MATEMATIKAI LOGIKA

SIMON ANDRÁS

Tartalomjegyzék

1. Propozicionális logika

1.1. Bemelegítés Lovagok mindig igazat mondanak, lókötők mindig hazudnak. Az alábbi feladatokban a lehető legtöbb szereplőről kell eldönteni, hogy lovag vagy lókötő.

1.1. Gyakorlat. B azt mondja, hogy A azt mondja, hogy A lókötő.

1.2. Gyakorlat. B azt mondja, hogy mindketten lókötők.

1.3. Gyakorlat. B azt mondja, hogy kettőjük közül az legalább az egyik lókötő.

1.2. Szintaxis Atomi formulák: $\Pi = \{ p_0, \ldots, p_n \}$ de általában p, q és ezek indexelt változatait használjuk. Formulák:

$$Form_\Pi = \Pi \mid \neg Form_\Pi \mid Form_\Pi \wedge Form_\Pi$$

Magyarul: $Form_\Pi$ a legszűkebb, Π-t tartalmazó, $\neg$-ra és $\wedge$-ra zárt halmaz ($Form_\Pi = \bigcap\{ H : \Pi \subseteq H \quad \text{és} \quad (\forall \varphi, \psi \in H)(\neg\varphi \in H \quad \text{és} \quad \varphi \wedge \psi \in H) \}$). $\neg$ (*nem*) és $\wedge$ (*és*) *logikai konnektívumok* (formulákból formulákba képező függvények).

(Formulákat néha állításoknak, vagy mondatoknak is hívjuk.)

Precedencia: $\neg$, $\wedge$ (és majd később is: unér konnektívumok erősebben kötnek mint a binérek).

Példák: p, $\neg\neg(p \wedge q)$, $p \wedge \neg(p \wedge q)$, $p \wedge \neg q$. Nem-példák: $p \neg \wedge q$.

Jelölés: formulák: φ, ψ, χ,..., formula-halmazok: Σ, Δ,....

1.4. *Megjegyzés.*

$$\langle Form_\Pi, \neg, \wedge \rangle$$

(formula)algebra (Π által generált term-algebra, abszolút szabad algebra). Semmilyen nemtriviális azonosság (pl.: $x \wedge y = y \wedge x$) nem igaz benne.

1.5. Állítás (Formulaindukció)**.** *Ha egy tulajdonság igaz* Π *elemeire, és igazsága öröklődik a formulaképzés során, azaz invariáns az* $\neg$*-re és* $\wedge$*-re (ha igaz* φ *és* ψ*-re, akkor* $\neg\varphi$*-re és* $\varphi \wedge \psi$*-re is igaz), akkor igaz* $Form_\Pi$ *minden elemére.*

1.6. Definíció (Származtatott konnektívumok)**.**

- $\varphi \vee \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \wedge \neg\psi)$ („vagy”)
- $\varphi \to \psi \stackrel{\text{def}}{=} \neg\varphi \vee \psi$ („ha... akkor”)
- $\bot \stackrel{\text{def}}{=} p_0 \wedge \neg p_0$
- $\top \stackrel{\text{def}}{=} \neg\bot$
- $\varphi \leftrightarrow \psi \stackrel{\text{def}}{=} (\varphi \to \psi) \wedge (\psi \to \varphi)$ (ekvivalencia, csakkor)

1.3. Szemantika Mit „jelentenek” a formulák (speciel: mikor igazak). A formuláknak általában nem magukban van jelentésük/igazságértékük, hanem a dolgok egy lehetséges állása mellett, „egy világban”, magyarul: egy *modellben.*

1.7. Definíció (modell)**.** A propozicionális logika egy modellje: $\mathcal{M} : \Pi \longrightarrow \{0, 1\}$.

1.8. Definíció (formula jelentése)**.** $\varphi \in Form_\Pi$ jelentése az $\mathcal{M}$ modellben ($\varphi^\mathcal{M} = \mathcal{M}(\varphi)$; $\mathcal{M}$-et kiterjesztjük Π-ről $Form_\Pi$-re) (a formulák felépítésére vonatkozó rekurzióval):

- $p^\mathcal{M} = \mathcal{M}(p)$ ha $p \in \Pi$
- $(\neg\varphi)^\mathcal{M} = 1 - \varphi^\mathcal{M}$
- $(\varphi \wedge \psi)^\mathcal{M} = \varphi^\mathcal{M} \cdot \psi^\mathcal{M}$.

Azt mondjuk, hogy φ igaz $\mathcal{M}$-ben, vagy $\mathcal{M}$ modellje φ-nek, ha $\varphi^\mathcal{M} = 1$.

Tehát $\neg$-ot és $\wedge$-ot a modellben $\{0,1\}$-ből, ill. $\{0,1\}^2$-ből $\{0,1\}$-be képező függvények „implementálják” — az ilyen függvényeket igazságfüggvényeknek hívják. És igazságtáblázattal lehet megadni őket. Pl.: $\neg$ és $\wedge$ igazságtáblázata

p	$\neg p$
0	1
1	0

és

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

.

$\models$ definíciója direktebben:
- $\mathcal{M} \models p$ iff $\mathcal{M}(p) = 1$
- $\mathcal{M} \models \neg\varphi$ iff $\mathcal{M} \not\models \varphi$ (vagyis ha nem igaz, hogy $\mathcal{M} \models \varphi$)
- $\mathcal{M} \models \varphi \wedge \psi$ iff $\mathcal{M} \models \varphi$ és $\mathcal{M} \models \psi$.

1.9. Állítás. $\mathcal{M} \models \varphi \iff \varphi^{\mathcal{M}} = 1$

Biz. Formulaindukcióval: $p \in \Pi$-re $\mathcal{M} \models p \iff p^{\mathcal{M}} = \mathcal{M}(p) = 1$. Tegyük fel, hogy φ-re igaz az állítás; akkor

$$\mathcal{M} \models \neg\varphi \iff \mathcal{M} \not\models \varphi \iff \varphi^{\mathcal{M}} \neq 1 \iff \varphi^{\mathcal{M}} = 0 \iff (\neg\varphi)^{\mathcal{M}} = 1 - \varphi^{\mathcal{M}} = 1.$$

Végül, ha igaz φ, ψ-re, akkor

$$\begin{aligned}\mathcal{M} \models \varphi \wedge \psi &\iff (\mathcal{M} \models \varphi \quad \text{és} \quad \mathcal{M} \models \psi)\\ &\iff \varphi^{\mathcal{M}} = 1 = \psi^{\mathcal{M}} \iff (\varphi \wedge \psi)^{\mathcal{M}} = \varphi^{\mathcal{M}} \cdot \psi^{\mathcal{M}} = 1.\end{aligned}$$

$\square$

1.10. Gyakorlat. A bizonyításban használtuk, hogy $\varphi^{\mathcal{M}} \in \{0,1\}$. Hol? Bizonyítsuk ezt be formulaindukcióval!

1.11. Példák. (1) $\mathcal{M} \models \varphi \vee \psi$ iff $\mathcal{M} \models \neg(\neg\varphi \wedge \neg\psi)$ iff (nem igaz, hogy $\mathcal{M} \models \neg\varphi \wedge \neg\psi$) iff (nem igaz, hogy $\mathcal{M} \models \neg\varphi$ és $\mathcal{M} \models \neg\psi$) iff (nem igaz, hogy $\mathcal{M} \not\models \varphi$ és $\mathcal{M} \not\models \psi$) iff $\mathcal{M} \models \varphi$ vagy $\mathcal{M} \models \psi$.

(2) Mikor lesz $\mathcal{M} \models \varphi \to \psi$?

$$\mathcal{M} \models \varphi \to \psi \iff \mathcal{M} \models \neg\varphi \vee \psi \iff \mathcal{M} \models \neg\varphi \text{ vagy } \mathcal{M} \models \psi \iff \mathcal{M} \not\models \varphi \text{ vagy } \mathcal{M} \models \psi.$$

Következésképp $\mathcal{M} \not\models \varphi \to \psi$ iff $\mathcal{M} \models \varphi$ és $\mathcal{M} \not\models \psi$.

(3) $\mathcal{M} \models \neg\neg\varphi$ iff $\mathcal{M} \not\models \neg\varphi$ iff $\mathcal{M} \models \varphi$.

Hogy számoljuk ki egy formula igazságértékét egy modellben? Pl. igazságtáblázattal (oszlopok a részformulák): pl. igaz-e az $\mathcal{M}(p) = \mathcal{M}(q) = 1$, $\mathcal{M}(r) = 0$ modellben a $\neg((p \wedge q) \vee r)$ formula:

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$	$\neg((p \wedge q) \vee r)$
1	1	0	1	1	0

, tehát nem.

1.12. Definíció. Legyen $\mathcal{M}$ modell, és $\Sigma \cup \{\varphi\} \subseteq Form$. Akkor

(1) $\mathcal{M} \models \Sigma$ iff $(\forall\varphi \in \Sigma)\mathcal{M} \models \varphi$ ($\mathcal{M}$ modellje Σ-nak)

(2) $\Sigma \models \varphi$ iff $\forall\mathcal{M}(\mathcal{M} \models \Sigma \implies \mathcal{M} \models \varphi)$ (φ *szemantikus következménye* Σ-nak)

(3) $\models \varphi$ ha $\emptyset \models \varphi$, azaz ha φ minden modellben igaz (merthogy az üres halmaznak minden modell modellje) (φ *érvényes formula*, *logikai igazság*)

(4) φ ill. Σ *kielégíthető*, ha van modellje, *kielégíthetetlen* ha nem kielégíthető, azaz ha nincs modellje

(5) $\varphi \equiv \psi$ (*ekvivalensek*) ha ugyanazok a modelljei.

1.13. Példák. (1) Ha $\mathcal{M}(p) = 1$ és $\mathcal{M}(q) = 0$ akkor $\mathcal{M} \models \{p, \neg q, q \to p\}$; általában, $\mathcal{M} \models \{\varphi\} \iff \mathcal{M} \models \varphi$.

(2) $\{p \to q, p\} \models q$; ha $\varphi \in \Sigma$, akkor $\Sigma \models \varphi$

(3) $\models p \vee \neg p$, $\models p \to p$, de $\not\models p \to \neg p$

(4) Kielégíthetetlen: $p \wedge \neg p$. Kielégíthető minden érvényes formula; kielégíthető de nem érvényes: $p \to \neg p$, vagy akár: p.

(5) $\varphi \equiv \neg\neg\varphi$, ld. a fenti példát! $p \wedge q \equiv q \wedge p$, azaz a konjunkció kommutatív, és $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$, vagyis asszociatív is. És persze ugyanezek igazak $\vee$-ra is. Következésképp írhatunk olyanokat, hogy $p_1 \wedge p_2 \wedge \cdots \wedge p_n (= \bigwedge_{i=1}^{n} p_i)$, és ha Σ véges formulahalmaz, akkor $\bigwedge \Sigma$, $\bigvee \Sigma$ értelmes.

1.14. *Megjegyzés.* Véges Σ-ra (Σ kielégíthető iff $\bigwedge \Sigma$ kielégíthető).

1.15. Állítás. *φ pontosan akkor érvényes, ha $\neg\varphi$ kielégíthetetlen. Sőt: $\Sigma \models \varphi$ pontosan akkor, ha $\Sigma \cup \{\neg\varphi\}$ kielégíthetetlen.*

Biz.

$$\begin{aligned}\Sigma \models \varphi &\iff \forall \mathcal{M}(\mathcal{M} \models \Sigma \implies \mathcal{M} \models \varphi)\\ &\iff \nexists \mathcal{M}(\mathcal{M} \models \Sigma \ \&\ \mathcal{M} \not\models \varphi) \iff \nexists \mathcal{M}(\mathcal{M} \models \Sigma \ \&\ \mathcal{M} \models \neg\varphi)\end{aligned}$$

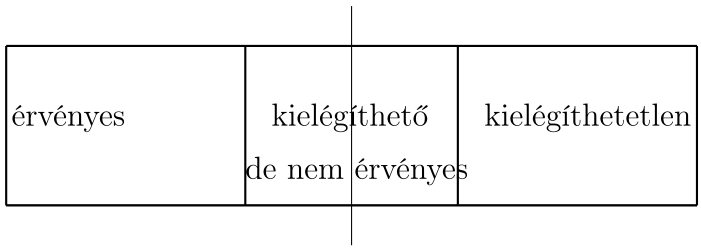
□

1.16. Következmény. *φ kielégíthető $\iff$ $\neg\varphi$ nem érvényes.*

Biz.

$$\begin{aligned}\varphi \text{ kielégíthető} &\iff \varphi \text{ nem kielégíthetetlen}\\ &\iff \neg\neg\varphi \text{ nem kielégíthetetlen} \iff \neg\varphi \text{ nem érvényes.}\end{aligned}$$

□



1. ábra. A középső függőleges vonal szimmetriatengely

Hogyan dönthető el egy formula kielégíthetősége (-hetetlensége, érvényessége)? (A logikák többségében sehogy; propozicionális logikában viszont könnyen — legalábbis elvileg.) Egy lehetséges módszer: igazságtáblázattal.

1.17. Példa. $\models \neg p \to (p \to q)$, mert

p	q	$\neg p$	$p \to q$	$\neg p \to (p \to q)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	0	1	1

azaz $\neg p \to (p \to q)$ valóban minden modellben (ld. alább!) igaz.

Ha n atomi formula szerepel φ-ben, akkor a φ érvényességét eldöntő igazságtáblázatnak 2^n sora van, következésképp ez nem egy praktikus eldöntési eljárás.

Miért működik? Két oka van: (1) adott $\mathcal{M}$-ben ki tudjuk számolni φ igazságértékét (2) noha végtelen (sőt, kontinuum sok) modell van, csak véges sok modellben kell φ igazságértékét kiszámolni, mert

1.18. Állítás. *$\mathcal{M}$, $\mathcal{M}'$ modellek, amik legfeljebb p-n különböznek. Ha p nem fordul elő φ-ben, akkor $\mathcal{M} \models \varphi \iff \mathcal{M}' \models \varphi$.*

Biz. Formulaindukcióval. $\square$

Ezért mondhattuk az előző példában, hogy a formula minden modellben igaz, noha csak négyben néztük meg.

1.19. Következmény. *A propozicionális logikában érvényes formulák halmaza ($\{\varphi : \ \models \varphi\}$) eldönthető.*

1.20. Állítás. *$\varphi \equiv \psi$ iff $\models \varphi \leftrightarrow \psi$; következésképp, mivel $\models \varphi \iff \models \varphi \leftrightarrow \top$, $\models \varphi \iff \varphi \equiv \top$.*

Úgyhogy $\equiv$ csak egy kényelmes rövidítés.

1.21. Gyakorlat. Adjunk példát olyan kételemű kielégíthetetlen formulahalmazra, aminek minden valódi részhalmaza kielégíthető.

1.22. Gyakorlat. Adjunk példát olyan 3-elemű kielégíthetetlen formulahalmazra, aminek minden valódi részhalmaza kielégíthető.

1.23. Gyakorlat. Adjunk példát olyan n-elemű kielégíthetetlen formulahalmazra, aminek minden valódi részhalmaza kielégíthető.

1.24. Gyakorlat. Kielégíthető-e a

$$\Sigma = \{p_1 \vee p_2, \neg p_2 \vee \neg p_3, p_3 \vee p_4, \neg p_4 \vee \neg p_5, \dots\} = \{\, p_{2n-1} \vee p_{2n}, \neg p_{2n} \vee \neg p_{2n+1} : n > 1\,\}$$

végtelen formulahalmaz?

1.25. Gyakorlat. Igazak-e a következő állítások?

(1) Ha $\models \varphi \vee \psi$, akkor $\models \varphi$ vagy $\models \psi$.
(2) Ha $\models \varphi \to \psi$ és $\models \varphi$, akkor $\models \psi$.
(3) Ha $\varphi \to \psi$ és φ kielégíthető, akkor ψ kielégíthető.
(4) Ha $\models \varphi \to \psi$, és φ kielégíthető, akkor ψ kielégíthető.

1.26. Gyakorlat. Helyes-e a következő érvelés? Ha esik az eső, viszek esőkabátot. Nem esik az eső. Tehát nem viszek esőkabátot. Formalizálva: $\{p \to q, \neg p\} \models \neg q$?

Ez nem tévesztendő össze a következővel: $\{p \to q, p\} \models q$ (modus ponens).

∗ ∗ ∗

Most már megkísérelhetjük a lovagos fejtörőket kijelentéslogikai problémákként kezelni. Nézzük az elsőt:

B azt mondja, hogy A azt mondja, hogy A lókötő.

A résztvevőkről feltehetjük, hogy minden általuk kijelentett állítással ekvivalens kijelentésváltozók (így a lovagok igaz, a lókötők hamis kijelentésváltozóknak felelnek meg), hiszen pontosan akkor lovagok, ha kijelentéseik igazak, és akkor lókötők, ha a kijelentéseik hamisak. Vagyis például ebben a fejtörőben „A azt mondja, hogy A lókötő" formalizálható az $A \leftrightarrow \neg A$ formulával; és mivel B ezt mondja, ezért $B \leftrightarrow (A \leftrightarrow \neg A)$. Tehát a kérdés A ill. B igazságértéke ez utóbbi formula modelljeiben. Amelyik igaz a modellben, az lovag, amelyik hamis, az lókötő. Ha több modell is kielégíti a formlá(ka)t, vagyis valamelyik résztvevőnek megfelelő kijelentésváltozó igaz és hamis is lehet, akkor arra a résztvevőre nézve semmi nem következik a feltevésekből. Mint például ebben az esetben is:

A	B	$A \leftrightarrow \neg A$	$B \leftrightarrow (A \leftrightarrow \neg A)$
0	0	0	1
0	1	0	0
1	0	0	1
1	1	0	0

Itt két jó modell is van, és ezek nem egyeznek meg A értékét illetően, de B mindkettőben hamis. Vagyis az jött ki, hogy $\{ B \leftrightarrow (A \leftrightarrow \neg A) \} \models \neg B$; ezért B lókötő — A viszont bármi lehet, mert $\{ B \leftrightarrow (A \leftrightarrow \neg A) \} \not\models A$ és $\{ B \leftrightarrow (A \leftrightarrow \neg A) \} \not\models \neg A$. Ez összhangban van azzal, amit eredetileg gondoltunk, nevezetesen, hogy B hazudik, mert senki sem mondhatja magáról, hogy lókötő (mert ha az, akkor azt hazudja magáról, hogy lovag, ha meg lovag, akkor azért).

Nézzük a következőt!

B azt mondja, hogy mindketten lókötők.

A nehéz rész ezt lefordítani logikára. De a fordítás biztosan úgy fog kezdődni, hogy $B \leftrightarrow \ldots$, mert B mond valamit, és ahogy ebben megegyeztünk, mindenki azzal ekvivalens, amit mond. És B azt mondja, hogy mindketten lókötők; de „X lókötő" azt jelenti, hogy X nem igaz, azaz $\neg X$ igaz. Vagyis „mindketten (azaz A és B is) lókötők" a $\neg A \wedge \neg B$ formulával fordítható le. Vagyis $B \leftrightarrow (\neg A \wedge \neg B)$ a végső formulánk, aminek a modelljeit keressük.

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$B \leftrightarrow (\neg A \wedge \neg B)$
0	0	1	1	1	0
0	1	1	0	0	0
1	0	0	1	0	1
1	1	0	0	0	0

Itt most pontosan egy jó modell van, tehát minden résztvevőről kiderül, hogy lovag, vagy lókötő. Történetesen A lovag és B lókötő, mert $\{ B \leftrightarrow (\neg A \wedge \neg B) \} \models A \wedge \neg B$. Ezt természetesen eredetileg is így gondoltuk, azzal az érveléssel, hogy B nem lehet lovag (mert akkor lókötő is lenne), tehát lókötő, tehát hazudott, azaz nem igaz, hogy mindketten lókötők, vagyis A lovag.

1.27. Gyakorlat. B azt mondja, kettőjük közül az legalább az egyik lókötő. Találjuk ki *logikával*, hogy mi a helyzet!

* * *

1.28. Tétel (Dedukciótétel $\models$-re)**.** $\Sigma \cup \{\varphi\} \models \psi \iff \Sigma \models \varphi \to \psi$.

Biz.

$$\begin{aligned}
& \Sigma \not\models \varphi \to \psi \\
\iff\ & \exists \mathcal{M}(\mathcal{M} \models \Sigma \quad \text{és} \quad \mathcal{M} \not\models \varphi \to \psi) \\
\iff\ & \exists \mathcal{M}(\mathcal{M} \models \Sigma \quad \text{és} \quad (\mathcal{M} \models \varphi \quad \text{és} \quad \mathcal{M} \not\models \psi)) \\
\iff\ & \exists \mathcal{M}(\mathcal{M} \models \Sigma \cup \{\varphi\} \quad \text{és} \quad \mathcal{M} \not\models \psi) \\
\iff\ & \Sigma \cup \{\varphi\} \not\models \psi
\end{aligned}$$

□

1.29. Tétel (Nevezetes azonosságok)**.**

(1) $\neg\neg\varphi \equiv \varphi$ *(volt)*
(2) $\varphi \to \bot \equiv \neg\varphi$ *(„indirekt biz.")*
(3) $\varphi \to (\psi \to \chi) \equiv \varphi \wedge \psi \to \chi$ *(„currying")*
(4) $\models (\varphi \wedge (\varphi \to \psi)) \to \psi$ *(volt: MP)*
(5) $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$ *(kontrapozíció)*
(6) $\varphi \vee \psi \equiv \neg\varphi \to \psi$
(7) $\neg(\varphi \wedge \psi) \equiv \varphi \to \neg\psi$.
(8) $\wedge$ *és* $\vee$ *kommutatív és asszociatív*
(9) $\varphi \wedge \varphi \equiv \varphi$, $\varphi \vee \varphi \equiv \varphi$ *(idempotencia)*
(10) $(\varphi \vee \psi) \wedge \varphi \equiv \varphi$, $(\varphi \wedge \psi) \vee \varphi \equiv \varphi$ *(abszorpció)*
(11) $\varphi \wedge (\psi \vee \chi) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$, $\varphi \vee (\psi \wedge \chi) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \chi)$ *(disztributivitás)*
(12) $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$, $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ *(De Morgan)*
(13) $\models \varphi \to \varphi \vee \psi$
(14) $\models \varphi \wedge \psi \to \varphi$

1.30. Tétel.

(1) *Ha* $\psi_1^{\mathcal{M}} = \psi_2^{\mathcal{M}}$*, és* φ_2*-t úgy kaptuk* φ_1*-ből, hogy benne* ψ_1 *egy előfordulását kicseréltük* ψ_2*-re, akkor* $\varphi_1^{\mathcal{M}} = \varphi_2^{\mathcal{M}}$.
(2) *Az* $\mathcal{M}$ *modellre,* $p_1, \ldots, p_n \in \Pi$*-re és* $\sigma_1, \ldots, \sigma_n \in Form$*-ra legyen* $\mathcal{M}'$ *a következő modell:* $\mathcal{M}'(p_i) = \sigma_i^{\mathcal{M}}$ *és* $\mathcal{M}'(p) = \mathcal{M}(p)$ *a többi kijelentésváltozóra. Akkor minden* φ *formulára* $\varphi^{\mathcal{M}'} = \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]^{\mathcal{M}}$*, ahol* $\varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$ *az a formula, amit* φ*-ből a* $p_1, \ldots, p_n$ *kijelentésváltozók* $\sigma_1, \ldots, \sigma_n$*-el való párhuzamos helyettesítésével kapunk.*[1]

Biz. Az első φ_1-re, a második φ-re vonatkozó formulaindukcióval. □

1.31. Következmény.

(1) *Ha* $\psi_1 \equiv \psi_2$*, és* φ_1*,* φ_2 *mint a tétel első pontjában, akkor* $\varphi_1 \equiv \varphi_2$.

[1] A párhuzamos helyettesítés hivatalos definíciója:

- $p[\sigma_1/p_1, \ldots, \sigma_n/p_n] = \sigma_i$ ha $p = p_i$ és p egyébként
- $(\neg\varphi)[\sigma_1/p_1, \ldots, \sigma_n/p_n] = \neg(\varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n])$
- $(\varphi \wedge \psi)[\sigma_1/p_1, \ldots, \sigma_n/p_n] = \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n] \wedge \psi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$

(2) *Ha* $\models \varphi$, *akkor* $\models \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$ *minden* $p_1, \ldots, p_n \in \Pi$*-re és* $\sigma_1, \ldots, \sigma_n \in Form$*-ra.*

Biz. 1. Ha $\varphi_1 \not\equiv \varphi_2$, akkor van olyan $\mathcal{M}$ modell, amire $\varphi_1^{\mathcal{M}} \neq \varphi_2^{\mathcal{M}}$, noha $\psi_1 \equiv \psi_2$ miatt $\psi_1^{\mathcal{M}} = \psi_2^{\mathcal{M}}$.
2. Ha $\not\models \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$, azaz $\mathcal{M} \not\models \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$ valamilyen $\mathcal{M}$ modellre, akkor a tétel (2) pontja miatt $\mathcal{M}' \not\models \varphi$, és így $\not\models \varphi$, ahol $\mathcal{M}'$ a (2)-ben definiált modell, amire $\varphi^{\mathcal{M}'} = \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n]^{\mathcal{M}} = 0$. □

Vagyis kijelentéslogikai formulákkal úgy „számolhatunk”, mint algebrában. A következmény első pontja miatt állíthatjuk például, hogy $\varphi \wedge (\psi \vee \psi) \equiv \varphi \wedge \psi$ (mert $(\psi \vee \psi)$-t kicseréltük a vele ekvivalens ψ-re), és a második pontja miatt mindegy, hogy azt állítjuk, $\models p \vee \neg p$, vagy azt, hogy $\models \varphi \vee \neg\varphi$. Az első speciális esete a másodiknak, a második viszont következik az elsőből a következmény második pontja miatt.

1.4. Interpoláció

1.32. Gyakorlat. Ha $\models \varphi \to \psi$, és φ-ben és ψ-ben nincsenek közös atomi formulák, akkor φ kielégíthetetlen vagy ψ érvényes.

1.33. Következmény. *Ha* $\models \varphi \to \psi$*, és* φ*-ben és* ψ*-ben nincsenek közös atomi formulák, akkor*

$$\models \varphi \to \bot \text{ és } \models \bot \to \psi$$

vagy

$$\models \varphi \to \top \text{ és } \models \top \to \psi.$$

A következő tételben, amely ennek az állításnak az általánosítása, feltesszük, hogy $\bot$ és $\top$ logikai konstansok (0-argumentumú konnektívumok), és nem definiált formulák. (Persze a jelentésük az eddigi, azaz $\top$ minden modellben igaz, $\bot$ minden modellben hamis.) Ez nem lényeges, csak sokkal egyszerűbbé teszi a tétel és a bizonyítás megfogalmazását.

1.34. Tétel (Craig interpoláció)**.** *Ha* $\models \varphi \to \psi$*,* X *ill.* Y *a* φ*-ben és* ψ*-ben előforduló atomi formulák és* $Z = X \cap Y$*,akkor van olyan* $\chi \in Form_Z$*, amire* $\models \varphi \to \chi$ *és* $\models \chi \to \psi$*.*

χ-t φ és ψ *interpolánsának* hívják.

Biz. Indukció $|X \setminus Y|$-ra. Ha $|X \setminus Y| = 0$, akkor $X \subseteq Y$, következésképp $Z = X$, tehát φ jó lesz interpolánsnak.

