Paketti I: LAUSELOGIIKKA

1. Lauselogiikan kieli
2. Totuustaulut ja semantiikka
3. Semanttinen taulu
4. Taulumenetelmän ominaisuuksia
5. Hilbert-tyyppinen lauselogiikan aksiomatisointi
6. Normaalimuodot
7. Lauseiden klausuulimuoto
8. Resoluutiosääntö
9. Resoluution ominaisuuksia
10. Laskennallisesta vaativuudesta

1 Lauselogiikan kieli

Lauselogiikan aakkosto:

- atomiset lauseet: $A, A_1, A_2, \ldots, B, B_1, \ldots, C, \ldots$
- negaatiosymboli: $\neg$ (ei)
- konjunktiosymboli: $\wedge$ (ja)
- disjunktiosymboli: $\vee$ (tai)
- implikaatiosymboli: $\rightarrow$ (jos...niin)
- ekvivalenssisymboli $\leftrightarrow$ (jos ja vain jos)
- sulut: ()

Symbolit $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ ovat *konnektiiveja*.

Lauselogiikan lauseenmuodostussäännöt:

1. Atomiset lauseet ovat *lauseita*.
2. Jos P ja Q ovat lauseita, niin myös $(\neg P)$, $(P \vee Q)$, $(P \wedge Q)$, $(P \rightarrow Q)$, $(P \leftrightarrow Q)$ ovat *lauseita*.
3. vain edellä olevien sääntöjen perusteella muodostetut merkkijonot ovat *lauseita*.

Atomisten lauseiden joukon $\mathcal{P}$ virittämä *lauselogiikan kieli* $\mathcal{L}$ voidaan määritellä pienimpänä joukkona, joka toteuttaa seuraavat ehdot:

1. Jos $A \in \mathcal{P}$, niin $A \in \mathcal{L}$ (eli $\mathcal{P} \subseteq \mathcal{L}$).
2. Jos $P \in \mathcal{L}$ ja $Q \in \mathcal{L}$, niin $(\neg P) \in \mathcal{L}$, $(P \vee Q) \in \mathcal{L}$, $(P \wedge Q) \in \mathcal{L}$, $(P \rightarrow Q) \in \mathcal{L}$ ja $(P \leftrightarrow Q) \in \mathcal{L}$.

Esimerkkejä lauseista ovat:

$$B$$
$$(B \rightarrow (\neg A))$$
$$((\neg(C \vee D)) \rightarrow (A \vee B))$$

A = "Australiassa on kevät",
B = "Belgiassa on kevät",
C = "Kanadassa on talvi",
D = "Uudessa Seelannissa on talvi".

Huomio 1. implikaatio $\rightarrow$ *ei* tarkoita syy-seuraus-suhdetta. Esim. olkoon

$A =$ "Kuu on juustoa",
$B =$ "Ruotsi sijaitsee Aasiassa".

Lause $(A \rightarrow B)$ on tosi.

Huomio 2. Disjunktio $(A \vee B)$ on tosi, jos A tai B tai sekä A että B (OR eikä XOR).

Poissulkevaa disjuktiota (XOR) merkitään usein symbolilla $\underline{\vee}$.

Esimerkki. Muotoillaan seuraava luonnollisen kielen lause lauselogiikan lauseena.

Jos tänään sataa, niin otan mukaan sateenvarjon tai kastun.

Valitaan atomiset lauseet

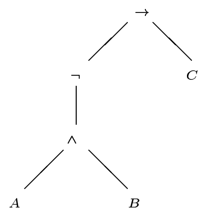
A = "Tänään sataa",
B = "Otan mukaan sateenvarjon",
C = "Kastun".

Saadaan: jos A, niin B tai C.

Tunnistetaan konnektiivit: $(A \rightarrow (B \vee C))$

Jokaisella lauselogiikan lauseella on yksikäsitteinen *jäsennyspuu*.

Esimerkki. Lauseen $((\neg(A \wedge B)) \rightarrow C)$ jäsennyspuu on seuraava:



Jäsennyspuun juuressa oleva konnektiivi $\rightarrow$ määrää, että annettu lause on *muodoltaan* implikaatio (tai *implikaatio* lyhyesti sanottuna).

Vastaavasti määritellään lauseet, jotka ovat muodoltaan negaatioita, konjunktioita, disjunktioita ja ekvivalensseja.

Lauseiden ominaisuuksia voidaan todistaa induktiolla yli lauseen (tai sitä vastaavan jäsennyspuun) rakenteen.

Sulkeiden käytöstä

- uloimmat sulkeet tapana jättää pois: $A \rightarrow B$ eikä $(A \rightarrow B)$
- konnektiivien presedenssi
  1. $\neg$ on vahvin konnektiiveista
  2. $\vee$, $\wedge$ ovat heikompia kuin $\neg$, mutta vahvempia kuin $\rightarrow$, $\leftrightarrow$
  3. $\rightarrow$, $\leftrightarrow$ ovat heikoimmat konnektiivit

     Esimerkiksi: $\neg A \rightarrow B$ eikä $(\neg A) \rightarrow B$,
     $A \wedge B \rightarrow B \vee C$ eikä $(A \wedge B) \rightarrow (B \vee C)$,
     mutta $(A \rightarrow B) \vee (B \leftrightarrow C)$.
- ketjudisjunktiot/konjunktiot: $A \vee B \vee C$ kirjoitetaan lauseiden $A \vee (B \vee C)$ ja $(A \vee B) \vee C$ sijaan.

Määritelmä. Lauseen *alilauseet*:

Atomisen lauseen A ainoa alilause on A.

Lauseen $(\neg\alpha)$ alilauseita ovat α:n alilauseet ja $(\neg\alpha)$.

Lauseen $(\alpha \wedge \beta)$ alilauseita ovat α:n ja β:n alilauseet ja $(\alpha \wedge \beta)$.

Lauseiden $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ ja $(\alpha \leftrightarrow \beta)$ alilauseet määritellään samaan tapaan kuin $(\alpha \wedge \beta)$:n.

Esimerkki. Lauseen $(A \rightarrow (B \vee C))$ alilauseet ovat $A, B, C, (B \vee C)$ ja $(A \rightarrow (B \vee C))$.

Esimerkki: rakenteinen induktio

Väite. Lauseessa ϕ on alilauseita korkeintaan niin monta kuin siinä on atomisia lauseita ja konnektiiveja.

Todistetaan väite rakenteisella induktiolla alilauseiden lukumäärän suhteen. Merkitään lauseen ϕ alilauseiden lukumäärää $\#\phi$:llä, atomisten lauseiden lukumäärää $A\phi$:llä ja konnektiivien lukumäärää $K\phi$:llä.

Näillä merkinnöillä väite saadaan muotoon $\#\phi \leq A\phi + K\phi$.

Perustapaus: ϕ on atominen lause A.

Koska $\#\phi = 1$ määritelmän mukaan, $A\phi = 1$ ja $K\phi = 0$, väittämä pitää tässä tapauksessa paikkansa.

Induktioaskel: ϕ on muotoa $(\neg\alpha)$.

