LAUSELOGIIKKA

1. Lauselogiikan kieli
2. Lauselogiikan semantiikka
3. Semanttiset peruskäsitteet
4. Semanttinen taulu
5. Vaihtoehtoisia todistusjärjestelmiä
6. Normaalimuodot
7. Resoluutio
8. Laskennallisesta vaativuudesta

1 Lauselogiikan kieli

- Lauselogiikan aakkosto
- Kielen määritelmä
- Lauseiden muodostamisesta
- Sopimukset sulkujen käytöstä
- Esimerkki: rakenteinen induktio

1.1 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: ()

Symboleja $\neg, \vee, \wedge, \rightarrow$ ja $\leftrightarrow$ kutsutaan *konnektiiveiksi*.

1.2 Kielen määritelmä

Olkoon $\mathcal{P}$ ei-tyhjä joukko atomisia lauseita.

Lauselogiikan lauseenmuodostussäännöt:

1. Jokainen atominen lause $A \in \mathcal{P}$ on *lause*.
2. Jos α ja β ovat lauseita, niin myös $(\neg\alpha)$, $(\alpha \vee \beta)$, $(\alpha \wedge \beta)$, $(\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$ ovat *lauseita*.
3. vain edellä olevien sääntöjen perusteella muodostetut merkkijonot ovat *lauseita*.

Näiden sääntöjen nojalla muodostettavissa olevien lauseiden joukkoa kutsutaan (atomisten lauseiden joukkoon $\mathcal{P}$ perustuvaksi) lauselogiikan kieleksi $\mathcal{L}$.

Vaihtoehtoinen määritelmä

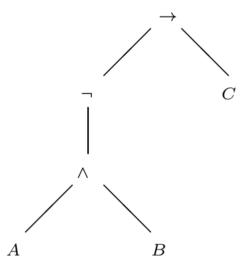
Määritelmä. Atomisten lauseiden joukkoon $\mathcal{P}$ perustuva *lauselogiikan kieli* $\mathcal{L}$ on pienin joukko, joka on suljettu seuraavien vaatimusten suhteen:

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

Esimerkki. Jos $\mathcal{P} = \{A, B\}$, niin esimerkiksi $A, B, (\neg A), ((\neg A) \vee B)$ ja $(((\neg A) \vee B) \rightarrow A)$ ovat kielen $\mathcal{L}$ lauseita, kun taas $(A \vee C)$ ei ole.

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 *negaatioita*, *konjunktioita*, *disjunktioita* ja *ekvivalensseja*.

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

1.3 Lauseiden muodostaminen

Jos lähtökohtana on joukko luonnollisen kielen lauseita,

- tunnistetaan atomiset lauseet eli väittämät, joita ei voida enää loogisessa mielessä pilkkoa osiin ja
- tunnistetaan konnektiivit ja muodostetaan vastaavat logiikan lauseet.

Tavoitteena voi olla myös jonkin systeemin määrittely suoraan logiikan lausein. Tällöin

- valitaan sopiva joukko systeemin ominaisuuksia kuvaavia atomisia lauseita ja
- määritellään näiden suhteet logiikan lausein.

Esimerkki. Muotoillaan seuraava luonnollisen kielen lause lauselogiikan lauseena.

Jos tiedosto on liian suuri, niin se tiivistetään tai poistetaan.

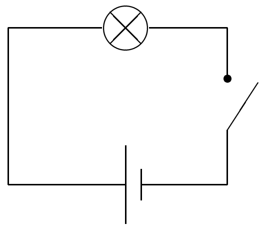
Valitaan atomiset lauseet

A = "Tiedosto on liian suuri",
B = "Tiedosto tiivistetään" ja
C = "Tiedosto poistetaan".

Saadaan: jos A, niin B tai C.

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

Esimerkki. Kuvataan seuraavaa yksinkertaista järjestelmää lauselogiikan lausein.



Valitaan atomisiksi lauseiksi

L = "Lamppu palaa",
K = "Kytkin on suljettu" ja
P = "Paristossa on riittävästi varausta".

Määritellään järjestelmän sallitut tilat lauseilla

$$((\neg P) \to (\neg L)) \text{ ja}$$
$$(P \to (L \leftrightarrow K)).$$

1.4 Sopimukset sulkeiden käytöstä

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

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

Lisähuomioita sulkeiden käytöstä

- Edellä tehdyt sopimukset (ketjukonjuktioita ja -disjunktioita lukuunottamatta) takaavat, että lauseen ϕ jäsennyspuu säilyy yksikäsitteisenä sulkeita vähennettäessä.
- Esimerkiksi merkkijonoa $A \to B \to C$ ei pystytä jäsentämään lauseeksi (yksikäsitteisesti).

  Tarvitaan sulkeet: $A \to (B \to C)$ tai $(A \to B) \to C$.

  Näillä lauseilla on yksikäsitteiset jäsennyspuut.
- Ketjudisjunktiokin $A \vee B \vee C$ voidaan jäsentää kahdella tavalla: $(A \vee B) \vee C$ tai $A \vee (B \vee C)$.

  Jatkossa näille annetaan kuitenkin sama merkitys, joten on samantekevää kuinka jäsennys suoritetaan.

1.5 Esimerkki: rakenteinen induktio

Määritelmä. Lauseen *alilauseet* määräytyvät seuraavasti:

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

Esimerkki. Lauseen $A \to B \vee C$ alilauseet ovat $A, B, C, B \vee C$ ja $A \to B \vee C$.

Väite. Lauseella 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 $\#\phi \leq A\phi + K\phi$.

Todistus.

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

Induktio-oletuksen perusteella: $\#\alpha \leq A\alpha + K\alpha$.

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

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

Induktioaskel jatkuu: ϕ on muotoa $(\alpha * \beta)$, missä $*$ on mikä tahansa binäärisistä konnektiiveista $\vee$, $\wedge$, $\rightarrow$ ja $\leftrightarrow$.

$$\begin{aligned}\#(\alpha * \beta) &= 1 + \#\alpha + \#\beta - \#(\alpha,\beta) \\ &\leq 1 + A\alpha + K\alpha + A\beta + K\beta - \#(\alpha,\beta) \quad \text{(ind.-oletus)} \\ &= A\alpha + A\beta - \#(\alpha,\beta) + 1 + K\alpha + K\beta \\ &\leq A\alpha + A\beta - A(\alpha,\beta) + K(\alpha * \beta) \\ &= A(\alpha * \beta) + K(\alpha * \beta).\end{aligned}$$

Merkintä $\#(\alpha,\beta)$ tarkoittaa lauseiden α ja β yhteisten alilauseiden lukumäärää ja $A(\alpha,\beta)$ lauseiden α ja β yhteisten atomisten lauseiden lukumäärää. Tällöin pätee $A(\alpha,\beta) \leq \#(\alpha,\beta)$.

Näin ollen väittämä tuli todistetuksi kaikille lauseille ϕ.

2 Lauselogiikan semantiikka

- Perustotuustaulukot
- Konnektiivien määriteltävyys/riittävyys
- Lauselogiikan totuusmääritelmä
- Vaihtoehtoinen totuusmääritelmä: valuaatiot

2.1 Perustotuustaulukot

Perustotuustaulukoilla määritellään eri muotoa olevien lauseiden totuusarvot alilauseidensa funktiona.

α	$(\neg\alpha)$
T	E
E	T

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

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

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

Huomio. Disjunktio $(\alpha \vee \beta)$ on tosi $\iff$ α on tosi **tai** β on tosi. Disjunktio $(\alpha \vee \beta)$ on siis tosi myös silloin, kun sekä α että β ovat tosia.

Voidaan määritellä myös poissulkeva disjuktio $(\alpha \underline{\vee} \beta)$, joka on epätosi molempien disjunktien ollessa tosia.

α	β	$(\alpha \underline{\vee} \beta)$
T	T	E
T	E	T
E	T	T
E	E	E

$(\alpha \underline{\vee} \beta)$ on tosi $\iff$ **joko** α on tosi **tai** β on tosi.

Perustotuustaulukot (jatkoa)

α	β	$(\alpha \rightarrow \beta)$
T	T	T
T	E	E
E	T	T
E	E	T

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

$(\alpha \rightarrow \beta)$ on tosi $\iff$ α on epätosi **tai** β on tosi
$\iff$ **jos** α on tosi, **niin** β on tosi.

Huomio. Implikaatio $\rightarrow$ *ei* edellytä syy-seuraus-suhdetta. Esim.

A = "Ruotsi sijaitsee Aasiassa", B = "Joulupukki on olemassa".

Lause $(A \rightarrow B)$ on tosi, koska A on epätosi.

Perustotuustaulukoiden avulla voidaan muodostaa totuustaulukko mille tahansa lauseelle (tai jopa lausejoukolle).

Esimerkki. Tutkittava lause: $(\neg B \wedge (A \rightarrow B))$
Alilauseet: $A, B, \neg B, (A \rightarrow B), (\neg B \wedge (A \rightarrow B))$
Totuustaulukossa on $2^2 = 4$ riviä ja 5 saraketta.

A	B	$\neg B$	$(A \rightarrow B)$	$(\neg B \wedge (A \rightarrow B))$
T	T	E	T	E
T	E	T	E	E
E	T	E	T	E
E	E	T	T	T

Muistathan, että jokaisessa lauseessa ϕ on korkeintaan niin monta alilausetta kuin lauseessa ϕ on atomisia lauseita ja konnektiiveja.

2.2 Konnektiivien määriteltävyys/riittävyys

Konnektiiveille voidaan antaa määritelmiä myös toistensa avulla.

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

Täten konnektiivit $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ eivät ole kaikki välttämättömiä:

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

Voidaan määritellä myös konnektiivit $\downarrow$ ja $|$:

- Peircen nuoli: $(\alpha \downarrow \beta) \equiv \neg(\alpha \vee \beta)$
- Shefferin viiva: $(\alpha \mid \beta) \equiv \neg(\alpha \wedge \beta)$

Nämä riittävät kumpikin yksinään muiden määrittelemiseen!

2.3 Lauselogiikan totuusmääritelmä

Määritelmä. *Totuusjakelu* $\mathcal{A}$ on atomisten lauseiden joukon $\mathcal{P}$ osajoukko.

Ajatuksena on, että

- $\mathcal{A}$:n atomiset lauseet ovat tosia,
- $\mathcal{P} - \mathcal{A}$:n atomiset lauseet ovat epätosia.

Huomioita.

- Jos $\mathcal{P}$ on äärellinen, erilaisia totuusjakeluja on $2^{|\mathcal{P}|}$ kappaletta.
- Jokainen totuusjakelu vastaa yhtä totuustaulukon riviä (ja kääntäen).

Totuusjakelu voidaan ymmärtää yhden asiantilan kuvauksena.

Esimerkki. (vrt. aikaisempi lamppuesimerkki)

$\mathcal{A}_1 = \{P\}$:	Patterissa on riittävästi varausta.
	Kytkin ei ole suljettu.
	Lamppu ei pala.
$\mathcal{A}_2 = \{L, K\}$:	Patterissa ei ole riittävästi varausta.
	Lamppu palaa.
	Kytkin on suljettu.

Näistä jälkimmäinen on mitä ilmeisimmin fyysisesti mahdoton, mutta kuitenkin loogisesti mahdollinen asiantila.

Määritelmä. Seuraavassa määritellään milloin mielivaltainen lause $\phi \in \mathcal{L}$ on **tosi** totuusjakelussa $\mathcal{A}$ (merk. $\mathcal{A} \models \phi$) ja milloin ϕ on **epätosi** totuusjakelussa $\mathcal{A}$ (merk. $\mathcal{A} \not\models \phi$).

1. $\mathcal{A} \models A \iff A \in \mathcal{A}$ (atomisille lauseille $A \in \mathcal{P}$).
2. $\mathcal{A} \models \neg\alpha \iff \mathcal{A} \not\models \alpha$.
3. $\mathcal{A} \models \alpha \land \beta \iff \mathcal{A} \models \alpha$ ja $\mathcal{A} \models \beta$.
4. $\mathcal{A} \models \alpha \lor \beta \iff \mathcal{A} \models \alpha$ tai $\mathcal{A} \models \beta$.
5. $\mathcal{A} \models \alpha \rightarrow \beta \iff \mathcal{A} \not\models \alpha$ tai $\mathcal{A} \models \beta$.
6. $\mathcal{A} \models \alpha \leftrightarrow \beta \iff$ joko $\mathcal{A} \models \alpha$ ja $\mathcal{A} \models \beta$ tai $\mathcal{A} \not\models \alpha$ ja $\mathcal{A} \not\models \beta$.

