MATEMATIKAI LOGIKA

SIMON ANDRÁS

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.

2. Klasszikus kijelentéslogika (propozicionális logika)

2.1. Szintaxis Atomi formulák: $\Pi = \{ p_0, \ldots, p_n, \ldots \}$ 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,….

2.1. *Megjegyzés.*

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

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

2.2. 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.*

2.3. 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)

2.2. 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*.

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

2.5. Definíció (formula jelentése)**.** $\varphi \in Form_\Pi$ jelentése az $\mathcal{M}$ modellben ($\mathcal{M}$-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

.

A modellbeli igazság 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 $\mathcal{M} \models \psi$.

2.6. 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

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

□

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

2.8. 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: $\begin{array}{c|c|c||c|c|c} p & q & r & p \wedge q & (p \wedge q) \vee r & \neg((p \wedge q) \vee r) \\ \hline 1 & 1 & 0 & 1 & 1 & 0 \end{array}$, tehát nem.

2.9. 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.

2.10. 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.

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

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

Biz.

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

□

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

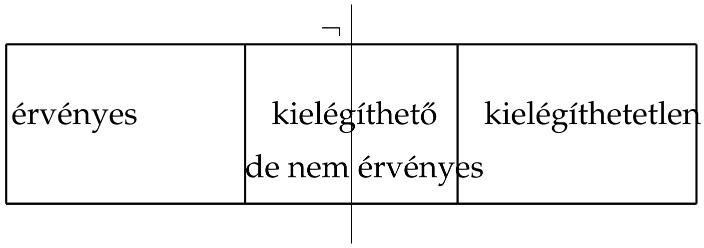
Biz.

$$\varphi \text{ kielégíthető} \iff \varphi \text{ nem kielégíthetetlen}$$
$$\iff \neg\neg\varphi \text{ nem kielégíthetetlen} \iff \neg\varphi \text{ nem érvényes.}$$

□

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

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



1. ábra. A középső függőleges vonal szimmetriatengely

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

2.15. 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.

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

2.17. 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.

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

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

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

2.21. Gyakorlat. Kielégíthető-e a

$$\Sigma = \{p_1 \vee p_2, \neg p_2 \vee \neg p_3, p_3 \vee p_4, \neg p_4 \vee \neg p_5, \dots\} = \{\, p_{2n-1} \vee p_{2n}, \neg p_{2n} \vee \neg p_{2n+1} : n > 0 \,\}$$

végtelen formulahalmaz ?

2.22. 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.

2.23. 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.

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

* * *

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

Biz.

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

□

2.26. 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) $\models \varphi \wedge \psi \to \varphi$

2.27. Tétel. (1) *Ha* $\sigma_1^{\mathcal{M}} = \sigma_2^{\mathcal{M}}$, *és* φ_2*-t úgy kaptuk* φ_1*-ből, hogy benne* σ_1 *egy előfordulását kicseréltük* σ_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. □

2.28. Következmény. (1) *Ha $\sigma_1 \equiv \sigma_2$, és φ_1, φ_2 mint a tétel első pontjában, akkor $\varphi_1 \equiv \varphi_2$.*

(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. A tétel (1) pontja és $\sigma_1 \equiv \sigma_2$ miatt minden $\mathcal{M}$ modellre $\varphi_1^{\mathcal{M}} = \varphi_2^{\mathcal{M}}$, azaz $\varphi_1 \equiv \varphi_2$.
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.

2.3. Normálformák

2.29. 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).

2.30. *Megjegyzés.* DNF kielégíthetősége gyorsan eldönthető, mert pontosan akkor kielégíthető, ha legalább 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.

2.31. 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.*

[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
- $(\neg\varphi)[\sigma_1/p_1, \ldots, \sigma_n/p_n] = \neg(\varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n])$
- $(\varphi \wedge \psi)[\sigma_1/p_1, \ldots, \sigma_n/p_n] = \varphi[\sigma_1/p_1, \ldots, \sigma_n/p_n] \wedge \psi[\sigma_1/p_1, \ldots, \sigma_n/p_n]$

Biz. (DNF) Legyen P a φ-ben előforduló kijelentésváltozók halmaza, M pedig 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

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

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

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

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

(ahol, ahogyan a bizonyítás hátralevő részében is, két modell egyenlősége úgy értendő, hogy megegyeznek φ változóin, azaz P-n) 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 2.15 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 (2.26(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

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

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

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

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

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 2.15 miatt igaz.

□

2.32. 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.

2.33. Példa. Adjunk meg egy, a $\varphi = \neg(p \wedge ((q \wedge r) \to s))$-vel ekvivalens 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 2.26 és 2.27 miatt.

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

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

2.35. Példa.

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

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

2.4. Horn formulák CNF-ek kielégíthetőségére nem ismert 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.

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

2.38. 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 a 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.

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

Vegyük észre, hogy a linearitás triviális, mert minden lépésben megjelölünk egy jelöletlen atomi formulát. Az algoritmus további jó tulajdonsága, hogy ha van ilyen, akkor a futása során kapunk is a bemenetet kielégítő modellt: ilyen lesz az a modell, ami pontosan a megjelölt kijelentésváltozókat teszi igazzá.

2.40. 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. $\square$

2.41. Példák. 1. A fenti példa $(q \to p) \land (p \land r \to s) \land (p \land q \to \bot) \land (\top \to s) \land (t \to \bot)$ 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. $(\neg p \lor \neg q \lor \neg s) \land \neg t \land (\neg r \lor p) \land r \land q \land (\neg u \lor s) \land u$, azaz

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

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 $p \land q \land s \to \bot$ az egyik diszjunkció, és p, q, s meg vannak jelölve.

2.5. Kompaktság

2.42. 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 $\cap_{n \in \mathbb{N}}(0, 1/n) = \emptyset$.

2.43. 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 $\Delta \models \varphi$. $\square$

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

- $p_{v1} \lor \ldots \lor p_{vk}$ 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")

2.44. 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). □

2.45. 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 kell megmutatni. Ehhez azt kell meggondolni, hogy ha G minden véges részgráfja kiszínezhető k színnel, akkor $\Sigma(G)$ minden véges részhalmaza kielégíthető. (Az a probléma, hogy $\Sigma(G)$-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 $\{v \in V(G)\colon p_{vi} \text{ előfordul } \Delta\text{-ban}\}$. □

2.46. Gyakorlat. Van-e olyan végtelen kielégíthetetlen formulahalmazra, aminek minden valódi részhalmaza kielégíthető?

3. A kijelentéslogika 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.

3.1. Hilbert típusú kalkulus kijelentéslogikára

3.1. 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.

3.2. Definíció (Levezetés)**.** Legyen $\Sigma \subseteq Form$, $n \in \mathbb{N}$. 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.

3.3. 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: $\vdash \varphi$.

3.4. Lemma. *Legyen* $\Sigma \cup \Delta \cup \{\, \varphi, \psi \,\} \subseteq Form$.

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

Az utolsó pont, amiről majd kiderül, hogy ekvivalens 2.42-el, ritka példa arra, hogy valamit egyszerűbb bizonyítani $\vdash$-re mint $\models$-re.

3.5. 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

3.6. Példák. (1) $\vdash (\varphi \to \bot) \to \neg\varphi$
(2) $\{\, \varphi, \neg\varphi \,\} \vdash \bot$
(3) $\{\varphi \to \psi, \psi \to \eta\} \vdash \varphi \to \eta$
(4) $\{\varphi \to (\psi \to \eta), \psi\} \vdash \varphi \to \eta$
(5) $\vdash \neg\neg\varphi \to \varphi$

3.7. Definíció. $\Sigma \subseteq Form_\Pi$ konzisztens, ha $\Sigma \nvdash \bot$; inkonzisztens, ha nem konzisztens.

Egyszerű példák inkonzisztens mondathalmazokra $\{\, \bot \,\}$ (3.4(1) miatt) és $\{\, p, \neg p \,\}$ (3.6(2) miatt).

3.8. 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)). A bizonyítás egyszerű indukcióval megy a levezetés hosszára. Azt kell megmutatni, hogy az axiómák érvényesek, és hogy az egyetlen levezetési szabály megőrzi az érvényességet.

3.9. Tétel (Dedukciótétel). $\Sigma \cup \{ \varphi \} \vdash \psi \iff \Sigma \vdash \varphi \to \psi.$

Ennek kicsit bonyolultabb a bizonyítása mint 2.25-é, és ez is a levezetés hosszára vonatkozó indukcióval történik.

3.10. Lemma. $\Sigma \vdash \varphi \iff \Sigma \cup \{\neg\varphi\}$ *inkonzisztens.*

Biz. ($\Rightarrow$) 3.4(2) miatt $\Sigma \cup \{\neg\varphi\} \vdash \varphi$ és 3.4(1) miatt $\Sigma \cup \{\neg\varphi\} \vdash \neg\varphi$, ezért 3.6(2) és 3.4(3) miatt $\Sigma \cup \{\neg\varphi\} \vdash \bot$.

