Logika és informatikai alkalmazśai[1]

Fülöp Zoltán

Szegedi Tudományegyetem
Természettudományi Kar
Számítástudomány Alapjai Tanszék

2005. május 4.

[1] Fejlesztés alatt. Letölthető a `www.inf.u-szeged.hu/~fulop/logika/szab3.ps` és `www.inf.u-szeged.hu/~fulop/logika/szab3.pdf` címről.

Előszó

Ez jegyzet az SZTE Informatikai Tanszékcsoportnál tartott Logika és informatikai alkalmazásai (korábban Logika a számítástudományban) c. kurzusom anyagát tartalmazza. Megértéséhez csak diszkrét matematikai ismeretekre van szükség.

Fel szeretném hívni az olvasó figyelmét, hogy a jegyzet még nem teljes, fejlesztés alatt lévő változat, ezért elképzelhető, hogy kisebb hibákat, hiányosságokat tartalmaz.

Ezúton fejezem ki köszönetemet azoknak a hallgatóknak, akik észrevételeikkel hozzájárultak a fent említett hiányosságok számának csökkentéséhez.

Fülöp Zoltán

Tartalomjegyzék

1. Ítéletkalkulus

1.1. Alapfogalmak

A formula fogalma

Az ítéletkalkulus formulái szimbólumokból és ítéletváltozókból (vagy röviden csak változókból) épülnek fel. Ezek a következők.

Ítéletváltozók: $p_1, p_2, \ldots$

Logikai szimbólumok: $\neg, \vee, \wedge$

Elválasztó szimbólumok: (és)

A rövidség kedvéért használni fogjuk a $Var = \{p_1, p_2, \ldots\}$ jelölést.

1.1. Definíció. Az ítéletkalkulusbeli formulák halmazán a legszűkebb olyan FRM halmazt értjük, melyre teljesülnek az alábbi feltételek.

(i) Minden $i \geq 1$-re $p_i \in FRM$.

(ii) Ha $F, G \in FRM$, akkor $\neg F, (F \vee G), (F \wedge G) \in FRM$. □

A formulákban szereplő legkülső zárójelpárt általában elhagyjuk. Továbbá, $F \to G$ jelöli majd az $\neg F \vee G$ alakú formulákat és $F \leftrightarrow G$ pedig az $(F \to G) \wedge (G \to F)$ alakú formulákat.

Az összes formulák halmazát $Form$-mal fogjuk jelölni.

Amennyiben az F és G formulákra teljesül, hogy $F = G_1 G G_2$, valamely G_1 és G_2 alkalmas szavakra akkor azt mondjuk, hogy a G az F részformulája. (A G_1 és G_2 általában nem formulák.) Egy részformula többször is előfordulhat ugyanabban a formulában.

A részformula speciális esete a közvetlen részformula. Legyen F egy formula. Ha $F = p$ valamely $p \in Var$-ra, akkor F-nek nincs közvetlen részformulája. Különben a következő három eset közül pontosan egy teljesül: van olyan $G \in Form$, hogy $F = \neg G$, van olyan $G, H \in Form$, hogy $F = G \vee H$, vagy van olyan $G, H \in Form$, hogy $F = G \wedge H$. Ekkor G-t (illetve G-t és H-t) az F közvetlen részformulájának (illetve közvetlen részformuláinak) nevezzük. A formula közvetlen részformulái egyértelműen meghatározottak, ezért érvényes a következő tétel.

1.2. Tétel. *(Minden formula egyértelműen olvasható.) Minden F formula esetén az alábbi (egymást kizáró) feltételek közül pontosan egy teljesül:*

1. *pontosan egy i-re $F = p_i$,*
2. *pontosan egy F_1 formulára $F = \neg F_1$,*
3. *pontosan egy F_1 és pontosan egy F_2 formulára $F = (F_1 \vee F_2)$,*
4. *pontosan egy F_1 és pontosan egy F_2 formulára $F = (F_1 \wedge F_2)$.*

1.3. Példa. Legyen $F = ((\neg p \vee q) \wedge p) \vee (p \wedge \neg q)$. Ekkor F-nek részformulája például önmaga (amikor G_1 és G_2 az üres szó) vagy például $(\neg p \vee q)$ (a $G_1 = ($ és $G_2 = \wedge p) \vee (p \wedge \neg q)$ szavak mellett). Ugyancsak részformulája F-nek p is, melynek három előfordulása van F-ben. Ugyanakkor F közvetlen részformulái csak a $((\neg p \vee q) \wedge p)$ és a $(p \wedge \neg q)$.

□

A hozzárendelés fogalma

Egy $\mathcal{A} : Var \to \{0,1\}$ leképezést hozzárendelésnek nevezünk. Minden $\mathcal{A}$ hozzárendelés kiterjeszthető egy (ugyancsak $\mathcal{A}$-val jelölt) $\mathcal{A} : Form \to \{0,1\}$ leképezéssé. A kiterjesztést formula indukcióval (vagyis a formulák felépítése szerinti indukcióval) definiáljuk az alábbi módon. Legyen $F \in Form$.

(i) Ha $F = p$ valamely $p \in Var$ esetén, akkor $\mathcal{A}(F) = \mathcal{A}(p)$.

(ii) Ha $F = \neg G$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 0 \\ 0 & \text{ha } \mathcal{A}(G) = 1 \end{cases}$$

Ha $F = G \vee H$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 1 \text{ vagy } \mathcal{A}(H) = 1 \\ 0 & \text{különben} \end{cases}$$

Ha $F = G \wedge H$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 1 \text{ és } \mathcal{A}(H) = 1 \\ 0 & \text{különben} \end{cases}$$

□

Elnevezések

Most bevezetünk néhány elnevezést. Legyen $F \in Form$.

1. Legyen $\mathcal{A}$ egy hozzárendelés. Ha $\mathcal{A}(F) = 1$, akkor ezt a tényt $\mathcal{A} \models F$-fel is jelöljük és azt mondjuk, hogy $\mathcal{A}$ kielégíti F-et vagy, hogy $\mathcal{A}$ modellje F-nek.
2. Ha F-nek van modellje, akkor azt mondjuk, hogy F kielégíthető.
3. Ha minden $\mathcal{A}$ hozzárendelés esetén $\mathcal{A} \models F$, akkor F tautológia (vagy másképpen: érvényes). Jele $\models F$.
4. Ha F-nek nincs modellje, akkor azt mondjuk, hogy F kielégíthetetlen.
5. Legyen Σ formulák egy halmaza. Ha valamely $\mathcal{A}$ hozzárendelés esetén minden $F \in \Sigma$-re $\mathcal{A} \models F$, akkor ezen tényt $\mathcal{A} \models \Sigma$-val jelöljük és azt mondjuk, hogy $\mathcal{A}$ kielégíti Σ-t vagy, hogy $\mathcal{A}$ modellje Σ-nak.
6. Ha Σ-nak van modellje, akkor azt mondjuk, hogy Σ kielégíthető.

□

Jelölések

Bevezetünk néhány sztenderd jelölést amelyek érvényesek lesznek az egész 2. fejezetben.

1. Ítéletváltozók: $p, q, r, p_1, p_2, \ldots$
2. Formulák: $F, G, H, F_1, F_2, \ldots$
3. Formulák halmaza: $\Sigma, \Delta, \Sigma_1, \Sigma_2, \ldots$
4. Hozzárendelések: $\mathcal{A}, \mathcal{A}'$

5. Tetszőleges tautológia (például $p \vee \neg p$): $\uparrow$
6. Tetszőleges kielégíthetetlen formula (például $p \wedge \neg p$): $\downarrow$

□

Nyilvánvalóan igaz az alábbi tétel.

1.4. Tétel. *Egy F formula akkor és csakis akkor tautológia, ha $\neg F$ kielégíthetetlen.*

A logikai következmény

1.5. Definíció. Legyen $\Sigma \subseteq Form$ és $F \in Form$. Azt mondjuk, hogy F logikai következménye Σ-nak, jele $\Sigma \models F$, ha minden $\mathcal{A}$ hozzárendelés esetén valahányszor $\mathcal{A} \models \Sigma$, mindannyiszor $\mathcal{A} \models F$ is teljesül. □

Ha $\Sigma = \{G\}$ egyelemű halmaz, akkor $\{G\} \models F$ helyett csak $G \models F$-et írunk.

A logikai következmény néhány tulajdonsága

1. F akkor és csak akkor érvényes, ha $\varnothing \models F$. Tehát $\models F$ és $\varnothing \models F$ ugyanazt jelenti.
2. Ha F érvényes, akkor minden Σ-ra $\Sigma \models F$.
3. Ha $F \in \Sigma$, akkor $\Sigma \models F$.
4. Minden F-re $\downarrow \models F$.
5. Minden F-re és G-re $F \models G$ akkor és csak akkor teljesül, ha $F \to G$ érvényes.
6. (Modus ponens, röviden Mp.) Minden Σ-ra, F-re és G-re $\Sigma \cup \{F, F \to G\} \models \Sigma \cup \{G\}$.
7. (Monotonitás.) Ha $\Sigma \subseteq \Sigma_1$, akkor minden F-re, ha $\Sigma \models F$, akkor $\Sigma_1 \models F$.
8. (Következmény.) Minden Σ-ra, F-re és G-re $\Sigma \models F \to G$ akkor és csak akkor, ha $\Sigma \cup \{F\} \models G$.

□

1.6. Tétel. *Legyenek $F, F_1, \ldots, F_n$ tetszőleges formulák. Ekkor a következő három állítás ekvivalens.*

(1) $\{F_1, \ldots, F_n\} \models F$

(2) $F_1 \wedge \ldots \wedge F_n \to F$ *tautológia*

(3) $F_1 \wedge \ldots \wedge F_n \wedge \neg F$ *kielégíthetelen.*

Bizonyítás. Gyakorlat. □

1.2. Ekvivalencia, normálformák

A következőkben megadjuk a logikai ekvivalencia fogalmának definícióját.

1.7. Definíció. Legyen F és G két tetszőleges formula. F és G *logikailag ekvivalensek*, ha minden $\mathcal{A}$ hozzárendelés esetén

$\mathcal{A} \models F$ akkor és csak akkor, ha $\mathcal{A} \models G$.

Azt a tényt, hogy F és G logikailag ekvivalensek $F \equiv G$-vel jelöljük. □

A logikai ekvivalencia egy tulajdonsága, hogy minden F-re és G-re $F \equiv G$ akkor és csak akkor teljesül, ha $F \leftrightarrow G$ érvényes.

Ekvivalens formulák

Ebben a részben néhány olyan fontos példát adunk a logikai ekvivalenciára, amelyeket a továbbiakban gyakran felhasználunk. A példákban F, G és H tetszőleges formulákat jelentenek. Az ekvivalenciák igazolása gyakorlat.

Az igaz és hamis szabályok:

$\neg \downarrow \equiv \uparrow$
$\neg \uparrow \equiv \downarrow$
$F \wedge \downarrow \equiv \downarrow$ és $\downarrow \wedge F \equiv \downarrow$
$F \wedge \uparrow \equiv F$ és $\uparrow \wedge F \equiv F$
$F \vee \uparrow \equiv \uparrow$ és $\uparrow \vee F \equiv \uparrow$
$F \vee \downarrow \equiv F$ és $\downarrow \vee \equiv F$

Az idempotencia szabályai:

$F \wedge F \equiv F$
$F \vee F \equiv F$

A kommutativitás szabályai:

$F \wedge G \equiv G \wedge F$
$F \vee G \equiv G \vee F$

Az asszociativitás szabályai:

$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
$(F \vee G) \vee H \equiv F \vee (G \vee H)$

Az abszorpció szabályai:

$F \wedge (F \vee G) \equiv F$
$F \vee (F \wedge G) \equiv F$

A disztributivitás szabályai:

$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$

A dupla negáció szabálya:

$\neg\neg F \equiv F$

A de Morgan szabályok:

$\neg(F \wedge G) \equiv \neg F \vee \neg G$
$\neg(F \vee G) \equiv \neg F \wedge \neg G$

□

Ugyancsak érvényes a következő tétel, amelyben szereplő formulákat az általánosított de Morgan szabálynak és az általánosított disztributivitás törvényének nevezünk.

1.8. Tétel.

$$\neg\left(\bigvee_{i=1}^{n} F_i\right) \equiv \bigwedge_{i=1}^{n} (\neg F_i)$$
$$\neg\left(\bigwedge_{i=1}^{n} F_i\right) \equiv \bigvee_{i=1}^{n} (\neg F_i)$$

$$\left(\left(\bigvee_{i=1}^{m} F_i\right) \wedge \left(\bigvee_{j=1}^{n} G_j\right)\right) \equiv \bigvee_{i=1}^{m}\left(\bigvee_{j=1}^{n} (F_i \wedge G_j)\right)$$
$$\left(\left(\bigwedge_{i=1}^{m} F_i\right) \vee \left(\bigwedge_{j=1}^{n} G_j\right)\right) \equiv \bigwedge_{i=1}^{m}\left(\bigwedge_{j=1}^{n} (F_i \vee G_j)\right)$$

Végül kimondjuk a helyettesítési lemmát.

1.9. Lemma. (Helyettesítési lemma) Legyenek F, G és H formulák, úgy, hogy F a H egy részformulája és $F \equiv G$. Akkor $H \equiv H[F/G]$, ahol $H[F/G]$ azt a formulát jelöli, amelyet úgy kaptunk, hogy H-ban F valamely előfordulásának a helyére G-t helyettesítettünk.

Bizonyítás. Formula indukcióval történik.

(i) Ha $H = p$ valamely $p \in Var$-ra, akkor $F = H$ és így $H[F/G] = G$. Tehát $H[F/G] = G \equiv F = H$.

(iia) Legyen $H = \neg H_1$. Ha $F = H$, akkor a bizonyítás ugyanaz mint az (i) esetben. Különben F-nek a szóban forgó előfordulása H_1-ben van és így az indukciós feltevés miatt $H_1 \equiv H_1[F/G]$. Következésképpen $H = \neg H_1 \equiv \neg H_1[F/G] = H[F/G]$.

(iib) Legyen $H = H_1 \vee H_2$. Az $F = H$ eset bizonyítása ismét analóg (i)-vel. Különben F-nek a szóban forgó előfordulása H_1-ben (vagy H_2-ben) van, így az indukciós feltevés miatt $H_1 \equiv H_1[F/G]$. Akkor $H = H_1 \vee H_2 \equiv H_1[F/G] \vee H_2 = H[F/G]$.

(iic) Legyen $H = H_1 \wedge H_2$. Ennek az esetnek a bizonyítás ugyanaz mint az előzőé. □

Konjunktív és diszjunktív normálformák

Most megadjuk a konjunktív normálforma és a diszjunktív normálforma definícióját. Ehhez először bevezetjük a literál fogalmát.

1.10. Definíció. Egy F formulát literálnak nevezünk, ha $F = p$ vagy $F = \neg p$ teljesül valamely $p \in Var$ esetén. Az első esetben F-et pozitív literálnak, a második esetben negatív literálnak nevezzük.

Egy literál tehát egy változó vagy egy változó negációja. A literálokat általában ℓ-lel jelöljük és használni fogjuk rájuk a következő jelölést is.

$$\overline{\ell} = \begin{cases} \neg p & \text{, ha } \ell = p \\ p & \text{, ha } \ell = \neg p \end{cases}$$

1.11. Definíció. Egy F formula konjunktív normálforma, ha

$$F = \bigwedge_{i=1}^{n}\left(\bigvee_{j=1}^{m_i} \ell_{i,j}\right),$$

ahol az $\ell_{i,j}$-k literálok. Hasonlóan, F diszjunktív normálforma, ha

$$F = \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_i} \ell_{i,j} \right),$$

ahol az $\ell_{i,j}$-k literálok.

Bebizonyítjuk a következő jól ismert tételt.

1.12. Tétel. *Minden F formulához van vele logikailag ekvivalens konjunktív és diszjunktív normálforma.*

Bizonyítás. A bizonyítást formula indukcióval végezzük.

(i) Ha $F = p$ vagy $F = \neg p$, akkor kész vagyunk, mert már F maga is konjunktív és diszjunktív normálforma is.

(iia) Tegyük fel, hogy $F = \neg G$. Az indukció feltevés miatt van G-vel ekvivalens konjunktív és diszjunktív normálforma is. Vegyük a G-vel ekvivalens konjunktív normálformát, azaz legyen

$$G \equiv G_1 = \bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_i} \ell_{i,j} \right).$$

Ekkor az általánosított de Morgan szabályokkal kapjuk, hogy

$$\begin{aligned} F &\equiv \neg G_1 = \neg \left(\bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_i} \ell_{i,j} \right) \right) \equiv \bigvee_{i=1}^{n} \left(\neg \bigvee_{j=1}^{m_i} \ell_{i,j} \right) \\ &\equiv \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_i} \overline{\ell_{i,j}} \right), \end{aligned}$$

tehát, van F-fel logikailag ekvivalens diszjunktív normálforma.

Az F-fel ekvivalens konjunktív normálformát pedig a G-vel ekvivalens diszjunktív normálformából kapjuk hasonló módon.

(iib) Tegyük most fel, hogy $F = G \vee H$. Az indukció feltevés miatt G-hez is és H-hoz is van vele ekvivalens konjunktív és diszjunktív normálforma is.

Az F-fel ekvivalens diszjunktív normálformát egyszerűen a G-vel ekvivalens és a H-val ekvivalens diszjunktív normálformák diszjunkciójaként kapjuk.

Az F-fel ekvivalens konjunktív normálforma pedig a következőképpen kapható. Vegyük a G-vel ekvivalens és a H-val ekvivalens konjunktív normálformákat, azaz legyen

$$G \equiv G_1 = \bigwedge_{i=1}^{n} G_i', \qquad \text{ahol a } G_i'\text{-k diszjunkciós tagok}$$

és

$$H \equiv H_1 = \bigwedge_{l=1}^{k} H_l', \qquad \text{ahol } H_l'\text{-ek diszjunkciós tagok}$$

Akkor $F \equiv G_1 \vee H_1 = \left(\bigwedge_{i=1}^{n} G_i'\right) \vee \left(\bigwedge_{l=1}^{k} H_l'\right) \equiv \bigwedge_{i=1}^{n} \left(\bigwedge_{l=1}^{k} (G_i' \vee H_l')\right)$. Mivel ekkor a $G_i' \vee H_l'$-ek is diszjunkciós tagok, a $\equiv$ jel jobb oldalán álló formula konjunktív normálforma.

(iic) Az $F = G \wedge H$ eset bizonyítása hasonló, az olvasóra bízzuk. □

Most megadjuk ugyanennek a tételnek egy másik, algoritmikusan jobban használható bizonyítását is.

1.13. Tétel. *Minden F formulához van vele logikailag ekvivalens konjunktív és diszjunktív normálforma.*

Bizonyítás. Legyen F egy formula. Akkor az F-fel ekvivalens konjunktív normálforma a következő eljárással kapható meg.

1. (Negáció bevitele.) Amíg lehetséges, helyettesítsük F-ben a

$\neg\neg G$	alakú részformulákat	G-vel,
$\neg(G \wedge H)$	alakú részformulákat	$\neg G \vee \neg H$-val,
$\neg(G \vee H)$	alakú részformulákat	$\neg G \wedge \neg H$-val.

2. Amíg lehetséges, helyettesítsük F-ben a

$F \vee (G \wedge H)$	alakú részformulákat	$(F \vee G) \wedge (F \vee H)$-val,
$(F \wedge G) \vee H$	alakú részformulákat	$(F \vee H) \wedge (G \vee H)$-val.

Az F-fel ekvivalens diszjunktív normálforma a következő eljárással kapható meg.

1. Ugyanaz mint a konjunktív normálforma esetén.

2. Amíg lehetséges, helyettesítsük F-ben a

$F \wedge (G \vee H)$	alakú részformulákat	$(F \wedge G) \vee (F \wedge H)$-val
$(F \vee G) \wedge H$	alakú részformulákat	$(F \wedge H) \vee (G \wedge H)$-val.

□

Most megadunk egy példát a fenti eljárás alkalmazására.

1.14. Példa. Adjuk meg a $(p \to q) \vee ((q \to \neg r) \wedge (r \to \neg p))$ formulával ekvivalens konjunktív normálformát. A következő számolás adódik:

$$
\begin{aligned}
&(p \to q) \vee ((q \to \neg r) \wedge (r \to \neg p)) \\
&\quad \equiv \quad (\neg p \vee q) \vee ((\neg q \vee \neg r) \wedge (\neg r \vee \neg p)) \\
&\quad \equiv \quad ((\neg p \vee q) \vee (\neg q \vee \neg r)) \wedge ((\neg p \vee q) \vee (\neg r \vee \neg p)) \\
&\quad \equiv \quad (\neg p \vee q \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r \vee \neg p) \\
&\quad \equiv \quad \uparrow \wedge (\neg p \vee q \vee \neg r) \\
&\quad \equiv \quad \neg p \vee q \vee \neg r.
\end{aligned}
$$

□

1.3. Az ítéletkalkulus funkcionális teljessége

1.15. Definíció. Tetszőleges $k \geq 0$ esetén egy $IT : \{0,1\}^k \to \{0,1\}$ leképezést k változós igazságtáblának, vagy Boole függvénynek nevezünk.

1.16. Definíció. Legyen $F \in Form$. Akkor F meghatároz egy IT_F igazságtáblát a következő módon. Legyenek $p_1, \ldots, p_n$ az F-ben előforduló változók. Tetszőleges $x_1, \ldots, x_n \in \{0,1\}$ esetén

$$IT_F(x_1, \ldots, x_n) = \mathcal{A}(F), \text{ ahol } \mathcal{A}(p_j) = x_j,\ 1 \leq j \leq n.$$

1.17. Lemma. Ha F és G formulák esetén $IT_F = IT_G$, akkor $F \equiv G$.

Bizonyítás. A megfelelő definíciók alapján nyilvánvaló. □

A következő tételben bebizonyítjuk, hogy az ítéletkalkulus funkcionálisan teljes, vagyis, hogy minden IT igazságtábla előáll IT_F alakban valamely alkalmas F formulára. Sőt, az is igaz, hogy van olyan F is, amelyik konjunktív (diszjunktív) normálforma.

1.18. Tétel. *Minden $k \geq 1$, $IT : \{0,1\}^k \to \{0,1\}$ igazságtáblához van egy olyan F diszjunktív (konjunktív) normálforma, melyre $IT = IT_F$.*

Bizonyítás. Legyen $F = \bigvee_{IT(x_1,\ldots,x_k)=1} (p_1^{x_1} \wedge \ldots \wedge p_k^{x_k})$, ahol

$$p_j^{x_j} = \begin{cases} p_j & \text{, ha } x_j = 1 \\ \neg p_j & \text{, ha } x_j = 0. \end{cases}$$

Nyilvánvaló, hogy F diszjunktív normálforma és, hogy $IT = IT_F$.

Továbbá, ha $F = \bigwedge_{IT(y_1,\ldots,y_k)=0} (p_1^{y_1} \vee \ldots \vee p_k^{y_k})$, ahol most

$$p_j^{y_j} = \begin{cases} p_j & \text{, ha } y_j = 0 \\ \neg p_j & \text{, ha } y_j = 1, \end{cases}$$

akkor F konjunktív normálforma és ismét $IT = IT_F$. □

A fenti tételből a konjunktív normálforma és diszjunktív normálforma tétel egy újabb bizonyítása következik.

1.19. Következmény. Minden F formulához van vele logikailag ekvivalens konjunktív és diszjunktív normálforma.

Bizonyítás. Legyen G egy tetszőleges formula. Akkor a 1.18. tétel alapján IT_G-hez is van olyan F konjunktív (és diszjunktív) normálforma, melyre $IT_G = IT_F$. Ugyanakkor, a 1.17. lemma szerint $F \equiv G$. □

1.20. Definíció. A $\neg, \wedge, \vee, \to$ műveleti jelek egy C halmazát adekvátnak nevezzük, ha bármely $IT : \{0,1\}^k \to \{0,1\}$, $k \geqslant 1$ igazságtábla esetén van olyan $F \in Form$, hogy

1. F-ben csak C-beli műveleti jelek szerepelnek,
2. $IT = IT_F$.

1.21. Tétel. A $\{\neg, \vee, \wedge\}$, $\{\neg, \vee\}$ és $\{\neg, \wedge\}$ halmazok mindegyike adekvát. Továbbá a $\{\vee, \wedge\}$ nem adekvát.

Bizonyítás. Az $\{\neg, \vee, \wedge\}$ halmaz adekvátsága a 1.18. tételből következik. Továbbá a $\{\neg, \vee\}$ és $\{\neg, \wedge\}$ adekvátsága közvetlenül adódik $\{\neg, \vee, \wedge\}$ adekvátságából és a De Morgan azonosságokból. Végül a $\{\vee, \wedge\}$ nem adekvát, mert nem fejezhető ki vele a $IT(0) = 1$, $IT(1) = 0$ egyváltozós igazságtábla. □

1.4. Horn formulák

1.22. Definíció. A Horn formula egy olyan konjunktív normálforma, amelyben minden diszjunkciós tag legfeljebb egy pozitív literált tartalmaz. □

1.23. Példa. $F = (\neg q \vee \neg r \vee p) \wedge r \wedge (\neg p \vee \neg q) \wedge \neg s$ egy Horn formula. □

Elnevezés

A Horn formulákban szereplő diszjunkciós tagokat Horn klózoknak nevezünk. □

Jelölés

Bevezetjük a következő jelöléseket:

$$\begin{array}{rll} p & \text{helyett} & 1 \to p\text{-t} \\ \neg p_1 \vee \ldots \vee \neg p_n \vee q & \text{helyett} & p_1 \wedge \ldots \wedge p_n \to q\text{-t} \\ \neg p_1 \vee \ldots \vee \neg p_n & \text{helyett} & p_1 \wedge \ldots \wedge p_n \to 0\text{-t írunk.} \end{array}$$

□

A Horn formulák kielégíthetőségének eldöntésére a változók számában mérve lineáris időbonyolultságú algoritmus adható.

1.24. Algoritmus.

Input: F Horn formula
Output: *Igen* és az F-et kielégítő $\mathcal{A}$ hozzárendelés, ha F kielégíthető,
Nem különben .

1. Minden $1 \to p$, F-beli klóz esetén jelöljünk meg p minden előfordulását F-ben.
2. Amíg F-ben van $p_1 \wedge \ldots \wedge p_n \to q$ alakú klóz, úgy, hogy $p_1, \ldots, p_n$ meg van jelölve, de q nincs megjelölve, jelöljük meg q minden előfordulását F-ben.
3. Ha F-ben van olyan $p_1 \wedge \ldots \wedge p_n \to 0$ alakú klóz, hogy $p_1, \ldots, p_n$ mindegyike meg van jelölve, akkor az output *Nem*; különben az output *Igen* és az a hozzárendelés, melyre

   $\mathcal{A}(p) = 1$ akkor és csak akkor, ha p meg van jelölve.

1.25. Tétel. A 1.24. algoritmus minden F Horn formula esetén terminál, továbbá F akkor és csak akkor kielégíthető, ha az output *Igen*.

Bizonyítás. Az, hogy az algoritmus terminál, abból következik, hogy a 2. pontjában szereplő ciklus legfeljebb annyiszor fut le, ahány változó szerepel F-ben.

Tegyük fel, hogy F outputja *Igen*. Megmutatjuk, hogy ekkor $\mathcal{A}$ kielégíti F-et, amihez elegendő megmutatni, hogy kielégíti F minden G klózát.

Ha $G = 1 \to p$, akkor az algoritmus az 1. pontjában megjelölte p-t, tehát $\mathcal{A}(p) = 1$ és így $\mathcal{A}(G) = 1$.

Ha $G = p_1 \wedge \ldots \wedge p_n \to q$, akkor két eset lehetséges. Az egyik, amikor az algoritmus a $p_1, \ldots, p_n$ változók mindegyikét megjelölte. Ekkor a 2. lépésben q-t is megjelölte, tehát $\mathcal{A}(p_1) = \ldots = \mathcal{A}(p_n) = \mathcal{A}(q) = 1$ és így $\mathcal{A}(G) = 1$. A másik eset, amikor az algoritmus valamely p_i-t nem jelölt meg. Ekkor $\mathcal{A}(p_i) = 0$, tehát megint csak $\mathcal{A}(G) = 1$.

Ha $G = p_1 \wedge \ldots \wedge p_n \to 0$, akkor, mivel az output *Igen*, van olyan p_i, amit az algoritmus nem jelölt meg. Erre $\mathcal{A}(p_i) = 0$, tehát újra $\mathcal{A}(G) = 1$.

Fordítva indirekt módszerrel bizonyítunk. Tegyük fel, hogy F outputja *Nem* és F mégis kielégíthető egy $\mathcal{A}'$ hozzárendeléssel. Először is észrevesszük, hogy ha az algoritmus megjelölt egy F-ben szereplő p változót, akkor szükségképpen $\mathcal{A}'(p) = 1$. Ez valóban így van, ugyanis az algoritmus két esetben jelöl megy egy változót. Egyrészt, ha az egy $1 \to p$ alakú klózban szerepel, amikor is nyilvánvaló, hogy $\mathcal{A}'(p) = 1$ kell legyen. Másrészt, ha a változó egy olyan $p_1 \wedge \ldots \wedge p_n \to q$ formulában szereplő q, melyben a $p_1, \ldots, p_n$ változók mindegyike meg van jelölve. Mivel ekkor $\mathcal{A}'(p_1) = \ldots = \mathcal{A}'(p_n) = 1$, szükségképpen $\mathcal{A}'(q) = 1$ kell legyen.

Mivel az algoritmus *Nem*-mel terminált, van egy olyan $G = p_1 \wedge \ldots \wedge p_n \to 0$ klóz, melyben a $p_1, \ldots, p_n$ változók mindegyike meg van jelölve. De akkor az előbbiek miatt $\mathcal{A}'(p_1) = \ldots = \mathcal{A}'(p_n) = 1$, azaz $\mathcal{A}'(G) = 0$. Ez viszont ellentmondás, mert $\mathcal{A}'$ kielégíti F-et. □

Észrevehető, hogy ha egy F Horn formulában nincs $1 \to p$ vagy $p_1 \wedge \ldots \wedge p_n \to 0$ alakú klóz, akkor F mindig kielégíthető. Valóban, az első esetben a minden változóhoz 0-t, míg a második esetben a minden változóhoz 1-et rendelő hozzárendelés elégíti ki F-et. (Tehát egy elegendő feltételt kaptunk az F Horn formula kielégíthetőségére.)

Továbbá az algoritmus 2. pontjában szereplő ciklus legfeljebb annyiszor fut le, ahány változó van F-ben, tehát az algoritmus gyors, futási ideje a változók számával egyenesen arányos.

1.26. Példa. Vegyük újra a 1.23. példában szereplő F Horn formulát, melynek klózai

$$\begin{array}{rcl} q \wedge r & \to & p \\ 1 & \to & r \\ p \wedge q & \to & 0 \\ s & \to & 0 \end{array}$$

Az algoritmus csak az r-et jelöli meg, tehát az F kielégíthető az $\mathcal{A}(r) = 1$, $\mathcal{A}(p) = \mathcal{A}(q) = \mathcal{A}(s) = 0$ hozzárendeléssel. □

1.5. A tabló módszer

A tabló módszer egy algoritmus annak eldöntésére, hogy egy F formula kielégíthető-e. Ismretes, hogy a kielégíthetőség $O(2^n)$ időbonyolultságú algoritmussal dönthető el, ahol n az F formula mérete. Ezen az időkorláton a tabló módszer sem tud javítani, bizonyos esetekben azonban a lépésszám kevesebb lehet.

A módszer lényege, hogy F-hez nemdeterminisztikus módon hozzárendelhető egy fa, az ún. szemantikus tabló, melynek bizonyos tulajdonságaiból az F kielégíthetőségére következtethetünk.

Mielőtt erre rátérnének, definiáljuk az α és a β formula fogalmát.

1.27. Definíció. A $\neg\neg F$, $F \wedge G$ és $\neg(F \vee G)$ alakú formulákat α-formuláknak, az $F \vee G$ és $\neg(F \wedge G)$ alakú formulákat β-formuláknak nevezzük.

Könyen bizonyítható, hogy a triviális esetek kivételével minden formula α-formula vagy β-formula.

1.28. Lemma. Legyen F egy tetszőleges formula. Akkor F literál, vagy α-formula, vagy β-formula.

Bizonyítás. A bizonyítást formula indukcióval végezzük.

(i) Ha $F \in Var$, akkor F literál.

(iia) Ha $F = \neg G$, akkor további esetek lehetségesek. Ha $G \in Var$, akkor F megint csak literál. Ha $G = \neg G_1$ vagy $G = G_1 \vee G_2$, akkor F egy α-formula és végül, ha $G = G_1 \wedge G_2$, akkor F egy β-formula.

(iib) Ha $F = G \vee H$, akkor F egy β-formula.

(iic) Ha $F = G \wedge H$, akkor F egy α-formula. □

A szemantikus tabló megkonstruálása tablók segítségével történik. Kétféle tabló van, az α formulákon operáló α-tabló és a β formulákon operáló β tabló, melyek az alábbiak.

α	α_1	α_2
$\neg\neg F_1$	F_1	
$F_1 \wedge F_2$	F_1	F_2
$\neg(F_1 \vee F_2)$	$\neg F_1$	$\neg F_2$

β	β_1	β_2
$F_1 \vee F_2$	F_1	F_2
$\neg(F_1 \wedge F_2)$	$\neg F_1$	$\neg F_2$

Az α tabló első oszlopának valamely sorában lévő formula akkor és csak akkor igaz valamely $\mathcal{A}$ hozzárendelés mellett, ha ugyanazon sor második és harmadik oszlopában lévő formulák mindegyike igaz $\mathcal{A}$ mellett. (Kivéve az első sort, ahol nyilván $\mathcal{A} \models \neg\neg F_1$ akkor és csak akkor, ha $A \models F_1$.) A β tabló első oszlopának valamely sorában lévő formula akkor és csak akkor igaz egy $\mathcal{A}$ hozzárendelés mellett, ha ugyanazon sor második és harmadik oszlopában lévő formulák valamelyike igaz $\mathcal{A}$ mellett.

Egy F formulához tartozó szemantikus tabló egy olyan véges, címkézett fa, melynek minden csúcspontja egy véges formulahalmazzal van megcímkézve. A szemantikus tablót felépítő nemdeterminisztikus algoritmus a következő.

1.29. Algoritmus.

Input: Egy F formula.
Output: Egy F-hez tartozó T szemantikus tabló.

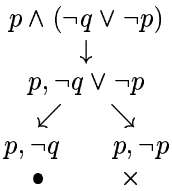
1. Kezdetben legyen $T = \{F\}$, vagyis az egyetlen szögpontból álló fa, melynek címkéje $\{F\}$.

2. **while** T-nek van megjelöletlen levele
   begin
   Válasszunk egy l megjelöletlen levelet, legyen a címkéje $\Sigma(l)$;
   if $\Sigma(l)$ csak literálokból áll
   then if $\Sigma(l)$ tartalmaz egy $p, \neg p$ párt
   then jelöljük meg $\Sigma(l)$-et $\times$-szel
   else jelöljük meg $\Sigma(l)$-et $\bullet$-rel.
   else begin
   Válasszunk egy $H \in \Sigma(l)$ formulát ami nem literál;
   if H α-formula
   then T-ben l fia legyen l', melynek címkéje legyen $\Sigma(l') = (\Sigma(l) - \{H\}) \cup \{H_1, H_2\}$,
   (Ha $H = \neg\neg H_1$, akkor $\Sigma(l') = (\Sigma(l) - \{H\}) \cup \{H_1\}$)
   /* H_1 és H_2 az α-tablóban a H sorában lévő formulák */
   else T-ben l fiai legyenek l' és l'', melyeknek címkéje legyen
   $\Sigma(l') = (\Sigma(l) - \{H\}) \cup \{H_1\}$ és
   $\Sigma(l'') = (\Sigma(l) - \{H\}) \cup \{H_2\}$.
   /* H_1 és H_2 a β-tablóban a H sorában lévő formulák */
   end
   end.

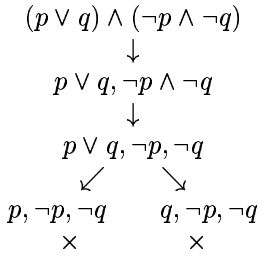
□

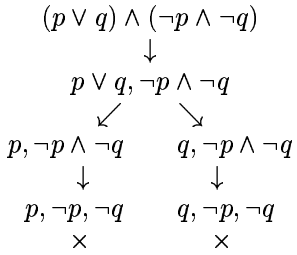
A fenti algoritmusban a megjelöletlen levél többféleképpen is választható, így további kikötések nélkül a formulához tartozó szemantikus tabló nem egyértelműen meghatározott.

1.30. Példa. Az a) $F = p \wedge (\neg q \vee \neg p)$ formulának egy szemantikus tablója van, a következő.



b) Az $F = (p \vee q) \wedge (\neg p \wedge \neg q)$ formulának két szemantikus tablója van.





□

Először megmutatjuk, hogy a szemantikus tabló konstrukciója mindig terminál.

