



## LAUSELOGIikka

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

### 1.1 Lauselogiikan aakkosto

- atomiset lauseet:  $A, A_1, A_2, \dots, B, B_1, \dots, C, \dots$
- 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*, koska niiden avulla kytketään yksinkertaisempia lausekkeitä (lauseita) monimutkaisemmiksi.



## 1 Lauselogiikan kieli

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

### 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  $\alpha$  ja  $\beta$  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  $\mathcal{L}$ .



## Vaihtehtoinen määritelmä

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

**Määritelmä.** Atomisten lauseiden joukkoon  $\mathcal{P}$  perustuva *lauselogiikan kieli*  $\mathcal{L}$  on merkkijonojen joukon  $(\mathcal{P} \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (, )\})^*$  *pienin* osajoukko, joka on suljettu seuraavien vaatimusten suhteen:

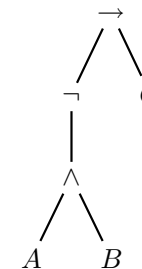
1. Jos  $A \in \mathcal{P}$ , niin  $A \in \mathcal{L}$ .
2. Jos  $\alpha \in \mathcal{L}$  ja  $\beta \in \mathcal{L}$ , niin  $(\neg\alpha) \in \mathcal{L}$ ,  $(\alpha \vee \beta) \in \mathcal{L}$ ,  $(\alpha \wedge \beta) \in \mathcal{L}$ ,  $(\alpha \rightarrow \beta) \in \mathcal{L}$  ja  $(\alpha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

**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. Sen sijaan merkkijonot  $(\neg())$  ja  $(A \vee C)$  eivät ole  $\mathcal{L}$ :n lauseita.

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

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

Vastaavasti määritellään lauseet, jotka ovat *negatioita*, *konjunktioita*, *disjunktioita* ja *ekvivalensseja*.



Lauseiden ominaisuuksia voidaan todistaa induktiolla lauserakenteen suhteen (tai lauseita vastaavien jäsenyspuiden rakenteen suhteen).



Jokaisella lauselogiikan lauseella on yksikäsitteinen *jäsenyspuu*.

**Määritelmä.** Määritellään jäsenyspuut lauserakenteen mukaisesti:

1. Atomisen lauseen  $A \in \mathcal{P}$  jäsenyspuu  $JP(A)$  on alla vasemmalla.
2. Negaation  $(\neg\alpha)$  jäsenyspuu  $JP(\neg\alpha)$  on annettu keskellä.
3. Jos  $*$  on jokin lauselogiikan binäärikonnektiiveista, lauseen  $(\alpha * \beta)$  jäsenyspuu  $JP(\alpha * \beta)$  on annettu oikealla.



Yllä  $JP(\alpha)$  ja  $JP(\beta)$  ovat lauseiden  $\alpha$  ja  $\beta$  rekursiivisesti määräytyvät jäsenyspuut, jotka sijoitetaan kyseisten jäsenyspuiden *alipuiksi*.

## 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 järjestelmän määrittely suoraan logiikan lausein. Tällöin

- valitaan sopiva joukko järjestelmän ominaisuuksia kuvaavia atomisia lauseita ja
- määritellään näiden väliset suhteet/riippuvuudet 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:  $(A \rightarrow (B \vee C))$ .

## 1.4 Sopimukset sulkeiden käytöstä

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

Esimerkiksi:  $\neg A \rightarrow B$  eikä  $(\neg A) \rightarrow B$ ,

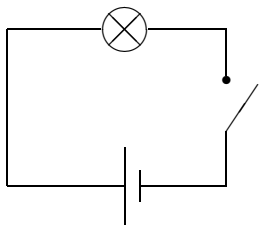
$A \wedge B \rightarrow B \vee C$  eikä  $(A \wedge B) \rightarrow (B \vee C)$ ,

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

- Poikkeuksena ketjudisjunktioit/konjunktioit: kirjoitetaan  $A \vee B \vee C$  lauseiden  $A \vee (B \vee C)$  ja  $(A \vee B) \vee C$  sijaan.



**Esimerkki.** Kuvataan seuraavaa yksinkertaista järjestelmää lauselogiikan lausein.



Valitaan atomisiksi lauseiksi

$L$  = "Lamppu palaa",

$K$  = "Kytкин on suljettu" ja

$P$  = "Paristossa on riittävästi varausta".

Määritellään järjestelmän sallitut tilat lauseilla

$((\neg P) \rightarrow (\neg L))$  ja

$(P \rightarrow (L \leftrightarrow K))$ .

Tulkitse nämä kaksi lausetta luonnolliselle kielelle!

## Lisähuomioita sulkeiden käytöstä

- Edellä tehdyt sopimukset (ketjukonjunktioita ja -disjunktioita lukuunottamatta) takaavat, että lauseen  $\phi$  jäsenyspuu säilyy yksikäsitteisenä sulkeita vähennettäessä.
- Esimerkiksi merkkijonoa  $A \rightarrow B \rightarrow C$  ei pystytä jäsentämään lauseeksi (yksikäsitteisesti).  
Tarvitaan sulkeet:  $A \rightarrow (B \rightarrow C)$  tai  $(A \rightarrow B) \rightarrow C$ .  
Näillä lauseilla on yksikäsitteiset jäsenyspuut.
- Ketjudisjunktioikin  $A \vee B \vee C$  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 jäsenys suoritetaan.



## 1.5 Esimerkki: rakenteinen induktio

**Määritelmä.** Lauseen *alilauseet* määräytyvät seuraavasti:

Atomisen lauseen  $A$  ainoa alilause on  $A$ .

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

Lauseen  $(\alpha \wedge \beta)$  alilauseita ovat  $\alpha$ :n ja  $\beta$ :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  $A \rightarrow B \vee C$ .

*Todistus.*

**Perustapaus:**  $\phi$  on atominen lause  $A$ .

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

**Induktioaskel:**  $\phi$  on muotoa  $(\neg\alpha)$ .

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

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

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

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



**Väite.** Lauseen  $\phi$  alilauseita on korkeintaan niin monta kuin on  $\phi$ :ssä esiintyvien atomisten lauseiden lukumäärän ja  $\phi$ :n konnektiivien lukumäärän summa.

Todistetaan väite induktiolla lauserakenteen suhteen.

Otetaan lauseelle  $\phi$  käyttöön seuraavat merkinnät:

- $\#\phi$ : lauseen  $\phi$  alilauseiden lukumäärä,
- $A\phi$ : lauseessa  $\phi$  esiintyvien atomisten lauseiden lukumäärä ja
- $K\phi$ : lauseen  $\phi$  konnektiivien lukumäärä.

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

**Esimerkki.** Väittämä pitää paikkansa ainakin lauseen  $\phi = (B \rightarrow C) \rightarrow (B \rightarrow C)$  tapauksessa:  $\#\phi = 4$ ,  $A\phi = 2$  ja  $K\phi = 3$ .

**Induktioaskel jatkuu:**  $\phi$  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  $\alpha$  ja  $\beta$  yhteisten alilauseiden lukumäärää ja  $A(\alpha, \beta)$  lauseiden  $\alpha$  ja  $\beta$  yhteisten atomisten lauseiden lukumäärää. Tällöin pätee  $A(\alpha, \beta) \leq \#(\alpha, \beta)$ .

Näin ollen väittämä tuli todistetuksi kaikille lauseille  $\phi$ .



## 2 Lauselogiikan semantiikka

- Perustotuustaulukot
- Konnektiivien keskinäisestä määriteltävyydestä
- Lauselogiikan totuusmääritelmä
- Vaihtoehtoinen totuusmääritelmä: valuaatiot

**Huomio.** Disjunktio ( $\alpha \vee \beta$ ) on tosi  $\iff \alpha$  on tosi **tai**  $\beta$  on tosi.  
 Disjunktio ( $\alpha \vee \beta$ ) on siis tosi myös silloin, kun sekä  $\alpha$  että  $\beta$  ovat tosia.  
 Voidaan määritellä myös poissulkeva disjunktio ( $\alpha \underline{\vee} \beta$ ), joka on epätosi molempien disjunktien ollessa tosia.

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

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



### 2.1 Perustotuustaulukot

Perustotuustaulukoilla määritellään eri muotoa olevien lauseiden totuusarvot alilauseidensa funktiona.

$\alpha$	$(\neg\alpha)$	$\alpha$	$\beta$	$(\alpha \wedge \beta)$	$\alpha$	$\beta$	$(\alpha \vee \beta)$
$T$	$E$	$T$	$T$	$T$	$T$	$T$	$T$
$E$	$T$	$T$	$E$	$E$	$T$	$E$	$T$
		$E$	$T$	$E$	$E$	$T$	$T$
		$E$	$E$	$E$	$E$	$E$	$E$

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

### Perustotuustaulukot (jatkoa)

$\alpha$	$\beta$	$(\alpha \rightarrow \beta)$	$\alpha$	$\beta$	$(\alpha \leftrightarrow \beta)$
$T$	$T$	$T$	$T$	$T$	$T$
$T$	$E$	$E$	$T$	$E$	$E$
$E$	$T$	$T$	$E$	$T$	$E$
$E$	$E$	$T$	$E$	$E$	$T$

$(\alpha \rightarrow \beta)$  on tosi  $\iff \alpha$  on epätosi **tai**  $\beta$  on tosi  
 $\iff$  **jos**  $\alpha$  on tosi, **niin**  $\beta$  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  $\phi$  on korkeintaan niin monta alilauseetta kuin lauseessa  $\phi$  on atomisia lauseita ja konnektiiveja!

## Konnektiivien tyypillisiä määritelmiä

Konnektiiveja voidaan määritellä toistensa avulla esim. seuraavasti:

- $(\alpha \wedge \beta)$  lauseena  $\neg(\neg\alpha \vee \neg\beta)$
- $(\alpha \vee \beta)$  lauseena  $\neg(\neg\alpha \wedge \neg\beta)$
- $(\alpha \underline{\vee} \beta)$  lauseena  $(\alpha \leftrightarrow \neg\beta)$  tai lauseena  $\neg(\alpha \leftrightarrow \beta)$
- $(\alpha \rightarrow \beta)$  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  $((\neg\alpha \vee \beta) \wedge (\alpha \vee \neg\beta))$

$\implies$  Kaikkia peruskonnektiiveista  $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$  ei välttämättä tarvita.



## 2.2 Konnektiivien keskinäisestä määriteltävyydestä

**Esimerkki.** Tarkastellaan lauseille  $(\alpha \wedge \beta)$  ja  $\neg(\neg\alpha \vee \neg\beta)$  muodostettua yhteistä totuustaulukkoa.

$\alpha$	$\beta$	$\alpha \wedge \beta$	$\neg\alpha$	$\neg\beta$	$\neg\alpha \vee \neg\beta$	$\neg(\neg\alpha \vee \neg\beta)$
$T$	$T$	$T$	$E$	$E$	$E$	$T$
$T$	$E$	$E$	$E$	$T$	$T$	$E$
$E$	$T$	$E$	$T$	$E$	$T$	$E$
$E$	$E$	$E$	$T$	$T$	$T$	$E$

Koska lauseiden  $\alpha \wedge \beta$  ja  $\neg(\neg\alpha \vee \neg\beta)$  sarakkeissa on identtiset totuusarvot, lauseet ovat semantiikan kannalta samaistettavissa.

$\implies$  Lause  $\alpha \wedge \beta$  voidaan (tarvittaessa) määritellä syntaktisena lyhennysmerkintänä lauseelle  $\neg(\neg\alpha \vee \neg\beta)$ .

## Konnektiivien riittävyys

Tarvittaessa voidaan rajoittua seuraaviin konnektiiveihin:

- $\neg$  ja  $\vee$  riittävät muiden konnektiivien ( $\wedge, \rightarrow, \leftrightarrow, \underline{\vee}$ ) määrittelemiseen,
- $\neg$  ja  $\wedge$  riittävät myös,
- $\neg$  ja  $\rightarrow$  riittävät myös ja
- $\perp$  (aina epätosi lause) ja  $\rightarrow$  riittävät myös.

**Huomio.** Toistaiseksi käsitellyt konnektiivit eivät ole ainoat mahdolliset.

Esimerkiksi *binäärikonnektiiveja* \*, jotka kytkevät kaksi lausetta  $\alpha$  ja  $\beta$  lauseeksi  $\alpha * \beta$ , voidaan olennaisesti määritellä  $2^{(2 \times 2)} = 16$  erilaista.



## Yksittäisten konnektiivien riittävyys/riittämättömyys

**Huomio.** On myös konnektiiveja, jotka riittävät yksinään muiden määrittelemiseen:

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

**Esimerkki.** Implikaatio ei riitä yksinään muiden konnektiivien kuten esimerkiksi negaation määrittelemiseen.

Tarkastellaan lauseita  $\phi$ , jotka on muodostettu käyttäen ainoastaan konnektiivia  $\rightarrow$ , atomista lausetta  $A$  ja sulkeita aakkosina.

Voidaan osoittaa rakenteisella induktiolla, että lauseen  $\phi$  totuustaulun sarake on identtinen joko lauseen  $A$  tai lauseen  $A \vee \neg A$  kanssa.

Näinollen mikään lauseista  $\phi$  ei voi ilmaista lausetta  $\neg A$ .

Totuusjaku voidaan ymmärtää yhden *asiintilan* 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 asiintila.



## 2.3 Lauselogiikan totuusmääritelmä

**Määritelmä.** *Totuusjaku*  $\mathcal{A}$  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 totuusjakuja on  $2^{|\mathcal{P}|}$  kappaletta.
- Jokainen totuusjaku vastaa yhtä totuustaulukon riviä (ja kääntäen).

**Määritelmä.** Seuraavassa määritellään milloin mielivaltainen lause  $\phi \in \mathcal{L}$  on *tosi* totuusjakuksella  $\mathcal{A}$  (merk.  $\mathcal{A} \models \phi$ ) ja milloin  $\phi$  on *epätosi* totuusjakuksella  $\mathcal{A}$  (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.  $\mathcal{A} \models \alpha \wedge \beta \iff \mathcal{A} \models \alpha$  ja  $\mathcal{A} \models \beta$ .

4.  $\mathcal{A} \models \alpha \vee \beta \iff \mathcal{A} \models \alpha$  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  $\mathcal{A} \not\models \beta$ .

**Huomio.** Esim. kohdan 3 nojalla  $\mathcal{A} \not\models \alpha \wedge \beta \iff \mathcal{A} \not\models \alpha$  tai  $\mathcal{A} \not\models \beta$ .



**Esimerkki.** Olkoon  $\mathcal{A} = \emptyset$  totuusjakelu. Totuusmääritelmän nojalla:

$$\mathcal{A} \not\models A, \mathcal{A} \not\models B, \mathcal{A} \models \neg B, \mathcal{A} \models A \rightarrow B \text{ ja } \mathcal{A} \models \neg B \wedge (A \rightarrow B).$$

Vertaa tätä laskelmaa kalvon 21 totuustaulukon viimeiseen riviin.

### 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  $\text{At}(\phi)$ :llä  $\phi$ :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  $\mathcal{A}_1 \cap \text{At}(\phi) = \mathcal{A}_2 \cap \text{At}(\phi)$ , niin  $\mathcal{A}_1 \models \phi \iff \mathcal{A}_2 \models \phi$ .

Nämä voidaan todistaa induktiolla  $\phi$ :n rakenteen suhteen.

## 3 Semanttiset peruskäsitteet

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



## 2.4 Vaihtoehtoinen totuusmääritelmä: valuaatiot

(Tätä määritelmää käytetään Neroden ja Shoren kirjassa).

**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  $\mathcal{A} = \{A \in \mathcal{P} \mid \mathcal{V}(A) = T\}$ .

## 3.1 Mallin käsite

**Määritelmä.** Totuusjakelu  $\mathcal{A} \subseteq \mathcal{P}$  on lauseen  $\alpha \in \mathcal{L}$  *malli*, joss lause  $\alpha$  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  $\Sigma$  lauseille  $\sigma \in \Sigma$  pätee  $\mathcal{A} \models \sigma$ . Näin ollen lausejoukon  $\Sigma$  lauseet tulkitaan konjunktiiivisesti.