($\Leftarrow$) A dedukciótétel miatt $\Sigma \cup \{\neg\varphi\} \vdash \bot$-ból $\Sigma \vdash \neg\varphi \to \bot$ következik, és így 3.6(1) és 3.4(4) miatt $\Sigma \vdash \neg\neg\varphi$. De akkor $\Sigma \vdash \varphi$ 3.6(5) és 3.4(4) miatt. □

3.11. 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.

3.12. Következmény. Σ *konzisztens pontosan akkor, ha kielégíthető.*

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

* * *

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

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

Biz. Következik a teljességből (3.11) és abból, hogy $\models \bot \to \varphi$ minden φ formulára. □

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

3.14. 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 3.11 és azon egyszerű tény következménye, hogy minden $\varphi \in Form_{\{ p \}}$-re, $\{ \neg p \} \models \varphi$ pontosan akkor, ha $\mathcal{M} \models \varphi$ minden olyan $\mathcal{M}$ modellre, amelyre $\mathcal{M}(p) = 0$; a második pedig 3.8 következménye, mert könnyű látni, hogy $\{ \neg p \vee q \} \not\models p$ és $\{ \neg p \vee q \} \not\models \neg p$.

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

3.16. 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. 3.11 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. □

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

Biz. 3.4(3) miatt $\{\, \varphi \colon \Sigma \vdash \varphi \,\} \vdash \psi$-ből $\Sigma \vdash \psi$ következik. □

3.18. Állítás. *Legyen $\Sigma \subseteq Form_\Pi$ zárt levezetésre, és legyen $\Sigma' = \{\, \neg\varphi \colon \Sigma \vdash \varphi \,\} = \{\, \neg\varphi \colon \varphi \in \Sigma \,\}$. 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 3.13 miatt igaz, a másik meg azért, mert ha $\varphi \in \Sigma \cap \Sigma'$, azaz ha $\{\, \varphi, \neg\varphi \,\} \subseteq \Sigma$, akkor $\Sigma \vdash \bot$ 3.6(2) és 3.4(3) (vagy 3.4(2)) miatt. □

3.2. Rezolúció kijelentéslogikára

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

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

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

3.21. Definíció. Igaz egy clause az $\mathcal{M}$ modellben, ha legalább egy eleme igaz $\mathcal{M}$-ben (speciálisan □ kielégíthetetlen); clause-ok egy halmaza igaz $\mathcal{M}$-ben, ha minden eleme igaz $\mathcal{M}$-ben.

3.22. 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. Nyilván elég megmutatni, hogy egy *CNF* pontosan akkor igaz egy modellben ha a clause halmaza az. És ez így van, mert $\mathcal{M} \models \bigvee_{j=1}^{m} l_j \iff \mathcal{M} \models \{l_1, \ldots l_m\}$, ezért

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

és ebből már következik az állítás. □

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

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

3.25. 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 $\mathcal{M} \models E$. $\square$

3.26. *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 $(C \cup D) \setminus \{p, \neg p\} = \square$, de $\{C, D\} \not\models \square$, mert $\{C, D\}$-nek van, $\square$-nak viszont nincs modellje.

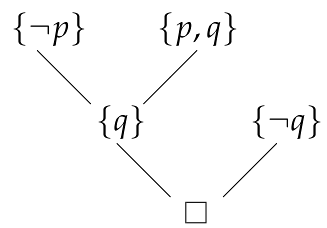
Nem lehet „felgyorsítani” a rezolúciót oly módon, hogy egyszerre két atomi formula szerint rezolválunk: pl. $C = \{p, q\}$, $D = \{\neg p, \neg q\}$-nak *nem* rezolvense $\square$, és nem is következik belőle, hiszen $\{C, D\}$ kielégíthető.

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

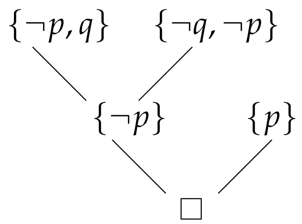
- T minden csúcsa egy clause
- E a T gyökere
- T minden levele Σ egy eleme
- T minden olyan D csúcsának ami nem levél, van két gyermeke aminek D a rezolvense.

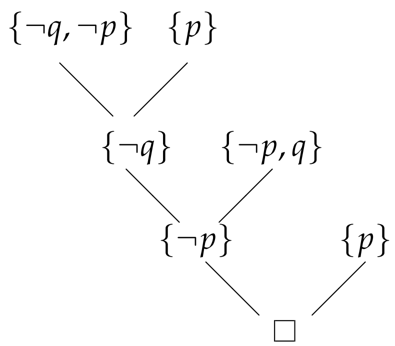
(Ahelyett, hogy a csúcsok clause-ok, helyesebb lenne azt mondani, hogy minden csúcs egy clause-zal van címkézve. Máskülönben ui. nem használhatnánk fel kétszer ugyanazt a clause-t, mert ezzel a fa megszűnne fa lenni. Ld. az alábbi második példát!) A levezetés hossza a nem-levél csúcsok száma. Σ-ból levezethető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

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



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





3.30. 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 3.25 miatt E igaz e két clause minden modelljében, speciel $\mathcal{M}$-ben is. $\square$

3.31. *Megjegyzés.* $\vdash_r$ nem teljes, mert például $\emptyset \models \{p, \neg p\}$, de $\emptyset \nvdash_r \{p, \neg p\}$ (az üres clause-halmazból ugyanis nyilván semmi sem vezethető le).

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

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

3.33. Következmény. $\Sigma \models \varphi \iff \Sigma \cup \{\neg\varphi\} \vdash_r \square$.

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

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

3.34. 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 3.32 miatt levezethető belőle $\square$; 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 $\square$ levezethető, vagyis ami 3.30 miatt kielégíthetetlen.

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

3.35. 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.

3.36. 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, tehát $Res^*(\Sigma)$ véges. Ebből már következik az állítás, mert $Res_0(\Sigma) \subseteq Res_1(\Sigma) \subseteq \cdots \subseteq Res_n(\Sigma) \subseteq \cdots \subseteq Res^*(\Sigma)$ nem lehet mind különböző. $\square$

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

Biz. Ha egy Σ véges clause-halmaz kielégíthetetlen, akkor a teljességi tétel (3.32) 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. $\square$

4. Közjáték: néhány tipikus ZH-kérdés kijelentéslogikából

Kérdés Melyik érvényes a következő formulák közül?

(a) $$(p \to \neg q) \to \neg(q \wedge p)$$

(b) $$(p \to r) \wedge (q \to \neg r) \to (p \to \neg q)$$

(c) $$(p \to \bot) \to \neg p$$

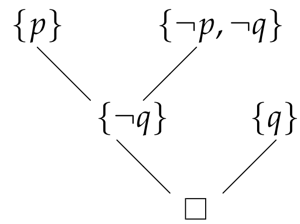
(d) $$(p \vee q) \wedge (\neg p \vee \neg q) \to (p \to q)$$

Válasz. (a) érvényes, mert ha $(p \to \neg q) \to \neg(q \wedge p)$ hamis egy $\mathcal{M}$ modellben, akkor $\mathcal{M} \models p \to \neg q$, de $\mathcal{M} \not\models \neg(q \wedge p)$, vagyis $\mathcal{M} \models q \wedge p$. De akkor $\mathcal{M} \models p, p \to \neg q$, tehát $\mathcal{M} \models \neg q \wedge q$, ami ellentmondás.

Ugyanezt rezolúcióval is meg lehet mutatni:

$$\models (p \to \neg q) \to \neg(q \wedge p) \iff \{p \to \neg q\} \models \neg(q \wedge p) \iff \{p \to \neg q, q \wedge p\} \text{ kielégíthetetlen}$$

Clause-halmazzá konvertálva ezt kapjuk: $\{\{\neg p, \neg q\}, \{q\}, \{p\}\}$, ami valóban kielégíthetetlen, mert levezethető belőle az üres clause:



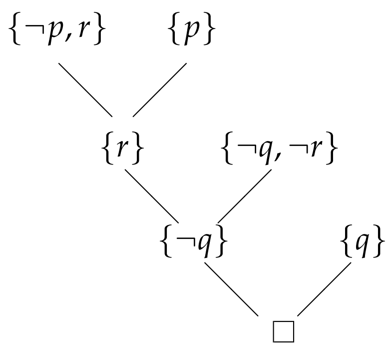
És persze igazságtáblázattal is lehet ellenőrizni (a) érvényességét.