1.31. Lemma. Bizonyítás. Tetszőleges F formula esetén a fenti algoritmus terminál.

A szemantikus tabló konstruálása során egyetlen (az $\{F\}$) csúcsból kiindulva egy fát építünk fel, melynek minden l csúcsa egy $\Sigma(l)$ formulahalmazzal van megcímkézve. Minden l csúcshoz rendeljük hozá a $w(l) = 2b(l) + n(l)$ számot, ahol $b(l)$ a $\Sigma(l)$ formuláiban szereplő $\wedge$ és $\vee$ jelek száma, és $n(l)$ a $\neg$ jelek száma. Megmutatjuk, hogy a fa gyökerétől a levelei felé haladva, a csúcsokhoz rendelt számok szigorúan csökkenő sorozatot alkotnak. Ebből nyilvánvalóan következik, hogy az algoritmus egy véges fában terminál.

Tegyük fel, hogy a konstrukció során a **while** ciklusba való belépes után az l levelet választjuk, mely a $\Sigma(l)$ formulahalmazzal van címkézve. Legyen $b(l)$ a $\Sigma(l)$ formuláiban szereplő $\wedge$ és $\vee$ jelek száma, és legyen $n(l)$ a $\neg$ jelek száma. Tehát l-hez a $w(l) = 2b(l) + n(l)$ számot rendeljük.

Azt mutatjuk meg, hogy

- ha $\Sigma(l)$-ből α formulát választunk ki, akkor a konstrukció által az l-hez csatlakoztatott l' levélhez rendelt $w(l')$ szám kisebb lesz (kisebbek lesznek) mint $w(l)$,
- ha $\Sigma(l)$-ből β formulát választunk ki, akkor a konstrukció által az l-hez csatlakoztatott l' és l'' levelekhez rendelt $w(l')$ és $w(l'')$ számok kisebbek lesznek mint $w(l)$.

A teljes bizonyítás helyett annak csak két részesetét mutatjuk meg. Ha például $\Sigma(l)$-ből egy $\neg(F_1 \vee F_2)$ alakú α-formulát választunk, akkor l-hez egy l' levelet csatlakoztatunk, melyre

$$w(l') = 2(b(l) - 1) + n(l) + 1 = w(l) - 1.$$

Vagy, ha $\Sigma(l)$-ből egy $F_1 \vee F_2$ alakú β-formulát választjuk ki, akkor l-hez az l' és l'' leveleket csatlakoztatjuk, melyekre

$$w(l'), w(l'') \leq 2(b(l) - 1) + n(l) = w(l) - 2.$$

Mindegyik esetben $w(l'), w(l'') < w(l)$. A többi eset hasonlóan igazolható. □

1.32. Definíció. Egy szemantikus tabló zárt, ha minden levele $\times$ jellel van megcímkézve. Különben a szemantikus tabló nyitott.

□

1.33. Lemma. Ha egy F formula valamely szemantikus tablója zárt, akkor F kielégíthetetlen.

Bizonyítás. Legyen T az F egy szemantikus tablója és tegyük fel, hogy T zárt. Azt mutatjuk meg, hogy T minden d csúcspontját címkéző $\Sigma(d)$ halmaz kielégíthetelen. Ez elegendő lesz a lemma bizonyításához, mert T gyökerének címkéje $\{F\}$. A bizonyítást d-nek a T-ben levő $h(d)$ magassága szerint mutatjuk meg.

(i) Ha $h(d) = 0$, akkor d levél, és mivel T zárt, $\Sigma(d)$ $\times$-szel van megjelölve. Így $\Sigma(d)$ tartalmaz egy $p, \neg p$ párt, tehát kielégíthetetlen.

(ii) Legyen most $h(d) > 0$. Ekkor különböző esetek lehetségesek, aszerint, hogy d-ben α típusú vagy β típusú formulát választottunk.

Az első esetben három aleset van, nevezetesen, amikor a választott formula $\neg\neg F_1, F_1 \wedge F_2$ vagy $\neg(F_1 \vee F_2)$ alakú. Vegyük a második alesetet. Ekkor $\Sigma(d) = \Sigma_0 \cup \{F_1 \wedge F_2\}$, d-nek egyetlen d' leszármazottja van, melyre $\Sigma(d') = \Sigma_0 \cup \{F_1, F_2\}$. Mivel a $h(d') = h(d) - 1$, alkalmazhatjuk az indukció feltevést, mely szerint $\Sigma(d')$ kielégíthetetlen. Ekkor viszont $\Sigma(d)$ sem lehet kielégíthető, ugyanis minden olyan $\mathcal{A}$ hozzárendelés, amely kielégíti $\Sigma(d)$-t, ugyancsak kielégíti $\Sigma(d')$-t is. (Ha $\mathcal{A} \models \Sigma_0 \cup \{F_1 \wedge F_2\}$, akkor $\mathcal{A} \models \Sigma_0$ és $\mathcal{A} \models F_1 \wedge F_2$. Ez utóbbi azt jelenti, hogy $\mathcal{A} \models F_1$ és $\mathcal{A} \models F_2$, tehát $\mathcal{A} \models \Sigma_0 \cup \{F_1, F_2\}$.)

Az α-formulák másik két alesete hasonlóan igazolható.

Most tegyük fel, hogy d-nél β-formulát választottunk, ami lehetett $F_1 \vee F_2$ vagy $\neg(F_1 \wedge F_2)$. Csak az első esettel foglalkozunk, a második hasonlóan igazolható.
Ha az $F_1 \vee F_2$ formulát választottuk, akkor $\Sigma(d) = \Sigma_0 \cup \{F_1 \vee F_2\}$, továbbá d-nek két fia van, a d' és a d'', melyekre $\Sigma(d') = \Sigma_0 \cup \{F_1\}$ és $\Sigma(d'') = \Sigma_0 \cup \{F_2\}$.

Mivel $h(d'), h(d'') < h(d)$, az indukció feltevés sem $\Sigma(d')$ sem $\Sigma(d'')$ nem kielégíthető.

Ekkor viszont $\Sigma(d)$ sem lehet kielégíthető, ugyanis minden olyan $\mathcal{A}$ hozzárendelés, amely kielégíti $\Sigma(d)$-t, ugyancsak kielégíti $\Sigma(d')$-t vagy $\Sigma(d')$-t.

(Ha $\mathcal{A} \models \Sigma_0 \cup \{F_1 \vee F_2\}$, akkor $\mathcal{A} \models \Sigma_0$ és $\mathcal{A} \models F_1 \vee F_2$. Ez utóbbi azt jelenti, hogy $\mathcal{A} \models F_1$ vagy $\mathcal{A} \models F_2$, tehát $\mathcal{A} \models \Sigma_0 \cup \{F_1\}$ vagy $\mathcal{A} \models \Sigma_0 \cup \{F_2\}$.)

Az β-formula másik alesete is hasonlóan igazolható.

□

Mielőtt a fordított állítást bebizonyítanánk, bevezetünk egy fogalmat.

1.34. Definíció. Legyen Σ formulák egy halmaza. Σ Hintikka halmaz, ha teljesülnek rá a következő feltételek.

1. Minden $p \in Var$ esetén, ha $p \in \Sigma$, akkor $\neg p \notin \Sigma$, és ha $\neg p \in \Sigma$, akkor $p \notin \Sigma$.

2. Ha $F \in \Sigma$ és F egy α formula, akkor az α tabló F-nek megfelelő sorában a második **és** a harmadik oszlopban lévő elem is Σ-ban van. (Például, ha $F = \neg(F_1 \vee F_2)$, akkor $\neg F_1 \in \Sigma$ és $\neg F_2 \in \Sigma$.)

3. Ha $F \in \Sigma$ és F egy β formula, akkor a β tabló F-nek megfelelő sorában a második **vagy** a harmadik oszlopban lévő elem Σ-ban van. (Például, ha $F = F_1 \vee F_2$, akkor $F_1 \in \Sigma$ vagy $F_2 \in \Sigma$.) □

1.35. Lemma. Ha Σ Hintikka halmaz, akkor Σ kielégíthető.

Bizonyítás. Legyen $\mathcal{A} : Var \to \{0,1\}$ az a hozzárendelés, melyre minden Σ-ban előforduló p változó esetén

$$\mathcal{A}(p) = \begin{cases} 1 & \text{ha } p \in \Sigma, \\ 0 & \text{ha } \neg p \in \Sigma. \end{cases}$$

A Σ-ban nem előforduló változókon $\mathcal{A}$ legyen tetszőleges.
Először is megjegyezzük, hogy a Hintikka halmaz definíciójának 1. pontja szerint $\mathcal{A}$ jóldefiniált.
A formulák felépítése szerinti indukcióval megmutatjuk, hogy minden $F \in \Sigma$-ra $\mathcal{A}(F) = 1$.

(i) Ha $F = p$, akkor $\mathcal{A}$ definíciója szerint $\mathcal{A}(F) = 1$. Ha $F = \neg p$, akkor $\mathcal{A}(p) = 0$ tehát megint csak $\mathcal{A}(F) = 1$.

(iia) F egy α-formula. Csak az $F = F_1 \wedge F_2$ esettel foglalkozunk, a másik két eset bizonyítása hasonló. Ekkor a Hintikka halmaz definíciója szerint $F_1 \in \Sigma$ és $F_2 \in \Sigma$. Így az indukció feltevés miatt $\mathcal{A}(F_1) = 1$ és $\mathcal{A}(F_2) = 1$, tehát $\mathcal{A}(F) = 1$.

(iib) F egy β-formula. Most csak az $F = F_1 \vee F_2$ esetet bizonyítjuk. Ekkor a Hintikka halmaz definíciója szerint $F_1 \in \Sigma$ vagy $F_2 \in \Sigma$. Az indukció feltevés miatt $\mathcal{A}(F_1) = 1$ vagy $\mathcal{A}(F_2) = 1$, tehát $\mathcal{A}(F) = 1$.

□

1.36. Lemma. Legyen F egy formula, T az F egy nyitott szemantikus tablója, l pedig a T egy nyitott levele. Legyen

$$\Sigma = \bigcup_d \Sigma(d),$$

ahol d végigfut a T gyökerétől az l leveléig vezető úton lévő csúcsokon. Ekkor Σ egy Hintikka halmaz.

Bizonyítás. A szemantikus tabló konstrukciója során valahányszor egy literál belekerül egy olyan d csúcspontot címkéző $\Sigma(d)$ halmazba, amelyből később út vezet l-hez, akkor az a literál benne lesz $\Sigma(l)$-ben is, mivel a tabló szabályok nem rendelkeznek literálok eltüntetéséről.

Feltevésünk szerint l nyitott, tehát $\Sigma(l)$-ben nincsenek $p, \neg p$ alakú párok. Akkor a T gyökerétől l-hez vezető úton sem lehetnek olyan d és d' csúcspontok, melyekre $p \in \Sigma(d)$ és $\neg p \in \Sigma(d')$ teljesülne (hiszen akkor $p, \neg p$ pár belekerülne $\Sigma(l)$-be is). Tehát Σ-ban sincs ilyen pár és így Σ-ra a Hintikka halmaz definíciójának 1. feltétele teljesül.

Most legyen $H \in \Sigma$ egy α formula. A T gyökerétől l-hez vezető úton van olyan d csúcspont, hogy $H \in \Sigma(d)$ és d-ben egy α szabályt alkalmaztunk H-ra. Akkor d-nek egyetlen fia van, a d', és $H_1, H_2 \in \Sigma(d')$, ahol H_1 és H_2 az α-tabló H-hoz tartozó sorának második és harmadik oszlopában lévő formulák. Következésképpen $H_1, H_2 \in \Sigma$, tehát a Hintikka halmaz definíciójának 2. feltétele is teljesül Σ-ra.

Végül legyen $H \in \Sigma$ egy β formula. A T gyökerétől l-hez vezető úton van olyan d csúcspont, hogy $H \in \Sigma(d)$ és d-ben egy β szabályt alkalmaztunk H-ra. Akkor d-nek két fia van d' és d'', és $H_1 \in \Sigma(d')$ és $H_2 \in \Sigma(d'')$ teljesülnek, ahol H_1 és H_2 a β-tabló H-hoz tartozó sorának második és harmadik oszlopában lévő formulák. Továbbá, vagy d' vagy d'' rajta van a T gyökerétől az

l-hez vezető úton. Tehát $H_1 \in \Sigma$ vagy $H_2 \in \Sigma$, így a Hintikka halmaz definíciójának 3. feltétele is teljesül Σ-ra. □

1.37. Következmény. Legyen F egy formula. Ha F valamely T szemantikus tablója nyitott, akkor F kielégíthető.

Bizonyítás. A feltétel szerint T-nek van egy nyitott l levele. Továbbá a 1.36. lemma szerint a

$$\Sigma = \bigcup_d \Sigma(d)$$

halmaz Hintikka halmaz, ahol d végigfut a T gyökerétől az l levélig vezető úton levő csúcsokon. A 1.35. lemma szerint Σ kielégíthető. Akkor F is kielégíthető, mert a szemantikus tabló konstrukciója miatt $F \in \Sigma$. □

1.38. Következmény. Ha egy F formula kielégíthetetlen, akkor F minden szemantikus tablója zárt.

1.39. Tétel. *Tetszőleges F formula esetén a következő 3 állítás ekvivalens:*

(1) F kielégíthetetlen,

(2) F-nek van zárt szemantikus tablója,

(3) F valamennyi szemantikus tablója zárt.

Bizonyítás. A (3) $\Rightarrow$ (2) nyilvánvaló, a (2) $\Rightarrow$ (1) a 1.33. lemmából, míg (1) $\Rightarrow$ (3) a 1.38. következményből következik. □

Mivel egy formula vagy kielégíthető vagy kielégíthetetlen, a következő tételt is igazoltuk.

1.40. Tétel. *Tetszőleges F formula esetén a következő 3 állítás ekvivalens:*

(1) F kielégíthető,

(2) F-nek van nyitott szemantikus tablója,

(3) F valamennyi szemantikus tablója nyitott.

1.41. Tétel. *Egy F formula akkor és csakis akkor érvényes, ha $\neg F$ valamely szemantikus tablója zárt.*

Bizonyítás. A 1.4. tétel szerint F akkor és csakis akkor érvényes, ha $\neg F$ kielégíthetetlen, mely a 1.38. következmény szerint akkor és csakis akkor áll fenn, ha $\neg F$ valamely szemantikus tablója zárt. □

Megjegyzések. 1) A szematikus tabló mérete a formula hosszában mérve exponenciális is lehet, ezért a tabló módszer időbonyolultsága exponenciális.

2) Az algoritmus gyorsítható azzal, hogy egy csúcsot már akkor megjelölünk $\times$-szel, amikor felfedezünk benne egy ellentétes literálpárt, függetlenül attól, hogy a csúcsban még van olyan formula, amelyik nem literál (és ezért a csúcs még tovább bontható).

3) Különböző heurisztikákat alkalmazhatunk. Például, alkalmazzunk α szabályt, amíg lehet, és csak utána β-szabályt. Ezzel elkerülhetjük formulák fölösleges megkettőzését.

1.6. Az ítéletkalkulus kompaktsági tétele

Az ítéletkalkulus kompaktsági tétele a következőképpen hangzik.

1.42. Tétel. *Egy Σ formulahalmaz akkor és csak akkor elégíthető ki, ha minden véges részhalmaza kielégíthető.*

A bizonyítás az úgynevezett Kőnig lemmán alapszik, amely a végtelen bináris fákról mond ki egy állítást. Egy fa végtelen, ha végtelen sok csúcspontja van. Egy fában útnak nevezzük csúcsok egy olyan $x_0, \ldots, x_n$ sorozatát, ahol x_0 a fa gyökere és minden $0 \leq i \leq n-1$-re x_{n+1} az x_n fia.

Bináris fának olyan fát nevezünk, amelyben minden csúcspont vagy levél, vagy ha nem az, akkor a csúcspontnak két leszármazottja van. Egy bináris fa teljes, ha nincsenek levelei. Tehát a teljes bináris fa végtelen egyben végtelen is.

1.43. Lemma. (Kőnig lemma.) Minden végtelen bináris fában van legalább egy végtelen hosszúságú út.

Bizonyítás. Legyen T egy végtelen bináris fa. Minden $n \geq 0$-ra megadunk egy olyan n hosszúságú $x_0, \ldots, x_n$ utat T-ben, hogy T x_n gyökerű részfája végtelen.

Valóban, legyen x_0 a fa gyökere. (Ekkor az x_0 gyökerű részfa maga T, tehát végtelen.)

Ha n-re az $x_0, \ldots, x_n$ utat már megadtuk, akkor, lévén az x_n gyökerű részfa végtelen, az x_n csúcsnak két fia van és azok között van olyan, amelyik egy végtelen részfának a gyökere. Válasszuk x_{n+1}-nek x_n ezen fiát.

Az ily módon kiválasztott $x_0, x_1, \ldots$ csúcsok végtelen utat alkotnak a T-ben. □

Most már bebizonyíthatjuk a kompaktsági tételt.

Bizonyítás. (**Kompaktsági tétel.**) Ha Σ kielégíthető, akkor minden véges részhalmaza is kielégíthető.

Megfordítva, tegyük fel, hogy Σ minden véges részhalmaza kielégíthető. Minden $n \geq 0$-ra legyen Σ_n a Σ azon formuláinak halmaza, melyekben legfeljebb az első n, vagyis $p_1, \ldots, p_n$ változók fordulnak elő. Mivel ekvivalencia erejéig véges olyan formula van, amelyekben csak az első n változó fordul elő, minden $n \geq 0$-ra Σ_n kielégíthető.

A teljes végtelen bináris fában minden út meghatároz egy hozzárendelést és minden $n \geq 0$ mélységű csúcs meghatározza a $p_1, \ldots, p_n$ változók egy hozzárendelését. Minden $n \geq 0$-ra jelöljük meg a teljes végtelen bináris fa azon n-mélységű csúcsait, amelyeknek megfelelő hozzárendelések kielégík Σ_n-et. A megjelölt csúcsok egy vételen bináris fát határoznak meg. König lemmája szerint ez tartalmaz egy végtelen hosszú utat. Ezen végtelen út által meghatározott hozzárendelés kielégíti Σ-t.

□

1.44. Következmény. *Legyen Σ egy formulahalmaz és F egy formula. $\Sigma \models F$ akkor és csak akkor teljesül, ha van olyan $\Sigma_0 \subseteq \Sigma$ véges formulahalmaz, hogy $\Sigma_0 \models F$.*

Bizonyítás.

$$
\begin{aligned}
\Sigma \models F \quad &\Leftrightarrow \quad \Sigma \cup \{\neg F\} \text{ nem kielégíthető} \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \cup \{\neg F\} \text{ véges halmaz mely nem kielégíthető} \\
&\qquad\quad (1.42.\ \text{tétel}) \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \text{ véges halmaz, hogy } \Sigma_0 \cup \{\neg F\} \text{ nem kielégíthető} \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \text{ véges halmaz, hogy } \Sigma_0 \models F.
\end{aligned}
$$

□

1.7. Deduktív bizonyítások az ítéletkalkulusban

1.7.1. Hilbert típusú bizonyítások

Legyen Σ egy formulahalmaz és tekintsük a $Th(\Sigma) = \{F \mid \Sigma \models F\}$ halmazt, vagyis Σ összes logikai következményeinek halmazát. $Th(\Sigma)$-t a Σ *által generált elméletnek* nevezzük.

Egy olyan "mechanikus" eljárást vagy más szóval módszert szeretnénk kifejleszetni, melynek segítségével $Th(\Sigma)$ elemei, a tételek, megkaphatók Σ-ból. Ez az eljárás a Σ -ból történő, (vagy Σ feletti) bizonyítás lesz.

Bizonyítás tautológiákkal

1.45. Definíció. Legyen Σ formulák egy halmaza. Formulák egy $F_1, \ldots, F_n$ sorozatát Σ -ból történő, (vagy Σ feletti) bizonyításnak (vagy levezetésnek) nevezzük, ha minden $1 \leq i \leq n$ esetén az alábbi három feltétel valamelyike teljesül:

1. $F_i \in \Sigma$,
2. F_i tautológia,
3. van olyan $k, l < i$, hogy $F_l = F_k \to F_i$

Egy F formula bebizonyítható (vagy levezethető) Σ-ból, jele: $\Sigma \vdash F$, ha van olyan Σ feletti $F_1, \ldots, F_n$ bizonyítás, melyre $F_n = F$.

A 1.45. definícióban szereplő 3. feltétel úgy is mondható, hogy a F_i-t két megelőző formulából, nevezetesen F_k-ból és F_l-ből a Modus ponens (Mp) következtetési szabállyal kaptuk. A Modus ponens következtetési szabályt az

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

alakban is szokás írni. Először is észrevesszük a következőt.

1.46. Tétel. *A Modus ponens szabály helyes, vagyis ha valamely $\mathcal{A}$ hozzárendelésre teljesül, hogy $\mathcal{A} \models F$ és $\mathcal{A} \models F \to G$, akkor $\mathcal{A} \models G$.*

Bizonyítás. Nyilvánvaló, lásd a logikai következmény tulajdonságainál. □

Most lássunk néhány példát a levezetésre.

1.47. Példa. Mutassuk meg a következőket.

a) $\Sigma = \{F, \neg G\} \vdash \neg(\neg F \vee G)$

1.	$F \to (\neg G \to (F \wedge \neg G))$	tautológia
2.	F	Σ-ban van
3.	$\neg G \to (F \wedge \neg G)$	Modus ponenssel 1-ből és 2-ből
4.	$\neg G$	Σ-ban van
5.	$F \wedge \neg G$	Mp(3,4)
6.	$(F \wedge \neg G) \to \neg(\neg F \vee G)$	tautológia
7.	$\neg(\neg F \vee G)$	Mp(5,6)

b) $\Sigma = \{F \to (G \wedge H)\} \vdash F \to G$

1.	$F \to (G \wedge H)$	Σ-ban van
2.	$(F \to (G \wedge H)) \to (F \to G)$	tautológia
3.	$F \to G$	Mp(1,2)

c) $\Sigma = \{F \to G, F \vee H\} \vdash G \vee H$

1.	$(F \to G) \to ((F \vee H) \to (G \vee H))$	tautológia
2.	$F \to G$	Σ-ban van
3.	$(F \vee H) \to (G \vee H)$	Mp(1,2)
4.	$F \vee H$	Σ-ban van
5.	$G \vee H$	Mp(3,4)

□

Most megmutatjuk a levezetés néhány tulajdonságát.

1.48. Tétel. (Dedukció tétel) *Tetszőleges Σ formula halmaz esetén $\Sigma \vdash F \to G$ akkor és csak akkor teljesül, ha $\Sigma \cup \{F\} \vdash G$.*

Bizonyítás. Először tegyük fel, hogy $\Sigma \vdash F \to G$. Akkor persze $\Sigma \cup \{F\} \vdash F \to G$ is teljesül. Másrészt $\Sigma \cup \{F\} \vdash F$, tehát a Mp alkalmazásával kapjuk, hogy $\Sigma \cup \{F\} \vdash G$.

Fordítva, legyen $G_1, \ldots, G_n$ egy $\Sigma \cup \{F\}$ feletti bizonyítás. Az n szerinti indukcióval megmutatjuk, hogy $\Sigma \vdash F \to G_n$.

(i) $n = 1$: Ekkor három esetet különböztetünk meg.

a) $G_n \in \Sigma$. Ekkor $\Sigma \vdash G_n$ és mivel $G_n \to (F \to G_n)$ tautológia, kapjuk, hogy $\Sigma \vdash F \to G_n$.

b) $G_n = F$. Mivel $F \to G_n$ tautológia, kapjuk, hogy $\Sigma \vdash F \to G_n$.

c) G_n tautológia. Akkor $F \to G_n$ is tautológia, tehát $\Sigma \vdash F \to G_n$.

(ii) n-ről $n+1$-re: Tegyük fel, hogy n-re igazoltuk az állítást és legyen $G_1, \ldots, G_{n+1}$ egy $\Sigma \cup \{F\}$ feletti bizonyítás. Most négy eset lehetséges.

a) $G_{n+1} \in \Sigma$, b) $G_{n+1} = F$, c) G_{n+1} tautológia: ekkor $\Sigma \vdash F \to G_{n+1}$ ugyanúgy, mint az $n = 1$ esetben.

d) van olyan $k, l \leqslant n$, hogy $G_l = G_k \to G_{n+1}$. Ekkor az indukciós feltevés szerint $\Sigma \vdash F \to G_k$ és $\Sigma \vdash F \to (G_k \to G_{n+1})$. Továbbá

$$(F \to G_k) \to ((F \to (G_k \to G_{n+1})) \to (F \to G_{n+1}))$$

egy tautológia, ezért a Mp kétszeri alkalmazásával kapjuk, hogy $\Sigma \vdash F \to G_{n+1}$. □

1.49. Következmény. (Dichotómia tétel) *Legyen Σ tetszőleges formulahalmaz. Ha $\Sigma \cup \{F\} \vdash G$ és $\Sigma \cup \{\neg F\} \vdash G$, akkor $\Sigma \vdash G$.*

Bizonyítás. A $\Sigma \cup \{F\} \vdash G$ feltételből és a 1.48. tételből kapjuk, hogy $\Sigma \vdash F \to G$. A $\Sigma \cup \{\neg F\} \vdash G$ feltételből hasonlóan következik, hogy $\Sigma \vdash \neg F \to G$. Továbbá

$$(F \to G) \to ((\neg F \to G) \to G)$$

tautológia, tehát a Mp szabály kétszeri alkalmazásával kapjuk, hogy $\Sigma \vdash G$. □

Egy formális bizonyítási módszertől azt várjuk el, hogy rendelkezzék a következő két tulajdonsággal.

1. Legyen helyes, vagyis csak az elmélethez tartozó formulákat lehessen bebizonyítani. Más szóval, ha $\Sigma \vdash F$, akkor $\Sigma \models F$.

2. Legyen teljes, vagyis minden, az elmélethez tartozó formulát be lehessen bizonyítani. Röviden, ha $\Sigma \models F$, akkor $\Sigma \vdash F$.

A kettő együtt a bevezetett bizonyítási módszer helyességét és teljességét kifejező tétel. A következőkben ezt a tételt szeretnénk igazolni.

A levezetés 1.45. definícióból valamit a 1.46. tételből azonnal adódik, hogy $\Sigma = \varnothing$ esetén mind a helyesség mind a teljesség fennáll. Valóban, ha $\Sigma = \varnothing$, akkor a 1.45. definíció 1. pontja soha nem teljesül, tehát csak tautológiából indulhatunk ki. Továbbá, a 1.46. tétel szerint a Mp megőrzi a tautológiákat, tehát $\varnothing$-ból csak tautológiákat vezethetünk le. Másrészt, a 1.45. definíció 2. pontja miatt, minden tautológia nyilvánvalóan levezethető $\varnothing$-ból.
A helyesség az általános esetben is viszonylag egyszerűen bizonyítható.

1.50. Tétel. (Helyességi tétel.) *Tetszőleges Σ és F esetén, ha $\Sigma \vdash F$, akkor $\Sigma \models F$.*

Bizonyítás. Megmutatjuk, hogy minden, Σ feletti $F_1, \ldots, F_n$ bizonyítás esetén $\Sigma \models F_n$. A bizonyítást n szerinti indukcióval végezzük.

(i) $n = 1$: Ekkor két lehetőség van: $F_n \in \Sigma$ vagy az, hogy F_n tautológia. Nyilvánvalóan mindkét esetben $\Sigma \models F_n$.

(ii) n-ről $n+1$-re: Legyen $F_1, \ldots, F_{n+1}$ egy Σ feletti bizonyítás. Ha $F_{n+1} \in \Sigma$ vagy F_{n+1} tautológia, akkor megint csak $\Sigma \models F_{n+1}$.

Különben van olyan $k, l \leqslant n$, hogy $F_l = F_k \to F_{n+1}$. Az indukciós feltevés szerint $\Sigma \models F_k$ és $\Sigma \models F_l = F_k \to F_{n+1}$, ezért a 1.46. tétel alkalmazásával kapjuk, hogy $\Sigma \models F_{n+1}$. □

A teljességet kétféleképpen bizonyítjuk.

A teljesség első bizonyítása

1.51. Tétel. (A teljességi tétel bizonyítása.) *Minden Σ-ra és F-re, ha $\Sigma \models F$, akkor $\Sigma \vdash F$.*

Bizonyítás. Tegyük fel, hogy $\Sigma \models F$. Az 1.42. tétel szerint a Σ-nak van olyan véges $\Sigma_0 = \{F_1, \ldots, F_n\}$ részhalamaza, melyre $\Sigma_0 \models F$. Ekkor, 1.6. tétel miatt $(F_1 \wedge \ldots \wedge F_n) \to F$ tautológia, amiből következik, hogy $F_1 \to (F_2 \to \ldots (F_n \to F) \ldots)$ szintén tautológia. Tekintsük a következő Σ_0 feletti bizonyítást.

1.	$F_1 \to (F_2 \to \ldots (F_n \to F) \ldots)$	tautológia
2.	F_1	Σ_0-ban van
3.	$F_2 \to (F_3 \ldots (F_n \to F) \ldots)$	Mp(1,2)
4.	F_2	Σ_0-ban van
⋮		
2n-1.	$F_n \to F$	Mp(2n-2,2n-3)
2n.	F_n	Σ_0-ban van
2n+1.	F	Mp(2n-1,2n)

Azt kaptuk tehát, hogy $\Sigma_0 \vdash F$, amiből következik, hogy $\Sigma \vdash F$, amit bizonyítani akartunk. □

A teljesség második bizonyítása

Ebben a második bizonyításban nem használjuk fel az 1.42. kompaktsági tételt. Helyette konzisztens formulahalmazokkal dolgozunk. Bebizonyítjuk a konzisztencia tételt, melynek következményeként kapjuk majd a teljességi tétel és a kompaktsági tétel egy másik bizonyítását, lásd 1.58. és 1.60. tételek.

1.52. Definíció. Egy Σ formulahalmaz konzisztens, ha nem vezethető le belőle a $\downarrow$. Továbbá egy konzisztens Σ formulahalmaz maximális, ha minden F formula esetén $F \in \Sigma$, vagy $\neg F \in \Sigma$.

Ha Σ nem konzisztens, akkor azt mondjuk, hogy inkonzisztens.

1.53. Lemma. Σ akkor és csakis akkor konzisztens, ha nem vezethető le belőle minden formula.

Bizonyítás. Ha Σ konzisztens, akkor nem vezethető le belőle a $\downarrow$.
Most tegyük fel, hogy Σ nem konzisztens és legyen F egy tetszőleges formula. Ekkor $\Sigma \vdash \downarrow$, mivel Σ nem konzisztens, továbbá $\downarrow \to F$ pedig egy tautológia. Így a Mp szabály alkalmazásával $\Sigma \vdash F$. □

1.54. Lemma. Legyen Σ egy konzisztens formulahalmaz. Akkor van olyan Σ^* maximális konzisztens formulahalmaz, melyre $\Sigma \subseteq \Sigma^*$.

Bizonyítás. Legyen $(F_i \mid i = 0, 1, \ldots)$ az összes formulák egy felsorolása. Definiáljuk a $\Sigma_0, \Sigma_1, \ldots$ sorozatot a következőképpen

(i) $\Sigma_0 = \Sigma$

(ii) Minden $n \geq 0$-ra legyen

$$\Sigma_{n+1} = \begin{cases} \Sigma_n \cup \{F_n\} & \text{ha } \Sigma_n \cup \{F_n\} \text{ konzisztens} \\ \Sigma_n \cup \{\neg F_n\} & \text{különben.} \end{cases}$$

Legyen továbbá $\Sigma^* = \bigcup_{n \geqslant 0} \Sigma_n$.
Azt állítjuk, hogy Σ^* maximális konzisztens. Az állítás igazolását három lépésben végezzük el.
1. lépés. n szerinti indukcióval megmutatjuk, hogy minden n-re a Σ_n konzisztens.

(i) $n = 0$ esetben a definíció miatt.

(ii) Tegyük fel, hogy Σ_n konzisztens. Azt kell megmutatni, hogy ha $\Sigma_n \cup \{F_n\}$ nem konzisztens, akkor $\Sigma_n \cup \{\neg F_n\}$ az. Tegyük fel, hogy $\Sigma_n \cup \{\neg F_n\}$ sem az. Akkor $\Sigma_n \cup \{F_n\} \vdash \downarrow$ és $\Sigma_n \cup \{\neg F_n\} \vdash \downarrow$, tehát a dichotómia tétel (1.49. következmény) szerint $\Sigma_n \vdash \downarrow$. Ez pedig nem lehet, mert Σ_n konzisztens.

2. lépés. Megmutatjuk, hogy Σ^* konzisztens. Ha ugyanis nem lenne az, akkor lenne olyan $G_1, \ldots, G_m$, Σ^* feletti bizonyítás, melyre $G_m = \downarrow$. Tehát lenne olyan n, hogy a $G_1, \ldots, G_m$ egyben Σ_n feletti bizonyítás is, ami azt jelentené, hogy Σ_n inkonzisztens. Ellentmondás, mert minden n-re Σ_n konzisztens.
3. lépés. Megmutatjuk, hogy Σ^* maximális. Ez abból következik, hogy $F_1, F_2, \ldots$ az összes formulák egy felsorolása volt, ezért minden F formula esetén van olyan n, melyre $F = F_n$. Továbbá Σ^* definiciója szerint $F_n \in \Sigma^*$, vagy $\neg F_n \in \Sigma^*$. □
Szükségünk lesz még a következő állításra.

1.55. Lemma. Legyen Σ maximális konzisztens. Ha $\Sigma \vdash F$, akkor $F \in \Sigma$.

Bizonyítás. Indirekt bizonyítást adunk, ezért feltesszük, hogy $\Sigma \vdash F$ és $F \notin \Sigma$. Mivel Σ maximális, ezért $\neg F \in \Sigma$, tehát $\Sigma \vdash F$ és $\Sigma \vdash \neg F$. Mivel $F \to (\neg F \to \downarrow)$ tautológia, a Mp kétszeri alkalmazásával kapjuk, hogy $\Sigma \vdash \downarrow$, tehát Σ nem konzisztens. Ez viszont ellentmondás, tehát az állítás igaz. □

Megjegyezzük, hogy természetesen a fenti lemma megfordítása is érvényes.

1.56. Tétel. *Legyen Σ egy maximális konzisztens formulahalmaz. Akkor Σ kielégíthető.*

Bizonyítás. Először bebizonyítjuk az (a)–(c) állításokat.

(a) Minden F formula esetén $F \in \Sigma$ akkor és csak akkor teljesül, ha $\neg F \notin \Sigma$.

Mivel Σ maximális, $F \in \Sigma$ vagy $\neg F \in \Sigma$. Tehát csak azt kell megmutatni, hogy $F \in \Sigma$ és $\neg F \in \Sigma$ egyszerre nem teljesülhet. Ez azonban nyilvánvaló, mert Σ konzisztens.

(b) Minden F, G-re $F \wedge G \in \Sigma$ akkor és csak akkor teljesül, ha $F \in \Sigma$ és $G \in \Sigma$.

Először tegyük fel, hogy $F \wedge G \in \Sigma$. Ekkor $\Sigma \vdash F \wedge G$ és mivel $F \wedge G \to F$ tautológia, kapjuk, hogy $\Sigma \vdash F$. Így a 1.55. lemma értelmében $F \in \Sigma$. Hasonlóan kapható, hogy $G \in \Sigma$.

Fordítva, tegyük fel, hogy $F, G \in \Sigma$. Ekkor $\Sigma \vdash F$ és $\Sigma \vdash G$. Másrészt, $F \to (G \to (F \wedge G))$ tautológia, tehát az Mp kétszeri alkalmazásával $\Sigma \vdash F \wedge G$. Így ismét a 1.55. lemma miatt $F \wedge G \in \Sigma$.

(c) Minden F, G -re $F \vee G \in \Sigma$ akkor és csak akkor teljesül, ha $F \in \Sigma$ vagy $G \in \Sigma$.

Tegyük fel, hogy $F \vee G \in \Sigma$. Ekkor nyilván $\Sigma \vdash F \vee G$. Ha $F \in \Sigma$, akkor készen vagyunk. Ha $F \notin \Sigma$, akkor $\neg F \in \Sigma$, mivel Σ maximális, és így $\Sigma \vdash \neg F$. Továbbá $\neg F \to ((F \vee G) \to G)$ tautológia, tehát a Mp kétszeri alkalmazásával $\Sigma \vdash G$. Végül a 1.55. lemma értelmében $G \in \Sigma$.

Fordítva, tegyük fel, hogy $F \in \Sigma$ vagy $G \in \Sigma$. Akkor $\Sigma \vdash F$ vagy $\Sigma \vdash G$. Mivel mind $F \to (F \vee G)$ mind $G \to (F \vee G)$ tautológia, mindkét esetben $\Sigma \vdash (F \vee G)$ tehát a 1.55. lemma értelmében $F \vee G \in \Sigma$.

Most megmutatjuk, hogy Σ kielégíthető. Kétféle bizonyítás is adható. Az elsőben megadunk egy $\mathcal{A}$ hozzárendelést amely kielégíti Σ-t. A másodikban megmutatjuk, hogy Σ Hintikka halmaz, amiből a 1.35. lemma szerint azonnal adódik, hogy Σ kielégíthető.

1) bizonyítás: Legyen $\mathcal{A} : Var \to \{0, 1\}$ a következő hozzárendelés. Minden $p \in Var$-ra

$$\mathcal{A}(p) = 1 \iff p \in \Sigma.$$

Ekkor a formulák felépítése szerinti indukcióval megmutatható, hogy minden F formula esetén

$$\mathcal{A}(F) = 1 \iff F \in \Sigma.$$

(i) Ha $F = p$, akkor az állítás definíció szerint teljesül.

