INF3170 – Logikk

Forelesning 14: Avanserte emner

Christian Mahesh Hansen

Institutt for informatikk, Universitetet i Oslo

14. mai 2007

Dagens plan

Overblikk

- John Alan Robinson, 1965.
- Metode for å avgjøre gyldighet av formler.
- Populær, effektiv og enkel å implementere.
- En av verdens raskeste teorembevisere, Vampire, bruker resolusjon.
- Vi begynner med å se på resolusjon for utsagnslogikk.

Resolusjon: regel og utledninger

- I resolusjon har man kun én regel: resolusjonsregelen.
  - Den forteller hvordan utleder nye klausuler fra de man har.
- Utledningene i resolusjon har kun én gren.

Definisjon

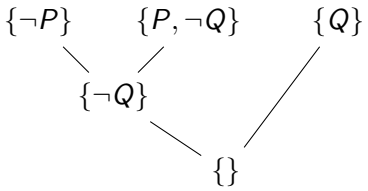
Resolusjonsregelen er

$$\frac{C \cup \{A\} \qquad D \cup \{\neg A\}}{C \cup D}$$

hvor C og D er klausuler og A en utsagnsvariabel. En resolusjonsutledning fra en mengde klausuler M er en endelig sekvens av klausuler hvor hvert element kommer fra M eller fra to foregående elementer ved anvendelse av resolusjonsregelen.

Eksempel 1

- La M bestå av klausulene $\{\neg P\}$, $\{P, \neg Q\}$ og $\{Q\}$.
- Vi kan nå anvende resolusjonsregelen og utlede $\{\}$.



1. $\{\neg P\}$
2. $\{P, \neg Q\}$
3. $\{Q\}$
4. $\{\neg Q\}$ (fra 1 og 2)
5. $\{\}$ (fra 3 og 4)

- Dette brukes for å vise at $(P \wedge (P \rightarrow Q)) \rightarrow Q$ er gyldig.

Definisjon

Et resolusjonsbevis for en formel F er en resolusjonsutledning fra matrisen som representerer F hvor den siste klausulen er tom.

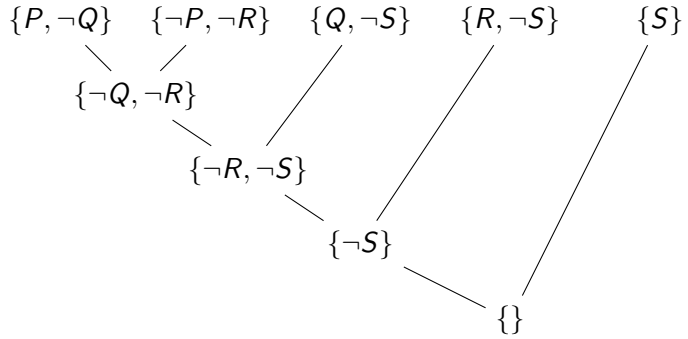
Teorem

En formel F er gyldig hvis og bare hvis det fins et resolusjonsbevis for F.

- Sunnhet. Anta at matrisen M representerer F.
  - Anta at en resolusjonsutledning for M ender med $\{\}$.
  - Resolusjonsregelen bevarer falsifiserbarhet (av mengden av klausuler).
  - Den tomme klausulen er ikke falsifiserbar.
  - Matrisen M og formelen F er ikke falsifiserbar.
  - F er gyldig.
- Kompletthet.
  - Kan gjøres direkte ved et modelleksistensargument.
  - Kan gjøres indirekte ved oversettelse til LK.

Eksempel 2

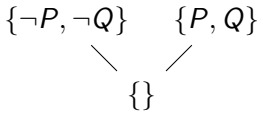
- Avgjør om $(P \rightarrow Q) \wedge (\neg P \rightarrow R) \wedge (Q \vee R \rightarrow S) \rightarrow S$ er gyldig.
- Overfører til DNF: $(P \wedge \neg Q) \vee (\neg P \wedge \neg R) \vee (Q \wedge \neg S) \vee (R \wedge \neg S) \vee S$
- Mengden av klausuler: $\{P, \neg Q\}$, $\{\neg P, \neg R\}$, $\{Q, \neg S\}$, $\{R, \neg S\}$, $\{S\}$.



