Luento 4: Klassiset todistusjärjestelmät

1. Hilbertin järjestelmä
2. Suppesin järjestelmä
3. Järjestelmien välistä vertailua

1. HILBERTIN JÄRJESTELMÄ

- Tavoitteena on tuottaa joko päteviä lauseita tai vaihtoehtoisesti jonkin lausejoukon Σ loogisia seurauksia *syntaktisesti*.
- Aksiomia A1–A3 käytetään valitsemalla alilauseiksi α, β ja γ jotkin konkreettiset lauseet (aksioman ilmentymä).
- Modus ponens -sääntö mahdollistaa seurauksen β päättelemisen, jos implikaatio $\alpha \rightarrow \beta$ ja sen ehto α on saatu muutoin pääteltyä.

Määritelmä 5.2 Hilbertin todistusjärjestelmä perustuu seuraaviin *aksiomiin* A1–A3 ja *modus ponens* -päättelysääntöön (MP):

A1: $\alpha \rightarrow (\beta \rightarrow \alpha)$

A2: $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$

A3: $(\neg\beta \rightarrow \neg\alpha) \rightarrow ((\neg\beta \rightarrow \alpha) \rightarrow \beta)$

MP: $$\frac{\alpha \rightarrow \beta \qquad \alpha}{\beta}$$

Rajoitettu syntaksi

- Hilbertin järjestelmässä käytetään konnektiiveina ainoastaan negaatiota ($\neg$) ja implikaatiota ($\rightarrow$).
- Muut lauselogiikan peruskonnektiivit voidaan lausua negaation ja implikaation avulla seuraavasti:

$$\alpha \land \beta \equiv \neg\neg(\alpha \land \beta) \equiv \neg(\neg\alpha \lor \neg\beta) \equiv \neg(\alpha \rightarrow \neg\beta) \tag{5.1}$$

$$\alpha \lor \beta \equiv \neg\neg\alpha \lor \beta \equiv \neg\alpha \rightarrow \beta \tag{5.2}$$

$$\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \land (\beta \rightarrow \alpha) \equiv \neg((\alpha \rightarrow \beta) \rightarrow \neg(\beta \rightarrow \alpha)) \tag{5.3}$$

Esimerkki 5.1 Lamppuesimerkin lauseet saadaan muotoon $L \rightarrow P$,

$$P \land L \rightarrow K \quad \rightsquigarrow \quad \neg(P \rightarrow \neg L) \rightarrow K$$

ja vastaavasti $\neg(P \rightarrow \neg K) \rightarrow L$. ■

Todistukset Hilbertin järjestelmässä

Määritelmä 5.3 *Todistus* lausejoukosta $\Sigma \subseteq \mathcal{L}$ on jono $\alpha_1, \ldots, \alpha_n$ (rajoitetun) kielen $\mathcal{L}$ lauseita siten, että kaikille $i \in \{1, \ldots, n\}$ pätee:

1. lause $\alpha_i \in \Sigma$, tai
2. lause α_i on jokin aksiomien A1, A2, tai A3 ilmentymä, tai
3. lause α_i on voidaan päätellä modus ponens -säännöllä joistain jonon edeltävistä lauseista α_j ja $\alpha_k = (\alpha_j \rightarrow \alpha_i)$.

Määritelmä 5.4 Lause ϕ on *johdettavissa* lausejoukosta Σ Hilbertin järjestelmällä (merkitään $\Sigma \vdash_{\mathrm{H}} \phi$), jos ja vain jos on olemassa todistus $\alpha_1, \ldots, \alpha_n$ lausejoukosta Σ siten, että $\phi = \alpha_n$.

Määritelmä 5.5 Lause ϕ on *teoreema* / *todistuva* Hilbertin järjestelmällä (merkitään $\vdash_{\mathrm{H}} \phi$), jos ja vain jos $\emptyset \vdash_{\mathrm{H}} \phi$.

