

Matematikai logika

2010/2011 őszi

1. előadás

- 1., Ha pő és mindegy, akkor vildagur.
 - 2., A bégahur pő és mindegy.
 - 3., Tehát a bégahur vildagur.
- / Karinthy után szabadon/

Ez a következtetés helyes, noha nem tudjuk, mit jelentenek a fenti állítások.

Mi számít állításnak?

- 0. rendű nyelvek (ítéletkalkulus)
- 1. rendű nyelvek

0. rendű nyelvek

- ítéletváltozók: $X_0, X_1, X_2, \dots$
- logikai összekötő jelek: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- tagoló jelek: $(,)$ (a zárójelek)

Definíció: 0-rendű formula (~formalizált állítás)

- (1) ha ϕ ítéletváltozó, akkor ϕ formula,
- (2) ha ϕ, ψ formulák, akkor $\neg\phi, \phi \wedge \psi, \phi \vee \psi, \phi \Rightarrow \psi, \phi \Leftrightarrow \psi$ is formula (sőt, (ϕ) is formula),
- (3) Minden formula az előző két szabály véges sok alkalmazásával áll elő.

Példák: formula-e?

- | | |
|---|-------------|
| 1. X | <i>igen</i> |
| 2. $X \neg \Rightarrow Y$ | <i>nem</i> |
| 3. $\neg(X \Rightarrow Y)$ | <i>igen</i> |
| 4. $\neg \neg \neg X$ | <i>igen</i> |
| 5. $\wedge XY \Rightarrow \vee \vee \neg$ | <i>nem</i> |

Példák formalizálásra

Amelyik állat csíkos (C), az nem pettyes (P).

$(C \Rightarrow \neg P)$

Ha Zita nem puskázik (P), akkor megbukik (M).

$(\neg P \Rightarrow M)$

1. Rendű nyelvek

- (1) nem változtatható komponensek:
 - individum változók: $X_0, X_1, X_2, \dots$
 - logikai összekötő jelek: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists, =$
 - tagoló jelek: $(,), ,$ (zárójelek és vessző)
- (2) változtatható komponensek:
 - függvényszimbólumok,
 - konstansszimbólumok (= 0-változós függvényszimbólumok),

- relációszimbólumok.

Definíció: *TERM (elem különírás)*

- (1) ha t változó, vagy konstansszimbólum, akkor term;
- (2) ha f n -változós függvényszimbólum, $t_1, \dots, t_n$ term, akkor $f(t_1, \dots, t_n)$ is term;
- (3) Minden term az előző két szabály véges sok alkalmazásával áll elő.

Definíció. *Elsőrendű formula:*

- (1) ha $t_1, \dots, t_n$ term, R n változós reláció szimbólum, akkor $R(t_1, \dots, t_n)$ és $t_1=t_2$ is formulák (atomi formulák);
- (2) ha ϕ, ψ formula, x változó, akkor $\neg\phi$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \implies \psi$, $\phi \iff \psi$, $\exists x\phi$, $\forall x\phi$, $[(\phi)]$ is formulák ;
- (3) Minden formula az előző két szabály véges sok alkalmazásával áll elő.

Példák:

- 1) Legyen
 f egyváltozós függvény szimbólum,
 g kétváltozós függvény szimbólum,
 Q egyváltozós relációsimbólum.

Term-e?

- | | | |
|----|----------------|-------------|
| 1. | Q | <i>nem</i> |
| 2. | $f(g(X,Y))$ | <i>igen</i> |
| 3. | $g(f(X,Y))$ | <i>nem</i> |
| 4. | $X \implies Y$ | <i>nem</i> |

Formula-e?

- | | | |
|----|---|-----------------------|
| 1. | X | <i>nem</i> |
| 2. | $X \implies Y$ | <i>nem</i> |
| 3. | $\forall X \exists Y (Q(f(X)) \implies Q(Y))$ | <i>igen</i> |
| 4. | $\forall X \exists X Q(X)$ | <i>igen</i> |
| 5. | $\forall XY (X=Y)$ | <i>nem</i> |
| 6. | $Q(f(X))$ | <i>igen</i> |
| 7. | $f(Q(X))$ | <i>nem</i> |
| 8. | $\exists X (X=f(X))$ | <i>igen</i> |
| 9. | $\exists f(X=f(X))$ | <i>nem (2. rendű)</i> |

Formalizáljuk:

Röplabda:

- $J(X)$: X játékos,
 $C(X)$: X csapat,
 $T(X,Y)$: X játékos tagja az Y csapatnak,
 $E(X,Y)$: X erősebb, mint Y ,
 Fradi: konstans szimbólum.

1. Van olyan játékos, aki nem a Fradiban játszik:
 $\exists X (J(X) \wedge \neg T(X, \text{Fradi}))$.
2. Minden játékos tagja valamelyik csapatnak:
 $\forall X \exists Y (J(X) \implies C(Y) \wedge T(X, Y))$.

3. Mit jelent: $\exists X \forall Y (J(X) \implies (C(Y) \wedge T(X, Y)))$

Van olyan X objektum, hogy ha ez az objektum játékos, akkor az összes objektum csapat és X mindnek tagja.

4. Pontosan 1 csapat erősebb, mint a Fradi:

$$\exists X (C(X) \wedge E(X, \text{Fradi})) \wedge$$

$$\neg (\exists X_1 \exists X_2 (\neg (X_1 = X_2) \wedge C(X_1) \wedge C(X_2) \wedge E(X_1, \text{Fradi}) \wedge E(X_2, \text{Fradi}))).$$

5. Minden csapatnál van erősebb:

$$\forall X (C(X) \implies \exists Y (C(Y) \wedge E(Y, X))).$$

Matematikai logika – 2. előadás

Begépelte: Csikós Donát

2010. november 11.

1. Szemantika

1.1. Szemantika az ítéletkalkulusban

Definíció A $k : \{\text{változók}\} \rightarrow \{i, h\}$ függvényeket *kiértékeléseknek* nevezzük. A kiértékelés tehát minden egyes változóhoz igazságértéket rendel.

Logikai műveletek jelentése. Az egyes logikai műveletek jelentését az alábbi táblázat foglalja össze.

x	y	$\neg x$	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \Leftrightarrow y$
i	i	h	i	i	i	i
i	h	h	h	i	h	h
h	i	i	h	i	i	h
h	h	h	h	h	i	i

$A \Rightarrow$ csak úgy lehet hamis, ha előtagja igaz és utótagja hamis. Ebből adódik, hogy hamis előtagból bármi következik.

Definíció Legyen k kiértékelés, φ, ψ, θ formula. $k \models \varphi$, azaz k -ban φ igaz, ha:

1. $k(\varphi) = i$, és φ ítéletváltozó.
2. $k \models \psi$ és $k \models \theta$ és $\varphi = \psi \wedge \theta$.
3. $k \models \psi$ vagy $k \models \theta$ és $\varphi = \psi \vee \theta$.
4. $k \not\models \psi$ vagy $k \models \theta$ és $\varphi = \psi \Rightarrow \theta$.
5. $k \models \psi$ és $k \models \theta$ egyszerre teljesül, és $\varphi = \psi \Leftrightarrow \theta$.
6. $k \not\models \psi$ esetén: $\varphi = \neg \psi$.

A definíció szerint tehát egy összetett formula jelentése a részformulái jelentése és a fenti táblázat alapján számítható ki.

Megjegyzés A formulák igazságértéke csak a bennük szereplő változók igazságától függ.

Definíció Legyen φ, ψ formula. $\varphi \equiv \psi$, azaz φ és ψ *ekvivalensek*, ha ha minden k kiértékelésre $k \models \varphi$ és $k \models \psi$ egyszerre áll fenn.

Példa

A	B	C	$A \Rightarrow (B \Rightarrow C)$	$(A \Rightarrow B) \Rightarrow C$
i	i	i	i	i
i	i	h	h	h
i	h	i	i	i
i	h	h	i	i
h	i	i	i	i
h	i	h	i	h
h	h	i	i	i
h	h	h	i	h

A 6. és a 8. sor közti eltérés mutatja, hogy a két kifejezés nem ekvivalens egymással:
 $A \Rightarrow (B \Rightarrow C) \not\equiv (A \Rightarrow B) \Rightarrow C$.

Konvenció

- (1) $A \Rightarrow B \Rightarrow C$ konvenció szerint $A \Rightarrow (B \Rightarrow C)$ -t jelent.
- (2) A műveletek szokásos sorrendje csökkenő precedencia szerint: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$.

1.2. Szemantika elsőrendű logikában

Definíció t egy típus, ha $t = (I, J, K, \rho, \delta)$, ahol I, J, K páronként diszjunkt halmaz, $\rho : I \rightarrow N, \delta : J \rightarrow N$ függvény.

Legyen L egy elsőrendű nyelv. Ennek $t = (I, J, K, \rho, \delta)$ a típusa, ha L -ben:

I : a relációszimbólumok halmaza, és ha $R \in I$, akkor R $\rho(R)$ változós,

J : a függényszimbólumok halmaza, és ha $f \in J$, akkor f $\delta(f)$ változós,

K : a konstansszimbólumok halmaza.

A típus tehát az elsőrendű nyelv változtatható részét adja meg.

Definíció Legyen $t = (I, J, K, \rho, \delta)$ típus. $\mathcal{A} = \langle A, R_i, f_j, C_k \rangle_{i \in I, j \in J, k \in K}$ egy t típusú *struktúra*, ha A egy nemüres (alap)halmaz, és minden $i \in I, j \in J, k \in K$ -ra $R_i \subseteq A^{\rho(i)}$ egy $\rho(i)$ változós reláció, $f_j : A^{\delta(j)} \rightarrow A$ egy $\delta(j)$ változós függvény, $C_k \in A$ konstans.

Példa

- (1) Minden gráf egy struktúra. $G = \langle V, E, = \rangle$, a V csúcshalmaz az alaphalmaz, az E élhalmaz egy kétváltozós reláció. I egyelemű, J, K üresek.
- (2) Minden csoport egyben egy struktúra is.
- (3) $A = \{\text{csapatok, játékosok}\}$. $R(x, y)$: x erősebb, mint y . Fradi: konstans. $J(x)$: játékos. $C(x)$: csapat. Ekkor $\mathcal{A} = \langle A, J, C, R, =, \text{Fradi} \rangle$. J üres.

Definíció Az $\mathcal{A}$ struktúra *modellje* a nyelvnek, ha $\mathcal{A}$ és L típusa azonos (L formuláit mindig L típusú struktúrákban nézzük).

Definíció k elsőrendű $\mathcal{A}$ feletti kiértékelés, ha $k : \{\text{változók}\} \rightarrow A$.

Definíció Legyen $\mathcal{A}$ struktúra, t term, k egy $\mathcal{A}$ feletti kiértékelés. Ekkor t értéke $\mathcal{A}$ -ban k mellett:

$$t^{\mathcal{A}}[k] = \begin{cases} c & , \text{ ha } t = c \text{ konstans szimbólum,} \\ k(x) & , \text{ ha } t = x \text{ változó,} \\ f(t_1^{\mathcal{A}}[k], t_2^{\mathcal{A}}[k], \dots, t_n^{\mathcal{A}}[k]) & , \text{ ha } t = f(t_1, t_2, \dots, t_n). \end{cases}$$

Definíció Legyen k, k' kiértékelés, x változó. $k \stackrel{x}{\equiv} k'$, azaz k közel van k' -höz, ha $x \neq y \Rightarrow k(y) = k'(y)$ (azaz x -től eltérő változóknak ugyanaz a képe).

Definíció Legyen φ formula, $\mathcal{A}$ struktúra, k kiértékelés. $\mathcal{A} \models \varphi[k]$ (azaz $\mathcal{A}$ -ban igaz φ a k mellett), ha

- (1) $(t_1^{\mathcal{A}}[k], t_2^{\mathcal{A}}[k], \dots, t_n^{\mathcal{A}}[k]) \in R^{\mathcal{A}}$, ha $\varphi = R(t_1, t_2, \dots, t_n)$ atomi formula,
- (2) $t_1^{\mathcal{A}}[k] = t_2^{\mathcal{A}}[k]$, ha $\varphi = t_1^n = t_2^n$,
- (3) $\mathcal{A} \not\models \psi[k]$, ha $\varphi = \neg\psi$,
- (4) $\mathcal{A} \models \psi[k]$ és $\mathcal{A} \models \delta[k]$, ha $\varphi = \psi \wedge \delta$ (ez ugyanúgy az ítéletkalkulus többi $\vee, \Rightarrow, \Leftrightarrow$ műveletére is kell),
- (5) létezik olyan $k' \stackrel{x}{\equiv} k$, hogy ha $\varphi = \exists x\psi$, akkor $\mathcal{A} \models \psi[k']$,
- (6) minden $k' \stackrel{x}{\equiv} k$, teljesül hogy ha $\varphi = \forall x\psi$, akkor $\mathcal{A} \models \psi[k']$.

Definíció $\mathcal{A} \models \varphi$ (azaz φ kiértékelés nélkül igaz $\mathcal{A}$ -ban), ha minden k -ra $\mathcal{A} \models \varphi[k]$.

Példa $G = \langle V, E \rangle$, $V = \{1, 2, 3\}$, $E = \{(1, 2)\}$. Legyen $\varphi = \exists y E(x, y)$. $k = \left| \frac{x}{1} \right|$,
 $l = \left| \frac{x}{2} \right|$ Kérdés: $G \stackrel{?}{\models} \varphi$. Ez nem igaz, mivel $G \not\models \varphi[k]$, de $G \models \varphi[l]$.

Példa A gyűrűk esetén: $\exists x(x^2 = -1)$? Ez a valós számok körében $\langle \mathbb{R}, +, \cdot, = \rangle \not\models \varphi$, de komplex számok esetén $\langle \mathbb{C}, +, \cdot, = \rangle \models \varphi$.

Ebből is látszik, hogy egy formula más-más struktúrában lehet igaz, és lehet hamis is. Emellett nincs előre kitüntetve, hogy az adott formulát milyen struktúra felett kell vizsgálni.

Matematikai logika

3. előadás

Begépelte: Vajna Miklós (AYU9RZ)

2010. november 2.

1. Táblázatból formula

Példa Egy nem túl nagy, nem túl kis táblázat, 3 változóval:

x	y	z	f	ϕ_1	ϕ_2	ϕ_6
i	i	i	i	i	h	h
i	i	h	i	h	i	h
i	h	i	h	h	h	h
i	h	h	h	h	h	h
h	i	i	h	h	h	h
h	i	h	i	h	h	i
h	h	i	h	h	h	h
h	h	h	h	h	h	h

keressünk formulát, melynek pont ez a táblázata.

$\phi_1 = x \wedge y \wedge z$ - ez csak az első sorban igaz.

$\phi_2 = x \wedge y \wedge \neg z$ - ez csak a második sorban igaz.

$\phi_6 = \neg x \wedge y \wedge \neg z$ - ez csak a hatodik sorban igaz.

$f = \phi_1 \vee \phi_2 \vee \phi_6$ jó lesz.