(b): Ha $\mathcal{M} \not\models (p \to r) \wedge (q \to \neg r) \to (p \to \neg q)$ valamely $\mathcal{M}$ modellre, akkor $\mathcal{M} \not\models p \to \neg q$, tehát $\mathcal{M}(p) = 1 = \mathcal{M}(q)$; de akkor $\mathcal{M} \models p \to r$ miatt $\mathcal{M}(r) = 1$, miközben $\mathcal{M} \models q \to \neg r$ miatt $\mathcal{M}(r) = 0$, ami ellentmondás. Tehát nincs ilyen modell, vagyis a formula érvényes.

Vagy rezolúcióval:

$$\begin{aligned}\models (p \to r) \wedge (q \to \neg r) \to (p \to \neg q) &\iff \{(p \to r) \wedge (q \to \neg r)\} \models p \to \neg q\\ &\iff \{(p \to r) \wedge (q \to \neg r), \neg(p \to \neg q)\} \text{ kielégíthetetlen}\\ &\iff \{\{\neg p, r\}, \{\neg q, \neg r\}, \{p\}, \{q\}\} \text{ kielégíthetetlen}\end{aligned}$$

és ez utóbbi igaz, mert az üres clause levezethető $\{\{\neg p, r\}, \{\neg q, \neg r\}, \{p\}, \{q\}\}$-ból:



(b) tehát érvényes. És nyilvánvalóan (c) is.

De (d) nem. Ezt lehetne igazságtáblázattal, mert csak két kijelentésváltozó szerepel benne, de persze lehet rezolúcióval, vagy józan ésszel is.

Józan ésszel: ahhoz, hogy $(p \vee q) \wedge (\neg p \vee \neg q) \to (p \to q)$ hamis legyen egy $\mathcal{M}$ modellben, $(p \vee q) \wedge (\neg p \vee \neg q)$-nak igaznak és $p \to q$-nak hamisnak kell lennie $\mathcal{M}$-ben. Az utóbbi miatt $\mathcal{M}(p) = 1$ és $\mathcal{M}(q) = 0$ (következésképp legfeljebb egy ilyen modell van), de akkor $\mathcal{M} \models (p \vee q) \wedge (\neg p \vee \neg q)$, tehát $\mathcal{M}$ valóban olyan modell, amiben (d) nem igaz.

Rezolúcióval:

$$\begin{aligned} \models (p \vee q) \wedge (\neg p \vee \neg q) \to (p \to q) &\iff \{(p \vee q) \wedge (\neg p \vee \neg q), \neg(p \to q)\} \text{ kielégíthetetlen} \\ &\iff \{\{p, q\}\{\neg p, \neg q\}, \{p\}, \{\neg q\}\} \text{ kielégíthetetlen} \end{aligned}$$

Valójában erről a clause-halmazról azonnal, tehát rezolúció nélkül is látszik, hogy kielégíthető, mert az utolsó két clause előírja, hogy ha van modellje, abban p-nek igaznak, q-nak pedig hamisnak kell lennie; tehát csak ellenőrizni kell, hogy ebben a modellben a maradék két clause is igaz. És hát persze ez a helyzet, hiszen az egyiknek eleme p, a másiknak meg $\neg q$.

De ha ezt nem is vettük volna észre, és elkezdenénk rezolválni, hamar kiderülne, hogy az üres clause-t nem fogjuk tudni levezetni, mert ha $\Sigma = \{\{p, q\}\{\neg p, \neg q\}, \{p\}, \{\neg q\}\}$, akkor $Res(\Sigma) = \Sigma \cup \{\{p, \neg p\}, \{q, \neg q\}\}$ és $Res(Res(\Sigma)) = Res(\Sigma)$.

Kérdés. (A, B, C lovagok, akik mindig igazat mondanak, vagy lókötők, akik mindig hazudnak.) A: Közülünk pontosan egyvalaki lovag. B: Lovag vagyok. C: Mindhárman lókötők vagyunk.

Ki lovag és ki lókötő?

Válasz. Egy kis józan ész és igazságtáblázat kombinációja tűnik célravezetőnek. A következő formulahalmazt kielégítő modell(eke)t kellene találnunk

$$\Sigma = \{A \leftrightarrow \bigtriangledown(A, B, C), B \leftrightarrow B, C \leftrightarrow \neg A \wedge \neg B \wedge \neg C\}$$

Itt $\bigtriangledown(A, B, C)$ olyan formula, ami pontosan akkor igaz, ha A, B és C közül pontosan egy igaz. Ezt definiálhatnánk pl. így: $(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$, de a részletek nem számítanak, ami fontos, az az, hogy van ilyen formula, és hogy tudjuk, mikor igaz egy modellben.

És akkor most egy kis józan ész, egyebek mellett azért, hogy ne kelljen mind a nyolc elvben lehetséges modellben számolni. Először is, $B \leftrightarrow B$-vel nyilván nem kell foglalkoznunk, mert ez minden modellben igaz. Aztán: C csakis hamis lehet Σ minden modelljében, mert

$C \leftrightarrow \neg A \wedge \neg B \wedge \neg C \in \Sigma$ miatt ha C igaz lenne egy ilyenben, akkor $\neg C$ is. Ez nem csak megfelezi a vizsgálandó modellek számát, de egy további egyszerűsítést is lehetővé tesz: a $C \leftrightarrow \neg A \wedge \neg B \wedge \neg C$ formulát helyettesíthetjük $\neg(\neg A \wedge \neg B)$-vel, és így az azzal ekvivalens $A \vee B$-vel, mert Σ tetszőleges $\mathcal{M}$ modelljében $\mathcal{M} \not\models C$ miatt

$$\mathcal{M} \models C \leftrightarrow \neg A \wedge \neg B \wedge \neg C \iff \mathcal{M} \models \bot \leftrightarrow \neg A \wedge \neg B \wedge \top \iff \mathcal{M} \models \neg(\neg A \wedge \neg B)$$

Ezek után az igazságtáblázat így néz ki:

A	B	C	$A \vee B$	$\triangledown(A,B,C)$	$A \leftrightarrow \triangledown(A,B,C)$	$\bigwedge \Sigma$
0	0	0	0	0	1	0
0	1	0	1	1	0	0
1	0	0	1	1	1	1
1	1	0	1	0	0	0

Vagyis Σ-nak egyetlen modellje van, és abban csak A igaz, tehát A lovag és mindenki más lókötő.

Kérdés. A következő formulahalmazok közül melyek konzisztensek, és melyek teljesek?

$$\Sigma = \{p \wedge \neg q, r \to (p \vee q)\} \qquad \Gamma = \{p \wedge \neg r, p \to (q \wedge r)\}$$

Válasz. Az a kérdés, hogy van-e modelljük (3.11 miatt), és ha igen, mennyi (3.16 miatt).

A Σ-nak megfelelő clause-halmaz $\{\{p\}, \{\neg q\}, \{\neg r, p, q\}\}$. Ebből több modell is leolvasható: az első két clause miatt ha $\mathcal{M}$ modellje Σ-nak, akkor $\mathcal{M}(p) = 1$ és $\mathcal{M}(q) = 0$; de akkor a harmadik clause is igaz $\mathcal{M}$-ben, r igazságától függetlenül. Tehát Σ-nak legalább két modellje van: az egyik az, amiben p és r igaz és q hamis, a másik amiben p igaz és q és r hamis. Tehát Σ konzisztens és nem teljes.

Γ viszont inkonzisztens (és ennek következtében teljes is, ld. 3.13), mert $p \wedge \neg r \in \Gamma$ miatt p igaz minden Γ-t kielégítő modellben, következésképp $\neg r$ és r is igaz kell legyen (utóbbi $p \to (q \wedge r) \in \Gamma$ miatt). Persze ez rezolúcióval is megmutatható: a Γ-nak megfelelő clause-halmaz

$$\{\{p\}, \{\neg r\}, \{\neg p, q\}, \{\neg p, r\}\}$$

(használtuk, hogy $p \to (q \wedge r) \equiv \neg p \vee (q \wedge r) \equiv (\neg p \vee q) \wedge (\neg p \vee r)$), és ebből levezethető az üres clause, pl. így:

$$\begin{tikzcd}[column sep=small]
\{p\} \arrow[dr, dash] & & \{\neg p, r\} \arrow[dl, dash] & \\
& \{r\} \arrow[dr, dash] & & \{\neg r\} \arrow[dl, dash] \\
& & \square &
\end{tikzcd}$$

Kérdés. Legyen $\Sigma = \{\neg p, q\}$. Melyik igaz az alábbiak küzül?

(a) $$\Sigma \models r \to (p \vee \neg q)$$

(b) $$\Sigma \models p \vee q$$

(c) $$\Sigma \models (p \vee \neg q) \to r$$

(d) $$\Sigma \models \neg p \to (q \to \neg p)$$

Válasz. (a) nem, mert $p \vee \neg q$ hamis Σ minden modelljében, tehát $r \to (p \vee \neg q)$ is az, ha r igaz.

