Repetisjonsforelesning

INF3170

Andreas Nakkerud

Institutt for informatikk

24. november 2014

Institutt for informatikk

Universitetet i Oslo

Utsagnslogikk

Utsagnslogikk (eng: Propositional Logic) er en av de enkleste logikkene.

Utsagnslogikk brukes til å beskrive enkle utsagn som er enten sanne eller usanne.

Definisjon (Utsagn)

Et utsagn (eng: proposition) er en setning som er enten sann eller usann.

Eksempel (Utsagn)

"Solen står opp", "klokken er 4" og "jeg liker epler" er alle utsagn.
"Hvor gammel er du?" og "god morgen" er ikke utsagn slik vi har har definert ordet.

Syntaks

Definisjon (Utsagnsvariabel)

En utsagnsvariabel (eng:propositional variable) er et symbol, typisk $P, Q, R, \ldots$, som står for et utsagn.

Vi definerer mengden av utsagnslogiske formler induktivt.

Definisjon (Utsagnslogisk formel)

Mengden M av utsagnslogiske formler (eng: propositional formulas) er den minste mengden slik at

1. *M innholder alle utsagnsvariable.*
2. *Dersom $F, G \in M$, da er $\neg F, (F \wedge G), (F \vee G), (F \rightarrow G) \in M$.*

Utsagnsvariablene kalles de atomære (eng: atomic) formlene.

Utsagnslogiske formler

Eksempel (Utsagnslogiske formler)

Følgende er utsagnslogiske formler:

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

Følgende er ikke utsagnslogiske formler (etter definisjonen):

$$P \vee Q$$
$$(P$$
$$\neg \wedge Q$$

Vi kommer tilbake til $P \vee Q$ senere.

Semantikk

En utsagnslogisk formel er enten sann eller usann. Vi bruker ofte verdiene 1 (sann) og 0 (usann), men vi kan også bruke "SANN" og "USANN", eller $\top$ og $\perp$. Det vesentlige er at vi har to verdier.

Sannhetsverdien til en formel, hvorvidt den er sann eller ikke, avgjøres av sannhetsverdiene til de utsagnsvariablene som inngår i formelen.

Eksempel (Sannhetsverdier)

Vi lar P være "SANN" og Q være "USANN". Da er det naturlig at $P \vee Q$ er "SANN", mens $P \wedge Q$ er "USANN".

I eksempelet skriver vi at *P er* "SANN". Dette er ikke helt presist. Det er *sannhetsverdien* til P som er "SANN".

Valuasjoner

En valuasjon er en (rekursiv) funksjon som tilordner sannhetsverdier til utsagnslogiske formler.

Definisjon (Valuasjon)

En valuasjon (eng: valuation) v er en funksjon, slik at $v(P)$ er enten 0 eller 1 for alle utsagnsvariable. For alle andre utsagnslogiske formler er v definert som følger:

$$v(\neg F) = \begin{cases} 1, & \textit{hvis } v(F) = 0 \\ 0, & \textit{ellers.} \end{cases}$$

$$v(F \wedge G) = \begin{cases} 1, & \textit{hvis } v(F) = 1 \textit{ og } v(G) = 1 \\ 0, & \textit{ellers.} \end{cases}$$

$$v(F \vee G) = v(\neg[\neg F \wedge \neg G])$$

$$v(F \rightarrow G) = v(\neg F \vee G)$$

Valuasjoner

Når vi bruker utsagnslogikk til å beskrive noe, må vi huske på at valuasjoner bestemmer betydningen av utsagnslogiske formler.

$P \to Q$ betyr ikke at Q inntraff som en konsekvens av P, men at Q er sann hver gang P er det.

Sannhetsverditabeller er nyttige verktøy for å studere formler.

P	Q	$P \to Q$
1	1	1
1	0	0
0	1	1
0	0	1

Parenteser

Vi har tidligere sagt at $P \vee Q$ ikke er en formel, fordi den ikke kan genereres av den induktive definisjonen av formler. Vi utvider nå mengden av utsagnslogiske formler til å innholde formler der par av overflødige parenteser er fjernet.