Definíció Logikai műveletek egy F halmazát funkcionálisan teljesnek nevezzük, ha minden $f : \{i, h\}^n \rightarrow \{i, h\}$ kifejezhető F-beli műveletekkel.

1.1. Tétel. $\{\neg, \wedge, \vee\}$ *funkcionálisan teljes.*

Bizonyítás Legyen $f : \{i, h\}^n \rightarrow \{i, h\}$ tetszőleges. Ha $s \in \{i, h\}^n$, akkor legyen

$$x_j^s = \begin{cases} x_j & \text{ha } s \text{ j. koordinátája igaz} \\ \neg x_j & \text{ha } s \text{ j. koordinátája hamis} \end{cases}$$

f a következő formula táblázata:

$$\bigvee_{s:f(s)=i} (x_1^s \wedge x_2^s \wedge \dots \wedge x_n^s) \text{ (diszjunktív normálforma, DNF.)}$$

A zárójelen belüli rész csak s-ben lesz igaz. Rögzített s-re $x_1^s \wedge \dots \wedge x_n^s$: elemei konjunkció. ■

Bizonyítás (másik.) Legyen $f : \{i, h\}^n \rightarrow \{i, h\}$. Ha $s \in \{i, h\}^n$, akkor

$$!(x_j)_s = \begin{cases} x_j & \text{ha } s_j = h \\ \neg x_j & \text{ha } s_j = i \end{cases}$$

f a következő formula táblázata:

$$\bigwedge_{s:f(s)=h} ((x_1)_s \vee (x_2)_s \vee \dots \vee (x_n)_s) \text{ (konjunktív normálforma, KNF.)}$$

A zárójelen belüli rész csak s-ben lesz hamis. Rögzített s-re $(x_1)_s \vee \dots \vee (x_n)_s$: elemi diszjunktív. ■

Következmény:

1.2. Tétel. Minden ϕ formulához van ϕ' DNF: $\phi \equiv \phi'$.

Bizonyítás ϕ táblázatához van őt leíró DNF, ez lesz a ϕ' . ■

Megjegyzés . Ugyanez igaz KNF-re is.

1.3. Tétel. $\{\wedge, \neg\}$ is funkcionálisan teljes.

Bizonyítás Elég: $x \vee y$ kifejezhető.

$$x \vee y \equiv \neg\neg(x \vee y) \equiv \neg(\neg x \wedge \neg y) \quad \blacksquare$$

Emlékeztető: a fenti a De Morgan azonosságok miatt igaz.

Diszjunkcióra: $\neg(x \vee y) \equiv \neg x \wedge \neg y$.

Konjunkcióra: $\neg(x \wedge y) \equiv \neg x \vee \neg y$.

1.4. Tétel. $\{\vee, \neg\}$ is funkcionálisan teljes.

Bizonyítás $x \wedge y \equiv \neg\neg(x \wedge y) \equiv \neg(\neg x \vee \neg y)$. ■

1.5. Tétel. $\{\Rightarrow, \neg\}$ is funkcionálisan teljes.

Bizonyítás $x \vee y \equiv \neg x \Rightarrow y$. ■

Mese:

1. $\{\wedge, \vee\}$ nem funkcionálisan teljes: összetettség szerinti indukcióval igazolható, hogy az ezekkel felírt függvények minden változójukban monoton növekvőek, a negáció viszont nem az, emiatt nem fejezhető ki.
2. $\{\neg\}$ nem funkcionálisan teljes. Indoklás: az ezzel felírt függvények egy változósak, és például a $\wedge$ két változós.
3. Legyen $x|y$ a következő művelet (Sheffer-féle sem-sem):

x	y	$x y$
i	i	h
i	h	h
h	i	h
h	h	i

1.6. Tétel. Ez funkcionálisan teljes.

Bizonyítás $\neg x \equiv x|x$,
 $x \vee y \equiv \neg(x|y) \equiv (x|y)|(x|y)$. ■

Megjegyzés .

1. $\{\neg, \vee, \wedge\}$ áramköri elemekkel megvalósítható.
2. Kevés jelet tartalmazó formulát "nehéz" találni (optimum megtalálása NP-teljes).
3. Kevés igaz érték esetén DNF-et célszerű keresni, kevés hamis érték esetén KNF-et.

2. Elsőrendű formulák között normálformák keresése

Definíció Legyen ϕ, ψ elsőrendű formula. $\phi \equiv \psi$, ha tetszőleges $\mathcal{A}$ -ra és k -ra $\mathcal{A} \models \phi[k]$ pont akkor, ha $\mathcal{A} \models \psi[k]$.

Ismert: általánosított De Morgan szabályok:

- $\neg \exists x \phi \equiv \forall x \neg \phi$.
- $\neg \forall x \phi \equiv \exists x \neg \phi$.

További példák:

- Univerzális kvantor disztributív az $\wedge$ -re:
 $\forall x (P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$.
- Egzisztenciális kvantor disztributív a $\vee$ -ra:
 $\exists x (P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x))$.
- De: $\forall x (P(x) \vee Q(x)) \not\equiv (\forall x P(x)) \vee (\forall x Q(x))$.
Indoklás: Legyen $A = N$, $P(x) : x$ páros, $Q(x) : x$ páratlan.
! $\mathcal{N} = \langle A, P, Q \rangle$. Ekkor
 $\mathcal{N} \models \forall x (P(x) \vee Q(x))$ és
 $\mathcal{N} \not\models (\forall x P(x)) \vee (\forall x Q(x))$.

Definíció Legyen ϕ formula, x változó.

- x egy előfordulása ϕ -ben szabad, ha x nincs rá vonatkozó kvantor hatáskörében.

- x előfordulása ϕ -ben kötött, ha nem szabad.
- ϕ formula egy mondat, ha minden változójának minden előfordulása kötött.

2.1. Tétel. *Legyen ϕ formula, $\mathcal{A}$ struktúra, k és l értékelések $\mathcal{A}$ felett úgy, hogy ha x szabad ϕ -ben, akkor $k(x) = l(x)$. Ekkor*

$$(*)\mathcal{A} \models \phi[k] \text{ pontosan akkor, ha } \mathcal{A} \models \phi[l].$$

Azaz ϕ igazsága csak szabad változóitól függ.

Bizonyítás $(*)$ -ot ϕ összetettsége szerinti indukcióval igazoljuk.

Atomi formulákra $(*)$ triviális.

Tegyük fel, hogy $(*)$ igaz ϕ, ψ -re (és minden k -ra).

Kell: $\neg\phi$ -re öröklődik, mert

$\mathcal{A} \models \neg\phi[k]$ pont akkor, ha

$\mathcal{A} \not\models \phi[k]$ pont akkor (indukció), ha

$\mathcal{A} \not\models \phi[l]$ pont akkor, ha

$\mathcal{A} \models \phi[l]$.

$\phi \wedge \psi$ -re:

$\mathcal{A} \models \phi \wedge \psi[k]$ pont akkor, ha

$\mathcal{A} \models \phi[k]$ és $\mathcal{A} \models \psi[k]$ pont akkor (indukció), ha

$\mathcal{A} \models \phi[l]$ és $\mathcal{A} \models \psi[l]$ pont akkor, ha

$\mathcal{A} \models \phi \wedge \psi[l]$.

$\exists x\phi$ -re: $\mathcal{A} \models \exists x\phi[k]$ pont akkor, ha

$(**) \text{ van } k \equiv^x k' \text{ (x-közel): } \mathcal{A} \models \phi[k']$.

$$\text{Legyen } l'(y) = \begin{cases} l(y) & \text{ha } y \neq x \\ k'(x) & \text{különben.} \end{cases}$$

Mivel k' és l' megegyezik ϕ szabad változóin, az indukciós feltevés miatt $(**)$ ekvivalens azzal, hogy van $l' \equiv^x l$: $\mathcal{A} \models \phi[l']$. Ez viszont pont akkor teljesül, ha, $\mathcal{A} \models \exists x\phi[l]$.

$\{\neg, \wedge, \exists\}$ -al minden formula kifejezhető. ■

A fentiek következménye: A kötött változók a jelentés megváltoztatása nélkül átnevezhetők.

Általános kvantor-kiemelési szabály:

$(Qx\phi) \vee \wedge \psi \equiv Qx(\phi \vee \wedge \psi)$, ha x nem fordul elő ψ -ben szabadon.

Q lehet $\exists, \forall$; $\vee \wedge$ lehet $\wedge, \vee$. (Nem bizonyítjuk.)

Definíció A ϕ prenex-formájú, ha $\phi \equiv Q_1x_1Q_2x_2\ldots Q_nx_n\psi$, ahol $Q_1\ldots Q_n$ kvantorok és ψ kvantormentes formula ($n = 0$ is megengedett, ekkor nincs kvantorblokk a formula elején).

2.2. Tétel. Tetszőleges elsőrendű ϕ -hez van prenex alakú Φ' úgy, hogy $\phi \equiv \Phi'$.

Bizonyítás Hajtsuk végre a következő algoritmust:

1. $\Leftrightarrow, \Rightarrow$ kiküszöbölése ($\vee, \wedge, \neg$ -re cserélése);
2. $\neg$ hatásköreinek redukálása (De Morgan, disztributivitás);
3. Az egyes változókat esetleg átnevezve alkalmazzuk az általános kvantor-kiemelési szabályt.

Példa . Formula prenex-alakra hozása:

$$\begin{aligned} & \neg \forall y (\exists x P(x) \Rightarrow \forall y (P(x) \vee R(x, f(y)))) \equiv \\ & \neg \forall y (\neg (\exists x P(x)) \vee \forall y (P(x) \vee R(x, f(y)))) \equiv \\ & \neg \forall y (\forall x \neg P(x)) \vee \forall y (P(x) \vee R(x, f(y))) \equiv \\ & \exists y (\neg \forall x \neg P(x)) \wedge \neg \forall y (P(x) \vee R(x, f(y))) \equiv \\ & \exists y (\exists x P(x) \wedge \exists y (\neg (P(x)) \wedge \neg R(x, f(y)))) \equiv \end{aligned}$$

A baloldali x változót z -re nevezzük át, hogy kiemelhessük:

$$\exists y \exists z (P(z) \wedge \exists y (\neg P(x) \wedge \neg R(x, f(y)))) \equiv$$

A jobb oldali y változót v -re nevezzük át:

$$\exists y \exists z \exists v (P(z) \wedge (\neg P(x) \wedge \neg R(x, f(v)))).$$

Ez már prenex-alak.

Matematikai logika – 4. előadás

Begépelte: Devecseri Viktor

2010. november 4.

1. Logikai következmény

1.1. Ítéletkalkulusban

Definíció. Legyen $k : \{változók\} \rightarrow \{i, h\}$. Legyen Σ formulahalmaz, ϕ formula.

- $\underbrace{k \models \Sigma}_{k\text{-ban igaz } \Sigma}$, ha minden $\rho \in \Sigma : k \models \rho$.
- $\underbrace{\Sigma \models \rho}_{\Sigma\text{-nak következménye } \rho}$, ha minden k -ra, $k \models \Sigma$ esetén $k \models \rho$.

Példa.

Szövegesen:

1. Ha Zita nem éri el az 50%-ot, akkor megbukik.
2. Vagy puskázik, vagy nem éri el az 50%-ot.
3. Tehát ha puskázik, akkor átmegy.

Változók:

1. E: eléri az 50%-ot.
2. B: megbukik
3. P: puskázik

Formulákkal:

1. $\neg E \Rightarrow B$
2. $P \vee \neg E$
3. $P \Rightarrow \neg B$

Kérdés. $\underbrace{\{1, 2\}}_{\Sigma} \models \underbrace{3}_{\phi}$?

n	E	B	P	$\neg E \Rightarrow B$	$P \vee \neg E$	$P \Rightarrow \neg B$
1	i	i	i	i	i	h
2	i	i	h	i	h	i
3	i	h	i	i	i	i
4	i	h	h	i	h	i
5	h	i	i	i	i	h
6	h	i	h	i	i	i
7	h	h	i	h	i	i
8	h	h	h	h	i	i

Σ a táblázat 1, 3, 5 és 6. sorában igaz.

A táblázat első sora mutatja, hogy $\Sigma \not\models \phi$, mert Zita bár puskázik, de mégis megbukik.

Ha n db feltétel változó van, akkor 2^n db esetet kell ellenőrizni.

1.2. Elsőrendű logikában

Definíció. Legyen Σ formulahalmaz, ϕ formula, $\mathcal{A}$ struktúra.

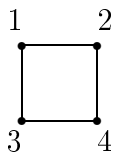
- $\underbrace{\mathcal{A} \models \Sigma}_{\Sigma \text{ igaz } \mathcal{A}\text{-ban}}$, ha minden $\rho \in \Sigma$ -ra $\mathcal{A} \models \rho$.
- $\underbrace{\Sigma \models \phi}_{\Sigma\text{-nak következménye } \phi}$, ha minden $\mathcal{A}$ struktúrában $\mathcal{A} \models \Sigma$ esetén $\mathcal{A} \models \phi$.

Példa.

- $\Sigma = \{\forall x \exists y R(x, y)\}$,
- $\phi = \exists y \forall x R(x, y)$.

Kérdés. $\Sigma \models \phi$?

Legyen $A = \{1, 2, 3, 4\}$ alaphalmaz, $R(x, y)$: az ábra szerint él megy x -ből y -ba, $\mathcal{G} = \langle A, R, = \rangle$ struktúra.



- $\mathcal{G} \models \Sigma$, mert minden csúcsnak van szomszédja.
- $\mathcal{G} \not\models \phi$, mert nincs olyan csúcs, amely minden csúccsal össze lenne kötve.

Tehát: $\Sigma \not\models \phi$.

2. Bizonyításelmélet

2.1. Halálcsillag

Legyen az L nyelvben 1 db 2 változós reláció szimbólum, és legyen n egy véges szám. Hány n elemű modellje van L -nek? Annyi, ahány részhalmaza van egy n elemű halmaz direkt-négyzetének. $\rightarrow 2^{n^2}$ db van.

Például $n = 20$ -ra: $2^{n^2} = 2^{400} = (2^4)^{100} = 16^{100} > 10^{100}$.

Ezeket géppel próbáljuk megvizsgálni. Legyen egy lépés 1 db struktúra megvizsgálása, amely legalább annyi idő, amíg fénysebességgel átmegyünk egy elektron átmérőjén. Az elektron átmérője $> 10^{-15}\text{m}$. A fénysebességet ($< 3 \cdot 10^8 \frac{\text{m}}{\text{s}}$) nagyvonalúan felülről becsüljük $10^9 \frac{\text{m}}{\text{s}}$ -el. Tehát másodpercenként legfeljebb 10^{24} eset vizsgálható meg.

