Gamma \vdash \Delta$:

$$\Gamma \vdash \Delta$$

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

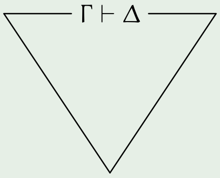
$$\frac{\Gamma' \vdash \Delta'}{\Gamma \vdash \Delta}\ \alpha$$



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

$$\dfrac{\Gamma' \vdash \Delta' \qquad \Gamma'' \vdash \Delta''}{\Gamma \vdash \Delta}\,\beta$$



- 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.

Alle aksiomer er gyldige

Lemma.
Alle aksiomer er gyldige.

Bevis.
¡2-¿

$$\Gamma, A \vdash A, \Delta$$

- 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.

Bevis for sunnhetsteoremet

Bevis (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.

Kompletthet

Introduksjon

Definisjon.
¡+-¿[Sunnhet] Sekventkalkylen LK er *sunn* hvis enhver LK-bevisbar sekvent er gyldig.

Definisjon.
¡+-¿[Kompletthet] Sekventkalkylen LK er *komplett* hvis enhver gyldig sekvent er LK-bevisbar.

Gyldighet
(semantisk)
Universell påstand:
"for alle valuasjoner..."

$\xleftarrow{\text{sunnhet}}$

$\xrightarrow{\text{kompletthet}}$

Bevisbarhet
(syntaktisk)
Eksistensiell påstand:
"det fins et bevis..."

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 ...

Kompletthetsteoremet

Teorem (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 (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.

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
$G^\bot$ 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 $G^\bot$) usanne.

Eksempel

$$\dfrac{\dfrac{\dfrac{\overset{\times}{P \vdash Q, P} \quad \overset{\times}{Q, P \vdash Q}}{P \to Q, P \vdash Q} \quad \dfrac{R \vdash Q, P \quad \overset{\times}{Q, R \vdash Q}}{P \to Q, R \vdash Q}}{P \to Q, P \lor R \vdash Q}}{P \to Q \vdash (P \lor R) \to Q}$$

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

$G^\top = \{R, P \to Q, P \lor R\}$
$G^\bot = \{Q, P, (P \lor R) \to Q\}$
$v =$ 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 $\neg A$, $(A \land B)$, $(A \lor B)$ og $(A \to B)$. 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 $(A \land B) \in G^\top$.

- 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 $v(A \land B) = 1$.

Anta at $(A \land B) \in G^\perp$.

- 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 $v(A \land B) = 0$.

Anta at $(A \to B) \in G^\top$.

- 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 $v(A \to B) = 0$.

Egenskaper ved utsagnslogikk

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^i_j 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: $P^1_1 \lor P^1_2$.
  - Objekt 3 ligger i en av boksene: $P^3_1 \lor P^3_2$.
  - Boks 1 inneholder både objekt 1 og 2: $P^1_1 \land P^2_1$.
  - Boks 2 inneholder både objekt 1 og 3: $P^1_2 \land P^3_2$.

Avgjørbarhet

Teorem.
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.

Kompleksitet

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

Teorem.
Gyldighetsproblemet for utsagnslogikk er coNP-komplett.

Repetisjon

Motivasjon

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

- Er utsagnene *sanne*?
- Avhengig av hvordan vi *tolker* utsagnene!
- Finnes det utsagn som alltid er sanne?

- Vi ønsker å en måte å finne slike utsagn på!
- Vi ønsker *matematisk presisjon*, så vi må *formalisere* utsagn og tolkninger.

Formalisering

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

Syntaks: Utsagnslogiske formler

Alfabet

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

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

Induktiv definisjon – stegvis bygge opp en uendelig mengde

Mengden av utsagnslogiske formler – $\mathcal{F}_u$
Basismengde: Enhver utsagnsvariabel er en utsagnslogisk formel.
Induksjonssteg: Hvis A og B er utsagnslogiske formler, så er

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

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

Semantikk: Tolke utsagn – valuasjoner

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

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

Oppfylle og falsifisere

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

Sekventer og sekventkalkyle

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

Innledning til førsteordens logikk

Introduksjon

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

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

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

Flere eksempler
Av mindre matematisk art:

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

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.

Syntaks – språk og termer

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

- De logiske konnektivene $\land$, $\lor$, $\to$ 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 (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 (Signatur).

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

Definisjon (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.

Eksempler på førsteordens språk

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

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

Termer i dette språket:

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

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

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

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

Kommentarer:

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

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

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

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

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

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

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

Termer i språket for familierelasjoner:

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

Syntaks

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

Merk.

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

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

1. Alle atomære formler er formler.
2. Hvis φ og ψ er formler, så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ 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.

Eksempler på førsteordens formler

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

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

Formler i språket:

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

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

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

Førsteordens logikk - syntaks

Repetisjon og presiseringer

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

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

- De ikke-logiske symbolene utgjør en *signatur*

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

Vi så følgende signaturer sist:

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

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

1. Mengden $\mathcal{T}$ av termer i $\mathcal{L}$:
    - Enhver variabel og konstant er en term.
    - Hvis f er et funksjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer,så er $f(t_1, ..., t_n)$ en term.
2. Mengden $\mathcal{F}$ av formler i $\mathcal{L}$:
    - Hvis R er et relasjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer,så er $R(t_1, \ldots, t_n)$ en (atomær) formel.
    - Hvis φ og ψ er formler,så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \rightarrow \psi)$ formler.
    - Hvis φ er en formel og x er en variabel,så er $\forall x\varphi$ og $\exists x\varphi$ formler.

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

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

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

Frie variable i termer

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

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

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

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

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 (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.