Boolen funktioiden ja lauselogiikan yhteys

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

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

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

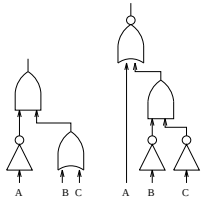
Väite. Olkoon f boolen funktio ja lause ϕ sitä vastaava esitys:

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

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

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

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



Taulumenetelmän ominaisuuksia

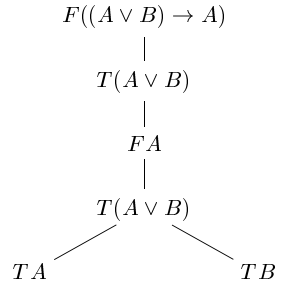
Väite. Todistusmenetelmän virheettömyys: Jos lause α on todistettavissa semanttisella taululla ($\vdash \alpha$), niin α on pätevä ($\models \alpha$).

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

Kirjassa osoitetaan, että:

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

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



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

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

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

Olkoon valuaatio $\mathcal{V}$ seuraavanlainen.

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

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

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

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

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

Lauseen toteutuvuuden tutkiminen

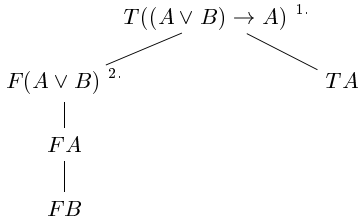
Määritelmä. Lause α on *toteutuva*, jos ja vain jos on olemassa valuaatio $\mathcal{V}$ siten, että $\mathcal{V}(\alpha) = T$.

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

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

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

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



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

Johdettavuus lausejoukosta

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

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

		$T\alpha_1$
	$\Sigma \models \beta$	$\vdots$
joss	$\Sigma \cup \{\neg\beta\}$	$\vdots$
	ei ole toteutuva	$T\alpha_n$
joss	$\Sigma \vdash \beta$	$F\beta$
		$\vdots$

Hilbert-tyyppinen lauselogiikan aksiomatisointi

Aksioomat:

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

Päättelysääntö:

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

(modus ponens)

Määritelmä. Olkoon Σ joukko lauseita.

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

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

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

Lause α on *teoreema* (todistuva) jos se on johdettavissa tyhjästä lausejoukosta $\Sigma = \emptyset$. ($\vdash \alpha$)

Esimerkki. Osoitetaan $\{A, B \to (A \to C)\} \vdash B \to C$.

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

Normaalimuodot

- Polynomien esittäminen muodossa:

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

- Lineaaristen yhtälöryhmien esittäminen matriiseina:

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

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

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

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

Esimerkki.

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

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

Esimerkki.

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

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

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

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

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

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

1. Poista konnektiivit $\leftrightarrow$ seuraavanlaisilla korvauksilla:

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

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

2. Poista konnektiivit $\rightarrow$ seuraavanlaisilla korvauksilla:

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

3. Siirrä negaatiot välittömästi atomisten lauseiden eteen:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Kokeile näiden normaalimuotojen johtamista myös muunnossäännöillä !!!