МАТЕМАТИЧКА ЛОГИКА У РАЧУНАРСТВУ

Небојша Икодиновић

– Белешке, 2020/21 –

Испитна питања 2020/21

1. Операцијско-релацијске структуре (хомоморфизми, утапања, изоморфизми . . .)
2. Подструктуре
3. Терми. Терм алгебра
4. Атомске формуле. Канонски модел (дијаграми)
5. Формуле првог реда. Дефинабилни скупови, Ваљане формуле
6. Нормалне форме. Сколемизација
7. Семантичка и синтаксна последица (важни примери теорија првог реда)
8. Хинтикин скуп
9. Теорема компактности. Примене теореме компактности - (не)аксиоматске класе
10. Примене теореме компактности - нестандардни модели аритметике и инфинитезималног рачуна
11. Елементарна еквивалентност. Елементарна утапања. Елементарни подмодели
12. Комплетне и ω-категоричне теорије
13. Случајни графови; 0-1 закон
14. Елиминација квантификатора

Операцијско-релацијске структуре

Логика првог реда описује такозване **операцијско-релацијске структуре**. Једну овакву структуру чини скуп заједно са неким својим операцијама, релацијама и елементима (константама), па је зато схватамо као уређену четворку $\mathbf{M} = (M, \mathcal{R}, \mathcal{F}, C)$, при чему је M неки непразан скуп, $\mathcal{R}$ скуп неких релација скупа M, $\mathcal{F}$ скуп неких операција скупа M и $C \subseteq M$. Скуп M се назива *доменом*, док се елементи скупа C називају *константама* структуре $\mathbf{M}$. Подсећамо да свака операција и свака релација има своју дужину: n-арна операција скупа M јесте функција $f : M^n \to M$, а n-арна релација скупа M јесте подскуп $R \subseteq M^n$.[1] Када је $\mathcal{R} = \{R_1, \ldots, R_k\}$, $\mathcal{F} = \{F_1, \ldots, F_\ell\}$ и $C = \{c_1, \ldots, c_m\}$, тј. $\mathcal{R}$, $\mathcal{F}$ и $\mathcal{C}$ су коначни скупови, уместо записа $\mathbf{M} = (M, \{R_1, \ldots, R_k\}, \{F_1, \ldots, F_\ell\}, \{c_1, \ldots, c_n\})$ краће пишемо

$$\mathbf{M} = (M, R_1, \ldots, R_k, F_1, \ldots, F_m, c_1, \ldots, c_n).$$

[1] Скуп свих релација над непразним скупом M је $\bigcup_{n \in N} \mathcal{P}(M^n)$, а скуп свих операција скупа M је $\bigcup_{n \in N} \{f | f : M^n \to M\}$.

Ако структуру чини само домен са операцијама и константама, без релација, онда је називамо *алгебром*.

Моделе ћемо обележавати $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$, по потреби са индексима, а њихове домене редом са $A, B, C, \ldots$, са одговарајућим индексима.

Кардиналност модела је кардиналност његовог домена. Тако, кажемо да је модел $\mathbf{M}$ коначан (пребројив, кардиналности κ) ако је његов домен M коначан (пребројив, кардиналности κ).

Најједноставнија класификација поменутих структура врши се према језику структуре, односно према броју и дужини релација и операција, као и броју константи које учествују у њиховој дефиницији. Другим речима, врсту неке структуре одређујемо избором три међусобно дисјунктна скупа чију ћемо унију називати *језиком* структуре и обележавати је са $\mathcal{L}$. *Језик* је сваки скуп $\mathcal{L} = \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L} \cup \mathrm{Const}_\mathcal{L}$, где су $\mathrm{Rel}_\mathcal{L}$, $\mathrm{Fun}_\mathcal{L}$, $\mathrm{Const}_\mathcal{L}$ међусобно дисјунктни скупови. Елементи скупа $\mathrm{Rel}_\mathcal{L}$ називају се *релацијски знаци*, елементи скупа $\mathrm{Fun}_\mathcal{L}$ *операцијски (функцијски) знаци*, а елементи скупа $\mathrm{Const}_\mathcal{L}$ *симболи константи*. За сваки језик $\mathcal{L}$, на скупу $\mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L}$ дефинисана је функција $\mathtt{ar} : \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L} \to \mathbb{N}$ која сваком знаку $S \in \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L}$ придружује неки природан број $\mathtt{ar}(S)$, тзв. *дужину* („*арност*") знака S.

Нека је $\mathcal{L}$ језик и M неки непразан скуп. **Интерпретација** језика $\mathcal{L}$ на скупу M јесте свака функција $\mathcal{I}_M$ са доменом $\mathcal{L}$ која сваком $R \in \mathrm{Rel}_\mathcal{L}$ придружује једну $\mathtt{ar}(R)$-арну релацију скупа M, тј. $\mathcal{I}_M(R) \subseteq M^{\mathrm{ar}(R)}$, сваком $F \in \mathrm{Fun}_\mathcal{L}$ придружује једну $\mathtt{ar}(F)$-арну операцију скупа M, тј. $\mathcal{I}_M(F) : M^{\mathrm{ar}(F)} \to M$ и сваком $c \in \mathrm{Const}_\mathcal{L}$ један елемент скупа M, тј. $\mathcal{I}_M(c) \in M$. **Модел** језика $\mathcal{L}$ над непразним скупом M је

$$\mathbf{M} = (M, \{\mathcal{I}_M(R) \mid R \in \mathrm{Rel}_{\mathcal{L}}\}, \{\mathcal{I}_M(F) \mid F \in \mathrm{Fun}_{\mathcal{L}}\}, \{\mathcal{I}_M(c) \mid c \in \mathrm{Const}_{\mathcal{L}}\}),$$

где је $\mathcal{I}_M$ нека интерпретација језика $\mathcal{L}$ на скупу M. Дакле, сваки модел неког језика једнозначно је одређен скупом M и интерпретацијом $\mathcal{I}_M$ тог језика у датом скупу. Ако је $\mathbf{M}$ модел језика $\mathcal{L}$ одређен неком интерпретацијом $\mathcal{I}_M$, за сваки $S \in \mathcal{L}$ уместо $\mathcal{I}_M(S)$ краће се пише $S^{\mathbf{M}}$.[2]

[2] Треба приметити да S и $S^{\mathbf{M}}$ имају потуно различити смисао; S је само симбол, знак, док је $S^{\mathbf{M}}$ скуповни објекат. Ипак, када то контекст допушта, користићемо исти знак да означимо симбол језика $\mathcal{L}$, као и његову интерпретацију у неком моделу језика $\mathcal{L}$, а то значи да ћемо, када нема опасности од забуне, уместо $S^{\mathbf{M}}$ писати само S, али ће се из контекста видети да ли је $S \in \mathcal{L}$ или је S интерпретација неког симбола језика $\mathcal{L}$. Често ћемо убудуће говорити о некој структури $\mathbf{M}$ без експлицитног навођења одговарајућег језика. Из дефиниције модела биће јасно о којем језику је реч.

Пример 1. Нека је $\mathcal{L} = \{\leqslant, +, \cdot, 0, 1\}$, при чему је $\mathrm{Rel}_{\mathcal{L}} = \{\leqslant\}$, $\mathrm{Fun}_{\mathcal{L}} = \{+, \cdot\}$, $\mathrm{Const}_{\mathcal{L}} = \{0, 1\}$ и $\mathrm{ar}(\leqslant) = \mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$. Бирајући један овакав језик, тј. користећи наведене ознаке за симболе језика, углавном ћемо прећутно указивати да желимо да описујемо неки скуп бројева заједно са уобичајеним уређењем, сабирањем и множењем, и константама 0 и 1. Један такав модел јесте $\mathbf{R} = (\mathbb{R}, \leqslant, +, \cdot, 0, 1)$. Посебно наглашавамо да $\leqslant$ у запису $\mathbf{R} = (\mathbb{R}, \leqslant, +, \cdot, 0, 1)$ означава **конкретну бинарну релацију скупа реалних бројева**, док $\leqslant$ као елемент језика $\mathcal{L}$ означава само **знак који називамо релацијским и коме је придружен природан број** 2 и ништа више; иста напомена важи и за знаке $+, \cdot, 0, 1$. Иако би требало приликом навођења структуре $\mathbf{R}$, уместо $\leqslant$, $+$, $\cdot$, 0 и 1 писати редом $\leqslant^{\mathbf{R}}$, $+^{\mathbf{R}}$, $\cdot^{\mathbf{R}}$, $0^{\mathbf{R}}$ и $1^{\mathbf{R}}$, то не чинимо јер бисмо на тај начин непотребно компликовали запис, нарочито када нас једно овакво скраћивање не може збунити.

Исти језик можемо интерпретирати и на скупу целих бројева $\mathbb{Z}$, тј. посматрати модел $\mathbf{Z} = (\mathbb{Z}, \leqslant, +, \cdot, 0, 1)$. И овога пута, уместо, на пример $\leqslant^{\mathbf{Z}}$ пишемо само $\leqslant$.

Наравно, језик може да послужи за описивање великог броја сасвим другачијих структура, тј. било које структуре коју чине једна бинарна релација, две бинарне операције и два конкретна елемента домена. Нови пример такве структуре јесте $\mathbf{X} = (\{a, b, c\}, \lhd, *, \circ, a, b)$, где је $\lhd = \{(a,a), (b,b), (c,c), (a,b), (b,c), (a,c)\}$, а операције $*$ и $\circ$ су задате следећим таблицама.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\circ$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

У овом случају[3], релацијски знак $\leqslant$ дужине 2 тумачи (интерпретира) се у скупу $X = \{a, b, c\}$ као бинарна релација $\lhd$ скупа X ($\leqslant^{\mathbf{X}} = \lhd$), операцијски знаци $+$ и $\cdot$ дужине 2 редом као бинарне операције $*$ и $\circ$ скупа X ($+^{\mathbf{X}} = *$ и $\cdot^{\mathbf{X}} = \circ$), а симболи константи 0 и 1 као елементи a и b скупа X ($0^{\mathbf{X}} = a$ и $1^{\mathbf{X}} = b$).

[3] Приметимо да је $\mathbf{X}$ само једна од 1 785 233 613 312 могућих интерпретација језика $\mathcal{L}$ у трочланом скупу $X = \{a, b, c\}$. Наравно, исти језик можемо интерпретирати и у скупу реалних бројева $\mathbb{R}$ на неограничен број начина.

Ако су $\mathcal{L}'$ и $\mathcal{L}''$ језици и $\mathcal{L}' \subseteq \mathcal{L}''$, тада се $\mathcal{L}'$ назива *редукт* језика $\mathcal{L}''$, а $\mathcal{L}''$ *експанзија* језика $\mathcal{L}'$. Ако је $\mathcal{L}' \subseteq \mathcal{L}''$ а $Rel_{\mathcal{L}'} = Rel_{\mathcal{L}''}$ и $Fun_{\mathcal{L}'} = Fun_{\mathcal{L}''}$ онда је $\mathcal{L}''$ *проста експанзија* језика $\mathcal{L}'$. Ако је $\mathcal{L}''$

(проста) експанзија језика $\mathcal{L}'$ а $\mathbf{M}'$ и $\mathbf{M}''$ редом модели језика $\mathcal{L}$ и $\mathcal{L}'$ над истим скупом $M = M' = M''$ и сваки симбол језика $\mathcal{L}'$ је интерпретиран на исти начин у оба модела, тада је модел $\mathbf{M}''$ (проста) експанзија модела $\mathbf{M}'$, док је $\mathbf{M}'$ (прост) редукт модела $\mathbf{M}''$. Дакле, ако је $\mathcal{L}' \subseteq \mathcal{L}''$ и $\mathbf{M}''$ модел језика $\mathcal{L}''$ испуштањем $S^{\mathbf{M}''}$ за $S \in \mathcal{L}'' \setminus \mathcal{L}'$ из "списка" релација, операција и константи модела $\mathbf{M}''$ добијамо нов модел $\mathbf{M}$ који је редукт модела $\mathbf{M}''$. Слично, ако је $\mathcal{L}' \subseteq \mathcal{L}''$ и $\mathbf{M}''$ модел језика $\mathcal{L}''$ који је експанзија модела $\mathbf{M}'$, језика $\mathcal{L}'$, онда ћемо писати $\mathbf{M}'' = (\mathbf{M}', S^{\mathbf{M}''})_{S \in \mathcal{L}'' \setminus \mathcal{L}'}$ или $\mathbf{M}'' = (\mathbf{M}', S_1^{\mathbf{M}''}, \dots, S_k^{\mathbf{M}''})$ ако је $\mathcal{L}'' \setminus \mathcal{L}' = \{S_1, \dots, S_k\}$. Алгебарски редукт модела $\mathbf{M}$ језика $\mathcal{L}$ је редукт модела $\mathbf{M}$ на алгебарски део језика $\mathcal{L}$.

Хомоморфизми

Нека су $\mathbf{A}$ и $\mathbf{B}$ модели истог језика $\mathcal{L}$. *Хомоморфизам* модела $\mathbf{A}$ у модел $\mathbf{B}$ је свако пресликавање $f : A \to B$ такво да:

(1) ако $R \in \mathrm{Rel}_{\mathcal{L}}$, онда за све $a_1, \dots, a_n \in A$, где је $n = ar(R)$,

$$\text{из } R^{\mathbf{A}}(a_1, \dots, a_n) \text{ следи да је и } R^{\mathbf{B}}(f(a_1), \dots, f(a_n));$$

(2) ако $F \in \mathrm{Fun}_{\mathcal{L}}$, онда за све $a_1, \dots, a_n \in A$, где је $n = ar(F)$, важи

$$f(F^{\mathbf{A}}(a_1, \dots, a_n)) = F^{\mathbf{B}}(f(a_1), \dots, f(a_n));$$

(3) ако је $c \in \mathrm{Const}_{\mathcal{L}}$, онда је $f(c^{\mathbf{A}}) = c^{\mathbf{B}}$.

Ако је $f : A \to B$ хоморфизам модела $\mathbf{A}$ у модел $\mathbf{B}$, онда користимо ознаку $f : \mathbf{A} \to \mathbf{B}$. Скуп свих хомоморфизама из $\mathbf{A}$ у $\mathbf{B}$ обележавамо са $Hom(\mathbf{A}, \mathbf{B})$.

Хомоморфизам $f : \mathbf{A} \to \mathbf{B}$ је:

(i) *јак хоморфизам* ако за све $R \in \mathrm{Rel}_{\mathcal{L}}$ и за све $a_1, \dots, a_n \in A$, где је $n = ar(R)$,важи: $R^{\mathbf{A}}(a_1, \dots, a_n)$ ако и само ако $R^{\mathbf{B}}(f(a_1), \dots, f(a_n))$;

(ii) *епиморфизам* ако је $f : A \to B$ *на* пресликавање и у том случају користимо ознаку $f : \mathbf{A} \overset{\mathrm{na}}{\to} \mathbf{B}$;

(iii) *утапање* ако је f јак хомоморфизам и $1-1$ пресликавање и у том случају користимо ознаку $f : \mathbf{A} \hookrightarrow \mathbf{B}$;

(iv) *изоморфизам* ако је f јак хомоморфизам и бијекција и у том случају користимо ознаку $f : \mathbf{A} \cong \mathbf{B}$.

Хомоморфизам $f : \mathbf{M} \to \mathbf{M}$ назива се *унутрашњи хомоморфизам* или *ендоморфизам* модела $\mathbf{M}$. Скуп свих ендоморфизама модела $\mathbf{M}$ означава се са $End(\mathbf{M})$. Изоморфизам $f : \mathbf{M} \cong \mathbf{M}$ назива се *аутоморфизам* модела $\mathbf{M}$. Скуп свих аутоморфизама модела $\mathbf{M}$ означава се са $Aut(\mathbf{M})$.

Модели $\mathbf{A}$ и $\mathbf{B}$ истог језика су изоморфни, у ознаци $\mathbf{A} \cong \mathbf{B}$, ако постоји пресликавање $f : A \to B$ тако да је $f : \mathbf{A} \cong \mathbf{B}$. Модел $\mathbf{A}$

се утапа у модел $\mathbf{B}$, у ознаци $\mathbf{A} \hookrightarrow \mathbf{B}$, ако постоји пресликавање $f : A \to B$ тако да је $f : \mathbf{A} \hookrightarrow \mathbf{B}$.

Лема 1. *Нека су* $\mathbf{A}$, $\mathbf{B}$ *и* $\mathbf{C}$ *модели истог језика. Доказати:*
(a) Ако $f : \mathbf{A} \to \mathbf{B}$ *и* $g : \mathbf{B} \to \mathbf{C}$, *онда* $h = g \circ f : \mathbf{A} \to \mathbf{C}$.
(b) Ако $f : \mathbf{A} \overset{\text{na}}{\to} \mathbf{B}$ *и* $g : \mathbf{B} \overset{\text{na}}{\to} \mathbf{C}$, *онда* $h = g \circ f : \mathbf{A} \overset{\text{na}}{\to} \mathbf{C}$
(c) Ако $f : \mathbf{A} \hookrightarrow \mathbf{B}$ *и* $g : \mathbf{B} \hookrightarrow \mathbf{C}$, *онда* $h = g \circ f : \mathbf{A} \hookrightarrow \mathbf{C}$
(d) Ако $f : \mathbf{A} \cong \mathbf{B}$ *и* $g : \mathbf{B} \cong \mathbf{C}$, *онда* $h = g \circ f : \mathbf{A} \cong \mathbf{C}$

Лема 2. *Ако* $f : \mathbf{A} \cong \mathbf{B}$, *доказати да* $f^{-1} : \mathbf{B} \cong \mathbf{A}$.

Задатак **1.** Ако је $N_0 = N \cup \{0\}$, $+$ и $\cdot$ редом сабирање и множење, а $\leq$ уобичајено уређење скупа N_0, испитати да ли је:

1) $(N_0, \leq, +, 0) \hookrightarrow (N_0, \leq, \cdot, 1)$

2) $(N_0, \leq, \cdot, 1) \hookrightarrow (N_0, \leq, +, 0)$

Задатак **2.** Навести пример модела $\mathbf{A}$ и $\mathbf{B}$ истог језика и хомоморфизма $f : \mathbf{A} \to \mathbf{B}$ који није јак хомоморфизам.
Задатак **3.** Нека су $\mathbf{A}$ и $\mathbf{B}$ модели језика $\mathcal{L}$ и $f : \mathbf{A} \hookrightarrow \mathbf{B}$. Доказати да постоји:

1) модел $\mathbf{A}^*$, тако да је $\mathbf{A}^* \subseteq \mathbf{B}$ и $\mathbf{A} \cong \mathbf{A}^*$;

2) модел $\mathbf{B}^*$, тако да је $\mathbf{A} \subseteq \mathbf{B}^*$ и $\mathbf{B} \cong \mathbf{B}^*$.

Задатак **4.** Нека је R скуп реалних бројева, $+$ сабирање а $\leq$ уобичајено уређење реалних бројева. Нека је

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

1) Доказати да је $\mathbb{Q}(\sqrt{2})$ подмодел модела $(\mathbb{R}, \leq, +, 0, 1)$.

2) Одредити $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}), \leq, +, 0)$.

3) Одредити $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}), \leq, +, 0, 1)$.

Подструктуре

Дефиниција 1. *Нека су* $\mathbf{A}$ *и* $\mathbf{B}$ *модели истог језика и* $A \subseteq B$. *Структура* $\mathbf{A}$ *је подмодел (подструктура) од* $\mathbf{B}$, *у ознаци* $\mathbf{A} \subseteq \mathbf{B}$ *ако је инклузионо пресликавање* $i_A : A \to B$, *дато са* $i_A(a) = a$, $a \in A$, *утапање.*

Лема 3. *Нека су* $\mathbf{M}$ *и* $\mathbf{D}$ *модели истог језика* $\mathcal{L}$. $\mathbf{D} \subseteq \mathbf{M}$ *акко је* $D \subseteq M$ *и важе следећи услови:*

(1) за сваки $R \in \mathrm{Rel}_{\mathcal{L}}$, $R^{\mathbf{D}} = R^{\mathbf{M}} \cap D^{ar(R)}$;

(2) за сваки $F \in \mathrm{Fun}_{\mathcal{L}}$, $F^{\mathbf{D}} = F^{\mathbf{M}} \lceil D^{ar(F)}$, *тј. за све* $d_1, \ldots, d_n \in D$, *где је* $n = ar(F)$, *је* $F^{\mathbf{D}}(d_1, \ldots, d_n) = F^{\mathbf{M}}(d_1, \ldots, d_n)$;

(3) за сваки $c \in \mathrm{Const}_{\mathcal{L}}$, $c^{\mathbf{D}} = c^{\mathbf{M}}$.

Доказ. ($\rightarrow$) Претпоставимо да је $\mathbf{D} \subseteq \mathbf{D}$, тј. према претходној дефиницији, да је $D \subseteq M$ и $i_D : \mathbf{D} \hookrightarrow \mathbf{M}$. Докажимо услове (1), (2) и (3).
(1) За сваки симбол $R \in \mathrm{Rel}_{\mathcal{L}}$, $ar(R) = n$ и све $a_1, \ldots, a_n \in D$ важи:

$$R^{\mathbf{D}}(a_1, \ldots, a_n) \text{ акко } R^{\mathbf{M}}(i_D(a_1), \ldots, i_D(a_n)),$$

тј. $R^{\mathbf{D}}(a_1, \ldots, a_n)$ акко $R^{\mathbf{M}}(a_1, \ldots, a_n)$, па је $R^{\mathbf{D}} = R^{\mathbf{M}} \cap D^{ar(R)}$.
(2) За сваки симбол $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$ и све $a_1, \ldots, a_n \in D$ важи:

$$i_D(F^{\mathbf{D}}(a_1, \ldots, a_n)) = F^{\mathbf{M}}(i_D(a_1), \ldots, i_D(a_n)).$$

Према дефиницији инклузионог пресликавања имамо $i_D(a_i) = a_i$, $i = \overline{1, n}$, и $i_D(F^{\mathbf{D}}(a_1, \ldots, a_n)) = F^{\mathbf{D}}(a_1, \ldots, a_n)$, па је:

$$F^{\mathbf{D}}(a_1, \ldots, a_n) = F^{\mathbf{M}}(a_1, \ldots, a_n),$$

тј. $F^{\mathbf{M}} \upharpoonright D^{ar(F)} = F^{\mathbf{D}}$.
(3) За сваки симбол константе c важи:
$i_D(c^{\mathbf{D}}) = c^{\mathbf{M}}$, јер је i_D хомоморфизам;
$i_D(c^{\mathbf{D}}) = c^{\mathbf{D}}$, према дефиницији инклузионог пресликавања i_D. Дакле, $c^{\mathbf{D}} = c^{\mathbf{M}}$.
($\leftarrow$) Претпоставимо да је $D \subseteq M$ и да важе услови (1), (2) и (3). Остављамо за вежбу доказ да је инклузионо пресликавање $i_D : D \rightarrow M$, $i_D(a) = a$, $a \in D$, утапање структуре $\mathbf{D}$ у $\mathbf{M}$. □

Лема 4. *Нека је* $\mathbf{M}$ *модел језика* $\mathcal{L}$ *и* $\emptyset \neq D \subseteq M$. *Постоји јединствен модел* $\mathbf{D}$ *језика* $\mathcal{L}$ *са доменом* D *такав да је* $\mathbf{D} \subseteq \mathbf{M}$ *ако важе следећа два услова:*

(1) за свако $c \in \mathrm{Const}_{\mathcal{L}}$, $c^{\mathbf{M}} \in D$;

(2) за свако $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$, *и све* $d_1, \ldots, d_n \in D$, $F^{\mathbf{M}}(d_1, \ldots, d_n) \in D$.

Доказ. Ако важе услови (1) и (2), $\mathcal{L}$-структуру над скупом D дефинишмо на следећи начин:

- за сваки симбол $R \in \mathrm{Rel}_{\mathcal{L}}$, $ar(R) = n$, и све $d_1, \ldots, d_n \in D$,

$$R^{\mathbf{D}}(d_1, \ldots, d_n) \overset{\text{def}}{\Leftrightarrow} R^{\mathbf{M}}(d_1, \ldots, d_n)$$

- за сваки симбол $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$, и све $d_1, \ldots, d_n \in D$, $F^{\mathbf{D}}(d_1, \ldots, d_n) \overset{\text{def}}{=} F^{\mathbf{M}}(d_1, \ldots, d_n)$.

- за сваки симбол $c \in \mathrm{Const}_{\mathcal{L}}$, $c^{\mathbf{D}} \overset{\text{def}}{=} c^{\mathbf{M}}$

Једноставно се доказује да је $\mathbf{D} \subseteq \mathbf{M}$. □

Задатак **5.** Ако је $f : \mathbf{A} \to \mathbf{B}$ доказати да је $f[A] = \{f(a) | a \in A\}$ подмодел модела $\mathbf{B}$.
Задатак **6.** Доказати да за сваки $n \in N$ постоји групоид који има тачно n елемената и нема прави подгрупоид.
Задатак **7.** Доказати да постоји пребројив групоид који нема прави подгрупоид.
Задатак **8.** Наћи пример бесконачног модела чији је сваки прави подмодел (1) бесконачан; (2) коначан.

Према претходној леми, сваки подмодел неког модела у потпуности одређен својим доменом. Наиме, ако је $\mathbf{D}_1$, $\mathbf{D}_2 \subseteq \mathbf{M}$ и $D_1 = D_2$, онда је и $\mathbf{D}_1 = \mathbf{D}_2$. Отуда, уместо $\mathbf{D} \subseteq \mathbf{M}$ често пишемо да је $D \subseteq \mathbf{M}$ и кажемо да је подскуп $D \subseteq M$ подмодел модела $\mathbf{M}$. Ако је $D \subseteq \mathbf{M}$ и $D \neq M$, кажемо да је D *прави* подмодел модела $\mathbf{M}$.