(ii) Ha $F = \neg G$, akkor a következő számolás adódik.
$\mathcal{A}(F) = 1 \iff \mathcal{A}(G) = 0 \iff G \notin \Sigma \iff \neg G = F \in \Sigma$

(iii) Ha $F = G \wedge H$, akkor kapjuk, hogy

$$\begin{aligned} \mathcal{A}(F) = 1 &\iff \mathcal{A}(G) = 1 \text{ és } \mathcal{A}(H) = 1 \\ &\iff G \in \Sigma \text{ és } H \in \Sigma \\ &\iff F = G \wedge H \in \Sigma. \end{aligned}$$

(iv) Ha $F = G \vee H$, akkor a bizonyítás hasonló az előbbi esethez.

2) bizonyítás: Megmutatjuk, hogy Σ Hintikka halmaz. A Hintikka halmaz definíciójának (1.34. definíció) 1. feltétele a jelen bizonyításban szereplő (a) feltétel miatt teljesül.

Most bebizonyítjuk, hogy a 1.34. definíció 2. feltétele is teljesül. Legyen F egy α-formula, mondjuk $F = \neg(F_1 \vee F_2)$ és tegyük fel, hogy $F \in \Sigma$. Akkor az (a) feltétel miatt $F_1 \vee F_2 \notin \Sigma$. A

(c) feltétel miatt $F_1 \notin \Sigma$ és $F_2 \notin \Sigma$, majd újra az (a) feltétel miatt $\neg F_1 \in \Sigma$ és $\neg F_2 \in \Sigma$. Tehát ez esetben teljesül a 1.34. definíció 2. feltétele. A másik két α-formulára a bizonyítás hasonlóan megy.

Végül bebizonyítjuk, hogy a 1.34. definíció 3. feltétele is teljesül. Legyen evégett F egy β-formula, mondjuk $F = \neg(F_1 \wedge F_2)$ és tegyük fel, hogy $F \in \Sigma$. Akkor az (a) feltétel miatt $F_1 \wedge F_2 \notin \Sigma$. A (b) feltétel miatt $F_1 \notin \Sigma$ vagy $F_2 \notin \Sigma$, majd újra az (a) feltétel miatt $\neg F_1 \in \Sigma$ vagy $\neg F_2 \in \Sigma$. Tehát ez esetben is teljesül a 1.34. definíció 2. feltétele. A másik β-formulára a bizonyítás hasonlóan végezhető.

□

1.57. Tétel. (A konzisztencia tétel.) *Tetszőleges Σ formulahalmaz akkor és csak akkor konzisztens, ha kielégíthető.*

Bizonyítás. Tegyük fel, hogy Σ konzisztens. Akkor a 1.54. lemma miatt van olyan Σ^* maximális konzisztens formula halmaz, melyre $\Sigma \subseteq \Sigma^*$. A 1.56. tétel miatt van olyan $\mathcal{A}$ hozzárendelés, melyre $\mathcal{A} \models \Sigma^*$ és így $\mathcal{A} \models \Sigma$.

Fordítva, tegyük fel, hogy valamely $\mathcal{A}$ hozzárendelés esetén $\mathcal{A} \models \Sigma$. Ha most Σ inkonzisztens, akkor $\Sigma \vdash \downarrow$, tehát a 1.50. tétel miatt $\Sigma \models \downarrow$. Így $\mathcal{A} \models \downarrow$, ami ellentmondás. □

Most már be tudjuk bizonyítani a teljességi tételt.

1.58. Tétel. (A teljességi tétel második bizonyítása.) *Minden Σ-ra és F-re, ha $\Sigma \models F$, akkor $\Sigma \vdash F$.*

Bizonyítás. Tegyük fel, hogy $\Sigma \models F$. Akkor $\Sigma \cup \{\neg F\}$ kielégíthetetlen és ezért a 1.57. tétel miatt $\Sigma \cup \{\neg F\}$ inkonzisztens. Ekkor $\Sigma \cup \{\neg F\} \vdash \downarrow$, tehát a 1.48. tétel miatt $\Sigma \vdash \neg F \rightarrow \downarrow$. Továbbá $(\neg F \rightarrow \downarrow) \rightarrow F$ egy tautológia, és így a Mp alkalmazásával kapjuk, hogy $\Sigma \vdash F$. □

Ezzel igazoltuk, hogy a bizonyítási rendszerünk helyes és teljes.

1.59. Tétel. *Tetszőleges Σ formulahalmaz és F formula esetén $\Sigma \models F$ akkor és csakis akkor teljesül, ha $\Sigma \vdash F$.*

Bizonyítás. A szükségesség következik az 1.50. (helyességi) tételből, míg az elegendőség következik az 1.51. (vagy az 1.58.) (teljességi) tételből. □

Végül kimondjuk a konzisztencia tétel egy másik fontos következményét.

1.60. Tétel. (Kompaktsági tétel második bizonyítás.) *Legyen Σ tetszőleges formulahalmaz. Σ akkor és csak akkor elégíthető ki, ha minden véges részhalmaza kielégíthető.*

Bizonyítás. Ha Σ kielégíthető, akkor minden véges részhalmaza is kielégíthető.

Megfordítva, tegyük fel, hogy Σ minden véges részhalmaza kielégíthető (és így a 1.57. tétel miatt konzisztens). Ha ekkor Σ nem elégíthető ki, akkor ugyancsak a 1.57. tétel miatt Σ nem konzisztens. Akkor $\Sigma \vdash \downarrow$, tehát van $F_1, \ldots, F_n = \downarrow$ bizonyítás Σ felett. Akkor viszont a bizonyítás definíciója miatt van olyan véges $\Sigma' \subseteq \Sigma$, melyre $F_1, \ldots, F_n = \downarrow$ a Σ' feletti bizonyítás is. Tehát Σ' inkonzisztens, ami ellentmondás. □

Bizonyítás axiómákkal

Vannak olyan bizonyítási rendszerek, melyeknél a levezetésbe nem írhatunk be tetszőlges tautológiát, hanem csak bizonyos kitüntetett alakú és véges számú tautológiát (amelyeket axiómáknak nevezünk). Az ilyen esetekben formulán csak olyan formulát értünk, melyben

csak olyan műveleti jelek szerepelnek, amyelek az axiómákban is szerepelnek. Elvárható tehát, hogy az axiómákban szereplő műveletek adekvát halmazt alkossanak.

Most ismertetünk egy ilyen bizonyítási rendszert, amely $\mathcal{H}$ bizonyítási rendszernek nevezünk. A $\mathcal{H}$ rendszerben három axióma van. Továbbá, amikor a $\mathcal{H}$ rendszerről beszélünk, akkor formulán olyan formulát értünk, melyben csak az adekvát halmazt alkotó $\{\neg, \rightarrow\}$ műveleti jelek szerepelnek.

Axiómák Minden F, G és H formula esetén az

$$\begin{array}{lll} \text{AX1} & : & F \rightarrow (G \rightarrow F) \\ \text{AX2} & : & (F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H)) \\ \text{AX3} & : & (\neg F \rightarrow \neg G) \rightarrow ((\neg F \rightarrow G) \rightarrow F) \end{array}$$

formulák axiómák.

Mivel F, G és H tetszőleges formulák lehetnek, AX1, AX2 és AX3 mindegyike végtelen sok axiómát jelent. Könnyen igazolható, hogy mindegyik axióma érvényes.

1.61. Definíció. (A bizonyítás definíciója a $\mathcal{H}$ rendszerben.) Legyen Σ formulák egy halmaza. Egy $F_1, \ldots, F_n$ sorozatot Σ-ból történő (vagy Σ feletti) bizonyításnak nevezünk, ha minden $1 \leq i \leq n$ esetén az alábbi feltételek valamelyike teljesül:

1. $F_i \in \Sigma$,
2. F_i axióma,
3. Van olyan $k, l < i$, hogy $F_l = F_k \rightarrow F_i$ (Modus ponens).

Egy F formula bebizonyítható (vagy levezethető) Σ-ból, jele: $\Sigma \vdash_{\mathcal{H}} F$, ha van olyan Σ feletti $F_1, \ldots, F_n$ bizonyítás, melyre $F_n = F$.

Belátható, hogy ez a bizonyítási rendszer is helyes és teljes, mint ahogy azt az alábbi tétel kimondja.

1.62. Tétel. *Minden Σ-ra és F-re $\Sigma \vdash_{\mathcal{H}} F$ akkor és csakis akkor teljesül, ha $\Sigma \models F$.*

Bizonyítás. a) Helyesség: Mivel az axiómák tautológiák, ha $\Sigma \vdash_{\mathcal{H}} F$, akkor egyben $\Sigma \vdash F$ is, tehát a 1.50. tétel szerint $\Sigma \models F$.

b) Teljeség: Ha azt be tudjuk bizonyítani, hogy minden F tautológia esetén $\vdash_{\mathcal{H}} F$ (azaz $\varnothing \vdash_{\mathcal{H}} F$), akkor készen vagyunk. Ez esetben ugyanis a 1.45. definícióban szereplő 2. feltétel helyettesíthető egy AX1, AX2 és AX3-ból kiinduló $\mathcal{H}$-bizonyítással, tehát $\Sigma \vdash_{\mathcal{H}} F$ akkor és csakis akkor, ha $\Sigma \vdash F$. Így a 1.58. tételből a $\mathcal{H}$ rendszer teljessége is adódik. A teljes bizonyítást elhagyjuk.

□

Megadunk néhány további axiómarendszert, melyekkel való levezetés helyes és teljes (az axiómákban szereplő műveleti jeleket tartalmazó formulák körében). A helyességet és teljességet nem bizonyítjuk.

1)

$$\begin{array}{lll} \text{AX1} & : & (F \vee F) \rightarrow F \\ \text{AX2} & : & F \rightarrow (F \vee G) \\ \text{AX3} & : & (F \rightarrow G) \rightarrow ((H \vee F) \rightarrow (H \vee G)) \\ \text{AX4} & : & (F \vee G) \rightarrow (G \vee F) \end{array}$$

2)

AX1 : $F \to (F \wedge F)$
AX2 : $(F \wedge G) \to F$
AX3 : $(F \to G) \to (\neg(G \wedge H) \to \neg(H \wedge F))$

3)

AX1 : $F \to (G \to F)$
AX2 : $(F \to (G \to H)) \to ((F \to G) \to (F \to H))$
AX3 : $\neg F \to (F \to G)$
AX4 : $(\neg F \to F) \to F$

4)

AX1 : $F \to (G \to F)$
AX2 : $(F \to (G \to H)) \to ((F \to G) \to (F \to H))$
AX3 : $(\neg G \to \neg F) \to (F \to G)$

1.7.2. Gentzen típusú bizonyítások

Legyen Γ egy formulahalmaz, F pedig egy formula. Ebben a fejezetben a $\Gamma \cup \{F\}$ alakú kifejezések helyett Γ, F -et írunk.

A $\mathcal{G}_u$ kalkulus

A $\mathcal{G}_u$ kalkulusban az bizonyítható be, hogy egy Γ formulahalmaz kielégíthetetlen. Emlékeztetőül: Γ akkor kielégíthetetlen, ha nincs modellje, vagyin minden $\mathcal{A}$ hozzárendeléshez vagy egy olyan $F \in \Gamma$, melyre $\mathcal{A} \not\models F$.

Az ilyen típusú bizonyítást *cáfolati bizonyításnak* nevezzük.

A cáfolati bizonyítások az $\{F_1, \ldots, F_n\} \models G$ típusú állítások igazolására használhatók. Mivel tudjuk, hogy $\{ F_1, \ldots, F_n \} \models G$ akkor és csak akkor teljesül, ha $\{ F_1, \ldots, F_n, \neg G \}$ kielégíthetetlen, elegendő azt igazolni, hogy $\{ F_1, \ldots, F_n, \neg G \}$ kielégíthetetlen.

A $\mathcal{G}_u$ kalkulus a következőkből áll.

Axiómák Formulák minden olyan véges Γ halmaza, melyre $p, \neg p \in \Gamma$ valamely $p \in Var$ esetén.

Tehát az axiómák kielégíthetetlenek.

Következtetési szabályok

(1) a $\neg\neg$ - szabály $\dfrac{\Gamma, F}{\Gamma, \neg\neg F}$

(2) az $\wedge$ - szabály $\dfrac{\Gamma, F, G}{\Gamma, F \wedge G}$

(3) a $\neg\vee$ - szabály $\dfrac{\Gamma, \neg F, \neg G}{\Gamma, \neg(F \vee G)}$

(4) a $\vee$ - szabály $\dfrac{\Gamma, F \qquad \Gamma, G}{\Gamma, F \vee G}$

(5) a $\neg\wedge$ - szabály $\qquad \dfrac{\Gamma, \neg F \qquad \Gamma, \neg G}{\Gamma, \neg(F \wedge G)}$

Most megadjuk a $\mathcal{G}_u$ - beli bizonyítás definícióját.

1.63. Definíció. (A bizonyítás definíciója a $\mathcal{G}_u$ rendszerben.) $\mathcal{G}_u$-beli bizonyításnak nevezünk egy olyan $\Gamma_1, \ldots, \Gamma_n$ sorozatot, ahol bármely $1 \leq i \leq n$-re az alábbi feltételek valamelyike teljesül

1. Γ_i axióma,
2. van olyan $k < i$, hogy Γ_i a Γ_k-ból kapható az (1), (2) vagy (3) szabályok valamelyikének az alkalmazásával,
3. van olyan $k, l < i$, hogy Γ_i a Γ_k-ból és Γ_l-ből kapható a (4) vagy (5) szabályok valamelyikének az alkalmazásával.

□

Például, a 2. pontban a (3) szabály alkalmazása azt jelenti, hogy $\Gamma_k = \Gamma \cup \{\neg F, \neg G\}$ és $\Gamma_i = \Gamma \cup \{\neg(F \vee G)\}$. Vagy, a 3. pontban a (4) szabály alkalmazása azt jelenti, hogy $\Gamma_k = \Gamma \cup \{F\}$, $\Gamma_l = \Gamma \cup \{G\}$ és $\Gamma_i = \Gamma \cup \{F \vee G\}$.

Formulák egy véges Γ halmazának $\mathcal{G}_u$-beli bizonyításán egy olyan $\Gamma_1, \ldots, \Gamma_n$ $\mathcal{G}_u$-beli bizonyítást értünk, melyre $\Gamma_n = \Gamma$. Ha Γ bebizonyítható $\mathcal{G}_u$ -ban, akkor azt úgy jelöljük, hogy $\vdash_{\mathcal{G}_u} \Gamma$.

Most belátjuk, hogy $\mathcal{G}_u$-ban pontosan a kielégíthetetlen formulahalmazok bizonyíthatók be.

1.64. Tétel. *Teteszőleges Γ formulahalmaz esetén $\vdash_{\mathcal{G}_u} \Gamma$ akkor és csakis akkor teljesül, ha Γ kielégíthetetlen.*

Bizonyítás. Vegyük észre a következőket.

(a) $\mathcal{G}_u$ axiómái nem mások mint a 1.5 alfejezeben, a tabló módszernél megismert szemantikus tabló zárt levelei.

(b) $\mathcal{G}_u$ következtetési szabályai nem mások, mint a tabló módszernél alkalmazott α és β szabályok "fordított módon" történő alkalmazásai. Nevezetesen az (1)–(3) szabályok az α szabályoknak, a (4)–(5) szabályok a β-szabályoknak felelnek meg.

Mindebből az következik, hogy egy Γ formulahalmaz akkor és csak akkor bizonyítható be $\mathcal{G}_u$-ban, ha Γ-nak van egy zárt szemantikus tablója. Ez utóbbi viszont a 1.39. tétel szerint akkor és csakis akkor áll fenn, ha Γ kielégíthetetlen. (A tétel formulahalmazra ugyanúgy vezethető le, mint formulára.)

Azt kaptuk, hogy $\vdash_{\mathcal{G}_u} \Gamma$ akkor és csakis akkor, ha Γ kielégíthetetlen. □

Valójában egy $\mathcal{G}_u$-beli bizonyítás nem más, mint a szematikus tabló szögpontjainak egy lineáris rendezése.

A $\mathcal{G}_t$ kalkulus

Most bevezetünk egy olyan kalkulust, a $\mathcal{G}_t$ kalkulust, melyben az bizonyítható be, hogy egy F formula tautológia.

A $\mathcal{G}_t$ kalkulus a következőkből áll.

Axiómák Formulák minden olyan véges Γ halmaza, melyre $p, \neg p \in \Gamma$ valamely $p \in Var$ esetén.

Tehát az axiómák tautológiák.

Következtetési szabályok

(1) a $\neg\neg$ - szabály $\dfrac{\Gamma, F}{\Gamma, \neg\neg F}$

(2) a $\wedge$ - szabály $\dfrac{\Gamma, F \qquad \Gamma, G}{\Gamma, F \wedge G}$

(3) a $\neg\vee$ - szabály $\dfrac{\Gamma, \neg F \qquad \Gamma, \neg G}{\Gamma, \neg(F \vee G)}$

(4) a $\vee$ - szabály $\dfrac{\Gamma, F, G}{\Gamma, F \vee G}$

(5) az $\neg\wedge$ - szabály $\dfrac{\Gamma, \neg F, \neg G}{\Gamma, \neg(F \wedge G)}$

Most megadjuk a $\mathcal{G}_t$ - beli bizonyítás definícióját is.

1.65. Definíció. (A bizonyítás definíciója a $\mathcal{G}_t$ rendszerben.) $\mathcal{G}_t$ - beli bizonyításnak nevezünk egy olyan $\Gamma_1, \ldots, \Gamma_n$ sorozatot, ahol bármely $1 \leq i \leq n$-re az alábbi feltételek valamelyike teljesül

1. Γ_i axióma,
2. van olyan $k < i$, hogy Γ_i a Γ_k-ból kapható az (1), (4) vagy (5) szabályok valamelyikének az alkalmazásával,
3. van olyan $k, l < i$, hogy Γ_i a Γ_k-ból és Γ_l-ből kapható a (2) vagy (3) szabályok valamelyikének az alkalmazásával.

Formulák egy véges Γ halmazának $\mathcal{G}_t$-beli bizonyításán egy olyan $\Gamma_1, \ldots, \Gamma_n$ $\mathcal{G}_t$-beli bizonyítást értünk, melyre $\Gamma_n = \Gamma$. Ha Γ bebizonyítható $\mathcal{G}_t$ -ban, akkor azt úgy jelöljük, hogy $\vdash_{\mathcal{G}_t} \Gamma$.

Most megmutatjuk, hogy ez milyen összefüggést eredményez a $\mathcal{G}_u$ és a $\mathcal{G}_t$ rendszerek között. Evégett definiáljuk a formula komplemensét.

1.66. Definíció. Tetszőleges F formula esetén F komplemensét $\overline{F}$-fel jelöljük és az alábbi módon indukcióval definiáljuk:

(i) $\overline{\neg^{2k}p} = \neg^{2k+1}p$, minden $k \geq 0$-ra, ahol $\neg^0 p = p$,

(ii) $\overline{\neg^{2k+1}p} = \neg^{2k}p$, minden $k \geq 0$-ra,

(iii) $\overline{\neg G} = \neg\overline{G}$, ha $G \neq \neg^k p$ semmilyen $k \geq 0$-ra,

(iv) $\overline{G \vee H} = \overline{G} \wedge \overline{H}$,

(v) $\overline{G \wedge H} = \overline{G} \vee \overline{H}$.

Továbbá, ha Γ egy formulahalmaz, akkor $\overline{\Gamma} = \{\overline{F} \mid F \in \Gamma\}$.

□

Igazolható, hogy $\overline{F} \equiv \neg F$ és $\overline{\overline{F}} = F$. Az előbbiből következik, hogy egy F formula akkor és csak akkor érvényes, ha $\overline{F}$ kielégíthetetlen.

Igazolható, hogy a $\mathcal{G}_t$ rendszer a $\mathcal{G}_u$ rendszer egyfajta duálisa. Nevezetesen, a $\mathcal{G}_t$ rendszer (2), (3), (4) és (5) szabályai rendre a $\mathcal{G}_u$ rendszer (4), (5), (2) és (3) szabályaiból kaphatók olyan módon, hogy a megfelelő szabályok premissza és konklúzió részében lévő formulákat és halmazokat a komplemenseikkel helyettesítjük.

1.67. Tétel. *Tetszőleges Γ formulahalmaz esetén $\vdash_{\mathcal{G}_u} \Gamma$ akkor és csakis akkor teljesül, ha $\vdash_{\mathcal{G}_t} \overline{\Gamma}$.*

Bizonyítás. Először azt mutatjuk meg, hogy minden $\mathcal{G}_u$-beli $\Gamma_1, \ldots, \Gamma_n$ bizonyítás esetén $\vdash_{\mathcal{G}_t} \overline{\Gamma}_n$. n szerinti idukcióval haladunk tovább.

Tegyük fel tehát, hogy $\Gamma_1, \ldots, \Gamma_n$ egy $\mathcal{G}_u$-beli bizonyítás.

(i) $n = 1$: Ekkor Γ_1 egy $\mathcal{G}_u$-beli axióma, vagyis olyan véges formulahalmaz, amely tartalmaz legalább egy $p, \neg p$ párt. Következésképpen $\overline{\Gamma}_1$ tartalmazza a $\neg p, p$ párt, tehát $\overline{\Gamma}_1$ egy $\mathcal{G}_t$-beli axióma. Kapjuk, hogy $\vdash_{\mathcal{G}_t} \overline{\Gamma}_1$.

(ii) n-ről $n+1$-re: Legyen $\Gamma_1, \ldots, \Gamma_{n+1}$ egy $\mathcal{G}_u$-beli bizonyítás.

Ha Γ_{n+1} axióma, akkor $\vdash_{\mathcal{G}_t} \overline{\Gamma}_{n+1}$, ugyanúgy mint az $n = 1$ esetben.

Ha Γ_{n+1} nem axióma, akkor a $\mathcal{G}_u$-beli (1)–(5) szabályok valamelyikének az alkalmazásával kaptuk. Csak az (5) szabály alkalmazásával adódó esettel foglalkozunk részeletesen, a többi eset hasonlóan igazolható. Ekkor van olyan $k, l < n+1$, hogy $\Gamma_k = \Sigma \cup \{\neg F\}$, $\Gamma_l = \Sigma \cup \{\neg G\}$ és $\Gamma_{n+1} = \Sigma \cup \{\neg(F \wedge G)\}$. Az indukciós feltevés miatt $\vdash_{\mathcal{G}_t} \overline{\Sigma} \cup \{\overline{\neg F}\}$ és $\vdash_{\mathcal{G}_t} \overline{\Sigma} \cup \{\overline{\neg F}\}$. Akkor a $\mathcal{G}_t$-beli (3) szabály alkalmazásával $\vdash_{\mathcal{G}_t} \overline{\Sigma} \cup \{\neg(\overline{F} \vee \overline{G})\}$.

Mivel

$$\overline{\neg(F \wedge G)} = \neg(\overline{F \wedge G}) = \neg(\overline{F} \vee \overline{G}),$$

kapjuk, hogy $\vdash_{\mathcal{G}_t} \overline{\Gamma}_{n+1}$.

A fordított irányt úgy igazoljuk, hogy minden $\mathcal{G}_t$-beli $\Gamma_1, \ldots, \Gamma_n = \overline{\Gamma}$ bizonyítás esetén $\vdash_{\mathcal{G}_u} \Gamma$.

(i) $n = 1$: Ekkor Γ_1 egy $\mathcal{G}_t$-beli axióma. Mivel $\overline{\Gamma} = \Gamma_1$, a Σ is axióma és ezért $\vdash_{\mathcal{G}_u} \Gamma$.

(ii) n-ről $n+1$-re: Legyen $\Gamma_1, \ldots, \Gamma_{n+1}$ egy $\mathcal{G}_t$-beli bizonyítás.

Ha Γ_{n+1} axióma, akkor ugyanúgy járunk el, mint az $n = 1$ esetben.

Ha Γ_{n+1} nem axióma, akkor a $\mathcal{G}_t$-beli (1)–(5) szabályok valamelyikének az alkalmazásával kaptuk. Csak az (4) szabály alkalmazásával adódó esettel foglalkozunk részeletesen, a többi eset hasonlóan igazolható. Ekkor van olyan $k < n+1$, hogy $\Gamma_k = \overline{\Sigma} \cup \{\overline{F}, \overline{G}\}$ és $\Gamma_{n+1} = \overline{\Sigma} \cup \{\overline{F} \vee \overline{G}\}$. Továbbá, a $\overline{\Sigma} = \Gamma_{n+1}$ miatt $\Gamma_{n+1} = \Sigma \cup \{F \wedge G\}$.

Az indukciós feltevés miatt $\vdash_{\mathcal{G}_u} \Sigma \cup \{F, G\}$. Akkor a $\mathcal{G}_u$-beli (2) szabály alkalmazásával $\vdash_{\mathcal{G}_u} \Sigma \cup \{F \wedge G\} = \Gamma_{n+1}$. □

1.68. Következmény. Tetszőleges F formula esetén $\vdash_{\mathcal{G}_t} F$ akkor és csak akkor teljesül, ha F tautológia.

Bizonyítás. Legyen F egy formula. Akkor

$$\begin{array}{lll} & \vdash_{\mathcal{G}_t} F & \\ \Longleftrightarrow & \vdash_{\mathcal{G}_u} \overline{F} & \text{(1.67. tétel)} \\ \Longleftrightarrow & \overline{F} \text{ kielégíthetetlen} & \text{(1.64. tétel)} \\ \Longleftrightarrow & F \text{ tautológia.} & \end{array}$$

□

!!!!!!!!!!!!!!!!!!!!!!!!!!!! Nem kell !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

A $\mathcal{G}$ kalkulus

1.69. Definíció. Legyen Σ és Γ két formulahalmaz. Azt mondjuk, hogy Γ logikai következménye Σ -nak, jele $\Sigma \models \Gamma$, ha minden $\mathcal{A}$ hozzárendelés esetén, ha $\mathcal{A} \models \Sigma$, akkor Γ -ban van legalább egy olyan F formula, melyre $\mathcal{A} \models$ F.

A $\mathcal{G}$ kalkulusban olyan típusú állításokat tudunk bebizonyitani, hogy $\Sigma \models \Gamma$.

1.70. Definíció. Egy Σ formulahalmaz tautológia, ha minden $\mathcal{A}$ hozzárendelés esetén van egy olyan $F \in \Sigma$, melyre $\mathcal{A} \models$ F.

Tulajdonságok

(a) Amennyiben Σ és Γ csak változókból áll, úgy $\Sigma \models \Gamma$ akkor és csak akkor áll fenn, ha van olyan $p \in Var$, melyre $p \in \Sigma$ és $p \in \Gamma$.

(b) Tetszőleges $F_1, \ldots, F_n, G_1, \ldots, G_m$ formulák esetén a következő állítások ekvivalensek

1, $\{F_1, \ldots, F_n\} \models \{G_1, \ldots, G_m\}$

2, $\{\neg F_1, \ldots, \neg F_n, G_1, \ldots, G_m\}$ tautológia

3, $\{F_1, \ldots, F_n, \neg G_1, \ldots, \neg G_m\}$ kielégíthetetlen

4, $\{F_1 \wedge \ldots \wedge F_n\} \to \{G_1 \vee \ldots \vee G_m\}$ tautológia

A továbbiakban $\Sigma \models \Gamma$ helyett $\Sigma \Rightarrow \Gamma$ -t írunk.
Axiómák Minden $\Sigma \Rightarrow \Gamma$ pár, amelyre van olyan $p \in Var$, hogy $p \in \Sigma$ és $p \in \Gamma$.

Következtetési szabályok

(1) $\neg$- szabályok $\dfrac{\Sigma \Rightarrow \Gamma, F}{\Sigma, \neg F \Rightarrow \Gamma}$ $\qquad$ $\dfrac{\Sigma, F \Rightarrow \Gamma}{\Sigma \Rightarrow \Gamma, \neg F}$

(2) $\vee$- szabályok $\dfrac{\Sigma \Rightarrow \Gamma, F, G}{\Sigma \Rightarrow \Gamma, F \vee G}$ $\qquad$ $\dfrac{\Sigma, F \Rightarrow \Gamma \qquad \Sigma, G \Rightarrow \Gamma}{\Sigma, F \vee G \Rightarrow \Gamma}$

(3) $\wedge$- szabályok $\dfrac{\Sigma \Rightarrow \Gamma, F \qquad \Sigma \Rightarrow \Gamma, G}{\Sigma \Rightarrow \Gamma, F \wedge G}$ $\qquad$ $\dfrac{\Sigma, F, G \Rightarrow \Gamma}{\Sigma, F \wedge G \Rightarrow \Gamma}$

1.71. Definíció. (A bizonyítás definíciója.) $\mathcal{G}$-beli bizonyításnak nevezünk egy $\Sigma_1 \Rightarrow \Gamma_1, \ldots, \Sigma_n \Rightarrow \Gamma_n$ sorozatot, ahol minden $1 \leq i \leq n$-re

(i) $\Sigma_i \Rightarrow \Gamma_i$ egy axióma vagy

(ii) $\Sigma_i \Rightarrow \Gamma_i$ -t valamely következtetési szabállyal kapjuk őt megelőző pár(ok)ból.

Tetszőleges, véges Σ és Γ esetén a $\Sigma \Rightarrow \Gamma$ bebizonyítható $\mathcal{G}$-ben, ha van olyan $\Sigma_1 \Rightarrow \Gamma_1, \ldots, \Sigma_n \Rightarrow \Gamma_n$ $\mathcal{G}$-beli bizonyítás, melyre $\Sigma_n \Rightarrow \Gamma_n = \Sigma \Rightarrow \Gamma$. Ekkor azt írjuk, hogy $\mathcal{G} \vdash \Sigma \Rightarrow \Gamma$.

A $\mathcal{G}$-beli bizonyítás teljességének igazolásához először megállapítjuk a következtetési szabályok egy fontos tulajdonságát.

1.72. Tétel.

1. $\Sigma \models \Gamma, F \iff \Sigma, \neg F \models \Gamma$
2. $\Sigma, F \models \Gamma \iff \Sigma \models \Gamma, \neg F$
3. $\Sigma \models \Gamma, F, G \iff \Sigma \models \Gamma, F \vee G$
4. $\Sigma, F \vee G \models \Gamma \iff \Sigma, F \models \Gamma$ *és* $\Sigma, G \models \Gamma$
5. $\Sigma \models \Gamma, F \wedge G \iff \Sigma \models \Gamma, F$ *és* $\Sigma \models \Gamma, G$
6. $\Sigma, F \wedge G \models \Gamma \iff \Sigma, F, G \models \Gamma$.

Bizonyítás. Triviális.

Ezután be tudjuk bizonyítani a $\mathcal{G}$ bizonyítási rendszer helyességét és teljességét.

1.73. Tétel. $\mathcal{G} \vdash \Sigma \Rightarrow \Gamma$ *akkor és csak akkor, ha* $\Sigma \models \Gamma$.

Bizonyítás. Hasonlóan a $\mathcal{G}_u$ esethez.

1.74. Következmény.

(a) $\mathcal{G} \vdash \{F_1, \ldots, F_n\} \Rightarrow G \iff \{F_1, \ldots, F_n\} \models G$.

(b) $\mathcal{G} \vdash \emptyset \Rightarrow F \iff \emptyset \models F \iff F$ tautológia.

□

!!

1.7.3. Bizonyítás rezolúcióval

Ebben a fejezetben egy olyan módszert adunk meg, mellyel az bizonyítható be, hogy egy konjunktív normálforma nem kielégíthető. Tehát megint egy cáfolati bizonyításról van szó, amely az $\{F_1, \ldots, F_n\} \models G$ alakú állítások bizonyítására használható.

Ha F egy konjunktív normálforma, akkor $F = (\ell_{11} \vee \ldots \vee \ell_{1,n_1}) \wedge \ldots \wedge (\ell_{k1} \vee \ldots \vee \ell_{k,n_k})$, ahol az ℓ_{ij}-k literálok.

Az $\ell_{i1} \vee \ldots \vee \ell_{i,n_i}$ diszjunkciós tagokat *klózoknak* nevezzük. Egy klóz pozitív, ha csak pozitív literálokból áll és negatív ha csak negatív literálokból áll.

Üres klóznak nevezzük azt a klózt, amelynek nincs egyetlen diszjunkciós tagból sem. Az üres klóz jele □. A □ kielégíthetetlen (mert nincsen olyan tagja ami kielégíthető).

A továbbiakban a konjunktív normálformákat $F = \{\{\ell_{11}, \ldots, \ell_{1,n_1}\}, \ldots, \{\ell_{k1}, \ldots, \ell_{k,n_k}\}\}$ alakban írjuk, tehát $\{\ell_{i1}, \ldots, \ell_{i,n_i}\}$ egy klóz.

Ha C egy olyan klóz ami szerepel F-ben diszjunkciós tagként, akkor azt írjuk, hogy $C \in F$. Ha $\square \in F$, ami szintén lehetséges, akkor F kielégíthetetlen. Ugyanakkor, ha $F = \emptyset$, tehát nem tartalmaz egyetlen diszjunkciós tagot sem, akkor F kielégíthető, sőt érvényes.

1.75. Definíció. Legyenek C_1 és C_2 klózok, ℓ pedig egy olyan literál, hogy $\ell \in C_1$ és $\overline{\ell} \in C_2$. Ekkor az $R = (C_1 - \{\ell\}) \cup (C_2 - \{\overline{\ell}\})$ klózt a C_1 és C_2 rezolvensének nevezzük. Továbbá, ha F egy konjunktív normálforma, akkor egy R klóz az F egy rezolvense, ha van olyan $C_1, C_2 \in F$, hogy R a C_1 és C_2 rezolvense. □

Amennyiben R a C_1 és C_2 rezolvense, akkor azt mondjuk, hogy R rezolúcióval kapható C_1-ből és C_2-ből.

A rezolúciót, vagy rezolválást következtetési szabály alakban is írhatjuk.

$$\frac{C_1,\ C_2}{(C_1 - \{\ell\}) \cup (C_2 - \{\overline{\ell}\})}$$

1.76. Lemma. (Rezolúciós lemma) Legyen F egy konjunktív normálforma, R pedig az F egy rezolvense. Akkor $F \equiv F \cup \{R\}$.

Bizonyítás. Ha $\mathcal{A} \models F \cup \{R\}$, akkor $\mathcal{A} \models F$

Fordítva, tegyük fel, hogy $\mathcal{A} \models F$ és legyen $R = (C_1 - \{\ell\}) \cup (C_2 - \{\overline{\ell}\})$. Mivel $C_1, C_2 \in F$, ezért szintén $\mathcal{A} \models C_1$ és $\mathcal{A} \models C_2$.

Két eset lehetséges.

1 eset: $\mathcal{A} \models \ell$. Akkor $\mathcal{A} \not\models \overline{\ell}$, de mivel $\mathcal{A} \models C_2$, kapjuk, hogy $\mathcal{A} \models C_2 - \{\overline{\ell}\}$ tehát $\mathcal{A} \models R$.

2 eset: $\mathcal{A} \not\models \ell$. Akkor $\mathcal{A} \models C_1$ miatt $\mathcal{A} \models C_1 - \{\ell\}$, tehát ismét $\mathcal{A} \models R$.

Tehát mindkét esetben $\mathcal{A} \models F \cup \{R\}$.

□

1.77. Definíció. Ha F egy konjunktív normálforma, akkor

$$Res(F) = F \cup \{R \mid R \text{ az } F \text{ egy rezolvense }\}.$$

□

1.78. Lemma. $F \equiv Res(F)$

Bizonyítás. Mivel $Res(F) = F \cup \{R_1, \ldots, R_n\}$, a 1.76. lemma n-szeri alkalmazásával kapjuk, hogy

$$\begin{aligned} F &\equiv F \cup \{R_1\} \\ &\equiv F \cup \{R_1\} \cup \{R_2\} \\ &\quad \ldots \\ &\equiv F \cup \{R_1\} \cup \ldots \cup \{R_n\}. \end{aligned}$$

□

Bevezetjük a következő jelöléseket.

1.79. Definíció. $Res^{(0)}(F) = F$

$$Res^{(n+1)}(F) = Res(Res^{(n)}(F))$$

$$Res^*(F) = \bigcup_{n=0}^{\infty} Res^{(n)}(F)$$

Egy F konjunktív normálforma bármely rezolvense klóz, tehát $Res(F)$ és $Res^*(F)$ is klózhalmazok. Most megadjuk $Res^*(F)$-nek egy ekvivalens definícióját.

1.80. Definíció. Legyen F egy konjunktív normálforma. Egy F-ből történő rezolúciós bizonyításnak klózok egy olyan $C_1, \ldots, C_n$ sorozatát nevezzük, amelyben minden $1 \leq i \leq n$-re az alábbi feltételek valamelyike teljesül

1. $C_i \in F$

2. van olyan $k, l < i$, hogy C_i a C_k és a C_l egy rezolvense.

Egy C klóz bebizonyítható F-ből rezolúcióval (vagy röviden C rezolválható F-ből), ha van olyan F-ből történő $C_1, \ldots, C_n$ rezolúciós bizonyítás, melyre $C_n = C$.

1.81. Példa. Legyen $F = (p \vee q \vee \neg r) \wedge \neg p \wedge (p \vee q \vee r) \wedge (p \vee \neg q)$. Akkor $\square$ rezolválható F-ből, a következő rezolúciós bizonyítással.