**Esimerkki.** Olkoon  $\mathcal{P} = \{P, L, K\}$ . Laaditaan lampuesimerkin lausejoukko  $\Sigma = \{\neg P \rightarrow \neg L, P \rightarrow (L \leftrightarrow K)\} \subseteq \mathcal{L}$  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	<u>T</u>	T	<u>T</u>
T	T	E	E	E	T	E	E
T	E	T	E	T	T	E	E
T	E	E	E	T	<u>T</u>	T	<u>T</u>
E	T	T	T	E	E	T	T
E	T	E	T	E	E	E	T
E	E	T	T	T	<u>T</u>	E	<u>T</u>
E	E	E	T	T	<u>T</u>	T	<u>T</u>

Malleja on siis neljä erilaista vastaten järjestelmän sallittuja tiloja.

### Toteutuvuuden tutkiminen totuustaulukolla:

- muodostetaan  $\alpha$ :lle ( $\Sigma$ :lle) totuustaulukko ja
- tarkastetaan onko  $\alpha$  tosi (kaikki  $\Sigma$ :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	<u>T</u>
T	E	T	<u>T</u>
E	T	E	E
E	E	T	<u>T</u>

Kyllä.



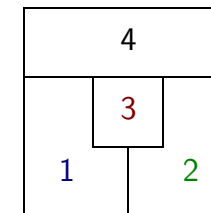
## 3.2 Toteutuvuus

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

**Huomio.** Koska lauseiden totuusarvot määräytyvät niissä esiintyvien atomisten lauseiden totuusarvoista, voimme rajoittua totuusjakeluihin  $\mathcal{A} \subseteq \text{At}(\phi)$ , missä  $\text{At}(\phi)$  on lauseessa  $\phi$  esiintyvien atomisten lauseiden joukko, tai totuusjakeluihin  $\mathcal{A} \subseteq \text{At}(\Sigma) = \cup\{\text{At}(\sigma) \mid \sigma \in \Sigma\}$  selvittäessämme lauseen  $\phi$  tai lausejoukon  $\Sigma$  malleja.

- *Toteutumattomalla* lauseella/lausejoukolla ei ole yhtään mallia.
- Lauseen toteutuvuuden selvittäminen on yksi keskeisimmistä logiikkaan liittyvistä laskennallisista ongelmista.

**Esimerkki.** (Rajoiteohjelmointi) Tarkastellaan oheisen kuvan mukaisen kartan värittämistä kolmella eri värillä siten, että vierekkäisillä alueilla on eri värit. Oheiset lauseet kuvaavat kolmiväristystä vastaavat rajoitteet.



Jokaiselle alueelle  $i$  värin valitsevat lauseet:

$$P_i \vee V_i \vee S_i,$$

$$\neg(P_i \wedge V_i), \neg(V_i \wedge S_i) \text{ ja } \neg(S_i \wedge P_i).$$

Jokaiselle alueparille  $\langle i, j \rangle$  ( $i < j$ ) rajoitteet:

$$\neg(P_i \wedge P_j), \neg(V_i \wedge V_j) \text{ ja } \neg(S_i \wedge S_j).$$

Totuusarvojakelua (mallikandidaatteja) on yhteensä  $2^{12} = 4096$  kpl!

Toisaalta alueet voidaan värittää  $3^4 = 81$  eri tavalla.

Tämä lausejoukko on toteutumaton  $\implies$  *kolmiväristys on mahdoton*.

Muistanet, että neljä väriä riittää aina tasograafin värittämiseen.



### 3.3 Pätevyys

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

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

#### Vastamallit

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

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

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

### 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  $\Sigma$  malleille  $\mathcal{A} \subseteq \mathcal{P}$ .

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

1. Jos  $\mathcal{A} \models \{A\}$ , niin välttämättä  $\mathcal{A} \models A$ , jolloin myös  $\mathcal{A} \models \neg\neg A$ .
2. Ei löydy totuusjakelua  $\mathcal{A}$  siten, että  $\mathcal{A} \models \{A \wedge \neg A\}$ .

Käytämme *vastamallin* käsitettä myös loogisen seuraavuuden yhteydessä.

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

**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  $\mathcal{A} \not\models \neg\neg B$ .



#### Pätevyyden tutkiminen totuustaulukolla:

- muodostetaan  $\alpha$ :lle totuustaulukko ja
- tarkistetaan, että  $\alpha$  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	E
E	E	E	T

Ei.

#### Loogisen seuraavuuden tutkiminen totuustaulukolla:

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

**Esimerkki.** Todetaan  $\{A, (A \rightarrow D)\} \models D$  ja  $\{(A \rightarrow B)\} \not\models B$  vastaavista totuustaulukoista:

A	D	$(A \rightarrow D)$		A	B	$(A \rightarrow B)$	
T	T	T	←	T	T	T	←
T	E	E		T	E	E	
E	T	T		E	T	T	←
E	E	T		E	E	T	←



**Huomio.** Kaikille lausejoukoille  $\Sigma$  pätee  $\Sigma \models A \vee \neg A$ .

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

P	L	K	$\neg P$	$\neg L$	$\neg P \rightarrow \neg L$	$L \leftrightarrow K$	$P \rightarrow (L \leftrightarrow K)$	$\neg L \vee K$
T	T	T	E	E	T	T	T	T
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	T
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	T
E	E	E	T	T	T	T	T	T

### Lauseiden loogisen ekvivalenssin selvittäminen:

- muodostetaan lauseille  $\alpha$  ja  $\beta$  yhteinen totuustaulukko ja
- tarkastetaan, että  $\alpha$ :lla ja  $\beta$ :lla on sama totuusarvo jokaisella rivillä.

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

A	B	$\neg A$	$\neg B$	$A \rightarrow B$	$\neg B \rightarrow \neg A$
T	T	E	E	T	T
T	E	E	T	E	E
E	T	T	E	T	T
E	E	T	T	T	T

Kyllä.



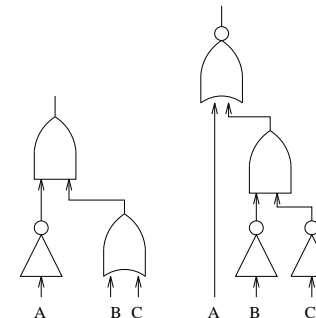
## 3.5 Looginen ekvivalenssi

**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 totuusjakeleuille  $\mathcal{A} \subseteq \mathcal{P}$ .

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

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

**Esimerkki.** Palataan johdannon esimerkkiin, jossa ongelmana oli selvittää laskevatko seuraavat kombinatoriset piirit samat funktiot:



Piirit voidaan esittää lauselogiikalla seuraavina lauseina

$$\phi = \neg A \wedge (B \vee C) \text{ ja } \psi = \neg(A \vee (\neg B \wedge \neg C)).$$



**Esimerkki.** Ratkaistaan ongelma osoittamalla, että piirejä vastaavat lauseet ovat loogisesti ekvivalentit.

A	B	C	$\neg A$	$\neg B$	$\neg C$	$B \vee C$	$\phi$	$\neg B \wedge \neg C$	$A \vee (\neg B \wedge \neg C)$	$\psi$
T	T	T	E	E	E	T	E	E	T	E
T	T	E	E	E	T	T	E	E	T	E
T	E	T	E	T	E	T	E	E	T	E
T	E	E	E	T	T	E	E	T	T	E
E	T	T	T	E	E	T	T	E	E	T
E	T	E	T	E	T	T	T	E	E	T
E	E	T	T	T	E	T	T	E	E	T
E	E	E	T	T	T	E	E	T	T	E

Koska lauseita  $\phi$  ja  $\psi$  vastaavat sarakkeet ovat identtiset, ne ovat loogisesti ekvivalentit. Tästä seuraa, että piirit laskevat samat funktiot.

**Esimerkki.** Kirjoitetaan lamppeesimerkin järjestelmälle vaihtoehtoinen määritelmä  $\Sigma' = \{L \rightarrow P, P \wedge L \rightarrow K, P \wedge K \rightarrow L\}$ .

P	L	K	$L \rightarrow P$	$P \wedge L$	$P \wedge L \rightarrow K$	$P \wedge K$	$P \wedge K \rightarrow L$
T	T	T	T	T	T	T	T
T	T	E	T	T	E	E	T
T	E	T	T	E	T	T	E
T	E	E	T	E	T	E	T
E	T	T	E	E	T	E	T
E	T	E	E	E	T	E	T
E	E	T	T	E	T	E	T
E	E	E	T	E	T	E	T

$\Rightarrow \Sigma' \equiv \Sigma$ , koska mallit ovat samat kuin alkuperäisellä määritelmällä  $\Sigma$ .



**Määritelmä.** Lausejoukot  $\Sigma_1 \subseteq \mathcal{L}$  ja  $\Sigma_2 \subseteq \mathcal{L}$  ovat *loogisesti ekvivalentit* (merk.  $\Sigma_1 \equiv \Sigma_2$ ), joss kaikille totuusjakeleille  $\mathcal{A} \subseteq \mathcal{P}$  pätee seuraavaa:

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

**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 loogisen ekvivalenssin selvittäminen:** *joko*

- todetaan, että  $\mathcal{A} \models \Sigma_2$  kaikille lausejoukon  $\Sigma_1$  malleille  $\mathcal{A}$  ja
- todetaan, että  $\mathcal{A} \models \Sigma_1$  kaikille lausejoukon  $\Sigma_2$  malleille  $\mathcal{A}$ ,

*tai vaihtoehtoisesti*

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

### 3.6 Peruskäsitteiden väliset yhteydet

Olkoon  $\mathcal{L}$  atomisten lauseiden joukkoon  $\mathcal{P}$  perustuva kieli.

Tarkastellaan jatkossa tämän kielen lauseita.

Looginen ekvivalenssi liittyy läheisesti pätevytyteen:

$$\alpha \equiv \beta \iff \models \alpha \leftrightarrow \beta.$$

*Todistus.*

$$\alpha \not\equiv \beta$$

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

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

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



Pätevydellä ja loogisella seuraavuudella on kiinteät yhteydet.

- $\models \alpha \iff \emptyset \models \alpha$ .  
Seuraa helposti, koska kaikki totuusjaketut  $\mathcal{A} \subseteq \mathcal{P}$  ovat tyhjän lausejoukon  $\emptyset$  malleja.
- $\{\phi_1, \dots, \phi_n\} \models \phi \iff \models \phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi$ .

*Todistus.*

$$\begin{aligned} \{\phi_1, \dots, \phi_n\} \not\models \phi & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \mathcal{A} \text{ on } \{\phi_1, \dots, \phi_n\}\text{:n malli ja } \mathcal{A} \not\models \phi \\ & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \forall i \in \{1, \dots, n\} : \mathcal{A} \models \phi_i \text{ ja } \mathcal{A} \not\models \phi \\ & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \mathcal{A} \models \phi_1 \wedge \dots \wedge \phi_n \text{ ja } \mathcal{A} \not\models \phi \\ & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \mathcal{A} \not\models \phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi \\ & \iff \not\models \phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi. \end{aligned}$$

### 3.7 Loogisten seurausten ominaisuuksia

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

*Todistus.* Sivuutetaan.

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

Loogisten seurausten joukolla  $\text{Cn}(\Sigma)$  on seuraavat perusominaisuudet:

- $\Sigma \subseteq \text{Cn}(\Sigma)$ .
- Monotonisuus:  $\Sigma_1 \subseteq \Sigma_2 \implies \text{Cn}(\Sigma_1) \subseteq \text{Cn}(\Sigma_2)$ .
- $\text{Cn}(\text{Cn}(\Sigma)) = \text{Cn}(\Sigma)$ .
- $\Sigma \equiv \text{Cn}(\Sigma)$ .



Pätevyyden ja loogisen seuraavuuden yhteys toteutuvuuteen:

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

*Todistus.*

$$\begin{aligned} \Sigma \not\models \alpha & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \mathcal{A} \models \Sigma \text{ ja } \mathcal{A} \not\models \alpha \\ & \iff \exists \mathcal{A} \subseteq \mathcal{P} \text{ s.e. } \mathcal{A} \models \Sigma \cup \{\neg \alpha\} \\ & \iff \Sigma \cup \{\neg \alpha\} \text{ on toteutuva} \\ & \iff \Sigma \cup \{\neg \alpha\} \text{ ei ole toteutumaton.} \end{aligned}$$

Edellä esitetyt yhteydet mahdollistavat lauselogiikan päättelyongelmien väliset muunnokset. Esim. loogisen ekvivalenssin, pätevyden ja loogisen seuraavuuden tutkiminen voidaan palauttaa toteutuvuuden tutkimiseen.

### Lisähuomioita loogisesta seuraavuudesta

- Jos  $\Sigma \models \phi$ , niin  $\text{Cn}(\Sigma) = \text{Cn}(\Sigma \cup \{\phi\})$ .  
Jos tavoitteena on lausejoukon koon minimointi, lausejoukon loogisia seurauksia ei siis kannata lisätä lausejoukkoon!
- Oletetaan, että  $\Sigma \not\models \phi$  ja että lausejoukko  $\Sigma$  halutaan laajentaa lausejoukoksi  $\Sigma'$  siten, että  $\Sigma \subseteq \Sigma'$  ja  $\Sigma' \models \phi$ .  
Apuna voidaan käyttää vastamallia/vastamalleja  $\mathcal{A}$ , joille  $\mathcal{A} \models \Sigma$  ja  $\mathcal{A} \not\models \phi$ : lausejoukkoon  $\Sigma$  lisättävän lauseen  $\psi$  tulisi sulkea pois vastamalli/vastamalleja  $\mathcal{A}$ , ts.  $\mathcal{A} \not\models \psi$ .  
Lause  $\phi$  toteuttaa myös tämän vaatimuksen, mutta lausetta  $\phi$  ei välttämättä haluta liittää eksplisiittiseen tietämykseen.

**Esimerkki.** Lamppuesimerkissä  $\Sigma = \{P \wedge L \rightarrow K, P \wedge K \rightarrow L\}$ , lause  $\phi = \neg L \vee K$ , vastamalli  $\mathcal{A} = \{L\}$  ja lisättävä lause  $\psi = L \rightarrow P$ .



### 3.8 Tietämyksen esittämisestä

- Jokainen lausejoukko  $\Sigma$  määrittää joukon *malleja*, eli totuusjakoja  $\mathcal{A}$ , joissa lausejoukon kaikki lauseet ovat tosia.

**Esimerkki.** Lamppuesimerkin lausejoukolla

$$\Sigma = \{\neg P \rightarrow \neg L, P \rightarrow (L \leftrightarrow K)\} \subseteq \mathcal{L}$$

on mallit  $\mathcal{A}_1 = \{P, L, K\}$ ,  $\mathcal{A}_2 = \{P\}$ ,  $\mathcal{A}_3 = \{K\}$  ja  $\mathcal{A}_4 = \{\}$ .

- Lausejoukon  $\Sigma$  mallit puolestaan määräävät lausejoukon loogisten seurausten joukon  $\text{Cn}(\Sigma)$ .

**Esimerkki.** Lamppuesimerkissä lausejoukon  $\Sigma$  loogisten seurausten joukko on  $\text{Cn}(\Sigma) = \{\neg L \vee K, L \rightarrow P \wedge K, \neg P \vee P, \dots\}$ .

- Atomisten lauseiden joukkoon  $\mathcal{P}$  perustuvia lausejoukkoja  $\Sigma \subseteq \mathcal{L}$  voidaan olennaisesti määrittellä  $2^{2^{|\mathcal{P}|}}$  erilaista.

## 4 Semanttinen taulu

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



*Tietämyksen esittäminen:* ongelmana rajata mallien joukko sopivat lauseet valitsemalla siten, että saadaan halutut loogiset seuraukset.

- Lähtökohtana olevan tyhjän lausejoukon  $\emptyset$  malleja ovat kaikki totuusjakolet. Täten  $\text{Cn}(\emptyset)$  on itse asiassa pätevien lauseiden joukko.
- Lauseiden lisääminen karsii mahdollisesti mallien joukkoa ja kasvattaa loogisten seurausten joukkoa (*monotonisuus*).
- Toisessa ääripäässä lausejoukko  $\Sigma$  voi tulla *ristiriitaiseksi*, jolloin sillä ei ole yhtään mallia ja kaikki lauseet ovat tällöin lausejoukon loogisia seurauksia (eli  $\text{Cn}(\Sigma) = \mathcal{L}$ ).