(b) igaz, mert q igaz Σ minden modelljében.

(c) is igaz, ugyanazért, amiért (a) nem: $p \vee \neg q$ hamis Σ minden modelljében, tehát $(p \vee \neg q) \to r$ igaz minden ilyen modellben.

(d) igaz, mert $\models \neg p \to (q \to \neg p)$ is az.

5. 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.

5.1. 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.[2] 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.

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

5.2. 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 $\cdot(y, \cdot(x, e)) \in$

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

$Term_{\mathcal{L}}$. A szokásos, infix írásmódot használva ezt persze így írjuk: $y \cdot (x \cdot e)$ $\mathcal{L}$ mellesleg a csoportelmélet nyelve.

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

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

akkor minden term kielégíti T-t.

5.4. 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 $t_1, \dots, t_{\rho R} \in Term_{\mathcal{L}}$, akkor $R(t_1, \dots, t_{\rho R}) \in F$
(2) ha $t_1, t_2 \in Term_{\mathcal{L}}$, akkor $t_1 = t_2 \in F$.
(3) ha $\varphi, \psi \in F$, 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.

5.5. 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.

5.6. 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: $\forall x \exists y S(x, y)$. Mindenkit szeret valakit: $\forall x \exists y S(y, x)$. 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: $\exists x (L(x) \wedge \forall y (S(x, y) \to F(y)))$.

5.7. 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.

5.2. Szemantika

5.8. 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.

5.9. 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.

5.10. 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 $t_1, \dots, t_{\rho f} \in Term_{\mathcal{L}}$.

5.11. 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 $\cdot(+(0, y), +(x, 1))^{\mathcal{M}}[\sigma] = \cdot^{\mathcal{M}}(+^{\mathcal{M}}(1, 3), +^{\mathcal{M}}(3, 33)) = \cdot^{\mathcal{M}}(1, 3) = 3$.

5.12. 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 $\mathcal{M} \models \varphi[\sigma]$.

5.13. 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 $\mathcal{M} \models \varphi[\sigma(x/m)]$. ☐

5.14. 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 $\mathcal{M} \models \forall x(x \neq 0 \to \exists y(x \cdot y = 1))[\sigma]$.

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

5.16. 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 $\mathcal{M} \models \varphi[\sigma] \iff \mathcal{M} \models \varphi[\tau]$.*

5.17. 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 $\mathcal{M} \models \varphi[\sigma]$.*

5.18. 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 $FV(\varphi) \subseteq \{ x_1, \dots, x_n \}$, akkor $\mathcal{M} \models \varphi \iff \mathcal{M} \models \forall x_1 \dots \forall x_n \varphi$.*

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

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

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

5.16 miatt ebben a definícióban „van olyan σ értékelés” helyett „minden olyan σ értékelés”-t is mondhattunk volna. Lényeg: 5.16 miatt elég a szabad változókat kiértékelni.

5.20. 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 $FV(\varphi) = \{ x \in Var : x\text{-nek van szabad előfordulása } \varphi\text{-ben} \}$.

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

5.22. 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: $\int_0^1 x\, dx (= 1/2) \neq x$.

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

(1) $\mathcal{M} \models \Sigma$ csakkor ha minden Σ-beli φ-re $\mathcal{M} \models \varphi$[3] ($\Sigma$ 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, $\varphi \equiv \psi \iff \models \varphi \leftrightarrow \psi$.

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

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

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. □

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 csak fel sem sorolható rekurzívan.

5.25. 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) $\models \exists x\forall y\varphi \to \forall y\exists x\varphi$

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

(10) $\not\models \forall x \exists y \varphi \rightarrow \exists y \forall x \varphi$

Biz. A pozitív állítások könnyen következnek az igazság definíciójából, a negatívakra pedig könnyű ellenpéldákat adni. Azért lássunk be néhányat!
(1) Tetszőleges $\mathcal{M}$ modellre és hozzá tartozó σ kiértékelésre

$$\begin{aligned}
&\mathcal{M} \models \forall x(\varphi \wedge \psi)[\sigma] \\
\iff &\text{minden } m \in M\text{-re } \mathcal{M} \models \varphi \wedge \psi[\sigma(x/m)] \\
\iff &\text{minden } m \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)] \text{ és } \mathcal{M} \models \psi[\sigma(x/m)] \\
\iff &\text{minden } m \in M\text{-re } \mathcal{M} \models \varphi[\sigma(x/m)] \text{ és minden } m \in M\text{-re } \mathcal{M} \models \psi[\sigma(x/m)] \\
\iff &\mathcal{M} \models \forall x \varphi[\sigma] \text{ és } \mathcal{M} \models \forall x \psi[\sigma] \\
\iff &\mathcal{M} \models \forall x \varphi \wedge \forall x \psi[\sigma]
\end{aligned}$$

(3) 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 $\mathcal{M} \not\models \forall x R(x) \vee \forall x S(x)$. Avagy: abból, hogy „minden ragad vagy sáros" nem következik, hogy „minden ragad vagy minden sáros".

(3) második részének belátásához tegyük fel, hogy $x \notin FV(\psi)$ és legyen $\mathcal{M}, \sigma$ 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 5.16 állítást használtuk.)
(5) Azt kell megmutatnunk, hogy $\models (\forall x(\varphi \rightarrow \psi) \wedge \forall x \varphi) \rightarrow \forall x \psi$. Tetszőleges $\mathcal{M}$ modellre és σ kiértékelésre

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

(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 $\mathcal{M} \models \forall x.R(x) \rightarrow \forall x.S(x)$, mert $\mathcal{M} \not\models \forall x.R(x)$; de $\mathcal{M} \not\models \forall x(R(x) \rightarrow S(x))$, mert $\mathcal{M} \not\models R(x) \rightarrow S(x)[a]$. 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 $\mathcal{M} \not\models \forall x \exists y. x = y \to \exists y \forall x. x = y$. $\square$

5.26. 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 kijelentéslogikában, pl., $\{\varphi\} \models \forall x \varphi$ (ld. 5.18), 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).

5.27. 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

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

5.3. Példák

5.28. Példa. Legyen $\mathcal{L}$ az üres nyelv. Azt, hogy „az univerzum legalább kételemű” kifejezhetjük a $\exists x \exists y. x \neq y$ $\mathcal{L}$-mondattal (azaz ennek a mondatnak a modelljei pontosan az olyan modellek, melyeknek legalább kételemű az univerzuma); azt, hogy „az univerzum pontosan kételemű”, a $\exists x \exists y (x \neq y \wedge \forall z (z = x \vee z = y))$ $\mathcal{L}$-mondattal; azt, hogy az univerzum legfeljebb háromelemű”, a $\forall x \forall y \forall z \forall w ((x \neq y \wedge x \neq z \wedge y \neq z) \to (w = x \vee w = y \vee w = z))$ $\mathcal{L}$-mondattal.

5.29. Gyakorlat. Adjon meg egy olyan Σ formulahalmazt üres nyelven, amire igaz, hogy $\mathcal{M} \models \Sigma$ pontosan akkor, ha M végtelen.

Tehát az, hogy az univerzum végtelen, kifejezhető egy formulahalmazzal; ezzel szemben az, hogy véges, nem, a következő miatt. Ha Δ olyan formulahalmaz, amely pontosan a véges modellekben igaz, és σ_n egy olyan formula, ami azt mondja, hogy az univerzum legalább n elemű, akkor a $\Sigma = \Delta \cup \{\sigma_n : n \in \mathbb{N}\}$ formulahalmaz minden véges részhalmaza kielégíthető. De akkor Σ is az, ellentmondva annak a feltevésnek, hogy Δ-nak csak véges modelljei vannak, mert a kompaktsági tétel elsőrendű logikában is igaz:

5.30. Tétel. *Ha elsőrendű formulák egy halmazának minden véges részhalmaza kielégíthető, akkor az egész is az.*

Így az is kiderült, hogy nincs olyan formula, ami pontosan a végtelen modellekben igaz (mert annak tagadása definiálná a véges modelleket).

5.31. Példa. Legyen $\mathcal{L}$ egy elsőrendű nyelv a $<$ kétargumentumú relációjellel és az a, b konstansjelekkel. a jelentése Aliz, b-é Béla, és jelentse $x < y$ azt, hogy x (értéke) kisebb, mint y-é. (Vegyük észre, hogy ez utóbbi csak annyit mond, hogy tetszőleges $\mathcal{M}$ modellben $a^{\mathcal{M}}$-et Aliznak, $b^{\mathcal{M}}$-et Bélának, a $<^{\mathcal{M}}$ kétargumentumú relációt pedig „kisebb"-nek fogjuk hívni.)