1.	$\{p, q, \neg r\}$	F-beli klóz
2.	$\{p, q, r\}$	F-beli klóz
3.	$\{p, q\}$	rezolúcióval kapjuk 1-ből és 2-ből
4.	$\{p, \neg q\}$	F-beli klóz
5.	$\{p\}$	rezolúcióval kapjuk 3-ból és 4-ből
6.	$\{\neg p\}$	F-beli klóz
7.	$\square$	rezolúcióval kapjuk 5-ből és 6-ból

$\square$

Viszonylag könnyen igazolható a következő lemma.

1.82. Lemma. Tetszőleges C klóz esetén $C \in Res^*(F)$ akkor és csakis akkor teljesül, ha C bebizonyítható F-ből rezolúcióval.

Bizonyítás. Először azt mutatjuk meg, hogy minden F-ből történő $C_1, \ldots, C_n$ rezolúciós bizonyítás esetén $C_n \in Res^*(F)$. n szerinti indukciót alkalmazunk.

(i) $n = 1$: Ekkor $C_1 \in F$, tehát $C_1 \in Res^*(F)$.

(ii) n-ről $n+1$-re: Legyen $C_1, \ldots, C_{n+1}$ egy F-ből történő rezolúciós bizonyítás.

Ha $C_{n+1} \in F$, akkor az állítás ugyanúgy következik, mint az $n = 1$ esetben.

Különben van olyan $k, l \leq n$, hogy C_{n+1} a C_k és a C_l egy rezolvense. Az indukciós feltevés miatt $C_k, C_l \in Res^*(F)$, tehát van olyan m, hogy $C_k, C_l \in Res^{(m)}(F)$. Akkor viszont $C_{n+1} \in Res^{(m+1)}(F)$, tehát $C_{n+1} \in Res^*(F)$.

A fordított irány igazolása végett azt mutatjuk meg, hogy minden $m \geq 0$-ra, ha $C \in Res^{(m)}(F)$, akkor C klóz bebizonyítható F-ből rezolúcióval. Most m szerinti indukcióval megyünk tovább.

(i) $m = 0$: Ekkor $C \in F$, tehát a $C_1 = C$ sorozat C-nek egy rezolválása F-ből.

(ii) m-ről $m+1$-re: Tegyük fel, hogy $C \in Res^{(m+1)}(F)$. Akkor vannak olyan $D_1 \in Res^{(m)}(F)$ és $D_2 \in Res^{(m)}(F)$ klózok, hogy C a D_1 és a D_2 egy rezolvense. Az indukciós feltevés miatt mind D_1 mind D_2 bebizonyítható F-ből rezolúcióval. Akkor viszont C is, valóban C-nek egy F-ből történő rezolúciós bizonyítását úgy kapjuk, hogy D_1 és D_2 rezolúciós bizonyításait egymás után írjuk, majd a legvégére leírjuk C-t. $\square$

Speciális esetként a lemma természetesen igaz $\square$-ra is.

Most megmutatjuk, hogy $Res^*(F)$ véges halmaz.

1.83. Tétel. *Van olyan n, hogy $Res^{(n)}(F) = Res^{(n+1)}(F) = \ldots$*

Bizonyítás. Tegyük fel, hogy F-ben k változó van. Akkor F egy klózában legfeljebb $2k$ literál szerepel. Ezen klózok száma viszont legfeljebb $\sum_{j=0}^{2k} \binom{2k}{j}$, tehát n lehet ez a szám. $\square$

1.84. Tétel. (A zérusrendű rezolúció helyességi és teljességi tétele.) *Legyen F egy (esetleg végtelen) klóz halmaz. F akkor és csakis akkor kielégíthetetlen, ha $\square \in Res^*(F)$.*

Bizonyítás. Ha $\Box \in Res^*(F)$, akkor van olyan n, melyre $\Box \in Res^{(n)}(F)$. Tehát $Res^{(n)}(F)$ kielégíthetetlen. Ugyanakkor, a 1.78. lemma n-szeri alkalmazásával kapjuk, hogy $F \equiv Res^{(n)}(F)$. Tehát F is kielégíthetetlen.

Megfordítva, tegyük fel, hogy F nem kielégíthető. Ekkor az F-ben szereplő változók száma szerinti indukcióval bizonyítunk. Jelöljük ezt a számot n-nel.

(i) $n = 0$ eset. Ekkor $F = \{\Box\}$ és így $\Box \in Res^*(F)$, tehát az állítás igaz.

(ii) Tegyük fel, hogy az állítás igaz minden olyan formulára, melyben legfeljebb n változó szerepel és tegyük fel, hogy F-ben a $p_1, \ldots, p_{n+1}$ változók szerepelnek. Az is feltehető hogy F-ben nincs olyan klóz, ami p_{n+1}-et és $\neg p_{n+1}$-et is tartalmazza, ugyanis ezen klóz elhagyásával F-fel ekvivalens formulát kapnánk.

Legyen most F_0 az a formula, amelyet úgy kapunk F-ből, hogy kitöröljük belőle a p_{n+1} minden előfordulását, továbbá a $\neg p_{n+1}$-et tartalmazó klózokat is. (Amennyiben $\{p_{n+1}\}$ maga is klóz volt F-ben, akkor a kitörlés után a helyén a $\Box$ marad.) Nyilvánvaló, hogy ekkor F_0 is kielégíthetetlen lesz, ugyanis ha F_0-t kielégítené $\mathcal{A}$, akkor F-et kielégítené $\mathcal{A}'$, ahol $\mathcal{A}'(p_i) = \mathcal{A}(p_i)$ minden $1 \leq i \leq n$-re és $\mathcal{A}'(p_{n+1}) = 0$.

Legyen továbbá F_1 az a formula, amelyet úgy kapunk F-ből, hogy kitöröljük belőle a $\neg p_{n+1}$ minden előfordulását, továbbá a p_{n+1}-et tartalmazó klózokat is. Ugyancsak nyilvánvaló, hogy F_1 is kielégíthetetlen.

Ekkor F_0-ban és F_1-ben már csak a $p_1, \ldots, p_n$ változók szerepelnek, tehát az indukció feltevés miatt $\Box \in Res^*(F_0)$ és $\Box \in Res^*(F_1)$.

Tehát, a 1.82. lemma miatt a $\Box$ bizonyítható mind F_0-ból mind F_1-ből. Amennyiben az F_0-beli bizonyításban nem szerepel olyan klóz ami F egy klózából a p_{n+1} törlésével keletkezett, akkor az egy F feletti bizonyítás is, tehát $\Box \in Res^*(F)$. Ugyanez érvényes, ha az F_1-beli bizonyításban nem szerepel olyan klóz ami F egy klózából a $\neg p_{n+1}$ törlésével keletkezett.

Ha viszont mind az F_0-beli mind az F_1-beli bizonyításban vannak ilyen klózok, akkor helyezzük ezekbe vissza rendre p_{n+1}-et és $\neg p_{n+1}$-et. Így két F-beli rezolúciós bizonyítást kapunk, az első esetben a $\{p_{n+1}\}$ míg a második esetben a $\{\neg p_{n+1}\}$ bizonyítását. Ezekből egy további rezolúciós lépés alkalmazásával $\Box$ egy F-beli bizonyítását kapjuk.

Így a 1.82. lemma miatt $\Box \in Res^*(F)$. □

Az ítéletkalkulus-beli rezolúciós algoritmus

F megcáfolásához nem kell a teljes $Res^*(F)$ halmazt kiszámolni, hanem elegendő csak $\Box$-nak egy bizonyítását megtalálni.

Algoritmus.

Input: Egy F konjunktív normálforma.
Output: *Kielégíthető*, ha F kielégíthető, különben *kielégíthetetlen*.

1. Írjuk fel F-et klóz halmaz alakban.
2. **repeat**
   $G := F$
   $F := Res(F)$
   until $\Box \in F$ or $F = G$;
3. Ha $\Box \in F$ akkor output *kielégíthetetlen*, különben output *kielégíthető*. □

A 1.84. tétel a következő alakban is kimondható.

1.85. Tétel. *Egy F konjunktív normálforma akkor és csakis akkor kielégíthetetlen, ha van olyan $C_1, \ldots, C_n$ sorozat, amely eleget tesz a következő feltételeknek:*

1. $C_n = \square$
2. *Minden $1 \leqslant i \leqslant n$-re C_i egy F-beli klóz vagy van olyan $1 \leqslant k, l < i$, hogy C_i-t a C_k és C_l egy rezolvense.*

Bizonyítás. Következik a 1.82. lemmából és a 1.84. tételből. □

1.86. Példa. Bizonyítsuk be, hogy a következő konjunktív normálforma nem kielégíthető.

$$F = (p \vee q) \wedge (p \vee \neg r) \wedge (\neg p \vee r) \wedge (\neg p \vee \neg q) \wedge (r \vee \neg q) \wedge (\neg r \vee q)$$

1.	$\{p, q\}$	F-beli klóz
2.	$\{\neg p, r\}$	F-beli klóz
3.	$\{q, r\}$	rezolúcióval kapjuk 1-ből és 2-ből
4.	$\{\neg r, q\}$	F-beli klóz
5.	$\{q\}$	rezolúcióval kapjuk 3-ból és 4-ből
6.	$\{p, \neg r\}$	F-beli klóz
7.	$\{\neg p, \neg q\}$	F-beli klóz
8.	$\{\neg r, \neg q\}$	rezolúcióval kapjuk 6-ból és 7-ből
9.	$\{r, \neg q\}$	F-beli klóz
10.	$\{\neg q\}$	rezolúcióval kapjuk 8-ból és 9-ből
11.	$\square$	rezolúcióval kapjuk 5-ből és 10-ből

□

2. Predikátumkalkulus

2.1. Alapfogalmak

Függvények, predikátumok

Legyen $n \geq 0$ és $f : A^n \to A$ egy n változós függvény. Az $n = 0$ esetben $A^n = \{(\,)\}$ egyelemű halmaz. Ilyenkor f-et konstansnak hívjuk és azonosítjuk A azon a elemével, melyre $f((\,)) = a$.

A feletti n változós predikátumnak egy $p : A^n \to \{0, 1\}$ függvényt nevezünk. A fentiekkel összhangban, az $n = 0$ esetben $p \in \{0, 1\}$. Ha valamely $a_1, \ldots, a_n \in A$-ra $p(a_1, \ldots, a_n) = 1$, akkor azt mondjuk, hogy $p(a_1, \ldots, a_n)$ igaz.

Az elsőrendű nyelv szintaxisa

Egy $\mathcal{L}$ elsőrendű nyelven a következő szintaxist értjük.

2.1. Definíció. Az $\mathcal{L}$ szimbólumai a következők.

Változók: $x, y, u, v, w, \ldots, x_1, x_2, \ldots$. A változók halmazát Var-ral jelöljük.

Függvényszimbólumok: $f, g, h, \ldots, f_1, f_2, \ldots$. Minden függvényszimbólumnak van egy aritása (más szóval rangja), ami egy nemnegatív egész szám.

Predikátumszimbólumok: $p, q, r, \ldots, p_1, p_2, \ldots$ A predikátumszimbólumok halmaza nem üres és minden predikátumszimbólumnak van egy aritása, ami ugyancsak egy nemnegatív egész szám.

Logikai szimbólumok: $\neg, \vee, \wedge, \exists, \forall$

Elválasztó szimbólumok: $(\,,\,)$ és a , (vessző).

Ha egy f függvény (p predikátum) szimbólum aritása n, akkor azt mondjuk, hogy f (p) n változós. A 0 változós függvényszimbólumokat konstans szimbólumoknak (vagy konstans jeleknek) hívjuk és a, b, c-vel jelöljük.

2.2. Definíció. Az $\mathcal{L}$ nyelv formulái a következő szabályok szerint képezhetők.

(a) *Termek:* a legszűkebb olyan halmaz, amelyre az alábbi két feltétel teljesül:

  (i) Minden változó term.

  (ii) Ha $t_1, \ldots, t_n$ termek valamely $n \geqslant 0$-ra, f pedig egy n változós függvényszimbólum, akkor $f(t_1, \ldots, t_n)$ is term. (Ha $n = 0$, akkor $f(\,)$ helyett csak f-et írunk.)

(b) *Atomi formulák:* a legszűkebb olyan halmaz, amely kielégíti az alábbi feltételt:

  (i) Ha $t_1, \ldots, t_n$ termek valamely $n \geqslant 0$-ra, p pedig egy n változós predikátumszimbólum, akkor $p(t_1, \ldots, t_n)$ atomi formula. (Az $n = 0$ esetben $p(\,)$ helyett most is csak p-t írunk.)

(c) *Formulák:* A legszűkebb olyan halmaz, amelyre az alábbi feltételek teljesülnek:

  (i) Minden atomi formula egyben formula is.

  (ii) Ha F és G formulák, akkor $\neg F$, $(F \vee G)$ és $(F \wedge G)$ is formulák,

  (iii) Ha F formula, x pedig egy változó, akkor $\exists x F$ és $\forall x F$ is formulák.

A formulák halmazát $Form(\mathcal{L})$-lel, vagy ha csak egy $\mathcal{L}$-ről beszélünk, akkor $Form$-al jelöljük.

Mint az ítéletkalkulus esetében, most is $F \to G$ jelöli az $\neg F \vee G$ alakú formulákat és $F \leftrightarrow G$ az $(F \to G) \wedge (G \to F)$ alakú formulákat. A formulákban szereplő legkülső zárójelpárt általában most is elhagyjuk.

Elnevezések

1. Az olyan termeket amelyekben nem szerepelnek változók ground termeknek nevezzük.
2. Ha F egy formula, $F = F_1 G F_2$ és G is formula, akkor G az F részformulája.
3. Egy x változó valamely (nem közvetlenül kvantor utáni) előfordulása egy F formulában kötött, ha ez az előfordulás F-nek egy $\exists x G$ vagy $\forall x G$ alakú részformulája G részében van. Különben x szóban forgó előfordulása szabad.
4. Egy x változó szabad F-ben, ha van F-ben szabad előfordulása.
5. A szabad változó nélküli formulákat zárt formuláknak vagy mondatoknak hívjuk.
6. Egy F formula mátrixának azt az F^* formulát nevezzük, amelyet úgy kapunk F-ből, hogy töröljük belőle a $\forall x$ és $\exists x$ alakú részeket.

2.3. Példa. Tekintsük az

$$F = q(x) \vee \exists x \forall y (p(f(x), z) \wedge q(y)) \vee \forall x r(x, y, g(x))$$

formulát. Ekkor $\forall y (p(f(x), z) \wedge q(y))$ az F egy részformulája.

Továbbá, F változóinak előfordulásai balról jobbra haladva: x szabad, x kötött, z szabad, y kötött, x kötött, y szabad, x kötött.

Végül $q(x) \vee (p(f(x), z) \wedge q(y)) \vee r(x, y, g(x))$ az F mátrixa. □

Az elsőrendű nyelv szemantikája

2.4. Definíció. Legyen $\mathcal{L}$ egy elsőrendű nyelv. $\mathcal{L}$ típusú strukturának nevezünk egy $\mathcal{A} = (U, \mathcal{I}, \varphi)$ hármast, ahol:

- U egy nem üres halmaz, az univerzum,
- $\varphi : Var \to U$ egy változó hozzárendelés,
- $\mathcal{I}$ egy olyan leképezés, amely
  - minden $\mathcal{L}$-beli n változós f függvényszimbólumhoz hozzárendel egy $\mathcal{I}(f) : U^n \to U$ függvényt. (Ha $n = 0$, akkor $\mathcal{I}(f) \in U$.)
  - minden $\mathcal{L}$-beli n változós p predikátumszimbólumhoz hozzárendel egy $\mathcal{I}(p) : U^n \to \{0, 1\}$ predikátumot. (Ha $n = 0$, akkor $\mathcal{I}(p) \in \{0, 1\}$.)

□

2.5. Példa. Tekintsük az $F = \forall x p(x, f(x)) \wedge q(g(a, z))$ formulát. Ekkor $\mathcal{A} = (U, \mathcal{I}, \varphi)$ egy struktúra, ahol

- $U = \{0, 1, 2, \dots\}$, továbbá minden $m, n \in U$ esetén
- $\mathcal{I}(p)(n, m) = n < m$, vagyis

$$\mathcal{I}(p)(n, m) = \begin{cases} 1 & \text{ha } n < m \\ 0 & \text{különben,} \end{cases}$$

- $\mathcal{I}(q)(n) = \text{prím}(n)$, vagyis

$$\mathcal{I}(q)(n) = \begin{cases} 1 & \text{ha } n \text{ prím} \\ 0 & \text{különben,} \end{cases}$$

- $\mathcal{I}(f)(n) = n + 1$,
- $\mathcal{I}(g)(n, m) = n + m$,
- $\mathcal{I}(a) = 2$,
- $\varphi(z) = 3$,
- $\varphi(x) = 2$.

□

2.6. Definíció. Legyen t egy term, $\mathcal{A} = (U, \mathcal{I}, \varphi)$ pedig egy struktúra. A t értékét $\mathcal{A}$-ban (melyet $\mathcal{A}(t)$-vel jelölünk), a következőképpen definiáljuk.

(i) Ha $t = x$, akkor $\mathcal{A}(t) = \varphi(x)$.

(ii) Ha $t = f(t_1, \ldots, t_n)$, ahol $t_1, \ldots, t_n$ termek, f pedig egy n változós függvényszimbólum, akkor $\mathcal{A}(t) = \mathcal{I}(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$. (Ha $n = 0$, akkor $\mathcal{A}(t) = \mathcal{I}(f) \in U$.)

Jegyezzük meg, hogy mindegyik esetben $\mathcal{A}(t) \in U$.

□

Most definiáljuk egy F formula jelentését (vagy: értékét) egy $\mathcal{A} = (U, \mathcal{I}, \varphi)$ struktúrában. Előtte azonban bevezetünk egy olyan jelölést amit a következőkben igen gyakran használunk majd.

2.7. Jelölés Legyen $\mathcal{A} = (U, \mathcal{I}, \varphi)$ egy struktúra, $x_1, \ldots, x_n \in Var$ és $u_1, \ldots, u_n \in U$. $\mathcal{A}_{[x_1/u_1]\ldots[x_n/u_n]}$-val jelöljük azt az $\mathcal{A}' = (U, \mathcal{I}, \varphi')$ struktúrát, melyre minden $y \in Var$ esetén

$$\varphi'(y) = \begin{cases} u_1 & \text{ha } y = x_1 \\ \vdots & \\ u_n & \text{ha } y = x_n \\ \varphi(y) & \text{különben.} \end{cases}$$

□

A jelölést legtöbbször az $n = 1$ esetben használjuk majd, amikor is $\mathcal{A}_{[x/u]}$-t írunk.

2.8. Definíció. Legyen F egy formula, $\mathcal{A} = (U, \mathcal{I}, \varphi)$ pedig egy struktúra. Ekkor F értékét (vagy: jelentését) $\mathcal{A}$-ban $\mathcal{A}(F)$-fel jelöljük és a következőképpen értelmezzük.

(i) Ha F atomi formula, vagyis $F = p(t_1, \ldots, t_n)$, valamely n változós p predikátumszimbólum és $t_1, \ldots, t_n$ termek esetén, akkor $\mathcal{A}(F) = \mathcal{I}(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$. (Tehát $\mathcal{A}(F) \in \{0, 1\}$.)

(ii) Ha $F = \neg(G)$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 0 \\ 0 & \text{ha } \mathcal{A}(G) = 1. \end{cases}$$

Ha $F = (G \vee H)$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 1 \text{ vagy } \mathcal{A}(H) = 1 \\ 0 & \text{különben.} \end{cases}$$

Ha $F = (G \wedge H)$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha } \mathcal{A}(G) = 1 \text{ és } \mathcal{A}(H) = 1 \\ 0 & \text{különben.} \end{cases}$$

(iii) Ha $F = \exists x G$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha van olyan } u \in U, \text{ hogy } \mathcal{A}_{[x/u]}(G) = 1 \\ 0 & \text{különben.} \end{cases}$$

Ha $F = \forall x G$, akkor

$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha minden } u \in U \text{ esetén } \mathcal{A}_{[x/u]}(G) = 1 \\ 0 & \text{különben.} \end{cases}$$

Legyen F egy formula, $\mathcal{A}$ pedig egy struktúra. Akkor az ítéletkalkulussal analóg módon használjuk az $\mathcal{A} \models F$, $\models F$ jelöléseket, továbbá a kielégíthető, a kielégíthetetlen és az érvényes (vagy tautológia) kifejezéseket. Ha $\mathcal{A} \models F$, akkor most is azt mondjuk, hogy $\mathcal{A}$ modellje F-nek.

2.9. Példa. A 2.5. példában szereplő F formula és $\mathcal{A}$ struktúra esetén $\mathcal{A} \models F$.

Most is igaz a következő tétel.

2.10. Tétel. *F akkor és csak akkor érvényes, ha $\neg F$ kielégíthetetlen.*

2.11. Tétel. *Legyen F egy elsőrendű formula, $\mathcal{A} = (U, \mathcal{I}, \varphi)$ és $\mathcal{A}' = (U, \mathcal{I}, \varphi')$ pedig két struktúra. Tegyük fel, hogy $\varphi(x) = \varphi'(x)$ minden olyan x változó esetén, amely szabad F-ben. Ekkor $\mathcal{A}(F) = \mathcal{A}'(F)$.*

Bizonyítás. Formula indukcióval.

(i) Ha F atomi formula akkor minden F-ben szereplő változó minden előfordulása szabad. Ezért $\varphi(x) = \varphi'(x)$, minden F-ben szereplő x változó esetén, amiből persze nyilvánvalóan következik, hogy $\mathcal{A}(F) = \mathcal{A}'(F)$.

(ii) Legyen először $F = \neg G$. Ekkor F szabad változói ugyanazok mint G szabad változói, tehát az is teljesül, hogy $\varphi(x) = \varphi'(x)$ minden olyan x változó esetén, amely szabad G-ben. Így az indukció feltevés miatt $\mathcal{A}(G) = \mathcal{A}'(G)$, amiből azonnal adódik, hogy $\mathcal{A}(F) = \mathcal{A}'(F)$.

Legyen $F = G \vee H$. Ekkor F szabad változóinak halmaza az F szabad változói halmazának és a H szabad változói halmazának egyesítése, következésképpen φ és φ' egybeesik mind G mind H szabad változóin. Az indukció feltevés miatt $\mathcal{A}(G) = \mathcal{A}'(G)$ és $\mathcal{A}(H) = \mathcal{A}'(H)$, amiből $\mathcal{A}(F) = \mathcal{A}'(F)$ következik.

Az $F = G \wedge H$ eset hasonlóan igazolható.

Most legyen $F = \forall x G$. Ekkor G szabad változóinak halmaza nem más mint F szabad változóinak halmaza plusz még az x változó. Így minden $u \in U$ esetén igaz, hogy azon ψ_u és ψ'_u hozzárendelések egybesenek G szabad változóin, melyeket úgy definiálunk, hogy $\psi_u(x) = \psi'_u(x) = u$ és minden más $y \neq x$-re $\psi_u(y) = \varphi(y)$ és $\psi'_u(y) = \varphi'(y)$.

Most $\mathcal{A} \models F$ akkor és csak akkor áll fenn, ha minden $u \in U$-ra $\mathcal{A}_{[x=u]} \models G$, mely, az indukció feltevés és a G szabad változóira és a ψ_u és ψ'_u hozzárendelésekre tett fenti megjegyzésünk értelmében akkor és csak teljesül, ha minden $u \in U$-ra $\mathcal{A}'_{[x=u]} \models G$. Ez utóbbi viszont éppen azt jelenti, hogy $\mathcal{A}' \models F$.

Az $F = \exists x G$ eset hasonlóan igazolható, a tétel bizonyítását befejeztük. □

2.12. Következmény. Tetszőleges F mondat (zárt formula) és $\mathcal{A} = (U, \mathcal{I}, \varphi)$ struktúra esetén az alábbi két feltétel közül pontosan az egyik áll fenn:

(a) Minden $\psi : Var \to U$-ra $\mathcal{A}' \models F$, ahol $\mathcal{A}' = (U, \mathcal{I}, \psi)$

(b) Nincsen olyan $\psi : Var \to U$, melyre $\mathcal{A}' \models F$, ahol $\mathcal{A}' = (U, \mathcal{I}, \psi)$

□

Ebből következik, hogy ha F zárt formula, akkor tetszőleges $\mathcal{A} = (U, \mathcal{I}, \varphi)$ struktúra esetén φ-nek nincsen szerepe abban, hogy $\mathcal{A} \models F$ teljesül-e. Ezért az ilyen esetekben néha csak $\mathcal{A} = (U, \mathcal{I})$-t írunk.

Szükségünk lesz a következő lemmára:

2.13. Lemma. Legyen F tetszőleges formula, melynek szabad változói $x_1, \ldots, x_n$. Ekkor

(a) $\models F$ akkor és csakis akkor teljesül, ha $\models \forall x_1 \ldots \forall x_n F$.

(b) F akkor és csakis akkor kielégíthető, ha a $\exists x_1 \ldots \exists x_n F$ kielégíthető.

Bizonyítás. A megfelelő definíciók alapján nyilvánvaló. □

Kapcsolat az ítéletkalkulus és a predikátumkalkulus között

1. Minden zérusrendű (vagyis ítéletkalkulusbeli nyelv) tekinthető úgy mint egy speciális elsőrendű nyelv. Nevezetesen, annak az elsőrendű nyelvnek felel meg, amelyben

(a) a változók halmaza üres,

(b) a függvényszimbólumoknak halmaza üres,

(c) csak 0 változós predikátumok vannak.

Egy ilyen speciális elsőrendű nyelv formuláiban nem lesznek termek, nem szerepelnek bennük kvantorok. A formulák zérusrendű nyelv formulák lesznek. Továbbá minden $\mathcal{A} = (U, \mathcal{I}, \varphi)$ strukúra esetén

(a) φ irreleváns lesz, mert nincsenek változók,

(b) U felesleges, mert nincsenek függvényszimbólumok és csak 0 változós predikátumszimbólumok vannak,

(c) minden p predikátumszimbólumra $\mathcal{I}(p) \in \{0, 1\}$ (mert p aritása 0).

Ezért az ítéletkalkulus a predikátumkalkulusnak egy speciális esete.

2. Tekintsünk egy olyan $\mathcal{L}$ elsőrendű nyelvet, amelyben a változók halmaza üres és amelyben van legalább egy 0 változós függvényszimbólum. Ez esetben csak ground termek lesznek, így az $\mathcal{A} = (U, \mathcal{I}, \varphi)$ struktúrában egy formula kiértékelése szempontjából φ most is felesleges lesz. $\mathcal{L}$ formuláiban most sem szerepelnek kvantorok. Belátható, hogy $\mathcal{L}$ ekvivalens azzal a zérusrendű nyelvvel, amit úgy kapunk, hogy $\mathcal{L}$ minden atomi formuláját egy új ítéletváltozóval reprezentáljuk. Például az

$$F = (q(a) \vee \neg r(f(b), c)) \wedge p(a, b)$$

elsőrendű formula az

$$F' = (q_1 \vee \neg q_2) \wedge q_3$$

zérusrendű formulának felel meg, ahol q_1, q_2 és q_3 az új (ítélet)változók. Ekkor teljesül az, hogy F akkor és csakis akkor kielégíthető (vagy tautológia), ha F' kielégíthető (vagy tautológia).

2.2. Ekvivalencia, normálformák

2.14. Definíció. Az F és G formulák logikailag ekvivalensek, jele $F \equiv G$, ha minden $\mathcal{A}$ struktúra esetén $\mathcal{A} \models F$ akkor és csak akkor, ha $\mathcal{A} \models G$.

Ekvivalens formulák

Tetszőleges F és G formulák esetén érvényesek a következők.

1. $\neg\forall xF \equiv \exists x\neg F$
   $\neg\exists xF \equiv \forall x\neg F$

2. Ha x nem fordul elő szabadon G-ben, akkor

   $\forall xF \wedge G \equiv \forall x(F \wedge G)$
   $\forall xF \vee G \equiv \forall x(F \vee G)$
   $\exists xF \wedge G \equiv \exists x(F \wedge G)$
   $\exists xF \vee G \equiv \exists x(F \vee G)$

3. $\forall xF \wedge \forall xG \equiv \forall x(F \wedge G)$
   $\exists xF \vee \exists xG \equiv \exists x(F \vee G)$

4. $\forall x\forall yF \equiv \forall y\forall xF$
   $\exists x\exists yF \equiv \exists y\exists xF$

Ugyanakkor könnyen igazolható, hogy általában

$\exists xF \wedge \exists xG \not\equiv \exists x(F \wedge G)$ és $\forall xF \vee \forall xG \not\equiv \forall x(F \vee G)$.

2.15. Példa. Mutassuk meg, hogy $\exists xp(x) \to p(y) \equiv \forall x(p(x) \to p(y))$. A következő számolás adódik:

$$\begin{aligned} & \exists xp(x) \to p(y) \\ \equiv\ & \neg\exists xp(x) \vee p(y) \\ \equiv\ & \forall x\neg p(x) \vee p(y) \\ \equiv\ & \forall x(\neg p(x) \vee p(y)) \\ \equiv\ & \forall x(p(x) \to p(y)) \end{aligned}$$

□

Könnyen igazolható, hogy az előző példa általánosítható: ha x nem szabad G-ben, akkor $\exists xF \to G \equiv \forall x(F \to G)$ és $\forall x(G \to F) \equiv G \to \forall xF$.

Helyettesítés, kiigazított és prenex alakú formulák

Legyen F egy formula, $x_1, \ldots, x_n$ különböző szabad változók F-ben, $t_1, \ldots, t_n$ pedig termek. Akkor $F[x_1/t_1] \ldots [x_n/t_n]$ az a formula, melyet úgy kapunk F-ből, hogy benne az $x_1, \ldots, x_n$ változók szabad előfordulásai helyére rendre a $t_1, \ldots, t_n$-t termeket írjuk. A formális definíció a következő.

2.16. Definíció. a) Először definiáljuk $u[x/t]$-t, ahol u és t termek, x pedig egy változó. Ha u maga is egy változó, akkor

$$u[x/t] = \begin{cases} t & \text{ha } u = x \\ u & \text{különben.} \end{cases}$$

Különben, ha $u = f(t_1, \ldots, t_n)$, akkor $u[x/t] = f(t_1[x/t], \ldots, t_n[x/t])$.

Ha $x_1, \ldots, x_n$ különböző változók, $t_1, \ldots, t_n$ pedig termek, akkor

$$u[x_1/t_1] \ldots [x_n/t_n] = (u[x_1/t_1] \ldots [x_{n-1}/t_{n-1}])[x_n/t_n].$$

(Megjegyezzük, hogy $u[x_1/t_1] \ldots [x_{n-1}/t_{n-1}]$-ben x_n-nek olyan előfordulásai is lehetnek, amelyek eredetileg u-ban nem szerepeltek.)

b) Eztán definiáljuk $F[x/t]$-t, ha $F = p(t_1, \ldots, t_n)$, vagyis atomi formula. Ekkor $F[x/t] = p(t_1[x/t], \ldots, t_n[x/t])$.

Most definiáljuk $F[x/t]$-t tetszőleges formulára. Ha $F = \neg G$, akkor $F[x/t] = \neg G[x/t]$, ha $F = G \vee H$, akkor $F[x/t] = G[x/t] \vee H[x/t]$, ha $F = G \wedge H$, akkor $F[x/t] = G[x/t] \wedge H[x/t]$. Végül, ha $F = \forall y G$ vagy $F = \exists y G$, ahol $x \neq y$, akkor $F[x/t] = \forall y G[x/t]$ és $F[x/t] = \exists y G[x/t]$.

Végül, ha $x_1, \ldots, x_n$ különböző szabad változók F-ben, $t_1, \ldots, t_n$ pedig termek, akkor $F[x_1/t_1] \ldots [x_n/t_n] = (F[x_1/t_1] \ldots [x_{n-1}/t_{n-1}])[x_n/t_n]$.

□

Egyúttal azt is igazoltuk, hogy $F[x_1/t_1] \ldots [x_n/t_n]$ maga is formula lesz.

2.17. Példa. Legyen $F = p(x, a) \wedge \forall x(q(x, y) \rightarrow r(y))$ és $t = g(f(z), a)$. Akkor $F[x/t] = p(g(f(z), a), a) \wedge \forall x(q(x, y) \rightarrow r(y))$

2.18. Lemma. (Helyettesítési lemma.) Minden F formula, $x_1, \ldots, x_n$ különböző változók, $t_1, \ldots, t_n$ ground termek és $\mathcal{A}$ struktúra esetén

$$\mathcal{A}(F[x_1/t_1] \ldots [x_n, t_n]) = \mathcal{A}_{[x_1/\mathcal{A}(t_1)] \ldots [x_n/\mathcal{A}(t_n)]}(F).$$

Bizonyítás. Formula indukcióval. □

Mint látjuk, a fenti lemmában $t_1, \ldots, t_n$ nem lehetnek tetszőleges termek. Ha ugyanis megengedjük, hogy egy t_i-ben változók is szerepeljenek, akkor előfordulhat, hogy lesz benne egy olyan y változó, amely kötötté válik miután t_i-t behelyettesítjük x_i helyére, ami gondokat okozhat. Ha azonban ezt kizárjuk, akkor a lemma kimondható általánosabb formában is: igaz lesz minden olyan $t_1, \ldots, t_n$-re, amelyek teljesítik azt a feltételt, hogy egyetlen t_i-ben sem szerepel olyan y változó melyhez létezik F-nek olyan $\forall y G$ vagy $\exists y G$ alakú részformulája ami tartalmazza x_i egy szabad előfordulását.

2.19. Lemma. (Átnevezési lemma.) Legyen $F = \forall x G$ ($F = \exists x G$) egy formula és legyen y olyan változó, amely nem fordul elő szabadon G-ben. Akkor $F \equiv \forall y G[x/y]$ ($F \equiv \exists y G[x/y]$).

Bizonyítás. Formula indukcióval.

2.20. Definíció. Egy formula *kiigazított*, ha

(a) nem fordul elő benne egy változó szabadon és kötötten is
(b) különböző kvantor előfordulások különböző változókat kötnek le.

2.21. Példa. Az $F = \forall x \exists y p(x, f(y)) \wedge \forall y (q(x, y) \vee r(x))$ formula nem kiigazított, mivel sem az (a) sem a (b) feltétel nem teljesül. Valóban, az x változó előfordul F-ben szabadon is és kötötten is, továbbá a $\exists$ és a második $\forall$ kvantorok mindegyike az y változót köti le. Ugyanakkor alkalmas változó átnevezésekkel, vagyis a 2.19. lemma többszöri alkalmazásával F könnyedén "kiigazítható", vagyis átalakítható egy F-fel ekvivalens kiigazított formulává. Valóban,

$$\begin{aligned} & \forall x \exists y p(x, f(y)) \wedge \forall y (q(x, y) \vee r(x)) \\ \equiv \quad & \forall x \exists y p(x, f(y)) \wedge \forall z (q(x, z) \vee r(x)) \\ \equiv \quad & \forall u \exists y p(u, f(y)) \wedge \forall z (q(x, z) \vee r(x)). \end{aligned}$$

2.22. Definíció. Egy F formula *prenex alakú*, ha $F = Q_1 y_1 \dots Q_n y_n G$, ahol

- $Q_1, \dots, Q_n = \exists / \forall$
- $y_1, \dots, y_n$ változók
- G-ben nem fordul elő kvantor.

(Ekvivalens definíció: F prenex alakú, ha $F = Q_1 y_1 \dots Q_n y_n F^*$ valamely alkalmas $Q_1, \dots, Q_n$ kvantorok és $y_1, \dots, y_n$ változók esetén.) □

2.23. Lemma. (Prenex alakra hozás.) Bármely F formula ekvivalens egy prenex alakú kiigazított F' formulával.

Bizonyítás. Formula indukcióval.
(i) Ha F atomi formula, akkor egyben prenex alakú és kiigazított, tehát $F' = F$.
Ha F nem atomi formula, akkor az alábbi esetek lehetségesek.
(iia) eset: $F = \neg G$. Az indukció feltevés miatt G ekvivalens egy $Q_1 y_1 \dots Q_n y_n G'$ prenex alakú kiigazított formulával. Akkor legyen $F' = P_1 y_1 \dots P_n y_n \neg G'$, ahol minden $1 \leq i \leq n$ esetén

$$P_i = \begin{cases} \exists & \text{, ha } Q_i = \forall \\ \forall & \text{, ha } Q_i = \exists. \end{cases}$$

Ekkor nyilvánvalóan F' is prenex alakú kiigazított formula és ekvivalens F-fel.
(iib) eset: $F = F_1 \vee F_2$. Az indukció feltevés értelmében $F_1 \equiv Q_1 y_1 \dots Q_m y_m G_1$ és $F_2 \equiv P_1 y'_1 \dots P_n y'_n G_2$. Feltehető, hogy az $y_1, \dots, y_m$ változók nem szerepelnek G_2-ben és az $y'_1, \dots, y'_n$ változók nem szerepelnek G_1-ben, különben G_1 és G_2 kötött változóit alkalmasan átneveznénk, lásd 2.19. lemma. (Feltevésünk értelmében mellesleg $\{y_1, \dots, y_m\} \cap \{y'_1, \dots, y'_n\} = \emptyset$ is teljesül.) Legyen $F' \equiv Q_1 y_1 \dots Q_m y_m P_1 y'_1 \dots P_n y'_n (G_1 \vee G_2)$. Nyilvánvaló, hogy F' prenex alakú kiigazított formula és ekvivalens F-fel.
(iic) eset: $F = F_1 \wedge F_2$. Bizonyítás az előző esethez hasonlóan.
(iid) eset: $F = QxG$, ahol $Q = \forall$ vagy $Q = \exists$. Az indukció feltevés miatt G ekvivalens egy $Q_1 y_1 \dots Q_m y_m G'$ prenex alakú kiigazított formulával. Feltehető, hogy x nem szerepel az $y_1, \dots, y_m$ változók között, különben megint egy alkalmas változó átnevezést végeznénk. Legyen $F' = QxQ_1 y_1 \dots Q_m y_m G'$. Nyilvánvaló, hogy F' megfelelő. □

2.24. Példa. Hozzuk kiigazított prenex alakra az $F = (\forall x \exists y p(x, g(y, f(x))) \vee \neg q(z)) \vee \neg \forall x r(x, y)$ formulát. A következő számolás adódik:

$$(\forall x \exists y p(x, g(y, f(x))) \vee \neg q(z)) \vee \neg \forall x r(x, y)$$

$\equiv$ $\forall x \exists y (p(x, g(y, f(x))) \vee \neg q(z)) \vee \neg \forall x r(x, y)$
(ekvivalens formulák 2.)

