INF1800 – Logikk og beregnbarhet

Forelesningsnotater
Høsten 2008

Roger Antonsen
Universitetet i Oslo

Sist oppdatert: 17. november 2008 12:46

Dette kompendiet er automatisk generert fra materialet som ble presentert på forelesningene og må leses med dette forbeholdet. Kommentarer, feil og forslag til forbedringer kan sendes til Roger Antonsen (rantonse@ifi.uio.no).

Innhold

Forelesning 1: Introduksjon 5

Velkommen til INF1800! 5

Introduksjon 5

Praktiske opplysninger 5

Forelesere, tid og sted 5
Gruppelærere og gruppeundervisning 5
Obligatoriske oppgaver og eksamen 6
Oversikt over semesteret 6
Pensum og lærebok 6

Om kurset INF1800 7

Generelt 7
Kort om emnet (fra kursbeskrivelsen) 7
Hva lærer du? (fra kursbeskrivelsen) 7
Et nyttig kurs 7
Begreper og temaer som vi skal lære å kjenne 8

Litt om logikk 8

Språk og representasjon 8
Representasjon (eksempler) 9
Logikk er et stort fag 9

Forelesning 2: Mengdelære 11

Mengdelære 11

Læreboken 11
Mengder 11
Noen spesielle mengder 12
Union – slå sammen mengder 12
Snitt – felles elementer 13
Mengdedifferanse – fjerne elementer 13
Delmengder 14
Mengdebygger 14
Mengder av mengder 14
Multimengder 15
Tupler 15
Kryssprodukt 16

Forelesning 3: Mengdelære, Relasjoner, Funksjoner 17

Repetisjon 17

Mengder 17
Multimengder og tupler 17

Litt mer mengdelære 17

Potensmengder 17
Venn-diagrammer 18
Kardinalitet 18
Tellbar og overtellbar 19

Relasjoner 20

Definisjon 20
Eksempler 20
Egenskaper ved relasjoner 21
Refleksivitet 21
Symmetri 22
Transitivitet 22
Ekvivalens 22
Anti-symmetri 23

Irrefleksivitet 23
Eksempler 23
Litt om funksjoner 24
Læreboken 24
Funksjoner 24
Operatorer 25
Forelesning 4: Utsagnslogikk – Syntaks og semantikk 27
Før vi begynner 27
Praktiske opplysninger 27
Forelesningene og læreboken 27
Utsagnslogikk 27
Utsagnslogikk handler om utsagn 27
Sånt som ikke er utsagn 28
Atomære utsagn 28
Syntaks for atomære utsagn: Utsagnsvariable 28
Sammensatte utsagn 29
Syntaks for sammensatte utsagn 29
Konnektiver 29
Utsagnslogiske formler 30
Semantikk 31
Semantikk 31
Sannhetsverdier 31
Negasjon (ikke) 32
Konjunksjon (og) 32
Disjunksjon (eller) 32
Implikasjon (hvis, så) 32
Forelesning 5: Utsagnslogikk – Syntaks og semantikk 35
Praktisk informasjon 35
Endringer i undervisningen 35
Spørreskjemaet 35
Oppvarming 35
Hvordan tjene en million på logikk 35
Repetisjon 36
Eksempler & Sannhetsverditabeller 36
Eksempel 1 36
Eksempel 2 36
Eksempel 3 37
Sannhetsverditabeller 37
Semantikk for utsagnslogikk 38
Valuasjoner 38
Oppfyllbarhet 39
Falsifiserbarhet 40
Tautologi / Gyldighet 40
Motsigelse / Kontradiksjon 40
Oppsummering av disse begrepene 41
Eksempler 41
Noen viktige begreper 42
Bruk av utsagnslogikk 43
Hvordan fange inn utsagn? 43
Forelesning 6: Utsagnslogikk – Syntaks og semantikk 45
Mer om bruk av utsagnslogikk 45
Hvordan fange inn utsagn? 45

Nødvendig og tilstrekkelig 45
Mer syntaks 45
Presedensregler 45
Symboler for sannhetsverdiene 46
Mer semantikk 46
Ekvivalens 46
Viktige ekvivalenser 47
Ekvivalenser som omskrivingsregler 48
Normalformer 48
Hva er normalformer? 48
Literaler 49
Disjunktiv normalform (DNF) 49
Konjunktiv normalform (CNF) 51
Noen oppgaver 51
Tillegg 52
Oppfyllbare mengder 52
Forelesning 15: Utsagnslogikk – Sekventkalkyle **53**
Sekventkalkyle for utsagnslogikk 53
Introduksjonseksempel 53
Noen kommentarer 54
Sekventer og aksiomer 55
Sekventkalkyleregler 56
Begreper knyttet til regler 57
Slutninger 57
Begreper knyttet til slutninger 57
Utledninger 58
Bevis 59
Semantikk for sekventer 60
Gyldige sekventer 60
Falsifiserbare sekventer 60
Oppsummering 61
Forelesning 16: Utsagnslogikk – Sekventkalkyle **63**
Noen kommentarer 63
Forelesningene, notatene og boken 63
Eksempel på et bevis 63
Eksempel på en utledning som ikke er et bevis 63
Litt om sunnhet og kompletthet 64
Sunnhet og kompletthet 64
Forelesning 16x: Utsagnslogikk – Sunnhetsteoremet **65**
Bevis for sunnhetsteoremet 65
Sunnhet av LK 65
Bevaring av falsifiserbarhet 65
Eksistens av falsifiserbar løvsekvent 67
Alle aksiomer er gyldige 68
Bevis for sunnhetsteoremet 68
Forelesning 17: Førsteordens logikk **69**
Før vi begynner 69
Repetisjon og kommentarer 69
Nytt tema 69
Innledning til førsteordens logikk 70
Introduksjon 70

Noen eksempler fra matematikk 70
Noen eksempler med naturlig språk 70
Overblikk 70
Førsteordens logikk: Syntaks 71
Syntaks: Signaturer 71
Syntaks: Termer 72
Eksempler på førsteordens språk 72
Syntaks: Formler 73
Eksempler på førsteordens formler 74
Flere eksempler 74
Frie variable i termer 74
Frie variable i formler 75
Substitusjoner 75
Førsteordens logikk: Semantikk 76
Introduksjon 76
Modeller – Intuisjon 77
Modeller 77
Forelesning 18: Førsteordens logikk 79
Repetisjon og noen løse tråder 79
Førsteordens språk 79
Eksempler på signaturer 79
Mengden av førsteordens termer og formler 79
En kort oppsummering av modeller 80
Substitusjoner og frie variable 80
Lukkede og åpne formler 81
Presedensregler 81
Semantikk (fortsettelse) 82
Noen kommentarer 82
Eksempel – Et figurspråk 82
Utvidete språk 83
Utvidete språk (i detalj – for spesielt interesserte) 84
Tolkning av termer 84
Tolkning av formler 85
Oppfyllbarhet 85
Gyldighet 85
Forelesning 19: Førsteordens logikk 87
Repetisjon 87
Semantikk 87
Språk og modeller: Et komplekst forhold 87
Noen eksempler 87
Eksempel 1 87
Eksempel 2 88
Eksempel 3 88
Eksempel 4 89
Eksempel 5 89
Figurspråket igjen 90
En utvidelse av figurspråket 90
Forklarende eksempel til semantikken 90
Eksempel 1 91
Eksempel 2 91
Eksempel 3 92
Eksempel 4 92
Eksempel 5 93
Eksempel 6 93
Bruke språket til å beskrive modeller 93

Forelesning 20: Førsteordens logikk 95
Mer om førsteordens logikk 95
Tillukninger 95
Ekvivalens 95
Kvantorer og negasjon 95
Distribusjon av kvantorer 96
Omdøping av variable 96
Flere ekvivalenser 97
Preneks normalform 97
Litt om å føre bevis 99
Bevisteknikker 99
Direkte versus indirekte bevis 99
Å vise at noe ikke holder 99
Noen tommelfingerregler 100
Bevis for "for alle"-påstander 100
Forelesning 21: Førsteordens logikk 101
Førsteordens sekventkalkyle 101
Introduksjon 101
Motivasjon 102
Sekventer og aksiomer 102
Sekventkalkyleregler 103
Slutninger 104
Utledninger 104
Bevis 104
Sunnhet og kompletthet 105
Eksempler 105
Eksempel 1 105
Eksempel 2 106
Eksempel 3 106
Eksempel 4 106
Eksempel 5 107
Eksempel 6 107
Forelesning 22: Førsteordens logikk 109
Litt om konsistens 109
Oppfyllbarhet og konsistens 109

INF1800 – Forelesning 1

Introduksjon

Roger Antonsen - 19. august 2008

Velkommen til INF1800!

Introduksjon

- Velkommen til INF1800: Logikk og beregnbarhet!
- Plan for i dag:
  - Praktiske opplysninger
  - Innholdet i kurset
  - Litt om logikk (Roger)
  - Litt om beregnbarhet (Lars)
- Før vi begynner:
  - Det er lov å stille spørsmål.
  - Dette vil bli lagt ut på kursets hjemmeside.
  - Vi begynner kvart over.
  - Spørsmål, kommentarer eller bemerkninger?

Praktiske opplysninger

Forelesere, tid og sted

- Roger Antonsen <rantonse@ifi.uio.no>
- Lars Kristiansen <larsk@math.uio.no>
- Tirsdag kl. 14:15–16:00, Store auditorium
- Onsdag kl. 09:15–10:00, Store auditorium
- 15 uker $\times$ 3 (timer / uke) = 45 timer
- Logikkdelen: Roger
- Beregnbarhetsdelen: Lars

Gruppelærere og gruppeundervisning

- Xiang He Kong <xianghek@student.matnat.uio.no>
- Alfred Bratterud <alfredb@student.matnat.uio.no>
- 15 uker $\times$ 3 (timer / uke) = 45 timer
- Se kursets hjemmeside for tidspunkt og grupper.
- Bruk gruppelærerene og gruppeundervisningen!
- Veldig viktig for læringen.

Obligatoriske oppgaver og eksamen

- Kurset har fire obligatoriske oppgaver.
  - Fredag 12. september: Innlevering av oblig 1
  - Fredag 3. oktober: Innlevering av oblig 2
  - Fredag 24. oktober: Innlevering av oblig 3
  - Fredag 14. november: Innlevering av oblig 4
- Oppgavene vil legges ut senest 14 dager før.
- Bedømmes til bestått/ikke bestått.
- Alle obligene må bestås for å kunne gå opp til eksamen.
- Skriftlig eksamen, 3 timer, uten hjelpemidler.
  - Mandag 15. desember kl. 0900

Oversikt over semesteret

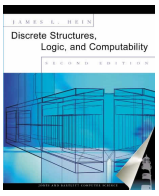
Uke	Ma	Ti	On	To	Fr	Lø	Sø	
34	18	**19**	**20**	21	22	23	24	
35	25	**26**	**27**	28	29	30	31	
36	1	**2**	**3**	4	5	6	7	September
37	8	**9**	**10**	11	12	13	14	
38	15	**16**	**17**	18	19	20	21	
39	22	**23**	**24**	25	26	27	28	
40	29	**30**	**1**	2	3	4	5	Oktober
41	6	**7**	**8**	9	10	11	12	
42	13	**14**	**15**	16	17	18	19	
43	20	**21**	**22**	23	24	25	26	
44	27	**28**	**29**	30	31	1	2	November
45	3	**4**	**5**	6	7	8	9	
46	10	**11**	**12**	13	14	15	16	
47	17	**18**	**19**	20	21	22	23	
48	24	**25**	**26**	27	28	29	30	
49	1	2	3	4	5	6	7	Desember
50	8	9	10	11	12	13	14	
51	15	16	17	18	19	20	21	

Pensum og lærebok

- Pensum defineres av forelesningene.
- Vi har også en lærebok

Referanser

[1] James L. Hein *Discrete Structures, Logic, and Computability* (2. edition) Jones and Bartlett Publishers (2002) ISBN: 0-7637-1843-2



- De delene av boken som er relevant og som er pensum vil defineres presist etter hvert.
- Boken inneholder bakgrunnsstoff som strengt tatt ikke er nødvendig, men som kan komme godt med.
- Boken går også langt utover pensum, og inneholder mye bra for spesielt interesserte.
- Bruk boken som en ressurs.
  - (Ikke les hele; det vil sannsynligvis ta for lang tid.)

Om kurset INF1800

Generelt

- Kurset har en lang tradisjon ved UiO.
- Litt om logikkmiljøet ved UiO.
- Temaet er formelle språk og hvordan vi kan manipulere og gjøre beregninger med slike.

Kort om emnet (fra kursbeskrivelsen)

- Innføring i utsagnslogikk og predikatlogikk.
- Bruk av logikk som språk for kunnskapsrepresentasjon og spesifikasjon,
- og metoder for påvisning eller avkrefting av logisk gyldighet ved hjelp av beviskalkyler og modellkonstruksjon.
- Formelle modeller for beregninger, som endelige automater, stakkautomater og turingmaskiner,
- og den elementære teorien for disse.

Hva lærer du? (fra kursbeskrivelsen)

- Å kunne bruke utsagnslogikk og predikatlogikk som formelle språk.
- Å kunne vise hvordan en kan argumentere for logisk gyldighet,
- eller vise ved falsifikasjon at noe ikke er logisk gyldig.
- Kjennskap til metoder knyttet til beregnbarhetsmodeller.

Et nyttig kurs

- Man lærer mye som er nyttig å kunne til senere.
- Grunnleggende notasjon og begrepsdannelse.
- Resonnering og presis argumentasjon.
- Man får skjerpet språkbruk og klarere tankegang.
- Introduksjon til matematisk resonnering.
- Men. . . ikke uten egeninnsats!

Begreper og temaer som vi skal lære å kjenne

- utsagnslogikk
- første-ordens logikk
- syntaks
- semantikk
- formler
- konnektiver
- kvantorer
- logiske symboler
- sekventer
- gyldighet
- oppfyllbarhet
- sunnhet
- kompletthet
- mengdelære
- konsistens
- bevisbarhet
- sannhetsverdier
- normalformer
- presedensregler
- skopregler
- åpne formler
- lukkede formler
- sannhetstabeller
- sekventkalkyle
- modeller
- språk

- grammatikker
- automater
- deterministiske automater
- ikke-deterministiske automater
- regulære uttrykk
- regulære grammatikker
- pumpelemmaet
- kontekstfrie språk
- Turingmaskiner
- ...

Litt om logikk

Språk og representasjon

- Logiske språk kan brukes til å beskrive verden.
- Når man har beskrivelsen, så kan man regne på den.
- Det er en veldig kraftfull idé.
- Man representerer og bruker representasjonen.
- Forskjellige språk har forskjellig uttrykkskraft.
  - Utsagnslogikk
  - Første-ordens logikk
- Uttrykkskraft, beregnbarhet og kompleksitet står i et forhold til hverandre.

Representasjon (eksempler)

- Musikk og noter
- Matematikk (funksjoner, grafer, integraler, ...)
- Modellering
- Egenskaper ved programmer
- Navigasjon, romlig beskrivelse, GPS
- Kunnskapsrepresentasjon
- Statistikk og sannsynlighet
- Notasjonssystemer (sjonglering, skolisser, kirkeklokker)
- ...

Logikk er et stort fag

- Filosofi og filosofisk logikk
  - Matematikkens fundamenter
  - Logiske paradokser og feilslutninger
- Matematikk og matematisk logikk
  - Bevisteori, modellteori og mengdelære
  - Rekursjonsteori, beregnbarhet
- Informatikk
  - Programvareverifikasjon, modellsjekking, debugging
  - Spesifikasjonsspråk, formelle semantikker for programmeringsspråk
  - Logiske kretser
  - Teorembevisere, kunstig intelligens
  - Distribuerte prosesser
  - Semantiske verktøy, semantic web
  - Logikker: Modallogikk, temporallogikk, beskrivelseslogikker, epistemisk logikk, deontisk logikk, fuzzy logikk

INF1800 – Forelesning 2

Mengdelære

Roger Antonsen - 20. august 2008

Mengdelære

Læreboken

- Det meste av det vi gjør her kan leses uavhengig av boken.
- Følgende avsnitt i boken regnes som pensum.
  - Kapittel 1.2, side 13–35: *Sets*
  - Kapittel 1.3, side 35–55: *Ordered Structures*

Mengder

Definisjon (Mengde).

- En *mengde* (eng: *set*) er en endelig eller uendelig samling av objekter der innbyrdes rekkefølge og antall forekomster av hvert objekt ignoreres.
- Objektene i en mengde kalles *elementer*.
- Hvis a er element i mengden S, skriver vi $a \in S$.
- Hvis a *ikke* er element i S, skriver vi $a \notin S$.
- To mengder S og T er *like*, $S = T$, hvis de inneholder de samme elementene.
- Hvis både a og b er elementer i S, skriver vi $a, b \in S$.

Notasjon.
Mengden med elementene a, b, c og d skrives ofte $\{a, b, c, d\}$.

Eksempel.

- $\{0, 1\}$ er mengden av digitale verdier en bit kan ha.
- $\{a, c, f, g, k\}$ er en mengde med bokstaver.
- $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ er mengden av de 10 minste primtallene.
- $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ er mengden av naturlige tall

Eksempel.
La oss anta at $a, b, c, d, 1, 2, \gamma, \Phi$ alle er forskjellige. Vi har at følgende holder:

- $a \in \{a, b, c\}$
- $d \notin \{a, b, c\}$
- $1 \in \{a, 1, \gamma, \Phi\}$
- $2 \notin \{a, 1, \gamma, \Phi\}$
- $\{a, b\} = \{b, a\}$
- $\{a, a, b\} = \{a, b\}$
- $\{a, b\} \neq \{b, c\}$ (mengdene er *ulike*)

Noen spesielle mengder

Definisjon (Den tomme mengden).

- Den *tomme mengden* (eng: *empty set*) er mengden som ikke inneholder noen elementer.
- Skrives ofte $\{\}$ eller $\emptyset$.

Definisjon (Singletonmengde).
En *singletonmengde* er en mengde som har nøyaktig ett element.

Eksempel.
Både $\{a\}$, $\{b\}$ og $\{b, b\}$ er singletonmengder.

Union – slå sammen mengder

Definisjon (Union).

- *Unionen* (eng: *union*) av to mengder S og T er den mengden som inneholder alle objekter som er element i S *eller* T.
- Unionen av S og T skrives ofte $S \cup T$.

Eksempel.

- $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$
- $\{a, b\} \cup \{b, c\} = \{a, b, c\}$
- $\{1, 2, 3\} \cup \emptyset = \{1, 2, 3\}$

Snitt – felles elementer

Definisjon (Snitt).

- Hvis S og T er mengder, så er *snittet* (eng: *intersection*) mellom S og T, eller S *snittet med* T, mengden som inneholder alle objekter som er element i både S *og* T.
- S snittet med T skrives ofte $S \cap T$.

Eksempel.

- $\{a, b\} \cap \{c, d\} = \emptyset$
- $\{a, b\} \cap \{b, c\} = \{b\}$
- $\{1, 2, 3\} \cap \emptyset = \emptyset$

Mengdedifferanse – fjerne elementer

Definisjon (Mengdedifferanse).

- Hvis S og T er mengder, så er *mengdedifferansen* (eng: *difference*) mellom S og T, eller S *minus* T, mengden som inneholder alle objekter som er element i S men *ikke* element i T.
- S minus T skrives ofte $S \setminus T$. Boka skriver $S - T$.

Eksempel.

- $\{a, b\} \setminus \{c, d\} = \{a, b\}$
- $\{a, b\} \setminus \{b, c\} = \{a\}$
- $\{1, 2, 3\} \setminus \emptyset = \{1, 2, 3\}$
- $\emptyset \setminus \{a, b, c\} = \emptyset$

Delmengder

Definisjon (Delmengde).

- En mengde S er en *delmengde* (eng: *subset*) av en mengde T hvis alle elementer i S også er elementer i T.
- Skrives ofte $S \subseteq T$. Boka skriver $S \subset T$.

Eksempel.

- $\{a, b\} \subseteq \{a, b, c\}$
- $\{a, b\} \subseteq \{a, b\}$ *(enhver mengde er en delmengde av seg selv)*
- $\{a, b, c\} \not\subseteq \{a, b\}$
- $\emptyset \subseteq \{a, b\}$ *(den tomme mengden er en delmengde av alle mengder)*
- $\{a, b\} \not\subseteq \emptyset$

Mengdebygger

Notasjon.
En definisjon på formen

"mengden av alle elementer x slik at x har egenskapen P"

kan skrives slik

$$\{x \mid x \text{ har egenskapen } P\}.$$

En slik konstruksjon kalles en *mengdebygger*. Det som er til venstre for streken kan også være sammensatte uttrykk.

Eksempel.

- $\{n \mid n \in \mathbb{N} \text{ og } n \text{ er partall }\}$ betegner mengden av alle partall.
- $\{2k + 1 \mid k \in \mathbb{N}\}$ betegner mengden av alle oddetall.
- $\{x \mid x \text{ er informatikkstudent }\}$ betegner mengden av alle informatikkstudenter.

Mengder av mengder

- Det er også mulig å konstruere mengder som inneholder andre mengder (med visse restriksjoner).

Eksempel.

- $\{\emptyset\} \neq \emptyset$
- $\{\{0\},\{1\},\{2\},\ldots\} = \{\{n\} \mid n \in \mathbb{N}\}$
- $\{\{0\},\{0,1\},\{0,1,2\},\ldots\} = \{\{m \mid 0 \leqslant m \leqslant n\} \mid n \in \mathbb{N}\}$
- $\{\{0,2,4,6,\ldots\},\{1,3,5,7,\ldots\}\}$

Multimengder

Definisjon (Multimengde).