(1) Aliz kisebb mint Béla: $a < b$
(2) Aliz kisebb mint valaki, aki kisebb mint Béla: $\exists x(a < x \wedge x < b)$
(3) Aki Bélánál kisebb, az Aliznál is kisebb. $\forall x(x < b \to x < a)$.
(4) Mindenki, aki kisebb valakinél aki kisebb Bélánál, kisebb Aliznál is:

$$\forall x(\exists y(x < y \wedge y < b) \to x < a)$$

(5) Ha van, aki mindenkinél kisebb, akkor valaki kisebb magánál:

$$(\exists x \forall y . x < y) \to \exists x . x < x$$

(6) Valaki kisebb bárkinél, akinél Aliz kisebb:

$$\exists x \forall y(a < y \to x < y)$$

5.32. Példa. Legyen $\mathcal{L}$ az az elsőrendű nyelv, melyben $\{\leq\}$ binér relációjel. Olyan $\mathcal{L}$-mondatokat fogalmazunk meg, amelyek a $\leq$ által jelölt relációról állítanak különféle dolgokat:

(1) $\leq$ (jelentése) előrendezés (azaz reflexív, tranzitív reláció):

$$\forall x(x \leq x) \wedge (\forall x)(\forall y)(\forall z)((x \leq y \wedge y \leq z) \to x \leq z)$$

(2) minden elemnek van közvetlen rákövetkezője (ahol y közvetlen rákövetkezője x-nek, ha $x \leq y$ és $x \neq y$, de nincs szigorúan köztük semmi):

$$(\forall x)(\exists y)(x \leq y \wedge x \neq y \wedge \forall z((x \leq z \wedge z \leq y) \to (x = z \vee y = z)))$$

(3) egyik elemnek sincs közvetlen rákövetkezője:

$$(\forall x)(\forall y)((x \leq y \wedge x \neq y) \to \exists z(x \leq z \wedge z \leq y \wedge x \neq z \wedge z \neq y))$$

(4) van mindenkivel összehasonlítható elem:

$$(\exists x)(\forall y)(x \leq y \vee y \leq x)$$

(5) minden egy- vagy kételemű halmaznak van legkisebb felső korlátja:

$$(\forall x)(\forall y)(\exists z)\,(x \leq z \wedge y \leq z \wedge (\forall w)((x \leq w \wedge y \leq w) \to z \leq w))$$

5.33. Példa. Legyen $\mathcal{L}$ az $\mathcal{N} = \langle \mathbb{N}, 0^{\mathcal{N}}, s^{\mathcal{N}}, +^{\mathcal{N}}, \cdot^{\mathcal{N}} \rangle$ modell nyelve (ahol $s^{\mathcal{N}}$ a „rákövetkező" függvény). Először olyan $\varphi(x)$ $\mathcal{L}$-formulákat írunk le, amelyeknek $\mathcal{N}$-beli jelentése (azaz $\{n \in \mathbb{N} \colon \mathcal{N} \models \varphi(x)[n]\}$)

(1) a négyzetszámok: $(\exists y)x = y \cdot y$
(2) a páros számok: $(\exists y)x = y + y$

(3) a páratlan számok: $(\exists y) x = s(y+y)$
(4) a prímek: $(\forall y)\,((\exists z)(x = y \cdot z) \to y = s(0) \vee y = x)$

Ezek segítségével formalizálni tudjuk a Goldbach sejtést (minden 2-nél nagyobb páros szám két prím összege) ezen a nyelven, az $E(x)$ („x páros") és $P(x)$ („x prím") rövidítéseket használva:

$$(\forall x)\,(E(x) \wedge 2 < x \to (\exists y)(\exists z)(P(y) \wedge P(z) \wedge x = y + z))\,,$$

vagy, rövidítések nélkül:

$$\begin{aligned}(\forall x)(\overbrace{(\exists y)(x = y+y)}^{E(x)} \wedge 2 < x \\ \to (\exists y)(\exists z)(\overbrace{(\forall w)\,((\exists z)(y = w \cdot z) \to w = s(0) \vee w = y)}^{P(y)} \\ \wedge \underbrace{(\forall y)\,((\exists w)(z = y \cdot w) \to y = s(0) \vee y = z)}_{P(z)} \wedge x = y + z))\end{aligned}$$

Vegyük észre, hogy itt át kellett neveznünk kötött változókat az ütközések elkerülése végett.

6. Modális és temporális logikák

A modális (és speciálisan a temporális) logikák egyebek mellett a számítástudományi alkalmazásaik (pl. programhelyességről ill. tudásról való érvelés) miatt érdekesek.

6.1. Propozicionális modális logika Az elsőrendű logikához hasonlóan a modális logika is a kijelentéslogika egy kiterjesztése, csak egy másik irányban.

Szintaxis A modális kijelentéslogika legegyszerűbb változatának (BML — *basic (propositional) modal logic*) ugyanaz a szintaxisa, mint a kijelentéslogikának, azzal az egyetlen különbséggel, hogy van egy új egyargumentumú logikai konnektívum, a $\Box$. Úgyhogy most a formulák:

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

ahol, mint a közönséges kijelentéslogikában, Π a kijelentésváltozók halmaza. Tehát $Form_\Pi$ a legszűkebb Π-t tartalmazó, $\neg$-re $\wedge$-re és $\Box$-ra zárt halmaz. $\Box\,\varphi$-t „szükségszerűen φ"-nek vagy egyszerűen „doboz φ"-nek olvassuk.

Precedencia: ahogy eddig is, az unér konnektívumok erősebben kötnek, mint a binérek, úgyhogy pl. $\Box\,\varphi \wedge \psi$ $(\Box\,\varphi) \wedge \psi$-nek és nem $\Box(\varphi \wedge \psi)$-nek értendő.

6.1. Példák. Minden kijelentéslogikai formula modális formula; és $\Box\, p$, $\neg\Box\neg(p \wedge \Box\, q)$, stb. stb. is azok.

A kijelentéslogikában definiált konnektívumok ($\vee$, $\to$, $\leftrightarrow$, $\bot$, $\top$, etc.) itt is ugyanúgy vannnak definiálva, de most van egy új definiált konnektívum is a $\Diamond$: $\Diamond\,\varphi \overset{\text{def}}{=} \neg\Box\neg\varphi$, ezt „lehetséges, hogy φ"-nek vagy egyszerűen „gyémánt φ"-nek olvassuk.

Szemantika

6.2. Definíció (frame, modell). $\mathcal{F} = \langle W, R \rangle$ *frame* (vagy *transition system*), ha W nemüres halmaz (*világok* vagy *állapotok* halmaza) es $R \subseteq W \times W$ (*elérhetőségi reláció* vagy *átmenet reláció*). (Ha sRt valamely s és $t \in W$-re, akkor azt is mondjuk, hogy t az s *szomszédja*, vagy hogy s *látja* t-t.) $\mathcal{M} = \langle \mathcal{F}, v \rangle$ *modell* ha $\mathcal{F}$ frame, $v : \Pi \longrightarrow \mathcal{P}(W)$; v-t *értékelésnek* hívják.

Ahogy az a következő definíció első pontjából látszik, a v mögötti elgondolás az, hogy $v(p)$ azokat az állapotokat jelöli ki, amelyekben p igaz.

6.3. Definíció (formula jelentése). Formulák igazsága a $\mathcal{M} = \langle W, R, v \rangle$ modell egy világában a következő módon van definiálva:

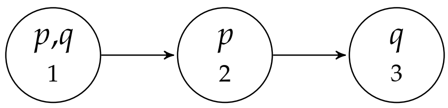
- $\mathcal{M} \models_s p$ ha $s \in v(p)$
- $\mathcal{M} \models_s \neg\varphi$ ha $\mathcal{M} \not\models_s \varphi$
- $\mathcal{M} \models_s \varphi \wedge \psi$ ha $\mathcal{M} \models_s \varphi$ és $\mathcal{M} \models_s \psi$
- $\mathcal{M} \models_s \Box\,\varphi$ ha $\mathcal{M} \models_t \varphi$ minden olyan $t \in W$-re, amelyre sRt.

Végül $\mathcal{M} \models \varphi$ (φ *igaz* $\mathcal{M}$-ben) ha $(\forall s \in W)\mathcal{M} \models_s \varphi$; és $\mathcal{F} \models \varphi$ (φ *érvényes* $\mathcal{F}$-ben) ha $\langle \mathcal{F}, v \rangle \models \varphi$ minden v értékelésre. Ha K frame-ek egy osztálya, akkor $K \models \varphi$ (φ *érvényes* K-ban) ha φ érvényes K minden elemében. φ *érvényes* (jelölés: $\models \varphi$), ha érvényes minden frame-ben.