Egy gép tömege legalább annyi, mint egy elektron tömege ($9.1 \cdot 10^{-31}\text{kg} \geq 10^{-31}\text{kg}$). Vegyünk annyi ilyen gépet, amennyi a Föld tömege ($5.974 \cdot 10^{24}\text{kg} \leq 10^{25}\text{kg}$). Egy ilyen halálcsillaggal másodpercenként maximum $10^{24} \cdot 10^{56} = 10^{80}$ eset vizsgálható meg. Egy nap kevesebb, mint $86\,400 \leq 10^5$ másodperc, és egy évben $365 \leq 10^3$ nap van. Tehát a halálcsillaggal évente 10^{88} eset vizsgálható át. Az Univerzum kora $1.3 \cdot 10^9 \leq 10^{10}$ év. Tehát a 20 elemű struktúrák átnézése halálcsillaggal legalább 100-szorosa az univerzum korának.

Mi van a 21 elemű struktúrákkal? A végtelen alaphalmazú struktúrák *elvileg* sem nézhetők így át. Tehát $\Sigma \models \phi$ eldöntéséhez mást kell csinálni.

2.2. Bizonyításelmélet (ítéletkalkulusban)

Definíció. Axióma sémák:

1. $\alpha \Rightarrow \beta \Rightarrow \gamma$,
2. $(\alpha \Rightarrow \beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)$,
3. $(\neg\alpha \Rightarrow \beta) \Rightarrow (\neg\alpha \Rightarrow \neg\beta) \Rightarrow \alpha$.

α, β, γ formula változók.

Axiómák: α, β, γ helyére tetszőleges formulákat írhatunk.

Definíció. Modus Ponens: $\frac{\alpha \Rightarrow \beta, \alpha}{\beta}$

Definíció. Legyen Σ formulahalmaz, ϕ formula.

$\underbrace{\Sigma \vdash \phi}_{\Sigma\text{-ből } \phi \text{ levezethető}}$ ha van olyan véges $\alpha_1, \dots, \alpha_n$ formulasorozat, hogy $\alpha_n = \phi$ és mindent $i \leq n$ -re:

- α_i axióma, vagy
- $\alpha_i \in \Sigma$, vagy
- α_i Modus Ponens-el megkapható korábbi α_j -kből.

Megjegyzések.

1. $\Sigma \vdash \phi$ definíciójában nincs szó a jelentésről.
2. Adott $\alpha_1, \dots, \alpha_n$ -ről algoritmikusan eldönthető, hogy ϕ -t vezeti-e le Σ -ból.

Példa. Tetszőleges ϕ formulára $\emptyset \vdash \phi \Rightarrow \phi$.

$$1. \left(\underbrace{\phi}_{\alpha} \Rightarrow \underbrace{(\phi \Rightarrow \phi)}_{\beta} \Rightarrow \underbrace{\phi}_{\gamma} \right) \Rightarrow \left(\underbrace{\phi}_{\alpha} \Rightarrow \underbrace{(\phi \Rightarrow \phi)}_{\beta} \right) \Rightarrow \left(\underbrace{\phi}_{\alpha} \Rightarrow \underbrace{\phi}_{\gamma} \right)$$

2. axióma

$$2. \underbrace{\phi}_{\alpha} \Rightarrow \underbrace{(\phi \Rightarrow \phi)}_{\beta} \Rightarrow \underbrace{\phi}_{\alpha}$$

1. axióma

$$3. (\phi \Rightarrow (\phi \Rightarrow \phi)) \Rightarrow (\phi_{\alpha} \Rightarrow \phi_{\gamma})$$

MP 1 és 2-n

$$4. \underbrace{\phi}_{\alpha} \Rightarrow \left(\underbrace{\phi}_{\beta} \Rightarrow \underbrace{\phi}_{\alpha} \right)$$

1. axióma

$$5. \phi \Rightarrow \phi$$

MP(3,4)

Cél: *Teljeségi tétel:* Legyen Σ formulahalmaz, ϕ formula. $\Sigma \models \phi$ pontosan akkor, ha $\Sigma \vdash \phi$.

(Azaz egy következtetés pontosan akkor helyes, ha formálisan be lehet bizonyítani.)

Definíció. Legyen Σ formulahalmaz, $\text{Ded}(\Sigma) = \{\phi : \Sigma \vdash \phi\}$.

Állítás.

1. $\Sigma \subseteq \text{Ded}(\Sigma)$,
2. Ha $\Gamma \subseteq \Sigma$ akkor $\text{Ded}(\Gamma) \subseteq \text{Ded}(\Sigma)$ (monotonitás),
3. $\text{Ded}(\text{Ded}(\Sigma)) = \text{Ded}(\Sigma)$ (ideompotencia).

Bizonyítás.

1. Triviális. Ha $\phi \in \Sigma$, akkor ϕ egy 1-lépéses levezetése ϕ -nek Σ -ból. Így $\phi \in \text{Ded}(\Sigma)$.
2. Legyen $\phi \in \text{Ded}(\Gamma)$, tehát van $\alpha_1, \dots, \alpha_n$ ($\alpha_n = \phi$) úgy, hogy $(\forall i \leq n)$:
 - (a) α_i axióma, vagy
 - (b) $\alpha_i \in \Gamma$, vagy
 - (c) α_i MP-vel jön korábbi α_j -kből.

$\alpha_1, \dots, \alpha_n$ mutatja, hogy $\Sigma \vdash \phi$ azaz $\phi \in \text{Ded}(\Sigma)$.

3. (1) miatt $\Sigma \subseteq \text{Ded}(\Sigma)$, (2) miatt $\text{Ded}(\Sigma) \subseteq \text{Ded}(\text{Ded}(\Sigma))$. Elég: $\text{Ded}(\text{Ded}(\Sigma)) \subseteq \text{Ded}(\Sigma)$

Legyen $\phi \in \text{Ded}(\text{Ded}(\Sigma))$. Ekkor van $\alpha_1, \dots, \alpha_n$ ($\alpha_n = \phi$), hogy $\forall i \leq n$ -re:

- (a) α_i axióma, vagy
- (b) $\alpha_i \in \text{Ded}(\Sigma)$, vagy
- (c) α_i MP-vel jön korábbi α_j -kből.

Kell: $\phi \in \text{Ded}(\Sigma)$.

Ha $\alpha_i \in \text{Ded}(\Sigma)$, akkor $\alpha_1, \dots, \alpha_n$ -ben α_i -t cseréljük ki egy Σ -beli levezetésre. Amit így kapunk mutatja, hogy $\Sigma \vdash \phi$.

□

Tétel. (Dedukciós tétel) Legyen Σ formulha halmaz, ϕ, ψ formula. Ekkor a következők ekvivalensek:

- 1. $\Sigma \vdash \phi \Rightarrow \psi$,
- 2. $\Sigma \cup \{\phi\} \vdash \psi$;

(Implikáció levezethető, ha $\Sigma \cup \{\phi\} \vdash \psi$.)

Bizonyítás.

- (1) $\Rightarrow$ (2): (1) és előző állítás (2) (monotonitás) miatt
 - 1. $\Sigma \cup \{\phi\} \vdash \phi \Rightarrow \psi$
 - 2. $\Sigma \cup \{\phi\} \vdash \phi$
 - 3. MP(1,2): $\Sigma \cup \{\phi\} \vdash \psi$.
- (2) $\Rightarrow$ (1): legközelebb.

□

Matematikai logika - 5. előadás

2010. november 9.

Bizonyításelmélet (folytatás)

Dedukciós tétel Legyen Σ formulahalmaz és ϕ, ψ formula. Ekkor a következők ekvivalensek:

$$\Sigma \vdash \phi \Rightarrow \psi \quad (1)$$

$$\Sigma \cup \{\phi\} \vdash \psi \quad (2)$$

Bizonyítás $(1) \Rightarrow (2)$: lásd előző előadás. $(2) \Rightarrow (1)$: ha $\Sigma \cup \{\phi\} \vdash \psi$, akkor van olyan véges $\alpha_1 \dots \alpha_n$ formulasorozat, hogy $\alpha_n = \psi$ és $\forall i \leq n$ -re

$$\alpha_i \begin{cases} \text{axióma vagy} \\ \in \Sigma \cup \{\phi\} \text{ (azaz } \alpha_i \in \Sigma \text{ vagy } \alpha_i = \phi) \text{ vagy} \\ \text{van } k, l < i : \alpha_i \text{ megkapható Modus Ponenssel } \alpha_k, \alpha_l\text{-ből.} \end{cases}$$

i -re vonatkozó teljes indukcióval megmutatjuk, hogy $\Sigma \vdash \phi \Rightarrow \alpha_i$ ($i = n$ -re ez éppen (1)).

$i = 1$ esetén

α_1 axióma esetén:

$\Sigma \vdash \alpha_1 \Rightarrow \phi \Rightarrow \alpha_1$ (ez az első axióma egy példánya)

α_1 axióma

$\phi \Rightarrow \alpha_1$ Modus Ponenssel kapható az előző kettőből.

$\alpha_1 \in \Sigma$ hasonlóan:

$\Sigma \vdash \alpha_1 \Rightarrow \phi \Rightarrow \alpha_1$ (ez az első axióma egy példánya)

$\alpha_1 \in \Sigma$

$\phi \Rightarrow \alpha_1$ Modus Ponenssel kapható az előző kettőből.

ha $\alpha_1 = \phi$:

$\emptyset \vdash \phi \Rightarrow \phi$ ezért $\Sigma \vdash \phi \Rightarrow \phi$.

Indukciós lépés Tegyük fel, hogy ha $j < i$, akkor $\Sigma \vdash \phi \Rightarrow \alpha_j$ (kell $\Sigma \vdash \phi \Rightarrow \alpha_i$)

ha α_i axióma vagy $\alpha_i \in \Sigma \cup \{\phi\}$, akkor $i = 1$ esethez hasonlóan $\Sigma \vdash \phi \Rightarrow \alpha_i$.

ha α_i Modus Ponenssel jön α_k, α_l -ből ($k, l < i$), akkor $\alpha_k = \alpha_l \Rightarrow \alpha_i$ és az indukciós feltevés miatt $\Sigma \vdash \phi \Rightarrow \alpha_k$ azaz $\Sigma \vdash \phi \Rightarrow (\alpha_l \Rightarrow \alpha_i)$ és $\Sigma \vdash \phi \Rightarrow \alpha_l$

Ekkor a 2. axiómát kétszer kombinálva a modus ponens-sel:

$$\begin{aligned} (\phi \Rightarrow \alpha_l \Rightarrow \alpha_i) &\Rightarrow (\phi \Rightarrow \alpha_l) \Rightarrow \phi \Rightarrow \alpha_i \\ (\phi \Rightarrow \alpha_l) &\Rightarrow \phi \Rightarrow \alpha_i \\ \phi &\Rightarrow \alpha_i. \end{aligned}$$

□

Definíció Legyen Σ formulahalmaz. Azt mondjuk, hogy Σ ellentmondásos, ha van olyan ϕ formula, hogy $\Sigma \vdash \phi, \Sigma \vdash \neg\phi$.

Tétel Az alábbiak közül (1) ekvivalens (2)-vel és (3) ekvivalens (4)-el.

1. $\Sigma \vdash \phi$
2. $\Sigma \cup \{\neg\phi\}$ ellentmondásos.
3. $\Sigma \vdash \neg\phi$
4. $\Sigma \cup \{\phi\}$ ellentmondásos.

Bizonyítás

(1) $\Rightarrow$ (2) $\vdash$ monotonitása (azaz multkori (1)) miatt $\Sigma \cup \{\neg\phi\} \vdash \phi$. Továbbá nyilván $\Sigma \cup \{\neg\phi\} \vdash \neg\phi$. (mert $\neg\phi \in \Sigma \cup \{\neg\phi\}$). Tehát $\Sigma \cup \{\neg\phi\}$ ellentmondásos.

(2) $\Rightarrow$ (1) $\Sigma \cup \{\neg\phi\}$ ellentmondásos, ezért van olyan α , hogy

$$\begin{array}{ccc} \Sigma \cup \{\neg\phi\} \vdash \alpha & \text{és} & \Sigma \cup \{\neg\phi\} \vdash \neg\alpha \\ \downarrow \text{dedukciós t. miatt} & & \downarrow \text{dedukciós t. miatt} \\ \Sigma \vdash \neg\phi \Rightarrow \alpha & & \Sigma \vdash \neg\phi \Rightarrow \neg\alpha \end{array}$$

Ekkor

$\Sigma \vdash (\neg\phi \Rightarrow \alpha) \Rightarrow (\neg\phi \Rightarrow \neg\alpha) \Rightarrow \phi$ (3. axióma miatt)

$\Sigma \vdash \phi$ (Modus Ponens kétszer).

(3) $\Rightarrow$ (4) (3) miatt

$\Sigma \cup \{\phi\} \vdash \neg\phi$ (monotonitás miatt)

$\Sigma \cup \{\phi\} \vdash \phi$ (mert szerepel a bal oldalon)

Tehát $\Sigma \cup \{\phi\}$ ellentmondásos.

(4) $\Rightarrow$ (3) Vegyük észre: $\{\neg\neg\phi, \neg\phi\}$ ellentmondásos, ezért a tétel már igazolt része miatt $\{\neg\neg\phi\} \vdash \phi$. (4) szerint $\Sigma \cup \{\phi\}$ ellentmondásos így $\Sigma \cup \{\neg\neg\phi\}$ is ellentmondásos (hiszen $\Sigma \cup \{\neg\neg\phi\} \vdash \phi$ és $\Sigma \cup \{\phi\}$ ellentmondásos). Így (2) $\Leftrightarrow$ (1) miatt $\Sigma \vdash \neg\phi$ azaz (3) teljesül.
□

Tétel Ellentmondásos Σ -ból minden levezethető.

Bizonyítás Legyen Σ ellentmondásos és ϕ tetszőleges. Mivel Σ ellentmondásos, ezért van olyan α , hogy $\Sigma \vdash \alpha, \Sigma \vdash \neg\alpha$, ekkor $\Sigma \cup \{\neg\phi\} \vdash \alpha$ és $\Sigma \cup \{\neg\phi\} \vdash \neg\alpha$. Ezekből pedig következik, hogy $\Sigma \cup \{\neg\phi\}$ is ellentmondásos. Így az előző tétel miatt $\Sigma \vdash \phi$. □

Definíció Legyen Σ formulahalmaz. Σ teljes, ha tetszőleges ϕ formulára $\Sigma \vdash \phi$ vagy $\Sigma \vdash \neg\phi$.

Tétel Ha Σ ellentmondástalan formulahalmaz, akkor van olyan Σ' teljes, ellentmondástalan formulahalmaz, hogy $\Sigma \subseteq \Sigma'$. Sőt tetszőleges ϕ -re $\phi \in \Sigma'$ vagy $\neg\phi \in \Sigma'$.

Bizonyítás A formulák halmaza megszámlálhatóan végtelen, így fel tudjuk őket sorolni. Legyen $\{\alpha_i : i \in N\}$ egy ilyen felsorolás.

