Logika és informatikai alkalmazásai

3. gyakorlat

Németh L. Zoltán

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

SZTE, Informatikai Tanszékcsoport

2009 tavasz

Irodalom

Szükséges elmélet a mai gyakorlathoz

Előadás fóliák: #31-#41, #52-#58

Feladatsorok

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

- **Critical Thinking Webpage:** philosophy.hku.hk/think

A szemantika alapfogalmai I.

Egy F elsőrendű formula

- **tautológia** (azonosan igaz), ha **bármely modellben igaz**, azaz $\forall \mathcal{A}$ struktúrára $\mathcal{A} \models F$;
- **kielégíthető**, ha **létezik modellje**, azaz $\exists \mathcal{A}$ struktúra, melyre $\mathcal{A} \models F$;
- **kielégíthetetlen** (azonosan hamis), ha **nem létezik modellje**, azaz $\forall \mathcal{A}$ struktúrára $\mathcal{A} \not\models F$.

Állítás

1. F kielégíthető $\Leftrightarrow \neg F$ nem tautológia;
2. F tautológia $\Leftrightarrow \neg F$ kielégíthetetlen.

Összefoglaló ábra és példák a táblán.

Az itéletkalkulus a predikátumkalkulus speciális esete

Az *ítéletkalkulus* vagy *zérusrendű logika*, az elsőrendű logikának (a predikátum kalkulusnak) azzal a speciális esetével (is) azonosítható, amelyben nincsenek függvényszimbólumok és a predikátum szimbólumok is mind 0 változósak, azaz logikai konstansok.
Ekkor nincs szükségünk változókra és kvantorokra, a modell fogalma, pedig a konstans predikátumszimbólumokhoz rendelt 0 vagy 1 logikai érték megadására egyszerűsödik:

$$\mathcal{A} : \mathcal{P}red \to \{0, 1\}.$$

Ezért zérusrendű logikában a konstans pedikátumszimbólumokat ítéletváltozóknak a modellt pedig az itéletváltozók kiértékelésének, vagy változóhozzárendelésnek is hívjuk. Jelölése: $\mathcal{A}(p)$, a p ítéletváltozó értéke az $\mathcal{A}$ modellben.

FZ1 I/3.

Mutassuk meg, hogy az alábbi formulák tautológiák, bármely F és G formulák esetén!

a) $(F \to G) \leftrightarrow (\neg F \vee G)$;
b) $(F \to G) \leftrightarrow \neg(F \wedge \neg G)$;
c) $(F \to G) \leftrightarrow (\neg F \vee (F \wedge G))$;
d) $(F \to G) \leftrightarrow ((\neg G) \to (\neg F))$.

c) megoldása. Igazságtábla módszerrel:
A sorokban F-nek és G-nek minden lehetséges igazságértéke fel van sorolva.

$(F$	$\to$	$G)$	$\boxed{\leftrightarrow}$	$(\neg$	F	$\vee$	$(F$	$\wedge$	$G))$
0	1	0	1	1	0	1	0	0	0
0	1	1	1	1	0	1	0	0	1
1	0	0	1	0	1	0	1	0	0
1	1	1	1	0	1	1	1	1	1

Ha a kimenetben (amit a legkülső műveleti jel alatt van)

- mindig 1 szerepel $\Leftrightarrow$ a formula tautológia;
- van 1-es $\Leftrightarrow$ kielégíthető;
- mindig 0 szerepel $\Leftrightarrow$ kielégíthetetlen;

Az indirekt igazságtábla módszerrel:

Ez a módszer azt jelenti, hogy csak azt a sort (sorokat) írom le az igazságtáblából, melyek végeredménye **nem felelnek meg** a bizonyítandó állításnak, majd a részeredményekre visszafele következtetve ellentmondásra jutunk.
A következtetésekhez többek között az alábbiakat lehet használni:

(	A	$\wedge$	B	)	$\Leftrightarrow$	(	A	$\wedge$	B	)		
		1					1		1			
(	A	$\vee$	B	)	$\Leftrightarrow$	(	A	$\vee$	B	)		
		0					0		0			
(	A	$\to$	B	)	$\Leftrightarrow$	(	A	$\to$	B	)		
		0					1		0			
(	A	$\leftrightarrow$	B	)	$\Leftrightarrow$	(	A	$\leftrightarrow$	B	)		
		1					0		0		vagy	Azaz, utolsó
		1					1		1			

esetben a balról jobbra következtetés nem egyértelmű, ezért mindkét esetben (azaz sorban) ellentmondásra kell jutnunk!

