Lõplikud disjunktsioonid ja konjunktsioonid

- Kuna binaarne disjunktsioon ja binaarne konjunktsioon on assotsiatiivsed ja omavad ühikuid falsum ja verum ning on pealegi kommutatiivsed ja idempotentsed, siis alternatiivselt võiksime nende asemel kasutada lõplikke disjunktsioone ja konjunktsioone:

$$\begin{array}{rclrcl} \bigvee \emptyset & = & \bot & \bigwedge \emptyset & = & \top \\ \bigvee \{A\} & = & A & \bigwedge \{A\} & = & A \\ \bigvee (A \cup \Gamma) & = & A \vee \bigvee \Gamma & \bigwedge (A \cup \Gamma) & = & A \wedge \bigwedge \Gamma \end{array}$$

Praktikas kirjutame $\bigvee \{A_1, \ldots, A_n\}$ asemel lihtsalt $A_1 \vee \ldots \vee A_n$ ning $\bigwedge \{A_1, \ldots, A_n\}$ asemel lihtsalt $A_1 \wedge \ldots \wedge A_n$, arvestades, et valemite esinemise järjekord ja kordsus nimistus $A_1, \ldots, A_n$ ei ole oluline.

Lauseloogika: Normaalkujud

- Lauseloogika keel süntaks on liiane selles mõttes, et üht ja sama tõeväärtusfunktsiooni saab väljendada paljude erinevate valemitega.
- *Literaal* on valem kujul p või $\neg p$, kus p on lausesümbol.
- *Elementaardisjunktsioon* on $l_1 \vee \ldots \vee l_n$, kus $\{l_1, \ldots, l_n\}$ on lõplik hulk literaale.
- *Elementaarkonjunktsioon* on $l_1 \wedge \ldots \wedge l_n$, kus $\{l_1, \ldots, l_n\}$ on lõplik hulk literaale.
- *Konjunktiivne normaalkuju* on $c_1 \wedge \ldots \wedge c_m$, kus $\{c_1, \ldots, c_m\}$ on lõplik hulk elementaardisjunktsioone.
- *Disjunktiivne normaalkuju* on $c_1 \vee \ldots \vee c_m$, kus $\{c_1, \ldots, c_m\}$ on lõplik hulk elementaarkonjunktsioone.

- Iga valemi jaoks saab järkjärgulise ümberkirjutamise teel leida temaga loogiliselt ekvivalentse konjunktiivse või disjunktiivse normaalkuju.
  Teisendusalgoritm:
  - implikatsioonid ära, kasutades $A \supset B \Leftrightarrow \neg A \vee B$,
  - eitused sisse ning kahekordsed eitused ära, kasutades $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$, $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$, $\neg\neg A \Leftrightarrow A$,
  - disjunktsioonid või konjunktsioonid sisse, kasutades $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ ja $A \vee \top \Leftrightarrow \top$ või $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ ja $A \wedge \bot \Leftrightarrow \bot$,
  - kordused ning vastandpaarid elementaardisjunktsioonides ja -konjunktsioonides ära, kasutades idempotentsiseadusi $A \vee A \Leftrightarrow A$, $A \wedge A \Leftrightarrow A$, välistatud kolmanda seadust $A \vee \neg A \Leftrightarrow \top$ ja vastuolu seadust $A \wedge \neg A \Leftrightarrow \bot$,
  - triviaalsed elementaardisjunktsioonid ja -konjuktsioonid ära, kasutades ühikute seadusi $A \wedge \top \Leftrightarrow A$, $A \vee \bot \Leftrightarrow A$
- Saadud kuju võib veel optimeerida kasutades absorptsioone $A \wedge (A \vee B) \Leftrightarrow A$ ja $A \vee (A \wedge B) \Leftrightarrow A$.