$\equiv$ $\forall x \exists y (p(x, g(y, f(x))) \vee \neg q(z)) \vee \exists x \neg r(x, y)$
(ekvivalens formulák 1.)

$\equiv$ $\forall x \exists y (p(x, g(y, f(x))) \vee \neg q(z)) \vee \exists u \neg r(u, y)$
(2.19. lemma)

$\equiv$ $\forall x \exists v (p(x, g(v, f(x))) \vee \neg q(z)) \vee \exists u \neg r(u, y)$
(2.19. lemma)

$\equiv$ $\forall x \exists v \exists u (p(x, g(v, f(x))) \vee \neg q(z) \vee \neg r(u, y))$
(ekvivalens formulák 2.)

□

Skolemizáció

2.25. Definíció. Egy prenex alakú F formuláról azt mondjuk, hogy *Skolem normálalak* (vagy:*Skolem normálforma*), ha a prefixében csak $\forall$ kvantor szerepel.

2.26. Definíció. Az F és G formulák *s-ekvivalensek*, ha F akkor és csak akkor elégíthető ki, ha G kielégíthető.

Nyilvánvaló, hogy ha $F \equiv G$, akkor F és G s-ekvivalensek, fordítva általában nem igaz.

2.27. Lemma. (Skolemizációs lemma.) Minden F kiigazított prenex normálformához van vele s-ekvivalens G Skolem normálalak. Továbbá G minden modellje F-nek is modellje.

Bizonyítás. A keresett G Skolem normálalakot a következő algoritmus állítja elő.

Algoritmus (Skolemizációs algoritmus)

Input: F kiigazított prenex alakú formula
Output: F-fel s-ekvivalens G Skolem normálalak

while F-ben van $\exists$ kvantor **do**
begin Legyen $F = \forall y_1 \ldots \forall y_n \exists z H$, ahol $n \geq 0$ és H kiigazított prenex alakú.
Legyen f egy új (vagyis F-ben nem szereplő) n változós függvényszimbólum.
$F := \forall y_1 \ldots \forall y_n H[z/f(y_1, \ldots, y_n)]$.
end
$G := F$

Az nyilvánvaló, hogy az algoritmus által szolgáltatott G Skolem normálalak. Azt kell még igazolni, hogy F s-ekvivalens G-vel és G minden modellje F-nek is modellje.

Ehhez viszont elegendő megmutatni a következő két dolgot. Egyrészt, hogy a **while**-hurok egyszeri végrehajtása a formulát vele s-ekvivalens formulába alakítja át, vagyis, hogy $F = \forall y_1 \ldots \forall y_n \exists z H$ s-ekvivalens $F' = \forall y_1 \ldots \forall y_n H[z/f(y_1, \ldots, y_n)]$-vel. Másrészt, hogy a **while**-hurok egyszeri végrehajtása után kapott formula (vagyis F') minden modellje az eredeti formulának (vagyis F-nek) is modellje.

Tegyük fel, hogy $\mathcal{A} = (U, \mathcal{I}, \varphi)$-re $\mathcal{A} \models F$. Akkor minden $u_1, \ldots, u_n \in U$ esetén van olyan $v \in U$, hogy $\mathcal{A}_{[y_1/u_1]\ldots[y_n/u_n][z/v]} \models H$. Legyen $\mathcal{A}' = (U, \mathcal{I}', \varphi)$ az a struktúra, mely $\mathcal{A}$-tól csak az

f interpretációjának megadásában különbözik. Erre nézve viszont legyen $\mathcal{I}'(f) : U^n \to U$ az a függvény, melyre minden $u_1, \ldots, u_n \in U$ esetén $\mathcal{I}'(f)(u_1, \ldots, u_n) = v$. Nyilvánvaló, hogy ekkor $\mathcal{A}' \models F'$. Fordítva, tegyük fel, hogy $\mathcal{A} = (U, \mathcal{I}, \varphi)$-re $\mathcal{A} \models F'$. Akkor minden $u_1, \ldots, u_n \in U$-ra van olyan $v \in U$, tudniillik $v = \mathcal{I}(f)(u_1, \ldots, u_n)$, melyre $\mathcal{A}_{[y_1/u_1]\ldots[y_n/u_n][z/v]} \models H$. Tehát $\mathcal{A} \models F$ is teljesül. Mivel $\mathcal{A}$ az F'-nek tetszőleges modellje volt, a **while**-hurokra vonatkozó állítás második részét is bizonyítottuk. □

Megjegyezzük, hogy a Skolemizációs algoritmus alkalmazása előtt az F formulát néha érdemes átrendezni, hogy az eredményül kapott, F-fel s-ekvivalens formula egyszerűbb legyen. Legyen például $F = \forall x \forall y \exists z (p(x, y) \wedge q(z))$. F-re alkalmazva a Skolemizációs algoritmust, a $G = \forall x \forall y (p(x, y) \wedge q(f(x, y)))$ formulát kapjuk, mely természetesen s-ekvivalens F-fel.

Ugyanakkor nyilvánvaló, hogy $F \equiv F'$, ahol $F' = \exists z \forall x \forall y (q(z) \wedge p(x, y))$, továbbá, F'-re alkalmazva a Skolemizációs algoritmust, a $G' = \forall x \forall y (q(a) \wedge p(x, y))$ formulát kapjuk, mely s-ekvivalens F'-vel és így F-fel is.

Konjunktív és diszjunktív normálformák

Ebben a részben csak kvantormentes formulákat vizsgálunk. Kvantormentes formula például egy tetszőlges formula mátrixa vagy minden olyan formula, melyben nincsenek változók (lásd fentebb).

Könnyen látható, hogy a kvantormentes formulák pontosan az atomi formulákból a $\neg, \vee$ és a $\wedge$ szimbólumok segítségével felépíthető formulák. Vegyük észre az analógiát az ítéletkelkulus formulái és a kvantormentes elsőrendű formulák között: az ítéletkalkulusbeli változóknak a predikátumkalkulusban az atomi formulák felelnek meg, innen kezdve a az ítéletkalkulusbeli formulák és a kvantormentes elsőrendű formulák felépítése ugynaz, vö. 1.1. definíció.

Így világos, hogy az elsőrendű literál fogalmát a következőképpen vezetjük be.

2.28. Definíció. Elsőrendű literálnak egy $p(t_1, \ldots, t_n)$ atomi formulát, vagy annak a $\neg p(t_1, \ldots, t_n)$ tagadását nevezzük. A literálokat most is ℓ-el jelöljük és alkalmazzuk az

$$\overline{\ell} = \begin{cases} \neg p(t_1, \ldots, t_n) & \text{, ha } \ell = p(t_1, \ldots, t_n) \\ p(t_1, \ldots, t_n) & \text{, ha } \ell = \neg p(t_1, \ldots, t_n) \end{cases}$$

jelölést.
Amennyiben ℓ-ben nem szerepelnek változók (tehát $t_1, \ldots, t_n$ mindegyike ground term), akkor ℓ-et ground literálnak nevezzük.

□

Ezek után az ítéletkalkulusbeli esettel analóg módon definiálhatjuk predikátumkalkulusbeli kvantormentes formulákra a konjunktív és a diszjunktív normálalak fogalmát és kimondhatjuk a következő tételt.

2.29. Tétel. *Minden F kvantormentes formula logikailag ekvivalens egy (kvantormentes) konjunktív és egy diszjunktív normálalakkal.*

Bizonyítás. Az ítéletkalkulusbeli esettel analóg módon. □

Teteszőleges F (elsőrendű) konjunktív normálalak esetén $F = C_1 \wedge \ldots \wedge C_n$, ahol $C_1, \ldots, C_n$ diszjunkciós tagok. A diszjunkciós tagokat, csakúgy mint a zérusrendű esetben, *klózoknak* nevezzük. F-et most is írhatjuk halmaz alakban: $F = \{C_1, \ldots, C_n\}$, ahol minden $1 \leq i \leq n$-re $C_i = \{l_{i_1}, \ldots, l_{i_{k_i}}\}$, továbbá $l_{i_1}, \ldots, l_{i_{k_i}}$ elsőrendű literálok.

Formula átalakítások

2.30. Lemma. Tetszőleges F formula esetén van olyan F' formula, melyre teljesülnek az alábbi feltételek:

(a) F' zárt

(b) F' Skolem normálalak

(c) F' mátrixa konjunktív normálforma

(d) F' s-ekvivalens F-fel

(e) F' minden $\mathcal{A} = (U, \mathcal{I})$ modellje esetén van olyan φ hozzárendelés, hogy $\mathcal{B} = (U, \mathcal{I}, \varphi)$ modellje F-nek.

Bizonyítás. Hajtsuk végre a következő lépéseket

1. Legyenek F szabad változói $x_1, \ldots, x_n$. Ekkor F s-ekvivalens az $F_1 = \exists x_1 \ldots \exists x_n F$ formulával (2.13. lemma (b) pont). Továbbá F_1-ben nincsenek szabad változók (tehát zárt).

2. Hozzuk F_1-et prenex alakra (2.23. lemma). Kapunk egy olyan prenex alakú F_2 formulát, melyre $F_1 \equiv F_2$.

3. Alkalmazzuk F_2-re a Skolemizációs algoritmust (2.27. lemma). Kapunk egy olyan F_3 Skolem normálalakot, amely s-ekvivalens F_2-vel.

4. Hozzuk konjunktív normálformára F_3 mátrixát. Kapunk egy olyan F_4 formulát, amelyre $F_3 \equiv F_4$.

5. Legyen $F' = F_4$.

Az, hogy az (a)–(d) feltételek teljesülnek, nyilvánvaló. Az (e) bizonyítása végett tegyük fel, hogy $\mathcal{A} \models F'$, ahol $\mathcal{A} = (U, \mathcal{I})$. Ekkor, $F_3 \equiv F_4$ miatt $\mathcal{A} \models F_3$, a 2.27. lemma miatt $\mathcal{A} \models F_2$, végül $F_1 \equiv F_2$ miatt $\mathcal{A} \models F_1$. Tehát vannak olyan $u_1, \ldots, u_n \in U$ elemek, melyre $\mathcal{A}_{[x_1/u_1]\ldots[x_n/u_n]} \models F$ és így a $\mathcal{B} = (U, \mathcal{I}, \varphi)$ választás megfelelő, ahol $\varphi(x_1) = u_1, \ldots, \varphi(x_n) = u_n$.

□

2.3. Az elsőrendű érvényesség eldönthetetlensége

2.31. Tétel. *Nem létezik olyan algoritmus, amely tetszőleges F elsőrendű formuláról eldönti, hogy F érvényes-e. (Az elsőrendű formulák érvényessége eldönthetetlen.)*

Bizonyítás. Még hiányzik.

2.32. Következmény. Az elsőrendű formulák kielégíthetősége eldönthetetlen.

Bizonyítás. Indirekt bizonyítást adunk, tegyük fel, hogy a kielégíthetőség eldönthető. Akkor a kielégíthetetlenség is eldönthető (hiszen egy F formula akkor és csakis akkor kielégíthetetlen, ha nem igaz, hogy F kielégíthető).

Másrészt egy F formula akkor és csakis akkor érvényes, ha $\neg F$ kielégíthetetlen, (lásd 2.10. tétel), tehát azt kapjuk, hogy az érvényesség is eldönthető. Ez pedig ellentmond a 2.31. tételnek. □

2.4. Bizonyítások a pedikátumkalkulusban

Ebben a részben olyan $\mathcal{L}$ nyelveket vizsgálunk, melyek formuláiban csak az $\wedge, \vee, \neg$ logikai szimbólumok és a $\forall$ kvantor szerepel. Továbbá feltesszük, hogy $\mathcal{L}$ predikátumszimbólumai között ott van az $=$ jel. Ennek megfelelően az atomi formulák halmazának a definíciója (2.2. definíció, (b) pont) a következővel egészül ki:

(ii) Ha t_1, t_2 termek, akkor $t_1 = t_2$ atomi formula.

Megjegyezzük, hogy a $t_1 = t_2$ atomi formulában az $=$ jelről csak azt tudjuk, hogy egy bináris reláció, amelynek interpretációja még bármi lehet. Azonban – nem túlságosan meglepő módon – az $=$ interpretációja minden struktúrában az egyenlőség lesz. Ennek megfelelően az atomi formula értékének definíciója egy $\mathcal{A} = (U, \mathcal{I}, \varphi)$ strukúrában (2.8. definíció, (i) pont) így módosul:
Ha F atomi formula, akkor két eset van. Ha F alakja $t_1 = t_2$, akkor $\mathcal{A}(F) = 1$, ha $\mathcal{A}(t_1) = \mathcal{A}(t_2)$, különben pedig 0. A másik eset, amikor $F = p(t_1, \ldots, t_n)$, megegyezik a korábbival.
(Az $\mathcal{A}(t_1) = \mathcal{A}(t_2)$ kifejezésben szereplő $=$ jel viszont már azt jelenti, hogy $\mathcal{A}(t_1)$ és $\mathcal{A}(t_2)$, mint U két eleme, megegyeznek.)

2.33. Definíció. a) Legyen F egy formula. Az F alapvető részformuláinak $\mathrm{arf}(F)$ halmazát a következőképpen definiáljuk:

(i) Ha F atomi formula, vagy $F = \forall x G$ alakú, akkor $\mathrm{arf}(F) = \{F\}$

(ii) Ha $F = \neg G$, $F = G \vee H$ (vagy $F = G \wedge H$), akkor $\mathrm{arf}(F) = \mathrm{arf}(G)$, $\mathrm{arf}(F) = \mathrm{arf}(G) \cup \mathrm{arf}(H)$.

b) Azt a zérusrendű formulát, melyet úgy kapunk F-ből, hogy minden alapvető részformuláját egy ítéletváltozóval helyettesítjük az F *Boole vázának* nevezzük.

2.34. Példa. Legyen

$$F = \forall x p(x, y) \wedge \neg \forall x \neg r(x, y) \wedge (p(z, x) \vee \forall x p(x, y)).$$

Ekkor F alapvető részformulái rendre $\forall x p(x, y)$, $\forall x \neg r(x, y)$ és $p(z, x)$, tehát F Boole váza a

$$p_1 \wedge (\neg p_2) \wedge (p_3 \vee p_1)$$

2.35. Lemma. Ha F olyan formula, melynek Boole váza tautológia, akkor F is tautológia.

Bizonyítás. Legyen $\mathcal{A}$ tetszőleges struktúra. Értékeljük ki $\mathcal{A}$-ban F minden alapvető részformuláját. Ezen kiértékelések definiálnak egy hozzárendelést az F Boole vázában szereplő ítéletváltozókhoz, mely hozzárendelés mellett F Boole váza igaz lesz, mivel tautológia. Ebből az következik, hogy $\mathcal{A} \models F$. □

Axiómák és bizonyítások

Axiómák

AX0: Minden olyan formula, melynek Boole váza tautológia

AX1: (a) Minden t term esetén $t = t$.

(b) Minden $k \geqslant 0$, $t_1, t_1', \ldots, t_k, t_k'$ term és f k-változós függvényszimbólum esetén a $(t_1 = t_1' \wedge \ldots \wedge t_k = t_k') \to (f(t_1, \ldots, t_k) = f(t_1', \ldots, t_k'))$ formula.

(c) Minden $k \geqslant 0$, $t_1, t_1', \ldots, t_k, t_k'$ term és p k-változós predikátumszimbólum esetén a $(t_1 = t_1' \wedge \ldots \wedge t_k = t_k') \to (p(t_1, \ldots, t_k) \to p(t_1', \ldots, t_k'))$ formula.

AX2: Minden $\forall xF \to F[x/t]$ alakú formula, ahol F formula, t pedig egy olyan term amiben nem szerepel olyan y változó melyhez létezik F-nek olyan $\forall yG$ vagy $\exists yG$ alakú részformulája ami tartalmazza x egy F-beli szabad előfordulását.

AX3: Minden $F \to \forall xF$ alakú formula, ahol x nem szabad F-ben.

AX4: Minden $\forall x(F \to G) \to (\forall xF \to \forall xG)$ alakú formula.

Könnyen igazolható, hogy valamennyi axióma érvényes.

Következtetési szabály (modus ponens)

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

Könnyen igazolható, hogy ha F és $F \to G$ érvényes, akkor G is érvényes.

Bizonyítás (levezetés)

2.36. Definíció. a) Legyen Σ formulák egy halmaza. Σ feletti (vagy Σ-ból történő) bizonyításnak formulák egy olyan $F_1, \ldots, F_n$ sorozatát nevezzük, ahol minden $1 \leq i \leq n$ esetén az alábbi feltételek valamelyike teljesül:

1. $F_i \in \Sigma$
2. F_i axióma
3. Van olyan $k, l < i$, hogy $F_l = F_k \to F_i$.

b) Egy F formula bizonyítható (vagy levezethető) Σ-ból, jele $\Sigma \vdash F$, ha van olyan $F_1, \ldots, F_n$ Σ feletti bizonyítás, hogy $F_n = F$.
c) Ha $\Sigma = \emptyset$, akkor $\Sigma \vdash F$ helyett $\vdash F$-et írunk.

A predikátumkalkulusban is igaz a dedukció tétel.

2.37. Tétel. (Dedukció tétel.) *$\Sigma \cup \{F\} \vdash G$ akkor és csak akkor, ha $\Sigma \vdash F \to G$.*

Bizonyítás. A bizonyítás analóg az az ítéletkalkulusban adott bizonyítással. □

Az elsőrendű levezetés teljessége

2.38. Tétel. (Gödel teljességi tétele.) *$\Sigma \vdash F$ akkor és csak akkor teljesül, ha $\Sigma \models F$.*

Bizonyítás. A helyesség egyszerű, a teljesség a tétel egy másik alakjából következik. □

Gödel teljességi tételének másik alakja a következőképpen fogalmazható meg.

2.39. Definíció. Σ formulahalmaz konzisztens, ha nem vezethető le belőle minden formula. (különben Σ inkonzisztens.)

2.40. Tétel. (A Gödel teljességi tétel másik alakja). *Ha Σ konzisztens, akkor van modellje.*

Bizonyítás. Hosszú. □

Az első alak bizonyítása a másodikból. Tegyük fel, hogy $\Sigma \models F$. Ha $\Sigma \models F$, akkor $\Sigma \cup \{\neg F\}$ kielégíthetetlen, tehát (a Gödel tétel második alakja miatt) inkonzisztens. Tehát $\Sigma \cup \{\neg F\} \vdash F$ A dedukció tétel miatt $\Sigma \vdash \neg F \to F$. Továbbá, $(\neg F \to F) \to F$ Boole váza tautológia, tehát axióma. Így Modus ponenssel kapjuk, hogy $\Sigma \vdash F$.

Elméletek, axiomatizálás

2.41. Definíció. Elméletnek nevezzük formulák egy Σ nemüres halmazát, ha van modellje (konzisztens) és zárt a logikai következményre, vagyis valahányszor $\Sigma \models F$ mindannyiszor $F \in \Sigma$.

A definícióból következik, hogy minden elmélet tartalmazza az érvényes formulákat.
Ha Σ egy olyan formulahalmaz, amelynek van modellje, akkor

$$Cn(\Sigma) = \{F \mid \Sigma \models F\}$$

elmélet. Például $Cn(\varnothing)$ az összes érvényes formulákból álló elmélet.
Ugyancsak elmélet az összes olyan formulák halmaza, melyeket egy $\mathcal{A}$ struktúra kielégít, vagyis

$$Th(\mathcal{A}) = \{F \mid \mathcal{A} \models F\}$$

is elmélet.

2.42. Példa. a) Legyenek 0, 1 nullaváltozós, $+$, $*$ kétváltozós függvényszimbólumok, $<$ kétváltozós predikátumszimbólum és $\mathcal{A} = (N, \mathcal{I})$ az a struktúra, ahol ahol N a természetes számok halmaza, $\mathcal{I}$ pedig a sztenderd interpretáció: $\mathcal{I}(0) = 0$, $\mathcal{I}(1) = 1$, $\mathcal{I}(+)$ sz összeadás, stb. Akkor például

$$\forall x \forall y((x + y) * (x + y) = (x * x) + (x * y) + (x * y) + (y * y)),$$

$$\forall x(x < x + 1)$$

a $Th(\mathcal{A})$ elemei. A $Th(\mathcal{A})$ elmélet neve a Peano aritmetika, jele PA.
b) Legyenek 0, 1 nullaváltozós, $+$ kétváltozós függvényszimbólum, $<$ kétváltozós predikátumszimbólum és $\mathcal{A} = (N, \mathcal{I})$ az a struktúra, ahol ahol N a természetes számok halmaza, $\mathcal{I}$ pedig a sztenderd interpretáció. Ekkor $Th(\mathcal{A})$-t Presburger aritmetikának nevezük.

Egy Σ elmélet teljes, ha minden zárt F formula esetén $F \in \Sigma$ vagy $\neg F \in \Sigma$. (Ugyanakkor F és $\neg F$ egyszerre nem lehetnek Σ-ban, mivel Σ konzisztents.)

2.43. Tétel. *Tetszőleges Σ elméletre, a következő három állítás ekvivalens:*

(1) Σ *teljes,*

(2) van olyan $\mathcal{A}$ *struktúra, hogy* $\Sigma = Th(\mathcal{A})$,

(3) Σ *minden* $\mathcal{A}$ *modelljére* $\Sigma = Th(\mathcal{A})$.

Bizonyítás. (3) $\Rightarrow$ (2): Mivel Σ elmélet, van olyan $\mathcal{A}$ struktúra, hogy $\mathcal{A} \models \Sigma$. Ekkor (3) miatt $\Sigma = Th(\mathcal{A})$.
(2) $\Rightarrow$ (1): Legyen F egy zárt formula. Ekkor $\mathcal{A} \models F$ vagy $\mathcal{A} \models \neg F$. Ezért, $\Sigma = Th(\mathcal{A})$ miatt, $F \in \Sigma$ vagy $\neg F \in \Sigma$.
(1) $\Rightarrow$ (3): Tegyük fel, hogy $\mathcal{A} \models \Sigma$. Ekkor $\Sigma \subseteq Th(\mathcal{A})$. Tegyük fel, hogy van olyan $F \in Th(\mathcal{A})$, hogy $F \notin \Sigma$. Mivel Σ teljes, $\neg F \in \Sigma$. De akkor $\mathcal{A} \models \neg F$, ami ellentmondás. □

A fenti tételből következik, hogy mind a Peano aritmetika, mind a Presburger aritmetika teljesek (mert $Th(\mathcal{A})$ alakúak). Nem teljes viszont például az összes érvényes formulákból álló elmélet.
Ugyanakkor, nem következik, hogy ha egy elmélet teljes, akkor annak csak egy modellje van. Például, a Peano aritmetikának több modellje is van.

2.44. Definíció. Egy Σ elmélet axiomatizálható, ha van olyan rekurzív Δ formulahalmaz, – az axiómarendszer – hogy

$$\Sigma = \{F \mid \Delta \vdash F\}.$$

Ha Δ még véges is, akkor Σ végesen axiomatizálható.

Ha egy Σ elmélet axiomatizálható és Δ az axiómarendszer, akkor persze a 2.38. tétel miatt $\Sigma = Cn(\Delta)$.

2.45. Példa. a) Az összes érvényes formulák halmaza axiomatizálható, mert $\Delta = \varnothing$ egy axiómarendszere. (Gödel teljességi tétele miatt $\models F$, akkor és csak akkor teljesül, ha $\vdash F$, tehát $\{F \mid \vdash F\}$ az összes érvényes formulák hamaza.) Ugyanakkor ez az elmélet nem eldönthető, lásd 2.31. tétel.

b) Legyen 0 egy nullaváltozós, S egy egyváltozós függvényszimbólum. Legyen $\mathcal{A} = (N, \mathcal{I})$ az a struktúra, melyben $\mathcal{I}(0) = 0$ és minden $n \in N$-re $\mathcal{I}(S)(n) = n + 1$. Ekkor $Th(\mathcal{A})$-t a természetes számok rákövetkezés függvénnyel ellátott elméletének nevezzük. $Th(\mathcal{A})$ axiomatizálható a következő Z végtelen, de eldönthető axiómarendszerrel:

$$\begin{aligned} Z \quad = \quad & \{\forall x \neg(S(x) = 0), \\ & \forall x, y(S(x) = S(y) \to x = y), \\ & \forall x(\neg(x = 0) \to \exists y(x = S(y))), \\ & \forall x \neg(x = S(x)), \\ & \forall x \neg(x = S(S(x))), \\ & \ldots\} \end{aligned}$$

Mivel $Th(\mathcal{A})$ teljes, ezért eldönthető is.

c) A Presburger aritmetika eldönthető, ezért definíció szerint axiomatizálható. (Axiómaremdszer az $\mathcal{A}$-ban érvényes formulák halmaza.)

Kérdés, hogy minden elmélet axiomatizálható-e? A válasz az, hogy nem, sőt már PA sem axiomatizálható.

2.46. Tétel. (Gödel nemteljességi tétele). *Nincsen olyan Δ (rekurzívan felsorolható) axiómarendszer, melyre minden F formula esetén $\Delta \vdash F$ akkor és csakis akkor teljesül, ha $F \in PA$.*

Bizonyítás. Túl messzire vezetne.

2.5. Herbrand tétele és alkalmazásai

2.47. Definíció. (Herbrand univerzum.) Legyen F egy formula. Az F *Herbrand univerzuma* a következőképpen definiált $D(F)$ term-halmaz.

1. Minden F-ben előforduló konstans (vagyis 0-változós függvényszimbólum) legyen $D(F)$-ben. Ha F nem tartalmaz konstanst, akkor legyen $a \in D(F)$.
2. Ha $t_1, \ldots, t_m \in D(F)$, f pedig F-ben előforduló m változós függvényszimbólum, akkor $f(t_1, \ldots, t_m) \in D(F)$.

2.48. Példa.

a) Ha $F = \forall x \forall y \forall z p(x, f(y), g(z, x))$, akkor
$D(F) = \{a, f(a), g(a, a), g(f(a), a), g(f(a), f(a)), f(f(a)), f(g(a, a)), \ldots\}$.

b) Ha $F = \forall x \forall y p(b, f(x), g(c, y))$, akkor
$D(F) = \{b, c, f(b), f(c), g(c, b), f(f(b)), f(f(c)), g(c, f(f(b))) \ldots\}$.

2.49. Definíció. (Herbrand struktúra.) Legyen F egy formula. Az $\mathcal{A} = (U, \mathcal{I}, \varphi)$ struktúra az F *egy Herbrand struktúrája*, ha teljesülnek rá a következő feltételek.

1. $U = D(F)$
2. Minden F-ben előforduló m változós f függvényszimbólumra, $t_1, \ldots, t_m \in D(F)$ -re $\mathcal{I}(f)(t_1, \ldots, t_m) = f(t_1, \ldots, t_m)$.
3. Ha F-ben nincs konstans (és ezért $a \in D(F)$), akkor $\mathcal{I}(a) = a$.
4. A relációk interpretációi és φ tetszőlegesek.

2.50. Példa. Az megelőző példában

a) $\mathcal{I}(g)(f(a), a) = g(f(a), a), \mathcal{I}(f)(a) = f(a), \ldots$

b) $\mathcal{I}(g)(f(c), b) = g(f(c), b), \ldots$

2.51. Lemma. Legyen F egy formula, $\mathcal{A} = (U, \mathcal{I}, \varphi)$ pedig F egy Herbrand struktúrája. Akkor minden $t \in D(F)$ esetén $\mathcal{A}(t) = t$.

Bizonyítás. A t term felépítése szerinti indukcióval egyszerűen elvégezhető. □

2.52. Lemma. (Helyettesítési lemma Herbrand struktúrákra.) Legyen F egy formula, $x_1, \ldots, x_n$ különböző szabad változók, $\mathcal{A} = (D(F), \mathcal{I})$ az F egy Herbrand struktúrája és $t_1, \ldots, t_n \in D(F)$. Akkor $\mathcal{A}(F[x_1/t_1] \ldots [x_n/t_n]) = \mathcal{A}_{[x_1/t_1] \ldots [x_n/t_n]}(F)$.

Bizonyítás. Mivel $\mathcal{A}$ Herbrand struktúra, a 2.51. lemma szerint minden $t \in D(F)$ termre $\mathcal{A}(t) = t$. Így, a 2.18. lemma alkalmazásával kapjuk, hogy

$$\mathcal{A}(F[x_1/t_1] \ldots [x_n/t_n]) = \mathcal{A}_{[x_1/\mathcal{A}(t_1)] \ldots [x_n/\mathcal{A}(t_n)]}(F) = \mathcal{A}_{[x_1/t_1] \ldots [x_n/t_n]}(F).$$

□

A következő tételben bebizonyítjuk, hogy amennyiben egy zárt Skolem normálforma kielégíthetőségéről akarunk meggyőződni, akkor elegendő csak a Herbrand struktúrái között keresgélni és nem kell valamennyi struktúrát vizsgálni.

2.53. Tétel. Legyen F egy zárt Skolem normálforma. F akkor és csak akkor elégíthető ki, ha F-nek van Herbrand modellje.

Bizonyítás. Ha F-nek van Herbrand modellje, akkor kielégíthető.

Megfordítva, tegyük fel, hogy F kielégíthető, vagyis, hogy az $\mathcal{A} = (U, \mathcal{I})$ struktúra modellje F-nek.
Ha F-ben nincs konstans, akkor a $D(F)$-ben szereplő a konstansra (lásd 2.47. definíció), legyen $\mathcal{I}(a) = u$, ahol u az U egy tetszőleges eleme. Ezáltal minden $t \in D(F)$-re $\mathcal{A}(t) \in U$ definiált lesz.

Legyen $\mathcal{A}' = (D(F), \mathcal{I}')$ F-nek az a Herbrand struktúrája, amelyben

- a függvények a Herbrand struktúra szabályai szerint vannak definiálva.
- minden, F-ben előforduló m változós p predikátumszimbólum és $t_1, \ldots, t_m \in D(F)$ esetén legyen

$$\mathcal{I}'(p)(t_1, \ldots, t_m) = 1 \iff \mathcal{I}(p)(\mathcal{A}(t_1) \ldots \mathcal{A}(t_m)) = 1.$$

Azt állítjuk, hogy $\mathcal{A}' \models F$.

Többet igazolunk, nevezetesen azt, hogy minden, az F szimbólumaiból (ha F-ben nincs konstans akkor F szimbólumaiból és a-ból) felépülő G zárt Skolem normálforma esetén, ha $\mathcal{A} \models G$, akkor $\mathcal{A}' \models G$. (Állításunk bizonyítását a $G = F$ választással kapjuk.)

Ezen utóbbi állítás bizonyítását a G-ben szereplő univerzális kvantorok száma szerinti indukcióval végezzük el. Tegyük fel, hogy G-ben n darab univerzális kvantor szerepel.

(i) Ha $n = 0$, akkor a feltétel miatt G-ben nem szerepelnek változók, tehát G egy olyan formula, amely ground atomi formulákból és logikai szimbólumokból épül fel. Ezért $\mathcal{A}'(G) = \mathcal{A}(G)$.

Ezt a G-ben szereplő logikai szimbólumok száma szerinti indikcióval bizonyíthatjuk be.

Ha G-ben nem szerepel logikai változó, akkor $G = p(t_1, \ldots, t_m)$ valamely p predikátumszimbólum és $t_1, \ldots, t_m$ termek esetén. Így

$$\begin{array}{ll} & \mathcal{A}'(p(t_1, \ldots, t_m)) \\ = & \mathcal{I}'(p)(\mathcal{A}'(t_1), \ldots, \mathcal{A}'(t_m)) \\ = & \mathcal{I}'(p)(t_1, \ldots, t_m) \qquad \text{(mert } \mathcal{A}' \text{ Herbrand struktúra)} \\ = & \mathcal{I}(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_m)) \qquad (\mathcal{I}' \text{ definíciója}) \\ = & \mathcal{A}(p(t_1, \ldots, t_m)). \end{array}$$

Ha G-ben szerepel logikai szimbólum, akkor $G = \neg G_1$, $G = G_1 \vee G_2$ vagy $G = G_1 \wedge G_2$. Például a harmadik esetben

$$\begin{array}{ll} & \mathcal{A}(G) = 1 \\ \iff & \mathcal{A}(G_1) = 1 \text{ és } \mathcal{A}(G_2) = 1 \\ \iff & \mathcal{A}'(G_1) = 1 \text{ és } \mathcal{A}'(G_2) = 1 \\ & (G_1\text{-ben és } G_2\text{-ben kevesebb logikai szimbólum van mint } G\text{-ben}) \\ & \mathcal{A}'(G) = 1. \end{array}$$

(ii) Tegyük fel, hogy G-ben $n+1$ univerzális kvantor van. Akkor $G = \forall x H$, ahol H n darab univerzális kvantort tartalmaz. Mivel $\mathcal{A} \models G$, minden $u \in U$ esetén $\mathcal{A}_{[x/u]}(H) = 1$. Speciálisan minden $t \in D(G)$-re $\mathcal{A}_{[x/\mathcal{A}(t)]}(H) = 1$ (ekkor $u = \mathcal{A}(t)$).

Ugyanakkor, a 2.18. lemma miatt $\mathcal{A}_{[x/\mathcal{A}(t)]}(H) = \mathcal{A}(H[x/t])$, tehát $\mathcal{A}(H[x/t]) = 1$.

A $H[x/t]$ formula egy n kvantort tartalmazó zárt Skolem normálforma, így az indukció feltevés szerint $\mathcal{A}'(H[x/t]) = 1$.

Azt kaptuk, hogy minden $t \in D(G)$-re $\mathcal{A}'(H[x/t]) = 1$, tehát, a 2.52. lemma miatt, minden $t \in D(G)$-re $\mathcal{A}'_{[x/t]}(H) = 1$. Ez pedig éppen azt jelenti, hogy $\mathcal{A}' \models \forall x H = G$. □

2.54. Következmény. (Löweinhem-Skolem tétel) Minden kielégíthető formulának van megszámlálható modellje.

Bizonyítás. Legyen F kielégíthető formula. Ekkor (a 2.30. lemmában szereplő transzformációkat alkalmazva) van egy olyan zárt G Skolem normálforma, amely s-ekvivalens F-el (tehát kielégíthető). A 2.53. tétel miatt G-nek van Herbrand modellje, melynek univerzuma megszámlálható. Továbbá, ugyancsak a 2.30. lemma miatt, G minden modellje, és így minden $\mathcal{A} = (D(G), \mathcal{I})$ Herbrand modellje esetén is, van olyan φ hozzárendelés, hogy $\mathcal{B} = (D(G), \mathcal{I}, \varphi)$ modellje lesz F-nek. Tehát F-nek van megszámlálható modellje. □

2.55. Definíció. (Herbrand kiterjesztés.) Legyen F egy zárt Skolem normálforma. (Tehát $F = \forall x_1 \ldots \forall x_m F^*$, ahol F^* az F mátrixa.) Akkor az F Herbrand kiterjesztése az

$$E(F) = \{F^*[x_1/t_1] \ldots [x_m/t_m] \mid t_1, \ldots, t_m \in D(F)\}$$

formulahalmaz.

Megjegyezzük, hogy $E(F)$ elemei ground atomi formulákból és logikai szimbólumokból felépülő formulák.