d) megoldása

	1	2	3		4			5	6		7		8	9		
(	F	$\rightarrow$	G	)	$\leftrightarrow$	(	(	$\neg$	G	)	$\rightarrow$	(	$\neg$	F	)	)
	1	0	0		0			1	0		1		0	1		
	1	1	0		0			1	0		0		0	1		

- #4=0 indirekt feltevés alapján;
- #2 és #7 rendre 0, 1 **vagy** 1, 0 két sorba szétválasztva;
- 1. sor: #1 = 1 és #3= 0 $\rightarrow$ def. alapján;
- 1. sor: #6 = 0 és #9= 1 változó értékének másolása;
- 1. sor: #5 = 1 és #8= 0 $\neg$ def. alapján;
- 1. sor: **ellentmondás:** #7=0 következne, de ott már #7=1 szerepel.
- A 2. sor kitöltése és az ellentmondás pl. #2 értékén hasonló.

Példák elsőrendű logikában

Döntsük el, hogy az alábbi formulák melyik kategóriába esnek:
A) tautológiák, B) nem taut., de kielégíthetők, C) kielégíthetetlenek.

1. $\exists x p(x) \vee \neg \exists x p(x)$ A
2. $p(x) \wedge \neg p(y)$ B
3. $\forall x p(x) \rightarrow \neg \exists x p(x)$ B
4. $\forall x p(x) \rightarrow \neg \exists x \neg p(x)$ A
5. $\forall x \exists y r(x, y) \rightarrow \exists x \forall y r(x, y)$ B!
6. $\exists x(p(x) \vee q(x)) \rightarrow \exists x p(x) \vee \exists x q(x)$ A
7. $\forall x(p(x) \vee q(x)) \rightarrow \forall y p(y) \vee \forall z q(z)$ B
8. $\neg[\forall x(p(x) \wedge q(x)) \rightarrow (\forall x p(x) \wedge \forall x q(x))]$ C
9. $\forall x p(x) \rightarrow q(y) \leftrightarrow \forall x[p(x) \rightarrow q(y)]$ B
10. $\exists x \forall y[r(x, y) \leftrightarrow \neg r(y, y)]$ C
11. $\forall x \exists y[r(x, y) \leftrightarrow \neg r(y, y)]$ B
12. $\forall x p(x) \wedge \forall y(p(f(y)) \rightarrow q(y)) \wedge \exists z \neg q(z)$ C

FZ1 I/10. Bizonyítsuk be, vagy adjunk ellenpéldát!

a) Ha $\models (F \rightarrow G)$ és $\models F$, akkor $\models G$;

b) Ha $F \rightarrow G$ kielégíthető és F kielégíthető, akkor G is kielégíthető.

Megoldások:

a) **IGAZ.** <ID>(ID=indirekt)
Ha G nem tautológia $\Rightarrow \exists \mathcal{A}$ modell: $\mathcal{A}(G) = 0$
$\Rightarrow \mathcal{A}(F \rightarrow G) = 0$, mert $\mathcal{A}(F) = 1$, $\mathcal{A}(G) = 0$
$\Rightarrow$ de ez ellentmond annak, hogy $\models F \rightarrow G$.

b) **NEM IGAZ.**
Pl: $F = p$, $G = \downarrow$ esetén.

Egy kicsit komolyabb feladat (HF)

FZ1 I/6. Legyenek F és G az **ítéletkalkulus** formulái. Tegyük fel, hogy $\models (F \rightarrow G)$, továbbá, hogy F-nek és G-nek **nincs közös ítéletváltozója**. Mutassuk, meg, hogy ekkor F kielégíthetetlen vagy G tautológia. Mutassuk meg, hogy a bizonyításhoz szükséges feltenni, hogy ne legyen F-nek és G-nek közös ítéletváltozója.

Bizonyítás. Tegyük fel, hogy

$\models F \rightarrow G \overset{\text{def.}}{\Longleftrightarrow} \forall \mathcal{A} : Var \rightarrow \{0, 1\}$ kiértékelésre $\mathcal{A}(F \rightarrow G) = 1$
$\Leftrightarrow \forall \mathcal{A}$ kiértékelésre ($\mathcal{A}(F) = 0$ vagy $\mathcal{A}(G) = 1$)