Tegyük fel, hogy $|X \setminus Y| = n$-re tudjuk (azaz ha a φ-ben előforduló, de ψ-ben nem előforduló atomi formulák száma n, akkor van interpoláns), és legyen $|X \setminus Y| = n + 1$. Rögzítsük $p \in X \setminus Y$-t, és legyen $\varphi_\top$, $\varphi_\bot$ olyan, hogy φ-ben p minden előfordulását $\top$-ra ill. $\bot$-ra cseréljük. Akkor egyrészt $\varphi_\top$, $\varphi_\bot$-ban eggyel kevesebb ψ-ben nem szereplő atomi formula van, másrészt $\models \varphi_\top \to \psi$ és $\models \varphi_\bot \to \psi$, pl. az első azért, mert

$$\mathcal{M} \models \varphi_\top \implies \mathcal{M}[p/1] \models \varphi_\top \implies \mathcal{M}[p/1] \models \varphi \implies \mathcal{M}[p/1] \models \psi \implies \mathcal{M} \models \psi$$

mivel p nem fordul elő ψ-ben (az első és utolsó implikációban 1.18-t, a másodikban 1.30(1)-et használtuk). Tehát az indukciós feltevés miatt van $\chi_\top$, $\chi_\bot \in Form_{(X \setminus \{p\}) \cap Y} = Form_{X \cap Y}$, hogy

$$\models \varphi_\top \to \chi_\top, \qquad \models \chi_\top \to \psi$$
$$\models \varphi_\bot \to \chi_\bot, \qquad \models \chi_\bot \to \psi.$$

No de akkor $\chi_\top \vee \chi_\bot$ jó lesz interpolánsnak, mert

- $\models \varphi \to (\chi_\top \vee \chi_\bot)$: tegyük fel ui., hogy $\mathcal{M} \models \varphi$; ha $\mathcal{M}(p) = 0$, akkor (1.30(1) miatt) $\mathcal{M} \models \varphi_\bot$ és így $\mathcal{M} \models \chi_\bot$, ha meg $\mathcal{M}(p) = 1$, akkor (1.30(1) miatt) $\mathcal{M} \models \varphi_\top$ és így $\mathcal{M} \models \chi_\top$.
- $\models (\chi_\top \vee \chi_\bot) \to \psi$: mert ha $\mathcal{M} \models \chi_\top \vee \chi_\bot$, akkor $\mathcal{M} \models \chi_\top$ vagy $\mathcal{M} \models \chi_\bot$, tehát mindkét esetben $\mathcal{M} \models \psi$.

□

1.35. Gyakorlat. Keressünk interpolánst a következő két érvényes formulára: $p \wedge q \to p \vee r$ ill. $p \wedge q \to (r \to p)$.

1.5. Galois-kapcsolat

1.36. Definíció (1.12 folytatása).

- Modellek egy M egy halmazára $M \models \Sigma \iff (\forall \mathcal{M} \in M)(\mathcal{M} \models \Sigma)$.
- $\Sigma \subseteq Form$-ra és modellek egy M halmazára legyen $\mathrm{Mod}(\Sigma) = \{\mathcal{M} : \mathcal{M} \models \Sigma\}$ és $\mathrm{Th}(M) = \{\varphi \in Form : M \models \varphi\}$.

1.37. Tétel. *$\Sigma \subseteq Form$-ra és modellek egy M halmazára*

(1) $M \subseteq \mathrm{Mod}(\Sigma) \iff \Sigma \subseteq \mathrm{Th}(M)$
(2) $M \subseteq \mathrm{Mod}(\mathrm{Th}(M))$ *és* $\Sigma \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma))$
(3) Mod *és* Th *monoton csökkennek.*
(4) $\mathrm{Th}(\mathrm{Mod}(X))$ *és* $\mathrm{Mod}(\mathrm{Th}(X))$ *monoton nőnek.*
(5) $\mathrm{Th}(M) \subseteq \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(M)))$ *és* $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma)))$
(6) $\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(M))) = \mathrm{Th}(M)$ *és* $\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma))) = \mathrm{Mod}(\Sigma)$
(7) $\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(M)))) = \mathrm{Mod}(\mathrm{Th}(M))$ *és* $\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma)))) = \mathrm{Th}(\mathrm{Mod}(\Sigma))$

Biz. 1. Mindkét oldal ekvivalens azzal, hogy $M \models \Sigma$.

2. (1) miatt $M \subseteq \mathrm{Mod}(\mathrm{Th}(M)) \iff \mathrm{Th}(M) \subseteq \mathrm{Th}(M)$ és $\Sigma \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma)) \iff \mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\Sigma)$.

3. Ha $M \subseteq M'$, akkor (2) miatt $M \subseteq M' \subseteq \mathrm{Mod}(\mathrm{Th}(M'))$, amiből (1) miatt $\mathrm{Th}(M') \subseteq \mathrm{Th}(M)$. Ugyanígy, ha $\Sigma \subseteq \Sigma'$, akkor (2) miatt $\Sigma \subseteq \Sigma' \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma'))$, amiből (1) miatt $\mathrm{Mod}(\Sigma') \subseteq \mathrm{Mod}(\Sigma)$.

4. Ha $M \subseteq M'$, akkor (3) miatt $\mathrm{Th}(M') \subseteq \mathrm{Th}(M)$, amiből (3) másik állítása miatt $\mathrm{Mod}(\mathrm{Th}(M)) \subseteq \mathrm{Mod}(\mathrm{Th}(M'))$. Hasonlóan a másik.

5. (2)-t alkalmazzuk $\mathrm{Th}(M)$-re és $\mathrm{Mod}(\Sigma)$-ra.

6. (5)-ből következik, mert (2) és (3) miatt $\mathrm{Th}(M) \supseteq \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(M)))$ és $\mathrm{Mod}(\Sigma) \supseteq \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma)))$.

7. (6) miatt. □

1.38. Definíció. $c : \mathcal{P}(X) \to \mathcal{P}(X)$ lezárási operátor, ha

monoton: $x \subseteq y$-ra $c(x) \subseteq c(y)$
extenzív: $x \subseteq c(x)$
idempotens: $c(c(x)) = c(x)$

1.39. Következmény. $\mathrm{Th}(\mathrm{Mod}(X))$ *és* $\mathrm{Mod}(\mathrm{Th}(X))$ *lezárási operátorok.*

Biz. Monoton 1.37(4), idempotens 1.37(7) és extenzív 1.37(2) miatt. □

1.40. Állítás. *Modellek egy M halmaza ill. $\Sigma \subseteq Form$ pontosan akkor zárt (azaz $M = \operatorname{Mod}\operatorname{Th} M$ ill. $\Sigma = \operatorname{Th}\operatorname{Mod}\Sigma$) ha $M = \operatorname{Mod}\Delta$ ill. $\Sigma = \operatorname{Th}\mathcal{N}$ valamely $\Delta \subseteq Form$-ra és modellek valamely N halmazára.*

Biz. Ha zártak, akkor persze van ilyen Δ és N ($\operatorname{Th} M$ ill. $\operatorname{Mod}\Sigma$). Fordítva, ha van ilyen Δ és N, akkor 1.37(6) szerint zártak. □

1.41. Állítás. $\operatorname{Mod}(\operatorname{Th}(X))$ *disztribuál* $\cup$ *fölött.*

Biz. $\operatorname{Mod}(\operatorname{Th}(X))$ monotonitása miatt $\operatorname{Mod}(\operatorname{Th}(M_1)) \cup \operatorname{Mod}(\operatorname{Th}(M_2)) \subseteq \operatorname{Mod}(\operatorname{Th}(M_1 \cup M_2))$. A fordított irányú tartalmazás is igaz, mert ha $\mathcal{M} \notin \operatorname{Mod}(\operatorname{Th}(M_1)) \cup \operatorname{Mod}(\operatorname{Th}(M_2))$, akkor vannak olyan φ_1, φ_2, M_1-ben ill. M_2-ben igaz formulák, amikre $\mathcal{M} \not\models \varphi_1 \vee \varphi_2$. De akkor $\mathcal{M} \notin \operatorname{Mod}(\operatorname{Th}(M_1 \cup M_2))$, hiszen $M_1 \cup M_2 \models \varphi_1 \vee \varphi_2$. □

1.6. Normálformák

1.42. Definíció. Egy formula

- *literális* ha atomi vagy atomi negáltja;
- *diszjunktív normálforma* (DNF) ha literálisok konjunkcióinak diszjunkciója, azaz ilyen alakú: $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} l_{ij}$, ahol l_{ij}-k literálisok;
- *konjunktív normálforma* (CNF) ha literálisok diszjunkcióinak konjunkciója ($\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{ij}$, ahol l_{ij}-k literálisok).

1.43. *Megjegyzés.* DNF kielégíthetősége gyorsan eldönthető, mert pontosan akkor kielégíthető, ha az egyik konjunkció kielégíthető, és utóbbi pontosan akkor áll fent, ha nem szerepel benne ugyanaz a kijelentésváltozó ellenkező előjellel.

Hasonlóan: CNF érvényessége gyorsan eldönthető, mert pontosan akkor érvényes, ha minden benne szereplő diszjunkció érvényes, és egy ilyen pontosan érvényes, ha szerepel benne ugyanaz a kijelentésváltozó ellenkező előjellel.

1.44. Tétel (DNF, CNF)**.** *Minden φ formulához létezik vele ekvivalens $\varphi^{\vee}$ és $\varphi^{\wedge}$ DNF ill. CNF amik legfeljebb a φ-ben előforduló atomi formulákat tartalmazzák.*

Biz. (DNF) Legyen M φ igazságtáblázata azon sorainak halmaza, melyek φ-t igazra értékelik (azaz ahol az utolsó oszlopban 1 áll), és legyen $\varphi^{\vee} = \bigvee_{\mathcal{M} \in M} \varphi_{\mathcal{M}}$, ahol

$$\varphi_{\mathcal{M}} = \bigwedge \{p : \mathcal{M}(p) = 1\} \wedge \bigwedge \{\neg p : \mathcal{M}(p) = 0\}$$

minden $\mathcal{M} \in M$-re.

Akkor $\varphi_{\mathcal{M}}$ definíciója miatt

$$(1) \qquad \mathcal{M} \models \varphi_{\mathcal{M}'} \iff \mathcal{M}' = \mathcal{M} \quad \text{minden } \mathcal{M} \text{ modellre és } \mathcal{M}' \in M\text{-re}$$

(ahol, ahogyan a bizonyítás hátralevő részében is, két modell egyenlősége úgy értendő, hogy φ változóin ugyanazt veszik fel) és ebből már következik $\varphi \equiv \varphi^{\vee}$, mert minden $\mathcal{M}$ modellre

$$\begin{aligned} \mathcal{M} \models \varphi^{\vee} \iff & (\exists \mathcal{M}' \in M)\mathcal{M} \models \varphi_{\mathcal{M}'} \\ & \iff (\exists \mathcal{M}' \in M)\mathcal{M} = \mathcal{M}' \iff \mathcal{M} \in M \iff \mathcal{M} \models \varphi \end{aligned}$$

ahol a második ekvivalencia (1) miatt igaz, az utolsó pedig M definíciója és 1.18 miatt.

(CNF) Már tudjuk, hogy $\neg\varphi \equiv \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} l_{ij}$ valamilyen n-re, $m_1, \ldots, m_n$-re és literálisok egy $\{l_{ij} \colon 0 < i \leq n, 0 < j \leq m_i\}$ halmazára. De akkor a De Morgan azonosságok (1.29(12)) miatt

$$\varphi \equiv \neg\neg\varphi \equiv \neg \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} l_{ij} \equiv \bigwedge_{i=1}^{n} \neg \bigwedge_{j=1}^{m_i} l_{ij} \equiv \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} \neg l_{ij} \equiv \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l'_{ij},$$

ahol $l'_{ij} = \neg l_{ij}$ ha l_{ij} atomi, és $l'_{ij} = p$ ha $l_{ij} = \neg p$.

Vagy a DNF-re vonatkozó bizonyítást „dualizáljuk":

Legyen M φ igazságtáblázata azon sorainak halmaza, melyek φ-t hamisra értékelik, és legyen $\varphi^{\wedge} = \bigwedge_{\mathcal{M} \in M} \varphi_{\mathcal{M}}$, ahol

$$\varphi_{\mathcal{M}} = \bigvee \{p : \mathcal{M}(p) = 0\} \vee \bigvee \{\neg p : \mathcal{M}(p) = 1\}$$

minden $\mathcal{M} \in M$-re.

Akkor $\varphi_{\mathcal{M}}$ definíciója miatt

$$(2) \qquad \mathcal{M} \not\models \varphi_{\mathcal{M}'} \iff \mathcal{M}' = \mathcal{M} \quad \text{minden } \mathcal{M} \text{ modellre és } \mathcal{M}' \in M\text{-re,}$$

és ebből már következik $\varphi \equiv \varphi^{\wedge}$, mert minden $\mathcal{M}$ modellre

$$\begin{aligned} \mathcal{M} \not\models \varphi^{\wedge} \iff (\exists \mathcal{M}' \in M) \mathcal{M} \not\models \varphi_{\mathcal{M}'} \\ \iff (\exists \mathcal{M}' \in M) \mathcal{M} = \mathcal{M}' \iff \mathcal{M} \in M \iff \mathcal{M} \not\models \varphi \end{aligned}$$

ahol a második ekvivalencia (2), az utolsó pedig M definíciója és 1.18 miatt igaz.

□

1.45. Példa. Adjunk meg egy, a $\varphi = (p \to q) \leftrightarrow (\neg p \to \neg q)$-val ekvivalens CNF-et és DNF-et.

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg p \to \neg q$	$(p \to q) \leftrightarrow (\neg p \to \neg q)$
0	0	1	1	1	1	1
0	1	1	1	0	0	0
1	0	0	0	1	1	0
1	1	1	0	0	1	1

Tehát $\varphi^{\wedge} = (p \vee \neg q) \wedge (\neg p \vee q)$ és $\varphi^{\vee} = (\neg p \wedge \neg q) \vee (p \wedge q)$ jó lesz.

1.46. Példa. Adjunk meg egy, a $\varphi = \neg(p \wedge ((q \wedge r) \to s))$-vel ekvivalens DNF-et és CNF-et.

p	q	r	s	$q \wedge r$	$(q \wedge r) \to s$	$p \wedge ((q \wedge r) \to s)$	$\neg(p \wedge ((q \wedge r) \to s))$
0	0	0	0	0	1	0	1
0	0	0	1	0	1	0	1
0	0	1	0	0	1	0	1
0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	1
0	1	0	1	0	1	0	1
0	1	1	0	1	0	0	1
0	1	1	1	1	1	0	1
1	0	0	0	0	1	1	0
1	0	0	1	0	1	1	0
1	0	1	0	0	1	1	0
1	0	1	1	0	1	1	0
1	1	0	0	0	1	1	0
1	1	0	1	0	1	1	0
1	1	1	0	1	0	0	1
1	1	1	1	1	1	1	0

Tehát $\varphi^{\wedge} = (\neg p \vee\ q \vee r \vee s) \wedge (\neg p \vee\ q \vee r \vee \neg s) \wedge (\neg p \vee\ q \vee \neg r \vee s) \wedge (\neg p \vee\ q \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee r \vee s) \wedge (\neg p \vee \neg q \vee r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg r \vee \neg s) \equiv (\neg p \vee\ q \vee r) \wedge (\neg p \vee\ q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee \neg r \vee \neg s) \equiv (\neg p \vee\ q) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee \neg r \vee \neg s)$

Nem így szokás CNF-et csinálni, hanem kicsit szintaktikusabban: Adott φ amit CNF-é akarunk alakítani.

(1) A definiált konnektívumokat küszöböljük ki (úgy, hogy csak $\neg$, $\vee$, $\wedge$ maradjon).
(2) Amíg lehet, cseréljük ki a benne előforduló $\neg\neg\psi$, $\neg(\psi_1 \wedge \psi_2)$ és $\neg(\psi_1 \vee \psi_2)$ alakú részformulákat ψ, $\neg\psi_1 \vee \neg\psi_2$, ill. $\neg\psi_1 \wedge \neg\psi_2$-re.
(3) Amíg lehet, cseréljük ki a benne előforduló $\psi \vee (\chi_1 \wedge \chi_2)$ és $(\chi_1 \wedge \chi_2) \vee \psi$ alakú részformulákat $(\psi \vee \chi_1) \wedge (\psi \vee \chi_2)$ ill. $(\chi_1 \vee \psi) \wedge (\chi_2 \vee \psi)$-re.
(4) (Ezen a ponton már CNF, tehát abba is hagyhatnánk, de inkább) alkalmazzuk $\wedge$ és $\vee$ asszociativitását, kommutativitását és idempotenciáját.

Így az eredeti formulával ekvivalens formulát kapunk 1.29 és 1.31?? miatt.

1.47. Példa. A fenti példa CNF-re íly módon:

$$
\begin{aligned}
& (p \to q) \leftrightarrow (\neg p \to \neg q) && \text{def.} \\
\equiv & (\neg p \vee q) \leftrightarrow (\neg\neg p \vee \neg q) && \text{def.} \\
\equiv & [(\neg p \vee q) \to (\neg\neg p \vee \neg q)] \wedge [(\neg\neg p \vee \neg q) \to (\neg p \vee q)] && \text{def.} \\
\equiv & [\neg(\neg p \vee q) \vee (\underline{\neg\neg p} \vee \neg q)] \wedge [\neg(\underline{\neg\neg p} \vee \neg q) \vee (\neg p \vee q)] && \text{kettős tagadás} \\
\equiv & [\underline{\neg(\neg p \vee q)} \vee (p \vee \neg q)] \wedge [\underline{\neg(p \vee \neg q)} \vee (\neg p \vee q)] && \text{De Morgan} \\
\equiv & (\underline{\neg\neg p} \wedge \neg q) \vee (p \vee \neg q)[(\neg p \wedge \underline{\neg\neg q}) \vee (\neg p \vee q)] && \text{kettős tagadás} \\
\equiv & [(p \wedge \neg q) \vee (p \vee \neg q)] \wedge [(\neg p \wedge q) \vee (\neg p \vee q)] && \text{disztributivitás} \\
\equiv & [(p \vee (p \vee \neg q)) \wedge (\neg q \vee (p \vee \neg q))] \wedge [(\neg p \vee (\neg p \vee q)) \wedge (q \vee (\neg p \vee q))] && \text{asszoc., komm., idemp.} \\
\equiv & [(p \vee \neg q) \wedge (\neg q \vee p)] \wedge [(\neg p \vee q) \wedge (q \vee \neg p)] \equiv (p \vee \neg q) \wedge (\neg p \vee q). && \blacksquare
\end{aligned}
$$

1.48. Példa.

$$
\begin{aligned}
&\neg(p \wedge ((q \wedge r) \to s)) && \text{def.}\\
\equiv&\neg(p \wedge (\neg(q \wedge r) \vee s)) && \text{De Morgan}\\
\equiv&\neg p \vee \neg(\neg(q \wedge r) \vee s) && \text{De Morgan}\\
\equiv&\neg p \vee (\neg\neg(q \wedge r) \wedge \neg s) && \text{kettős tagadás}\\
\equiv&\neg p \vee ((q \wedge r) \wedge \neg s) && \text{disztributivitás}\\
\equiv&(\neg p \vee (q \wedge r)) \wedge (\neg p \vee \neg s) && \text{disztributivitás}\\
\equiv&((\neg p \vee q) \wedge (\neg p \vee r)) \wedge (\neg p \vee \neg s)
\end{aligned}
$$

1.49. Gyakorlat. Gyártsuk le igazságtáblázattal és a fenti módon is $(p \wedge q) \leftrightarrow (r \vee s)$ egy CNF-jét!

Mindjárt látni fogjuk, hogy más tanulsága is van a normálforma tételnek (pontosabban a bizonyításának).

1.7. Igazságfüggvények Amikor a kijelentéslogikát definiáltuk, miért pont éppen $\neg$-ot és $\wedge$-et vettük be logikai konnektívumoknak? Az világos (és nem túl érdekes), hogy $\neg$-ot és $\vee$-t is választhattuk volna (ld. a De Morgan azonosságot 1.29-ben). A kérdés az, hogy vajon ezzel a választással nem zártunk-e ki valamit. Avagy: új konnektívumok felvételével vajon erősebbé (kifejezőbbé) tehetnénk-e a kijelentéslogikát.

Nevezzük (n-argumentumu) *igazságfüggvény*eknek a $\{0,1\}^n \to \{0,1\}$ függvényeket. Az n-argumentumu f igazságfüggvényt *megvalósítja* a $p_1, \dots, p_n$ atomi formulákat tartalmazó φ formula, ha minden $s \in \{0,1\}^n$-re (vagyis n hosszú 0-1 sorozatra) igaz, hogy $\varphi^{\mathcal{M}} = f(s)$ ha $\mathcal{M}(p_i) = s_i$ minden $i \in \{1, \dots, n\}$-re; vagyis ha minden $\mathcal{M}$-re $\varphi^{\mathcal{M}} = f(p_1^{\mathcal{M}}, \dots, p_n^{\mathcal{M}})$.

Igazságfüggvényeket persze igazságtáblázattal kényelmes megadni. Az, hogy milyen igazságfüggvények valósíthatók meg, nyilván azon múlik, hogy milyen konnektívumok vannak a logikában. A normálforma tétel bizonyítása mutatja, hogy kijelentéslogikában minden igazságfüggvény megvalósítható. A tételben előállított DNF (vagy CNF) a $\neg$, $\wedge$ és $\vee$ konnektívumokat használta, de $\neg$, $\wedge$-ból definiálható $\neg$, $\vee$ és fordítva, tehát minden igazságfüggvényt megvalósít egy csak $\neg$ és $\wedge$-t vagy $\neg$ és $\vee$-t használó formula.

1.50. *Megjegyzés.* Azt, hogy kijelentéslogikában minden igazságfüggvényt megvalósít egy formula, másképp, a függvény változóinak számára vonatkozó indukcióval is be lehet látni. Az egyargumentumúakat: a konstans 0 és 1 függvényeket, a tagadást és az identitásfüggvényt megvalósítja $p \wedge \neg p$, $p \vee \neg p$, $\neg p$ ill. p. Tegyük fel, hogy igaz az állítás az n-változós függvényekre, f $n+1$-változós, és legyen $\varphi_i(p_1, \dots, p_n)$ az $f(s_1, \dots, s_n, i)$-t $(i = 0,\ 1)$ megvalósító formula. Akkor f-et megvalósítja a

$$(\varphi_0(p_1, \dots, p_n) \wedge \neg q) \vee (\varphi_1(p_1, \dots, p_n) \wedge q)$$

formula, mert ha $\mathcal{M}(q) = 0$, akkor

$$f(p_1^{\mathcal{M}}, \dots, p_n^{\mathcal{M}}, q^{\mathcal{M}}) = f(p_1^{\mathcal{M}}, \dots, p_n^{\mathcal{M}}, 0) = \varphi_0^{\mathcal{M}} = \varphi^{\mathcal{M}}$$

(ahol az utolsó előtti egyenlőség azért igaz, mert φ_0 megvalósítja $f(\dots, 0)$-t, az utolsó meg φ definíciója miatt), és hasonlóan, ha $\mathcal{M}(q) = 1$, akkor

$$f(p_1^{\mathcal{M}}, \dots, p_n^{\mathcal{M}}, q^{\mathcal{M}}) = f(p_1^{\mathcal{M}}, \dots, p_n^{\mathcal{M}}, 1) = \varphi_1^{\mathcal{M}} = \varphi^{\mathcal{M}}.$$

1.51. Gyakorlat. Ha $\Sigma \subseteq Form_\Pi$, Π véges, akkor van olyan $\varphi \in Form_\Pi$, amire $\mathrm{Mod}(\Sigma) = \mathrm{Mod}(\varphi)$.

Konnektívumok egy K halmazát nevezzük *bázis*nak ha minden igazságfüggvényt megvalósít egy csak K-beli konnektívumokat használó formula. Az imént láttuk, hogy $\{\neg, \wedge\}$ és $\{\neg, \vee\}$ bázisok. Vagyis a kijelentéslogika definíciójában nem egészen véletlenül szerepelt éppen $\{\neg, \wedge\}$.

1.52. Példák. Definiáljuk a $|$ és $||$ konnektívumok jelentését így: $\mathcal{M} \models \varphi|\psi$ pontosan akkor, ha $\mathcal{M} \not\models \varphi$ vagy $\mathcal{M} \not\models \psi$ (azaz pontosan akkor, ha $\mathcal{M} \not\models \varphi \wedge \psi$). $\mathcal{M} \models \varphi||\psi$ pontosan akkor, ha $\mathcal{M} \not\models \varphi$ és $\mathcal{M} \not\models \psi$ (azaz pontosan akkor, ha $\mathcal{M} \models \neg\varphi \wedge \neg\psi$). Ezekkel a definíciókkal $\{|\}$ és $\{||\}$ bázisok, mert

- $\neg\varphi \equiv \varphi|\varphi$ és $\varphi \wedge \psi \equiv \neg(\varphi|\psi) \equiv (\varphi|\psi)|(\varphi|\psi)$
- $\neg\varphi \equiv \varphi||\varphi$ és $\varphi \wedge \psi \equiv \neg\varphi||\neg\psi \equiv (\varphi||\varphi)||(\psi||\psi)$,

$\{\neg, \wedge\}$-ról meg már tudjuk, hogy bázis.

$\{\wedge, \to\}$ viszont nem bázis, mert $p \not\models \neg p$, de formulaindukcióval könnyű belátni, hogy minden, csak a p-t tartalmazó, $\wedge$-el és $\to$-val felépülő φ formulára $p \models \varphi$.

De például $\{\neg, \to\}$ bázis, mert $p \wedge q \equiv \neg(p \to \neg q)$.

1.8. Kompaktság

1.53. Lemma. *Tegyük fel, hogy a Γ formulahalmaz minden véges része kielégíthető, és legyen p egy kijelentésváltozó. Ha Γ-nak van olyan Δ véges részhalmaza, amire $\Delta \models p$, akkor $\Gamma \cup \{p\}$, ellenkező esetben $\Gamma \cup \{\neg p\}$ minden véges része kielégíthető.*

Biz. A második eset triviális, hiszen $\Delta \not\models p$ éppen azt jelenti, hogy $\Delta \cup \{\neg p\}$ kielégíthető.

De az első eset sem probléma, mert ha Γ valamilyen Δ' véges részére $\Delta' \cup \{p\}$ kielégíthetetlen, akkor $\Delta' \models \neg p$, amiből $\Delta \cup \Delta'$ (ahol Δ Γ-nak az a véges része, amire $\Delta \models p$) Γ kielégíthetetlen véges része. □

1.54. Tétel. *Ha a Σ formulahalmaz minden véges része kielégíthető, akkor Σ kielégíthető.*

Ez nagyon nem magától értetődő. Végtelen sok feltétel szimultán kielégítésében általában nem segít, hogy közülük bármely véges sokat egyszerre ki tudunk. Pl. ha minden n-re C_n-et csak $(0, 1/n)$-beli valós számok elégítik ki, akkor véges sok C_n kielégíthető egyszerre, de az összes nem, mert $\cap_{n\in\mathbb{N}}(0, 1/n) = \emptyset$.

Biz. Atomi és negált atomi formulák olyan $\varphi_o, \dots, \varphi_i, \dots$ sorozatát fogjuk definiálni indukcióval, amire igaz, hogy minden $n \in \mathbb{N}$-re

(1) $\varphi_i \in \{\, p_i, \neg p_i \}$, és
(2) $\Sigma \cup \{\, \varphi_i : i < n \,\}$ minden véges része kielégíthető.

