Logika és informatikai alkalmazásai

6. gyakorlat

Németh L. Zoltán

http://www.inf.u-szeged.hu/~zlnemeth

SZTE, Informatikai Tanszékcsoport

2009 tavasz

Irodalom

Szükséges elmélet a mai gyakorlathoz

Előadás fóliák: Hilbert típusú bizonyítások

Feladatsorok

FZ1 Fülöp Zoltán: Gyakorló feladatok a "Logika a számítástudományban" tárgyhoz I. "Ítéletkalkulus"
www.inf.u-szeged.hu/~fulop/logika/feladat1.ps

Hilbert féle bizonyítások

Axióma sémák:

1. $(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$
2. $F \rightarrow (G \rightarrow F)$
3. $((F \rightarrow \downarrow) \rightarrow \downarrow) \rightarrow F$

Ezek axióma sémák, azaz a fenti képletekben F G és H helyére tetszőleges formulákat helyettesíthetünk.

Következtetési szabály:
Modus Ponens (leválasztás szabálya, MP)

$$\frac{F, F \rightarrow G}{G}$$

Ezt szintén tetszőleges F és G formulákra szabad alkalmazni.

Hogyan lehet ezeket megtanulni?

AX1: $(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$,
ez az „implikáció öndisztributivitása”:
„$F \cdot (G + H) = F \cdot G + F \cdot H$”.
Miért tautológia ez? A láncolt implikáció viselkedése miatt
$F \rightarrow (G \rightarrow H) \equiv F \wedge G \rightarrow H$, és
$(F \wedge G \rightarrow H) \wedge (F \rightarrow G) \rightarrow (F \rightarrow H)$ ugye már látszik?
AX2: $F \rightarrow (G \rightarrow F)$
Ez arra jó, hogy F-ből, $G \rightarrow F$-et készíthessünk. Valóban:

1. F
2. $F \rightarrow (G \rightarrow F)$ AX2
3. $G \rightarrow F$ MP 1,2

Ez alapján, ha már levezettük F-et, levezethetjük $G \rightarrow F$-et bármely G formulára.
AX3: $((F \rightarrow \downarrow) \rightarrow \downarrow) \rightarrow F$
Ez a dupla tagadás törvénye, vagyis $\neg\neg F \rightarrow F$.

Bizonyításokat konstruálni nem könnyű ...

Némi segítség ez az applet:
`logik.phl.univie.ac.at/~chris/formular-uk-hilbert.html`
Csak ez egy kicsit más axiómákat használ az előadás axiómái
a setupban így etethetők meg vele:

(F -> (G -> H)) -> ((F -> G) -> (F -> H))
F -> (G -> F)
((F -> O) -> O) -> F

És utána „O"-t (vagyis nagy „ó”-t) az azonosan hamis ($\downarrow$) jelnek
kell tekinteni és nem szabad helyére semmit sem helyettesíteni.

$\vdash P \to P$ bizonyítása

1. $P \to ((P \to P) \to P)$
   AX2$[F/P, G/(P \to P)]$
2. $(P \to ((P \to P) \to P)) \to ((P \to (P \to P)) \to (P \to P))$
   AX1$[F/P, G/(P \to P), H/P]$
3. $(P \to (P \to P)) \to (P \to P)$
   MP 1,2
4. $P \to (P \to P)$
   AX2$[F/P, G/P]$
5. $P \to P$
   MP 3,4

Logikai következtetés bizonyítása

Jele: $\Sigma \vdash F$
Ekkor a F bizonyításához az axiómákon túl a Σ-beli formulák is felhasználhatók (azok persze helyettesítés nélkül!).
Például: $\Sigma = \{(P \to \downarrow) \to \downarrow, P \to Q\}$ esetén $\Sigma \vdash Q$-nak ez a levezetése (bizonyítása):

1.	$(P \to \downarrow) \to \downarrow$	$\in \Sigma$
2.	$((P \to \downarrow) \to \downarrow) \to P$	AX3[F/P]
3.	P	MP 1,2
4.	$P \to Q$	$\in \Sigma$
5.	Q	MP 3,4

Tétel. (A Hilbert kalkulus helyessége és teljessége) Bármely Σ és F zérusrendű formulahalmazra illetve formulára

$$\Sigma \vdash F \Leftrightarrow \Sigma \models F$$

Megjegyzés. Némileg bonyolultabb axiómákkal és szabályokkal ugyan de a tétel igaz elsőrendben is. Így a logikai következmény fogalma formalizálható.

$\vdash \downarrow \to P$ bizonyítása (azaz „hamisból minden következik")

1. $(\downarrow \to (((P \to \downarrow) \to \downarrow) \to P)) \to ((\downarrow \to ((P \to \downarrow) \to \downarrow)) \to (\downarrow \to P))$
   AX1[$F/\downarrow, G/(P \to \downarrow) \to \downarrow, H/P$]
2. $((P \to \downarrow) \to \downarrow) \to P$ AX3[F/P]
3. $(((P \to \downarrow) \to \downarrow) \to P) \to (\downarrow \to (((P \to \downarrow) \to \downarrow) \to P))$
   AX2[$F/((P \to \downarrow) \to \downarrow) \to P, G/\downarrow$]
4. $\downarrow \to (((P \to \downarrow) \to \downarrow) \to P)$ MP 2,3
5. $(\downarrow \to ((P \to \downarrow) \to \downarrow)) \to (\downarrow \to P)$ MP 1,4
6. $\downarrow \to ((P \to \downarrow) \to \downarrow)$ AX2[$F/\downarrow, G/P \to \downarrow$]
7. $\downarrow \to P$ MP 5,6