- En *multimengde* (eng: *bag/multiset*) er en endelig eller uendelig samling objekter der innbyrdes rekkefølge ignoreres, men hvor hvert objekt kan forekomme flere ganger.
- Multimengder er mengder der antall forekomster av hvert element teller.
- Vi bruker union ($\cup$), snitt ($\cap$), mengdedifferanse ($\setminus$) og delmengderelasjonen ($\subseteq$) også på multimengder. (I tillegg kan man bruke $+$. Se boka for detaljer.)
- Vi bruker $\emptyset$ om den tomme multimengden.

Notasjon.
Multimengden med elementene a, b, c og d skrives ofte med firkantklammer, slik: $[a,b,c,d]$.

Eksempel.

- $[a,b,c] = [c,b,a]$
- $[a,b,c,a] \neq [a,b,c]$ (a forekommer ikke like mange ganger)
- $[a,a,b,c] \cup [a,c] = [a,a,b,c]$
- $[a,a,b,c] + [a,c] = [a,a,a,b,c,c]$
- $[a,a,a,b,c] \cap [a,a,d] = [a,a]$
- $[a,a,a,b,c] \setminus [a,a,d] = [a,b,c]$
- $[a,a] \subseteq [a,a,b,c]$, men $[a,a,a] \not\subseteq [a,a,b,c]$

Tupler

Definisjon (Tuppel).

- Et *tuppel* (eng: *tuple*) med n elementer, et n-tuppel, er en samling med n objekter der både innbyrdes rekkefølge og antall forekomster av hvert objekt teller.
- 0-tuppelet, det tomme tuppelet, skrives $\langle\rangle$
- Et 2-tuppel med to elementer x og y kalles også et (ordnet) *par* (eng: *ordered pair*) og skrives $\langle x, y\rangle$.
- To n-tupler $\langle a_1, \ldots, a_n\rangle$ og $\langle b_1, \ldots, b_n\rangle$ er *like* hvis for enhver i slik at $1 \leqslant i \leqslant n$ vi har at $a_i = b_i$.

Kryssprodukt

Definisjon (Kryssprodukt).

- Hvis S og T er mengder, så er *kryssproduktet* (eng: *cross product*) av S og T mengden av alle par $\langle s, t\rangle$ slik at $s \in S$ og $t \in T$.
- Kryssproduktet av S og T skrives ofte $S \times T$.
- Kryssproduktet av S og T kan skrives slik: $S \times T = \{\langle s, t\rangle \mid s \in S \text{ og } t \in T\}$

Eksempel.

- $\{a, b\} \times \{c, d\} = \{\langle a, c\rangle, \langle a, d\rangle, \langle b, c\rangle, \langle b, d\rangle\}$
- $\{a, b\} \times \{b, c\} = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, b\rangle, \langle b, c\rangle\}$
- $\{a\} \times \{1, 2\} = \{\langle a, 1\rangle, \langle a, 2\rangle\}$

Notasjon.

- En mengde kan krysses med seg selv: $S \times S$
- $\{a, b\} \times \{a, b\} = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle\}$
- $S \times S \times S$ skrives ofte S^3.
- Generalisert: $\underbrace{S \times S \times \ldots \times S}_{n}$ skrives S^n.

INF1800 – Forelesning 3

Mengdelære, Relasjoner, Funksjoner

Roger Antonsen - 26. august 2008

Repetisjon

Mengder

- Definisjon av en mengde.
  - Innbyrdes rekkefølge og antall forekomster spiller ingen rolle.
- Symboler vi bruker når vi snakker om og regner på mengder:

$$\{\,\}\quad\in\quad\notin\quad=\quad\neq\quad|\quad\ldots\quad\emptyset\quad\cap\quad\cup\quad\setminus\quad\subseteq\quad\times$$

- Noen eksempler:
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$
  - $x \in \mathbb{N}$
  - $\{x \mid x \in \mathbb{N}$ og x er delelig med $3\}$

Multimengder og tupler

- Definisjon av en multimengde.
  - Innbyrdes rekkefølge spiller ingen rolle, men det gjør antall forekomster.
- Noen eksempler:
  - $[k, l, e, m] = [m, e, l, k]$, men $[k, l, e, m] \neq [k, l, e, m, m]$
- En kommentar om union. Med multimengder får vi to typer:
  - $[a, b] \cup [a, b, c] = [a, b, c]$
  - $[a, b] + [a, b, c] = [a, a, b, b, c]$
  - Vi vil kun bruke den siste varianten.
- Definisjon av et n-tuppel.
  - Både innbyrdes rekkefølge og antall forekomster er viktig.
- Noen eksempler:
  - $\{1\} \times \{a, b\} = \{\langle 1, a\rangle, \langle 1, b\rangle\}$
  - $\{a, b\} \times \{1\} = \{\langle a, 1\rangle, \langle b, 1\rangle\}$

Litt mer mengdelære

Potensmengder

Definisjon (Potensmengde).

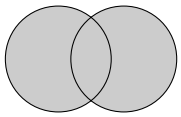
- Hvis S er en mengde, så er *potensmengden* (eng: *power set*) til S mengden av alle delmengder av S.

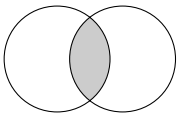
Eksempel.

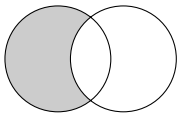
- Potensmengden til $\{1, 2\}$ er $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
- Potensmengden til $\{1, 2, 3\}$ er $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
- Potensmengden til $\{1\}$ er $\{\emptyset, \{1\}\}$.
- Potensmengden til $\emptyset$ er $\{\emptyset\}$.

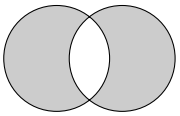
Venn-diagrammer

- Venn-diagrammer brukes til å illustrere mengder og operasjoner på mengder. Dette står forklart i boka.
- Vi ser på hvordan noen enkle Venn-diagrammer ser ut for to mengder.









Kardinalitet

- Kardinalitet = "størrelsen på en mengde"
- Følgende avsnitt i boken regnes som pensum.
  - Kapittel 2.4.1, side 115–116: *Comparing the Size of Sets*
  - Kapittel 2.4.2, side 116–118: *Sets that Are Countable*

Definisjon (Kardinalitet).

- To mengder S og T har *lik kardinalitet* (eng: *cardinality*) hvis det fins en en-til-en korrespondanse mellom elementene i S og T.
- Mengden S har *kardinalitet mindre eller lik* T hvis det fins en en-til-en korrespondanse mellom S og en delmengde av T.
- Hvis S er en endelig mengde, så er kardinaliteten til S lik antall elementer i S.
- Vi bruker notasjonen $|S|$ for kardinaliteten til S.

Eksempel.
Hva er kardinaliteten til følgende mengder:

- $\{a, b, c\}$ (3)
- $\{a, b, a\}$ (2)
- $\{a\}$ (1)
- $\emptyset$ (0)
- $\mathbb{N}$ (uendelig)

Eksempel.

- $\mathbb{N}$ = mengden av alle naturlige tall, $\{0, 1, 2, 3, 4, 5, \ldots\}$
- $2\mathbb{N}$ = mengden av alle partall, $\{0, 2, 4, 6, 8, 10, \ldots\}$
- Funksjonen $f(x) = 2x$ gir en en-til-en korrespondanse mellom $\mathbb{N}$ og $2\mathbb{N}$, så $\mathbb{N}$ og $2\mathbb{N}$ har samme kardinalitet. Vi skriver $|\mathbb{N}| = |2\mathbb{N}|$.

Tellbar og overtellbar

Definisjon (Tellbar).
En uendelig mengde S er *tellbar* (eng: *countable*) hvis det fins en en-til-en korrespondanse mellom elementene i S og de naturlige tallene. Hvis ikke, er S *overtellbar* (eng: *uncountable*). Alle endelige mengder er tellbare.

Eksempel.

- Mengden av alle partall er tellbar.
- Mengden av binære tall er tallbar.
- Mengden av brøktall er tellbar.
- Mengden av nålevende mennesker er tellbar.
- Mengden av reelle tall er *ikke* tellbar.

Relasjoner

Definisjon

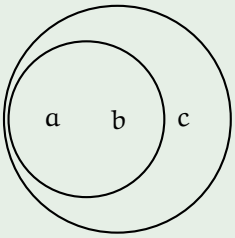
Definisjon (Relasjon).

- En *unær relasjon* (eng: *unary relation*) på S er en delmengde av S. Kalles også ofte for et *predikat* (eng: *predicate*).
- En *binær relasjon* (eng: *binary relation*) fra S til T er en delmengde av $S \times T$.
- En n*-ær relasjon* (eng: n*-ary relation*) på mengdene $S_1, S_2, \ldots, S_n$ er en delmengde av kryssproduktet $S_1 \times S_2 \times \ldots \times S_n$.
- En n*-ær relasjon* på en mengde S er en delmengde av S^n.

Eksempler

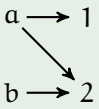
Eksempel.

- Hvis $S = \{a, b, c\}$, så er $\{a, b\}$ en unær relasjon på S.
- Vi kan illustrere dette slik:



Eksempel.

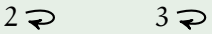
- Hvis $S = \{a, b\}$ og $T = \{1, 2\}$, så er $\{\langle a, 1\rangle, \langle a, 2\rangle, \langle b, 2\rangle\}$ en binær relasjon fra S til T.
- Vi kan illustrere dette slik:



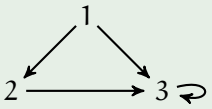
Eksempel.

La $S = \{1, 2, 3\}$.

- $\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$ er en binær relasjon på S.



- $\{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle, \langle 3,3\rangle\}$ er også en binær relasjon på S.



Eksempel (Flere eksempler på binære relasjoner).

- *Likhetsrelasjonen* på en mengde S, $\{\langle x,x\rangle \mid x \in S\}$.
- *Mindre enn*-relasjonen på f.eks. naturlige tall, $\{\langle x,y\rangle \mid x,y \in \mathbb{N} \text{ og } x \leqslant y\}$
- *Foreldrerelasjonen* på f.eks. mengden av mennesker, $\{\langle a,b\rangle | a \text{ er forelder til } b\}$
- *Delmengde*-relasjonen på en mengde av mengder.
- Og så videre.

Egenskaper ved relasjoner

- Vi skal nå se på noen viktige egenskaper ved binære relasjoner:
  - Refleksivitet
  - Symmetri
  - Transitivitet
  - Anti-symmetri
  - Irrefleksivitet
- Følgende avsnitt i boken regnes som pensum.

  Kapittel 4.1, side 194–195: *Properties of Binary Relations*

Refleksivitet

Definisjon (Refleksiv).
En binær relasjon R på mengden S er *refleksiv* (eng: *reflexive*) hvis det for alle x i S er slik at $\langle x,x\rangle \in R$.

Eksempel.
La $S = \{1,2,3\}$.

- Er $\{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle\}$ en refleksiv relasjon på S?
- Hva med $\{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle\}$?

Symmetri

Definisjon (Symmetrisk).
En binær relasjon R på mengden S er *symmetrisk* (eng: *symmetric*) hvis det for alle x, y er slik at hvis $\langle x, y\rangle \in R$, så $\langle y, x\rangle \in R$.

Eksempel.
La $S = \{a, b, c\}$.

- Er $\{\langle a, b\rangle, \langle b, a\rangle, \langle c, b\rangle, \langle b, c\rangle\}$ en symmetrisk relasjon på S?
- Hva med $\{\langle a, b\rangle, \langle b, a\rangle, \langle a, c\rangle\}$?

Transitivitet

Definisjon (Transitiv).
En binær relasjon R på mengden S er *transitiv* (eng: *transitive*) hvis det for alle x, y, z er slik at hvis $\langle x, y\rangle \in R$ og $\langle y, z\rangle \in R$, så $\langle x, z\rangle \in R$.

Eksempel.
La $S = \{x, y, z\}$.

- Er $\{\langle x, y\rangle, \langle y, z\rangle, \langle x, z\rangle\}$ en transitiv relasjon på S?
- Hva med $\{\langle x, y\rangle, \langle y, z\rangle, \langle x, z\rangle, \langle y, x\rangle\}$?

Ekvivalens

Definisjon (Ekvivalensrelasjon).
En binær relasjon på mengden S er en *ekvivalensrelasjon* (eng: *equivalence relation*) hvis den er refleksiv, symmetrisk og transitiv.

Eksempel.
La $S = \{1, 2, 3\}$.

- Er $\{\langle 1,1\rangle, \langle 2,1\rangle, \langle 1,2\rangle\}$ en ekvivalensrelasjon på S?
- Hva med $\{\langle 1,1\rangle, \langle 2,1\rangle, \langle 1,2\rangle, \langle 2,2\rangle\}$?

Anti-symmetri

Definisjon (Anti-symmetrisk).
En binær relasjon R på mengden S er *anti-symmetrisk* (eng: *anti-symmetric*) hvis det for alle x, y er slik at hvis $\langle x, y\rangle \in R$ og $\langle y, x\rangle \in R$, så $x = y$.

Eksempel.
La $S = \{1, 2, 3\}$.

- Er $\{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle\}$ en anti-symmetrisk relasjon på S?
- Hva med $\{\langle 1,2\rangle, \langle 2,1\rangle\langle 1,3\rangle, \langle 2,3\rangle\}$?

Irrefleksivitet

Definisjon (Irrefleksiv).
En binær relasjon R på mengden S er *irrefleksiv* (eng: *irreflexive*) hvis det ikke fins noen $x \in S$ slik at $\langle x, x\rangle \in R$.

Eksempel.
La $S = \{1, 2, 3\}$.

- Er $\{\langle 1,2\rangle, \langle 2,1\rangle\}$ en irrefleksiv relasjon på S?
- Hva med $\{\langle 3,1\rangle, \langle 3,2\rangle, \langle 3,3\rangle\}$?

Eksempler

Vi ser på "er sønnen til"-relasjonen på mengden av alle mennesker.

- Refleksiv? `Nei`, det fins en som ikke er sin egen sønn.
- Symmetrisk? `Nei`, fordi "X er sønnen til Y" ikke medfører at "Y er sønnen til X".

- Transitiv? `Nei`, "X er sønnen til Y" og "Y er sønnen til Z" ikke medfører at "X er sønnen til Z".
- Antisymmetrisk? `Ja`, fordi "X er sønnen til Y" og "Y er sønnen til X" aldri er sanne samtidig.
- Irrefleksiv? `Ja`, ingen er sin egen sønn.
- Ekvivalensrelasjon? `Nei`, den er hverken refleksiv, symmetrisk eller transitiv.

Vi ser på "er større enn eller lik"-relasjonen ($\geqslant$) på mengden av reelle tall

- Refleksiv? `Ja`, alle reelle tall er like seg selv.
- Symmetrisk? `Nei`, f.eks. har vi $3 \geqslant 2$, men det er ikke slik at $2 \geqslant 3$.
- Transitiv? `Ja`, hvis $x \geqslant y$ og $y \geqslant z$, så vil $x \geqslant z$.
- Antisymmetrisk? `Ja`, hvis $x \geqslant y$ og $y \geqslant x$, så vil $x = y$.
- Irrefleksiv? `Nei`, f.eks. har vi at $1 \geqslant 1$.
- Ekvivalensrelasjon? `Nei`, den er ikke symmetrisk.

Litt om funksjoner

Læreboken

- Følgende avsnitt i boken regnes som pensum.

  Kapittel 2.1.1, side 74–78: *Definition of a Function*

Funksjoner

Definisjon (Funksjon).

- La A og B være mengder.
- Anta at hvert element i A assosieres med *nøyaktig* ett element i B.
- En slik assosiasjon kalles en *funksjon* fra A til B.
- Mengdeteoretisk har vi følgende, litt mer presise, definisjon.
- En *funksjon* fra A til B en binær relasjon f fra A til B slik at for enhver $x \in A$ så fins et *unikt* element $y \in B$ slik at $\langle x, y \rangle \in f$. Vi skriver $f(x) = y$ når $\langle x, y \rangle \in f$.
- A kalles *definisjonsområdet* (eng: *domain*) til f.
- B kalles *verdiområdet* (eng: *codomain*) til f.

- Det er vanlig å skrive $f : A \to B$ for funksjonen f når den er en funksjon fra A til B.
- $f(x) = y$ kan leses på flere måter, bl.a. slik:
  - "f av x er lik y"
  - "f sender x til y"
  - "f mapper x til y"
  - "f anvendt på x gir y"
- Viktig å huske på:
  - En funksjon kan ikke sende et element i definisjonsområdet til to *forskjellige* elementer i verdiområdet.

– En funksjon skal sende *ethvert element* i definisjonsområdet til et element i verdiområdet.

Eksempel.
Funksjonen $\mathtt{Par} : \mathbb{N} \to \{0, 1\}$ definert ved $\mathtt{Par}(x) = \begin{cases} 1 \text{ hvis } x \text{ er et partall} \\ 0 \text{ hvis } x \text{ er et oddetall} \end{cases}$ har $\mathbb{N}$ som definisjonsmengde og $\{0, 1\}$ som verdimengde.

Operatorer

Definisjon (Operator).
La S være en mengde.

- En *unær operator* (eng: *unary operator*) på S er en funksjon fra S til S.
- En *binær operator* (eng: *binary operator*) på S er en funksjon fra $S \times S$ til S.

Eksempel.

- Suksessorfunksjonen $(n + 1)$ er en unær operator på $\mathbb{N}$.
- Addisjonsfunksjonen $(+)$ er en binær operator på $\mathbb{N}$.
- Subtraksjonsfunksjonen $(-)$ er en binær operator på $\mathbb{Z}$.

INF1800 – Forelesning 4

Utsagnslogikk – Syntaks og semantikk

Roger Antonsen - 27. august 2008

Før vi begynner

Praktiske opplysninger

- Kursets hjemmeside blir stadig oppdatert: `http://www.uio.no/studier/emner/matnat/ifi/INF1800/h08/`
- Undervisningsplanen og forelesningsnotatene: `/undervisningsplan.xml`
- Oppgaver til gruppetimene: `/oppgaver.html`
- Ressurser: `/ressurser.html`
- Beskjeder: `/beskjeder.xml`
- Spørreskjema kommer!
- Obligatorisk oppgave 1 – innlevering to uker fra fredag.

Forelesningene og læreboken

- I denne delen legger vi mest vekt på forelesningsnotatene.
- Forelesningsnotatene kan leses helt uavhengig av boken.
- Noen steder vil vi være mer presis enn boken, og andre steder vil boken si mer enn det vi gjør her.
- Følgende avsnitt i boken regnes som pensum.
  - Kapittel 1.1.1, side 2–5: *Logical Statements*
  - Kapittel 6.1, side 345–348: *How Do We Reason?*
  - Kapittel 6.2, side 348–369: *Propositional Calculus*
  - Kapittel 6.5, side 394–395: *Chapter Summary*

Utsagnslogikk

Utsagnslogikk handler om utsagn

- Temaet for de neste ukene er utsagnslogikk.
- Hva er et utsagn?
- La oss definere det!

Definisjon (Utsagn).
Et *utsagn* (eng: *proposition*) er noe som enten er sant eller usant.

- Dette "noe" kan være en setning, ytring eller meningsinnholdet til slike.
- Vi skal ikke gå nærmere inn på den filosofiske analysen av hva et utsagn er. Vi skal være ganske liberale i hva vi anser som utsagn.

Sånt som ikke er utsagn

Følgende er setninger/ytringer som ikke er utsagn.

- *Når er eksamen?*
- *Hipp, hipp, hurra!*
- *Kom hit!*
- *Måtte nysgjerrigheten blant studentene blomstre.*

Et nyttig prinsipp for å forstå noe er å også forstå *det motsatte*, i dette tillfellet hva et utsagn *ikke* er!

- Det viktige når vi betrakter noe som et utsagn, er at vi ser bort fra alt annet enn egenskapen at den vil være sann eller usann.

Atomære utsagn

- Vi starter med en mengde atomære (eng: *atomic*) utsagn, f.eks.
  - *Matematikk er spennende.*
  - *Uten mat og drikker, duger helten ikke.*
  - *Foreleseren kan sjonglere.*
  - *Det fins mengder som ikke er tellbare.*
  - *Studenter drikker for mye.*
  - $5 + 6 = 4$
- Den interne strukturen til atomære utsagn blir ikke analysert.
- Etter hvert skal vi lære første-ordens logikk, og da skal vi analysere utsagn i større detalj.

Syntaks for atomære utsagn: Utsagnsvariable

Definisjon (Utsagnsvariable).
Mengden av *utsagnsvariable* (eng: *propositional variables*) er en tellbart uendelig mengde $\{P, Q, R, \ldots\}$ av symboler.

- Utsagnsvariable representerer atomære utsagn.
- Nøyaktig hva som er i mengden av utsagnsvariable er ikke så nøye. Det som er viktig er at vi har *nok* utsagnsvariable til å uttrykke det vi ønsker.
- Mengden av utsagnsvariable er en del av syntaksen til utsagnslogikk. I utgangspunktet kan symbolene bety hva som helst.

Sammensatte utsagn

- Fra atomære utsagn kan vi bygge opp sammensatte utsagn ved hjelp av logiske bindeord, som f.eks.:

  og *eller* *ikke* *hvis . . . så . . .*

- Eksempler:
  - *Studenter drikker for mye og* $5 + 6 = 4$*”*
  - *Hvis matematikk er spennende, så er fysikk spennende.*
  - *Jeg er glad eller jeg er ikke glad.*
- Vi skal bl.a. se på følgende spørsmål:
  - 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.)

Syntaks for sammensatte utsagn

- For å fange slike inn sammensatte utsagn, f.eks.