2.56. Példa. Legyen $F = \forall x \forall y p(a, f(x), g(b, y))$. Akkor

$$E(F) = \{p(a, f(a), g(b, a)), p(a, f(b), g(b, a)), p(a, f(b), g(b, f(a))), p(a, f(f(b)), g(b, f(a))), \ldots\}.$$

2.57. Tétel. (Gödel-Herbrand-Skolem.) *Legyen F egy zárt Skolem normálforma. F akkor és csak akkor elégíthető ki, ha $E(F)$ kielégíthető.*

Bizonyítás. Legyen $F = \forall x_1 \ldots \forall x_m F^*$. Ekkor a következő számolás adódik:

	F kielégíthető	
$\Longleftrightarrow$	van Herbrand modelje	(2.53. tétel)
$\Longleftrightarrow$	van $\mathcal{A} = (D(F), \mathcal{I})$ H-struktúra, melyre $\mathcal{A}(F) = 1$	(2.49. definíció)
$\Longleftrightarrow$	van $\mathcal{A} = (D(F), \mathcal{I})$, melyre minden $t_1, \ldots, t_m \in D(F)$ esetén $\mathcal{A}_{[x_1/t_1]\ldots[x_m/t_m]}(F^*) = 1$	(2.8. definíció)
$\Longleftrightarrow$	van $\mathcal{A} = (D(F), \mathcal{I})$, melyre minden $t_1, \ldots, t_m \in D(F)$ esetén $\mathcal{A}(F^*[x_1/t_1]\ldots[x_m/t_m]) = 1$	(2.52. lemma)
$\Longleftrightarrow$	van $\mathcal{A} = (D(F), \mathcal{I})$ melyre minden $G \in E(F)$ esetén $\mathcal{A}(G) = 1$	(2.55.definíció)
$\Longleftrightarrow$	$E(F)$ kielégíthető.	

□

A fenti tételből az következik, hogy egy tetszőleges elsőrendű formula kielégíthetőségének vizsgálata visszavezethető megszámlálhatóan végtelen sok ground elsőrendű formula kielégíthetőségének vizsgálatára. Ez utóbbi viszont a zérusrendű logika és a változók nélküli elsőrendű kalkulus közötti kapcsolat miatt ekvivalens megszámlálhatóan végtelen sok zérusrendű formula kielégíthetőségének vizsgálatával. Innen valamint a kompaktsági tételből azonnal adódik a következő eredmény.

2.58. Tétel. *Legyen F egy zárt Skolem normálforma. F akkor és csakis akkor kielégíthetetlen, ha $E(F)$-nek van olyan véges részhalmaza, ami kielégíthetetlen.*

Bizonyítás. A következő számolással adódik:

	F kielégíthetetlen	
$\Longleftrightarrow$	$E(F)$ kielégíthetetlen	(2.57. tétel)
$\Longleftrightarrow$	$E(F)$ valamely véges részhalmaza kielégíthetetlen	(1.60. tétel)

□

Parciális eldöntési algoritmusnak egy olyan algoritmust nevezünk, amely a probléma igen példányaira *Igen* outputtal áll meg, míg a nem példányaira nem áll meg.

A megelőző tételből egy parciális algoritmust kapunk annak eldöntésére, hogy egy formula kielégíthetetlen-e. Tehát, F input formula esetén a parciális algoritmus *Igen*-ben áll meg, ha F kielégíthetetlen és nem áll meg, különben. (Ugyanakkor persze a kielégíthetetlenség algoritmikusan eldönthetetlen, lásd 2.32. Következmény.)

2.59. Tétel. *Az elsőrendű formulák kielégíthetetlensége parciálisan eldönthető.*

Bizonyítás. Egy algoritmust adunk meg, amely minden F formula esetén, ha F kielégíthetetlen akkor megáll és *Igen* outputot ad ki. (Amennyiben F kielégíthető úgy az algoritmus nem áll meg.) Feltételezzük, hogy F-et már zárt Skolem normálformává alakítottuk.

Algoritmus

Input: Egy F zárt Skolem normálforma
Output: *Igen*, ha F kielégíthetetlen.

1. $n := 0$
2. $n := n + 1$
3. Állítsuk elő $E(F)$ n-edik elemét, legyen ez F_n.
4. Ha $F_1 \wedge \ldots \wedge F_n$ kielégíthetetlen, akkor az algoritmus álljon meg és adjon *Igen* outputot, különben ugorjon 2-re.

2.60. Következmény. *Az elsőrendű formulák érvényessége parciálisan eldönthető.*

Bizonyítás. Legyen F egy tetszőleges formula. Mivel F akkor és csakis akkor érvényes, ha $\neg F$ kielégíthetetlen, $\neg F$-et zárt Skolem normálformává alakítjuk, majd alkalmazhatjuk az előbbi algoritmust. □

2.61. Következmény. *Az elsőrendű formulák kielégíthetősége még parciálisan sem dönthető el.*

Bizonyítás. Azonnal adódik a 2.59. tételből. □

2.6. Elsőrendű rezolúció

A ground eset

Legyen F egy olyan formula amely ground atomi formulákból épül fel a $\neg, \wedge$ és $\vee$ műveleti jelek segítségével, úgy, hogy F konjunktív normálforma is.

A ground elsőrendű formulák és a zérusrendű formulák között fennálló kapcsolat miatt azt, hogy F kielégíthetetlen-e, eldönthetjük a zérusrendű rezolúcióhoz igen közel álló úgynevezett ground elsőrendű rezolúcióval.

A ground rezolúció esetén egy literál $p(t_1, \ldots, t_n)$, vagy $\neg p(t_1, \ldots, t_n)$ alakú, ahol a $t_1, \ldots, t_n$ ground termek. (Vegyük észre, hogy a zérusrendű literál ennek az $n = 0$ esetből kapott speciális esete.)

Ettől kezdve a ground (elsőrendű) rezolúció ugyanúgy működik, mint a zérusrendű rezolúció, lásd 1.75., 1.80. definíciók és 1.85. tétel.

Ezt egy példán keresztül mutatjuk be:

2.62. Példa. *Legyen*

$$\begin{aligned} F = & (p(a, f(b)) \vee q(b) \vee r(f(a), a)) \\ \wedge & \quad \neg p(a, f(b)) \\ \wedge & \quad (p(a, f(b)) \vee q(b) \vee \neg r(f(a), a)) \\ \wedge & \quad (p(a, f(b)) \vee \neg q(b)) \end{aligned}$$

F tehát egy elsőrendű ground konjunktív normálforma. Bizonyítsuk be (rezolúcióval), hogy F kielégíthetetlen. F klózait most is átírhatjuk halmaz alakba.

1. $\{p(a, f(b)), q(b), r(f(a), a)\}$	F-beli klóz
2. $\{p(a, f(b)), q(b), \neg r(f(a), a)\}$	F-beli klóz
3. $\{p(a, f(b)), q(b)\}$	rezolúcióval kapjuk 1-ből és 2-ből
4. $\{p(a, f(b)), \neg q(b)\}$	F-beli klóz
5. $\{p(a, f(b))\}$	rezolúcióval kapjuk 3-ból és 4-ből
6. $\{\neg p(a, f(b))\}$	F-beli klóz
7. $\square$	rezolúcióval kapjuk 5-ből és 6-ból

$\square$

Legyen most F egy olyan zárt Skolem normálforma, melynek F^* mátrixa konjunktív normálforma. A 2.58. és 2.59. tételek miatt F akkor és csakis akkor kielégíthetetlen, ha van olyan $n \geqslant 1$, hogy $F_1 \wedge \ldots \wedge F_n$ kielégíthetetlen, ahol $F_1, F_2, \ldots$ az $E(F)$ elemeinek egy felsorolása. Ha F^* konjunktív normálforma, akkor minden F_i is az, sőt ground konjunktív normálforma. Ugyanez érvényes $F_1 \wedge \ldots \wedge F_n$-re is, mivel úgy kapjuk, hogy ground konjunktív normálformákat kapcsolunk össze az $\wedge$ jellel.

Következésképpen, azt, hogy $F_1 \wedge \ldots \wedge F_n$ kielégíthetetlen-e eldönthetjük ground elsőrendű rezolúcióval.

A fentieket összefoglalva egy F zárt Skolem normálforma akkor és csak akkor kielégíthetetlen, ha van olyan $n \geqslant 1$, hogy $F_1 \wedge \ldots \wedge F_n$-ből, (vagy halmaz alakban írva $\{F_1, \ldots, F_n\}$-ből) bizonyítható $\square$ ground rezolúcióval, ahol $F_1, F_2, \ldots$ az $E(F)$ elemeinek egy felsorolása.
Innen kapjuk a következő tételt:

2.63. Tétel. (Ground rezolúció elsőrendű formulákra, v.ö. 1.85. tétel.) *Legyen F egy zárt Skolem normálforma, melynek mátrixa konjunktív normálformában van. F akkor és csakis akkor kielégíthetetlen, ha van olyan $C_1, \ldots, C_n$ sorozat, amely eleget tesz a következő feltételeknek:*

1. *$C_n = \square$*
2. *Minden $1 \leqslant i \leqslant n$-re C_i az $E(F)$ valamely elemének egy klóza vagy van olyan $1 \leqslant k, l < i$, hogy C_i-t a C_k-ból és C_l-ből kapjuk (elsőrendű) ground rezolúcióval.*

Vegyük észre, hogy a fenti tétel ugyancsak egy parciális algoritmust ad annak eldöntésére, hogy F kielégíthetetlen-e. Ugyanis a rezolúció szervezhető úgy, hogy ha F kielégíthetetlen, akkor megtalálja $\square$-t, ha viszont F kielégíthető, akkor a végtelenségig fut.

2.64. Példa. a) Legyen $F = \forall x(p(x) \wedge \neg p(f(x)))$, mutassuk meg, hogy F kielégíthetetlen. Mivel F^* konjunktív normálforma, alkalmazzuk a ground rezolúciót.

- $D(F)$ elemei: $a, f(a), f(f(a)), \ldots$
- $E(F)$ elemei: $F_1 = p(a) \wedge \neg p(f(a)), F_2 = p(f(a)) \wedge \neg p(f(f(a))), \ldots$

Azonnal adódik a következő rezolúció:

1. $\neg p(f(a))$	F_1 egy klóza
2. $p(f(a))$	F_2 egy klóza
3. $\square$	ground rezolúcióval 1-ből és 2-ből.

b) Legyen $F = \forall x \forall y((\neg p(x) \vee \neg p(f(a)) \vee q(y)) \wedge p(y) \wedge (\neg p(g(b,x)) \vee \neg q(b)))$. Bizonyítsuk be, hogy F kielégíthetetlen. Mivel

$$\begin{aligned} F^* &= \{\{\neg p(x), \neg p(f(a)), q(y)\}, \{p(y)\}, \{\neg p(g(b,x)), \neg q(b)\}\} \\ &= \{C_1, C_2, C_3\} \end{aligned}$$

a következő rezolúciós számolás adódik.

1. $\{\neg p(f(a)), q(b)\}$	C_1-ből $[x/f(a)][y/b]$ helyettesítéssel
2. $\{p(f(a))\}$	C_2-ből az $[y/f(a)]$ helyettesítéssel
3. $\{q(b)\}$	rezolúcióval kapjuk 1-ből és 2-ből
4. $\{p(g(b,a))\}$	C_2-ből $[y/g(b,a)]$ helyettesítéssel
5. $\{\neg p(g(b,a)), \neg q(b)\}$	C_3-ból az $[x/a]$ helyettesítéssel
6. $\{\neg q(b)\}$	rezolúcióval kapjuk 4-ből és 5-ből
7. $\square$	rezolúcióval kapjuk 3-ból és 6-ból

□

Most azt vizsgáljuk, hogy $E(F)$ kielégíthetetlenségének eldöntését hogyan tudnánk hatékonyabban végezni.

A 2.64. példából az alábbi következtetéseket vonjuk le:

1. $E(F)$ elemeinek felsorolásával fölösleges klózokat is előállíthatunk (lásd a) példát).
2. A helyettesítéseket (vagyis a ground példányok előállítását) célszerű F^* klózaira külön-külön végezni, nem pedig magára F^*-ra (a) és b) példák).
3. Egy klóznak több ground példányára is szükség lehet $\square$ levezetéséhez. (b) példa 2. és 4. lépések).
4. Egy n elemű klózból egy helyettesítés után m $(< n)$ elemű ground klóz is keletkezhet (b) példa 1. lépés).

Ugyancsak észrevehető, hogy a $\square$ levezetéséhez esetleg nem is szükséges kizárólag ground helyettesítéseket találni (és így nagyméretű ground klózokat tárolni). Ezt mutatjuk be a következő példán.

2.65. Példa. Mutassuk meg, hogy az $F = \forall x \forall y(p(x, g(y)) \wedge \neg p(f(y), x))$ formula nem kielégíthető. Legyen $C_1 = \{p(x, g(y))\}$ és $C_2 = \{\neg p(f(y), x)\}$

1. $\{p(f(z), g(y)\}$	C_1 -ből az $[x/f(z)]$ helyettesítéssel
2. $\{\neg p(f(z), g(y)\}$	C_2 -ből az $[y/z][x/g(y)]$ helyettesítéssel
3. $\square$	rezolúcióval 1-ből és 2-ből

□

A fenti példa 3. lépésében végzett rezolúciót (habár az nem ground és így nem igazolható a zérusrendű rezolúciónál megismert tételekkel) az teszi jogossá, hogy az 1. és 2. lépésekben szereplő klózokhoz már nyilvánvalóan található olyan ground helyettesítés, melynek elvégzése után ground rezolúzió alkalmazható. Ilyen helyettesítés például az $[z/a][y/a]$.

A továbbiakban ezen észrevételekből kiindulva szeretnénk kifejleszteni egy hatékony elsőrendű rezolúciós bizonyítási módszert.

Unifikáció

2.66. Definíció. Legyen $sub = [x_1/t_1]\dots[x_n/t_n]$ helyettesítések egy sorozata, melyet az $n = 0$ esetben $[\,]$-val jelölünk. Tetszőleges t term esetén a $t\,sub$ termet n szerinti indukcióval definiáljuk:

(i) Ha $sub = [\,]$, akkor $t\,sub = t$.

(ii) Ha $sub = [x_1/t_1]\dots[x_n/t_n]$, valamely $n \geqslant 1$ -re, akkor $t\,sub = (t\,sub')[x_n/t_n]$, ahol sub' jelöli az $[x_1/t_1]\dots[x_{n-1}/t_{n-1}]$ helyettesítést.

Van két olyan speciális helyettesítés, melyeket külön névvel is szokás ellátni. Legyen $sub = [x_1/t_1]\dots[x_n/t_n]$ egy helyettesítés.

a) Ha $t_1, \dots, t_n$ ground termek, akkor sub-ot ground helyettesítésnek nevezzük.

b) Ha $x_1, \dots, x_n$ páronként különböző változók, valamint ugyanez teljesül $t_1, \dots, t_n$-re is, akkor sub-ot változó átnevezésnek hívjuk.

□

2.67. Példa. Legyen $t = f(x, g(y))$.

a) Ha $sub = [x/g(x)][y/a]$, akkor

$$\begin{aligned} & t\,sub \\ = \;& (t[x/g(x)])[y/a] \\ = \;& f(g(x), g(y))[y/a] \\ = \;& f(g(x), g(a)). \end{aligned}$$

b) Ha $sub = [x/g(b)][y/a]$, akkor sub ground helyettesítés és $t\,sub = f(g(b), g(a))$.

c) Ha $sub = [x/u][y/v]$, akkor sub változó átnevezés és $t\,sub = f(u, g(v))$.

□

2.68. Definíció. Legyen sub egy helyettesítés és ℓ egy literál. Akkor

$$\ell\,sub = \begin{cases} p(t_1 sub, \dots, t_n sub) & , \text{ ha } \ell = p(t_1, \dots, t_n) \\ \neg p(t_1 sub, \dots, t_n sub) & , \text{ ha } \ell = \neg p(t_1, \dots, t_n) \end{cases}$$

Továbbá, ha $L = \{\ell_1, \dots, \ell_k\}$ literálok egy halmaza, sub pedig egy helyettesítés, akkor $L\,sub = \{\ell_1 sub, \dots, \ell_k sub\}$.

Ha sub ground helyettesítés, akkor azt mondjuk, hogy $L\,sub$ az L egy *ground példánya.* (Ez esetben $L\,sub$ ground literálokból áll.)

□

2.69. Definíció. Legyen $L = \{\ell_1, \dots, \ell_k\}$ literálok egy halmaza, sub pedig egy helyettesítés. Azt mondjuk, hogy sub az L egyesítője, ha $L\,sub$ egyelemű halmaz, vagyis, ha $\ell_1 sub = \dots = \ell_k sub$ teljesül. L egyesíthető (vagy: unifikálható), ha van egyesítője. Továbbá sub az L legkisebb egyesítője, ha L bármely további sub' egyesítője esetén van olyan s helyettesítés, hogy $sub' = sub\,s$. □

2.70. Példa. Az $L = \{p(f(x), y), p(f(a), u)\}$ halmaz egyesíthető, mert a $sub = [x/a][u/y]$ helyettesítés egyesíti. Ez egyúttal L legkisebb egyesítője. Ugyanakkor könnyen látható, hogy $L_1 = \{p(f(x), z), p(a, u)\}$ nem egyesíthető.

□

Az, hogy egy literálhalmaz unifikálható-e, algoritmikusan eldönthető, sőt a legkisebb egyesítő is megkonstruálható.

2.71. Tétel. (Unifikációs tétel.) *Tetszőleges L literálhalmazról eldönthető, hogy unifikálható-e vagy sem. Ha L unifikálható, akkor a legkisebb egyesítője megkonstruálható.*

Bizonyítás. Algoritmus (Unifikációs algoritmus)

Input: L literálhalmaz
Output: L legkisebb egyesítője, ha L unifikálható, különben *nem*.

$sub := [\,]$
while $|\, L\,sub\,| > 1$ **do**
begin
Hasonlítsuk össze $Lsub$ elemeit és keressük meg a legelső olyan pozíciót,
ahol két literál, ℓ_1 és ℓ_2 különböznek.
if A két különböző szimbólum egyike sem változó
then begin output: *nem*; **stop**; **end**
else begin
Legyen x a változó és t a term, amelyek ℓ_1-nek és ℓ_2-nek
a szóban forgó pozícióján kezdődnek.
if x előfordul t-ben
then begin output: *nem*; **stop**; **end**
else $sub := sub[x/t]$
end if
end if
end while;
output: sub /* az L legkisebb egyesítője */

2.72. Példa. Egyesíthető-e az $L = \{\neg p(f(z, g(a, y)), h(z)), \neg p(f(f(u, v), w), h(f(a, b)))\}$ halmaz? Ha igen adjuk meg a legkisebb egyesítőjét!

Alkalmazzuk az unifikációs algoritmust.

$sub := [\,]$

1. $\neg p(f(z, g(a, b)), h(z)) = \ell_1$
2. $\neg p(f(f(u, v), w), h(f(a, b))) = \ell_2$

Az első pozíción, ahol ℓ_1 és ℓ_2 különböznek, ℓ_1-ben z, ℓ_2-ben $f(u, v)$ van, tehát $sub := [\,][z/f(u, v)] = [z/f(u, v)]$.

1. $\neg p(f(f(u, v), g(a, y)), h(f(u, v))) = \ell_1 sub$
2. $\neg p(f(f(u, v), w), h(f(a, b))) = \ell_2 sub$

$sub := [z/f(u, v)][w/g(a, y)]$

1. $\neg p(f(f(u,v),g(a,y)),h(f(u,v))) = \ell_1 sub$
2. $\neg p(f(f(u,v),g(a,y)),h(f(a,b))) = \ell_2 sub$

   $sub := [z/f(u,v)][w/g(a,b)][u/a]$

1. $\neg p(f(f(a,v),g(a,y)),h(f(a,v))) = \ell_1 sub$
2. $\neg p(f(f(a,v),g(a,y)),h(f(a,b))) = \ell_2 sub$

   $sub := [z/f(u,v)][w/g(a,y)][u/a][v/b]$

Mivel ekkor $\ell_1 sub = \ell_2 sub = \neg p(f(f(a,b),g(a,y)),h(f(a,b)))$, a két literál ℓ_1 és ℓ_2 egyesíthető és sub a legkisebb egyesítője.

□

Az általános eset

2.73. Definíció. Legyenek C_1 és C_2 (elsőrendű) klózok. Az R klóz a C_1 és a C_2 egy rezolvense, ha teljesülnek a következő feltételek.

1. Vannak olyan s_1, s_2 változó átnevezések, hogy $C_1 s_1$ és $C_2 s_2$ nem tartalmaznak közös változót.
2. Vannak olyan $\ell_1, \ldots, \ell_m \in C_1 s_1$ és $\ell'_1, \ldots, \ell'_n \in C_2 s_2$ literálok $(m, n \geqslant 1)$, hogy az $L = \{\ell_1, \ldots, \ell_m, \overline{\ell'_1}, \ldots, \overline{\ell'_n}\}$ halmaz unifikálható. Legyen sub a legkisebb egyesítő.
3. $R = ((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell'_1, \ldots, \ell'_n\}))sub$.

2.74. Példa. Adjuk meg a C_1 és C_2 egy rezolvensét, ahol $C_1 = \{p(f(x)), \neg q(z), p(z)\}$ és $C_2 = \{\neg p(x), r(g(x), a)\}$

1. Az $s_1 = []$ és $s_2 = [x/u]$ átnevezésekkel élve $C_1 s_1 = C_1$ és $C_2 s_2 = \{\neg p(u), r(g(u), a)\}$.
2. Az $\ell_1 = p(f(x))$, $\ell_2 = p(z)$ és $\ell'_1 = \neg p(u)$ választás esetén $L = \{\ell_1, \ell_2, \overline{\ell'_1}\}$ egyesíthető a $sub = [z/f(x)][u/f(x)]$ legkisebb egyesítővel.
3. $$\begin{aligned} R &= ((C_1 s_1 - \{\ell_1, \ell_2\}) \cup (C_2 s_2 - \{\ell'_1\}))sub \\ &= (\{\neg q(z)\} \cup \{r(g(u), a)\})sub \\ &= \{\neg q(z), r(g(u), a)\}\,[z/f(x)][u/f(x)] \\ &= \{\neg q(f(x)), r(g(f(x)), a)\} \end{aligned}$$

□

2.75. Definíció. Legyen F egy zárt Skolem normálforma, melynek F^* mátrixa konjunktív normálforma.

1. R az F egy rezolvense, ha F^*-ban vannak olyan C_1 és C_2 klózok, hogy R a C_1 és C_2 egy rezolvense.

2. F-ből történő rezolúciós bizonyításnak, klózok egy olyan $C_1, \ldots, C_n$ sorozatát nevezzük, amelyben minden $1 \leq i \leq n$-re az alábbi feltételek valamelyike teljesül

   (a) $C_i \in F^*$

   (b) van olyan $k, l < i$, hogy C_i a C_k és a C_l egy rezolvense.

   Egy C klóz bebizonyítható F-ből rezolúcióval (vagy röviden C rezolválható F-ből), ha van olyan F-ből történő $C_1, \ldots, C_n$ rezolúciós bizonyítás, melyre $C_n = C$.

3. Bevezetjük a következő jelöléseket is (a zérusrendű esethez hasonlóan).

   - $Res(F) = F^* \cup \{R \mid R \text{ az } F \text{ egy rezolvense}\}$
   - $Res^*(F) = \bigcup_{n \geqslant 0}^{\infty} Res^{(n)}(F)$, ahol

     (i) $Res^{(0)}(F) = F^*$

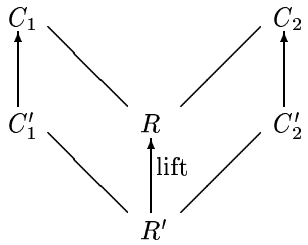
     (ii) $Res^{(n+1)}(F) = Res(Res^{(n)}(F)), n \geqslant 0.$

□

2.76. Lemma. Legyen F egy zárt Skolem normálforma, melynek F^* mátrixa konjunktív normálforma és legyen C egy klóz. $C \in Res^*(F)$ akkor és csak akkor teljesül, ha C bebizonyítható F-ből rezolúcióval.

Bizonyítás. Ugyanúgy mint a zérusrendű esetben, lásd 1.82. lemma. □

2.77. Lemma. (Lift lemma.) Legyenek C_1 és C_2 elsőrendű klózok és legyenek C_1' és C_2' a C_1 és C_2 ground példányai. Továbbá, legyen R' a C_1' és C_2' egy rezolvense. Akkor, a C_1-nek és C_2-nek van egy olyan R rezolvense, hogy R' az R egy ground példánya.



Bizonyítás. Legyenek s_1 és s_2 változó átnevezések úgy, hogy $C_1 s_1$-ben és $C_2 s_2$-ben nincsenek közös változók. Mivel C_1' és C_2' ground példányok, és $C_1 s_1$-ben és $C_2 s_2$-ben nincsenek közös változók, van olyan sub helyettesítés, hogy $C_1' = C_1 s_1 sub$ és $C_2' = C_2 s_2 sub$.
Legyen $R' = (C_1' - \{\ell\}) \cup (C_2' - \{\overline{\ell}\})$. Vannak olyan $\ell_1, \ldots, \ell_m \in C_1 s_1$ és $\ell_1', \ldots, \ell_n' \in C_2 s_2$, hogy $\ell = \ell_1 sub = \ldots = \ell_m sub$ és $\overline{\ell} = \ell_1' sub = \ldots = \ell_n' sub$. Ezért $C_1 s_1$ és $C_2 s_2$ rezolválhatók, mivel sub az

$$L = \{\ell_1, \ldots, \ell_m, \overline{\ell'}_1, \ldots, \overline{\ell'}_n\}$$

halmaz egyesítője. Legyen sub_0 az L legkisebb egyesítője. Ekkor van olyan s ground helyettesítés, hogy $sub = sub_0\ s$, és

$$R = ((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\}))sub_0$$

a $C_1 s_1$ és $C_2 s_2$ (predikátumkalkulusbeli) rezolvense.

Továbbá,

$$\begin{aligned} R' &= (C_1' - \{\ell\}) \cup (C_2' - \{\overline{\ell}\}) \\ &= (C_1 s_1 sub - \{\ell\}) \cup (C_2 s_2 sub - \{\overline{\ell}\}) \\ &= ((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\}))sub \\ &= ((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\}))sub_0\ s \\ &= Rs, \end{aligned}$$

tehát R' az R egy ground példánya. □

2.78. Tétel. (A predikátumkalkulus rezolúciós tétele.) Legyen F egy olyan zárt Skolem normálforma, melyre F^* konjunktív normálforma. F akkor és csakis akkor kielégíthetetlen, ha $\square \in Res^*(F)$.

Bizonyítás. a) (Helyesség : ha $\square \in Res^*(F)$, akkor F kielégíthetetlen.) Tetszőleges C klóz esetén, melynek szabad változói $x_1, \ldots, x_m$, jelöljük röviden $\forall C$-vel a $\forall x_1 \ldots \forall x_m C$ formulát. Ekkor $F \equiv \bigwedge_{C \in F^*} \forall C$.
Elegendő lesz azt igazolni, hogy minden $C_1, \ldots, C_n$, F-ből történő rezolúciós bizonyítás esetén $F \models \forall C_n$. (Valóban,

ha $\square \in Res^*(F)$,
$\Longrightarrow$ $\square$ bebizonyítható F-ből rezolúcióval (2.76. lemma),
$\Longrightarrow$ van F-ből történő $C_1, \ldots, C_n = \square$ rezolúciós bizonyítás,
$\Longrightarrow$ $F \models \forall C_n = \forall \square = \square$,
$\Longrightarrow$ F kielégíthetetlen.)

Legyen tehát $C_1, \ldots, C_n$ egy F-ből történő rezolúciós bizonyítás. Az állításunk bizonyítását n szerinti indukcióval végezzük.

Az $n = 1$ esetben csak $C_n \in F^*$ lehetséges, lásd 2.75. definíció 2. pontja. Ekkor persze $\bigwedge_{C \in F^*} \forall C \models \forall C_n$, tehát $F \models \forall C_n$.

Az $n \Rightarrow n+1$ esetben, a 2.75. definíció 2. pontja értelmében, megint csak az alábbi részesetek lehetségesek.
1. $C_{n+1} \in F^*$. Ekkor az $n = 1$ esethez hasonlóan kapjuk, hogy $F \models \forall C_{n+1}$.
2. Van olyan $k, l \leq n$, hogy C_{n+1} a C_k és a C_l egy rezolvense. Az indukció feltevés miatt $F \models \forall C_k$ és $F \models \forall C_l$, amiből kapjuk, hogy $F \models \forall C_k \wedge \forall C_l$. Elegendő tehát igazolni, hogy a C_k és C_l minden R rezolvensére $\forall C_k \wedge \forall C_l \models \forall R$.

Legyen evégett $\mathcal{A}$ egy olyan struktúra, melyre $\mathcal{A}(\forall C_k) = 1$ és $\mathcal{A}(\forall C_l) = 1$. Legyen

$$\begin{aligned} R &= ((C_k s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_l s_2 - \{\ell_1', \ldots, \ell_n'\}))sub \\ &= (C_k s_1 sub - \{\ell\}) \cup (C_l s_2 sub - \{\overline{\ell}\}), \end{aligned}$$

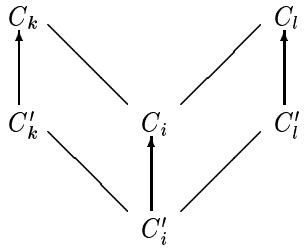
ahol sub az $L = \{\ell_1, \ldots, \ell_m, \overline{\ell'}_1, \ldots, \overline{\ell'}_n\}$ literál halmaz legkisebb egyesítője és $Lsub = \{\ell\}$.

Most ad abszurdum tegyük fel, hogy $\mathcal{A}(\forall R) = 0$. Ekkor van olyan $\mathcal{A}'$ struktúra, melyre $\mathcal{A}'(R) = 0$. (Mivel $\mathcal{A}(\forall R) = 0$, az $\mathcal{A} = (U, \mathcal{I})$ struktúra U univerzumának vannak olyan $u_1, \ldots, u_t$ elemei, hogy az $\mathcal{A}' = \mathcal{A}_{[x_1/u_1]\ldots[x_t/u_t]}$ struktúra esetén $\mathcal{A}'(R) = 0$, ahol $\forall R = \forall x_1 \ldots \forall x_t R$.) Tehát $\mathcal{A}'(C_k s_1 sub - \{\ell\}) = 0$ és $\mathcal{A}'(C_l s_2 sub - \{\overline{\ell}\}) = 0$. Ugyanezen $\mathcal{A}'$-re (az $\mathcal{A}(\forall C_k) = 1$ és $\mathcal{A}(\forall C_l) = 1$ feltételek miatt), $\mathcal{A}'(C_k s_1 sub) = 1$ és $\mathcal{A}'(C_l s_2 sub) = 1$ is teljesül. De ez csak úgy lehet, ha $\mathcal{A}'(\ell) = 1$ és $\mathcal{A}'(\overline{\ell}) = 1$, ami ellenetmondás. Tehát $\mathcal{A}(\forall R) = 1$.

b) (Teljesség : ha F kielégíthetetlen, akkor $\square \in Res^*(F)$.) Tételezzük fel, hogy F kielégíthetetlen. A 2.63. (ground rezolúciós) tétel miatt van egy olyan $C_1', \ldots, C_n'$ sorozat, mely eleget tesz a következő feltételeknek. $C_n' = \square$ és minden $1 \leq i \leq n$-re

1. C_i' az F^* valamely klózának egy ground példánya, vagy
2. van olyan $1 \leq k, l < i$, hogy C_i'-t a C_k'-ból és C_l'-ből kapjuk ground rezolúcióval.

Minden $i = 1, \ldots, n$-re megadunk egy olyan C_i klózt, hogy C_i' a C_i egy ground példánya és a $C_1, \ldots, C_n$ a $\square$ bizonyítása lesz F-ből. Legyen $1 \leq i \leq n$. Ha C_i' az F^* egy C klózának egy ground példánya, akkor legyen $C_i = C$. Ha nem ez a helyzet, akkor C_i'-t a C_k'-ból és C_l'-ből kaptuk ground rezolúcióval valamely $k, l < i$ esetén. Legyenek C_k és C_l a már megkonstruált klózok (melyeknek C_k' és C_l' ground példányaik). Ekkor a 2.77. lemma miatt van olyan C_i, hogy C_i' a C_i egy ground példánya és C_i a C_k és C_l-ből kapható rezolúcióval.



A bizonyítás kész. $\square$

2.79. Példa. Mutassuk meg, hogy az

$$F = \forall x \forall y \forall z((\neg p(x) \vee q(x) \vee r(x, f(x))) \wedge (\neg p(x) \vee q(x) \vee s(f(x)))) \wedge t(a) \wedge p(a) \\ \wedge (\neg r(a, z) \vee t(z)) \wedge (\neg t(x) \vee \neg q(x)) \wedge (\neg t(y) \vee \neg s(y))$$

formula kielégíthetetlen, ahol p, q, r, s és t predikátumszimbólumok, f pedig függvényszimbólum! Először F-et felírjuk halmaz alakban:

$$F = \{\{\neg p(x), q(x), r(x, f(x))\}, \{\neg p(x), q(x), s(f(x))\}, \{t(a)\}, \{p(a)\}, \\ \{\neg r(a, z), t(z)\}, \{\neg t(x), \neg q(x)\}, \{\neg t(y), \neg s(y)\}\}.$$

Ezután rezolváljuk $\square$-t F-ből.

1. $\{\neg t(x), \neg q(x)\}$	F-beli klóz
2. $\{t(a)\}$	F-beli klóz
3. $\{\neg q(a)\}$	rezolúcióval 1-ből és 2-ből
4. $\{p(a)\}$	F-beli klóz
5. $\{\neg p(x), q(x), s(f(x))\}$	F-beli klóz
6. $\{q(a), s(f(a))\}$	rezolúcióval 4-ből és 5-ből
7. $\{\neg p(x), q(x), r(x, f(x))\}$	F-beli klóz
8. $\{s(f(a))\}$	rezolúcióval 3-ból és 6-ból
9. $\{q(a), r(a, f(a))\}$	rezolúcióval 4-ből és 7-ből
10. $\{r(a, f(a))\}$	rezolúcióval 3-ból és 9-ből
11. $\{\neg r(a, z), t(z)\}$	F-beli klóz
12. $\{t(f(a))\}$	rezolúcióval 10-ből és 11-ből
13. $\{\neg t(y), \neg s(y)\}$	F-beli klóz
14. $\{\neg s(f(a))\}$	rezolúcióval 12-ből és 13-ból
15. $\square$	rezolúcióval 8-ból és 14-ből

$\square$

Az elsőrendű rezolúció alkalmas automatikus tételbizonyításra is.

2.80. Példa. Tekintsük a csoportelmélet következő axióma rendszerét, ahol a $p(x,y,z)$ predikátum az $x \cdot y = z$ egyenlőséget jelenti.

(1) $\forall x \forall y \exists z p(x,y,z)$ (a műveletre való zártság)

(2) $\forall u \forall v \forall w \forall x \forall y \forall z((p(x,y,u) \wedge p(y,z,v)) \rightarrow (p(x,v,w) \leftrightarrow p(u,z,w)))$ (asszociativitás)

(3) $\exists x(\forall y p(x,y,y) \wedge \forall y \exists z p(z,y,x))$ (bal egységelem és bal inverz létezése)

Itt a $p(x,v,w) \leftrightarrow p(u,z,w)$ kifejezés a $(p(x,v,w) \rightarrow p(u,z,w)) \wedge (p(u,z,w) \rightarrow p(x,u,w))$ formula rövidítése.

Bizonyítsuk be, hogy a fenti axiómákból következik a jobb inverz létezése is. Ez utóbbi tény a

(4) $\exists x(\forall y p(x,y,y) \wedge \forall y \exists z p(y,z,x))$

formulával írható le.

Azt kell tehát igazolni, hogy $\{(1),(2),(3)\} \models \{(4)\}$, vagyis, hogy az $F = (1) \wedge (2) \wedge (3) \wedge \neg(4)$ kielégíthetetlen. F-fen alkalmas ekvivalens átalakításokat, majd Skolemizációt végrehajtva egy olyan F-fel s-ekvivalens Skolem normálformát kapunk, melynek mátrixa egy olyan konjunktív normálforma lesz, melynek klózai a következők:

(a) $\{p(x,y,m(x,y))\}$
(b) $\{\neg p(x,y,u), \neg p(y,z,v), \neg p(x,v,w), p(u,z,w)\}$
(c) $\{\neg p(x,y,u), \neg p(y,z,v), \neg p(u,z,w), p(x,v,w)\}$
(d) $\{p(e,y,y)\}$
(e) $\{p(i(y),y,e)\}$
(f) $\{\neg p(x,j(x),j(x)), \neg p(k(x),z,x)\}$

Annak igazolására, hogy F kielégíthetetlen, elegendő $\square$-t rezolválni a fenti klózokból. Ez a következőképpen történhet.

1.	(f)	alapklóz
2.	(d)	alapklóz
3.	$\{\neg p(k(e),z,e)\}$	$Res(1,2)$
4.	(b)	alapklóz
5.	$\{\neg p(x,y,k(e)), \neg p(y,z,v), \neg p(x,v,e)\}$	$Res(3,4)$
6.	(e)	alapklóz
7.	$\{\neg p(i(v),w,k(e)), \neg p(w,z,v))\}$	$Res(5,6)$
8.	(d)	
9.	$\{\neg p(i(v),e,k(e))\}$	$Res(7,8)$
10.	(c)	
11.	$\{\neg p(i(t),y,u), \neg p(y,z,e), \neg p(u,z,k(e))\}$	$Res(9,10)$
12.	(d)	
13.	$\{\neg p(i(t),y,e), \neg p(y,k(e),e)\}$	$Res(11,12)$
14.	(e)	
15.	$\{\neg p(i(t),i(k(e)),e)\}$	$Res(13,14)$
16.	(e)	
17.	$\square$	$Res(15,16)$

$\square$

2.7. Korlátozott rezolúciós módszerek

2.7.1. Lineáris rezolúció

2.81. Definíció. Legyen F egy zárt Skolem normálforma, melynek F^* mátrixa konjunktív normálforma (klóz halmaz) és legyen $C_0 \in F^*$. Egy C klóz lineárisan rezolválható F-ből a C_0-ból kiindulva, ha van olyan $C_0, C_1, \ldots, C_n$ klóz sorozat, melyre

1) $C_n = C$

2) minden $1 \leq i \leq n$-re C_i a C_{i-1} és egy B klóz egy rezolvense, ahol $B \in F^*$ vagy $B = C_j$ valamilyen $j < i - 1$-re.