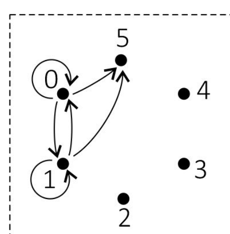
Последица 1. *Нека је $\mathcal{L}$ језик који садржи само релацијске знаке и $\mathbf{M}$ модел језика $\mathcal{L}$. Сваки непразан подскуп $D \subseteq M$ подмодел модела $\mathbf{M}$.*

Лема 5. *Нека је $\mathbf{M}$ модел језика $\mathcal{L}$ и $\mathcal{D} \subseteq \mathcal{P}(M)$ непразна колекција подмодела модела $\mathbf{M}$, тј. за сваки $D \in \mathcal{D}$, $D \subseteq \mathbf{M}$. Доказати да је $\bigcap \mathcal{D} \subseteq \mathbf{M}$.*

Нека је $\mathbf{M}$ модел језика $\mathcal{L}$ и X непразан подскуп скупа M. Пошто је колекција $\mathcal{D} = \{D | D \subseteq \mathbf{M}, X \subseteq D\}$ непразна (јер $\mathbf{M} \in \mathcal{D}$) колекција подмодела модела $\mathbf{M}$, скуп $\langle X \rangle_M = \bigcap \mathcal{D}$ је, према претходном задатку домен подмодел модела $\mathbf{M}$, који означавамо са $\langle X \rangle_{\mathbf{M}}$. Дакле, модел $\langle X \rangle_{\mathbf{M}}$ је јединствено одређен и назива се *подмодел модела* $\mathbf{M}$ *генерсан скупом* X. Скуп $X \subseteq M$ је *скуп генератора* модела $\mathbf{M}$ ако је $\langle X \rangle_{\mathbf{M}} = \mathbf{M}$. Ако је X коначан скуп генератора за $\mathbf{M}$, кажемо да је модел $\mathbf{M}$ *коначно генерисан*.
Задатак **9.** Нека је $D_1 \subseteq D_2 \subseteq \cdots \subseteq D_n \subseteq \ldots$ низ подмодела модела $\mathbf{M}$. Доказати да је $\cup_{n \in N} D_n$ подмодел модела $\mathbf{M}$.
Задатак **10.** Ако је модел $\mathbf{M}$ коначно генерисан и $D_1 \subseteq D_2 \subseteq \ldots$ низ подмодела од $\mathbf{M}$ такав да је $M = \cup_{n \in N} D_n$, доказати да постоји природан број m такав да је $M = \cup_{i=1}^{m} D_i$.
Задатак **11.** Дате су две структуре:
$(\{0, 1, 2, 3, 4, 5\}, *, \leqslant)$

$*$	0	1	2	3	4	5
0	1	0	2	3	3	4
1	1	1	3	4	2	2
2	5	5	0	1	0	5
3	5	5	1	1	1	5
4	5	5	1	1	0	5
5	3	2	0	0	1	5

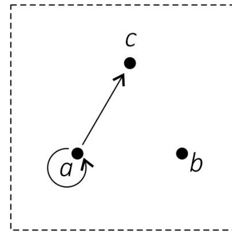
$\leqslant$	0	1	2	3	4	5
0	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
1	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
2	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
3	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
4	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
5	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$



$(\{a,b,c\},\star,\sqsubseteq)$

$\star$	a	b	c
a	a	b	b
b	c	a	c
c	b	a	c

$*$	a	b	c
a	$\top$	$\bot$	$\top$
b	$\bot$	$\bot$	$\bot$
c	$\bot$	$\bot$	$\bot$



Да ли је $f:\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ a & a & b & b & b & c \end{pmatrix}$ хомоморфизам?

Терми. Терм алгебра

Дефиниција 2. *Скуп свих* ***израза*** *језика $\mathcal{L}$, у ознаци $\mathrm{Term}_{\mathcal{L}}$, јесте* *<u>најмањи</u> скуп коначних низова (логичких и нелогичких) симбола такав да:*

- $\mathrm{Const}_{\mathcal{L}} \subseteq \mathrm{Term}_{\mathcal{L}}$ *и* $\mathrm{Var} \subseteq \mathrm{Term}_{\mathcal{L}}$ *(односно, променљиве и симболи константи су изрази језика $\mathcal{L}$);*
- *ако* $F \in \mathrm{Fun}_{\mathcal{L}}$ *и* $t_1, \dots, t_{\mathrm{ar}(F)} \in \mathrm{Term}_{\mathcal{L}}$, *онда* $F(t_1, \dots, t_{\mathrm{ar}(F)}) \in \mathrm{Term}_{\mathcal{L}}$

Приметимо да је дефиниција израза (терма) индуктивна, и да су скупови израза различити за различите изборе језика (сигнатуре) $\mathcal{L}$. Природно се дефиниче сложеност израза.

Ако је $t \in \mathrm{Term}_{\mathcal{L}}$, са $V(t)$ означићемо скуп оних променљивих које учествују у грађењу терма t. Наравно, за сваки терм t, скуп $V(t)$ је коначан. Функцију $V : \mathrm{Term}_{\mathcal{L}} \to \mathcal{P}(\mathrm{Var})$ дефинишемо индуктивно:

- $V(x) = \{x\}$, за свако $x \in \mathrm{Var}$; $V(c) = \emptyset$, за свако $c \in \mathrm{Const}_{\mathcal{L}}$;
- $V(F(t_1, \dots, t_{\mathrm{ar}(F)})) = V(t_1) \cup \dots \cup V(t_{\mathrm{ar}(F)})$, за све $F \in \mathrm{Fun}_{\mathcal{L}}$ и $t_1, \dots, t_{\mathrm{ar}(F)} \in \mathrm{Term}_{\mathcal{L}}$.

Да бисмо одређивали вредности израза потребно је да прецизирамо контекст у коме изразе посматрамо. То чинимо тако што изаберемо неки скуп M (тзв. домен интерпретације), а затим на том скупу интерпретирамо нелогичке симболе и променљивама доделимо неке елементе скупа M.

Валуација променљивих у скупу M јесте свака функција $v : \mathrm{Var} \to M$. Ако је задат модел $\mathbf{M}$ језика $\mathcal{L}$ и валуација $v : \mathrm{Var} \to M$, онда сваком изразу $t \in \mathrm{Term}_{\mathcal{L}}$ придружујемо јединствену вредност $t^{\mathbf{M}}[v] \in M$ коју називамо *вредност израза t у моделу $\mathbf{M}$ за валуацију v.* Функцију $t \mapsto t^{\mathbf{M}}[v]$ дефинишемо индукцијом по сложености израза t:

- $x^{\mathbf{M}}[v] = v(x)$, $x \in \mathrm{Var}$;
- $c^{\mathbf{M}}[v] = c^{\mathbf{M}}$, $c \in \mathrm{Const}_{\mathcal{L}}$;
- $\Big(F(t_1, \dots, t_{\mathrm{ar}(F)})\Big)^{\mathbf{M}}[v] = F^{\mathbf{M}}(t_1^{\mathbf{M}}[v], \dots, t_{\mathrm{ar}(F)}^{\mathbf{M}}[v])$, $F \in \mathrm{Fun}_{\mathcal{L}}$, $t_1, \dots, t_{\mathrm{ar}(F)} \in \mathrm{Term}_{\mathcal{L}}$.

Лема 6. *Нека је $\mathbf{M}$ произвољан модел језика $\mathcal{L}$ и $v_1, v_2 : \mathrm{Var} \to M$ две валуације. За сваки израз $t \in \mathrm{Term}_{\mathcal{L}}$, ако је $v_1(v) = v_2(v)$, за све $v \in V(t)$, онда је $t^{\mathbf{M}}[v_1] = t^{\mathbf{M}}[v_2]$.*

На вредност израза у неком моделу утичу само вредности променљивих које се појављују у том изразу.

Претходна лема се једноставно доказује индукцијом по сложености израза.

Из претходне леме закључујемо да је при одређивању вредности израза t у моделу $\mathbf{M}$ за валуацију $v : \mathrm{Var} \to M$ значајна само рестрикција $v \upharpoonright_{V(t)}$. Како је $V(t)$ коначан скуп, тј. $|V(t)| = n$, за неки природан број n, онда одговарајуће рестрикције свих валуација можемо идентификовати са скупом M^n, јер је при неком подразумеваном уређењу променљивих $V(t) = \{x_1, \ldots, x_n\}$ сваким $\vec{a} = (a_1, \ldots, a_n) \in M^n$ одређена рестрикција $v = \begin{pmatrix} x_1 & \cdots & x_n \\ a_1 & \cdots & a_n \end{pmatrix}$. Наведени разлози оправдавају употребу ознаке $t^{\mathbf{M}}[\vec{a}]$ за вредност израза t у моделу $\mathbf{M}$ за $\vec{a} \in M^n$.

Ако је $V(t) = \emptyset$, тј. ако је t тзв. *затворени израз* (израз без променљивих), при одређивању његове вредност у неком моделу валуације не играју никакву улогу (за било које две валуације v_1 и v_2 важи $t^{\mathbf{M}}[v_1] = t^{\mathbf{M}}[v_2]$). Другим речима, вредност затвореног израза t потпуно је одређена само изабраним моделом $\mathbf{M}$ и ту вредност означавамо са $t^{\mathbf{M}}$.

Лема 7. *Нека су* $\mathbf{A}$ *и* $\mathbf{B}$ *неке* $\mathcal{L}$*-структуре.*

1. *Ако* $f : \mathbf{A} \to \mathbf{B}$, *онда за сваки израз* t *и сваку валуацију* $v : \mathrm{Var} \to A$, $f(t^{\mathbf{A}}[v]) = t^{\mathbf{B}}[f \circ v]$.

2. *Ако је* $\mathbf{A} \subseteq \mathbf{B}$, *онда за сваки израз* t *и сваку валуацију* $v : \mathrm{Var} \to A$, $t^{\mathbf{B}}[v] \in A$.

3. *За сваки подскуп* $X \subseteq A$,
$$\langle X \rangle_{\mathbf{A}} = \{t^{\mathbf{A}}[v] \mid t \in \mathrm{Term}_{\mathcal{L}}, v : \mathrm{Var} \to X\}.$$

Доказ. 1) Индукцијом по сложености терма t.

Ако је t симбол константе c, онда је $t^{\mathbf{A}}[v] = c^{\mathbf{A}}$ и $t^{\mathbf{B}}[f \circ v] = c^{\mathbf{B}}$. Пошто је f хомоморфизам: $f(c^{\mathbf{A}}) = c^{\mathbf{B}}$.

Ако је t променљива x, онда је $t^{\mathbf{A}}[v] = v(x)$ и $t^{\mathbf{B}}[f \circ v] = f \circ v(x) = f(v(x))$.

Нека је t облика $F(t_1, \ldots, t_{\mathrm{ar}(F)})$, за неке $F \in \mathrm{Fun}_{\mathcal{L}}$ и $t_1, \ldots, t_{\mathrm{ar}(F)} \in \mathrm{Term}_{\mathcal{L}}$ и претпоставимо да тврђење важи за све терме сложености мање од сложености терма t. Тада:

Индуктивна претпоставка!

$$\begin{aligned} f(t^{\mathbf{A}}[v]) &= f(F^{\mathbf{A}}(t_1^{\mathbf{A}}[v], \ldots, t_{\mathrm{ar}(F)}^{\mathbf{A}}[v]) \\ &= F^{\mathbf{B}}(f(t_1^{\mathbf{A}}[v]), \ldots, f(t_{\mathrm{ar}(F)}^{\mathbf{A}}[v]) \quad [\text{јер је } f \text{ хомоморфизам}] \\ &= F^{\mathbf{B}}(t_1^{\mathbf{B}}[f \circ v], \ldots, t_{\mathrm{ar}(F)}^{\mathbf{B}}[f \circ v] \quad [\text{према инд. претпоставци}] \\ &= t^{\mathbf{B}}[f \circ v] \end{aligned}$$

2) је једноставна последица 1). Из $\mathbf{A} \subseteq \mathbf{B}$, следи да је инклузионо пресликавање утапање, $i_A : \mathbf{A} \hookrightarrow \mathbf{B}$. За сваки израз t и сваку валуацију $v : \mathrm{Var} \to A$, имамо:

За $A \subseteq B$, инклузионо пресликавање $i_A : A \to B$ је дато са $i_A(x) = x$, $x \in A$.

$i_A(t^{\mathbf{A}}[v]) = t^{\mathbf{A}}[v]$, по дефиницији пресликавања i_A, као и

$i_A(t^{\mathbf{A}}[v]) = t^{\mathbf{B}}[i_A \circ v] = t^{\mathbf{B}}[v]$, јер је i_A хомоморфизам и важи $i_A \circ v = v$.

Дакле, $t^{\mathbf{A}}[v] = t^{\mathbf{B}}[v]$, одакле директно закључујемо да $t^{\mathbf{B}}[v] \in A$.

3) Нека је $\emptyset \neq X \subseteq A$ и

$$B_X = \{t^{\mathbf{A}}[v] \mid t \in \mathrm{Term}_{\mathcal{L}}, v : \mathrm{Var} \to X\}.$$

Истичемо два главна дела доказа.

3.(i) Прво доказујемо да је $X \subseteq B_X \subseteq \mathbf{A}$, тј. да је скуп X подскуп од B_X и да је B_X подструктура (тј. домен јединствене подструктуре) од $\mathbf{A}$.

3.(ii) Затим доказујемо је B_X најмањи, у смислу инклузије, подскуп од A који садржи X и одређује домен подструктуре од $\mathbf{A}$.

3.(i) Једноставно се уочава да је $X \subseteq B_X$. Треба да докажемо да се било који елемент $a \in X$ може приказати у облику $t^{\mathbf{A}}[v]$, за неки израз t, и неку валуацију $v : \mathrm{Var} \to X$. Изаберимо било који елемент $a \in X$. Ако је t променљива x и v валуација таква да је $v(x) = a$, онда је $t^{\mathbf{A}}[v] = a$, одакле следи $a \in B_X$.

$$v = \begin{pmatrix} x & \cdots \\ a & \cdot \end{pmatrix}$$

Дакле, $X \subseteq B_X$.

Да бисмо доказали $B_X \subseteq \mathbf{A}$ користимо одговарајућу лему из претходне лекције. Докажимо да за сваки симбол константе c, $c^{\mathbf{A}} \in B_X$. Ако изаберемо да t буде симбол константе c, а $v : \mathrm{Var} \to X$ произвољно, онда је $t^{\mathbf{A}}[v] = c^{\mathbf{A}}$, одакле непосредно следи да $c^{\mathbf{A}} \in B_X$.

Лема. Нека је $\mathbf{M}$ модел језика $\mathcal{L}$ и $\emptyset \neq D \subseteq M$. Постоји јединствен модел $\mathbf{D}$ језика $\mathcal{L}$ са доменом Dтакав да је $\mathbf{D} \subseteq \mathbf{M}$ ако и само ако важе следећа два услова:
(1) за свако $c \in \mathrm{Const}_{\mathcal{L}}$, $c^{\mathbf{M}} \in D$;
(2) за свако $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$, и све $d_1, \ldots, d_n \in D$, $F^{\mathbf{M}}(d_1, \ldots, d_n) \in D$.

Докажимо да за свако $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$ и све $a_1, \ldots, a_n \in B_X$, $F^{\mathbf{A}}(a_1, \ldots, a_n) \in B_X$. За свако $a_i \in B_X$, $i = \overline{1,n}$, постоји терм t_i и валуација $v_i : \mathrm{Var} \to X$, тако да је $a_i = t_i^{\mathbf{A}}[v_i]$. Без губљења општости можемо претпоставити да свака два терма t_i и t_j, $i, j = \overline{1,n}$, садрже међусобно различите променљиве, тј. $V(t_i) \cap V(t_j) = \emptyset$. Ова претпоставка нам омогућава да уводемо валуацију $v : \mathrm{Var} \to A$ која променљивама из $V(t_i)$ додељује исте вредности као и валуација v_i. Ако је $V(t_i) = \{x_{i1}, \ldots, x_{ik_i}\}$, $i = \overline{1,n}$, онда

$$v = \begin{pmatrix} x_{11} & \cdots & x_{1i_1} & \cdots & x_{n1} & \cdots & x_{ni_n} \\ v_1(x_{11}) & \cdots & v_1(x_{1i_1}) & \cdots & v_n(x_{n1}) & \cdots & v_n(x_{ni_n}) \end{pmatrix}$$

Очигледно је $a_i = t_i^{\mathbf{A}}[v_i] = t_i^{\mathbf{A}}[v]$, $i = \overline{1,n}$. Ако је t терм $F(t_1, \ldots, t_n)$, онда је $t^{\mathbf{A}}[v] = F^{\mathbf{A}}(t_1[v], \ldots, t_n[v]) = F^{\mathbf{A}}(a_1, \ldots, a_n)$, одакле следи да $F^{\mathbf{A}}(a_1, \ldots, a_n) \in B_X$.

Дакле, $B_X \subseteq \mathbf{A}$.

3.(ii) Ако је C подскуп A такав да је $X \subseteq C \subseteq \mathbf{A}$, онда за сваки терм t и сваку валуацију $v : \mathrm{Var} \to X$, $t^{\mathbf{A}}[v] \in C$, према тврђењу

(2). Сходно томе, $B_X \subseteq C$, тј. B_X је најмањи, у смислу инклузије, подскуп A који садржи X и домен је подструктуре од $\mathbf{A}$. $\square$

Пример 2. Нека је $\mathbf{A} = (\{a,b,c,d\}, F)$, при чему је F унарна операција дата са $F = \begin{pmatrix} a & b & c & d \\ a & a & b & a \end{pmatrix}$ Тада је:
$\langle\{a\}\rangle_{\mathbf{A}} = \{a, F(a), F(F(a)), F(F(F(a))), \ldots\} = \{a\}$
$\langle\{c\}\rangle_{\mathbf{A}} = \{c, F(c), F(F(c)), F(F(F(c))), \ldots\} = \{a,b,c\}$

Задатак. Нека су $\mathbf{A}$ и $\mathbf{M}$ две $\mathcal{L}$-структуре, $\emptyset \neq X \subseteq A$ и $f, g : \langle X\rangle_{\mathbf{A}} \to \mathbf{M}$. Ако је $f \restriction X = g \restriction X$, онда је $f = g$.

Нека је $X \subseteq \mathrm{Var}$ непразан скуп променљивих језика $\mathcal{L}$ (за који се углавном претпосатавља да садржи бар један опрацијски знак и бар један симбол константе). Нека је $\mathbf{T}_X$ модел језика $\mathcal{L}$ са доменом $T_X = \{t \in \mathrm{Term}_{\mathcal{L}} \mid V(t) \subseteq X\}$, такав да је:

(i) за свако $c \in \mathrm{Const}_{\mathcal{L}}$, $c^{\mathbf{T}_X} = c$;

(ii) за све $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$, и све $t_1, \ldots, t_n \in T$ нека је $F^{\mathbf{T}_X}(t_1, \ldots, t_n) = F(t_1, \ldots, t_n)$;

(iii) за све $R \in \mathrm{Rel}_{\mathcal{L}}$, нека је $R^{\mathbf{T}_X} = \emptyset$.

Овако дефинисана структура $\mathbf{T}_X$ назива се *апсолутно слободна алгебра* или *терм алгебра* језика $\mathcal{L}$ над скупом променљивих X. Уместо T_{Var}, одн. $\mathbf{T}_{\mathrm{Var}}$, пишемо краће T, одн. $\mathbf{T}$. Приметимо да је $T_\emptyset$ скуп свих затворених израза.

$T_\emptyset$ је непразан само у случају да $\mathcal{L}$ садржи бар један симбол константе.

Задатак **12.** Доказати да за сваку $\mathcal{L}$-структуру $\mathbf{M}$ и сваку функцију $f : X \to M$, постоји јединствен хомоморфизам $\overline{f} : \mathbf{T}_X \to \mathbf{M}$ који проширује функцију f.

Сваку валуацију променљивих у скупу T, $v : \mathrm{Var} \to T$ посматрамо као *супституцију*, тј. упуство којим се одређују замена променљиве одговарајућим изразом. Валуацију

$$v = \begin{pmatrix} x_1 & \cdots & x_n & \cdots \\ t_1 & \cdot & t_n & \cdots \end{pmatrix},$$

где су $t_1, \ldots, t_n$ неки изрази, означамо $[x_1/t_1, \ldots, x_n/t_n]$. Углавном ћемо посматрати супституције облика $[x/u]$ – истовремене замене променљиве x термом u; сходно томе,

$t[x/u]$ означава терм добије тако што је у терму t свако појављивање променљиве x замењено термом u.

Ако је x променљива, $a \in A$ и $v : \mathrm{Var} \to A$, онда је $v(x := a)$ валуација која свим променљивама додељује исте вредности као и v, осим променљивој x којој додељује вредност a; другим речима

$v(x := a) : \mathrm{Var} \to A$,

$$v(x := a)(y) = \begin{cases} a, & y \text{ је променљива } x \\ v(y), & \text{иначе} \end{cases}$$

Задатак **13.** Нека је $\mathbf{M}$ произвољна $\mathcal{L}$-структура, $t, u \in \mathrm{Term}_{\mathcal{L}}$ и $v : \mathrm{Var} \to M$. Тада је $t[x/u]^{\mathbf{M}}[v] = t^{\mathbf{M}}[v(x := u^{\mathbf{M}}[v])]$.

Атомске формуле. Канонски модел

Скуп *атомских (елементарних) формула* језика $\mathcal{L}$, у ознаци $\mathrm{At}_{\mathcal{L}}$, јесте скуп који садржи:

- једнакости $t = u$, за све $t, u \in \mathrm{Term}_{\mathcal{L}}$, и
- записе облика $R(t_1, \dots, t_{\mathrm{ar}(R)})$, за сваки релацијски симбол $R \in \mathrm{Rel}_{\mathcal{L}}$ и терме $t_1, \dots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$.

Ако је $\mathbf{M}$ нека $\mathcal{L}$-структура и $v : \mathrm{Var} \to M$ валуација, свакој атомској формули $\alpha \in \mathrm{At}_{\mathcal{L}}$ природно придружујемо истинитосну вредност $\alpha^{\mathbf{M}}[v] \in \{0, 1\}$ коју називамо *истинитосна вредност формуле α у моделу $\mathbf{M}$ за валуацију v.*:

- $(t = u)^{\mathbf{M}}[v] = 1$ акко $t^{\mathbf{M}}[v] = u^{\mathbf{M}}[v]$, $t, u \in \mathrm{Term}_{\mathcal{L}}$;
- $\Big(R(t_1, \dots, t_{\mathrm{ar}(R)})\Big)^{\mathbf{M}}[v] = 1$ акко $R^{\mathbf{M}}(t_1^{\mathbf{M}}[v], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[v])$, тј. $(t_1^{\mathbf{M}}[v], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[v]) \in R^{\mathbf{M}}$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \dots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$

Ако је $\rho \subseteq M^n$ нека n-арна релација скупа M, онда се уместо $(x_1, \dots, x_n) \in \rho$ често пише $\rho(x_1, \dots, x_n)$.

Уместо $\alpha^{\mathbf{M}}[v] = 1$ пишемо $\mathbf{M} \models \alpha[v]$ (или $\mathbf{M}, v \models \alpha$). За неку атомску формулу α, пишемо $\alpha(x_1, \dots, x_n)$ када желимо да истакнемо да се у α појављују само (неке, не нужно све) променљиве $x_1, \dots, x_n$; ако $v = \begin{pmatrix} x_1 & \cdots & x_n \\ a_1 & \cdots & a_n \end{pmatrix}$, онда уместо $\alpha[v]$ пишемо $\alpha[a_1, \dots, a_n]$. Атомске формуле које не садрже променљиве називамо *атомским реченицама*. На истинитосну вредност атомске реченице не утиче валуација променљивих (већ само интерпретација сигнатуре $\mathcal{L}$), па зато за сваку атомску реченицу α, пишемо $\mathbf{M} \models \alpha$, имајући на уму да је $\mathbf{M} \models \alpha[v]$, за било коју валуацију v.

Лема 8. *Нека су $\mathbf{A}$ и $\mathbf{B}$ неке $\mathcal{L}$-структуре и $f : A \to B$.*

1. $f : \mathbf{A} \to \mathbf{B}$ акко за сваку атомску формулу α и сваку валуацију $v : \mathrm{Var} \to A$ важи:

$$(*) \qquad \text{из } \mathbf{A} \models \alpha[v] \text{ следи } \mathbf{B} \models \alpha[f \circ v]$$

2. $f : \mathbf{A} \hookrightarrow \mathbf{B}$ акко за сваку атомску формулу α и сваку валуацију $v : \mathrm{Var} \to A$ важи:

$$(\star) \qquad \mathbf{A} \models \alpha[v] \text{ акко } \mathbf{B} \models \alpha[f \circ v]$$

Доказ. 1. ($\to$) Претпоставимо $f : \mathbf{A} \to \mathbf{B}$ и нека је $v : \mathrm{Var} \to A$ било која валуација.

Нека је α облика $t = u$, за неке терме t, u.