  Hvis man trener, så blir man sterk.

  trenger vi altså flere symboler i språket.
- I dette tilfellet har vi to naturlige *atomære* utsagn:
  - *man trener*
  - *man blir sterk*
- Disse utsagnene kan representeres ved hjelp av utsagnsvariablene T og S, henholdsvis.
- Det sammensatte utsagnet kan representeres ved hjelp av den utsagnslogiske formelen $(\mathsf{T} \to \mathsf{S})$.
- Dette skal vi se nærmere på nå.

Konnektiver

Definisjon (Konnektiv).
De *logiske konnektivene* (eng: *connective*) er $\wedge$, $\vee$, $\to$ og $\neg$.

- Intuisjonen bak disse er følgende:
  - $\neg$ skal bety *ikke*
  - $\wedge$ skal bety *og*
  - $\vee$ skal bety *eller*
  - $\to$ skal bety *impliserer* eller *hvis-så*
- Konnektivene er en del av syntaksen; de er symboler vi skal bruke for å sette mindre formler (fra utsagnsvariable) sammen til større.
- Vi skal også bruke parenteser som hjelpesymboler.

Utsagnslogiske formler

- Vi skal nå definere mengden av utsagnslogiske formler.
- Denne mengden kaller vi **Prop**, for *propositional*.
- Husk: vi er fortsatt kun opptatt av syntaksen. Snart skal vi se hvordan disse formlene kan *tolkes*.
- Den enkleste utsagnslogiske formelen er utsagnsvariabelen.
- Det er vanlig å kalle en utsagnsvariabel for en *atomær* formel, så vi fanger opp det i en definisjon.

Definisjon (Atomær formel).
Enhver utsagnsvariabel er en *atomær formel* (eng: *atomic formula*).

Definisjon (Utsagnslogisk formel).
Mengden av *utsagnslogiske formler* (eng: *propositional formula/well-formed formula*) er den minste mengden **Prop** slik at:

1. **Prop** inneholder alle atomære formler.
2. Hvis $F \in$ **Prop**, så er $\neg F \in$ **Prop**.
3. Hvis $F, G \in$ **Prop**, så er $(F \wedge G)$, $(F \vee G)$ og $(F \to G)$ med i **Prop**.

- Det er den *minste* mengden som oppfyller 1-3 vi er ute etter.
- Forsøk å se for dere dette som en løk. Det innerste skallet består av atomære formler. Det neste skallet av formler med ett konnektiv, og så videre.
- Vi definerte nå *helt presist* en mengde **Prop**.
- Når vi snakker om utsagnslogiske formler, så mener vi altså denne mengden.
- Denne mengden er en mengde av *syntaktiske* objekter. (Foreløpig har vi ikke definert semantikken til utsagnslogiske formler.)
- Boka kaller en utsagnslogisk formel for en well-formed formula (wff), en velformet formel.
- Hvis det går klart frem hva vi mener, så sier vi bare formler.

Eksempel (Utsagnslogiske formler).

- P, Q, R, S, T
- $\neg P, (Q \wedge R), (S \to T)$
- $(\neg P \vee (Q \wedge R)), \neg(S \to T)$
- $\neg(\neg P \vee (Q \wedge R)), \neg\neg(S \to T)$

Notasjon.
Vi dropper ofte unødvendige parenteser:

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

Eksempel.
Ikke alle strenger over det utsagnslogiske alfabet er utsagnslogiske formler:

- $P \to$
- $\to\to$
- $((Q \wedge P)$

Semantikk

Semantikk

- Vi skal tolke utsagnslogiske formler som sanne eller usanne.
- Semantikken skal fortelle oss hva formler betyr.
- Matematisk sett er dette en helt presis disiplin; alt blir definert fra bunnen av.
- Vi skal holde et skarpt skille mellom syntaks (formler, symboler, tegn) og semantikk (meningen til symbolene, sannhetsverdiene, modellene), for å unngå forvirring.

Sannhetsverdier

Definisjon (Sannhetsverdi).
La **Bool** $= \{\mathbf{0}, \mathbf{1}\}$. Dette er mengden av *sannhetsverdier* (eng: *truth values*).

- Det finnes mange andre bokstaver eller symboler man kan anvende for å betegne sannhetsverdiene.
  - true og false (som i læreboken)
  - T og F
  - $\top$ og $\bot$
  - True og False
  - sann og usann (ordet "gal" anbefales ikke)
  - **S** og **U**
- Jeg anbefaler å bruke **0** og **1** i dette kurset.

Negasjon (ikke)

- Hvis F er et utsagn, så er *negasjonen* (eng: *negation*) til F utsagnet *ikke* F.
- Dette gjenspeiles i syntaksen slik:
  - Hvis $F \in$ **Prop**, så er $\neg F \in$ **Prop**.
- Sannhetsverdien til $\neg F$ avhenger av sannhetsverdien til F på følgende måte.

F	$\neg F$
1	**0**
0	**1**

Konjunksjon (og)

- Hvis F og G er utsagn, så er *konjunksjonen* (eng: *conjuction*) av F og G utsagnet F *og* G.
- Dette gjenspeiles i syntaksen slik:
  - Hvis $F, G \in$ **Prop**, så er $(F \wedge G) \in$ **Prop**.
  - F og G kalles ofte *konjunktene* (eng: *conjunct*).
- Sannhetsverdien til $(F \wedge G)$ avhenger av sannhetsverdiene til F og G på følgende måte.

F	G	$(F \wedge G)$
1	**1**	**1**
1	**0**	**0**
0	**1**	**0**
0	**0**	**0**

Disjunksjon (eller)

- Hvis F og G er utsagn, så er *disjunksjonen* (eng: *disjunction*) av F og G utsagnet F *eller* G.
- Dette gjenspeiles i syntaksen slik:
  - Hvis $F, G \in$ **Prop**, så er $(F \vee G) \in$ **Prop**.
  - F og G kalles ofte *disjunktene* (eng: *disjunct*).
- Sannhetsverdien til $(F \vee G)$ avhenger av sannhetsverdiene til F og G på følgende måte.

F	G	$(F \vee G)$
1	**1**	**1**
1	**0**	**1**
0	**1**	**1**
0	**0**	**0**

Implikasjon (hvis, så)

- Hvis F og G er utsagn, så er *implikasjonen* (eng: *implication*) mellom F og G utsagnet *hvis* F, *så* G.
- Dette gjenspeiles i syntaksen slik:
  - Hvis $F, G \in$ **Prop**, så er $(F \rightarrow G) \in$ **Prop**.

- Sannhetsverdien til $(F \to G)$ avhenger av sannhetsverdiene til F og G på følgende måte.

F	G	$(F \to G)$
1	**1**	**1**
1	**0**	**0**
0	**1**	**1**
0	**0**	**1**

INF1800 – Forelesning 5

Utsagnslogikk – Syntaks og semantikk

Roger Antonsen - 2. september 2008

Praktisk informasjon

Endringer i undervisningen

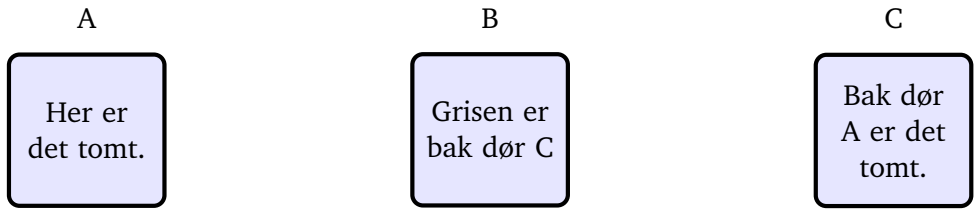
- Lars overtar neste uke med *beregnbarhet*.
- Det blir minst fire uker med beregnbarhet før jeg kommer tilbake og fortsetter med logikkdelen.
- Fra og med neste uke utgår onsdagsforelesningene (09:15–10:00) og tirsdagsforelesningene blir én time lenger. *Forelesningene vil gå som normalt hvis ikke annet er spesifisert!*
- Det vil si at tirsdagsforelesingene vil gå fra 14:15 til 17:00.

Spørreskjemaet

- Fyll ut!
- For at det skal bli et bra kurs trenger vi tilbakemeldinger fra dere.
- Hvis mange nok har svart i løpet av i morgen (onsdag), kommer jeg med et lite sammendrag.
- Foreløpig (13:30) har 12 av 75 svart. Siden skjemet har vært ute kun siden 08:00 i morges, syns jeg det er helt ok.

Oppvarming

Hvordan tjene en million på logikk



- Følgende informasjon er gitt.
  - Bak èn av dørene ligger det en million kroner. Det som står på denne døren er *sant*.
  - Bak en annen dør er det en gris. Det som står på denne døren er *usant*.
  - Bak én dør er det tomt.
- Hvor ligger millionen?
  - Bak dør A? `Nei` Bak dør B? `Nei` Bak dør C? `Ja`

Repetisjon

- Utsagn: noe som enten er sant eller usant.
- Utsagnsvariable: symboler $\{P, Q, R, \ldots\}$ som vi bruker til å representere utsagn.
- Logiske bindeord: *og*, *eller*, *ikke*, *hvis-så*, ...
- Konnektiver: $\wedge$, $\vee$, $\neg$ og $\rightarrow$.
- Utsagnslogiske formler: mengden **Prop** som er bygget opp av utsagnsvariable og konnektiver.
- Sannhetsverdier: $\mathbf{Bool} = \{\mathbf{1}, \mathbf{0}\}$.
- Hvordan sannhetsverdiene til en formel avhenger av sannhetsverdiene til utsagnsvariablene.
- Synaks: **Prop**, $\{P, Q, R, \ldots\}$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, parenteser, ...
- Semantikk: **Bool**, sannhetsverdier, mening, utsagn, ...

Eksempler & Sannhetsverditabeller

Eksempel 1

Hvis solen skinner, så er jeg glad.	$(S \rightarrow G)$
Solen skinner.	S
Jeg er glad.	G

- Dette er et eksempel på et *gyldig* eller *holdbart* (eng: *valid*) argument.
- Hvis $(S \rightarrow G)$ er sann og S er sann, så må også G være sann.
- Vi sier at G er en *logisk konsekvens* (eng: *logical consequence*) av $(S \rightarrow G)$ og S.
- Vi skal si dette på en mer presis måte ved å la ν være en funksjon fra utsagnslogiske formler til $\{\mathbf{0}, \mathbf{1}\}$.
  - Hvis $\nu(S \rightarrow G) = \mathbf{1}$ og $\nu(S) = \mathbf{1}$, så $\nu(G) = \mathbf{1}$.

Eksempel 2

Hvis solen skinner, så er jeg glad.	$(S \rightarrow G)$
Jeg er ikke glad.	$\neg G$
Solen skinner ikke.	$\neg S$

- Dette er også et eksempel på et *gyldig* argument.
- En sannhetsverditabell kan brukes til å analysere argumentet.

S	G	$(S \rightarrow G)$	$\neg G$	$\neg S$
1	**1**	**1**	**0**	**0**
1	**0**	**0**	**1**	**0**
0	**1**	**1**	**0**	**1**
0	**0**	**1**	**1**	**1**

- Det er den nederste raden som er relevant, for det er kun her både $(S \rightarrow G)$ og $\neg G$ sanne. Vi ser at også $\neg S$ er sann da.

Eksempel 3

Hvis solen skinner, så er jeg glad.	$(S \rightarrow G)$
Solen skinner ikke.	$\neg S$
Jeg er ikke glad.	$\neg G$

- Dette er *ikke* et gyldig argument.
- Det er fordi $(S \rightarrow G)$ og $\neg S$ kan begge være sanne uten at $\neg G$ er det. (Jeg kan være glad selv om solen ikke skinner.)
- Med andre ord, $\neg G$ er *ikke* en logisk konsekvens av $(S \rightarrow G)$ og $\neg S$.
- Vi kan også se dette via (en rad i) en sannhetsverditabell.

S	G	$(S \rightarrow G)$	$\neg S$	$\neg G$
0	**1**	**1**	**1**	**0**

Sannhetsverditabeller

- En *sannhetsverditabell* (eng: *truth table*) forteller hva sannhetsverdien til en sammensatt utsagnslogisk formel er på bakgrunn av hvilke sannhetsverdier som er tilordnet utsagnsvariablene.
- Sagt på en annen måte: Hvis en tilordning av sannhetsverdier til utsagnsvariablene er gitt, så kan vi bruke en sannhetsverditabell til å regne ut sannhetsverdiene til de sammensatte utsagnene.
- Vi så forrige gang sannhetsverditabellene for konnektivene.
- Disse tabellene definerer meningen til de fire konnektivene.
- Vi ser på tabellene en gang til.

F	$\neg F$
1	**0**
0	**1**

F	G	$(F \wedge G)$
1	**1**	**1**
1	**0**	**0**
0	**1**	**0**
0	**0**	**0**

F	G	$(F \vee G)$
1	**1**	**1**
1	**0**	**1**
0	**1**	**1**
0	**0**	**0**

F	G	$(F \rightarrow G)$
1	**1**	**1**
1	**0**	**0**
0	**1**	**1**
0	**0**	**1**

Semantikk for utsagnslogikk

Valuasjoner

Definisjon (Valuasjon).
En *valuasjon* (eng: *valuation*) er en funksjon ν fra **Prop** til **Bool** slik at:

- $\nu(\neg A) = \mathbf{1}$ hvis og bare hvis $\nu(A) = \mathbf{0}$
- $\nu(A \wedge B) = \mathbf{1}$ hvis og bare hvis $\nu(A) = \mathbf{1}$ *og* $\nu(B) = \mathbf{1}$
- $\nu(A \vee B) = \mathbf{1}$ hvis og bare hvis $\nu(A) = \mathbf{1}$ *eller* $\nu(B) = \mathbf{1}$
- $\nu(A \to B) = \mathbf{1}$ hvis og bare hvis $\nu(A) = \mathbf{1}$ *impliserer* $\nu(B) = \mathbf{1}$.

- Meningen til *og*, *eller* og *impliserer* betraktes som definert av sannhetsverditabellene for konnektivene.
- Det siste punktet kunne ha vært slik:
  - $\nu(A \to B) = \mathbf{1}$ hvis og bare hvis $\nu(A) = \mathbf{0}$ *eller* $\nu(B) = \mathbf{1}$.
- En valuasjon er en presisering av "en tilordning av sannhetsverdier".
- En valuasjon svarer til *en rad* i en sannhetsverditabell.
- En sannhetsverditabell kan altså si noe om *alle* valuasjoner.
- Når vi gir en valuasjon, så behøver vi kun gi verdier for utsagnsvariablene.
- Verdiene for utsagnslogiske formler er dermed også gitt (ved definisjonen av en valuasjon).
- Vi sier at vi har en *tilordning av sannhetsverdier* (eng: *assignment of truth values*) til utsagnsvariable.
- Vi skal se på noen eksempler for å få en bedre forståelse av hva en valuasjon er.

Eksempel.
- Se på formelen $(P \wedge \neg Q)$.
- La ν være en valuasjon slik at $\nu(P) = \mathbf{1}$ og $\nu(Q) = \mathbf{0}$.
- Hva er $\nu(P \wedge \neg Q)$?
- Definisjonen sier
  - $\nu(P \wedge \neg Q) = \mathbf{1}$ hvis og bare hvis $\nu(P) = \mathbf{1}$ og $\nu(\neg Q) = \mathbf{1}$.
- Vi vet at $\nu(P) = \mathbf{1}$, så det holder å sjekke om $\nu(\neg Q) = \mathbf{1}$.
- Definisjonen sier
  - $\nu(\neg Q) = \mathbf{1}$ hvis og bare hvis $\nu(Q) = \mathbf{0}$.
- Siden $\nu(Q) = \mathbf{0}$, så er det greit.
- Vi konkluderer med at $\nu(P \wedge \neg Q) = \mathbf{1}$.

Eksempel.

- En alternativ måte å finne frem til dette på er ved å se på kun én rad i sannhetsverditabellen.
- Valuasjonen ν som er slik at $\nu(\mathrm{P}) = \mathbf{1}$ og $\nu(\mathrm{Q}) = \mathbf{0}$ kan representeres ved å sette **1** under P og **0** under Q.
- Deretter kan vi bruke sannhetsverditabellene som definerer meningen til konnektivene for å finne sannhetsverdien til hele uttrykket.
- Vi må arbeide oss "innenfra og utover".

P	$\wedge$	$\neg$	Q
1	**1**	**1**	**0**

Eksempel.

- Se på formelen $(\neg\mathrm{P} \to \mathrm{Q})$.
- La ν være en valuasjon slik at $\nu(\mathrm{P}) = \mathbf{1}$ og $\nu(\mathrm{Q}) = \mathbf{0}$.
- Hva er $\nu(\neg\mathrm{P} \to \mathrm{Q})$?
- Definisjonen sier
  - $\nu(\neg\mathrm{P} \to \mathrm{Q}) = \mathbf{1}$ hvis og bare hvis $\nu(\neg\mathrm{P})$ impliserer $\nu(\mathrm{Q})$.
- $\nu(\neg\mathrm{P}) = \mathbf{0}$ og $\nu(\mathrm{Q}) = \mathbf{0}$.
- Siden **0** impliserer **0**, konkluderer vi med at $\nu(\neg\mathrm{P} \to \mathrm{Q}) = \mathbf{1}$.
- En rad i en sannhetsverditabell ville ha gitt oss følgende:

$\neg$	P	$\to$	Q
0	**1**	**1**	**0**

Oppfyllbarhet

Definisjon (Oppfyllbarhet).

- En valuasjon ν *oppfyller* (eng: *satisfies*) en utsagnslogisk formel A hvis $\nu(\mathrm{A}) = \mathbf{1}$. Dette skrives ofte $\nu \models \mathrm{A}$.
- En utsagnslogisk formel er *oppfyllbar* (eng: *satisfiable*) hvis det fins en valuasjon som oppfyller den.

Eksempel.

- Formelen $(P \to Q)$ er oppfyllbar; den oppfylles av enhver valuasjon ν slik at $\nu(P) = \mathbf{0}$ eller $\nu(Q) = \mathbf{1}$.
- Formelen $(P \wedge \neg P)$ er *ikke* oppfyllbar; det fins ingen valusjon ν slik at både $\nu(P) = \mathbf{1}$ og $\nu(\neg P) = \mathbf{1}$.

Falsifiserbarhet

Definisjon (Falsifiserbarhet).

- En valuasjon ν *falsifiserer* (eng: *falsifies*) en utsagnslogisk formel A hvis $\nu(A) = \mathbf{0}$. Dette skrives ofte $\nu \not\models A$.
- En utsagnslogisk formel er *falsifiserbar* (eng: *falsifiable*) hvis det fins en valuasjon som falsifiserer den.

Eksempel.

- Formelen $(P \to Q)$ er falsifiserbar; den falsifiseres av enhver valuasjon ν slik at $\nu(P) = \mathbf{1}$ og $\nu(Q) = \mathbf{0}$.
- Formelen $(P \vee \neg P)$ er *ikke* falsifiserbar; det fins ingen valusjon ν slik at både $\nu(P) = \mathbf{0}$ og $\nu(\neg P) = \mathbf{0}$.

Tautologi / Gyldighet

Definisjon (Tautologi / Gyldighet).
En utsagnslogisk formel A er en *tautologi* (eng: *tautology*) eller er *gyldig* (eng: *valid*) hvis $\nu(A) = \mathbf{1}$ for *alle* valuasjoner ν. Dette skrives ofte $\models A$.

Eksempel.

- Formelen $(P \vee \neg P)$ er en tautologi; for enhver valuasjon ν så vil enten $\nu(P) = \mathbf{1}$ eller $\nu(\neg P) = \mathbf{1}$.
- Formelen P er *ikke* en tautologi; det fins nemlig en valusjon ν slik at $\nu(P) = \mathbf{0}$.

Motsigelse / Kontradiksjon

Definisjon (Motsigelse / Kontradiksjon).
En utsagnslogisk formel A er *kontradiktorisk* (eng: *contradictory*), eller en *kontradiksjon* (eng: *contradiction*), eller en *motsigelse*, hvis $\nu(A) = \mathbf{0}$ for *alle* valuasjoner ν.

Eksempel.

- Formelen $(P \wedge \neg P)$ er kontradiktorisk; det fins ingen valuasjon ν som er slik at $\nu(P) = \mathbf{1}$ og $\nu(\neg P) = \mathbf{1}$.
- Formelen P er *ikke* kontradiktorisk; det fins nemlig en valusjon ν slik at $\nu(P) = \mathbf{1}$.

Oppsummering av disse begrepene

En formel er ...

- oppfyllbar hvis det er *mulig* å gjøre den sann.

  (Det fins en valuasjon ν slik at $\nu(A) = \mathbf{1}$.)
- falsifiserbar hvis det er *mulig* å gjøre den usann.
- gyldig hvis den *alltid* er sann.

  (For enhver valuasjon ν, så er det slik at $\nu(A) = \mathbf{1}$.)
- kontradiktorisk hvis den *alltid* er usann.

Merk.

- Det motsatte av en tautologi er en falsifiserbar formel.
- Det motsatte av en motsigelse er en oppfyllbar formel.
- En tautologi er *ikke* det motsatte av en motsigelse!

Eksempler

Eksempel.

- Er $\neg P$ en kontradiksjon?

  `Nei`, fordi det fins en valuasjon ν slik at $\nu(\neg P) = \mathbf{1}$.
- Er $\neg(P \to P)$ en kontradiksjon?

  `Ja`, fordi $\nu(\neg(P \to P)) = \mathbf{0}$ for enhver valuasjon ν.

– Det er lett å se dette ved hjelp av en sannhetsverditabell:

P	¬	(P → P)
1	**0**	**1**
0	**0**	**1**

- Er $(P \to P)$ en kontradiksjon?