Totuusmääritelmän seurauksia

Väite. Jos $\mathcal{A} \subseteq \mathcal{P}$ on totuusjakelu, niin kaikille lauseille $\phi \in \mathcal{L}$, joko $\mathcal{A} \models \phi$ tai $\mathcal{A} \not\models \phi$.

Merkitään $At(\phi)$:llä ϕ:ssä esiintyvien atomisten lauseiden joukkoa.

Väite. Olkoon $\mathcal{A}_1 \subseteq \mathcal{P}$ ja $\mathcal{A}_2 \subseteq \mathcal{P}$ kaksi totuusjakelua ja $\phi \in \mathcal{L}$ lause. Jos $\mathcal{A}_1 \cap At(\phi) = \mathcal{A}_2 \cap At(\phi)$, niin $\mathcal{A}_1 \models \phi \iff \mathcal{A}_2 \models \phi$.

Nämä voidaan todistaa induktiolla ϕ:n rakenteen suhteen.

2.4 Vaihtoehtoinen totuusmääritelmä: valuaatiot

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

Valuaatioilla ja totuusjakeluilla on seuraava yhteys.

1. Olkoon $\mathcal{V}$ valuaatio ja $\mathcal{A} = \{A \in \mathcal{P} \mid \mathcal{V}(A) = T\}$.
   Tällöin kaikille lauseille $\phi \in \mathcal{L}$ pätee:
   $\mathcal{A} \models \phi \iff \mathcal{V}(\phi) = T$.
2. Jos $\mathcal{A}$ on totuusjakelu, niin on olemassa yksikäsitteinen valuaatio $\mathcal{V}$ siten että $\mathcal{A} = \{A \in \mathcal{P} \mid \mathcal{V}(A) = T\}$.

3 Semanttiset peruskäsitteet

- Mallin käsite
- Toteutuvuus
- Pätevyys
- Looginen seuraavuus
- Looginen ekvivalenssi
- Peruskäsitteiden väliset yhteydet
- Loogisten seurauksien ominaisuuksia

3.1 Mallin käsite

Määritelmä. Totuusjakelu $\mathcal{A} \subseteq \mathcal{P}$ on lauseen $\alpha \in \mathcal{L}$ *malli*, joss lause α on tosi $\mathcal{A}$:ssa eli $\mathcal{A} \models \alpha$.

Esimerkki. Totuusjakelut $\mathcal{A}_1 = \{A\}, \mathcal{A}_2 = \{B\}$ ja $\mathcal{A}_3 = \{A, B\}$ ovat malleja lauseelle $A \vee B$.

Määritelmä. Totuusjakelu $\mathcal{A} \subseteq \mathcal{P}$ on lausejoukon $\Sigma \subseteq \mathcal{L}$ *malli* (merk. $\mathcal{A} \models \Sigma$), joss kaikille lausejoukon Σ lauseille $\sigma \in \Sigma$ pätee $\mathcal{A} \models \sigma$.

Näin ollen lausejoukon Σ lauseet tulkitaan konjunktiivisesti.

Olkoon $\mathcal{P} = \{P, L, K\}$. Lamppuesimerkin lausejoukko on $\Sigma = \{\neg P \rightarrow \neg L, P \rightarrow (L \leftrightarrow K)\} \subseteq \mathcal{L}$. Totuustaulukko:

P	L	K	$\neg P$	$\neg L$	$\neg P \rightarrow \neg L$	$L \leftrightarrow K$	$P \rightarrow (L \leftrightarrow K)$	
T	T	T	E	E	$\boxed{T}$	T	$\boxed{T}$	$\longleftarrow$
T	T	E	E	E	T	E	E	
T	E	T	E	T	T	E	E	
T	E	E	E	T	$\boxed{T}$	T	$\boxed{T}$	$\longleftarrow$
E	T	T	T	E	E	T	T	
E	T	E	T	E	E	E	T	
E	E	T	T	T	$\boxed{T}$	E	$\boxed{T}$	$\longleftarrow$
E	E	E	T	T	$\boxed{T}$	T	$\boxed{T}$	$\longleftarrow$

Lausejoukolla Σ on siis neljä erilaista mallia (merkitty nuolin), jotka vastaavat järjestelmän sallittuja tiloja.

3.2 Toteutuvuus

Määritelmä. Lause $\alpha \in \mathcal{L}$ (tai lausejoukko $\Sigma \subseteq \mathcal{L}$) on *toteutuva*, joss ainakin yksi totuusjakelu $\mathcal{A} \subseteq \mathcal{P}$ on sen malli.

Huomio. Koska lauseiden totuusarvot määräytyvät niissä esiintyvien atomisten lauseiden totuusarvoista, voimme rajoittua totuusjakeluihin $\mathcal{A} \subseteq At(\phi)$ tai $\mathcal{A} \subseteq At(\Sigma) = \cup\{At(\sigma) | \sigma \in \Sigma\}$ selvittäessämme ϕ:n tai Σ:n malleja.

Jos lauseella tai lausejoukolla ei ole yhtään mallia, se on *toteutumaton*.

Toteutuvuuden tutkiminen totuustaulukolla:

- muodostetaan α:lle (Σ:lle) totuustaulukko ja
- tarkastetaan onko α tosi (kaikki Σ:n lauseet tosia) jollakin rivillä.

Esimerkki.

Onko $A \wedge \neg A$ toteutuva?

A	$\neg A$	$A \wedge \neg A$
T	E	E
E	T	E

Ei.

Onko $A \vee \neg B$ toteutuva?

A	B	$\neg B$	$A \vee \neg B$
T	T	E	$\boxed{T}$
T	E	T	$\boxed{T}$
E	T	E	E
E	E	T	$\boxed{T}$

Kyllä.

3.3 Pätevyys

Määritelmä. Lause $\alpha \in \mathcal{L}$ on *pätevä/tautologia* (merkitään $\models \alpha$), jos $\mathcal{A} \models \alpha$ kaikille totuusjakeluille $\mathcal{A} \subseteq \mathcal{P}$.

Esimerkki. Olkoon $\mathcal{P} = \{A\}$ ja $\mathcal{L}$ vastaava kieli. Lause $A \vee \neg A$ on pätevä, koska $A \vee \neg A$ on tosi totuusjakeluissa $\mathcal{A}_1 = \{\}$ ja $\mathcal{A}_2 = \{A\}$.

Vastamallit

Tarkastellaan mielivaltaista lausetta $\phi \in \mathcal{L}$.

- Jos ϕ on pätevä, $\mathcal{A} \models \phi$ kaikille totuusjakeluille $\mathcal{A} \subseteq \mathcal{P}$.
- Jos ϕ ei ole pätevä, löytyy totuusjakelu $\mathcal{A}$ siten, että $\mathcal{A} \not\models \phi$.

Jälkimmäisessä tapauksessa kutsumme totuusjakelua $\mathcal{A}$ *vastamalliksi* (tai vastaesimerkiksi) lauseen ϕ pätevyydelle.

Pätevyyden tutkiminen totuustaulukolla:

- muodostetaan α:lle totuustaulukko ja
- tarkistetaan, että α on tosi jokaisella rivillä.

Esimerkki.

Onko $A \wedge B \rightarrow A$ pätevä?

A	B	$A \wedge B$	$A \wedge B \rightarrow A$
T	T	T	T
T	E	E	T
E	T	E	T
E	E	E	T

Kyllä.

Onko $A \vee B \rightarrow A$ pätevä?

A	B	$A \vee B$	$A \vee B \rightarrow A$
T	T	T	T
T	E	T	T
E	T	T	$\boxed{E}$
E	E	E	T

Ei.

3.4 Looginen seuraavuus

Määritelmä. Lause $\alpha \in \mathcal{L}$ on lausejoukon $\Sigma \subseteq \mathcal{L}$ looginen seuraus (merkitään $\Sigma \models \alpha$), jos $\mathcal{A} \models \alpha$ kaikille lausejoukon Σ malleille $\mathcal{A} \subseteq \mathcal{P}$.

Esimerkki. $\neg\neg A$ seuraa loogisesti lausejoukoista $\{A\}$ ja $\{A \wedge \neg A\}$.

Käytämme *vastamallin* käsitettä myös loogisen seuraavuuden yhteydessä.

- Jos $\Sigma \not\models \phi$, lausejoukolla Σ on malli $\mathcal{A}$ siten, että $\mathcal{A} \not\models \phi$.

Esimerkki. $\{A, B \rightarrow A\} \not\models \neg\neg B$, koska löytyy vastamalli $\mathcal{A} = \{A\}$ siten, että $\mathcal{A} \models \{A, B \rightarrow A\}$ ja $\mathcal{A} \not\models \neg\neg B$.

Loogisen seuraavuuden tutkiminen totuustaulukolla:

- muodostetaan lausejoukolle $\Sigma \cup \{\alpha\}$ totuustaulukko,
- todetaan rivit, joilla kaikki Σ:n lauseet ovat tosia (Σ:n mallit) ja
- tarkistetaan, että α on näillä riveillä tosi.

Esimerkki.

$\{A, (A \to D)\} \models D$? $\{(A \to B)\} \models B$?

A	D	$(A \to D)$	
T	T	T	$\longleftarrow$
T	E	E	
E	T	T	
E	E	T	

Kyllä.

A	B	$(A \to B)$	
T	T	T	$\longleftarrow$
T	E	E	
E	T	T	$\longleftarrow$
E	$\boxed{E}$	T	$\longleftarrow$

Ei.

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

Esimerkki. Tutkitaan, onko lause $\neg L \vee K$ looginen seuraus lamppuesimerkin lausejoukolle $\Sigma = \{P \to (L \leftrightarrow K), \neg P \to \neg L\}$. On.

P	L	K	$\neg P$	$\neg L$	$\neg P \to \neg L$	$L \leftrightarrow K$	$P \to (L \leftrightarrow K)$	$\neg L \vee K$	
T	T	T	E	E	T	T	T	$\boxed{T}$	$\longleftarrow$
T	T	E	E	E	T	E	E	E	
T	E	T	E	T	T	E	E	T	
T	E	E	E	T	T	T	T	$\boxed{T}$	$\longleftarrow$
E	T	T	T	E	E	T	T	T	
E	T	E	T	E	E	E	T	E	
E	E	T	T	T	T	E	T	$\boxed{T}$	$\longleftarrow$
E	E	E	T	T	T	T	T	$\boxed{T}$	$\longleftarrow$

3.5 Looginen ekvivalenssi

Määritelmä. Lauseet $\alpha \in \mathcal{L}$ ja $\beta \in \mathcal{L}$ ovat *loogisesti ekvivalentteja* ($\alpha \equiv \beta$), joss $\mathcal{A} \models \alpha \iff \mathcal{A} \models \beta$ kaikille totuusjakeluille $\mathcal{A} \subseteq \mathcal{P}$.

Esimerkki. A ja $\neg\neg A$ ovat loogisesti ekvivalentit, koska näillä on sama totuusarvo kaikissa totuusjakeluissa.

Väite. Lauseet $\alpha \in \mathcal{L}$ ja $\beta \in \mathcal{L}$ ovat loogisesti ekvivalentit, joss niillä on täsmälleen samat mallit $\mathcal{A} \subseteq \mathcal{P}$.

Lauseiden α ja β loogisen ekvivalenssin selvittäminen:

- muodostetaan α:lle ja β:lle yhteinen totuustaulukko ja
- tarkastetaan, että α:lla ja β:lla on sama totuusarvo jokaisella rivillä.

Esimerkki. Ovatko lauseet $A \to B$ ja $\neg B \to \neg A$ loogisesti ekvivalentit?

$\neg A$	$\neg B$	$A \to B$	$\neg B \to \neg A$
E	E	T	T
E	T	E	E
T	E	T	T
T	T	T	T

Kyllä.

Määritelmä. Lausejoukot $\Sigma_1 \subseteq \mathcal{L}$ ja $\Sigma_2 \subseteq \mathcal{L}$ ovat loogisesti ekvivalentit, joss kaikille totuusjakeluille $\mathcal{A} \subseteq \mathcal{P}$ pätee seuraava:

$$\begin{aligned} & \mathcal{A} \models \sigma_1 \text{ kaikille } \sigma_1 \in \Sigma_1 \\ \iff & \mathcal{A} \models \sigma_2 \text{ kaikille } \sigma_2 \in \Sigma_2. \end{aligned}$$

Väite. Lausejoukot $\Sigma_1 \subseteq \mathcal{L}$ ja $\Sigma_2 \subseteq \mathcal{L}$ ovat loogisesti ekvivalentit, mikäli niillä on täsmälleen samat mallit $\mathcal{A} \subseteq \mathcal{P}$.