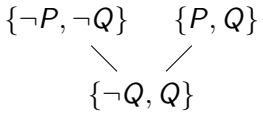
- Vi konkluderer med at formelen er gyldig!

Eksempel 3

- Merk: dette er ikke en resolusjonsutledning:



- Korrekt anvendelse av resolusjonsregelen gir:



- $(\neg P \wedge \neg Q) \vee (P \wedge Q)$ er ikke gyldig.
- La f.eks. $v(P) = \mathbf{1}$ og $v(Q) = \mathbf{0}$.

Resolusjon for første-ordens logikk

Definisjon

Resolusjonsreglene for førsteordens logikk er

$$\frac{C \cup \{A\} \quad D \cup \{\neg B\}}{(C \cup D)\sigma} \qquad \frac{C \cup \{A, B\}}{(C \cup \{A\})\sigma}$$

hvor C og D er klausuler, A og B er atomære formler og σ er en mest generell unifikator for A og B.

- Krever skolemisering og overføring til klausalform.
- Mengden av genererte klausuler eksploderer.
  - I teorembevisere er målet å ha effektiv subsumering, som løses ved hashing-teknikker (termindeksering).

Konjunktiv normalform og oppfyllbarhet

- Det er vanlig å presentere resolusjon på den *duale* måten:
  - Med utgangspunkt i konjunktiv normalform.
  - En klausul tolkes disjunktivt. (Klausul = disjunkson av literaler.)
  - En matrise tolkes konjunktivt. (Matrise = konjunksjon av klausuler.)
  - Resolusjonsregelen bevarer oppfyllbarhet i stedet for falsifiserbarhet.
  - Den tomme klausulen er ikke oppfyllbar.
  - For å avgjøre gyldigheten av en formel φ, overfører man $\neg\varphi$ til konjunktiv normalform og sjekker for oppfyllbarhet.
  - Resten er likt.

Dualiteter

Oppfyllbarhet

- Søker etter bevis for $\Gamma \vdash$
- En motmodell oppfyller Γ
- Tablåer (vanligvis også resolusjon)
- Konjunktiv normalform / negativ representasjon

Falsifiserbarhet

- Søker etter bevis for $\vdash \Gamma$
- Et motmodell falsifiserer Γ
- Ensidig sekventkalkyle, matriser, koblingskalkyle
- Disjunktiv normalform / positiv representasjon

Dualitet

For å finne ut om φ er gyldig, sjekk om $\neg\varphi$ er oppfyllbar.
Sekventkalkylen ivaretar begge aspektene!

Modallogikk på en under en halvtime

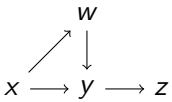
- Modale språk er enkle, men utrykksfulle, språk for å snakke om relasjonelle strukturer.
  - Enkel syntaks og avgjørbarhet.
  - Uttrykkskraftig nok til å fange inn aspekter ved andreordens logikk.
- Modale språk gir et internt, lokalt perspektiv på relasjonelle strukturer.
  - "Vi ser grafer innenfra."
- Anbefaler *Modal Logic* av Blackburn, de Rijke og Venema (2001).

Modallogikk på en under en halvtime

Vi utvider utsagnslogikk med de modale operatorene $\Box$ og $\Diamond$.

- Alle utsagnslogiske formler er formler.
- Hvis φ er en formel, så er $\Box\varphi$ og $\Diamond\varphi$ formler.
- $\Box$ og $\Diamond$ er duale: $\Box\varphi := \neg\Diamond\neg\varphi$.
- Modallogiske formler tolkes i Kripke-modeller, men vi stiller ingen krav til den binære relasjonen (partiell ordning, monotoni) slik vi gjorde for intuisjonistisk logikk.

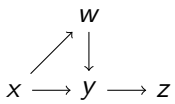
En enkel graf:



punkt	sanne utsagnsvariable
x	P
y	Q, R
z	S
w	R

- En mengde punkter: $\{x, y, z, w\}$.
- En binær relasjon R: xRw, xRy, yRz og wRy.
  - x kan se w og y, men kan ikke se z.
- For hvert punkt en mengde sanne utsagnsvariable.
  - $x \Vdash P$ betyr at P er sann i x
- $\Diamond\varphi$ uttrykker at vi kan se et punkt hvor φ er sann.
  - $x \Vdash \Diamond\varphi$ betyr at det fins et punkt x' slik at xRx' og $x' \Vdash \varphi$.
- $\Box\varphi$ uttrykker at φ er sann i *alle* punkter vi kan se.
  - $x \Vdash \Box\varphi$ betyr at for alle punkter x' slik at xRx', så $x' \Vdash \varphi$.