  Nei, fordi det fins en valuasjon ν slik at $\nu(P \to P) = \mathbf{1}$.

Eksempel.

- Er $((P \vee Q) \to P)$ en tautologi?

  Nei, fordi det fins en valuasjon ν slik at $\nu((P \vee Q) \to P) = \mathbf{0}$.

  – Vi kan bruke en sannhetsverditabell for å se dette:

P	Q	((P	∨	Q)	→	P)
1	**0**	1	**1**	0	**1**	1
1	**1**	1	**1**	1	**1**	1
0	**1**	0	**1**	1	**0**	0
0	**0**	0	**0**	0	**1**	0

  – Den aktuelle valuasjonen kan leses ut av rad tre.

  – Den er slik at $\nu(P) = \mathbf{0}$ og $\nu(Q) = \mathbf{1}$.

Eksempel.

- Er $(P \to (P \vee Q))$ en tautologi?

  Ja, fordi enhver valuasjon ν er slik at $\nu(P \to (P \vee Q)) = \mathbf{1}$.

  Grunnen til dét er at hvis $\nu(P) = \mathbf{1}$, så vil også $\nu(P \vee Q) = \mathbf{1}$.

- Er $(P \to P)$ en tautologi?

  Ja, fordi enhver valuasjon ν er slik at $\nu(P \to P) = \mathbf{1}$.

Noen viktige begreper

- 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 (eng: *calculus*) — syntaktisk manipulasjon av uttrykk i symbolspråket for å finne bevisbare uttrykk.

- Sunnhet (eng: *soundness*) — alle bevisbare uttrykk er tautologier (korrekthet av kalkylen).
- Kompletthet (eng: *completeness*) — alle tautologier er bevisbare (kalkylen sterk nok til å fange inn *alle* interessante uttrykk).

Bruk av utsagnslogikk

Hvordan fange inn utsagn?

Griser liker polka.	P
Griser liker disco.	Q
Griser liker ikke disco.	$\neg Q$
Griser liker disco og polka.	$(P \wedge Q)$
Hvis griser liker polka, så liker de disco.	$(P \rightarrow Q)$
Griser liker hverken polka eller disco.	$(\neg P \wedge \neg Q)$ eller $\neg(P \vee Q)$
Griser liker enten polka eller disco.	$(P \vee Q)$
Griser liker polka eller liker ikke polka.	$(P \vee \neg P)$
Griser liker polka hvis de liker disco.	$(Q \rightarrow P)$
Griser liker polka bare hvis de liker disco.	$(P \rightarrow Q)$

- Hvis jeg vinner i lotto eller står på eksamen, så blir jeg glad.
  - L = jeg vinner i lotto
  - E = jeg står på eksamen
  - G = jeg blir glad
  - Vi kan representere utsagnet ved formelen $((L \vee E) \rightarrow G)$.
- Jeg blir glad hvis og bare hvis jeg vinner i lotto.
  - Vi kan dele denne påstanden inn i to:
  - Jeg blir glad hvis jeg vinner i lotto: $(L \rightarrow G)$
  - Jeg blir glad bare hvis jeg vinner i lotto: $(G \rightarrow L)$
  - Vi får dermed utsagnet: $(G \rightarrow L) \wedge (L \rightarrow G)$
  - Vi kan godt bruke konnektivet $\leftrightarrow$ og skrive: $(G \leftrightarrow L)$.
  - Da leser vi $(G \leftrightarrow L)$ som en forkortelse for $(G \rightarrow L) \wedge (L \rightarrow G)$.

INF1800 – Forelesning 6

Utsagnslogikk – Syntaks og semantikk

Roger Antonsen - 3. september 2008

Mer om bruk av utsagnslogikk

Hvordan fange inn utsagn?

- Jeg spiser det hvis det er godt.
  - Jeg spiser det $\leftarrow$ det er godt.
  - Det er godt $\rightarrow$ jeg spiser det.
    (Med andre ord, jeg er glupsk.)
- Jeg spiser det bare hvis det er godt.
  - Jeg spiser det $\rightarrow$ det er godt.
    (Med andre ord, jeg er kresen.)
- Jeg spiser det hvis og bare hvis det er godt.
  - Jeg spiser det $\leftrightarrow$ det er godt.
  - Jeg spiser det hviss det er godt.
    (Med andre ord, jeg er glupsk, men kresen.)
  - På engelsk: I eat it iff it is good.

Nødvendig og tilstrekkelig

- Formelen $A \rightarrow B$ uttrykker *hvis* A*, så* B.
- Det er verdt å tenke litt over hva som ligger i det.
- A er en tilstrekkelig betingelse for B.
  - Det er *nok* at A er sann for at B også skal være sann.
  - B kan være sann uten at A er sann, men *hvis* A er sann, *så* må B være sann.
- B er en nødvendig betingelse for A.
  - A kan ikke være sann uten at B også er sann.
  - A er sann bare hvis B er sann.
- Alt dette betyr det samme, nemlig at *hvis* A*, så* B.

Mer syntaks

Presedensregler

- Vi kan være ganske frie når vi skriver utsagnslogiske formler, men da må vi ha noen konvensjoner som fjerner tvetydigheter.
- Mengden **Prop** er helt presist definert, men vi skal også godta f.eks. $P \vee Q$ og $P \vee Q \rightarrow R$ som utsagnslogiske formler (selv om parentesene mangler).

- Vi gir konnektivene ulik *presedens* i forhold til hverandre.
  1. $\neg$ binder sterkest.
  2. $\wedge$ binder svakere enn $\neg$.
  3. $\vee$ binder svakere enn både $\neg$ og $\wedge$.
  4. $\rightarrow$ binder svakest.
- I tillegg er $\wedge$, $\vee$ og $\rightarrow$ *venstre-assosiative*.
- Vi skal se på eksempler på dette nå.

Eksempel.

- $\neg$ binder sterkere enn $\rightarrow$

  $\neg P \rightarrow Q$ betyr $(\neg P \rightarrow Q)$ og *ikke* $\neg(P \rightarrow Q)$.
- $\wedge$ binder sterkere enn $\rightarrow$

  $P \rightarrow Q \wedge R$ betyr $(P \rightarrow (Q \wedge R))$ og *ikke* $((P \rightarrow Q) \wedge R)$.
- $\rightarrow$ er venstre-assosiativ

  $P \rightarrow Q \rightarrow R$ betyr $((P \rightarrow Q) \rightarrow R)$ og *ikke* $(P \rightarrow (Q \rightarrow R))$.
- $\wedge$ og $\vee$ er venstre-assosiative og binder sterkere enn $\rightarrow$

  $P \wedge Q \wedge R \rightarrow S \vee T \vee U$ betyr $((P \wedge Q) \wedge R) \rightarrow ((S \vee T) \vee U)$

Symboler for sannhetsverdiene

- Det er ofte hensiktsmessig å ha utsagnslogiske formler som betegner sannhetsverdiene, **1** og **0**.
- Boka bruker true og false.
  - Det er også vanlig å bruke $\top$ og $\bot$.
- Vi må i så fall ta med følgende i definisjonen av mengden **Prop** av utsagnslogiske formler.
  - **Prop** inneholder true og false.
- Vi må også ha med følgende krav i definisjonen av en valuasjon.
  - $\nu(\mathsf{true}) = \mathbf{1}$ og $\nu(\mathsf{false}) = \mathbf{0}$.
- Så lenge vil følger disse konvensjonene, så er det greit å bruke true og false.

Mer semantikk

Ekvivalens

Definisjon (Ekvivalens).
To formler A og B er *ekvivalente* (eng: *equivalent*) hvis de har samme sannhetsverdi for enhver tilordning av sannhetsverdier til utsagnvariable. Sagt på en annen måte, for alle valuasjoner ν så vil $\nu(A) = \nu(B)$. Vi skriver $A \equiv B$ når A og B er ekvivalente. (En annen vanlig skrivemåte er $A \Leftrightarrow B$.)

- Hvis to formler er ekvivalente, så har de samme meningsinnhold.
- Hvis to formler *ikke* er ekvivalente, så fins en valuasjon som gjør den ene formelen sann, men ikke den andre.
- A og B er *ekvivalente* hvis og bare hvis $A \leftrightarrow B$ er en tautologi.

Eksempel.

- P og $\neg\neg P$ er ekvivalente.

  Hvis $v(P) = \mathbf{1}$, så er $v(\neg\neg P) = \mathbf{1}$.
  Hvis $v(P) = \mathbf{0}$, så er $v(\neg\neg P) = \mathbf{0}$.

Eksempel.

- $P \to Q$ og $\neg P \vee Q$ er ekvivalente.

  Hvis $v(P) = \mathbf{1}$ og $v(Q) = \mathbf{1}$, så er $v(P \to Q) = v(\neg P \vee Q) = \mathbf{1}$.
  Hvis $v(P) = \mathbf{1}$ og $v(Q) = \mathbf{0}$, så er $v(P \to Q) = v(\neg P \vee Q) = \mathbf{0}$.
  Hvis $v(P) = \mathbf{0}$ og $v(Q) = \mathbf{1}$, så er $v(P \to Q) = v(\neg P \vee Q) = \mathbf{1}$.
  Hvis $v(P) = \mathbf{0}$ og $v(Q) = \mathbf{0}$, så er $v(P \to Q) = v(\neg P \vee Q) = \mathbf{1}$.

- Dette er nøyaktig dette vi gjør når vi lager en sannhetsverditabell.

Viktige ekvivalenser

- De Morgans lover

  $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$
  $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

- Distributive lover

  $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
  $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

- Dobbel negasjon

  $\neg\neg A \equiv A$

- Implikasjon

  $A \to B \equiv \neg A \vee B$
  $\neg(A \to B) \equiv A \wedge \neg B$
  $A \to \mathsf{false} \equiv \neg A$

- Assosiative lover

  $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
  $A \vee (B \vee C) \equiv (A \vee B) \vee C$

- Kommutative lover

  $A \wedge B \equiv B \wedge A$

  $A \vee B \equiv B \vee A$
- Det er mange flere...

  Side 354: Figur 6.6: *Equivalences, conversions, basic laws.*
- Det er en fin øvelse å forsøke å forstå disse, men man trenger ikke å pugge dem.

Ekvivalenser som omskrivingsregler

Å erstatte likt med likt endrer ikke verdien til et uttrykk.

Definisjon (Substitusjonsregelen).
Hvis en utsagnslogisk formel A innholder en annen utsagnslogisk formel B, og B er ekvivalent med C, så kan B erstattes med C uten at sannhetsverdien til A endres. (eng: *Replacement Rule*)

Vi har en notasjon for å beskrive substitusjon.

- $A[B/C] = A$ hvor alle forekomster av B er erstattet med C.
- Substitusjonsregelen sier derfor:
  - Hvis $B \equiv C$, så $A \equiv A[B/C]$.
- Dette danner utgangspunktet for å transformere formler ved hjelp av omskrivingsregler.

Eksempel.

$$\begin{aligned}
(A \wedge B) \rightarrow C &\equiv \neg(A \wedge B) \vee C && \text{(implikasjon)} \\
&\equiv (\neg A \vee \neg B) \vee C && \text{(De Morgan)} \\
&\equiv \neg A \vee (\neg B \vee C) && \text{(assosiativitet)} \\
&\equiv \neg A \vee (B \rightarrow C) && \text{(implikasjon)} \\
&\equiv A \rightarrow (B \rightarrow C) && \text{(implikasjon)}
\end{aligned}$$

Normalformer

Hva er normalformer?

- Normalformer er forskjellige syntaktiske former som utsagnslogiske formler kan ha.
- Vi skal se på:
  - Disjunktiv normalform
  - Konjunktiv normalform
- Normalformer gjør oss i stand til å forenkle formler.
- Normalformer er viktig for *automatisk bevissøk*.
- Vi skal lære oss å transformere en formel til de ulike normalformene.

Literaler

Definisjon (Literal).
Et *literal* er en utsagnsvariabel eller negasjonen av en utsagnsvariabel. (Samt true og false hvis vi tar disse med i det utsagnslogiske språket.)

Eksempel.
Hvis P og Q er utsagnsvariable, så er P, $\neg P$, Q og $\neg Q$ literaler, men $P \wedge Q$ og $\neg\neg P$ er *ikke* literaler.

Disjunktiv normalform (DNF)

Definisjon.
En utsagnslogisk formel er på *disjunktiv normalform (DNF)* hvis den er en disjunksjon av en eller flere konjunksjoner og hvor hver konjunksjon består av en eller flere literaler. (En slik konjunksjon kalles i boka en *fundamental konjunksjon*.)

Eksempel.

- En formel som er på DNF:
  - $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$
- En formel som *ikke* er på DNF:
  - $(P \wedge Q) \vee (R \wedge (S \vee T))$ (fordi konjunksjonen ikke består av kun literaler)

- Vi godtar disjunksjoner med kun én disjunkt.
- Vi godtar konjunksjoner med kun én konjunkt.

Eksempel.

- $P \wedge (Q \vee R)$ er *ikke* på DNF, siden den er en konjunksjon.
- $P \wedge Q$ er på DNF. Det er fordi den er en disjunksjon som består av kun én konjunksjon. Denne konjunksjonen består igjen av to literaler.
- P er også på DNF. Det er fordi den er en disjunksjon som består av kun én konjunksjon. Denne konjunksjonen består igjen av kun ett literal.

Teorem.
Enhver formel er ekvivalent med en formel på disjunktiv normalform.

Eksempel.
- $P \to Q$ er ekvivalent med $\neg P \vee Q$, som er på DNF.
- $\neg(P \wedge \neg Q)$ er ekvivalent med $\neg P \vee Q$, som er på DNF.

- Vi kan bevise dette på to forskjellige måter:
  1. Bruke sannhetsverditabeller og konstruere en formel på DNF.
  2. Bruke ekvivalenser og transformere til en formel på DNF.
- Vi finner DNF av $(P \to Q) \wedge (Q \to P)$ ved å bruke en sannhetsverditabell.

P	Q	(P	→	Q)	∧	(Q	→	P)
1	**1**	1	**1**	1	**1**	1	**1**	1
1	**0**	1	**0**	0	**0**	0	**1**	1
0	**1**	0	**1**	1	**0**	1	**0**	0
0	**0**	0	**1**	0	**1**	0	**1**	0

- Rad 1 "svarer til" formelen $(P \wedge Q)$.
- Rad 4 "svarer til" formelen $(\neg P \wedge \neg Q)$.
- Ved å ta disjunksjonen av disse får vi DNF av den opprinnelige formelen, $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
- Boken kaller dette for full disjunktiv normalform.

Definisjon (Full disjunktiv normalform).
En formel på disjunktiv normalform er på *full disjunktiv normalform* hvis hver konjuksjon består av n literaler, hvor n er antall forskjellige utsagnsvariable i formelen.

Eksempel.
- $(P \wedge Q) \vee (\neg P \wedge \neg Q)$ er på full DNF.
- $(P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$ er på full DNF.
- $P \vee (\neg P \wedge Q)$ er på DNF, men ikke på full DNF.

- Vi finner DNF av $(P \vee (Q \rightarrow R) \wedge S$ ved å bruke ekvivalenser og å transformere formelen.

$$\begin{aligned} & (P \vee (Q \rightarrow R)) \wedge S \\ \equiv \; & (P \vee (\neg Q \vee R)) \wedge S \\ \equiv \; & (P \vee \neg Q \vee R) \wedge S \\ \equiv \; & (P \wedge S) \vee (\neg Q \wedge S) \vee (R \wedge S) \end{aligned}$$

- Denne er på DNF, men ikke på full DNF.
- Her ville vi ellers ha brukt en sannhetsverditabell med 16 rader.

Konjunktiv normalform (CNF)

Definisjon.
En utsagnslogisk formel er på *konjunktiv normalform (CNF, eller KNF)* hvis den er en konjunksjon av en eller flere disjunksjoner og hvor hver disjunksjon består av en eller flere literaler. (En slik disjunksjon kalles i boka en *fundamental disjunksjon*.)

Teorem.
Enhver formel er ekvivalent med en formel på konjunktiv normalform.

Noen oppgaver

Oppgave.
Vis at $\neg(P \rightarrow Q) \equiv P \wedge \neg Q$.

- Oppgaven går ut på å vise at $\neg(P \rightarrow Q)$ og $P \wedge \neg Q$ er ekvivalente.
  - Da må man (selvfølgelig!) vite hva det betyr at to formler er ekvivalente.
  - Det er at formlene *har samme sannhetsverdi for samme tilordning av sannhetsverdier til utsagnvariablene*.
- Den enkleste måten å løse denne oppgaven på er å lage en sannhetsverditabell og bruke denne til å forklare hvorfor formlene er ekvivalente.

Oppgave.
Vis at $\equiv$ er en ekvivalensrelasjon på mengden av utsagnslogiske formler.

- Oppgaven går ut på å bevise eller føre et presist argument for påstanden.

  - Da må man (selvfølgelig!) vite hva en ekvivalensrelasjon er.
  - Det er *binær relasjon (på mengden av formler) som er refleksiv, symmetrisk og transitiv*.
- Her bør man ta for seg de ulike bestanddelene av hva det vil si å være en ekvivalensrelasjon og sjekke de hver for seg.

Tillegg

Oppfyllbare mengder

Definisjon (Oppfyllbar mengde).

- En valuasjon ν *oppfyller* (eng: *satisfies*) en mengde S av utsagnslogiske formler hvis $\nu(A) = \mathbf{1}$ for alle A i S. Dette skrives ofte $\nu \models S$.
- En mengde utsagnslogisk formler er *oppfyllbar* (eng: *satisfiable*) hvis det fins en valuasjon som oppfyller den.

Eksempel.

- Mengden $\{\neg P, Q\}$ er oppfyllbar; den oppfylles av enhver valuasjon ν slik at $\nu(P) = \mathbf{0}$ eller $\nu(Q) = \mathbf{1}$.
- Mengden $\{P, \neg P\}$ er *ikke* oppfyllbar; det fins ingen valusjon ν slik at både $\nu(P) = \mathbf{1}$ og $\nu(\neg P) = \mathbf{1}$.

INF1800 – Forelesning 15

Utsagnslogikk – Sekventkalkyle

Roger Antonsen - 7. oktober 2008

Sekventkalkyle for utsagnslogikk

Introduksjonseksempel

- 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.

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

Eksempel

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

- $(P \to Q) \to (\neg Q \to \neg P)$ kan ikke falsifiseres!

Noen kommentarer

- 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 rot-node 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!

Sekventer og aksiomer

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 *antesedent*.
- Formlene som står til høyre for $\vdash$ kalles *suksedent*.

Notasjon.
I sekventer leses $,$ som union (kalles *sum* i boken):

- Γ, A skal bety $\Gamma + \{A\}$.
- Hvis $\Gamma = [A, B, C]$, så er $\Gamma, A = [A, A, B, C]$.

Eksempel.
Hvilke av uttrykkene nedenfor er sekventer?

- P, Q Nei
- $\vdash P \vdash Q$ Nei
- $P \vdash Q$ Ja
- $P, P \vdash Q$ Ja
- $\vdash Q$ Ja
- $P \vdash$ Ja
- $23 \vdash Q$ Nei
- $P, Q \to R \vdash Q \to R$ Ja

Definisjon (Aksiom).
Et *aksiom* er en sekvent på formen

$$\Gamma, A \vdash A, \Delta$$

slik at A er en *atomær* utsagnslogisk formel, dvs. en *utsagnsvariabel*.

Eksempel.
Hvilke av sekventene nedenfor er aksiomer?

- $P \vdash Q$ Nei
- $P, P \vdash Q, P$ Ja
- $P \to Q \vdash P \to Q$ Nei
- $P, Q \to R \vdash Q \to R, P$ Ja

Sekventkalkyleregler

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

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

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

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

α-reglene kalles ofte *ett-premissregler*.

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

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

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

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

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

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

- 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*.

Slutninger

Definisjon (LK-slutning).

- En *slutning* er en *instans* av en regel hvor
  - A og B er erstattet med utsagnslogiske formler, og
  - 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 $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\, \mathsf{R}\neg$ definerer uendelig mange $\mathsf{R}\neg$-slutninger:

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

Begreper knyttet til slutninger

Begrepene knyttet til regler anvendes om slutninger:

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

- 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

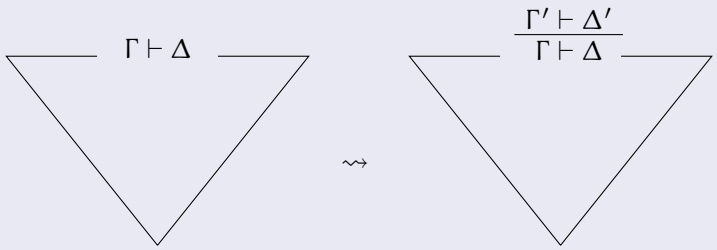
- En utledning er et tre der nodene er sekventer.
- Rotnoden er nederst og løvnodene er øverst.
- Rotnoden kalles *rotsekvent*.
- Løvnodene kalles *løvsekventer*.

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

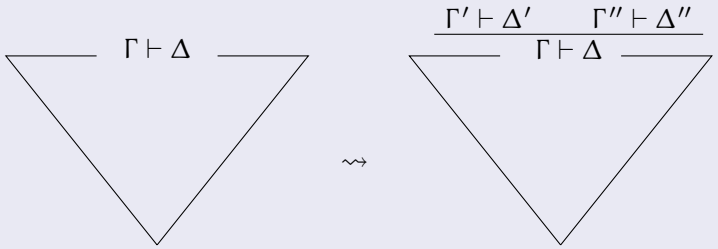
$$\Gamma \vdash \Delta$$

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

Definisjon (Mengden av LK-utledninger – α-utvidelse).
Hvis det fins 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 fins 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).