Lausejoukkojen Σ_1 ja Σ_2 loogisen ekvivalenssin selvittäminen:

- todetaan, että $\Sigma_1 \models \sigma_2$ kaikille $\sigma_2 \in \Sigma_2$ ja
- todetaan, että $\Sigma_2 \models \sigma_1$ kaikille $\sigma_1 \in \Sigma_1$.

3.6 Peruskäsitteiden väliset yhteydet

Tarkastellaan atomisten lauseiden joukkoon $\mathcal{P}$ perustuvan kielen $\mathcal{L}$ lauseita.

- Lauseet α ja β ovat *loogisesti ekvivalentteja* $\iff \models \alpha \leftrightarrow \beta$.

  Todistus.

  α ja β eivät ole loogisesti ekvivalentit

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \models \alpha$ ja $\mathcal{A} \not\models \beta$, tai $\mathcal{A} \not\models \alpha$ ja $\mathcal{A} \models \beta$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \not\models \alpha \leftrightarrow \beta$

  $\iff \not\models \alpha \leftrightarrow \beta$.

Pätevyydellä ja loogisella seuraavuudella on kiinteät yhteydet.

- $\models \alpha \iff \emptyset \models \alpha$.

  Seuraa helposti, koska kaikki totuusjakelut $\mathcal{A} \subseteq \mathcal{P}$ ovat tyhjän lausejoukon $\emptyset$ malleja

- $\{\phi_1, \ldots, \phi_n\} \models \phi \iff \models \phi_1 \land \cdots \land \phi_n \rightarrow \phi$.

  Todistus.

  $\{\phi_1, \ldots, \phi_n\} \not\models \phi$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A}$ on $\{\phi_1, \ldots, \phi_n\}$:n malli ja $\mathcal{A} \not\models \phi$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\forall i \in \{1, \ldots, n\} : \mathcal{A} \models \phi_i$ ja $\mathcal{A} \not\models \phi$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \models \phi_1 \land \cdots \land \phi_n$ ja $\mathcal{A} \not\models \phi$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \not\models \phi_1 \land \cdots \land \phi_n \rightarrow \phi$

  $\iff \not\models \phi_1 \land \cdots \land \phi_n \rightarrow \phi$.

Pätevyyden ja loogisen seuraavuuden yhteys toteutuvuuteen:

- $\models \alpha \iff \neg\alpha$ on toteutumaton.

  Todistus. Erikoistapaus seuraavasta.

- $\Sigma \models \alpha \iff \Sigma \cup \{\neg\alpha\}$ on toteutumaton.

  Todistus.

  $\Sigma \not\models \alpha$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \models \Sigma$ ja $\mathcal{A} \not\models \alpha$

  $\iff \exists \mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \models \Sigma \cup \{\neg\alpha\}$

  $\iff \Sigma \cup \{\neg\alpha\}$ on toteutuva

  $\iff \Sigma \cup \{\neg\alpha\}$ ei ole toteutumaton.

Edellä esitettyjen yhteyksien avulla logiikan päättelyongelmien välillä voidaan suorittaa muunnoksia.

3.7 Loogisten seurauksien ominaisuuksia

Väite. (Kompaktius). Jos $\Sigma \models \phi$, niin on olemassa äärellinen osajoukko $\Sigma' \subseteq \Sigma$ siten, että $\Sigma' \models \phi$.

Määritelmä. Lausejoukon $\Sigma \subseteq \mathcal{L}$ loogisten seurausten joukko on $\mathrm{Cn}(\Sigma) = \{\phi \in \mathcal{L} \mid \Sigma \models \phi\}$.

Loogisten seurauksien joukolla $\mathrm{Cn}(\Sigma)$ on seuraavat perusominaisuudet:

- $\Sigma \subseteq \mathrm{Cn}(\Sigma)$.
- Monotonisuus: $\Sigma_1 \subseteq \Sigma_2 \Longrightarrow \mathrm{Cn}(\Sigma_1) \subseteq \mathrm{Cn}(\Sigma_2)$.
- $\mathrm{Cn}(\mathrm{Cn}(\Sigma)) = \mathrm{Cn}(\Sigma)$.

Tietämyksen esittämisen problematiikkaa

- Jokainen lausejoukko Σ määrittää joukon *malleja*, eli totuusjakeluja $\mathcal{A}$, joissa lausejoukon kaikki lauseet ovat tosia.
- Lausejoukon Σ mallit puolestaan määräävät lausejoukon loogisten seurauksien joukon $\mathrm{Cn}(\Sigma)$.
- Kaikki totuusjakelut ovat tyhjän lausejoukon $\emptyset$ malleja. Täten $\mathrm{Cn}(\emptyset)$ on itse asiassa pätevien lauseiden joukko.
- Enemmän lauseita $\Longrightarrow$ vähemmän malleja $\Longrightarrow$ enemmän loogisia seurauksia (*monotonisuus*).
- *Tietämyksen esittäminen*: ongelmana rajoittaa mallien joukko siten, että saadaan halutut loogiset seuraukset.
- Jos lausejoukko tulee ristiriitaiseksi, sillä ei ole mallia ja kaikki lauseet ovat tällöin lausejoukon loogisia seurauksia.

Lisähuomioita loogisesta seuraavuudesta

- Jos $\Sigma \models \phi$, niin $\mathrm{Cn}(\Sigma) = \mathrm{Cn}(\Sigma \cup \{\phi\})$.

  Lausejoukon loogisia seurauksia ei siis kannata lisätä lausejoukkoon, koska lausejoukon mallit eivät näin muutu!

- Oletetaan, että $\Sigma \not\models \phi$ ja että Σ halutaan laajentaa lausejoukoksi Σ' siten, että $\Sigma' \models \phi$.

  Apuna voidaan käyttää vastamallia/vastamalleja $\mathcal{A}$, joille $\mathcal{A} \models \Sigma$ ja $\mathcal{A} \not\models \phi$: lausejoukkoon Σ lisättävän lauseen ψ tulisi sulkea pois vastamalli/vastamalleja $\mathcal{A}$, ts. $\mathcal{A} \not\models \Sigma \cup \{\psi\}$.

  Lause ϕ toteuttaa myös tämän vaatimuksen, mutta lausetta ϕ ei välttämättä haluta liittää eksplisiittiseen tietämykseen.

  Esimerkki. $\Sigma = \{P \rightarrow Q\}$, $\phi = Q$ ja $\psi = P$.

4 Semanttinen taulu

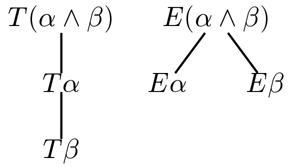
- Konnektiivikohtaiset taulusäännöt
- Semanttisen taulun määritelmä
- Taulumenetelmän ominaisuuksia
- Loogisten ongelmien ratkominen taulumenetelmällä
- Esimerkkejä

4.1 Konnektiivikohtaiset taulusäännöt

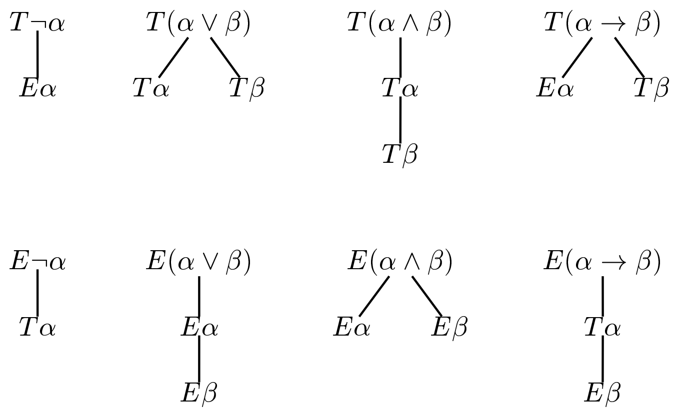
- Totuustaulukkoja käytetään lauseiden totuusarvojen laskemiseen, kun annettuna on atomisten lauseiden totuusarvot
- Semanttisissa tauluissa idea on käänteinen: määrätään alilauseiden (ja lopulta atomisten lauseiden) totuusarvot lähtien lauseen totuusarvosta.

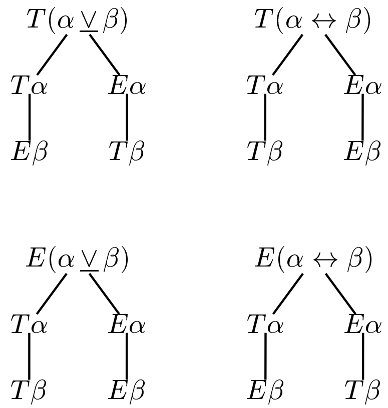
Esimerkki.

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



Konnektiiveille saadaan seuraavat säännöt:



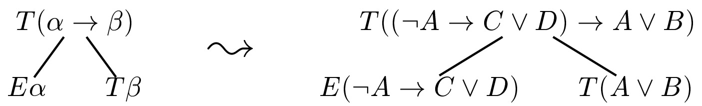


Taulusäännön instantiointi

Esimerkki. Tarkastellaan lausetta $(\neg A \rightarrow C \vee D) \rightarrow A \vee B$:

Lause on muodoltaan implikaatio $\alpha \rightarrow \beta$, missä ehtona on lause $\alpha = \neg A \rightarrow C \vee D$ ja seurauksena lause $\beta = A \vee B$.

Korvataan α ja β kyseisillä lauseilla implikaation säännössä:



4.2 Semanttisen taulun määritelmä

Semanttinen taulu on rakenteeltaan puu, jonka

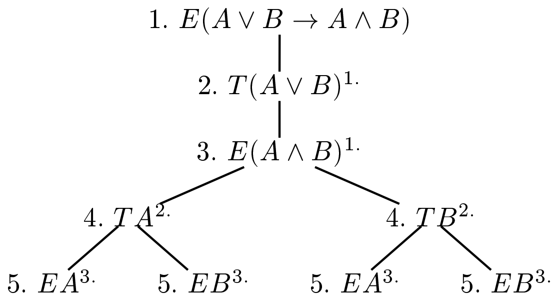
- solmujen asteluku on enintään kaksi ja
- solmuina on muotoa $T\phi$ ja $E\phi$ olevia lausekkeita.

Määritelmä. Semanttinen taulu muodostetaan seuraavilla periaatteilla:

- Jokainen yksisolmuinen puu, jonka juurisolmuna on $T\phi$ tai $E\phi$, on semanttinen taulu.
- Olkoon τ semanttinen taulu, P jokin τ:n polku juurisolmusta lehtisolmuun, $T\phi$ ($E\phi$) jokin τ:n solmu polulla P.

  Jos τ' saadaan τ:sta liittämällä $T\phi$:n ($E\phi$:n) taulusääntö (ilman juurisolmua) polun P jatkoksi, niin τ' on myöskin semanttinen taulu.

Esimerkki.

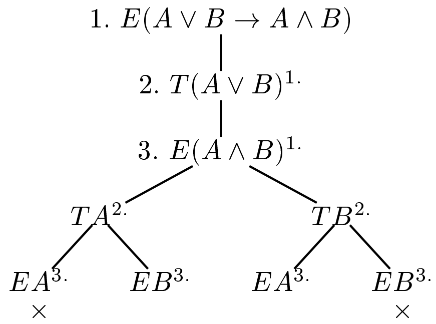


Semanttisen taulun solmut on numeroitu luettavuuden parantamiseksi. *Poluille lisättävät solmut numeroidaan juoksevasti.* Yläindeksinä oleva numero kertoo, mistä solmusta kyseinen solmu on saatu taulusääntöä soveltamalla.

Määritelmä. Olkoon τ semanttinen taulu, P polku juurisolmusta lehtisolmuun τ:ssa ja $T\phi$ ($E\phi$) polun P solmu.

1. Alkio $T\phi$ ($E\phi$) on *hajoitettu* polulla P, jos
   (a) ϕ on atominen lause, tai
   (b) $T\phi$:n ($E\phi$:n) taulusäännön jonkun polun jokainen alkio on P:n alkio.
2. Polku P on *ristiriitainen*, jos siinä esiintyy sekä $T\alpha$ että $F\alpha$ jollekin lauseelle α (tämän merkiksi kirjoitetaan usein $\times$ polun loppuun).
3. Polku P on *valmis*, jos se on ristiriitainen tai jokainen sen alkioista on hajoitettu polulla P.
4. Taulu τ on *valmis*, jos jokainen sen poluista on valmis.
5. Taulu τ on *ristiriitainen*, jos jokainen sen poluista on ristiriitainen.

Esimerkki. Palataan edelliseen esimerkkiin.



- Taulun reunimmaiset polut ovat ristiriitaiset.
- Kaikki taulun polut ovat valmiita.
- Taulu on valmis, muttei ristiriitainen.