I. Ha most $\forall \mathcal{A}$ kiértékelésre $\mathcal{A}(F) = 0$ akkor F kielégíthetetlen.

II. Ha van olyan $\mathcal{A}'$ kiértékelés, hogy $\mathcal{A}'(F) \neq 0$ akkor meg kell mutatnunk, hogy G tautológia.

A bizonyítás folytatása

II. igazolásához, vegyünk egy tetszőleges $\tilde{\mathcal{A}}$ kiértékelést. Mivel F-nek és G-nek nincs közös ítéletváltozója, készíthetünk egy olyan $\mathcal{B}$ kiértékelés melyre

$$\mathcal{B}(p_i) = \begin{cases} \mathcal{A}'(p_i) & \text{ha } p_i \in \mathrm{Var}(F) \\ \tilde{\mathcal{A}}(p_i) & \text{ha } p_i \in \mathrm{Var}(G) \end{cases}$$

Ekkor $\mathcal{B}(F \to G) = 1$ mert $F \to G$ tautológia, de $\mathcal{B}(F) = \mathcal{A}'(F) = 1$ ezért $\mathcal{B}(G) = 1$. Mivel $\tilde{\mathcal{A}}(G) = \mathcal{B}(G) = 1$ teljesül tetszőleges $\tilde{\mathcal{A}}$ kiértékelésre, ezért $\models G$.

A nincs közös ítéletváltozójuk feltétel valóban szükséges. Pl. $F = p \wedge q, G = p$ esetén $\models F \to G$ teljesül de F kielégíthető és G nem tautológia.

Formulahalmazok kielégíthetősége

Formulák egy Σ halmaza kiekielégíthető ha létezik olyan modell, mely egyszerre minden elemét igazzá teszi, azaz $\exists \mathcal{A}$ modell, hogy minden $F \in \Sigma$-ra $\mathcal{A} \models F$.

FZ1 I/8. Kielégíthetők-e a következő formulahalmazok?

a) $\{p, q, p \to r, \neg r\}$

b) $\{p_1 \vee p_2, \neg p_2 \vee \neg p_3, p_3 \vee p_4, \neg p_4 \vee \neg p_5, \ldots\}$

a) NEM. Ha az első kettő és az utolsó formula igaz egy $\mathcal{A}$ modellben, akkor szükségképpen $\mathcal{A}(p) = \mathcal{A}(q) = 1$ és $A(r) = 0$, de ekkor az implikáció definíciója miatt $\mathcal{A} \not\models p \to r$.

b) IGEN.

Legyen például $\mathcal{A}(p_i) = \begin{cases} 1 & \text{ha i páratlan} \\ 0 & \text{ha i páros} \end{cases}$ (vagy fordítva)

FZ1 I/9. Adjunk példát olyan három elemű Γ formulahalmazra amely kielégíthetetlen, de minden két elemű részhalmaza kielégíthető. Általánosítsuk a példát n elemű halmazra is.

Megoldás:

$$\{p_1 \leftrightarrow p_2, p_2 \leftrightarrow p_3, p_3 \leftrightarrow \neg p_1\}$$

Általánosítása:

$$\{p_1 \leftrightarrow p_2, p_2 \leftrightarrow p_3, \ldots, p_{n-1} \leftrightarrow p_n, p_n \leftrightarrow \neg p_1\}$$

Logikai következmény és ekvivalencia

Legyen Σ egy formulahalmaz, ekkor Σ modelljeinek a halmaza legyen

$$\mathrm{Mod}(\Sigma) := \{\mathcal{A} \mid \mathcal{A} \models \Sigma\}.$$

Egy Σ formulahalmaznak logikai következménye egy F formula, ha Σ minden modellje modellje F-nek is. Jelölése: $\Sigma \models F$.

Röviden: $\Sigma \models F \;\Leftrightarrow\; \mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(F)$.

Azt mondjuk, hogy az F és G formula ekvivalens, ha F pontosan ugyanazokban a modellekben igaz, mint G. Jele: $F \equiv G$.

Röviden: $F \equiv G \;\Leftrightarrow\; \mathrm{Mod}(F) = \mathrm{Mod}(G)$.

Alapvető összefüggések

Az ítéletkalkulusban

- két formula ekvivalens $\Leftrightarrow$ igazságtáblázatuk eredmény oszlopa megegyezik;
- $\Sigma \models F \Leftrightarrow$ ha az igazságtáblázatokban ha Σ minden formulájának eredmény oszlopa 1, akkor ott F eredméynoszlopában is 1 van.

Állítás.

- $F \equiv G \Leftrightarrow \models F \leftrightarrow G \Leftrightarrow \neg(F \leftrightarrow G)$ kielégíthetetlen.;
- $\Sigma \models F \Leftrightarrow \Sigma \cup \{\neg F\}$ kielégíthetetlen.