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

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

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

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 fins et LK-bevis med $\Gamma \vdash \Delta$ som rotsekvent.

Eksempel (LK-bevis).

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

$$\dfrac{\dfrac{\times}{P \vdash P}}{\vdash P \to P}\,R{\to}$$

- Sekventene $\vdash P \to P$ og $P \to Q \vdash \neg Q \to \neg P$ er bevisbare, siden det fins 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.

Semantikk for sekventer

Gyldige sekventer

Definisjon (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:

- $P \vdash P$
- $P \vdash P, Q$
- $P \to Q \vdash P \to Q$
- $P, P \to Q \vdash Q$
- $P \to Q \vdash \neg Q \to \neg P$

Falsifiserbare sekventer

Definisjon (Motmodell/falsifiserbar sekvent).

- En valuasjon ν er en *motmodell* til sekventen $\Gamma \vdash \Delta$ hvis ν 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: $\nu(P) = \mathbf{1}, \nu(Q) = \mathbf{0}$
- $P \vee Q \vdash P \wedge Q$ Motmodell: som over eller $\nu(P) = \mathbf{0}, \nu(Q) = \mathbf{1}$
- $\vdash P$ Motmodell: $\nu(P) = \mathbf{0}$
- $P \vdash$ Motmodell: $\nu(P) = \mathbf{1}$
- $\vdash$ Motmodell: *alle modeller!*

Oppsummering

Gyldig

- $P, P \to Q \vdash Q$
- Hvis $\nu \models P$ og $\nu \models P \to Q$, så $\nu \models Q$.

Bevisbar

$$\dfrac{P \vdash P \qquad Q \vdash Q}{P, P \to Q \vdash Q}$$

Falsifiserbar

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

Ikke bevisbar

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

INF1800 – Forelesning 16

Utsagnslogikk – Sekventkalkyle

Roger Antonsen - 8. oktober 2008

Noen kommentarer

Forelesningene, notatene og boken

- Jeg sier stor sett mye mer i timen enn det som står i forelesningsnotatene.
- Derfor: for å få fullt utbytte av undervisningen, så holder det ikke å *kun* lese notatene.
- Kalkylen for utsagnslogikk kan leses helt uavhengig av boken.
- Boka kan allikevel godt leses som et supplement til det vi gjør her.
- Finner dere feil i notatene, så si ifra.
- Noen oppfordringer:
  - Regn oppgaver!
  - Gå på gruppetimene!
  - Vær nysgjerrig!
  - Repetér begrepene!

Eksempel på et bevis

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\times \qquad \times}{A, B \vdash A \qquad A, B \vdash B}}{A, B \vdash A \wedge B}}{\neg(A \wedge B), A, B \vdash}}{\neg(A \wedge B), A \vdash \neg B}}{\dfrac{\neg(A \wedge B) \vdash \neg A, \neg B}{\neg(A \wedge B) \vdash \neg A \vee \neg B}}$$

Eksempel på en utledning som ikke er et bevis

$$\dfrac{\dfrac{\times \qquad \dfrac{\times}{B, A \vdash B \qquad B, A \vdash C}}{A \vdash B \wedge C, A \qquad B, A \vdash B \wedge C}}{\dfrac{A \to B, A \vdash B \wedge C}{A \to B \vdash A \to B \wedge C}}$$

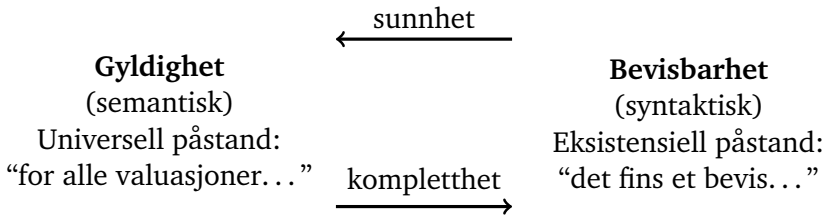
- Rotsekventen er falsifiserbar!
- Vi kan lese ut en motmodell fra løvsekventen som ikke er lukket.
- Motmodellen er en valuasjon v slik at $v(A) = \mathbf{1}$, $v(B) = \mathbf{1}$ og $v(C) = \mathbf{0}$.

Litt om sunnhet og kompletthet

Sunnhet og kompletthet

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

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



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

INF1800 – Forelesning 16x

Utsagnslogikk – Sunnhetsteoremet

Roger Antonsen - 8. oktober 2008

Bevis for sunnhetsteoremet

Sunnhet av LK

- Vi ønsker at alle LK-bevisbare sekventer skal være gyldige!
- Hvis ikke, så er LK *ukorrekt* eller *usunn* ...

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

Teorem.
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.

Bevaring av falsifiserbarhet

Definisjon.
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.
Alle LK-reglene er falsifiserbarhetsbevarende.

- Vi får ett delbevis for hver LK-regel.
- Se på f.eks. L→-regelen:

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

- 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 (Bevis for R¬).

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

- Anta at v falsifiserer konklusjonen.
- Det betyr at $v \models \Gamma$, $v \not\models \neg A$ og v *falsifiserer alle formlene i* Δ.
- Per 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 (Bevis for L→).

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

- 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 per 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.

Eksistens av falsifiserbar løvsekvent

Lemma.
Hvis en valuasjon v falsifiserer rotsekventen i en LK-utledning D, så falsifiserer v minst én av løvsekventene i D.

Bevis.
Ved såkalt *strukturell induksjon* på LK-utledningen D.
Basissteg: D 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 D, nemlig $\Gamma \vdash \Delta$.

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

$$\dfrac{\Gamma' \vdash \Delta'}{\Gamma \vdash \Delta}$$

- Anta at v falsifiserer rotsekventen i D, 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 D. Dermed falsifiserer v en løvsekvent i D.
- Hvis den falsifiserte løvsekventen *er* $\Gamma \vdash \Delta$, så falsifiserer v også $\Gamma' \vdash \Delta'$ siden α-reglene bevarer falsifiserbarhet.

Bevis (Bevis (induksjonssteg – β-utvidelse)).
Induksjonssteg: D er en utledning på formen

$$\dfrac{\Gamma' \vdash \Delta' \qquad \Gamma'' \vdash \Delta''}{\Gamma \vdash \Delta}$$

- Anta at ν falsifiserer rotsekventen i D, og anta at ν falsifiserer en løvsekvent i utledningen *før* β-utvidelsen.
- Hvis den falsifiserte løvsekventen *ikke* er $\Gamma \vdash \Delta$, så er den også løvsekvent i D. Dermed falsifiserer ν en løvsekvent i D.
- Hvis den falsifiserte løvsekventen *er* $\Gamma \vdash \Delta$, så falsifiserer ν også $\Gamma' \vdash \Delta'$ eller $\Gamma'' \vdash \Delta''$ siden β-reglene bevarer falsifiserbarhet.

Alle aksiomer er gyldige

Lemma.
Alle aksiomer er gyldige.

Bevis.

$$\Gamma, A \vdash A, \Delta$$

- Vi skal vise at alle valuasjoner som oppfyller antesedenten også oppfyller én formel i suksedenten.
- La ν være en tilfeldig valgt valuasjon som oppfyller antesedenten.
- Da oppfyller ν formelen A i suksedenten.
- Siden ν var tilfeldig valgt, fins ingen motmodell til aksiomet.

Bevis for sunnhetsteoremet

Bevis (Bevis for sunnhet).
- Anta at D er et LK-bevis for sekventen $\Gamma \vdash \Delta$.
- Anta for motsigelse at $\Gamma \vdash \Delta$ *ikke* er gyldig.
- Da har den en motmodell ν som falsifiserer $\Gamma \vdash \Delta$.
- Vi har da fra tidligere lemma at ν falsifiserer minst én løvsekvent i D.
- Da har D en løvsekvent som ikke er et aksiom, siden ingen aksiomer er falsifiserbare.
- Men da er ikke D et LK-bevis.

INF1800 – Forelesning 17

Førsteordens logikk

Roger Antonsen - 14. oktober 2008

Før vi begynner

Repetisjon og kommentarer

- Vi skal nå kunne
  - Utsagnslogikk: syntaks og semantikk
  - Sekventkalkyle for utsagnslogikk
- Under den detaljert undervisningsplanen ligger det ekstramateriale om sunnhet av sekventkalkylen.
- Det er ikke pensum, men bør leses av alle.
- Alla skal være i stand til å forklare (intuitivt) hvorfor sekventkalkylen er sunn.
- Praktisk: Hvis dere ønsker å gi tilbakemeldinger til gruppelærerene, så kan skjemaet på nettsidene også brukes til dette.

Nytt tema

- Vi begynner nå med førsteordens logikk!
- Vi har satt av minst tre uker til dette.
- Følgende avsnitt i boken regnes som pensum.


Kapittel 7.1, side 397–416: *First-order Predicate Calculus*


Kapittel 7.2, side 416–432: *Equivalent Formulas*

- Forelesningsnotatene kan leses helt uavhengig av boken.
- Legg vekt på forelesningsnotatene, men les boken også.
- Boken er et godt supplement for å få bedre forståelse.
- På noen områder er forelesningsnotatene mer detaljerte.
  - Vi har f.eks. et skarpere skille mellom syntaks og semantikk.
- Det vi gjør i timene er mest relevant for eksamen.

Innledning til førsteordens logikk

Introduksjon

- I utsagnslogikk har vi kun konnektivene $\neg$, $\wedge$, $\vee$ og $\rightarrow$.
- Med disse kan vi representere, analysere og resonnere over *utsagn*.
- Førsteordens logikk (også kalt predikatlogikk) utvider utsagnslogikk med *kvantorer*:
  - $\exists$ (eksistenskvantoren) og
  - $\forall$ (allkvantoren).
- Vi kan med disse uttrykke påstander om at det finnes et objekt med en bestemt egenskap eller at alle objekter har en bestemt egenskap.
- Førsteordens logikk er langt rikere enn utsagnslogikk.
  - For utsagnslogikk fins det effektive metoder for å *avgjøre* om en formel er gyldig eller ikke.
  - Det fins ikke for førsteordens logikk; vi sier at førsteordens logikk er ikke *avgjørbar*.

Noen eksempler fra matematikk

Noen enkle matematisk påstander som vi kan representere og analysere ved førsteordens logikk er følgende.

- "Ethvert heltall er enten partall eller oddetall."
- "Det fins uendelig mange primtall."
- "Mellom to brøktall fins det et annet brøktall."
- "Ethvert partall er summen av to primtall."
- "Hvis a er mindre enn b og b er mindre enn c, så er a mindre enn c."

Noen eksempler med naturlig språk

Her er noen ekempler av mindre matematisk art.

- "Alle Ifi-studenter er late."
- "Ingen Ifi-studenter er late."
- "Noen Ifi-studenter er late."
- "Alle Ifi-studenter som er late, får problemer på eksamen."
- "Noen Ifi-studenter som er late, får ingen problemer på eksamen."
- "Enhver Ifi-student er enten lat eller ikke lat."
- "Alle bevisbare formler er gyldige."
- "Det fins to sheriffer i byen."

Overblikk

Syntaks: Førsteordens språk og formler – en utvidelse av utsagnslogikk.

Semantikk: Tolkninger av førsteordens formler – modeller, sannhet, oppfyllbarhet, gyldighet.

Kalkyle: Tillegg av regler.

Sunnhet: Alle bevisbare sekventer er gyldige.

Kompletthet: Alle gyldige sekventer er bevisbare.

Førsteordens logikk: Syntaks

Syntaks: Signaturer

Definisjon (Førsteordens språk: logiske symboler).
Alle *førsteordens språk* består av følgende *logiske symboler*:

- De logiske konnektivene $\wedge$, $\vee$, $\rightarrow$ og $\neg$.
- *Kvantorene* $\exists$ (det fins) og $\forall$ (for alle).
- En tellbart uendelig mengde $\mathcal{V}$ av *variable* $x_1, x_2, x_3, \ldots$ (vi skriver som oftest x, y, z, $\ldots$, for variable).
- Vi skal også bruke parenteser og kommaer som hjelpesymboler.

Definisjon (Førsteordens språk: ikke-logiske symboler).
I tillegg består et *førsteordens språk* av følgende mengder av *ikke-logiske symboler*:

- En tellbar mengde av *konstantsymboler* $c_1, c_2, c_3, \ldots$.
- En tellbar mengde av *funksjonssymboler* $f_1, f_2, f_3, \ldots$.
- En tellbar mengde av *relasjonssymboler* $R_1, R_2, R_3, \ldots$.

Vi antar at mengdene av variable, konstant-, funksjons- og relasjonssymboler er disjunkte, og vi assosierer med ethvert funksjons- og relasjonssymbol et ikke-negativt heltall, kalt *ariteten* til symbolet.

Merk.

- Det eneste som skiller to førsteordens språk fra hverandre er de ikke-logiske symbolene.

Definisjon (Signatur).

- De ikke-logiske symbolene utgjør det som kalles en *signatur*.
- En signatur angis ved et tuppel

$$\langle c_1, c_2, c_3, \ldots; f_1, f_2, f_3, \ldots; R_1, R_2, R_3, \ldots \rangle,$$

  hvor konstant-, funksjons- og relasjonssymboler er adskilt med semikolon.

Syntaks: Termer

Definisjon (Termer).
Mengden $\mathcal{T}$ av *førsteordens termer* er induktivt definert som den minste mengden slik at:

- Enhver variabel og konstant er en term.
- Hvis f er et funksjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer, så er $f(t_1, ..., t_n)$ en term.

Eksempler på førsteordens språk

Et enkelt språk: $\langle a; f, g; P, R\rangle$

- Konstantsymboler: a
- Funksjonssymboler: f (med aritet 1) og g (med aritet 2)
- Relasjonssymboler: P (med aritet 1) og R (med aritet 2)

Termer i dette språket:

- a, x, y, $\ldots$, $f(a)$, $f(x)$, $f(y)$, $\ldots$
- $g(a,a)$, $g(a,x)$, $g(a,y)$, $g(x,x)$, $g(x,y)$, $g(y,y)$, $\ldots$
- $f(f(a))$, $f(f(x))$, $f(f(y))$, $\ldots$

Notasjon.
Så lenge det er entydig og ariteten er kjent, kan vi droppe parentesene og skrive fa, fx, fy, gaa, gax, $\ldots$.

Et språk for aritmetikk: $\langle 0; s, +; =\rangle$

- Konstantsymboler: 0
- Funksjonssymboler: s (med aritet 1) og $+$ (med aritet 2)
- Relasjonssymboler: $=$

Kommentarer:

- Termer: $x, y, 0, s0, ss0, sss0, +xy, +00, +(s0)0, +0s0, \ldots$
- *Ikke* termer: $=(x,x), ++, +0, \ldots$
- Når vi skriver $+xy$ bruker vi *prefiks notasjon*.
- Vi kan også bruke *infiks notasjon* og skrive: $(x+y), (0+0), (s0+0), (0+s0), \ldots$.

Et annet språk for aritmetikk: $\langle 0, 1; +, \times; =, <\rangle$

- Konstantsymboler: $0, 1$
- Funksjonssymboler: $+$ og $\times$ (begge med aritet 2)
- Relasjonssymboler: $=$ og $<$ (begge med aritet 2)

Et språk for mengdelære: $\langle \emptyset; \cap, \cup; =, \in\rangle$

- Konstantsymboler: $\emptyset$
- Funksjonssymboler: $\cap$ og $\cup$ (begge med aritet 2)
- Relasjonssymboler: $=$ og $\in$ (begge med aritet 2)

Termer: $\emptyset$, $x \cap \emptyset$, $y \cup (x \cap z)$,...

Et språk for familierelasjoner: $\langle \mathsf{Ola}, \mathsf{Kari}; \mathsf{mor}, \mathsf{far}; \mathsf{Mor}, \mathsf{Far}, \mathsf{Slektning} \rangle$

- Konstantsymboler: Ola og Kari
- Funksjonssymboler: mor, far (begge med aritet 1)
- Relasjonssymboler: Mor, Far, Slektning (alle med aritet 2)

Termer i språket for familierelasjoner:

- x, Ola og Kari er termer.
- $\mathsf{mor}(\mathsf{Ola})$, $\mathsf{mor}(\mathsf{Kari})$, $\mathsf{far}(\mathsf{Ola})$ og $\mathsf{far}(\mathsf{Kari})$ er termer.
- $\mathsf{mor}(x)$ og $\mathsf{far}(x)$ er termer.
- $\mathsf{mor}(\mathsf{mor}(x))$ og $\mathsf{mor}(\mathsf{far}(\mathsf{Kari}))$ er termer.

Syntaks: Formler

Definisjon (Atomær formel: førsteordens).
Hvis R er et relasjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer, så er $R(t_1, \ldots, t_n)$ en *atomær formel*.

Merk.
- Hvis R har aritet 0, så er R en atomær formel. Dette svarer til utsagnsvariable i utsagnslogikk.
- Så lenge det er entydig og ariteten er kjent, kan vi skrive Rx, Rfa, $Rafa$, etc. for $R(x)$, $R(f(a))$ og $R(a, f(a))$.

Definisjon (Førsteordens formler).
Mengden $\mathcal{F}$ av *førsteordens formler* er den minste mengden slik at:

1. Alle atomære formler er formler.
2. Hvis φ og ψ er formler, så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \to \psi)$ formler.
3. Hvis φ er en formel og x er en variabel, så er $\forall x\varphi$ og $\exists x\varphi$ formler.

Alle forekomster av en variabel x i φ sies å være *bundet* i formlene $\forall x\varphi$ og $\exists x\varphi$ og innenfor *skopet* til den gjeldende kvantoren.

Eksempler på førsteordens formler

Et språk for beundring: $\langle a, b; -; \mathsf{Idol}, \mathsf{Liker}\rangle$

- Konstantsymboler: a og b
- Funksjonssymboler: (ingen)
- Relasjonssymboler: Idol (med aritet 1) og Liker (med aritet 2)

- Signaturen er $\langle a, b; -; \mathsf{Idol}, \mathsf{Liker}\rangle$
- Atomære formler i språket:

1	Alice er et idol:	$\mathsf{Idol}(a)$
2	Alice liker Bob:	$\mathsf{Liker}(a, b)$
3	x liker Alice:	$\mathsf{Liker}(x, a)$

- Ikke-atomære formler i språket:

4	Alice liker alle:	$\forall x \mathsf{Liker}(a, x)$
5	Det finnes et idol:	$\exists x \mathsf{Idol}(x)$
6	Alice liker alle som Bob liker:	$\forall x(\mathsf{Liker}(b, x) \to \mathsf{Liker}(a, x))$
7	Noen liker seg selv:	$\exists x \mathsf{Liker}(x, x)$
8	Bob liker alle som liker seg selv:	$\forall x(\mathsf{Liker}(x, x) \to \mathsf{Liker}(b, x))$
9	Ingen liker både Alice og Bob:	$\neg\exists x(\mathsf{Liker}(x, a) \wedge \mathsf{Liker}(x, b))$
10	Noen liker ikke seg selv:	$\exists x \neg \mathsf{Liker}(x, x)$
11	Bob liker noen som liker Alice:	$\exists x(\mathsf{Liker}(b, x) \wedge \mathsf{Liker}(x, a))$
12	Alle liker noen:	$\forall x(\exists y \mathsf{Liker}(x, y))$
13	En som blir likt av alle er et idol:	$\forall x(\forall y \mathsf{Liker}(y, x) \to \mathsf{Idol}(x))$
14	Et idol blir likt av alle:	$\forall x(\mathsf{Idol}(x) \to \forall y \mathsf{Liker}(y, x))$

Flere eksempler

I språket for aritmetikk, $\langle 0; s, +; =\rangle$, har vi følgende formler.

- $s0 + s0 = ss0$ – "en pluss en er to"
- $\forall x \forall y(x + y = y + x)$ – "addisjon er kommutativt"
- $\neg\exists x(0 = sx)$ – "0 er ikke etterfølgeren til noe"
- $\exists x \exists y \neg(x = y)$ – "det fins to forskjellige objekter"

Frie variable i termer

Definisjon (Frie variable i en term).
$\mathrm{FV}(t)$ betegner mengden av *frie variable* i termen t.

Definisjon (Lukket term).
En term t er *lukket* hvis $\mathrm{FV}(t) = \emptyset$, dvs. t inneholder ingen frie variable.

Eksempel.
I språket $\langle a, b; f; - \rangle$ har vi:

- Termen $f(x, a)$ har en fri variabel x.
- Termen $f(a, b)$ har ingen frie variable og er en lukket term.

Frie variable i formler

Definisjon (Frie variable i en formel).
En variabelforekomst i en førsteordens formel er *fri* hvis den ikke er bundet, dvs. hvis den ikke er innenfor skopet til en kvantor. Vi skriver $\mathrm{FV}(\varphi)$ for mengden av frie variable i φ.

Eksempel ($\forall x Rxy \wedge Pz$).

- x er bundet
- y er fri
- z er fri

Eksempel ($\forall x Pxy \rightarrow \forall z Pzx$).

- x er bundet
- x er fri
- y er fri
- z er bundet

Substitusjoner

Definisjon (Substitusjon for termer).
La s og t være termer og x en variabel. Da er $s[x/t]$ resultatet av å erstatte alle forekomster av x i s med t. Det kan defineres helt presist slik:

1. $y[x/t] = \begin{cases} t & \text{hvis } x = y \\ y & \text{ellers} \end{cases}$ (når s er en variabel y).
2. $c[x/t] = c$ (når s er en konstant c).
3. $f(t_1[x/t], \ldots, t_n[x/t])$ (når s er en funksjonsterm $f(t_1, \ldots, t_n)$).

Eksempel.