Формуле пишемо унутар заграда (које суштински нису потребне) да бисмо олакшали читљивост.

$$\begin{aligned} \mathbf{A} \models (t = u)[v] \quad & \text{акко} \quad t^{\mathbf{A}}[v] = u^{\mathbf{A}}[v] \\ & \text{следи} \quad f(t^{\mathbf{A}}[v]) = f(u^{\mathbf{A}}[v]) \\ & \text{акко} \quad t^{\mathbf{B}}[f \circ v] = u^{\mathbf{B}}[f \circ v] \\ & \text{акко} \quad \mathbf{B} \models (t = u)[f \circ v] \end{aligned}$$

Ако је α облика $R(t_1, \dots, t_n)$, за неко $R \in \mathrm{Rel}_{\mathcal{L}}$, $ar(R) = n$ и неке изразе $t_1, \dots, t_n$, тада:

$$\begin{array}{rcl} \mathbf{A} \models R(t_1, \dots, t_n)[v] & \text{акко} & R^{\mathbf{A}}(t_1^{\mathbf{A}}[v], \dots, t_n^{\mathbf{A}}[v]) \\ & \text{следи} & R^{\mathbf{B}}(f(t_1^{\mathbf{A}}[v]), \dots, f(t_n^{\mathbf{A}}[v])) \\ & \text{акко} & R^{\mathbf{B}}(t_1^{\mathbf{B}}[f \circ v], \dots, t_n^{\mathbf{B}}[f \circ v]) \\ & \text{акко} & \mathbf{B} \models R(t_1, \dots, t_n)[f \circ v] \end{array}$$

($\leftarrow$) Претпоставимо да за сваку атомску формулу α и сваку валуацију $v : \mathrm{Var} \to A$ важи $(*)$.

Докажимо да је $f(c^{\mathbf{A}}) = c^{\mathbf{B}}$. Нека је x променљива и $v : \mathrm{Var} \to A$ валуација која променљивој x додељује вредност $c^{\mathbf{A}}$, $v(x) = c^{\mathbf{A}}$. Применимо услов $(*)$ узимајући да је α атомска формула $x = c$. Из очигледне чињенице $\mathbf{A} \models (x = c)[v]$, тј. $\mathbf{A} \models (x = c)[c^{\mathbf{A}}]$, према услову $(*)$, следи $\mathbf{B} \models (x = c)[f \circ v]$, тј. $\mathbf{B} \models (x = c)[f(c^{\mathbf{A}})]$, што значи да је $f(c^{\mathbf{A}}) = c^{\mathbf{B}}$.

Ако $F \in \mathrm{Fun}_{\mathcal{L}}$, $ar(F) = n$ и $a_1, \dots, a_n \in A$, треба доказати $f(F^{\mathbf{A}}(a_1, \dots, a_n)) = F^{\mathbf{B}}(f(a_1), \dots, f(a_n))$. Нека су $x_1, \dots, x_n, y$ међусобно различите променљиве. Применимо услов $(*)$ узимајући да је α атомска формула $F(x_1, \dots, x_n) = y$ и $v : \mathrm{Var} \to A$ валуација дата са:

$$v = \begin{pmatrix} x_1 & \cdots & x_n & y \\ a_1 & \cdots & a_n & F^{\mathbf{A}}(a_1, \dots, a_n) \end{pmatrix}$$

Из $\mathbf{A} \models (F(x_1, \dots, x_n) = y)[v]$, тј.

$$\mathbf{A} \models (F(x_1, \dots, x_n) = y)[a_1, \cdots, a_n, F^{\mathbf{A}}(a_1, \dots, a_n)]$$

следи $\mathbf{B} \models (F(x_1, \dots, x_n) = y)[f \circ v]$, тј.

$$\mathbf{B} \models (F(x_1, \dots, x_n) = y)[f(a_1), \cdots, f(a_n), f(F^{\mathbf{A}}(a_1, \dots, a_n))],$$

одакле добијамо $F^{\mathbf{B}}(f(a_1), \dots, f(a_n)) = f(F^{\mathbf{A}}(a_1, \dots, a_n))$.

Ако $R \in \mathrm{Rel}_{\mathcal{L}}$, $ar(R) = n$ и $a_1, \dots, a_n \in A$, треба доказати да:

$$\text{Из } R^{\mathbf{A}}(a_1, \dots, a_n) \text{ следи } R^{\mathbf{B}}(f(a_1), \dots, f(a_n)).$$

Нека су $x_1, \dots, x_n$ међусобно различите променљиве. Применимо услов $(*)$ узимајући да је α атомска формула $R(x_1, \dots, x_n)$ и $v : \mathrm{Var} \to A$ валуација дата са:

$$v = \begin{pmatrix} x_1 & \cdots & x_n \\ a_1 & \cdots & a_n \end{pmatrix}$$

Тврђење које треба доказати следи из дефиниције хомоморфизма и чињеница да је
$\mathbf{A} \models R(x_1, \dots, x_n)[a_1, \dots, a_n]$ еквивалентно са $R^{\mathbf{A}}(a_1, \dots, a_n)$, и

$\mathbf{B} \models R(x_1,\ldots,x_n)[f(a_1),\ldots,f(a_n)]$ еквивалентно са $R^{\mathbf{B}}(f(a_1),\ldots,f(a_n))$.

$\square$

Било коју $\mathcal{L}$-структуру $\mathbf{A}$, са доменом A, згодно је описивати атомским реченицама сигнатуре $\mathcal{L}_A = \mathcal{L} \cup \{\underline{a} \mid a \in A\}$, која је добијена прширивањем сигнатуре $\mathcal{L}$ скупом нових симбола константи $\{\underline{a} \mid a \in A\}$ – за сваки елемент $a \in A$, додаје се по један симбол константе $\underline{a}$. Приметимо да је $\mathcal{L}_A$ проста еспанзија сигнатуре $\mathcal{L}$. Одговарајућу просту експанзију модела $\mathbf{M}$ означавамо $\underline{\mathbf{M}}$, при чему је: $S^{\mathbf{M}} = S^{\underline{\mathbf{M}}}$, за сваки симбол $S \in \mathcal{L}$, и $\underline{a}^{\underline{\mathbf{M}}} = a$, за сваки $a \in A$.

Дефиниција 3. *Позитивни дијаграм $\mathcal{L}$-структуре $\mathbf{A}$, у ознаци* $\mathrm{Diag}^+(\mathrm{A})$ *је скуп свих атомских реченица сигнатуре $\mathcal{L}_A$ које су тачне у $\underline{\mathbf{A}}$.*

Позитивни дијаграм неке структуре јесте природно уопштење таблица којима су дефинисане релације и операције те структуре.

Пример 3. Нека је $\mathcal{L} = \{U, \leqslant, *\}$, при чему је $\mathrm{Fun}_{\mathcal{L}} = \{*\}$, $\mathrm{Rel}_{\mathcal{L}} = \{U, \leqslant\}$, $ar(*) = ar(\leqslant) = 2$, $ar(U) = 1$. Посматрајмо структуру $\mathbf{M} = (\{0,1,2\}, U, \leqslant)$, где је:

$U = \{0,1\}$ $\qquad \leqslant = \{(0,0),(0,1),(1,1),(1,2)\}$

$*$	0	1	2
0	0	1	1
1	2	2	0
2	0	1	2

Позитивни дијаграм дате структуре садржи атомске реченице сигнатуре $\mathcal{L}_{\{0,1,2\}} = \{*, U, \leqslant\}$:

$$\begin{aligned}
\mathrm{Diag}^+(\mathrm{A}) \quad = \quad & \{U(\underline{0}),\, U(\underline{1}),\, \underline{0} \leqslant \underline{0},\, \underline{0} \leqslant \underline{1},\, \underline{1} \leqslant \underline{1},\, \underline{1} \leqslant \underline{2},\\
& \underline{0} * \underline{0} = \underline{0},\, \underline{0} * \underline{1} = \underline{1},\, \underline{0} * \underline{2} = \underline{1},\\
& \underline{1} * \underline{0} = \underline{2},\, \underline{1} * \underline{1} = \underline{2},\, \underline{1} * \underline{2} = \underline{0},\\
& \underline{2} * \underline{0} = \underline{0},\, \underline{2} * \underline{1} = \underline{1},\, \underline{2} * \underline{2} = \underline{2},\\
& (\underline{0} * \underline{0}) * \underline{1} = \underline{1},\, \underline{1} * (\underline{1} * \underline{2}) = \underline{2} * \underline{2}, \ldots\\
& U(\underline{0} * \underline{0}), \underline{0} * \underline{1} \leqslant \underline{1} * \underline{1}, \ldots\}
\end{aligned}$$

Нека је $t(x_1,\ldots,x_n)$ неки терм сигнатуре $\mathcal{L}$ и $v = \begin{pmatrix} x_1 & \cdots & x_n \\ a_1 & \cdots & a_n \end{pmatrix}$ валуација. Дата валуација одређује супституцију $\sigma = [x_1/\underline{a_1},\ldots,x_n/\underline{a_n}]$ променљивих новим симболима констани сигнатре $\mathcal{L}_A$, а самим тим и $\mathcal{L}_A$-терм $t[\sigma]$. Није тешко уочити да је $t^{\mathbf{A}}[v] = t[\sigma]^{\underline{\mathbf{A}}}$. Такође, за сваку атомску формулу $\alpha(x_1,\ldots,x_n)$ важи:

$$\mathbf{A} \models \alpha[v] \text{ акко } \underline{\mathbf{A}} \models \alpha[\sigma].$$

Задатак **14.** Нека су $\mathbf{A}$ и $\mathbf{B}$ модели језика $\mathcal{L}$. Постоји хомоморфизам из $\mathbf{A}$ у $\mathbf{B}$ акко постоји $\mathcal{L}_A$-експанзија $\underline{\mathbf{B}}$ структуре $\mathbf{B}$ таква да је $\underline{\mathbf{B}} \models \mathrm{Diag}^+(\mathrm{A})$.

Упутство. ($\rightarrow$) Ако $f : \mathbf{A} \rightarrow \mathbf{B}$, онда структуру $\mathbf{B}$ проширујемо до $\underline{\mathbf{B}}$ следећим интерпретацијама нових константи $\underline{a}^{\underline{\mathbf{B}}} = f(a)$, $a \in A$ и важи:

$$\underline{\mathbf{B}} = (\mathbf{B}, f(a))_{a \in A} \models \mathrm{Diag}^{+}(\mathrm{A}).$$

($\leftarrow$) Ако је $\underline{\mathbf{B}}$ $\mathcal{L}_A$-експанзија структуре $\mathbf{B}$, таква да је $\underline{\mathbf{B}} \models \mathrm{Diag}^{+}(\mathrm{A})$, онда је функција $f : A \rightarrow B$, дата са

$$f(a) = \underline{a}^{\underline{\mathbf{B}}},\ a \in A$$

хомоморфизам из $\mathbf{A}$ у $\mathbf{B}$. □

Из претходних разматрања видимо како се нека структура може описивати атомским реченицама над одговарајућом сигнатуром. У наставку показујемо да је могуће и обрнуто.

Теорема 1. *За сваки скуп атомских реченица T над неком сигнатуром $\mathcal{L}$, постоји $\mathcal{L}$-структура $\mathbf{C}$ у којој су тачне све реченице из T и сваки елемент из C је облика $t^{\mathbf{C}}$ за неки затворени терм t.*

Доказ. Нека је T^* најмањи у смислу инклузије скуп атомских реченица који садржи T и задовољава следећа два услова:

(J1) за сваки затворен терм t, једнакост $t = t$ припада T^*;

(J2) ако је $\alpha(x)$ атомична формула, а u и v затворени терми такви да $u = v \in T^*$, онда: $\alpha(u) \in T^*$ акко $\alpha(v) \in T^*$.

Подсећамо да је $\alpha(u)$ краћа ознака за $\alpha[x/t]$. Нека је M скуп свих затворених термова над $\mathcal{L}$. Дефинишимо релацију $\sim$ на M:

$$t \sim v \ \text{ акко } \ t = v \in T^*.$$

Докажимо да је $\sim$ релација еквиваленције на M.
(Р) Очигледно, према услову (J1).
(С) Претпоставимо да је $t \sim v$, тј. $t = v \in T^*$. Нека је $\alpha(x)$ формула $x = t$. Према (J1), $\alpha(t) \in T^*$, па из услова (J2) и $t = v \in T^*$, следи $\alpha(v) \in T^*$, одн. $v = t \in T^*$; дакле, $v \sim t$.
(Т) Претпоставимо да је $t \sim v$ и $v \sim w$, тј. $t = v, v = w \in T^*$. Нека је $\alpha(x)$ формула $t = x$. Из $\alpha(v) \in T^*$ и $v = w \in T^*$, према (J2), следи $\alpha(w) \in T^*$, одн. $t = w \in T^*$; дакле $t \sim w$.

Нека је $C = M/\sim = \{t^{\sim} \mid t \in M\}$. Дефинишимо $\mathcal{L}$-структуру $\mathbf{C}$ над C:

- ако је c симбол константе, онда је $c^{\mathbf{C}} \overset{\text{def}}{=} c^{\sim}$;
- ако је F операцијски симбол дужине n, онда $F^{\mathbf{C}}(t_1^{\sim}, \ldots, t_n^{\sim}) \overset{\text{def}}{=} F(t_1, \ldots, t_n)^{\sim}$;
- ако је R релацијски симбол дужине n, онда

$$R^{\mathbf{C}}(t_1^{\sim}, \ldots, t_n^{\sim}) \overset{\text{def}}{\Leftrightarrow} R(t_1, \ldots, t_n) \in T^*$$

Докажимо да су интерпретације операцијских и релацијских симбола добро дефинисане.

Нека је F операцијски симбол дужине n и $t_1 \sim v_1, \ldots, t_n \sim v_n$. Нека је $\alpha(x_1, \ldots, x_n)$ формула $F(t_1, \ldots, t_n) = F(x_1, \ldots, x_n)$. Из $\alpha(t_1, \ldots, t_n), t_1 = v_1, \ldots, t_n = v_n \in T^*$, применом (Ј2) довољан број пута закључујемо да $\alpha(t_1, \ldots, t_n) \in T^*$, одн. $F(t_1, \ldots, t_n) = F(v_1, \ldots, v_n) \in T^*$, одакле следи да је $F(t_1, \ldots, t_n) \sim F(v_1, \ldots, v_n)$, па је $F^{\mathbf{C}}(t_1^{\sim}, \ldots, t_n^{\sim}) = F^{\mathbf{C}}(v_1^{\sim}, \ldots, v_n^{\sim})$.

НАПОМЕНА. У доказу добре дефинисаности операције $F^{\mathbf{C}}$ изостављени су неки детаљи и директно је примењена једна од последица особине (Ј2). Укратко ћемо указати на детаље који су изостављени. Нека је $\alpha_1(x)$ формула $F(t_1, t_2, \ldots, t_n) = F(x, t_2, \ldots, t_n)$. Из $\alpha(t_1), t_1 = v_1 \in T^*$, применом (Ј2), следи $\alpha(v_1) \in T^*$, тј. $F(t_1, t_2, \ldots, t_n) = F(v_1, t_2, \ldots, t_n) \in T^*$. Даље, нека је $\alpha_2(x)$ формула $F(t_1, t_2, \ldots, t_n) = F(v_1, x, \ldots, t_n)$. Из $\alpha(t_2), t_2 = v_2 \in T^*$, применом (Ј2), следи $\alpha(v_2) \in T^*$, тј.

$$F(t_1, t_2, \ldots, t_n) = F(v_1, v_2, \ldots, t_n) \in T^*.$$

Настављамо приказани поступак док не добијемо $F(t_1, \ldots, t_n) = F(v_1, \ldots, v_n) \in T^*$.

Нека је R релацијски симбол дужине n и $t_1 \sim v_1, \ldots, t_n \sim v_n$. Поступајући аналогно као у случају операцијских симбола доказујемо да важи:

$$R(t_1, \ldots, t_n) \in T^* \text{ акко } R(v_1, \ldots, v_n) \in T^*.$$

Дакле, коректно је дефинисана $\mathcal{L}$-структура $\mathbf{C}$ над C. Издвајамо најважнија својства структуре $\mathbf{C}$:

- за сваки затворени $\mathcal{L}$-терм t важи: $t^{\mathbf{C}} = t^{\sim}$;
- за сваку атомичну $\mathcal{L}$-реченицу α важи: $\mathbf{C} \models \alpha$ акко $\alpha \in T^*$.
- ако је $\mathbf{M}$ било која $\mathcal{L}$-структура таква да $\mathbf{M} \models T$, онда постоји јединствени хомоморфизам $f : \mathbf{C} \to \mathbf{M}$.

Докази прве две тврдње су сасвим једноставни и из њих директно следи теорема. Прво тврђење доказујемо индукцијом по сложености затвореног терма t. Тврђење је тривијално тачно ако је t симбол константе. Нека је t облика $F(t_1, \ldots, t_n)$. Тада је

$$\begin{aligned} t^{\mathbf{C}} &= F^{\mathbf{C}}(t_1^{\mathbf{C}}, \ldots, t_n^{\mathbf{C}}) \\ &= F^{\mathbf{C}}(t_1^{\sim}, \ldots, t_n^{\sim}) \text{ (инд. претпоставка)} \\ &= F(t_1, \ldots, t_n)^{\sim} = t^{\sim}. \end{aligned}$$

Докажимо и друго тврђење. Нека су t_1, t_2 затворени терми:

$$\begin{aligned}\mathbf{C} \models t_1 = t_2 \text{ акко } & t_1^{\mathbf{C}} = t_2^{\mathbf{C}} \\ \text{акко } & t_1^{\sim} = t_2^{\sim} \\ \text{акко } & t_1 = t_2 \in T^*.\end{aligned}$$

Нека је R релацијски симбол дужине n и нека су $t_1, \ldots, t_n$ затворени терми:

$$\begin{aligned}\mathbf{C} \models R(t_1, \ldots, t_n) \text{ акко } & R^{\mathbf{C}}(t_1^{\mathbf{C}}, \ldots, t_n^{\mathbf{C}}) \\ \text{акко } & R^{\mathbf{C}}(t_1^{\sim}, \ldots, t_n^{\sim}) \\ \text{акко } & R(t_1, \ldots, t_n) \in T^*.\end{aligned}$$

Последње тврђење има веома значајне последице. Нека је $T_{\mathbf{M}}$ скуп свих атомских $\mathcal{L}$-реченица које су тачне у $\mathbf{M}$. Ако $\mathbf{M} \models T$, онда је $T \subseteq T_{\mathbf{M}}$.

Нека је $f : C \to M$ функција дефинисана са $f(t^{\sim}) = t^{\mathbf{M}}$. Није тешко показати да је f добро-дефинисано и да је хомоморфизам. Ово је и једини хомоморфизам из $\mathbf{C}$ у $\mathbf{M}$. Заиста, нека $h : \mathbf{C} \to \mathbf{M}$. Тада за сваки затворени терм t важи $h(t^{\mathbf{C}}) = t^{\mathbf{M}}$. Како је $t^{\sim} = t^{\mathbf{C}}$, непосредно изводимо жељени закључак.

НАПОМЕНА. За сваки терм t и сваку валуацију $v : \mathrm{Var} \to C$ важи $f(t^{\mathbf{C}}[v]) = t^{\mathbf{M}}[f \circ v]$. □

Понекад, за потребе логичког програмирања, једнакости се не убрајају у атомске формуле. У том случају је много једноставније конструисати канонски модел јер нема потребе 'сећи' скуп свих затворених термова неком релацијом еквиваленције. Овако добијени модел назива се *Ербранов универзум*. У алгебри је често потребна управо супротна ситуација – посматрају се само једнакости.

Формуле првог реда. Дефинабилни скупови

$\mathcal{L}$-формуле, у логици првог реда, градимо користећи симболе из $\mathcal{L}$ и тзв. *логичке симболе*:

- бесконачан скуп променљивих $Var = \{x, y, z, x_1, y_1, z_1, \ldots\}$;
- логички везници: $\wedge$, $\vee$, $\neg$, $\Rightarrow$ и $\Leftrightarrow$;
- логичке константе: $\perp$, $\top$;
- квантификатори: $\forall$ (универзални) и $\exists$ (егзистенцијални);
- знак једнакости: $=$ (овај знак се понекада и изоставља);
- помоћни знаци, тј. уобичајени симболи за зарез и заграде.

Дефиниција 4. *Скуп свих* **формула** *језика $\mathcal{L}$, у ознаци $\mathrm{For}_{\mathcal{L}}$, јесте* <u>*најмањи*</u> *скуп коначних низова симбола такав да:*

- $\mathrm{At}_{\mathcal{L}} \subseteq \mathrm{For}_{\mathcal{L}}$ *(односно, све атомичне формуле су формуле);*
- *ако $\alpha \in \mathrm{For}_{\mathcal{L}}$, онда $\neg\alpha \in \mathrm{For}_{\mathcal{L}}$;*
- *ако $\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$ и $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$, онда $(\alpha * \beta) \in \mathrm{For}_{\mathcal{L}}$;*
- *ако $\alpha \in \mathrm{For}_{\mathcal{L}}$, $x \in \mathrm{Var}$, онда $\forall x\alpha \in \mathrm{For}_{\mathcal{L}}$ и $\exists x\alpha \in \mathrm{For}_{\mathcal{L}}$.*

Дефиниција скупа формула је индуктивна; скупови формула су различити за различите изборе садржаја језика $\mathcal{L}$. При писању формула примењују се разни договори усвојени ради једноставнијег и прегледнијег записа. Претпостављамо да је читалац упознат са основним конвенцијама о писању формула, као што су правила о брисању заграда, договорени приоритети логичких везника итд.

Појављивање променљиве у формули може бити *слободно* или *везано*. Свако појављивање променљиве које није под дејством квантификатора назива се слободним, а она појављивања која јесу под дејством квантификатора називају се везаним.

Све променљиве које имају слободна појављивања у некој формули називају се **слободне променљиве** те формуле. Скуп свих слободних променљивих формуле α означавамо са $\mathrm{Fr}(\alpha)$. Функцију $\mathrm{Fr} : \mathrm{For}_{\mathcal{L}} \to \mathcal{P}(\mathrm{Var})$ прецизно дефинишемо индукцијом по сложености формуле:

- $\mathrm{Fr}(\perp) = \mathrm{Fr}(\top) = \emptyset$;
- $\mathrm{Fr}(u = v) = V(u) \cup V(v)$, $u, v \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(R(t_1, \ldots, t_{\mathrm{ar}(R)})) = V(t_1) \cup \cdots \cup V(t_{\mathrm{ar}(R)})$,
  $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \ldots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(\neg\alpha) = \mathrm{Fr}(\alpha)$;

- $\mathrm{Fr}(\alpha * \beta) = \mathrm{Fr}(\alpha) \cup \mathrm{Fr}(\beta)$, $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$;
- $\mathrm{Fr}(\forall x \alpha) = \mathrm{Fr}(\exists x \alpha) = \mathrm{Fr}(\alpha) \setminus \{x\}$, $x \in \mathrm{Var}$.

За сваку формулу α, скуп $\mathrm{Fr}(\alpha)$ је коначан. Ако је $\mathrm{Fr}(\alpha) \subseteq \{x_1, \dots, x_n\}$, онда формулу α означавамо и са $\alpha(x_1, x_2, \dots, x_n)$ када желимо да истакнемо чињеницу да су све слободне промењиве формуле α неке од промењивих $x_1, x_2, \dots, x_n$.

Дефиниција 5. *Формула σ је* ***реченица*** *језика $\mathcal{L}$ ако нема слободних промењивих, тј. ако је $\mathrm{Fr}(\alpha) = \emptyset$. Скуп свих реченица језика $\mathcal{L}$ означавамо са $\mathrm{Sent}_{\mathcal{L}}$.*

Ако је $\mathcal{L}$ највише пребројив скуп, онда су скупови $\mathrm{Term}_{\mathcal{L}}$, $\mathrm{For}_{\mathcal{L}}$ и $\mathrm{Sent}_{\mathcal{L}}$ пребројиви.

Релација задовољења

Ако је задат модел $\mathbf{M}$ језика $\mathcal{L}$ и валуација $v : \mathrm{Var} \to M$, онда свакој формули $\alpha \in \mathrm{For}_{\mathcal{L}}$ придружујемо истинитосну вредност $\alpha^{\mathbf{M}}[v] \in \{0, 1\}$ коју називамо *истинитосна вредност формуле α у моделу $\mathbf{M}$ за валуацију v.* Функцију $\alpha \mapsto \alpha^{\mathbf{M}}[v]$ дефинишемо индукцијом по сложености формуле α (при чему узимамо у обзир уобичајене логичке операције на скупу $\{0, 1\}$ и поредак $0 < 1$):

- $\perp^{\mathbf{M}}[v] = 0$, $\top^{\mathbf{M}}[v] = 1$;
- $(u = v)^{\mathbf{M}}[v] = 1$ акко $u^{\mathbf{M}}[v] = v^{\mathbf{M}}[v]$, $u, v \in \mathrm{Term}_{\mathcal{L}}$;
- $\Big(R(t_1, \dots, t_{\mathrm{ar}(R)})\Big)^{\mathbf{M}}[v] = 1$ акко $R^{\mathbf{M}}(t_1^{\mathbf{M}}[v], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[v])$, тј. $(t_1^{\mathbf{M}}[v], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[v]) \in R^{\mathbf{M}}$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \dots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$;
- $(\neg \alpha)^{\mathbf{M}}[v] = \neg\, \alpha^{\mathbf{M}}[v]$;
- $(\alpha * \beta)^{\mathbf{M}}[v] = \alpha^{\mathbf{M}}[v] * \beta^{\mathbf{M}}[v]$, $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$;
- $(\forall x \alpha)^{\mathbf{M}}[v] = \min\{\alpha^{\mathbf{M}}[v(x := a)] \mid a \in M\}$;
- $(\exists x \alpha)^{\mathbf{M}}[v] = \max\{\alpha^{\mathbf{M}}[v(x := a)] \mid a \in M\}$.

Подсећамо да је $v(x := a)$ валуација која промењивама додељује исте вредности као и валуација v, осим промењивој xкојој додељује вредност a, или прецизније $v(x := a) : \mathrm{Var} \to M$ и

$$v(x := a)(v) = \begin{cases} v(v), & v \neq x, \\ a, & v = x. \end{cases}$$

На истинитосну вредност формуле у неком моделу утичу само вредности слободних промењивих те формуле.