FZ1 I/11. első rész

FZ1 I/11. Legyen Γ és Δ két formulahalmaz, és F és G legyenek formulák. Bizonyítsuk be a következőket!

a) Ha $\Gamma \models F$ és $\Gamma \subseteq \Delta$, akkor $\Delta \models F$;

b) $\Gamma \cup \{F\} \models G$ akkor és csak akkor, ha $\Gamma \models F \to G$.

c) Ha $\Gamma \cup \{\neg F\} \models G$ és $\Gamma \cup \{\neg F\} \models \neg G$, akkor $\Gamma \models F$;

Megoldások:

a) triviális, ha $\triangle$ minden formulája igaz, akkor Γ-é is.

b) $\forall \mathcal{A}$ modellre, ha $\mathcal{A} \models \Gamma$ akkor

I.eset Ha $\mathcal{A}(F) = 0 \quad \Rightarrow \quad \mathcal{A}(F \to G) = 1$

II.eset Ha $\mathcal{A}(F) = 1 \quad \Rightarrow \quad \mathcal{A} \models \Gamma \cup \{F\}$, így $\Gamma \cup \{F\} \models G$ miatt $\mathcal{A}(G) = 1$. Ezért $\mathcal{A}(F \to G) = 1$

c) $\Gamma \models F \Leftrightarrow \Gamma \cup \{\neg F\}$ kielégíthetetlen. Ez indirekt bizható:
Tfh. $\Gamma \cup \{\neg F\}$ kielégíthető $\Leftrightarrow \exists \mathcal{A}$ modell, melyre $\mathcal{A} \models \Gamma \cup \{\neg F\}$.
Ha most $\mathcal{A}(G) = 0$, akkor $\Gamma \cup \{\neg F\} \models G$ nem teljesül.
Ha viszont $\mathcal{A}(G) = 1$, akkor $\Gamma \cup \{\neg F\} \models \neg G$ nem teljesül.
ELLENTMONDÁS!

FZ1 I/11. második rész

FZ1 I/11. Legyen Γ és Δ két formulahalmaz, és F és G legyenek formulák. Bizonyítsuk be a következőket!

d) Ha $\Gamma \cup \{F\} \models H$ és $\Gamma \cup \{G\} \models H$, akkor $\Gamma \cup \{F \vee G\} \models H$;

e) Ha $\Gamma \models F$ és $\Delta \models \neg F$, akkor $\Gamma \cup \Delta$ kielégíthetetlen.

Megoldások:

d) $\forall \mathcal{A}$ modellre $\mathcal{A} \models \Gamma \cup \{F \vee G\}$
$\Rightarrow \mathcal{A} \models \Gamma$ és $\mathcal{A}(F \vee G) = 1$
$\Rightarrow \mathcal{A} \models \Gamma$ és $(\mathcal{A}(F) = 1$ vagy $\mathcal{A}(G) = 1)$
$\Rightarrow (\mathcal{A} \models \Gamma$ és $\mathcal{A}(F) = 1)$ vagy $(\mathcal{A} \models \Gamma$ és $\mathcal{A}(G) = 1)$.
Mindkét esetben a feltételek miatt $\mathcal{A}(H) = 1$.

e) ID Tfh. $\Gamma \cup \Delta$ kielégíthető $\Leftrightarrow \exists \mathcal{A} : \mathcal{A} \models \Gamma$ és $\mathcal{A} \models \Delta$.
I.eset Ha $\mathcal{A}(F) = 0$, akkor $\Gamma \models F$ nem teljesül.
II.eset Ha $\mathcal{A}(F) = 1$, akkor $\Delta \models \neg F$ nem teljesül.
ELLENTMONDÁS!!!

Log. következmények az ítéletkalkulusban.

Vizsgáljuk meg indirekt igazságtábla módszerrel az alábbi logikai következtetések helyességét, amennyiben a következtetés nem áll fenn adjunk is meg egy olyan ítéletváltozó kiértékelést, mely a feltételeket kielégíti a következményt azonban nem.

a) $(P \to (Q \wedge (R \to S))), P, \neg S \models \neg(Q \wedge R)$
b) $(P \leftrightarrow (R \to (P \vee \neg Q))), \neg(R \to (P \vee Q)) \models Q$
c) $(\neg(P \wedge Q) \wedge \neg(\neg P \vee \neg Q)) \models \neg(\neg(P \vee Q) \leftrightarrow (\neg P \wedge \neg Q))$
d) $\neg((\neg P \wedge Q) \vee (R \to S)), (\neg(\neg P \vee \neg Q) \wedge \neg(R \to S)) \models$
$(\neg((R \to S) \wedge \neg P) \leftrightarrow (P \vee (R \leftrightarrow S)))$
e) $(((P \vee Q) \to R) \leftrightarrow ((\neg P \wedge \neg Q) \leftrightarrow R)) \models (P \vee Q)$
f) $(P \to (Q \wedge \neg R)), (\neg P \vee \neg(\neg Q \vee \neg S)) \models (S \to (\neg P \vee T))$
g) $(\neg R \to \neg Q), ((\neg P \wedge R) \wedge \neg Q) \models \neg(P \leftrightarrow (\neg R \vee Q))$

