

Forelesning 2: Induktive definisjoner, utsagnslogikk og sekventkalkyle

Christian Mahesh Hansen - 29. januar 2007

1 Induktive definisjoner

Induktive definisjoner

Definisjon 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 Utsagnslogikk

2.1 Introduksjon

Utsagnslogikk

Studie av de *utsagnslogiske konnektivene*.

- Vi starter med en mengde *atomære* utsagn, f.eks.
 - “*parkeringsplassen er stengt*”
 - “*IF12 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: “*IF12 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: “*IF12 bygges eller IF12 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 Syntaks

Syntaks

Definisjon 2.1 (Utsagnsvariable). Mengden av *utsagnsvariable* er en tellbart uendelig mengde $\mathcal{V}_u = \{P_1, P_2, P_3, \dots\}$.

- Utsagnsvariable representerer *atomære utsagn*, f.eks.
 - “*IF12 bygges*”

- "Forskningsparken er yngre enn IF1"
- "logikk er gøy"

Notasjon. Vi skriver ofte utsagnsvariable som P, Q, R, \dots

For å fange inn sammensatte utsagn, f.eks.

"hvis IF12 bygges, så er parkeringsplassen stengt,"

trengs flere symboler i språket:

Definisjon 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 2.3 (Atomær formel). Enhver utsagnsvariabel er en **atomær formel**.

Definisjon 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:

$(P \rightarrow Q)$ 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 2.1. Alle utsagnslogiske formler har like mange venstre- og høyreparenteser.

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 2.1 (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 (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 2.3. $((Q \wedge P)$ 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.

□

2.4 Semantikk

Semantikk

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

Definisjon 2.5. La $\mathbf{Bool} = \{1, 0\}$.

Definisjon 2.6 (Operatorene \neg , \wedge , \vee og \rightarrow).

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

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$
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 2.7 (Boolsk valuasjon). En *boolsk valuasjon* er en funksjon v fra \mathcal{F}_u til \mathbf{Bool} slik at:

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

Merk.

- Symbolene \neg , \wedge , \vee og \rightarrow på venstresiden er de utsagnslogiske konnektivene, som er en del av syntaksen.

- Symbolene $\hat{\wedge}$, $\hat{\vee}$ og $\hat{\rightarrow}$ på høyresiden er operatører 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:

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

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

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

Definisjon 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 $\neg(P \rightarrow P)$?
- Og $P \rightarrow P$?

Definisjon 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 oppfylbar formel.
- En tautologi er ikke det motsatte av en motsigelse!

Påstand 2.4. En utsagnslogisk formel A er en tautologi hvis og bare hvis A ikke er falsifiserbar.

Bevis. formelen A er en tautologi $\Leftrightarrow \forall v \models A$ 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 $\rightarrow \Leftrightarrow$

Merk.

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

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

3 Sekventkalkyle

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.

$$\frac{\frac{\frac{\neg Q, P \vdash P}{\neg Q \vdash \neg P, P}}{\vdash P, \neg Q \rightarrow \neg P} \quad \frac{\frac{Q \vdash Q, \neg P}{Q, \neg Q \vdash \neg P}}{Q \vdash \neg Q \rightarrow \neg P}}{\frac{P \rightarrow Q \vdash \neg Q \rightarrow \neg P}{\vdash (P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)}}$$

Eksempel

- Falsifisere formelen $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$:

- oppfylle $P \rightarrow Q$,
- og falsifisere $\neg Q \rightarrow \neg P$.
- *Formler til venstre for '⊢' skal oppfylles.*
- *Formler til høyre for '⊢' skal falsifiseres.*
- Oppfylle $P \rightarrow Q$:
 - falsifisere P ,
 - eller oppfylle Q .
- $\neg Q \rightarrow \neg P$ må kunne falsifiseres uavhengig av hvordan $P \rightarrow Q$ oppfylles.
- Formelen kopieres derfor inn i begge de nye løvnodene.
- Falsifisere $\neg Q \rightarrow \neg P$ i venstre løvnode:
 - oppfylle $\neg Q$,
 - og falsifisere $\neg P$.
- Tilsvarende, falsifisere $\neg Q \rightarrow \neg P$ 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 !
- $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$ kan ikke falsifiseres!

Kommentarer til det foregående eksempelet:

- Vi arbeidet med objekter av typen ' $\dots \vdash \dots$ '. 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 sider av '⊢'. En utledning med denne egenskapen kalles et *bevis*.

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

3.2 Sekventer og aksiomer

Sekventkalkylen LK

Definisjon 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 '⊢' kalles *antecedent*.
- Formlene som står til høyre for '⊢' kalles *succedent*.

Notasjon. I sekventer leses ', ' som union:

- Γ, A skal bety $\Gamma \cup \{A\}$.