Määritelmän mukaisesti: $\#(\neg\alpha) = 1 + \#\alpha$.

Induktiohypoteesin perusteella: $\#\alpha \leq A\alpha + K\alpha$.

$$\text{Täten} \quad \begin{aligned} \#(\neg\alpha) &\leq 1 + A\alpha + K\alpha \\ &= A\alpha + (1 + K\alpha) \\ &= A(\neg\alpha) + (1 + K\alpha) \\ &= A(\neg\alpha) + K(\neg\alpha). \end{aligned}$$

Näin väittämä tuli todistetuksi muotoa $(\neg\alpha)$ oleville lauseille.

Binääriset konnektiivit $*$ tulee käsitellä samaan tapaan.
Lause ϕ on tällöin muotoa $(\alpha * \beta)$ ja induktiohypoteesia joudutaan soveltamaan sekä α:n että β:n suhteen.

2 Totuustaulut ja semantiikka

Keskeisiä käsitteitä:

- milloin lauselogiikan lause on *tosi* tai *epätosi*
- mikä on *mallin* käsite lauselogiikassa
- mitkä lauseet ovat *päteviä*
- mitkä lauseet ovat *toteutuvia*
- milloin lause on joidenkin toisten lauseiden *looginen seuraus*

Perustotuustaulukot

α	$\neg\alpha$
T	F
F	T

α	β	$(\alpha \wedge \beta)$
T	T	T
T	F	F
F	T	F
F	F	F

α	β	$(\alpha \vee \beta)$
T	T	T
T	F	T
F	T	T
F	F	F

Totuustaulut on helppo sisäistää muistisääntöjen avulla:
esim. $(\alpha \wedge \beta)$ on tosi $\iff$ α on tosi **ja** β on tosi.

Perustotuustaulukot (jatkoa)

α	β	$(\alpha \to \beta)$
T	T	T
T	F	F
F	T	T
F	F	T

α	β	$(\alpha \leftrightarrow \beta)$
T	T	T
T	F	F
F	T	F
F	F	T

Huomaa, että $(\alpha \to \beta)$ on tosi $\iff$ α on epätosi **tai** β on tosi
$\iff$ **jos** α on tosi, **niin** β on tosi

Esimerkki. Tutkittava lause: $(\neg B \wedge (A \to B))$
Alilauseet: $A, B, \neg B, (A \to B), (\neg B \wedge (A \to B))$
Sarakkeita: 5
Rivejä: $2^2 = 4$.

A	B	$\neg B$	$(A \to B)$	$(\neg B \wedge (A \to B))$
T	T	F	T	F
T	F	T	F	F
F	T	F	T	F
F	F	T	T	T

Muistathan, että jokaisessa lauseessa ϕ on korkeintaan niin monta alilausetta kuin lauseessa ϕ on atomisia lauseita ja konnektiiveja (tästä saadaan yläraja lauseen ϕ totuustaulukon leveydelle).

Konnektiivien määriteltävyys/riittävyys

Konnektiivit $\neg, \vee, \wedge, \to, \leftrightarrow$ eivät ole kaikki välttämättömiä:

- $\neg, \vee$ riittävät muiden konnektiivien määrittelemiseen
- $\neg, \wedge$ riittävät myös
- $\neg, \to$ riittävät myös
- $\perp, \to$ riittävät myös (missä $\perp$ on aina epätosi lause)

Esim.

- $(\alpha \wedge \beta)$ lauseena $\neg(\neg\alpha \vee \neg\beta)$
- $(\alpha \to \beta)$ lauseena $(\neg\alpha \vee \beta)$ tai lauseena $\neg(\alpha \wedge \neg\beta)$
- $(\alpha \leftrightarrow \beta)$ lauseena $((\neg\alpha \vee \beta) \wedge (\alpha \vee \neg\beta))$

Totuusjakelut ja valuaatiot

Määritelmä. *Totuusjakelu* $\mathcal{A}$ on funktio kielen $\mathcal{L}$ *atomisten lauseiden joukolta* $\mathcal{P}$ joukolle $\{T, F\}$ (totuusarvot tosi ja epätosi).

Määritelmä. *Valuaatio* $\mathcal{V}$ on *konnektiivien totuustaulukkoja noudattava* funktio kielen $\mathcal{L}$ *lauseiden joukolta* joukolle $\{T, F\}$.

Esimerkki. Olkoon $\mathcal{P} = \{A, B\}$ ja $\mathcal{L}$ vastaava kieli.

Totuusjakelu $\mathcal{A} : \mathcal{P} \to \{T, F\}$	Valuaatio $\mathcal{V} : \mathcal{L} \to \{T, F\}$
	$\mathcal{V}(A) = T$
	$\mathcal{V}(B) = F$
$\mathcal{A}(A) = T$	$\mathcal{V}(A \wedge B) = F$
$\mathcal{A}(B) = F$	$\mathcal{V}(A \vee B) = T$
	$\vdots$

Totuusjakelu määrää yksikäsitteisesti lauseen totuusarvon:

Väite. Jokaiselle totuusjakelulle $\mathcal{A}$ on olemassa täsmälleen yksi valuaatio $\mathcal{V}$ siten että $\mathcal{V}(P) = \mathcal{A}(P)$ kaikille atomisille lauseille P.

$\Rightarrow$ Valuaatio määritellään antamalla totuusarvot atomisille lauseille.

Väite. Jos $\mathcal{V}_1(P) = \mathcal{V}_2(P)$ kaikille α:ssa esiintyville atomisille lauseille P, niin $\mathcal{V}_1(\alpha) = \mathcal{V}_2(\alpha)$.

A	B	$A \to B$	valuaatiot
T	T	T	$\mathcal{V}(A) = T, \quad \mathcal{V}(B) = T, \quad \mathcal{V}(C) = ?$
T	F	F	$\mathcal{V}(A) = T, \quad \mathcal{V}(B) = F, \quad \mathcal{V}(C) = ?$
F	T	T	$\mathcal{V}(A) = F, \quad \mathcal{V}(B) = T, \quad \mathcal{V}(C) = ?$
F	F	T	$\mathcal{V}(A) = F, \quad \mathcal{V}(B) = F, \quad \mathcal{V}(C) = ?$

Peruskäsitteitä

- **Määritelmä.** Valuaatio $\mathcal{V}$ on lauseen α *malli*, jos lause α on tosi valuaatiossa $\mathcal{V}$ eli $\mathcal{V}(\alpha) = T$.

  Esim. jos $\mathcal{V}(A) = T$, niin $\mathcal{V}$ on lauseen $A \vee B$ malli.
- **Määritelmä.** Lause α on *pätevä/tautologia* (merkitään $\models \alpha$), jos $\mathcal{V}(\alpha) = T$ kaikille valuaatiolle $\mathcal{V}$.

  Esim. $A \vee \neg A$ on pätevä.
- **Määritelmä.** Lause α on *toteutuva*, jos $\mathcal{V}(\alpha) = T$ jollekin valuaatiolle $\mathcal{V}$.

  Esim. $A \to B$ on toteutuva ja $P \wedge \neg P$ on toteutumaton.