Megadjuk formulahalmazok egy $\Sigma_0, \Sigma_1 \dots$ végtelen sorozatát úgy, hogy

1. $\Sigma_0 = \Sigma, i \leq j \Rightarrow \Sigma_i \subseteq \Sigma_j$;
2. Σ_i ellentmondástalan;
3. $\alpha_i \in \Sigma_{i+1}$ vagy $\neg\alpha_i \in \Sigma_{i+1}$;

Legyen $\Sigma_0 = \Sigma$. Tegyük fel, hogy ha $j \leq i$, akkor Σ_j adott már úgy, hogy 1-3 teljesül.

Legyen $\Sigma_{i+1} = \begin{cases} \Sigma_i \cup \{\alpha_i\}, & \text{ha ez ellentmondástalan} \\ \Sigma_i \cup \{\neg\alpha_i\} & \text{egyébként.} \end{cases}$

Ha $\Sigma \cup \{\alpha_i\}$ ellentmondásos, akkor az előző tétel szerint $\Sigma_i \vdash \neg\alpha_i$, ezért mindkét esetben 1-3. érvényben marad.

Legyen $\Sigma' = \bigcup_{n \in N} \Sigma_n$.

1. miatt $\Sigma \subseteq \Sigma'$.
3. miatt tetszőleges α -ra $\alpha \in \Sigma'$ vagy $\neg\alpha \in \Sigma'$.

Végül Σ' ellentmondástalan, mert tegyük fel indirekt, hogy Σ' ellentmondásos. Ekkor van olyan ϕ formula, hogy $\Sigma' \vdash \phi, \Sigma' \vdash \neg\phi$. $\Sigma' \vdash \phi$ és $\Sigma' \vdash \neg\phi$ véges levezetés, így van olyan n , hogy $\Sigma_n \vdash \phi, \Sigma_n \vdash \neg\phi$, ami pedig ellentmond 2.-nek.

□

Teljességi tétel Ekvivalensek:

1. $\Sigma \models \phi$.
2. $\Sigma \vdash \phi$.

Megjegyzés $1 \Rightarrow 2$ a kalkulus teljessége: ha egy következtetés helyes, akkor azt formálisan be is lehet bizonyítani. $2 \Rightarrow 1$ a kalkulus helyessége.

Bizonyítás

$1 \Rightarrow 2$ Tegyük fel, hogy $\Sigma \models \phi$, de $\Sigma \not\models \phi$, azaz $\Sigma \cup \{\neg\phi\}$ ellentmondástalan.

Cél: van olyan k interpretáció, hogy $k \models \Sigma \cup \{\neg\phi\}$. (Ez elég, mert ez a k mutatja, hogy $\Sigma \not\models \phi$, ami ellentmond 1.-nek.

Legyen $\Gamma = \Sigma \cup \{\neg\phi\}$; ez ellentmondástalan. Ekkor elég: van $k \models \Gamma$.

Az előző tétel szerint van teljes, ellentmondástalan $\Gamma' : \Gamma \subseteq \Gamma'$. (Sőt tetszőleges α -ra $\alpha \in \Gamma'$ vagy $\neg\alpha \in \Gamma'$).

Ha x ítéletváltozó, akkor legyen $k(x) = \begin{cases} \text{igaz, ha } x \in \Gamma' \\ \text{hamis különben} \end{cases}$

Figyeljük meg: $k(x) = i \Leftrightarrow x \in \Gamma'$.

ϕ összetettsége szerinti indukcióval megmutatjuk, hogy

$$k \models \phi \text{ pontosan akkor, ha } \phi \in \Gamma'. \quad (3)$$

1. Ha ϕ ítéletváltozó, akkor (3) k definíciója miatt igaz.

2. Tegyük fel, hogy (3) igaz ϕ -re és ψ -re.

3. Belátjuk (3)-t $\neg\phi$ -re: $k \models \neg\phi$ pont akkor, ha $k \not\models \phi$. Az indukció miatt pont akkor, ha $\phi \notin \Gamma'$ pont akkor $\neg\phi \in \Gamma'$.

(3)-t belátjuk $\phi \Rightarrow \psi$ -re is:

$k \models \phi \Rightarrow \psi$ pont akkor, ha $k \not\models \phi$ vagy $k \models \psi$ (az implikáció definíciója miatt)

Az indukcióból: $\phi \notin \Gamma'$ ((a) eset) vagy $\psi \in \Gamma'$ ((b) eset). Kell: $\phi \Rightarrow \psi \in \Gamma'$.

(a) esetben $\neg\phi \in \Gamma'$ (Γ teljessége és ellentmondásmentessége miatt.) $\{\neg\phi, \phi\}$ ellentmondásos ezért $\{\neg\phi, \phi\} \vdash \psi$ így a dedukciós tétel miatt $\neg\phi \vdash \phi \Rightarrow \psi$.

Ezért $\phi \Rightarrow \psi \in \Gamma$, különben Γ' teljessége miatt ellentmondásos lenne.

(b) esetben $\psi \in \Gamma'$

$\psi \vdash \psi \Rightarrow \phi \Rightarrow \psi$ (1. axióma)

ψ

$\phi \Rightarrow \psi$ (MP)

Ezért $\phi \Rightarrow \psi \in \Gamma'$, különben Γ' teljessége miatt ellentmondásos lenne.

Eddig kaptuk: Ha $k \models \phi \Rightarrow \psi$ akkor $\phi \Rightarrow \psi \in \Gamma'$.

Fordítva: Ha $\phi \Rightarrow \psi \in \Gamma'$ akkor állítjuk, hogy $\neg\phi \in \Gamma'$ vagy $\psi \in \Gamma'$: különben, $\phi \in \Gamma'$, $\neg\psi \in \Gamma'$ következne, ezt $\Gamma' \vdash \phi \Rightarrow \psi$ -vel és MP-vel kombinálva $\Gamma' \vdash \psi$ adódna, de ekkor Γ' ellentmondásos lenne.

Ha tehát $\phi \Rightarrow \psi \in \Gamma'$, akkor az előző néhány sor miatt $\neg\phi \in \Gamma'$ vagy $\psi \in \Gamma'$ következésképp, az indukció miatt $k \models \neg\phi$ vagy $k \models \psi$.

Mindkét esetben $k \models \phi \Rightarrow \psi$.

Tehát (3) fennáll.

Így $1 \Rightarrow 2$ (teljesség) megvan. $\square$

<Teljességi tétel bizonyításának folytatása>:

(2) $\Rightarrow$ (1): tegyük fel, hogy 2. szerint: $\Sigma \vdash \varphi$. Ekkor van olyan véges formula sorozat ($\alpha_1 \dots \alpha_n$), hogy $\alpha_n = \varphi$ és az összes többi α_i -re ($1 \leq i \leq n$):

- α_i axióma, vagy
- $\alpha_i \in \Sigma$, vagy
- α_i *modus ponens*-sel kapható korábbi α_j -kből.

Ezután i szerinti indukcióval megmutatjuk, hogy $\Sigma \models \alpha_i$ minden i -re (így $\Sigma \models \alpha_n$ azaz $\Sigma \models \varphi$).

(*) Vegyük észre, hogy a *modus ponens* helyes: $\{P, P \Rightarrow Q\} \models Q$:
Ha $\sigma \models P$, $\sigma \models P \Rightarrow Q$ akkor σ -ban igaz a Q ($\sigma \models Q$).

Legyen σ olyan interpretáció, hogy $\sigma \models \Sigma$. Ekkor elég megmutatnunk, hogy $\sigma \models \alpha_i$.

Indukciós alaplépés: α_1 vagy axióma, ekkor $\sigma \models \alpha_1$ (táblázattal ellenőrizhető, hogy az axiómák minden interpretációban igazak), vagy $\alpha_1 \in \Sigma$.

Tegyük fel, hogy minden $j(<i)$ -re $\sigma \models \alpha_j$.

α_i vagy axióma, vagy $\alpha_i \in \Sigma$ (mint az alaplépésnél), vagy *modus ponens*-sel jön korábbi α_j -kből. Utóbbi esetben van $j, k < i$: $\alpha_k = \alpha_j \Rightarrow \alpha_i$, az indukció miatt $\sigma \models \{\alpha_k, \alpha_j\}$, azaz $\sigma \models \{\alpha_j \Rightarrow \alpha_i, \alpha_j\}$, így (*) miatt $\sigma \models \alpha_i$.

KÉSZ

Az elsőrendű logika bizonyításelmélete

Teljességi tétel

Megadható összesen 7 axiómaséma, hogy ezekből Modus Ponens-sel minden helyes következtetés bizonyítható.

Bizonyítás: vázlat (Elsőrendű esetben)

Ha $\Sigma \vdash \varphi$ akkor $\Sigma \models \varphi$: mint ítéletkalkulusban, indukció a levezetés hosszára.

Ha $\Sigma \models \varphi$ akkor $\Sigma \vdash \varphi$: be kell látni, hogy

- a.) $\Sigma \vdash \varphi$ pontosan akkor, ha $\Sigma \cup \{\neg \varphi\}$ ellentmondásos;
- b.) ellentmondástalan Σ kiterjeszthető teljes ellentmondástalan Σ' -vé;
- c.) teljes, ellentmondástalan Σ' formulahalmaznak van modellje.

Ezek után a többi részlet hasonló az ítéletkalkulus esetéhez.

Megjegyzés: (c) olyan $\mathcal{A}$ struktúrát ad, hogy $\mathcal{A} \models \Sigma$ és $|A| \leq |\Sigma|$.

Tétel: Eldönthetőség

Legyen Σ (nulladrendű vagy elsőrendű) véges és teljes formulahalmaz.

Van olyan algoritmus, mely minden bemenetre véges sok lépésben megáll (befejeződik) és adott φ -re (mint inputra) helyes választ ad arra, hogy „ $\Sigma \stackrel{?}{\models} \varphi$ ”.

Bizonyítás: Feltéhetjük, hogy Σ ellentmondástalan, mert ellentmondásos Σ -ra az állítás triviális. Mivel Σ véges, így felsorolhatók azok a véges $\alpha_1, \alpha_2 \dots \alpha_n$ formulasorozatok, melyek Σ -ból való levezetések. Soroljuk ezeket fel addig, amíg φ vagy $\neg\varphi$ meg nem jelenik egy levezetés végén. Σ teljes, így az algoritmus befejeződik. A teljességi tétel miatt a válasz helyes lesz. $(\Sigma \models \varphi$ pontosan akkor, ha $\Sigma \vdash \varphi)$

KÉSZ

Megjegyzés: lesz jobb módszer is erre.

Tétel: Kompaktsági tétel első alakja

Legyen Σ (nulladrendű vagy elsőrendű) formulahalmaz, φ formula.
Ekvivalensek:

- (1) $\Sigma \models \varphi$.
- (2) van olyan véges $\Sigma' \subseteq \Sigma$: $\Sigma' \models \varphi$.

Bizonyítás: $(2) \Rightarrow (1)$ triviális.

$(1) \Rightarrow (2)$: tegyük fel, hogy $\Sigma \models \varphi$, ekkor a teljességi tétel miatt: $\Sigma \vdash \varphi$.

Legyen $\alpha_1, \alpha_2 \dots \alpha_n$ egy ilyen levezetés ($\alpha_n = \varphi$), ebben Σ -nak csak véges sok eleme van, ezért $\Sigma' = \Sigma \cap \{\alpha_1, \alpha_2 \dots \alpha_n\}$ véges és ugyanez a sorozat $(\alpha_1, \alpha_2 \dots \alpha_n)$ mutatja, hogy $\Sigma' \vdash \varphi$. Végül a teljességi tétel miatt $\Sigma' \models \varphi$.

KÉSZ

Tétel: Kompaktsági tétel második alakja

Legyen Σ (nulladrendű vagy elsőrendű) formulahalmaz.
Ekvivalensek:

- (1) Σ -nak van modellje.
- (2) Σ összes VÉGES részének van modellje.

Bizonyítás: $(1) \Rightarrow (2)$ triviális.

$(2) \Rightarrow (1)$: tegyük fel, hogy Σ összes VÉGES részének van modellje, de Σ -nak nincs. A teljességi tétel (c) pontja miatt Σ ellentmondásos kell legyen. Ekkor létezik α formula, amire $\Sigma \vdash \alpha$, $\Sigma \vdash \neg\alpha$, így van véges $\Sigma' \subseteq \Sigma$: $\Sigma' \vdash \alpha$ és $\Sigma' \vdash \neg\alpha$ (úgy, mint az első kompaktsági tétel bizonyításában). A teljességi tétel miatt $\Sigma' \models \alpha$, $\Sigma' \models \neg\alpha$. Σ' véges, így $(\Sigma'$ -nek is) van $\mathcal{A}$ modellje: $\mathcal{A} \models \Sigma'$. Tehát $\mathcal{A} \models \alpha$ és $\mathcal{A} \models \neg\alpha$, ami viszont nem lehetséges, ellentmondásra jutunk.

KÉSZ

Definíció: Legyen $\mathcal{A}$ elsőrendű *struktúra*. $\mathcal{A}$ elmélete:

$$TH(\mathcal{A}) = \{\varphi : \mathcal{A} \models \varphi\}.$$

Legyen $\mathcal{B}$ struktúra. $\mathcal{A} \equiv_e \mathcal{B}$ *elemi ekvivalens*, ha $TH(\mathcal{A}) = TH(\mathcal{B})$.

Definíció:

$$! \mathcal{A} = \left\langle A, R_i^{\mathcal{A}}, f_j^{\mathcal{A}}, c_k^{\mathcal{A}} \right\rangle_{\substack{i \in I \\ j \in J \\ k \in K}} \quad ! \mathcal{B} = \left\langle B, R_i^{\mathcal{B}}, f_j^{\mathcal{B}}, c_k^{\mathcal{B}} \right\rangle_{\substack{i \in I \\ j \in J \\ k \in K}}$$

$\mathcal{A} \cong \mathcal{B}$ (izomorfok), ha létezik $\varphi : A \rightarrow B$ bijekció úgy, hogy

$$\forall a_1, a_2, \dots, a_n \in \mathcal{A}, \forall i \in I, \forall j \in J, \forall k \in K \text{-ra}$$

$$(a_1, a_2, \dots, a_n) \in R_i^{\mathcal{A}} \text{ pontosan akkor, ha } (\varphi(a_1), \varphi(a_2), \dots, \varphi(a_n)) \in R_i^{\mathcal{B}}$$

$$\varphi(f_j^{\mathcal{A}}(a_1 \dots a_n)) = f_j^{\mathcal{B}}(\varphi(a_1) \dots \varphi(a_n))$$

$$\varphi(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$$

Tétel:

- (1) Ha $\mathcal{A} \cong \mathcal{B}$, akkor $\mathcal{A} \equiv_e \mathcal{B}$.
- (2) (1) visszafele nem igaz. Sőt, ha $\mathcal{A}$ végtelen struktúra, akkor van olyan $\mathcal{A}'$, amire $\mathcal{A}' \equiv_e \mathcal{A}$, de $\mathcal{A}' \not\cong \mathcal{A}$. (azaz a végtelen struktúrák elsőrendben izomorfizmus erejéig leírhatatlanok.)

Bizonyítás:

(2) Legyen $\mathcal{A}$ végtelen struktúra.