Лема 9. *Нека је $\mathbf{M}$ произвољан модел језика $\mathcal{L}$ и $v_1, v_2 : \mathrm{Var} \to M$ две валуације. За сваку формулу $\alpha \in \mathrm{For}_{\mathcal{L}}$, ако је $v_1(v) = v_2(v)$, за све $v \in \mathrm{Fr}(\alpha)$, онда је $\alpha^{\mathbf{M}}[v_1] = \alpha^{\mathbf{M}}[v_2]$.*

Закључујемо да је при одређивању истинитосне вредности формуле $\alpha(x_1, \dots, x_n)$ у моделу $\mathbf{M}$ за валуацију $v : \mathrm{Var} \to M$ значајна само рестрикција $v \restriction \{x_1, \dots, x_n\}$. Рестрикције свих валуација можемо идентификовати са скупом M^n, па за $\vec{a} = (a_1, \dots, a_n) \in$

M^n, са $\alpha^{\mathbf{M}}[\vec{a}]$ означавамо одговарајућу истинитосну вредност формуле α у моделу $\mathbf{M}$.

Дефиниција 6. *Формула α је тачна (тј. важи) у моделу $\mathbf{M}$ за $\vec{a}$, у ознаци $\mathbf{M} \models \alpha[\vec{a}]$, ако је $\alpha^{\mathbf{M}}[\vec{a}] = 1$.*

Пример 4. Овај пример је наставак примера 1, у коме смо посматрали језик $\mathcal{L} = \{\leqslant, +, \cdot, 0, 1\}$ и три модела овог језика: $\mathbf{R} = (\mathbb{R}, \leqslant, +, \cdot, 0, 1)$, $\mathbf{Z} = (\mathbb{Z}, \leqslant, +, \cdot, 0, 1)$ и $\mathbf{X} = (\{a, b, c\}, \lhd, *, \circ, a, b)$, где је $\lhd = \{(a,a), (b,b), (c,c), (a,b), (b,c), (a,c)\}$, а операције $*$ и $\circ$ су задате таблицама.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\circ$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

Нека је $\varphi(x, y)$ формула $\exists z(0 \leqslant z \land z \neq 0 \land x + z \leqslant y \land x + z \neq y)$. У структури $\mathbf{R}$ за валуацију $x \mapsto 5$, $y \mapsto 6$, наведена формула јесте тачна, $\mathbf{R} \models \varphi[5, 6]$, јер *постоји реалан број z већи од нуле такав да је $5 + z \leqslant 6$ и $5 + z \neq 6$.* Наведена валуација може се схватити и као валуација промењљивих у $\mathbb{Z}$, али тада $\mathbf{Z} \not\models \varphi[5, 6]$. Ако променимо валуацију, и ставимо, на пример, $x \mapsto 5$, $y \mapsto 5$, онда $\mathbf{R} \not\models \varphi[5, 5]$ и $\mathbf{Z} \not\models \varphi[5, 5]$.

За изразе t_1 и t_2, записом $t_1 \neq t_2$ скраћујемо формулу $\neg t_1 = t_2$

Испитајмо тачност формуле $\varphi(x, y)$ у структури $\mathbf{X}$ при валуацији $x \mapsto a$ и $x \mapsto c$. То значи да треба испитати да ли постоји $z \in X = \{a, b, c\}$ такав да је $a \lhd z$, $z \neq a$, $a * z \lhd c$ и $a * z \neq c$. Одговор је потврдан, b је елемент који задовољава наведене услове: $a \lhd b$ (тј. $(a, b) \in \lhd$), $b \neq a$, $a * b = b \lhd c$ и $a * b = b \neq c$. Остављамо читаоцима да провере тачност формуле φ у моделу $\mathbf{X}$ за неке друге валуације. На пример, да ли је $\mathbf{X} \models \varphi[a, b]$?

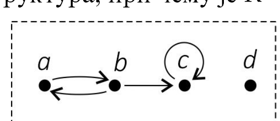
Ако је $\mathbf{M}$ нека $\mathcal{L}$-структура и $\varphi(x_1, \ldots, x_n)$ нека $\mathcal{L}$-формула, за скуп, тј. n-арну релацију скупа M

$$\varphi[M^n] = \{(a_1, \ldots, a_n) \in M^n \mid \mathbf{M} \models \varphi[a_1, \ldots, a_n]\}$$

кажемо да је дефинисан формулом φ.

Дефиниција 7. *Нека је $\mathbf{M}$ нека $\mathcal{L}$-структура. Скуп $D \subseteq M^n$ је дефинабилан ако постоји формула $\varphi(x_1, \ldots, x_n)$ таква да је $D = \varphi[M^n]$.*

Пример 5. Нека је R бинарни релацијски симбол и $\mathbf{A} = (\{a, b, c, d\}, R^{\mathbf{A}})$ структура, при чему је $R^{\mathbf{A}} = \{(a, b), (b, a), (b, c), (c, c)\}$.



$\varphi(x)$	$\mathbf{A} \models \varphi[?]$	$\varphi[A]$
$\forall y \neg R(x,y)$	$\mathbf{A} \not\models \varphi[a]$, $\mathbf{A} \not\models \varphi[b]$, $\mathbf{A} \not\models \varphi[c]$, $\mathbf{A} \models \varphi[d]$	$\{d\}$
$\exists y R(x,y) \wedge \exists y R(y,x)$	$\mathbf{A} \models \varphi[a]$, $\mathbf{A} \models \varphi[b]$, $\mathbf{A} \models \varphi[c]$, $\mathbf{A} \not\models \varphi[d]$	$\{a,b,c\}$

Дакле, подскупови $\{a,b,c\}$ и $\{d\}$ су дефинабилни. Навести формуле које дефинишу све остале подскупове од $\{a,b,c,d\}$.

Пример 6. 1) Посматрајмо алгебру $\mathbf{R} = (\mathbb{R}, +, \cdot, 0, 1)$. Да ли је уобичајено уређење реалних бројева дефинабилно у овој структури?

Приметимо најпре да је дефинабилан подскуп свих ненегативних бројева, тј. да ли постоји формула $\varphi(x)$ таква да за све $r \in \mathbb{R}$ важи:

$$\begin{aligned} \mathbf{R} \models \varphi[r] \quad & \text{акко} \quad r \in [0, +\infty) \\ & \text{акко} \quad r \geqslant 0 \end{aligned}$$

Тражена формула постоји: $\exists y\, x = y \cdot y$. Уређење реалних бројева дефинише формула $\psi(x,y)$ дата са $\exists z\, x + (z \cdot z) = y$; за све $a, b \in \mathbb{R}$,

$$\begin{aligned} \mathbf{R} \models \psi[a,b] \quad & \text{акко} \quad a \leqslant b \\ & \text{акко} \quad \text{постоји } c \text{ тако да је } a + c = b. \end{aligned}$$

2) Издвајамо неке дефинабилне подскупове домена структуре $(\mathbb{N}, s, +, \cdot, 0)$: s је операција *следбеник*.

- строго уређење је десинабилно формулом $\exists z\, x + Sz = y$
- сваки једночлани скуп $\{n\}$ је дефинабилан

  $\{0\}$ дефинише формула $x = 0$

  $\{1\}$ дефинише формула $x = s0$

  $\{2\}$ дефинише формула $x = ss0 \ldots$

скуп простих бројева је дефинабилан формулом:

$$1 < x \wedge \forall y \forall z\, (x = y \cdot z \Rightarrow y = 1 \vee z = 1).$$

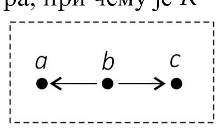
У наведеној формули коришћена је дефинабилност строгог уређења, и елемента 1; наравно, можемо саставити одговарајућу формулу на полазној сигнатури:

$$\exists z\, (s0 + sz = sx) \wedge \forall y \forall z\, (x = y \cdot z \Rightarrow y = s0 \vee z = s0).$$

3) Да ли је скуп простих бројева дефинабилан у структури $(\mathbb{N}^+, |)$, где је $\mathbb{N}^+ = \{1, 2, 3, 4, \ldots\}$? Приметимо најпре да је елемент 1 (тј. скуп $\{1\}$) дефинабилан формулом $\forall y\, x \mid y$. Скуп простих бројева дефинише формула:

$$x \neq 1 \wedge \forall y (y \mid x \Rightarrow y = 1 \vee y = x).$$

4) Нека је R бинарни релацијски симбол и $\mathbf{A} = (\{a,b,c\}, R^{\mathbf{A}})$ структура, при чему је $R^{\mathbf{A}} = \{(a,b), (a,c)\}$.



- Скуп $\emptyset$ дефинише формула $x \neq x$.
- Скуп $\{b\}$ дефинише формула $\exists y\, Rxy$.
- Скуп $\{a, c\}$ дефинише формула $\exists y\, Ryx$.
- Скуп $\{a, b, c\}$ дефинише формула $x = x$.

Да ли је $\{a\}$ дефинабилан скуп? Интуитивно, одговор је негативан, јер не постоји 'својство' којим би се елемент a могао разликовати од елемета c.

Теорема 2. *Ако $f : \mathbf{A} \cong \mathbf{B}$, онда за сваку формулу φ и сваку валуацију $v : \mathrm{Var} \to A$ важи:*

$$\mathbf{A} \models \varphi[v] \text{ акко } \mathbf{B} \models \varphi[f \circ v].$$

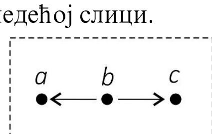
Доказ. Како је f утапање, тврђење важи за сваку атомску формулу. Индукцијом по сложености формуле доказује се да тврђење важи за све формуле. Наводимо само случај када је φ облика $\exists x\theta$, претпостављајући да је тврђење тачно за формулу θ:

$$\begin{aligned}
\mathbf{A} \models \exists x\, \theta[v] \quad & \text{акко} \quad \text{постоји } a \in A \text{ тако да } \mathbf{A} \models \theta[v(x := a)] \\
& \text{акко} \quad \text{постоји } a \in A \text{ тако да } \mathbf{B} \models \theta[f \circ v(x := a)] \\
& \text{акко} \quad \text{постоји } a \in A \text{ тако да } \mathbf{B} \models \theta[(f \circ v)(x := f(a))] \\
& \text{акко} \quad \text{постоји } b \in B \text{ тако да } \mathbf{B} \models \theta[(f \circ v)(x := b)] \quad (\text{јер је } f \text{ бијекција.}) \\
& \text{акко} \quad \mathbf{B} \models \exists x\, \theta[f \circ v] \quad \square
\end{aligned}$$

Последица 2. *Ако $f : \mathbf{A} \cong \mathbf{A}$ (тј. f је аутоморфизам структуре $\mathbf{A}$) и $D \subseteq A^n$ дефинабилан скуп, онда за све $a_1, \ldots, a_n \in A$ важи:*

$$(a_1, \ldots, a_n) \in D \text{ акко } (f(a_1), \ldots, f(a_n)) \in D.$$

Пример 7. 1) У претходном примеру је наговештено да скуп $\{a\}$ није дефинабилан у структури $\mathbf{A} = (\{a, b, c\}, R^{\mathbf{A}})$, при чему је $R^{\mathbf{A}}$ дата на следећој слици.



Није тешко проверити да је $f = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$ аутоморфизам структуре $\mathbf{A}$. Према претходној последици, за сваки дефинабилан подскуп D и сваки $x \in \{a, b, c\}$ важи: $x \in D$ акко $f(x) \in D$. Посебно, $a \in D$ акко $c \in D$, па самим тим $\{a\}$ није дефинабилан скуп.

2) Скуп природних бројева $\mathbb{N}$ није дефинабилан у структури $(\mathbb{R}, <)$. Заиста, $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$ је аутоморфизам структуре $(\mathbb{R}, <)$, па ако би $\mathbb{N}$ био дефинабилан онда би за сваки $a \in \mathbb{R}$ важило: $a \in \mathbb{N}$ акко $f(a) \in \mathbb{N}$. Наравно, ова еквиваленција није тачна за $a = \sqrt[3]{2}$.

Реченице су формуле у којима нема променљивих које се слободно појављују; α је речиница ако је $\mathrm{Fr}(\alpha) = \emptyset$. Истинитосна вредност реченице зависи само од изабраног модела $\mathbf{M}$, а валуације нису од значаја па их потпуно изостављамо из разматрања. Чињеницу да је реченица α тачна у $\mathbf{M}$ означавамо са $\mathbf{M} \models \alpha$ (што значи да је $\mathbf{M} \models \alpha[v]$, за било коју валуцаију).

Последица 3. *Ако $f : \mathbf{A} \cong \mathbf{B}$, онда за сваку речеинницу σ важи:*

$$\mathbf{A} \models \sigma \text{ акко } \mathbf{B} \models \sigma.$$

Пример 8. Претходно тврђење се користи да се докаже да две структуре нису изоморфне: тражи се својство првог реда која је тачна у једној, а није тачна у другој. На пример, $(\mathbb{N}, <) \ncong (\mathbb{Z}, <)$, јер

$$(\mathbb{N}, <) \not\models \forall x \exists y\, (y < x) \qquad (\mathbb{Z}, <) \models \forall x \exists y\, (y < x).$$

Задатак **15.** Дато је неколико модела сигнатуре $\mathcal{L} = \{*, \star, a, b\}$ ($\mathrm{Fun}_{\mathcal{L}} = \{*, \star\}$, $\mathrm{ar}(*) = \mathrm{ar}(\star) = 2$, $\mathrm{Const}_{\mathcal{L}} = \{a, b\}$):

- $\mathbf{Z}_1 = (\mathbb{Z}, +, \cdot, 0, 1)$;
- $\mathbf{Z}_2 = (\mathbb{Z} \times \mathbb{Z}, \oplus, \odot, (0,0), (1,0))$, при чему је

  $(k, \ell) \oplus (m, n) = (k + m, \ell + n)$ и
  $(k, \ell) \odot (m, n) = (k \cdot m - \ell \cdot n, k \cdot n + \ell \cdot m)$.
- $\mathbf{Z}_3 = \left(\mathrm{M}_2(\mathbb{Z}), \boxplus, \boxdot, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$, при чему је $\mathrm{M}_2(\mathbb{Z})$ скуп свих квадратних матрица типа 2×2 над $\mathbb{Z}$,

$$\begin{bmatrix} k & \ell \\ m & n \end{bmatrix} \boxplus \begin{bmatrix} k' & \ell' \\ m' & n' \end{bmatrix} = \begin{bmatrix} k + k' & \ell + \ell' \\ m + m' & n + n' \end{bmatrix}$$
$$\begin{bmatrix} k & \ell \\ m & n \end{bmatrix} \boxdot \begin{bmatrix} k' & \ell' \\ m' & n' \end{bmatrix} = \begin{bmatrix} kk' + \ell m' & k\ell' + \ell n' \\ mk' + nm' & m\ell' + nn' \end{bmatrix}$$

Наћи бар по једну реченицу сигнатуре $\mathcal{L}$ која важи у једној од ових структура и не важи у остале две.

Ваљане формуле

Посебно су значајне реченице које су тачне у било којој структури одговарајућег језика.

Дефиниција 8. *Формула $\alpha \in \mathrm{For}_{\mathcal{L}}$ је **ваљана**, у ознаци $\models \alpha$, ако за сваки модел $\mathbf{M}$ и сваку валуацију $v : \mathrm{Var} \to M$ важи $\mathbf{M} \models \alpha[v]$. Специјално, реченица $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ је **ваљана** (што ће бити и најважнији случајеви ваљаних формула) ако је тачна у сваком моделу језика $\mathcal{L}$.*

Образложимо најпре коментар наведен у загради у претходној дефиницији, тј. разлоге због којих не морамо разматрати ваљане формуле већ пажњу можемо усмерити само на ваљане реченице. Ако је $\alpha(x_1, \ldots, x_n)$ ваљана формула, онда је то и њено *универзално затворење*, тј. реченица $\forall x_1 \ldots \forall x_n \alpha(x_1, \ldots, x_n)$.

Нажалост, за разлику од исказних формула, не постоји универзални поступак помоћу којег бисмо могли да испитамо ваљаност било које формуле логике првог реда. Неке опште закључке ипак можемо да изведемо.

Инстанце исказних таутологија. Све формуле логике првог реда које су *инстанце* исказних *таутологија* сигурно су ваљане. Под инстанцом таутологије подразумевамо формулу која се добија заменом свих исказних слова неким формулама првог реда при чему наравно иста слова мењамо истим формулама. Свака таутологија има неограничено много инстанци. На пример, инстанце таутологије $p \Rightarrow (q \Rightarrow p)$ су формуле $\alpha \Rightarrow (\beta \Rightarrow \alpha)$, за било које $\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$. Није тешко уочити да су инстанце таутологија заиста ваљане: ако је $\tau(p_1, \ldots, p_n)$ таутологија, онда је формула $\underline{\tau}$, добијена тако што су слова $p_1, \ldots, p_n$ редом замењена формулама $\alpha_1, \ldots, \alpha_n \in \mathrm{For}_{\mathcal{L}}$, ваљана.

Својства импликације:

$\models \alpha \Rightarrow \alpha$

$\models \bot \Rightarrow \alpha$ $\quad$ $\models \alpha \Rightarrow \top$

$\models (\alpha \Rightarrow \beta) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma))$ *транзитивност импликације*

$\models (\alpha \Rightarrow \beta) \vee (\beta \Rightarrow \alpha)$ *линеарност импликације*

Својства конјункције:

$\models \alpha \wedge \beta \Rightarrow \alpha$ $\quad$ $\models \alpha \wedge \beta \Rightarrow \beta$

$\models (\gamma \Rightarrow \alpha) \Rightarrow ((\gamma \Rightarrow \beta) \Rightarrow (\gamma \Rightarrow \alpha \wedge \beta))$ *формула $\alpha \wedge \beta$ је највеће доње ограничење за α и β*

Својства дисјункције:

$\models \alpha \Rightarrow \alpha \vee \beta$ $\quad$ $\models \beta \Rightarrow \alpha \vee \beta$

$\models (\alpha \Rightarrow \gamma) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow (\alpha \vee \beta \Rightarrow \gamma))$ *формула $\alpha \vee \beta$ је најмање горње ограничење за α и β*

Својства негације:

$\models \alpha \wedge \neg\alpha \Rightarrow \beta$ *ex falso quodibet – из лажне претпоставке следи све (што желиш)*

$\models (\alpha \Rightarrow \beta) \Rightarrow ((\alpha \Rightarrow \neg\beta) \Rightarrow \neg\alpha)$ *reduction ad absurdum – свођење на противречност*

$\models \alpha \vee \neg\alpha$ *закон искључења трећег*

Корисно је издвојити и неке еквивалентне формуле – формуле које имају исте истинитосне вредности у свим моделима, за сваку валуацију. Уместо $\models \alpha \Leftrightarrow \beta$, краће пишемо $\alpha \equiv \beta$.

$\alpha \wedge \alpha \equiv \alpha$	$\alpha \vee \alpha \equiv \alpha$	*закони идемпотентности*
$\alpha \wedge (\alpha \vee \beta) \equiv \alpha$	$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$	*закони апсорпције*
$\alpha \wedge \beta \equiv \beta \wedge \alpha$	$\alpha \vee \beta \equiv \beta \vee \alpha$	*закони комутативности*
$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$	$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$	*закони асоцијативности*
$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$	*закони дистрибутивности* $\wedge$ *према* $\vee$	
$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	*закони дистрибутивности* $\vee$ *према* $\wedge$	
$\neg(\alpha \wedge \beta) \equiv (\neg\alpha \vee \neg\beta)$	*Де Морганов закон*	
$\neg(\alpha \vee \beta) \equiv (\neg\alpha \wedge \neg\beta)$	*Де Морганов закон*	
$(\alpha \Rightarrow \beta) \equiv (\neg\beta \Rightarrow \neg\alpha)$	*закон контрапозиције*	
$\alpha \equiv \neg\neg\alpha$	*закон двојне негације*	
$\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$		

Постоји доста ваљаних формула које нису инстанце исказних таутологија. Наводимо неке од најједноставнијих.

Универзални квантор и конјункција; егзистенцијални квантор и дисјункција. Да се универзални квантификатор „лепо слаже“ са конјункцијом, а егзистенцијални са дисјункцијом, показују наредне две ваљане формуле (за било које $\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$).

$\forall x(\alpha \wedge \beta) \equiv \forall x\alpha \wedge \forall x\beta$
$\exists x(\alpha \vee \beta) \equiv \exists x\alpha \vee \exists x\beta$

$$\forall x(\alpha \wedge \beta) \Leftrightarrow \forall x\alpha \wedge \forall x\beta \text{ и } \exists x(\alpha \vee \beta) \Leftrightarrow \exists x\alpha \vee \exists x\beta$$

У ваљаност прве формуле једноставно се уверавамо:

$$\begin{aligned}
(\forall x(\alpha \wedge \beta))^{\mathbf{M}}[v] &= \min_{a \in M} (\alpha \wedge \beta)^{\mathbf{M}}[v(x := a)] \\
&= \min_{a \in M} \min\{\alpha^{\mathbf{M}}[v(x := a)], \beta^{\mathbf{M}}[v(x := a)]\} \\
&= \min\{\min_{a \in M} \alpha^{\mathbf{M}}[v(x := a)], \min_{a \in M} \beta^{\mathbf{M}}[v(x := a)]\} \\
&= \min\{(\forall x\alpha)^{\mathbf{M}}[v], (\forall x\beta)^{\mathbf{M}}[v]\} \\
&= (\forall x\alpha \wedge \forall x\beta)^{\mathbf{M}}[v]
\end{aligned}$$

На потпуно аналоган начин проверавамо и ваљаност друге формуле.

Универзални квантор и дисјункција; Егзистенцијални квантор и конјункција. Универзални квантификатор се само „делимично слаже“ са дисјункцијом, а егзистенцијани са конјункцијом. Следеће формуле су ваљане ($\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$):

$$\forall x(\alpha \vee \beta) \Leftarrow \forall x\alpha \vee \forall x\beta \text{ и } \exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta.$$

$$\begin{aligned}
(\forall x(\alpha \vee \beta))^{\mathbf{M}}[v] &= \min_{a \in M} (\alpha \vee \beta)^{\mathbf{M}}[v(x := a)] \\
&= \min_{a \in M} \max\{\alpha^{\mathbf{M}}[v(x := a)], \beta^{\mathbf{M}}[v(x := a)]\} \\
&\geqslant \max\{\min_{a \in M} \alpha^{\mathbf{M}}[v(x := a)], \min_{a \in M} \beta^{\mathbf{M}}[v(x := a)]\} \\
&= \max\{(\forall x\alpha)^{\mathbf{M}}[v], (\forall x\beta)^{\mathbf{M}}[v]\} \\
&= (\forall x\alpha \vee \forall x\beta)^{\mathbf{M}}[v]
\end{aligned}$$

Да обрнуте импликације наведених формула нису ваљане једноставно показујемо. Изаберимо, на пример језик који садржи два унарна релацијска симбола U и V и интерпретирајмо их на скупу природних бројева $\mathbb{N}$: $U^{\mathbf{N}} = 2\mathbb{N} = \{0, 2, 4, \ldots\}$ и $V^{\mathbf{N}} = 2\mathbb{N} + 1 = \{1, 3, 5, \ldots\}$. Тада $\mathbf{N} \models \forall x(U(x) \vee V(x))$, али $\mathbf{N} \not\models \forall x U(x) \vee \forall x V(x)$, тј. $\mathbf{N} \not\models \forall x(U(x) \vee V(x)) \Rightarrow \forall x U(x) \vee \forall x V(x)$. Такође, $\mathbf{N} \not\models \exists x U(x) \wedge \exists x V(x) \Rightarrow \exists x(U(x) \wedge V(x))$.

Уколико x **није** слободна променљива формуле α, онда су ваљане и формуле $\forall x(\alpha \vee \beta) \Leftrightarrow \alpha \vee \forall x \beta$ и $\exists x(\alpha \wedge \beta) \Leftrightarrow \alpha \wedge \exists x \beta$.

Два узастопна квантора. Два квантификатора исте врсте могу заменити места. Ваљане су следеће формуле $\forall x \forall y \alpha \Leftrightarrow \forall y \forall x \alpha$ и $\exists x \exists y \alpha \Leftrightarrow \exists y \exists x \alpha$, за било коју формулу α. За било које α ваљана је и следећа формула $\exists x \forall y \alpha \Rightarrow \forall y \exists x \alpha$. Обрнута импликација није ваљана. На пример, ако бинарни релацијски симбол R интерпретирамо на скупу природних бројева $\mathbb{N}$ као строго уређење, $R^{\mathbf{N}} =<$, онда $\mathbf{N} \not\models \forall y \exists x R(x, y) \Rightarrow \exists x \forall y R(x, y)$

$\forall x \forall y \alpha \equiv \forall y \forall x \alpha$
$\exists x \exists y \alpha \equiv \exists y \exists x \alpha$

Де Моргановии закони за кванторе. Ваљане су следеће реченице $\neg \forall x \alpha \Leftrightarrow \exists x \neg \alpha$ и $\neg \exists x \alpha \Leftrightarrow \forall x \neg \alpha$.