□

Ha a fenti definícióban a $B \in F^*$ eset fordul elő, akkor B-t oldalklóznak nevezzük. Megjegyezzük továbbá, hogy a $C_0, C_1, \ldots, C_n$ klóz sorozat nem F-ből történő rezolúciós bizonyítás a 2.75. definíció értelmében. Valóban, a C-nek egy F-ből történő rezolúciós bizonyítását akkor kapjuk meg, ha a $C_0, C_1, \ldots, C_n$ sorozatba elhelyezzük az oldalklózokat is.

Azt szeretnénk megmutatni, hogy a lineáris rezolúció is teljes. A lift lemma miatt ezt elegendő csak ítéletkalkulusbeli rezolúcióra bizonyítani. Ehhez szükségünk lesz a következő jelölésre.

2.82. Definíció. Legyen F egy zérusrendű klóz halmaz és legyen ℓ egy literál ami előfordul F-ben. Akkor

(a) $F_{\ell=0}$ az a klózhalmaz, melyet úgy kapunk F-ből, hogy
- elhagyjuk belőle ℓ minden előfordulását és
- elhagyunk belőle minden olyan klózt, ami $\overline{\ell}$-et tartalmazza.

(b) $F_{\ell=1}$ az a klózhalmaz, melyet úgy kapunk, F-ből, hogy
- elhagyjuk belőle $\overline{\ell}$ minden előfordulását és
- elhagyunk belőle minden olyan klózt, ami ℓ-et tartalmazza.

2.83. Tétel. (A lineáris rezolúció helyessége és teljessége.) *Egy F klóz halmaz (véges esetben konjunktív normálforma) akkor és csakis akkor kielégíthetetlen, ha van olyan $C \in F$, hogy* □ *lineárisan rezolválható F-ből C-ből kiindulva.*

Bizonyítás. Ha □ rezolválható F-ből akkor F kielégíthetetlen (mindegy, hogy a rezolúció lineáris-e vagy sem és ugyancsak nem számít, hogy miből indul ki).

Megfordítva, tegyük fel, hogy az F konjunktív normálforma kielégíthetetlen. A kompaktsági tétel miatt az is feltehető, hogy F véges. Legyen F' az F-nek egy minimális kielégíthetetlen részhalmaza. (Tehát $F' \subseteq F$, F' kielégíthetetlen és minden $F'' \subset F'$ esetén F'' már kielégíthető.)

Megmutatjuk, hogy minden $C \in F'$ esetén □ lineárisan rezolválható F-ből C-ből kiindulva. Az állítást az F'-ben szereplő literálok száma szerinti indukcióval bizonyítjuk be, legyen ez n.

(i) $n = 0$ eset. Ekkor $F' = \{\square\}$ és így $C = \square$, tehát nincs mit bizonyítani.

(ii) Tegyük fel, hogy F'-ben $n + 1$ literál szerepel. Ekkor két esetet különböztetünk meg.

1. eset: $|C| = 1$, vagyis $C = \{\ell\}$. Mivel F' kielégíthetetlen, $F'_{\ell=1}$ is kielégíthetetlen. Legyen $F'' \subseteq F'_{\ell=1}$ egy minimális kielégíthetetlen részhalmaz. Ekkor F'' tartalmaz egy olyan C' klózt, melyre $C' \cup \{\overline{\ell}\} \in F'$ (vagyis egy olyan C' klózt, amelyet $\overline{\ell}$ elhagyásával kaptunk). Ha ugyanis F'' nem tartalmazna ilyen C'-t, akkor $F'' \subseteq F' - \{C\}$ is igaz lenne, ami viszont lehetetlen, mert F' minimális kielégíthetetlen részhalmaz.

Mivel F''-ben már legfeljebb csak n literál van, alkalmazható az indukció feltevés, mely szerint $\Box$ lineárisan rezolválható F''-ből ezen C'-ből kiindulva.

Legyen

$$C_0 = C', C_1, \ldots, C_n = \Box \qquad (*)$$

ezen F''-beli lineáris rezolúciós bizonyítás. Ezen bizonyításból kiindulva meg fogjuk konstruálni $\Box$-nak egy lineáris rezolúcióját F'-ből a $C = \{\ell\}$ klózból indulva. A konstrukció a következő.

1. Helyezzük $(*)$ elé a $C(= \{\ell\}), C' \cup \{\overline{\ell}\}, C'$, F'-beli lineáris rezolúciós lépést, majd a $C_1, \ldots, C_n$ klózok közül helyezzük vissza $\overline{\ell}$-t azokba, amelyekből elhagytuk. Ekkor kapunk egy
$$C, C' \cup \{\overline{\ell}\}, C'(= C_0), C'_1, \ldots, C'_n = \{\overline{\ell}\}, \qquad (**)$$
F'-beli rezolúciós bizonyítást.

2. A $(**)$ bizonyításhoz adjuk még hozzá a $C'_n = \{\overline{\ell}\}, C, \Box$ ugyancsak F'-beli rezolúciós lépést. Ekkor $\Box$-nak a következő F'-beli C-ből kiinduló rezolúciós bizonyítását kapjuk

$$C, C' \cup \{\overline{\ell}\}, C', C'_1, \ldots, C'_n = \{\overline{\ell}\}, C, \Box.$$

2. eset: $|C| > 1$. Legyen $\ell \in C$ egy tetszőleges literál és legyen $C' = C - \{\ell\}$. Ekkor $C' \in F'_{\ell=0}$, ugyanakkor az $F'_{\ell=0} - \{C'\}$ klóz halmaz kielégíthető lesz. Legyen ugyanis $\mathcal{A} \models F' - \{C\}$ (ilyen azért van, mert F' minimális kielégíthetetlen részhalmaz volt). Mivel F' kielégíthetetlen, ezért $\mathcal{A}(F') = 0$, tehát $\mathcal{A}(C) = 0$. Így $\ell \in C$ miatt $\mathcal{A}(\ell) = 0$. Következésképpen $\mathcal{A}(F'_{\ell=0} - \{C'\}) = 1$.

Legyen F'' egy minimális kielégíthetetlen részhalmaza $F'_{\ell=0}$-nak. Ezen F''-nek tartalmaznia kell C'-t, mert ha nem tartalmazná, akkor $F'' \subseteq F'_{\ell=0} - \{C'\}$ lenne és így - mint egy kielégíthető klóz halmaz része - F'' is kielégíthető lenne a fenti $\mathcal{A}$-val.

Mivel F''-ben már legfeljebb n literál szerepel, alkalmazható az indukciós feltevés, mely szerint van egy

$$C_0 = C', C_1, \ldots, C_n = \Box$$

alakú, F''-beli lineáris rezolúciós bizonyítás. Helyezzük vissza ℓ-et az ezen bizonyításban szereplő olyan klózokba, amelyekből elhagytuk. Kapunk egy

$$C'_0 = C' \cup \{\ell\}, C'_1, \ldots, C'_n = \{\ell\} \qquad (+)$$

lineáris, F'-ből történő bizonyítást.

Másrészt észrevesszük, hogy az $(F' - \{C\}) \cup \{\{\ell\}\}$ nem elégíthető ki, mert mint ahogy láttuk, az $F' - \{C\}$ minden $\mathcal{A}$ modellje esetén $\mathcal{A}(\ell) = 0$. Ugyanakkor, az $(F' - \{C\}) \cup \{\{\ell\}\}$ minden minimális kielégíthetetlen részhalmaza tartalmazza $\{\ell\}$-t is, mert $(F' - \{C\})$ kielégíthető.
Így az 1. eset felhasználásával, létezik egy

$$C''_0 = \{\ell\}, C''_1, \ldots, C''_m = \Box \qquad (++)$$

F'-ből történő lineáris rezolúciós bizonyítás.

Végül $(++)$-ot $(+)$ után rakva kapjuk $\Box$-nak egy C-ből induló F-beli lineáris rezolúcióját.
$\Box$

2.7.2. SLD rezolúció

2.84. Definíció. Legyen F egy zárt Skolem normálforma, melynek F^* mátrixa Horn formula. Egy C klóz SLD rezolválható F-ből, ha C lineárisan rezolválható F-ből valamely $C_0 \in F^*$ negatív klózból kiindulva (lásd 2.81. definíció). □

Megjegyezzük, hogy, mivel az SLD rezolúció negatív klózból indul ki és, mivel F Horn formula, minden rezolúciós lépés alkalmazása után negatív klózt kapunk. Így a 2.81. definícióban szereplő B klóz csak oldalklóz lehet, ugyanis két negatív klóznak nem létezik rezolvense.

Bebizonyítjuk, hogy az SLD rezolúció helyes és teljes a Horn formulák osztályán. A lift lemma miatt itt is elegendő csak a zérusrendű esettel foglalkozni.

2.85. Tétel. (Az SLD rezolúciós teljessége a Horn formulák osztályán.) *Egy F Horn formula akkor és csakis akkor kielégíthetetlen, ha $\square$ SLD rezolválható F-ből.*

Bizonyítás. Ha $\square$ rezolválható F-ből, akkor F kielégíthetetlen (függetlenül attól, hogy a szóban forgó rezolúció SLD rezolúció-e vagy sem.

Fordítva, ha F kielégíthetetlen, akkor szükségképpen tartalmaznia kell egy negatív klózt. Ugyanez érvényes F minden minimális kielégíthetetlen F' részhalmazára is. Legyen $C \in F'$ egy negatív klóz. A 2.83. tétel (lineáris rezolúció teljességi tétele) bizonyításából következik, hogy létezik egy

$$C_0 = C, C_1, \ldots, C_n = \square$$

F'-beli lineáris rezolúciós sorozat. Ezen sorozat szükségképpen SLD rezolúció, mert egy negatív klózból indul ki és ezért minden rezolúciós lépés eredménye is negatív klóz lesz. Következésképpen, minden rezolúciós lépés után egy F-beli nem csak negatív literálokat tartalmazó klózt kell venni oldalklóznak.

□

3. A logikai programozás alapjai

Ebben a fejezetben elsőrendű Horn formulákkal foglalkozunk. A logikai programozás motivációja az, hogy a gyakorlatban gyakran kerülünk szembe a következő típusú feladattal.

Adott $\forall(Q_1 \wedge \ldots \wedge Q_n \rightarrow P)$ alakú állítások egy véges $\mathcal{P}$ halmaza (n lehet 0 is), ahol $Q_1, \ldots, Q_n, P$ atomi formulák. Adott továbbá egy $\exists(R_1 \wedge \ldots \wedge R_m)$ alakú formula, ahol $R_1, \ldots, R_m$ ugyancsak atomi formulák. Kérdés, hogy $\mathcal{P}$-nek logikai következménye-e $\exists(R_1 \wedge \ldots \wedge R_m)$?

Ismeretes, hogy $\mathcal{P} \models \exists(R_1 \wedge \ldots \wedge R_m)$ akkor és csak akkor áll fenn, ha $\mathcal{P} \cup \{\forall(\neg R_1 \vee \ldots \vee \neg R_m)\}$ kielégíthetetlen.

A $\mathcal{P} \cup \{\forall(\neg R_1 \vee \ldots \vee \neg R_m)\}$ halmazban lévő fomulákat konjunkcióval összekapcsolva, majd az így kapott formulát prenex normálalakra hozva egy olyan F zárt Skolem normálformát kapunk, melynek a mátrixa Horn formula és így konjunktív normálforma. Igaz lesz, hogy $\mathcal{P} \cup \{\forall(\neg R_1 \vee \ldots \vee \neg R_m)\}$ akkor és csak akkor kielégíthetetlen, ha az F formula kielégíthetetlen.

Persze az nem dönthető el algoritmussal, hogy F kielégíthető-e (lásd 2.32. következmény). Ugyanakkor, az ilyen esetekre kifejlesztett rezolúciós eljárás parciális algoritmust ad a kielégíthetetlenség eldöntésére.

Az itt szereplő klózok speciális alakjából következik, hogy ez a rezolúció csak a $\{\neg R_1, \ldots, \neg R_m\}$ negatív klózból kiinduló lineáris rezolúció, tehát SLD rezolúció lehet. Ezen meggondolások vezettek a következő fogalmak megalkotásához.

3.1. Definíció. Programklóznak nevezünk egy $\{P, \neg Q_1, \ldots, \neg Q_n\}$ alakú klózt, ahol $P, Q_1, \ldots, Q_n$ elsőrendű atomi formulák. Továbbá, logikai programon (vagy Horn klóz programon) programklózok egy $\mathcal{P}$ véges halmazát értjük. Végül kérdés klóznak (vagy cél klóznak) egy $\{\neg R_1, \ldots, \neg R_m\}$ alakú negatív klózt nevezünk, ahol $R_1, \ldots, R_m$ ugyancsak atomi formulák.

A LOGIKAI PROGRAMOZÁS ALAPFELADATA ANNAK ELDÖNTÉSE, HOGY EGY LOGIKAI PROGRAM UNIVERZÁLIS LEZÁRTJÁNAK KÖVETKEZMÉNYE-E EGY KÉRDÉS KLÓZ EGZISZTENCIÁLIS LEZÁRTJA.

A programklózokat a továbbiakban $P : -Q_1, \ldots, Q_n$, a kérdés klózt $? : -R_1, \ldots, R_m$ alakban fogjuk írni.

3.2. Példa. Legyenek *Éva*, *Ádám*, *alma* és *bor* konstansok, *szereti* pedig egy 2 változós predikátum. Akkor

$$\begin{aligned} \mathcal{P}: \quad & szereti\ (Éva,\ alma) : - \\ & szereti\ (Éva,\ bor) : - \\ & szereti\ (Ádám,\ x) : -\ szereti\ (x,\ bor) \end{aligned}$$

egy logikai program, ahol az x változó univerzálisan kötött. Ennek ismeretében azt szeretnénk megtudni, hogy *Ádám* szeret-e valakit vagy valamit, tehát, hogy $\mathcal{P}$ univerzális lezártjának következménye-e $\exists y\ szereti\ (Ádám,\ y)$.

A korábban ismertetett összefüggések miatt kérdésünk ekvivalens annak megválaszolásával, hogy a

$$\begin{aligned} \{ \quad & \{\ szereti\ (Éva,\ alma)\}, \\ & \{\ szereti\ (Éva,\ bor)\}, \\ & \{\ szereti\ (Ádám,\ x),\ \neg szereti\ (x,\ bor)\ \}, \\ & \{\neg szereti\ (Ádám,\ y)\ \} \qquad\qquad\qquad\qquad \} \end{aligned}$$

klóz halmaz (konjunktív normálforma) kielégíthetetlen-e. Ezt pedig az alábbi rezolúciós számolással tudjuk megválaszolni.

1.	$\{\neg szereti(Ádám,\ y)\}$	alapklóz
2.	$\{szereti(Ádám,\ x),\ \neg szereti(x,\ bor)\}$	alapklóz és $[x/y]$ helyettesítés
3.	$\{\neg szereti(y,\ bor)\}$	rezolúcióval 1-ből és 2-ből és $[y/Éva]$ helyettesítés
4.	$\{szereti(Éva,\ bor)\}$	alapklóz
5.	$\square$	rezolúcióval 3-ból és 4-ből.

Sőt azt is kaptuk, hogy a cáfolat az $[y/Éva]$ helyettesítés mellett jött létre, tehát $\mathcal{P}$-nek logikai következménye, hogy $\exists y\ szereti(Ádám,\ y)$, mert az is következménye, hogy $szereti(Ádám,\ Éva)$. Ebből látható, hogy nem csak az $\square$ rezolválásából, hanem a rezolválás során alkalmazott helyettesítésekből is kapunk információt.

3.3. Definíció. Legyen $\mathcal{P}$ egy logikai program, G pedig egy negatív klóz.

(a) Konfigurációnak nevezünk egy (G_1, sub) párt, ahol G_1 negatív klóz, sub pedig egy helyettesítés.

(b) Az átmeneti reláció a konfigurációk halmazán az alábbi módon értelmezett $\rightsquigarrow$ bináris reláció. Tetszőleges (G_1, sub_1) és (G_2, sub_2) konfigurációk esetén

$$(G_1, sub_1) \rightsquigarrow (G_2, sub_2),$$

ha $G_1 = \{\neg R_1, \ldots, \neg R_m\}$ és van olyan $C = \{P, \neg Q_1, \ldots, \neg Q_n\} \in \mathcal{P}$, hogy valamely i-re R_i és P unifikálhatóak és legkisebb egyesítőjük s. Továbbá,
$G_2 = \{\neg R_1, \ldots, \neg R_{i-1}, \neg Q_1, \ldots, \neg Q_n, \neg R_{i+1}, \ldots, \neg R_m\}s$ és $sub_2 = sub_1 s$.

(c) G-n alapuló kiszámításnak egy véges vagy végtelen $(G, [\,]) \rightsquigarrow (G_1, sub_1) \rightsquigarrow (G_2, sub_2) \rightsquigarrow \ldots$ alakú sorozatot nevezünk.

(d) Egy G-n alapuló kiszámítás sikeres, ha véges és az utolsó konfigurációja $(\square, sub)$ alakú.

(e) Ha egy G-n alapuló kiszámítás sikeres, ahol $G = \{\neg R_1, \ldots, \neg R_m\}$, akkor $(R_1 \wedge \ldots \wedge R_m)sub$-ot a kiszámítás eredményének nevezzük.

(f) A $\rightsquigarrow$ reflexív, tranzitív lezártját $\rightsquigarrow^*$-gal jelöljük.

□

3.4. Tétel. *Legyen $\mathcal{P}$ egy logikai program, $G = \{\neg R_1, \ldots, \neg R_m\}$ pedig egy negatív klóz. Akkor a következő két állítás érvényes*
1. (Helyesség.) *Ha van $(G, [\,]) \rightsquigarrow^* (\square, sub)$, akkor $(R_1 \wedge \ldots \wedge R_m)sub$ minden ground példánya logikai következménye $\mathcal{P}$ univerzális lezártjának.*
2. (Teljesség.) *Tetszőleges sub' helyettesítés esetén, ha $(R_1 \wedge \ldots \wedge R_m)sub'$ minden ground példánya logikai következménye $\mathcal{P}$ univerzális lezártjának, akkor van egy olyan $(G, [\,]) \rightsquigarrow^* (\square, sub)$ sikeres kiszámítás, hogy $(R_1 \wedge \ldots \wedge R_m)sub' = (R_1 \wedge \ldots \wedge R_m)sub\, s$ valamely alkalmas s helyettesítés esetén.*

Bizonyítás. Még hiányzik.

A Prolog kiértékelési startégiája

Algoritmus

Input: Egy $\mathcal{P} = \{C_1, \ldots, C_m\}$ logikai program, ahol $C_i = Q_i :- P_{i1}, \ldots, P_{in_i}$ és egy $G = ? :- R_1, \ldots, R_k$ célklóz.
Output: *Igen*, ha $\mathcal{P} \models G$, *Nem* különben.

Főprogram:

sikeres := ↓
kiértékel $(G, [\,])$
if *sikeres* **then output:** *Igen* **else output:** *Nem*

A *kiértékel* eljárás:

```
procedure kiértékel (G : célklóz, sub : helyettesítés)
var i: integer;
begin
    if G = □ then
      begin
      H := (R_1 ∧ ... ∧ R_k)sub;
      output: H;
      sikeres := ↑
      end
    else /* G =? :- E_1, ..., E_k */
      begin
      i = 0;
```

while $(i < m) \wedge \neg$ *sikeres* **do**
begin
$i := i + 1$;
if $\{E_1, Q_i\}$ unifikálható és a legkisebb egyesítő s
then *kiértékel* $(? : -(P_{i1}, \ldots, P_{in_i}, E_2, \ldots, E_k)s, sub\, s)$
end
end
end

4. Programhelyesség bizonyítás

Ebben a fejezetben megmutatjuk, hogyan lehet a logika eszözeit alkalmazva, programok helyességét bizonyítani. Több mószer is ismeretes, mi ezek közül egyet, Hoare axiomatikus módszerét fogjuk ismertetni.

Először bevezetünk néhány jelölést. Bázisnak nevezünk egy olyan $B = (F, P)$ párt, ahol F függvényszimbólumok, P pedig predikátumszimbólumok egy halmaza. A B-re épülő (elsőrendű) formulák halmazát WFF_B-vel jelöljük.

Ebben a fejezetben egy $B = (F, P)$ bázis feletti struktúrán egy $\mathcal{A} = (D, \mathcal{I})$ párt értünk, ahol D az alaphalmaz és $\mathcal{I}$ az interpretáció. Amennyiben $\sigma : Var \to D$ egy hozzárendelés (értékelés), akkor $\mathcal{A}_\sigma$-val jelöljük a $(D, \mathcal{I}, \sigma)$ struktúrát.

Az összes hozzárendelések halmazát Σ-val jelöljük: $\Sigma = \{\sigma \mid \sigma : Var \to D\}$.

Tetszőleges $\mathcal{A} = (D, \mathcal{I})$ struktúra és t term esetén az $\mathcal{A}(t) : \Sigma \to D$ leképezést a következőképpen értelmezzük: $\mathcal{A}(t)(\sigma) = \mathcal{A}_\sigma(t)$, ahol az egyenlet jobb oldalát a 2.6. definíció szerint értelmezzük.

Tetszőleges $p \in WFF_B$ esetén az $\mathcal{A}(p) : \Sigma \to \{0, 1\}$ leképezést a következőképpen definiáljuk: $\mathcal{A}(p) = \mathcal{A}_\sigma(p)$, ahol az egyenlet jobb oldalát a 2.8. definíció szerint értelmezzük.

Most definiáljuk programoknak egy olyan osztályát, amelyen Hoare axiomatikus módszerét.

4.1. While programok

a) Szintaxis. Egy S programot while programnak (vagy $\mathcal{L}_2$ programnak) nevezünk, ha teljesíti az alábbi négy feltétel valamelyikét:

1) S : $x := t$,
ahol $x \in Var$ és t egy term.
2) S : $S_1; S_2$
3) S : **if** e **then** S_1 **else** S_2 **fi**
4) S : **while** e **do** S_1 **od**

ahol e egy kvantormentes formula, S_1, S_2 pedig while programok.

b) Szemantika. Minden S while program, minden $\mathcal{A} = (D, \mathcal{I})$ struktúra esetén meghatároz egy $M_\mathcal{A}(S) : \Sigma \to \Sigma$ parciális leképezést (ami az S szemantikája $\mathcal{A}$-ban) a következőképpen:

1. eset: $M_\mathcal{A}(S)(\sigma) = \sigma[x/\mathcal{A}(t)(\sigma)]$.
2. eset: $M_\mathcal{A}(S)(\sigma) = M_\mathcal{A}(S_2)(M_\mathcal{A}(S_1)(\sigma))$.
3. eset: $M_\mathcal{A}(S)(\sigma) = \begin{cases} M_\mathcal{A}(S_1)(\sigma) & \text{, ha } \mathcal{A}(e)(\sigma) = 1 \\ M_\mathcal{A}(S_2)(\sigma) & \text{, különben.} \end{cases}$
4. eset: $M_\mathcal{A}(S)(\sigma) = \sigma'$, ha van olyan $n \geq 0$ nemnegatív egész szám és $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}, \sigma_n \in \Sigma$ sorozat, hogy

- $\sigma_0 = \sigma$, $\sigma_n = \sigma'$,
- $M_{\mathcal{A}}(S_1)(\sigma_i) = \sigma_{i+1}$ $(i = 0, 1, \ldots, n-1)$,
- $\mathcal{A}(e)(\sigma_0) = \ldots = \mathcal{A}(e)(\sigma_{n-1}) = 1$ és $\mathcal{A}(e)(\sigma_{n-1}) = 0$.

Különben $M_{\mathcal{A}}(S)(\sigma)$ definiálatlan.

4.1. Példa. Legyen S a kövekező while program:

$y_1 := 0$; $y_2 := 1$; $y_3 := 1$;
while $y_3 \leq x$ **do**
$y_1 := y_1 + 1$;
$y_2 := y_2 + 2$;
$y_3 := y_3 + y_2$ **od**

Legyen továbbá $\sigma = (15, \sigma(y_1), \sigma(y_2), \sigma(y_3))$. Akkor $M(S)(\sigma) = (15, 3, 7, 16)$, vagyis S az y_1 változóban $\lfloor\sqrt{x}\rfloor$-et számolja ki.

4.2. Példa. Legyen most S a következő while program:

$y := 1$;
while $x > 0$ **do**
$y := y * x$;
$x := x - 1$ **od**

Ha $\sigma = (-3, \sigma(y))$, akkor $M(S)(\sigma) = (-3, 1)$ és ha $\sigma = (6, \sigma(y))$, akkor $M(S)(\sigma) = (0, 6!)$, vagyis pozitív x-re S az y változóban az x faktoriálisát számolja ki.

Egy S while program helyességét úgy próbáljuk megfogalmazni, hogy megadunk egy $p \in WFF_B$ kezdeti és egy $q \in WFF_B$ végső feltételt, amelyek az S program futása előtti feltételeket és futása utáni feltételeket írják le. Azt, hogy S-ről mikor mondjuk, hogy helyesen működik, többféleképpen is meg lehet fogalmazni.

Az egyik lehetőség, hogy akkor mondjuk, hogy S helyesen működik, ha valahányszor teljesülnek az input feltételek (vagyis p) és a program definiált értéket ad, mindannyiszor teljesülnek az output feltételek (vagyis q) is. Ezt parciális helyességnek nevezzük, mert nem követeljük meg S-től, hogy az input feltételek teljesülése esetén mindig megálljon.

A másik lehetőség, hogy akkor mondjuk, hogy S helyesen működik, ha valahányszor teljesülnek az input feltételek (vagyis p), mindannyiszor a program definiált értéket ad és teljesülnek az output feltételek (vagyis q) is. Ezt totális helyességnek nevezzük,

Hoare axiomatikus módszere a fenti értelemben vett parciális illetve a totális helyesség bizonyítására szolgál.

4.2. Hoare axiomatikus módszere

Parciális helyesség

4.3. Definíció. (A Hoare logika szintaxisa) Legyen B egy bázis. B feletti Hoare formulának (vagy parciális helyességi kifejezésnek) egy

$$\{p\}S\{q\}$$

alakú kifejezést nevezünk, ahol $p, q \in WFF_B$ és S egy while $(\mathcal{L}_2)$ program. □

Az összes, B feletti Hoare fomulák halmazát HF_B-vel jelöljük.

4.4. Definíció. (Hoare logika szemantikája) Legyen $\mathcal{A}$ egy struktúra és Σ az összes kiértékelések halmaza. Minden $\{p\}S\{q\}$ Hoare formulához hozzárendelünk egy

$$\mathcal{A}(\{p\}S\{q\}) : \Sigma \to \{0,1\}$$

leképezést a következő módon:

$\mathcal{A}(\{p\}S\{q\})(\sigma) = 1$ akkor és csak akkor, ha
ha $\mathcal{A}(p)(\sigma) = 1$ és $M_{\mathcal{A}}(S)(\sigma)$ definiált, akkor $\mathcal{A}(q)(M_{\mathcal{A}}(S)(\sigma)) = 1$. □

Ha minden $\sigma \in \Sigma$-ra $\mathcal{A}(\{p\}S\{q\})(\sigma) = 1$, akkor azt mondjuk, hogy $\mathcal{A}$ kielégíti $\{p\}S\{q\}$-t és $\mathcal{A} \models \{p\}S\{q\}$-t írunk.
Ha minden $\mathcal{A}$ struktúra esetén $\mathcal{A} \models \{p\}S\{q\}$, akkor $\{p\}S\{q\}$ érvényes, amit $\models \{p\}S\{q\}$-val jelölünk.
Továbbá, tetszőleges $W \subseteq WFF_B$ esetén $W \models \{p\}S\{q\}$, ha valahányszor $\mathcal{A} \models W$, mindannyiszor, $\mathcal{A} \models \{p\}S\{q\}$.

4.5. Példa. 1) $\{p\}S\{q\} = \{x > 5\}\ x := 2 * x\ \{x > 20\}$
A sztenderd $\mathcal{A} = (N, \mathcal{I})$ struktúra esetén

$\mathcal{A}(\{p\}S\{q\})(\sigma) = 1$
$\Leftrightarrow$ $\mathcal{A}(p)(\sigma) = 0$ vagy $\mathcal{A}(q)(M_{\mathcal{A}}(S)(\sigma)) = 1$
(mert $M_{\mathcal{A}}(S)(\sigma)$ definiált minden σ-ra)
$\Leftrightarrow$ $\sigma(x) \leq 5$ vagy $M_{\mathcal{A}}(S)(\sigma)(x) > 20$
$\Leftrightarrow$ $\sigma(x) \leq 5$ vagy $\sigma(x) > 10$
Tehát nem igaz, hogy $\mathcal{A} \models \{p\}S\{q\}$.

2) $\{p\}S\{q\} = \{\uparrow\}$ **while** $x \neq 10$ **do** $x := x + 1$ **od** $\{x = 10\}$

A sztenderd $\mathcal{A}$ struktúra esetén $\mathcal{A} \models \{p\}S\{q\}$, mivel minden $\sigma \in \Sigma$-ra vagy $\sigma(x) \leq 10$ és akkor $M_{\mathcal{A}}(S)(\sigma)(x) = 10$ vagy $\sigma(x) > 10$ és akkor $M_{\mathcal{A}}(S)(\sigma)(x)$ nem definiált.

A parciális elnevezés onnan adódik, hogy (nem teljesen pontosan fogalmazva) ha a p input feltétel fennáll, akkor a q output feltétel fennállását csak abban az esetben követejük meg, ha az S program lefut. Mindenek persze csak egy $\mathcal{A}$ struktúrára vonatkozóan van értelme.
A továbbiakban azt vizsgáljuk, hogyan kaphatjuk meg azon Hoare formulákat, amelyeket egy adott $\mathcal{A}$ struktúra kielégít. Evégett definiálunk egy kalkulust, a Hoare Kalkulust.

A Hoare Kalkulus

1) Az értékadás axiómája

$$\{p[x/t]\}\ x := t\ \{p\}$$

minden $p \in WFF_B$, $x \in V$ és $t \in T_B$ term esetén.

2) A kompozíciós szabály

$$\frac{\{p\}S_1\{r\},\ \{r\}S_2\{q\}}{\{p\}S_1; S_2\{q\}}$$

minden $p, q, r \in WFF_B$, $S_1, S_2 \in \mathcal{L}_2$ esetén.

3) Feltételes szabály

$$\frac{\{p\wedge e\}S_1\{q\},\ \{p\wedge\neg e\}S_2\{q\}}{\{p\}\ \textbf{if}\ e\ \textbf{then}\ S_1\ \textbf{else}\ S_2\ \textbf{fi}\ \{q\}}$$

minden $p, q \in WFF_B$, e kvantormentes formula és $S_1, S_2 \in \mathcal{L}_2$ esetén.

4) While szabály

$$\frac{\{p \wedge e\}S_1\{p\}}{\{p\}\ \textbf{while}\ e\ \textbf{do}\ S_1\ \textbf{od}\ \{p\wedge\neg e\}}$$

minden $p \in WFF_B$, e kvantormentes formula és $S_1 \in \mathcal{L}_2$ esetén.

5) A következmény szabálya

$$\frac{p \to q,\ \{q\}S\{r\},\ r \to s}{\{p\}S\{s\}}$$

minden $p, q, r, s \in WFF_B$ és $S \in \mathcal{L}_2$ esetén.

A fenti kalkulussal levezetést tudunk definiálni. Legyen W Hoare formulák és WFF_B-beli (elsőrendű) formulák egy halmaza, $\{p\}S\{q\}$ pedig egy Hoare formula. Azt mondjuk, hogy W-ből levezethető $\{p\}S\{q\}$, jele $W \vdash \{p\}S\{q\}$, ha van olyan $E_0, \ldots, E_n$ sorozat hogy $E_n = \{p\}S\{q\}$ és minden $0 \leq i \leq n$-re E_i W egy eleme vagy axióma vagy megkapható az $E_0, \ldots, E_{i-1}$ elemek közül bizonyosakból a 2)-5) szabályok valamelyikének alkamazásával.

Hogy a kalkulus könnyebben használható legyen, bevezetünk további, ún. származtatott szabályokat:

1')

$$\frac{p \to q[x/t]}{\{p\}\ x := t\ \{q\}}$$

melynek bizonyítása:

(i)	$p \to q[x/t]$	(adott, W egy eleme)
(ii)	$\{q[x/t]\}\ x := t\ \{q\}$	(az 1) axióma)
(iii)	$q \to q$	(tautológia)
(iv)	$\{p\}\ x := t\ \{q\}$	(az 5) következmény szabály alkalmazása (i), (ii) és (iii)-ra).

2')

$$\frac{\{p_0\}S_1\{p_1\},\ \{p_1\}S_2\{p_2\},\ \ldots,\ \{p_{n-1}\}S_n\{p_n\}}{\{p_0\}S_1; S_2; \ldots; S_n\{p_n\}}$$

melyet a 2) kompozíciós szabály többszöri alkalmazásával kapunk.

4')

$$\frac{p \to r,\ \{r \wedge e\}S_1\{r\},\ (r \wedge \neg e) \to q}{\{p\}\ \textbf{while}\ e\ \textbf{do}\ S_1\ \textbf{od}\ \{q\}}$$

melynek bizonyítása:

(i)	$p \to r$	(adott)
(ii)	$\{r \wedge e\} S_1 \{r\}$	(adott)
(iii)	$(r \wedge \neg e) \to q$	(adott)
(iv)	$\{r\}$ **while** e **do** S_1 **od** $\{r \wedge \neg e\}$	(a 4) while szabály alkalmazva (ii)-re)
(v)	$\{p\}$ **while** e **do** S_1 **od** $\{q\}$	(következmény szabály (i), (iii) és (iv)-re).

4.6. Példa. A Hoare kalkulus alkalmazásaként megmutatjuk, hogy

$$PA \vdash \{x = a\}\, y_1 := 0; y_2 := 1; y_3 := 1; \textbf{while } y_3 \leq x \textbf{ do } y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_3 + y_2 \textbf{ od } \{y_1 = \sqrt{a}\},$$

ahol PA a Peano aritmetika, lásd 2.42. példa, és ahol $\sqrt{a}$ az a négyzetgyökének alsó egész része.

A következtetési szabályok fordított irányú alkalmazásával eljutunk a bizonyítási fa leveleiig, amelyek az értékadó axióma vagy PA elemei lehetnek.

(1) $\{x = a\}\ y_1 := 0; y_2 := 1; y_3 := 1;$
while $y_3 \leq x$ **do** $y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_3 + y_2$ **od**
$\{y_1 = \sqrt{a}\}$

(1) $\to$ (2), (3), (4), (5) (a 2' szabály fordított alkalmazásával)

(2) $\{x = a\}\ y_1 := 0\ \{x = a \wedge y_1 = 0\}$

(3) $\{x = a \wedge y_1 = 0\}\ y_2 := 1\ \{x = a \wedge y_1 = 0 \wedge y_2 = 1\}$

(4) $\{x = a \wedge y_1 = 0 \wedge y_2 = 1\}\ y_3 := 1\ \{x = a \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\}$

(5) $\{x = a \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\}$
while $y_3 \leq x$ **do** $y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_3 + y_2$ **od**
$\{y_1 = \sqrt{a}\}$

(2) $\to$ (6) (az 1' szabály fordított alkalmazásával)

(6) $(x = a) \to (x = a \wedge 0 = 0)$
Itt megállhatunk, mert a kapott formula PA egy eleme.

(3) $\to$ (7) (az 1' szabállyal)

(7) $(x = a \wedge y_1 = 0) \to (x = a \wedge y_1 = 0 \wedge 1 = 1)$

(4) $\to$ (8) (az 1' szabály fordított alkalmazásával)

(8) $(x = a \wedge y_1 = 0 \wedge y_2 = 1) \to (x = a \wedge y_1 = 0 \wedge y_2 = 1 \wedge 1 = 1)$

(5) $\to$ (9), (10), (11) (a 4' szabály fordított alkalmazásával)

(9) $(x = a \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1) \to$
$(x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1)$
Ez is PA egy eleme.

(10) $\{x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_3 \leq x\}$
$y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_3 + y_2$
$\{x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1\}$

(11) $(x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge \neg(y_3 \leq x))$
$\rightarrow \; y_1 = \sqrt{a}$
Ez is PA egy eleme.