Ez a feladat innen származik és ott meg is oldható interaktív módon: Critical Thinking Webpage:
`philosophy.hku.hk/think/sl/indirect-ex.php`
Az oldalon $\& = \wedge$ (és), $\sim = \neg$ (tagadás), $T = 1$ (true, igaz), $F = 0$ (false, hamis)

Konjunktív és diszjunktív normálformára hozás

FZ1 II/3. c Hozzuk DNF-ra és KNF-re következő formulát:

$$(p \leftrightarrow q) \rightarrow (r \vee s)$$

1.lépés: $F \rightarrow G$ helyett $\neg F \vee G$

$F \leftrightarrow G$ helyett $(F \rightarrow G) \wedge (G \rightarrow F) \equiv (\neg F \vee G) \wedge (\neg G \vee F)$

$(p \leftrightarrow q) \rightarrow (r \vee s) \equiv \neg(p \leftrightarrow q) \vee (r \vee s) \equiv$

$\neg \Big((\neg p \vee q) \wedge (\neg q \vee p) \Big) \vee (r \vee s) \equiv$

2.lépés: $\neg$ bevitele

$\neg(F \vee G) \equiv \neg F \wedge \neg G$, $\neg(F \wedge G) \equiv \neg F \vee \neg G$, és $\neg\neg F \equiv F$ alapján.

$\equiv \Big(\neg(\neg p \vee q) \vee \neg(\neg q \vee p) \Big) \vee (r \vee s) \equiv \Big((\neg\neg p \wedge \neg q) \vee$ $(\neg\neg q \wedge \neg p) \Big) \vee r \vee s \equiv (p \wedge \neg q) \vee (q \wedge \neg p) \vee r \vee s.$

Ez már DNF, a harmadik lépésre most nincs szükség.

Folytatás

A KNF-hez szükséges még a

3. lépés: a disztributivitás használata

KNF-nál a $\wedge$ kivitele: $(F \wedge G) \vee H \equiv (F \vee H) \wedge (G \vee H)$ alapján.

DNF-nál a $\vee$ kivitele: $(F \vee G) \wedge H \equiv (F \wedge H) \vee (G \wedge H)$ alapján.

$\Big((p \wedge \neg q) \vee (q \wedge \neg p) \Big) \vee r \vee s \equiv$

$\Big((p \vee q) \wedge (p \vee \neg p) \wedge (\neg q \vee q) \wedge (\neg q \vee \neg p) \Big) \vee r \vee s \equiv$

$\equiv \Big((p \vee q) \wedge (\neg q \vee \neg p) \Big) \vee r \vee s \equiv$

$(p \vee q \vee r \vee s) \wedge (\neg p \vee \neg q \vee r \vee s)$ Ez már KNF!

Gyakorláshoz

A **FZ1 II/3.** feladat megoldásai:

a) $(\neg p \vee q \vee r) \wedge (\neg r \vee p) \wedge (\neg r \vee \neg q)$
$(\neg r \wedge \neg p) \vee (\neg r \wedge q) \vee (p \wedge \neg q \wedge r)$

b) $(\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$
$\neg p \vee (q \wedge \neg p) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \equiv \neg p \vee (r \wedge q) \vee (\neg q \vee \neg r)$

c) $(\neg p \vee \neg q \vee r \vee s) \wedge (p \vee q \vee r \vee s)$
$(\neg p \wedge q) \vee (\neg q \wedge p) \vee r \vee s$

d) $\uparrow$ (tautológia) (üres KNF)
pl: $p \vee \neg p$ VIGYÁZAT az üres DNF azonosan HAMIS!

e) $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee r)$
$(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$

Konjunktív és diszjunktív normálformák ellenőrzéséhez (és még sok minden máshoz) ajánlom még a következő linket:
`logik.phl.univie.ac.at/~chris/formular-uk.html`

Jövő hétre

- HF, a kimaradt példák és még **FZ1 I/1, 2, 4, 5, 12**.
- **FZ2 I/4**.
- HF* (nehezebb példa): **FZ1 I/7**.
- Szükséges az előadás további részének ismerete, különösen a Boole függvények és formulák kapcsolata és az adekvát (teljes) rendszer fogalma.