$\neg \forall x \alpha \equiv \exists x \neg \alpha$
$\neg \exists x \alpha \equiv \forall x \neg \alpha$

$$\begin{aligned}
(\neg \forall x \alpha)^{\mathbf{M}}[v] &= 1 - \min_{a \in M} \alpha^{\mathbf{M}}[v(x := a)] = \max_{a \in M}(1 - \alpha^{\mathbf{M}}[v(x := a)]) \\
&= \max_{a \in M}(\neg \alpha^{\mathbf{M}}[v(x := a)]) \\
&= (\exists x \neg \alpha)^{\mathbf{M}}[v]
\end{aligned}$$

Замена променљиве термом. Посебну пажњу заслужује следећа чињеница: ако је t затворен израз неког језика и α формула истог језика, онда је формула $\forall x \alpha \Rightarrow \alpha(x/t)$ ваљана, при чему је $\alpha(x/t)$ формула добијена из α тако што су сва слободна појављивања променљиве x замењена изразом t. Наиме, за било који модел $\mathbf{M}$ и валуацију v важи:

$$(\forall x \alpha)^{\mathbf{M}}[v] = \min_{a \in M} \alpha^{\mathbf{M}}[v(x := a)] \leqslant \alpha^{\mathbf{M}}[v(x := t^{\mathbf{M}}[v])] \overset{(*)}{=} \alpha(x/t)^{\mathbf{M}}[v].$$

Доказ једнакости $(*)$ препуштамо читаоцима. Природно је запитати се да ли ће формула $\forall x \alpha \Rightarrow \alpha(x/t)$ бити ваљана за било који израз (који не мора бити затворен). Негативан одговор даје следећи једноставан пример на језику који садржи један бинарни релацијски симбол $<$. Нека је α формула $\exists y\,(x < y)$ (па је $\forall x \alpha$ формула $\forall x \exists y\,(x < y)$) и t променљива y. Тада је $\alpha(x/t)$ формула $\exists y\,(y < y)$. Ако $<$ интерпретирамо у скупу природних бројева $\mathbb{N}$ као строго уређење, тада $\mathbf{N} \models \forall x \exists y\,(x < y)$ и $\mathbf{N} \not\models \exists y\,(y < y)$, тј. $\mathbf{N} \models \forall x \alpha$, али $\mathbf{N} \not\models \alpha(x/t)$. Већ на први поглед видимо да је проблем то што је након замене променљиве x са y у формули $\alpha(x/y)$ променљива y постала везана. Уколико се то не догоди, проблеми нестају. Заиста, ако је α' формула $\exists z\,(x < z)$ и

t променљива y, тада је $\alpha'(x/t)$ формула $\exists z\,(y < z)$. Из тачности реченице $\forall x \exists z\,(x < z)$ у неком моделу, следи тачност формуле $\exists z\,(y < z)$ у истом моделу за било коју валуацију. Ако приметимо да се не разликују значења формула $\forall x \exists y\,(x < y)$ и $\forall x \exists z\,(x < z)$ у било ком моделу, онда једноставно налазимо решење поменутих проблема које се заснива на следећим општим чињеницама:

1. ако је формула α' *варијанта* формуле α, тј. ако се α' добија преименовањем свих везаних појављивања неке променљиве у формули α новом променљивом која се не појављује (ни слободно ни везано) у α, онда је формула $\alpha' \Leftrightarrow \alpha$ ваљана;

2. ако након замене свих слободних појављивања променљиве x у формули α изразом t, ниједна променљива израза t није постала везана, онда је формула $\forall x \alpha \Rightarrow \alpha(x/t)$ ваљана.

Кључни корак у оправдавању друге тврдње јесте доказ да под уведеним претпоставкама важи једнакост $\alpha^{\mathbf{M}}[v(x := t^{\mathbf{M}}[v])] = \alpha(x/t)^{\mathbf{M}}[v]$, за било који модел $\mathbf{M}$ и валуацију v.

Да бисмо избегли непотребно оптерећивање текста усвајамо следеће договор: за формулу α, променљиву x и израз t, формула $\alpha[x/t]$ означава било коју од формула $\alpha'(x/t)$, где је α' варијанта формуле α добијена преименовањем свих везаних појављивања неке променљиве у формули α новом променљивом која се не појављује (ни слободно ни везано) у α нити се појављује у изразу t. Дакле, $\forall x \alpha \Rightarrow \alpha(x/t)$ је ваљана формула.

Нормалне форме

Често је погодно формуле трансформисати у неки погоднији облик, користећи издвојене еквивалентне формуле и следећа очигледна својства:

(Р) $\alpha \equiv \alpha$, тј. $\models \alpha \Leftrightarrow \alpha$, за сваку формулу α;

(С) ако је $\alpha \equiv \beta$, онда је и $\beta \equiv \alpha$, за било које формуле α, β (из $\models \alpha \Leftrightarrow \beta$ следи $\models \beta \Leftrightarrow \alpha$);

(Т) ако је $\alpha \equiv \beta$ и $\beta \equiv \gamma$, онда је и $\alpha \equiv \gamma$, за било које формуле α, β, γ (из $\models \alpha \Leftrightarrow \beta$ и $\models \beta \Leftrightarrow \gamma$, следи $\models \alpha \Leftrightarrow \gamma$);

(К) ако је $\alpha \equiv \beta$, онда је $\neg\alpha \equiv \neg\beta$; ако је $\alpha \equiv \beta$ и $\gamma \equiv \delta$, онда је и $\alpha * \gamma \equiv \beta * \delta$, при чему је $*$ неки од логичких везника $\wedge$, $\vee$, $\Rightarrow$; ако је $\alpha \equiv \beta$ и x нека променљива, онда је $Qx\alpha \equiv Qx\beta$, где је Q један од квантификатора $\forall$ или $\exists$.

Дефиниција 9. *Формула α је у* ***пренекс нормалној форми*** *уколико је облика $Q_1 x_1 \ldots Q_n x_n \theta$, где је сваки Q_i неки квантификатор, а θ*

је формула без квантификатора ($Q_1 x_1 \dots Q_n x_n$ се назива префикс формуле α). Префикс може бити празан, па се и свака формула без квантификатора сматра формулом у пренекс нормалној форми.

Лема 10. *Свака формула је еквивалентна формули која је у пренекс нормалној форми.*

Доказ леме скицираћемо у наредном примеру.

Пример 9. Нека је $\mathrm{Rel}_{\mathcal{L}} = \{R, S\}$, $\mathrm{ar}(R) = \mathrm{ar}(S) = 2$. Трансформишимо формулу $\neg\exists x \neg(\exists y R(x,y) \Rightarrow \exists y S(x,y))$ у пренекс нормалну форму.

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

1. Елиминисати везнике $\Rightarrow$ и $\Leftrightarrow$

2. Примењивати Де Морганове законе (за везнике и квантификаторе) уз елиминацију двојних негација док год се негације „не спусте“ до атомских формула

3. Извлачити квантификаторе напред уз преименовање везаних промењљивих када је то потребно.

Није тешко уочити да се дата формула може трансформисати и у следећи пренекс облик $\forall x \exists y \forall z(\neg R(x,z) \vee S(x,y))$, па закључујемо да једна формула може да има више пренекс форми. Поред тога, формула у пренекс форми може бити еквивалентна синтаксно различитим формулама.

Пример 10. Пренекс нормална форма неке формуле може бити посебно корисна приликом налажења модела те формуле.

Посматрајмо формулу из претходног примера $\neg\exists x \neg(\exists y R(x,y) \Rightarrow \exists y S(x,y))$. Уместо да трагамо за моделом ове формуле, много је једноставније потражити модел њене пренекс нормалне форме $\forall x \forall y \exists z(\neg R(x,y) \vee S(x,z))$. Дакле, треба да одредимо неки скуп M и на њему две бинарне релације $R^{\mathbf{M}}$ и $S^{\mathbf{M}}$, тако да за свака два елемента $x, y \in M$ постоји неки $z \in M$ такав да из $R^{\mathbf{M}}(x,y)$ следи да $S^{\mathbf{M}}(x,z)$. Ово ћемо најједноставније постићи, ако најпре дефинишемо једну помоћну функцију $f : M \times M \to M$, која за сваки пар елемената $(x,y) \in M^2$ одређује жељени елемент $f(x,y)$. Тада, како год да дефинишемо релацију $R^{\mathbf{M}}$, можемо узети да је $S^{\mathbf{M}} = \{(x, f(x,y)) \mid R^{\mathbf{M}}(x,y)\}$. На пример, ако је $M = \{a, b\}$, $f : M \times M \to M$ је дефинисана са

f	a	b
a	a	b
b	b	a

и $R^{\mathbf{M}} = \{(a,a), (b,a)\}$, онда ако узмемо да је $S^{\mathbf{M}} = \{(a,a), (b,b)\}$, закључујемо да $(M, R^{\mathbf{M}}, S^{\mathbf{M}}) \models \neg\exists x \neg(\exists y R(x,y) \Rightarrow \exists y S(x,y))$.

Описаним поступком једноставно налазимо и контрамодел дате формуле, тј. модел формуле $\exists x \exists y \forall z (R(x,y) \wedge \neg S(x,z))$. Није тешко уочити да домен траженог модела M треба да садржи нека два елемента a и b, таква да је $R^{\mathbf{M}}(a,b)$, али да $S^{\mathbf{M}}$ не садржи ниједан пар чија је прва координата a. Остављамо читаоцу да наведе пример оваквог модела.

У претходном примеру илустрована је једна веома звначјна метода – *сколемизација*. Нека је φ формула сигнатудре $\mathcal{L}$ и $\varphi \equiv Q_1 x_1 \cdots Q_n x_n \theta$, при чему је θ формула без квантификатора. Нека су $i_1 < \ldots < i_m$ индекси такви да је Q_{i_j}, $j = \overline{1,m}$, егзистенцијални квантификатор $\exists$. Проширимо сигнатуру $\mathcal{L}$ новим операцијским симболима $f_1, \ldots, f_m$, таквим да је $\mathrm{ar}(f_j) = i_j - j$, $j = \overline{1,m}$; проширени језик означавамо $\mathcal{L}_S$:

Сколем (1887–1963) је био норвешки математичар.

$$\mathcal{L}_S = \mathcal{L} \cup \{f_1, \ldots, f_m\}.$$

Приметимо да је дужина симбола f_{i_j} једнака броју универзалних кванитифкатора који се у пренекс форми $Q_1 x_1 \cdots Q_n x_n \theta$ налазе лево до (егзистенцијалног) квантификатора Q_{i_j}. Нека је t_j, $j = \overline{1,m}$, терм добијен применом симбола f_{i_j} на универзално квантификоване променљиве лево од Q_{i_j}. *Сколемова форма* формуле φ јесте формула φ_S добијена:

- изостављањем егзистенцијалних кванитификатора из префикса $Q_1 x_1 \cdots Q_n x_n$, тј. $Q_{i_j} x_{i_j}$, $j = \overline{1,m}$;
- заменом променљиве x_{i_j} у θ термом t_j, $j = \overline{1,m}$.

Пример 11. Одредимо Сколемову форму формуле φ облика

$$\exists y_0 \forall x_1 \forall x_2 \exists y_1 \forall x_3 \exists y_3 \theta(x_1, x_2, x_3, y_0, y_1, y_2),$$

при чему је θ формула без квантификатора неке сигнатуре $\mathcal{L}$. Најпре додајемо нове операцијске симболе: $\mathcal{L}_S = \mathcal{L} \cup \{c, f, g\}$, при чему је $\mathrm{ar}(c) = 0$ (тј. c је симбол константе), $\mathrm{ar}(f) = 2$ и $\mathrm{ar}(g) = 3$, а затим састављамо формулу φ_S у Сколемовом облику:

$$\forall x_1 \forall x_2 \forall x_3 \theta(x_1, x_2, x_3, c, f(x_1, x_2), g(x_1, x_2, x_3)).$$

Лема 11. $\models \varphi_S \Rightarrow \varphi$

Доказ. Претпоставимо да је φ дата у пренекс нормалној форми и да је n_φ број егзистенцијалних квантификатора у префиксу. Нека је $\mathbf{M}$ $\mathcal{L}_S$-структура и $v : \mathrm{Var} \to M$ валуација, тако да је $\mathbf{M} \models \varphi_S[v]$, где је φ_S Сколемова форма формуле φ. Треба доказати да $\mathbf{M} \models \varphi[v]$. Доказ спроводимо индукцијом по n_φ.

Ако је $n_\varphi = 0$, формуле φ и φ_S су истоветне и тврђење тривијално важи.

Ако је $n_\varphi \geqslant 1$, тада је φ облика $\forall x_1 \cdots \forall x_m \exists y \theta$, где је θ формула у пренекс форми са $n_\varphi - 1$ егзистенцијалних квантификатора у префиксу. Нека је φ' формула $\forall x_1 \cdots \forall x_m \theta$ и $\mathcal{L}'_S$ проширена сигнатура за Сколемову форму формуле φ' и f функцијски знак дужине m тако да је:

$$\mathcal{L}_S = \mathcal{L}'_S \cup \{f\},\ \mathrm{ar}(f) = m.$$

Формуле φ_S и $\varphi'(y/f(\overline{x}))_S$ су еквивалентне, па $\mathbf{M} \models \varphi'(y/f(\overline{x}))_S[v]$. Према индуктивној претпоставци $\mathbf{M} \models \varphi'(y/f(\overline{x}))[v]$, односно

$$\mathbf{M} \models \forall x_1 \cdots \forall x_m \theta(y/f(\overline{x}))[v].$$

За све $a_1, \ldots, a_m \in M$, важи

$$\mathbf{M} \models \theta(y/f(\overline{x}))[v(x_1 := a_1, \ldots, x_m := a_m)],$$

односно $\mathbf{M} \models \theta[v(x_1 := a_1, \ldots, x_m := a_m, y := f^{\mathbf{M}}(\overline{a}))]$, одакле следи $\mathbf{M} \models \exists y \theta[v(x_1 := a_1, \ldots, x_m := a_m)]$. Дакле,

$$\mathbf{M} \models \forall x_1 \cdots \forall x_m \exists y \theta[v],\ \text{тј. } \mathbf{M} \models \varphi[v].$$

Лема 12. *Ако* $\mathbf{M} \models \varphi$, *онда постоји експанзија* $\mathbf{M}_S$ *модела* $\mathbf{M}$ *таква да је* $\mathbf{M}_S \models \varphi_S$.

Доказ. Претпоставимо да је φ формула облика

$$\forall x_1 \cdots \forall x_k \exists y \theta(x_1, \ldots, x_k, y),$$

при чему је θ формула без квантификатора. Из

$$\mathbf{M} \models \forall x_1 \cdots \forall x_k \exists y \theta(x_1, \ldots, x_k, y)$$

следи да свака k-торка $\overline{a} = (a_1, \ldots, a_k)$ елемената из M одређује један непразан скуп,

$$Y_{\overline{a}} = \{b \in M \mid \mathbf{M} \models \theta[a_1, \ldots, a_k, b]\} \neq \emptyset.$$

Према аксиоми избора постоји функција $f : M^k \to M$ таква да $f(\overline{a}) \in Y_{\overline{a}}$, за све $\overline{a} \in M^k$. Ако је F нови операцијски симбол дужине k који не припада сигнатури формуле φ, онда је φ_S формула

$$\forall x_1 \cdots \forall x_k \theta[y/f(x_1, \ldots, x_k)].$$

Ако је $\mathbf{M}_S = (\mathbf{M}, f)$ екстензија структуре $\mathbf{M}$, при чему је $F^{\mathbf{M}_S} = f$, није тешко уочити да

$$\mathbf{M}_S \models \forall x_1 \cdots \forall x_k \theta[y/f(x_1, \ldots, x_k)],$$

тј. $\mathbf{M}_S \models \varphi_S$. $\square$

Последица 4. *1) Формула φ је задовољива акко је задовољива формула φ_S.*

2) Формула φ је ваљана акко $(\neg\varphi)_S$ није задовољива.

Пример 12. Да бисмо показали да је нека формула φ ваљана: можемо најпре наћи *пренекс конјунктивну нормалну форму* формуле $\neg\varphi$, а након *сколемизације* и трансформације формуле без квантификатора у конјунктивну нормалну форму, применом тзв. *резолуције* на одговарајући скуп клауза извести празну клаузу.

Детаљнији приказ методе резолуције биће дат на вежбама.

Докажимо помоћу резолуције да је формула

$$\exists x(\exists y(P(y) \Rightarrow \exists z Q(z)) \Rightarrow (P(x) \Rightarrow Q(x)))$$

ваљана.

Означимо са φ дату формулу.

$$\begin{aligned}
\neg\varphi &\equiv \neg\exists x(\exists y(P(y) \Rightarrow \exists z Q(z)) \Rightarrow (P(x) \Rightarrow Q(x)))\\
&\equiv \neg\exists x(\neg\exists y(\neg P(y) \vee \exists z Q(z)) \vee \neg P(x) \vee Q(x))\\
&\equiv \forall x(\exists y(\neg P(y) \vee \exists z Q(z)) \wedge P(x) \wedge \neg Q(x))\\
&\equiv \forall x \exists y \exists z((\neg P(y) \vee Q(z)) \wedge P(x) \wedge \neg Q(x))
\end{aligned}$$

Сколемизација.

$$\begin{aligned}
&\forall x((\neg P(f(x)) \vee Q(g(x))) \wedge P(x) \wedge \neg Q(x))\\
\equiv\ &\forall x(\neg P(f(x)) \vee Q(g(x)) \wedge \forall x P(x) \wedge \forall x \neg Q(x)\\
\equiv\ &\forall x(\neg P(f(x)) \vee Q(g(x)) \wedge \forall u P(u) \wedge \forall v \neg Q(v)
\end{aligned}$$

Нека је $\mathbb{C}_1 : \neg P(f(x)), Q(g(x))$; $\mathbb{C}_2 : P(u)$; $\mathbb{C}_3 : \neg Q(v)$. Није тешко уочити да E нема модел (тј. да из $E = \{\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_3\}$ изводимо празну клаузу), па ни $\neg\varphi$ нема модел.

Семантичка и синтаксна последица

Семантичка последица

Проблем испитивања (не)задовољивости неке реченице, природно се проширује на проблем испитивања (не)задовољивости неког скупа реченица, тј. неке *теорије*. Било који скуп реченица $T \subseteq \mathrm{Sent}_{\mathcal{L}}$ назива се **теоријом** језика $\mathcal{L}$, а реченице које припадају T називају се *аксиомама* те теорије.

Дефиниција 10. *Модел теорије T језика $\mathcal{L}$ јесте било која структура на језику $\mathcal{L}$ која задовољава све реченице из T. Контрамодел теорије T јесте било која структура која не задовољава бар једну реченицу из T.*

Пример 13. Нека је $\mathrm{Rel}_{\mathcal{L}} = \{R\}$, $\mathrm{ar}(R) = 2$, и T_{LU} теорија која садржи следеће четири реченице:

- $\forall x R(x,x)$,
- $\forall x \forall y (R(x,y) \land R(y,x) \Rightarrow x = y)$,
- $\forall x \forall y \forall z (R(x,y) \land R(y,z) \Rightarrow R(x,y))$,
- $\forall x \forall y (R(x,y) \lor R(y,x))$.

Реч је о веома важној теорији која зато носи и посебно име *теорија линеарног уређења*. Свима су блиски поједини модели ове теорије: $(\mathbb{N}, \leqslant)$, $(\mathbb{Z}, \leqslant)$, $(\mathbb{Q}, \leqslant)$, $(\mathbb{R}, \leqslant)$. Познати су и многи контрамодели: $(\mathbb{N}, |)$ (скуп природних бројева са релацијом дељивости, јер она није линеарна), $(\mathcal{P}(\mathbb{N}), \subseteq)$ (скуп подскупова од $\mathbb{N}$ са релацијом инклузије), $(\mathbb{Z}, <)$ (скуп целих бројева са релацијом строгог уређења), итд.

У математици је уобичајено да се стално преплићу проблеми трагања за формулама које су тачне у неком конкретном моделу и трагања за моделима у којима су тачне неке задате формуле. То ћемо илустровати у наредном примеру.

Пример 14. **Теорија група.**
На језику $\mathcal{L}_{\mathrm{GR}} = \{*, ^{-1}, e\}$, $\mathrm{Fun}_{\mathcal{L}_{\mathrm{GR}}} = \{*, ^{-1}\}$, $\mathrm{ar}(*) = 2$; $\mathrm{ar}(^{-1}) = 1$, $\mathrm{Cons}_{\mathcal{L}_{\mathrm{GR}}} = \{e\}$ формулишему теорију група

$$T_{\mathrm{GR}} = \{\forall x \forall y \forall z (x * (y * z) = (x * y) * z),\ \forall x (x * e = x),\ \forall x (x * x^{-1} = e)\}.$$

Модели теорије T_{GR} јесу *групе*.

Пример 15. **Теорија уређених поља.**
Посматрајмо језик $\mathcal{L}_{\mathrm{OF}} = \{\leqslant, +, -, \cdot, 0, 1\}$, при чему је $\mathrm{Rel}_{\mathcal{L}} = \{\leqslant\}$, $\mathrm{Fun}_{\mathcal{L}} = \{+, -, \cdot\}$, $\mathrm{Const}_{\mathcal{L}} = \{0, 1\}$ и $\mathrm{ar}(\leqslant) = \mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$,

$\mathrm{ar}(-) = 1$. Означимо са T_{FO} теорију језика $\mathcal{L}_{\mathrm{FO}}$ познату као *теорија уређених поља*, чије су аксиоме следеће реченице:

(**Sk**) $\forall x \forall y (x + y = y + x)$,
(**Sa**) $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$,
(**Sn**) $\forall x (x + 0 = x)$,
(**Si**) $\forall x (x + (-x) = 0)$,
(**Mk**) $\forall x \forall y (x \cdot y = y \cdot x)$,
(**Ma**) $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,
(**Mn**) $\forall x (x \cdot 1 = x)$,
(**Mi**) $\forall x (x \neq 0 \Rightarrow \exists y (x \cdot y = 1))$,
(**SM**) $\forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$,
(**01**) $0 \neq 1$,
(**Ur**) $\forall x (x \leqslant x)$,
(**Ua**) $\forall x \forall y (x \leqslant y \wedge y \leqslant x \Rightarrow x = y)$,
(**Ut**) $\forall x \forall y \forall z (x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z)$,
(**Ul**) $\forall x \forall y (x \leqslant y \vee y \leqslant x)$,
(**US**) $\forall x \forall y \forall z (x \leqslant y \Rightarrow x + z \leqslant y + z)$,
(**UM**) $\forall x \forall y \forall z (x \leqslant y \wedge 0 \leqslant z \Rightarrow x \cdot z \leqslant y \cdot z)$.

Сваки модел у коме су тачне све наведене реченице називамо *уређеним пољем*. Структуре $\mathbf{R} = (\mathbb{R}, \leqslant, +, -, \cdot, 0, 1)$ и $\mathbf{Q} = (\mathbb{Q}, \leqslant, +, -, \cdot, 0, 1)$, са стандардним интерпретацијама нелогичких симбола, јесу уређена поља. Са још неким уређеним пољима срешћемо се касније.

Пример 16. **Теорије модела.** Посебно су занимљиве теорије које окупљају све реченице тачне у некој фиксираној структури, нарочито ако она заузима важно место у математици. Пример такве структуре јесте свакако уређено поље реалних бројева $\mathbf{R} = (\mathbb{R}, \leqslant, +, -, \cdot, 0, 1)$. Нека је

$$\mathrm{Th}(\mathbf{R}) = \{\sigma \in \mathrm{Sent}_{\mathcal{L}_{\mathrm{FO}}} \mid \mathbf{R} \models \sigma\}.$$

Очигледно је $T_{\mathrm{OF}} \subseteq \mathrm{Th}(\mathbf{R})$ и $\mathbf{R} \models \mathrm{Th}(\mathbf{R})$. Међутим, има ли теорија $\mathrm{Th}(\mathbf{R})$ других модела који су различити од $\mathbf{R}$? Притом, наравно, мислимо на структуре које нису изоморфне са $\mathbf{R}$ (видети наредну дефиницију). Одговор је потврдан, а касније ћемо видети и зашто.

Слична питања се намећу и за било коју структуру $\mathbf{M}$ неког језика $\mathcal{L}$, тј. за теорију $\mathrm{Th}(\mathbf{M}) = \{\sigma \in \mathrm{Sent}_{\mathcal{L}} \mid \mathbf{M} \models \sigma\}$.

Ако је $\mathbf{M}$ нека $\mathcal{L}$-структура, скуп свих $\mathcal{L}$-реченица тачних у $\mathbf{M}$, тј.

$$\mathrm{Th}(\mathbf{M}) = \{\sigma \in \mathrm{Sent}_{\mathcal{L}} \mid \mathbf{M} \models \sigma\},$$

називамо *теоријом модела* $\mathbf{M}$.

Лема 13. *Ако је* $\mathbf{A} \cong \mathbf{B}$, *онда је* $\mathrm{Th}(\mathbf{A}) = \mathrm{Th}(\mathbf{B})$.

Дефиниција 11. *Ако је* Γ *неки скуп формула и* α *формула језика* $\mathcal{L}$, *кажемо да је* α ***семантичка последица*** *скупа* Γ, *у ознаци* $\Gamma \models \alpha$, *ако за сваки модел* $\mathbf{M}$ *језика* $\mathcal{L}$ *и сваку валуацију* $v : \mathrm{Var} \to M$,

$$\text{из } \mathbf{M} \models \gamma[v], \text{ за свако } \gamma \in \Gamma, \text{ следи да } \mathbf{M} \models \alpha[v].$$

Уместо $\emptyset \models \alpha$ *пишемо* $\models \alpha$.

Приметимо да $\models \alpha$ заправо значи да је α ваљана формула. Као што се и очекује, најзанимљивији ће нам бити случајеви када је Γ скуп реченица и α нека реченица истог језика.

Пример 17. Сетимо се да је група свака структура $\mathbf{G} = (G, *, ^{-1}, e)$ која је модел теорије група T_{GR}. Посматрајмо тврђење

У свакој групи важи десни закон канцелације (скраћивања).

Десни закон канцелације, на језику теорије група, можемо изразити следећом реченицом $\forall x \forall y \forall z(x * z = y * z \Rightarrow x = y)$, коју ћемо означити са σ. Уз ове ознаке, $T_{\mathrm{GR}} \models \sigma$ каже исто што и наведено тврђење. Уобичајен доказ тече овако.