Esimerkki

Esimerkki 5.6 Johdetaan $B \to C$ *premissijoukosta* $\{A, B \to (A \to C)\}$:

1.	A	P
2.	$B \to (A \to C)$	P
3.	$A \to (B \to A)$	A1
4.	$B \to A$	MP, 1, 3
5.	$(B \to (A \to C)) \to ((B \to A) \to (B \to C))$	A2
6.	$(B \to A) \to (B \to C)$	MP, 2, 5
7.	$B \to C$	MP, 4, 6

$\Longrightarrow \{A, B \to (A \to C)\} \vdash_{\mathrm{H}} B \to C$

$\Longrightarrow \{\alpha \to (\beta \to \gamma), \beta\} \vdash_{\mathrm{H}} \alpha \to \gamma$ (edeltävä todistus yleistäen). ■

Virheettömyys

Väite 5.7 Jos lausejono $\alpha_1, \ldots, \alpha_n$ on todistus lausejoukosta Σ Hilbertin järjestelmässä, niin $\Sigma \models \alpha_i$ kaikille $i \in \{1, \ldots, n\}$.

Todistus. Kaikki aksiomien A1–A3 ilmentymät ovat päteviä lauseita. Todistetaan väite täydellisellä induktiolla indeksin $i \geq 1$ suhteen.

- **Perustapaus:** $i = 1$.

  Jos α_1 on aksiomien A1–A3 ilmentymä, niin $\models \alpha_1$ ja $\Sigma \models \alpha_1$. Jos $\alpha_1 \in \Sigma$, niin $\Sigma \models \alpha_1$ (looginen sulkeuma).

- **Induktioaskel:** $i > 1$.

  Jos α_i on aksiomien A1–A3 ilmentymä tai $\alpha_i \in \Sigma$, niin $\Sigma \models \alpha_i$.

  Jos α_i pääteltiin modus ponensilla lauseista α_j ja $\alpha_k = (\alpha_j \to \alpha_i)$, niin $\Sigma \models \alpha_j$ ja $\Sigma \models \alpha_j \to \alpha_i$ (induktiohypoteesi). Siis $\Sigma \models \alpha_i$. □

Täydellisyys

Apulause 5.8 Kaikille lausejoukoille $\Sigma \subseteq \mathcal{L}$ ja lauseille $\alpha, \beta \in \mathcal{L}$,

$$\Sigma \cup \{\alpha\} \vdash_{\mathrm{H}} \beta, \text{ jos ja vain jos } \Sigma \vdash_{\mathrm{H}} \alpha \to \beta.$$

Apulause 5.12 Olkoon $\phi \in \mathcal{L}$ lause ja $\mathrm{At}(\phi)$ sen atomilauseiden joukko, $\mathcal{A} \subseteq \mathrm{At}(\phi)$ totuusjakelu ja $\mathrm{Lit}(\mathcal{A}) = \mathcal{A} \cup \{\neg A \mid A \in \mathrm{At}(\phi) \setminus \mathcal{A}\}$.

1. Jos $\mathcal{A} \models \phi$, niin $\mathrm{Lit}(\mathcal{A}) \vdash_{\mathrm{H}} \phi$.
2. Jos $\mathcal{A} \not\models \phi$, niin $\mathrm{Lit}(\mathcal{A}) \vdash_{\mathrm{H}} \neg\phi$.

Teoreema 5.13 Kaikille rajoitetun synktaksin (konnektiivit $\neg$, $\to$) mukaisille äärellisille lausejoukoille $\Sigma \subseteq \mathcal{L}$ ja lauseille $\phi \in \mathcal{L}$,

$$\Sigma \vdash_{\mathrm{H}} \phi, \text{ jos ja vain jos } \Sigma \models \phi.$$

2. SUPPESIN JÄRJESTELMÄ

➤ Suppesin *luonnollisen päättelyn* järjestelmässä ei ole aksiomia, mutta päättelysääntöjä on varsin kattava valikoima:

MP (modus ponens):

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

TT (modus tollendo tollens):

$$\frac{\alpha \to \beta \qquad \neg\beta}{\neg\alpha}$$

TP (modus tollendo ponens):