Ezzel kész is leszünk, mert legyen $\mathcal{M}$ az az egyetlen modell, amire $\mathcal{M} \models \{\, \varphi_n : n \in \mathbb{N} \,\}$. Akkor minden $\sigma \in \Sigma$-ra $\mathcal{M} \models \sigma$ a következő miatt. Legyen n olyan, hogy csak annál kisebb indexű kijelentésváltozók fordulnak elő σ-ban. Akkor $\{\, \varphi_i : i < n \,\} \cup \{\, \sigma \,\}$ véges része $\Sigma \cup \{\, \varphi_i : i < n \,\}$-nak, tehát kielégíthető; mondjuk $\mathcal{N}$ egy modellje. De akkor $\mathcal{N} \restriction \{p_0, \dots p_{n-1}\} = \mathcal{M} \restriction \{p_0, \dots p_{n-1}\}$, és σ-ban nincs más kijelentésváltozó, tehát 1.18 miatt $\mathcal{M} \models \sigma$.

φ_0 legyen p_0 vagy $\neg p_0$, annak megfelelően, hogy mit ad a (feltevés miatt alkalmazható) lemma Σ-ra. Az így definiált φ_0-ra a lemma miatt igaz az indukciós feltevés.

Tegyük fel, hogy $\varphi_0, \dots, \varphi_{n-1}$-re igaz az indukciós feltevés, és φ_n legyen p_n vagy $\neg p_n$, annak megfelelően, hogy mit ad a ((2) miatt alkalmazható) lemma $\Sigma \cup \{\, \varphi_i : i < n \,\}$-re és p_n-re. □

1.55. Következmény. *Ha $\Sigma \models \varphi$, akkor Σ-nak van olyan Δ véges része, amire $\Delta \models \varphi$.*

Biz. $\Sigma \models \varphi$ iff $\Sigma \cup \{\neg\varphi\}$ kielégíthetetlen iff Σ-nak van olyan Δ véges része, amire $\Delta \cup \{\neg\varphi\}$ kielégíthetetlen iff Σ-nak van olyan Δ véges része, amire $\Delta \models \varphi$. □

1.8.1. Kompaktság egy alkalmazása A $G = \langle V, E \rangle$ gráf egy színezése k színnel olyan $f : V \to \{1, \dots, k\}$ függvény, amire $f(v) \neq f(w)$, ha $\langle v, w \rangle \in E$. G gráfra legyen $\Pi_G = \{p_{vi} \colon v \in V(G) \text{ és } 1 \leq i \leq k\}$, és álljon $\Sigma(G) \subseteq Form_{\Pi_G}$ a következő formulákból:

- $p_{v1} \vee \ldots \vee p_{vk}$ minden $v \in V$-re („minden csúcsnak van színe")
- $\neg(p_{vi} \wedge p_{vj})$ minden $v \in V$-re és $1 \leq i < j \leq k$-ra („minden csúcsnak legfeljebb egy színe van")
- $\neg(p_{vi} \wedge p_{wi})$ minden $\langle v, w \rangle \in E$-re és $1 \leq i \leq k$-ra („szomszédos csúcsok különböző színűek")

1.56. Állítás. *G pontosan akkor színezhető ki k színnel, ha $\Sigma(G)$ kielégíthető.*

Biz. Az $\mathcal{M}(p_{vi}) = 1 \iff f(v) = i$ ekvivalenciát ($v \in V$, $1 \leq i \leq k$) kell használni, az egyik irányban egy $\Sigma(G)$-t kielégítő $\mathcal{M}$ modell, a másik irányban f definíciójaként.

Azaz: ha G kiszínezhető, akkor az így definiált modellben igaz $\Sigma(G)$; az első adag formula azért, mert minden csúcsnak van színe, a második azért, mert minden csúcsnak legfeljebb egy színe van, a harmadik meg mert szomszédos csúcsoknak különbözik a színük.

Fordítva: ha $\mathcal{M} \models \Sigma(G)$, akkor az első adag formula $\mathcal{M}$-beli igazsága miatt f értelmes V-n, a második miatt függvény, a harmadik miatt pedig színezés (szomszédos csúcsokhoz különböző színeket rendel). □

1.57. Következmény. *Ha egy gráf minden véges részgráfja kiszínezhető k színnel, akkor az egész gráf is.*

Biz. Legyen G a kiszínezendő gráf. Az előző állítás miatt $\Sigma(G)$, a kompaktsági tétel szerint tehát $\Sigma(G)$ minden véges részhalmazának kielégíthetőségét elegendő megmutatni. Ehhez azt kell meggondolni, hogy ha G minden véges részgráfja kiszínezhető k színnel, akkor $\Sigma(G)$ minden véges részhalmaza kielégíthető. (Ez azért nem értetődik magától, mert $\Sigma(G)$-nek nem minden véges részhalmaza $= \Sigma(H)$ G valamely véges H részgráfjára.) De ez igaz, mert ha $\Delta \subseteq \Sigma(G)$ véges, akkor G-nek van olyan véges H részgráfja, amire $\Delta \subseteq \Sigma(H) (\subseteq \Sigma(G))$: választhatjuk H-t G azon feszített részgráfjának, amelynek csúcsai $\{v \in V(G) \colon p_{vi} \text{ előfordul } \Delta\text{-ban}\}$. □

1.9. Horn formulák DNF kielégíthetőségét könnyű eldönteni: $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} l_{ij}$ kielégíthető pontosan akkor, ha van olyan $1 \leq i \leq n$, hogy $\bigwedge_{j=1}^{m_i} l_{ij}$ kielégíthető. De literálisok konjunkciója nyilván pontosan akkor elégíthető ki, ha nem szerepel köztük két ellentétes (azaz p és $\neg p$).

Duálisan: CNF-ek érvényességét könnyű eldönteni: $\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{ij}$ pontosan akkor érvényes, ha minden $1 \leq i \leq n$-re $\bigvee_{j=1}^{m_i} l_{ij}$ érvényes. És literálisok diszjunkciója pontosan akkor érvényes, ha szerepel köztük két ellentétes (azaz p és $\neg p$).

CNF-ek kielégíthetőségére viszont nem ismerünk gyors módszert: az igazságtáblázatos eljárás például a formulában előforduló atomi formulák számában exponenciális. De van egy fontos részhalmaza a CNF-eknek, amire létezik lineáris lineáris időben futó, a kielégíthetőséget eldöntő algoritmus.

1.58. Definíció. Egy CNF *Horn-formula*, ha minden diszjunkcióban legfeljebb egy pozitív literális (azaz kijelentésváltozó) fordul elő.

1.59. Példa. Példa Horn formulára: $(p \vee \neg q) \wedge (\neg r \vee \neg p \vee s) \wedge (\neg p \vee \neg q) \wedge s \wedge \neg t$.

Érdemes a Horn-formulákban szereplő diszjunkciókat „implikációs” alakba írni a következő ekvivalenciákat használva (annak megfelelően, hogy negatív és pozitív, csak negatív, ill. csak pozitív literális szerepel az diszjunkcióban):

$$\neg p_1 \vee \cdots \vee \neg p_n \vee q \equiv \bigwedge_{i=1}^{n} p_i \to q \qquad \neg p_1 \vee \cdots \vee \neg p_n \equiv \bigwedge_{i=1}^{n} p_i \to \bot \qquad p \equiv \top \to p.$$

(Az így kapott részformulákat jobb híján továbbra is diszjunkcióknak fogjuk hívni.) Az előbbi példából így $(q \to p) \wedge (p \wedge r \to s) \wedge (p \wedge q \to \bot) \wedge (\top \to s) \wedge (t \to \bot)$ lesz.

Íme az algoritmus, ami lineáris időben eldönti egy Horn formuláról, hogy kielégíthető-e.

(1) Jelöljük meg az összes olyan p kijelentésváltozót, amire $\top \to p$ az egyik diszjunkció.
(2) Amíg van olyan $\bigwedge_{i=1}^{n} p_i \to q$ vagy $\bigwedge_{i=1}^{n} p_i \to \bot$ diszjunkció, hogy $p_1, \ldots, p_n$ már meg van jelölve de q nincs megjelölve (a) az első esetben jelöljük meg q-t (b) a második esetben legyen KIELÉGÍTHETETLEN a kimenet, és álljunk meg.
(3) Legyen KIELÉGÍTHETŐ a kimenet, és álljunk meg.

1.60. Tétel. *Ez az algoritmus korrekt, és az atomi formulák számában lineáris idő alatt fut.*

Biz. A linearitás triviális, mert minden lépésben megjelölünk egy jelöletlen atomi formulát. Azt kéne tehát belátni, hogy minden φ formulára

$$\text{az algoritmus kielégíthetőnek nyilvánítja } \varphi\text{-t} \iff \varphi \text{ kielégíthető.}$$

($\Rightarrow$) Definiáljuk az $\mathcal{M}$ modellt így: legyen $\mathcal{M}(p) = 1$ csakkor ha az algoritmus megjelölte p-t. Azt állítjuk, hogy $\mathcal{M} \models \varphi$. Ehhez persze elég azt belátni, hogy mindegyik diszjunkció igaz $\mathcal{M}$-ben. Legyen ψ az egyik diszjunkció.

- Ha $\psi = \top \to p$, akkor az algoritmus megjelölte p-t (az első fázisban), tehát $\mathcal{M}(p) = 1$, következésképp $\mathcal{M} \models \top \to p$.
- Ha $\psi = \bigwedge_{i=1}^{n} p_i \to q$, akkor az algoritmus vagy megjelölte az összes p_i-t, de akkor a második fázisban q-t is, tehát $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i \to q$, vagy valamelyik p_i-t nem jelölte meg, és akkor $\mathcal{M}(p_i) = 0$, tehát $\mathcal{M} \not\models \bigwedge_{i=1}^{n} p_i$, következésképp $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i \to q$.
- Ha $\psi = \bigwedge_{i=1}^{n} p_i \to \bot$, akkor valamelyik p_i-t nem jelölte meg az algoritmus (különben a második fázisban szólt volna, hogy φ KIELÉGÍTHETETLEN), tehát, mint az előbb, $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i \to q$ mert $\mathcal{M} \not\models \bigwedge_{i=1}^{n} p_i$.

($\Leftarrow$) Legyen $\mathcal{M} \models \varphi$. Elég belátni, hogy

$$(\dagger) \qquad \text{ha az algoritmus megjelöli } p\text{-t, akkor } \mathcal{M} \models p$$

mert tegyük fel, hogy az algoritmus KIELÉGÍTHETETLENnek nyilvánítja φ-t; akkor van olyan $\bigwedge_{i=1}^{n} p_i \to \bot$ diszjunkció, hogy megjelölte a p_i-ket $(1 \leq i \leq n)$; de akkor $(\dagger)$ miatt $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i$, következésképp $\mathcal{M} \not\models \bigwedge_{i=1}^{n} p_i \to \bot$, tehát $\mathcal{M} \not\models \varphi$, ami ellentmondás.

$(\dagger)$ bizonyítása: Ha az algoritmus az első fázisban jelölte meg p-t, akkor $\top \to p$ az egyik diszjunkció, tehát $\mathcal{M} \models \top \to p$, tehát $\mathcal{M} \models p$.

Ha a második fázisban jelöli meg p-t, akkor van olyan $\bigwedge_{i=1}^{n} p_i \to p$ diszjunkció, hogy p_i-ket $(1 \leq i \leq n)$ már korábban megjelölte. Használni fogjuk, hogy $\mathcal{M} \models \varphi$ miatt $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i \to p$. Mondjuk indukció arra, hogy a ciklus hányadik végrehajtásánál jelöli p-t. Ha az első, akkor

p_i-ket az első fázisban jelölte meg, tehát $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i$ és így $\mathcal{M} \models p$. Ha nem a ciklus első végrehajtásánál jelöli meg p-t, akkor minden i-re p_i-t vagy az első fázisban jelölte meg (és akkor azért $\mathcal{M} \models p_i$), vagy a második fázisban, de a ciklus egy korábbi végrehajtásában, és akkor az indukciós feltevés miatt $\mathcal{M} \models p_i$. Tehát $\mathcal{M} \models \bigwedge_{i=1}^{n} p_i$ és így $\mathcal{M} \models p$. □

1.61. Következmény. *Ha egy Horn-formula nem tartalmaz csak negatív literálisokból álló diszjunkciót ($\bigwedge_{i=1}^{n} p_i \to \bot$), akkor kielégíthető. Ha egy Horn-formula nem tartalmaz egyetlen pozitív literálisból álló diszjunkciót ($\top \to p$), akkor kielégíthető.*

Biz. Az első esetben sosem lépünk rá a ciklusban KIELÉGÍTHETETLEN-t adó ágra, a második esetben pedig egyáltalán be sem kerülünk a ciklusba. □

1.62. Példák. 1. A fenti példa $(q \to p) \wedge (p \wedge r \to s) \wedge (p \wedge q \to \bot) \wedge (\top \to s) \wedge (t \to \bot)$ kielégíthető: Az első fázisban megjelöljük s-et. A másodikba viszont bele sem kerülünk (mert csak s van megjelölve, és nincs $s \to p$ vagy $s \to \bot$ diszjunkció).

2. $(\neg p \vee \neg q \vee \neg s) \wedge \neg t \wedge (\neg r \vee p) \wedge r \wedge q \wedge (\neg u \vee s) \wedge u$, azaz

$$(p \wedge q \wedge s \to \bot) \wedge (t \to \bot) \wedge (r \to p) \wedge (\top \to r) \wedge (\top \to q) \wedge (u \to s) \wedge (\top \to u)$$

implikációs alakba átírva.

Itt az első fázisban megjelöljük r, q, u-t. Második fázisban először megjelöljük p, s-t, másodszor viszont kijön, hogy KIELÉGÍTHETETLEN, mert $p \wedge q \wedge s \to \bot$ az egyik diszjunkció, és p, q, s meg vannak jelölve.

2. Propozicionális logika bizonyításelmélete

Eddig az a kérdés, hogy formulák valamely halmazából következik-e egy formula, halmazelméleti terminusokban volt megfogalmazva (hiszen a kielégíthetőség egy modell létezését jelenti). Ez nem probléma a kijelentéslogika esetében, de bonyolultabb logikákban kívánatos a „következmény” fogalmának szintaktikusabb, pl. számítógéppel jobban kezelhető megfogalmazása. Az ilyet nevezik egy logika bizonyításelméletének. Ez rendszerint valami kalkulusból áll, ami formulahalmazok következményeit hivatott levezetni valamilyen mechanikus módon. Ez különösen fontos olyan logikák esetében, ahol az érvényes formulák halmaza nem eldönthető.

Az egyik legegyszerűbb kalkulus a következő.

2.1. Hilbert típusú kalkulus kijelentéslogikára

2.1. Definíció (Logikai axiómák). (A1) $\varphi \to (\psi \to \varphi)$
(A2) $[\varphi \to (\psi \to \chi)] \to [(\varphi \to \psi) \to (\varphi \to \chi)]$
(A3) $(\neg\varphi \to \neg\psi) \to [(\neg\varphi \to \psi) \to \varphi]$

Könnyű látni, hogy a logikai axiómák érvényesek.

2.2. Definíció (Levezetés). Legyen $\Sigma \subseteq Form$. A $\varphi_1, \dots \varphi_n$ formulasorozat egy (n-hosszú) levezetés (bizonyítás) Σ-ból, ha minden $1 \leq k \leq n$-re teljesül az alábbi feltételek valamelyike:

- φ_k valamelyik logikai axióma instanciája
- $\varphi_k \in \Sigma$
- van olyan $1 \leq i, j < k$, hogy $\varphi_i = \varphi_j \to \varphi_k$ (ebben az esetben azt mondjuk, hogy φ_k leválasztással (avagy modus ponens-sel) keletkezett φ_j-ből és $\varphi_j \to \varphi_k$-ból).

Ha a tételek nem is lennének eldönthetők (mint ahogy a logikák többségében nem azok), a bizonyítások eldönthetők. Ezért van az, hogy azon, hogy elfogadható-e egy bizonyítás, nem szokás összeveszni.

2.3. Definíció (Levezethetőség)**.** Legyen $\Sigma \cup \{\varphi\} \subseteq Form$.

- φ levezethető (bizonyítható) Σ-ból, ha van olyan levezetés Σ-ból, aminek φ az utolsó formulája. Jelölés: $\Sigma \vdash \varphi$.
- φ logikai tétel (vagy: levezethető), ha $\emptyset \vdash \varphi$. Jelölés: $\vdash \varphi$.

2.4. Lemma. *Legyen $\Sigma \subseteq Form$. A Σ-ból levezethető formulák halmaza a legszűkebb, az axiómákat és Σ-t tartalmazó olyan Δ formulahalmaz, amire igaz, hogy ha $\varphi \to \psi, \varphi \in \Delta$, akkor $\psi \in \Delta$.*

2.5. Lemma. *Legyen $\Gamma \cup \Delta \cup \{\varphi, \psi\} \subseteq Form$.*

(1) *Ha $\varphi \in \Gamma$, akkor $\Gamma \vdash \varphi$.*
(2) *(monotonitás) Ha $\Gamma \vdash \varphi$ és $\Gamma \subseteq \Delta$, akkor $\Delta \vdash \varphi$.*
(3) *(tranzitivitás) Ha $\Gamma \vdash \psi$ minden $\psi \in \Delta$-ra és $\Delta \vdash \varphi$, akkor $\Gamma \vdash \varphi$.*
(4) *(kompaktság) Ha $\Gamma \vdash \varphi$, akkor Γ-nak van olyan véges Γ' része, amire $\Gamma' \vdash \varphi$.*

Az utolsó pont, amiről majd kiderül, hogy ekvivalens 1.54-el, ritka példa arra, hogy valamit egyszerűbb bizonyítani $\vdash$-re mint $\models$-re.

2.6. Példa. $\vdash \varphi \to \varphi$

(1)	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	(A1)
(2)	$[\varphi \to ((\varphi \to \varphi) \to \varphi)] \to [(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)]$	(A2)
(3)	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	MP 1,2
(4)	$\varphi \to (\varphi \to \varphi)$	(A1)
(5)	$\varphi \to \varphi$	MP 3,4

2.7. Példa. $\vdash (\varphi \to \bot) \to \neg\varphi$

2.8. Példa. $\{\varphi, \neg\varphi\} \vdash \bot$

2.9. Definíció. A Σ formulahalmaz konzisztens, ha $\Sigma \nvdash \bot$; inkonzisztens, ha nem konzisztens.

Egyszerű példák inkonzisztens mondathalmazokra $\{\bot\}$ (2.5(1) miatt) és $\{p, \neg p\}$ ((2.8) miatt).

2.10. Tétel (Helyesség)**.** *$\vdash$ helyes $\models$-re nézve, azaz $\Sigma \vdash \varphi \implies \Sigma \models \varphi$.*

Ez a minimum, amit egy kalkulustól elvárunk (tehát azt, hogy ne vezessen le olyat, ami nem következik (szemantikusan)).

Biz. Tegyük fel, hogy $\mathcal{M} \models \Sigma$, kéne: $\mathcal{M} \models \varphi$. Indukció φ levezetésének hosszára. Ha van 1-hosszú levezetése, akkor φ logikai axióma (és akkor minden modellben igaz), vagy $\varphi \in \Sigma$ (és akkor triviális, hogy $\mathcal{M} \models \varphi$). Tegyük fel, hogy a Σ-ból legfeljebb n lépésben levezetett formulák igazak $\mathcal{M}$-ben, és φ-nek van $n+1$-hosszú $\varphi_1, \ldots, \varphi_n, \varphi_{n+1} = \varphi$ levezetése. Ha φ logikai axióma vagy $\in \Sigma$, akkor mint az előbb. Ha nem, akkor van $1 \leq i,\ j < n+1$, hogy $\varphi_i = \varphi_j \to \varphi$; az indukciós feltevés miatt $\mathcal{M} \models \varphi_j \to \varphi$ és $\mathcal{M} \models \varphi_j$, tehát $\mathcal{M} \models \varphi$. $\square$

2.11. Tétel (Dedukciótétel)**.** $\Sigma \cup \{ \varphi \} \vdash \psi \implies \Sigma \vdash \varphi \to \psi$.

Biz. Indukció ψ levezetésének hosszára. Legyen ψ egy levezetése $\Sigma \cup \{ \varphi \}$-ből $\varphi_1, \dots \varphi_n = \psi$ és tegyük fel, hogy a rövidebb levezetésekre igaz a tétel.

Ha ψ axióma: $\Sigma \vdash \psi \to (\varphi \to \psi)$ (A1) és $\Sigma \vdash \psi$ 2.4 miatt, amikből MP-vel $\Sigma \vdash \varphi \to \psi$.

Ha $\psi \in \Sigma$: az előző esethez hasonlóan.

Ha $\psi = \varphi$: 2.6 miatt $\vdash \varphi \to \psi$, és így 2.5.2 miatt $\Sigma \vdash \varphi \to \psi$.

Végül ha $\Sigma \cup \{ \varphi \} \vdash \sigma \to \psi$ és $\Sigma \cup \{ \varphi \} \vdash \sigma$, akkor az indukciós feltevés miatt $\Sigma \vdash \varphi \to (\sigma \to \psi)$ és $\Sigma \vdash \varphi \to \sigma$. De $\Sigma \vdash \varphi \to (\sigma \to \psi) \to [(\varphi \to \sigma) \to (\varphi \to \psi)]$ (A2), és ezekből MP kétszeri alkalmazásával kapjuk $\Sigma \vdash \varphi \to \psi$-t. □

2.12. Példa. $\{\varphi \to \psi, \psi \to \eta\} \vdash \varphi \to \eta$
A dedukciótétel miatt elég azt belátni, hogy $\{\varphi \to \psi, \psi \to \eta, \varphi\} \vdash \eta$.

(1)	$\varphi \to \psi$	(feltevés)
(2)	$\psi \to \eta$	(feltevés)
(3)	φ	(feltevés)
(4)	ψ	MP 1,3
(5)	η	MP 2,4

2.13. Példa. $\{\varphi \to (\psi \to \eta), \psi\} \vdash \varphi \to \eta$
A dedukciótétel miatt elég azt belátni, hogy $\{\varphi \to (\psi \to \eta), \psi, \varphi\} \vdash \eta$.

(1)	$\varphi \to (\psi \to \eta)$	(feltevés)
(2)	φ	(feltevés)
(3)	$\psi \to \eta$	MP 1,2
(4)	ψ	(feltevés)
(5)	η	MP 3,4

2.14. Példa. $\vdash \neg\neg\varphi \to \varphi$

(1)	$(\neg\varphi \to \neg\neg\varphi) \to [(\neg\varphi \to \neg\varphi) \to \varphi]$	(A3)
(2)	$\neg\varphi \to \neg\varphi$	(2.6)
(3)	$(\neg\varphi \to \neg\neg\varphi) \to \varphi$	2.13, 1,2
(4)	$\neg\neg\varphi \to (\neg\varphi \to \neg\neg\varphi)$	(A1)
(5)	$\neg\neg\varphi \to \varphi$	2.12, 3,4, 2.5(3)

2.15. Lemma. (1) $\Sigma \vdash \varphi \iff \Sigma \cup \{\neg\varphi\}$ *inkonzisztens.*
(2) *Ha* $\Sigma \cup \{\varphi\}$ *és* $\Sigma \cup \{\neg\varphi\}$ *inkonzisztens, akkor* Σ *is az.*

Biz. (1)($\Rightarrow$) 2.5(2) miatt $\Sigma \cup \{\neg\varphi\} \vdash \varphi$ és 2.5(1) miatt $\Sigma \cup \{\neg\varphi\} \vdash \neg\varphi$, ezért 2.8 és 2.5(3) miatt $\Sigma \cup \{\neg\varphi\} \vdash \bot$.

($\Leftarrow$) A dedukciótétel miatt $\Sigma \cup \{\neg\varphi\} \vdash \bot \implies \Sigma \vdash \neg\varphi \to \bot$, amiből $\Sigma \vdash \neg\neg\varphi$ 2.7 és 2.5.3 miatt, amiből meg $\Sigma \vdash \varphi$ 2.14 és 2.5.3 miatt.

(2) $\Sigma \vdash \neg\varphi, \varphi$ (1) miatt, amiből 2.8 és 2.5.3 miatt $\Sigma \vdash \bot$. □

2.16. Tétel (Teljesség)**.** $\vdash$ *teljes* $\models$*-re nézve, azaz* $\Sigma \models \varphi \implies \Sigma \vdash \varphi$.

A teljesség bizonyítása már nem szimpla formulaindukció; viszonylag nehéz, és főleg elég hosszadalmas.

2.17. Következmény. *Σ konzisztens pontosan akkor, ha van modellje.*

Biz. Σ konzisztens csakkor ha $\Sigma \nvdash \bot$ csakkor ha $\Sigma \not\models \bot$ csakkor ha Σ-nak van modellje. $\square$

* * *

Visszatérve egy pillanatra az inkonzisztens formulahalmazokra: ezekkel az baj, hogy minden levezethető belőlük.

2.18. Állítás. *$\Sigma \subseteq Form_\Pi$ pontosan akkor inkonzisztens ha $\Sigma \vdash \varphi$ minden $\varphi \in Form_\Pi$-re.*

Az inkonzisztencia fogalmának „duálisa" a teljesség (mondathalmazé, nem kalkulusé).

2.19. Definíció. Legyen Π a legszűkebb halmaz, amire $\Sigma \subseteq Form_\Pi$. Akkor Σ teljes, ha $\Sigma \vdash \varphi$ vagy $\Sigma \vdash \neg\varphi$ minden $\varphi \in Form_\Pi$-re.

Például $\{\neg p\} \subseteq Form_{\{p\}}$ teljes, de $\{\neg p \vee q\} \subseteq Form_{\{p,q\}}$ nem. Az első 2.16 és azon egyszerű tény következménye, hogy minden $\varphi \in Form_{\{p\}}$-re, $\{\neg p\} \models \varphi$ pontosan akkor, ha $\mathcal{M} \models \varphi$, ahol $\mathcal{M}$ olyan modell, amelyre $\mathcal{M}(p) = 0$; a második pedig 2.10 következménye, mert könnyű látni, hogy $\{\neg p \vee q\} \not\models p$ és $\{\neg p \vee q\} \not\models \neg p$.

2.20. Gyakorlat. $\{p, q\}$ teljes.

2.21. Állítás. *Legyen Π a legszűkebb olyan halmaz, amire $\Sigma \subseteq Form_\Pi$. Akkor Σ pontosan akkor teljes, ha legfeljebb egy modellje van.*

Itt is, mint mindig, azonosnak tekintjük a Π-n megegyező modelleket.