**Huomio.** Kaikille lausejoukoille  $\Sigma$  pätee  $\text{Cn}(\emptyset) \subseteq \text{Cn}(\Sigma)$ .

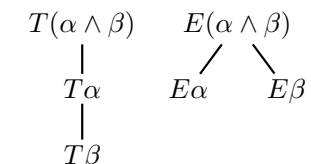
**Esimerkki.** Lamppuesimerkissä  $\Sigma \not\models L \leftrightarrow K$ , mutta lauseen  $P$  lisäämisestä seuraa  $\Sigma \cup \{P\} \models L \leftrightarrow K$ . Sen sijaan lausejoukko  $\Sigma \cup \{K \leftrightarrow \neg P, L\}$  on ristiriitainen/toteutumaton.

### 4.1 Konnektiivikohtaiset taulusäännöt

- Totuustaulukkoja käytetään lauseen  $\phi$  totuusarvon laskemiseen, kun annettuna on atomisten lauseiden  $A \in \text{At}(\phi)$  totuusarvot.
- Semanttisissa tauluissa idea on käänteinen: määrätään lauseen  $\phi$  alilauseiden (ja lopulta atomisten lauseiden  $A \in \text{At}(\phi)$ ) totuusarvoja lähtien liikkeelle lauseen  $\phi$  totuusarvosta (tosi tai epätosi).

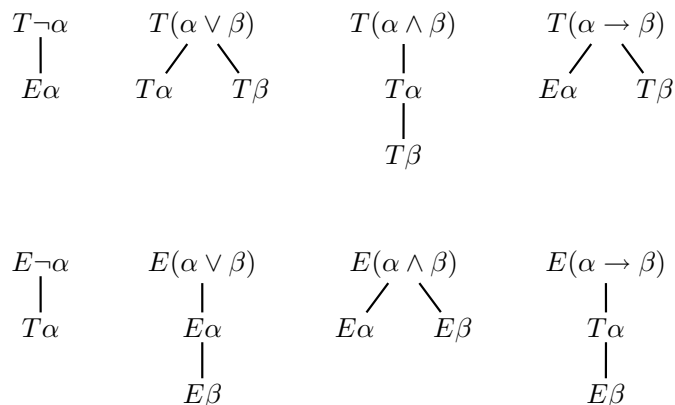
**Esimerkki.** Verrataan konjunktion totuustaulukkoa ja taulusääntöjä:

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



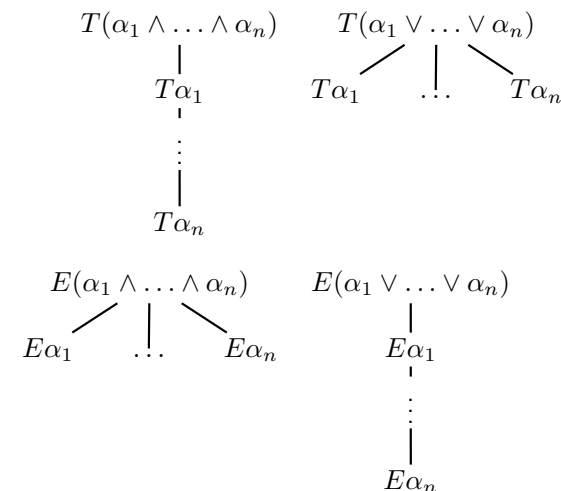


Konnektiivien  $\neg$ ,  $\vee$ ,  $\wedge$  ja  $\rightarrow$  taulusäännöt ovat seuraavat:



Ajatuksena on, että jokaiselle juurisolmusta lehtisolmuun johtavalle *polulle* kirjatut totuusarvo vaatimukset ovat yhtäaikaan voimassa.

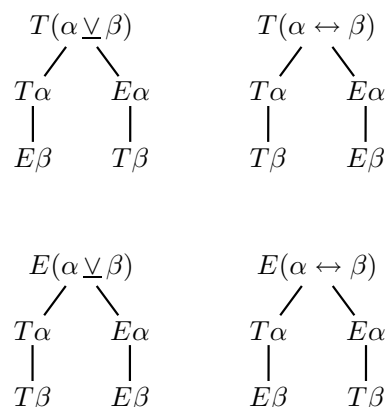
Ketjukonjunktioille ja -disjunktioille voidaan johtaa seuraavat säännöt:



**Huomio.** Jatkossa nämä ymmärretään lyhennysmerkintöinä!



Konnektiivien  $\underline{\vee}$  ja  $\leftrightarrow$  taulusäännöt ovat seuraavat:



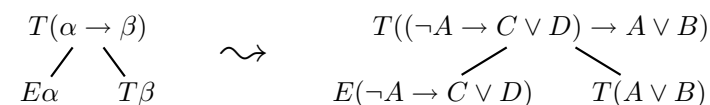
**Huomio.** Näistä taulusäännöistä voi todeta konnektiivien  $\underline{\vee}$  ja  $\leftrightarrow$  väliset suhteet:  $\alpha \underline{\vee} \beta \equiv \alpha \leftrightarrow \neg\beta \equiv \neg\alpha \leftrightarrow \beta \equiv \neg(\alpha \leftrightarrow \beta)$ .

### 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  $\alpha$  ja  $\beta$  kyseisillä lauseilla implikaation säännössä:



**Huomio.** Jatkossa on olennaista osata tunnistaa, mitä muotoa mihin lause on, koska taulusäännön valinta suoritetaan tällä perusteella.



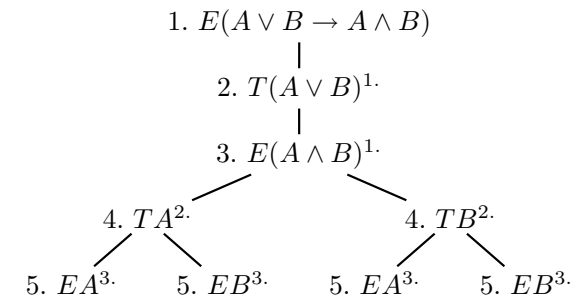
## 4.2 Semanttisen taulun määrittelmä

- Edellä määriteltiin jokaiselle lausetyypille omat taulusääntönsä.
- Yksittäinen taulusääntö tuottaa totuusarvovaatimuksia alilauseille lauseen totuusarvosta lähtien.
- Näitä vaatimuksia voidaan analysoida taulusäännöillä rekursiivisesti, kunnes saadaan atomisia lauseita koskevia totuusarvovaatimuksia.

Seuraavaksi määriteltävät *semanttiset taulut* ovat rakenteeltaan puita, joiden

1. solmujen asteluku on enintään kaksi ja
2. solmuina on muotoa  $T\phi$  ja  $E\phi$  olevia lausekkeita, jotka tulkitaan totuusarvovaatimuksiksi asianomaisille lauseille  $\phi$ .

**Esimerkki.** Muodostetaan semanttinen taulu lähtien liikkeelle juurisolmusta  $E(A \vee B \rightarrow A \wedge B)$ .

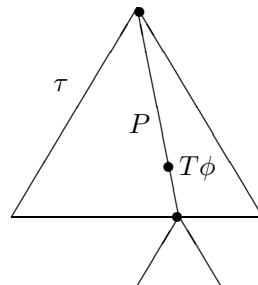


Semanttisen taulun solmut on numeroitu luettavuuden parantamiseksi. *Poluille lisättävät solmut numeroidaan juoksevasti.* Yläindeksinä oleva numero kertoo, monennestako asianomaisen polun solmusta kyseinen solmu on saatu taulusääntöä soveltamalla.



**Määrittelmä.** *Semanttinen taulu* muodostetaan seuraavilla periaatteilla:

- Jokainen yksisolmuinen puu, jonka ainoana solmuna on juurisolmu  $T\phi$  tai  $E\phi$ , on semanttinen taulu.
- Monimutkaisempia tauluja muodostetaan seuraavalla tavalla: Olkoon  $\tau$  semanttinen taulu. Jos  $P$  on jokin  $\tau$ :n polku juurisolmusta lehtisolmuun,  $T\phi$  ( $E\phi$ ) jokin  $\tau$ :n solmu polulla  $P$  ja  $\tau'$  saadaan  $\tau$ :sta liittämällä  $T\phi$ :n ( $E\phi$ :n) taulusääntö *ilman juurisolmua* polun  $P$  jatkoksi, niin  $\tau'$  on myöskin semanttinen taulu.



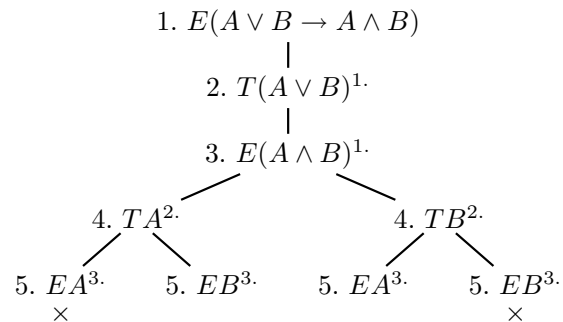
**Määrittelmä.** Olkoon  $\tau$  semanttinen taulu,  $P$  polku juurisolmusta lehtisolmuun taulussa  $\tau$  ja  $T\phi$  ( $E\phi$ ) polun  $P$  solmu.

1. Solmu  $T\phi$  ( $E\phi$ ) on *hajoitettu* polulla  $P$ , jos
  - (a)  $\phi$  on atominen lause, tai
  - (b) solmun  $T\phi$  ( $E\phi$ ) taulusääntöä jonkun polun  $P'$  jokainen solmu on polulla  $P$ .
2. Polku  $P$  on *ristiriitainen*, jos sillä esiintyy sekä  $T\alpha$  että  $E\alpha$  jollekin lauseelle  $\alpha$  (tämän merkiksi kirjoitetaan usein  $\times$  polun loppuun).
3. Polku  $P$  on *valmis*, jos se on ristiriitainen tai jokainen sen solmuista on hajoitettu polulla  $P$ .
4. Taulu  $\tau$  on *valmis*, jos jokainen sen poluista on valmis.
5. Taulu  $\tau$  on *ristiriitainen*, jos jokainen sen poluista on ristiriitainen.





**Esimerkki.** Palataan edelliseen esimerkkiin.



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

### Taulumenetelmän virheettömyys

Olkoon  $\phi \in \mathcal{L}$  mikä tahansa lause ja  $\tau$  juurisolmusta  $T\phi$  ( $E\phi$ ) muodostettu *valmis* semanttinen taulu.

**Väite.** Jos semanttisessa taulussa  $\tau$  on ei-ristiriitainen polku  $P$ , niin  $\mathcal{A} \parallel P$  ja  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ ) jokaiselle totuusjaketulle  $\mathcal{A} \subseteq \mathcal{P}$  joka täyttää seuraavat vaatimukset kaikille atomisille lauseille  $A \in \mathcal{P}$ :

- jos  $TA$  esiintyy polulla  $P$ , niin  $A \in \mathcal{A}$ , ja
- jos  $EA$  esiintyy polulla  $P$ , niin  $A \notin \mathcal{A}$ .

**Todistus.** Olkoon  $P$  mikä tahansa taulun  $\tau$  ei-ristiriitainen polku ja  $\mathcal{A}$  totuusjaketu, joka täyttää edellä mainitut vaatimukset atomisille lauseille.

Polku  $P$  on valmis, koska taulu  $\tau$  on valmis.

Todistetaan  $\mathcal{A} \parallel P$  induktiolla polun  $P$  solmujen rakenteen suhteen.



### 4.3 Taulumenetelmän ominaisuuksia

Olkoon  $\phi$  atomisten lauseiden joukkoon  $\mathcal{P}$  perustuvan kielen  $\mathcal{L}$  lause.

Semanttisella taululla voidaan ratkaista seuraava looginen ongelma: onko olemassa totuusjaketua  $\mathcal{A} \subseteq \mathcal{P}$  siten, että  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ )?

Todistamme jatkossa seuraavan ominaisuuden:

**Väite.** Olkoon  $\phi \in \mathcal{L}$  mikä tahansa lause. Juurisolmusta  $T\phi$  ( $E\phi$ ) muodostetussa valmiissa semanttisessa taulussa on ei-ristiriitainen polku, jos ja vain jos  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ ) jollekin totuusjaketulle  $\mathcal{A} \subseteq \mathcal{P}$ .

**Määritelmä.** Semanttisen taulun  $\tau$  polku  $P$  on *yhteensopiva* totuusjaketun  $\mathcal{A}$  kanssa (merkitään  $\mathcal{A} \parallel P$ ), jos ja vain jos

1.  $\mathcal{A} \models \alpha$  jokaiselle polun  $P$  solmulle  $T\alpha$ , ja
2.  $\mathcal{A} \not\models \beta$  jokaiselle polun  $P$  solmulle  $E\beta$ .

**Perustapaus:**  $TA \in P$  ( $EA \in P$ ), missä  $A$  on  $\mathcal{P}$ :n atominen lause. Totuusjaketulle  $\mathcal{A}$  asetettujen ehtojen perusteella  $\mathcal{A} \models A$  ( $\mathcal{A} \not\models A$ ).

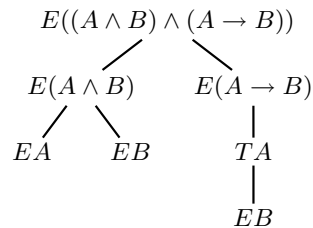
**Induktioaskel:** Käydään läpi kaikki tapaukset  $T(\alpha \wedge \beta) \in P$ ,  $E(\alpha \wedge \beta) \in P$ ,  $T(\alpha \vee \beta) \in P$ ,  $E(\alpha \vee \beta) \in P$ ,  $T(\alpha \rightarrow \beta) \in P$ , ...

- $E(\alpha \rightarrow \beta) \in P$ , jolloin  $T\alpha \in P$  ja  $E\beta \in P$ , koska  $P$  on valmis. 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  $T\beta \in P$ , koska  $P$  on valmis. 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.

Koska  $\mathcal{A} \parallel P$  ja  $T\phi \in P$  ( $E\phi \in P$ ), niin  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ ).



**Esimerkki.** Tarkastellaan joukkoon  $\mathcal{P} = \{A, B\}$  perustuvan kielen  $\mathcal{L}$  lausetta  $(A \wedge B) \wedge (A \rightarrow B)$  sekä seuraavaa valmista semanttista taulua:



- Ei-ristiriitaisia polkuja on kolme  $P_1$ ,  $P_2$  ja  $P_3$  (vasemmalta oikealle).
- Sama totuusjako voi olla yhteensopiva usean ei-ristiriitaisen polun kanssa. Esimerkissä totuusjaketulle  $\mathcal{A}_1 = \emptyset$  pätee  $\mathcal{A}_1 \parallel P_1$  ja  $\mathcal{A}_1 \parallel P_2$ .
- Yhteensopivia totuusjakoja voi olla myös useita ( $\mathcal{A}_1 \parallel P_2$  ja  $\mathcal{A}_2 \parallel P_2$ , missä  $\mathcal{A}_2 = \{A\}$ ) tai näitä voi olla myös täsmälleen yksi ( $\mathcal{A}_2 \parallel P_3$ ).

**Induktioaskel:** taulu  $\tau$  saadaan taulusta  $\tau'$  soveltamalla taulusääntöä  $\tau'$ :n polun  $P$  solmuun  $T\gamma$  tai  $E\gamma$  (jollekin lauseelle  $\gamma$ ).

Induktio-oletuksen nojalla  $\tau'$ :ssa polku  $P'$  siten, että  $\mathcal{A} \parallel P'$ .

Jos  $P \neq P'$ , niin  $P'$  myös taulun  $\tau$  polku.

Jos  $P = P'$ , niin  $\mathcal{A} \parallel P$  ja päädyimme tapausanalyysiin:

- $\gamma = \neg\alpha$  ja  $T(\neg\alpha) \in P$ :  
 $\implies \mathcal{A} \models \neg\alpha$  (koska  $\mathcal{A} \parallel P$ ) ja  $E\alpha$  lisätään  $P$ :n jatkoksi  
 $\implies \mathcal{A} \not\models \alpha$  ja syntyvä  $\tau$ :n polku on yhteensopiva  $\mathcal{A}$ :n kanssa.
- $\gamma = \neg\alpha$  ja  $E(\neg\alpha) \in P$ :  
 $\implies \mathcal{A} \not\models \neg\alpha$  (koska  $\mathcal{A} \parallel P$ ) ja solmu  $T\alpha$  lisätään  $P$ :n jatkoksi.  
 $\implies \mathcal{A} \models \alpha$  ja syntyvä  $\tau$ :n polku on yhteensopiva  $\mathcal{A}$ :n kanssa.
- Muut tapaukset (vaihtoehdot lauseeksi  $\gamma$ ) käsitellään vastaavasti.