Siden $P \wedge (Q \wedge R)$ er det samme som $(P \wedge Q) \wedge R$ tillater vi å skrive $P \wedge Q \wedge R$. Vi bestemmer oss også for følgende prioritering av konnektiver:

$$\begin{array}{c} \neg \\ \wedge \\ \vee \\ \to . \end{array}$$

Dette betyr at $\neg P \wedge Q$ er forskjellig fra $\neg(P \wedge Q)$. Og at $P \wedge Q \to R$ er det samme som $(P \wedge Q) \to R$.

Sekventkalkyle (LK) for utsagnslogikk

Definisjon (Sekvent)

En sekvent (eng: sequent) er en konstruksjon på formen

$$\Gamma \vdash \Delta,$$

hvor Γ *og* Δ *er multimengder med formler. Vi skriver ofte* Γ, F *for* $\Gamma \cup \{F\}$ *hvis vi ønsker å fremheve et element i en av multimengdene.*

Definisjon (Aksiom)

Et aksiom (eng: axiom) er en sekvent på formen

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

hvor A *er en atomær formel.*

Syntaks

Definisjon (Regler)

En regel (eng: rule) definerer en overgang fra en sekvent til en annen. Regler skrives som

$$\frac{\Gamma'_1 \vdash \Delta'_1 \qquad \dots \qquad \Gamma'_n \vdash \Delta'_n}{\Gamma \vdash \Delta}$$

hvor $\Gamma'_i \vdash \Delta'_i$ *er premissene og* $\Gamma \vdash \Delta$ *konklusjonen.*

Negasjon

Definisjon (Negasjonregler)

Vi definerer følgende regler for negasjon:

$$\frac{\Gamma, F \vdash \Delta}{\Gamma \vdash \neg F, \Delta}\ R\neg$$

og

$$\frac{\Gamma \vdash F, \Delta}{\Gamma, \neg F \vdash \Delta}\ L\neg$$

Semantikk

Definisjon

En sekvent $\Gamma \vdash \Delta$ *er gyldig (eng: valid) hvis alle valuasjoner som gjør alle formlene i* Γ *sanne, gjør minst én formel i* Δ *sann.*
En sekvent er falsifiserbar (eng: falsifiable) hvis den ikke er gyldig.

Når vi definerer regler ønsker vi at de bevarer falsifiserbarhet oppover, og dermed også gyldighet nedover. Med dette mener vi at konklusjonen må være gyldig hvis alle premissene er gyldige, eller at minst ett premiss er falsifiserbart hvis konklusjonen er falsifiserbar.

Eksempel

Hvis $\Gamma, F \vdash \Delta$ *er gyldig må alle valuasjoner som oppfyller* Γ, F *oppfylle minst én formel i* Δ. *Da vil enhver valuasjon som oppfyller* Γ *enten oppfylle* $\neg F$, *eller minst én formel i* Δ, *så* $\Gamma \vdash \neg F, \Delta$ *er gyldig.*

Konjunksjon

Definisjon (Konjunksjonsregler)

Vi definerer følgende regler for konjunksjon:

$$\frac{\Gamma \vdash F, \Delta \qquad \Gamma \vdash G, \Delta}{\Gamma \vdash F \wedge G, \Delta} \; R\wedge$$

og

$$\frac{\Gamma, F, G \vdash \Delta}{\Gamma, F \wedge G \vdash \Delta} \; L\wedge$$

Disjunksjon

Definisjon (Disjunksjonsregler)

Vi definerer følgende regler for disjunksjon:

$$\frac{\Gamma \vdash F, G, \Delta}{\Gamma \vdash F \vee G, \Delta} \; R\vee$$

og

$$\frac{\Gamma, F \vdash \Delta \qquad \Gamma, G \vdash \Delta}{\Gamma, F \vee G \vdash \Delta} \; L\vee$$

Implikasjon

Definisjon (Implikasjonsregler)

Vi definerer følgende regler for implikasjon:

$$\frac{\Gamma, F \vdash G, \Delta}{\Gamma \vdash F \to G, \Delta} \; R\to$$

og

$$\frac{\Gamma \vdash F, \Delta \qquad \Gamma, G \vdash \Delta}{\Gamma, F \to G \vdash \Delta} \; L\to$$