4.3 Taulumenetelmän ominaisuuksia

Semanttisella taululla voidaan selvittää annetun lauseen $\alpha \in \mathcal{L}$ osalta, onko olemassa totuusjakelua $\mathcal{A} \subseteq \mathcal{P}$, joka täyttää annetun totuusarvovaatimuksen ($\mathcal{A} \models \alpha$ tai $\mathcal{A} \not\models \alpha$).

Tarkemmin sanottuna:

Väite. Olkoon $\alpha \in \mathcal{L}$ mikä tahansa lause. Juurialkiosta $T\alpha$ ($E\alpha$) muodostetussa valmiissa semanttisessa taulussa on ei-ristiriitainen polku, joss $\mathcal{A} \models \alpha$ ($\mathcal{A} \not\models \alpha$) jollekin totuusjakelulle $\mathcal{A} \subseteq \mathcal{P}$.

Taulumenetelmän virheettömyys

Olkoon $\alpha \in \mathcal{L}$ mikä tahansa lause ja τ juurialkiosta $T\alpha$ ($E\alpha$) muodostettu valmis semanttinen taulu.

Jos semanttisessa taulussa τ on ei-ristiriitainen polku,
niin $\mathcal{A} \models \alpha$ ($\mathcal{A} \not\models \alpha$) jollekin totuusjakelulle $\mathcal{A} \subseteq \mathcal{P}$.

Todistus.
Olkoon P mikä tahansa τ:n ei-ristiriitainen polku.

Olkoon totuusjakelu $\mathcal{A} = \{A \in \mathcal{P} \mid TA \text{ esiintyy polulla } P\}$.

Todistetaan induktiolla P:n alkioiden rakenteen suhteen, että $\mathcal{A} \models \beta$ kaikille $T\beta \in P$, ja $\mathcal{A} \not\models \beta$ kaikille $F\beta \in P$.

Perustapaus: $TA \in P$ ($EB \in P$), missä A (B) on $\mathcal{P}$:n atominen lause. Totuusjakelun $\mathcal{A}$ määritelmän perusteella $\mathcal{A} \models A$ ($\mathcal{A} \not\models B$).

Induktioaskel: Käydään läpi kaikki tapaukset
$T(\alpha \wedge \beta), E(\alpha \wedge \beta), T(\alpha \vee \beta), E(\alpha \vee \beta), T(\alpha \rightarrow \beta), E(\alpha \rightarrow \beta), \ldots$

- $E(\alpha \rightarrow \beta) \in P$, jolloin $T\alpha \in P$ ja $E\beta \in P$:
  Induktio-oletuksella $\mathcal{A} \models \alpha$ ja $\mathcal{A} \not\models \beta$.
  Totuusmääritelmän perusteella tällöin $\mathcal{A} \not\models \alpha \rightarrow \beta$.
- $T(\alpha \rightarrow \beta) \in P$, jolloin $E\alpha \in P$ tai $T\beta \in P$:
  Induktio-oletuksella $\mathcal{A} \not\models \alpha$ jos $E\alpha \in P$, tai $\mathcal{A} \models \beta$ jos $T\beta \in P$.
  Totuusmääritelmän perusteella tällöin $\mathcal{A} \models \alpha \rightarrow \beta$.
- Muut tapaukset käsitellään samaan tapaan.

Tarvitsemme seuraavaa apukäsitettä:

Määritelmä. Semanttisen taulun τ polku P on *yhteensopiva* totuusjakelun $\mathcal{A}$ kanssa, joss $\mathcal{A} \models \beta$ jokaiselle P:n alkiolle $T\beta$, ja $\mathcal{A} \not\models \beta$ jokaiselle P:n alkiolle $E\beta$.

Taulumenetelmän täydellisyys

Olkoon $\alpha \in \mathcal{L}$ mikä tahansa lause ja τ juurialkiosta $T\alpha$ ($E\alpha$) muodostettu valmis semanttinen taulu.

Jos $\mathcal{A} \models \alpha$ ($\mathcal{A} \not\models \alpha$) jossain totuusjakelussa $\mathcal{A} \subseteq \mathcal{P}$, **niin** semanttisessa taulussa τ on $\mathcal{A}$:n kanssa yhteensopiva (ja täten ei-ristiriitainen) polku P.

Todistus. Käytetään induktiota semanttisen taulun τ rakenteen suhteen.

Perustapaus: Oletetaan $\mathcal{A} \models \alpha$ ($\mathcal{A} \not\models \alpha$) jollekin totuusjakelulle $\mathcal{A} \in \mathcal{P}$. τ koostuu ainoastaan juurisolmusta $T\alpha$ ($E\alpha$).Tällöin τ:ssa on 0:n mittainen polku P juurisolmusta $T\alpha$ ($E\alpha$) juurisolmuun $T\alpha$ ($E\alpha$).

Induktioaskel: τ on saatu τ':sta soveltamalla jotain taulusääntöä polun P alkioon $T\beta$ tai $E\beta$. Induktio-oletuksen nojalla τ':ssa on $\mathcal{A}$:n kanssa yhteensopiva polku P'.

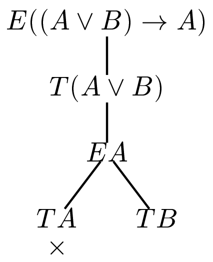
Jos $P \neq P'$, niin myös τ:ssa on $\mathcal{A}$:n kanssa yhteensopiva polku (P'). Jos $P = P'$, joudumme suorittamaan tapausanalyysin.

- Taulusääntöä sovellettiin alkioon $T\beta \in P$ ja $\beta = \neg\gamma$:
  $\Longrightarrow \mathcal{A} \models \neg\gamma$ ja $E\gamma$ lisätään P:n jatkoksi.
  $\Longrightarrow \mathcal{A} \not\models \gamma$ ja syntyvä polku on yhteensopiva $\mathcal{A}$:n kanssa.
- Taulusääntöä sovellettiin alkioon $E\beta \in P$ ja $\beta = \neg\gamma$:
  $\Longrightarrow \mathcal{A} \not\models \neg\gamma$ ja $T\gamma$ lisätään P:n jatkoksi.
  $\Longrightarrow \mathcal{A} \models \gamma$ ja syntyvä polu on yhteensopiva $\mathcal{A}$:n kanssa.

- Muut tapaukset käsitellään samaan tapaan.

Edellä osoitettu taulumenetelmän ominaisuus voidaan todeta seuraavasta esimerkistä.

Esimerkki.



Esimerkissä $\mathcal{A} \not\models (A \lor B) \to A$, $\mathcal{A} \models A \lor B$, $\mathcal{A} \not\models A$ ja $\mathcal{A} \models B$.

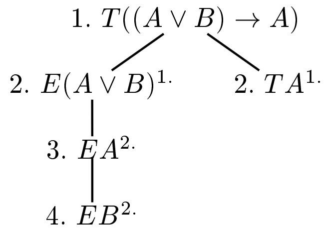
4.4 Loogisten ongelmien ratkominen taulumenetelmällä

Lauseen toteutuvuuden tutkiminen

Lähtökohtana ovat seuraavat yhteydet:

- Lause $\alpha \in \mathcal{L}$ on *toteutuva*
  $\Longleftrightarrow \exists$ totuusjakelu $\mathcal{A} \subseteq \mathcal{P}$ s.e. $\mathcal{A} \models \alpha$
  $\Longleftrightarrow$ juurisolmusta $T\alpha$ muodostetussa valmiissa semanttisessa taulussa on ainakin yksi ei-ristiriitainen polku P.
- Jokaisesta ei-ristiriitaisesta polusta P voidaan konstruoida α:lle malleja $\mathcal{A}$ seuraavasti. Jos atomiselle lauseelle $A \in \mathcal{P}$ pätee
  - $TA \in P$, niin $A \in \mathcal{A}$
  - $EA \in P$, niin $A \notin \mathcal{A}$
  - $TA \notin P$ ja $EA \notin P$, niin joko $A \in \mathcal{A}$ tai $A \notin \mathcal{A}$.

Esimerkki. Tutkitaan lauseen $A \lor B \to A$ toteutuvuutta.



Ei-ristiriitaisista poluista voidaan muodostaa lauseelle mallit $\mathcal{A}_1 = \{\}$, $\mathcal{A}_2 = \{A\}$ ja $\mathcal{A}_3 = \{A, B\}$.

Lausejoukon toteutuvuuden tutkiminen

- Äärellinen lausejoukko $\Sigma = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{L}$ on toteutuva

  $\iff$ lause $\alpha_1 \wedge \cdots \wedge \alpha_n \in \mathcal{L}$ on toteutuva

  $\iff$ juurisolmusta $T(\alpha_1 \wedge \cdots \wedge \alpha_n)$ muodostetussa valmiissa semanttisessa taulussa on ainakin yksi ei-ristiriitainen polku P.

- Lausejoukolle voidaan konstruoida malleja samaan tapaan kuin yksittäisen lauseen tapauksessa.

- Käytännössä juurisolmu $T(\alpha_1 \wedge \cdots \wedge \alpha_n)$ voidaan jättää kirjoittamatta näkyviin.

Lauseen pätevyyden tutkiminen

- $\models \alpha$

  $\iff \neg\alpha$ on toteutumaton

  $\iff$ juurisolmusta $T\neg\alpha$ muodostettu valmis semanttinen taulu on ristiriitainen

  $\iff$ juurisolmusta $E\alpha$ muodostettu valmis semanttinen taulu on ristiriitainen.

Täten taulumenetelmästä saadaan lauselogiikalle todistusmenetelmä.

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

Esimerkki.
Osoitetaan lause
$A \wedge B \to A \vee B$
teoreemaksi.

$\times$ = "polku on ristiriitainen"

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

Todistusmenetelmän virheettömyys ja täydellisyys

Todistusmenetelmä M on

- *virheetön*, jos lauseen α todistettavuudesta menetelmällä M ($\vdash_M \alpha$) seuraa lauseen α pätevyys ($\models \alpha$).

- *täydellinen*, jos lauseen α pätevyydestä ($\models \alpha$) seuraa lauseen todistettavuus menetelmällä M ($\vdash_M \alpha$)

Edellä määritelty semanttiseen tauluun perustuva todistusmenetelmä on virheetön ja täydellinen, koska $\vdash \alpha \iff \models \alpha$.

Loogisen seuraavuuden tutkiminen

- $\{\phi_1, \ldots, \phi_n\} \models \phi$
  $\iff \models \phi_1 \wedge \cdots \wedge \phi_n \to \phi$
  $\iff$ juurisolmusta $E(\phi_1 \wedge \cdots \wedge \phi_n \to \phi)$ muodostettu valmis semanttinen taulu on ristiriitainen.
- Jos juurisolmusta $E(\phi_1 \wedge \cdots \wedge \phi_n \to \phi)$ muodostettuun valmiiseen semanttiseen tauluun jää ei-ristiriitaisia polkuja, näistä voidaan konstruoida vastamalleja $\mathcal{A}$ siten, että $\mathcal{A} \models \{\phi_1, \ldots, \phi_n\}$ ja $\mathcal{A} \not\models \phi$.
- Käytännössä taulun juureen tulevat solmut $E(\phi_1 \wedge \cdots \wedge \phi_n \to \phi)$ ja $T(\phi_1 \wedge \cdots \wedge \phi_n)$ voidaan jättää kirjoittamatta näkyviin.

Johdettavuus lausejoukosta

Määritelmä. Lause β on johdettavissa äärellisestä lausejoukosta $\Sigma = \{\alpha_1, \ldots, \alpha_n\}$ (merkitään $\Sigma \vdash \beta$), joss juurialkiosta $E(\alpha_1 \wedge \cdots \wedge \alpha_n \to \beta)$ muodostettu valmis semanttinen taulu on ristiriitainen.

Huomioita.

- $\Sigma \vdash \beta \iff \Sigma \models \beta$.
- Taulumenetelmä on siis virheetön ja täydellinen todistusmenetelmä myös tässä tapauksessa.

Loogisen ekvivalenssin tutkiminen

- Lauseet α ja β ovat loogisesti ekvivalentit
  $\iff \models \alpha \leftrightarrow \beta$
  $\iff$ juurialkiosta $E(\alpha \leftrightarrow \beta)$ muodostettu valmis semanttinen taulu on ristiriitainen.
- Lausejoukkojen loogisen ekvivalenssin toteaminen edellyttää semanttisen taulun konstruointia (kts. loogisen ekvivalenssin määritelmät).