## Taulumenetelmän täydellisyys

Olkoon  $\phi \in \mathcal{L}$  mikä tahansa lause ja  $\tau$  juurisolmusta  $T\phi$  ( $E\phi$ ) muodostettu (ei välttämättä valmis) semanttinen taulu.

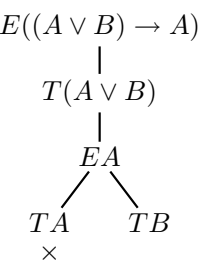
**Väite.** Jos  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ ) jossain totuusjaketussa  $\mathcal{A} \subseteq \mathcal{P}$ , niin semanttisessa taulussa  $\tau$  on ei-ristiriitainen polku  $P$  siten, että  $\mathcal{A} \parallel P$ .

**Todistus.** Oletetaan  $\mathcal{A} \models \phi$  ( $\mathcal{A} \not\models \phi$ ) jollekin totuusjaketulle  $\mathcal{A} \subseteq \mathcal{P}$ . Käytetään induktiota semanttisen taulun  $\tau$  rakenteen suhteen (vrt. semanttisen taulun induktiivinen määritelmä).

**Perustapaus:** taulu  $\tau$  koostuu ainoastaan juurisolmusta  $T\phi$  ( $E\phi$ ). Tällöin ainoa mahdollinen polku  $P$  juurisolmusta  $T\phi$  ( $E\phi$ ) itseensä toteuttaa vaatimuksen  $\mathcal{A} \parallel P$ , koska  $T\phi$  ( $E\phi$ ) on polun ainoa solmu.

Edellä osoitettu taulumenetelmän ominaisuus voidaan todeta seuraavasta esimerkistä.

**Esimerkki.** Totuusjako  $\mathcal{A} = \{B\}$  on yhteensopiva allaolevan semanttisen taulun oikeanpuoleisen polun kanssa.



Täten  $\mathcal{A} \not\models (A \vee B) \rightarrow A$ ,  $\mathcal{A} \models A \vee B$ ,  $\mathcal{A} \not\models A$  ja  $\mathcal{A} \models B$ .



## 4.4 Loogisten ongelmien ratkominen taulumenetelmällä

### Lauseen toteutuvuuden tutkiminen

- Lause  $\phi \in \mathcal{L}$  on *toteutuva*
  - $\iff \exists$  totuusjaku  $\mathcal{A} \subseteq \mathcal{P}$  s.e.  $\mathcal{A} \models \phi$
  - $\iff$  juurisolmusta  $T\phi$  muodostetussa valmiissa semanttisessa taulussa on ainakin yksi ei-ristiriitainen polku  $P$ .
- Jokaisesta ei-ristiriitaisesta polusta  $P$  voidaan konstruoida lauseelle  $\phi$  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 voidaan valita joko  $A \in \mathcal{A}$  tai  $A \notin \mathcal{A}$ .

© 2007 TKK / Tietojenkäsittelyteorian laboratorio

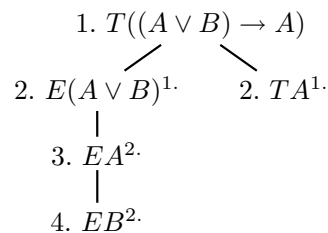
### Lausejoukon toteutuvuuden tutkiminen

- Äärellinen lausejoukko  $\Sigma = \{\phi_1, \dots, \phi_n\} \subseteq \mathcal{L}$  on toteutuva
  - $\iff$  lause  $\phi_1 \wedge \dots \wedge \phi_n \in \mathcal{L}$  on toteutuva
  - $\iff$  juurisolmusta  $T(\phi_1 \wedge \dots \wedge \phi_n)$  muodostetussa valmiissa semanttisessa taulussa on ainakin yksi ei-ristiriitainen polku  $P$ .
- Lausejoukko voidaan konstruoida malleja samaan tapaan kuin yksittäisen lauseen tapauksessa.
- Käytännössä juurisolmu  $T(\phi_1 \wedge \dots \wedge \phi_n)$  voidaan jättää kirjoittamatta näkyviin tilan säästämiseksi ja taulun juureen voidaan kirjata samalle polulle solmut  $T\phi_1, \dots, T\phi_n$ .

© 2007 TKK / Tietojenkäsittelyteorian laboratorio



**Esimerkki.** Tutkitaan lauseen  $A \vee B \rightarrow A$  toteutuvuutta.



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

**Huomio.** Mallien lukumäärä voi kasvaa eksponentiaalisesti lauseen pituuteen nähden (esim. lause  $(A_1 \vee B_1) \wedge \dots \wedge (A_n \vee B_n)$ ), joten kaikkien mallien ylöskirjaaminen ei välttämättä ole tilasyistä mielekästä.

© 2007 TKK / Tietojenkäsittelyteorian laboratorio

### Lauseen pätevyden tutkiminen

- $\models \phi$ 
  - $\iff \neg\phi$  on toteutumaton
  - $\iff$  juurisolmusta  $T\neg\phi$  muodostettu valmis semanttinen taulu on ristiriitainen
  - $\iff$  juurisolmusta  $E\phi$  muodostettu valmis semanttinen taulu on ristiriitainen.

Täten taulumenetelmästä saadaan lauselogiikalle todistusmenetelmä.

**Määritelmä.** Taulu  $\tau$  on lauseen  $\phi$  *todistus*, jos taulun  $\tau$  juurisolmuna on  $E\phi$  ja  $\tau$  on ristiriitainen (ja siten myös valmis).

Jos lauseella  $\phi$  on todistus,  $\phi$ :tä sanotaan *teoreemaksi/todistuvaksi* (merk.  $\vdash \phi$ ).

© 2007 TKK / Tietojenkäsittelyteorian laboratorio



**Esimerkki.** Osoitetaan lause  $A \wedge B \rightarrow A \vee B$  teoreemaksi:

1.  $E(A \wedge B \rightarrow A \vee B)$
- |
2.  $T(A \wedge B)^1$
- |
3.  $E(A \vee B)^1$
- |
4.  $TA^2$
- |
5.  $TB^2$
- |
6.  $EA^3$
- |
7.  $EB^3$
- ×

### Loogisen seuraavuuden tutkiminen

- $\{\phi_1, \dots, \phi_n\} \models \phi$   
 $\iff \models \phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi$   
 $\iff$  juurisolmusta  $E(\phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi)$  muodostettu valmis semanttinen taulu on ristiriitainen.
- Jos juurisolmusta  $E(\phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi)$  muodostettuun valmiiseen semanttiseen tauluun jää ei-ristiriitaisia polkuja, näistä voidaan konstruoida vastamalleja  $\mathcal{A}$  siten, että  $\mathcal{A} \models \{\phi_1, \dots, \phi_n\}$  ja  $\mathcal{A} \not\models \phi$ .
- Käytännössä taulun juureen tulevat solmut  $E(\phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi)$  ja  $T(\phi_1 \wedge \dots \wedge \phi_n)$  voidaan jättää kirjoittamatta näkyviin, ja taulu aloitetaan totuusarvovaatimuksilla  $E\phi$  ja  $T\phi_1, \dots, T\phi_n$  kirjattuina samalle polulle. Tämä voidaan nähdä vastamallin spesifikaationa.



### Todistusmenetelmän virheettömyys ja täydellisyys

Todistusmenetelmä  $M$  on

- **virheetön**, jos lauseen  $\phi$  todistettavuudesta menetelmällä  $M$  ( $\vdash_M \phi$ ) seuraa lauseen  $\phi$  pätevyys ( $\models \phi$ ).
- **täydellinen**, jos lauseen  $\phi$  pätevyydestä ( $\models \phi$ ) seuraa lauseen todistettavuus menetelmällä  $M$  ( $\vdash_M \phi$ ).

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

**Huomio.** Semanttisiin tauluihin perustuva menetelmä poikkeaa melkoisesti klassisista todistusjärjestelmistä, joissa pätevät lauseet tuotetaan syntaktisesti aksiomien ja päättelysääntöjen avulla.

### Johdettavuus lausejoukosta

**Määritelmä.** Lause  $\phi$  on johdettavissa äärellisestä lausejoukosta  $\Sigma = \{\phi_1, \dots, \phi_n\}$  (merkitään  $\Sigma \vdash \phi$ ), joss juurisolmusta  $E(\phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi)$  muodostettu valmis semanttinen taulu on ristiriitainen.

#### Huomioita.

- $\Sigma \vdash \phi \iff \Sigma \models \phi$ .
- Semanttisiin tauluihin perustuva todistusmenetelmä on täten virheetön ja täydellinen myös tutkittaessa loogista seuraavuutta.

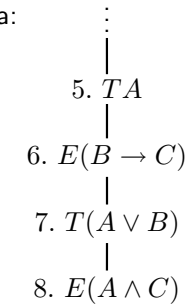


## Loogisen ekvivalenssin tutkiminen

- Lauseet  $\phi$  ja  $\psi$  ovat loogisesti ekvivalentit  
 $\iff \models \phi \leftrightarrow \psi$   
 $\iff$  juurisolmusta  $E(\phi \leftrightarrow \psi)$  muodostettu  
 valmis semanttinen taulu on ristiriitainen.
- Äärellisten lausejoukkojen  $\Sigma_1$  ja  $\Sigma_2$  loogisen ekvivalenssin toteaminen voi edellyttää usean semanttisen taulun konstruointia:
  1. Jokaiselle  $\sigma_1 \in \Sigma_1$  tulee osoittaa  $\Sigma_2 \models \sigma_1$ .
  2. Jokaiselle  $\sigma_2 \in \Sigma_2$  tulee osoittaa  $\Sigma_1 \models \sigma_2$ .

**Esimerkki.** Totea lamppuesimerkissä laadittujen spesifikaatioiden  $\{\neg P \rightarrow \neg L, P \rightarrow (L \leftrightarrow K)\}$  ja  $\{L \rightarrow P, P \wedge L \rightarrow K, P \wedge K \rightarrow L\}$  välinen ekvivalenssi käyttämällä semanttista taulua!

**Esimerkki.** Tarkastellaan alla annettua polkua eräässä keskeneräisessä semanttisessa taulussa:



- Solmun 6 käsittely lienee paras vaihtoehto (taulu ei haaraudu).
- Solmu 8 olisi seuraavaksi paras vaihtoehto, koska syntyvistä poluista toinen (jolle kirjataan solmu  $EA$ ) on suoraan ristiriitainen.
- Solmun 7 käsittely haarauttaa taulun.



## Ohjeita semanttisten taulujen laadintaan:

- Taulun solmussa  $T\phi$  (tai  $E\phi$ ) olevan lauseen  $\phi$  rakenne määrää käytettävän taulusäännön: esim. implikaation  $\phi = \alpha \rightarrow \beta$  käsittely.
- Polun laajentaminen voidaan lopettaa ristiriidan ilmentymiseen.
- Solmujen hajottamisjärjestyksellä voi usein vaikuttaa taulun kokoon.
- Taulun koon kasvua kannattaa välttää esim. seuraavilla periaatteilla.
  1. Hajoitetaan ensisijaisesti solmuja, jotka eivät haarauta taulua.
  2. Hajoitetaan toissijaisesti jäljelle jääviä solmuja, joista syntyvät totuusarvovaatimukset johtavat (välittömään) ristiriitaan.
  3. Tämän jälkeen hajoitetaan muita (taulua haarauttavia) solmuja.
- Kaikkia lauseita koskevat totuusarvovaatimukset eivät välttämättä ole tarpeen ristiriidan aikaansaamiseen (edes tietyllä polulla)!

## 4.5 Esimerkkejä

### Boolean funktioiden ja lauselogiikan yhteys

Mikä tahansa Boolean funktio  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  voidaan esittää lauselogiikan lauseena:

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

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



**Väite.** Olkoon  $f$  boolean funktio ja lause  $\phi$  sitä vastaava esitys: funktion  $f$  arvon laskeminen tietyillä muuttujien arvoilla vastaa lauseen  $\phi$  totuusarvon laskentaa vastaavassa totuusjakeleussa.

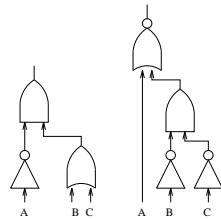
**Esimerkki.**

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

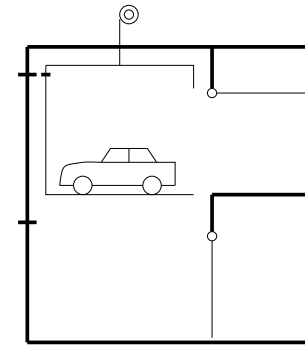
Aikaisemmalle esimerkille  $f(0, 0, 1) = 0 \cdot \bar{0} + 1 = 0 \cdot 1 + 1 = 0 + 1 = 1$  ja vastaavasti  $\mathcal{A} \models (A \wedge \neg B) \vee C$ .

**Esimerkki.**

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



**Esimerkki.** Mallinnetaan yksinkertaistettua hissijärjestelmää lauselogiikalla:



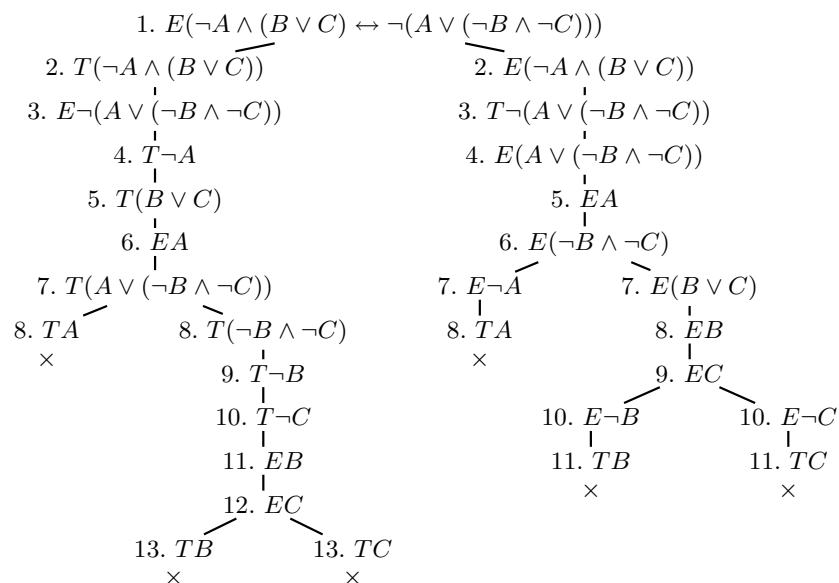
Atomiset lauseet:

$A_i$ : 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  $\Sigma$ , jonka *mallit* vastaavat sallittuja tiloja).



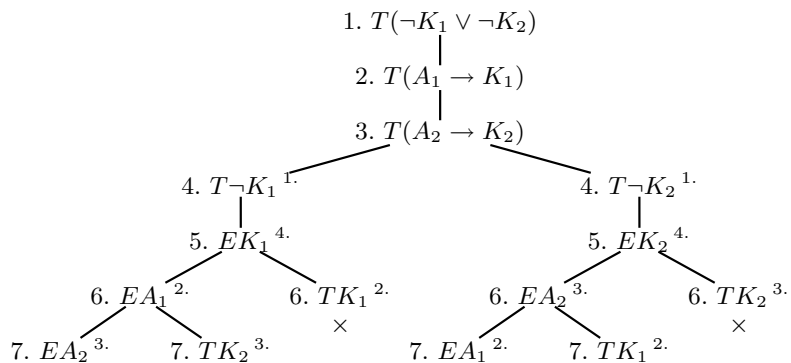
- Tyhjällä lausejoukolla  $\emptyset$  on  $2^4 = 16$  mallia, kuten esimerkiksi  $\mathcal{A} = \{K_1, K_2, A_1, A_2\}$ .  
Tämä vastaa järjestelmän tilaa, jossa hissi on yhtäaikaan molemmissa kerroksissa ja molemmat ovet ovat auki. Tämän pitäisi olla mahdotonta, joten tarvitaan lisää lauseita (rajoitteita).
- Fyysisen maailman asettama rajoitus:  $\neg K_1 \vee \neg K_2$  (huomaa, että edellä annettu  $\mathcal{A}$  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.