$\vdash ((P \rightarrow \downarrow) \rightarrow P) \rightarrow ((P \rightarrow \downarrow) \rightarrow \downarrow)$ bizonyítása

1. $((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)) \rightarrow (((P \rightarrow \downarrow) \rightarrow P) \rightarrow ((P \rightarrow \downarrow) \rightarrow \downarrow))$
   AX1$[F/(P \rightarrow \downarrow), G/P, H/\downarrow]$
2. $((P \rightarrow \downarrow) \rightarrow (((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)) \rightarrow (P \rightarrow \downarrow))) \rightarrow$
   $(((P \rightarrow \downarrow) \rightarrow ((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow))) \rightarrow ((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)))$
   AX1$[F/P \rightarrow \downarrow, G/((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)), H/(P \rightarrow \downarrow)]$
3. $(P \rightarrow \downarrow) \rightarrow (((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)) \rightarrow (P \rightarrow \downarrow))$
   AX2$[F/P \rightarrow \downarrow, G/(P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)]$
4. $((P \rightarrow \downarrow) \rightarrow ((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow))) \rightarrow ((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow))$
   MP 2,3
5. $(P \rightarrow \downarrow) \rightarrow ((P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow))$
   AX2$[F/P \rightarrow \downarrow, G/P \rightarrow \downarrow]$
6. $(P \rightarrow \downarrow) \rightarrow (P \rightarrow \downarrow)$ MP 4,5
7. $((P \rightarrow \downarrow) \rightarrow P) \rightarrow ((P \rightarrow \downarrow) \rightarrow \downarrow)$ MP 1,6

A dedukció tétel

Ez így roppant nehézkes és hosszadalmas, de segítségünkre siet a **dedukció tétel:**

$$\Sigma \vdash F \rightarrow G \Leftrightarrow \Sigma \cup \{F\} \vdash G$$

Az mindaddig, amíg implikációt, azaz $F \rightarrow G$ alakú formulát kell bebizonyítani, annak előtagja F felvehető a feltételek közé és elég csak G-t bizonyítani. **Például:**

$$\vdash F \rightarrow ((F \rightarrow \downarrow) \rightarrow \downarrow) \Leftrightarrow \{F\} \vdash (F \rightarrow \downarrow) \rightarrow \downarrow \Leftrightarrow \{F, F \rightarrow \downarrow\} \vdash \downarrow$$

Ez meg már könnyű:

1.	F	$\in \Sigma$
2.	$F \rightarrow \downarrow$	$\in \Sigma$
3.	$\downarrow$	MP 1,2

Feladatok

Mutassuk meg az alábbiakat, a dedukció tétel használható.

1. $\vdash F \to F$ (dedukcióval triviális)
2. $\vdash ((P \to\downarrow) \to P) \to ((P \to\downarrow) \to\downarrow)$
   (az előző példa, ugye, hogy könnyebb?)
3. $\vdash\downarrow\to P$
   (azért ez is könnyebb mint az előbb, bár nem triviális)
4. $\{P, P \to\downarrow\} \vdash Q$ (HF)
5. $\vdash (P \to\downarrow) \to (P \to Q)$ (HF)
6. $\{(P \to\downarrow) \to (Q \to\downarrow)\} \vdash Q \to P$ (táblán)
7. $\vdash ((F \to\downarrow) \to (G \to\downarrow)) \to (((F \to\downarrow) \to G) \to F)$
   (Ez a Fülöp Z. jegyzet 3. axiómája)
8. $\{(P \to\downarrow) \to P\} \vdash P$
   (ehhez felhasználjuk azt, hogy $F \to F$-et már le tudjuk vezetni (és esetleg az előző feladatot.))

További példák **FZ1 IV/5** (átírva az előadás jelölésére, azaz $\neg F \equiv F \to\downarrow$, vagy az előző példa 7. pontjának értelmében a feladatsor axiómáit is használhatjuk).

Követelmények a ZH-ra

1. Elsőrendű szintaxis: term, atomi formula, formula, részformulák, kvantorok hatásköre.
2. Struktúrák és modelljeik: egy struktúra egy formulának modellje-e, formulához adjon meg modelljét, nem modelljét, olyan formulák felírása, melyek minden modellje bizonyos tulajdonságú, formalizálás
3. A szemantika további alapfogalmai: kielégíthetőség, tautológia, ekvivalencia , logikai következmény, és ezek egyszerű összefüggései.

Követelmények a ZH-ra II

4. Az ítéletkalkulus alapvető algoritmikus kérdéseinek:
   - Egy F formula, vagy véges Σ formulahalmaz **kielégíthető-e**;
   - Egy F formula **tautológia-e** ($\models F$);
   - Formulák egy véges Σ halmazának egy F formula **logikai következménye-e** ($\Sigma \models F$);
   - Egy F és egy G formula **ekvivalens-e** ($F \equiv G$);

   eldöntése az alábbi módszerekkel
   - igazságtáblázattal;
   - indirekt igazságtáblázat módszerrel;
   - Horn-formulák algoritmusával (persze ez csak akkor alkalmazható, ha csak Horn-klózok kielégíthetőségét kell eldönteni);
   - rezolúcióval.
5. Boole-műveletek egymással való kifejezhetősége, rendszerek teljessége és nem teljessége.
6. Hilbert típusú bizonyítások dedukcióval és anélkül.

A Zh-ban lehet feladat a kiadott házifeladatok közül.