Biz. 2.16 miatt végig $\models$-t írunk $\vdash$ helyett.
($\Rightarrow$) Σ teljessége miatt $\Sigma \models p$ vagy $\Sigma \models \neg p$ minden $p \in \Pi$-re. Ha mindkettő fennáll, akkor Σ-nak nincs modellje, mert abban p igaz és hamis is volna. Tehát feltehetjük, hogy pontosan az egyik áll fenn. Ha az első, akkor p igaz, ha a második, akkor p hamis Σ minden modelljében. Tehát Σ modelljei megegyeznek minden $p \in \Pi$-n.
($\Leftarrow$) Ha Σ-nak nincs modellje, akkor $\Sigma \models \varphi$ minden $\varphi \in Form_\Pi$-re, következésképp Σ teljes. Máskülönben legyen $\mathcal{M}$ a Σ egyetlen modellje; akkor $\Sigma \models \varphi$ csakkor, ha $\mathcal{M} \models \varphi$. És mivel egy modellben minden formula vagy a negációja igaz, $\Sigma \models \varphi$ vagy $\Sigma \models \neg\varphi$ minden $\varphi \in Form_\Pi$-re. $\square$

2.22. Állítás. *Ha Σ egy formulahalmaz, akkor $\Sigma^+ = \{\varphi : \Sigma \vdash \varphi\}$ levezetésre ($\vdash$-re) zárt, azaz $\Sigma^+ \vdash \varphi$-ből $\varphi \in \Sigma^+$ következik.*

Biz. 2.5(3) miatt $\{\varphi : \Sigma \vdash \varphi\} \vdash \psi$-ből $\Sigma \vdash \psi$ következik. $\square$

2.23. Állítás. *Legyen $\Sigma \subseteq Form_\Pi$ zárt levezetésre, és legyen $\Sigma' = \{\neg\varphi : \Sigma \vdash \varphi\} = \{\neg\varphi : \varphi \in \Sigma\}$. Akkor*

(1) *Σ pontosan akkor teljes, ha $\Sigma \cup \Sigma' = Form_\Pi$*
(2) *Σ pontosan akkor konzisztens, ha $\Sigma \cap \Sigma' = \emptyset$.*

Biz. Az első igaz a teljesség definíciója miatt. A második ($\Leftarrow$) iránya 2.18 miatt igaz, a másik meg azért, mert ha $\varphi \in \Sigma \cap \Sigma'$, azaz ha $\{\varphi, \neg\varphi\} \subseteq \Sigma$, akkor $\Sigma \vdash \bot$ 2.8 és 2.5(3) (vagy 2.5(2)) miatt. $\square$

2.2. Rezolúció kijelentéslogikára

2.24. Definíció. Literálisok egy véges halmazát *clause*-nak hívják. Az üres clause jele: $\Box$. Az $\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{ij}$ CNF clause halmaza:

$$\{\{l_{11}, l_{12}, \dots, l_{1m_1}\}, \{l_{21}, l_{22}, \dots, l_{2m_2}\}, \dots, \{l_{n1}, l_{n2}, \dots, l_{nm_n}\}\}.$$

2.25. Példa. $(p \vee \neg q) \wedge (\neg p \vee q \vee q)$ clause halmaza $\{\{p, \neg q\}, \{\neg p, q\}\}$.

2.26. Állítás. *Ha két CNF-nek ugyanaz a clause halmaza, akkor ekvivalensek.*

Fordítva persze nem igaz, pl. $p \vee \neg p \equiv q \vee \neg q$ de a clause halmazaik $\{\{p, \neg p\}\} \neq \{\{q, \neg q\}\}$.

Biz. Definiáljuk clause-ok és clause halmazok jelentését egy modellben így: $\mathcal{M}$-ben igaz egy clause csakkor ha valamelyik eleme igaz, $\mathcal{M}$-ben igaz egy clause halmaz csakkor ha mindegyik eleme igaz. Ekkor $\mathcal{M} \models \bigvee_{j=1}^{m} l_j \iff \mathcal{M} \models \{l_1, \dots l_m\}$, ezért

$$\begin{aligned}\mathcal{M} \models \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{ij} &\iff \text{minden } 1 \leq i \leq n\text{-re} \quad \mathcal{M} \models \bigvee_{j=1}^{m_i} l_{ij} \\ &\iff \text{minden } 1 \leq i \leq n\text{-re} \quad \mathcal{M} \models \{l_{i1}, l_{i2}, \dots, l_{im_i}\} \\ &\iff \mathcal{M} \models \{\{l_{11}, l_{12}, \dots, l_{1m_1}\}, \{l_{21}, l_{22}, \dots, l_{2m_2}\}, \dots, \{l_{n1}, l_{n2}, \dots, l_{nm_n}\}\}\end{aligned}$$

és ebből már következik az állítás. $\Box$

2.27. Definíció (Rezolúció)**.** Legyen C és D két clause, $p \in C$ és $\neg p \in D$. C és D p szerinti *rezolvens*e $C \setminus \{p\} \cup D \setminus \{\neg p\}$.

2.28. Példa. $\{p, q, \neg r\}$ és $\{p, \neg q\}$ q szerinti rezolvense $\{p, \neg r\}$.

2.29. Állítás. *Ha E a C és D (valamilyen atomi formula szerinti) rezolvense, akkor $\{C, D\} \models E$.*

Biz. Mondjuk $p \in C$ és $\neg p \in D$, és $E = C \setminus \{p\} \cup D \setminus \{\neg p\}$ a C és D p-szerinti rezolvense, és legyen $\mathcal{M} \models \{C, D\}$. Ha $\mathcal{M}(p) = 0$, akkor $\mathcal{M} \models C \setminus \{p\}$ (mert $\mathcal{M} \models C$ de $\mathcal{M} \not\models p$), tehát $\mathcal{M} \models E$ mert $C \setminus \{p\} \subseteq E$. Ha pedig $\mathcal{M}(p) = 1$, akkor $\mathcal{M} \models D \setminus \{\neg p\}$ (mert $\mathcal{M} \models D$ de $\mathcal{M} \not\models \neg p$), tehát $\mathcal{M} \models E$ mert $D \setminus \{\neg p\} \subseteq E$. Tehát mindkét esetben $\mathcal{M} \models E$. $\Box$

2.30. *Megjegyzés.* A rezolúció következő enyhe variációja viszont már nem helyes: $p \in C$ és $\neg p \in D$, akkor C és D p szerinti rezolvens'-je $(C \cup D) \setminus \{p, \neg p\}$. Pl. ha $C = \{p\}$, $D = \{p, \neg p\}$, akkor $(C \cup D) \setminus \{p, \neg p\} = \Box$, de $\{C, D\} \not\models \Box$, mert $\{C, D\}$-nek van, $\Box$-nak viszont nincs modellje.

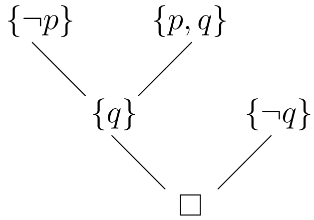
Nem lehet „felgyorsítani” a rezolúciót oly módon, hogy egyszerre két atomi formula szerint rezolválunk: pl. $C = \{p, q\}$, $D = \{\neg p, \neg q\}$-nak *nem* rezolvense $\Box$, és nem is következik belőle, hiszen $\{C, D\}$ kielégíthető.

2.31. Definíció. Az E clause egy rezolúciós levezetése a Σ clause-halmazból olyan véges T fa, amire igaz, hogy

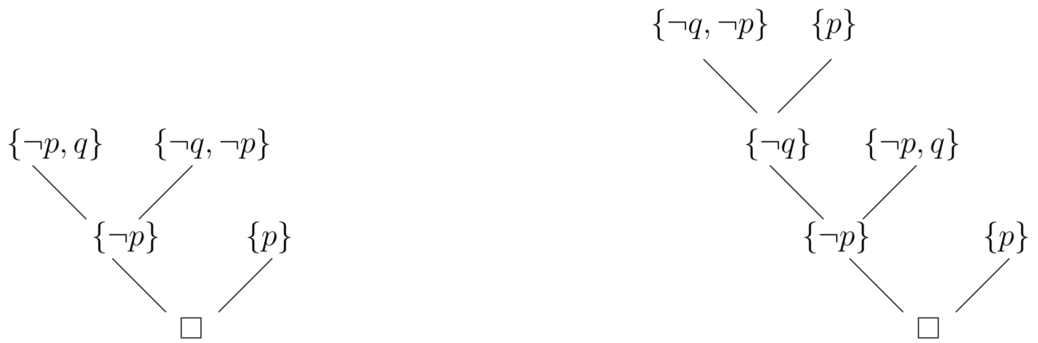
- T minden csúcsa egy clause
- E a T gyökere
- T minden levele Σ egy eleme
- T minden olyan D csúcsának ami nem levél, van két gyermeke aminek D a rezolvense.

(Ahelyett, hogy a csúcsok clause-ok, helyesebb lenne azt mondani, hogy minden csúcs egy clause-zal van címkézve. Máskülönben ui. nem használhatnánk fel kétszer ugyanazt a clause-t, mert ezzel a fa megszűnne fa lenni. Ld. az alábbi második példát!) A levezetés hossza a nem-levél csúcsok száma. Σ-ból levezethető E ($\Sigma \vdash_r E$) ha E-nek van rezolúciós levezetése Σ-ból. Σ *cáfolható* ha $\Sigma \vdash_r \Box$.

2.32. Példa. $\{\{\neg p\}, \{p, q\}, \{\neg q\}\}$ cáfolata (két lépésben):



2.33. Példa. $(p \to q) \wedge (q \to \neg p) \wedge p$, azaz $\{\{\neg p, q\}, \{\neg q, \neg p\}, \{p\}\}$ cáfolata két különböző módon:



2.34. Állítás (Helyesség)**.** *Ha Σ clause-halmaz, E egy clause, akkor $\Sigma \vdash_r E \implies \Sigma \models E$.*

Biz. Indukció a levezetés hosszára. Legyen $\mathcal{M}$ a Σ egy modellje. Ha E 0-lépésben levezethető Σ-ból, akkor $E \in \Sigma$, tehát $\mathcal{M} \models E$. Ha E $n > 0$ lépésben vezethető le, akkor egy ilyen levezetésben E két clause gyermeke, akik $n-1$ lépésben levezethetők (tehát igazak $\mathcal{M}$-ben), de akkor 2.29 miatt E igaz e két clause minden modelljében, speciel $\mathcal{M}$-ben is. $\Box$

2.35. Gyakorlat. $\vdash_r$ nem teljes.

2.36. Tétel. *A Σ clause-halmaz kielégíthetetlen akkor és csak akkor ha $\Sigma \vdash_r \Box$.*

Biz. ($\Leftarrow$) következik 2.34-ból, mert ha $\Sigma \vdash_r \Box$, akkor $\Sigma \models \Box$, de akkor Σ kielégíthetelen, hiszen $\Box$-nak nincs modellje.

($\Rightarrow$) Azt kéne belátni, hogy ha $\Sigma \nvdash_r \Box$, akkor Σ-nak van modellje. Feltehetjük, hogy Σ zárt $\vdash_r$-re (azaz, hogy minden E clause-ra, ha $\Sigma \vdash_r E$, akkor $E \in \Sigma$), mert ha nem, akkor egyszerűen bevesszük Σ-ba az összes belőle levezethető clause-t. (Így tényleg $\vdash_r$-re zárt clause-halmazt kapunk, mert ha $\Sigma \vdash_r A$ és $\Sigma \cup \{A\} \vdash_r B$, akkor $\Sigma \vdash_r B$.[2]) És persze ha ennek a kibővített halmaznak van modellje, akkor az eredetinek is.

[2] B-nek $\Sigma \cup \{A\}$-ból való levezetésében cseréljük ki az A-val címkézett leveleket A-nak Σ-ból való egy levezetésére.

$C \in \Sigma$-ra legyen $i(C) = \max\{\, i : p_i \in C$ vagy $\neg p_i \in C \,\}$ ($C \neq \Box$ miatt ez értelmes). Definiáljuk az $\mathcal{M}$ modellt így: Tegyük fel, hogy $\mathcal{M}(p_i)$ már definiálva van minden $i < j$-re. $\mathcal{M}(p_j) \stackrel{\text{def}}{=} 1$, kivéve ha $(\exists C \in \Sigma)(i(C) = j$ és $(\mathcal{M} \restriction \{p_0, \dots, p_{j-1}\}) \cup \{\langle\, p_j, 1\,\rangle\} \not\models C)$. (Ez értelmes, mert ha $i(C) = j$, akkor C-ben minden atomi formula indexe legfeljebb j.) Azt állítjuk, hogy $\mathcal{M} \models \Sigma$. Ehhez persze elég belátni, hogy

$$(\dagger) \qquad (\forall j \in \mathbb{N})(\forall C \in \Sigma)(i(C) \leq j \implies \mathcal{M} \models C)$$

Tegyük fel, hogy nem, és legyen j a legkisebb amire van olyan $C \in \Sigma$, hogy $i(C) \leq j$ de $\mathcal{M} \not\models C$. Akkor $i(C) = j$ (mert $i(C) < j$ ellentmond j minimalitásának). De akkor $\mathcal{M}$ definíciója miatt $\mathcal{M}(p_j)$ nem lehet 1.

$\mathcal{M}(p_j) = 0$ miatt viszont van $D \in \Sigma$, hogy $i(D) = j$ és $(\mathcal{M} \restriction \{p_0, \dots p_{j-1}\}) \cup \{\langle\, p_j, 1\,\rangle\} \not\models D$. Következésképp $p_j \notin D$ (mert akkor D igaz lenne minden olyan modellben, ami p_j-hez 1-et rendel) és így $\neg p_j \in D$, mert $i(D) = j$ miatt p_j és $\neg p_j$ valamelyike biztosan $\in D$. Hasonlóan: $\neg p_j \notin C$, mert különben $\mathcal{M}(p_j) = 0$ miatt $\mathcal{M} \models C$ lenne; de akkor $p_j \in C$, mert $i(C) = j$. Tehát C és D rezolválható p_j szerint, és a rezolvensnek sem p_j, sem $\neg p_j$ nem lesz eleme.

Legyen E a C és D p_j szerinti rezolvense. Σ zártsága miatt $E \in \Sigma$ (speciálisan E nem az $\Box$, és így $j > 0$) . $\mathcal{M} \not\models E$, mert csupa $C \setminus \{p_j\}$ ill. $D \setminus \{\neg p_j\}$-beli literálisok szerepelnek benne, amik viszont mind hamisak $\mathcal{M}$-ben (mert $\mathcal{M} \not\models C \setminus \{p_j\}$, sőt, $\mathcal{M} \not\models C$, C választása, és $\mathcal{M} \not\models D \setminus \{\neg p_j\}$, $(\mathcal{M} \restriction \{p_0, \dots p_{j-1}\}) \cup \{\langle\, p_j, 1\,\rangle\} \not\models D$ miatt.) Csakhogy $i(E) < j$, és ez ellentmond j minimalitásának. $\Box$

Azaz: a rezolúció nem teljes ugyan, de *cáfolat-teljes*, és ez a gyakorlatban elég, a következő következmény miatt.

2.37. Következmény. $\Sigma \models \varphi \iff \Sigma \cup \{\neg\varphi\} \vdash_r \Box$.

Persze $\Sigma \subseteq Form$-ra $\Sigma \vdash_r \Box$ úgy értendő, hogy $\cup\{\, \sigma^\wedge$ clause halmaza $: \sigma \in \Sigma \,\} \vdash_r \Box$.

Biz. $\Sigma \models \varphi \iff \Sigma \cup \{\neg\varphi\}$ kielégíthetetlen $\iff \Sigma \cup \{\neg\varphi\} \vdash_r \Box$. $\Box$

2.38. Következmény (Kompaktság)**.** *Egy formulahalmaz pontosan akkor elégíthető ki ha minden véges része kielégíthető.*

Biz. Elég persze clause-halmazokra belátni (miért?). Azokra meg triviális, mert ha egy clause halmaz kielégíthetetlen, akkor 2.36 miatt levezethető belőle $\Box$; de a levezetés egy véges fa, tehát csak véges sok levele van, azaz csak véges sok Σ-beli clause-t használ. Vagyis Σ-nak van olyan véges részhalmaza, amiből $\Box$ levezethető, vagyis ami 2.29 miatt kielégíthetetlen.

A másik irány (ha Σ kielégithető, akkor minden véges része is az) triviális. $\Box$

2.39. Definíció. Legyen Σ egy clause halmaz.

$$Res(\Sigma) \stackrel{\text{def}}{=} \Sigma \cup \{\, C : C \text{ két } \Sigma\text{-beli clause rezolvense} \,\}.$$

Továbbá $Res_0(\Sigma) \stackrel{\text{def}}{=} \Sigma$, $Res_{n+1}(\Sigma) \stackrel{\text{def}}{=} Res(Res_n(\Sigma))$ és $Res^*(\Sigma) = \cup_{n \in \mathbb{N}} Res_n$.

Vagyis $Res_k(\Sigma)$ a Σ-ból legfeljebb k lépésben levezethető clause-ok, $Res^*(\Sigma)$ pedig a Σ-ból levezethető összes clause-ok halmaza.

2.40. Állítás. *Ha Σ véges, akkor $Res_{k+1}(\Sigma) = Res_k(\Sigma)$ vmilyen $k \in \mathbb{N}$-re.*

Biz. Mivel Σ véges, csak véges sok atomi formula fordul elő benne. A rezolúció során nem keletkezik új literális (azaz minden rezolvensben legfeljebb ugyanazok a literálisok fordulnak elő, mint azokban a clause-okban, akiknek a rezolvense). De véges sok literálisból csak véges sok különböző clause állhat[3] , tehát $Res^*(\Sigma)$ véges. Ebből már következik az állítás, mert így $Res_0(\Sigma) \subseteq Res_1(\Sigma) \subseteq \cdots \subseteq Res_n(\Sigma) \subseteq \ldots$ nem lehet mind különböző. $\square$

2.41. Következmény. *Véges clause-halmaz kielégíthetősége eldönthető rezolúcióval.*

Biz. Ha egy Σ véges clause-halmaz kielégíthetetlen, akkor a teljességi tétel (2.36) miatt $\square \in Res_n(\Sigma)$ valamilyen n-re, ha pedig kielégíthető, akkor az előbbi állítás miatt $Res_n(\Sigma) = Res_{n+1}(\Sigma)$ valamilyen n-re. $\square$

3. Elsőrendű logika

Kijelentéslogikával meglepően messzire lehet jutni, de arra nem alkalmas, hogy *dolgok*ról és köztük fennálló relációkról beszéljen. A kijelentéslogika olyan bővítésére van szükségünk, ami alkalmas pl. annak kifejezésére, hogy több mint egy dolog van, vagy hogy egy reláció tranzitív; és még esetleg egy relációs adatbázisból való lekérdezés is leírható vele.

3.1. Szintaxis Propozicionális logikában csak kétféle szimbólum (atomi formulák és konnektívumok) szerepelt, és egyfajta kifejezés, avagy szintaktikai kategória (formulák). Elsőrendű logikában nemcsak állítások, hanem „dolgok” is szerepelnek (amikről állíthatunk mindenfélét), ennek megfelelően a formulák mellett még egy szintaktikai kategória van, a *term*eké, és az elsőrendű formulák és termek ötféle szimbólumból épülnek fel:

(1) végtelen sok változójel ($x, y, z, \ldots$ és ezek indexelt változatai); Var jelöli a változók halmazát
(2) logikai konnektívumok ($\wedge$, $\neg$, $\forall$ (univerzális kvantor, „minden”-nek olvasandó), $=$)
(3) relációjelek ($P, R, S, \ldots$ és ezek indexelt változatai)
(4) függvényjelek ($f, g, h, \ldots$ és ezek indexelt változatai)
(5) konstansjelek ($c, d, e, \ldots$ és ezek indexelt változatai)

Megtehetnénk, hogy az utolsó három kategóriában szereplő jeleket egyszer és mindenkorra rögzítjük (pl. feltesszük, hogy végtelen sok függvényjel van, és mindig csak azokat használjuk közülük, amikre éppen szükség van), de egyszerűbb ezeket paraméternek tekinteni, és azt mondani, hogy *elsőrendű nyelv* egy $\mathcal{L} = \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$ halmaz, ahol $\mathcal{R}$ relációjelek, $\mathcal{F}$ függvényjelek, $\mathcal{C}$ pedig konstansok páronként diszjunkt halmazai.[4] Feltesszük, hogy van egy ρ függvény, ami minden relációjelhez és függvényjelhez hozzárendel egy természetes számot, a relációjel vagy függvényjel *rang*ját (vagy *aritás*át) (Ha $\rho R = n$ ill. $\rho f = n$, akkor azt mondjuk, hogy R (f) n-argumentumú.)

Ha mást nem mondunk, mindig feltételezzük, hogy egy tetszőleges, de rögzített $\mathcal{L}$ nyelvről van szó.

3.1. Definíció (Elsőrendű termek)**.** Legyen $\mathcal{L} = \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$ egy elsőrendű nyelv. $Term_{\mathcal{L}}$ a legszűkebb T halmaz, amire

(1) $Var \subseteq T$
(2) $\mathcal{C} \subseteq T$

[3] a clause-ok *halmazok*!

[4] Már a propozicionális logikában is bevezethettünk volna propozicionális nyelveket (Π részhalmazait).

(3) ha $f \in \mathcal{F}$ és $t_1, \ldots, t_{\rho f} \in T$, akkor $f(t_1, \ldots, t_{\rho f}) \in T$.

3.2. Példa. Legyen $\mathcal{L}$ az a nyelv, amiben e az egyetlen konstansjel (vagyis $\mathcal{C} = \{e\}$), és a kétargumentumú $\cdot$ az egyetlen függvényjel (azaz $\mathcal{F} = \{\cdot\}$ és $\rho(\cdot) = 2$). Akkor $\cdot(y, \cdot(x, e)) \in Term_{\mathcal{L}}$. A szokásos, infix írásmódot használva ezt persze így írjuk: $y \cdot (x \cdot e)$ $\mathcal{L}$ mellesleg a csoportelmélet nyelve.

3.3. Állítás (Term-indukció). *Ha T olyan tulajdonság, hogy*

- *a változók és konstansjelek kielégítik T-t*
- *ha f függvényjel és $t_1, \ldots, t_{\rho f}$ kielégítik T-t, akkor $f(t_1, \ldots, t_{\rho f})$ is kielégíti T-t,*

akkor minden term kielégíti T-t.

3.4. Definíció (Elsőrendű formulák). Legyen $\mathcal{L} = \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$ egy elsőrendű nyelv. $Form_{\mathcal{L}}$ a legszűkebb F halmaz, amire

(1) ha $R \in \mathcal{R}$ és $t_1, \ldots, t_{\rho R} \in Term_{\mathcal{L}}$, akkor $R(t_1, \ldots, t_{\rho R}) \in F$
(2) ha t_1, $t_2 \in Term_{\mathcal{L}}$, akkor $t_1 = t_2 \in F$.
(3) ha φ, $\psi \in F$, akkor $\neg\varphi$, $\varphi \wedge \psi \in F$
(4) ha $\varphi \in F$ és $x \in Var$, akkor $\forall x\varphi \in F$.

Az (1)-beli formulákat relációs atomi formuláknak, az 1. és 2.-beli formulákat atomi formuláknak nevezzük.

3.5. Definíció (Származtatott konnektívumok).

- $\varphi \vee \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \wedge \neg\psi)$
- $\varphi \to \psi \stackrel{\text{def}}{=} \neg\varphi \vee \psi$
- $\varphi \leftrightarrow \psi \stackrel{\text{def}}{=} (\varphi \to \psi) \wedge (\psi \to \varphi)$
- $\exists x\varphi \stackrel{\text{def}}{=} \neg\forall x\neg\varphi$ ($\exists$: egzisztenciális kvantor, „létezik”-nek vagy „van olyan”-nak olvasandó)

A következő szakaszban majd pontosan definiáljuk, hogy mit jelent az, hogy egy formula igaz. De intuitíve: a régi konnektívumok éppúgy működnek mint régen, $\forall x\varphi$ azt jelenti, hogy mindenre igaz a φ, $\exists x\varphi$ pedig azt, hogy van olyan dolog amire igaz a φ.

3.6. Példák. Az előző példabeli $\mathcal{L}$ nyelvben $\forall x\exists y \cdot (x, y) = e$, avagy $\forall x\exists y x \cdot y = e$ (azaz $\forall x\neg\forall y\neg x \cdot y = e$, avagy $\forall x\neg\forall y(x \cdot y \neq e)$) formula (ami történetesen igaz a csoportokban).

További példák: Legyenek A (alma) és R (rohadt) egyargumentumú relációjelek. Minden alma rohadt: $\forall x(A(x) \to R(x))$. Van rohadt alma (azaz némely almák rohadtak): $\exists x(A(x) \wedge R(x))$.

Legyenek F (fiú), L (lány) egyargumentumú, S ($S(x, y)$ azt jelenti, hogy „x szereti y-t”) kétargumentumú relációjelek. Mindenki szeret valakit: $\forall x\exists yS(x, y)$. Mindenkit szeret valakit: $\forall x\exists yS(y, x)$. Minden lány szeret egy fiút: $\forall x(L(x) \to \exists y(F(y) \wedge S(x, y)))$. Van egy lány, aki minden fiút szeret: $\exists x(L(x) \wedge \forall y(F(y) \to S(x, y)))$. Van olyan lány, aki csak fiúkat szeret: $\exists x(L(x) \wedge \forall y(S(x, y) \to F(y)))$.

3.7. Állítás (Formula-indukció). *Ha T olyan tulajdonság, hogy*

- *az atomi formulák rendelkeznek a T tulajdonsággal*
- *ha φ és ψ kielégíti T-t, akkor $\neg\varphi$, $\varphi \wedge \psi$ és $\forall x\varphi$ is kielégítik T-t (minden $x \in Var$-ra)*

akkor minden formula kielégíti T-t.

3.2. Szemantika

3.8. Definíció (Modell)**.** Legyen $\mathcal{L} = \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$ egy elsőrendű nyelv. $\mathcal{M}$ egy $\mathcal{L}$-*modell* (vagy $\mathcal{L}$-*struktúra*), ha olyan $\mathcal{L} \cup \{*\}$-on ($* \notin \mathcal{L}$) értelmezett függvény, amire ($\mathcal{M}(\cdot)$-t $\cdot^{\mathcal{M}}$-el jelölve)

- $*^{\mathcal{M}} = \mathcal{M}(*) = |\mathcal{M}|$ ($\mathcal{M}$ univerzuma) egy nemüres halmaz
- minden $R \in \mathcal{R}$-re $R^{\mathcal{M}} \subseteq |\mathcal{M}|^{\rho R}$ (azaz $R^{\mathcal{M}}$ ρR argumentumú reláció $|\mathcal{M}|$-en)
- minden $f \in \mathcal{F}$-re $f^{\mathcal{M}} : |\mathcal{M}|^{\rho f} \longrightarrow |\mathcal{M}|$ (azaz $f^{\mathcal{M}}$ ρf argumentumú függvény $|\mathcal{M}|$-en)
- minden $c \in \mathcal{C}$-re $c^{\mathcal{M}} \in |\mathcal{M}|$.

$|\mathcal{M}|$-et rendszerint egyszerűen M-mel jelöljük. $\mathcal{M}$ modell, ha $\mathcal{L}$-modell valamilyen $\mathcal{L}$ elsőrendű nyelvre.

$\mathcal{L}$-formulák jelentését $\mathcal{L}$-modellekben fogjuk definiálni. Az idea az, hogy az R relációjel jelentése az $\mathcal{M}$ modellben az $R^{\mathcal{M}}$ reláció, az f függvényjel jelentése az $f^{\mathcal{M}}$ függvény, a c konstansé pedig a modell $c^{\mathcal{M}}$ eleme. A gyakorlatban sokszor egyszerűen R-rel fogjuk jelölni az $\mathcal{M}$-beli $R^{\mathcal{M}}$ relációt (és hasonlóan járunk el függvényekkel és konstansokkal is). További jelölésbeli egyszerűsítés, hogy egy modellt úgy adunk meg, hogy felsoroljuk a komponenseit: $\mathcal{M} = \langle\, M, \dots \rangle$, ahol a kipontozott rész helyére a relációk, függvények és konstansok kerülnek. Az fontos, hogy egyértelmű legyen, melyik reláció (függvény konstans) melyik relációjel (függvényjel, konstansjel) modellbeli jelentése.

3.9. Definíció (Kiértékelés)**.** Legyen $\mathcal{M}$ egy modell M univerzummal. σ egy $\mathcal{M}$-hez tartozó kiértékelés, ha $\sigma : Var \longrightarrow M$.

Vagyis egy kiértékelés minden változóhoz egy modellbeli elemet rendel. Gondolhatunk rá úgy, mint „kontextusra” vagy „környezet”-re, ami értéket ad a (későbbi szóhasználattal élve: szabad) változóknak; vagy mint egy relációs adatbázis egy táblájának egy sorára.