- $f(x, y, a)[x/y] = f(x[x/y], y[x/y], a[x/y]) = f(y, y, a)$
- $f(y, y, a)[y/b] = f(y[y/b], y[y/b], a[y/b]) = f(b, b, a)$

Definisjon (Substitusjon for formler).
$\varphi[x/t]$ er definert (rekursivt) ved:

1. $R(t_1, \ldots, t_n)[x/t] = R(t_1[x/t], \ldots, t_n[x/t])$
2. $\neg\psi[x/t] = \neg(\psi[x/t])$
3. $(\varphi_1 \circ \varphi_2)[x/t] = (\varphi_1[x/t] \circ \varphi_2[x/t])$, hvor $\circ \in \{\wedge, \vee, \rightarrow\}$
4. $Qy\psi[x/t] = \begin{cases} Qy(\psi[x/t]) & \text{hvis } x \neq y \\ Qy\psi & \text{ellers} \end{cases}$, hvor $Q \in \{\forall, \exists\}$

Eksempel.

- $(Pxy \wedge \forall xPxy)[x/a] = (Pay \wedge \forall xPxy)$
- $(Pxy \wedge \forall xPxy)[y/a] = (Pxa \wedge \forall xPxa)$

Førsteordens logikk: Semantikk

Introduksjon

- Hvordan skal vi *tolke* førsteordens formler?
- Hva skal $\forall x\varphi$ og $\exists x\varphi$ bety?
- Hva kan vi bruke førsteordens formler til å uttrykke?

  (Hva er det førsteordens formler *ikke* kan uttrykke?)
- Hva gjør en formel *sann / gyldig / oppfyllbar*?
- Å gi en semantikk er å si noe om forholdet mellom språk og virkelighet.
  - Valuasjoner gir en semantikk for klassisk utsagnslogikk.
- I førsteordens logikk vil *modeller* gi oss en semantikk.

En modell består intuitivt av

1. en mengde, og
2. en tolkning av alle ikke-logiske symboler slik at
   - et konstantsymbol tolkes som et element i mengden,
   - et funksjonssymbol tolkes som en funksjon på mengden, og

- et relasjonssymbol tolkes som en relasjon på mengden.

Vi skal definere modeller helt presist, også skal vi definere hva det vil si at en formel er sann i en modell.

Husk
Hvis D er en mengde, så består D^n av alle n-tupler av elementer fra D, for $n \geqslant 0$.

$$D^n = \{\langle d_1, \ldots, d_n \rangle \mid d_1, \ldots, d_n \in D\}$$

Modeller – Intuisjon

- Se på formelen
$$\forall x \exists y R x y.$$
- Vi leser den som: *For alle* x, så *fins* det en y slik at Rxy.
- Hvorvidt denne formelen er sann eller usann avhenger av tolkningen eller modellen.
  - Hvis R tolkes som *ekte mindre enn*-relasjonen over de naturlige tallene, så er den sann.
  - Grunnen er at for alle tall så fins det ett som er større.
  - Hvis R tolkes som *ekte mindre enn*-relasjonen over mengden $\{1, 2, 3, 4, 5, 6, 7\}$, så er den usann.
  - Grunnen er at det fins et tall, nemlig 7, slik at det *ikke* fins noe større tall.
- Vi må definere hva vi mener med en *modell*.

Modeller

La et førsteordens språk $\mathcal{L}$ være gitt.

Definisjon (Modell).
En *modell* $\mathcal{M}$ for $\mathcal{L}$ består av en ikke-tom mengde D, kalt *domenet* til $\mathcal{M}$, og en funksjon $(\cdot)^{\mathcal{M}}$ som tolker alle ikke-logiske symboler på følgende måte:

- Hvis c er et konstantsymbol, så er $c^{\mathcal{M}} \in D$.
- Hvis f er et funksjonsymbol med aritet n, så er $f^{\mathcal{M}}$ en funksjon fra $D^n = \underbrace{D \times \cdots \times D}_{n}$ til D.
- Hvis R er et relasjonssymbol med aritet n, så er $R^{\mathcal{M}}$ en relasjon på $D^n = \underbrace{D \times \cdots \times D}_{n}$.

Vi skriver $|\mathcal{M}|$ for domenet D til modellen $\mathcal{M}$.

INF1800 – Forelesning 18

Førsteordens logikk

Roger Antonsen - 15. oktober 2008

Repetisjon og noen løse tråder

Førsteordens språk

Et førsteordens språk $\mathcal{L}$ består av:

1. Logiske symboler
   - konnektiver: $\wedge$, $\vee$, $\rightarrow$ og $\neg$
   - hjelpesymboler: '(' og ')' og ','
   - kvantorer: $\exists$ og $\forall$
   - variable: $\mathcal{V} = \{x_1, x_2, x_3, \ldots\}$
2. Ikke-logiske symboler:
   - en tellbar mengde konstantsymboler
   - en tellbar mengde funksjonssymboler (med aritet)
   - en tellbar mengde relasjonssymboler (med aritet)

- De ikke-logiske symbolene utgjør en *signatur*
  $\langle \underbrace{c_1, c_2, c_3, \ldots}_{\text{konstantsymboler}} ; \underbrace{f_1, f_2, f_3, \ldots}_{\text{funksjonssymboler}} ; \underbrace{R_1, R_2, R_3, \ldots}_{\text{relasjonssymboler}} \rangle$.

Eksempler på signaturer

Vi har sett følgende signaturer:

enkelt språk:	$\langle$	a	;	f, g	;	P, R	$\rangle$
aritmetikk 1:	$\langle$	0	;	$s, +$	;	$=$	$\rangle$
aritmetikk 2:	$\langle$	$0, 1$	;	$+, \times$	;	$=, <$	$\rangle$
mengdelære:	$\langle$	$\emptyset$	;	$\cap, \cup$	;	$=, \in$	$\rangle$
familierelasjoner:	$\langle$	Ola, Kari	;	mor, far	;	Mor, Far, Slektning	$\rangle$
beundring:	$\langle$	a, b	;		;	Idol, Liker	$\rangle$

Mengden av førsteordens termer og formler

Hvis et førsteordens språk $\mathcal{L}$ er gitt, så får vi (definert induktivt):

1. Mengden $\mathcal{T}$ av termer i $\mathcal{L}$:
   - Enhver variabel og konstant er en term.
   - Hvis f er et funksjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer, så er $f(t_1, \ldots, t_n)$ en term.

2. Mengden $\mathcal{F}$ av formler i $\mathcal{L}$:
    - Hvis R er et relasjonssymbol med aritet n og $t_1, \ldots, t_n$ er termer, så er $R(t_1, \ldots, t_n)$ en (atomær) formel.
    - Hvis φ og ψ er formler, så er $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ og $(\varphi \to \psi)$ formler.
    - Hvis φ er en formel og x er en variabel, så er $\forall x\varphi$ og $\exists x\varphi$ formler.

- En variabel x er bundet hvis den er innenfor skopet til en kvantor.
- En variabelforekomst er fri hvis den ikke er bundet.
- En term som ikke inneholder variable kalles lukket.

En kort oppsummering av modeller

En modell $\mathcal{M}$ for et språk $\mathcal{L}$ består av

1. en ikke-tom mengde $|\mathcal{M}|$, kalt domenet til $\mathcal{M}$, og
2. en tolkning av alle ikke-logiske symboler i språket.

For eksempel, hvis $\mathcal{L}$ er språket $\langle$ 🧍 , 🚹 , ☕ ; 🏭 ; ♀ , ♂$\rangle$, så må en modell $\mathcal{M}$ gi et domene og en tolkning til alle symbolene.

- 🧍$^{\mathcal{M}}$, 🚹$^{\mathcal{M}}$ og ☕$^{\mathcal{M}}$ må være elementer i domenet.
- 🏭$^{\mathcal{M}}$ må være en funksjon på domenet.
- ♀$^{\mathcal{M}}$ og ♂$^{\mathcal{M}}$ må være relasjoner på domenet.
- Husk på ariteten til symbolene.
- Her kan for eksempel 🏭 ha aritet 2, og ♀ og ♂ ha aritet 1.
- En mulig formel i dette språket er ♂(🚹) $\wedge \forall x($♀$(x) \to$ ♂(🏭(🚹, ☕))).

Substitusjoner og frie variable

- Vi har sett at substitusjon ikke blir gjort for bundne variable.
- Vi har enda et tilfelle hvor vi ønsker å forhindre substitusjon.

Eksempel.

- $\exists x P(x, y)[y/f(x)] = \exists x P(x, f(x))$

- Her blir en variabel bundet *etter* substitusjon.
- Dette kan endre meningen til en formel på en måte som vi ikke ønsker.

Definisjon.
Vi sier at t *er fri for* x i φ hvis ingen variabel i t blir bundet som følge av å substituere t for x i φ.

Eksempel.
Termen $f(x)$ er ikke fri for y i formelen $\exists x P(x, y)$.

- En måte å unngå dette på er å omdøpe bundne variable først.
- F.eks. se på $\exists z P(z, y)$ i stedet for $\exists x P(x, y)$.
- Fra nå av antar vi at alle substitusjoner er "fri for", det vil si at ingen variable blir bundet som følge av en substitusjon.

Lukkede og åpne formler

Definisjon (Lukket/åpen formel).
En formel φ er *lukket* hvis $FV(\varphi) = \emptyset$, det vil si at φ ikke inneholder noen frie variable. En formel er *åpen* hvis den ikke inneholder noen kvantorer.

Eksempel.
- $\forall x P x a$ er lukket.
- $\forall x P x y$ er *ikke* lukket.
- $P x y$ er *ikke* lukket, men åpen.
- $P a b$ er åpen *og* lukket.

Presedensregler

- På samme måte som for utsagnslogiske formler, har vi presedensregler for førsteordens formler.
- Mengden $\mathcal{F}$ av førsteordens formler er helt presist definert, men vi skal også godta f.eks. $\exists y P y \wedge P x$ som førsteordens formler (selv om parentesene mangler).
- Vi gir konnektivene ulik *presedens* i forhold til hverandre.
  1. $\neg$, $\forall$ og $\exists$ binder sterkest.
  2. $\wedge$ binder svakere.
  3. $\vee$ binder enda svakere.
  4. $\rightarrow$ binder svakest.
- For eksempel:
  - $\exists y P y \wedge P x$ betyr $(\exists y P y) \wedge P x$ og *ikke* $\exists y (P y \wedge P x)$

Semantikk (fortsettelse)

Noen kommentarer

1. Et funksjonssymbol f med aritet 0 kan betraktes som en konstant.
   - Da er $f^{\mathcal{M}}$ en funksjon fra D^0 til D.
   - Siden D^0 består av kun ett element $\langle\rangle$ – det tomme tuppelet – så består $f^{\mathcal{M}}$ også av kun ett element $\langle\langle\rangle, e\rangle$, hvor $e \in D$.
   - Vi kan derfor identifisere $f^{\mathcal{M}}$ med e.
2. Et relasjonssymbol R med aritet 0 kan betraktes som en utsagnsvariabel.
   - Da er $R^{\mathcal{M}}$ en delmengde av D^0.
   - Siden D^0 består av kun ett element $\langle\rangle$ – det tomme tuppelet - så fins det nøyaktig to muligheter for $R^{\mathcal{M}}$.
   - Enten så er $R^{\mathcal{M}}$ tom eller så er $\langle\rangle \in R^{\mathcal{M}}$.
   - Vi kan derfor tenke på mengden $\{\emptyset, \{\langle\rangle\}\}$ av delmengder av D^0 som **Bool**.
3. Et tuppel $\langle e\rangle$, hvor $e \in D$, kan vi identifisere med elementet e.
   - Når et relasjonssymbol R har aritet 1, så skriver vi derfor $\{e_1, \ldots, e_n\}$ i stedet for $\{\langle e_1\rangle, \ldots, \langle e_n\rangle\}$.
   - Vi antar derfor også at $R^{\mathcal{M}} \subseteq D$.

Eksempel – Et figurspråk

Relasjonssymboler

	aritet
Sirkel	1
Firkant	1
Trekant	1
Stor	1
Liten	1
Mindre	2

- Konstantsymboler: a, b, c, d, e, f.
- Funksjonssymboler: ingen.
- Vi leser på denne måten:

Sirkel(x)	x er en sirkel
Firkant(x)	x er en firkant
Trekant(x)	x er en trekant
Stor(x)	x er stor
Liten(x)	x er liten
Mindre(x, y)	x er mindre enn y

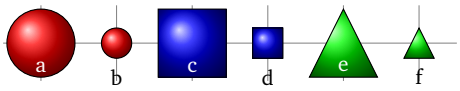
La oss nå lage en modell for dette språket!

En tolkning av figurspråket

La $\mathcal{M}$ være en modell med domene $D = \{\bigcirc, \bullet, \square, \blacksquare, \triangle, \blacktriangle\}$.

$$
\begin{aligned}
a^{\mathcal{M}} &= \bigcirc & \text{Sirkel}^{\mathcal{M}} &= \{\bigcirc, \bullet\} \\
b^{\mathcal{M}} &= \bullet & \text{Firkant}^{\mathcal{M}} &= \{\square, \blacksquare\} \\
c^{\mathcal{M}} &= \square & \text{Trekant}^{\mathcal{M}} &= \{\triangle, \blacktriangle\} \\
d^{\mathcal{M}} &= \blacksquare & \text{Stor}^{\mathcal{M}} &= \{\bigcirc, \square, \triangle\} \\
e^{\mathcal{M}} &= \triangle & \text{Liten}^{\mathcal{M}} &= \{\bullet, \blacksquare, \blacktriangle\} \\
f^{\mathcal{M}} &= \blacktriangle & \text{Mindre}^{\mathcal{M}} &= \{\langle \bullet, \bigcirc \rangle, \langle \bullet, \square \rangle, \langle \bullet, \triangle \rangle, \langle \blacksquare, \bigcirc \rangle, \ldots\}
\end{aligned}
$$

Vi foregriper begivenhetene og ser på hvilke atomære formler som er sanne og usanne i modellen $\mathcal{M}$.



Sant

- $\text{Sirkel}(a)$
- $\text{Firkant}(c)$
- $\text{Liten}(b)$
- $\text{Mindre}(b, e)$

Usant

- $\text{Trekant}(a)$
- $\text{Stor}(b)$
- $\text{Mindre}(a, b)$
- $\text{Mindre}(a, a)$

Utvidete språk

- I det foregående eksempelet hadde vi konstantsymboler for alle elementer i domenet.
- Det er veldig nyttig.
- Strengt tatt har vi ingen garanti for et språk er så rikt.
- For enkelhets skyld – og for å definere semantikken – så skal vi anta vi at for enhver modell og ethvert språk, så inneholder språket konstantsymboler for alle elementer i domenet til modellen.

Antakelse.
Hvis $\mathcal{M}$ er en modell for $\mathcal{L}$, så antar vi at for ethvert element a i $|\mathcal{M}|$, så fins et konstantsymbol $\bar{a}$ i $\mathcal{L}$. Vi antar også at $\mathcal{M}$ tolker $\bar{a}$ som a, med andre ord, at $\bar{a}^{\mathcal{M}} = a$.

Utvidete språk (i detalj – for spesielt interesserte)

- ⋆ Det går an å gjøre dette mer detaljert og nøyaktig, uten antakelsen om at alle språk har konstantsymboler for alle elementer.
- ⋆ Idéen er da å lage et nytt språk for hver modell og hvert språk.
- ⋆ Her er detaljene for de som er spesielt interessert.

Definisjon (Utvidet språk $\mathcal{L}(\mathcal{M})$).
La $\mathcal{L}$ være et førsteordens språk og $\mathcal{M}$ en modell for $\mathcal{L}$. Da er $\mathcal{L}(\mathcal{M})$ det førsteordens språket man får fra $\mathcal{L}$ ved å legge til *nye* konstantsymboler for hvert element i $|\mathcal{M}|$. Hvis a er i $|\mathcal{M}|$, så skriver vi $\bar{a}$ for den nye konstanten. Hvis $\mathcal{N}$ er en modell for $\mathcal{L}(\mathcal{M})$, så krever vi at $\bar{a}^{\mathcal{N}} = a$.

- ⋆ Når vi tolker termer og formler fra språket $\mathcal{L}$ i en modell $\mathcal{M}$, så bruker vi det utvidete språket $\mathcal{L}(\mathcal{M})$ og antar at $\mathcal{M}$ er en $\mathcal{L}(\mathcal{M})$-modell.

Tolkning av termer

Definisjon (Tolkning av lukkede termer).
La $\mathcal{L}$ være et førsteordens språk, og la $\mathcal{M}$ være en modell for $\mathcal{L}$. Da tolker vi en lukket term $f(t_1, \ldots, t_n)$ på følgende måte:

$$f(t_1, \ldots, t_n)^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}}).$$

- Dette er et eksempel på en *rekursiv* definisjon.
  - Tolkningen av konstantsymboler er allerede gitt, siden $\mathcal{M}$ er en modell for $\mathcal{L}$. Dette gir basistilfellet for rekursjonen.
  - Vi utvider tolkninger til å gjelde for sammensatte termer.
- Vi merker oss at tolkninger kun er definert for *lukkede* termer.
- Når vi nå har angitt hvordan lukkede termer skal tolkes, kan vi gå over til å definere hvordan *formler* skal tolkes.

Tolkning av formler

Definisjon (Tolkning av lukkede formler).
La $\mathcal{L}$ være et førsteordens språk, og la $\mathcal{M}$ en modell for $\mathcal{L}$. Vi definerer (ved rekursjon) hva det vil si at en lukket formel φ er *sann* i $\mathcal{M}$. Vi skriver $\mathcal{M} \models \varphi$ for at φ er sann i $\mathcal{M}$ eller at $\mathcal{M}$ gjør φ sann.

- For atomære formler: $\mathcal{M} \models R(t_1, \ldots, t_n)$ hvis $\langle t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M} \models \neg\varphi$ hvis det *ikke* er tilfelle at $\mathcal{M} \models \varphi$.
- $\mathcal{M} \models \varphi \wedge \psi$ hvis $\mathcal{M} \models \varphi$ *og* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \vee \psi$ hvis $\mathcal{M} \models \varphi$ *eller* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \to \psi$ hvis $\mathcal{M} \models \varphi$ *impliserer* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \forall x\varphi$ hvis $\mathcal{M} \models \varphi[x/\bar{a}]$ *for alle* a i $|\mathcal{M}|$.
- $\mathcal{M} \models \exists x\varphi$ hvis $\mathcal{M} \models \varphi[x/\bar{a}]$ *for minst en* a i $|\mathcal{M}|$.

Oppfyllbarhet

Definisjon (Oppfyllbarhet).
En lukket formel φ er *oppfyllbar* hvis det fins en modell $\mathcal{M}$ som gjør φ sann. Vi sier i så fall at $\mathcal{M}$ oppfyller φ og at $\mathcal{M}$ en en modell for φ. Hvis φ ikke er oppfyllbar, så er den *kontradiktorisk*.

Oppfyllbar

- $\exists x \mathsf{Liten}(x)$
- $\exists x(\mathsf{Liten}(x) \wedge \mathsf{Stor}(x))$
- $\exists x Px \to \forall x Px$

Ikke oppfyllbar

- $Pa \wedge \neg Pa$
- $\exists x(\mathsf{Liten}(x) \wedge \neg\mathsf{Liten}(x))$
- $\neg\mathsf{Stor}(a) \wedge \forall x \mathsf{Stor}(x)$

Gyldighet

Definisjon (Gyldighet).
En lukket formel φ er *gyldig* hvis den er sann i alle modeller $\mathcal{M}$, ellers så er den *falsifiserbar*.

Gyldig

- $\forall x Pxa \to \forall z Pza$
- $(\forall x Px \wedge \forall y Qy) \to \forall x Px$
- $\exists x \mathsf{Liten}(x) \vee \exists x \neg \mathsf{Liten}(x)$

Ikke gyldig (falsfiserbar)

- $\forall x Px$
- $\exists x \mathsf{Stor}(x) \to \forall x \mathsf{Stor}(x)$
- $\exists x Px \to \exists x(Px \wedge Qx)$

INF1800 – Forelesning 19

Førsteordens logikk

Roger Antonsen - 21. oktober 2008

Repetisjon

Semantikk

Hvis $\mathcal{M}$ er en modell og φ er en lukket formel, så definerte vi $\mathcal{M} \models \varphi$. Vi brukte det utvidete språket – med konstanter for hvert element i domenet – for å gjøre dette.

- For atomære formler: $\mathcal{M} \models R(t_1, \ldots, t_n)$ hvis $\langle t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}} \rangle \in R^{\mathcal{M}}$.
- $\mathcal{M} \models \neg\varphi$ hvis det *ikke* er tilfelle at $\mathcal{M} \models \varphi$.
- $\mathcal{M} \models \varphi \wedge \psi$ hvis $\mathcal{M} \models \varphi$ *og* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \vee \psi$ hvis $\mathcal{M} \models \varphi$ *eller* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \varphi \rightarrow \psi$ hvis $\mathcal{M} \models \varphi$ *impliserer* $\mathcal{M} \models \psi$.
- $\mathcal{M} \models \forall x\varphi$ hvis $\mathcal{M} \models \varphi[x/\bar{a}]$ *for alle* a i $|\mathcal{M}|$.
- $\mathcal{M} \models \exists x\varphi$ hvis $\mathcal{M} \models \varphi[x/\bar{a}]$ *for minst en* a i $|\mathcal{M}|$.

Vi skriver $\mathcal{M} \models \varphi$ for at φ er sann i $\mathcal{M}$ eller at $\mathcal{M}$ gjør φ sann.