Esimerkkejä

Onko $A \vee \neg A$ pätevä?

A	$\neg A$	$A \vee \neg A$
T	F	T
F	T	T

Onko $A \to A \vee B$ pätevä?

A	B	$A \vee B$	$A \to A \vee B$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Onko $A \vee \neg A$ toteutuva?

Onko $A \to A \vee B$ toteutuva?

Lisää peruskäsitteitä

- **Määritelmä.** Lauseet α ja β ovat *loogisesti ekvivalentteja*, jos $\mathcal{V}(\alpha) = \mathcal{V}(\beta)$ kaikille valuaatioille $\mathcal{V}$ (eli jos ja vain jos $\models \alpha \leftrightarrow \beta$).

  Esim. A and $\neg\neg A$ ovat loogisesti ekvivalentit.
- **Määritelmä.** Valuaatio $\mathcal{V}$ on (mahd. äärettömän) lausejoukon Σ *malli*, jos $\mathcal{V}(\sigma) = T$ kaikille lausejoukon Σ lauseille $\sigma \in \Sigma$.
- **Määritelmä.** Olkoon Σ (mahdollisesti ääretön) joukko lauseita. Lause α on Σ:n looginen seuraus (merkitään $\Sigma \models \alpha$), jos $\mathcal{V}(\alpha) = T$ kaikille lausejoukon Σ malleille $\mathcal{V}$.

  Esim. $\neg\neg A$ seuraa loogisesti lausejoukosta $\{A\}$.

Huomaa seuraavat yhteydet: $\models \phi_1 \wedge \ldots \wedge \phi_n \rightarrow \phi \iff \{\phi_1 \ldots \phi_n\} \models \phi$, jonka erikoistapauksena saadaan $\models \alpha \iff \emptyset \models \alpha$.

Esimerkkejä

Onko $A \vee \neg B$ pätevä?

A	B	$\neg B$	$(A \vee \neg B)$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

Onko $A \vee \neg B$ toteutuva?

Ovatko lauseet $A \rightarrow B$ ja $\neg B \rightarrow \neg A$ loogisesti ekvivalentit?

$\neg A$	$\neg B$	$A \rightarrow B$	$\neg B \rightarrow \neg A$
F	F	T	T
F	T	F	F
T	F	T	T
T	T	T	T

Seuraako $\neg B \rightarrow \neg A$ loogisesti lausejoukosta $\{A \rightarrow B\}$?

Seuraako lause D loogisesti lausejoukosta $\{A, (A \rightarrow D)\}$?

A	D	$(A \rightarrow D)$
T	T	T
T	F	F
F	T	T
F	F	T

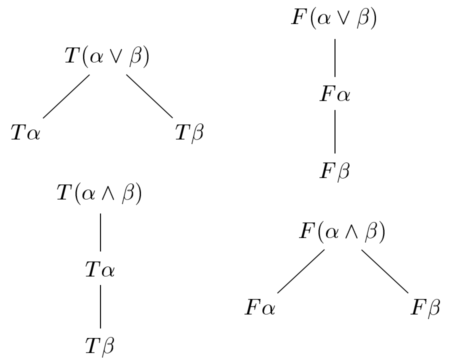
Seuraako lause B loogisesti lausejoukosta $\{(A \rightarrow B)\}$?

A	B	$(A \rightarrow B)$
T	T	T
T	F	F
F	T	T
F	F	T

Huomaa, että $\Sigma \models A \vee \neg A$ kaikille lausejoukoille Σ !!!

3 Semanttinen taulu

Atomiset taulut



$$\begin{array}{c} F(\alpha \to \beta) \\ | \\ T\alpha \\ | \\ F\beta \end{array} \qquad \begin{array}{ccc} & T(\alpha \to \beta) & \\ \swarrow & & \searrow \\ F\alpha & & T\beta \end{array} \qquad \begin{array}{c} T\neg\alpha \\ | \\ F\alpha \end{array} \qquad \begin{array}{c} F\neg\alpha \\ | \\ T\alpha \end{array}$$

$$\begin{array}{ccc} & T(\alpha \leftrightarrow \beta) & \\ \swarrow & & \searrow \\ T\alpha & & F\alpha \\ | & & | \\ T\beta & & F\beta \end{array} \qquad \begin{array}{ccc} & F(\alpha \leftrightarrow \beta) & \\ \swarrow & & \searrow \\ T\alpha & & F\alpha \\ | & & | \\ F\beta & & T\beta \end{array}$$

Atomisen taulun instantiointi

Lause γ: $(\neg A \to C \vee D) \to A \vee B$

$$\begin{array}{ccc} & T(\alpha \to \beta) & \\ \swarrow & & \searrow \\ F\alpha & & T\beta \end{array}$$

γ on implikaatio $\alpha \to \beta$, missä $\alpha = \neg A \to C \vee D$ ja $\beta = A \vee B$

$$\begin{array}{ccc} & T((\neg A \to C \vee D) \to A \vee B) & \\ \swarrow & & \searrow \\ F(\neg A \to C \vee D) & & T(A \vee B) \end{array}$$

Äärellinen taulu

Määritelmä. *Äärellinen taulu* on binääripuu, jonka solmuina on T:llä ja F:llä merkittyjä lauseita (puun alkioita), ja joka on seuraavien ehtojen mukainen.

- Jokainen atominen taulu on äärellinen taulu.
- Jos τ on äärellinen taulu, P on polku τ:ssa, E on τ:n alkio polussa P, ja τ' on saatu τ:sta liittämällä E:n atominen taulu τ:hun polun P jatkoksi, niin τ' on myöskin äärellinen taulu.

Sopimus taulujen koon pienentämiseksi: kun atominen taulu liitetään polun jatkoksi, sen juurta ei kirjoiteta näkyviin.

(Kirjassa määritellään myös *äärettömät taulut*, joita emme lauselogiikan kohdalla tarvitse.)

Esimerkki.

$$\begin{array}{ccccccc} & & & F((A \vee B) \to (A \wedge B)) & & & \\ & & & | & & & \\ & & & T(A \vee B)^{1.} & & & \\ & & & | & & & \\ & & & F(A \wedge B)^{1.} & & & \\ & & \swarrow & & \searrow & & \\ & TA^{2.} & & & & TB^{2.} & \\ \swarrow & & \searrow & & \swarrow & & \searrow \\ FA^{3.} & & FB^{3.} & & FA^{3.} & & FB^{3.} \\ \times & & & & & & \times \end{array}$$

Määritelmä. Olkoon τ taulu, P polku τ:ssa ja E polun P alkio.

1. E on *hajoitettu*, jos E:n atomisen taulun jonkun polun jokainen alkio on P:n alkio.
2. P on *ristiriitainen*, jos siinä esiintyy sekä $T\alpha$ että $F\alpha$ jollekin lauseelle α (tämän merkiksi kirjoitetaan usein $\times$ polun päähän).
3. P on *valmis*, jos se on ristiriitainen tai jokainen sen alkioista on hajoitettu.
4. τ on *valmis*, jos jokainen sen poluista on valmis.
5. τ on *ristiriitainen*, jos jokainen sen poluista on ristiriitainen.