Syntaks

Definisjon (Utledning)

En utledning for en sekvent $\Gamma \vdash \Delta$, er et tre med $\Gamma \vdash \Delta$ som rot. Vi bygger treet som følger:

1. *Start med $\Gamma \vdash \Delta$ som rot og eneste løvnode.*
2. *Velg en løvnode, og velg så en ikke-atomær formel i Γ eller Δ. Velge den reglen som passer toppnivåkonnektivet i den valgte formlen. Den valgte løvnoden er konklusjonen i den valgte reglen, og er ikke lenger en løvnode i treet. Premissene i den valgte reglen er de nye løvnodene.*
3. *Gjenta 2 eller avslutt.*

Syntaks

Eksempel (Utledning)

Vi lager en utledning for sekventen $(P \to Q) \to R \vdash (P \land Q) \to R$*:*

$$\cfrac{\cfrac{\cfrac{\cfrac{P, Q, P \vdash Q, R}{P, Q \vdash P \to Q, R}\; R\to \qquad R, P, Q \vdash R}{(P \to Q) \to R, P, Q \vdash R}\; L\to}{(P \to Q) \to R, P \land Q \vdash R}\; L\land}{(P \to Q) \to R \vdash (P \land Q) \to R}\; R\to$$

Definisjon (Bevis)

Et bevis (eng: proof) er en utledning der alle løvnodene er aksiomer.

Semantikk

Definisjon (Sunnhet)

Sekventkalkylen er sunn (eng: sound) hvis enhver bevisbar formel er gyldig.

Definisjon (Kompletthet)

Sekventkalkylen er komplett (eng: complete) hvis enver gyldig formel er bevisbar.

Dersom vi har en kalkyle som er både sunn og komplett kan vi se på gyldighet og bevisbarhet som to sider av samme sak.

Sunnhet

Lemma

Aksiomer $\Gamma, A \vdash A, \Delta$ *er gyldige sekventer.*

Bevis: En valuasjon som gjør alle formlene i $\Gamma \cup \{A\}$ sanne må gjøre A sann. Dermed er minst én formel i $\Delta \cup \{A\}$ sann i denne valuasjonen.

Lemma

Alle reglene vi har innført bevarer falsifiserbarhet oppover.

Bevis: Gjøres separat for hver regel.

Sunnhet

Lemma

En utledning med falsifiserbar rot har minst én falsifiserbar løvnode.

Bevis: Ved strukturell induksjon på mengden av utledninger. Induksjonssteger følger fra forrige lemma.

Teorem

Sekventkalkylen er sunn.

Bevis: Anta for motsigelse at vi har et bevis for en falsifiserbar sekvent. Siden roten av beviset er falsifiserbar må det finnes minst én falsifiserbar løvnode, men dette er ikke mulig, da bevis kun har aksiomer som løvnoder, og alle aksiomer er gyldige.

Kompletthet

Lemma

En valuasjon som falsifiserer et av premissene i en regel vi falsifisere konklusjonen.

Bevis: Gjøres separat for hver regel.

Lemma

En sekvent som ikke er bevisbar vil i en maksimal utledning (en utledning der alle konnektiver fjernes) ha minst én løvnode som bare innholder atomære formler, men ikke er et aksiom.

Bevis: Det er lett å se at vi kan lage en maksimal utledning, vi bare anvender reglene til det ikke er flere konnektiver. Siden rotsekventen ikke er bevisbar må vi ende med en løvnode som ikke er et aksiom, ellers ville utledningen være et bevis.

Lemma

En løvsekvent som kun innholder atomære formler, men som ikke er et aksiom, er falsifiserbar.

Bevis: Løvsekventen har formen $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$, der $A_i \neq B_j$ for alle i, j. Valuasjonen som setter $v(A_i) = 1$ og $v(B_j) = 0$ falsifiserer sekventen.

Teorem

Sekventkalkylen er komplett.