4.5 Esimerkkejä

Ohjeita semanttisten taulujen laadintaan:

- Taulun solmussa $T\phi$ (tai $E\phi$) olevan lauseen ϕ rakenne määrää, mitä taulusääntöä käytetään.
  Esimerkki. Jos ϕ on muodoltaan implikaatio $\alpha \to \beta$ käytetään sääntöä $T(\alpha \to \beta)$ (tai $E(\alpha \to \beta)$).
- Solmujen hajoittamisjärjestyksellä voi usein vaikuttaa taulun kokoon (haarautumista kannattaa välttää).
  Esimerkki.

$$\begin{array}{c} \vdots \\ | \\ TA \\ | \\ 6. E(B \to C) \\ | \\ 7. T(A \vee B) \\ | \\ 8. E(A \wedge C) \end{array}$$

  - Solmu 6 käsitellään ensin, koska taulu ei näin haaraudu.
  - Solmu 8 olisi seuraavaksi paras vaihtoehto, koska syntyvistä haaroista toinen (EA) on suoraan ristiriitainen.
  - Solmun 7 käsittely haarauttaa taulun.

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 E ja T
- Boolen muuttuja a (jolla arvona 0 tai 1) esitetään atomisena lauseena A (jolla totuusarvo E 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 $(A \wedge \neg B) \vee C$.

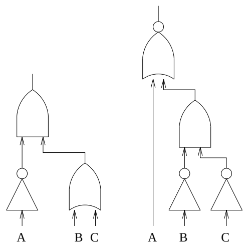
Väite. Olkoon f boolen funktio ja lause ϕ sitä vastaava esitys:

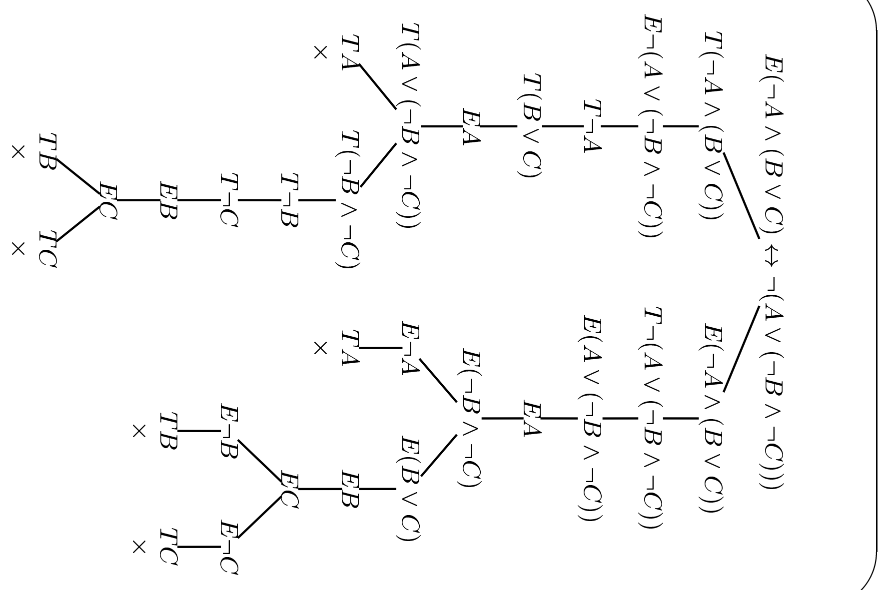
funktion f arvon laskeminen tietyillä muuttujien arvoilla vastaa lauseen ϕ totuusarvon laskentaa vastaavassa totuusjakelussa.

Esimerkki. Jos $a = 0$, $b = 0$ ja $c = 1$, niin vastaava totuusjakelu on $\mathcal{A} = \{c\}$.

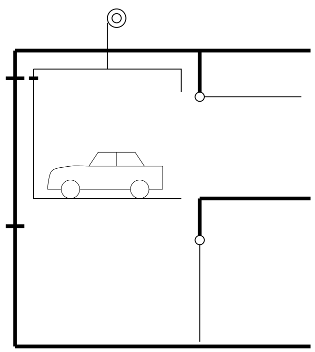
Aikaisemmalle esimerkille $f(0,0,1) = 0 \cdot \overline{0} + 1 = 0 \cdot 1 + 1 = 0 + 1 = 1$ ja vastaavasti $\mathcal{A} \models (A \wedge \neg B) \vee C$.

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





Esimerkki. Mallinnetaan yksinkertaistettua hissijärjestelmää lauselogiikalla:



Atomiset lauseet:

A_i: kerroksen i ovi on auki ja
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 $2^4 = 16$ mallia, kuten esimerkiksi $\mathcal{A} = \{K_1, K_2, A_1, A_2\}$.

  Tämä vastaa järjestelmän tilaa, jossa hissi on yhtäaikaa molemmissa kerroksissa ja molemmat ovet ovat auki. Tämä on mahdotonta, joten tarvitaan lisää lauseita (rajoitteita).

- Fyysisen maailman asettama rajoitus: $\neg K_1 \vee \neg K_2$ (huomaa, että $\mathcal{A}$ ei ole tämän lauseen malli).

- Emme kuitenkaan halua asettaa vaatimusta $K_1 \vee K_2$ (hissi voi olla matkalla kerrosten välillä).

- Oville asetettavat turvallisuusvaatimukset: $A_1 \rightarrow K_1$ ja $A_2 \rightarrow K_2$.

Järjestelmälle saadaan spesifikaatioksi lausejoukko

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

Etsitään spesifikaation mallit semanttisen taulun avulla.

- 1. $T(\neg K_1 \vee \neg K_2)$
- 2. $T(A_1 \rightarrow K_1)$
- 3. $T(A_2 \rightarrow K_2)$
  - 4. $T\neg K_1$ 1.
    - 5. EK_1 4.
      - 6. EA_1 2.
        - 7. EA_2 3.
        - 7. TK_2 3.
      - 6. TK_1 2. $\times$
  - 4. $T\neg K_2$ 1.
    - 5. EK_2 4.
      - 6. EA_2 2.
        - 7. EA_1 3.
        - 7. TK_1 3.
      - 6. TK_2 2. $\times$

Taulun avoimista haaroista lausejoukolle löydetään siis seuraavat mallit: $\mathcal{A}_1 = \emptyset$, $\mathcal{A}_2 = \{K_1\}$, $\mathcal{A}_3 = \{K_1, A_1\}$, $\mathcal{A}_4 = \{K_2\}$ ja $\mathcal{A}_5 = \{K_2, A_2\}$.

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

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

- 1. $E\neg(A_1 \wedge A_2)$
- 2. $T(\neg K_1 \vee \neg K_2)$
- 3. $T(A_1 \rightarrow K_1)$
- 4. $T(A_2 \rightarrow K_2)$
- 5. $T(A_1 \wedge A_2)$ 1.
- 6. TA_1 5.
- 7. TA_2 5.
  - 8. EA_1 3. $\times$
  - 8. TK_1 3.
    - 9. FA_2 4. $\times$
    - 9. TK_2 4.
      - 10. $T\neg K_1$ 2.
        - 11. EK_1 $\times$
      - 10. $T\neg K_2$ 2.
        - 11. EK_2 $\times$

5 Vaihtoehtoisia todistusjärjestelmiä

- Hilbertin järjestelmä
- Suppesin järjestelmä
- Järjestelmien vertailua

5.1 Hilbertin järjestelmä

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:

$$\frac{\alpha \to \beta \quad \alpha}{\beta} \quad \text{(modus ponens)}$$

Huomio. Hilbertin järjestelmässä negaatio ja implikaatio ovat peruskonnektiiveina.

Määritelmä. Olkoon Σ joukko lauseita.

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

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

Lause α on *teoreema/todistuva* Hilbert-järjestelmässä ($\vdash_{\mathrm{H}} \alpha$), joss $\emptyset \vdash_{\mathrm{H}} \alpha$

Lause α on *johdettavissa* lausejoukosta Σ Hilbert-järjestelmällä ($\Sigma \vdash_{\mathrm{H}} \alpha$), joss on olemassa todistus $\alpha_1, \ldots, \alpha_n$ Σ:sta siten, että $\alpha = \alpha_n$.

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

Väite. Olkoon lausejono $\alpha_1, \ldots, \alpha_n$ todistus lausejoukosta Σ Hilbertin järjestelmässä. Tällöin $\Sigma \models \alpha_i$ kaikille $i \in \{1, \ldots, n\}$.

Todistus induktiolla i:n suhteen.

- **Perustapaus:**
  Jos α_1 on aksiooma $\implies\ \models \alpha_1 \implies \Sigma \models \alpha_1$.
  Jos $\alpha_1 \in \Sigma \implies \Sigma \models \alpha_1$.
- **Induktioaskel:**
  Tapaukset missä α_i on aksiooma tai $\alpha_i \in \Sigma$ käsitellään kuten edellä.

- **Induktioaskel jatkuu:**
  Jos α_i saatiin modus ponensilla lauseista α_j ja $\alpha_k = (\alpha_j \rightarrow \alpha_i)$, missä $j < i$ ja $k < i$, niin induktiohypoteesin nojalla saadaan $\Sigma \models \alpha_j$ ja $\Sigma \models \alpha_j \rightarrow \alpha_i$.
  Oletetaan $\Sigma \not\models \alpha_i$
  $\Longrightarrow$ $\exists$ totuusjakelu $\mathcal{A}$ s.e. $\mathcal{A} \models \Sigma$ ja $\mathcal{A} \not\models \alpha_i$
  $\Longrightarrow$ $\mathcal{A} \not\models \alpha_j$ (koska $\Sigma \models \alpha_j \rightarrow \alpha_i \implies \mathcal{A} \models \alpha_j \rightarrow \alpha_i$)
  $\Longrightarrow$ $\Sigma \not\models \alpha_j$, ristiriita.
  Siis $\Sigma \models \alpha_i$.

Hilbertin järjestelmä on virheetön ja täydellinen.

Väite. Jos $\Sigma \vdash_{\mathrm{H}} \alpha$, niin $\Sigma \models \alpha$ (todistettiin edellä).
Jos $\Sigma \models \alpha$, niin $\Sigma \vdash_{\mathrm{H}} \alpha$ (todistus sivuutetaan).

5.2 Suppesin järjestelmä

Suppesin luonnollisen päättelyn järjestelmässä ei ole aksioomia ja päättelysäännöt ovat seuraavat:

MP (modus ponens):

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

TT (modus tollendo tollens):

$$\frac{\alpha \rightarrow \beta \quad \neg\beta}{\neg\alpha}$$

TP (modus tollendo ponens):

$$\frac{\alpha \vee \beta \quad \neg\alpha}{\beta}$$

Kommutaatiosäännöt:

KV:
$$\frac{\alpha \wedge \beta}{\beta \wedge \alpha}$$

DV:
$$\frac{\alpha \vee \beta}{\beta \vee \alpha}$$

Tuonti- ja eliminointisäännöt:

KNT:
$$\frac{\alpha}{\neg\neg\alpha}$$

KT:
$$\frac{\alpha \quad \beta}{\alpha \wedge \beta}$$

DT:
$$\frac{\alpha}{\alpha \vee \beta \quad \beta \vee \alpha}$$

ET:
$$\frac{\alpha \rightarrow \beta \quad \beta \rightarrow \alpha}{\alpha \leftrightarrow \beta}$$

KNE:
$$\frac{\neg\neg\alpha}{\alpha}$$

KE:
$$\frac{\alpha \wedge \beta}{\alpha \quad \beta}$$

DE:
$$\frac{\alpha \vee \alpha}{\alpha}$$

EE:
$$\frac{\alpha \leftrightarrow \beta}{\alpha \rightarrow \beta \quad \beta \rightarrow \alpha}$$

De Morganin säännöt:

DM 1:
$$\frac{\alpha \wedge \beta}{\neg(\neg\alpha \vee \neg\beta)}$$

DM 2:
$$\frac{\neg(\alpha \wedge \beta)}{\neg\alpha \vee \neg\beta}$$

DM 3:
$$\frac{\alpha \vee \beta}{\neg(\neg\alpha \wedge \neg\beta)}$$

DM 4:
$$\frac{\neg(\alpha \vee \beta)}{\neg\alpha \wedge \neg\beta}$$

HS:
$$\frac{\alpha \rightarrow \beta \quad \beta \rightarrow \gamma}{\alpha \rightarrow \gamma}$$

DS:
$$\frac{\alpha \vee \beta \quad \alpha \rightarrow \gamma \quad \beta \rightarrow \delta}{\gamma \vee \delta}$$

ET (ehdollisen todistamisen sääntö):[1]

$$\frac{[\alpha] \quad \beta}{\alpha \rightarrow \beta}$$

ES (epäsuoran todistamisen sääntö):

$$\frac{\neg\beta \rightarrow \alpha \wedge \neg\alpha}{\beta}$$

(1) Hakasulut α:n ympärillä tarkoittavat, ettei päätelmä $\alpha \rightarrow \beta$ riipu oletuksesta α.