Määritelmä. Taulu τ on lauseen α *todistus*, jos τ on ristiriitainen ja sen juuressa on $F\alpha$. Jos α:lla on todistus, on α *teoreema* ($\vdash \alpha$).

Esimerkki.
Todistetaan lause
$(A \wedge B) \to (A \vee B)$
päteväksi.

$$
\begin{array}{c}
F((A \wedge B) \to (A \vee B)) \\
| \\
T(A \wedge B)\ ^{1.} \\
| \\
F(A \vee B)\ ^{1.} \\
| \\
TA\ ^{2.} \\
| \\
TB\ ^{2.} \\
| \\
FA\ ^{3.} \\
| \\
FB\ ^{3.} \\
\times
\end{array}
$$

Jokaiseen solmuun on merkitty, monennestako solmusta ko. **polulla** solmu on saatu $\Rightarrow$ todistuksen luettavuus paranee.

$\times$ = "polku on ristiriitainen"

4 Taulumenetelmän ominaisuuksia

Väite. Todistusmenetelmän virheettömyys: Jos lause α on todistettavissa semanttisella taululla ($\vdash \alpha$), niin α on pätevä ($\models \alpha$).

Väite. Todistusmenetelmän täydellisyys: Jos α on pätevä ($\models \alpha$), niin α on todistettavissa semanttisella taululla ($\vdash \alpha$).

Kirjassa osoitetaan, että:

- Jos lause α ei ole pätevä, niin jokaisessa lauseen α semanttisessa taulussa on ei-ristiriitainen polku.
- Jos lauseen α semanttisessa taulussa on ei-ristiriitainen polku, niin lause α ei ole pätevä.

Jos jollekin valuaatiolle $\mathcal{V}(\alpha) = F$, **niin** $F\alpha$:n taulussa on ei-ristiriitainen polku, jonka jokaiselle alkiolle $T\beta$, $\mathcal{V}(\beta) = T$ ja alkiolle $F\beta$, $\mathcal{V}(\beta) = F$ (todistus induktiolla).

$$
\begin{array}{ccc}
 & F((A \vee B) \to A) & \\
 & | & \\
 & T(A \vee B) & \\
 & | & \\
 & FA & \\
 & | & \\
 & T(A \vee B) & \\
 \swarrow & & \searrow \\
TA & & TB
\end{array}
$$

Esimerkissä $\mathcal{V}((A \vee B) \to A) = F$, $\mathcal{V}(A) = F$ ja $\mathcal{V}(B) = T$.

Jos $F\alpha$:n taulussa on ei-ristiriitainen polku,
niin jollekin valuaatiolle $\mathcal{V}(\alpha) = F$.

Olkoon P mikä tahansa $F\alpha$:n ei-ristiriitainen polku.

Olkoon valuaatio $\mathcal{V}$ seuraavanlainen.

- $\mathcal{V}(A) = T$, jos TA on polussa P (A on atominen lause) ja
- $\mathcal{V}(A) = F$, muutoin.

Todistetaan induktiolla P:n alkioiden rakenteen suhteen, että $\mathcal{V}(\beta) = T$ kaikille $T\beta \in P$, ja $\mathcal{V}(\beta) = F$ kaikille $F\beta \in P$.

Perustapaus: TA tai FB, missä A, B ovat atomisia lauseita.
Valuaation $\mathcal{V}$ määritelmän perusteella $\mathcal{V}(A) = T$ ja $\mathcal{V}(B) = F$.

Induktioaskel: Tutkitaan kaikki tapaukset
$T(\alpha \wedge \beta), F(\alpha \wedge \beta), T(\alpha \vee \beta), F(\alpha \vee \beta), T(\alpha \to \beta), F(\alpha \to \beta), \ldots$.

- $F(\alpha \to \beta) \in P$, jolloin $T\alpha \in P$ ja $F\beta \in P$:
  Induktio-oletuksella $\mathcal{V}(\alpha) = T, \mathcal{V}(\beta) = F$.
  Totuustaulukkojen perusteella tällöin $\mathcal{V}(\alpha \to \beta) = F$.
- $T(\alpha \to \beta) \in P$, jolloin $F\alpha \in P$ tai $T\beta \in P$:
  Induktio-oletuksella $\mathcal{V}(\alpha) = F$ jos $F\alpha \in P$, tai $\mathcal{V}(\beta) = T$ jos $T\beta \in P$.
  Totuustaulukkojen perusteella tällöin $\mathcal{V}(\alpha \to \beta) = T$.
- muut kohdat samalla tavalla

Lauseen toteutuvuuden tutkiminen

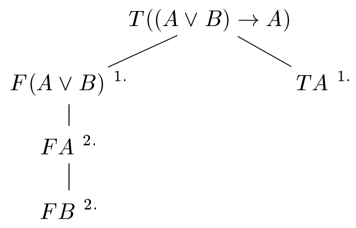
Määritelmä. Lause α on *toteutuva*, jos ja vain jos on olemassa valuaatio $\mathcal{V}$ siten, että $\mathcal{V}(\alpha) = T$.

- Lause α on toteutuva, jos ja vain jos $T\alpha$:n semanttisessa taulussa on ainakin yksi ei-ristiriitainen polku ja
- lause α on toteutuva, jos ja vain jos $\neg\alpha$ **ei ole** pätevä.

Määritelmä. (Äärellinen) lausejoukko Σ on *toteutuva*, jos ja vain jos on olemassa valuaatio $\mathcal{V}$ siten, että $\mathcal{V}(\alpha) = T$ kaikille $\alpha \in \Sigma$.

- Äärellinen lausejoukko $\Sigma = \{\alpha_1, \ldots, \alpha_n\}$ on toteutuva, jos ja vain jos $T\alpha_1 - \cdots - T\alpha_n$:n semanttisessa taulussa on ainakin yksi ristiriitainen polku.

Esimerkki. Tutkitaan lauseen $(A \vee B) \to A$ toteutuvuutta.



Ei-ristiriitaisista poluista voidaan muodostaa valuaatioita $\mathcal{V}$, joissa lause on tosi. Esim. valuaatiolle, jolle $\mathcal{V}(A) = F$ ja $\mathcal{V}(B) = F$ (vasen polku), pätee $\mathcal{V}((A \vee B) \to A) = T$. Tutkittava lause $(A \vee B) \to A$ on siis toteutuva (ts. ko. lauseella on malli).

Johdettavuus lausejoukosta

Tutkitaan lauseen β *johdettavuutta* äärellisestä lausejoukosta $\Sigma = \{\alpha_1, \ldots, \alpha_n\}$ (johdettavuutta merkitään $\Sigma \vdash \beta$).

Rakennetaan valmis semanttinen taulu edellisellä luennolla opittuun tapaan lähtien seuraavasta taulusta.