A látszat ellenére valójában a modális kijelentéslogika szematikája is csak egy lényeges ponton különbözik a kijelentéslogika szematikájától (ahogyan a szintaxisa is). Az, hogy a modellek most nem egyszerűen az igazságértékek halmazába képező függvények, látványos, de nem lényeges eltérés. A (nem modális) kijelentéslogika szemantikáját is definiálhattuk volna a fentihez hasonló módon (természetesen elérhetőségi reláció és az igazságdefiníció utolsó sora nélkül — vegyük észre, hogy az elérhetőségi relációnak semmi szerepe a kijelentéslogikai konnektívumok igazságfeltételeiben), ez egyetlen fontos kijelentéslogikai tételre sem lenne hatással. Például az így definiált szemantikában pontosan ugyanazok maradnának az érvényes formulák. Az meg természetes, hogy valahogyan értelmet kell adnunk az új konnektívumnak. És a definíció azt mondja, hogy $\Box\,\varphi$ akkor igaz az $\mathcal{M}$ modell s állapotában, ha φ igaz $\mathcal{M}$ minden, s-sel szomszédos állapotában; másszóval ha s csak olyan állapotokat lát, amelyekben φ igaz. Következésképp

6.4. Állítás. *$\mathcal{M} \models_s \Diamond\,\varphi$ pontosan akkor, ha $\mathcal{M} \models_t \varphi$ s valamely t szomszédjára.*

6.5. Példa. Legyen $\mathcal{F} = \langle W, R \rangle$ és $\mathcal{M} = \langle \mathcal{F}, v \rangle$, ahol $W = \{1, 2, 3\}$, $R = \{(1,2), (2,3)\}$, $v(p) = \{1, 2\}$, és $v(q) = \{1, 3\}$. Akkor



(1) $\mathcal{M} \models_2 p \wedge \neg q$
(2) $\mathcal{M} \models_1 \neg \Diamond\, q$, mert 2 az 1 egyetlen szomszédja, és $\mathcal{M} \not\models_2 q$
(3) $\mathcal{M} \models_1 \Diamond\,\Diamond\, q$, mert 1-nek van olyan szomszédja (2) aminek van olyan szomszédja (3) amelyben q igaz.

(4) $\mathcal{M} \models_1 \Box \Diamond q$, mert 1-nek csak egy szomszédja van (2), és annak van olyan szomszédja (3) amelyben q igaz.
(5) $\mathcal{M} \models_1 \Diamond(p \wedge \Diamond q)$, mert 1-nek van olyan szomszédja (2) amelyben p igaz, és amelynek van olyan szomszédja (3) amelyben q igaz.
(6) $\mathcal{M} \models_1 \Box(p \wedge \Diamond q)$, mert 1-nek csak egy szomszédja van (2), úgyhogy 1 minden szomszédjára igaz, hogy p igaz ott, és hogy van olyan szomszédja (3) ahol q igaz.
(7) $\mathcal{M} \models_3 \Box \bot$ mert 3-nak nincs szomszédja.
(8) $\mathcal{M} \models_2 \Box(p \to \neg q)$ mert 3 a 2 egyetlen szomszédja, és $\mathcal{M} \not\models_3 p$, úgyhogy $\mathcal{M} \models_3 p \to \neg q$
(9) $\mathcal{F} \models \Diamond p \to \Box p$ mert minden állapotnak legfeljebb egy szomszédja van; ha tehát valami igaz egy állapot valamely szomszédjában, akkor az igaz annak az állapotnak minden szomszédjában.

6.6. Példák. (1) $\models \Box \top$ mert $\top$ igaz minden modell minden állapotában
(2) $\not\models \Diamond \top$, mert tetszőleges modellben $\Diamond \top$ pontosan akkor igaz egy állapotban, ha annak van szomszédja; ezért $\Diamond \top$ pontosan akkor érvényes egy frame-ben, ha a frame minden állapotának van szomszédja
(3) $\models \Box(\varphi \to \psi) \to (\Box \varphi \to \Box \psi)$ (v.ö. 5.25(5))
(4) $\not\models (\Box \varphi \to \Box \psi) \to \Box(\varphi \to \psi)$ (v.ö. 5.25(6))
(5) $\models \Diamond(\varphi \vee \psi) \leftrightarrow (\Diamond \varphi \vee \Diamond \psi)$ (v.ö. 5.25(2))
(6) $\models \Diamond(\varphi \to \psi) \to (\Box \varphi \to \Diamond \psi)$
(7) ha $K \models \varphi$, akkor $K \models \Box \varphi$ (v.ö. 5.18)
(8) $\not\models \varphi \to \Box \varphi$ (v.ö. a 5.18 utáni megjegyzéssel)

6.7. Állítás. *Legyen R az $\mathcal{F}$ frame elérhetőségi relációja.*
(1) $\mathcal{F} \models \Box \bot \iff \mathcal{F} \models \forall s \neg \exists t . sRt$
(2) $\mathcal{F} \models \Box p \to p \iff \mathcal{F} \models \forall s . sRs$, *azaz ha R reflexív*
(3) $\mathcal{F} \models \Box p \to \Box \Box p \iff$ *R tranzitív*
(4) $\mathcal{F} \models \Box \Box p \to \Box p \iff$ *R sűrű, azaz ha $\mathcal{F} \models \forall s, t(sRt \to \exists w . sRwRt)$*
(5) $\mathcal{F} \models p \to \Box \Diamond p \iff$ *R szimmetrikus*
(6) $\mathcal{F} \models \Diamond p \to \Box p \iff \mathcal{F} \models \forall s \forall t \forall w (sRt \wedge sRw \to t = w)$, *azaz ha R parciális függvény*
(7) $\mathcal{F} \models \Diamond p \to \Box \Diamond p \iff \mathcal{F} \models \forall s \forall t \forall w (sRt \wedge sRw \to tRw)$.

Biz. Belátunk néhányat ezek közül. (A $\Leftarrow$ irány általában csak számolás, a másik irányban kicsit dolgozni kell.)
(2) ($\Leftarrow$) Ha R reflexív és $\langle \mathcal{F}, v \rangle \models_s \Box p$ valamilyen v-re, akkor $\langle \mathcal{F}, v \rangle \models_s p$ is, mert s is szomszédja s-nek.

($\Rightarrow$) Ha s irreflexív állapot, akkor $v(p) = W \setminus \{ s \}$ (képben: $\underset{\neg p}{\bullet}$) mellett $\langle \mathcal{F}, v \rangle \not\models_s \Box p \to p$ (röviden: $s \not\models \Box p \to p$), hiszen s minden szomszédjában igaz p, de s-ben nem.

(3) ($\Leftarrow$) Ha R tranzitív és $\langle \mathcal{F}, v \rangle \models_s \Box p$, akkor p igaz ebben a modellben s minden szomszédjában; de akkor a tranzitivitás miatt p igaz s minden szomszédjának minden szomszédjában is; ezért s minden szomszédjában igaz $\Box p$, következésképp $\langle \mathcal{F}, v \rangle \models_s \Box \Box p$.
($\Rightarrow$) Ha R nem tranzitív, akkor vannak olyan $rRsRt$ állapotok, amikre $\neg rRt$; legyen $v(p) = W \setminus \{ t \}$. Képben: $\bullet \to \bullet \to \overset{\neg p}{\bullet}$. Node akkor $r \not\models \Box p \to \Box \Box p$, hiszen r minden szomszédjában igaz p, de van egy olyan szomszédja (s), amiben nem igaz $\Box p$.

(5) ($\Leftarrow$) Ha R szimmetrikus és $\langle\mathcal{F}, v\rangle \models_s p$ valamilyen v-re, akkor $\Diamond p$ igaz s minden szomszédjában, mert ezek mind látják s-et. Tehát $\langle\mathcal{F}, v\rangle \models_s \Box\Diamond p$.
($\Rightarrow$) Ha R nem szimmetrikus, akkor sRt és $\neg tRs$ valamely s és t állapotokra; legyen $v(p) = \{ s \}$. Akkor $\langle\mathcal{F}, v\rangle \models_s p$, de $\langle\mathcal{F}, v\rangle \not\models_s \Box\Diamond p$ mert sRt, de $\langle\mathcal{F}, v\rangle \not\models_t \Diamond p$.

$\Box$

6.2. Propozicionális temporális logika Hogyan lesz a modális logikából temporális logika? Ha az elérhetőségi reláció történetesen valamilyen rendezés, és ezért mondhatjuk, hogy sRt azt jelenti, hogy t „később van” mint s, akkor $\Box\varphi$ s állapotbeli igazsága azzal ekvivalens, hogy φ igaz minden s-nél későbbi állapotban, azaz azzal, hogy s-ben igaz hogy „a jövőben mindig φ”. (Itt használjuk azt a tényt, hogy minden rendezés tranzitív.)

De ha időről van szó, akkor rendszerint nem csak a jövőről, de a múltról is szeretnénk beszélni, tehát legalább két modális konnektívumra van szükségünk. Ezért kicsit tágítanunk kell a modális logika kereteit.

