INF3170 – Logikk

Forelesning 2: Induktive definisjoner, utsagnslogikk og sekventkalkyle

Christian Mahesh Hansen

Institutt for informatikk, Universitetet i Oslo

29. januar 2007

Dagens plan

Induktive definisjoner

Definisjon (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 b*0 *og b*1 *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: $aaaa$ $abba$ $baab$ $bbbb$
$\vdots$

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.

Syntaks

Definisjon (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 (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 (Atomær formel)

Enhver utsagnsvariabel er en atomær formel.

Definisjon (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:

$(P \rightarrow Q)$	*skrives*	$P \rightarrow Q$
$((P \vee Q) \wedge \neg(P \vee R))$	*skrives*	$(P \vee Q) \wedge \neg(P \vee R)$

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

Alle utsagnslogiske formler har like mange venstre- og høyreparenteser.

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 (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 (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

$((Q \wedge P)$ *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.

□

Semantikk

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

Definisjon

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

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

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

Definisjon (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 (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 (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 (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

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*

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

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.

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

Eksempel

- 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!

Sekventkalkylen LK

Definisjon (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 (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?

Sekventkalkyleregler

Definisjon (α-regler)

α-reglene i sekventkalkylen LK *er:*

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

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

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

α-reglene kalles ofte ett-premissregler.

Definisjon (β-regler)

β-reglene i sekventkalkylen LK *er:*

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

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

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

β-reglene kalles ofte to-premissregler.

Definisjon (Slutningsreglene i LK)

Slutningsreglene i sekventkalkylen LK *er α- og β-reglene.*

Begreper knyttet til regler

Se på regelen

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

- 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.

Regler vs. slutninger

Definisjon (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 $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\,\mathrm{R}\neg$ *definerer uendelig mange* R$\neg$*-slutninger:*

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

Begrepene knyttet til regler anvendes om slutninger:

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

- 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.

Utledninger

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

Definisjon (Mengden av LK-utledninger – basistilfelle)

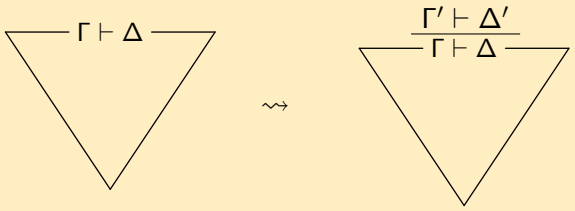
En sekvent $\Gamma \vdash \Delta$ er en LK-utledning.

$$\Gamma \vdash \Delta$$

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

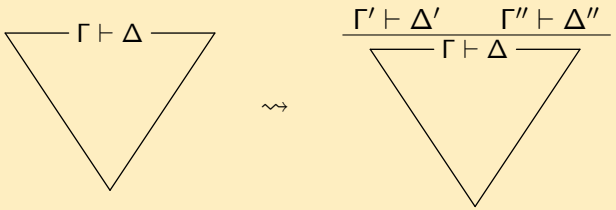
Definisjon (Mengden av LK-utledninger – α-utvidelse)

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 (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)

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

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

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

LK-bevis

Definisjon (LK-bevis)

Et LK*-bevis er en* LK*-utledning der alle løvsekventene er aksiomer.*

Definisjon (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)

$$\frac{\overset{\times}{P \vdash P}}{\vdash P \to P}\,\mathrm{R}\to$$

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

- *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.