Нека је $(G, *, ^{-1}, e)$ произвољна група (модел за T_{GR}).

1. Изаберимо произвољне елементе x, y, z из G, такве да је $x * z = y * z$. Тада је

2. $(x * z) * z^{-1} = (y * z) * z^{-1}$, [добра дефинисаност операције $*$]

3. $x * (z * z^{-1}) = y * (z * z^{-1})$, [из претходног према закону асоцијативности]

4. $x * e = y * e$, [из претходног јер је $z * z^{-1} = e$]

5. $x = y$, [из претходног јер је $x * e = x$ и $y * e = y$]

6. $\forall x \forall y \forall z(x * z = y * z \Rightarrow x = y)$. [јер су x, y, z произвољни елементи]

Синтаксна последица

Појам синтаксне последице пружа веома добар увид у то како спроводимо доказе у математици. Осврнимо се мало детаљније на доказ дат у примеру 17 и доказ да десни закон канцелације важи у свакој групи. Иако смо током доказа замишљали да радимо са неком конкретном (произвољно изабраном) групом, ниједног тренутка нисмо имали потребу да прецизирамо о којој је заиста групи реч, већ смо искључиво користили законитости које група задовољава по дефиницији, као и добро позната својства једнакости и операција (функција). Другим речима, значајне су само аксиоме теорије група, док је семантика у овом случају само психолошка подршка за онога ко спроводи доказ.

Дефиниција 12. *Формула* α *је синтаксна последица скупа формула* Γ, *ако се секвент* $\Gamma \vdash \alpha$ *може добити применом следећих правила коначан број пута:*

Аксиома

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ (\mathrm{ax})$$

Слабљење

$$\frac{\Gamma \vdash \varphi}{\Gamma, \gamma \vdash \varphi}\ (\mathrm{slab})$$

Увођење импликације

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \Rightarrow \psi}\ (\Rightarrow_{\mathrm{U}})$$

Елиминација импликације

$$\frac{\Gamma \vdash \varphi \Rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\Rightarrow_{\mathrm{E}})$$

Увођење конјункције

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge_{\mathrm{U}})$$

Елиминација конјункције

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ (\wedge^{\mathrm{l}}_{\mathrm{E}}) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ (\wedge^{\mathrm{d}}_{\mathrm{E}})$$

Увођење дисјункције

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee^{\mathrm{l}}_{\mathrm{U}}) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee^{\mathrm{d}}_{\mathrm{U}})$$

Елиминација дисјункције

$$\frac{\Gamma \vdash \varphi \vee \psi \quad \Gamma, \varphi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\ (\vee_{\mathrm{E}})$$

Увођење негације

$$\frac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi}\ (\neg_{\mathrm{U}})$$

Елиминација негације

$$\frac{\Gamma \vdash \neg\varphi \quad \Gamma \vdash \varphi}{\Gamma \vdash \bot}\ (\neg_{\mathrm{E}})$$

Увођење универзалног квантификатора

$$\frac{\Gamma \vdash \varphi \quad x \text{ није слободно у формулама скупа } \Gamma}{\Gamma \vdash \forall x \varphi}\ (\forall_{\mathrm{U}})$$

Елиминација универзалног квантификатора

$$\frac{\Gamma \vdash \forall x \varphi}{\Gamma \vdash \varphi[x/t]}\ (\forall_{\mathrm{E}})$$

Увођење егзистенцијалног квантификатора

$$\frac{\Gamma \vdash \varphi[x/t]}{\Gamma \vdash \exists x \varphi}\ (\exists_{\mathrm{U}})$$

Елиминација егзистенцијалног квантификатора

$$\frac{\Gamma \vdash \exists x \varphi \quad \Gamma, \varphi \vdash \theta \quad x \text{ није слободно у формулама скупа } \Gamma \cup \{\theta\}}{\Gamma \vdash \theta}\ (\exists_{\mathrm{U}})$$

Увођење једнакости

$$\frac{}{\Gamma \vdash t = t}\ (=_{\mathrm{U}})$$

Елиминација једнакости

$$\frac{\Gamma \vdash \varphi[v/t] \quad \Gamma \vdash t = u}{\Gamma \vdash \varphi[v/u]}\ (=_{\mathrm{E}})$$

Класична противречност

$$\frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}\ (\bot_{\mathrm{c}})$$

Дефиниција 13. *Формула σ је доказива, тј. јесте теорема логике првог реда, у ознаци $\vdash \sigma$, ако је доказив секвент $\emptyset \vdash \sigma$.*

У наредним примерима илустроваћемо примену правила која се односе на квантификаторе и једнакост.

Пример 18. $\vdash \forall x\alpha \vee \forall x\beta \Rightarrow \forall x(\alpha \vee \beta)$

1. $\forall x\alpha \vee \forall x\beta \vdash \forall x\alpha \vee \forall x\beta$ (ax)
2. $\forall x\alpha \vee \forall x\beta, \forall x\alpha \vdash \forall x\alpha$ (ax)
3. $\forall x\alpha \vee \forall x\beta, \forall x\alpha \vdash \alpha$ из 2 према $(\forall_{\mathrm{E}})$

4. $\forall x\alpha \vee \forall x\beta, \forall x\alpha \vdash \alpha \vee \beta$ из 3 према $(\vee^{\mathrm{l}}_{\mathrm{U}})$
5. $\forall x\alpha \vee \forall x\beta, \forall x\alpha \vdash \forall x(\alpha \vee \beta)$ из 4 према $(\forall_{\mathrm{U}})$
[променљива x није слободна у формулама са леве стране рампе]
6. $\forall x\alpha \vee \forall x\beta, \forall x\beta \vdash \forall x\beta$ (ax)
7. $\forall x\alpha \vee \forall x\beta, \forall x\beta \vdash \beta$ из 6 према $(\forall_{\mathrm{E}})$
8. $\forall x\alpha \vee \forall x\beta, \forall x\beta \vdash \alpha \vee \beta$ из 7 према $(\vee^{\mathrm{d}}_{\mathrm{U}})$
9. $\forall x\alpha \vee \forall x\beta, \forall x\beta \vdash \forall x(\alpha \vee \beta)$ из 8 према $(\forall_{\mathrm{U}})$
10. $\forall x\alpha \vee \forall x\beta \vdash \forall x(\alpha \vee \beta)$ из 1, 5, 9 према $(\vee_{\mathrm{E}})$
11. $\vdash \forall x\alpha \vee \forall x\beta \Rightarrow \forall x(\alpha \vee \beta)$ из 10 према $(\Rightarrow_{\mathrm{U}})$

Пример 19. $\vdash \exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$
1. $\exists x(\alpha \wedge \beta) \vdash \exists x(\alpha \wedge \beta)$ (ax)
2. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \alpha \wedge \beta$ (ax)
3. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \alpha$ из 2 према $(\wedge^{\mathrm{l}}_{\mathrm{E}})$
4. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \exists x\alpha$ из 3 према $(\exists_{\mathrm{U}})$
5. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \beta$ из 2 према $(\wedge^{\mathrm{d}}_{\mathrm{E}})$
6. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \exists x\beta$ из 5 према $(\exists_{\mathrm{U}})$
7. $\exists x(\alpha \wedge \beta), \alpha \wedge \beta \vdash \exists x\alpha \wedge \exists x\beta$ из 4, 6 према $(\wedge_{\mathrm{U}})$
8. $\exists x(\alpha \wedge \beta) \vdash \exists x\alpha \wedge \exists x\beta$ из 1,7 према $(\exists_{\mathrm{E}})$
[променљива x није слободна у формулама $\exists x(\alpha \wedge \beta)$ и $\exists x\alpha \wedge \exists x\beta$]
9. $\vdash \exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$ из 8 према $(\Rightarrow_{\mathrm{U}})$

Пример 20. $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$
1. $x_1 = x_2 \vdash x_1 = x_1$ $(=_{\mathrm{U}})$

Ако са $\alpha(x)$ означимо формулу $x = x_1$, онда је $\alpha[x/x_1]$ формула $x_1 = x_1$.

2. $x_1 = x_2 \vdash x_1 = x_2$ (ax)
3. $x_1 = x_2 \vdash x_2 = x_1$ из 1, 2 према $(=_{\mathrm{E}})$
$\alpha[x/x_2]$ је формула $x_2 = x_1$.
4. $\vdash x_1 = x_2 \Rightarrow x_2 = x_1$ из 3 према $(\Rightarrow_{\mathrm{U}})$
5. $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$ из 4 према $\forall_{\mathrm{U}}$ (два пута)

Пример 21. $\vdash \forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$
1. $x_1 = x_2 \wedge x_2 = x_3 \vdash x_1 = x_2 \wedge x_2 = x_3$ (ax)
2. $x_1 = x_2 \wedge x_2 = x_3 \vdash x_1 = x_2$ из 1 према $(\wedge^{\mathrm{l}}_{\mathrm{E}})$

Ако са $\alpha(x)$ означимо формулу $x_1 = x$, онда је $\alpha[x/x_2]$ формула $x_1 = x_2$.

3. $x_1 = x_2 \wedge x_2 = x_3 \vdash x_2 = x_3$ из 1 према $(\wedge^{\mathrm{d}}_{\mathrm{E}})$
4. $x_1 = x_2 \wedge x_2 = x_3 \vdash x_1 = x_3$ из 2, 3 према (= E)
$\alpha[x/x_3]$ формула $x_1 = x_2$.
5. $\vdash x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3$ из 4 према $(\Rightarrow_{\mathrm{U}})$
6. $\vdash \forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$ из 5 према $(\forall_{\mathrm{U}})$ (три пута)

Као и у случају исказне логике, изведена правила нам могу знатно олакшати доказивање секвената. У наредној леми дајемо само једно овакво правило, док су многа друга дата у задатку ??.

Лема 14. $\dfrac{}{\Gamma, r = s \vdash t[x/r] = t[x/s]}\ (=_{\mathrm{C}})$

Доказ.
1. $\Gamma, r = s \vdash r = s$ (ax)
2. $\Gamma, r = s \vdash t = t$ $(=_{\mathrm{U}})$
3. $\Gamma, r = s \vdash t[x/r] = t[x/s]$ из 1, 2 према $(=_{\mathrm{E}})$.

□

У наставку овог одељка анализираћемо неколико „обичних“ математичких доказа. Примери које наводимо не само да илуструју значај уведеног списка правила за доказивање секвената, већ имају за циљ и да расветле уобичајене математичке доказе.

Пример 22. Нека је f унарни операцијски симбол и нека је:

- Inj_f формула $\forall x \forall y (f(x) = f(y) \Rightarrow x = y)$ (која значи: f је 1-1 функција);
- Sur_f формула $\forall y \exists x (f(x) = y)$ (која значи: f је на функција);
- Bij_f формула $\mathrm{Inj}_f \wedge \mathrm{Sur}_f$ (која значи: f је бијекција);
- Inv_f формула $\forall x (f(f(x)) = x)$ (која значи: f је инволуција).

Докажимо $\mathrm{Inv}_f \vdash \mathrm{Bij}_f$.

1. $\mathrm{Inv}_f \vdash \forall x (f(f(x)) = x)$ (ax)
2. $\mathrm{Inv}_f \vdash (f(f(y)) = y)$ из 1 према $(\forall_{\mathrm{E}})$, односно $\mathrm{Inv}_f \vdash (f(x) = y)[x/f(y)]$
3. $\mathrm{Inv}_f \vdash \exists x (f(x) = y)$ из 2 према $(\exists_{\mathrm{U}})$
4. $\mathrm{Inv}_f \vdash \forall y \exists x (f(x) = y)$ из 3 према $(\forall_{\mathrm{U}})$, односно $\mathrm{Inv}_f \vdash \mathrm{Sur}_f$
5. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(x) = f(y)$ (ax)
6. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(x)) = f(f(y))$ $(=_{\mathrm{C}})$
7. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(x)) = x$ из 1 према $(\forall_{\mathrm{E}})$ и (slab)
8. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(y)) = y$ из 1 према $(\forall_{\mathrm{E}})$ и (slab)
9. $\mathrm{Inv}_f, f(x) = f(y) \vdash x = y$ из 6, 7, 8 према $2 \times (=_{\mathrm{E}})$
10. $\mathrm{Inv}_f \vdash \forall x \forall y (f(x) = f(y) \Rightarrow x = y)$ из 9 према $(\Rightarrow_{\mathrm{U}}) + 2 \times (\forall_{\mathrm{U}})$, односно $\mathrm{Inv}_f \vdash \mathrm{Inj}_f$
11. $\mathrm{Inv}_f \vdash \mathrm{Bij}_f$ из 4, 10 према $(\wedge_{\mathrm{U}})$

Дато извођење у потпуности одговара уобичајеном доказу да *инволуција мора бити бијекција.*

Претпоставимо да је f инволутивна функција. Доказаћемо да је бијекција. Потребно је доказати да је 1-1 и на-функција $(\wedge_{\mathrm{U}})$.
f је 1-1 функција? Нека су x и y произвољни $(\forall_{\mathrm{U}})$. Претпоставимо да је $f(x) = f(y)$, и докажимо да је $x = y$ $(\Rightarrow_{\mathrm{U}})$. Ово је последица следеће три једнакости $(2\times =_{\mathrm{E}})$:
(i) $f(f(x)) = x$,
(ii) $f(f(y)) = y$,

$(iii)\ f(f(x)) = f(f(y))$.
Једнакости (i) и (ii) важе јер је f инволуција $(\exists_E), (\mathrm{ax})$. Једнакост (iii) је последица претпоставке $f(x) = f(y)$ $(=_c)$.
$\underline{f \text{ је на-функција}}$? Ако је y произвољно, доказаћемо да постоји x тако да је $f(x) = y$ $(\forall_U)$. Нека је $x = f(y)$ $(\exists_U)$. Пошто је f инволуција, добијамо да је $f(f(y)) = y$, $(\exists_E), (\mathrm{ax})$.

ПРИМЕР 23. **Лева правила извођења и један доказ из анализе**. Већ смо рекли да изведена правила значајно олакшавају извођење секвената. Што више таквих правила знамо, једноставније изводимо доказе. Посебно су корисна тзв. *лева правила* којима се смањује сложеност формула са леве стране рампе ако се читају одоздо на горе. Сетимо се да овако читамо правила када трагамо за неким доказом. Наводимо четири таква правила:

$$\frac{\Gamma, \varphi, \psi \vdash \theta}{\Gamma, \varphi \wedge \psi \vdash \theta}(\wedge_L) \quad \frac{\Gamma, \varphi, \psi \vdash \theta}{\Gamma, \varphi, \varphi \Rightarrow \psi \vdash \theta}(\Rightarrow_L) \quad \frac{\Gamma, \forall x\varphi, \varphi[x/t] \vdash \theta}{\Gamma, \forall x\varphi \vdash \theta}(\forall_L)$$

$$\frac{\Gamma, \alpha \vdash \theta \quad x \text{ није слободно у формулама из } \Gamma \cup \{\theta\}}{\Gamma, \exists x\alpha \vdash \theta}(\exists_L)$$

Грубо говорећи, изведена правила имају сличну улогу као разна помоћна тврђења која користимо приликом доказивања било које нове теореме. Све ово илустроваћемо на једној теореми из математичке анализе.

Нека је језик уређених поља $\{\leqslant, +, \cdot, -, 0, 1\}$ проширен бинарним релацијским симболима $<$, $\geqslant$, $>$, унарним операцијским симболима $|\ |$ и $/2$ (овај последњи ће здесна „дејствовати" на аргумент). Усвајамо и следећи уобичајен договор да формула $(\forall x > u)\, \alpha$ означава формулу $\forall x(x > u \Rightarrow \alpha)$, а $(\exists x > u)\, \alpha$ формулу $\forall x(x > u \wedge \alpha)$, и слично за било коју другу променљиву и за остале знаке $<$, $\leqslant$, $\geqslant$.

Означимо са $\lim\limits_{x\to+\infty} f(x) = \ell$ формулу $\forall \varepsilon > 0\, \exists \delta\, \forall x \geqslant \delta\ |f(x) - \ell| < \varepsilon$. Нека је и:

Lema_1 формула $\forall x\, \forall y\, \exists z\, (z \geqslant x \wedge z \geqslant y)$;

Lema_2 формула $\forall x\, \neg(x < x)$;

Lema_3 формула $\forall x\, \forall y \forall z_1 \forall z_2(|y - z_1| < x/2 \wedge |y - z_2| < x/2 \Rightarrow |z_1 - z_2| < x)$;

Lema_4 формула $\forall x\, \forall y(x \neq y \Rightarrow |x - y|/2 > 0)$.

Доказаћемо да

$$\mathrm{Lema}_1, \mathrm{Lema}_2, \mathrm{Lema}_3, \mathrm{Lema}_4 \vdash \lim_{x\to+\infty} f(x) = \ell \wedge \lim_{x\to+\infty} f(x) = \ell' \Rightarrow \ell = \ell'.$$

1. Доказивање жељеног секвента, према правилима $(\Rightarrow_U)$, $(\wedge_L)$ и $(\perp_c)$, можемо свести на доказивање секвента:

   $$\mathrm{Lema}_1, \mathrm{Lema}_2, \mathrm{Lema}_3, \mathrm{Lema}_4, \lim_{x\to+\infty} f(x) = \ell, \lim_{x\to+\infty} f(x) = \ell', \ell \neq \ell' \vdash \perp.$$

   Да бисмо поједноставили записивање, означимо са Γ скуп формула са леве стране рампе.

2. Нека је $\bar{\varepsilon}$ терм $|\ell - \ell'|/2$. Тада према правилу $(\forall_{\mathrm{L}})$ примењеном три пута, претходни секвент сводимо на

$$\Gamma, \exists \delta \, \forall x \geqslant \delta \; |f(x) - \ell| < \bar{\varepsilon}, \exists \delta \, \forall x \geqslant \delta \; |f(x) - \ell'| < \bar{\varepsilon}, \bar{\varepsilon} > 0 \vdash \bot.$$

Правилом $(\forall_{\mathrm{L}})$ „активирали смо“ формуле $\lim\limits_{x \to +\infty} f(x) = \ell$, $\lim\limits_{x \to +\infty} f(x) = \ell'$ супституцијама $[\varepsilon/\bar{\varepsilon}]$, као и формулу Lema_4, супституцијама $[x/\ell]$ и $[y/\ell']$.

3. Формуле, које су додате са леве стране рампе у претходном кораку, даље разграђујемо употребом правила $(\exists_{\mathrm{L}})$, тако што уводимо нове променљиве δ_1 и δ_2 које се не појављују слободно у осталим формулама.

$$\cdots, \forall x \geqslant \delta_1 \; |f(x) - \ell| < \bar{\varepsilon}, \forall x \geqslant \delta_2 \; |f(x) - \ell'| < \bar{\varepsilon}, \bar{\varepsilon} > 0 \vdash \bot.$$

Да бисмо поједноставили запис, уместо набрајања свих формула са леве стране рампе, издвојили смо само најважније, а остале заменили тачкицама.

4. Ако формулу Lema_1 активирамо двоструком применом правила $(\forall_{\mathrm{L}})$ при супституцијама $[x/\delta_1]$ и $[y/\delta_2]$, а затим уведемо нову променљиву z која није слободна у осталим формулама, позивајући се на правило $(\exists_{\mathrm{L}})$, и најзад применимо $(\wedge_{\mathrm{L}})$ добијамо:

$$\cdots, z \geqslant \delta_1, z \geqslant \delta_2, \forall x \geqslant \delta_1 \; |f(x) - \ell| < \bar{\varepsilon}, \forall x \geqslant \delta_2 \; |f(x) - \ell'| < \bar{\varepsilon}, \bar{\varepsilon} > 0 \vdash \bot.$$

5. Након одговарајуће примене правила $(\forall_{\mathrm{L}})$ и $(\Rightarrow_{\mathrm{L}})$, два пута, долазимо до следећег секвента

$$\cdots, |f(z) - \ell| < \bar{\varepsilon}, |f(z) - \ell'| < \bar{\varepsilon} \vdash \bot.$$

6. Активирањем формуле Lema_3 при супституцијама $[x/|\ell - \ell'|]$, $[y/f(z)]$, $[z_1/\ell]$ и $[z_2/\ell']$ (подсећамо да је $\bar{\varepsilon}$ терм $|\ell - \ell'|/2$), а затим применом правила $(\wedge_{\mathrm{L}})$ и $(\Rightarrow_{\mathrm{L}})$, долазимо до секвента:

$$\cdots, |\ell - \ell'| < |\ell - \ell'| \vdash \bot.$$

7. Најзад, активирањем формуле Lema_4 при супституцији $[x/|\ell - \ell'|]$, стижемо до секвента

$$\cdots, |\ell - \ell'| < |\ell - \ell'|, \neg |\ell - \ell'| < |\ell - \ell'| \vdash \bot,$$

који се може добити применом правила $(\neg_{\mathrm{L}})$. Доказ је завршен.

Приметимо да су главне досетке у изложеном доказу супституције којим активирамо претпоставке са леве стране рампе.

Пример 24. У овом примеру користићемо неколико, интуитивно јасних, изведених правила који се односе на једнакост.

$$\frac{}{\Gamma \vdash t = t}(=_{\mathrm{R}}) \quad \frac{\Gamma \vdash t_1 = t_2}{\Gamma \vdash t_2 = t_1}(=_{\mathrm{S}}) \quad \frac{\Gamma \vdash t_1 = t_2 \quad \Gamma \vdash t_2 = t_3}{\Gamma \vdash t_1 = t_3}(=_{\mathrm{T}})$$

$$\frac{\Gamma \vdash t_1 = t_2}{\Gamma \vdash t(x/t_1) = t(x/t_2)}(=_{\mathrm{sup}}).$$

Поред тога, значајно ћемо поједноставити записивање, тако што ћемо само једном, на почетку доказа, навести скуп претпоставки Γ, а затим током извођења подразумевати и изостављати део „$\Gamma \vdash$“, што је иначе уобичајена пракса у математици.

Претпоставимо да језик садржи један бинарни операцијски знак, који ћемо означавати двема вертикалним цртама $|\ |$ (између којих долазе аргументи), и два тернарна знака које ћемо означавати са $\angle$ и $\triangle$ (и који очекују три аргумента са десне стране). Нека је T_{cong} теорија чије су аксиоме универзална затворења следећих формула:

γ_1 $|xy| = |yx|$,

γ_2 $\angle xyz = \angle zyx$,

γ_3 $\triangle xyz = \triangle uvw \Rightarrow |xy| = |uv| \wedge |yz| = |vw| \wedge |zx| = |wu|$,

γ_4 $\triangle xyz = \triangle uvw \Rightarrow \angle xyz = \angle uvw \wedge \angle yzx = \angle vwu \wedge \angle zxy = \angle wuv$,

γ_5 $|xy| = |uv| \wedge \angle xyz = \angle uvw \wedge |yz| = |vw| \Rightarrow \triangle xyz = \triangle uvw$.

Доказаћемо

$$T_{\mathrm{cong}} \vdash |ab| = |ac| \Rightarrow \angle abc = \angle acb.$$

Према правилу $(\Rightarrow_{\mathrm{U}})$, доказивање жељеног секвента сводимо на

$$T_{\mathrm{cong}}, |ab| = |ac| \vdash \angle abc = \angle acb.$$

Дакле, скуп претпоставки Γ садржи формуле γ_1, γ_2, γ_3, γ_4, γ_5 и $|ab| = |ac|$ (па у наставку испред сваке формуле подразумевамо да стоји $\Gamma \vdash$).

1. $|ab| = |ac|$ претпоставка, тј. (ax)
2. $|ac| = |ab|$ из 1 према $(=_{\mathrm{S}})$
3. $|ab| = |ba|$ активирањем γ_1 правилом $(\forall_{\mathrm{E}})$ при $[x/a]$, $[y/b]$
4. $|ba| = |ab|$ из 3 према $(=_{\mathrm{S}})$
5. $|ba| = |ac|$ из 4, 1 према $(=_{\mathrm{T}})$
6. $|ac| = |ca|$ активирањем γ_1 правилом $(\forall_{\mathrm{E}})$ при $[x/a]$, $[y/c]$
7. $|ba| = |ca|$ из 5, 6 према $(=_{\mathrm{T}})$
8. $\angle bac = \angle cab$ активирањем γ_2 правилом $(\forall_{\mathrm{E}})$ при $[x/b]$, $[y/a]$, $[z/c]$
9. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab|$ из 7, 8, 2 применом $(\wedge_{\mathrm{U}})$ два пута
10. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab| \Rightarrow \triangle bac = \triangle cab$ активирањем γ_5 правилом $(\forall_{\mathrm{E}})$ при $[x/b]$, $[y/a]$, $[z/c]$, $[u/c]$, $[v/a]$, $[z/b]$
11. $\triangle bac = \triangle cab$ из 9, 10 према $(\Rightarrow_{\mathrm{E}})$
12. $\triangle cab = \triangle bac$ из 11 према $(=_{\mathrm{S}})$

13. $\triangle cab = \triangle bac \Rightarrow \angle cab = \angle bac \land \angle abc = \angle acb \land \angle bca = \angle cba$,
активирањем γ_4 правилом $(\forall_{\mathrm{E}})$ при $[x/c]$, $[y/a]$, $[z/b]$, $[u/b]$, $[v/a]$, $[w/c]$
14. $\angle cab = \angle bac \land \angle abc = \angle acb \land \angle bca = \angle cba$ из 12, 13 према $(\Rightarrow_{\mathrm{E}})$
15. $\angle abc = \angle acb$ из 14 према $(\land^{\mathrm{l}}_{\mathrm{E}})$ и $(\land^{\mathrm{d}}_{\mathrm{E}})$.