A *multimodális* kijelentéslogikában egy helyett több modális konnektívum van, azaz $\Box$ helyett dobozok egy $\{\Box_i : i \in I\}$ családja. Ennek megfelelően a frame-ek $\langle W, R_i \rangle_{i\in I}$ alakúak, ahol R_i a $\Box_i$-nek megfelelő elérhetőségi reláció. Tehát itt $Form_\Pi$ a legszűkebb Π-t tartalmazó, $\neg$-re, $\wedge$-re, és (minden $i \in I$-re) a $\Box_i$-re zárt halmaz, és $\mathcal{M} \models_s \Box_i \varphi$ ha $\mathcal{M} \models_t \varphi$ minden olyan $t \in W$-re, amelyre sR_it.

A legegyszerűbb temporális logika egy bimodális logika, azzal az extra feltétellel, hogy a két doboznak (amelyeket ilyenkor $[\mathrm{F}]$-nek és $[\mathrm{P}]$-nek hívunk $\Box_1$ és $\Box_2$ helyett) megfelelő elérhetőségi relációk (R_F és R_P; vagy $<$ és $>$) szigorú részbenrendezések (azaz irreflexív, tranzitív relációk), amelyek egymás konverzei, azaz $sR_Ft \iff tR_Ps$ minden s és t állapotra. Ez annak az elvárásnak felel meg, hogy a jövőbe ugyanazon a reláción keresztül nézünk, mint a múltba.

6.8. Állítás. *Legyen $\mathcal{F} = \langle W, R_F, R_P\rangle$ tetszőleges frame. Akkor*

(1) *$\mathcal{F} \models \varphi \to [\mathrm{F}]\,\langle\mathrm{P}\rangle\,\varphi$ pontosan akkor, ha $sR_Ft \implies tR_Ps$ minden $s, t \in W$-re.*
(2) *$\mathcal{F} \models \varphi \to [\mathrm{P}]\,\langle\mathrm{F}\rangle\,\varphi$ pontosan akkor, ha $sR_Pt \implies tR_Fs$ minden $s, t \in W$-re.*

Biz. Csak az elsőt látjuk be, a második bizonyítása analóg.
($\Leftarrow$) Ez az implikáció igaz, mert a feltevésünk szerint minden állapot a „múltjában van” minden, a jövőjében lévő állapotnak. Kicsit részletesebben: Tegyük fel, hogy $\langle F, v\rangle \models_s \varphi$ valamilyen v értékelésre és s állapotra; azt kell megmutatnunk, hogy $\langle F, v\rangle \models_s [\mathrm{F}]\,\langle\mathrm{P}\rangle\,\varphi$, vagyis azt, hogy $\langle F, v\rangle \models_t \langle\mathrm{P}\rangle\,\varphi$ minden olyan t-re, amelyre sR_Ft. De ez igaz, mert a feltevésünk miatt tR_Ps, és φ igaz s-ben.
($\Rightarrow$) Tegyük fel, hogy sR_Ft de $\neg tR_Ps$ valamely $s, t \in W$-re, és legyen $v(p) = \{s\}$. Akkor $\langle F, v\rangle \models_s p$, de $\langle F, v\rangle \not\models_s [\mathrm{F}]\,\langle\mathrm{P}\rangle\,p$, mert sR_Ft, de $\langle F, v\rangle \not\models_t \langle\mathrm{P}\rangle\,p$, mivel s az egyetlen állapot, amelyben p igaz, de $\neg tR_Ps$. $\Box$

6.9. Definíció (temporális frame, ideiglenes változat). Az $\mathcal{F} = \langle W, R_F, R_P\rangle$ frame *temporális frame* ha R_F és R_P egymás konverzei és R_F (következésképp R_P is) szigorú részbenrendezés.

Az előző állítás és 6.7(3) miatt igaz a következő.

6.10. Következmény. *A $\mathcal{F} = \langle W, R_F, R_P\rangle$ frame pontosan akkor temporális frame, ha R_F irreflexív és*

$$\mathcal{F} \models (\varphi \to [\mathrm{F}]\,\langle\mathrm{P}\rangle\,\varphi) \wedge (\varphi \to [\mathrm{P}]\,\langle\mathrm{F}\rangle\,\varphi) \wedge ([\mathrm{F}]\,\varphi \to [\mathrm{F}]\,[\mathrm{F}]\,\varphi)$$

Mivel egy temporális frame két elérhetőségi relációja megkapható egymásból, nem szükséges mindkettőt magunkkal hurcolnunk. Ezzel viszont kilépünk a multimodális logika keretei közül.

6.11. Definíció (temporális frame, végleges változat)**.** Az $\mathcal{F} = \langle W, R \rangle$ frame *temporális frame* ha R szigorú részbenrendezés, amely az $[\mathrm{F}]$ modalitásnak felel meg. A $[P]\varphi$ igazságfeltétele egy ilyen frame-ben a következő:

$$\mathcal{M} \models_s [P]\varphi \iff \mathcal{M} \models_t \varphi \quad \text{minden olyan } t\text{-re, amelyre } tRs.$$

6.12. Példák. Legyen $\mathcal{F} = \langle \mathbb{N}, < \rangle$, ahol $<$ a természetes számok szokásos rendezése; és legyen $\mathcal{M} = \langle \mathcal{F}, v \rangle$, ahol $v(r) = \{42\}$. Akkor

(1) $\mathcal{M} \models r \vee <\mathrm{P}> r \vee <\mathrm{F}> r$
(2) $\mathcal{M} \models <\mathrm{F}> <\mathrm{P}> r$
(3) $\mathcal{M} \not\models <\mathrm{P}> <\mathrm{F}> r$ mert $\mathcal{M} \not\models_0 <\mathrm{P}> <\mathrm{F}> r$, mivel $\mathcal{M} \not\models_0 <\mathrm{P}> \varphi$ minden φ formulára, mert 0 múltja üres
(4) $\mathcal{F} \not\models <\mathrm{P}> <\mathrm{F}> \top$ ugyanezért
(5) $\mathcal{F} \models <\mathrm{F}> <\mathrm{P}> \top$
(6) $\mathcal{F} \models [\mathrm{P}] \perp \vee <\mathrm{P}> [\mathrm{P}] \perp$ mert van olyan állapot, amelynek üres a múltja, és amely minden állapot múltjában van
(7) $\mathcal{F} \models \varphi \wedge [\mathrm{P}]\, \varphi \to <\mathrm{F}> [\mathrm{P}]\, \varphi$ (ld. alább!)
(8) $\models <\mathrm{F}> [\mathrm{P}]\, \varphi \to \varphi$
(9) $\models <\mathrm{P}> [\mathrm{F}]\, \varphi \to \varphi$

6.13. Állítás. *Legyen $\mathcal{F} = \langle W, < \rangle$ olyan temporális frame, amelyben $<$ teljes rendezés (azaz minden $s, t \in W$-re legalább (és így a tranzitivitás és az irreflexivitás miatt pontosan) egyike áll az $s < t$, $s = t$ és $t < s$ feltételeknek). Akkor minden $s \in W$-nek van közvetlen rákövetkezője (azaz olyan $t \in W$, amelyre $s < t$ és amelyre $(s, t) \cap W = \emptyset$) pontosan akkor, ha*

$$\mathcal{F} \models \varphi \wedge [\mathrm{P}]\, \varphi \to <\mathrm{F}> [\mathrm{P}]\, \varphi$$

Biz. ($\Rightarrow$) Tegyük fel, hogy $\langle \mathcal{F}, v \rangle \models_s \varphi \wedge [\mathrm{P}]\, \varphi$ valamely v értékelésre és s állapotra; azt kell megmutatnunk, hogy $\langle \mathcal{F}, v \rangle \models_s <\mathrm{F}> [\mathrm{P}]\, \varphi$. A feltevésünk miatt φ igaz s előtt és s-ben. Ha tehát t közvetlen rákövetkezője s-nek, akkor $\langle \mathcal{F}, v \rangle \models_t [\mathrm{P}]\, \varphi$.
($\Leftarrow$) Ha s-nek nincs közvetlen rákövetkezője, akkor legyen $v(p) = \{t \colon t < s \text{ vagy } t = s\}$. Akkor $\langle \mathcal{F}, v \rangle \models_s p \wedge [\mathrm{P}]\, p$, de $\langle \mathcal{F}, v \rangle \not\models_s <\mathrm{F}> [\mathrm{P}]\, p$, mert $\langle \mathcal{F}, v \rangle \not\models_t [\mathrm{P}]\, p$ minden $t > s$-re, mivel minden ilyen t-hez van olyan w amelyre $s < w < t$, és így $\langle \mathcal{F}, v \rangle \not\models_w p$. $\square$