Taulun ei-ristiriitaisista haaroista voidaan muodostaa lausejoukolle viisi erilaista mallia, jotka vastaavat järjestelmän sallittuja tiloja:

$$\mathcal{A}_1 = \emptyset, \mathcal{A}_2 = \{K_1\}, \mathcal{A}_3 = \{K_1, A_1\}, \mathcal{A}_4 = \{K_2\} \text{ ja } \mathcal{A}_5 = \{K_2, A_2\}.$$

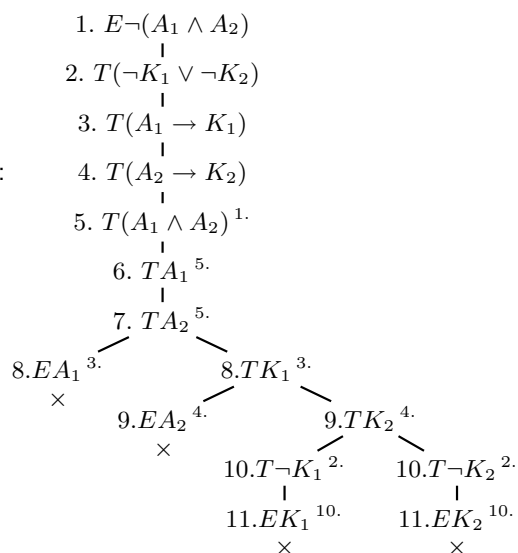
## 5 Vaihtoehtoisia todistusjärjestelmiä

- Hilbertin järjestelmä
- Suppesin järjestelmä
- Järjestelmien välistä vertailua



Voimme myös osoittaa, että hissien molemmat ovet eivät voi olla yhtäaikaaisesti auki (turvallisuusominaisuus):

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



### 5.1 Hilbertin järjestelmä

Hilbertin järjestelmä perustuu seuraaviin *aksiomiin* ja *päätelysääntöön*:

Aksiomat:

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

Päätelysääntö:

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



- Ajatuksena on, että pätevät lauseet pystytään tuottamaan *syntaktisesti* aksiomien instansseina (valisemalla  $\alpha$ ,  $\beta$  ja  $\gamma$  sopivasti) tai modus ponens -päätelysääntöä soveltamalla.
- Hilbertin järjestelmässä negaatio ja implikaatio ovat peruskonnektiiveina.

**Huomio.** Muut lauselogiikan peruskonnektiivit ovat lausuttavissa negaation ja implikaation avulla seuraavasti:

$$\alpha \vee \beta \equiv \neg\neg\alpha \vee \beta \equiv \neg\alpha \rightarrow \beta,$$

$$\alpha \wedge \beta \equiv \neg\neg(\alpha \wedge \beta) \equiv \neg(\neg\alpha \vee \neg\beta) \equiv \neg(\alpha \rightarrow \neg\beta) \text{ ja}$$

$$\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \equiv \neg((\alpha \rightarrow \beta) \rightarrow \neg(\beta \rightarrow \alpha)).$$

**Esimerkki.** Osoitetaan  $\{A, B \rightarrow (A \rightarrow C)\} \vdash_H B \rightarrow C$ .

- |    |   |           |
|----|---|-----------|
| 1. | $A$   | olettamus |
| 2. | $B \rightarrow (A \rightarrow C)$   | olettamus |
| 3. | $A \rightarrow (B \rightarrow A)$   | aksioma 1 |
| 4. | $B \rightarrow A$   | MP, 1, 3  |
| 5. | $(B \rightarrow (A \rightarrow C)) \rightarrow ((B \rightarrow A) \rightarrow (B \rightarrow C))$ | aksioma 2 |
| 6. | $(B \rightarrow A) \rightarrow (B \rightarrow C)$   | MP, 2, 5  |
| 7. | $B \rightarrow C$   | MP, 4, 6  |



**Määritelmä.** Olkoon  $\Sigma$  joukko lauseita.

*Todistus* lausejoukosta  $\Sigma$  on jono lauseita  $\alpha_1, \dots, \alpha_n$  siten, että kaikille  $i \in \{1, \dots, n\}$  pätee jokin seuraavista

- $\alpha_i \in \Sigma$ ,
- $\alpha_i$  on aksioman instanssi tai
- $\alpha_i$  on saatu modus ponensilla lauseista  $\alpha_j$ , missä  $j < i$  ja  $\alpha_k = (\alpha_j \rightarrow \alpha_i)$ , missä  $k < i$ .

**Määritelmä.** Lause  $\alpha$  on *johdettavissa* lausejoukosta  $\Sigma$  Hilbert-järjestelmällä (merk.  $\Sigma \vdash_H \alpha$ ), joss on olemassa todistus  $\alpha_1, \dots, \alpha_n$  lausejoukosta  $\Sigma$  siten, että  $\alpha = \alpha_n$ .

**Määritelmä.** Lause  $\alpha$  on *teoreema/todistuva* Hilbert-järjestelmässä (merk.  $\vdash_H \alpha$ ), joss  $\emptyset \vdash_H \alpha$

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

*Todistus.* Käytetään induktiota  $i$ :n suhteen.

- Perustapaus:**  $i = 1$ 
  - $\alpha_1$  on instanssi jostain kolmesta aksiomasta  
 $\implies \models \alpha_1$  (voidaan osoittaa esim. semanttisilla tauluilla)  
 $\implies \Sigma \models \alpha_1$  (loogisen seurausrelaation ominaisuudet).
  - $\alpha_1 \in \Sigma$   
 $\implies \Sigma \models \alpha_1$  (loogisen seurausrelaation ominaisuudet).
- Induktioaskel:**  $i > 1$   
 Tapaukset missä lausejonon jäsen  $\alpha_i$  on jonkin aksioman instanssi tai  $\alpha_i \in \Sigma$  käsitellään kuten edellä.



### • Induktioaskel jatkuu:

Jos  $\alpha_i$  saatiin modus ponensilla lauseista  $\alpha_j$  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  $\Sigma \not\models \alpha_i$

$\Rightarrow \exists$  totuusjaku  $\mathcal{A}$  s.e.  $\mathcal{A} \models \Sigma$  ja  $\mathcal{A} \not\models \alpha_i$

$\Rightarrow \mathcal{A} \not\models \alpha_j$  (koska  $\Sigma \models \alpha_j \rightarrow \alpha_i \Rightarrow \mathcal{A} \models \alpha_j \rightarrow \alpha_i$ )

$\Rightarrow \Sigma \not\models \alpha_j$ , ristiriita.

Siis  $\Sigma \models \alpha_i$ .

Hilbertin järjestelmä on virheetön ja täydellinen.

**Väite.** Jos  $\Sigma \vdash_H \alpha$ , niin  $\Sigma \models \alpha$  (todistettiin edellä).

Jos  $\Sigma \models \alpha$ , niin  $\Sigma \vdash_H \alpha$  (todistus sivuutetaan).

Tuonti- ja eliminointisäännöt:

KNT: $\frac{\alpha}{\neg\neg\alpha}$	KT: $\frac{\alpha \quad \beta}{\alpha \wedge \beta}$	DT: $\frac{\alpha}{\alpha \vee \beta} \quad \frac{\alpha}{\beta \vee \alpha}$	ET: $\frac{\alpha \rightarrow \beta \quad \beta \rightarrow \alpha}{\alpha \leftrightarrow \beta}$
---	---	--	---

KNE: $\frac{\neg\neg\alpha}{\alpha}$	KE: $\frac{\alpha \wedge \beta}{\alpha} \quad \frac{\alpha \wedge \beta}{\beta}$	DE: $\frac{\alpha \vee \alpha}{\alpha}$	EE: $\frac{\alpha \leftrightarrow \beta}{\alpha \rightarrow \beta} \quad \frac{\alpha \leftrightarrow \beta}{\beta \rightarrow \alpha}$
---	---	--	--

**Huomio.** Implikaation eliminointi tapahtuu päättelysäännöillä MP, TT tai ES ja tuonti päättelysäännöillä ET ja HS (kts. myös seuraava kalvo).

## 5.2 Suppesin järjestelmä

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

MP (modus ponens):

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

TP (modus tollendo ponens):

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

TT (modus tollendo tollens):

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

Vaihtosäännöt:

KV:

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

DV:

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

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 (ehdollinen todistaminen):

$$\frac{[\alpha]^{(1)} \quad \vdots \quad \beta}{\alpha \rightarrow \beta}$$

ES (epäsuora todistaminen):

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

<sup>(1)</sup> Apuolettamus  $\alpha$  merkitään hakasuluilla perutuksi, kun johtopäätös  $\alpha \rightarrow \beta$  on tehty.



**Määritelmä.** Suppes-todistus lausejoukosta  $\Sigma$  on jono lauseita  $\alpha_1, \dots, \alpha_n$ , joihin liittyy apuolettamusten joukot  $H_0 = \emptyset$  ja  $H_1, \dots, H_n$  siten, että kaikille  $i \in \{1, \dots, n\}$  pätee jokin seuraavista:

- $H_i = H_{i-1}$  ja  $\alpha_i \in \Sigma$ .
- $H_i = H_{i-1} \cup \{\alpha_i\}$  ja  $\alpha_i$  on uusi apuolettamus  $\alpha_i \notin H_{i-1}$ .
- $H_i = H_{i-1}$  ja  $\alpha_i$  on saatu jollain Suppes-järjestelmän päättelysäännöllä (paitsi ehdollisen todistamisen säännöllä) jonon aikaisemmista lauseista  $\alpha_j$  ( $j < i$ ), joille  $H_j \subseteq H_{i-1}$ .
- $H_i = H_{i-1}$  ja  $\alpha_i = \alpha_j$  jollekin jonon aikaisemmalle lauseelle  $\alpha_j$  ( $j < i$ ), jolle  $H_j \subseteq H_{i-1}$ .
- $H_i = H_{i-1} - \{\alpha_j\}$  ja  $\alpha_i = \alpha_j \rightarrow \alpha_{i-1}$  on saatu ehdollisen todistamisen säännöllä viimeisimmästä apuolettamuksesta  $\alpha_j$  ( $j < i$ ) ja edeltävästä lauseesta  $\alpha_{i-1}$ .

### Esimerkki.

Osoitetaan  $\{A, B \rightarrow (A \rightarrow C)\} \vdash_S B \rightarrow C$ .

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

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



### Määritelmä.

1. Lause  $\alpha$  on *johdettavissa* Suppes-järjestelmällä lausejoukosta  $\Sigma$  (merk.  $\Sigma \vdash_S \alpha$ ), joss on olemassa Suppes-todistus  $\alpha_1, \dots, \alpha_n$  lausejoukosta  $\Sigma$  siten, että  $\alpha_n = \alpha$  ja  $H_n = \emptyset$ .
2. Lause  $\alpha$  on *teoreema/todistuva* Suppes-järjestelmässä (merk.  $\vdash_S \alpha$ ), joss  $\emptyset \vdash_S \alpha$

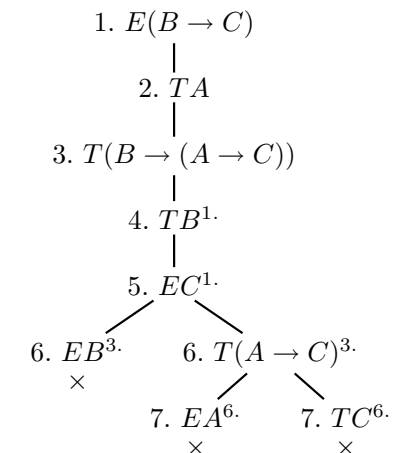
**Huomio.** Suppes-todistukselle asetettu lisäehto  $H_n = \emptyset$  edellyttää, että kaikki apuolettamukset on peruttava johtopäätöksen tekoon mennessä.

**Väite.** Suppesin järjestelmä on lauselogiikan virheetön ja täydellinen todistusmenetelmä ( $\Sigma \vdash_S \alpha \iff \Sigma \models \alpha$ ).

## 5.3 Järjestelmien vertailua

### Esimerkki.

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



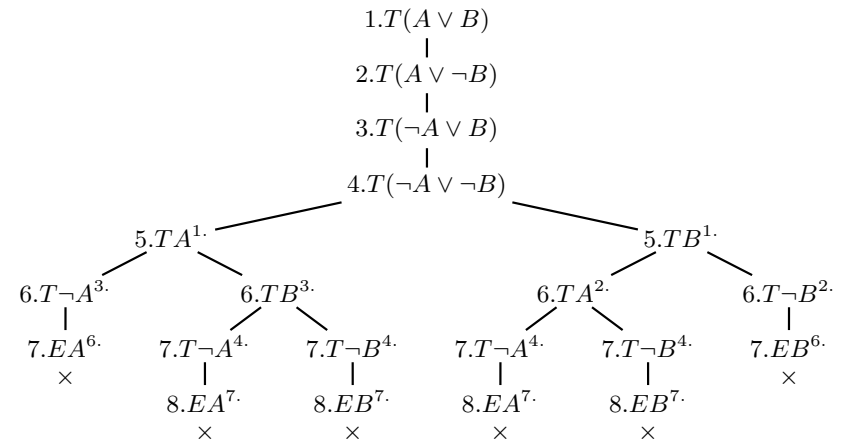
### 1. Hilbertin järjestelmä

- + Minimalistinen koneisto teoreemien tuottamiseksi.
- Lauseet esitettävä implikaation ja negaation avulla.
- 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.
- + Lauseissa voi esiintyä kaikkia peruskonnektiiveja.
- Hankala todeta milloin lause ei ole todistuva/johdettavissa.

**Esimerkki.** Pahimmassa tapauksessa taulun koko voi kasvaa eksponentiaalisesti atomisten lauseiden lukumäärään nähden.



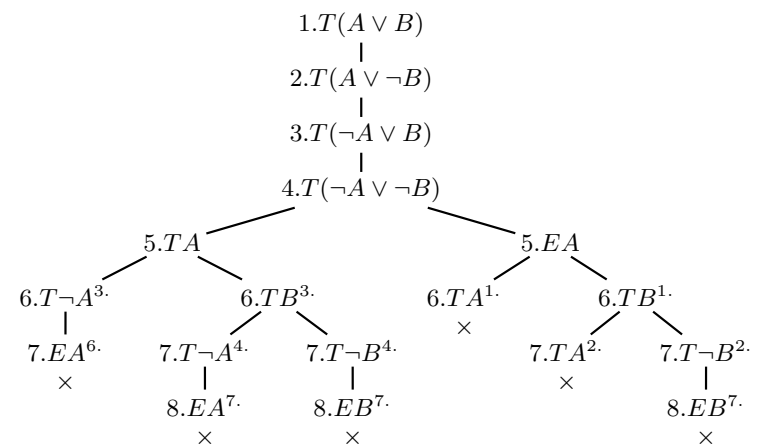
### 3. Semanttinen taulu

- + Lauseissa voi esiintyä kaikkia peruskonnektiiveja.
- + Lauseiden syntaksi ohjaa päättelysäännön (taulusäännöt) valintaa.
- + Mikäli lause ei ole todistuva/johdettavissa saadaan konkreettinen vastaesimerkki (eli vastamalli  $\mathcal{A}$ ).
- + Helppo toteuttaa tietokoneella.
- Semanttinen taulu ei ole tehokkain mahdollinen menetelmä lauselogiikan päättelyongelmien ratkomiseen.

**Huomio.** Semanttisen taulun menetelmää voidaan edelleen tehostaa lisäämällä taulusääntöjä. Esimerkkinä mainittakoon ns. *cut-sääntö*, joka haarauttaa polun jonkin väittämän  $\alpha$  suhteen ( $T\alpha$  ja  $E\alpha$ ).

Harkiten käytettynä tällä säännöllä voi tiivistää todistuksia.