Пример 25. Значајну врсту теорија представљају оне којима се уводе важне алгебарске структуре, као групе на пример. Реч је о теоријама чије су аксиоме универзална затворења атомичних формула облика $t_1 = t_2$, где су t_1 и t_2 неки изрази одговарајућег језика. Овакве реченице се називају *алгебарским законима*, па се сходно томе теорије које садрже само алгебарске законе називају *алгебарским теоријама*. Алгебарски закони често се наводе без навођења универзалних квантификатора (који се, наравно, имплицитно подразумевају). Ослањајући се на запажања која се намећу у претходном примеру, наслућујемо да се значајно може поједноставити доказивање да је неки алгебраски закон последица дате алгебраске теорије. Тако, доказ да је неки алгебарски закон синтаксна последица алгебарске теорије Γ спроводимо користећи правила тзв. *једнакосне логике*:

$$\frac{}{t = t}(=_{\mathrm{R}}) \quad \frac{t_1 = t_2}{t_2 = t_1}(=_{\mathrm{S}}) \quad \frac{t_1 = t_2 \quad t_2 = t_3}{t_1 = t_3}(=_{\mathrm{T}}) \quad \frac{t_1 = t_2}{t[x/t_1] = t[x/t_2]}(=_{\mathrm{sup}}).$$

Кажемо да је алгебарски закон $u = v$ последица алгебарске теорије Γ, у ознаци $\Gamma \vdash_{\mathrm{J}} u = v$, ако постоји коначан низ једнакости $u_1 = v_1, \ldots, u_n = v_n$, $u = v$ (који се завршава једнакошћу $u = v$) такав да свака једнакост у низу или припада Γ или се може добити применом неког од правила једнакосне логике, директно (према правилу $(=_{\mathrm{R}})$) или на једнакости које јој претходе у низу. Није тешко доказати да се може користити и следеће изведено правило:

Индекс DD можемо схватити као скраћеницу за „добра дефинисаност“.

$$\frac{u_1 = v_1 \quad u_2 = v_2 \quad \cdots \quad u_n = v_n}{F(u_1, \ldots, u_n) = F(v_1, \ldots, v_n)}(=_{\mathrm{DD}}),$$

где је F неки n-арни операцијски знак.

Докажимо, на пример, да је

$$x * (y * z) = (x * y) * z, x * e = x, x * x^{-1} = e \vdash_{\mathrm{J}} (x * y) * y^{-1} = x.$$

1. $x * (y * z) = (x * y) * z$ претпоставка (аксиома)
2. $(x * y) * z = x * (y * z)$ из 1 према $(=_{\mathrm{S}})$
3. $(x * y) * y^{-1} = x * (y * y^{-1})$ из 2 према $(=_{\mathrm{sup}})$, $[z/y^{-1}]$
4. $x * x^{-1} = e$ претпоставка (аксиома)
5. $y * y^{-1} = e$ из 4 према $(=_{\mathrm{sup}})$, $[x/y]$
6. $x = x$ претпоставка (аксиома)
7. $x * (y * y^{-1}) = x * e$ из 6, 5 према $(=_{\mathrm{DD}})$
8. $x * e = x$ претпоставка (аксиома)
9. $x * (y * y^{-1}) = x$ из 7, 8 према $(=_{\mathrm{T}})$

Приметимо да све ове кораке подразумевамо (укључујући и одговарајућа објашњења) и када наводимо исти доказ у најсажетијем облику:

$$(x * y) * y^{-1} = x * (y * y^{-1}) = x * e = x.$$

Није тешко уочити да се наведени („једнакосни“) доказ једноставно може прерадити у доказ секвента $T_{\mathrm{GR}} \vdash \forall x \forall y((x * y) * y^{-1} = x)$.

Теорема 3. [***Теорема потпуности***] *$\Gamma \vdash \alpha$ акко $\Gamma \models \alpha$.*

ЗАДАТАК **16.**

Пеанова аритметика (првог реда), у ознаци **PA**, јесте теорија на језику $\mathcal{L}_{\mathrm{PA}} = \{\leqslant, s, +, \cdot, 0\}$ ($\mathrm{Rel}_{\mathcal{L}_{\mathrm{PA}}} = \{\leqslant\}$, $\mathrm{Fun}_{\mathcal{L}_{\mathrm{PA}}} = \{s, +, \cdot\}$, $\mathrm{ar}(\leqslant) = \mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$, $\mathrm{ar}(s) = 1$, $\mathrm{Const}_{\mathcal{L}_{\mathrm{PA}}} = \{0\}$), која садржи следеће реченице

PA1 $\forall x \neg 0 = s(x)$,
PA2 $\forall x \forall y (s(x) = s(y) \Rightarrow x = y)$,
PA3 $\forall x (x + 0 = x)$,
PA4 $\forall x \forall y (x + s(y) = s(x + y))$,
PA5 $\forall x (x \cdot 0 = 0)$,
PA6 $\forall x \forall y (x \cdot s(y) = (x \cdot y) + x)$,
PA7 $\forall x \forall y (x \leqslant y \Leftrightarrow \exists z (z + x = y))$,
PA8 $(\varphi(0) \wedge \forall x(\varphi(x) \Rightarrow \varphi(s(x)))) \Rightarrow \forall x \varphi(x)$.

Приметимо да је *принцип индукције* (**PA8**) исказан бесконачним списком аксиома – за сваку формулу $\varphi(x)$ уведена је по једна аксиома.

Доказати:
(а) **PA** $\vdash \forall x \forall y (x + y = y + x)$,
(*Упутство.* Доказати најпре да је **PA** $\vdash \forall y (0 + y = y + 0)$.)
(б) **PA** $\vdash \forall x (x \leqslant x)$,
(в) **PA** $\vdash \forall x \forall y (x \leqslant y \wedge y \leqslant x \Rightarrow x = y)$,
(г) **PA** $\vdash \forall x \forall y \forall z (x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z)$,
(д) **PA** $\vdash \forall x (x \leqslant 0 \Rightarrow x = 0)$,
(ђ) **PA** $\vdash \forall x \forall y (x \leqslant S(y) \Rightarrow x \leqslant y \vee x = s(y))$,
(е) **PA** $\vdash \forall x \forall y (x \leqslant y \vee y)$,
(ж) **PA** $\vdash \exists x \alpha(x) \Rightarrow \exists x (\alpha(x) \wedge \forall y (y < x \Rightarrow \neg \alpha(y)))$, за сваку формулу α.

ЗАДАТАК **17.** На скупу $\mathcal{M} = \{0\} \times \mathcal{N} \cup \{1, 2\} \times \mathcal{Z}$ интерпретиран је језик аритметике $\{S, +, \cdot, 0\}$ на следећи начин:

$S^{\mathbf{M}}(i, n) = (i, n + 1)$, $i = 0, 1, 2$,

$(0, n) +^{\mathbf{M}} (i, m) = (i, m) +^{\mathbf{M}} (0, n) = (i, n + m)$, $i = 0, 1, 2$, и $(i, n) +^{\mathbf{M}} (j, m) = (i, n + m)$, $i = 1, 2$,

$(0, n) \cdot^{\mathbf{M}} (i, m) = (i, m) \cdot^{\mathbf{M}} (0, n) = (i, n \cdot m)$, $i = 0, 1, 2$, и $(i, n) \cdot^{\mathbf{M}} (j, m) = (i, n \cdot m)$, $i = 1, 2$, $0^{\mathbf{M}} = (0, 0)$.

Доказати да у моделу **M** важе све аксиоме Пеанове аритметике, осим аксиоме индукције **PA8**. Такође, доказати:

- **M** $\not\models \forall x \forall y (x + y = y + x)$;

• $\mathbf{PA} - \mathbf{PA8} \nvdash \forall x(\neg x' = x)$, при чему је $\mathbf{PA} - \mathbf{PA8}$ теорија коју чини седам аксиома Пеанове аритметике без аксиоме индукције.

Хинтикин скуп

Подсећамо да сваки скуп атомичних реченица има модел. Ову чињеницу можемо уопштити.

Хинтикин скуп је теорија T која има следеће особине:

(А) за сваку атомичну реченицу α, ако $\alpha \in T$, онда $\neg\alpha \notin T$;

(J1) за сваки затворен терм t, једнакост $t = t$ припада T;

(J2) ако је $\varphi(x)$ атомична формула, а u и v затворени терми такви да $u = v \in T$, онда: $\varphi(u) \in T$ акко $\varphi(v) \in T$;

(НН) ако $\neg\neg\varphi \in T$, онда $\varphi \in T$;

(К) ако $\theta_1 \wedge \theta_2 \in T$, онда $\theta_1, \theta_2 \in T$; ако $\neg(\theta_1 \wedge \theta_2) \in T$, онда $\neg\theta_1 \in T$ или $\neg\theta_2 \in T$;

(Д) ако $\theta_1 \vee \theta_2 \in T$, онда $\theta_1 \in T$ или $\theta_2 \in T$; ако $\neg(\theta_1 \vee \theta_2) \in T$, онда $\neg\theta_1 \in T$ и $\neg\theta_2 \in T$;

(У) ако $\forall x\theta \in T$, онда $\theta(x/t) \in T$, за сваки затворени терм t; ако $\neg\forall x\theta \in T$, онда $\neg\theta(x/t) \in T$, за неки затворени терм t;

(Е) ако $\exists x\theta \in T$, онда $\theta(x/t) \in T$, за неки затворени терм t; ако $\neg\exists x\theta \in T$, онда $\neg\theta(x/t) \in T$, за сваки затворени терм t.

Теорема 4. *Хинтикин скуп T има модел $\mathbb{C}$ у коме је сваки елемент облика $t^{\mathbb{C}}$, за неки затворени терм t. Другим речима, канонски модел атомичких реченица из T јесте модел за T.*

Доказ. Нека је T_{at} скуп свих атомских реченица из T, $T_{\mathrm{at}} \subseteq T$. Ослањајући се на услове (J1) и (J2), конструишемо канонски модел $\mathbb{C}$ скупа T_{at}. Доказаћемо да за сваку реченицу σ важи:

$$(1)\ \text{ако } \sigma \in T, \text{ онда } \mathbb{C} \models \sigma;$$
$$(2)\ \text{ако } \neg\sigma \in T, \text{ онда } \mathbb{C} \models \neg\sigma.$$

Приметимо најпре да тврђење (1) важи за сваку атомску реченицу σ, што је директна последица већ доказане чињенице да за сваку атомску реченицу σ важи еквиваленција

$$(*) \qquad \sigma \in T \ \text{ акко } \ \mathbb{C} \models \sigma.$$

Доказ тврђења (2) такође је једноставан: претпоставимо да за атомску реченицу σ важи $\neg\sigma \in T$; тада према (А) важи $\sigma \notin T$, што значи да $\mathbb{C} \not\models \sigma$, тј. $\mathbb{C} \models \neg\sigma$.

Нека је σ облика $\neg\theta$. (1) Ако $\sigma \in T$, тј. $\neg\theta \in T$, онда према индуктивној претпоставци за формулу θ важи (2), што значи да $\mathbb{C} \models \neg\theta$, тј. $\mathbb{C} \models \sigma$. (2) Ако $\neg\sigma \in T$, тј. $\neg\neg\theta \in T$, онда због

(НН) важи $\theta \in T$, па према индуктивној претпоставци за формулу θ важи (1), што значи да $\mathbb{C} \models \theta$, тј. $\mathbb{C} \models \neg\sigma$.

Нека је σ облика $\theta_1 \wedge \theta_2$. (1) Ако $\sigma \in T$, тј. $\theta_1 \wedge \theta_2 \in T$, према првом делу тврђења (К) важи $\theta_1, \theta_2 \in T$, па према индуктивној претпоставцу добијамо $\mathbb{C} \models \theta_1$ и $\mathbb{C} \models \theta_2$, тј. $\mathbb{C} \models \theta_1 \wedge \theta_2$. (2) Ако $\neg\sigma \in T$, тј. $\neg(\theta_1 \wedge \theta_2) \in T$, према другом делу тврђења (К) важи $\neg\theta_1 \in T$ или $\neg\theta_2 \in T$, па према индуктивној претпоставцу добијамо $\mathbb{C} \models \neg\theta_1$ или $\mathbb{C} \models \neg\theta_2$, тј. $\mathbb{C} \models \neg\theta_1 \vee \neg\theta_2$, па $\mathbb{C} \models \neg(\theta_1 \wedge \theta_2)$.

Нека је σ облика $\forall x\theta$. (1) Ако $\sigma \in T$, тј. $\forall x\theta \in T$, према првом делу тврђења (У), за сваки затворени терм t важи $\theta[x/t] \in T$, а према индуктивној претпоставци $\mathbb{C} \models \theta[x/t]$; како је сваки елемент структуре $\mathbb{C}$ облика $t^{\mathbb{C}}$ за неки затворени терм t, следи да $\mathbb{C} \models \forall x\theta$. (2) Ако $\neg\sigma \in T$, тј. $\neg\forall x\theta \in T$, према другом делу тврђења (У), за постоји затворени терм t такав да важи $\neg\theta[x/t] \in T$, а према индуктивној претпоставци $\mathbb{C} \models \neg\theta[x/t]$; како је сваки елемент структуре $\mathbb{C}$ облика $t^{\mathbb{C}}$ за неки затворени терм t, следи да $\mathbb{C} \models \neg\forall x\theta$.

Аналогно се доказују остали случајеви. □

Теорема 5. *Ако је T теорија таква да:*

- *($H1$) сваки коначан подскуп од T има модел;*
- *($H2$) за сваку реченицу σ важи $\sigma \in T$ или $\neg\sigma \in T$, и не важе оба;*
- *($H3$) за сваку реченицу $\exists x\varphi$ из T постоји затворени терм t такав да $\varphi(x/t) \in T$.*

онда је T Хинтикин скуп.

Доказ. Приметимо најпре да важи:
($\star$) Ако је U коначан подскуп од T и θ реченица таква да $U \models \theta$, онда $\theta \in T$.

Доказ за ($\star$): Претпоставимо да постоји коначан подскуп U од T и реченица θ таква да $U \models \theta$ и $\theta \notin T$. Из $\theta \notin T$, према ($H2$), следи $\neg\theta \in T$; према ($H1$), скуп $U \cup \{\neg\theta\}$, као коначан подскуп од T, има модел, што није могуће, јер $U \models \theta$.

Докажимо да T задовољава све Хинтикине услове.

(А) За сваку атомичну реченицу α, ако $\alpha \in T$, онда $\neg\alpha \notin T$.

Услов (А) директно следи из ($H1$).

(Ј1) За сваки затворен терм t, једнакост $t = t$ припада T.

Услов (Ј1) следи из ($\star$) и чињенице да $\models t = t$.

(Ј2) Ако је $\varphi(x)$ атомична формула, а u и v затворени терми такви да $u = v \in T$, онда: $\varphi(u) \in T$ акко $\varphi(v) \in T$.

Услов (J1) следи из ($\star$) и чињенице да $\varphi(x/t), t = v \models \varphi(x/v)$.

(НН) Ако $\neg\neg\varphi \in T$, онда $\varphi \in T$.

Услов (НН) следи из ($\star$) и чињенице да $\neg\neg\varphi \models \varphi$.

(К) Ако $\theta_1 \wedge \theta_2 \in T$, онда $\theta_1, \theta_2 \in T$; ако $\neg(\theta_1 \wedge \theta_2) \in T$, онда $\neg\theta_1 \in T$ или $\neg\theta_2 \in T$.

Прва половина тврђења (К) следи из ($\star$) и чињеница да $\theta_1 \wedge \theta_2 \models \theta_1$ и $\theta_1 \wedge \theta_2 \models \theta_2$. Докажимо другу половину тврђења (К). Нека $\neg(\theta_1 \wedge \theta_2) \in T$, и претпоставимо да $\neg\theta_1 \notin T$ и $\neg\theta_2 \notin T$. Тада, према ($H2$) следи $\theta_1 \in T$ и $\theta_2 \in T$, што није могуће према услову ($H1$), јер је $\{\neg(\theta_1 \wedge \theta_2), \theta_1, \theta_2\}$ коначан подскуп од T који нема модел.

(Д) ако $\theta_1 \vee \theta_2 \in T$, онда $\theta_1 \in T$ или $\theta_2 \in T$; ако $\neg(\theta_1 \vee \theta_2) \in T$, онда $\neg\theta_1 \in T$ и $\neg\theta_2 \in T$;

Доказ остављамо за вежбу.

(У) ако $\forall x\theta \in T$, онда $\theta(x/t) \in T$, за сваки затворени терм t; ако $\neg\forall x\theta \in T$, онда $\neg\theta(x/t) \in T$, за неки затворени терм t;

Доказ остављамо за вежбу.

(Е) ако $\exists x\theta \in T$, онда $\theta(x/t) \in T$, за неки затворени терм t; ако $\neg\exists x\theta \in T$, онда $\neg\theta(x/t) \in T$, за сваки затворени терм t.

Прва половина тврђења (Е) је претпостављена условом ($H3$). Докажимо другу половину тврђења (Е). Претпоставимо да $\neg\exists x\theta \in T$ и $\neg\theta(x/t) \notin T$, за неки затворени терм t. Према ($H2$), следи да $\theta(x/t) \notin T$, што није могуће према услову ($H1$), јер је $\{\neg\exists x\theta, \theta(x/t)\}$ коначан подскуп од T који нема модел. $\square$

Теорема компактности

Теорема 6. *Ако сваки коначан подскуп теорије T има модел, онда и T има модел.*

Доказ. Нека је T теорија чији сваки коначан подскуп има модел. Претпоставимо да је сигнатура $\mathcal{L}$ највише пребројива. Доказ се без већих потешкоћа може уопштити на све сигнатуре.

Сигнатуру $\mathcal{L}$ проширићемо пребројивим скупом нових симбола константи које ћемо називати *сведоцима*: $\mathcal{L}^* = \mathcal{L} \cup \{c_i \mid i \geqslant 0\}$. Показаћемо да се T може проширити до Хинтикиног скупа T^* сигнатуре $\mathcal{L}^*$. Дефинисаћемо растући низ теорија $T_0 \subseteq T_1 \subseteq T_2 \subseteq \cdots$ такав да важе следећи услови:

(i) сваки коначан подскуп од T_i има модел, за свако $i \geqslant 0$;

(ii) у реченицама скупа $T_i \setminus \bigcup_{j<i} T_j$ појављује се само коначно много сведока.

Поређајмо у низ све реченице сигнатуре $\mathcal{L}^*$: $\sigma_0, \sigma_1, \sigma_2, \ldots$.

Нека је $T_0 = T$. За $i \geqslant 0$,

$$T'_{i+1} = \begin{cases} T_i \cup \{\sigma_i\}, & \text{ако сваки коначан подскуп од } T_i \cup \{\sigma_i\} \text{ има модел;} \\ T_i, & \text{иначе.} \end{cases}$$

У случају да $\sigma_i \in T'_{i+1}$ и σ_i је облика $\exists x\theta$, бирамо најмањи индекс k такав да се c_k не појављује у T'_{i+1} и дефинишемо скуп $T_{i+1} = T'_{i+1} \cup \{\theta(x/c_k)\}$. Ако $\sigma_i \notin T'_{i+1}$ или σ_i није облика $\exists x\theta$, онда је $T_{i+1} = T'_{i+1}$. Овако дефинисан скуп T_{i+1} задовољава услове (i) и (ii). Услов (ii) је очигледно задовољен. Докажимо услов (i). Једини нетривијалан случај који треба размотрити односи се на ситуацију када $\sigma_i \in T'_{i+1}$ и σ_i је облика $\exists x\theta$. Довољно је да докажемо да за произвољан коначан подскуп $U \subseteq T'_{i+1} = T_i \cup \{\exists x\theta\}$, скуп $U \cup \{\theta(x/c_k)\}$ има модел (над $\mathcal{L}^*$). Изаберимо произвољан $\mathcal{L}^*$-модел скупа $U \cup \{\exists x\theta\}$:

$$\mathbb{A}^* = (\mathbb{A}, c_0^{\mathbb{A}^*}, c_1^{\mathbb{A}^*}, \ldots, c_k^{\mathbb{A}^*}, \ldots),$$

при чему је $\mathbb{A}$ одговарајућа $\mathcal{L}$-структура. Тада постоји $a \in A$ такав да $\mathbb{A}^* \models \theta[a]$. Очигледно је да важи:

$$(\mathbb{A}, c_0^{\mathbb{A}^*}, c_1^{\mathbb{A}^*}, \ldots, a, \ldots) \models U \cup \{\exists x\theta\} \cup \{\theta(x/c_k)\}.$$

Нека је $T^* = \bigcup_{i \geqslant 0} T_i$. Доказаћемо да је T^* Хинтикин скуп, тј. задовољава услове $(H1)$, $(H2)$ и $(H3)$ претходне теореме.

(H1) Сваки коначан подскуп од T^* има модел.

За сваки коначан подскуп U од T^*, постоји m такав да је $U \subseteq T_m$, одакле према дефиницији низа (T_n) следи да U има модел.

(Н2) За сваку $\mathcal{L}^*$-реченицу σ важи $\sigma \in T^*$ или $\neg\sigma \in T^*$, и не важе оба.

Претпоставимо да постоји $\mathcal{L}^*$-реченица σ таква да $\sigma \notin T$ и $\neg\sigma \notin T$. Реченице σ и $\neg\sigma$ појављују се у низу свих $\mathcal{L}^*$-реченица; нека су i и j одговарајући индекси, тј. σ_i и σ_j су редом формуле σ и $\neg\sigma$. Према дефиницији низа (T_n), постоје коначни подскупови U_i и U_j редом од T_i и T_j такви да скупову $U_i \cup \{\sigma_i\} = U_i \cup \{\sigma\}$ и $U_j \cup \{\sigma_j\} = U_i \cup \{\neg\sigma\}$ немају моделе. Скуп $U_i \cup U_j$ је коначан подскуп од T^* и као такав мора имати модел; означимо тај модел $\mathbb{A}$. Свакако мора бити $\mathbb{A} \models \sigma$ или $\mathbb{A} \not\models \sigma$, што значи да је $\mathbb{A}$ модел скупа $U_i \cup \{\sigma_i\}$ и $U_j \cup \{\sigma_j\}$, што је супротно избору скупова U_i и U_j.

(Н3) За сваку реченицу $\exists x\varphi$ из T^* постоји затворени терм t такав да $\varphi(x/t) \in T^*$.

Из $\exists x\varphi \in T^*$ следи да постоји m такав да $\exists x\varphi \in T_m$ и да T_{m+1}, а самим тим и T^* садржи $\varphi(x/c_k)$, за неког сведока c_k. □

Последица 5. *Ако $T \models \sigma$, онда постоји коначан подскуп $U \subseteq T$ такав да $U \models \sigma$.*

ПРИМЕР 26. Ако нека теорија T има моделе произвољно велике коначне кардиналности, доказаћемо да тада мора имати и бесконачан модел.
I начин:
Претпоставимо, дакле, да је T теорија таква да за свако n постоји модел теорије T чији домен има бар n елемената. Ако је m позитиван природан број, означимо са γ_m реченицу $\exists x_1 \cdots \exists x_m \bigwedge_{1 \leqslant i < j \leqslant m} x_i \neq x_j$. Није тешко уочити да реченица γ_m важи у неком моделу акко домен тог модела има бар m елемената. Нека је

$$T^* = T \cup \{\gamma_m \mid m \geqslant 1\}.$$

Доказаћемо да теорија T^* има модел, тако што ћемо показати да сваки њен коначан подскуп има модел. Нека је T_0 коначан подскуп од T^*. Тада постоји природан број n такав да је $T_0 \subseteq T_0' = T \cup \{\gamma_1, \ldots, \gamma_n\}$. Теорија T_0' има модел по претпоставци. Ако је $\mathbf{M}$ било који модел теорије T који има најмање n елемената, онда $\mathbf{M} \models \gamma_i$, $1 \leqslant i \leqslant n$, па $\mathbf{M} \models T_0'$, а самим тим и $\mathbf{M} \models T_0$. Према теореми компактности и T^* има модел; означимо га са $\mathbf{M}^*$. Домен овог модела M^* мора бити бесконачан, јер ако би био коначан, онда би било $|M^*| = n$, за неко $n \geqslant 1$, па не би важило $\mathbf{M}^* \models \gamma_{n+1}$.
II начин:
Нека је $L^* = L \cup \{c_n \mid n \in \mathbb{N}\}$ и $T^* = T \cup \{c_i \neq c_j \mid i \neq j\}$. Слично претходном, доказује се да T^* има модел, што ће бити бесконачан модел теорије T.

ЗАДАТАК **18.** Свако уређење се може проширити до линеарног уређења. Прецизније, ако је $(P, \leqslant)$ уређење, онда постоји линеарно уређење $\preceq$ на P које проширује $\leqslant$, тј. за све $x, y \in P$, из $x \leqslant y$ следи $x \preceq y$.

Тврђење се једноставно доказује када је P коначан скуп (индукцијом по броју елемената).

Нека је $L = \{\preceq\} \cup \{c_a \mid a \in P\}$ и $T = T_{\text{LO}} \cup \{c_a \neq c_b \mid a \neq b\} \cup \{c_a \preceq c_b \mid a \leqslant b\}$. Доказати да T има модел.

Теорема компактности свакако је један од најзначајнијих резултата који има бројне примене. Наводимо неколико примена које представљају полазиште неких важних области математичке логике, али и математике уопште.

Примене теореме компактности - (не)аксиоматске класе

Нека је L произвољна сигнатура. Нека је $\mathfrak{M}_L$ класа свих L-структура. Ако је T било која теорија сигнатуре L, класу свих модела теорије T означавамо $\mathfrak{mod}(T)$. Нпр. $\mathfrak{mod}(T_{\text{GR}})$ јесте класа свих група. Приметимо да је $\mathfrak{mod}(T) \subseteq \mathfrak{M}_L$.