Bevis: Merk at rotsekventen i en utledning falsifiseres av alle valuasjoner som falsifiserer en av løvsekventene i utledningen. Anta for motsigelse at sekventkalkylen ikke er komplett. Da finnes det en gyldig sekvent som ikke er bevisbar. Siden formlen ikke er bevisbar må den ha en maksimal utledning der ikke alle løvsekventene er aksiomer. Vi bruker en av de ikke-aksiomatiske løvsekventene til å lage en valuasjon som falsifiserer rotsekventen. Da kan ikke rotsekventen være gyldig.

Førsteordens logikk: mengder og relasjoner

En modell $\mathcal{M}$ er en forenklet beskrivelse av virkeligheten. Uformelt kan vi definere en modell til å være en mengde, og en samling relasjoner og funksjoner over denne mengden. For eksempel kan vi ha

$$\begin{aligned} \mathit{Univers} &= \{\text{Anne}, \text{Frode}, \text{Lise}, \text{Peter}\} \\ \mathit{Barn} &= \{\text{Lise}, \text{Peter}\} \\ \mathit{ErFarTil} &= \{\langle \text{Frode}, \text{Lise} \rangle, \langle \text{Frode}, \text{Peter} \rangle\} \\ \mathit{ErMorTil} &= \{\langle \text{Anne}, \text{Lise} \rangle, \langle \text{Anne}, \text{Peter} \rangle\} \end{aligned}$$

Modellen vår ($\mathcal{M}$) består av en mengde med alle tingene modellen beskriver (*Univers*), og noen relasjoner over denne mengden (*Barn*, *ErFarTil* og *ErMorTil*).

Språk og signaturer

Vi definerer nå et språk for å beskrive modellen $\mathcal{M}$. I språket kan vi bruke konnektivene ($\neg$,$\wedge$,$\vee$,$\rightarrow$) fra utsagnslogikk, men i stedet for utsagnsvariable lager vi nye atomære formler.

De atomære formlene er bygget opp fra en signatur. Signaturen innholder symboler for alle tingene i modellen $\mathcal{M}$. For Anne, Frode, Lise og Peter lager vi symbolene a, f, l og p. For relasjonen *Barn* lager vi symbolet B, og for *ErFarTil* og *ErMorTil*, symbolene F og M.

For å si at Lise er et *Barn*, kan vi nå skrive $B(l)$. For å si at Anne er mor til Peter kan vi skrive $M(a, p)$. Vi kan også skrive disse kortere som Bl og Map hvis det ikke er tvetydig.

Signatur

Definisjon (Signatur)

En signatur (eng: signature) er et tuppel

$$\langle a, b, c, \ldots; f, g, h, \ldots; R, S, T, \ldots \rangle$$

hvor $a, b, c, \ldots$ er konstantsymboler, $f, g, h, \ldots$ er funksjonssymboler, og $R, S, T, \ldots$ er relasjonssymboler. Funksjons- or relasjonssymbolene har aritet (eng: arity) bestemt av funksjonen $aritet(X)$.

I vårt løpende eksempel har vi signaturen

$$\langle a, f, l, p; ; B, F, M \rangle,$$

hvor $aritet(B) = 1$ og $aritet(F) = aritet(M) = 2$.

Førsteordens termer

Definisjon (Term)

Gitt en signatur

$$\langle a_1, a_2, a_3, \ldots; f_1, f_2, f_3, \ldots; R_1, R_2, R_3, \ldots \rangle$$

og en uendelig mengde variabelsymboler $x_1, x_2, x_3, \ldots$*, kan vi definere termer (eng: terms)*

1. a_i *og* x_j *er termer for alle* i *og* j*, og*
2. *hvis* f_i *er et funksjonssymbol med aritet* n *og* $t_1, \ldots, t_n$ *er termer, så er* $f_i(t_1, \ldots, t_n)$ *en term.*

En lukket term (eng: ground term) en en term uten variabelsymboler.

Førsteordens formler

Definisjon (Førsteordens formel)

La R være et relasjonssymbol med aritet n, og $t_1, \dots, t_n$ termer. Da er $R(t_1, \dots, t_n)$ en atomær førsteordens formel.
Hvis F og G er formler, og x en variabel, da er $\neg F$, $F \wedge G$, $F \vee G$, $F \rightarrow G$, $\forall x F$ og $\exists x F$ førsteordens formler.