Määritelmä. Todistus lausejoukosta Σ on jono lauseita $\alpha_1, \ldots, \alpha_n$, joihin liittyy lausejoukot $H_0 = \emptyset$ ja $H_1, \ldots, H_n$ (apuolettamukset) siten, että kaikille $i \in \{1, \ldots, n\}$ pätee jokin seuraavista:

- $H_i = H_{i-1}$ ja $\alpha_i \in \Sigma$ tai
- $H_i = H_{i-1} \cup \{\alpha_i\}$ ja α_i voi olla mikä tahansa lause tai
- $H_i = H_{i-1}$ ja α_i on saatu jollain Suppes-järjestelmän päättelysäännöllä (paitsi ehdollisen todistamisen säännöllä) sekvenssin aikaisemmista lauseista α_j, joille $H_j \subseteq H_i$ tai
- $H_i = H_{i-1} - \{\alpha_j\}$ ja $\alpha_i = \alpha_j \to \alpha_{i-1}$ on saatu ehdollisen todistamisen säännöllä lauseista α_j (viimeisin tehty apuolettamus) ja α_{i-1}.

Määritelmä. Lause α on *johdettavissa* lausejoukosta Σ Suppes-järjestelmällä ($\Sigma \vdash_{\mathrm{S}} \alpha$), joss on olemassa todistus $\alpha_1, \ldots, \alpha_n$ Σ:sta siten, että $\alpha_n = \alpha$ ja $H_n = \emptyset$.

Lause α on *teoreema/todistuva* Suppes-järjestelmässä ($\vdash_{\mathrm{S}} \alpha$), joss $\emptyset \vdash_{\mathrm{S}} \alpha$

Väite. Suppesin järjestelmä on lauselogiikan virheetön ja täydellinen todistusmenetelmä ($\Sigma \vdash_{\mathrm{S}} \alpha \iff \Sigma \models \alpha$).

Esimerkki.

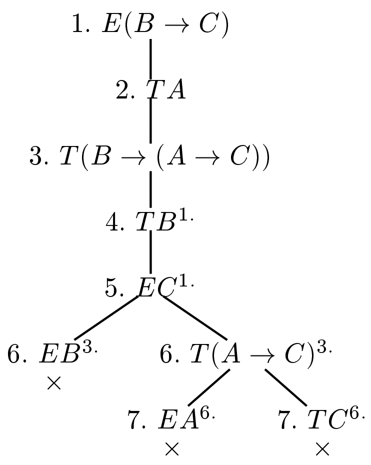
Osoitetaan $\{A, B \to (A \to C)\} \vdash_{\mathrm{S}} B \to C$.

1.	A	olettamus	$H_1 = \emptyset$
2.	$B \to (A \to C)$	olettamus	$H_2 = \emptyset$
3.	B	apuolettamus	$H_3 = \{B\}$
4.	$A \to C$	MP, 3, 2	$H_4 = \{B\}$
5.	C	MP, 1, 4	$H_5 = \{B\}$
6.	$B \to C$	ET, 3, 5	$H_6 = \emptyset$

Käytännössä apuolettamusten joukoista pidetään kirjaa tekemällä todistukseen sisennyksiä, jolloin H_i:t voidaan jättää pois todistuksesta.

5.3 Järjestelmien vertailua

Esimerkki.
Osoitetaan vielä semanttisella taululla, että $B \to C$ on johdettavissa lausejoukosta $\{A, B \to (A \to C)\}$.

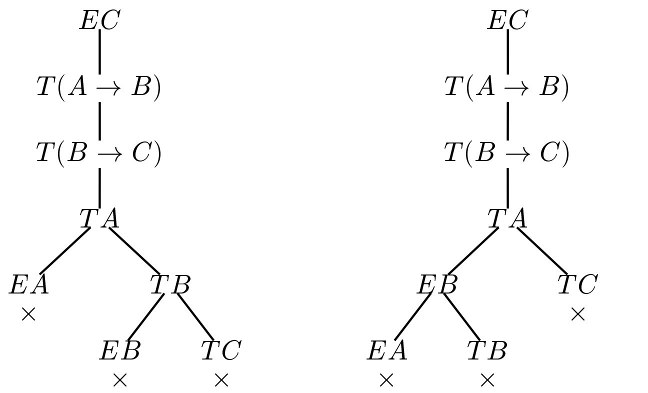


1. **Hilbertin järjestelmä**
   - \+ Minimalistinen koneisto teoreemien tuottamiseksi.
   - – Yksittäisten todistusten löytäminen voi olla vaikeaa.
   - – Hankala todeta milloin lause ei ole todistuva/johdettavissa.

2. **Suppesin järjestelmä**
   - \+ Päättelysääntöjen laaja valikoima tukee erilaisten loogisten päätelmien tekemistä ja todistusten löytämistä.
   - – Hankala todeta milloin lause ei ole todistuva/johdettavissa.

3. **Semanttinen taulu**
   - \+ Lauseiden syntaksi ohjaa päättelysäännön (taulusäännöt) valintaa.
   - \+ Mikäli lause ei ole todistuva/johdettavissa saadaan konkreettinen vastaesimerkki.
   - \+ Helppo toteuttaa tietokoneella.

Esimerkki. Semanttisella taululla pystytään *simuloimaan* monia Suppes-järjestelmän päättelysääntöjä.



"Modus ponens" "Modus tollendo tollens"

6 Normaalimuodot

- Konjunktiivinen ja disjunktiivinen normaalimuoto
- Muunnokset normaalimuotoihin
- Normaalimuotojen hakeminen taulumenetelmällä
- Normaalimuotojen sieventäminen
- Lauseiden klausuulimuoto

Motivaatio

- Normaalimuotojen tarkoituksena on saattaa tutkittava asia johonkin säännölliseen muotoon, jotta sen käsittely saadaan yksinkertaisemmaksi.
- Polynomien esittäminen muodossa:

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

- Lineaaristen yhtälöryhmien esittäminen matriiseina:

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

6.1 Konjunktiivinen ja disjunktiivinen normaalimuoto

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

Määritelmä. Lause α on *konjunktiivisessa normaalimuodossa*, jos α on muodoltaan konjunktio $\beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_n$, missä jokainen β_i on literaaleista $l_1, l_2, \ldots, l_{m_i}$ koostuva disjunktio $l_1 \vee l_2 \vee \cdots \vee l_{m_i}$.

Disjunktiivinen normaalimuoto määritellään samaan tapaan, mutta konjunktion ja disjunktion roolit vaihdetaan keskenään:

Määritelmä. Lause α on *disjunktiivisessa normaalimuodossa*, jos α on muodoltaan disjunktio $\beta_1 \vee \beta_2 \vee \cdots \vee \beta_n$, missä jokainen β_i on literaaleista $l_1, l_2, \ldots, l_{m_i}$ koostuva konjunktio $l_1 \wedge l_2 \wedge \cdots \wedge l_{m_i}$.

Esimerkki.

KNM:	$(A_1 \vee \neg A_2) \wedge (\neg A_1 \vee \neg A_3) \wedge (A_5 \vee A_6 \vee A_7)$
	$A_5 \wedge (\neg A_3 \vee A_6)$
KNM & DNM:	$A_1 \vee \neg A_2 \vee A_3$
	$\neg A_7$
	$A_1 \wedge A_2 \wedge A_3$
DNM:	$(\neg A_1 \wedge \neg A_2) \vee (A_3 \wedge A_1) \vee (A_1 \wedge \neg A_2 \wedge A_3)$
	$(A_1 \wedge \neg A_1) \vee A_2$

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

6.2 Muunnokset normaalimuotoihin

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

1. Poista konnektiivit $\leftrightarrow$ seuraavanlaisilla korvauksilla:

$$\alpha \leftrightarrow \beta \quad \rightsquigarrow \quad (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \qquad (1)$$

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

2. Poista konnektiivit $\rightarrow$ seuraavanlaisilla korvauksilla:

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

3. Siirrä negaatiot välittömästi atomisten lauseiden eteen:

$$\neg\neg\alpha \quad \rightsquigarrow \quad \alpha \qquad (3)$$

$$\neg(\alpha \vee \beta) \quad \rightsquigarrow \quad \neg\alpha \wedge \neg\beta \qquad (4)$$

$$\neg(\alpha \wedge \beta) \quad \rightsquigarrow \quad \neg\alpha \vee \neg\beta \qquad (5)$$

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

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

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

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

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

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

Huomio. Muunnossäännöt säilyttävät loogisen ekvivalenssin, joten lopputuloksena saadaan lauseelle konjunktiivinen tai disjunktiivinen normaalimuoto.

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

$$A \vee B \rightarrow (B \leftrightarrow C)$$

$$A \vee B \rightarrow (B \rightarrow C) \wedge (C \rightarrow B) \qquad (1)$$

$$\neg(A \vee B) \vee ((\neg B \vee C) \wedge (\neg C \vee B)) \qquad (2)$$

$$(\neg A \wedge \neg B) \vee ((\neg B \vee C) \wedge (\neg C \vee B)) \qquad (4)$$

Konjunktiivinen normaalimuoto:

$$(\neg A \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \qquad \mathbf{(7)}$$

$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \qquad \mathbf{(6)}$$

$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge ((\neg B \vee (\neg B \vee C)) \wedge (\neg B \vee (\neg C \vee B))) \qquad \mathbf{(6)}$$

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

Disjunktiivinen normaalimuoto:

$$(\neg A \wedge \neg B) \vee ((\neg B \vee C) \wedge \neg C) \vee ((\neg B \vee C) \wedge B) \qquad \mathbf{(8)}$$

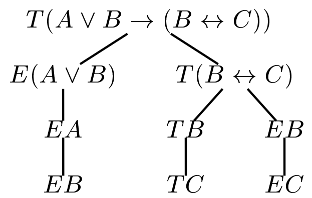
$$(\neg A \wedge \neg B) \vee (\neg B \wedge \neg C) \vee (C \wedge \neg C) \vee (\neg B \wedge B) \vee (C \wedge B) \qquad \mathbf{(9)}$$

6.3 Normaalimuotojen hakeminen taulumenetelmällä

Normaalimuodon voi hakea myös taulumenetelmällä.

Lauseen α disjunktiivinen normaalimuoto saadaan juurisolmusta $T\alpha$ muodostetun valmiin semanttisen taulun ristiriidattomista poluista.

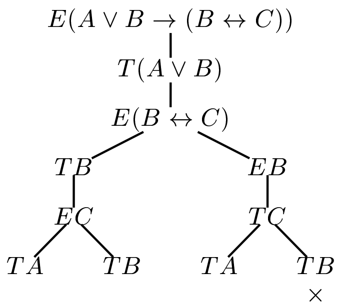
Esimerkki.



Tässä vasemmalla polulla on vaatimukset EA ja EB, keskimmäisellä TB ja TC ja oikealla EB ja EC. Nämä yhdistämällä saadaan disjunktiiviseksi normaalimuodoksi: $(\neg A \wedge \neg B) \vee (B \wedge C) \vee (\neg B \wedge \neg C)$.

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

Esimerkki.



Ristiriidattomista poluista saadaan DNM lauseelle $\neg\alpha$:
$\neg\alpha \equiv (A \land B \land \neg C) \lor (B \land \neg C) \lor (A \land \neg B \land C)$.
Lauseen α konjunktiivinen normaalimuoto on tällöin:
$\alpha \equiv \neg\neg\alpha \equiv (\neg A \lor \neg B \lor C) \land (\neg B \lor C) \land (\neg A \lor B \lor \neg C)$.