(10) $\rightarrow$ (12), (13), (14) (a 2' szabály fordított alkalmazásával)

(12) $\{x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_3 \leq x\}$
$y_1 := y_1 + 1$
$\{x = a \wedge y_3 = y_1^2 \wedge y_2 = 2 * y_1 - 1 \wedge y_3 \leq x \wedge y_1 > 0\}$

(13) $\{x = a \wedge y_3 = y_1^2 \wedge y_2 = 2 * y_1 - 1 \wedge y_3 \leq x \wedge y_1 > 0\}$
$y_2 := y_2 + 2$
$\{x = a \wedge y_1^2 \leq x \wedge y_3 = y_1^2 \wedge y_2 = 2 * y_1 + 1\}$

(14) $\{x = a \wedge y_1^2 \leq x \wedge y_3 = y_1^2 \wedge y_2 = 2 * y_1 + 1\}$
$y_3 := y_3 + y_2$
$\{x = a \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1\}$

A megelőzőekhez hasonlóan, az 1' szabály fordított alkalmazásával

(12) $\rightarrow$ (15)

(13) $\rightarrow$ (16)

(14) $\rightarrow$ (17),

ahol (15), (16) és (17) a PA egy-egy formulája lesz.
A fordított irányú bizonyításból kapjuk a formula bizonyítását:

(6), (2), (7), (3), (8), (4), (9), (15), (12), (16), (13), (17), (14), (10), (11), (5), (1).

A Hoare kalkulus helyessége:

4.7. Tétel. *Minden $W \subseteq WFF_B$, $\{p\}S\{q\}$ Hoare formula esetén,*

$$\text{ha } W \vdash \{p\}S\{q\} \text{ akkor } W \models \{p\}S\{q\}.$$

Bizonyítás. Nem adjuk meg. □

Speciálisan, minden $\mathcal{A}$ struktúra esetén

$$\text{ha } Th(\mathcal{A}) \vdash \{p\}S\{q\} \text{ akkor } Th(\mathcal{A}) \models \{p\}S\{q\},$$

mely utóbbi azt jelenti, hogy $\mathcal{A} \models \{p\}S\{q\}$, vagyis S parciálisan helyes a p kezdeti és a q végső feltételre nézve az $\mathcal{A}$ struktúrában.
A 4.7. tétel fordítva nem igaz. Ugyanis az

$$\{\uparrow\}\ x := 1\ \{x = 1\}$$

Hoare formula minden $\mathcal{A}$ struktúrában érvényes, tehát $\emptyset \models \{\uparrow\}\ x := 1\ \{x = 1\}$.
Ugyanakkor, a formula nem vezethető le az $\emptyset$-ból, mert

$$\{1 = 1\}\ x := 1\ \{x = 1\}$$

axióma, de nem áll rendelkezésre az $\uparrow\rightarrow (1 = 1)$ formula. (Ha rendelkezésre állna, a következtetési szabállyal kapnánk, hogy $\{\uparrow\}\ x := 1\ \{x = 1\}$.)

Tehát a Hoare kalkulus nem teljes.

A teljesség egy gyengébb formája lenne, hogy minden T elmélet esetén (2.41. definíció),

$$\text{ha } T \models \{p\}S\{q\} \text{ akkor } T \vdash \{p\}S\{q\}.$$

Sajnos a teljességnek ezen gyengébb formája sem áll fenn.

4.8. Lemma. (A Hoare logika elsőrendű logika) Legyen B egy bázis, $\mathcal{A}$ egy struktúra. Akkor minden $h \in HF_B$ Horn-formula esetén

$$\mathcal{A} \models h \quad \Leftrightarrow \quad \mathrm{Th}(\mathcal{A}) \models h.$$

Bizonyítás. (Más fogalmakat is igényel, a jegyzet nem elég a megértéséhez.) Minden while program lefordítható folyamatábra programmá. Ezért az állítás következik a folyamatábra programokra vonatkozó megfelelő tételből:

S parciálisan helyes p-re és q-ra vonatkozóan $\Leftrightarrow$ bármely, S-en át vezető α út esetén $vc(p, \alpha, q)$ érvényes. □

4.9. Tétel. *Legyen $B = (\{0, 1, +\}, \{<\})$ egy bázis, $\mathcal{A} = (N, \mathcal{I})$ az a struktúra, ahol $\mathcal{I}$ a sztenderd interpretáció és tekintsük a* Th $(\mathcal{A})$ *Presburger aritmetikát. Akkor nincs olyan $\mathcal{K}$ kalkulus, melyre minde $h \in HF_B$ esetén*

$$\mathrm{Th}\,(\mathcal{A}) \models h \quad \Leftrightarrow \quad \mathrm{Th}\,(\mathcal{A}) \vdash_{\mathcal{K}} h.$$

Bizonyítás. (Más fogalmakat is igényel, a jegyzet nem elég a megértéséhez.) A Presburger aritmetika eldönthető. Tegyük fel, hogy van a fenti tulajdonsággal rendelkező $\mathcal{K}$ kalkulus. Akkor a

$$\{h \in HF_B |\ \mathrm{Th}\,(\mathcal{A}) \models h\} \ = \ \{h \in HF_B |\ \mathrm{Th}\,(\mathcal{A}) \vdash_{\mathcal{K}} h\}$$

halmazok rekurzívan felsorolhatók. Így, a 4.8. lemma miatt, a $\{h \in HF_B |\ \mathcal{A} \models h\}$ halmaz is rekurzívan felsorolható. Ellentmondás. □

A Hoare kalkulus csak az ún. kifejező (expressive) interpretációk esetén teljes.

4.10. Definíció. (Más fogalmakat is igényel, a jegyzet nem elég a megértéséhez.) Legyen B egy bázis. Egy $\mathcal{A}$ struktúra kifejező, ha minden $S \in \mathcal{L}_2$ while program és $q \in WFF_B$ formula esetén van olyan $r \in WFF_B$ formula, hogy $\mathcal{A}(r)$ az S-re és $\mathcal{A}(q)$-ra vonatkozó leggyengébb szabad előfeltétel. (Ez esetben az $\mathcal{A}(r)$ predikátumot kifejezhetőnek mondjuk.)

4.11. Tétel. *(Cook relatív teljességi tétele). Legyen B egy bázis, $\mathcal{A}$ egy kifejező struktúra. Akkor minden $h \in HF_B$ Hoare formula esetén*

$$\textit{ha } \mathrm{Th}\,(\mathcal{A}) \models h, \textit{ akkor } \mathrm{Th}\,(\mathcal{A}) \vdash h.$$

(Ezért a Presburger aritmetikát eredményező sztenderd interpretáció nem kifejező.)

Totális helyesség

A totális helyesség a Hoare logika és kalkulus egy változatával bizonyítható.

A Hoare totális helyességi logika formulái

$$[p]S[q],$$

alakúak ahol p, S, q ugyanazok, mint a parciális Hoare logika esetén.

A szemantika definíciója. Tetszőleges $\mathcal{A}$ struktúra esetén az

$$\mathcal{A}([p]S[q]) : \Sigma \to \{0,1\}$$

leképezést a következő módon definiáljuk. Minden $\sigma \in \Sigma$-ra,

$$\mathcal{A}([p]S[q])(\sigma) = 1$$

akkor és csak akkor, ha

$$\text{ha } \mathcal{A}(p)(\sigma) = 1, \text{ akkor } M_{\mathcal{A}}(S)(\sigma) \text{ definiált és } \mathcal{A}(q)(M_{\mathcal{A}}(S)(\sigma)) = 1.$$

Ez annyiban különbözik a parciális helyességi szemantikától, hogy a p input feltétel teljesülése esetén megköveteljük, hogy az S program megálljon és a q output feltétel is teljesüljön.

A totális helyességi kalkulushoz szükségünk van a jól megalapozott halmaz fogalmára.

4.12. Definíció. Egy $(W, \leq)$ parciálisan rendezett halmazt *jól megalapozottnak* nevezünk, ha nem léteznek benne $\ldots < a_2 < a_1 < a_0$ alakú, végtelen leszálló láncok. ($A <$ relációt úgy definiáljuk, hogy $a < b$-t írunk, ha $a \leq b$ de $a \neq b$.)

Például, a természetes számok halmaza a szokásos $\leq$ relációval ellátva jól megalapozott halmaz.

A totális helyességi kalkulus csak olyan B bázis és $\mathcal{A} = (D, \mathcal{I})$ struktúra esetén működik, amely eleget tesz a következő feltételeknek:

- B-ben van egy $\leq$ kétváltozós reláció,
- van olyan $H \subseteq D$, hogy $(H, \mathcal{I}(\leq))$ jól megalapozott halmaz,
- van olyan $w \in WFF_B$, amelynek egy szabad változója van, az x és amely H-t definiálja a következő értelemben:

$$H = \{\sigma(x) |\ \sigma \in \Sigma \text{ és } \mathcal{I}(w)(\sigma) = 1\}.$$

A totális helyességi Hoare kalkulus a Hoare kalkulus 1, 2, 3, és 5 szabályaiból és a következő (módosított while) szabályból áll:

$$\frac{(p \wedge e) \to w[x/t],\ [p \wedge e \wedge (t = y)]S[p \wedge (t < y)]}{[p]\ \textbf{while}\ e\ \textbf{do}\ S\ \textbf{od}\ [p \wedge \neg e]}$$

ahol $p \in WFF_B$, e kvantormentes formula, t term, $S \in \mathcal{L}_2$, y egy olyan változó, amely nem fordul elő e, p, S, t-ben.

A totális helyességi kalkulus helyes minden olyan $\mathcal{A}$ struktúra esetén, amely kielégíti a fenti 3 feltételt.

4.13. Tétel. *Legyen B egy olyan bázis és $\mathcal{A}$ egy olyan struktúra, amelyek kielégítik a fenti 3 feltételt. Akkor minden $[p]S[q]$ totális helyességi kifejezés esetén,*

$$\text{ha } Th(\mathcal{A}) \vdash [p]S[q], \text{ akkor } \mathcal{A} \models [p]S[q].$$

Ugyanakkor, a kalkulus nem teljes.

5. Modellellenőrzés (modellvizsgálat)

Egyidejű, újraéledő hardver-szoftver rendszerek működésének helyességét vizsgáljuk. (Concurrent, reactive systems) Az ilyen rendszerek teszteléssel nem vizsgálhatók, mivel a rendszer működése nem reprodukálható. Helyette, felállítjuk a rendszer egy M *modelljét*, melynek véges sok (általában nagyon sok) állapota van és amely az állapotait diszkrét időpillanatonként változtatja. A *temporális logika* egy f formulájával megfogalmazzuk a rendszer valamely (kívánatos vagy nemkívánatos) tulajdonságát. Azt vizsgáljuk, hogy az M modell mely s állapotai elégítik ki f-et, vagyis mely s-ekre igaz $M, s \models f$.

5.1. Kripke struktúrák: az egyidejű rendszerek modelljei

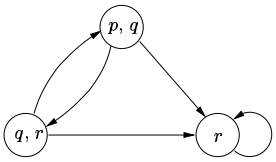
Legyen AP *atomi propozíció*k (állítások) véges halmaza.

5.1. Definíció. AP *feletti Kripke struktrúrá*nak nevezünk egy $M = (S, S_0, R, L)$ rendszert, ahol

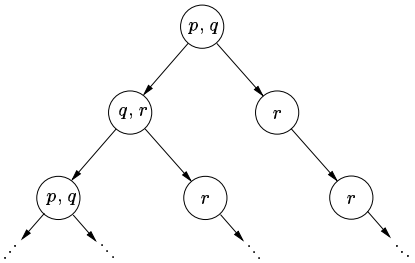
- S az állapotok véges halmaza
- $S_0 \subseteq S$ a *kezdőállapotok* halmaza
- $R \subseteq S \times S$ egy totális reláció, az *átmeneti reláció* $((\forall s \in S)(\exists s' \in S) : sRs')$.
- $L : S \to \mathcal{P}(AP)$ egy *címkézőfüggvény*, mely minden $s \in S$ állapothoz hozzárendeli azon $L(s)$ atomi állításokat, melyek igazak s-ben.

Egy $s \in S$ *állapotból kiinduló úton* egy olyan $s_0, s_1, s_2, \ldots$ *végtelen sorozat*ot értünk, melyre $s = s_0$ és bármely $i \geq 0$ esetén $s_i R s_{i+1}$ $((s_i, s_{i+1}) \in R)$.

Minden Kripke struktúra ábrázolható irányított gráfként. Például, a következő ábrán egy, az $AP = \{p, q, r\}$ halmaz feletti Kripke struktúra látható.



Minden Kripke struktúra minden állapotából kiindulva „széthajtogatható" egy általában végtelen fává. Például, ha az előbbi ábrán látható Kripke struktúrát széthajtogatjuk a $\{p, q\}$ állapotból, akkor a következő végtelen fát kapjuk. A végtelen fán, annak gyökeréből kiindulva a Kripke struktúra $\{p, q\}$-val címkézett állapotából kiinduló utak láthatók.



Mind a hardver mind a szoftver rendszerek, mind ezek kombinációi modellezhetők Kripke struktúrákkal.

Például, tekintsük az alábbi, kölcsönös kizárást (mutual exclusion) realizáló programrészletet,

$P = m$: **cobegin** $P_0 \parallel P_1$**coend** m'

P_0 : l_0 : **while** *True* **do**
NC_0 : **await** $(turn = 0)$;
$CR_0 : turn = 1$;
endwhile
l_0'

P_1 : l_1 : **while** *True* **do**
NC_1 : **await** $(turn = 1)$;
$CR_1 : turn = 0$;
endwhile
l_1'

ahol NC jelenti a nem kritikus szekciót és CR a kritikus szekciót. Feltétel, hogy P_0 és P_1 egyszerre nem lehetnek a kritikus szekcióban.

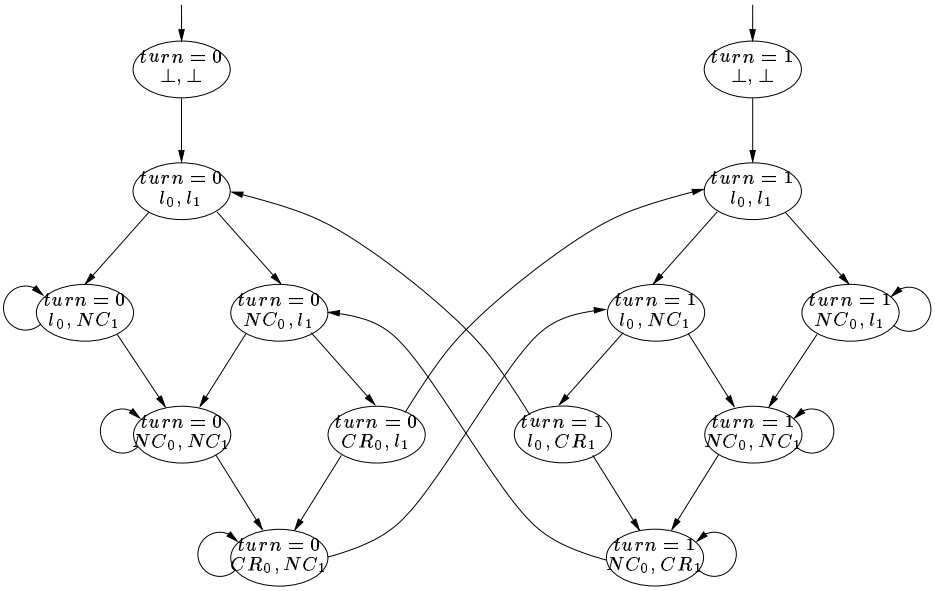
A rendszer Kripke struktúrával való leírásához vezessük be a következő atomi változókat:

- pc (a P program számlálója), értékei $m, m', \perp$,
- pc_i (a P_i program számlálója, $i = 0, 1$), értékei $l_i, l_i', NC_i, CR_i, \perp$,
- $turn$, értékei 0 és 1.

Az, hogy P_0 és P_1 egyszerre nem lehetnek a kritikus szekcióban, a következő formulával írható le:

$$\neg(pc_0 = CR_0 \wedge pc_1 = CR_1).$$

A rendszer működését a következő Kripke struktúra modellezi.

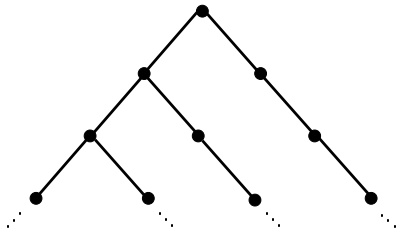


5.2. CTL* logika

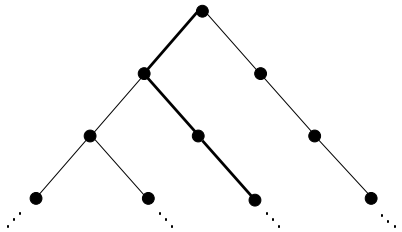
Számítási fának egy egy olyan végtelen fát nevezünk, amelyet valamely Kripke struktúrából kapunk oly módon, hogy egy állapotából széthajtogatjuk. A CTL* logikával számítási fák tulajdonságait tudjuk leírni.

Útkvantorok: a számítási fa egy pontjából kiinduló utakra vonatkoznak. Két útkvator van.

A = **A**ll, minden út:

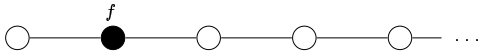


E = **E**xists, van olyan út:

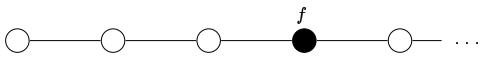


Időoperátorok: a számítási fa egy konkrét útjára vonatkoznak. Öt időoperátor van.

X =ne**X**t time: az út következő pontján teljesül valami:

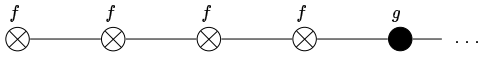


F = **F**uture, eventually: az út valamely pontján teljesül valami:

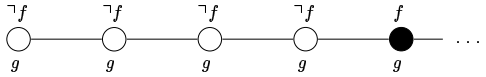


G = always, **G**lobally: az út minden pontján teljesül valami:

U = **U**ntil: van egy olyan pont, amelyen teljesül valami és eddig a pontig teljesül egy másik valami:



R = **R**elease: ha valami nem teljesül egy pontig, akkor a következő pontban teljesül egy másik valami:



A CTL* logika szintaxisa

Legyen AP az atomi változók halmaza.

Állapotformulák:

- ha $p \in AP$, akkor p állapotformula
- ha f, g állapotformulák, akkor $\neg f$, $f \vee g$, $f \wedge g$ is állapotformulák
- ha f útformula, akkor $\mathbf{E}f$ és $\mathbf{A}f$ állapotformula

Útformulák:

- ha f állapotformula, akkor f útformula is
- ha f, g útformulák, akkor $\neg f$, $f \vee g$, $f \wedge g$, $\mathbf{X}f$, $\mathbf{F}f$, $\mathbf{G}f$, $f\,\mathbf{U}\,g$, $f\,\mathbf{R}\,g$ is útformulák

A CTL* logika szemantikája

Legyen $M = (S, R, L)$ egy Kripke struktúra. Egy $\pi = s_0, s_1, \ldots$ út és $i \geq 0$ esetén $\pi^i = s_i, s_{i+1}, \ldots$.

Legyen f egy állapotformula és $s \in S$ egy állapot. f szerinti indukcióval definiáljuk az „M az s állapotban kielégíti f-et", jele $M, s \models f$, fogalmát:

- $M, s \models p$, ahol $p \in AP \iff p \in L(s)$
- $M, s \models \neg f_1 \iff$ nem teljesül, hogy $M, s \models f_1$
- $M, s \models f_1 \vee f_2 \iff M, s \models f_1$ vagy $M, s \models f_2$
- $M, s \models f_1 \wedge f_2 \iff M, s \models f_1$ és $M, s \models f_2$
- $M, s \models \mathbf{E}f_1 \iff$ van olyan s-ből kiinduló π út, amelyre $M, \pi \models f_1$
- $M, s \models \mathbf{A}f_1 \iff$ az s-ből kiinduló minden π útra $M, \pi \models f_1$

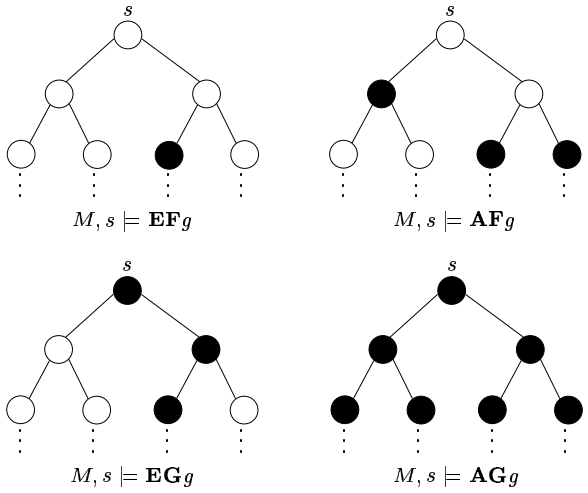
Ha nem okoz félreértést, akkor $M, s \models f$ és $M, \pi \models f$ helyett csak $s \models f$-et és $\pi \models f$-et írunk.

Legyen π egy állapotból kiinduló út és f egy útformula. f szerinti indukcióval definiáljuk az „M π útja kielégíti f-et" fogalmát, jele $M, \pi \models f$, fogalmát:

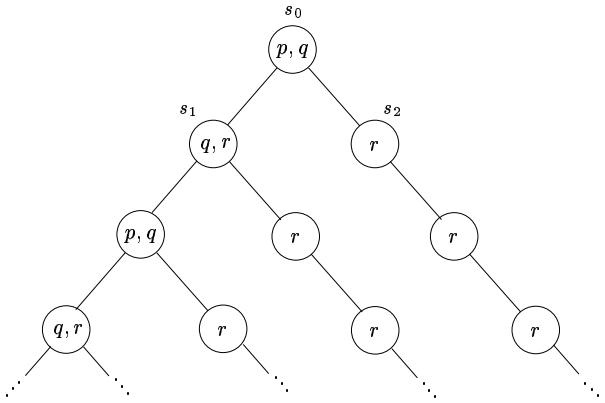
- ha f egyben állapotformula is, akkor $M, \pi \models f \iff \pi = s_0, s_1, \ldots$ és $M, s_0 \models f$
- $M, \pi \models \neg f_1$, $M, \pi \models f_1 \vee f_2$, $M, \pi \models f_1 \wedge f_2$ a szokásos módon
- $M, \pi \models \mathbf{X}f_1 \iff M, \pi^1 \models f_1$
- $M, \pi \models \mathbf{F}f_1 \iff$ van olyan $i \geq 0$, hogy $M, \pi^i \models f_1$
- $M, \pi \models \mathbf{G}f_1 \iff$ minden $i \geq 0$-ra $M, \pi^i \models f_1$
- $M, \pi \models f_1\,\mathbf{U}\,f_2 \iff$ van olyan $k \geq 0$, hogy $M, \pi^k \models f_2$ és minden $0 \leq i < k$-ra $M, \pi^i \models f_1$

- $M, \pi \models f_1 \mathbf{R} f_2 \iff$ minden $j \geq 0$-ra, ha tetszőleges $0 \leq i < j$-re $M, \pi^i \not\models f_1$, akkor $M, \pi^j \models f_2$

A következő négy ábrán tipikus példák láthatók. A feketével jelölt állapotokban teljesül a g.



A következő ábrán egy Kripke struktúrából széthajtogatott számítási fa látható, alatta pedig példák olyan formulákra, amelyek a Kripke struktúra bizonyos állapotaiban teljesülnek.



1. $M, s_0 \models p \wedge q$
2. $M, s_0 \models \neg r$
3. $M, s_0 \models \mathbf{EX}(q \wedge r)$
4. $M, s_0 \models \neg \mathbf{AX}(q \wedge r)$
5. $M, s_0 \models \neg \mathbf{EF}(p \wedge r)$
6. $M, s_2 \models \mathbf{EG}r$
7. $M, s_2 \models \mathbf{AG}r$
8. $M, s_0 \models \mathbf{AF}r$
9. $M, s_0 \models \mathbf{E}((p \wedge q)\mathbf{U}r)$
10. $M, s_0 \models \mathbf{A}(p\mathbf{U}r)$

5.2. Definíció. Az f és g állapotformulák ekvivalensek, azaz $f \equiv g$, ha minden $M = (S, R, L)$ Kripke struktúra és minden $s \in S$ esetén $M, s \models f \iff M, s \models g$ teljesül.

Az útformulák ekvivalenciája hasonlóan definiálható.

Példák ekvivalens formulákra:

$f \wedge g \equiv \neg(\neg f \vee \neg g)$
$f\mathbf{R}g \equiv \neg(\neg f \mathbf{U} \neg g)$

$\mathbf{F}f \equiv True\mathbf{U}f$, ahol $True$ egy azonosan igaz formula
$\mathbf{G}f \equiv \neg\mathbf{F}(\neg f)$
$\mathbf{A}f \equiv \neg\mathbf{E}(\neg f)$

5.3. Következmény. A $\vee, \neg, \mathbf{X}, \mathbf{U}$ és $\mathbf{E}$ operátorok adekvát (teljes) rendszert alkotnak, azaz bármely CTL* formula átalakítható olyan, az eredetivel ekvivalens formulává, amely csak a fenti operátorokat tartalmazza.

5.3. A CTL logika (branching time logic) és a modellvizsgálat alapfeladata

Csak olyan CTL* formulákat engedünk meg, amelyekben az $\mathbf{X}, \mathbf{F}, \mathbf{G}, \mathbf{U}$ és $\mathbf{R}$ időoperátorokat közvetlenül megelőzi valamely útkvantor.

Állapotformulák:

- ha $p \in AP$, akkor p állapotformula,
- ha f, g állapotformulák, akkor $\neg f, f \vee g, f \wedge g$ is állapotformulák,
- ha f útformula, akkor $\mathbf{E}f$ és $\mathbf{A}f$ állapotformula.

Útformulák

- ha f, g állapotformulák, akkor $\mathbf{X}f, \mathbf{F}f, \mathbf{G}f, f\mathbf{U}g$ és $f\mathbf{R}g$ útformulák.

Azonosságok CTL-ben

A CTL-ben 10 alapvető operátor van: **AX**, **EX**, **AF**, **EF**, **AG**, **EG**, **AU**, **EU**, **AR**, **ER**.

5.4. Tétel. *Az* **EX**, **EG**, **EU** *operátorhalmaz teljes.*

Bizonyítás.

$$\begin{aligned}
\mathbf{AX}f &\equiv \neg\mathbf{EX}(\neg f)\\
\mathbf{EF}f &\equiv \mathbf{E}(True\ \mathbf{U}\ f)\\
\mathbf{AG}f &\equiv \neg\mathbf{EF}(\neg f)\\
\mathbf{AF}f &\equiv \neg\mathbf{EG}(\neg f)\\
\\
\mathbf{A}(f\,\mathbf{U}\,g) &\equiv \neg\mathbf{E}(\neg g\,\mathbf{U}\,(\neg f \wedge \neg g)) \wedge \neg\mathbf{EG}(\neg g)\\
&\equiv \neg(\mathbf{E}(\neg g\,\mathbf{U}\,(\neg f \wedge \neg g)) \vee \mathbf{EG}(\neg g))\\
\mathbf{A}(f\,\mathbf{R}\,g) &\equiv \neg\mathbf{E}(\neg f\,\mathbf{U}\,\neg g)\\
\mathbf{E}(f\,\mathbf{R}\,g) &\equiv \neg\mathbf{A}(\neg f\,\mathbf{U}\,\neg g)
\end{aligned}$$

□

5.5. Tétel. *Az* **EX**, **AU**, **EU** *operátorhalmaz teljes.*

Bizonyítás. Az **EX**, **EG**, **EU** teljes, továbbá

$$\begin{aligned}
\mathbf{EG}f &\equiv \neg\mathbf{AF}(\neg f)\\
&\equiv \neg\mathbf{A}(True\ \mathbf{U}\,\neg F)
\end{aligned}$$

□

További teljes operátorhalmazok:

- **AG**, **AU**, **AX**
- **AF**, **EU**, **EX**

A modellvizsgálat alapfeladata

1) Adott: $M = (S, R, L)$ Kripke struktúra, $s_0 \in S$ állapot és f CTL formula. Kérdés: teljesül-e $M, s_0 \models f$?

2) Adott: $M = (S, R, L)$ Kripke struktúra és f CTL formula. Feladat: határozzuk meg az

$$\{s \in S \mid M, s \models f\}$$

halmazt!

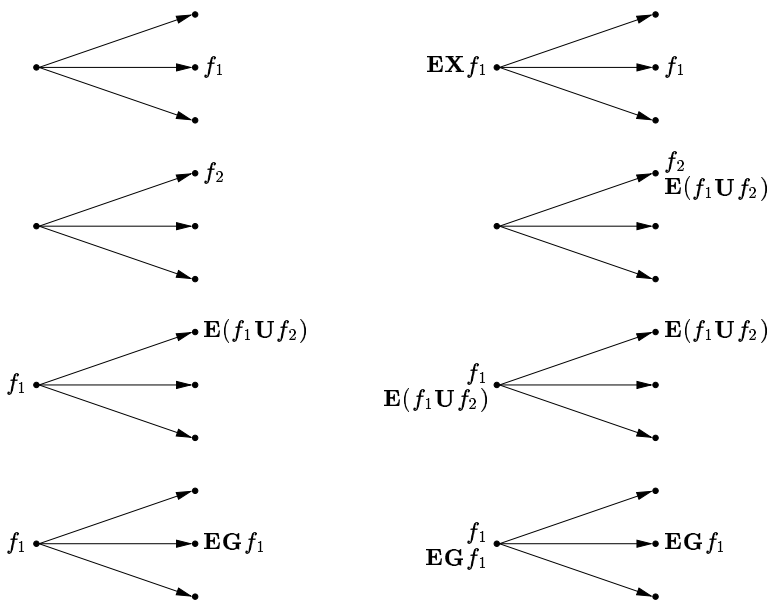
1) $\Rightarrow$ 2) (mivel véges számú állapot van)
2) $\Rightarrow$ 1) $s_0 \in \{s \in S \mid M, s \models f\}$?

5.4. A CTL modellvizsgálat címkézéssel

A modellvizsgálat alapfeladatát a következőképpen oldjuk meg. Adott $M = (S, R, L)$ Kripke struktúra és f formula esetén minden $s \in S$-re meghatározzuk a $lab(s)$ halmazt, amely f azon f' részformuláiból áll, melyekre $M, s \models f'$. Így

$$M, s \models f \iff f \in lab(s)$$

Példák: **EX**, **EU**, **EG**



A címkézési algoritmust pszeudokód formában adjuk meg, arra alapozva, hogy **EX**, **EU** és **EG** teljes operátorhalmazt alkotnak a CTL-ben.

A következő pszeudokódok egy $M = (S, R, L)$ Kripke struktúrára és egy f formulára vonatkoznak.

Előkészítő rész: **forall** $s \in S$ **do** $lab(s) := \emptyset$;

A főprogram neve $MC(f)$.

```
procedure MC(f);
    begin
    case
    f ∈ AP: forall s ∈ S do
        if f ∈ L(s) then lab(s) = lab(s) ∪ {f} endforall ;
    f = ¬f1 : MC(f1); forall s ∈ S do
        if f1 ∉ lab(s) then lab(s) = lab(s) ∪ {f} endforall ;
    f = f1 ∨ f2 : MC(f1); MC(f2); forall s ∈ S do
        if (f1 ∈ lab(s) or f2 ∈ lab(s)) then
            lab(s) = lab(s) ∪ {f} endforall ;
    f = EXf1 : MC(f1);
            CheckEX(f1);
    f = E(f1Uf2) : MC(f1); MC(f2);
            CheckEU(f1, f2);
    f = EG(f1) : MC(f1);
            CheckEG(f1);
    endcase
    end
```

A $Check\mathbf{EX}(f)$ és $Check\mathbf{EU}(f_1, f_2)$ eljárásokat a következőképpen adjuk meg.

```
procedure CheckEX(f);
var s, t, U;
begin
    U = {t ∈ S | f ∈ lab(t)}
    forall s ∈ S do
    if (∃t ∈ U) : s R t then
        lab(s) = lab(s) ∪ {EXf}
    endforall
end
```

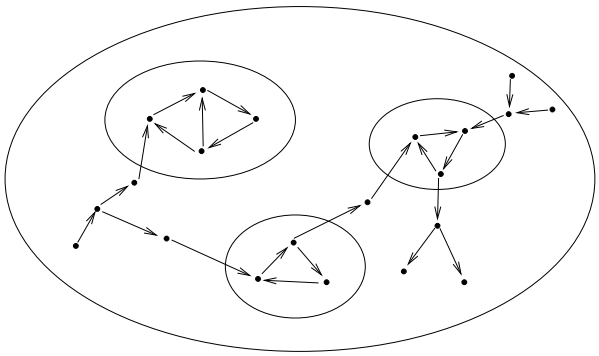
```
procedure CheckEU(f1, f2);
var s, t, U, V;
begin
    U = {s | f2 ∈ lab(s)}; V = {s | f1 ∈ lab(s)};
    forall s ∈ U do
        lab(s) = lab(s) ∪ {E(f1Uf2)}
    endforall
    while U ≠ ∅ do
        legyen s ∈ U
        forall t ∈ V do
            if tRs and t ∉ U then
                begin lab(t) = lab(t) ∪ {E(f1Uf2)}
                    U = U ∪ {t}
                end
        endforall
        U = U − {s}
    endwhile
```

end

A Check**EG** eljárás bonyolultabb, egy irányított gráf erősen összefüggő komponenseinek (SCC) meghatározásán alapul.

Egy irányított gráf valamely C részgráfja erősen összefüggő komponens, ha olyan maximális részgráf, melyben bármely $a, b \in C$ csúcsokra a elérhető b-ből és b elérhető a-ból.

C nemtriviális, ha egynél több csúcsból áll, vagy ha egy olyan csúcsból áll, amelyből hurokél vezet önmagába.

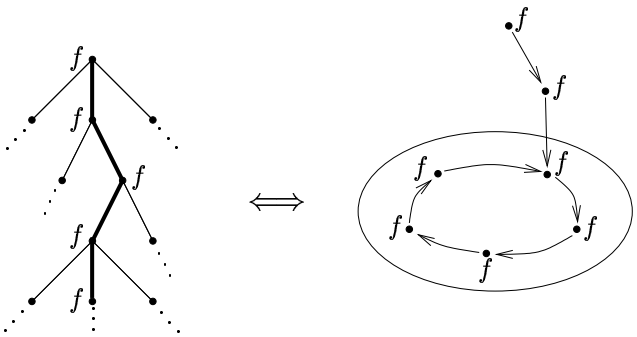


Legyen $M = (S, R, L)$ egy Kripke struktúra és f egy formula. Jelöljük $M' = (S', R', L')$-vel M azon részstruktúráját, amelyre

- $S' = \{s \in S \mid M, s \models f\}$
- $R' = R \cap (S' \times S')$
- L' az L S'-re való megszorítása

5.6. Lemma. Tetszőleges $s \in S$-re $M, s \models \mathbf{EG}f$ akkor és csak akkor áll fenn, ha a következő két feltétel teljesül:

1. $s \in S'$
2. az (S', R') irányított gráfnak van olyan C nemtriviális SCC-je, hogy s-ből út vezet valamely $t \in C$-be.



$s \models \mathbf{EG}f \iff s \in S'$ és az (S', R') irányított gráfnak van olyan C nemtriviális SCC-je, hogy s-ből út vezet valamely $t \in C$-be.

Az előbbi lemma alapján $Check\mathbf{EG}$ a következő lesz.

procedure $Check\mathbf{EG}(f_1)$;
var S', T, SCC, s, t;
  $S' = \{s \in S \mid f_1 \in lab(s)\}$;
  $SCC = \{C \mid$ nemtriviális SCC S'-ben $\}$;
  $T = \bigcup_{C \in SCC} C$;
  forall $s \in T$ **do** $lab(s) := lab(s) \cup \{\mathbf{EG}(f_1)\}$ **endforall**
  while $T \neq 0$ **do**
    Legyen $s \in T$
    forall $t \in S'$ **do**
      if $t\,R\,s$ **and** $t \notin T$ **then**
        begin $lab(t) = lab(t) \cup \{\mathbf{EG}(f_1)\}$
          $T = T \cup \{t\}$
        end
    endforall
    $T = T - \{s\}$
  endwhile
end

Időbonyolultsági kérdések:

A $Check\mathbf{EU}$ és a $Check\mathbf{EG}$ időbonyolultsága $O(\mid S \mid + \mid R \mid)$. Jelölje $\mid f \mid$ egy formula részformuláinak számát. Összefoglalásként kimondhatjuk a következő tételt.

5.7. Tétel. *Létezik olyan algoritmus, amely tetszőleges $M = (S, R, L)$ Kripke struktúrára, $s \in S$ és f CTL formula esetén eldönti, hogy $M, s \models f$ teljesül-e. Az algoritmus időbonyolultsága $O(\mid f \mid (\mid S \mid + \mid R \mid))$.*

Hivatkozások

[AO91] K. O. Apt, E.-R. Olderog, *Verification of Sequential and Concurrent Programs*, Springer-Verlag, 1991.

[BA01] M. Ben-Ari, *Mathematical Logic for Computer Science*, Springer-Verlag, 2001.

[CGP99] E. M. Clarke, O. Grumberg, D. A. Peled, *Model Checking*, The MIT Press, 1999.

[G86] J. H. Gallier, *Logic for Computer Science*, John Wiley & Sons, 1986.

[HR00] M. Huth, M. Ryan, *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge Unicersity Press, 2000.

[LS87] J. Loeckx, K. Sieber, *The Foundations of Program Verification*, John Wiley & Sons, 1987.

[S89] Uwe Schöning, *Logic for Computer Scientists*, Birkäuser, 1989.

[NS97] A. Nerode, R. A. Shoare, *Logic for Applications*, Springer-Verlag, 1997.