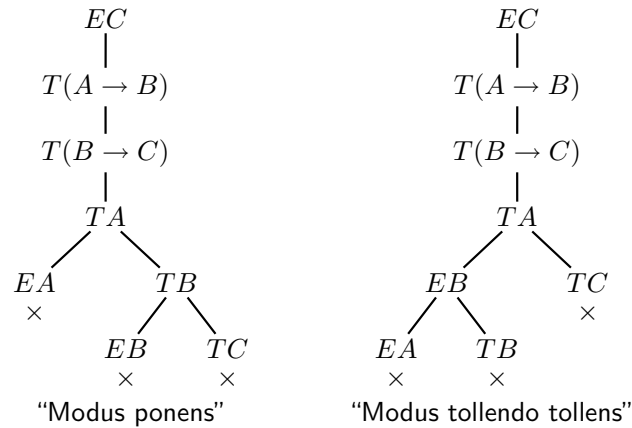
**Esimerkki.** Cut-säännön avulla taulu jää hieman pienemmäksi:



Merkitys korostuisi, jos atomisten lauseitten määrää lisättäisiin.



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



© 2007 TKK / Tietojenkäsittelyteorian laboratorio

## Motivaatio

Normaalimuotojen tarkoituksena on saattaa käsiteltävät lausekkeet johonkin säännölliseen muotoon, jotta niiden käsittely yksinkertaistuu. Esimerkkeinä mainittakoon seuraavat.

- Polynomien esittäminen muodossa

$$c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \dots + c_0 \cdot x^0.$$

- Lineaaristen yhtälöryhmien esittäminen matriiseina:

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

© 2007 TKK / Tietojenkäsittelyteorian laboratorio



## 6 Normaalimuodot

- Konjunkttiivinen ja disjunkttiivinen normaalimuoto
- Muunnokset normaalimuotoihin
- Normaalimuotojen hakeminen taulumenetelmällä
- Normaalimuotojen sieventäminen
- Lauseiden klausuulimuoto

© 2007 TKK / Tietojenkäsittelyteorian laboratorio

## 6.1 Konjunkttiivinen ja disjunkttiivinen normaalimuoto

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

**Määritelmä.** *Positiivisen* literaalin  $A$  *komplementti*  $\bar{A} = \neg A$  ja *negatiivisen* literaalin  $\neg A$  *komplementti*  $\overline{\neg A} = A$ .

**Määritelmä.** Lause  $\alpha$  on *konjunkttiivisessa normaalimuodossa*, jos  $\alpha$  on muodoltaan konjunktio  $\beta_1 \wedge \beta_2 \wedge \dots \wedge \beta_n$ , missä jokainen  $\beta_i$  on literaaleista  $l_1, l_2, \dots, l_{m_i}$  koostuva disjunktio  $l_1 \vee l_2 \vee \dots \vee l_{m_i}$ .

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

**Määritelmä.** Lause  $\alpha$  on *disjunkttiivisessa normaalimuodossa*, jos  $\alpha$  on muodoltaan disjunktio  $\beta_1 \vee \beta_2 \vee \dots \vee \beta_n$ , missä jokainen  $\beta_i$  on literaaleista  $l_1, l_2, \dots, l_{m_i}$  koostuva konjunktio  $l_1 \wedge l_2 \wedge \dots \wedge l_{m_i}$ .

© 2007 TKK / Tietojenkäsittelyteorian laboratorio

**Esimerkki.**

$$\begin{aligned} \text{KNM:} \quad & (A_1 \vee \neg A_2) \wedge (\neg A_1 \vee \neg A_3) \wedge (A_5 \vee A_6 \vee A_7) \\ & A_5 \wedge (\neg A_3 \vee A_6) \\ \text{KNM \& DNM:} \quad & A_1 \vee \neg A_2 \vee A_3 \\ & \neg A_7 \\ & A_1 \wedge A_2 \wedge A_3 \\ \text{DNM:} \quad & (\neg A_1 \wedge \neg A_2) \vee (A_3 \wedge A_1) \vee (A_1 \wedge \neg A_2 \wedge A_3) \\ & (A_1 \wedge \neg A_1) \vee A_2 \end{aligned}$$

**6.2 Muunnokset normaalimuotoihin**

Mikä hyvänsä lauselogiikan lause voidaan muuttaa konjunkttiiviseen tai disjunkttiiviseen normaalimuotoon seuraavalla menettelyllä.

1. Poista konnektiivit  $\leftrightarrow$  seuraavanlaisilla korvauksilla:

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

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

2. Poista konnektiivit  $\rightarrow$  seuraavanlaisilla korvauksilla:

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

3. Siirrä negaatiot välittömästi atomisten lauseiden eteen:

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

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

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



**Väite.** Jokaiselle lauselogiikan lauseelle  $\alpha$  on olemassa konjunkttiivisessa (disjunkttiivisessa) normaalimuodossa oleva lause  $\beta$ , joka on loogisesti ekvivalentti  $\alpha$ :n kanssa.

**Määritelmä.** Sanotaan, että em.  $\beta$  on  $\alpha$ :n konjunkttiivinen (disjunkttiivinen) normaalimuoto.

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

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

Viimeinen vaihe riippuu tavoiteltavasta normaalimuodosta:

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

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

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

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

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

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

**Huomio.** Jokainen edellä annetuista muunnoksista säilyttää loogisen ekvivalenssin, joten lopputuloksena saadaan lauseelle konjunkttiivinen tai disjunkttiivinen normaalimuoto.



**Esimerkki.** Muutetaan lause  $A \vee B \rightarrow (B \leftrightarrow C)$  konjunkttiiviseen ja disjunkttiiviseen normaalimuotoon.

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

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

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

Konjunkttiivinen normaalimuoto:

$$(\neg A \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \quad (7)$$

$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge (\neg B \vee ((\neg B \vee C) \wedge (\neg C \vee B))) \quad (6)$$

$$((\neg A \vee (\neg B \vee C)) \wedge (\neg A \vee (\neg C \vee B))) \wedge ((\neg B \vee (\neg B \vee C)) \wedge (\neg B \vee (\neg C \vee B))) \quad (6)$$

$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee \neg C \vee B) \wedge (\neg B \vee \neg B \vee C) \wedge (\neg B \vee \neg C \vee B) \quad (6)$$

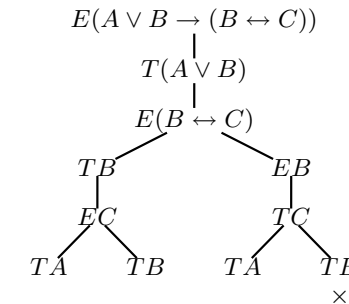
Disjunkttiivinen normaalimuoto:

$$(\neg A \wedge \neg B) \vee ((\neg B \vee C) \wedge \neg C) \vee ((\neg B \vee C) \wedge B) \quad (8)$$

$$(\neg A \wedge \neg B) \vee (\neg B \wedge \neg C) \vee (C \wedge \neg C) \vee (\neg B \wedge B) \vee (C \wedge B) \quad (9)$$

Lauseelle  $\alpha$  saadaan konjunkttiivinen normaalimuoto lauseen  $\neg\alpha$  disjunkttiivisesta normaalimuodosta sääntöjen (3)-(5) avulla.

**Esimerkki.**



Ristiriidattomista poluista saadaan DNM lauseelle  $\neg\alpha$ :

$$\neg\alpha \equiv (A \wedge B \wedge \neg C) \vee (B \wedge \neg C) \vee (A \wedge \neg B \wedge C).$$

Lauseen  $\alpha$  konjunkttiivinen normaalimuoto on tällöin:

$$\alpha \equiv \neg\neg\alpha \equiv (\neg A \vee \neg B \vee C) \wedge (\neg B \vee C) \wedge (\neg A \vee B \vee \neg C).$$

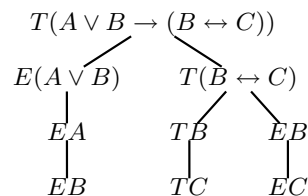


### 6.3 Normaalimuotojen hakeminen taulumenetelmällä

Normaalimuodon voi hakea myös taulumenetelmällä.

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

**Esimerkki.**



Vasemmanpuolisella polulla on vaatimukset  $EA$  ja  $EB$ , keskimmäisellä  $TB$  ja  $TC$  ja oikeanpuolisella  $EB$  ja  $EC$ . Näistä saadaan lauseen disjunkttiiviseksi normaalimuodoksi  $(\neg A \wedge \neg B) \vee (B \wedge C) \vee (\neg B \wedge \neg C)$ .

### 6.4 Normaalimuotojen sieventäminen

Konjunkttiivista/disjunkttiivista normaalimuotoa voidaan sieventää mm. seuraavilla periaatteilla:

- Poistetaan literaalien disjunktioista/konjunktioista literaalien moninkertaiset esiintymät.

**Esimerkki.**

$$\begin{aligned}
 &(\neg A \vee \neg B \vee C) \wedge (\neg A \vee \neg C \vee B) \wedge (\neg B \vee \neg B \vee C) \wedge (\neg B \vee \neg C \vee B) \\
 &\rightsquigarrow (\neg A \vee \neg B \vee C) \wedge (\neg A \vee \neg C \vee B) \wedge (\neg B \vee C) \wedge (\neg B \vee \neg C \vee B)
 \end{aligned}$$

- Poistetaan literaalien disjunktiot/konjunktiot, joissa esiintyy jokin literaali  $l$  ja sen komplementti  $\bar{l}$ .

**Esimerkki.** Jatketaan edellisestä:

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



- Jos **konjunkttiivisessa** normaalimuodossa esiintyy disjunktiot  $(l_1 \vee \dots \vee l_n)$  ja  $(k_1 \vee \dots \vee k_m)$  s.e.  $\{l_1, \dots, l_n\} \subseteq \{k_1, \dots, k_m\}$ , poistetaan jälkimmäinen (joka on edellisen looginen seuraus).

**Esimerkki.**  $(A \vee B \vee C) \wedge (A \vee B) \wedge (C \vee \neg B \vee A) \wedge (A \vee C) \rightsquigarrow (A \vee B) \wedge (C \vee \neg B \vee A) \wedge (A \vee C) \rightsquigarrow (A \vee B) \wedge (A \vee C)$

- Jos **konjunkttiivisessa** normaalimuodossa esiintyy yksiliteraalin disjunktio  $l$ , poistetaan muut disjunktiot, joissa  $l$  esiintyy, sekä mahdolliset komplementin  $\bar{l}$  esiintymät muista disjunktioista.

**Esimerkki.**  $\neg A \wedge (A \vee B \vee C) \wedge (\neg A \vee \neg B) \rightsquigarrow \neg A \wedge (B \vee C)$

**Huomio.** Jos disjunktioista poistetaan kaikki jäsenet, jäljelle jää tyhjä disjunktio  $\perp$ , joka on aina epätosi.

**Esimerkki.**  $A \wedge B \wedge (\neg A \vee \neg B) \rightsquigarrow A \wedge B \wedge \neg B \rightsquigarrow A \wedge B \wedge \perp \rightsquigarrow \perp$  (alkuperäinen lause on siis toteutumaton).

Konjunkttiivisesta normaalimuodosta voidaan muodostaa vastaava klausuulijoukko.

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

Huomaa seuraavat erikoistapaukset:

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

**Huomio.** Muistanet seuraavan analogian matematiikasta (tyhjät summat ja tulot):  $\sum_{i=1}^n x_i = 0$  ja  $\prod_{i=1}^n x_i = 1$ , kun  $n = 0$ .



## 6.5 Lauseiden klausuulimuoto

- Atomiset lauseet  $A$  ja niiden negaatiot  $\neg A$  ovat **literaaleja**.
- Literaalin komplementti:  $\overline{\overline{A}} = A$ ,  $\overline{\neg A} = A$ .
- Literaalien  $l_1, \dots, l_n$  disjunktio  $l_1 \vee \dots \vee l_n$  on **klausuuli**.
- Klausuulit esitetään usein literaalien **joukkoina**  $\{l_1, \dots, l_n\}$ .
- Joukko klausuuleita  $S$  edustaa klausuuliensa konjunktiota.

**Huomio.** Esitystavoilla on hienoiset erot:

$$\neg A \vee B \vee \neg A \rightsquigarrow \{\neg A, B\}$$

$$\neg A \vee B \rightsquigarrow \{\neg A, B\}$$

$$B \vee \neg A \rightsquigarrow \{\neg A, B\}$$

## 7 Resoluutio

- Totuusmääritelmä ja toteutuvuus klausuuleille
- Resoluutiosääntö
- Resoluutiotodistukset
- Resoluution virheettömyys ja täydellisyys
- Loogisten ongelmien ratkominen resoluutiolla



## 7.1 Totuusmääritelmä ja toteutuus klausuuleille

Klausuulien tapauksessa totuusmääritelmä voidaan kirjoittaa varsin yksinkertaiseen muotoon.

### Määritelmä.

1. Totuusjaketun  $\mathcal{A} \subseteq \mathcal{P}$  *literaaliesitys*  $\text{Lit}(\mathcal{A}) = \mathcal{A} \cup \{\neg A \mid A \in \mathcal{P} - \mathcal{A}\}$ .
2. Klausuuli  $C$  on *tosi* totuusjaketussa  $\mathcal{A} \subseteq \mathcal{P}$  (merk.  $\mathcal{A} \models C$ ), joss  $C \cap \text{Lit}(\mathcal{A}) \neq \emptyset$ .
3. Klausuulijoukko  $S$  on *tosi* totuusjaketussa  $\mathcal{A}$  (merk.  $\mathcal{A} \models S$ ), joss kaikille klausuuleille  $C \in S$  pätee  $\mathcal{A} \models C$ .
4. Totuusjaketu  $\mathcal{A} \subseteq \mathcal{P}$  on klausuulijoukon  $S$  *malli*, joss  $\mathcal{A} \models S$ .



**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  $\{\square\}$  ovat toteutumattomia, koska molemmista klausuulijoukoista löytyy klausuulit  $C_1$  ja  $C_2$  siten, että  $C_1 \cap \{A\} = \emptyset$  ja  $C_2 \cap \{\neg A\} = \emptyset$ .

Huomaa, että edellä  $\{A\} = \text{Lit}(\{A\})$  ja  $\{\neg A\} = \text{Lit}(\emptyset)$  kattavat kaikki mahdolliset totuusjaketut  $\mathcal{A} \subseteq \mathcal{P} = \{A\}$ .



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

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

Nyt esimerkiksi

$$\mathcal{A} \models \{\{A, C, E\}, \{\neg A, \neg B\}\}$$

$$\mathcal{A} \models \emptyset$$

$$\mathcal{A} \not\models \{\{A, B\}, \{C\}\}$$

$$\mathcal{A} \models \{\neg A, B, \neg D\}$$

$$\mathcal{A} \not\models \{\neg A, D\}$$

$$\mathcal{A} \not\models \square$$



**Esimerkki.** Aiemmin esitetyn kartan kolmiväritysongelman kuvaus vastaa seuraavaa toteutumattonta klausuulijoukkoa  $S =$

$$\begin{aligned} & \{ \{P_1, V_1, S_1\}, \{\neg P_1, \neg V_1\}, \{\neg V_1, \neg S_1\}, \{\neg S_1, \neg P_1\}, \\ & \{P_2, V_2, S_2\}, \{\neg P_2, \neg V_2\}, \{\neg V_2, \neg S_2\}, \{\neg S_2, \neg P_2\}, \\ & \{P_3, V_3, S_3\}, \{\neg P_3, \neg V_3\}, \{\neg V_3, \neg S_3\}, \{\neg S_3, \neg P_3\}, \\ & \{P_4, V_4, S_4\}, \{\neg P_4, \neg V_4\}, \{\neg V_4, \neg S_4\}, \{\neg S_4, \neg P_4\}, \\ & \{\neg P_1, \neg P_2\}, \{\neg V_1, \neg V_2\}, \{\neg S_1, \neg S_2\}, \\ & \{\neg P_1, \neg P_3\}, \{\neg V_1, \neg V_3\}, \{\neg S_1, \neg S_3\}, \\ & \{\neg P_1, \neg P_4\}, \{\neg V_1, \neg V_4\}, \{\neg S_1, \neg S_4\}, \\ & \{\neg P_2, \neg P_3\}, \{\neg V_2, \neg V_3\}, \{\neg S_2, \neg S_3\}, \\ & \{\neg P_2, \neg P_4\}, \{\neg V_2, \neg V_4\}, \{\neg S_2, \neg S_4\}, \\ & \{\neg P_3, \neg P_4\}, \{\neg V_3, \neg V_4\}, \{\neg S_3, \neg S_4\} \}. \end{aligned}$$





## 7.2 Resoluutiosääntö

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

**Esimerkki.** Sovelletaan resoluutiosääntöä seuraaviin klausuuleihin:

$$\begin{array}{ccc} \{A, B, \neg C\} & & \{\neg A, D, \neg C\} \\ & \searrow \quad \swarrow & \\ & \{B, \neg C, D\} & \end{array}$$

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

## 7.3 Resoluutiotodistukset

Lähtökohtana klausuulijoukko  $S$ , jonka klausuuleihin sovelletaan resoluutiosääntöä.