6.4 Normaalimuotojen sieventäminen

Konjunktiivista/disjunktiivista normaalimuotoa voidaan sieventää seuraavilla periaatteilla:

- Poistetaan literaalien disjunktioista/konjunktioista literaalien moninkertaiset esiintymät.
  Esimerkki.
  $(\neg A \lor \neg B \lor C) \land (\neg A \lor \neg C \lor B) \land (\neg B \lor \neg B \lor C) \land (\neg B \lor \neg C \lor B)$
  $\rightsquigarrow\ (\neg A \lor \neg B \lor C) \land (\neg A \lor \neg C \lor B) \land (\neg B \lor C) \land (\neg B \lor \neg C \lor B)$
- Poistetaan disjunktiot/konjunktiot, joissa esiintyy jokin literaali l ja sen komplementti $\bar{l}$.
  Esimerkki.
  $\rightsquigarrow\ (\neg A \lor \neg B \lor C) \land (\neg A \lor \neg C \lor B) \land (\neg B \lor C)$

- jos konjunktiivisessa normaalimuodossa esiintyy disjunktiot $(\alpha_1 \lor \cdots \lor \alpha_n)$ ja $(\beta_1 \lor \cdots \lor \beta_n)$ siten, että $\{\alpha_1, \ldots, \alpha_n\} \subseteq \{\beta_1, \ldots, \beta_n\}$, poistetaan jälkimmäinen (joka on edellisen looginen seuraus).
  Esimerkki.
  $(A \lor B \lor C) \land (A \lor B) \land (C \lor \neg B \lor A) \land (A \lor C)$
  $\rightsquigarrow\ (A \lor B) \land (C \lor \neg B \lor A) \land (A \lor C)$

6.5 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 $l_1 \lor \cdots \lor l_n$ on *klausuuli*.
- Klausuulit kirjoitetaan usein muodossa $\{l_1, \ldots, l_n\}$.
- Joukko klausuuleita S edustaa klausuuliensa konjunktiota.

Huomaa ero:
$\neg A \lor B \lor \neg A\ \rightsquigarrow\ \{\neg A, B\}$.

Konjunktiivisesta normaalimuodosta saadaan muodostettua sitä vastaava klausuulijoukko.

Esimerkki. Konjunktiivista normaalimuotoa $(A \vee \neg B) \wedge (\neg C \vee \neg A \vee D)$ vastaava klausuulijoukko on $\{\{A, \neg B\}, \{\neg C, \neg A, D\}\}$

Huomaa seuraavat erikoistapaukset:

- *Tyhjä klausuuli* $\Box$ edustaa tyhjää disjunktiota ja on siten aina epätosi.
- Tyhjä klausuulijoukko $\emptyset$ edustaa tyhjää konjunktiota ja on siten aina tosi.

Huomio. Muistanet seuraavan analogian: $\sum_{i=1}^{n} x_i = 0$ ja $\prod_{i=1}^{n} x_i = 1$, kun $n = 0$.

7 Resoluutio

- Totuusmääritelmä ja toteutuvuus klausuuleille
- Resoluutiosääntö
- Resoluutiotodistukset
- Resoluution virheettömyys ja täydellisyys
- Resoluution käyttökohteita

7.1 Totuusmääritelmä ja toteutuvuus klausuuleille

Määritelmä. Totuusjakelun $\mathcal{A} \subseteq \mathcal{P}$ literaaliesitys $lit(\mathcal{A}) = \mathcal{A} \cup \{\neg A \mid A \in \mathcal{P} - \mathcal{A}\}$.

Määritelmä. Klausuuli C on tosi totuusjakelussa $\mathcal{A} \subseteq \mathcal{P}$ (merkitään $\mathcal{A} \models C$), joss $C \cap lit(\mathcal{A}) \neq \emptyset$.

Määritelmä. Klausuulijoukko S on tosi totuusjakelussa $\mathcal{A}$ (merkitään $\mathcal{A} \models S$), joss kaikille klausuuleille $C \in S$ pätee $\mathcal{A} \models C$.

Määritelmä. Totuusjakelu $\mathcal{A} \subseteq \mathcal{P}$ on klausuulijoukon S malli, joss $\mathcal{A} \models S$.

Esimerkki. Tarkastellaan atomisten lauseiden joukkoon $\mathcal{P} = \{A, B, C, D, E\}$ perustuvia klausuuleita.

Olkoon $\mathcal{A} = \{A\}$, jolloin $lit(\mathcal{A}) = \{A, \neg B, \neg C, \neg D, \neg E\}$.

Nyt esimerkiksi

$$\begin{array}{lcl}
\mathcal{A} & \models & \{\{A, C, E\}, \{\neg A, \neg B\}\} \\
\mathcal{A} & \models & \emptyset \\
\mathcal{A} & \not\models & \{\{A, B\}, \{C\}\} \\
\mathcal{A} & \models & \{\neg A, B, \neg D\} \\
\mathcal{A} & \not\models & \{\neg A, D\} \\
\mathcal{A} & \not\models & \Box
\end{array}$$

Määritelmä. Klausuulijoukko S on *toteutuva* joss S:llä on ainakin yksi malli $\mathcal{A} \subseteq \mathcal{P}$. Muuten S on *toteutumaton*.

Esimerkki. Klausuulijoukot $\{\{A, C, E\}, \{\neg A, \neg B\}\}$ ja $\emptyset$ ovat toteutuvia, koska esimerkiksi $\mathcal{A} = \{A\}$ on näiden molempien malli.

Esimerkki. Klausuulijoukot $\{\{A\}, \{\neg A\}\}$ ja $\{\Box\}$ ovat toteutumattomia.

7.2 Resoluutiosääntö

Määritelmä. Olkoot $C_1 = \{l, l_1, \ldots, l_n\}$ ja $C_2 = \{\bar{l}, l'_1, \ldots, l'_m\}$ klausuuleja. Klausuuli $C = (C_1 \cup C_2) - \{l, \bar{l}\} = \{l_1, \ldots, l_n, l'_1, \ldots, l'_m\}$ on klausuulien C_1 ja C_2 *yhdistelmä*.

Esimerkki.

$$\{A, B, \neg C\} \qquad \{\neg A, D, \neg C\}$$

$$\{B, \neg C, D\}$$

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

Huomio. Resoluutiosääntöä saa soveltaa korkeintaan yhden literaaliparin (l ja $\bar{l}$) suhteen kerrallaan.

Esimerkki. Tarkastellaan klausuulijoukkoa $S = \{\{A, \neg B\}, \{\neg A, B\}\}$.

- Klausuuljoukosta voidaan johtaa resoluutiosäännöllä klausuulit $\{A, \neg A\}$ (literaali $l = B$) ja $\{B, \neg B\}$ (literaali $l = A$).
- Edelleen näistä ja joukon S klausuuleista voidaan johtaa resoluutiosäännöllä ainoastaan S:ään kuuluvia klausuuleita.
- Missään tapauksessa S:stä ei saada resoluutiosäännöllä tyhjää klausuulia $\Box$ (tämä tarkoittaisi, että S on toteutumaton).
- Huomaa, että S on toteutuva ($\mathcal{A} \models S$) totuusjakelussa $\mathcal{A} = \{A, B\}$.

7.3 Resoluutiotodistukset

Lähtökohtana klausuulijoukko S, jonka klausuuleihin sovelletaan resoluutiosääntöä.

Määritelmä. 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 yhdistelmä.

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

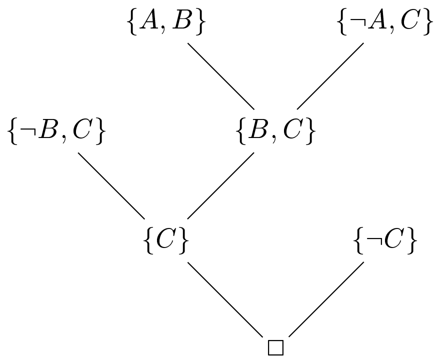
Ajatuksena on, että tällöin S joudutaan hylkäämään toteutuvana klausuulijoukkona.

Esimerkki. Tarkastellaan klausuulijoukkoa
$S = \{\{A, B\}, \{\neg A, C\}, \{\neg B, C\}, \{\neg C\}\}$,
jolle saadaan seuraava hylkäys:

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

Edellä esitetty resoluutiotodistus voidaan kirjoittaa myös puumuotoon.



Esimerkki. Klausuulijoukolle

$$S = \{\ \{A, B, \neg C, \neg D\}, \{\neg A, E\}, \{\neg B, \neg F\}, \{C, E\}, \{D, \neg F\}, \{\neg E\}, \{F\}\ \}$$

saadaan seuraava hylkäys:

1.	$\{A, B, \neg C, \neg D\}$	S
2.	$\{\neg A, E\}$	S
3.	$\{E, B, \neg C, \neg D\}$	1,2
4.	$\{\neg B, \neg F\}$	S
5.	$\{E, \neg F, \neg C, \neg D\}$	3,4
6.	$\{C, E\}$	S
7.	$\{E, \neg F, \neg D\}$	5,6
8.	$\{D, \neg F\}$	S
9.	$\{E, \neg F\}$	7,8
10.	$\{\neg E\}$	S
11.	$\{\neg F\}$	9,10
12.	$\{F\}$	S
13.	$\Box$	11, 12

7.4 Resoluution virheettömyys ja täydellisyys

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

Todistus. Suoraan sillä perusteella, että jos klausuulijoukolla S on malli $\mathcal{A} \subseteq \mathcal{P}$ ja C on kahden S:n klausuulin C_1 ja C_2 yhdistelmä, niin $\mathcal{A}$ on myös klausuulijoukon $S' = S \cup \{C\}$ malli.

$$\begin{aligned}
\text{Oletetaan } \mathcal{A} \not\models S \cup \{C\} \quad &\Longrightarrow \quad \mathcal{A} \not\models C \\
&\Longrightarrow \quad C \cap lit(\mathcal{A}) = \emptyset \\
&\Longrightarrow \quad C_1 \cap lit(\mathcal{A}) = \emptyset \text{ tai } C_2 \cap lit(\mathcal{A}) = \emptyset \\
&\Longrightarrow \quad \mathcal{A} \not\models C_1 \text{ tai } \mathcal{A} \not\models C_2 \\
&\Longrightarrow \quad \mathcal{A} \not\models S, \text{ ristiriita.}
\end{aligned}$$

Siis $\mathcal{A} \models S \cup \{C\}$.

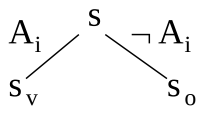
Väite. Jos S on toteutumaton, on S:llä refutaatio.

Todistus. Olkoon S atomisten lauseiden joukkoon $\mathcal{P} = \{A_1, \ldots, A_n\}$ perustuva klausuulijoukko.

Muodostetaan binääripuu seuraavasti. Olkoon s syvyydellä i $(0 \le i \le n)$ oleva puun solmu (juurisolmu on tasolla 0) ja L_s niiden literaalien joukko, jotka ovat juurisolmusta solmuun s johtavilla kaarilla.

Jos $\overline{C} \subseteq L_s$ jollekin klausuulille $C \subseteq S$, merkitään C solmuun s ja lopetetaan puun laajentaminen tästä solmusta eteenpäin.

Muussa tapauksessa: Jos $i < n$, merkitään solmulle s vasen lapsi s_v ja oikea lapsi s_o sekä merkitään kaarelle $s \to s_v$ literaali A_i ja kaarelle $s \to s_o$ literaali $\neg A_i$. Jos $i = n$, lopetetaan puun laajentaminen solmusta s eteenpäin.

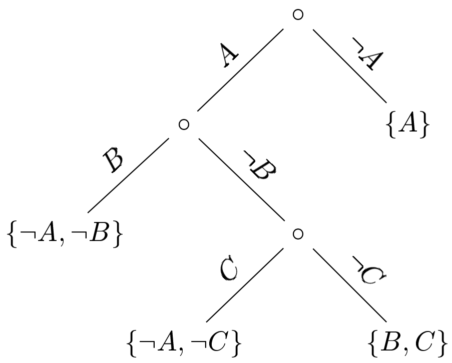


Todistamme muodostettavan binääripuun osalta seuraavaa:

Väite. Jos S on toteutumaton, niin valmiin binääripuun jokainen haara päättyy solmuun s, johon on merkitty klausuuli $C \in S$ siten, että $\overline{C} \subseteq L_s$.

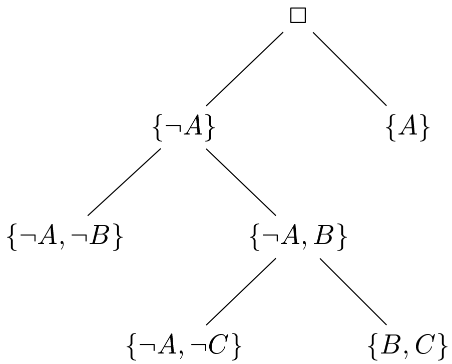
Vastaoletus. Valmiissa binääripuussa on solmu s tasolla n siten, että $\overline{C} \not\subseteq L_s$ pätee kaikille $C \in S$.
$\Longrightarrow L_s = lit(\mathcal{A})$ jollekin totuusjakelulle $\mathcal{A}$ ja $C \cap L_s \neq \emptyset$ kaikille $C \in S$.
$\Longrightarrow \mathcal{A} \models C$ kaikille $C \in S$.
$\Longrightarrow \mathcal{A} \models S$, eli S on toteutuva, ristiriita.

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



Lehtisolmuihin merkityt klausuulit ovat epätosia ko. totuusjakelussa.