Legyen I olyan halmaz, hogy $|I| > |A|$.

Legyen $\Sigma = \text{TH}(\mathcal{A}) \cup \{c_i \dot{=} c_j : i \dot{=} j, i, j \in I\}$, ahol a c_i -k új konstansszimbólumok.

Belátjuk, hogy Σ minden véges részének van modellje.

Legyen $\Sigma^* \subseteq \Sigma$ véges.

Van véges Γ_1, Γ_2 : $\Sigma^* = \Gamma_1 \cup \Gamma_2$

$$\Gamma_1 \subseteq \text{TH}(\mathcal{A}), \Gamma_2 = \{c_{i1} \dot{=} c_{j1}, \dots, c_{in} \dot{=} c_{jn}\}$$

Legyen $a_1 \dots a_k \in A$ annyi páronként különböző elem, amennyi „c” van Γ_2 -ben (ilyen van, mert Γ_2 véges és $\mathcal{A}$ végtelen).

$$\text{Legyen } \mathcal{A}^* = \langle A, \dots, a_1 \dots a_k \rangle$$

(<mint $\mathcal{A}$ leírása; $a_1 \dots a_k$: Γ_2 -beli konstans szimbólumok megfelelői>)

- $\mathcal{A}^* \models \Sigma^*$. Emiatt Σ véges részeinek van modellje, a kompaktsági tétel 2. alakja miatt Σ -nak van modellje (és ez $\mathcal{A}'$) $\Rightarrow |A'| \geq |I| > |A|$, ezért $A \rightarrow A'$ bijekció közöttük nem lehet, így $\mathcal{A}' \not\cong \mathcal{A}$.

De $\mathcal{A}' \models \Sigma$ miatt $\mathcal{A} \equiv_e \mathcal{A}'$.

KÉSZ

November 16.:

Def: Legyen $A = \langle A, R_i^A, f_j^A, c_k^A \rangle, i \in I, j \in J, k \in K$,

legyen $B = \langle B, R_i^B, f_j^B, c_k^B \rangle$

$A \cong B$, ha van $\varphi: A \rightarrow B$, hogy:

(a) φ bijekció

(b) $(\forall a_1, a_2, \dots, a_n \in A)(\forall i \in I) (a_1, \dots, a_n) \in R_i^A \Leftrightarrow (\varphi(a_1), \dots, \varphi(a_n)) \in R_i^B$

(c) $(\forall a_1, a_2, \dots, a_n \in A)(\forall j \in J) \varphi(f_j^A(a_1, \dots, a_n)) = f_j^B(\varphi(a_1), \dots, \varphi(a_n))$

(d) $(\forall k \in K) \varphi(c_k^A) = c_k^B$

- (a)-(d) teljesítő φ : izomorfizmus.
- ha csak (b),(c),(d) teljesül φ -re, akkor φ : homomorfizmus.

Tétel: (1) $A \cong B \Rightarrow A \equiv_e B$

(1b) ha $\varphi: A \rightarrow B$ szürjektív homomorfizmus, és Ψ -et nem tartalmazó formula, akkor tetszőleges $(a_1, \dots, a_n \in A)$: $A \models \psi[a_1, \dots, a_n]$ pont akkor, ha $B \models \psi[\varphi(a_1), \dots, \varphi(a_n)]$

(2) ha A végtelen, akkor van $A': A \equiv_e A'$, de $A \not\cong A'$

Biz.: (2) volt a múltkor.

(1),(1b) egyszerre: formulaindukcióval belátjuk, hogy tetszőleges Ψ formulára és $k \in A$ feletti értékelésére:

(*) $A \models \psi[k]$ pont akkor, ha $B \models \psi[\varphi \circ k]$ ($\varphi: A \rightarrow B$ izomorfizmus)

- Atomi formulákra (*) definíció szerint igaz:

(1) esetben φ izomorfizmus

(1b) esetben φ szürjektív homomorfizmus

- Tegyük fel, hogy (*) igaz $\psi_1, \dots, \psi_n$ -re

- (*) öröklődik $\neg \psi_1$ -re:

$A \models \neg \psi_1[k]$ pont akkor, ha $A \not\models \psi_1[k]$ indukció miatt pont akkor, ha $B \not\models \psi_1[\varphi \circ k]$ pont akkor, ha $B \models \neg \psi_1[\varphi \circ k]$.

- (*) öröklődik $\psi_1 \wedge \psi_2$ -re:

$A \models \psi_1 \wedge \psi_2[k]$ pont akkor, ha $A \models \psi_1[k]$ és $A \models \psi_2[k]$

Ind. miatt ez ekvivalens: $B \models \psi_1[\varphi \circ k]$ és $B \models \psi_2[\varphi \circ k]$ -el, ami ekvivalens $B \models \psi_1 \wedge \psi_2[\varphi \circ k]$ -el.

- (*) öröklődik $\exists x \psi_1$ -re:

$A \models \exists x \psi_1[k]$ pont akkor, ha van $k' \equiv^x k$: $A \models \psi_1[k']$

Ind. miatt van $k' \equiv^x k$: $B \models \psi_1[\varphi \circ k']$ azaz $B \models \exists x \psi_1[\varphi \circ k]$, mert $k' \equiv^x k$ az (1)

és (1b) esetben is ekvivalens $\varphi \circ k' \equiv \varphi \circ k$ -el.

0.-rendű logikában

Def: Σ formulahalmaz kielégíthetetlen, ha nincs olyan k kiértékelés, melyre $k \models \Sigma$.

Tétel:

(1) ha Σ ellentmondásos, akkor kielégíthetetlen (teljességi tétel miatt visszafelé is igaz)

(2) Ekvivalensek:

(a) $\Sigma \models \varphi$.

(b) $\Sigma \cup \{\neg\varphi\}$ kielégíthetetlen.

Biz: (1): ha Σ ellentmondásos, akkor van α :

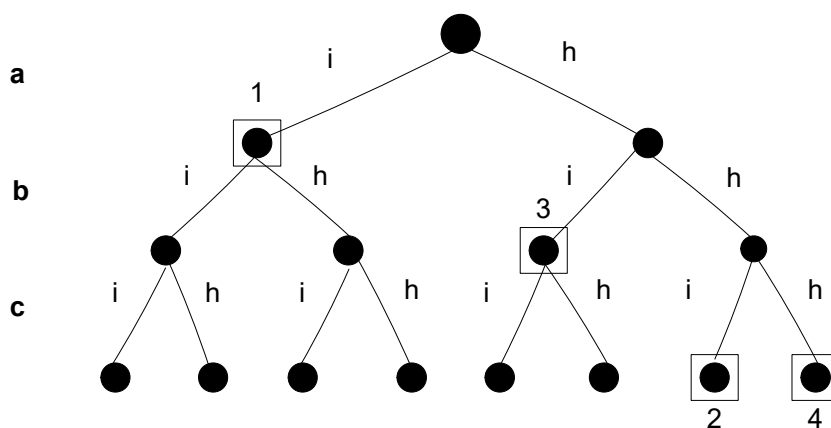
$\Sigma \vdash \alpha$ és $\Sigma \vdash \neg\alpha$. Teljességi tétel miatt $\Sigma \models \alpha$ és $\Sigma \models \neg\alpha$.

- Tegyük fel, hogy van olyan k : $k \models \Sigma$. Ekkor $k \models \alpha$ és $k \models \neg \alpha$. Így ellentmondásra jutottunk.

(2) $\Sigma \models \varphi$ pont akkor, ha $\Sigma \cup \{\neg\varphi\}$ ellentmondásos $\stackrel{(1)}{\Leftrightarrow} \Sigma \cup \{\neg\varphi\}$ kielégíthetetlen.

- Elemi diszjunkció $\sim$ klóz.
- KNF-t azonosítunk a benne szereplő klózok halmazával
- Klózt azonosítunk a benne szereplő atomi formulák és negált atomi formulák halmazával.
- Üres klóz: $\square$. Ez kielégíthetetlen, mert nem érhető el, hogy min. 1 diszjunkciós komponense igazra váljon (mivel nincs diszjunkciós komponense).
- Γ kielégíthetőségének vizsgálatánál feltehető, hogy Γ elemei klózok

Példa: $\{\neg a, a \vee b \vee \neg c, \neg b, c\}$ kielégíthető?



Látható, hogy nem kielégíthető, mivel nincsen olyan gyökér-levél út, amiben nincs $\square$. ($\square$: cáfoló, lezáró csúcsok).

Def: Szemantikus fa: olyan teljes bináris fa, amelynek szintjeit azonosítottuk az ítéletváltozókkal, ágai megfelelnek az interpretációnak.

-Ha C klóz, akkor C illesztése a szemantikus fára:

- Sorra vesszük a szinteket: ha a szinthez tartozó ítélet változó: negátlanul / negálva / ahogy sem szerepel C-ben, ennek megfelelően: jobbra / balra / mindkét irányba megyünk tovább
- Az így elért csúcsok C cáfoló csúcsai.

Def: Szemantikus fa **zárt**, ha minden ágán van cáfoló csúcs.

Tétel: Ekvivalensek:

- (1) Γ kielégíthetetlen
- (2) Γ szemantikus fája zárt

Def: Legyen $c = c_1 \vee L$, $c' = c_1 \vee \neg L$, ahol L és $\neg L$ ellentétesen negált atomi formulák.
 c és c' rezolvense: $c_1 \vee c_1'$

Tétel: Legyen Γ klózhalmoz, c klóz.

$\Gamma \vdash_R c$ (Γ -ból rezolúcióval levezethető c), ha van olyan véges $c_1, \dots, c_n$ klózsorozat, hogy $c_n = c$, és minden i -re $c_i \in \Gamma$, vagy korábbi c_j -k rezolvense.

Tétel: Rezolúciós kalkulus teljessége

Ekvivalensek:

- (1) Γ kielégíthetetlen.
- (2) $\Gamma \vdash_R \square$.

Példa: $\{A \Rightarrow B, B \Rightarrow C\} \models (A \Rightarrow C) ?$
 $\Sigma \qquad \qquad \varphi$

$\Sigma \models \varphi$ pont akkor, ha $\Sigma \cup \{\neg \varphi\}$ kielégíthetetlen (tétel mondja ki).

Γ klóz alakja: $A \Rightarrow B \equiv \neg A \vee B$
 $B \Rightarrow C \equiv \neg B \vee C$
 $\neg(A \Rightarrow C) \equiv \neg(\neg A \vee C) \equiv A \wedge \neg C$

Ennek alapján: $\Gamma = \{\neg A \vee B, \neg B \vee C, A, \neg C\}$

Levezetés:

- (1) $A \qquad \qquad \in \Gamma$
- (2) $\neg A \vee B \qquad \in \Gamma$
- (3) $B \qquad \qquad R(1,2)$
- (4) $\neg B \vee C \qquad \in \Gamma$
- (5) $C \qquad \qquad R(3,4)$
- (6) $\neg C \qquad \qquad \in \Gamma$
- (7) $\square \qquad \qquad R(5,6)$

Tehát Γ kielégíthetetlen, így $\Sigma \models \varphi$.

Biz:

(2) $\Rightarrow$ (1):

Vegyük észre: ha $c = c_1 \cup L$, $c' = c_1 \cup \neg L$, akkor $\{c, c'\} \models c_1 \vee c_2$, mert ha $k \models c, c'$, akkor $k \models c$ két módon lehet: $k \models c_1 \rightarrow k \models c_1 \vee c_1'$

$$k \not\models c_1 \rightarrow k \models L \rightarrow k \not\models \neg L \rightarrow k \models c_1' \rightarrow k \models c_1 \vee c_1'$$

(2) szerint van olyan $c_1, \dots, c_n (= \square)$, hogy mindegyik c_i : $\in \Gamma$ vagy korábbiak rezolvense.

Tegyük fel, hogy van k : $k \models \Gamma$.

„i” szerinti indukcióval belátjuk $k \models c_i$ -t

- $i=1$: $c_1 \in \Gamma$, ezért $k \models c_1$

- $i \rightarrow i+1$: Tegyük fel, hogy ha $j \leq i$, akkor $k \models c_j$.

o ha $c_{i+1} \in \Gamma$, akkor $k \models c_{i+1}$

o ha $c_{i+1} : R(c_j, c_k)$ valamely $j, k \leq i$ -re, akkor indukció miatt $k \models c_j$, $k \models c_k$.

Az észrevétel miatt $k \models c_{i+1}$.

Tehát $k \models c_n = \square$ (ellentmondásra jutottunk).

Másik irány: későbbi előadáson lesz.

Felsőbb matematika informatikusoknak C

2010. november 18.-i Logika előadás

Farkas Péter

2010. december 6.

1. Előző óráról maradt

1.1. Tétel (Rez. kalkulus teljességi tétele). *Ekvivalensek:*

1. Γ kielégíthetetlen.

2. $\Gamma \vdash_R \Box$.

Bizonyítás: (2) $\implies$ (1) előző órán volt.

(1) $\implies$ (2): Ha Γ kielégíthetetlen akkor szemantikus fája zárt. Legyen a zárt szemantikus fában az élek száma n .

Indukció n -re:

Ha $n = 0$ akkor $\Box \in \Gamma$ így $\Gamma \vdash_R \Box$.

Tegyük fel, hogy ha valamely kielégíthetetlen Γ' zárt szemantikus fájában az élek száma $< n$, akkor $\Gamma' \vdash_R \Box$.

1.1. Állítás. Γ szemantikus fájában van olyan csúcs melynek mindkét rákövetkezője cáfoló.

Bizonyítás: Indirekt: Tegyük fel, hogy nincs ilyen csúcs. Legyen a_0 gyökér, ha

a_i adott akkor $\begin{cases} a_i \text{ levél vagy} \\ a_i \text{ valamelyik rákövetkezője nem cáfoló csúcs, ez legyen } a_{i+1}. \end{cases}$

Ekkor az $a_1 \dots a_n$ ágon nincs cáfoló csúcs, ami ellentmond annak, hogy Γ szemantikus fája zárt. $\boxtimes$

Tehát van olyan csúcs melynek mindkét rákövetkezője cáfoló, a rákövetkezők rezolválhatók. Legyen c a rezolvensük.

Legyen $\Gamma' = \Gamma \cup \{c\}$. Γ' zárt szemantikus fájában n -nél kevesebb él van. Az indukció miatt $\Gamma' \vdash_R \Box$, tehát $\Gamma \vdash_R \Box$. $\boxtimes$

2. Elsőrendű rezolúciós kalkulus

Emlékeztető: φ prenex-normálforma, ha $\varphi = Q_1x_1Q_2x_2\ldots Q_nx_n\psi$ ahol Q_i kvantor, ψ kvantor mentes.