3.10. Definíció (Termek értéke)**.** Legyen σ egy $\mathcal{M}$ $\mathcal{L}$-modellhez tartozó kiértékelés. $\mathcal{L}$ termjeinek σ szerinti $\mathcal{M}$-beli értékét a termek felépítése szerinti rekurzióval definiáljuk.

- $x^{\mathcal{M}}[\sigma] = \sigma(x)$ ha $x \in Var$
- $c^{\mathcal{M}}[\sigma] = c^{\mathcal{M}}$ ha $c \in \mathcal{C}$
- $f(t_1, \dots, t_{\rho f})^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \dots, t_{\rho f}^{\mathcal{M}}[\sigma])$ ha $f \in \mathcal{F}$ és $t_1, \dots, t_{\rho f} \in Term_{\mathcal{L}}$.

3.11. Példa. Legyen $\mathcal{L}$ a számelmélet nyelve: $\mathcal{R} = \{\leq\}$, $\rho(\leq) = 2$, $\mathcal{F} = \{+, \cdot\}$, $\rho(+) = \rho(\cdot) = 2$, $\mathcal{C} = \{0, 1\}$. Egy $\mathcal{L}$-modell a természetes számok: $\mathcal{N} = \langle\, \mathbb{N}, \leq^{\mathcal{N}}, +^{\mathcal{N}}, \cdot^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}} \rangle$, ahol $\mathbb{N}$ a természetes számok halmaza, $\leq^{\mathcal{N}}$ a természetes számok szokásos rendezése, $+^{\mathcal{N}}$ a szokásos összadás függvény a természetes számokon, s.í.t. Legyen σ az a kiértékelés, amely minden változóhoz a 3-at rendeli. Akkor $\cdot(+(0, y), +(x, 1))^{\mathcal{N}}[\sigma]$, vagyis a szokásos, infix írásmódot használva $((0 + y) \cdot (x + 1))^{\mathcal{N}}[\sigma] = 12$. Vigyázat: $\cdot(3, +(x, 1))$ (azaz $3 \cdot (x + 1)$ nem term ebben a nyelvben (mert 3 nem term).

De $\mathcal{L}$-modell az az $\mathcal{M}$ struktúra is, aminek az univerzuma $\mathbb{N}$, $\leq^{\mathcal{M}}$ az oszthatóság, $+^{\mathcal{M}}$ a legnagyobb közös osztó, $\cdot^{\mathcal{M}}$ a legkisebb közös többszörös, $0^{\mathcal{M}} = 1$ és $1^{\mathcal{M}} = 33$. Az előbbi σ kiértékelés ehhez a modellhez is jó, és $\cdot(+(0, y), +(x, 1))^{\mathcal{M}}[\sigma] = \cdot^{\mathcal{M}}(+^{\mathcal{M}}(1, 3), +^{\mathcal{M}}(3, 33)) = \cdot^{\mathcal{M}}(1, 3) = 3$.

3.12. Definíció (Formulák értéke)**.** Legyen σ egy $\mathcal{M}$ $\mathcal{L}$-modellhez tartozó kiértékelés. $\mathcal{L}$ formuláinak igazságát $\mathcal{M}$-ben a σ kiértékelés mellett a formulák felépítése szerinti rekurzióval definiáljuk.

- $\mathcal{M} \models R(t_1, \ldots, t_{\rho R})[\sigma] \iff \langle\, t_1^{\mathcal{M}}[\sigma], \ldots, t_{\rho R}^{\mathcal{M}}[\sigma]\,\rangle \in R^{\mathcal{M}}$
- $\mathcal{M} \models (t_1 = t_2)[\sigma] \iff t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma]$
- $\mathcal{M} \models \neg\varphi[\sigma] \iff \mathcal{M} \not\models \varphi[\sigma]$
- $\mathcal{M} \models (\varphi \wedge \psi)[\sigma] \iff \mathcal{M} \models \varphi[\sigma]$ és $\mathcal{M} \models \psi[\sigma]$
- $\mathcal{M} \models \forall x\varphi[\sigma] \iff \mathcal{M} \models \varphi[\sigma']$ minden olyan σ' kiértékelésre, ami legfeljebb x-en tér el σ-tól.

Az utolsó feltétel egy kicsit más (ekvivalens) megfogalmazásban:

$$\mathcal{M} \models \forall x\varphi[\sigma] \iff \text{ minden } m \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)]$$

ahol $\sigma(x/m)$ az az értékelés, ami minden x-től különböző változóhoz ugyanazt az értéket rendeli mint σ, x-hez pedig m-et.

Végül: $\mathcal{M} \models \varphi$ ha minden σ értékelésre $\mathcal{M} \models \varphi[\sigma]$.

3.13. Következmény. $\mathcal{M} \models \exists x\varphi[\sigma] \iff$ *van olyan* $m \in M$ *amire* $\mathcal{M} \models \varphi[\sigma(x/m)]$

Biz. $\mathcal{M} \models \exists x\varphi[\sigma]$ csakkor ha $\mathcal{M} \models \neg\forall x\neg\varphi[\sigma]$ csakkor ha $\mathcal{M} \not\models \forall x\neg\varphi[\sigma]$ csakkor ha nem igaz, hogy minden $m \in M$-re $\mathcal{M} \models \neg\varphi[\sigma(x/m)]$ csakkor, ha nem igaz, hogy minden $m \in M$-re $\mathcal{M} \not\models \varphi[\sigma(x/m)]$ csakkor ha van olyan $m \in M$ amire $\mathcal{M} \models \varphi[\sigma(x/m)]$. □

3.14. Példa. Legyen $\mathcal{L}$, $\mathcal{N}$ és σ mint az előző példában. $\mathcal{N} \models \forall x\neg(x + y = 0))[\sigma]$ (vagyis, a matematikában szokásos írásmódot alkalmazva: $\mathcal{N} \models \forall x(x+y \neq 0)[\sigma]$) $\mathcal{N} \models \forall x(0 \leq x+y)[\sigma]$, $\mathcal{N} \not\models \forall x(x \neq 0 \to \exists y(x \cdot y = 1))[\sigma]$. Ha $\mathcal{M}$ univerzuma $\mathbb{Q}$, $\leq^{\mathcal{M}}$ a racionális számok szokásos rendezése, $+^{\mathcal{M}}$ a összeadás $\mathbb{Q}$-n, s.í.t., akkor $\mathcal{M} \models \forall x(x \neq 0 \to \exists y(x \cdot y = 1))[\sigma]$.

3.15. Definíció (Szabad változók)**.** $t \in Term_{\mathcal{L}}$-re és $\varphi \in Form_{\mathcal{L}}$-re $FV(t)$ ill. $FV(\varphi)$ jelöli t és φ szabad változóinak halmazát, amit így definiálunk:

- $FV(x) = \{x\}$ ha $x \in Var$
- $FV(c) = \emptyset$ ha $c \in \mathcal{C}$
- $FV(f(t_1, \ldots, t_{\rho f})) = \cup\{\, FV(t_i) : 1 \leq i \leq \rho f\,\}$
- $FV(R(t_1, \ldots, t_{\rho R})) = \cup\{\, FV(t_i) : 1 \leq i \leq \rho R\,\}$
- $FV(t_1 = t_2) = FV(t_1) \cup FV(t_2)$
- $FV(\neg\varphi) = FV(\varphi)$
- $FV(\varphi \wedge \psi) = FV(\varphi) \cup FV(\psi)$
- $FV(\forall x\varphi) = FV(\varphi) \setminus \{x\}$

Speciálisan, egy term szabad változói egyszerűen a termben előforduló változók.

φ *mondat* ha $FV(\varphi) = \emptyset$. $Sent_{\mathcal{L}} = \{\, \varphi \in Form_{\mathcal{L}} : FV(\varphi) = \emptyset\,\}$ az $\mathcal{L}$-mondatok halmaza.

Például $FV(x = y \to \forall yR(x, y)) = \{\, x, y\,\}$.

3.16. Állítás. *Legyenek σ és τ az $\mathcal{M}$ $\mathcal{L}$-modellhez tartozó kiértékelések, $t \in Term_{\mathcal{L}}$ és $\varphi \in Form_{\mathcal{L}}$.*

(1) *Ha* $\sigma \restriction FV(t) = \tau \restriction FV(t)$*, akkor* $t^{\mathcal{M}}[\sigma] = t^{\mathcal{M}}[\tau]$*, és*
(2) *ha* $\sigma \restriction FV(\varphi) = \tau \restriction FV(\varphi)$*, akkor* $\mathcal{M} \models \varphi[\sigma] \iff \mathcal{M} \models \varphi[\tau]$.

Biz. 1. Term-indukcióval: Ha $t = x \in Var$, akkor $t^{\mathcal{M}}[\sigma] = \sigma(x) = \tau(x) = t^{\mathcal{M}}[\tau]$ mert $x \in \{x\} = FV(t)$. Ha $t = c \in \mathcal{C}$, akkor $t^{\mathcal{M}}[\sigma] = c^{\mathcal{M}} = t^{\mathcal{M}}[\tau]$. Végül ha $t = f(t_1, \ldots, t_{\rho f})$ ($f \in \mathcal{F}$), akkor az indukciós feltevés és $FV(t_i) \subseteq \cup\{\, FV(t_i) : 1 \leq i \leq \rho f\,\} = FV(t)$ miatt $t_i^{\mathcal{M}}[\sigma] = t_i^{\mathcal{M}}[\tau]$ ($i = 1, \ldots, \rho f$), és így $t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \ldots, t_{\rho f}^{\mathcal{M}}[\sigma]) = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\tau], \ldots, t_{\rho f}^{\mathcal{M}}[\tau]) = t^{\mathcal{M}}[\tau]$.

2. Formula-indukcióval: Ha $\varphi = R(t_1, \ldots, t_{\rho R})$, $R \in \mathcal{R}$, akkor $FV(t_i) \subseteq \cup\{ FV(t_i) : 1 \le i \le \rho r \} = FV(\varphi)$ és 1. miatt $t_i^{\mathcal{M}}[\sigma] = t_i^{\mathcal{M}}[\tau]$ $(i = 1, \ldots, \rho R)$, és így $\mathcal{M} \models \varphi[\sigma] \iff \langle t_1^{\mathcal{M}}[\sigma], \ldots, t_{\rho R}^{\mathcal{M}}[\sigma] \rangle \in R^{\mathcal{M}} \iff \langle t_1^{\mathcal{M}}[\tau], \ldots, t_{\rho R}^{\mathcal{M}}[\tau] \rangle \in R^{\mathcal{M}} \iff \mathcal{M} \models \varphi[\tau]$. Ha $\varphi = (t_1 = t_2)$, t_1, $t_2 \in Term_{\mathcal{L}}$, akkor $FV(t_i) \subseteq FV(t_1) \cup FV(t_2) = FV(\varphi)$ és 1. miatt $t_i^{\mathcal{M}}[\sigma] = t_i^{\mathcal{M}}[\tau]$ $(i = 1, 2)$, és így $\mathcal{M} \models \varphi[\sigma] \iff t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma] \iff t_1^{\mathcal{M}}[\tau] = t_2^{\mathcal{M}}[\tau] \iff \mathcal{M} \models \varphi[\tau]$. Ha $\varphi = \psi_1 \wedge \psi_2$, akkor $FV(\psi_i) \subseteq FV(\psi_1) \cup FV(\psi_2) = FV(\varphi)$ és az indukciós feltevés miatt $\mathcal{M} \models \psi_i[\sigma] \iff \mathcal{M} \models \psi_i[\tau]$ $(i = 1, 2)$, és így $\mathcal{M} \models \varphi[\sigma] \iff (\mathcal{M} \models \psi_1[\sigma]$ és $\mathcal{M} \models \psi_2[\sigma]) \iff (\mathcal{M} \models \psi_1[\tau]$ és $\mathcal{M} \models \psi_2[\tau]) \iff \mathcal{M} \models \psi_i[\sigma]$. Az öröklődés bizonyítása $\neg$-ra hasonlóan megy.

Végül ha $\varphi = \forall x \psi$, akkor minden $m \in M$-re $\mathcal{M} \models \psi[\sigma(x/m)] \iff \mathcal{M} \models \psi[\tau(x/m)]$ mert az indukciós feltevés alkalmazható ψ-re és $\sigma(x/m)$, $\tau(x/m)$-re, mivel $\sigma \restriction FV(\varphi) = \tau \restriction FV(\varphi)$ miatt $\sigma(x/m) \restriction FV(\varphi) = \tau(x/m) \restriction FV(\varphi)$, tehát $\sigma(x/m) \restriction (FV(\varphi) \cup \{x\}) = \tau(x/m) \restriction (FV(\varphi) \cup \{x\})$ és $FV(\psi) \subseteq FV(\varphi) \cup \{x\}$. Ezért $\mathcal{M} \models \varphi[\sigma] \iff$ minden $m \in M$-re $\mathcal{M} \models \psi[\sigma(x/m)] \iff$ minden $m \in M$-re $\mathcal{M} \models \psi[\tau(x/m)] \iff \mathcal{M} \models \varphi[\tau]$. □

3.17. Következmény. *$\mathcal{M}$ $\mathcal{L}$-modellre és $\varphi \in Sent_{\mathcal{L}}$-re $\mathcal{M} \models \varphi$ pontosan akkor, ha van olyan σ kiértékelés, amire $\mathcal{M} \models \varphi[\sigma]$.*

3.18. Állítás. *Minden $\mathcal{M}$ $\mathcal{L}$-modellre és $\varphi \in Form_{\mathcal{L}}$-re $\mathcal{M} \models \varphi \iff \mathcal{M} \models \forall x \varphi$. Következésképp ha $FV(\varphi) \subseteq \{ x_1, \ldots, x_n \}$, akkor $\mathcal{M} \models \varphi \iff \mathcal{M} \models \forall x_1 \ldots \forall x_n \varphi$.*

$\forall x_1 \ldots \forall x_n \varphi \in Sent_{\mathcal{L}}$-t a φ formula *univerzális lezártjá*nak mondjuk ha $FV(\varphi) \subseteq \{ x_1, \ldots, x_n \}$.

Biz. Az első állítás azért igaz, mert

$$\begin{aligned} & \mathcal{M} \not\models \forall x \varphi \\ \iff & \text{van olyan } \sigma \text{ amelyre } \mathcal{M} \not\models \forall x \varphi[\sigma] \\ \iff & \text{van olyan } \sigma \text{ és } \sigma', \text{ hogy } \sigma' \text{ legfeljebb } x\text{-en tér le } \sigma\text{-tól és } \mathcal{M} \not\models \varphi[\sigma'] \\ \iff & \text{van olyan } \sigma' \text{ amelyre } \mathcal{M} \not\models \varphi[\sigma'] \\ \iff & \mathcal{M} \not\models \varphi \end{aligned}$$

Csak a harmadik ekvivalencia igazsága nem követetkezik közvetlenül a definícióból, de abban is, a balról jobbra irány triviális, a másikban meg választhatjuk σ-t σ'-nek.

Ebből már következik (pl. indukcióval $FV(\varphi)$ elemeinek számára) az állítás második része. □

Vigyázat: azt nem állítjuk (és nem is igaz), hogy minden $\mathcal{M}$ modellben $\mathcal{M} \models \varphi \to \forall x \varphi$. Például $\mathcal{M} \not\models x = c \to \forall x(x = c)$ ha $\mathcal{M}$ legalább kételemű, mert $\mathcal{M} \not\models x = c \to \forall x(x = c)[\sigma]$ ha $\sigma(x) = c^{\mathcal{M}}$.

Azt, hogy $FV(\varphi) \subseteq \{ x_1, x_2, \ldots, x_n \}$, szokás úgy jelezni, hogy φ helyett $\varphi(x_1, x_2, \ldots, x_n)$-et írunk.

3.19. Definíció. Legyen $\mathcal{M}$ $\mathcal{L}$-modell, $\varphi(x_1, x_2, \ldots, x_n) \in Form_{\mathcal{L}}$ és $m_1, m_2, \ldots, m_n \in M$. Ekkor $\mathcal{M} \models \varphi(x_1, x_2, \ldots, x_n)[m_1, m_2, \ldots, m_n]$ ha van olyan σ értékelés, amire $\sigma(x_i) = m_i$ $(1 \le i \le n$-re$)$ és $\mathcal{M} \models \varphi(x_1, x_2, \ldots, x_n)[\sigma]$.

3.16 miatt ebben a definícióban „van olyan σ értékelés” helyett „minden olyan σ értékelés”-t is mondhattunk volna. Lényeg: 3.16 miatt elég a szabad változókat kiértékelni.

3.20. Definíció. Az x változó egy *előfordulása* a φ formulában *kötött*, ha φ-nek egy $\forall x\psi$ (és ezért aztán akkor is, ha $\exists x\psi$) alakú részformulájába esik; *szabad* ha nem kötött.

Például $x = y \to \forall y(R(x,y))$-ban x mindkét előfordulása szabad, y második előfordulása kötött, első előfordulása szabad. Nem nehéz belátni, hogy minden φ formulára $FV(\varphi) = \{\, x \in Var : x\text{-nek van szabad előfordulása } \varphi\text{-ben} \,\}$.

3.21. Definíció (behelyettesítés)**.** $\varphi(x_1, x_2, \ldots, x_n) \in Form_{\mathcal{L}}$-re és $t_1, t_2, \ldots, t_n \in Term_{\mathcal{L}}$-re $\varphi(x_1/t_1, x_2/t_2, \ldots, x_n/t_n)$ jelöli azt a formulát, amit úgy kapunk φ-ből, hogy $x_1, x_2, \ldots, x_n$ szabad előfordulásai helyére $t_1, t_2, \ldots, t_n$-et írunk.

3.22. Példa. Ha $\varphi(x,y)$ a fenti $x = y \to \forall y(R(x,y))$ formula, akkor $\varphi(x/f(x,y), y/g(x))$ az $f(x,y) = g(x) \to \forall y(R(f(x,y),y))$ formula. Ez a példa azt is mutatja, hogy ez „szimultán" (vagy „párhuzamos") helyettesítés; máskülönben az eredménye

$$\begin{aligned}&(x = y \to \forall y(R(x,y)))\,(x/f(x,y))(y/g(x))\\ &\qquad\equiv (f(x,y) = y \to \forall y(R(f(x,y),y)))\,(y/g(x))\\ &\qquad\qquad\equiv f(x,g(x)) = g(x) \to \forall y(R(f(x,y),y))\end{aligned}$$

lenne.

Csábító, de nem igaz, hogy $\mathcal{M} \models \forall x\varphi(x)$-ből $\mathcal{M} \models \varphi(x/t)$ következik minden t termre. Például legyen $\mathcal{M}$ olyan modell, aminek az univerzuma legalább kételemű, $\varphi(x)$ legyen a $\exists y\neg(x = y)$ formula, t pedig y. Akkor $\mathcal{M}$-ben igaz $\forall x\varphi(x)$ (azaz $\forall x\exists y\neg(x = y)$), de $\mathcal{M}$-ben nem igaz $\varphi(x/t)$ (azaz $\exists y\neg(y = y)$). A bajt az okozza, hogy a behelyettesítés során egy változó (most y) egy t-beli előfordulása kötötté válik. Ugyanez a jelenség előfordul mindenhol, ahol változót lekötő operátorok (mint most a $\forall$ és a $\exists$) vannak. Pl. $\int_0^1 y\, dx = y$, és ez igaz, bármilyen term-et (mint mondjuk $z \cdot y^2$) is írunk y helyébe, kivéve ha abban a term-ben x előfordul: $\int_0^1 x\, dx (= 1/2) \neq x$.

3.23. Definíció. Legyen $\mathcal{M}$ $\mathcal{L}$-modell, és $\Sigma \cup \{\varphi\} \subseteq Form_{\mathcal{L}}$. Akkor

(1) σ M-hez tartozó kiértékelésre $\mathcal{M} \models \Sigma[\sigma]$ csakkor ha minden Σ-beli φ-re $\mathcal{M} \models \varphi[\sigma]$ (Σ igaz $\mathcal{M}$-ben a σ kiértékelés szerint). Speciálisan, $\mathcal{M} \models \Sigma$ csakkor ha minden Σ-beli φ-re $\mathcal{M} \models \varphi$[5] ($\Sigma$ igaz $\mathcal{M}$-ben).
(2) $\Sigma \models \varphi$ csakkor ha $\mathcal{M} \models \varphi$ minden minden $\mathcal{M}$ modellben amire $\mathcal{M} \models \Sigma$ (φ *szemantikus következménye* Σ-nak)
(3) ($\varphi \in Form_{\mathcal{L}}$-re) $\models \varphi$ ha $\emptyset \models \varphi$, azaz ha φ minden $\mathcal{L}$-modellben minden kiértékelés mellett igaz (φ *érvényes formula*)
(4) $\varphi \in Form_{\mathcal{L}}$ ill. $\Sigma \subseteq Form_{\mathcal{L}}$ *kielégíthető*, ha van olyan modell és kiértékelés amiben igaz, *kielégíthetetlen* ha nem kielégíthető
(5) $\varphi \equiv \psi$ (*ekvivalensek*) ha ugyanazon modellekben ugyanazon kiértékelések mellett igazak. (Pl. $x = y \equiv y = x$ vagy $(\forall x)(\forall y)\varphi \equiv (\forall y)(\forall x)\varphi$.)

Könnyű belátni, hogy most is, mint kijelentéslogikában, $\varphi \equiv \psi \iff\ \models \varphi \leftrightarrow \psi$.

3.24. Állítás. $\Sigma \cup \{\varphi\} \subseteq Sent_{\mathcal{L}}$*-re*

$$\Sigma \models \varphi \iff \Sigma \cup \{\neg\varphi\} \text{ kielégíthetetlen.}$$

[5] azaz ha minden Σ-beli φ-re és minden σ kiértékelésre $\mathcal{M} \models \varphi[\sigma]$

Biz. $\Sigma \models \varphi$ csakkor ha φ igaz Σ minden modelljében, csakkor ha $\neg\varphi$ hamis Σ minden modelljében, csakkor ha $\Sigma \cup \{\neg\varphi\}$ kielégíthetetlen. $\square$

A propozicionális logikával ellentétben, az érvényes elsőrendű formulák halmaza *nem* eldönthető. (Ha az lenne, akkor az egész matematika eldönthető lenne.) Ennek nem az az oka, hogy a modellek végtelenek, sőt: az érvényes elsőrendű formulák halmaza rekurzíve felsorolható (van egy Turing gép, ami felsorolja az összes érvényes formulát), míg a véges modelleken érvényes formulák halmaza nemhogy nem eldönthető de még fel sem sorolható.

3.25. Állítás.

(1) $\models \forall x(\varphi \wedge \psi) \leftrightarrow (\forall x\varphi \wedge \forall x\psi)$
(2) $\models \exists x(\varphi \vee \psi) \leftrightarrow (\exists x\varphi \vee \exists x\psi)$
(3) $\not\models \forall x(\varphi \vee \psi) \to (\forall x\varphi \vee \forall x\psi)$, *de ha* $x \notin FV(\psi)$, *akkor* $\models \forall x(\varphi \vee \psi) \leftrightarrow (\forall x\varphi \vee \psi)$
(4) $\not\models (\exists x\varphi \wedge \exists x\psi) \to \exists x(\varphi \wedge \psi)$, *de ha* $x \notin FV(\psi)$, *akkor* $\models (\exists x\varphi \wedge \psi) \leftrightarrow \exists x(\varphi \wedge \psi)$
(5) $\models \forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$
(6) $\not\models (\forall x\varphi \to \forall x\psi) \to \forall x(\varphi \to \psi)$
(7) $\models \forall x\forall y\varphi \to \forall y\forall x\varphi$
(8) $\models \exists x\exists y\varphi \to \exists y\exists x\varphi$
(9) $\models \exists x\forall y\varphi \to \forall y\exists x\varphi$
(10) $\not\models \forall x\exists y\varphi \to \exists y\forall x\varphi$

Biz. A pozitív állítások könnyen következnek az igazság definíciójából, a negatívakra pedig könnyű ellenpéldákat adni. Példaként belátjuk a (3) állítást. Tartalmazzon az $\mathcal{L}$ nyelv két egyargumentumú relációjelet (R és S), és legyen $\mathcal{M} = \langle M, R^{\mathcal{M}}, S^{\mathcal{M}} \rangle$, ahol $M = \{a, b\}$, $R^{\mathcal{M}} = \{a\}$ és $S^{\mathcal{M}} = \{b\}$. Akkor $\mathcal{M} \models \forall x(R(x) \vee S(x))$ de $\mathcal{M} \not\models \forall xR(x) \vee \forall xS(x)$.

(3) második részének belátásához tegyük fel, hogy $x \notin FV(\psi)$ és legyen $\mathcal{M}$, σ tetszőleges. Akkor

$$\begin{aligned}
& \mathcal{M} \not\models \forall x(\varphi \vee \psi)[\sigma] \\
\iff & \text{ van } m \in M, \text{ hogy } \mathcal{M} \not\models \varphi \vee \psi[\sigma(x/m)] \\
\iff & \text{ van } m \in M, \text{ hogy } \mathcal{M} \not\models \varphi[\sigma(x/m)] \text{ és } \mathcal{M} \not\models \psi[\sigma(x/m)] \\
\iff & \mathcal{M} \not\models \forall x\varphi[\sigma] \text{ és } \mathcal{M} \not\models \psi[\sigma] \\
\iff & \mathcal{M} \not\models \forall x\varphi \vee \psi[\sigma]
\end{aligned}$$

(az utolsó előtti lépésben az 3.16 állítást használtuk.)
(5) Azt kell megmutatnunk, hogy $\models (\forall x(\varphi \to \psi) \wedge \forall x\varphi) \to \forall x\psi$. Tetszőleges $\mathcal{M}$ modellre és σ kiértékelésre

$$\begin{aligned}
& \mathcal{M} \models \forall x(\varphi \to \psi) \wedge \forall x\varphi[\sigma] \\
\Longrightarrow & \mathcal{M} \models \forall x(\varphi \to \psi)[\sigma] \text{ és } \mathcal{M} \models \forall x\varphi[\sigma] \\
\Longrightarrow & \text{ minden } m \in M\text{-re } \mathcal{M} \models \varphi \to \psi[\sigma(x/m)] \text{ és minden } m \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)] \\
\Longrightarrow & \text{ minden } m \in M\text{-re, ha } \mathcal{M} \models \varphi[\sigma(x/m)], \text{ akkor } \mathcal{M} \models \psi[\sigma(x/m)]; \\
& \qquad \text{és minden } m \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)] \\
\Longrightarrow & \text{ minden } m \in M\text{-re } \mathcal{M} \models \psi[\sigma(x/m)] \\
\Longrightarrow & \mathcal{M} \models \forall x\psi[\sigma]
\end{aligned}$$

(6) Abból, hogy „Ha mindenki milliomos, akkor mindenki szőke" nem következik, hogy „minden milliomos szőke". Kicsit formálisabban: legyen $\mathcal{L}$ egy elsőrendű nyelv két unér relációjellel R-rel és S-sel, és legyen $\mathcal{M}$ a $\langle M, R^{\mathcal{M}}, S^{\mathcal{M}} \rangle$ $\mathcal{L}$-struktúra, ahol $M = \{a, b\}$, $R^{\mathcal{M}} = \{a\}$ és $S^{\mathcal{M}} = \{b\}$. Akkor $\mathcal{M} \models \forall x.R(x) \to \forall x.S(x)$, mert $\mathcal{M} \not\models \forall x.R(x)$; de $\mathcal{M} \not\models \forall x(R(x) \to S(x))$, mert $\mathcal{M} \not\models R(x) \to S(x)[a]$. Vegyük észre, hogy $S^{\mathcal{M}} = \emptyset$ ugyanilyen jó lett volna. Csak az volt fontos, hogy $R^{\mathcal{M}}$ ne legyen részhalmaza $S^{\mathcal{M}}$-nek.
(9) Legyen $\mathcal{M}$ és σ tetszőleges. Akkor

$$\begin{aligned}
&\mathcal{M} \models \exists x \forall y \varphi[\sigma] \\
\Longrightarrow\ &\text{van olyan } m \in M, \text{ hogy } \mathcal{M} \models \forall y \varphi[\sigma(x/m)] \\
\Longrightarrow\ &\text{van olyan } m \in M, \text{ hogy minden } m' \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)(y/m')] \\
\Longrightarrow\ &\text{minden } m' \in M\text{-re van olyan } m \in M, \text{ hogy } \mathcal{M} \models \varphi[\sigma(x/m)(y/m')] \\
\Longrightarrow\ &\text{minden } m' \in M\text{-re } \mathcal{M} \models \exists x \varphi[\sigma(y/m')] \\
\Longrightarrow\ &\mathcal{M} \models \forall y \exists x \varphi[\sigma]
\end{aligned}$$

(10) Abból, hogy „Mindenkit szeret valaki", azaz, hogy „Mindenkihez van valaki aki őt szereti", nem következik, hogy „Van valaki, aki mindenkit szeret". Kicsit formálisabban: legyen $\mathcal{L}$ az üres nyelv és legyen $\mathcal{M}$ egy legalább kételemű $\mathcal{L}$-struktúra. Akkor $\mathcal{M} \not\models \forall x \exists y.x = y \to \exists y \forall x.x = y$. □

3.26. Gyakorlat. Hol használtuk (9) bizonyításában, hogy x és y különböző változók? Mutassuk meg, hogy (9) akkor is igaz, ha x és y ugyanaz a változó.