	$\Sigma \models \beta$
joss	$\Sigma \cup \{\neg\beta\}$
	ei ole toteutuva
joss	$\Sigma \vdash \beta$

$$\begin{array}{c} T\alpha_1 \\ | \\ \vdots \\ | \\ T\alpha_n \\ | \\ F\beta \\ \vdots \end{array}$$

Boolen funktioiden ja lauselogiikan yhteys

Huomaa, että mikä tahansa Boolen funktio $f : \{0,1\}^n \to \{0,1\}$ voidaan aina esittää lauselogiikan lauseena.

- Arvoja 0 ja 1 vastaavat totuusarvot F ja T
- Boolen muuttuja a (jolla arvona 0 tai 1) esitetään atomisena lauseena A (jolla totuusarvo F tai T)
- Komplementti esitetään negaation $\neg$ avulla
- Tulo $\cdot$ esitetään konjunktion $\wedge$ avulla
- Summa $+$ esitetään disjunktion $\vee$ avulla

Esimerkki. Esim. funktiolle $f(a,b,c) = a \cdot \overline{b} + c$ saadaan näillä periaatteilla esitys $(A \wedge \neg B) \vee C$.

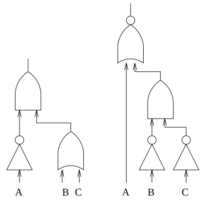
Väite. Olkoon f boolen funktio ja lause ϕ sitä vastaava esitys:

funktion f arvon laskeminen tietyillä muuttujien arvoilla vastaa lauseen ϕ totuusarvon laskentaa vastaavassa valuaatiossa.

Esimerkki. Jos $a = 0$, $b = 0$ ja $c = 1$, niin vastaava valuaatio $\mathcal{V}$ antaa totuusarvot $\mathcal{V}(A) = F$, $\mathcal{V}(B) = F$ ja $\mathcal{V}(C) = T$.

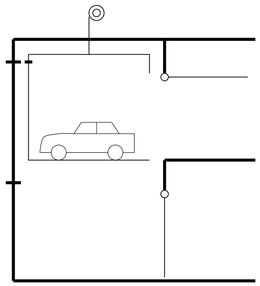
Aikaisemmalle esimerkille $f(0,0,1) = 0 \cdot \overline{0} + 1 = 0 \cdot 1 + 1 = 0 + 1 = 1$ ja vastaavasti $\mathcal{V}((A \wedge \neg B) \vee C) = T$.

Esimerkki. Jos haluamme osoittaa, että kaksi Boolen funktiota f ja f' ovat samat, riittää, että toteamme lause-esitysten ϕ ja ϕ' loogisen ekvivalenssin ($\models \phi \leftrightarrow \phi'$).



Konkreettisempi esimerkki

Mallinnetaan yksinkertaistettua hissijärjestelmää lauselogiikalla:



Atomiset lauseet:

A_i: kerroksen i ovi on auki
K_i: hissi on kerroksessa i

missä $i = 1$ tai $i = 2$

Kuvataan lauselogiikalla järjestelmän sallitut tilat (eli haetaan lausejoukko Σ, jonka *mallit* vastaavat sallittuja tiloja).

- Tyhjällä lausejoukolla $\emptyset$ on ei-toivottu malli $\mathcal{V}$:
  $\mathcal{V}(K_1) = T$, $\mathcal{V}(K_2) = T$, $\mathcal{V}(A_1) = T$ ja $\mathcal{V}(A_2) = T$.
  Tämä vastaa järjestelmän tilaa, jossa hissi on yhtäaikaa molemmissa kerroksissa ja molemmat ovet olisivat auki (mahdoton) $\Rightarrow$ Tarvitaan lisää lauseita (rajoitteita).
- Fyysisen maailman asettama rajoitus: $\neg K_1 \vee \neg K_2$
  (huomaa, että $\mathcal{V}$ ei ole tämän lauseen malli)
- Emme kuitenkaan halua asettaa vaatimusta $K_1 \vee K_2$
  (hissi voi olla matkalla kerrosten välillä).
- Oville asetettavat turvallisuusvaatimukset: $A_1 \to K_1$, $A_2 \to K_2$.

$\Rightarrow$ Järjestelmälle saadaan spesifikaatio

$$\Sigma = \{\neg K_1 \vee \neg K_2, A_1 \to K_1, A_2 \to K_2\}.$$

- Spesifikaatiolla on olennaisesti seuraavat mallit:

	K_1	A_1	K_2	A_2
$\mathcal{V}_1$	F	F	F	F
$\mathcal{V}_2$	T	F	F	F
$\mathcal{V}_3$	T	T	F	F
$\mathcal{V}_4$	F	F	T	F
$\mathcal{V}_5$	F	F	T	T

- Voimme myös osoittaa, että hissin molemmat ovet eivät voi olla yhtäaikaisesti auki (turvallisuusominaisuus):

$$\Sigma \models \neg(A_1 \wedge A_2).$$

Kokeile tämän todistamista semanttisella taululla.

5 Hilbert-tyyppinen lauselogiikan aksiomatisointi

Aksioomat:

1. $\alpha \to (\beta \to \alpha)$
2. $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$
3. $(\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta)$

Päättelysääntö:

$$\frac{\alpha \to \beta \quad \alpha}{\beta}$$

(modus ponens)

Määritelmä. Olkoon Σ joukko lauseita.

Todistus Σ:sta on jono lauseita $\alpha_1, \ldots, \alpha_n$ siten että kaikille $i \in \{1, \ldots, n\}$

- $\alpha_i \in \Sigma$,
- α_i on aksiooma tai
- α_i on saatu modus ponensilla lauseista $\alpha_j, j < i$ ja $\alpha_k = (\alpha_j \to \alpha_i), k < i$.

Lause α on *johdettavissa* Σ:sta, jos on olemassa todistus $\alpha_1, \ldots, \alpha_n$ Σ:sta ja $\alpha = \alpha_n$. ($\Sigma \vdash_{\mathrm{H}} \alpha$)

Lause α on *teoreema* (todistuva) jos se on johdettavissa tyhjästä lausejoukosta $\Sigma = \emptyset$. ($\vdash_{\mathrm{H}} \alpha$)

Esimerkki. Osoitetaan $\{A, B \to (A \to C)\} \vdash_{\mathrm{H}} B \to C$.

1.	A	olettamus
2.	$B \to (A \to C)$	olettamus
3.	$A \to (B \to A)$	aksiooma 1
4.	$B \to A$	MP, 1, 3
5.	$(B \to (A \to C)) \to ((B \to A) \to (B \to C))$	aksiooma 2
6.	$(B \to A) \to (B \to C)$	MP, 2, 5
7.	$B \to C$	MP, 4, 6

6 Normaalimuodot

- Polynomien esittäminen muodossa:

$$c_0 \cdot x^0 + c_1 \cdot x^1 + \cdots + c_n \cdot x^n$$

- Lineaaristen yhtälöryhmien esittäminen matriiseina:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

- Normaalimuotojen tarkoituksena on siis saattaa tutkittava asia sellaiseen yksinkertaiseen säännölliseen muotoon, jossa sen käsittely saadaan yksinkertaisemmaksi.