En enkel graf:



punkt	sanne utsagnsvariable
x	P
y	Q, R
z	S
w	R

- $w \Vdash \Diamond Q$ $\surd$ siden wRy og $y \Vdash Q$.
- $x \Vdash \Diamond\Diamond Q$ $\surd$ siden xRw og $w \Vdash \Diamond Q$.
- $x \Vdash \Box Q$ Nei, siden $w \nVdash Q$.
- $x \Vdash \Box R$ $\surd$ siden både $w \Vdash R$ og $y \Vdash R$.
- $x \Vdash \Diamond\Diamond\Diamond S$ $\surd$
- $x \Vdash \Diamond\Box S$ $\surd$ siden xRy og $y \Vdash \Box S$.
- $x \Vdash \Box(Q \rightarrow \Diamond S)$ $\surd$ siden $y \Vdash \Box S$.

Lesninger av $\Diamond$ og $\Box$

1. Nødvendighet og mulighet / metafysisk
   - $\Diamond\varphi$ kan leses som 'det er mulig at φ'.
   - $\Box\varphi$ blir 'det er ikke mulig at ikke φ' eller 'det er nødvendig at φ'.
   - Vi bør ha $\Box\varphi \rightarrow \Diamond\varphi$: 'det som er nødvendig er mulig'.
   - Vi bør også ha $\varphi \rightarrow \Diamond\varphi$: 'det er tilfellet, er mulig'.
   - Bør vi ha $\Diamond\varphi \rightarrow \Box\Diamond\varphi$?
   - Hvis vi har $\Diamond\varphi \rightarrow \Box\varphi$, så kollapser modalitetene.
2. Epistemisk logikk og kunnskap
   - $\Box\varphi$, eller $K\varphi$, kan leses som 'vi vet at φ'.
   - Vi bør ha $K\varphi \rightarrow \varphi$: 'hvis vi vet at φ, så må φ være sann'
   - Vi bør *ikke* ha $\varphi \rightarrow K\varphi$.
   - Bør vi ha $K\varphi \rightarrow KK\varphi$? (positiv introspeksjon)
3. Bevisbarhetslogikk
   - Vi kan lese $\Box\varphi$ som 'φ er bevisbar'.
   - Hvordan aksiomatisere bevisbarhet?
   - Löb-formelen $\Box(\Box\varphi \rightarrow \varphi) \rightarrow \Box\varphi$ er sentral.

Kompakthet

- Alt vi har gjort til nå har vært for endelige sekventer, dvs. objekter på formen $\Gamma \vdash \Delta$ hvor Γ og Δ er *endelige* multimengder av formler.
- Nå tillater vi at Γ og Δ er tellbart uendelige multimengder av formler.
- Alle definisjoner og resultater overføres og holder fremdeles.
- Et bevis er fortsatt et endelig tre hvor alle grener er lukket.
- Sunnhet og kompletthet er likt:

  $\Gamma \vdash \Delta$ er gyldig hvis og bare hvis $\Gamma \vdash \Delta$ er bevisbar.
- Merk: hvis Γ og Δ er uendelige, så vil et bevis for sekventen $\Gamma \vdash \Delta$ ha endelig mange grener. Da fins det en endelig delmengde Γ' av Γ og en endelig delmengde Δ' av Δ slik at sekventen $\Gamma' \vdash \Delta'$ er bevisbar.

Kompakthet

Teorem (Kompakthet)

La Γ være en mengde førsteordens formler.
Γ er oppfyllbar $\Leftrightarrow$ enhver endelig delmengde Γ' av Γ er oppfyllbar.

Bevis

$\Rightarrow$ *Trivielt*
$\Leftarrow$ *Anta at Γ ikke er oppfyllbar. Da er sekventen $\Gamma \vdash$ gyldig. Ved kompletthet er $\Gamma \vdash$ bevisbar. Da fins det en endelig delmengde Γ' av Γ slik at $\Gamma' \vdash$ er bevisbar. Ved sunnhet kan ikke Γ' være oppfyllbar. Da fins en endelig delmengde av Γ som ikke er oppfyllbar.*

En anvendelse av kompakthet

Lemma

Hvis en mengde Γ har vilkårlig store endelige modeller, så har Γ en uendelig modell.