**Määritelmä.** Klausuulin  $C$  *johto* klausuulijoukosta  $S$  on äärellinen jono klausuuleja  $C_1, \dots, C_n$ , 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  $\square$ , kyseistä johtoa kutsutaan  $S$ :n *hylkäykseksi* (refutaatioksi).

Ajatuksena on, että tällöin  $S$  joudutaan hylkäämään toteutuvana klausuulijoukkona.



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

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

- Klausuulijoukosta 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  $\square$  (tämä tarkoittaisi, että  $S$  on toteutumaton).
- Huomaa, että  $S$  on toteutuva ( $\mathcal{A} \models S$ ) totuusjaketussa  $\mathcal{A} = \{A, B\}$ .

**Esimerkki.** Tarkastellaan klausuulijoukkoa

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

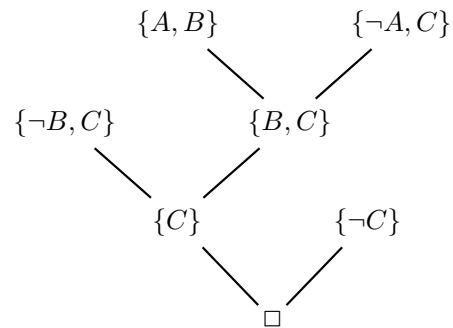
jolle saadaan seuraava hylkäys:

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.  $\square$  4, 6



## Resoluutiodistuksen puuesitys

Edellä esitetty hylkäys voidaan kirjoittaa myös puumuotoon.



**Huomio.** Lehtisolmuina on ainoastaan klausuulijoukon  $S$  klausuleja ja vastaava lineaarinen hylkäys voidaan tuottaa käymällä puumuotoinen todistus syvyyssjärjestyksessä lävitse.

## 7.4 Resoluution virheettömyys ja täydellisyys

**Väite.** Jos klausuulijoukolla  $S$  on malli  $\mathcal{A} \subseteq \mathcal{P}$  ja  $C$  on kahden klausuulin  $C_1 \in S$  ja  $C_2 \in S$  yhdistelmä, niin totuusjaku  $\mathcal{A}$  on myös laajennetun klausuulijoukon  $S' = S \cup \{C\}$  malli.

**Todistus.** Oletetaan  $\mathcal{A} \not\models S \cup \{C\}$ .

$$\Rightarrow \mathcal{A} \not\models C$$

$$\Rightarrow C \cap \text{Lit}(\mathcal{A}) = \emptyset$$

$$\Rightarrow C_1 \cap \text{Lit}(\mathcal{A}) = \emptyset \text{ tai } C_2 \cap \text{Lit}(\mathcal{A}) = \emptyset$$

$$\Rightarrow \mathcal{A} \not\models C_1 \text{ tai } \mathcal{A} \not\models C_2$$

$$\Rightarrow \mathcal{A} \not\models S, \text{ ristiriita.}$$

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



## Esimerkki.

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

saadaan seuraava hylkäys:

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

**Väite.** Jos klausuulijoukolle  $S$  on hylkäys, niin  $S$  on toteutumaton.

**Todistus.** Oletetaan, että klausuulijoukolle  $S$  on hylkäys  $C_1, \dots, C_n$ , missä  $C_n = \square$ . Tehdään vastaoletus, että  $S$  on toteutuva.

Osoitetaan induktiolla  $i$ :n suhteen, että  $S \cup \{C_1, \dots, C_i\}$  on toteutuva.

**Perustapaus**  $i = 0$ : Joukko  $S$  on toteutuva (vastaoletus).

**Induktioaskel:**  $S \cup \{C_1, \dots, C_{i-1}\}$  on toteutuva (induktio-oletus).

- Jos  $C_i \in S$ , joukko  $S \cup \{C_1, \dots, C_i\}$  on triviaalisti toteutuva.
- Muussa tapauksessa  $C_i$  on saatu resoluutiosäännöllä joukon  $\{C_1, \dots, C_{i-1}\}$  kahdesta klausuulista. Edellä todistamamme väitteen nojalla myös joukko  $S \cup \{C_1, \dots, C_i\}$  on toteutuva.

Induktiodistuksesta seuraa, että myös  $S \cup \{C_1, \dots, C_n\}$  on toteutuva.

Ristiriita, koska  $C_n = \square$  on epätosi kaikissa totuusjakeluissa.



### Puukonstruktio täydellisyydestä varten

Olkoon  $S$  atomisten lauseiden joukkoon  $\mathcal{P} = \{A_1, \dots, A_n\}$  perustuva klausulijoukko, jolle muodostetaan binääripuu seuraavilla periaatteilla.

Olkoon  $s$  syvydellä  $i$  ( $0 \leq i \leq n$ ) oleva puun solmu (juurisolmu on syvydellä 0) ja  $L_s$  niiden literaalien joukko, jotka ovat juurisolmusta solmuun  $s$  johtavilla kaarilla.

Jos  $\bar{C} = \{\bar{l} \mid l \in C\} \subseteq L_s$  jollekin klausulille  $C \in S$  (eli  $\mathcal{A} \not\models C$  kaikille totuusjakoille  $\mathcal{A}$  s.e.  $L_s \subseteq \text{Lit}(\mathcal{A})$ ), merkitään  $C$  solmuun  $s$  ja lopetetaan puun laajentaminen tästä solmusta eteenpäin. Muutoin:

1. Jos  $i < n$ , merkitään solmulle  $s$  vasen lapsi  $s_v$  ja oikea lapsi  $s_o$  sekä merkitään näihin solmusta  $s$  johtaville kaarille literaalit  $A_i$  ja  $\neg A_i$ . Jatketaan puun laajentamista solmuista  $s_v$  ja  $s_o$  vastaavasti.
2. Jos  $i = n$ , lopetetaan puun laajentaminen solmusta  $s$  eteenpäin.

**Väite.** Jos  $S$  on toteutumaton, niin binääripuun jokainen polku päättyy solmuun  $s$ , johon on merkitty klausuli  $C \in S$  s.e.  $\bar{C} \subseteq L_s$ .

**Todistus.** Vastaoletus: edellä kuvatulla tavalla muodostetussa binääripuussa on solmu  $s$  tasolla  $n$  siten, että  $\bar{C} \not\subseteq L_s$  kaikille  $C \in S$ .  
 $\implies L_s = \text{Lit}(\mathcal{A})$  jollekin  $\mathcal{A} \subseteq \mathcal{P}$  ja  $C \cap L_s \neq \emptyset$  kaikille  $C \in S$ .  
 $\implies \mathcal{A} \models C$  kaikille  $C \in S$ , eli  $S$  on toteutuva, ristiriita.

**Väite.** Jos klausulijoukko  $S$  on toteutumaton, sille on hylkäys.

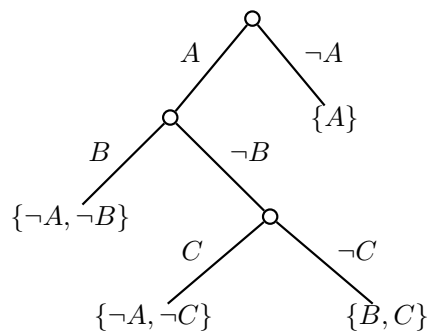
**Todistus.** Olkoon  $S$  toteutumaton, jolloin binääripuun lehtisolmuina on  $S$ :n klausulit. Käydään läpi sisäsolmut  $s$  (käänteisessä järjestyksessä).

Merkitään solmuun  $s$  klausuliksi lapsisolmuihin merkittyjen klausulien  $C_v$  ja  $C_o$  yhdistelmä  $C$ , jolle pätee  $\bar{C} \subseteq L_s$  ( $\bar{C}_v \subseteq L_{s_v}$  ja  $\bar{C}_o \subseteq L_{s_o}$ ). Tämä ominaisuus siirtyy kaikille sisäsolmujen  $s$  klausuleille  $C$ .

Juurisolmun  $s$  tapauksessa  $L_s = \emptyset$ , joten  $\bar{C} = \emptyset$  ja  $C = \square$ .

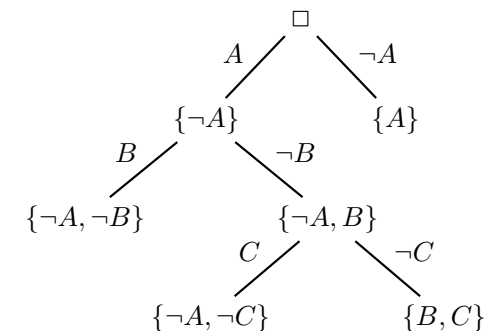


**Esimerkki.** Konstruoidaan edellä kuvattu binääripuu klausulijoukolle  $S = \{\{A\}, \{B, C\}, \{\neg A, \neg B\}, \{\neg A, \neg C\}\}$ :



**Huomio.** Kuhunkin lehtisolmuun  $s$  merkitty klausuli  $C$  on epätosi totuusjakoissa  $\mathcal{A}$ , joille  $L_s \subseteq \text{Lit}(\mathcal{A})$ .

**Esimerkki.** Palataan edelliseen esimerkkiin ja muodostetaan ko. klausulijoukolle  $S = \{\{A\}, \{B, C\}, \{\neg A, \neg B\}, \{\neg A, \neg C\}\}$  hylkäys:



**Huomio.** Tästä on helppo todeta edellä esitetty ominaisuus, että jokaiseen solmuun  $s$  merkitylle klausulille  $C$  pätee  $\bar{C} \subseteq L_s$ .



## 7.5 Loogisten ongelmien ratkominen resoluutiolla

### Toteutuvuuden tutkiminen resoluutiolla

- Menettely: muunnetaan tutkittava lause  $\alpha$  konjunkttiiviseen normaalimuotoon ja edelleen klausuulijoukoksi  $S_\alpha$ .
- Tällöin  $S_\alpha$  on toteutumaton  $\iff$  lauseen  $\alpha$  KNM on toteutumaton  $\iff \alpha$  on toteutumaton.
- Sen sijaan mallien hakeminen resoluutiolla on hankalaa.

Lausejoukkojen toteutuvuutta tutkitaan samaan tyyliin.

- Menettely: muodostetaan klausuulijoukko  $S_\Sigma = \bigcup \{S_\sigma \mid \sigma \in \Sigma\}$ .
- Tällöin  $S_\Sigma$  on toteutumaton  $\iff \Sigma$  on toteutumaton.



- |                                      |                                |
|--------------------------------------|--------------------------------|
| 19. $\{P_2, P_3, P_4\}$ (9,18)       | ...                            |
| 20. $\{\neg P_1, \neg P_2\}$         | 50. $\{\neg V_1\}$ (symmetria) |
| 21. $\{P_3, P_4, \neg P_1\}$ (19,20) | ...                            |
| 22. $\{\neg P_1, \neg P_3\}$         | 75. $\{\neg S_1\}$ (symmetria) |
| 23. $\{P_4, \neg P_1\}$ (21,22)      | 76. $\{P_1, V_1, S_1\}$        |
| 24. $\{\neg P_1, \neg P_4\}$         | 77. $\{V_1, S_1\}$ (25,76)     |
| 25. $\{\neg P_1\}$ (23,24)           | 78. $\{S_1\}$ (50,77)          |
| ...                                  | 79. $\square$ (75,78)          |

- Edellä olevan todistuksen hakemisessa (askelet 1–25) on hyödynnetty täydellisyystodistuksen puukonstruktiota.
- Lyhyempiäkin todistuksia löydettävissä (OTTER: 49 askelta).



**Esimerkki.** Osoitetaan karttaesimerkin klausuulijoukko toteutumattomaksi resoluutiolla.

- |  |   |
|--|---|
| 1. $\{P_4, V_4, S_4\}$                 | 10. $\{\neg V_3, \neg V_4\}$              |
| 2. $\{\neg S_3, \neg S_4\}$            | 11. $\{P_4, S_4, \neg V_3\}$ (1,10)       |
| 3. $\{P_4, V_4, \neg S_3\}$ (1,2)      | 12. $\{P_3, S_3, P_4, S_4\}$ (4,11)       |
| 4. $\{P_3, V_3, S_3\}$                 | 13. $\{\neg S_2, \neg S_4\}$              |
| 5. $\{P_3, V_3, P_4, V_4\}$ (3,4)      | 14. $\{P_3, S_3, P_4, \neg S_2\}$ (12,13) |
| 6. $\{\neg V_2, \neg V_4\}$            | 15. $\{\neg S_2, \neg S_3\}$              |
| 7. $\{P_3, V_3, P_4, \neg V_2\}$ (5,6) | 16. $\{P_3, P_4, \neg S_2\}$ (14,15)      |
| 8. $\{\neg V_2, \neg V_3\}$            | 17. $\{P_2, V_2, S_2\}$                   |
| 9. $\{P_3, P_4, \neg V_2\}$ (7,8)      | 18. $\{P_2, P_3, P_4, V_2\}$ (16,17)      |



### Pätevyyden tutkiminen resoluutiolla

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

- Menettely: muunnetaan tutkittavan lauseen negaatio  $\neg \alpha$  konjunkttiiviseen normaalimuotoon ja edelleen klausuulijoukoksi  $S_{\neg \alpha}$ .
- Tällöin  $S_{\neg \alpha}$  on toteutumaton  $\iff$  lauseen  $\neg \alpha$  KNM on toteutumaton  $\iff \neg \alpha$  on toteutumaton  $\iff \alpha$  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  $S = \{\{\neg A, B\}, \{A, C\}, \{\neg B\}, \{\neg C\}\}$ .

Resoluutiotodistus (hylkäys):

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 konjunkttiiviseen normaalimuotoon ja edelleen klausuulijoukoksi  $S_{\Sigma \cup \{\neg \alpha\}}$ .
- Tällöin  $S_{\Sigma \cup \{\neg \alpha\}}$  on toteutumaton  
 $\iff$  joukon  $\Sigma \cup \{\neg \alpha\}$  lauseiden KMN:en joukko on toteutumaton  
 $\iff$  lausejoukko  $\Sigma \cup \{\neg \alpha\}$  on toteutumaton  
 $\iff$   $\alpha$  on lausejoukon  $\Sigma$  looginen seuraus.



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

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

Resoluutiotodistus:

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

Muita klausuuleja (mukaanlukien  $\square$ ) ei ole enää johdettavissa.

Lause ei ole pätevä.

Vastamalli  $\mathcal{A} = \emptyset$  nähtävissä klausuuleista 3–5.

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

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

Saadaan klausuulijoukko  $S =$

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

Vastaus: lause  $A$  on lausejoukon looginen seuraus.



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

lause	KNM	klausuuleina
$\neg K_1 \vee \neg K_2$	$\neg K_1 \vee \neg K_2$	1. $\{\neg K_1, \neg K_2\}$
$A_1 \rightarrow K_1$	$\neg A_1 \vee K_1$	2. $\{\neg A_1, K_1\}$
$A_2 \rightarrow K_2$	$\neg A_2 \vee K_2$	3. $\{\neg A_2, K_2\}$
$\neg(A_1 \wedge A_2)$	$A_1 \wedge A_2$	4. $\{A_1\}$ , 5. $\{A_2\}$
Hylkäys:		6. $\{K_1\}$ 2,4
		7. $\{K_2\}$ 3,5
		8. $\{\neg K_2\}$ 1,6
		9. $\square$ 7,8

$\Rightarrow \neg(A_1 \wedge A_2)$  on muiden lauseiden looginen seuraus.

**Esimerkki.** Osoitetaan  $(A \rightarrow B) \wedge (\neg A \rightarrow C)$  ja  $(A \wedge B) \vee (\neg A \wedge C)$  loogisesti ekvivalenteiksi resoluutiolla.

