Forelesning 3: Utsagnslogikk – sekventkalkyle, sunnhet og kompletthet

Christian Mahesh Hansen - 5. februar 2007

1 Sekventkalkyle

1.1 Semantikk for sekventer

Semantikk for sekventer

Definisjon 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 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:* $v(P) = \mathbf{1}$, $v(Q) = \mathbf{0}$
- $P \lor Q \vdash P \land Q$ — *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!*

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

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

Falsifiserbar

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

Ikke bevisbar

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

2 Sunnhet

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

Teorem 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.

2.2 Bevaring av falsifiserbarhet

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

- Anta at v falsifiserer konklusjonen.
- Det betyr at $v \models \Gamma$, $v \not\models \neg A$ og v *falsifiserer alle formlene i* Δ.
- 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→. $$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \mathsf{L}{\to}$$

- 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.

2.3 Eksistens av falsifiserbar løvsekvent

Lemma 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.

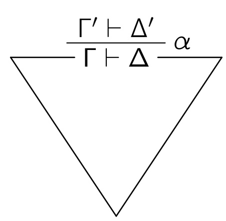
Basissteg: δ er en sekvent $\Gamma \vdash \Delta$:

$$\Gamma \vdash \Delta$$

- 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 $\Gamma \vdash \Delta$.

□

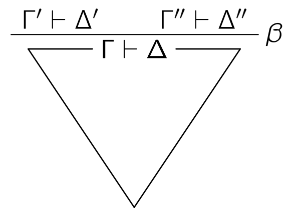
Bevis (induksjonssteg – α-utvidelse). *Induksjonssteg:* δ er en utledning på formen



- 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.

$\square$

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.

$\square$

2.4 Alle aksiomer er gyldige

Lemma 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.

$\square$

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 Kompletthet

3.1 Introduksjon

Definisjon 3.1 (Sunnhet)**.** *Sekventkalkylen* LK *er sunn hvis enhver* LK*-bevisbar sekvent er gyldig.*

Definisjon 3.2 (Kompletthet)**.** *Sekventkalkylen* LK *er* komplett *hvis enhver gyldig sekvent er* LK*-bevisbar.*

$$\xleftarrow{\text{sunnhet}}$$

Gyldighet (semantisk) Universell påstand: "for alle valuasjoner..."		**Bevisbarhet** (syntaktisk) Eksistensiell påstand: "det fins et bevis..."

$$\xrightarrow{\text{kompletthet}}$$

Sunnhet:	$\Gamma \vdash \Delta$ bevisbar	:	$\Gamma \vdash \Delta$ gyldig
Kompletthet:	$\Gamma \vdash \Delta$ gyldig	:	$\Gamma \vdash \Delta$ 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	:	$\Gamma \vdash \Delta$ ikke bevisbar
Kompletthet:	$\Gamma \vdash \Delta$ ikke bevisbar	:	$\Gamma \vdash \Delta$ 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 ...

3.2 Kompletthetsteoremet

Teorem 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 3.1 (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 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

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

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

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

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

$v =$ 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 $(A \to B)$. 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 $(A \wedge B) \in G^\top$.

- 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 $(A \to B) \in G^{\top}$.

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

4 Egenskaper ved utsagnslogikk

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: $P_2^1 \wedge P_2^3$.

4.2 Avgjørbarhet

Teorem 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.

4.3 Kompleksitet

Teorem 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 4.3. *Gyldighetsproblemet for utsagnslogikk er coNP-komplett.*