Määritelmä. Jos A on atominen lause, niin A ja $\neg A$ ovat *literaaleja.*

Määritelmä. Lause α on *konjunktiivisessa normaalimuodossa* jos α on muotoa $\beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_n$, ja kukin β_i on disjunktio $l_1 \vee l_2 \vee \cdots \vee l_{m_i}$, missä $l_1, l_2, \ldots, l_{m_i}$ ovat literaaleja.

Esimerkki.

$$(A_1 \vee \neg A_2) \wedge (\neg A_1 \vee \neg A_3) \wedge (A_5 \vee A_6 \vee A_7)$$
$$A_1 \wedge \neg A_2 \wedge A_3$$
$$(A_1 \vee \neg A_1) \wedge A_2$$
$$\neg A_7$$
$$A_1 \vee A_2 \vee A_3$$

Määritelmä. Lause α on *disjunktiivisessa normaalimuodossa* jos α on muotoa $\beta_1 \vee \beta_2 \vee \cdots \vee \beta_n$, ja kukin β_i on konjunktio $l_1 \wedge l_2 \wedge \cdots \wedge l_{m_i}$, missä $l_1, l_2, \ldots, l_{m_i}$ ovat literaaleja.

Esimerkki.

$$(\neg A_1 \wedge \neg A_2) \vee (A_3 \wedge A_1) \vee (A_1 \wedge \neg A_2 \wedge A_3)$$
$$A_1 \vee \neg A_2 \vee A_3$$
$$(A_1 \wedge \neg A_1) \vee A_2$$
$$\neg A_7$$
$$A_1 \wedge A_2 \wedge A_3$$

Väite. Jokaiselle lauselogiikan lauseelle α on olemassa konjunktiivisessa (disjunktiivisessa) normaalimuodossa oleva lause β, joka on loogisesti ekvivalentti α:n kanssa.

Määritelmä. Sanotaan, että em. β on α:n konjunktiivinen (disjunktiivinen) normaalimuoto.

Esimerkki. $A \vee (\neg B \wedge C)$ on loogisesti ekvivalentti konjunktiivisessa normaalimuodossa olevan lauseen $(A \vee \neg B) \wedge (A \vee C)$ kanssa.

A	B	C	$\neg B$	$\neg B \wedge C$	$A \vee \neg B$	$A \vee C$	$A \vee (\neg B \wedge C)$	$(A \vee \neg B) \wedge (A \vee C)$
F	F	F	T	F	T	F	F	F
F	F	T	T	T	T	T	T	T
F	T	F	F	F	F	F	F	F
F	T	T	F	F	F	T	F	F
T	F	F	T	F	T	T	T	T
T	F	T	T	T	T	T	T	T
T	T	F	F	F	T	T	T	T
T	T	T	F	F	T	T	T	T

Mikä hyvänsä lauselogiikan lause voidaan muuttaa konjunktiiviseen (disjunktiiviseen) normaalimuotoon seuraavalla menettelyllä.

1. Poista konnektiivit $\leftrightarrow$ seuraavanlaisilla korvauksilla:

$$\alpha \leftrightarrow \beta \quad \Rightarrow \quad (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \qquad (1)$$
$$\alpha \leftrightarrow \beta \quad \Rightarrow \quad (\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha) \qquad (1')$$

2. Poista konnektiivit $\rightarrow$ seuraavanlaisilla korvauksilla:

$$\alpha \rightarrow \beta \quad \Rightarrow \quad \neg\alpha \vee \beta \qquad (2)$$

3. Siirrä negaatiot välittömästi atomisten lauseiden eteen:

$$\neg\neg\alpha \quad \Rightarrow \quad \alpha \qquad (3)$$
$$\neg(\alpha \vee \beta) \quad \Rightarrow \quad \neg\alpha \wedge \neg\beta \qquad (4)$$
$$\neg(\alpha \wedge \beta) \quad \Rightarrow \quad \neg\alpha \vee \neg\beta \qquad (5)$$

4. (CNF) Lopuksi siirrä $\wedge$-konnektiivit $\vee$-konnektiivien ulkopuolelle:

$$\alpha \vee (\beta \wedge \gamma) \quad \Rightarrow \quad (\alpha \vee \beta) \wedge (\alpha \vee \gamma) \qquad (6)$$
$$(\alpha \wedge \beta) \vee \gamma \quad \Rightarrow \quad (\alpha \vee \gamma) \wedge (\beta \vee \gamma) \qquad (7)$$

Tai (DNF) siirrä $\vee$-konnektiivit $\wedge$-konnektiivien ulkopuolelle:

$$\alpha \wedge (\beta \vee \gamma) \quad \Rightarrow \quad (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \qquad (8)$$
$$(\alpha \vee \beta) \wedge \gamma \quad \Rightarrow \quad (\alpha \wedge \gamma) \vee (\beta \wedge \gamma) \qquad (9)$$

Normaalimuodon voi hakea myös taulumenetelmällä (selvittää lauseen mallit ja muodostaa disjunktiivisen normaalimuodon).

Lauseelle α saadaan konjunktiivinen normaalimuoto lauseen $\neg\alpha$ disjunktiivisesta normaalimuodosta sääntöjen (3)-(5) avulla.

Esimerkki. Muutetaan lause $(A \vee B) \rightarrow (B \leftrightarrow C)$ konjunktiiviseen normaalimuotoon.

$$(A \vee B) \rightarrow (B \leftrightarrow C)$$
$$(A \vee B) \rightarrow ((B \rightarrow C) \wedge (C \rightarrow B)) \qquad (1)$$
$$\neg(A \vee B) \vee ((\neg B \vee C) \wedge (\neg C \vee B)) \qquad (2)$$
$$(\neg A \wedge \neg B) \vee ((\neg B \vee C) \wedge (\neg C \vee B)) \qquad (4)$$

$$(\neg A \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \qquad (7)$$
$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \qquad (6)$$
$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge ((\neg B \vee (\neg B \vee C)) \wedge (\neg B \vee (\neg C \vee B))) \qquad (6)$$
$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee \neg C \vee B) \wedge (\neg B \vee \neg B \vee C) \wedge (\neg B \vee \neg C \vee B)$$

Tutkimme aikaisemmin lauseen $(A \vee B) \rightarrow A$ toteutuvuutta ja pätevyyttä, joten käytössämme on sekä $T\alpha$:n että $T\neg\alpha$:n taulut ($T\neg\alpha$:n taulu saadaan liittämällä $T\neg\alpha$:n jatkoksi $F\alpha$:n taulu).

- $T\alpha$:n ristiriidattomat polut antavat vaatimukset FA, FB (vasen polku) ja TA (oikea polku). Näistä saadaan α:lle DNF $(\neg A \wedge \neg B) \vee A$.
- $T\neg\alpha$:n ainoa ristiriidaton polku antaa vaatimukset FA, TB. Tästä saadaan $\neg\alpha$:lle DNF $(\neg A \wedge B)$ ja α:lle CNF $(A \vee \neg B)$.

Kokeile näiden normaalimuotojen johtamista myös muunnossäännöillä !!!