Johdetaan ensin tarvittavat klausuuliesitykset:

1. Lauseen  $(A \rightarrow B) \wedge (\neg A \rightarrow C)$  KNM on  $(\neg A \vee B) \wedge (A \vee C)$ , josta saadaan klausuulijoukko  $S_1 = \{\{\neg A, B\}, \{A, C\}\}$ .
2. Lauseen  $\neg((A \wedge B) \vee (\neg A \wedge C))$  KNM on  $(\neg A \vee \neg B) \wedge (A \vee \neg C)$  ja vastaava klausuulijoukko  $S_2 = \{\{\neg A, \neg B\}, \{A, \neg C\}\}$ .
3. Lauseelle  $\neg((A \rightarrow B) \wedge (\neg A \rightarrow C)) \equiv (A \wedge \neg B) \vee (\neg A \wedge \neg C)$  saadaan KNM  $(A \vee \neg C) \wedge (\neg A \vee \neg B) \wedge (\neg B \vee \neg C)$ , josta voidaan muodostaa  $S_3 = \{\{A, \neg C\}, \{\neg A, \neg B\}, \{\neg B, \neg C\}\}$ .
4. Lauseelle  $(A \wedge B) \vee (\neg A \wedge C)$  saadaan vastaavasti KNM  $(A \vee C) \wedge (\neg A \vee B) \wedge (B \vee C)$  ja edelleen klausuuliesitys  $S_4 = \{\{A, C\}, \{\neg A, B\}, \{B, C\}\}$ .



### Loogisen ekvivalenssin tutkiminen resoluutiolla

**Väite.**  $\alpha \equiv \beta \iff \models \alpha \leftrightarrow \beta \iff \models \alpha \rightarrow \beta$  ja  $\models \beta \rightarrow \alpha$   
 $\iff$  lausejoukot  $\{\alpha, \neg\beta\}$  ja  $\{\neg\alpha, \beta\}$  ovat toteutumattomia.

- Menettely: muunnetaan lausejoukkojen  $\{\alpha, \neg\beta\}$  ja  $\{\neg\alpha, \beta\}$  lauseet konjunktiiviseen normaalimuotoon ja edelleen klausuulijoukoiksi  $S_{\{\alpha, \neg\beta\}}$  ja  $S_{\{\neg\alpha, \beta\}}$ .
- Tällöin  $S_{\{\alpha, \neg\beta\}}$  ja  $S_{\{\neg\alpha, \beta\}}$  ovat toteutumattomia  
 $\iff \{\alpha, \neg\beta\}$  ja  $\{\neg\alpha, \beta\}$  ovat toteutumattomia  
 $\iff \alpha$  ja  $\beta$  ovat loogisesti ekvivalentit.
- Toinen mahdollisuus on tutkia lauseen  $\alpha \leftrightarrow \beta$  pätevyyttä (edellä kuvatulla menettelyllä).

**Esimerkki.** (Jatkoa) Osoitetaan  $S_1 \cup S_2$  ja  $S_3 \cup S_4$  toteutumattomiksi.

- Klausuulijoukolle  $S_1 \cup S_2 = \{\{\neg A, B\}, \{A, C\}, \{\neg A, \neg B\}, \{A, \neg C\}\}$  saadaan seuraava hylkäys:  
 $\{\neg A, B\}, \{\neg A, \neg B\}, \{\neg A\}, \{A, C\}, \{C\}, \{A, \neg C\}, \{\neg C\}, \square$ .
- Koska  $S_1 \cup S_2 \subseteq S_3 \cup S_4$ , yllä annettu klausuulien sekvenssi on hylkäys myös joukolle  $S_3 \cup S_4$ .

$\Rightarrow (A \rightarrow B) \wedge (\neg A \rightarrow C) \equiv (A \wedge B) \vee (\neg A \wedge C)$ .

### Huomioita.

- Klausuulijoukkojen  $S_3$  ja  $S_2$  erona oleva klausuuli  $\{\neg B, \neg C\}$  voidaan johtaa resoluutiosäännöllä joukon  $S_2$  klausuuleista.
- Klausuulijoukkojen  $S_4$  ja  $S_1$  välillä on vastaava suhde:  $\{B, C\}$  on johdettavissa joukon  $S_1$  klausuuleista.

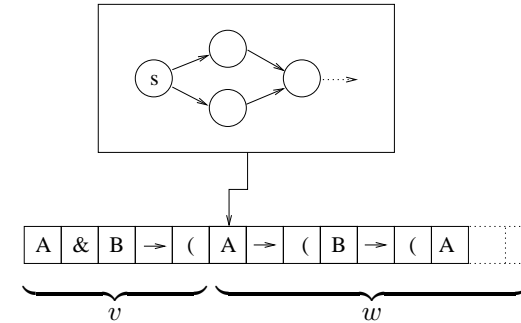


## 8 Laskennallisesta vaativuudesta

- Laskennan malli
- Keskeiset vaativuusluokat
- Redusoituvuus ja vaikeat ongelmat

**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.

Merkkijonot  $v$  ja  $w$  ovat peräkkäin koneen  $T$  työnauhalla:



$T$  käsittelee aina merkkijonon  $w$  ensimmäistä merkkiä, jonka kohdalla koneen luku-kirjoituspään ajatellaan sijaitsevan.



### 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).
- $t: S \times A \rightarrow S \times A \times \{\leftarrow, \rightarrow, \downarrow\}$  on *tilansiirtofunktio*.

**Huomio.** Tyhjää merkkijonoa merkitään symbolilla  $\epsilon$ .

### Laskennan määritelmä

- 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  $s' \in \{k, e, p\}$ .



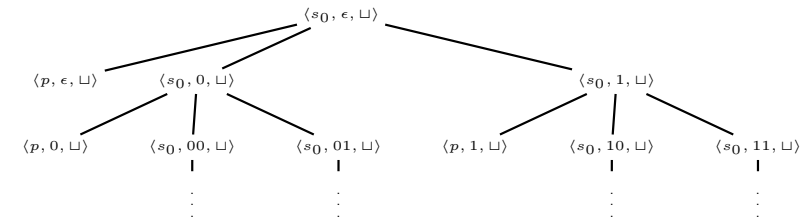
**Määritelmä.** Turing-koneen  $T$  laskenta on sekvenssi konfiguraatioita  $\langle s_0, v_0, w_0 \rangle \xrightarrow{T} \dots \xrightarrow{T} \langle s_{n-1}, v_{n-1}, w_{n-1} \rangle$  missä  $v_0 = \epsilon$  ja  $s_{n-1} \in \{k, e, p\}$ . Kone  $T$  hyväksyy syötteen  $w_0$ , joss  $s_{n-1} = k$ .

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

$S$	$A$	$S \times A \times \{\rightarrow, \leftarrow, \downarrow\}$	Syötteellä 101 $T_{\text{par}}$ suorittaa seuraavan laskennan:
$s_0$	0	$\langle s_0, 0, \rightarrow \rangle$	$\langle s_0, \epsilon, 101 \rangle$
$s_0$	1	$\langle s_1, 1, \rightarrow \rangle$	$\xrightarrow{T_{\text{par}}} \langle s_1, 1, 01 \rangle$
$s_0$	$\sqcup$	$\langle k, \sqcup, \downarrow \rangle$	$\xrightarrow{T_{\text{par}}} \langle s_1, 10, 1 \rangle$
$s_1$	0	$\langle s_1, 0, \rightarrow \rangle$	$\xrightarrow{T_{\text{par}}} \langle s_0, 101, \sqcup \rangle$
$s_1$	1	$\langle s_0, 1, \rightarrow \rangle$	$\xrightarrow{T_{\text{par}}} \langle k, 101, \sqcup \rangle$
$s_1$	$\sqcup$	$\langle e, \sqcup, \downarrow \rangle$	

## Epädeterministisen laskennan piirteitä

- Vaihtoehtoista laskentoja muodostuu *laskentapuun*:



**Huomio.** Deterministisellä Turing-koneella on vain yksi mahdollinen laskenta, joten vastaavassa laskentapuussa on vain yksi haara.



## 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:  $\langle s_0, \epsilon, \sqcup \rangle \xrightarrow{T} \langle s_0, 1, \sqcup \rangle \xrightarrow{T} \langle s_0, 10, \sqcup \rangle \xrightarrow{T} \langle s_0, 101, \sqcup \rangle \xrightarrow{T} \langle p, 101, \sqcup \rangle$ .

## Kielen hyväksyminen Turing-koneella

- Deterministinen Turing-kone  $T$  hyväksyy syötteen  $x \in (A - \{\sqcup\})^*$ , joss koneen  $T$  laskenta syötteellä  $x$  pysähtyy tilaan  $k$ .
  - Deterministinen Turing-kone  $T$  *hyväksyy kielen*  $L \subseteq (A - \{\sqcup\})^*$ , joss kaikille  $x \in (A - \{\sqcup\})^*$ : kone  $T$  hyväksyy syötteen  $x \iff x \in L$ .
- Esimerkki.** Edellä esitetty binääriluvun pariteetin tarkastava kone  $T_{\text{par}}$  hyväksyy vastaavan kielen  $L_{\text{parillinen}} \subseteq \{0, 1\}^*$ .
- Epädeterministisellä koneella hyväksyviä laskentoja voi olla useita ja täten hyväksymisehdosta tulee monimutkaisempi.

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





## Turing-koneiden käyttö päätösongelmien ratkaisemiseen

- **Päätösongelmat** ovat ongelmia, joiden instanssien ratkaisuksi riittää yksinkertainen vastaus "kyllä" tai "ei".

**Esimerkki.** Onko 561 alkuluku?

- Päätösongelman  $O$  ratkaiseminen Turing-koneella edellyttää ongelmainstanssien esittämistä merkkijonoina ja Turing-koneen  $T$  konstruointia "kyllä"-instansseja vastaavan kielen hyväksymiseen.

**Esimerkki.** Lauselogiikan toteutuvuusongelmassa SAT:ssa on tarkoituksena selvittää, onko annettu lause  $\phi \in \mathcal{L}$  toteutuva vai ei.

SAT-ongelmaa vastaava kieli ("kyllä"-instanssien joukko) on siis toteutuvien lauseiden  $\phi$  joukko (lauseet merkkijonoesityksinä).

$\implies$  SAT-ongelma voidaan samaistaa em. kielen kanssa.

**Väite.** SAT kuuluu luokkaan NP.

**Todistuksen idea:**

Voidaan konstruoida epädeterministinen Turing-kone  $T$ , joka

- valitsee epädeterministisesti totuusjakeun  $\mathcal{A}$ ,
- laskee syötteenä  $\phi$  annetun lauseen totuusarvon  $\mathcal{A}$ :ssa ja
- pysähtyy tilaan  $k$ , jos  $\mathcal{A} \models \phi$ , ja muutoin tilaan  $e$ .

Tarvittava laskenta pystytään suorittamaan polynomisessa ajassa lauseen  $\phi$  merkkijonoesityksen pituuden suhteen.

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



## 8.2 Keskeiset vaativuusluokat

- Päätösongelmien laskennallista vaativuutta voidaan analysoida asettamalla Turing-koneiden laskentaresursseille rajoituksia.

**Määritelmä.** Turing-kone  $T$  pysähtyy polynomisessa ajassa syötteen pituuden suhteen, joss 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

**P:** päätösongelmat, joiden instanssit voidaan ratkaista polynomisessa ajassa **deterministisellä** Turing-koneella.

**NP:** päätösongelmat, joiden instanssit voidaan ratkaista polynomisessa ajassa **epädeterministisellä** Turing-koneella.

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

## 8.3 Redusoituvuus ja vaikeat ongelmat

- Ongelman  $O_1$  **reduoituvuus** ongelmaksi  $O_2$  edellyttää, että löytyy instanssin  $i$  pituuden suhteen polynomisessa ajassa deterministisellä Turing-koneella laskettava funktio  $r : O_1 \rightarrow O_2$  siten, että

$$i \in O_1 \iff r(i) \in O_2.$$

- Tällaista funktiota  $r$  kutsutaan usein **reduktioksi**.

**Esimerkki.** Olkoon  $G = \langle S, K \rangle$  graafi, missä  $K \subseteq S \times S$  antaa kaaret.

Ongelma graafin  $G$  kolmiväritettävyydestä (3COL) voidaan redusoida lauselogiikan toteutuvuusongelmaksi seuraavasti:  $r(G) = r(\langle S, K \rangle) =$

$$\{M_s \vee V_s \vee H_s \mid s \in S\} \cup \{\neg M_s \vee \neg M_t, \neg V_s \vee \neg V_t, \neg H_s \vee \neg H_t \mid \langle s, t \rangle \in K\}.$$

Nyt voidaan osoittaa, että  $G \in \text{3COL} \iff r(G) \in \text{SAT}$ .



## Vaikeat ja täydelliset ongelmat

**Määritelmä.** Olkoon  $C$  jokin luokka ongelmia (kuten  $P$  tai  $NP$ ). Ongelma  $O$  on

1.  $C$ -*vaikea*, joss jokainen luokan  $C$  ongelma  $O'$  voidaan redusoida  $O$ :ksi polynomisessa ajassa ja
  2.  $C$ -*täydellinen*, joss  $O$  kuuluu luokkaan  $C$  ja  $O$  on  $C$ -vaikea.
- $\implies$   $C$ -täydelliset ongelmat ovat vaativimpia luokan  $C$  ongelmia.

**Väite.** SAT on  $NP$ -vaikea (Cook, 1971).

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

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

## DPLL-algoritmi

Olkoon  $S$  äärellinen klausuulijoukko ja  $L$  joukko literaaleja.

**Funktio**  $\text{OnToteutuva}(S, L): \{K, E\}$ ;

**Aloita**

$\langle S, L \rangle := \text{Yksinkertaista}(S, L)$ ;

**Jos**  $\square \in S$ , **Niin Vastaa**  $E$ ;

**Jos**  $S = \emptyset$ , **Niin Vastaa**  $K$ ;

$l := \text{Valitse}(S, L)$ ;

**Jos**  $\text{OnToteutuva}(S, L \cup \{l\})$ , **Niin Vastaa**  $K$

**Muutoin Vastaa**  $\text{OnToteutuva}(S, L \cup \{\bar{l}\})$ ;

**Lopeta**



$\implies$  SAT on  $NP$ -täydellinen ongelma.

## Huomioita.

- Näin ollen *epädeterministisen* Turing-koneen suorittama polynominen, syötteen hyväksyvä laskenta voidaan palauttaa polynomisessa ajassa lauselogiikan toteutuvuusongelman ratkaisemiseen.
- Nykykäsitysten mukaisesti SAT-ongelman ratkaiseminen *deterministisellä* Turing-koneella vaatii pahimmassa tapauksessa eksponentiaalisen ajan lauseen pituuteen nähden.
- Tehokas algoritmi: Davis-Putnam-Logemann-Loveland [1961,1962]
- Käytettävällä hakuheuristiikalla on kuitenkin olennainen vaikutus DPLL-algoritmin suorituskykyyn.

## Huomioita

- Funktion  $\text{Yksinkertaista}(S, L)$  tehtävänä on yksinkertaistaa klausuulijoukkoa  $S$  ja laajentaa literaalijoukkoa  $L$  hyödyntämällä literaaleja  $l$ , joille  $l \in L$  tai klausuuli  $\{l\} \in S$ , rekursiivisesti:
  1. Lisätään  $l$  joukkoon  $L$ , mikäli se ei siellä vielä ole.
  2. Poistetaan joukosta  $S$  toteutuneet klausuulit  $C \in S$ , joille  $l \in C$ , ja literaalin  $\bar{l}$  esiintymät  $S$ :n klausuuleista (ovat epätosia).
- Funktio  $\text{Valitse}(S, L)$  toteuttaa *hakuheuristiikan* eli valitsee literaalin  $l$  (s.e.  $l \notin L$  ja  $\bar{l} \notin L$ ), joka esiintyy joukossa  $S$  ja jonka suhteen haku seuraavaksi haarautuu.
- Tehokkaita DPLL-toteutuksia, näiden vertailuja ja benchmark-ongelmia on saatavilla verkossa; kts. esim. [www.satlive.org](http://www.satlive.org) ja [www.satcompetition.org](http://www.satcompetition.org).