A dedukciótétel elsőrendű logikában egy kicsit bonyolultabb mint propozicionális logikában, pl., $\{\varphi\} \models \forall x \varphi$ (ld. 3.18), de $\not\models \varphi \to \forall x \varphi$ (ha például φ az $x = c$ formula, akkor $\varphi \to \forall x \varphi$ egyetlen, legalább kételemű modellben sem igaz).

3.27. Tétel (Dedukciótétel)**.** *Ha* $\Sigma \cup \{\varphi, \psi\} \subseteq Form_{\mathcal{L}}$*, akkor*

$$\Sigma \cup \{\varphi\} \models \psi \iff \Sigma \models \forall \bar{x} \varphi \to \psi,$$

ahol $\bar{x} = x_1, \ldots, x_n$ *az* $FV(\varphi)$ *egy felsorolása (azaz* $\forall \bar{x} \varphi$ *a* φ *univerzális lezártja). Speciálisan, ha* $\Sigma \cup \{\varphi, \psi\} \subseteq Sent_{\mathcal{L}}$*, akkor*

$$\Sigma \cup \{\varphi\} \models \psi \iff \Sigma \models \varphi \to \psi.$$

Biz. ($\Rightarrow$) Tegyük fel, hogy $\Sigma \not\models \forall \bar{x} \varphi \to \psi$, azaz $\mathcal{M} \models \Sigma$ de $\mathcal{M} \not\models \forall \bar{x} \varphi \to \psi[\sigma]$ valamilyen $\mathcal{M}$ modellre és σ kiértékelésre. Akkor $\mathcal{M} \models \forall \bar{x} \varphi[\sigma]$ (tehát $\mathcal{M} \models \forall \bar{x} \varphi$ 3.16 miatt, mivel $\forall \bar{x} \varphi$ mondat, következésképp $\mathcal{M} \models \varphi$ 3.18 miatt) és $\mathcal{M} \not\models \psi[\sigma]$. De akkor $\mathcal{M} \models \Sigma \cup \{\varphi\}$, tehát $\Sigma \cup \{\varphi\} \not\models \psi$.

($\Leftarrow$) Tegyük fel, hogy $\Sigma \cup \{\varphi\} \not\models \psi$, azaz $\mathcal{M} \models \Sigma \cup \{\varphi\}$ de $\mathcal{M} \not\models \psi[\sigma]$ valamilyen $\mathcal{M}$ modellre és σ kiértékelésre. 3.18 miatt $\mathcal{M} \models \forall \bar{x} \varphi$ és így $\mathcal{M} \models \forall \bar{x} \varphi[\sigma]$, tehát $\mathcal{M} \not\models \forall \bar{x} \varphi \to \psi[\sigma]$, következésképp $\mathcal{M} \not\models \forall \bar{x} \varphi \to \psi$. □

3.3. Példák

3.28. Példa. Legyen $\mathcal{L} = \{<\}$, ahol $\rho(<) = 2$. Adjunk meg olyan $\mathcal{L}$-mondatokat, amiknek modelljeiben

(1) $<$ jelentése részbenrendezés (irreflexív, tranzitív)
(2) minden elemnek van közvetlen rákövetkezője (ahol y közvetlen rákövetkezője x-nek, ha $x < y \wedge \neg\exists z(x < z \wedge z < y)$)
(3) egyetlen elemnek sincs közvetlen rákövetkezője
(4) van olyan elem, ami minden elemmel összehasonlítható
(5) minden kételemű halmaznak van legkisebb felső korlátja.

3.29. Példa. Legyen $\mathcal{L}$ az $\mathcal{N} = \langle \mathbb{N}, 0, s, +, \cdot \rangle$ modell nyelve. Adjunk meg olyan $\mathcal{L}$-formulákat, amiknek jelentése $\mathcal{N}$-ben

(1) a négyzetszámok
(2) a páratlan számok
(3) a prímek.

Fogalmazzuk meg $\mathcal{L}$-en a Goldbach-sejtést. Fogalmazzuk meg $\mathcal{L}$-en a teljes indukció elvét.

3.4. Elsőrendű logika bizonyításelmélete Logikai axiómák :

(A1) $\varphi \to (\psi \to \varphi)$
(A2) $[\varphi \to (\psi \to \chi)] \to [(\varphi \to \psi) \to (\varphi \to \chi)]$
(A3) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$
(A4) $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$
(A5) $\varphi \to \forall x\varphi$ ha $x \notin FV(\varphi)$
(A6) $\exists x(x = t)$ ha $x \notin FV(t)$
(A7) $s = t \to (\varphi \to \psi)$ ha ψ úgy keletkezik φ-ből, hogy abban s egy előfordulását t-re cseréljük

Mint a kijelentéslogikában, itt is könnyű látni, hogy a logikai axiómák érvényesek.

3.30. Definíció. Legyen $\Sigma \subseteq Form$. A $\varphi_1, \dots \varphi_n$ formulasorozat egy (n-hosszú) levezetés (bizonyítás) Σ-ból, ha minden $1 \leq k \leq n$-re teljesül az alábbi feltételek valamelyike:

- φ_k logikai axióma
- $\varphi_k \in \Sigma$
- van olyan $1 \leq i, j < k$, hogy $\varphi_i = \varphi_j \to \varphi_k$ (ebben az esetben azt mondjuk, hogy φ_k leválasztással (avagy modus ponens-sel) keletkezett φ_j-ből és $\varphi_j \to \varphi_k$-ból)
- van olyan $1 \leq i < k$, hogy $\varphi_k = \forall x\varphi_i$ (ebben az esetben azt mondjuk, hogy φ_k generalizálással keletkezett φ_j-ből.

$\varphi \in Form$ levezethető Σ-ból (jelölés: $\Sigma \vdash \varphi$) ha van olyan $\varphi_1, \dots \varphi_n$ levezetés Σ-ból, hogy $\varphi = \varphi_n$. Σ konzisztens, ha nem vezethető le belőle minden formula.

3.31. Tétel (Teljességi tétel). *Minden $\Sigma \cup \{\varphi\} \subseteq Form$-ra $\Sigma \models \varphi \iff \Sigma \vdash \varphi$.*

A jobbról balra irányt (vagyis a helyességet) könnyű belátni a levezetés hosszára vonatkozó indukcióval. A másik irány az alábbi tétel következménye.

3.32. Tétel. *Minden konzisztens $\Sigma \subseteq Form_{\mathcal{L}}$-nek van modellje.*

A teljességi tétel bizonyítása ebből pontosan úgy megy, mint kijelentéslogikában.

3.5. Modellelmélet 3.32 egy nagyon fontos kiegészítése a következő, leszálló Löwenheim-Skolem tétel néven ismert állítás:

3.33. Tétel. *Ha $\Sigma \subseteq Sent_{\mathcal{L}}$-nek van modellje, akkor van $\mathcal{L}$ számosságánál nem nagyobb számosságú modellje is. ($|\mathcal{L}|$, az $\mathcal{L}$ nyelv számossága, a benne szereplő szimbólumok számossága, ha ez végtelen, és megszámlálhatóan végtelen máskor.)*

3.34. Tétel (Kompaktság)**.** *Egy mondathalmaz pontosan akkor elégíthető ki, ha minden véges része kielégíthető.*

Biz. A nemtriviális irány 3.31 és a levezethetőség definíciójának következménye. Ezek szerint ui. ha a Σ mondathalmaz kielégíthetetlen, akkor $\Sigma \models \perp$, 3.31 miatt tehát $\Sigma \vdash \perp$, akkor viszont Σ valamely Δ véges részére $\Delta \vdash \perp$, következésképp $\Delta \models \perp$ és így Δ kielégíthetetlen. □

3.35. Tétel (Felszálló Löwenheim-Skolem tétel)**.** *Ha $\Sigma \subseteq Sent_{\mathcal{L}}$-nek van végtelen modellje és $\lambda \geq |\mathcal{L}|$, akkor van λ számosságú modellje is.*

Biz. Legyen $\mathcal{L}' = \mathcal{L} \cup \{\, c_\kappa : \kappa < \lambda \,\}$, ahol c_κ-k $\mathcal{L}$-ben nem előforduló konstansjelek, és legyen $\Delta = \{\, c_\kappa \neq c_\mu : \kappa < \mu < \lambda \,\}$. Akkor $\Sigma \cup \Delta$ minden véges részének van modellje (mert Σ bármely végtelen modellje kiterjeszthető ilyenné), a kompaktsági tétel miatt tehát $\Sigma \cup \Delta$-nak is van $\mathcal{M}$ modellje. A leszálló Löwenheim-Skolem tétel miatt feltehetjük, hogy $|\mathcal{M}| \leq |\mathcal{L}'| = \lambda$, és $\mathcal{M} \models \Delta$ miatt $|\mathcal{M}| \geq \lambda$. Következésképp $\mathcal{M}$ reduktuma $\mathcal{L}$-re Σ egy λ számosságú modellje. □

3.6. Elméletek *Elmélet*en egyszerűen egy mondathalmazt értünk. $\Delta \subseteq Sent_{\mathcal{L}}$ *axiomatizálja* a Σ elméletet, ha $Cns(\Delta) = Cns(\Sigma)$, ahol tetszőleges Σ formulahalmazra $Cns(\Sigma) = \{\varphi : \Sigma \models \varphi\}$. $\Delta \subseteq Sent_{\mathcal{L}}$ *axiomatizálja* a K modell-osztályt, ha $K = \mathrm{Mod}(\Sigma) \stackrel{\text{def}}{=} \{\, \mathcal{M} : \mathcal{M} \models \Sigma \,\}$. A K modell-osztály *elemi*, ha van olyan Σ mondathalmaz, ami axiomatizálja, és végesen axiomatizálható, ha van olyan véges Σ mondathalmaz, ami axiomatizálja.

3.36. Gyakorlat. K pontosan akkor axiomatizálható végesen, ha van egy φ mondat, amire $K = \mathrm{Mod}(\varphi)$.

3.37. Gyakorlat. $Cns(\Sigma) = \mathrm{Th}\,\mathrm{Mod}(\Sigma)$.

3.38. Példa. Legyen n természetes szám. A legfeljebb n elemű modellek osztályát axiomatizálja $\chi_{\leq n} : \forall x_1 \forall x_2 \ldots \forall x_{n+1}(x_{n+1} = x_1 \vee x_{n+1} = x_2 \vee \cdots \vee x_{n+1} = x_n)$. A legalább n elemű modellek osztályát axiomatizálja $\chi_{\geq n} : \exists x_1 \exists x_2 \ldots \exists x_n(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \cdots \wedge x_{n-1} \neq x_n)$. A pontosan n-elemű modellek osztályát axiomatizálja $\chi_{\leq n} \wedge \chi_{\geq n}$.

3.39. Tétel. (1) *A véges modellek osztálya nem elemi.*
(2) *A végtelen modellek osztálya elemi, de nem axiomatizálható végesen.*

Biz. Tegyük fel, hogy Δ axiomatizálja a véges modellek $K_{<\infty}$ osztályát. Legyen $\Sigma = \{\, \chi_{\geq n} : n \in \mathbb{N} \,\}$. Akkor $\Delta \cup \Sigma$ minden véges része kielégíthető, tehát a kompaktsági tétel miatt $\Delta \cup \Sigma$-nak is van modellje, de az biztosan végtelen.

A végtelen modellek K_∞ osztályát axiomatizálja $\{\, \chi_{\geq n} : n \in \mathbb{N} \,\}$. Tegyük fel, hogy K_∞ végesen axiomatizálható, azaz van olyan φ mondat, amire $K_\infty = \mathrm{Mod}(\varphi)$. Akkor $\mathrm{Mod}(\neg\varphi) = K_{<\infty}$, ellentmondásban az állítás első részével. □

3.40. Következmény. (1) *A véges modellek elméletének van végtelen modellje.*
(2) *Ha K_∞ a végtelen modellek osztálya, akkor $K_\infty \models \varphi$ pontosan akkor, ha valamilyen n-re φ igaz minden legalább n-elemű véges modellben.*

Biz. (1) Ha $\operatorname{Mod}\operatorname{Th} K_{<\infty} \subseteq K_{<\infty}$, akkor $\operatorname{Mod}\operatorname{Th} K_{<\infty} = K_{<\infty}$, ellentmondva annak, hogy $K_{<\infty}$ nem elemi.

(2) Tudjuk, hogy

$$(*) \qquad K_\infty = \operatorname{Mod}\Sigma, \text{ ahol } \Sigma = \{\, \chi_{\geq n} : n \in \mathbb{N} \,\}$$

($\Rightarrow$) $(*)$ miatt $K_\infty \models \varphi \iff \Sigma \models \varphi$, amiből a kompaktság miatt $\Sigma_0 \models \varphi$ Σ valamely Σ_0 véges részére. De akkor, ha n a legnagyobb, amire $\chi_{\geq n} \in \Sigma_0$, akkor Σ_0-nak, és így φ-nek is modellje minden legalább n-elemű modell.

($\Leftarrow$) Ha φ igaz minden legalább n-elemű véges modellben, akkor $\chi_{\geq n} \models \varphi$, és így $\Sigma \models \varphi$, amiből $(*)$ miatt $K_\infty \models \varphi$. □

3.41. Definíció. Az $\mathcal{M}$ és $\mathcal{N}$ modellek *elemien ekvivalensek* (jelölés: $\mathcal{M} \equiv \mathcal{N}$) ha a közös nyelvük minden φ formulájára $\mathcal{M} \models \varphi \iff \mathcal{N} \models \varphi$.

3.42. Gyakorlat. $\mathcal{M} \equiv \mathcal{N} \iff \mathcal{M} \models \operatorname{Th}(\mathcal{N})$

3.43. Definíció. λ végtelen számosságra a T elmélet λ-kategorikus, ha T bármely két, λ-számosságú modellje izomorf. Vagyis ha izomorfizmus erejéig legfeljebb egy λ számosságú modellje van.

3.44. Tétel. *A természetes számok elmélete nem ω-kategorikus.*

Biz. Legyen $\mathcal{N}$ a természetes számok szokásos modellje, $\mathcal{L}$ ennek nyelve, és c egy, az $\mathcal{L}$-ben nem szereplő konstansjel. $n > 0$-ra jelölje $\mathbf{n}$ az $\underbrace{1 + 1 + \ldots + 1}_{n\text{-szer}}$ termet. A $\operatorname{Th}(\mathcal{N}) \cup \{\mathbf{n} < c : n > 0\}$ halmaz minden véges részének van modellje, tehát az egésznek is, és akkor a leszálló Löwenheim-Skolem tétel miatt megszámlálható is: legyen $\mathcal{M}$ egy ilyen modell és $\mathcal{M}'$ az $\mathcal{M}$ $\mathcal{L}$-reduktuma (vagyis az $\mathcal{M}$ modell, csak nincs kijelölve benne $c^{\mathcal{M}}$). Akkor $\mathcal{M}' \equiv \mathcal{N}$, mert $\mathcal{M}' \models \operatorname{Th}(\mathcal{N})$, de nem izomorf vele, mert ha $f : \mathcal{N} \to \mathcal{M}'$ beágyazás, akkor minden $n > 0$-ra $f(\mathbf{n}^{\mathcal{N}}) = \mathbf{n}^{\mathcal{M}'}$, márpedig $c^{\mathcal{M}}$ ezektől mind különbözik, azaz f nem lehet ráképezés. □

3.45. Definíció. A T elmélet teljes, ha bármely két modellje elemien ekvivalens.

3.46. Következmény. *T pontosan akkor teljes, ha nyelvének minden φ mondatára $T \models \varphi$ vagy $T \models \neg\varphi$.*

Biz. Ha T-nek nincs modellje, akkor mindkét oldal triviálisan igaz. Úgyhogy tegyük fel, hogy van, és legyen $\mathcal{L}$ a T nyelve. Ha T teljes, akkor minden $\varphi \in Sent_{\mathcal{L}}$-re $T \models \varphi$ (ha φ igaz T modelljeiben) vagy $T \models \neg\varphi$ (ellenkező esetben). Fordítva, a feltevés miatt T bármely két modelljében egyszerre igaz vagy hamis minden $\mathcal{L}$-beli mondat. □

Példák teljes elméletre: $\operatorname{Th}(\mathcal{M})$ tetszőleges $\mathcal{M}$ modellre (ez triviális); $\operatorname{Th} K_\infty$ (ez nem, de rövidesen ki fog jönni).

Miért fontos egy elmélet teljessége? Mert ha a T elmélet teljes, konzisztens, és *rekurzívan axiomatizálható*, azaz van olyan eldönthető Σ formulahalmaz, amelyre $T = Cns(\Sigma)$, akkor T eldönthető. Ugyanis intuitíve világos, hogy eldönthető Σ-ra $Cns(\Sigma)$ rekurzíve felsorolható, azaz van olyan algoritmus, ami szép sorban előállítja az összes elemét, és csak azokat. De ez általában nem eldöntő algoritmus, mert nem tudhatjuk, hogy meddig kell várni egy mondat megjelenésére: ha még nem jelent meg, annak az is lehet az oka, hogy még nem kerül rá sor, de az is, hogy soha nem is fog, mert nem eleme $Cns(\Sigma)$-nak. Az utóbbi csak akkor derül ki, ha a tagadása megjelenik (most feltesszük, hogy az elmélet konzisztens — máskülönben triviálisan eldönthető). T teljessége éppen azt biztosítja, hogy minden nem levezethető formula negáltja megjelenjen az algoritmus kimenetében; vagyis az algoritmus így előbb vagy utóbb minden formuláról „nyilatkozzon". Azaz:

3.47. Tétel. *Minden rekurzívan axiomatizálható teljes elmélet eldönthető.*

3.48. Tétel (Łos-Vaught teszt elmélet teljességére)**.** *Ha a T elméletnek csak végtelen modelljei vannak és T λ-kategorikus valamilyen $\lambda \geq |\mathcal{L}|$-re, ahol $\mathcal{L}$ a T nyelve, akkor T teljes.*

Biz. Legyen $\mathcal{M}$, $\mathcal{N}$ a T két modellje. A felszálló Löwenheim-Skolem tétel miatt $\mathrm{Th}(\mathcal{M})$-nek és $\mathrm{Th}(\mathcal{N})$-nek, mivel van végtelen modellje ($\mathcal{M}$ ill. $\mathcal{N}$) van $\mathcal{M}'$ ill. $\mathcal{N}'$ λ-számosságú modellje is. Ezek $T \subseteq \mathrm{Th}(\mathcal{M})$ és $T \subseteq \mathrm{Th}(\mathcal{N})$ miatt T-nek is modelljei, a λ-kategoricitás miatt tehát $\mathcal{M}' \cong \mathcal{N}'$ és így $\mathcal{M}' \equiv \mathcal{N}'$; de akkor $\mathcal{M} \equiv \mathcal{M}'$ és $\mathcal{N} \equiv \mathcal{N}'$ miatt $\mathcal{M} \equiv \mathcal{N}$. □

3.49. Következmény. $\mathrm{Th}\, K_\infty$ *teljes és eldönthető.*

Biz. $\mathrm{Th}\, K_\infty$-nek csak végtelen modellje van (hiszen $\chi_{\geq n} \in \mathrm{Th}\, K_\infty$ minden n-re), és triviálisan λ-kategorikus minden végtelen λ-ra, tehát a Łos-Vaught teszt miatt teljes. Ezért aztán, mivel $\Sigma = \{\, \chi_{\geq n} : n \in \mathbb{N} \,\}$ rekurzívan axiomatizálja, eldönthető is. □

3.50. Definíció. Az egyargumentumú D számelméleti tulajdonság T-reprezentálható, ha van olyan $\varphi(x)$ számelméleti formula, amire igaz, hogy minden n-re

$$(a) \quad D(n) \implies T \vdash \varphi(\mathbf{n}) \qquad (b) \quad \neg D(n) \implies T \vdash \neg\varphi(\mathbf{n})$$

T elég erős, ha minden eldönthető számelméleti tulajdonság T-reprezentálható.

3.51. Tétel. *Ha T konzisztens és elég erős, akkor eldönthetetlen.*

Biz. Tegyük fel, hogy T eldönthető, és legyen $\varphi_n(x)$ az egy szabad változós számelméleti formulák egy felsorolása, D pedig a

$$(*) \qquad D(n) \iff T \vdash \neg\varphi_n(\mathbf{n})$$

tulajdonság. T eldönthetősége miatt D eldönthető. Ezért, és mivel T elég erős, D-t reprezentálja $\varphi_d(x)$ valamely $d \in \mathbb{N}$-re. Ha $D(d)$ igaz, akkor D definíciója szerint $T \vdash \neg\varphi_d(\mathbf{d})$, ugyanakkor $T \vdash \varphi_d(\mathbf{d})$ is áll, ellentmondva T konzisztenciájának, mert $\varphi_d(x)$ reprezentálja D-t. $D(d)$ tehát hamis; de akkor 3.50(b) miatt $T \vdash \neg\varphi_d(\mathbf{d})$, azaz $D(d)$ igaz, vagyis ellentmondásra jutottunk. □

3.52. Definíció (Peano-aritmetika)**.** Legyen a $\{s, +, \cdot, 0, 1\}$ nyelv, ahol s egy-, $+$ és $\cdot$ pedig kétargumentumú függvényjelek, 0 és 1 pedig konstansok. A Peano aritmetika az az elmélet az nyelven, amelyet a következő mondatok axiomatizálnak:

- $\forall xy(sx = sy) \to x = y$
- $\forall x.0 \neq sx$
- $\forall x.x + 0 = x$
- $\forall xy.x + sy = s(x + y)$
- $\forall x.x \cdot 0 = 0$
- $\forall xy.x \cdot sy = (x \cdot y) + x$
- $\psi(0) \wedge \forall x(\psi(x) \to \psi(sx)) \to \forall x.\psi(x)$ minden $\psi(x) \in Form_L$-re.

3.53. Tétel (Gödel)**.** *A Peano-aritmetika elég erős.*

3.54. Következmény. *A Peano-aritmetika egyetlen konzisztens rekurzívan axiomatizálható bővítése sem teljes.*

Biz. 3.53 miatt elég erős (ha D egyargumentumú számelméleti tulajdonság, akkor pl. $D(n) \implies PA \vdash \varphi(\mathbf{n})$ miatt $D(n) \implies PA^+ \vdash \varphi(\mathbf{n})$ ha $PA \subseteq PA^+$), tehát ha konzisztens, akkor 3.51 miatt eldönthetetlen, vagyis 3.47 miatt nem teljes. $\square$

3.7. Normálforma Az 1.31 következmény elsőrendű logikában is igaz, azaz

3.55. Tétel. *Ha ψ részformulája φ-nek, $\psi \equiv \psi'$, és φ' úgy keletkezik φ-ből, hogy benne ψ-t ψ'-re cseréljük, akkor $\varphi \equiv \varphi'$.*

3.56. Állítás (Kötött változók átnevezése). *Ha y nem fodul elő φ-ben (kötötten sem!), akkor $\forall x\varphi \equiv \forall y(\varphi(x/y))$ és $\exists x\varphi \equiv \exists y(\varphi(x/y))$.*

3.57. Tétel (Skolemizálás). *Legyen $\varphi \in Sent_{\mathcal{L}}$, $\exists x\psi(x, y_1, \ldots, y_n)$ a φ egy olyan részformulája, ami nem áll egzisztenciális kvantor hatókörében. Ha $f \notin \mathcal{L}$ n-argumentumú függvényjel, és φ'-t úgy kapjuk φ-ból, hogy $\exists x\psi(x, y_1, \ldots, y_n)$-t kicseréljük $\psi(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$-re, akkor*

$$\varphi \text{ kielégíthető} \iff \varphi' \text{ kielégíthető.}$$

(Ha $n = 0$, akkor 0-argumentumú függvényjelre (magyarul: konstansra) cseréljük x-et.)

Pl. $\exists v\forall x\forall y\exists z\, r(x, y, z, v)$-ből $\forall x\forall y\, r(x, y, f(x, y), a)$ lesz (két lépésben). Azt nem állítjuk, hogy a két formula ekvivalens.

A biz. ötlete. Az egyszerűség kedvéért legyen $n = 1$.

($\Rightarrow$) Tegyük fel, hogy $\mathcal{M} \models \varphi$. Definiálunk egy $\mathcal{M}'$ $\mathcal{L} \cup \{f\}$ modellt ami modellje lesz φ'-nek. M' univerzuma ugyanaz mint $\mathcal{M}$-é, és az $\mathcal{L}$-ben szereplő relációjeleket, függvényjeleket és konstansjeleket ugyanúgy interpretálja mint $\mathcal{M}$, $f^{\mathcal{M}'}$ pedig a következő függvény $M' = M$-en: $m \in M$-re ha $\mathcal{M} \models \exists x\psi(x, y)[m]$, akkor legyen $f^{\mathcal{M}'}(m)$ egy olyan $m' \in M$ amire $\mathcal{M} \models \exists x\psi(x, y)[m', m]$, ha pedig $\mathcal{M} \not\models \exists x\psi(x, y)[m]$, akkor $f^{\mathcal{M}'}(m)$ tetszőleges $m' \in M$.

($\Leftarrow$) Ha $\mathcal{M}' \models \varphi'$, akkor $\mathcal{M} = \mathcal{M}' \restriction \mathcal{L}$-ben igaz lesz φ. $\square$

3.58. Definíció. Literális formulán most is atomi vagy negált atomi formulát értünk. (Pl. $\neg r(x, f(c, x))$.) Egy kvantormentes formula CNF ha literálisok diszjunkcióinak konjunkciója ($\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{ij}$, ahol l_{ij}-k literálisok).

3.59. Definíció. Egy elsőrendű formula

- prenex, ha $Q_1x_1 \ldots Q_nx_n\psi$ alakú, ahol Q_i-k kvantorok ($\forall$ vagy $\exists$), ψ pedig kvantormentes; ψ a prenex formula *mátrix*a.
- Skolem konjunktív normálforma ($SCNF$), ha prenex, minden kvantora univerzális, és a mátrixa CNF.