$[\mathrm{F}]$, $[\mathrm{P}]$ és a duálisaik mellett szokás bevezetni a $\mathcal{S}$ („since”) és az $\mathcal{U}$ („until”) binér modalitásokat. Az így kibővített formulahalmaz az eddigi temporális formulákat tartalmazza, de zárt $\mathcal{S}$-re és $\mathcal{U}$-ra is, azaz ha φ és ψ formulák, akkor $\varphi\, \mathcal{U}\, \psi$ („φ until ψ”) és $\varphi\, \mathcal{S}\, \psi$ („φ since ψ”) is az, a következő igazságdefiníciókkal:

6.14. Definíció. Ha $\mathcal{F} = \langle W, < \rangle$ temporális frame, $\mathcal{M}$ az $\langle \mathcal{F}, v \rangle$ modell, és $s \in W$, akkor

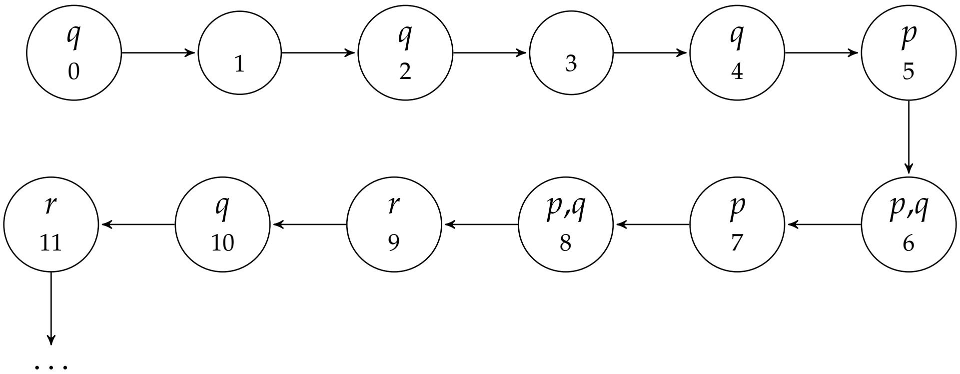
$$\mathcal{M} \models_s \varphi\, \mathcal{U}\, \psi \iff \text{van olyan } t > s, \text{ amelyre } \mathcal{M} \models_t \psi \text{ és } \mathcal{M} \models_w \varphi \text{ minden } w \in (s, t)\text{-re}$$

és

$$\mathcal{M} \models_s \varphi\, \mathcal{S}\, \psi \iff \text{van olyan } t < s, \text{ amelyre } \mathcal{M} \models_t \psi \text{ és } \mathcal{M} \models_w \varphi \text{ minden } w \in (t, s)\text{-re.}$$

Ezek a „since” és az „until” irreflexív változatai, és néha épp ezek kellenek. Például: „ez a változó inicializálatlan amíg nem adunk neki értéket”, vagy „éhes leszek amíg nem eszem valamit” (vagyis „éhes vagyok $\mathcal{U}$ eszem valamit”). „Féltem a farkasoktól mióta láttam egyszer egyet a konyhában”, azaz „félek a farkasoktól $\mathcal{S}$ látok egy farkast a konyhában”. De ha még mindig félek (reflexív változat), akkor csak hozzá kell tennem, hogy „$\ldots \wedge$ félek a farkasoktól”.

6.15. Példák. Legyen $\mathcal{F}$ a $\langle \mathbb{N}, < \rangle$ temporális frame, ahol $<$ a természetes számok szokásos rendezése, és legyen $\mathcal{M} = \langle \mathcal{F}, v \rangle$, ahol $v(p) = \{n \in \mathbb{N} \colon 5 \leq n \leq 8\}$, $v(q) = \{2n \colon n \in \mathbb{N}\}$ és $v(r) = \{9, 11\}$. Akkor



(1) $\mathcal{M} \models_4 (p\,\mathcal{U}\,r) \wedge [\mathrm{F}]\,\mathrm{<F>}\,q$: az első „éselendő” igaz a 4 állapotban, mert van olyan > 4 állapot, nevezetesen a 9, ahol r igaz, és ami olyan, hogy p igaz minden szigorúan 4 és 9 közti állapotban; a második pedig azért igaz a 4 állapotban, és valójában mindegyikben, mert minden s utáni t állapothoz van t utáni páros állapot.

(2) $\mathcal{M} \not\models_2 [\mathrm{F}]\,\mathrm{<F>}\,q \to (p\,\mathcal{U}\,r)$ mert, ahogy már láttuk, $[\mathrm{F}]\,\mathrm{<F>}\,q$ minden állapotban igaz, de $(p\,\mathcal{U}\,r)$ nem igaz 2-ben, mert 9 az egyetlen olyan állapot, ahol r igaz, de p nem igaz például $3 \in (2, 9)$-ben.

(3) $\mathcal{M} \models_{10} r\,\mathcal{S}\,p$ mert van olyan korábbi állapot, nevezetesen 8, ahol p igaz, és r igaz minden $(8, 10) = \{9\}$-beli állapotban.

(4) $\mathcal{M} \models_{10} r\,\mathcal{S}\,q$ pontosan ugyanezért.

(5) $\mathcal{M} \not\models_{10} r\,\mathcal{S}\,(p \wedge \neg q)$ mert a 7 állapot a 10 előtti legkésőbbi ahol $p \wedge \neg q$ igaz, de $8 \in (7, 10)$-ben nem igaz r.

6.16. Állítás. (1) $\models \varphi\,\mathcal{U}\,\psi \to \mathrm{<F>}\,\psi$

(2) $\models \top\,\mathcal{U}\,\psi \leftrightarrow \mathrm{<F>}\,\psi$

(3) $\models \top\,\mathcal{S}\,\psi \leftrightarrow \mathrm{<P>}\,\psi$

(4) *$\mathcal{M} \models_s \bot\,\mathcal{U}\,\psi$ pontosan akkor, ha s-nek van közvetlen rákövetkezője ahol ψ igaz; speciálisan $\mathcal{M} \models_s \bot\,\mathcal{U}\,\top$ pontosan akkor, ha s-nek van közvetlen rákövetkezője*

(5) *$\mathcal{M} \models_s \bot\,\mathcal{S}\,\psi$ pontosan akkor, ha s-nek van közvetlen megelőzője ahol ψ igaz; speciálisan $\mathcal{M} \models_s \bot\,\mathcal{S}\,\top$ pontosan akkor, ha s-nek van közvetlen megelőzője.*

Biz. (1) Ha $\varphi\,\mathcal{U}\,\psi$ igaz egy modell s állapotában, akkor az $\mathcal{U}$ igazságdefiníciója miatt van olyan $t > s$ állapot, ahol ψ igaz.

(2) Az $\to$ irány igaz az előző állítás miatt. És ha $\mathcal{M} \models_s \mathrm{<F>}\,\psi$ valamely $\mathcal{M}$ modell s állapotára, akkor van olyan $t > s$ ahol ψ igaz, és persze $\top$ igaz minden szigorúan s és t közti állapotban.

(3) Ez az előző állítás „tükörképe”, és épp úgy bizonyítható (csak a rendezés irányát kell megfordítani).
(4) Ha t az s közvetlen rákövetkezője és ψ igaz t-ben, akkor $\perp$ igaz az összes $(s, t) = \emptyset$-beli állapotban. Fordítva, ha $\mathcal{M} \models_s \perp \mathcal{U}\, \psi$, akkor van olyan $t > s$ állapot, ahol ψ is igaz és amire az (s, t) intervallum üres, mivel $\perp$ hamis minden állapotban.
(5) Ez az előző állítás tükörképe. $\square$

7. 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). Vagyis B hazudik, A bármi lehet.

1.2 B nem lehet lovag (mert akkor lókötő is lenne), tehát lókötő, tehát hazudott, azaz nem igaz, hogy mindketten lókötők, vagyis A lovag. Vagyis A lovag, B lókötő. (És tényleg! Különben igaza lenne!)

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. Vagyis B lovag, A lókötő.

2.18 $\{p, \neg p\}$

2.19 $\{p \vee q, \neg p, \neg q\}$

2.20 $\{p_1 \vee \cdots \vee p_{n-1}, \neg p_1, \ldots, \neg p_{n-1}\}$

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

2.22
(1) Nem, pl. $\varphi = p$, $\psi = \neg p$. De fordítva persze igen.
(2) Hát persze.
(3) Nem: pl. $\varphi = p$, $\psi = \bot$.
(4) Igen.

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

2.24

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.

2.46 Nincs, mert ha kielégíthetetlen, akkor a kompaktsági tétel miatt van véges (és így valódi) kielégíthetetlen részhalmaza.

3.15 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 3.11 miatt következik az állítás.

5.29 Legyen $\Sigma = \{\sigma_n : n \in \mathbb{N}\}$, ahol σ_n azt mondja, hogy az univerzum legalább n elemű. Tehát pl. σ_3 lehet ez: $\exists x \exists y \exists z (x \neq y \wedge x \neq z \wedge y \neq z)$.