Språk og modeller: Et komplekst forhold

- Ved førsteordens språk har vi fått betydelig større uttrykkskraft.
- Modeller kan være rike på struktur.
- Det er et ikke-trivielt forhold mellom språk og modeller.
- Noe av det vi er interessert i:
  - Sjekke om en formel er sann i en modell. (Modellsjekking)
  - Sjekke om en formel er oppfyllbar eller falsifiserbar.
  - Sjekke om en formel er gyldig.
  - Sjekke om formler er uavhengige av hverandre.
  - Bruke språket til å beskrive modeller, forsøke å "fange inn" og beskrive virkeligheten.

Noen eksempler

Eksempel 1

Oppgave.
Lag en modell som oppfyller følgende formler.

1. $\exists xPx$
2. $\forall x\neg Qx$

Følgende er én måte å løse denne oppgaven på.

- La domenet til modellen $\mathcal{M}$ være $\{1\}$, det vil si, $|\mathcal{M}| = \{1\}$.
- Det er ingen konstantsymboler eller funksjonssymboler i språket, så vi trenger ikke å spesifisere tolkningen av disse.
- La relasjonssymbolene tolkes slik at $P^{\mathcal{M}} = \{1\}$ og $Q^{\mathcal{M}} = \emptyset$.
- Formel 1 er sann fordi $P(\bar{1})$ er sann, og $P(\bar{1})$ er sann fordi $1 \in P^{\mathcal{M}}$.
- Formel 2 er sann fordi $\neg Q(\bar{1})$ er sann, og $\neg Q(\bar{1})$ er sann fordi $Q(\bar{1})$ er usann, og $Q(\bar{1})$ er usann fordi $1 \notin Q^{\mathcal{M}}$.

Eksempel 2

Oppgave.
Lag en modell som oppfyller følgende formler.

1. $Pa \wedge Pb$
2. $\neg\exists x(Px \wedge Qx)$
3. $\exists x Qx$.

Følgende er én måte å løse denne oppgaven på.

- La domenet til modellen være $\{1, 2\}$, det vil si, $|\mathcal{M}| = \{1, 2\}$.
- La konstantsymbolene tolkes slik at $a^{\mathcal{M}} = b^{\mathcal{M}} = 1$.
- Det er ingen funksjonssymboler i språket.
- La relasjonssymbolene tolkes slik at $P^{\mathcal{M}} = \{1\}$ og $Q^{\mathcal{M}} = \{2\}$.
- Formel 1 er sann fordi $1 \in P^{\mathcal{M}}$.
- Formel 2 er sann fordi $(P^{\mathcal{M}} \cap Q^{\mathcal{M}}) = \emptyset$.
- Formel 3 er sann fordi $2 \in Q^{\mathcal{M}}$.

Eksempel 3

Oppgave.
Vis at følgende formel er gyldig.

1. $(\forall x Px \wedge \forall x Qx) \rightarrow \forall x(Px \wedge Qx)$

- For å vise at en implikasjon $(F \rightarrow G)$ er *gyldig*, så er det tilstrekkelig å vise at hvis en modell gjør F sann, så gjør den også G sann.

A1 Anta derfor at $\mathcal{M}$ er en modell med domene D som gjør $(\forall x Px \wedge \forall x Qx)$ sann.
(Fra antakelsen A1 skal vi altså vise at $\mathcal{M}$ gjør $\forall x(Px \wedge Qx)$ sann.)

A2 Anta at a er et vilkårlig element i domenet D.

- Fra antakelse A1 følger det at $\mathcal{M}$ gjør både $\forall x Px$ og $\forall x Qx$ sann.
- Fra antakelse A2 følger det at $P\bar{a}$ og $Q\bar{a}$ begge er sanne i $\mathcal{M}$.

- Da må også $P\bar{a} \wedge Q\bar{a}$ være sann i $\mathcal{M}$.
- Siden a var vilkårlig valgt, så følger det at $\forall x(Px \wedge Qx)$ er sann i $\mathcal{M}$.

Eksempel 4

Oppgave.
Vis at følgende formel *ikke* er gyldig.

1. $\forall x(Px \vee Qx) \rightarrow (\forall xPx \vee \forall xQx)$

- Vi må finne en modell som gjør formelen usann.
- Vi må altså finne en modell $\mathcal{M}$ som gjør $\forall x(Px \vee Qx)$ sann, men som gjør $(\forall xPx \vee \forall xQx)$ usann.
- Da må modellen $\mathcal{M}$ gjøre både $\forall xPx$ og $\forall xQx$ usanne.
- La domenet til $\mathcal{M}$ være $\{1, 2\}$.
- For å gjøre $\forall xPx$ usann, la $P^{\mathcal{M}} = \{1\}$.

  Da vil $P\bar{2}$, og derfor også $\forall xPx$, være usann.
- For å gjøre $\forall xQx$ usann, la $Q^{\mathcal{M}} = \{2\}$.

  Da vil $Q\bar{1}$, og derfor også $\forall xQx$, være usann.
- Det er lett å sjekke at $\forall x(Px \vee Qx)$ er sann i $\mathcal{M}$.

Eksempel 5

Oppgave.
Vis at følgende formel er gyldig.

1. $\forall xRxx \rightarrow \forall x\exists yRxy$

- La $\mathcal{M}$ være en modell med domene D og anta at $\mathcal{M} \models \forall xRxx$.
- Det er tilstrekkelig å vise at $\mathcal{M} \models \forall x\exists yRxy$.
- La $a \in D$ være vilkårlig valgt.
- Ved antakelse vet vi at $\mathcal{M} \models R\bar{a}\bar{a}$.
- Da er det slik at $\mathcal{M} \models \exists yR\bar{a}y$.
- Siden a var vilkårlig valgt, vil $\mathcal{M} \models \forall x\exists yRxy$.

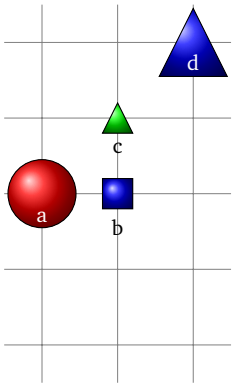
Figurspråket igjen

En utvidelse av figurspråket

Figurspråket

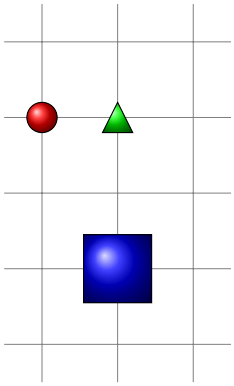
Atomær formel	Intendert tolkning
$\mathsf{Sirkel}(x)$	x er en sirkel
$\mathsf{Firkant}(x)$	x er en firkant
$\mathsf{Trekant}(x)$	x er en trekant
$\mathsf{Stor}(x)$	x er stor
$\mathsf{Liten}(x)$	x er liten
$\mathsf{Mindre}(x, y)$	x er mindre enn y
$\mathsf{Over}(x, y)$	x er nærmere toppen enn y
$\mathsf{Under}(x, y)$	x er nærmere bunnen enn y
$\mathsf{VenstreFor}(x, y)$	x er lenger til venstre enn y
$\mathsf{HoyreFor}(x, y)$	x er lenger til høyre enn y
$\mathsf{Inntil}(x, y)$	x er rett ved siden av, rett over eller rett under y
$\mathsf{Mellom}(x, y, z)$	x, y og z er i samme kolonne, rad eller diagonal, og x er mellom y og z

Forklarende eksempel til semantikken



- $a^{\mathcal{M}} =$  , $b^{\mathcal{M}} =$  , $c^{\mathcal{M}} =$  , $d^{\mathcal{M}} =$ 
  (vi antar at dette er alle konstantene)
- $\mathsf{Trekant}^{\mathcal{M}} =$ {,  }
- $\mathsf{Stor}^{\mathcal{M}} =$ {  ,  }
- $\mathsf{Liten}^{\mathcal{M}} =$ {, }
- $\mathcal{M} \models \mathsf{Under}(a, c)$
  fordi $\langle a^{\mathcal{M}}, c^{\mathcal{M}} \rangle = \langle$  , $\rangle \in \mathsf{Under}^{\mathcal{M}}$
- $\mathcal{M} \models \neg\mathsf{Under}(a, b)$
- $\mathcal{M} \models \mathsf{VenstreFor}(a, c) \wedge \neg\mathsf{VenstreFor}(b, c)$
- $\mathcal{M} \models \mathsf{Inntil}(a, b) \wedge \neg\mathsf{Inntil}(a, c)$
- $\mathcal{M} \models \mathsf{Mellom}(c, a, d) \wedge \neg\mathsf{Mellom}(c, b, d)$

Eksempel 1

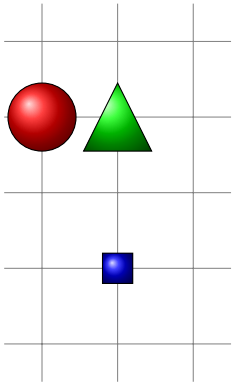


- Er det slik at $\mathcal{M} \models \exists x \mathsf{Liten}(x)$?
- For å svare, må vi se på definisjonen av $\models$.

$$\mathcal{M} \models \exists x \mathsf{Liten}(x)$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \mathcal{M} \models \mathsf{Liten}(\bar{a})$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } \bar{a}^{\mathcal{M}} \in \mathsf{Liten}^{\mathcal{M}}$$
$$\Updownarrow$$
$$\text{det fins en } a \in |\mathcal{M}| \text{ slik at } a \in \mathsf{Liten}^{\mathcal{M}}$$

- Siden $\mathsf{Liten}^{\mathcal{M}} = \{$●, ▲$\}$, kan vi konkludere med **JA**.

Eksempel 2

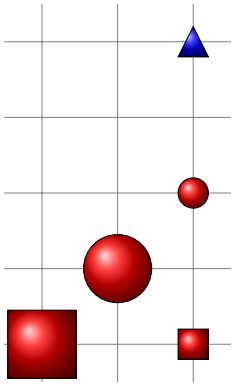


- Er det slik at $\mathcal{M} \models \forall x \mathsf{Stor}(x)$?
- For å svare, må vi se på definisjonen av $\models$.

$$\mathcal{M} \models \forall x \mathsf{Stor}(x)$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } \mathcal{M} \models \mathsf{Stor}(\bar{a})$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } \bar{a}^{\mathcal{M}} \in \mathsf{Stor}^{\mathcal{M}}$$
$$\Updownarrow$$
$$\text{for alle } a \in |\mathcal{M}| \text{ så } a \in \mathsf{Stor}^{\mathcal{M}}$$

- Siden $|\mathcal{M}| = \{$■, ●, ▲$\}$ og $\mathsf{Stor}^{\mathcal{M}} = \{$●, ▲$\}$, så kan vi konkludere med **NEI**.

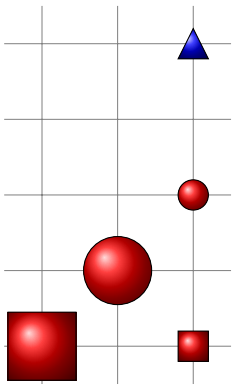
Eksempel 3



$$\mathcal{M} \models \forall x(\mathsf{Stor}(x) \rightarrow \mathsf{Sirkel}(x))$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \mathsf{Stor}(\bar{a}) \rightarrow \mathsf{Sirkel}(\bar{a})$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$\mathcal{M} \models \mathsf{Stor}(\bar{a})$ impliserer $\mathcal{M} \models \mathsf{Sirkel}(\bar{a})$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
hvis $a \in \mathsf{Stor}^{\mathcal{M}}$, så $a \in \mathsf{Sirkel}^{\mathcal{M}}$
$$\Updownarrow$$
"alle store objekter er sirkler"

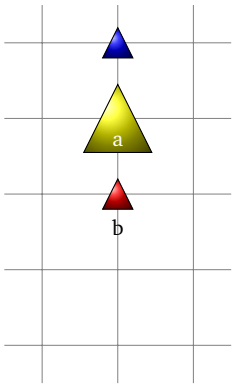
Påstanden holder ikke.

Eksempel 4



$$\mathcal{M} \models \forall x(\mathsf{Sirkel}(x) \rightarrow \exists y \exists z \mathsf{Mellom}(x, y, z))$$
$$\Updownarrow$$
for alle $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \mathsf{Sirkel}(\bar{a}) \rightarrow \exists y \exists z \mathsf{Mellom}(\bar{a}, y, z)$$
$$\Updownarrow$$
for alle sirkler $a \in |\mathcal{M}|$ så
$$\mathcal{M} \models \exists y \exists z \mathsf{Mellom}(\bar{a}, y, z)$$
$$\Updownarrow$$
for alle sirkler $a \in |\mathcal{M}|$ så
fins $b, c \in \mathcal{M}$ slik at $\mathcal{M} \models \mathsf{Mellom}(\bar{a}, \bar{b}, \bar{c})$
Påstanden holder, fordi
$\mathcal{M} \models \mathsf{Mellom}(\bar{\bigcirc}, \bar{\square}, \bar{\bigcirc})$ og
$\mathcal{M} \models \mathsf{Mellom}(\bar{\bigcirc}, \bar{\square}, \bar{\triangle})$.

Eksempel 5

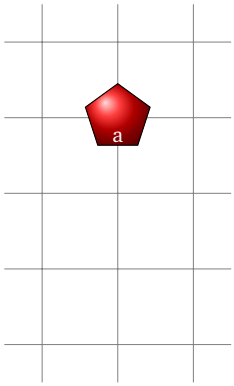


Er følgende formler oppfyllbare samtidig?

1. $\mathsf{Stor}(\mathfrak{a}) \wedge \mathsf{Liten}(\mathfrak{b})$
2. $\forall x(\mathsf{Trekant}(x))$
3. $\forall x(\mathsf{Inntil}(x, \mathfrak{a}) \vee \mathsf{Inntil}(x, \mathfrak{b}))$
4. $\neg\exists x(\mathsf{VenstreFor}(x, \mathfrak{a}) \vee \mathsf{HoyreFor}(x, \mathfrak{a}))$
5. $\forall x(\mathsf{Stor}(x) \rightarrow \exists y\mathsf{Over}(y, x))$

Svaret er JA!

Eksempel 6



Er følgende formler oppfyllbare?

1. $\neg\mathsf{Sirkel}(\mathfrak{a}) \wedge \neg\mathsf{Trekant}(\mathfrak{a}) \wedge \neg\mathsf{Firkant}(\mathfrak{a}))$

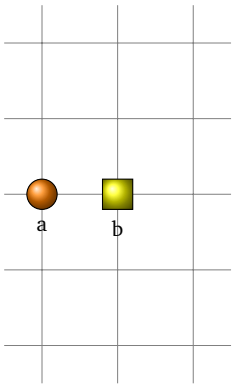
   Svaret er JA!

   La $|\mathcal{M}| = \{$ $\}$ og $\mathfrak{a}^{\mathcal{M}} =$.
2. $\mathsf{Liten}(\mathfrak{a}) \wedge \mathsf{Stor}(\mathfrak{a})$

   Svaret er JA!

   La $|\mathcal{M}| = \{$ $\}$, $\mathfrak{a}^{\mathcal{M}} =$ og $\mathsf{Liten}^{\mathcal{M}} = \mathsf{Stor}^{\mathcal{M}} = \{$ $\}$

Bruke språket til å beskrive modeller



Gi en mengde formler som beskriver denne modellen nøyaktig, dvs. som har denne og (essensielt) ingen andre modeller.

1. $\mathsf{Sirkel}(\mathfrak{a}) \wedge \mathsf{Firkant}(\mathfrak{b})$
2. $\forall x\mathsf{Liten}(x)$
3. $\mathsf{VenstreFor}(\mathfrak{a}, \mathfrak{b})$
4. $\forall x(\mathsf{Inntil}(x, \mathfrak{a}) \vee \mathsf{Inntil}(x, \mathfrak{b}))$
5. $\forall x(\neg\mathsf{Over}(x, \mathfrak{a}) \wedge \neg\mathsf{Under}(x, \mathfrak{a}))$
6. $\forall x(\neg\mathsf{VenstreFor}(x, \mathfrak{a}) \wedge \neg\mathsf{HoyreFor}(x, \mathfrak{b}))$

Ganske vanskelig...

INF1800 – Forelesning 20

Førsteordens logikk

Roger Antonsen - 22. oktober 2008

Mer om førsteordens logikk

Tillukninger

- Vi har definert semantikk kun for lukkede formler.
- Det er ikke vanskelig å utvide definisjonen til formler med frie variable; se boka for detaljer.
- Følgende er nyttig når vi har frie variable.

Definisjon (Tillukning).

- La F være en formel med frie variable $x_1, \ldots, x_n$.
- $\forall x_1 \forall x_2 \ldots \forall x_n F$ kalles den *universelle tillukningen* av F.
- $\exists x_1 \exists x_2 \ldots \exists x_n F$ kalles den *eksistensielle tillukningen* av F.

Ekvivalens

Definisjon (Ekvivalens).
To lukkede førsteordens formler A og B er *ekvivalente* hvis enhver modell som gjør A sann, også gjør B sann, og vice versa. Sagt på en annen måte, for enhver modell $\mathcal{M}$, så vil $\mathcal{M} \models A$ hvis og bare hvis $\mathcal{M} \models B$. Vi skriver $A \equiv B$ når A og B er ekvivalente. En annen vanlig skrivemåte er $A \Leftrightarrow B$.

- A og B er ekvivalente formler hvis og bare hvis formelen $(A \to B) \wedge (B \to A)$ er gyldig.
- Alle gyldige formler er ekvivalente med hverandre.
- Alle uoppfyllbare formler er ekvivalente med hverandre.

Kvantorer og negasjon

Merk.

- $\neg \forall x F$ er ekvivalent med $\exists x \neg F$.
- $\neg \exists x F$ er ekvivalent med $\forall x \neg F$.

- Det er en fin øvingsoppgave å bevise disse.
- For å bevise den øverste av dem, må vi bevise følgende.
    1. For alle modeller $\mathcal{M}$, hvis $\mathcal{M} \models \neg\forall x F$, så $\mathcal{M} \models \exists x \neg F$.
    2. For alle modeller $\mathcal{M}$, hvis $\mathcal{M} \models \exists x \neg F$, så $\mathcal{M} \models \neg\forall x F$.
- Vi nøyer oss med å vise 1; resten er øvingsoppgaver.
- For å vise 1, la $\mathcal{M}$ være en modell slik at $\mathcal{M} \models \neg\forall x F$.
- Da er det slik at $\mathcal{M} \not\models \forall x F$, det vil si, det *ikke* er slik at $\mathcal{M} \models \forall x F$
- Da fins et element a i domenet til $\mathcal{M}$ slik at $\mathcal{M} \not\models F[x/\bar{a}]$.
- Da vil $\mathcal{M} \models \neg F[x/\bar{a}]$, og da holder $\mathcal{M} \models \exists x \neg F$.

Distribusjon av kvantorer

Merk.

- $\exists x(Px \vee Qx)$ er ekvivalent med $\exists x Px \vee \exists x Qx$.
- $\forall x(Px \wedge Qx)$ er ekvivalent med $\forall x Px \wedge \forall x Qx$.

- Det er *ikke* slik at $\forall x(Px \vee Qx)$ er ekvivalent med $\forall x Px \vee \forall x Qx$.
- Det er *ikke* slik at $\exists x(Px \wedge Qx)$ er ekvivalent med $\exists x Px \wedge \exists x Qx$.

Merk.

- $\exists x(Px \to Qx)$ er ekvivalent med $\forall x Px \to \exists x Qx$.

- $\exists x(Px \to Qx)$ er ekvivalent med $\exists x(\neg Px \vee Qx)$,
  som er ekvivalent med $\exists x \neg Px \vee \exists x Qx$,
  som er ekvivalent med $\neg\forall x Px \vee \exists x Qx$,
  som er ekvivalent med $\forall x Px \to \exists x Qx$.

Omdøping av variable

Merk.
Hvis y er en variabel som ikke forekommer fri i F, så holder følgende.

- $\exists x F$ er ekvivalent med $\exists y F[x/y]$.
- $\forall x F$ er ekvivalent med $\forall y F[x/y]$.

Her er $F[x/y]$ resultatet av å erstatte alle frie forekomster av x i F med y.

Eksempel.

- $\exists x P x$ er ekvivalent med $\exists y P y$.
  - Her er $\exists y P x[x/y] = \exists y P y$, fordi $P x[x/y] = P y$.

Flere ekvivalenser

Merk.
Hvis x er en variabel som ikke forekommer fri i F, så holder følgende.

- $\forall x F$ er ekvivalent med F.
- $\forall x(F \wedge G)$ er ekvivalent med $F \wedge \forall x G$.
- $\exists x(F \wedge G)$ er ekvivalent med $F \wedge \exists x G$.
- $\forall x(F \vee G)$ er ekvivalent med $F \vee \forall x G$.
- $\exists x(F \vee G)$ er ekvivalent med $F \vee \exists x G$.
- $\forall x(F \to G)$ er ekvivalent med $F \to \forall x G$.
- $\exists x(F \to G)$ er ekvivalent med $F \to \exists x G$.
- $\forall x(G \to F)$ er ekvivalent med $\exists x G \to F$.
- $\exists x(G \to F)$ er ekvivalent med $\forall x G \to F$.

Vi kan "dytte kvantoren innover".

Preneks normalform

Definisjon.
En lukket førsteordens formel er på *preneks normalform (PNF)* hvis den er på formen

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n F$$

hvor $Q_i \in \{\forall, \exists\}$ og F er kvantorfri.

Eksempel.
Følgende formler er på preneks normalform.

- Pa
- $\forall x Px$
- $\forall x \exists y (Rxy \wedge Ryx)$

Eksempel.
Følgende formler er *ikke* på preneks normalform.