Eksempel. Hvilke av uttrykkene nedenfor er sekventer?

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

Definisjon 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?

3.3 Sekventkalkyleregler

Sekventkalkyleregler

Definisjon 3.3 (α -regler). α -reglene i sekventkalkylen LK er:

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} L\wedge \quad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} R\vee$$
$$\frac{\Gamma, A \vdash \quad B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} R\rightarrow$$
$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} L\neg \quad \frac{\Gamma, A \vdash \quad \Delta}{\Gamma \vdash \neg A, \Delta} R\neg$$

α -reglene kalles ofte *ett-premissregler*.

Definisjon 3.4 (β -regler). β -reglene i sekventkalkylen LK er:

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} R\wedge$$
$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} L\vee$$
$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta} L\rightarrow$$

β -reglene kalles ofte *to-premissregler*.

Definisjon 3.5 (Slutningsreglene i LK). *Slutningsreglene* i sekventkalkylen LK er α - og β -reglene.

Begreper knyttet til regler

Se på regelen

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

- 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*.

3.4 Slutninger

Regler vs. slutninger

Definisjon 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 $\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} R_{\neg}$ definerer uendelig mange R_{\neg} -slutninger:

$$\frac{P \vdash}{\vdash \neg P} \quad \frac{Q, P \vdash}{Q \vdash \neg P} \quad \frac{Q \rightarrow R, P \vdash P}{Q \rightarrow R \vdash \neg P, P} \quad \dots$$

Begrepene knyttet til regler anvendes om slutninger:

$$\frac{P \rightarrow Q, P \vdash Q \quad P \rightarrow Q, R \vdash Q}{P \rightarrow Q, P \vee R \vdash Q} LV$$

- 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**.

3.5 Utledninger

Utledninger

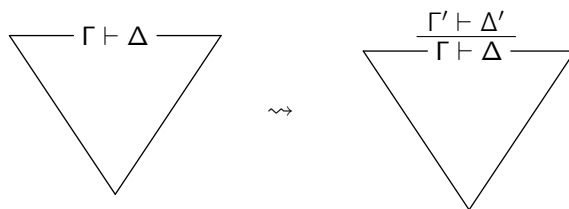
- En utledning er et tre der nodene er sekventer.
- Rotnoden er nederst og løvnodene er øverst.
- Rotnoden kalles **rotsekvent**.
- Løvnodene kalles **løvsekventer**.

Definisjon 3.7 (Mengden av LK-utledninger – basistilfelle). En sekvent $\Gamma \vdash \Delta$ er en **LK-utledning**.

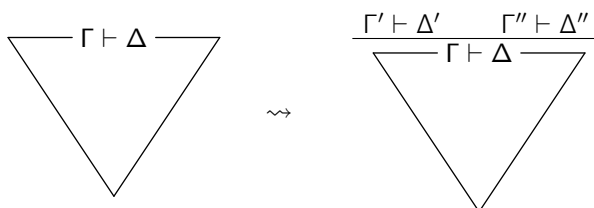
$$\Gamma \vdash \Delta$$

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

Definisjon 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 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).

$$\begin{array}{c} \vdash R \vee Q \qquad P \rightarrow Q \vdash \neg Q \rightarrow \neg P \\ \\ \frac{P \vdash Q}{\vdash P \rightarrow Q} R \rightarrow \qquad \frac{\vdash P \quad \vdash P}{\vdash P \wedge P} R \wedge \\ \\ \frac{\frac{P \vdash P \quad P \vdash Q}{P \vdash P \wedge Q} R \wedge \quad \frac{Q \vdash P \quad Q \vdash Q}{Q \vdash P \wedge Q} R \wedge}{P \vee Q \vdash P \wedge Q} LV \end{array}$$

3.6 Bevis

LK-bevis

Definisjon 3.10 (LK-bevis). Et LK-bevis er en LK-utledning der alle løvsekventene er aksiomer.

Definisjon 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).

$$\frac{\overset{\times}{P \vdash P}}{\vdash P \rightarrow P} R_{\rightarrow}$$

$$\frac{\frac{\frac{\overset{\times}{\neg Q, P \vdash P}}{\neg Q \vdash \neg P, P} R_{\neg}}{\vdash P, \neg Q \rightarrow \neg P} R_{\rightarrow}}{P \rightarrow Q \vdash \neg Q \rightarrow \neg P} R_{\rightarrow} \quad \frac{\frac{\frac{\overset{\times}{Q \vdash Q, \neg P}}{Q, \neg Q \vdash \neg P} L_{\neg}}{Q \vdash \neg Q \rightarrow \neg P} R_{\rightarrow}}{P \rightarrow Q \vdash \neg Q \rightarrow \neg P} L_{\rightarrow}}$$

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

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