Lauseloogika: Hilberti süsteem

- Hilberti süsteemid on klass *tõestussüsteeme* (proof systems).
- Tõestussüsteemid on vahendid semantiliste üldkehtivuse ja loogilise järelduvuse 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):
  - Aksioomid (õieti aksioomiskeemid):

$$A \supset (B \supset A)$$
$$(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$$
$$(A \supset \neg B) \supset ((A \supset B) \supset \neg A)$$
$$\neg\neg A \supset A$$
$$\top$$
$$\bot \supset C$$
$$A \supset (B \supset A \wedge B)$$
$$A \wedge B \supset A$$
$$A \wedge B \supset B$$
$$A \supset A \vee B$$
$$B \supset A \vee B$$
$$(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$$

- Üks tuletusreegel:

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

- Valemi A *tõestused* (proofs) on hulk valemipuid, mis on defineeritud induktiivselt järgmiselt:
  - kui A on aksioom, siis $\overline{A}$ (kui ühetipuline valemipuu) on A tõestus;
  - kui $A_1, \ldots, A_n$ ja B moodustavad tuletusreegli rakenduse ning $\mathcal{D}_1 \quad \mathcal{D}_n$ $A_1, \ldots A_n$ on valemite $A_1, \ldots, A_n$ tõestused, siis $\dfrac{\mathcal{D}_1 \quad \mathcal{D}_n}{\begin{array}{ccc} A_1 & \ldots & A_n \end{array}}{B}$ on valemi B tõestus.
- Valem A on *tõestatav* (provable) ehk *teoreem* (tähistus $\vdash A$), kui A-le leidub tõestus.

- Valemi 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 aksioom, siis $\overline{A}$ (kui ühetipuline valemipuu) on A tuletus Γ-st;
  - kui $A_1, \ldots, A_n$ ja B moodustavad tuletusreegli rakenduse ning $\mathcal{D}_1 \quad \mathcal{D}_n$ $A_1, \ldots A_n$ on valemite $A_1, \ldots, A_n$ tõestused, siis $\dfrac{\begin{array}{ccc}\mathcal{D}_1 & & \mathcal{D}_n \\ A_1 & \ldots & A_n\end{array}}{B}$ on valemi B tuletus Γ-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.

$$\dfrac{\dfrac{}{p \supset (p \supset p)} \qquad \dfrac{\dfrac{}{p \supset ((p \supset p) \supset p)} \qquad \dfrac{}{(p \supset ((p \supset p) \supset p)) \supset ((p \supset (p \supset p)) \supset (p \supset p))}}{(p \supset (p \supset p)) \supset (p \supset p)}}{p \supset p}$$

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

$$\dfrac{\dfrac{p \qquad \dfrac{}{p \supset (q \supset p)}}{q \supset p} \qquad \dfrac{q \supset (p \supset r) \qquad \dfrac{}{(q \supset (p \supset r)) \supset ((q \supset p) \supset (q \supset r))}}{(q \supset p) \supset (q \supset r)}}{q \supset r}$$

- Osutub, et toodud Hilberti süsteem on lauseloogika jaoks perfektne tõestussüsteem: korrektne ja täielik (tõestusi me siinkohal ei too).
- *Korrektsuse teoreem*: Kui $\vdash A$, siis $\models A$. Veel enam, kui $\Gamma \vdash A$, siis $\Gamma \models A$.
  Sõnades: Tõestatavusest järeldub loogiline tõesus, tuletatavusest järeldub loogiline järelduvus.
- *Täielikkuse teoreem*: Kui $\models A$, siis $\vdash A$. Veel enam, kui $\Gamma \models A$, siis $\Gamma \vdash A$.
  Sõnades: Loogilisest tõesusest järeldub tõestatavus, loogilisest järelduvusest järeldub 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:

$$\dfrac{\begin{array}{cc} \vdots & \\ B & \dfrac{}{B \supset (A \supset B)} \end{array}}{A \supset B}$$

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

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ C & C \supset B\end{array}}{B}$$

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:

$$\dfrac{\begin{array}{cc}\vdots & \dfrac{\begin{array}{cc}\vdots & \dfrac{}{(A \supset (C \supset B)) \supset (A \supset C) \supset (A \supset B))} \\ A \supset (C \supset B) & (A \supset C) \supset (A \supset B)\end{array}} \\ A \supset C & \end{array}}{A \supset B}$$

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