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

Vaihtosäännöt:

KV: $\dfrac{\alpha \wedge \beta}{\beta \wedge \alpha}$ DV: $\dfrac{\alpha \vee \beta}{\beta \vee \alpha}$

Tuonti- ja eliminointisäännöt

➤ Negaatioista, konjunktioista, disjunktioista ja ekvivalensseista tehdään päätelmiä *tuonti-* (T) ja *eliminointisäännöillä* (E):

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

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

De Morganin säännöt ja syllogismit

➤ De Morganin säännöt liittyvät negaatioiden uudelleenjärjestelyyn ja syllogismisäännöt implikaatioiden yhdistelyyn/soveltamiseen:

DM1: $\dfrac{\alpha\wedge\beta}{\neg(\neg\alpha\vee\neg\beta)}$ DM2: $\dfrac{\neg(\alpha\wedge\beta)}{\neg\alpha\vee\neg\beta}$ DM3: $\dfrac{\alpha\vee\beta}{\neg(\neg\alpha\wedge\neg\beta)}$ DM4: $\dfrac{\neg(\alpha\vee\beta)}{\neg\alpha\wedge\neg\beta}$

HS (hypoteettinen syllogismi): $\dfrac{\alpha\rightarrow\beta \qquad \beta\rightarrow\gamma}{\alpha\rightarrow\gamma}$

DS (disjunktiivinen syllogismi): $\dfrac{\alpha\vee\beta \qquad \alpha\rightarrow\gamma \qquad \beta\rightarrow\delta}{\gamma\vee\delta}$

Ehdollinen ja epäsuora todistaminen

➤ Tarkastellaan seuraavia päättelysääntöjä:

ET: $\dfrac{\begin{matrix}[\alpha]\\ \vdots \\ \beta\end{matrix}}{\alpha\rightarrow\beta}$ ES: $\dfrac{\neg\beta\rightarrow\alpha\wedge\neg\alpha}{\beta}$

➤ *Ehdollisen todistamisen* yhteydessä tehty *apuolettamus* perutaan, kun implikaatio $\alpha\rightarrow\beta$ päätellään säännöllä (ET).

➤ *Epäsuora todistaminen* (ES) perustuu vastaoletuksesta $\neg\beta$ seuraavaan ristiriitaan $\alpha\wedge\neg\alpha$, jolloin voidaan päätellä β.

Todistukset Suppesin järjestelmässä

Määritelmä 5.15 Suppes-todistus lausejoukosta $\Sigma\subseteq\mathcal{L}$ on jono $\alpha_1,\ldots,\alpha_n$ kielen $\mathcal{L}$ lauseita, joihin liittyy apuolettamusten joukot $H_0=\emptyset$ ja $H_1,\ldots,H_n$ siten, että kaikille $i\in\{1,\ldots,n\}$:

1. $H_i=H_{i-1}$ ja $\alpha_i\in\Sigma$.
2. $H_i=H_{i-1}\cup\{\alpha_i\}$ ja α_i on uusi apuolettamus $\alpha_i\notin H_{i-1}$.
3. $H_i=H_{i-1}$ ja α_i on päätelty muilla säännöillä (paitsi ET) jonon aikaisemmista lauseista α_j $(j<i)$, joille $H_j\subseteq H_{i-1}$.
4. $H_i=H_{i-1}$ ja $\alpha_i=\alpha_j$ jollekin jonon aikaisemmalle lauseelle α_j $(j<i)$, jolle $H_j\subseteq H_{i-1}$.
5. $H_i=H_{i-1}\setminus\{\alpha_j\}$ ja $\alpha_i=\alpha_j\rightarrow\alpha_{i-1}$ on saatu säännöllä ET viimeisimmästä apuolettamuksesta α_j $(j<i)$ ja lauseesta α_{i-1}.