2.1. Definíció. φ Skolem normálformájú, ha φ prenex alakú és $Q_1 = Q_2 = \ldots = Q_n = \forall$

2.1. Mese. $\mathcal{A} = \langle A^i, f_i^A, f_j^A, c_k^A \rangle_{\substack{i \in I \\ j \in J \\ k \in K}}$ részstruktúrája
 $\mathcal{B} = \langle B^i, R_i^B, f_j^B, c_k^B \rangle_{\substack{i \in I \\ j \in J \\ k \in K}}$ -nak, ha

$A \subseteq B$ és A -n az $\mathcal{A}$ -beli és $\mathcal{B}$ -beli relációk, függvények, konstansok ugyan úgy hatnak.

2.1. Állítás. Legyen $\mathcal{A}$ részstruktúrája $\mathcal{B}$ -nek. Legyen φ Skolem alakú. Ha $\mathcal{B} \models \varphi$, akkor $\mathcal{A} \models \varphi$ (ha φ -re $\mathcal{A}$ -ban lenne ellenpélda, akkor ez $\mathcal{B}$ -ben is ellenpélda lenne φ -re).

Legyen $\varphi = \exists x(x \cdot x = -1)$, $\mathcal{B}$ = komplex számok teste, $\mathcal{A}$ = valós számok teste. $\mathcal{A}$ részstruktúrája $\mathcal{B}$ -nek, $\mathcal{B} \models \varphi$, de $\mathcal{A} \not\models \varphi$.

Ezért φ egyetlen Skolem-formával sem ekvivalens.

2.1. Tétel. Tetszőleges φ formulához van olyan Skolem formájú φ' , hogy

- φ' esetleg bővebb nyelven van, mint φ .
- $\varphi' \models \varphi$.
- Ha $\mathcal{A} \models \varphi$, akkor van olyan $\mathcal{A}'$, hogy $\mathcal{A}' \models \varphi'$ és φ nyelvén $\mathcal{A}$ és $\mathcal{A}'$ megegyezik.

Bizonyítás: Volt, hogy φ ekvivalens egy prenex formájú formulával (így feltehető φ : prenex).

$$\varphi = Q_1x_1Q_2x_2\ldots Q_nx_n\psi, \text{ ahol } \psi \text{ kvantormentes.}$$

Keressük az első „ $\exists$ ”-t, (ha nincs, akkor φ Skolem alakú.)

$$\varphi = \forall x_1\forall x_2\ldots\forall x_k\exists x_{k+1}\varrho$$

Legyen f új k változós függvény szimbólum és tekintsük a $\varphi^* = \forall x_1\forall x_2\ldots\forall x_k\varrho^*$ formulát, ahol ϱ^* -ot úgy kapjuk, hogy ϱ -ban x_{k+1} szabad előfordulásait $f(x_1, x_2, \ldots, x_k)$ -ra cseréljük.

$\varrho^* : \varrho$ 1-lépéses skolemizáltja.

Világos, hogy $\varrho^* \models \varrho$ (x_{k+1} -t $f(x_1, x_2, \dots, x_k)$ szerint válasszuk). Fordítva, ha $\mathcal{A} \models \varphi$ akkor van k -változós f függvény $\mathcal{A}$ -n, hogy $\langle \mathcal{A}, f \rangle \models \varphi^*$. φ^* -ben a „ $\exists$ ”-ak száma kevesebb, mint φ -ben. Így φ^* Skolem alakú, ha φ -ben l darab „ $\exists$ ” volt. $\square$

2.1. Lemma. *Az algoritmus Skolem formára hozásra:*

1. Hozzuk prenex formára.
2. Az 1-lépéses skolemizálást ismétlegessük, míg van „ $\exists$ ”.

2.1. Példa. *Hozzuk Skolem alakra:*

1. $\exists x_1 \forall x_2 \exists x_3 \forall x_4 \forall x_5 P(x_1, x_2, x_3, x_4, x_5)$
 $\implies$ prenex. Első „ $\exists$ ” x_1 -nél. Legyen c új 0-változós függvény szimbólum (azaz konstans szimbólum).
 $\forall x_2 \exists x_3 \forall x_4 \forall x_5 P(c, x_2, x_3, x_4, x_5)$ Első „ $\exists$ ” x_3 -nál. Legyen f új 1-változós függvény szimbólum.
 $\forall x_2 \forall x_4 \forall x_5 P(c, x_2, f(x_2), x_4, x_5) \implies$ Skolem.
2. $\varphi = \forall x_1 (\exists x_2 P(x_2) \implies \exists x_3 R(x_1, x_2, x_3))$ (nem prenex)
 $\equiv \forall x_1 (\neg(\exists x_2 P(x_2)) \vee \exists x_3 R(x_1, x_2, x_3)) \equiv \forall x_1 (\forall x_2 \neg P(x_2) \vee \exists x_3 R(x_1, x_2, x_3))$
 $(x_2$ -t átnevezve x_4 -é, majd a kvantort kiemelve)
 $\equiv \forall x_1 \forall x_4 (\neg P(x_4) \vee \exists x_3 R(x_1, x_2, x_3)) \equiv \forall x_1 \forall x_4 \exists x_3 (\neg P(x_4) \vee R(x_1, x_2, x_3))$
 $(prenex)$
 $\equiv \forall x_1 \forall x_4 (\neg P(x_4) \vee R(x_1, x_2, f(x_1, x_4)))$ (Skolem)

2.2. Definíció (Herbrand-univerzum). Legyen Γ elsőrendű formulahalmaz. Ha Γ -ban nincs konstans szimbólum akkor hozzáveszünk egyet. (ha van konstans szimbólum, akkor nem veszünk hozzá). Legyen L' az így kapott nyelv. Ekkor Γ Herbrand-univerzuma L' változó mentes term-jei.

2.2. Példa. 1. $L' = c$ konstans szimbólum, $f : 2$ változós függvény szimbólum
Herbrand-univerzum: $c, f(c, c), f(c, f(c, c)), f(f(c, c), c), f(f(c, c), f(c, c)), \dots$

2. c_1, c_2 konstans szimbólum, $f, g : 1$ változós függvény szimbólum
Herbrand-univerzum: $c_1, c_2, f(c_1), f(c_2), g(c_1), g(c_2), f(g(c_1)), g(f(c_2)), \dots$

2.2. Tétel. Legyen Γ Skolem-formulák egy halmaza. Ekvivalensek:

1. Γ -nak van modellje.

2. Γ -nak van olyan modellje melynek alaphalmaza Γ Herbrand-univerzuma.

Bizonyítás: Később. □

2.3. Definíció. Ha $\varphi = \forall x_1 \forall x_2 \dots \forall x_n \psi$ Skolem formájú formula akkor ψ -hez tartozó elsőrendű klózok

- kvantorokat elhagyjuk (hiszen mindegyik „ $\forall$ ”)
- ψ -t KNF-é (Konjunktív normálformává) alakítjuk
- ezután, mint 0 rendben.

2.4. Definíció. Legyen Γ elsőrendű klózok halmaza, A tetszőleges halmaz. $\Gamma(A) = A$ elemeit Γ változóiba az összes lehetséges módon beleírjuk. $\Gamma(A) : \Gamma$ -nak A feletti alappéldányai.

2.3. Tétel (Alaprezolúció teljessége). Legyen Γ elsőrendű klóz halmaz. Ekvivalensek:

1. Γ -nak nincs modellje (azaz Γ kielégíthetetlen).
2. $\Gamma(H) \vdash_R \square$, ahol $H : \Gamma$ Herbrand-univerzuma.

Bizonyítás: (1) $\iff$ Γ -nak nincs olyan modellje aminek Γ Herbrand-univerzuma az alaphalmaza $\iff$ $\Gamma(H) \vdash_R \square$. Az utolsó ekvivalencia az alábbi tételből adódik. □

2.4. Tétel. Ekvivalensek:

1. Γ -nak A -n nincs modellje.
2. $\Gamma(A) \vdash_R \square$.

Bizonyítás: Később. □

2.3. Példa. Elsőrendű rezolúcióra

1. Minden kutyának van gazdája. ($k(x) : x$ kutya, $G(x, y) : x$ gazdája y -nak)
2. Bodri egy kutya.
3. Tehát Bodrinak is van gazdája.

Legyen:

- $\varphi_1 = \forall x(k(x) \Rightarrow \exists y G(y, x))$
- $\varphi_2 = k(Bodri)$
- $\varphi_3 = \exists x G(x, Bodri)$
- $\Sigma = \{\varphi_1, \varphi_2\}$

Kérdés: $\Sigma \models \varphi_3$ igaz-e, azaz $\Gamma = \Sigma \cup \{\neg \varphi_3\}$ kielégíthetetlen-e?

Hozzuk Skolem alakra:

- $\varphi_1 \equiv \forall x(\neg k(x) \vee \exists y G(y, x)) \equiv \forall x \exists y(\neg k(x) \vee G(y, x))$ (*prenex*) $\equiv \forall x(\neg k(x) \vee G(f(x), x))$ (*Skolem*)
- $\varphi_2 = k(Bodri)$ (*Skolem*)
- $\neg \varphi_3 = \neg \exists x G(x, Bodri) \equiv \forall x(\neg G(x, Bodri))$ (*Skolem*)

Klózok:

1. $\neg k(x) \vee G(f(x), x)$
2. $k(Bodri)$
3. $\neg G(x, Bodri)$

Herbrand-univerzum: $Bodri, f(Bodri), f(f(Bodri)), f(f(f(Bodri))), \dots$

1. $\neg k(Bodri) \vee G(f(Bodri), Bodri)$ (*felt. 1*)
2. $k(Bodri)$ (*felt. 2.*)
3. $G(f(Bodri), Bodri)$ (*Rezolúció(1,2)*)
4. $\neg G(f(Bodri), Bodri)$ (*felt. 3*)
5. $\square$ (*Rezolúció(3,4)*)

Tehát $\Sigma \models \varphi_3$.

Matematikai logika

9. előadás

2010. november 23.

1. Előző óráról maradt

1.1. Tétel:

Legyen Γ Skolemformulák halmaza. A következő állítások ekvivalensek:

- (1) Γ -nak van modellje (azaz létezik $\mathcal{A}$, hogy $\mathcal{A} \models \Gamma$).
- (2) Γ -nak van olyan modellje, melynek Γ Herbrand-univerzuma az alaphalmaza.

Bizonyítás:

(2) $\Rightarrow$ (1): Triviális.

(1) $\Rightarrow$ (2): Tegyük fel, hogy $\mathcal{A} \models \Gamma$.

Legyen $A_0 = \{ \Gamma\text{-beli konstansok } \mathcal{A}\text{-beli jelentése} - \text{ha } \Gamma\text{-ban nincs konstans, akkor tegyük } A_0\text{-ba } \mathcal{A} \text{ egy tetszőleges elemét} \}$.

Ha A_n adott, akkor legyen $A_{n+1} = A_n \cup \{ f^{\mathcal{A}}(a_0 \dots a_{k-1}) : a_0 \dots a_{k-1} \in A_n, f \text{ k változós függvényszimbólum } \Gamma \text{ nyelvében} \}$.

Legyen $B = \bigcup_{n \in \mathbb{N}} A_n$. Ekkor B zárt az $\mathcal{A}$ -beli műveletekre: ha f k változós függvényszimbólum Γ nyelvében és $a_0 \dots a_{k-1} \in B \Rightarrow \exists i_0 \dots i_{k-1} : a_0 \in A_{i_0}, a_1 \in A_{i_1}, \dots, a_{k-1} \in A_{i_{k-1}}$.

Legyen $j = \max\{i_0 \dots i_{k-1}\}$. Ekkor $a_0 \dots a_{k-1} \in A_j \Rightarrow f^{\mathcal{A}}(a_0 \dots a_{k-1}) \in A_{j+1} \subseteq B$.

Legyen $\mathcal{B}$ az a részstruktúra $\mathcal{A}$ -ban, amelynek B az alaphalmaza. Ekkor $\mathcal{B} \models \Gamma$ (a nov. 18-i mese miatt univerzális (Skolem)formulák igazsága részstruktúrákra öröklődik).

Legyen H Γ Herbrand-univerzuma, legyen: $\varphi: H \rightarrow \mathcal{B}$,

$$\varphi(t) = \begin{cases} c^{\mathcal{A}}, & \text{ha } t = c \text{ konstans szimbólum} \\ f^{\mathcal{A}}(\varphi(t_1) \dots \varphi(t_n)), & \text{ha } t = f(t_1 \dots t_n) \end{cases}$$

Ha R n változós relációs szimbólum Γ nyelvében, akkor legyen $R^{\mathcal{B}} = \{ \langle t_1 \dots t_n \rangle \in H^n : (\varphi(t_1) \dots \varphi(t_n)) \in R^{\mathcal{A}} \}$. Ekkor $\varphi: \langle H, f_i, R_j, c_k \rangle \xrightarrow{i \in I, j \in J, k \in K} \mathcal{B}$ szürjektív homomorfizmus (szürjektív, mert $\mathcal{B}$ -re képez, és homomorfizmus, mert φ -t így csináltuk).

Legyen $\alpha \in \Gamma$ tetszőleges.

Állítás:

$$\langle H, f_i, R_j, c_k \rangle \models_{i \in I, j \in J, k \in K} \alpha.$$

Bizonyítás:

Indirekt: tegyük fel, hogy $\langle H, f_i, R_j, c_k \rangle \models_{i \in I, j \in J, k \in K} \neg \alpha$. A nov. 16-i (1b) állítás miatt ekkor $\mathcal{B} \models \neg \alpha$, ami ellentmondás, tehát az állítás igaz.

Ezért $\langle H, f_i, R_j, c_k \rangle \models_{i \in I, j \in J, k \in K} \Gamma$. ■

Megjegyzés:

1-rendű rezolúcióban mindig egyenlőségmentes nyelveket nézünk.

1.2. Tétel:

Legyen Γ 1-rendű klózhalmaz. A következő állítások ekvivalensek:

(1) Γ -nak nincs A alaphalmazú modellje.

(2) $\Gamma(A) \vdash_R \square$.

Bizonyítás:

(2) $\Rightarrow$ (1): Indirekt: tegyük fel, hogy Γ -nak A modellje, de $\Gamma(A) \vdash_R \square$.

Legyen:

$$I(R(a_1 \dots a_n)) = \begin{cases} i, & \text{ha } (a_1 \dots a_n) \in R^{\mathcal{A}} \\ k & \text{különben} \end{cases}$$

$(R(a_1 \dots a_n))$: ítéletváltozó; R : relációszimboldum; $a_1 \dots a_n \in A$.

$I \models \Gamma(A)$, ezért $I \models \square$, mert a rezolúciós kalkulus teljes. Ezzel ellentmondásra jutottunk.

(1) $\Rightarrow$ (2): Γ -nak nincs A alaphalmazú modellje $\stackrel{(*)}{\Rightarrow} \Gamma(A)$ kielégíthetetlen. A rezolúció teljessége miatt $\Gamma(A) \vdash_R \square$.