3.60. Tétel. *Minden φ mondathoz van φ' Skolem konjunktív normálformájú mondat, ami pontosan akkor elégíthető ki, ha φ kielégíthető.*

Biz. Hét lépésben alakítjuk át φ-t $SCNF$-é (és ezt közben két mondaton illusztráljuk is). A két példamondat:

(A) $$\exists x\, \neg p(x) \wedge [\exists x\, p(x) \vee \exists x(p(x) \wedge q(x))] \wedge \neg\exists x\, p(x)$$

(B) $$\neg\exists z[\exists x\forall y\, p(x, y, y) \to \forall y\exists x(p(x, y, x) \vee p(z, y, x))]$$

(1. lépés) Kiküszöböljük a definiált konnektívumokat úgy, hogy csak $\forall$, $\exists$, $\neg$, $\vee$, $\wedge$ maradjon. Használjuk:

$$\varphi \to \psi \equiv \neg\varphi \vee \psi \qquad \neg(\varphi \to \psi) \equiv \varphi \wedge \neg\psi \qquad \varphi \leftrightarrow \psi \equiv (\neg\varphi \vee \psi) \wedge (\varphi \vee \neg\psi)$$

(A) nem változik,

(B1) $$\neg\exists z[\neg\exists x\forall y\, p(x,y,y) \vee \forall y\exists x(p(x,y,x) \vee p(z,y,x))]$$

(2. lépés) $\neg$-ot „bevisszük” amíg már csak atomi formulák előtt áll. Használjuk:

$$\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi \qquad \neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi \qquad \neg\neg\varphi \equiv \varphi$$
$$\neg\forall x\varphi \equiv \exists x\neg\varphi \qquad \neg\exists x\varphi \equiv \forall x\neg\varphi$$

(A2) $$\exists x\, \neg p(x) \wedge [\exists x\, p(x) \vee \exists x(p(x) \wedge q(x))] \wedge \forall x\neg p(x)$$

(B2) $$\forall z[\exists x\forall y\, p(x,y,y) \wedge \exists y\forall x(\neg p(x,y,x) \wedge \neg p(z,y,x))]$$

(3. lépés [nem muszáj, de hasznos]) Bevisszük a kvantorokat. Használjuk:

$$\forall x(\varphi \vee \psi) \equiv \forall x\varphi \vee \psi \qquad \forall x(\psi \vee \varphi) \equiv \psi \vee \forall x\varphi \qquad \forall x\psi \equiv \psi$$
$$\exists x(\varphi \wedge \psi) \equiv \exists x\varphi \wedge \psi \qquad \exists x(\psi \wedge \varphi) \equiv \psi \wedge \exists x\varphi \qquad \exists x\psi \equiv \psi$$

ha $x \notin FV(\psi)$ (ld. 3.25(3,4)), és

$$\forall x(\varphi \wedge \psi) \equiv \forall x\varphi \wedge \forall x\psi \qquad \exists x(\varphi \vee \psi) \equiv \exists x\varphi \vee \exists x\psi$$

bármely φ, ψ-re (ld. 3.25(1,2)). Ebben a lépésben érdemes még a következőket is használni (ld. 3.25(7,8))

$$\forall x\forall y(\varphi \vee \psi) \equiv \forall y\forall x(\varphi \vee \psi) \qquad \exists x\exists y(\varphi \wedge \psi) \equiv \exists y\exists x(\varphi \wedge \psi)$$

ha $y \in FV(\varphi) \cap FV(\psi)$ de $x \notin FV(\varphi) \cap FV(\psi)$.

(A2) nem változik,

(B3) $$\exists x\forall y\, p(x,y,y) \wedge \forall z\exists y(\forall x\neg p(x,y,x) \wedge \forall x\neg p(z,y,x))$$

(4. lépés) A kötött változókat átnevezzük úgy, hogy ne legyen két kvantor ami ugyanazt a változót köti le (v.ö. 3.56).

(A4) $$\exists x\, \neg p(x) \wedge [\exists y\, p(y) \vee \exists z(p(z) \wedge q(z))] \wedge \forall u\neg p(u)$$

(B4) $$\exists x\forall y\, p(x,y,y) \wedge \forall z\exists u(\forall v\neg p(v,u,v) \wedge \forall w\neg p(z,u,w))$$

(5. lépés) 3.57 segítségével kiküszöböljük az egzisztenciális kvantorokat (kívülről befelé), aztán az univerzális kvantorokat a formula elejére hozzuk (ez a 3. lépésben használt első négy ekvivalencia miatt nem változtat a kielégíthetőségen — most használjuk, hogy az előző lépésben átneveztük a kötött változókat: ha ezt nem tettük volna meg, akkor most lehetne a formulánk pl. $\forall xp(x) \vee \forall xq(x)$, ami nem ekvivalens $\forall x(p(x) \vee q(x))$-el).

(A4)-ből így

$$\neg p(a) \wedge [p(b) \vee (p(c) \wedge q(c))] \wedge \forall u\neg p(u)$$

majd

(A5) $$\forall u(\neg p(a) \wedge [p(b) \vee (p(c) \wedge q(c))] \wedge \neg p(u))$$

lesz, (B4)-ből pedig

$$\forall y\, p(a,y,y) \wedge \forall z(\forall v \neg p(v,f(z),v) \wedge \forall w \neg p(z,f(z),w))$$

amiből

$$\text{(B5)} \qquad \forall y \forall z \forall v \forall w[p(a,y,y) \wedge \neg p(v,f(z),v) \wedge \neg p(z,f(z),w)]$$

(6. lépés) Az előző lépésben kapott prenex formula mátrixát konjunktív normálformára hozzuk (úgy mint propozicionális logikában).

(A5)-ből

$$\text{(A6)} \qquad \forall u(\neg p(a) \wedge (p(b) \vee p(c)) \wedge (p(b) \vee q(c)) \wedge \neg p(u))$$

lesz, (B5) változatlan.

(7. lépés [nem muszáj, de hasznos]) A mátrix egyszerűsítése. Pl. ha az egyik „éselendő" (literálisok diszjunkciója) $l \vee \varphi \vee l$ (ahol l egy literális), akkor az l egyik előfordulását töröljük. Ha φ és ψ két olyan éselendő, hogy φ univerzális lezártjából következik ψ univerzális lezártja (vagyis ha $\varphi \models \psi$), akkor ψ-t töröljük. Speciáisan ha az egyik éselendő érvényes (pl. $r(x,f(z)) \vee p(x) \vee \neg r(x,f(z))$), akkor azt töröljük.

Ez a lépés egyik példát sem érinti.

(8. lépés) Átírjuk clause-halmaz alakba (csak mert ebben az alakban lehet majd a rezolúciót alkalmazni): elhagyjuk a formula elejéről az univerzális kvantorokat (ez nem probléma, mert tudjuk, hogy a mátrix minden változója univerzálisan van lekötve, az univerzális kvantorok sorrendje pedig nem számít (ld. 3.25.7), és a mátrixot clause-halmaz alakban írjuk (mint propozicionális logikában).

(A6)-ból így

$$\text{(A8)} \qquad \{\{\neg p(a)\}, \{p(b), p(c)\}, \{p(b), q(c)\}, \{\neg p(u)\}\},$$

(B5)-ből pedig

$$\text{(B8)} \qquad \{\{p(a,y,y)\}, \{\neg p(v,f(z),v)\}, \{p(z,f(z),w)\}\}$$

lesz. □

Az a célunk, hogy eljárást adjunk elsőrendű formulahalmazok kielégíthetőségének vizsgálatára (nem az eldöntésére, mert ilyen eljárás nincs). Ennek első lépése a fenti tétel. A következő az, hogy SCNF mondatok (vagy ami ugyanaz, clause-halmazok) kielégíthetőségének problémáját visszavezetjük propozicionális formulahalmazok kielégíthetőségére.

3.8. Herbrand Először azt látjuk be, hogy egy SCNF mondatnak pontosan akkor van modellje, ha van egy nagyon speciális modellje, nevezetesen egy olyan, aminek az elemei a mondat nyelvének term-jei.

3.61. Definíció (Herbrand univerzum)**.** Egy Σ formula- (vagy clause-) halmaz nyelve az a legszűkebb $\mathcal{L}$ nyelv, amire $\Sigma \subseteq Form_{\mathcal{L}}$ (itt és a továbbiakban az elsőrendű clause-halmazokat is formulának tekintjük).

Legyen $\mathcal{L}$ a Σ formulahalmaz nyelve. Ha $\mathcal{L}$ nem tartalmaz konstanst, akkor tegyük bele a c konstanst. A Σ formulahalmazhoz tartozó *Herbrand univerzum*, avagy Σ Herbrand univerzuma (jelölés: $H(\Sigma)$) $\mathcal{L}$ változómentes termjeiből áll, azaz $H(\Sigma) = \{\, t \in Term_{\mathcal{L}} : FV(t) = \emptyset \,\}$. A φ formula Herbrand-univerzuma $H(\varphi) \overset{\text{def}}{=} H(\{\varphi\})$.

Tehát ha Σ-ban előfordul függvényjel, akkor $H(\Sigma)$ biztosan végtelen lesz.

3.62. Példák.

$$H(\forall y(r(c,d) \vee r(y,c)) = H(\{\{r(c,d), r(y,c)\}\}) = \{c,d\},$$
$$H(\forall x \forall y(r(x, f(x,y))) = H(\{\{r(x, f(x,y))\}\})$$
$$= \{c, f(c,c), f(c, f(c,c)), f(f(c,c),c), f(f(c,c), f(c,c)), \dots\}.$$

3.63. Definíció (Herbrand modell)**.** Legyen $\mathcal{M}$ egy $\mathcal{L}$-struktúra, ahol $\mathcal{L}$ a Σ formulahalmaz nyelve (de tartalmazza a c konstanst ha más konstanst nem). Az $\mathcal{M}$ *Herbrand-modell* Σ-hoz, ha a következő két feltétel teljesül:

(1) $\mathcal{M}$ univerzuma $H(\Sigma)$
(2) ha a konstans $\mathcal{L}$-ben, akkor $a^{\mathcal{M}} = a$, és ha f n-argumentumú függvényjel $\mathcal{L}$-ben, akkor minden $m_1, \dots, m_n \in M$-re $f^{\mathcal{M}}(m_1, \dots, m_n) = f(m_1, \dots, m_n)$.

$\mathcal{M}$ Herbrand-modell a φ formulához, ha Herbrand-modell a $\{\varphi\}$ formulahalmazhoz.

Tehát egy formulahalmaz külöböző Herbrand modelljei csak a relációjelek jelentésében térhetnek el.

3.64. Gyakorlat. Ha $\mathcal{M}$ Herbrand-modell a φ formulához, akkor minden $t \in H(\varphi)$-re $t^{\mathcal{M}} = t$.

Be fogjuk látni, hogy egy SCNF mondat pontosan akkor kielégíthető, ha van hozzá Herbrand-modell, amiben igaz. Ehhez szükségünk lesz néhány definícióra és egyszerű állításra.

3.65. Definíció (Részmodell)**.** Legyen $\mathcal{M}$ és $\mathcal{N}$ két $\mathcal{L}$-modell. $\mathcal{M}$ *részmodell*je $\mathcal{N}$-nek (jelölés: $\mathcal{M} \subseteq \mathcal{N}$), ha az alábbi feltételek teljesülnek:

(1) $M \subseteq N$
(2) minden $c \in \mathcal{L}$ konstansra $c^{\mathcal{M}} = c^{\mathcal{N}}$
(3) minden $f \in \mathcal{L}$ függvényjelre $f^{\mathcal{M}} = f^{\mathcal{N}} \restriction M^{\rho f}$
(4) minden $r \in \mathcal{L}$ relációjelre $r^{\mathcal{M}} = r^{\mathcal{N}} \cap M^{\rho r}$, azaz $m_1, \dots, m_{\rho(r)} \in M$-re $\langle m_1, \dots, m_{\rho r} \rangle \in r^{\mathcal{M}} \iff \langle m_1, \dots, m_{\rho r} \rangle \in r^{\mathcal{N}}$.

3.66. Példa. Legyen $\mathcal{N} = \langle \mathbb{N}, \leq^{\mathcal{N}}, +^{\mathcal{N}}, \cdot^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}} \rangle$, ahol $\mathbb{N}$ a természetes számok halmaza, $\leq^{\mathcal{N}}$ a természetes számok szokásos rendezése, $+^{\mathcal{N}}$ a szokásos összadás függvény a természetes számokon, s.í.t. és legyen $\mathcal{Z} = \langle \mathbb{Z}, \leq^{\mathcal{Z}}, +^{\mathcal{Z}}, \cdot^{\mathcal{Z}}, 0^{\mathcal{Z}}, 1^{\mathcal{Z}} \rangle$, ahol $\mathbb{Z}$ az egész számok halmaza, $\leq^{\mathcal{Z}}$ az egész számok szokásos rendezése, $+^{\mathcal{Z}}$ a szokásos összadás függvény az egész számokon, s.í.t. Akkor $\mathcal{N} \subseteq \mathcal{Z}$. Ez a példa mutatja, hogy egy modell részmodelljében lehet valami igaz úgy, hogy a modellben nem, vagy fordítva. Pl. $\forall x(0 = x \vee 0 < x)$ igaz $\mathcal{N}$-ben de nem igaz $\mathcal{Z}$-ben, $\forall x \exists y(x + y = 0)$ igaz $\mathcal{Z}$-ben, de nem igaz $\mathcal{N}$-ben.

$\mathcal{Z}_3$, az egész számok $\mod 3$ maradékosztályainak modellje (az ott szokásos $\leq$-val és műveletekkel) *nem* részmodellje $\mathcal{Z}$-nek, pl. mert $+^{\mathcal{Z}_3} \neq +^{\mathcal{Z}} \restriction \{0,1,2\}^2$ ($\mathcal{Z}_3$ univerzuma nem is zárt $+^{\mathcal{Z}}$-re).

3.67. Definíció. *Kvantormentes* egy formula ha atomi formulákból épül fel $\neg$ és $\wedge$ segítségével (azaz pontosan akkor, ha nem szerepel benne kvantor). *Univerzális* egy formula, ha kvantormentes formulákból épül fel $\wedge$, $\vee$ és $\forall$ segítségével. *Egzisztenciális* egy formula, ha kvantormentes formulákból épül fel $\wedge$, $\vee$ és $\exists$ segítségével.

3.68. Példa. A SCNF formulák univerzálisak (mert a mátrixuk kvantormentes, és arra csak univerzális kvantorokat alkalmazunk).

3.69. Tétel. *Ha φ univerzális formula és $\mathcal{M} \subseteq \mathcal{N}$, akkor*

$$\mathcal{N} \models \varphi[\sigma] \Rightarrow \mathcal{M} \models \varphi[\sigma]$$

minden $\mathcal{M}$-hez tartozó σ kiértékelésre.

Biz. Először is, a részmodellség definíciójából term-indukcióval könnyen jön, hogy

$$(\dagger) \qquad t^{\mathcal{M}}[\sigma] = t^{\mathcal{N}}[\sigma]$$

minden $\mathcal{M}$-hez tartozó σ kiértékelésre. Másodszor: a tétel állításának következő erősítése:

$$(*) \qquad \mathcal{N} \models \varphi[\sigma] \iff \mathcal{M} \models \varphi[\sigma] \qquad \text{minden } \mathcal{M}\text{-hez tartozó } \sigma \text{ kiértékelésre.}$$

igaz kvantormentes formulákra, mert

$$\mathcal{M} \models t_1 = t_2[\sigma] \iff t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma] \iff t_1^{\mathcal{N}}[\sigma] = t_2^{\mathcal{N}}[\sigma] \iff \mathcal{N} \models t_1 = t_2[\sigma]$$

(a középső ekvivalencia ($\dagger$) miatt igaz) és

$$\begin{aligned}\mathcal{M} \models r(t_1, \dots, t_n)[\sigma] &\iff \langle\, t_1^{\mathcal{M}}[\sigma], \dots, t_n^{\mathcal{M}}[\sigma] \,\rangle \in r^{\mathcal{M}} \\ &\iff \langle\, t_1^{\mathcal{N}}[\sigma], \dots, t_n^{\mathcal{N}}[\sigma] \,\rangle \in r^{\mathcal{N}} \iff \mathcal{N} \models r(t_1, \dots, t_n)[\sigma]\end{aligned}$$

(a középső ekvivalencia ($\dagger$) és 3.65(4) miatt igaz) és $\neg$-ra és $\wedge$-ra triviálisan öröklődik. (Azért kellett ($*$) a tételbeli állítás helyett, mert az nem öröklődik $\neg$-ra.)

Végül: mivel $\wedge$-re és $\vee$-ra könnyen látható, hogy öröklődik az állítás, annak belátásához, hogy minden univerzális formulára igaz, elég megnézni, hogy $\forall$-re öröklődik. Tegyük fel, hogy φ-re igaz az állítás. Akkor

$$\begin{aligned}\mathcal{N} \models \forall x\varphi[\sigma] &\iff \text{minden } N\text{-beli } m\text{-re } \mathcal{N} \models \varphi[\sigma(x/m)] \\ &\Rightarrow \text{minden } M\text{-beli } m\text{-re } \mathcal{N} \models \varphi[\sigma(x/m)] \\ &\Rightarrow \text{minden } M\text{-beli } m\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)] \qquad \text{ind. felt. miatt} \\ &\iff \mathcal{M} \models \forall x\varphi[\sigma].\end{aligned}$$

□

3.70. Definíció (Homomorfizmus/Izomorfizmus)**.** Legyen M és $\mathcal{N}$ két $\mathcal{L}$-modell. A $\pi : M \longrightarrow N$ függvény homomorfizmus $\mathcal{M}$-ből $\mathcal{N}$-re (izomorfizmus $\mathcal{M}$-ből $\mathcal{N}$-be), ha

(1) π ráképezés (injektív ráképezés, azaz bijekció) M-ből N-re
(2) minden $c \in \mathcal{L}$ konstansra $\pi(c^{\mathcal{M}}) = c^{\mathcal{N}}$
(3) minden $f \in \mathcal{L}$ függvényjelre és minden $m_1, \dots, m_{\rho f} \in M$-re

$$\pi f^{\mathcal{M}}(m_1, \dots, m_{\rho f}) = f^{\mathcal{N}}(\pi m_1, \dots, \pi m_{\rho f})$$

(4) minden $r \in \mathcal{L}$ relációjelre és minden $m_1, \dots, m_{\rho r} \in M$-re

$$\langle\, m_1, \dots, m_{\rho r} \,\rangle \in r^{\mathcal{M}} \iff \langle\, \pi m_1, \dots, \pi m_{\rho r} \,\rangle \in r^{\mathcal{N}}.$$

$\mathcal{N}$ homomorf képe $\mathcal{M}$-nek ha van homorfizmus $\mathcal{M}$-ből $\mathcal{N}$-re, és $\mathcal{M}$, $\mathcal{N}$ izomorfak (jelölés: $\mathcal{M} \cong \mathcal{N}$), ha van izomorfizmus $\mathcal{M}$-ből $\mathcal{N}$-be.

Ez pontosan az a homo- és izomorfizmus-fogalom, amit algebrában (pl. csoportokra) ismerünk, kivéve, hogy a csoportok (és más algebraosztályok) nyelvében nincsenek relációjelek, ezért a 4. kikötésre ott nincs szükség.

3.71. Példa. Az egész számok modelljének *nem* homomorf képe $\mathcal{Z}_3$ (a $\mod 3$ maradékosztályok modellje) (ha utóbbin $<$ jelentése $\{\langle 0,1\rangle,\langle 1,2\rangle,\langle 0,2\rangle\}$) (ez látszik pl. a következő tételből, mert a $\exists x\exists y\exists z\exists v(x<y\wedge y<z\wedge z<v)$ mondat igaz $\mathcal{Z}$-ben de nem igaz $\mathcal{Z}_3$-ban), de ha elhagyjuk belőlük a $<$ relációt, akkor igen, mert $z\mapsto z \mod 3$ homomorfizmus.

3.72. Tétel. *Legyen $\varphi(x_1,\dots,x_n)\in Form_{\mathcal{L}}$ olyan, hogy nem fordul elő benne egyenlőség, és $\mathcal{M}$, $\mathcal{N}$ $\mathcal{L}$-modellek. Ha π homomorfizmus $\mathcal{M}$-ből $\mathcal{N}$-re, akkor minden $m_1,\dots,m_n\in M$-re*

$$\mathcal{M}\models\varphi(x_1,\dots,x_n)[m_1,\dots,m_n]\iff\mathcal{N}\models\varphi(x_1,\dots,x_n)[\pi m_1,\dots,\pi m_n].$$

Ha π izomorfizmus $\mathcal{M}$-ből $\mathcal{N}$-be, akkor ez minden formulára (tehát az egyenlőséget tartalmazókra is) igaz.

Biz. Először term-indukcióval belátjuk, hogy

(†) $\quad\pi(t^{\mathcal{M}}[\sigma])=t^{\mathcal{N}}[\pi\circ\sigma]\quad$ minden $t\in Term_{\mathcal{L}}$-re és $\mathcal{M}$-hez tartozó σ kiértékelésre

(itt $\circ$ függvénykompozíciót jelöl, tehát $\pi\circ\sigma$ az az $\mathcal{N}$-hez tartozó kiértékelés, ami az $x\in Var$-hoz $\pi(\sigma(x))\in N$-et rendeli.) Ha t a $c\in\mathcal{L}$ konstans, akkor $\pi(t^{\mathcal{M}}[\sigma])=\pi(c^{\mathcal{M}})=c^{\mathcal{N}}=t^{\mathcal{N}}[\pi\circ\sigma]$; ha t az $x\in Var$, akkor $\pi(t^{\mathcal{M}}[\sigma])=\pi(\sigma(x))=(\pi\circ\sigma)(x)=t^{\mathcal{N}}[\pi\circ\sigma]$; végül ha $f\in\mathcal{L}$ n-argumentumú függvényjel, $t_1,\dots,t_n\in Term_{\mathcal{L}}$-re igaz az állítás, és t az $f(t_1,\dots,t_n)$ term, akkor $\pi(t^{\mathcal{M}}[\sigma])=\pi(f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma],\dots,t_n^{\mathcal{M}}[\sigma]))=f^{\mathcal{N}}(\pi(t_1^{\mathcal{M}}[\sigma]),\dots,\pi(t_n^{\mathcal{M}}[\sigma]))=f^{\mathcal{N}}(t_1^{\mathcal{N}}[\pi\circ\sigma],\dots,t_n^{\mathcal{N}}[\pi\circ\sigma])=t^{\mathcal{N}}[\pi\circ\sigma]$. Itt az első és utolsó egyenlőségben 3.10-et, a második egyenlőségben 3.70(3)-at, a harmadik egyenlőségben pedig az indukciós feltevést használtuk. Ezzel beláttuk (†)-et.

Most formulaindukcióval belátjuk, hogy

$$\mathcal{M}\models\varphi[\sigma]\iff\mathcal{N}\models\varphi[\pi\circ\sigma]$$

minden (egyenlőségmentes ha π csak homomorfizmus) $\varphi\in Form_{\mathcal{L}}$-ra és $\mathcal{M}$-hez tartozó σ kiértékelésre — amiből már persze következik a tétel.

Ha φ a $t_1=t_2$ formula, akkor

$$\begin{aligned}\mathcal{M}\models\varphi[\sigma]\iff t_1^{\mathcal{M}}[\sigma]=t_2^{\mathcal{M}}[\sigma]&\iff\pi(t_1^{\mathcal{M}}[\sigma])=\pi(t_2^{\mathcal{M}}[\sigma])\\&\iff t_1^{\mathcal{N}}[\pi\circ\sigma]=t_2^{\mathcal{N}}[\pi\circ\sigma]\iff\mathcal{N}\models\varphi[\pi\circ\sigma]\end{aligned}$$

(a második ekvivalencia π injektivitása, a harmadik pedig (†) miatt igaz); ha pedig φ az $r(t_1,\dots,t_n)$ formula, akkor

$$\begin{aligned}\mathcal{M}\models\varphi[\sigma]\iff\langle t_1^{\mathcal{M}}[\sigma],\dots,t_n^{\mathcal{M}}[\sigma]\rangle\in r^{\mathcal{M}}&\iff\langle\pi(t_1^{\mathcal{M}}[\sigma]),\dots,\pi(t_n^{\mathcal{M}}[\sigma])\rangle\in r^{\mathcal{N}}\\&\iff\langle t_1^{\mathcal{N}}[\pi\circ\sigma],\dots,t_n^{\mathcal{N}}[\pi\circ\sigma]\rangle\in r^{\mathcal{N}}\iff\mathcal{N}\models\varphi[\pi\circ\sigma],\end{aligned}$$

(a második ekvivalenciában 3.70(4)-et, a harmadik ekvivalenciában (†)-et használtuk). $\neg$-ra és $\wedge$-ra triviális az öröklődés, úgyhogy tegyük fel, hogy φ a $\forall x\psi$ formula, és ψ-re már beláttuk az állítást. Akkor

$$\begin{aligned}\mathcal{M}\models\varphi[\sigma]&\iff\text{minden } M\text{-beli } m\text{-re } \mathcal{M}\models\psi[\sigma(x/m)]\\&\iff\text{minden } M\text{-beli } m\text{-re } \mathcal{N}\models\psi[\pi\circ(\sigma(x/m))]&&\text{ind. felt. miatt}\\&\iff\text{minden } M\text{-beli } m\text{-re } \mathcal{N}\models\psi[(\pi\circ\sigma)(x/\pi(m))]\\&\iff\text{minden } N\text{-beli } n\text{-re } \mathcal{N}\models\psi[(\pi\circ\sigma)(x/n)]&&\text{mert } \pi \text{ ráképezés}\\&\iff\mathcal{N}\models\varphi[\pi\circ\sigma]\end{aligned}$$

$\square$

3.73. Tétel (Herbrand I.). *Egy SCNF-ban levő φ egyenlőségmentes mondat pontosan akkor kielégíthető, ha igaz egy Herbrand-modelljében (azaz ha van Herbrand-modell φ-hez amiben φ igaz).*

Biz. ($\Leftarrow$) triviális, hiszen ha φ igaz egy Herbrand-modelljében, akkor van modellje, tehát kielégíthető.
($\Rightarrow$) Tegyük fel, hogy $\mathcal{M} \models \varphi$, és legyen $\mathcal{L}$ a φ nyelve, ill. ha φ-ben nem szerepel konstansjel, akkor $\mathcal{L}$-be tegyünk egyet (c), és $c^{\mathcal{M}}$ legyen M valamelyik eleme. (Persze ez a kibővített $\mathcal{M}$ továbbra is modellje φ-nek.)

Legyen $N = \{ t^{\mathcal{M}} : t \in H(\varphi) \}$.

(1) $$N \text{ az } \mathcal{M} \text{ egy részmodelljének univerzuma}$$

azaz minden $\mathcal{L}$-beli c konstansra $c^{\mathcal{M}} \in N$ és minden $\mathcal{L}$-beli f függvényjelre N zárt $f^{\mathcal{M}}$-re. Az első állítás ebből nyilvánvaló mert ha $c \in \mathcal{L}$ konstans, akkor $c \in H(\varphi)$, a második pedig azért igaz, mert ha $f \in \mathcal{L}$ k-argumentumú függvényjel és $n_1, \dots, n_k \in N$, akkor van olyan $t_1, \dots, t_k \in H(\varphi)$, hogy $t_1^{\mathcal{M}} = n_1, \dots, t_k^{\mathcal{M}} = n_k$, és akkor $f^{\mathcal{M}}(n_1, \dots, n_k) = f^{M}(t_1^{\mathcal{M}}, \dots, t_k^{\mathcal{M}}) = f(t_1, \dots, t_k)^{\mathcal{M}} \in N$, mivel $f(t_1, \dots, t_k) \in H(\varphi)$.