$\forall x$ og $\exists x$ er kvantorer som binder variablen x.

Frie variable

Definisjon (Frie variable)

Vi definerer mengden $\mathit{free}(\phi)$ *av frie variable i formelen* ϕ*:*

- $\mathit{free}(\phi)$ *er mengden av alle variabler i* ϕ *hvis* ϕ *er atomær,*
- $\mathit{free}(\neg\phi) = \mathit{free}(\phi)$,
- $\mathit{free}(\phi \land \psi) = \mathit{free}(\phi \lor \psi) = \mathit{free}(\phi \to \psi) = \mathit{free}(\phi) \cup \mathit{free}(\psi)$
- $\mathit{free}(\forall x\phi) = \mathit{free}(\exists x\phi) = \mathit{free}(\phi) \setminus \{x\}$

Skopet (eng: scope) til kvantorene i formlene $\forall x\phi$ og $\exists x\phi$ er ϕ. Hvis x er en fri variabel i ϕ, er de frie forekomstene av x i ϕ de forekomstene som ikke er i skopet til en kvantor som binder x.

Hvis x er en fri variabel i ϕ og t en term, da er ϕ^t_x formelen ϕ der alle frie forekomster av x er byttet ut med t.

En setning (eng: sentence) er en formel uten frie variable.

Semantikk

Vi tolker konnektivene $\neg, \wedge, \vee, \rightarrow$ på samme måte som for utsagnslogiske formler, men vi bruker modeller til å avgjøre sannhetsveridene til atomære formler. Vi jobber videre med modellen:

$$\begin{aligned} \mathit{Univers} &= \{\text{Anne}, \text{Frode}, \text{Lise}, \text{Peter}\} \\ \mathit{formynder} &= \{\langle \text{Anne}, \text{Anne}\rangle, \langle \text{Frode}, \text{Frode}\rangle, \\ &\qquad\qquad \langle \text{Lise}, \text{Anne}\rangle, \langle \text{Peter}, \text{Anne}\rangle\} \\ \mathit{Barn} &= \{\text{Lise}, \text{Peter}\} \\ \mathit{ErFarTil} &= \{\langle \text{Frode}, \text{Lise}\rangle, \langle \text{Frode}, \text{Peter}\rangle\} \\ \mathit{ErMorTil} &= \{\langle \text{Anne}, \text{Lise}\rangle, \langle \text{Anne}, \text{Peter}\rangle\} \end{aligned}$$

Vi tolker formler over signaturen

$$\langle a, f, l, p; f; B, F, M\rangle.$$

Modeller

Definisjon (Modell)

En modell $\mathcal{M}$ *er en ikke-tom mengde* $|\mathcal{M}|$, *kalt domenet eller universet til modellen, og en funksjon* $(\cdot)^{\mathcal{M}}$, *slik at*

- $c^{\mathcal{M}} \in |\mathcal{M}|$ *for konstantsymboler* c,
- $f^{\mathcal{M}}$ *er en funksjon* $f : |\mathcal{M}|^n \to |\mathcal{M}|$ *for funksjonssymboler* f *med aritet* n, *og*
- $R^{\mathcal{M}} \subseteq |\mathcal{M}|^n$ *for relasjonssymboler* R *med aritet* n.

Definisjon (Atomære formler i modeller)

En atomær formel $R(t_1, \ldots, t_n)$ *er sann i modellen* $\mathcal{M}$ *dersom*

$$\langle t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}} \rangle \in R^{\mathcal{M}}.$$

Vi sier at $\mathcal{M}$ *modellerer* $R(t_1, \ldots, t_n)$ *og skriver* $\mathcal{M} \models R(t_1, \ldots, t_n)$.