7 Lauseiden klausuulimuoto

- Atomiset lauseet A ja niiden negaatiot $\neg A$ ovat *literaaleja.*
- Literaalin komplementti: $\overline{A} = \neg A$, $\overline{\neg A} = A$.
- Literaalien $l_1, \ldots, l_n$ disjunktio $l_1 \vee \cdots \vee l_n$ on *klausuuli.* Klausuulit kirjoitetaan usein muodossa $\{l_1, \ldots, l_n\}$.
- *Tyhjä klausuuli* $\Box$ on aina epätosi.
- Joukko klausuuleita S on tosi, jos kaikki sen alkiot ovat tosia. Tyhjä klausuulijoukko $\emptyset$ on aina tosi.

Klausuulijoukko $\{\{A, \neg B\}, \{\neg C, \neg A, D\}\}$ vastaa lausetta $(A \vee \neg B) \wedge (\neg C \vee \neg A \vee D)$.

- *Totuusjakelu* $\mathcal{A}$ on joukko literaaleja siten, ettei millekään atomiselle lauseelle B sekä $B \in \mathcal{A}$ että $\neg B \in \mathcal{A}$ (*konsistenssi*).
- Totuusjakelu $\mathcal{A}$ on *täydellinen*, jos jokaiselle atomiselle lauseelle B joko $B \in \mathcal{A}$ tai $\neg B \in \mathcal{A}$.

  Täydellinen totuusjakelu vastaa valuaatiota $\mathcal{V}$, jolle $\mathcal{V}(B) = T$, kun $B \in \mathcal{A}$, ja $\mathcal{V}(B) = F$, kun $\neg B \in \mathcal{A}$.
- $\mathcal{A}$ *toteuttaa* klausuulijoukon S (merkitään $\mathcal{A} \models S$), joss kaikille klausuuleille $C \in S$ pätee $C \cap \mathcal{A} \neq \emptyset$.

  Vastaavasti: valuaatio $\mathcal{V}$ toteuttaa lauseen α joss $\mathcal{V}(\alpha) = T$.
- Klausuulijoukko S on *toteutuva* jos on totuusjakelu $\mathcal{A}$ siten että $\mathcal{A} \models S$. Muuten S on *toteutumaton.*

Esimerkkejä

Olkoon $\mathcal{A} = \{A, \neg B\}$.

Nyt

$$\begin{aligned} \mathcal{A} &\models \{\{A, C, E\}, \{\neg A, \neg B\}\} \\ \mathcal{A} &\models \emptyset \\ \mathcal{A} &\not\models \{\{A, B\}, \{C\}\} \end{aligned}$$

Klausuulijoukot $\{\{A, C, E\}, \{\neg A, \neg B\}\}$ ja $\emptyset$ ovat toteutuvia.

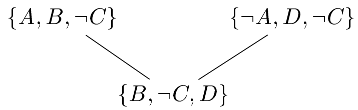
Mutta $\{\{A\}, \{\neg A\}\}$ ja $\{\Box\}$ eivät ole toteutuvia.

8 Resoluutiosääntö

Olkoot $C_1 = \{l, l_1, \ldots, l_n\}$ ja $C_2 = \{\bar{l}, l'_1, \ldots, l'_m\}$ klausuuleja.

Klausuuli $C = \{l_1, \ldots, l_n, l'_1, \ldots, l'_m\}$ on C_1:n ja C_2:n *resolventti.*

Esimerkki



Sääntöä on sovellettu literaaleihin A ja $\neg A$. Klausuulit ovat joukkoja, joten $\neg C$ esiintyy resolventissa $\{B, \neg C, D\}$ vain kerran.

Resoluutiotodistukset

Klausuulin C *johto* klausuulijoukosta S on äärellinen jono klausuuleja $C_1, \ldots, C_n$, missä $C_n = C$ ja jokaiselle C_i joko $C_i \in S$ tai C_i on joidenkin aikaisempien klausuulien resolventti.

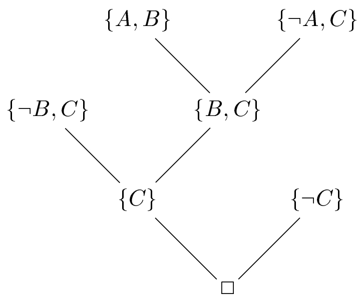
Jos klausuulijoukosta S voidaan johtaa tyhjä klausuuli $\Box$, kyseistä johtoa kutsutaan S:n *refutaatioksi* (hylkäykseksi).

Esimerkkejä

$S = \{\{A, B\}, \{\neg A, C\}, \{\neg B, C\}, \{\neg C\}\}$

1.	$\{A, B\}$	S
2.	$\{\neg A, C\}$	S
3.	$\{\neg B, C\}$	S
4.	$\{\neg C\}$	S
5.	$\{B, C\}$	1, 2
6.	$\{C\}$	3, 5
7.	$\Box$	4, 6

Resoluutiotodistuksen puuesitys



$S = \{\{A, B\}, \{\neg A, B\}, \{A, \neg B\}, \{\neg A, \neg B\}\}$

1.	$\{A, B\}$	S
2.	$\{\neg A, B\}$	S
3.	$\{A, \neg B\}$	S
4.	$\{\neg A, \neg B\}$	S
5.	$\{B\}$	1, 2
6.	$\{\neg B\}$	3, 4
7.	$\square$	5, 6

Pätevyyden tutkiminen resoluutiolla

Väite. Lause α on pätevä joss $\neg\alpha$ on toteutumaton.

($\mathcal{V}(\neg\alpha) = F$ eli $\mathcal{V}(\alpha) = T$ kaikille valuaatioille $\mathcal{V}$).

Menettely: $\neg\alpha$ $\Rightarrow$ konjunktiiviseen normaalimuotoon
$\Rightarrow$ klausuulijoukoksi S
$\Rightarrow$ suoritetaan S:n refutaatio
$\Rightarrow$ S toteutumaton
$\Rightarrow$ $\neg\alpha$ toteutumaton
$\Rightarrow$ α pätevä

Onko $(A \to B) \wedge (\neg A \to C) \to (B \vee C)$ pätevä?

Negaation CNF on $(\neg A \vee B) \wedge (A \vee C) \wedge \neg B \wedge \neg C$.

Klausuulijoukkona $\{\{\neg A, B\}, \{A, C\}, \{\neg B\}, \{\neg C\}\}$.

1.	$\{\neg A, B\}$	S	
2.	$\{A, C\}$	S	
3.	$\{\neg B\}$	S	
4.	$\{\neg C\}$	S	Lause on siis pätevä.
5.	$\{B, C\}$	1, 2	
6.	$\{C\}$	3, 5	
7.	$\square$	4, 6	

Loogisen seuraavuuden tutkiminen resoluutiolla

Väite. Lause α on lausejoukon Σ looginen seuraus, joss lausejoukko $\Sigma \cup \{\neg\alpha\}$ on toteutumaton.