Esimerkki

Esimerkki 5.17 Osoitetaan $\{A, B \to (A \to C)\} \vdash_S B \to C$:

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

■

Huomio Apuolettamusten joukoista voidaan pitää kirjaa tekemällä todistukseen sisennyksiä, jolloin joukot H_i voidaan jättää pois.

Virhettömyys ja täydellisyys

Määritelmä 5.16

1. Lause $\phi \in \mathcal{L}$ on *johdettavissa* Suppesin järjestelmällä lausejoukosta $\Sigma \subseteq \mathcal{L}$ (merkitään $\Sigma \vdash_S \phi$), jos ja vain jos joukosta Σ on Suppes-todistus $\alpha_1, \ldots, \alpha_n$ siten, että $\alpha_n = \phi$ ja $H_n = \emptyset$.
2. Lause $\phi \in \mathcal{L}$ on *teoreema/todistuva* Suppesin järjestelmässä (merkitään $\vdash_S \phi$), jos ja vain jos $\emptyset \vdash_S \phi$.

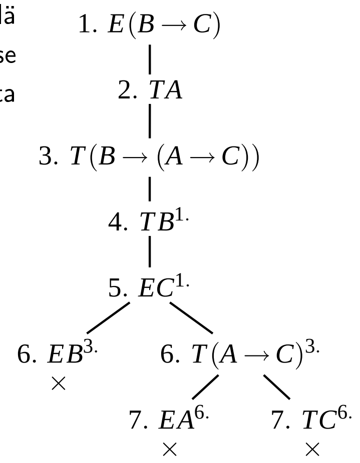
Huomio Kaikki apuolettamukset on muistettava purkaa ($H_n = \emptyset$)!

Teoreema 5.18 (Virheettömyys ja täydellisyys) Kaikille äärellisille lausejoukoille $\Sigma \subseteq \mathcal{L}$ ja lauseille $\phi \in \mathcal{L}$:

$$\Sigma \vdash_S \phi, \text{ jos ja vain jos } \Sigma \models \phi.$$

3. JÄRJESTELMIEN VERTAILUA

Esimerkki 5.19 Osoitetaan vielä semanttisella taululla, että lause $B \to C$ johdettavissa lausejoukosta $\Sigma = \{A, B \to (A \to C)\}$.



Klassisten todistusjärjestelmien piirteitä

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.

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.

Taulumenetelmän piirteitä

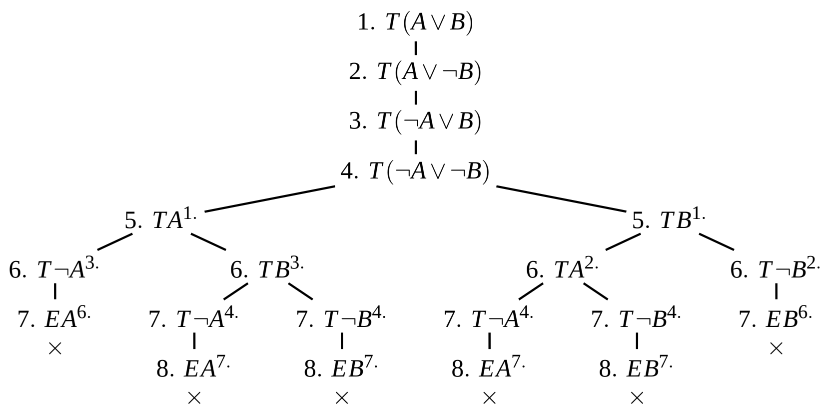
+ Lauseissa voi esiintyä kaikkia peruskonnektiiveja.
+ Lauseiden syntaksi ohjaa päättelysäännön (taulusäännöt) valintaa.
+ Mikäli lause ei ole todistuva/johdettavissa voidaan muodostaa konkreettinen vastaesimerkki eli *vastamalli* $\mathcal{A}$.
+ Helppo toteuttaa tietokoneella (vaatii lineaarisen tilan).

– Menetelmä ei ole mahdollisimman tehokas, vaikka tarjoaa hyvän lähtökohdan lauselogiikan päättelytehtävien toteuttamiselle.