- $Pa \wedge \forall x Qx$
- $\forall x (Px \rightarrow \exists y Rxy)$
- $\forall x (\forall y Rxy \rightarrow \forall z Sxz)$

Teorem.
Enhver lukket førsteordens formel er ekvivalent med en lukket førsteordens formel på preneks normalform.

- Hvis F er en lukket førsteordens formel, så kan vi konstruere en ekvivalent formel på preneks normalform på følgende måte.
  1. Omdøp alle variable slik at ingen kvantorer binder samme variabel.
  2. Flytt kvantorene utover ved hjelp av ekvivalensene vi har sett på.

Eksempel.

$$\begin{aligned}(Pa \wedge (\forall x Qx \vee \forall x Rx)) &\equiv (Pa \wedge (\forall x Qx \vee \forall y Ry)) \\ &\equiv (Pa \wedge \forall x (Qx \vee \forall y Ry)) \\ &\equiv (Pa \wedge \forall x \forall y (Qx \vee Ry)) \\ &\equiv \forall x (Pa \wedge \forall y (Qx \vee Ry)) \\ &\equiv \forall x \forall y (Pa \wedge (Qx \vee Ry))\end{aligned}$$

Litt om å føre bevis

Bevisteknikker

- Siden noe av det viktigste vi gjør i dette kurset er å bevise påstander, kan det være greit å si noe om hvordan vi gjør det.

Oppgave.
Vis at hvis $\boxed{1}$, så $\boxed{2}$.

1. Et direkte bevis. Forsøk alltid dette først.
   - Anta $\boxed{1}$ og vis klart og tydelig hvorfor denne antakelsen fører til $\boxed{2}$.
2. Et motsigelsesbevis. Hvis et direkte bevis ikke er mulig.
   - Anta for motsigelse at påstanden ikke holder, dvs. at $\boxed{1}$ og ikke $\boxed{2}$.
   - Vis klart og tydelig hvorfor denne antakelsen fører til en motsigelse.
   - Konkluder med at påstanden må holde.
3. Et bevis for den kontrapositive påstanden: hvis ikke $\boxed{2}$, så ikke $\boxed{1}$.
   - Dette er essensielt det samme som en motsigelsesbevis.

Direkte versus indirekte bevis

Noen fordeler med direkte bevis:

- Er som regel enklere å lese.
- Kan inneholde mer informasjon.
- Er mer konstruktivt.
- Kan gi mer intuisjon om grunnene for at noe holder.

Noen fordeler med motsigelsesbevis:

- Kan være enklere å gjennomføre.
- Kan være kortere enn direkte bevis.

Å vise at noe ikke holder

Oppgave.
Vis at ikke $\boxed{\text{X}}$.

- Anta $\boxed{\text{X}}$ og vis klart og tydelig hvorfor denne antakelsen fører til en motsigelse.
- Dette er *ikke* et motsigelsesbevis, men et *direkte* bevis.

$$\dfrac{\begin{array}{c}\neg A \\ \vdots \\ \bot\end{array}}{A} \qquad \dfrac{\begin{array}{c}A \\ \vdots \\ \bot\end{array}}{\neg A}$$

Noen tommelfingerregler

Oppgave.
Vis at $\boxed{X}$.

Noen tommelfingerregler:

1. Sjekk at du behersker alle begrepene som er brukt.
2. Vær klar og tydelig i argumentasjonen.
3. Bruk alle antakelsene.
4. Vis at antakelsene nødvendigvis medfører konklusjonen.
5. Forsøk først med et direkte bevis.

Bevis for "for alle"-påstander

- Se på påstanden "For alle x i S, så er det slik at $P(x)$".
- Vi kan vise denne påstanden ved å vise at $P(a)$ holder for hvert element a i S.
- Men 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, så må påstanden holde.

INF1800 – Forelesning 21

Førsteordens logikk

Roger Antonsen - 28. oktober 2008

Førsteordens sekventkalkyle

Introduksjon

- Sekventkalkyle for utsagnslogikk skal vi nå kunne **godt**.
- Vi har fokusert på to aspekter.
  1. *Finne bevis*. Hvis et bevis fins, så må rotsekventen være gyldig. (Det er sunnhet av kalkylen som sikrer oss det.)
  2. *Lage motmodeller*. Hvis et bevis ikke fins, så gir en "maksimal" utledning nok informasjon til å lage en motmodell. Dette er essensielt hva man gjør for å vise kompletthet av kalkylen.
- Nå skal vi gjøre det samme for førsteordens logikk!
- Gitt en førsteordens formel φ, er φ gyldig?
- Vi introduserte sekventkalkylen for utsagnslogikk som et systematisk forsøk på å falsifisere.
- La oss se hvordan dette blir for førsteordens logikk.

$$\dfrac{\dfrac{\dfrac{\times}{\neg Qa, Pa \vdash Pa}}{\neg Qa \vdash \neg Pa, Pa}}{\vdash Pa, \neg Qa \to \neg Pa} \qquad \dfrac{\dfrac{\dfrac{\times}{Qa \vdash Qa, \neg Pa}}{Qa, \neg Qa \vdash \neg Pa}}{Qa \vdash \neg Qa \to \neg Pa}$$

$$\dfrac{\dfrac{\vdash Pa, \neg Qa \to \neg Pa}{Pa \to Qa \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx) \vdash \neg Qa \to \neg Pa}$$

$$\dfrac{\forall x(Px \to Qx) \vdash \neg Qa \to \neg Pa}{\forall x(Px \to Qx) \vdash \forall x(\neg Qx \to \neg Px)}$$

Eksempel

- Falsifisere formelen $\forall x(\neg Qx \to \neg Px)$:
  - Introdusere et *vitne* som gjør formelen usann.
  - Sette inn et *nytt* konstantsymbol a for x.
- Oppfylle formelen $\forall x(Px \to Qx)$:
  - Da må delformelen være sann uansett hva vi setter inn for x.
  - Spesielt må delformelen være sann når vi setter inn a for x.
- Vi kan nå anvende α- og β-reglene og lukke.

La oss forsøke med en annen regel-rekkefølge:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(Px \to Qx), \neg Qa, Pa, Po \to Qo \vdash Pa}\times}{\forall x(Px \to Qx), \neg Qa, Po \to Qo \vdash \neg Pa, Pa}}{\forall x(Px \to Qx), Po \to Qo \vdash Pa, \neg Qa \to \neg Pa} \qquad \dfrac{\dfrac{\dfrac{}{\forall x(Px \to Qx), Qa, Po \to Qo \vdash Qa, \neg Pa}\times}{\forall x(Px \to Qx), Qa, \neg Qa, Po \to Qo \vdash \neg Pa}}{\forall x(Px \to Qx), Qa, Po \to Qo \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx), Pa \to Qa, Po \to Qo \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx), Po \to Qo \vdash \neg Qa \to \neg Pa}}{\forall x(Px \to Qx), Po \to Qo \vdash \forall x(\neg Qx \to \neg Px)}}{\forall x(Px \to Qx) \vdash \forall x(\neg Qx \to \neg Px)}$$

Eksempel

- Oppfylle $\forall x(Px \to Qx)$:
  - Hva skal vi sette inn for x? Vi bruker en *dummykonstant* o.
- Falsifisere $\forall x(\neg Qx \to \neg Px)$:
  - Vitnet må være *ubrukt*. Kan derfor ikke sette inn o. Setter inn a.
- Oppfylle $\forall x(Px \to Qx)$. Da må vi kunne sette inn a for x!
  - Vi må ta kopi av $\forall$-formelen når vi setter inn for x.
  - Setter inn a for x.
- Vi kan nå anvende α- og β-reglene og lukke.

Motivasjon

- Vi skal nå definere sekventkalkyle for førsteordens logikk.
- Vi trenger slutningsregler for formler med kvantorene $\forall/\exists$.
- Fra de foregående eksemplene har vi:
  - Hvis vi skal oppfylle en formel $\forall x\varphi$ så må vi oppfylle $\varphi[x/t]$ for alle valg av term t.
  - I tillegg trenger vi en ekstra kopi av $\forall x\varphi$.
  - Hvis vi skal falsifisere $\forall x\varphi$ må vi velge et *vitne* – et ubrukt konstantsymbol a – slik at $\varphi[x/a]$ er usann.
  - Å oppfylle/falsifisere $\exists$-formler blir dualt.
- Vi skal nå definere begreper som *sekvent*, *aksiom*, *utledning* og *bevis* for førsteordens språk.

Sekventer og aksiomer

Definisjon (Parameter).
La $\mathcal{L}$ være et førsteordens språk og la par være en tellbart uendelig mengde av konstantsymboler, kalt *parametre*, forskjellige fra symbolene i $\mathcal{L}$. La $\mathcal{L}^{\text{par}}$ være det førsteordens språket man får ved å ta med disse som konstantsymboler.

Definisjon (Sekvent).
En *sekvent* er et objekt på formen $\Gamma \vdash \Delta$ slik at Γ og Δ er multimengder av *lukkede* førsteordens formler i $\mathcal{L}^{\text{par}}$.

Definisjon (Aksiom).
Et *aksiom* er en sekvent på formen $\Gamma, A \vdash A, \Delta$ slik at A er en *atomær* formel.

Sekventkalkyleregler

Definisjon (γ-regler).
γ-reglene i sekventkalkylen LK er

$$\frac{\Gamma, \forall x \varphi, \varphi[x/t] \vdash \Delta}{\Gamma, \forall x \varphi \vdash \Delta} \, L\forall \qquad \frac{\Gamma \vdash \Delta, \exists x \varphi, \varphi[x/t]}{\Gamma \vdash \Delta, \exists x \varphi} \, R\exists$$

hvor t er en *lukket* term.

- Termen t kan være hvilken som helst lukket term.
- Kopieringen av hovedformelen i γ-reglene medfører at bevissøk i førsteordens logikk ikke nødvendigvis behøver å terminere.

Definisjon (δ-regler).
δ-reglene i sekventkalkylen LK er

$$\frac{\Gamma, \varphi[x/a] \vdash \Delta}{\Gamma, \exists x \varphi \vdash \Delta} \, L\exists \qquad \frac{\Gamma \vdash \Delta, \varphi[x/a]}{\Gamma \vdash \Delta, \forall x \varphi} \, R\forall$$

hvor a er en parameter som *ikke* forekommer i konklusjonen.

- Uten kravet om at a ikke skal være i konklusjonen får vi en usunn kalkyle.
- γ-reglene erstatter den bundne variabelen med en lukket term.
- δ-reglene erstatter den bundne variabelen med et konstantsymbol.
- Det betyr at hvis hovedformelen er lukket, så er også de aktive formlene lukkede.
- γ- og δ-reglene er derfor *veldefinerte* i den forstand at alle sekventer forblir lukket.

Definisjon (Slutningsreglene i førsteordens LK).
Slutningsreglene i førsteordens LK er α- og β-reglene fra utsagnslogisk LK *og* γ- og δ-reglene.

Slutninger

- Som i utsagnslogikk definerer reglene *slutninger* ved at vi erstatter symbolene i reglene med lukkede førsteordens formler:

$$\text{L}\forall\text{-regel}\qquad \frac{\Gamma, \forall x\varphi, \varphi[x/t] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}\,\text{L}\forall \qquad\qquad \text{L}\forall\text{-slutning}\qquad \frac{Pa, \forall x(Px \to Qx), Pa \to Qa \vdash Qa}{Pa, \forall x(Px \to Qx) \vdash Qa}\,\text{L}\forall$$

- Begrepene innført i tilknytning til regler/slutninger i utsagnslogisk LK gjelder også i førsteordens LK:
  - 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*.

Utledninger

- Utledninger er definert som for utsagnslogikk, men
  - vi har to ekstra regler, γ- og δ-reglene, og
  - basistilfellet i definisjonen av LK-utledninger er litt annerledes.

Definisjon (LK-utledninger – basistilfelle).
En sekvent $\Gamma \vdash \Delta$, hvor Γ og Δ er multimengder av lukkede førsteordens formler i $\mathcal{L}$, er en LK-*utledning*.

$$\Gamma \vdash \Delta$$

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

- Språket $\mathcal{L}^{\text{par}}$ brukes ikke i rotsekventen, men kun for å introdusere nye parametre i δ-reglene.
- Resten er som for utsagnslogikk.
- Slutninger brukes til å *utvide* utledninger.

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.

Definisjon (Bevisbar formel).
Et *bevis* for en formel φ er et bevis for sekventen $\vdash \varphi$. En formel φ er *bevisbar* hvis det fins en bevis for den.

Sunnhet og kompletthet

- Vi har følgende teoremer om førsteordens sekventkalkyle.

Teorem (Sunnhet).
Enhver bevisbar sekvent er gyldig.

Teorem (Kompletthet).
Enhver gyldig sekvent er bevisbar.

- Vi skal ikke bevise disse i dette kurset, men vi skal vite hva som er hva og ha noen intuisjoner om hvorfor det er slik.
- Når bruker vi at sekventkalkylen er sunn?

$$\begin{gathered}\text{sekventen } \Gamma \vdash \Delta \text{ er bevisbar i sekventkalkyle} \\ + \\ \text{sekventkalkylen er sunn} \\ = \\ \text{sekventen } \Gamma \vdash \Delta \text{ er gyldig}\end{gathered}$$

Eksempler

Eksempel 1

$$\dfrac{\dfrac{\times}{\forall x Px, Pa \vdash Pa}}{\dfrac{\forall x Px \vdash Pa}{\forall x Px \vdash \forall x Px}}$$

- Dette viser at sekventen $\forall x Px \vdash \forall x Px$ er bevisbar.
- Siden sekventkalkylen er sunn, så vet vi at sekventen er gyldig.
- Det er også lett å se direkte at sekventen er også gyldig.
  - Envher modell som oppfyller antesedenten, må oppfylle suksedenten.

Eksempel 2

$$\dfrac{\dfrac{\dfrac{}{\forall xPx, Po \vdash \exists xPx, Po}\times}{\forall xPx \vdash \exists xPx, Po}}{\forall xPx \vdash \exists xPx}$$

- Dette viser at sekventen $\forall xPx \vdash \exists xPx$ er bevisbar.
- Siden sekventkalkylen er sunn, så vet vi at sekventen er gyldig.
- Det er også lett å se direkte at sekventen er også gyldig.
  - Anta at modellen $\mathcal{M}$ gjør $\forall xPx$ sann.
  - Domenet må bestå av minst ett element e.
  - Siden $\mathcal{M}$ gjør $\forall xPx$ sann, må $\mathcal{M}$ gjøre formelen $P\bar{e}$ sann.
  - Siden $\mathcal{M}$ gjør $P\bar{e}$ sann, må $\mathcal{M}$ gjøre formelen $\exists xPx$ sann.

Eksempel 3

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(Px \wedge Qx), Pa, Qa \vdash Pa}\times}{\forall x(Px \wedge Qx), Pa \wedge Qa \vdash Pa}}{\forall x(Px \wedge Qx) \vdash Pa}}{\forall x(Px \wedge Qx) \vdash \forall xPx} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(Px \wedge Qx), Pa, Qa \vdash Qa}\times}{\forall x(Px \wedge Qx), Pa \wedge Qa \vdash Qa}}{\forall x(Px \wedge Qx) \vdash Qa}}{\forall x(Px \wedge Qx) \vdash \forall xQx}}{\forall x(Px \wedge Qx) \vdash \forall xPx \wedge \forall xQx}$$

- Dette viser at sekventen $\forall x(Px \wedge Qx) \vdash \forall xPx \wedge \forall xQx$ er bevisbar.
- Siden sekventkalkylen er sunn, så vet vi at sekventen er gyldig.
- Det er også lett å se direkte at sekventen er også gyldig.
  - Anta at modellen $\mathcal{M}$ gjør $\forall x(Px \wedge Qx)$ sann.
  - Velg et vilkårlig element e i domenet til $\mathcal{M}$.
  - Ved antakelsen må $\mathcal{M}$ gjøre $P\bar{e} \wedge Q\bar{e}$ sann.
  - Da må $\mathcal{M}$ gjøre $P\bar{e}$ og $Q\bar{e}$ sann.
  - Siden e var vilkårlig valgt, må $\mathcal{M}$ også gjøre $\forall xPx$ og $\forall xQx$ sanne.

Eksempel 4

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall yLya, Lba \vdash Lba, \exists yLby}\times}{\forall yLya, Lba \vdash \exists yLby}}{\forall yLya \vdash \exists yLby}}{\forall yLya \vdash \forall x\exists yLxy}}{\exists x\forall yLyx \vdash \forall x\exists yLxy}$$

- Dette viser at sekventen $\exists x\forall yLyx \vdash \forall x\exists yLxy$ er bevisbar.
- Siden sekventkalkylen er sunn, så vet vi at sekventen er gyldig.
- Det er også lett å se direkte at sekventen er også gyldig.
  - Anta at modellen $\mathcal{M}$ gjør $\exists x\forall yLyx$ sann.
  - Da fins det et element a slik at $\forall yLy\bar{a}$ er sann i $\mathcal{M}$.
  - For å vise at $\forall x\exists yLxy$ er sann i $\mathcal{M}$, velg et vilkårlig element b.

– Det er nok å vise at $\exists y L\bar{b}y$ er sann i $\mathcal{M}$.
– Vi har at $L\bar{b}\bar{a}$ er sann i $\mathcal{M}$, siden $\forall y Ly\bar{a}$ er sann i $\mathcal{M}$.
– "Hvis det fins en som blir likt av alle, så har alle noen de liker."

Eksempel 5

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\forall x\exists y Lxy, Lbc, Loa \vdash Lba, Ldc, \exists x\forall y Lyx}}{\forall x\exists y Lxy, Lbc, Loa \vdash Lba, \forall y Lyc, \exists x\forall y Lyx}}{\forall x\exists y Lxy, Lbc, Loa \vdash Lba, \exists x\forall y Lyx \exists x\forall y Lyx}}{\forall x\exists y Lxy, \exists y Lby, Loa \vdash Lba, \exists x\forall y Lyx}}{\forall x\exists y Lxy \forall x\exists y Lxy, Loa \vdash Lba, \exists x\forall y Lyx}}{\forall x\exists y Lxy, Loa \vdash \forall y Lya, \exists x\forall y Lyx}}{\forall x\exists y Lxy, Loa \vdash \exists x\forall y Lyx}}{\forall x\exists y Lxy, \exists y Loy \vdash \exists x\forall y Lyx}}{\forall x\exists y Lxy \vdash \exists x\forall y Lyx}$$

- Vi klarte ikke å bevise sekventen $\forall x\exists y Lxy \vdash \exists x\forall y Lyx$.
- Kan vi klare å lage en motmodell?
  – Kompletthet sier at det *alltid* fins motmodeller for ikke-bevisbare sekventer.
- **JA**, la $\mathcal{M} = \{a, b\}$ og la $L^{\mathcal{M}} = \{\langle a, a\rangle, \langle b, b\rangle\}$.
- "Alle liker seg selv og ingen andre."
- Da vil $\mathcal{M} \models \forall x\exists y Lxy$.
  – $\mathcal{M} \models \exists y L\bar{a}y$, siden $\mathcal{M} \models L\bar{a}\bar{a}$.
  – $\mathcal{M} \models \exists y L\bar{b}y$, siden $\mathcal{M} \models L\bar{b}\bar{b}$.
- Og $\mathcal{M} \not\models \exists x\forall y Lyx$.
  – $\mathcal{M} \not\models \forall y Ly\bar{a}$, siden $\mathcal{M} \not\models L\bar{b}\bar{a}$.
  – $\mathcal{M} \not\models \forall y Ly\bar{b}$, siden $\mathcal{M} \not\models L\bar{a}\bar{b}$.

Eksempel 6

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\times}{Po, Pa \vdash \forall xPx, Pa, \exists x(Px \to \forall xPx)}}{Po \vdash Pa, Pa \to \forall xPx, \exists x(Px \to \forall xPx)}}{Po \vdash Pa, \exists x(Px \to \forall xPx) \exists x(Px \to \forall xPx)}}{Po \vdash \forall xPx, \exists x(Px \to \forall xPx)}}{\vdash Po \to \forall xPx, \exists x(Px \to \forall xPx)}}{\vdash \exists x(Px \to \forall xPx)}$$

- Dette viser at sekventen $\vdash \exists x(Px \to \forall xPx)$ er bevisbar.
- "Det fins en x slik at hvis x liker fotball, så liker alle fotball."
- Dette er ikke den samme påstanden som: "Hvis det fins en x som liker fotball, så liker alle fotball."
- Oppgave: vis at formelen er gyldig. Argumenter for at formelen er sann i enhver modell.

INF1800 – Forelesning 22

Førsteordens logikk

Roger Antonsen - 29. oktober 2008

Litt om konsistens

Oppfyllbarhet og konsistens

Definisjon.
En mengde Γ av formler er *oppfyllbar* hvis det fins en modell som oppfyller alle formlene i mengden.

Definisjon.
En mengde Γ er *konsistent* hvis sekventen $\Gamma \vdash$ ikke er bevisbar. Hvis $\Gamma \vdash$ er bevisbar, så sier vi at Γ er *inkonsistent.*

Eksempel.
Mengden $\{P \vee Q, \neg P\}$ er oppfyllbar. La f.eks. ν være en valuasjon som gjør Q sann og P usann.

Eksempel.
Mengden $\{P \vee Q, \neg P\}$ er konsistent.

$$\dfrac{\dfrac{\times}{P \vdash P} \qquad Q \vdash P}{P \vee Q \vdash P}$$
$$P \vee Q, \neg P \vdash$$

Sunnhet og kompletthet – andre formuleringer

Sunnhet:	enhver oppfyllbar mengde er konsistent.
Kompletthet:	enhver konsistent mengde er oppfyllbar.

Oppgave (litt vanskelig).
Vis at disse formuleringene er ekvivalente med de vanlige formuleringene.