(*) részletesebben: ha $\Gamma(A)$ -t kielégítené egy I interpretáció, akkor legyen $R^{\mathcal{A}} = \{(a_1 \dots a_n) \in A^n : I \models R(a_1 \dots a_n)\}$. Ekkor $\mathcal{A} = \langle A, R^{\mathcal{A}}, \dots \rangle$ modellje lenne Γ -nak. ■

Megjegyzések:

1) Alaprezolúciónál 0-rendű rezolúciót használunk 1-rendű klózhalmazra. Most az ítéletváltozók neveinek van szerkezete, pl. $R(f(a, b), a)$ 1 db ítéletváltozó. Az ítéletváltozók akkor rezolválhatók, ha karakterről karakterre megegyeznek, pl.:

- $R(a, b)$ és $\neg R(f(a), b)$ nem rezolválható,
- $R(a, g(b))$ és $\neg R(a, g(b))$ rezolválható.

2) Alaprezolúción kívül vannak más rezolúciós módszerek is, melyek 1-rendben alkalmazhatók.

2. Feladatok

2.1. Példa:

a) Formalizáljuk elsőrendű nyelven az alábbi mondatokat:

1. Van olyan autó, amely minden biciklinél gyorsabb.
2. Ha egy autó gyorsabb egy biciklinél, akkor drágább is nála.
3. Minden biciklinél van drágább autó.

$A(x)$: x autó

$B(x)$: x bicikli

$G(x,y)$: x gyorsabb y -nél

$D(x,y)$: x drágább y -nél

$$1. \exists x (A(x) \wedge \forall y (B(y) \Rightarrow G(x,y)))$$

$$2. \forall x \forall y ((A(x) \wedge B(y) \wedge G(x,y)) \Rightarrow D(x,y))$$

$$3. \forall x (B(x) \Rightarrow \exists y (A(y) \wedge D(y,x)))$$

4. Alaprezolúcióval lássuk be, hogy $\{1,2.\} \models 3.$:

- Skolem normálformára hozás:

$$1. \equiv \exists x (A(x) \wedge \forall y (\neg B(y) \vee G(x,y)))$$

$$\equiv \exists x \forall y (A(x) \wedge (\neg B(y) \vee G(x,y)))$$

$$\equiv \forall y (A(c) \wedge (\neg B(y) \vee G(c,y))) \text{ Skolem}$$

$$2. \equiv \forall x \forall y (\neg A(x) \vee \neg B(y) \vee \neg G(x,y) \vee D(x,y)) \text{ Skolem}$$

$$\neg 3. \equiv \neg (\forall x (\neg B(x) \vee \exists y (A(y) \wedge D(y,x))))$$

$$\equiv \exists x (B(x) \wedge \forall y (\neg A(y) \vee \neg D(y,x)))$$

$$\begin{aligned} &\equiv \exists x \forall y (B(x) \wedge (\neg A(y) \vee \neg D(y, x))) \\ &\equiv \forall y (B(d) \wedge (\neg A(y) \vee \neg D(y, d))) \text{ Skolem} \end{aligned}$$

- Elsőrendű klózalmaz megadása:

$$\Gamma = \left\{ \begin{array}{c} A(c) \\ \neg B(y) \vee G(c, y) \\ \neg A(x) \vee \neg B(y) \vee \neg G(x, y) \vee D(x, y) \\ B(d) \\ \neg A(y) \vee \neg D(y, d) \end{array} \right\}$$

- Herbrand-univerzum megadása:

$$H = \{c, d\}$$

- Rezolúció:

1. $\neg A(c) \vee \neg B(d) \vee \neg G(c, d) \vee D(c, d)$	felt.
2. $A(c)$	felt.
3. $\neg B(d) \vee \neg G(c, d) \vee D(c, d)$	R(1,2)
4. $B(d)$	felt.
5. $\neg G(c, d) \vee D(c, d)$	R(3,4)
6. $\neg B(d) \vee G(c, d)$	felt.
7. $D(c, d) \vee \neg B(d)$	R(5,6)
8. $\neg A(c) \vee \neg D(c, d)$	felt.
9. $\neg B(d) \vee \neg A(c)$	R(7,8)
10. $\neg A(c)$	R(4,9)
11. $\square$	R(2,10)

2.2. Példa:

Teljességi tétel felhasználása nélkül igazoljuk a következő állítást: ha $\Sigma \cup \{\alpha\} \vdash \beta$ és $\Sigma \cup \{\neg\alpha\} \vdash \beta$, akkor $\Sigma \vdash \beta$.

Biz.:

- $\Sigma \cup \{\alpha\} \vdash \beta$ pont akkor, ha $\Sigma \cup \{\alpha, \neg\beta\}$ ellentmondásos pont akkor, ha $\Sigma \cup \{\neg\beta\} \vdash \neg\alpha$.

- $\Sigma \cup \{\neg\alpha\} \vdash \beta$ pont akkor, ha $\Sigma \cup \{\neg\alpha, \neg\beta\}$ ellentmondásos pont akkor, ha $\Sigma \cup \{\neg\beta\} \vdash \alpha$.
 $\Sigma \cup \{\neg\beta\}$ így ellentmondásos, tehát $\Sigma \vdash \beta$.

2.3. Példa:

Adjuk meg az alábbi formula egy modelljét: $\varphi = \forall x \forall y \exists z (R(x, z) \wedge R(z, y))$.

1. megoldás: $A = \{0\}$,

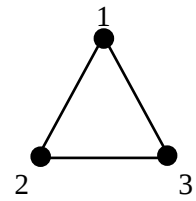
$$R(x, y) \Leftrightarrow x = y,$$

$$\mathcal{A} = \langle A, = \rangle \models \varphi.$$

2. megoldás: $A = \{1, 2, 3\}$ (egy konkrét gráf csúcsai),

$$R(x, y) \Leftrightarrow \text{él megy az ábra szerint } x \text{ és } y \text{ között},$$

$$\mathcal{A} = \langle A, R \rangle \models \varphi.$$



Matematikai logika

2010/2011 ősz

11. előadás

Definíció: *nemdeterminisztikus Turing gép*

$T = \langle \Gamma, Q, \delta \rangle$ egy nemdeterminisztikus Turing gép, ha

- Γ : a szalagábécé, egy véges halmaz;
 $*$ $\in \Gamma$, ahol $*$ az üres karakter a szalagon
- Q : az állapotok véges halmaza
 $START, STOP \in Q$ a kezdő és az elfogadó állapot.
- δ : az állapotátmenet-reláció:
 $\delta \subseteq (\Gamma \times Q) \times (\Gamma \times Q \times \{-1, 0, 1\})$ ahol $\{-1, 0, 1\}$: hátra lép, helyben marad, előre lép

Emlékeztető: *L nyelv NP-belisége*

Egy $L \subseteq \Gamma^*$ nyelv NP-beli, ha van olyan nemdeterminisztikus T-gép és $c_1, c_2 \in \mathbb{R}$ ($\in \mathbb{N}$ is lehetne) úgy, hogy tetszőleges $w \in \Gamma^*$ -ra: $w \in L \Leftrightarrow T$ elfogadja w -t legfeljebb $c_1|w|^{c_2}$ lépésben.

Tétel:

Legyen $sat =$ „a kielégíthető konjunktív normál formák halmaza”.
Ekkor sat NP-teljes.

Bizonyítás:

1) sat NP-beli ($sat \in NP$), erre tanú egy interpretáció, ami igazá teszi a kérdéses formulát.

2) Megmutatjuk, hogy sat NP-nehéz, tehát bármely $L \in NP$ nyelv polinom időben redukálható sat -ra.

$L \in NP \Rightarrow$ van $T = \langle \Gamma, Q, \delta \rangle$ nemdeterminisztikus Turing gép és van c_1, c_2 szám, hogy a T Turing-gép $\leq c_1|w|^{c_2}$ lépésben helyes választ ad a $w \in L$ kérdésre, ha tényleg $w \in L$. Rögzítsük $w \in \Gamma^*$ -t, és vezessük be az ítéletváltozók következő rendszerét:

Legyen $N = \lceil c_1|w|^{c_2} \rceil$

Legyen $X[n, p]$	$0 \leq n \leq N, \quad P \in Q'$
Legyen $Y[n, k]$	$0 \leq n \leq N, \quad -N \leq k \leq N'$
Legyen $Z[n, p, k]$	$0 \leq n \leq N, \quad -N \leq p \leq N, \quad k \in \Gamma.$

A szándékolt jelentés:

$X[n, p]:$	az n . lépés után T a p állapotban van,
$Y[n, k]:$	az n . lépés után a gép feje a k . pozíción áll,
$Z[n, p, k]:$	az n . lépés után a szalag p . pozícióján „ k ” szerepel.

Axiomatizáljuk T működését: megadunk egy φ formulát úgy, hogy φ hossza polinom $|w|$ -ben és φ pont akkor elégíthető ki, ha T elfogadja w -t. φ -t az alábbi lépésekkel adjuk meg:

(a) T mindig van valamilyen állapotban:

$$\left(\bigvee_{p \in Q} X[1, p] \right) \wedge \left(\bigvee_{p \in Q} X[2, p] \right) \wedge \cdots \wedge \left(\bigvee_{p \in Q} X[N, p] \right)$$

(b) T csak egy állapotban van:

$$\{\neg X[n, p] \vee \neg X[n, q] : p \neq q \in Q, 0 \leq n \leq N\}.$$

(c) a fej minden lépésben pontosan egy helyen van:

- van valahol
- nincs két helyen

(a) és (b) mintájára elképzelhető

(d) minden mezőn pont egy jel áll:

- áll valamin
- nem áll kettőn

(a) és (b) mintájára elképzelhető

(e) a 0. lépésben a START mezőn áll:

$$X[0, START]$$

az utolsó lépés után a STOP mezőn áll:

$$X[N, STOP]$$

(f) kezdetben $w = w_1 w_2 \dots w_k$ van a szalagon:

$$\{Z[0, i-1, w_i], \text{ ha } 1 \leq i \leq k\} \cup \{Z[0, i-1, *], \text{ ha } i \leq 0 \text{ vagy } i > k\}$$

(g) a gép a δ átmenetreláció szerint működik:

ha $q, q' \in Q, v, v' \in \Gamma, \varepsilon \in \{-1, 0, 1\}, -N \leq p \leq N, (q, v, q', v', \varepsilon) \notin \delta$ akkor:

$$\neg X[n, q] \vee \neg Y[n, p] \vee \neg Z[n, p, v] \vee \neg X[n+1, q'] \vee \neg Y[n+1, p+k] \vee \neg Z[n+1, p, v']$$

(tehát a gép nem tud a (q, v) állapotból a (q', v') -be lépni)

(h) ahol nem áll fej, ott nem változik a szalag tartalma:

$$(Y[n, p] \vee Z[n, p, v] \vee \neg Z[n+1, p, v]) \wedge (Y[n, p] \vee \neg Z[n, p, v] \vee Z[n+1, p, v]) \quad \forall n, p, v$$

Legyen $\varphi = (a) \wedge (b) \wedge \dots \wedge (h)$.

T elfogadja w -t pont akkor, ha φ kielégíthető.

■

Definíció: n -sat

Olyan kielégíthető konjunktív normál formák, melyek elemi diszjunkcióiban legfeljebb n ($n \in \mathbb{N}$) változó fordul elő.

Példa: $(X_1 \vee \neg X_2) \wedge (X_1 \vee X_3 \vee X_{17}) \wedge (X_{15} \vee \neg X_1) \in \mathcal{3}\text{-sat}$

Tétel:

$\mathcal{3}\text{-sat}$ NP teljes.

Bizonyítás:

1) $\mathcal{3}\text{-sat}$ NP-beli ($\in NP$), hiszen a $\mathcal{3}\text{-sat}$ -nál általánosabb sat is NP-beli.

2) Elég bebizonyítani, hogy az NP-teljes sat redukálható $\mathcal{3}\text{-sat}$ -ra. A konstrukció: legyen φ tetszőleges konjunktív normál forma:

$$\varphi = (X_1 \vee \dots \vee X_k) \wedge (\dots \vee \dots) \wedge (\dots \vee \dots)$$

A $(X_1 \vee \dots \vee X_k)$ tagon bemutatjuk, az átalakítást (a többi tagon ugyanígy történik).

Ötlet:

$$\begin{array}{lll} Y_1 = X_1 & \longleftrightarrow & Y_1 \Leftrightarrow X_1 \\ Y_2 = Y_1 \vee X_2 & \longleftrightarrow & Y_2 \Leftrightarrow Y_1 \vee X_2 \\ Y_3 = Y_2 \vee X_3 & \longleftrightarrow & Y_3 \Leftrightarrow Y_2 \vee X_3 \\ & \vdots & \end{array}$$

Megvalósítás: Cseréljük ki φ diszjunkciós komponenseit a következő módon (csak az első komponensre mutatjuk):

$$Y_1 \Leftrightarrow X_1 \quad \longleftrightarrow \quad (\neg Y_1 \vee X_1) \wedge (\neg X_1 \vee Y_1) \quad (1)$$

$$Y_2 \Leftrightarrow Y_1 \vee X_2 \quad \longleftrightarrow \quad (\neg Y_2 \vee Y_1 \vee X_2) \wedge (Y_2 \vee \neg Y_1) \wedge (Y_2 \vee \neg X_2) \quad (2)$$

$$\vdots$$

Legyen $\varphi' = (1) \wedge (2) \wedge \dots$

Ekkor $\varphi = \varphi'$ egyszerre elégíthető ki.

φ' polinomiális időben (sőt, lineáris időben) kiszámítható φ -ből.

■

Megjegyzés: *2-sat* P-beli; bizonyítás legközelebb.

2-SAT és véletlen gráfok

Bankó Tibor

2011. január 11.

1. 2-SAT P -beli

Jelöljük az irányított utat a $\rightsquigarrow$ szimbólummal!

1. Definíció. Legyen G irányított gráf és legyen $a, b \in V(G)$ csúcsok. Azt mondjuk, hogy $a \sim b$, ha $a \rightsquigarrow b$ és $b \rightsquigarrow a$.

1. Tétel. $A \sim$ ekvivalencia reláció. Az ekvivalencia osztályok a gráf erősen összefüggő komponensei.

2. Definíció. Legyen φ olyan KNF, melyben a diszjunkciós komponensek ≤ 2 változót tartalmaznak. Ekkor megadható egy gráf (amit G_φ -vel jelölünk) φ -hez:

- a csúcsok: φ változói és ezek negáltjai.
- az élek a következő módon vannak definiálva:
 - Ha $x \vee y$ elemi diszjunkció φ -ben, akkor fel kell venni a $\neg x \rightarrow y, \neg y \rightarrow x$ éleket.
 - Ha $\neg x \vee y$ elemi diszjunkció φ -ben, akkor fel kell venni az $x \rightarrow y, \neg y \rightarrow \neg x$ éleket.
 - Ha $x \vee \neg y$ elemi diszjunkció φ -ben, akkor fel kell venni a $\neg x \rightarrow \neg y, y \rightarrow x$ éleket.
 - Ha $\neg x \vee \neg y$ elemi diszjunkció φ -ben, akkor fel kell venni az $x \rightarrow \neg y, y \rightarrow \neg x$ éleket.

2. Tétel. Ekvivalensek.

(1) φ kielégíthető.