➤ Semanttisia tauluja voidaan tehostaa lisäämällä taulusääntöjä.

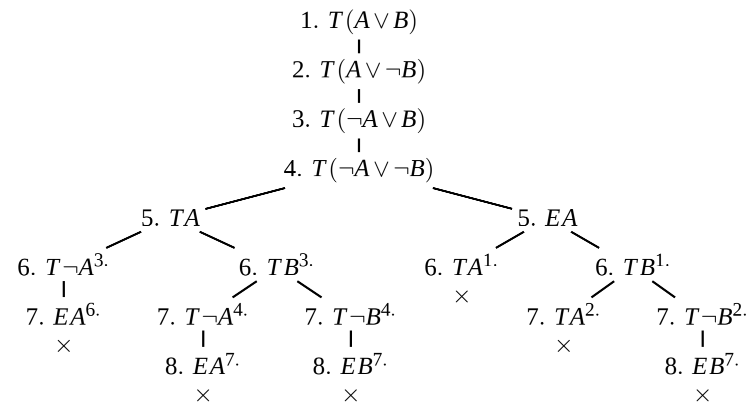
➤ Esimerkkinä mainittakoon ns. *cut-sääntö*, joka haarauttaa polun jonkin väittämän α suhteen ($T\alpha$ ja $E\alpha$). Käytettävä säästeliäästi!

Esimerkki



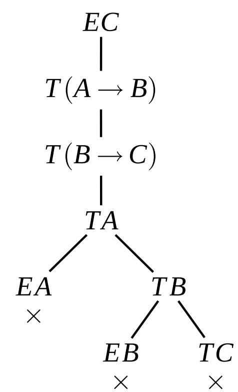
$\Longrightarrow$ Semanttisten polkujen lukumäärä voi kasvaa eksponentiaalisesti atomisten lauseiden lukumäärään nähden.

Jatkoesimerkki

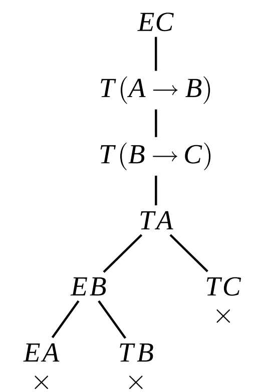


$\Longrightarrow$ Cut-säännön avulla taulu jää hieman pienemmäksi.

Klassisten järjestelmien simulointi



"Modus ponens"



"Modus tollendo tollens"

TAVOITTEET

- Ymmärrät, mitä perinteisesti tarkoitetaan *todistuksen* käsitteellä (jono aksiomilla ja päättelysäännöillä tuotettuja lauseita).
- Tunnet erityisesti Suppes-järjestelmän päättelysäännöt ja osaat hyödyntää niitä yksittäisten todistusten hakemisessa.
- Osaat käyttää erityisesti *ehdollisen* ja *epäsuoran* todistamisen periaatteita matemaattisissa todistuksissa.
- Tiedät semanttisiin tauluhin perustuvan todistusmenetelmän edut verrattuna klassisiin todistusjärjestelmiin.

PÄIVÄN PÄHKINÄ

Tarkastellaan konnektiiveihin $\neg$ ja $\rightarrow$ rajoitettua lauselogiikan kieltä $\mathcal{L}$ sekä seuraavia päättelysääntöjä:

IE:
$$\frac{\alpha \qquad \neg\beta}{\neg(\alpha \rightarrow \beta)}$$

IT1:
$$\frac{\neg\alpha}{\alpha \rightarrow \beta}$$

IT2:
$$\frac{\beta}{\alpha \rightarrow \beta}$$

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

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

TA:
$$\frac{\alpha \rightarrow \beta \qquad \neg\alpha \rightarrow \beta}{\beta}$$

Onko näihin implikaation ja negaation totuusarvot laskeviin sääntöihin (IE, IT1–2, NE, NT), *tapausanalyysiin* (TA) ja *ehdolliseen todistamiseen* (ET) perustuva menetelmä virheetön ja täydellinen?