

INF3170 – Logikk

Forelesning 1: Introduksjon. Utsagnslogikk og sekventkalkyle

Arild Waaler

Institutt for informatikk, Universitetet i Oslo

21. januar 2008



Dagens plan

- 1 Praktisk informasjon
- 2 Utsagnslogikk
- 3 Sekventkalkyle

- Forelesere:
 - Martin Giese (martingi@ifi.uio.no)
 - Arild Waaler (arild@ifi.uio.no)
 - Christian Mahesh Hansen (chrisha@ifi.uio.no)
 - Roger Antonsen (rantonse@ifi.uio.no)
 - Espen H. Lian (elian@ifi.uio.no)
 - Bjarne Holen (bjarneh@ifi.uio.no)
- Nettside:
 - <http://www.ifi.uio.no/inf4170>
- Forelesning:
 - Mandag 14:15 – 16:00
 - Seminarrom 3A Ifi
- Gruppeundervisning:
 - Onsdag 12:15 – 14:00, 3A, Ifi
 - Første gruppetime: onsdag 23. januar
 - Gruppelærer: Bjarne Holen (bjarneh@ifi.uio.no)

Obliger og eksamen

Obliger

- Planlagt 3 obliger.
- Se hjemmesiden for tidsfrister og regler.
- Bedømmes til bestått/ikke bestått.
- Alle obligene må bestås for å kunne gå opp til eksamen.

Eksamen

- Ingen midttermineksamen.
- Avsluttende eksamen: muntlig *eller* skriftlig.
- Bokstavkarakterer – avsluttende eksamen teller 100%

Pensum

- Definert av det som gjennomgås på forelesning og gruppeundervisning, samt obliger.
- Foiler deles ut på forelesning og legges ut på nettsiden.
- Ingen lærebok, men...

Støttelitteratur

Ikke pensum i seg selv, frivillig ekstraslesing!



J. Gallier.

Logic for Computer Science - Foundations of Automated Theorem Proving

- Ligger tett opptil forelest pensum i kurset.
- Oppdatert versjon fra 2003 tilgjengelig for gratis nedlasting.
- Kun kapitlene 3, 4, 5 og 8 er aktuelle.



M. C. Fitting.

First-Order Logic and Automated Theorem Proving

1 Praktisk informasjon

2 Utsagnslogikk

- Introduksjon
- Syntaks
- Strukturell induksjon
- Semantikk

3 Sekventkalkyle

Utsagnslogikk

- Grunnlaget for logikk er en antagelse om at gyldighet av argumenter avgjøres på bakgrunn av argumentets **form**, ikke **innhold**.
- Med et utsagn menes noe som enten er **sant** eller **usant**.
- Vi starter med en mengde **atomære** utsagn, f.eks.
 - "parkeringsplassen er stengt"
 - "IF12 bygges"
- Den interne strukturen til atomære utsagn blir ikke analysert.

- 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.

Syntaks

Definisjon (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 IF11*”
 - “*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 (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:

$$\begin{array}{ll} (P \rightarrow Q) & \text{skrives } P \rightarrow Q \\ ((P \vee Q) \wedge \neg(P \vee R)) & \text{skrives } (P \vee Q) \wedge \neg(P \vee R) \end{array}$$

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 **Q** hvis:

Basissteg: Alle atomære formler har egenskapen **Q**.

Induksjonssteg:

- Hvis A har egenskapen **Q**, så har også $\neg A$ egenskapen **Q**.
- Hvis A og B har egenskapen **Q**, så har også $(A \wedge B)$, $(A \vee B)$ og $(A \rightarrow B)$ egenskapen **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 $A \in \mathcal{F}_v$ 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 $\mathbf{Bool} = \{1, 0\}$.

Definisjon (Operatorene $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$ og $\hat{\rightarrow}$)

- Vi definerer en unær operator $\hat{\neg}$ på \mathbf{Bool} slik at $\hat{\neg}1 = 0$ og $\hat{\neg}0 = 1$.
- Vi definerer de binære operatorene $\hat{\vee}$, $\hat{\wedge}$ og $\hat{\rightarrow}$ på \mathbf{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}_i 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 $\neg P \rightarrow Q$.
- La v være en valuasjon slik at $v(P) = \mathbf{1}$ og $v(Q) = \mathbf{0}$.
- Vi får:

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

Definisjon (Oppfylldbar)

- En boolsk valuasjon v **oppfyller** en utsagnslogisk formel A hvis $v(A) = \mathbf{1}$. Skrives ofte $v \models A$.
- En utsagnslogisk formel er **oppfylldbar** hvis det finnes en boolsk valuasjon som oppfyller den.

Eksempel

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

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

1 Praktisk informasjon

2 Utsagnslogikk

3 Sekventkalkyle

- Motivasjon
- Sekventer og aksiomer
- Sekventkalkylereglene
- Slutninger
- Utledninger
- Bevis

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.

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

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 !
- $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$ 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 ' \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 '⊢' 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?

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

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:

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

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

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

α -reglene kalles ofte **ett-premissregler**.

Definisjon (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 (Slutningsreglene i LK)

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

Begreper knyttet til regler

Se på regelen

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

- 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 $\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} R_{\neg}$ 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:

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

- 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**.

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)

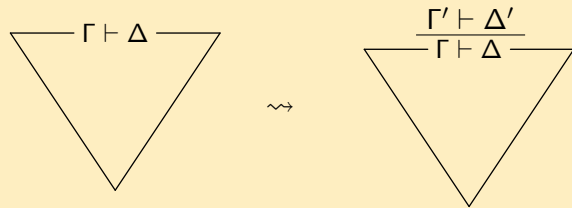
En sekvent $\Gamma \vdash \Delta$ er en **LK-utledning**.

$$\Gamma \vdash \Delta$$

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

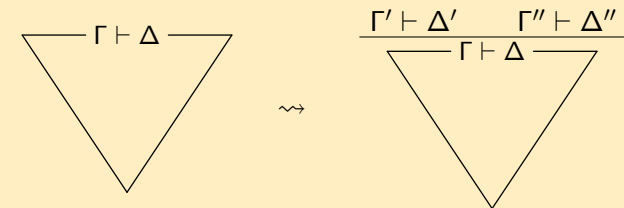
Definisjon (Mengden av LK-utledninger – α -utvidelse)

Hvis det finnes en LK-utledning med en løvsekvent $\Gamma \vdash \Delta$ og en α -slutning med konklusjon $\Gamma \vdash \Delta$ og premisser $\Gamma' \vdash \Delta'$, 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)

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

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)

$$\begin{array}{c}
 \times \\
 \frac{P \vdash P}{\vdash P \rightarrow P} R \rightarrow \\
 \\
 \frac{\frac{\frac{\times}{\neg Q, P \vdash P} R \neg}{\neg Q \vdash \neg P, P} R \neg}{\vdash P, \neg Q \rightarrow \neg P} R \rightarrow \quad \frac{\frac{\frac{\times}{Q \vdash Q, \neg P} L \neg}{Q, \neg Q \vdash \neg P} R \rightarrow}{Q \vdash \neg Q \rightarrow \neg P} L \rightarrow \\
 \hline
 P \rightarrow Q \vdash \neg Q \rightarrow \neg P
 \end{array}$$

- 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.