Menettely: $\Sigma \cup \{\neg\alpha\}$ $\Rightarrow$ konjunktiiviseen normaalimuotoon
$\Rightarrow$ klausuulijoukoksi S
$\Rightarrow$ suoritetaan S:n refutaatio
$\Rightarrow$ S toteutumaton
$\Rightarrow$ $\Sigma \cup \{\neg\alpha\}$ toteutumaton
$\Rightarrow$ α on Σ:n looginen seuraus

Onko A lausejoukon $\{\neg A \to B, B \lor C \to \neg B\}$ looginen seuraus?

lause	CNF	klausuuleina
$\neg A$	$\neg A$	$\{\neg A\}$
$\neg A \to B$	$A \lor B$	$\{A, B\}$
$B \lor C \to \neg B$	$(\neg B \lor \neg C) \land (\neg B \lor \neg B)$	$\{\neg B, \neg C\}, \{\neg B\}$

1.	$\{\neg A\}$	S
2.	$\{A, B\}$	S
3.	$\{\neg B, \neg C\}$	S
4.	$\{\neg B\}$	S
5.	$\{B\}$	1, 2
6.	$\square$	4, 5

Saadaan klausuulijoukko $S = \{\{\neg A\}, \{A, B\}, \{\neg B, \neg C\}, \{\neg B\}\}$

Vastaus: lause A on lausejoukon looginen seuraus.

9 Resoluution ominaisuuksia

Resoluution virheettömyys ja täydellisyys

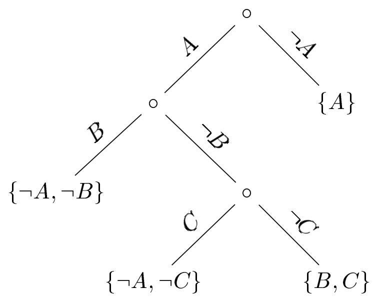
Väite. Jos S:llä on refutaatio, on S toteutumaton.

Todistus: Suoraan sillä perusteella, että jos on totuusjakelu $\mathcal{A}$ s.e. $\mathcal{A} \models C_1$ ja $\mathcal{A} \models C_2$, niin myös $\mathcal{A} \models C$ niiden resolventille C.

Väite. Jos S on toteutumaton, on S:llä refutaatio.

Todistuksen idea on annettu seuraavassa esimerkissä. Refutaatio voidaan hakea suorittamalla tapausanalyysi klausuulijoukossa esiintyvien atomisten lauseiden suhteen.

$S = \{\{A\}, \{B, C\}, \{\neg A, \neg B\}, \{\neg A, \neg C\}\}$



Lehtisolmuihin merkityt klausuulit ovat epätosia ko. totuusjakelussa.

Lineaarinen resoluutio

Lineaarisessa resoluutiossa rajoitetaan johdot klausuulijoukosta S seuraavanlaisiksi lineaarisiksi sekvensseiksi:

$$\begin{tikzcd}
B_0 \arrow[dr] & B_1 \arrow[dr] & B_2 \arrow[dr] & & \dots\ B_n \arrow[dr] & \\
C_0 \arrow[r] & C_1 \arrow[r] & C_2 \arrow[r] & C_3\ \dots & C_n \arrow[r] & \square
\end{tikzcd}$$

- $C_0 \in S$ ja jokainen $B_i \in S$ tai $B_i = C_j$ jollekin $0 \leq j < i$.
- Jokainen C_{i+1} on klausuuleiden C_i ja B_i resolventti.

Lineaarisuusvaatimus ei vaikuta resoluution virheettömyys- ja täydellisyysominaisuuksiin.

Klausuulijoukko: $\{\{\neg A, B\}, \{A, C\}, \{\neg B\}, \{\neg C\}\}$

$$\begin{tikzcd}
\{\neg A, B\} \arrow[d] & \{A, C\} \arrow[dl] \\
\{B, C\} \arrow[d] & \{\neg B\} \arrow[dl] \\
\{C\} \arrow[d] & \{\neg C\} \arrow[dl] \\
\Box &
\end{tikzcd}$$

Hissiesimerkki resoluutiolla

lause	CNF	klausuuleina	
$\neg K_1 \vee \neg K_2$	$\neg K_1 \vee \neg K_2$	1. $\{\neg K_1, \neg K_2\}$	
$A_1 \to K_1$	$\neg A_1 \vee K_1$	2. $\{\neg A_1, K_1\}$	
$A_2 \to K_2$	$\neg A_2 \vee K_2$	3. $\{\neg A_2, K_2\}$	
$\neg\neg(A_1 \wedge A_2)$	$A_1 \wedge A_2$	4. $\{A_1\}$, 5. $\{A_2\}$	
	Resoluutio:	6. $\{K_1\}$	2,4
		7. $\{K_2\}$	3,5
		8. $\{\neg K_2\}$	1,6
		9. $\Box$	7,8

10 Laskennallisesta vaativuudesta

Oletamme jatkossa, että laskennan mallina ovat *Turing-koneet*.

Turing-kone *hyväksyy* merkkijonojen joukon O, jos Turing-kone pysähtyy syötteellä i hyväksyvään tilaan jos ja vain jos $i \in O$.

Esitämme ongelmat merkkijonoina ja käytämme Turing-koneita näiden merkkijonojen hyväksymiseen (ts. ongelman ratkaisemiseen).

Kaksi keskeistä ongelmien luokkka ovat

- **P**: ongelmat, jotka voidaan ratkaista polynomisessa ajassa *deterministisellä* Turing-koneella.
- **NP**: ongelmat, jotka voidaan ratkaista polynomisessa ajassa *epädeterministisellä* Turing-konella.

Luokka **P** on luokan **NP** aliluokka (ja mitä ilmeisimmin aito).

Esimerkki. Lauselogiikan toteututuvuusongelmassa on tarkoituksena selvittää onko annetulla lauseella $\phi \in \mathcal{L}$ malli.

Ongelma SAT on siis toteutuvia lauseiden ϕ joukko (lauseet merkkijonoesityksinä).

Väite. SAT kuuluu luokkaan **NP**.

Todistuksen idea: voidaan konstruoida epädeterministinen Turing-kone M, joka valitsee epädeterministisesti valuaation $\mathcal{V}$ ja tarkistaa, että $\mathcal{V}(\phi) = T$.

Tarvittava laskenta pystytään suorittamaan polynomisessa ajassa lauseen ϕ pituuden suhteen.

Määritelmä. Ongelma O on **C**-kova, jos kaikki luokan **C** ongelmat voidaan redusoida O:ksi polynomisessa ajassa.

Ongelman O_1 *redusoituvuus* ongelmaksi O_2 edellyttää, että löytyy i:n pituuden suhteen polynomisessa ajassa laskettava funktio $f : O_1 \to O_2$ siten, että $i \in O_1$ jos ja vain jos $f(i) \in O_2$.

Määritelmä. Ongelma O on **C**-täydellinen, jos O kuuluu luokkaan **C** ja O on **C**-kova.

$\Rightarrow$ **C**-täydelliset ongelmat ovat vaativimpia luokan **C** ongelmia.

Väite. SAT on **NP**-kova (todistus sivutetaan).

$\Rightarrow$ Pahimmassa tapauksessa ko. ongelman ratkaisu vaatii eksponentiaalisen ajan lauseen pituuteen nähden.

Tehokas algoritmi: Davis-Putnam [1960]