Bevis

La φ_n være en formel som uttrykker at 'det fins minst n elementer'. (Vi kan anta at vi har likhet i språket.) La $\Gamma^* = \Gamma \cup \{\varphi_n \mid 1 \leq n\}$. Siden Γ har vilkårlig store endelige modeller, må hver endelig delmengde av Γ^* være oppfyllbar. Ved kompakthet må Γ^* være oppfyllbar. Modellen som oppfyller Γ^* må være uendelig, siden den oppfyller φ_n for alle n.

En anvendelse av kompakthet

Teorem

Det fins ingen mengde formler Γ som er slik at Γ er sann i alle og bare de endelige modellene. Med andre ord: endelighet er ikke aksiomatiserbart i førsteordens logikk.

Bevis

Følger umiddelbart fra forrige Lemma. Siden Γ har vilkårlig store endelige modeller, må Γ ha en uendelig modell.

Teorier og aksiomer

Definisjon (Teori)

En teori er en mengde formler T som er lukket under logisk konsekvens: hvis $T \models \varphi$, så er $\varphi \in T$.

- Ved sunnhet og kompletthet så er dette det samme som å si: hvis sekventen $T \vdash \varphi$ er bevisbar, så $\varphi \in T$.

Definisjon (Aksiom)

En mengde Γ slik at $T = \{\varphi \mid \Gamma \models \varphi\}$ kalles en aksiommengde for teorien T. Elementene i Γ kalles aksiomer.

Fullstendighet og konsistens

Definisjon (Fullstendig teori)

En teori T er fullstendig hvis for enhver formel φ i språket, så er enten φ eller $\neg\varphi$ med i T; ellers kalles teorien ufullstendig.

Definisjon (Konsistent teori)

En teori T er inkonsistent hvis både φ og $\neg\varphi$ er med i T, for en formel φ; ellers er teorien konsistent.

- Vi kan lage fullstendige teorier for mange områder av matematikken.
  - Teorien for grafer.
  - Teorien for boolske algebraer.
  - Teorien for algebraisk lukkede kropper.
  - Teorien for tett ordnede mengder uten endepunkter.
  - Presburgeraritmetikk (bare pluss, ikke gange).
- Mål: å lage en fullstendig teori for all matematikk!

Peanoaritmetikk

- Aksiomer for suksessor
  - $\forall x(Sx \neq 0)$
  - $\forall x \forall y(Sx = Sy \rightarrow x = y)$
  - $(\forall x(x \neq 0 \rightarrow \exists y(x = Sy)))$
- Aksiomer for addisjon
  - $\forall x(x + 0 = x)$
  - $\forall x \forall y(x + Sy = S(x + y))$
- Aksiomer for multiplikasjon
  - $\forall x(x \cdot 0 = 0)$
  - $\forall x \forall y(x \cdot Sy = (x \cdot y) + x)$
- Induksjonsaksiomet
  - $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(Sx)) \rightarrow \forall x \varphi(x)$, for hver formel $\varphi(x)$ med høyst x fri.
- Peanoaritmetikk er teorien vi får fra denne mengden av aksiomer.
- Uten induksjonsaksiomet får vi Robinsonaritmetikk.

Ufullstendighet

- Kurt Gödel beviste i 1931 sitt berømte ufullstendighetsteorem.

Teorem (Gödels første ufullstendighetsteorem)

Enhver konsistent, aksiomatisk teori som er tilstrekkelig sterk er ufullstendig.

- Tilstrekkelig sterk betyr at vi kan bevise grunnleggende påstander om pluss og gange. Robinsonaritmetikk er tilstrekkelig.
- Hvis teorien er sterk nok, så fins det *alltid* en påstand ikke kan bevises i teorien.
- I alle tilstrekkelig sterke tallteorier vil det finnes påstander som er sanne (i standardmodellen) men som ikke er bevisbare.

Avslutning

- Dette er siste ordinære forelesning...
- 21/5: gjennomgang av oppgaver
- 4/6: repetisjon
- Husk å komme med innspill til oppgaver og repetisjonsstoff!!
- Har dere spørsmål eller kommentarer?