Modeller

Definisjon (Kvantorer i modeller)

La $\mathcal{M}$ *være en modell og* ϕ *en førsteordens formel, da har vi at*

- $\mathcal{M} \models \exists x \phi$ *hvis det finnes en lukket term* t *slik at* $\mathcal{M} \models \phi^t_x$*, og*
- $\mathcal{M} \models \forall x \phi$ *hvis* $\mathcal{M} \models \phi^t_x$ *for alle lukkede termer* t*.*

Definisjon (Utsagnskonnektiver i modeller)

La F *og* G *være førsteordens formler, da har vi at*

- $\mathcal{M} \models \neg F$ *hvis og bare hvis* $\mathcal{M} \not\models F$*,*
- $\mathcal{M} \models F \land G$ *hvis og bare hvis* $\mathcal{M} \models F$ *og* $\mathcal{M} \models G$*,*
- $\mathcal{M} \models F \lor G$ *hvis og bare hvis* $\mathcal{M} \models F$ *eller* $\mathcal{M} \models G$*, og*
- $\mathcal{M} \models F \to G$ *hvis og bare hvis* $\mathcal{M} \not\models F$ *eller* $\mathcal{M} \models G$*.*

Eksempel: Modeller

Gitt signaturen $\langle a, f, l, p; f; B, F, M \rangle$ definerer vi modellen

$$
\begin{aligned}
|\mathcal{M}| &= \mathit{Univers} & a^{\mathcal{M}} &= \text{Anne} \\
f^{\mathcal{M}} &= \text{Frode} & l^{\mathcal{M}} &= \text{Lise} \\
p^{\mathcal{M}} &= \text{Peter} & f^{\mathcal{M}} &= \mathit{formynder} \\
B^{\mathcal{M}} &= \mathit{Barn} & F^{\mathcal{M}} &= \mathit{ErFarTil} \\
M^{\mathcal{M}} &= \mathit{ErMorTil}
\end{aligned}
$$

I denne modellen er det ikke sant at alle har en mor, men det er sant at alle barn har en mor, så

$$\mathcal{M} \not\models \forall x \exists y Mxy \qquad \mathcal{M} \models \forall x\,(Bx \rightarrow \exists y Mxy)$$

Sannhet og gyldighet

Om en formel er *sann* eller *usann* avhenger av hvordan vi tolker den. Sannhet er en egenskap som beksriver samspillet mellom en modell og en formel. Vi kan ikke si at en formel er sann eller usann uten å referere til en modell.

Eksempel

Formelen $M(f(l), l)$ *er sann i* $\mathcal{M}$*, fordi* $\mathcal{M} \models M(f(l), l)$

En formel er gyldig hvis den er sann i alle modeller.

Eksempel

Formelen $\forall x P(x) \rightarrow \exists x P(x)$ *er gyldig.*

Sekventkalkyle for førsteordens logikk

Sekventkalkyle for førsteordens logikk er en utvidelse av sekventkalkyle for utsagnslogikk.

Vi må legge til regler for eksistens- og allkvantor, og vi må vise sunnhet og kompletthet for den utvidede kalkylen. Sunnhet generaliserer enkelt.

Eksistenskvantor

Definisjon (Regler for eksistenskvantor)

Vi definerer følgende regler for eksistenskvantor:

$$\frac{\Gamma \vdash \Delta, \exists x \phi, \phi^t_x}{\Gamma \vdash \Delta, \exists x \phi} \; R\exists$$

hvor t er en lukket term, og

$$\frac{\Gamma, \phi^a_x \vdash \Delta}{\Gamma, \exists x \phi \vdash \Delta} \; L\exists$$

hvor a er en parameter som ikke forekommer i konklusjonen.

Allkvantor

Definisjon (Regler for allkvantor)

Vi definerer følgende regler for allkvantor:

$$\frac{\Gamma \vdash \Delta, \phi^a_x}{\Gamma \vdash \Delta, \forall x \phi} \; R\forall$$

hvor a er en parameter som ikke forekommer i konklusjonen, og

$$\frac{\Gamma, \forall x \phi, \phi^t_x \vdash \Delta}{\Gamma, \forall x \phi \vdash \Delta} \; L\forall$$

hvor t er en lukket term.

Sunnhet

Vi må beviset at

Lemma

Alle reglene vi har innført bevarer falsifiserbarhet oppover.

holder også for de nye reglene.

Kompletthet

Vi viser den kontrapositive påstanden: at en sekvent som ikke er bevisbar heller ikke er gyldig.

Teorem (Modelleksistens)

Enhver konsistent mengde formler har en modell.