(2) G_φ egyetlen összefüggő komponense sem tartalmaz változót és negáltját egyszerre.

Bizonyítás. (1) $\Rightarrow$ (2) Legyen k olyan értékelés, hogy $k \models \varphi$.

- ha $k \models x$, akkor az x -ből induló utakon szereplő csúcsoknak is igaznak kell lennie k -ban, mert különben az elemi diszjunkcióknak megfelelő implikációk nem lennének igazak (a KNF miatt minden ilyennek igaznak kell lennie).
- ha $k \not\models x$, akkor az előző pontban leírtak miatt az x -be bejövő utakon szereplő csúcsoknak is hamisnak kell lennie k -ban.

Így (2) már következik, mert változó és negáltja nem veheti fel ugyanazt az értéket, szóval nem lehetnek egy úton.

(2) $\Rightarrow$ (1)

(2) miatt x és $\neg x$ között legfeljebb az egyik irányban van út. Ha egyetlen irányban sincs, akkor fel kell venni egy új $x \rightarrow \neg x$ élet. Így elérhető, hogy minden x -re pontosan egy irányba legyen út x és $\neg x$ között. Legyen az így kapott gráf G'_φ és legyen

$$k(x) = \begin{cases} igaz & \text{ha van } \neg x \rightsquigarrow x \text{ út,} \\ hamis & \text{különben.} \end{cases}$$

Megmutatjuk, hogy az így kapott k esetén $k \models \varphi$.

Ehhez indirekt módon tegyük fel, hogy k egy φ -beli $x \vee y$ diszjunkciós komponens nem elégíti ki. Tehát $k \not\models x$ és $k \not\models y$, vagyis x és y is hamis. Ekkor k konstrukciója miatt G'_φ -ben léteznie kell $x \rightsquigarrow \neg x$ és $y \rightsquigarrow \neg y$ utaknak valamint a $x \vee y$ diszjunkciós komponens miatt $\neg x \rightarrow y$, $\neg y \rightarrow x$ élek. Ekkor $\neg x \rightsquigarrow x$ út is létezik, ami ellentmondás. $\square$

3. Tétel. A 2-SAT P -ben van.

Bizonyítás. Az előző tétel alapján látható, hogy elegendő G_φ előállítását és az erősen összefüggő komponenseinek megkeresését, tesztelését. Mindkettő megy polinom idő alatt. $\square$

2. Véletlen gráfok

3. Definíció. A gráfok nyelvének szokásos jelölését használva megadjuk a T_R formulahalmazt. Legyen

$$T_R = \{\forall x \neg E(x, x), \forall x \forall y (E(x, y) \Rightarrow E(y, x))\} \cup \{\varphi_{n,m} : n, m \in \mathbb{N}\}, \text{ ahol}$$

$$\varphi_{n,m} = \forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_m \exists z \{x_1, \dots, x_n, y_1, \dots, y_m \text{ páronként különböző} \wedge \wedge (\wedge_{i=1}^n E(x_i, z)) \wedge (\wedge_{i=1}^m \neg E(y_i, z))\}$$

4. Tétel. T_R -nek van modellje.

Bizonyítás. (I)

5. segédtétel. Ha G véges gráf, akkor van véges G' gráf úgy, hogy G feszített része G' -nek és ha $X, Y \subseteq V(G), X \cap Y = \emptyset$, akkor van $z \in V(G')$, hogy minden $a \in X, b \in Y : E(a, z), \neg E(b, z)$.

Bizonyítás. G -nek minden páronként csúcsdiszjunkt részhalmaz-párjához fel kell venni 1 új csúcsot, amit a megfelelő módon össze kell kötni a pontjaikkal. $\square$

Legyen $V_1 = \{\emptyset\}, E_1 = \emptyset, G_1 = \langle V_1, E_1 \rangle$.

Ekkor megadhatjuk gráfok sorozatát, az előző segédtétel alapján, oly módon, hogy $G_{n+1} = G'_n$ legyen.

Végül legyen $V^* = \cup_{n \in \mathbb{N}} V_n, E^* = \cup_{n \in \mathbb{N}} E_n, G^* = \langle V^*, E^* \rangle$.

Megmutatjuk, hogy G^* jó, vagyis $G^* \models T_R$.

Ugyanis tetszőleges $X, Y \subset V^*$ véges részhalmazra, ahol $X \cap Y = \emptyset$, a konstrukcióból adódóan van olyan n , hogy $X, Y \subseteq V_n$, így V_{n+1} -ben van olyan z , amire:

$$\forall x \in X E(x, z) \text{ és } \forall y \in Y \neg E(y, z).$$

$\square$

Bizonyítás. (II)

Legyen $V = \mathbb{N}$ ha $i, j \in \mathbb{N}, i \neq j$, akkor legyen $i^* = \min(i, j), j^* = \max(i, j)$

és legyen (i, j) él, ha j^* bináris alakjában az i^* helyen 1 áll (a pozíciókat 0-tól számozzuk). Látható, hogy ha (i, j) él, akkor (j, i) is él.

Például: a $(2, 6)$ él, mert $6 = 110$ a kettes számrendszerben, és a 2. helyen 1 áll.

Az így elkészített $G\langle V, E \rangle$ gráf modellje T_R -nek, mert tetszőleges $X, Y \subset \mathbb{N}$, $X \cap Y = \emptyset$ esetén legyen $Y > X$. Ekkor van z , hogy minden X -beli elemmel és egyetlen Y -beli sincs összekötve. Ilyen z -t például úgy kaphatunk, hogy a bináris alakjában minden X -beli pozícióba 1-t írunk, míg minden Y -beli pozícióba 0-t.

□

4. Definíció. k csúcsú véletlen gráf:

Olyan gráf, melynek k pontja van és a csúcspárok között egymástól függetlenül $\frac{1}{2}$ valószínűséggel kerülnek behúzásra az élek.

6. tétel. Legyen G_k egy k csúcsú véletlen gráf. Ha n, m rögzített, akkor $\lim_{k \rightarrow \infty} P(G_k \models \varphi_{n,m}) = 1$.

Bizonyítás. Az ellentett esemény valószínűségét vizsgáljuk meg.

$$P(G_k \not\models \varphi_{n,m}) \leq \binom{k}{n} \binom{k-n}{m} \left(1 - \frac{1}{2^{n+m}}\right)^{k-(m+n)} \leq k^{m+n} \left(1 - \frac{1}{2^{n+m}}\right)^{-(n+m)} \left(1 - \frac{1}{2^{n+m}}\right)^k$$

Az első egyenlőtlenség abból adódik, hogy így egy olyan gráfot, mely nem modellje $\varphi_{n,m}$ -nek, esetleg többször is leszámolunk. A harmadik tényezője azt fejezi ki, hogy a kiválasztott n és m pontokon kívüli minden pontja "rossz" kell, hogy legyen. A második egyenlőtlenség végén kapott szorzat első tényezője k polinomja, a második k -ban konstans, míg a harmadik k -nak egy exponenciális függvénye, egynél kisebb alappal. Így igaz, hogy:

$$\lim_{k \rightarrow \infty} P(G_k \not\models \varphi_{n,m}) = 0.$$

□

Matematikai logika

13. előadás

2010. december 7.

13.1. Definíció:

Legyen T elmélet (formulahalmaz), legyen κ számosság. T κ -kategorikus, ha teljesül a következő: ha $\mathcal{A}, \mathcal{B} \models T$ és $|\mathcal{A}| = |\mathcal{B}| = \kappa$, akkor $\mathcal{A} \cong \mathcal{B}$. (Azaz izomorfia erejéig T -nek 1 db κ számosságú modellje van.)

13.1. Tétel:

T_R $\aleph_0$ -kategorikus.

Bizonyítás:

Legyen $\mathcal{A}, \mathcal{B} \models T_R$ és $|\mathcal{A}| = |\mathcal{B}| = \aleph_0$.

Ekkor $\mathcal{A} = \{a_n : n \in \mathbb{N}\}$ és $\mathcal{B} = \{b_n : n \in \mathbb{N}\}$, mert $\mathcal{A}, \mathcal{B}$ megszámlálható.

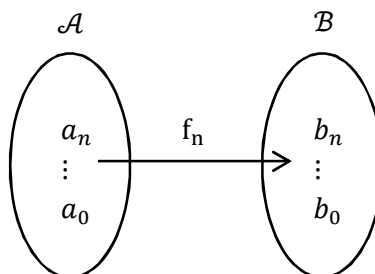
Minden n -re: megadunk egy f_n függvényt úgy, hogy:

- (1) $n < m \Rightarrow f_n \leq f_m$
- (2) $D(f_n)$ véges
- (3) $\{a_1 \dots a_{n-1}\} \subseteq D(f_n)$ és $\{b_1 \dots b_{n-1}\} \subseteq R(f_n)$
- (4) f_n izomorfizmus $D(f_n)$ és $R(f_n)$ között.

(Jelölés: D : értelmezési tartomány, R : értékkészlet)

Legyen $f_0 = \emptyset$ és feltesszük, hogy f_n adott.

- Ha $a_n \in D(f_n)$, akkor:
legyen $g = f_n$.
- Ha $a_n \notin D(f_n)$, akkor:
legyen $X = \{f_n(a) : (a, a_n) \in E(\mathcal{A}), a \in D(f_n)\}$ és $Y = \{f_n(a) : (a, a_n) \notin E(\mathcal{A}), a \in D(f_n)\}$.
(Jelölés: E : él)



$\mathcal{B} \models T_R$ miatt van $b \in \mathcal{B}$, hogy b össze van kötve X elemeivel, és nincs összekötve Y elemeivel.

Legyen $g = f_n \cup \{(a, b)\}$.

Mindkét esetben g olyan véges függvény, ami izomorfizmus értelmezési tartománya és értékkészlete között, egyúttal f -nek egy olyan kiterjesztése, ami a_n -t b -re képezi le.

Az így kapott g inverze kiterjeszthető úgy, hogy g^{-1} értelmezve legyen b_n -re. Ez a kiterjesztés legyen f_{n+1} . Végül legyen $f = \bigcup_{n \in \mathbb{N}} f_n$.

Ekkor f_0 -ra alkalmazva az előbbi kiterjesztést egy izomorfizmust kapunk $\mathcal{A}$ és $\mathcal{B}$ között. ■

13.2. Tétel: (Łoś (ejtsd: [ˈwɔɕ])–Vaught-teszt)

Ha T $\aleph_0$ -kategorikus elmélet egy megszámlálható nyelven, akkor T teljes.

Bizonyítás:

Indirekt: tegyük fel, hogy φ olyan formula, hogy $T \models \varphi$ és $T \not\models \neg\varphi$. Ekkor:

- Létezik $\mathcal{A}$, hogy $\mathcal{A} \models T$ és $\mathcal{A} \models \neg\varphi$.

$TH(\mathcal{A})$ megszámlálható és ellentmondástalan.

A nov. 11-i előadás c) pontjához tartozó megjegyzés miatt létezik megszámlálható $\mathcal{A}'$, hogy $\mathcal{A}' \models T$ és $\mathcal{A}' \models \neg\varphi$.

- Létezik $\mathcal{B}$, hogy $\mathcal{B} \models T$ és $\mathcal{B} \models \varphi$.

Az előzőhöz hasonlóan: létezik megszámlálható $\mathcal{B}'$, hogy $\mathcal{B}' \models T$ és $\mathcal{B}' \models \varphi$.

Mivel $\mathcal{A}'$ és $\mathcal{B}'$ megszámlálható modellek, ezért a kategoricitás miatt $\mathcal{A}' \cong \mathcal{B}'$ (lásd: nov. 16-i előadás 1. pontja). Ez ellentmondásra vezetett, tehát T teljes. ■

Következmény:

T_R teljes.

13.3. Tétel: (0–1 törvény)

Legyen φ a gráfelmélet tetszőleges formulája. Ekkor $\lim_{k \rightarrow \infty} P(G_k \models \varphi) \in \{0,1\}$. (Azaz annak a valószínűsége, hogy a k csúcsú G gráfon φ igaz, $k \rightarrow \infty$ esetén vagy 0, vagy 1.)

Bizonyítás:

Legyen $\mathcal{A} \models T_R$ megszámlálható modell.

Elég megmutatni, hogy ha $\mathcal{A} \models \varphi$, akkor $\lim_{k \rightarrow \infty} P(G_k \models \varphi) = 1$.

Tegyük fel, hogy $\mathcal{A} \models \varphi$. A tétel előtti következmény miatt T_R teljes, tehát $T_R \models \varphi$. A kompaktsági tétel miatt van véges $\Gamma = \{\varphi_{n_1 n_1} \dots \varphi_{n_l n_l}\} \subseteq T_R$, hogy $\Gamma \models \varphi$. Ekkor:

$$P(G_k \models \varphi) \geq P(G_k \models \Gamma) = 1 - P(G_k \not\models \Gamma) \geq 1 - \left(P(G_k \not\models \varphi_{n_1 n_1}) + \dots + P(G_k \not\models \varphi_{n_l n_l}) \right) \xrightarrow{k \rightarrow \infty} 1,$$

mert a zárójelben lévő tagok külön-külön 0-hoz tartanak. ■

Megjegyzés:

A 0–1 törvény nem igaz, ha a nyelv tartalmaz függvénszimbólumot. Például:

Legyen $\varphi = \forall x (x \neq f(x))$, legyen $\mathcal{A}_k$ a k elemű véletlen struktúra. Ekkor:

$$P(G_k \models \varphi) = \frac{(k-1)^k}{k^k} = \left(\frac{k-1}{k} \right)^k \xrightarrow{k \rightarrow \infty} e^{-1}.$$

Kitekintés

- További vizsgálati irányok:
 - rezolúciós stratégiák,
 - más automatikus tételbizonyító módszerek,
 - adatbázisok elmélete.
- Klasszikus logika:
 - bizonyításelmélet

13.4. Tétel: (Gödel nemteljességi tétele)

Legyen $\mathcal{N} = \langle \mathbb{N}, +, \cdot, 0, \leq, = \rangle$ (a természetes számok struktúrája).

Ha $\Gamma \subseteq \text{TH}(\mathcal{N})$ rekurzív halmaz, akkor Γ nem teljes (és ezért még kevésbé kategorikus).

Következmény:

$\text{TH}(\mathcal{N})$ részhalmazaira a következő 3 tulajdonság nem teljesülhet egyszerre, csak legfeljebb bármelyik 2 ezek közül: ellentmondástalan, teljes, rekurzív.

- modellelmélet
 - axiomatizálhatóság,
 - definiálhatóság,
 - véges modellelmélet (klasszikus kérdések véges modellekre).

13.5. Tétel: (Morley tétele)

A következő állítások ekvivalensek:

- (1) T elmélet $\aleph_1$ -kategorikus.
- (2) T elmélet κ -kategorikus minden $\kappa \geq \aleph_1$ -re.

- Végül:
 - más logikák (2-rendű logika, időlogikák, programlogikák,...)

„Végtelen sok logika van, de ez egy véges kurzus, úgyhogy vége.”