

Lauseloogika: Hilberti süsteem

- Hilberti süsteemid on klass *tõestussüsteeme* (proof systems).
- Tõestussüsteemid on vahendid semantiliste üldkehtivuse ja loogilise järeldivuse argumentide formaalseks esitamiseks. Tõestussüsteemi põhiülesanne on loogilise või matemaatilise keele kõigi valemite hulgast eraldada välja teatud alamhulk—teoreemid. Teoreemideks loetakse need valemid, mida kindlatest lähtevalemitest ehk aksioomidest kindlaid tuletusreegleid (inference rules) lõplik arv kordi rakendades on võimalik tuletada.
Taotlus on, et valem oleks teoreem parajasti siis, kui ta on üldkehtiv.
- Hilberti süsteemid: võimalikult vähe tuletusreegleid, aksioome (õieti aksioomiskeeme) võib olla palju.

- Lauseloogika Hilberti süsteem (üks mitmetest võimalikest):
 - Aksiomid (õieti aksiomiskeemid):

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

- Üks tuletusreegel:

$$\frac{A \quad A \supset B}{B} \quad (\text{modus ponens})$$

- Valemi A *tõestused* (proofs) on hulk valemipuid, mis on defineeritud induktiivselt järgmiselt:

- kui A on aksiom, siis A (kui ühetipuline valemipuu) on A tõestus;
- kui A_1, \dots, A_n ja B moodustavad tuletusreegli rakenduse ning

$$\frac{\mathcal{D}_1 \quad \mathcal{D}_n}{A_1 \dots A_n} \text{ on valemite } A_1, \dots, A_n \text{ tõestused, siis } \frac{\mathcal{D}_1 \quad \mathcal{D}_n}{A_1 \dots A_n} \frac{B}{B}$$

on valemi B tõestus.

- Valem A on *tõestatav* (provable) ehk *teoreem* (tähistus $\vdash A$), kui A -le leidub tõestus.

- Valem A *tuletused* (derivations) valemite hulgast Γ on hulk valemipuid, mis on defineeritud induktiivselt järgmiselt:
 - kui $A \in \Gamma$, siis A (kui ühetipuline valemipuu) on A tuletus Γ -st;
 - kui A on aksiom, siis A (kui ühetipuline valemipuu) on A tuletus Γ -st;
 - kui A_1, \dots, A_n ja B moodustavad tuletusreegli rakenduse ning

$$\frac{\begin{array}{c} \mathcal{D}_1 \quad \mathcal{D}_n \\ A_1, \dots, A_n \end{array}}{B} \text{ on valemite } A_1, \dots, A_n \text{ tõestused, siis } \frac{\mathcal{D}_1 \quad \dots \quad \mathcal{D}_n}{A_1 \quad \dots \quad A_n} \text{ on valemi } B \text{ tuletus } \Gamma\text{-st.}$$

- Valem A on valemite hulgast Γ *tuletatav* (derivable) ehk tema *järeldus* (consequence) (tähistus $\Gamma \vdash A$), kui A -le leidub tuletus Γ -st.
- $\emptyset \vdash A$ parajasti siis, kui $\vdash A$ (ehk A on tühjast valemite hulgast tuletatav parajasti siis, kui ta on tõestatav).

- Näide: Valem $p \supset p$ on tõestatav.

$$\frac{\frac{\frac{p \supset (p \supset p)}{p \supset ((p \supset p) \supset p)} \quad (p \supset ((p \supset p) \supset p)) \supset ((p \supset (p \supset p)) \supset (p \supset p))}{(p \supset (p \supset p)) \supset (p \supset p)}}{p \supset p}$$

- Näide: Valem $q \supset r$ on valemitest p ja $q \supset (p \supset r)$ tuletatav.

$$\frac{\frac{p \quad p \supset (q \supset p)}{q \supset p} \quad \frac{q \supset (p \supset r) \quad (q \supset (p \supset r)) \supset ((q \supset p) \supset (q \supset r))}{(q \supset p) \supset (q \supset r)}}{q \supset r}$$

- Osutub, et toodud Hilberti süsteem on lauseloogika jaoks perfektne tõestussüsteem: korrektne ja täielik (tõestusi me siinkohal ei too).
- *Korrekttsuse teoreem*: Kui $\vdash A$, siis $\models A$. Veel enam, kui $\Gamma \vdash A$, siis $\Gamma \models A$.
Sõnades: Tõestatavusest jäeldub loogiline tõesus, tuletatavusest jäeldub loogiline jäelduvus.
- *Täielikkuse teoreem*: Kui $\models A$, siis $\vdash A$. Veel enam, kui $\Gamma \models A$, siis $\Gamma \vdash A$.
Sõnades: Loogilisest tõesusest jäeldub tõestatavus, loogilisest jäelduvusest jäeldub tuletatvus.
- Siit aga ei tulene, et Hilberti süsteem oleks eriti kasulik praktiliseks tautoloogiakontrolliks tõestatavuskontrolli kaudu.

- Järgnev deduktsiooniteoreem võimaldab tuletusi drastiliselt lühendada ning on abiks ka täielikkuse teoreemi tõestamisel.
- Deduktsiooniteoreem: Kui $\Gamma \cup \{A\} \vdash B$, siis $\Gamma \vdash A \supset B$.
(Paneme tähele, et vastupidine kehtib ka, aga triviaalselt.)
- Tõestus. Induktsiooniga B tuletuse järgi ($\Gamma \cup \{A\}$)-st.
 - Kui B tuletus ($\Gamma \cup \{A\}$)-st on ühetipuline puu B , siis $B \in \Gamma$, $B = A$ või B on aksioom. Kui $B = A$, siis $\Gamma \vdash A \supset B$ meie vastse tähelepaneku põhjal, et $\vdash A \supset A$. Kui $B \in \Gamma$ või B on aksioom, siis on $A \supset B$ Γ -st tuletatav järgmiselt:

$$\frac{\begin{array}{c} \vdots \\ B \end{array} \quad \overline{B \supset (A \supset B)}}{A \supset B}$$

- Vastasel korral on B tuletusel $(\Gamma \cup \{A\})$ -st kuju

$$\frac{\begin{array}{c} \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ C \supset B \end{array}}{B}$$

ning induktsiooni eelduse põhjal on siis $A \supset C$ ja $A \supset (C \supset B)$ Γ -st tuletatavad. Sel juhul $A \supset B$ Γ -st tuletatav järgmiselt:

$$\frac{\begin{array}{c} \vdots \\ A \supset C \end{array} \quad \frac{A \supset (C \supset B) \quad \overline{(A \supset (C \supset B)) \supset (A \supset C) \supset (A \supset B)}}{(A \supset C) \supset (A \supset B)}}{A \supset B}$$

- Näide: Kuna me veendusime, et $p, q \supset (p \supset r) \vdash q \supset r$, siis deduktsiooniteoreemi põhjal võime olla kindlad, et $p \supset ((q \supset (p \supset r)) \supset (q \supset r))$.