Analyysin tuloksesta voidaan konstruoida S:lle hylkäys:



7.5 Resoluution käyttökohteita

Pätevyyden tutkiminen resoluutiolla

Väite. $\models \alpha \iff \neg\alpha$ on toteutumaton.

- Menettely: muutetaan lause $\neg\alpha$ konjunktiiviseen normaalimuotoon ja edelleen klausuulijoukoksi S.
- Tällöin S on toteutumaton
  $\iff$ $\neg\alpha$:n KNM on toteutumaton
  $\iff$ $\neg\alpha$ on toteutumaton
  $\iff$ α on pätevä.

Esimerkki. Onko $(A \rightarrow B) \wedge (\neg A \rightarrow C) \rightarrow B \vee C$ pätevä?

Lauseen negaation KNM on $(\neg A \vee B) \wedge (A \vee C) \wedge \neg B \wedge \neg C$.

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

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

Lause on siis pätevä.

Loogisen seuraavuuden tutkiminen resoluutiolla

Väite. $\Sigma \models \alpha \iff \Sigma \cup \{\neg\alpha\}$ on toteutumaton.

- Menettely: muutetaan lausejoukon $\Sigma \cup \{\neg\alpha\}$ lauseet konjunktiiviseen normaalimuotoon ja edelleen klausulijoukoksi S.
- Tällöin S on toteutumaton
  $\iff$ lausejoukon $\Sigma \cup \{\neg\alpha\}$ KMN:n joukko on toteutumaton
  $\iff$ lausejoukko $\Sigma \cup \{\neg\alpha\}$ on toteutumaton
  $\iff$ α on Σ:n looginen seuraus.

Esimerkki. Onko $\{\neg A \rightarrow B, B \vee C \rightarrow \neg B\} \models A$?

lause	KNM	klausuuleina
$\neg A$	$\neg A$	$\{\neg A\}$
$\neg A \rightarrow B$	$A \vee B$	$\{A, B\}$
$B \vee C \rightarrow \neg B$	$(\neg B \vee \neg B) \wedge (\neg C \vee \neg B)$	$\{\neg B\}, \{\neg B, \neg C\}$

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

Vastaus: lause A on lausejoukon looginen seuraus.

Esimerkki. Palataan hissiesimerkin spesifikaatioon ja osoitetaan ko. turvallisuusominaisuus resoluutiolla.

lause	KNM	klausuuleina	
$\neg K_1 \lor \neg K_2$	$\neg K_1 \lor \neg K_2$	1. $\{\neg K_1, \neg K_2\}$	
$A_1 \to K_1$	$\neg A_1 \lor K_1$	2. $\{\neg A_1, K_1\}$	
$A_2 \to K_2$	$\neg A_2 \lor K_2$	3. $\{\neg A_2, K_2\}$	
$\neg\neg(A_1 \land A_2)$	$A_1 \land A_2$	4. $\{A_1\}$, 5. $\{A_2\}$	
	Resoluutio:	6. $\{K_1\}$	2,4
		7. $\{K_2\}$	3,5
		8. $\{\neg K_2\}$	1,6
		9. $\square$	7,8

8 Laskennallisesta vaativuudesta

- Laskennan malli
- Keskeiset vaativuusluokat
- Redusoituvuus ja vaikeat ongelmat

8.1 Laskennan malli

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

Määritelmä. Deterministinen Turing-kone T on nelikkö $\langle A, S, s_0, t\rangle$, missä

- A on *aakkosto*, johon kuuluu aina erikoissymboli $\sqcup$ (tyhjä symboli).
- S on joukko tiloja, johon kuuluu aina annettu *alkutila* $s_0 \in S$ sekä erikoistilat k (kyllä), e (ei) ja p (pysähdy).
- $t : S \times A \to S \times A \times \{\leftarrow, \rightarrow, \downarrow\}$ on *tilansiirtofunktio*.

Huomio. Tyhjää merkkijonoa merkitään symbolilla ϵ.

Määritelmä. Turing-koneen T kokonaistilan määrää *konfiguraatio* $\langle s, v, w\rangle$, missä $s \in S$ on T:n tila ja $v \in A^*$ ja $w \in A^+$ ovat merkkijonoja. T käsittelee aina w:n ensimmäistä merkkiä.

- Laskenta alkaa konfiguraatiosta $\langle s_0, \epsilon, w\rangle$, missä merkkijono $w \in (A - \{\sqcup\})^*$ tai $w = \sqcup$ (T:n syöte).
- Yhdessä laskennan askeleessa siirrytään konfiguraatiosta $\langle s, v, aw\rangle$ tilansiirtofunktion t arvon $t(s,a) = \langle s', a', m\rangle$ perusteella uuteen konfiguraatioon seuraavasti:
  1. Jos $m = \downarrow$, uusi konfiguraatio on $\langle s', v, a'w\rangle$.
  2. Jos $m = \rightarrow$, uusi konfiguraatio on $\langle s', va', w'\rangle$, missä $w' = w$, jos $w \neq \epsilon$ ja $w' = \sqcup$, jos $w = \epsilon$.
  3. Jos $m = \leftarrow$ ja $v = v'b$ joillekin $v \in A^*$ ja $b \in A$, uusi konfiguraatio on $\langle s', v', ba'w\rangle$.
- Laskenta päättyy, jos $s' \in \{k, e, p\}$.

Määritelmä. Turing-koneen T laskenta on sekvenssi konfiguraatioita $\langle s_0, v_0, w_0 \rangle \xrightarrow{T} \ldots \xrightarrow{T} \langle s_{n-1}, v_{n-1}, w_{n-1} \rangle$ missä $s_{n-1} \in \{k, e, p\}$. Laskenta on hyväksyvä, jos $s_{n-1} = k$.

Esimerkki. Olkoon $A = \{0, 1, \sqcup\}$ ja $S = \{s_0, s_1, k, e, p\}$. Binääriluvun pariteetti voidaan tarkastaa seuraavalla Turing-koneella T:

S	A	$S \times A \times \{\rightarrow, \leftarrow, \downarrow\}$
s_0	0	$\langle s_0, 0, \rightarrow \rangle$
s_0	1	$\langle s_1, 1, \rightarrow \rangle$
s_0	$\sqcup$	$\langle k, \sqcup, \downarrow \rangle$
s_1	0	$\langle s_1, 0, \rightarrow \rangle$
s_1	1	$\langle s_0, 1, \rightarrow \rangle$
s_1	$\sqcup$	$\langle e, \sqcup, \downarrow \rangle$

Syötteellä 101 T suorittaa seuraavan laskennan:

$\langle s_0, \epsilon, 101 \rangle$
$\xrightarrow{T} \langle s_1, 1, 01 \rangle$
$\xrightarrow{T} \langle s_1, 10, 1 \rangle$
$\xrightarrow{T} \langle s_0, 101, \sqcup \rangle$
$\xrightarrow{T} \langle k, 101, \sqcup \rangle$

Epädeterministiset Turing-koneet

- Tilansiirtofunktio t korvataan tilansiirtorelaatiolla $t : S \times A \rightarrow 2^{S \times A \times \{\leftarrow, \rightarrow, \downarrow\}}$.
- Konfiguraatiossa $\langle s, v, aw \rangle$ valitaan epädeterministisesti $\langle s', a', m \rangle \in t(s, a)$ ja siirrytään tämän perusteella uuteen konfiguraatioon. Mahdollisia laskentoja voi olla useita.

Esimerkki. Olkoon $A = \{0, 1, \sqcup\}$ ja $S = \{s_0, k, e, p\}$. Määritellään epädeterministinen Turing-kone seuraavasti:

S	A	$2^{S \times A \times \{\leftarrow, \rightarrow, \downarrow\}}$
s_0	$\sqcup$	$\{\langle s_0, 0, \rightarrow \rangle, \langle s_0, 1, \rightarrow \rangle, \langle p, \sqcup, \downarrow \rangle\}$

Yksi mahdollinen laskenta: $\langle s_0, \epsilon, \sqcup \rangle \xrightarrow{T} \langle s_0, 1, \sqcup \rangle$
$\xrightarrow{T} \langle s_0, 10, \sqcup \rangle \xrightarrow{T} \langle s_0, 101, \sqcup \rangle \xrightarrow{T} \langle p, 101, \sqcup \rangle$

Määritelmä. Turing-kone T *hyväksyy* kielen $L \subseteq (A - \{\sqcup\})^*$, jos kaikille merkkijonoille $x \in (A - \{\sqcup\})^*$ pätee: T:llä on ainakin yksi hyväksyvä laskenta syötteellä $x \iff x \in L$.

Turing-koneiden käyttö ongelmien ratkaisemiseen

Konstruoidaan Turing-kone T siten, että T hyväksyy ongelman O ratkaisuja vastaavan kielen L:
T hyväksyy O:n merkkijonoesityksen $w \iff w$ on ongelman O ratkaisu.

Esimerkki. Lauselogiikan toteutuvuusongelmassa SAT:ssa on tarkoituksena selvittää onko annetulla lauseella $\phi \in \mathcal{L}$ malli.

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

8.2 Keskeiset vaativuusluokat

- Erilaisten ongelmien laskennallista vaativuutta voidaan analysoida asettamalla Turing-koneen laskentaresurssille rajoituksia.

  Keskeinen rajoitus: Turing-kone T pysähtyy polynomisessa ajassa syötteen pituuden suhteen $\iff$ on olemassa polynomi p siten, että kaikilla syötteillä $w \in (A - \{\sqcup\})^*$ koneen T laskenta käsittää korkeintaan $p(|w|)$ erilaista konfiguraatiota.
- Kaksi keskeistä ongelmien luokkaa ovat
  1. $\mathbf{P}$: ongelmat, jotka voidaan ratkaista polynomisessa ajassa *deterministisellä* Turing-koneella.
  2. $\mathbf{NP}$: ongelmat, jotka voidaan ratkaista polynomisessa ajassa *epädeterministisellä* Turing-konella.
- Luokka $\mathbf{P}$ on luokan $\mathbf{NP}$ aliluokka (ja mitä ilmeisimmin aito).

Väite. SAT kuuluu luokkaan $\mathbf{NP}$.

Todistuksen idea: voidaan konstruoida epädeterministinen Turing-kone T, joka

- valitsee epädeterministisesti totuusjakelun $\mathcal{A}$,
- laskee syötteenä ϕ annetun lauseen totuusarvon $\mathcal{A}$:ssa ja
- pysähtyy hyväksyvään tilaan, jos $\mathcal{A} \models \phi$ ja muutoin hylkäävään tilaan.

Tarvittava laskenta pystytään suorittamaan polynomisessa ajassa lauseen ϕ merkkijonoesityksen pituuden suhteen.

Voidaan osoittaa, että $\phi \in$ SAT $\iff$ koneella T on ainakin yksi hyväksyvä laskenta syötteellä ϕ.

8.3 Redusoituvuus ja vaikeat ongelmat

Määritelmä. Ongelma O on $\mathbf{C}$-vaikea, jos kaikki luokan $\mathbf{C}$ ongelmat voidaan redusoida O:ksi polynomisessa ajassa.

Ongelman O_1 *redusoituvuus* ongelmaksi O_2 edellyttää, että löytyy i:n pituuden suhteen polynomisessa ajassa deterministisellä Turing-koneella laskettava funktio $f : O_1 \rightarrow O_2$ siten, että $i \in O_1 \iff f(i) \in O_2$.

Määritelmä. Ongelma O on $\mathbf{C}$-täydellinen, jos O kuuluu luokkaan $\mathbf{C}$ ja O on $\mathbf{C}$-vaikea.

$\Longrightarrow$ $\mathbf{C}$-täydelliset ongelmat ovat vaativimpia luokan $\mathbf{C}$ ongelmia.

Väite. SAT on $\mathbf{NP}$-kova (Cook, 1971).

Todistuksen idea. Jokaiselle epädeterministiselle Turing-koneelle T, merkkijonolle $w \in (A - \{\sqcup\})^*$ ja polynomille p on olemassa lausejoukko Σ s.e.

- koneella T on syötteellä w ainakin yksi hyväksyvä laskenta, jonka pituus on pienempi kuin $p(|w|)$ $\iff$ lausejoukko Σ on toteutuva.

Huomioita.

- Näin ollen Turing-koneen laskenta voidaan palauttaa polynomisessa ajassa SAT-ongelman ratkaisemiseen.
- SAT on $\mathbf{NP}$-täydellinen ongelma.
- Pahimmassa tapauksessa SAT- ongelman ratkaisu vaatii eksponentiaalisen ajan lauseen pituuteen nähden.

Tehokas algoritmi: Davis-Putnam [1960]