Legyen $\mathcal{N}$ az $\mathcal{M}$-nek az a részmodellje, aminek N az univerzuma ((1) miatt van ilyen, és a részmodellség definíciójából látható, hogy csak egy). Vagyis $\mathcal{N}$ univerzuma N, minden $c \in \mathcal{L}$ konstansra $c^{\mathcal{N}} = c^{\mathcal{M}}$, minden $f \in \mathcal{L}$ függvényjelre $f^{\mathcal{N}} = f^{\mathcal{M}} \restriction N^{\rho(f)}$ és minden $r \in \mathcal{L}$ relációjelre $r^{\mathcal{N}} = r^{\mathcal{M}} \cap N^{\rho(r)}$. Mivel φ univerzális,

(2) $$\mathcal{N} \models \varphi$$

3.69 miatt. Végül: $\mathcal{H}$ legyen a következő Herbrand-modell φ-hez. Ha $r \in \mathcal{L}$ k-argumentumú relációjel és $t_1, \dots, t_k \in H(\varphi)$, $\langle t_1, \dots, t_k \rangle \in r^{\mathcal{H}}$ pontosan akkor, ha $\langle t_1^{\mathcal{N}}, \dots, t_k^{\mathcal{N}} \rangle \in r^{\mathcal{N}}$ (ezzel $\mathcal{H}$ definiálva van, mert az univerzum és a konstansok és függvényjelek értéke minden Herbrand-modellben ugyanaz). Azt állítjuk, hogy $\mathcal{H} \models \varphi$. De ez következik (2)-ből 3.72 miatt, ha belátjuk, hogy az a $H(\varphi)$-ből N-be képező π függvény amit $\pi(t) = t^{\mathcal{N}}$ definiál, homomorfizmus $\mathcal{H}$-ból $\mathcal{N}$-re.

N definíciója miatt π ráképezés, és $r^{\mathcal{H}}$ definíciója miatt 3.70(4) is teljesül. 3.70(2) igaz, mert ha $c \in \mathcal{L}$ konstans, akkor $\pi(c^{\mathcal{H}}) = \pi(c) = c^{\mathcal{N}}$. Végül ha $f \in \mathcal{L}$ k-argumentumú függvényjel és $t_1, \dots, t_k \in H(\varphi)$, akkor $\pi(f^{\mathcal{H}}(t_1, \dots, t_k)) = \pi(f^{\mathcal{H}}(t_1^{\mathcal{H}}, \dots, t_k^{\mathcal{H}})) = \pi(f(t_1, \dots, t_k)^{\mathcal{H}}) = \pi(f(t_1, \dots, t_k)) = f(t_1, \dots, t_k)^{\mathcal{N}} = f^{\mathcal{N}}(t_1^{\mathcal{N}}, \dots, t_k^{\mathcal{N}}) = f^{\mathcal{N}}(\pi(t_1), \dots, \pi(t_k))$. Az első és a harmadik egyenlőségben azt használtuk, hogy Herbrand modellben minden változómentes term értéke saját maga (3.64). $\square$

A tétel feltételei közül nem hagyható el, hogy φ egyenlőségmentes: pl. a $c = d$ SCNF mondat kielégíthető, de nem igaz egyik Herbrand-modelljében sem.

3.74. Állítás. *Ha $\varphi(x_1, \dots, x_n) \in Form_{\mathcal{L}}$, $t_1, \dots, t_n \in Term_{\mathcal{L}}$, σ az $\mathcal{M}$ $\mathcal{L}$-modellhez tartozó kiértékelés és $t_i^{\mathcal{M}}[\sigma] = \sigma(x_i)$ $(i = 1,\dots,n)$, akkor*

$$\mathcal{M} \models \varphi(x_1, \dots, x_n)[\sigma] \iff \mathcal{M} \models \varphi(x_1/t_1, \dots, x_n/t_n)[\sigma]$$

feltéve, hogy $1 \le i \le n$-re t_i behelyettesíthető φ-ben x_i helyére, azaz t_i egy szabad változója sem válik kötötté a behelyettesítés során. (Ez a feltétel biztosan áll, ha t_i-k változómentes termek.)

Biz. Egyszerű term- majd formulaindukció. $\square$

3.75. Definíció. Egy $\mathcal{L}$ elsőrendű nyelv egy *propozicionális modellje* olyan függvény, ami $\mathcal{L}$ minden változómentes atomi formulájához 0-t vagy 1-et rendel.

Legyen $\mathcal{M}$ az $\mathcal{L}$ nyelv egy propozicionális modellje, Σ pedig egyenlőség- és változómentes $\mathcal{L}$-mondatok halmaza. (Tehát $\mathcal{L}$ elemei relációs atomi mondatokból (relációjelek kitöltve változómentes term-ekkel) épülnek fel a propozicionális logika konnektívumaival.) Σ igaz $\mathcal{M}$-ben (jelölés: $\mathcal{M} \models_0 \Sigma$), ha Σ minden eleme igaz $\mathcal{M}$-ben propozicionális értelemben, azaz úgy, hogy az atomi mondatokat propozicionális atomi formuláknak tekintjük. Σ kielégíthető propozicionális értelemben, ha van olyan propozicionális modell, amiben igaz (ezt úgy is mondjuk, hogy van propozicionális modellje).

3.76. Definíció. A $\varphi = \forall x_1 \ldots \forall x_n \psi(x_1, \ldots, x_n)$ SCNF mondat *változómentes instanciái*:

$$G(\varphi) = \{\, \psi(x_1/t_1, \ldots, x_n/t_n) : t_1, \ldots, t_n \in H(\varphi) \,\}$$

3.77. Tétel (Herbrand II.). *Legyen φ egyenlőségmentes SCNF mondat. Akkor*

$$\varphi \text{ kielégíthető} \iff G(\varphi) \text{ kielégíthető propozicionális értelemben.}$$

Biz. Először is,

(†)

$$G(\varphi) \text{ igaz egy Herbrand-modelljében} \iff G(\varphi) \text{ kielégíthető propozicionális értelemben.}$$

Ui. ha $G(\varphi)$ igaz a $\mathcal{H}$ Herbrand-modellben, akkor legyen $\mathcal{M}$ az a propozicionális modell, ami az $r(t_1, \ldots, t_n)$ atomi mondathoz pontosan akkor rendel 1-et, ha $\langle\, t_1, \ldots, t_n \,\rangle \in r^{\mathcal{H}}$. Fordítva, ha $G(\varphi)$ igaz az $\mathcal{M}$ propozicionális modellben, akkor legyen $\mathcal{H}$ az a Herbrand-modell, amiben a relációjelek jelentését úgy definiáljuk, hogy $r^{\mathcal{H}} = \{\, \langle\, t_1, \ldots, t_n \,\rangle : \mathcal{M}(r(t_1, \ldots, t_n)) = 1 \,\}$.

Mindkét esetben a $G(\varphi)$-ben előforduló minden atomi mondat pontosan akkor igaz $\mathcal{H}$-ban, ha igaz $\mathcal{M}$-ben (így definiáltuk az első esetben $\mathcal{M}$-et $\mathcal{H}$-ból, a másodikban $\mathcal{H}$-ból $\mathcal{M}$-et); mivel a $G(\varphi)$-beli mondatok az atomiakból a propozicionális konnektívumokkal ($\neg$-el $\wedge$-sel és $\vee$-gyal) épülnek fel, és ezek értékelési szabályai propozicionális logkában és elsőrendű logikában megegyeznek, $G(\varphi)$ minden mondata pontosan akkor igaz $\mathcal{H}$-ban, ha igaz $\mathcal{M}$-ben. Ezzel beláttuk (†)-et.

Most már rátérhetünk a tétel állításának bizonyítására, de előbb még vegyük észre, hogy egy modell pontosan akkor Herbrand-modell φ-hez, ha Herbrand-modell $G(\varphi)$-hez (mert φ nyelve (plusz a c konstans ha ez a nyelv nem tartalmaz konstanst) és $G(\varphi)$ nyelve ugyanaz). Ezért a bizonyításban egyszerűen „Herbrand-modell"-t írunk „Herbrand-modell φ-hez" és „Herbrand-modell $G(\varphi)$-hez" helyett.

3.73 miatt φ pontosan akkor kielégíthető, ha igaz egy $\mathcal{H}$ Herbrand-modellben, azaz ha van $\mathcal{H}$ Herbrand-modell, hogy $\mathcal{H} \models \forall x_1 \ldots \forall x_n \psi(x_1, \ldots, x_n)$, azaz ha van $\mathcal{H}$ Herbrand-modell, hogy minden $t_1, \ldots, t_n \in H(\varphi)$-re $\mathcal{H} \models \psi(x_1, \ldots, x_n)[t_1, \ldots, t_n]$, azaz (3.74 miatt) ha van $\mathcal{H}$ Herbrand-modell, hogy $\mathcal{H} \models \psi(x_1/t_1, \ldots, x_n/t_n)$ minden $t_1, \ldots, t_n \in H(\varphi)$-re, azaz ha van $\mathcal{H}$ Herbrand-modell, hogy $\mathcal{H} \models G(\varphi)$, ami viszont (†) miatt ekvivalens azzal, hogy $G(\varphi)$ kielégíthető propozicionális értelemben. □

3.78. Következmény. *Ha φ egyenlőségmentes SCNF mondat, akkor*

$$\varphi \text{ kielégíthetetlen} \iff$$
$$G(\varphi)\text{-nak van véges része, ami propozicionális értelemben kielégíthetetlen.}$$

Biz. A tételből és a propozicionális logika kompaktsági tételéből (2.38) nyilvánvaló. □

Tehát elsőrendű fromulák kielégíthetetlenségének problémáját 3.60 és 3.77 segítségével visszavezettük propozicionális formulahalmazok kielégíthetetlenségére; amit viszont már tudunk kezelni, például rezolúcióval (ha előbb átírjuk őket clause-halmaz alakba). Vigyázat, ezzel nem kaptunk eldöntési algoritmus elsőrendű formulák kielégíthetőségére. Ha ψ a φ formulából az 3.60-el kapott $SCNF$ (ami tehát pontosan kielégíthető, ha φ az), akkor $G(\psi)$ rendszerint végtelen. Ezért ha φ kielégíthetetlen (és így $G(\psi)$ kielégíthetetlen propozicionális értelemben), akkor a rezolúció ezt jelzi[6], mert $G(\psi)$-ből levezethető rezolúcióval az üres clause. De ha φ kielégíthető, akkor bármilyen stratégiával is működtetjük a rezolúciót, az algoritmus nem fog megállni.

3.9. Elsőrendű rezolúció Ebben a részben (ha mást nem mondunk) kizárólag egyenlőségmentes SCNF formulákkal foglalkozunk, és azokról is feltesszük, hogy clause-halmaz alakban vannak írva.

Az előző részben láttuk, hogyan lehet SCNF mondatok kielégíthetetlenségét vizsgálni két lépésben: először változómentes instanciákat csinálunk, aztán ezekből (mint propozicionális formulákból) próbáljuk rezolúcióval levezetni az üres clause-t. Az elsőrendű rezolúció a két lépést egybevonja, és attól lesz viszonylag praktikus módszer kelégíthetelenség vizsgálatára, hogy csak azokat a változómentes instanciákat hozza létre, amiket aztán lehet is rezolválni. (Ez az ötlet: a kivitelezés egy kicsit más.)

3.79. Példa. Legyen φ a $\forall x(r(x) \wedge \neg r(f(x)))$ mondat. φ Herbrand-univerzuma $\{\, c, f(c), f(f(c)), \dots \}$, tehát

$$G(\varphi) = \{r(c) \wedge \neg r(f(c)), r(f(c)) \wedge \neg r(f(f(c))), \dots\},$$

clause-halmaz alakban

$$\{\{r(c)\}, \{\neg r(f(c))\}, \{r(f(c))\}, \{\neg r(f(f(c)))\}, \dots\}.$$

A második és harmadik clause rezolvense az üres clause, tehát φ kielégíthetetlen; de ehhez az egylépéses rezolúcióhoz előbb egy végtelen formulahalmazt ($G(\varphi)$-t) kellett generálnunk.

Elsőrendű rezolúcióval ezzel szemben így megy a dolog. Vesszük φ clause-halmaz alakját, vagyis $\{\{r(x)\}, \{\neg r(f(x))\}\}$-et, és megnézzük, hogy van-e benne két clause, ami rezolválható *lenne* ha a bennük szereplő változókat (külön-külön) változómentes termekkel helyettesítenénk be valahogy. Ha igen, akkor elvégezzük ezt a helyettesítést a két clause-ban, és rezolváljuk az így kapott instanciákat. A példában a válasz igen, pl. az első clause-ban $x/f(c)$ helyettesítés $\{r(f(c))\}$-t, az x/c helyettesítés második clause-ból $\{\neg r(f(c))\}$-t csinál, ez a két instancia már rezolválható, és az eredmény az üres clause.

3.80. Definíció. *Helyettesítés*en olyan véges[7] függvényt értünk, ami változókhoz termeket rendel. Ha A egy kifejezés (formula vagy term) és s egy helyettesítés, akkor As az a kifejezés, amit úgy kapunk A-ból, hogy benne minden s értelmezési tartományában levő x változó szabad előfordulásai helyébe $s(x)$-et helyettesítjük. Ha C kifejezések egy halmaza, $Cs = \{\, As : A \in C \,\}$. Azt a helyettesítést, ami x_1-hez t_1-et, ..., x_n-hez t_n-et rendeli, $x_1/t_1, \dots x_n/t_n$-nel jelöljük. (Ezt a jelölést eddig is használtuk.)

Az s helyettesítés *átnevezés* ha injektív és $\operatorname{ran} s \subseteq Var$ ($\operatorname{ran} s$ az s értékkészlete).

Kifejezések egy C halmaza *egyesíthető*, ha van olyan s helyettesítés, hogy Cs egyelemű.

[6] ha ügyesen csináljuk! `:-(`

[7] Egy függvény véges, ha az értelmezési tartománya véges.

Az elsőrendű rezolúció definíciójában az egyetlen igazi újdonság relációs atomi formulák egyesítése lesz, ezért először ezt nézzük meg.

Legyen α és β két relációs atomi formula. Ha különböző relációjelek szerepelnek bennük, akkor nem egyesíthetők. Máskülönben legyen az α-beli t_1 és β-beli t_2 az első (balról jobbra haladva) term amiben különböznek. Ha $t_1 \in Var$ és $t_1 \notin FV(t_2)$, akkor legyen $s_1 = t_1/t_2$; különben, ha $t_2 \in Var$ és $t_2 \notin FV(t_1)$, akkor legyen $s_1 = t_2/t_1$; különben α és β nem egyesíthető. Ha nem kaptuk azt a választ, hogy α és β nem egyesíthető, akkor ismételjük meg ezt az eljárást αs_1 és βs_1-gyel. Ha αs_1 és βs_1-ről kijön, hogy nem egyesíthetők, akkor α és β nem egyesíthető, különben legyen s_2 a kapott helyettesítés. És így tovább. Így véges sok lépésben kijön, hogy nem egyesíthetők, vagy kapunk egy helyesttesítés-sorozatot (mondjuk $s_1, \ldots, s_m$), úgy, hogy $\alpha s_1 \ldots s_m = \beta s_1 \ldots s_m$. Ilyenkor α és β egyesíthető, és az $\langle s_1 \ldots s_m \rangle$ helyettesítés-sorozatot α és β *legáltalánosabb egyesítőjének*[8] nevezik.

Vigyázat: helyettesítés és helyettesítés-sorozat nem összetévesztendő: az $x/y, y/x$ helyettesítés x-re alkalmazva y-t, ad, az $\langle x/y, y/x \rangle$ helyettesítés-sorozat viszont x-et.

3.81. Példák. (1) $\alpha = r(x)$, $\beta = r(x)$ egyesíthetők, és az mgu az üres helyettesítés-sorozat.

(2) $\alpha = r(f(y), z, c), \beta = r(x, f(y), y)$. $s_1 = x/f(y), \alpha s_1 = r(f(y), z, c), \beta s_1 = r(f(y), f(y), y)$. $s_2 = z/f(y)$, $\alpha s_1 s_2 = r(f(y), f(y), c)$, $\beta s_1 s_2 = r(f(y), f(y), y)$. $s_3 = y/c$, $\alpha s_1 s_2 s_3 = r(f(c), f(c), c)$, $\beta s_1 s_2 s_3 = r(f(c), f(c), c)$, tehát α és β egyesíthető, és $\langle x/f(y), z/f(y), y/c \rangle$ az mgu.

(3) $\alpha = r(f(y), z, c), \beta = r(x, f(y), x)$. $s_1 = x/f(y), \alpha s_1 = r(f(y), z, c), \beta s_1 = r(f(y), f(y), f(y))$. $s_2 = z/f(y)$, $\alpha s_1 s_2 = r(f(y), f(y), c)$, $\beta s_1 s_2 = r(f(y), f(y), f(y))$. Nem tudjuk folytatni, mert az első eltérés helyén egyik atomi formulában sem változó áll. Tehát α, β nem egyesíthetők.

(4) $\alpha = r(f(x)), \beta = r(x)$. Nem egyesíthetők, mert bár az első eltérés helyén β-ban változó áll (x), de α-ban olyan term ($f(x)$), amiben x előfordul.

(5) $\alpha = r(f(x, y)), \beta = r(f(g(y), z))$. $s_1 = x/g(y), \alpha s_1 = r(f(g(y), y)), \beta s_1 = r(f(g(y), z))$. $s_2 = z/y$, $\alpha s_1 s_2 = r(f(g(y), y))$, $\beta s_1 s_2 = r(f(g(y), y))$, tehát egyesíthetők, és az mgu az $\langle x/g(y), z/y \rangle$ helyettesítés-sorozat.

3.82. Definíció. Legyen C és D két közös változó nélküli clause, α atomi formula, $\alpha \in C$, $\neg\beta \in D$, és tegyük fel, hogy α és β egyesíthető, és az $\langle s_1, \ldots, s_m \rangle$ helyetesítés-sorozat mgu α, β-hoz. Akkor C és D α, β szerinti rezolvense a $(Cs_1, \ldots, s_m \setminus \{\alpha s_1, \ldots, s_m\}) \cup (Ds_1, \ldots, s_m \setminus \{\beta s_1, \ldots, s_m\})$ clause.

3.83. Példa. Számoljuk ki az $\{r(x, f(x)), p(x)\}$ és a $\{\neg r(y, z), p(z)\}$ $r(x, f(x))$ és $r(y, z)$ szerinti rezolvensét (ha van). Először mgu-t keresünk: $s_1 = x/y$, $r(x, f(x))s_1 = r(y, f(y))$ és $r(y, z)s_1 = r(y, z)$; $s_2 = z/f(y)$, $r(x, f(x))s_1 s_2 = r(y, f(y))s_2 = r(y, f(y))$ és $r(y, z)s_1 s_2 = r(y, z)s_2 = r(y, f(y))$. Tehát $r(x, f(x))$ és $r(y, z)$ egyesíthetők, és $\langle x/y, z/f(y) \rangle$ az mgu. Mivel $p(x)s_1 s_2 = p(y)s_2 = p(y)$ és $p(z)s_1 s_2 = p(z)s_2 = p(f(y))$, a rezolvens a $\{p(y), p(f(y))\}$ clause.

3.84. Definíció. Ha az l_1 és l_2 literálisok egyesíthetők, $\langle s_1, \ldots, s_m \rangle$ helyettesítés-sorozat mgu l_1 és l_2-höz, l_1 és l_2 elemei a C clause-nak, akkor C l_1 és l_2 szerinti *faktora* a $Cs_1 \ldots s_m$ clause.

[8] *most general unifier*, avagy *mgu*

3.85. Példa. Az $\{r(x,y), r(x,x), r(y,y)\}$ clause $r(x,x)$ és $r(y,y)$ szerinti faktora az $\{r(y,y)\}$ clause, mert $r(x,x)$ és $r(y,y)$-t egyesíti az x/y mgu, és $\{r(x,y), r(x,x), r(y,y)\}x/y = \{r(y,y), r(y,y), r(y,y)\} = \{r(y,y)\}$.

3.86. Gyakorlat. Találjuk meg az előző példabeli $\{r(x,y), r(x,x), r(y,y)\}$ clause összes faktorát!

3.87. Definíció. Az E clause egy rezolúciós levezetése a Σ egyenlőségmentes clause-halmazból olyan véges T fa, amire igaz, hogy

- T minden csúcsa egy clause
- E a T gyökere
- T minden levele Σ egy eleme
- T minden olyan D csúcsának ami nem levél, (a) van egy gyermeke, aminek D egy faktora, vagy (b) van egy gyermeke (D'), amiből D-t a változók átnevezésével kapjuk (azaz $D = D's$, ahol s egy átnevezés), vagy (c) van két gyermeke amiknek D a rezolvense.

A levezetés hossza a nem-levél csúcsok száma. Σ-ból levezethető E ($\Sigma \vdash_R E$) ha E-nek van rezolúciós levezetése Σ-ból. Σ *cáfolható* ha $\Sigma \vdash_R \square$.

A levezetést persze nem muszáj fa alakban lerajzolni, ld. a következő példát.

3.88. Példa. Legyen Σ a $\{\{r(x), r(y)\}, \{\neg r(x), \neg r(y)\}\}$ clause-halmaz. $\Sigma \vdash_R \square$ mert:

1.	$\{r(x), r(y)\}$	adott
2.	$\{\neg r(x), \neg r(y)\}$	adott
3.	$\{r(y)\}$	1. faktora
4.	$\{\neg r(y)\}$	2. faktora
5.	$\{r(x)\}$	3. átnevezése
6.	$\square$	4,5 rezolvense

3.89. Tétel. *Legyen $\Sigma \cup \{E\}$ egyenlőségmentes clause-halmaz. Ha $\Sigma \vdash_R E$, akkor $\Sigma \models E$ (vagyis $\vdash_R$ helyes), és ha Σ kielégíthetetlen, akkor $\Sigma \vdash_R \square$ (azaz $\vdash_R$ cáfolat-teljes).*

Éppúgy mint a propozicionális rezolúció, az elsőrendű sem teljes, pl. $\emptyset \models \{r(x), \neg r(x)\}$, de $\emptyset \not\vdash_R \{r(x), \neg r(x)\}$. De ez itt sem probléma, mert elsőrendű logikában is igaz, hogy $\Sigma \models \varphi$ pontosan akkor, ha $\Sigma \cup \{\varphi\}$ kielégíthetetlen.

3.90. Példa. Be akarjuk látni, hogy $\exists x \forall y r(x,y) \models \forall y \exists x r(x,y)$. Ez pontosan akkor igaz, ha $\exists x \forall y r(x,y) \land \neg \forall y \exists x r(x,y)$ kielégíthetetlen. 3.60 segítségével csinálunk egy SCNF mondatot, ami pontosan akkor elégíthető ki, ha ez kielégíthető:

$$\exists x \forall y r(x,y) \land \exists y \forall x \neg r(x,y)$$
$$\exists x \forall y r(x,y) \land \exists v \forall u \neg r(u,v)$$
$$\forall y r(c,y) \land \forall u \neg r(u,d)$$
$$\forall y \forall u (r(c,y) \land \neg r(u,d))$$

Az így kapott SCNF mondatot átírjuk clause-halmaz alakba:

$$\{\{r(c,y)\}, \{\neg r(u,d)\}\}$$

és ebből egy lépésben levezethető az $\Box$, tehát ez a clause-halmaz kielégíthetetlen, vagyis igaz az eredeti állítás.

4. Megoldások

1.1 B hazudik, mert senki sem mondhatja magáról, hogy lókötő (mert ha az, akkor azt hazudja magáról, hogy lovag, ha meg lovag, akkor azért).

1.2 B nem lehet lovag (mert akkor lókötő is lenne), tehát lókötő, tehát hazudott, azaz nem igaz, hogy mindketten lókötők, vagyis A lovag.

1.3 Ha B lovag, akkor A lókötő. És B nem lehet lókötő, mert akkor hazugság lenne, hogy van köztük lókötő, ami ellentmond annak, hogy B az.

1.21 $\{p, \neg p\}$

1.22 $\{p \vee q, \neg p, \neg q\}$

1.23 $\{p_1 \vee \dots \vee p_{n-1}, \neg p_1, \dots, \neg p_{n-1}\}$

1.24 Igen, páratlanok igazak, párosak hamisak, vagy fordítva.

1.25
(1) Nem, pl. $\varphi = p$, $\psi = \neg p$. De fordítva persze igen.
(2) Hát persze.
(3) Nem: pl. $\varphi = p$, $\psi = \bot$.
(4) Igen.

1.26 Nem. $\mathcal{M}(p) = 0, \mathcal{M}(q) = 1$ (nem esik az eső, viszek esőkabátot) modellje a premisszáknak, de nem modellje a konklúziónak.

1.27

A	B	$\neg A$	$\neg B$	$\neg A \vee \neg B$	$B \leftrightarrow (\neg A \vee \neg B)$
0	0	1	1	1	0
0	1	1	0	1	1
1	0	0	1	1	0
1	1	0	0	0	0

Vagyis B lovag, A lókötő. Ahogy eredetileg is gondoltuk: Ha B lovag, akkor A lókötő. És B nem lehet lókötő, mert akkor hazugság lenne, hogy van köztük lókötő, ami ellentmond annak, hogy B az.

1.32 Thf. egyik sem, és legyen $\mathcal{M}$, $\mathcal{N}$ olyan, hogy $\mathcal{M} \not\models \psi$, $\mathcal{N} \models \varphi$. Definiáljuk $\mathcal{M}'$-ot úgy, hogy φ atomi formuláin tegye amit $\mathcal{N}$ tesz, az összes többin meg amit $\mathcal{M}$. Akkor 1.18 miatt $\mathcal{M}' \models \varphi$ és $\mathcal{M}' \not\models \psi$, ellentmondás.

Megj.: $p \to p$ mutatja, hogy a diszjunktsági feltétel nem hagyható el.

2.20 Minden $\varphi \in Form_{\{p,q\}}$-re $\{p, q\} \models \varphi$ csakkor, ha $\mathcal{M}$ models φ, ahol $\mathcal{M}$ olyan modell, amelyre $\mathcal{M}(p) = 1 = \mathcal{M}(q)$. Ebből már 2.16 miatt következik az állítás.

2.35 $\emptyset \models \{p, \neg p\}$, de $\emptyset \not\vdash_r \{p, \neg p\}$. (Az üres clause-halmazból nyilván semmi sem vezethető le.)

3.42 $\mathcal{M} \equiv \mathcal{N} \iff \mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N}) \iff \mathrm{Th}(\mathcal{M}) \subseteq \mathrm{Th}(\mathcal{N}) \iff \mathcal{M} \models \mathrm{Th}(\mathcal{N})$. Itt a második ekvivalencia visszafele irányán kívül minden definíció szerint igaz. Az meg azért, mert $\mathrm{Th}(\mathcal{M}) \subsetneq \mathrm{Th}(\mathcal{N})$ azt jelentené, hogy $\mathcal{N}$-ben igaz volna valamely φ formula és annak tagadása is, hiszen ha $\varphi \in \mathrm{Th}(\mathcal{N}) \setminus \mathrm{Th}(\mathcal{M})$, akkor $\neg\varphi \in \mathrm{Th}(\mathcal{M}) \subseteq \mathrm{Th}(\mathcal{N})$. (Kicsit későbbi szóhasználattal élve: egy modell elmélete mindig teljes.)