– Приметимо да $\mathfrak{mod}(T_{\text{GR}})$ није скуп. За сваки скуп група $\mathcal{G}$, постоји група $\mathbf{G}$ таква да $\mathbf{G} \notin \mathcal{G}$.

Ако је $\mathcal{K}$ нека класа L-структура и $\text{Th}(\mathcal{K})$ скуп реченица које су тачне у свим моделима из $\mathcal{K}$, онда је $\mathcal{K} \subseteq \mathfrak{mod}(\text{Th}(\mathcal{K}))$. Обрнуто не мора да важи.

Дефиниција 14. *Класа L-структура $\mathcal{K}$ је аксиоматска ако постоји L-теорија T таква да је $\mathcal{K} = \mathfrak{mod}(T)$. Класа $\mathcal{K}$ је коначно аксиоматска ако постоји коначан скуп L-реченица T такв да је $\mathcal{K} = \mathfrak{mod}(T)$.*

Лема 15. *$\mathcal{K}$ је аксиоматска класа акко је $\mathcal{K} = \mathfrak{mod}(\text{Th}(\mathcal{K}))$.*

Пример 27. Нека је $\mathcal{K}$ класа свих коначних група:

$$\mathbf{G} \in \mathcal{K} \text{ акко } \mathbf{G} \text{ је коначна група.}$$

Претпоставимо да је $\mathcal{K}$ аксиоматска класа, тј. да постоји L_{GR}-теорија T таква да је $\mathcal{K} = \mathfrak{mod}(T)$. Нека је γ_m реченица $\exists x_1 \cdots \exists x_m \bigwedge_{1 \leqslant i < j \leqslant m} x_i \neq x_j$, $m \geqslant 1$ и $T^* = T \cup \{\gamma_m \mid m \geqslant 1\}$.

Уочимо било који коначан подскуп $T_0 \subseteq T^*$. Доказаћемо да T_0 има модел. Очигледно је да постоје природни бројеви $n_1, \ldots, n_k$ такви да је

$$T_0 \subseteq T \cup \{\gamma_{m_1}, \ldots, \gamma_{m_k}\}.$$

Ако је $n = \max\{m_1, \ldots, m_k\} + 1$, онда

$$\mathbf{Z}_n = (\mathbb{Z}_n, +_n, -_n, 0) \models T \cup \{\gamma_{m_1}, \ldots, \gamma_{m_k}\}.$$

Заиста, $\mathbf{Z}_n \models T$, јер је $\mathbf{Z}_n$ коначна група, и $\mathbf{Z}_n \models \gamma_{m_i}$, јер је $n > m_i$, $i = 1, \ldots, k$. Према теореми компактности, T^* има модел, тј. постоји

L_{GR}-структура $\mathbf{G}$ која је модел за T^*. Из $\mathbf{G} \models T$ следи да $\mathbf{G} \in \mathcal{K}$, тј. $\mathbf{G}$ је коначна група; из $\mathbf{G} \models \gamma_m$, за све $m \geqslant 1$, следи да је G бесконачна структура. Контрадикција.

Тврђење доказано у претходном примеру може се уопштити.

Теорема 7. *Ако нека аксиоматска класа садржи структуре произвољно велике коначне кардиналности, онда она садржи и бесконачну структуру.*

Последица 6. *Нека је L произвољна сигнатура.*
1) Класа свих коначних L-структура није аксиоматска.
2) Класа свих бесконачних L-структура није коначно аксиоматска. Приметимо да је класа свих бесконачних L-структура аксиоматска (одређује је скуп $\{\gamma_m \mid m \geqslant 1\}$).
3) Ако нека класа L-структура садржи само коначне моделе, она је аксиоматска само ако постоји горње ограничење кардиналности структура које садржи.

Примене теореме компактности - нестандардни модели аритметике и инфинитезималног рачуна

За сваку L структуру $\mathbf{M}$ очигледно важи $\mathbf{M} \in \mathfrak{mod}(\mathrm{Th}(\mathbf{M}))$. Да у општем случају $\mathfrak{mod}(\mathrm{Th}(\mathbf{M}))$ може да садржи и разне друге моделе, неизоморфне са $\mathbf{M}$, показују наредни важни примери.

Пример 28. Размотримо могућности које нам пружа логика првог реда при описивању једне од најважнијих структура математике – структуре $\mathbf{N} = (\mathbb{N}, \leqslant, s, +, \cdot, 0)$. Означимо са $\mathrm{Th}(\mathbf{N})$ скуп свих реченица одговарајућег језика $\mathcal{L}_{\mathrm{A}} = \{\leqslant, s, +, \cdot, 0\}$ које су истините у моделу $\mathbf{N}$. Теорија $\mathrm{Th}(\mathbf{N})$ се назива *комплетна аритметика*. Јасно, $\mathbf{N}$ је модел теорије $\mathrm{Th}(\mathbf{N})$ и назива се *стандардни модел аритметике*. Постоји ли још нека (нестандардна) структура језика $\mathcal{L}_{\mathrm{A}}$ која је модел за $\mathrm{Th}(\mathbf{N})$, али није изоморфна са $\mathbf{N}$. Одговор је потврдан.

$\mathrm{Rel}_{\mathcal{L}_{\mathrm{A}}} = \{\leqslant\}$, $\mathrm{Fun}_{\mathcal{L}_{\mathrm{A}}} = \{s, +, \cdot\}$, $\mathrm{ar}(s) = 1$, $\mathrm{ar}(\leqslant) = \mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$, $\mathrm{Const}_{\mathcal{L}_{\mathrm{A}}} = \{0\}$

Теорема. Постоји нестандардни модел комплетне аритметике.

Доказ. Проширимо језик $\mathcal{L}_{\mathrm{A}}$ новим симболом константе c. За $n \geqslant 1$, означимо са $\overline{n}$ терм $\underbrace{s(s(\cdots s}_{n \text{ пута}}(0)\cdots))$. Дакле, $\overline{1} = s(0)$, $\overline{2} = s(s(0))$, $\overline{3} = s(s(s(0)))$, итд. У складу са овим, симбол константе 0 означаваћемо и са $\overline{0}$. Нека је за сваки природан број n, $\overline{n} < c$ скраћење за формулу $\overline{n} \leqslant c \wedge \neg\, \overline{n} = c$. Посматрајмо теорију

Наведени терми се називају *нумерали*.

$$T = \mathrm{Th}(\mathbf{N}) \cup \{\overline{0} < c, \overline{1} < c, \overline{2} < c, \ldots, \overline{n} < c, \ldots\}$$

језика $\mathcal{L}_{\mathrm{A}} \cup \{c\}$.

Нека је T_0 произвољан коначан подскуп од T. Скуп T_0 садржи само коначно много реченица облика $\overline{n} < c$, $n \in \mathbb{N}$; нека су то: $\overline{n_1} < c$, $\overline{n_2} < c$, …, $\overline{n_k} < c$, за неке природне бројеве $n_1, n_2, \ldots, n_k$. Тада је очигледно

$$T_0 \subset \mathrm{Th}(\mathbf{N}) \cup \{\overline{n_1} < c, \overline{n_2} < c, \ldots, \overline{n_k} < c\}.$$

Нека је m било који природан број већи од свих $n_1, n_2, \ldots, n_k$; на пример, $m = \max\{n_1, n_2, \ldots, n_k\} + 1$. Тада је

$$\mathbf{N}^* = (\mathbb{N}, \leqslant, s, +, \cdot, 0, m) \models \mathrm{Th}(\mathbf{N}) \cup \{\overline{n_1} < c,\, \overline{n_2} < c,\, \ldots,\, \overline{n_k} < c\},$$

при чему је $c^{\mathbf{N}^*} = m$, па је и $\mathbf{N}^* \models T_0$.

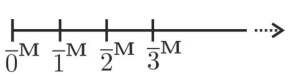
Дакле, сваки коначан подскуп од T има модел, па према ставу компактности и T има модел. Нека је $(M, \preccurlyeq, s^{\mathbf{M}}, \oplus, \odot, \mathbf{0}, m)$ модел теорије T. Добијена структура $\mathbf{M} = (M, \preccurlyeq, s^{\mathbf{M}}, \oplus, \odot, \mathbf{0})$ није изоморфна са $\mathbf{N}$. Претпоставимо супротно, да постоји бијекција $f : N \overset{1-1}{\underset{\text{na}}{\rightarrow}} M$, таква да за све $x, y \in \mathbb{N}$ важи: $x \leqslant y$ акко $f(x) \preccurlyeq f(y)$, $f(s(x)) = s^{\mathbf{M}}(f(x))$, $f(x+y) = f(x) \oplus f(y)$, $f(x \cdot y) = f(x) \odot f(y)$ и $f(0) = \mathbf{0}$. Индукцијом се једноставно показује да за свако $n \in \mathbb{N}$ важи $f(n) = \overline{n}^{\mathbf{M}}$. Пошто је f на функција, мора постојати $n_0 \in \mathbb{N}$ такав да је $f(n_0) = m$. Како је f и 1-1 функција, следи да је $m = \overline{n_0}^{\mathbf{M}}$. Међутим, то није могуће јер $(M, \preccurlyeq, s^{\mathbf{M}}, \oplus, \odot, \mathbf{0}, m) \models \overline{n_0} < c$. Дакле, $\mathbf{M} = (M, \preccurlyeq, s^{\mathbf{M}}, \oplus, \odot, \mathbf{0})$ је **нестандардни модел аритметике**, по много чему различит од стандардног модела, у шта се уверавамо ако покушамо да замислимо како ова структура „изгледа“.

Пођимо од следећих реченица које важе у стандардном моделу $\mathbf{N}$.

$$\forall x(\overline{0} = x \vee \overline{0} < x)$$

$$\overline{0} < \overline{1} \wedge \forall x(\overline{0} < x \Rightarrow (\overline{1} = x \vee \overline{1} < x))$$
$$\overline{1} < \overline{2} \wedge \forall x(\overline{1} < x \Rightarrow (\overline{2} = x \vee \overline{2} < x))$$
$$\overline{2} < \overline{3} \wedge \forall x(\overline{2} < x \Rightarrow (\overline{2} = x \vee \overline{3} < x))$$
$$\vdots$$

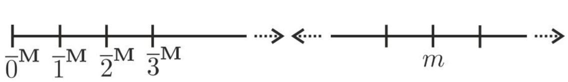
Оне кажу да је 0 најмањи елемент, затим да је 1 следећи најмањи после 0, па да је 2 следећи најмањи после 1, и тако даље. Како су ове реченице истините у стандардном моделу $\mathbf{N}$, па тиме и у нестандардном моделу $\mathbf{M}$, почетни сегмент од $\mathbf{M}$ изгледа овако:



Међутим, скуп M садржи и елемент m који се налази „иза“ (у смислу уређења $\preccurlyeq$) свих елемената $\overline{0}^{\mathbf{M}}$, $\overline{1}^{\mathbf{M}}$, $\overline{2}^{\mathbf{M}}$, … Како стандардни модел $\mathbf{N}$ задовољава реченицу

$$\forall x(\exists y(S(x) = y) \wedge (\neg x = 0 \Rightarrow \exists z(S(z) = x))),$$

која каже да сваки елемент има непосредног следбеника и сваки елемент различит од нуле непосредног претходника, скуп M поред елемента m садржи још бесконачно много нових елемената који су заједно са m поређани уређењем $\preccurlyeq$ као цели бројеви:



Ако узмемо у обзир елемент $m \oplus m$ добијамо нове елементе из M:

тј. нову копију целих бројева. Није тешко показати да се између сваке две копије уређења целих бројева $(\mathbb{Z}, \leqslant)$ у $\mathbf{M}$ налази нова таква копија.

Приметимо и да $\preccurlyeq$ није добро уређење скупа M. Читаоцима препуштамо да покажу да, на пример, непразан скуп $M_0 = M \setminus \{\overline{n}^{\mathbf{M}} \mid n \in \mathbb{N}\}$ нема најмањи елемент.

Међутим, и поред свих уочених разлика, не заборавимо да $\mathbf{M} \models \mathrm{Th}(\mathbf{N})$. Ово заправо значи да $\mathbf{M} = (M, \preccurlyeq, s^{\mathbf{M}}, \oplus, \odot, \mathbf{0})$ задовољава све реченице језика $\mathcal{L}_{\mathrm{A}}$ које задовољава и стандардни модел. Није тешко уочити да мора важити и обрнуто: ако је нека реченица језика $\mathcal{L}_{\mathrm{A}}$ тачна у $\mathbf{M}$, она мора бити тачна и у $\mathbf{N}$. Другим речима, реченицама језика $\mathcal{L}_{\mathrm{A}}$ не можемо разликовати стандардни и добијени нестандардни модел комплетне аритметике.

Као што се може наслутити, овај пример не представља само једну обичну примену теореме компактности, већ отвара читаву област истраживања на којима се нећемо задржавати.

Пример 29. Поред структуре природних бројева, о којој смо говорили у претходном примеру, важно место у математици заузима и уређено поље реалних бројева $\mathbf{R} = (\mathbb{R}, \leqslant, +, \cdot, -, 0, 1)$.

Применом теореме компактности доказаћемо да постоји уређено поље које задовољава исте реченице језика $\mathcal{L}_{\mathrm{FO}}$ које важе у $\mathbf{R}$, али се у одређеном смислу и битно разликује од уређеног поља реалних бројева.

Проширимо језик $\mathcal{L}_{\mathrm{FO}}$ новим симболом константе c. Нека је

$$T = \mathrm{Th}(\mathbf{R}) \cup \{0 < c, 1 < c, 1+1 < c, 1+1+1 < c, \ldots, \underbrace{1+1+\cdots+1}_{n} < c, \ldots\}$$

теорија у проширеном језику. Ако је T_0 произвољан коначан подскуп од T, тада се у T_0 налази само коначно много реченица облика $\underbrace{1+1+\cdots+1}_{n} < c$, $n \in \mathbb{N}$; нека су то реченице:

$$\underbrace{1+1+\cdots+1}_{n_1} < c,\ \underbrace{1+1+\cdots+1}_{n_2} < c, \ldots,\ \underbrace{1+1+\cdots+1}_{n_k} < c$$

за неке природне бројеве $n_1, n_2, \ldots, n_k$. Изаберимо било који реалан број r већи од свих $n_1, n_2, \ldots, n_k$; на пример, нека је $r = \max\{n_1, n_2, \ldots, n_k\} + 1$. Није тешто видети да је структура $\mathbf{R}^* = (\mathbb{R}, \leqslant, +, -, \cdot, 0, 1, r)$, при чему је $c^{\mathbf{R}^*} = r$, један модел скупа реченица T_0. Према теореми компактности теорија T има модел. Нека је структура $\mathbf{F} = (F, \preccurlyeq, \oplus, \odot, \ominus, \mathbf{0}, \mathbf{1}, K)$ модел теорије T, при чему је $c^{\mathbf{F}} = K$. Како је $\mathbf{F} \models \mathrm{Th}(\mathbf{R})$, закључујемо да је $(F, \preccurlyeq, \oplus, \odot, \ominus, \mathbf{0}, \mathbf{1})$ једно уређено поље (будући да је $T_{\mathrm{FO}} \subset \mathrm{Th}(\mathbf{R})$). Такође,

$$\mathbf{F} \models \{0 < c, 1 < c, 1+1 < c, 1+1+1 < c, \ldots, \underbrace{1+1+\cdots+1}_{n} < c, \ldots\},$$

одакле следи да је K елемент домена F који задовољава неједнакости

$$\mathbf{0} \prec K, \mathbf{1} \prec K, \ldots, \underbrace{\mathbf{1} \oplus \mathbf{1} \oplus \cdots \oplus \mathbf{1}}_{n} \prec K, \ldots$$

Самим тим, добијено уређено поље није *архимедско*, за разлику од уређеног поља реалних бројева. Уређено поље $\mathbf{F} = (F, \leqslant^{\mathbf{F}}, +^{\mathbf{F}}, \cdot^{\mathbf{F}}, -^{\mathbf{F}}, 0^{\mathbf{F}}, 1^{\mathbf{F}})$ је архимедско ако за сваки елемент $x \in F$, постоји природан број n такав да је $x \leqslant^{\mathbf{F}} \underbrace{1^{\mathbf{F}} +^{\mathbf{F}} \cdots +^{\mathbf{F}} 1^{\mathbf{F}}}_{n}$.

Постојање неархимедских уређених поља приближава нас идејама тзв. *нестандардне анализе*, која је развијена 60-тих година прошлог века и која је нашла бројне примене у другим областима математике (теорији вероватноће, економији, математичкој физици, бесконачној комбинаторици итд.).

Елементарна еквивалентност. Елементарна утапања

Подсећамо да је $\mathrm{Th}(\mathbf{A}) = \{\sigma \in \mathsf{Sent}_L \mid \mathbf{A} \models \sigma\}$.

Дефиниција 15. *Две L-структуре $\mathbf{A}$ и $\mathbf{B}$ су елементарно еквивалентне, у ознаци $\mathbf{A} \equiv \mathbf{B}$ ако је $\mathrm{Th}(\mathbf{A}) = \mathrm{Th}(\mathbf{B})$.*

Елементарна еквивалентност је релација еквиваленције класе свих L-структура:

- $\mathbf{A} \equiv \mathbf{A}$,
- ако је $\mathbf{A} \equiv \mathbf{B}$, онда је $\mathbf{B} \equiv \mathbf{A}$,
- ако је $\mathbf{A} \equiv \mathbf{B}$ и $\mathbf{B} \equiv \mathbf{C}$, онда је $\mathbf{A} \equiv \mathbf{C}$.

Лема 16. $\mathbf{A} \equiv \mathbf{B}$ *акко* $\mathbf{A} \models \mathrm{Th}(\mathbf{B})$ *акко* $\mathbf{B} \models \mathrm{Th}(\mathbf{A})$.

Лема 17. *Из* $\mathbf{A} \cong \mathbf{B}$ *следи* $\mathbf{A} \equiv \mathbf{B}$.

Доказ. Ако је $f : \mathbf{A} \cong \mathbf{B}$, онда за сваку формулу $\varphi(\overline{x})$ и све $\overline{a}$ из A важи: $\mathbf{A} \models \varphi[\overline{a}]$ акко $\mathbf{B} \models \varphi[f\overline{a}]$. □

Обрат претходне леме је тачан само за коначне L-структуре.

Лема 18. *Ако је* $\mathbf{A}$ *коначна структура и* $\mathbf{A} \equiv \mathbf{B}$, *онда је* $\mathbf{A} \cong \mathbf{B}$.

Скица доказа. Нека је $\mathbf{A}$ коначна структура. Из чињенице да је структура $\mathbf{A}$ коначна, следи и да $\mathbf{B}$ мора бити коначна; штавише, $|A| = |B|$. Ако елементе скупа A поређамо у низ $a_1, \ldots, a_n$, при чему је $|A| = n$, једноставно се генерише низ различитих елемената скупа B на основу следећих својстава:

- постоји $b_1 \in B$, тако да $(\mathbf{A}, a_1) \equiv (\mathbf{B}, b_1)$;
- постоји $b_2 \in B$, тако да $(\mathbf{A}, a_1, a_2) \equiv (\mathbf{B}, b_1, b_2)$;
- $\vdots$

- постоји $b_n \in B$, тако да $(\mathbf{A}, a_1, a_2, \ldots, a_n) \equiv (\mathbf{B}, b_1, b_2, \ldots, b_n)$.

Бијекција $a_i \mapsto b_i$, $i = \overline{1,n}$, је тражени изоморфизам. □

Пример 30. Кључне идеје доказа претходне леме ислутроваћемо једним једноставним примером. Нека је $L = \{R\}$, где је R бинарни релацијски симбол, и $\mathbf{A} = (\{0,1\}, R^{\mathbf{A}})$, где је $R^{\mathbf{A}} = \{(0,1),(1,1)\}$. Претпоставимо да је $\mathbf{A} \equiv \mathbf{B}$. Као и раније, γ_m означава реченицу $\exists x_1 \cdots \exists x_m \bigwedge_{1 \leqslant i < j \leqslant m} x_i \neq x_j$. Из $\mathbf{A} \models \gamma_2 \wedge \neg\gamma_3$, следи да $\mathbf{B} \models \gamma_2 \wedge \neg\gamma_3$, што значи да скуп B има тачно два елемента.

Посматрајмо конјункцију свих литерала над $L_A = \{R, \underline{0}, \underline{1}\}$ које су тачни у $(\mathbf{A}, 0, 1)$:

$$\underline{0} = \underline{0} \wedge \neg\underline{0} = \underline{1} \wedge \neg\underline{1} = \underline{0} \wedge \underline{1} = \underline{1} \wedge \neg R(\underline{0},\underline{0}) \wedge R(\underline{0},\underline{1}) \wedge \neg R(\underline{b},\underline{0}) \wedge R(\underline{1},\underline{1}).$$

Нека је σ реченица: $\exists x \exists y(\neg x = y \wedge \neg R(x,x) \wedge R(x,y) \wedge \neg R(y,x) \wedge R(y,y))$. Очигледно $\mathbf{A} \models \sigma$, одакле следи $\mathbf{B} \models \sigma$, што значи да скуп B садржи два различита елемента a, b и да је $R^{\mathbf{B}} = \{(a,b),(b,b)\}$.

У општем случају, обрат претходне леме није тачан: за сваку бесконачну структуру постоји јако пуно структура које су јој елементарно еквивалентне али не и изоморфне. Да бисмо дубље разматрали ова питања уводимо појам елементарног утапања.

Дефиниција 16. *Нека су* $\mathbf{A}$ *и* $\mathbf{B}$ *две* L*-структуре. Функција* $f : A \to B$ *је елементарно утапање, у ознаци* $f : \mathbf{A} \prec \mathbf{B}$, *ако за сваку формулу* $\varphi(\overline{x})$ *и све* $\overline{a}$ *из* A *важи:* $\mathbf{A} \models \varphi[\overline{a}]$ *акко* $\mathbf{B} \models \varphi[f\overline{a}]$.

Јасно, сваки изоморфизам је елементарно утапање, а свако елементарно утапање је утапање (пресликавање које чува литерале).

Подсећамо да је $\mathbf{A} \subseteq \mathbf{B}$ ($\mathbf{A}$ је подструктура од $\mathbf{B}$), ако је инклузионо пресликавање $i : A \to B$, $i(x) = x$, $x \in A$, утапање.

Дефиниција 17. *Нека је* $\mathbf{A} \subseteq \mathbf{B}$. *Структура* $\mathbf{A}$ *је елементарни подмодел од* $\mathbf{B}$, *у ознаци* $\mathbf{A} \prec \mathbf{B}$, *ако је инклузионо пресликавање* $i : A \to B$, $i(x) = x$, $x \in A$, *елементарно утапање.*

Дакле, $\mathbf{A} \prec \mathbf{B}$ акко за сваку формулу $\varphi(\overline{x})$ и све $\overline{a}$ из A важи:

$$(*) \qquad \mathbf{A} \models \varphi[\overline{a}] \text{ акко } \mathbf{B} \models \varphi[\overline{a}].$$

Специјално, из $\mathbf{A} \prec \mathbf{B}$ следи $\mathbf{A} \equiv \mathbf{B}$.

Пример 31. Нека је $\mathbf{A} = (\{1,2,3,\ldots\}, s)$ и $\mathbf{B} = (\{0,1,2,3,\ldots\}, s)$. Инклузионо пресликавање $i(x) = x$, $x \geqslant 1$, јесте утапање, па је $\mathbf{A} \subseteq \mathbf{B}$, али није елементарно утапање. Нпр. ако је $\varphi(x)$ формула $\neg\exists y(s(y) = x)$, онда $\mathbf{A} \models \varphi[1]$ и $\mathbf{B} \not\models \varphi[1]$. Приметимо да је $\mathbf{A} \cong \mathbf{B}$, и да је $x \mapsto x+1$ изоморфизам.

Теорема 8. [*Тарски-Вот критеријум*] *Нека је* $\mathbf{A} \subseteq \mathbf{B}$. *Ако за сваку формулу* $\theta(\overline{x}, y)$ *и све* $\overline{a}$ *из* A *важи:*

$$\text{из } \mathbf{B} \models \exists y\theta[\overline{a}] \text{ следи } \mathbf{A} \models \exists y\theta[\overline{a}],$$

онда $\mathbf{A} \prec \mathbf{B}$.

Доказ. Треба доказати $(*)$ за сваку формулу $\varphi(\overline{x})$ и све $\overline{a}$ из A: $\mathbf{A} \models \varphi[\overline{a}]$ акко $\mathbf{B} \models \varphi[\overline{a}]$. Доказ изводимо индукцијом по сложености формуле φ.

Ако је φ атомска формула, онда тврђење $(*)$ важи јер је $\mathbf{A} \subseteq \mathbf{B}$.

Размотримо само случај када је $\varphi(\overline{x})$ облика $\exists y\theta(\overline{x}, y)$. Нека је $\overline{a}$ из A. Ако $\mathbf{A} \models \exists y\theta[\overline{a}]$, онда постоји $b \in A$ такво да $\mathbf{A} \models \theta[\overline{a}, b]$. Према индуктивној претпоставци $\mathbf{B} \models \theta[\overline{a}, b]$, па како је $b \in A \subseteq B$, следи да $\mathbf{B} \models \exists y\theta[\overline{a}]$. Обратна инклузија тврђења $(*)$ важи по претпоставци теореме. $\square$

Последица 7. *Нека је* $\mathbf{M}$ *нека* L*-структура и* $X \subseteq M$. *Ако за сваку формулу* $\theta(\overline{x}, y)$ *и све* $\overline{a}$ *из* X:

$$\text{из } \mathbf{M} \models \exists y\theta[\overline{a}] \text{ следи да постоји } b \in X \text{ такав да } \mathbf{M} \models \theta[\overline{a}, b],$$

онда је $\mathbf{X}$ *домен елементарног подмодела од* $\mathbf{M}$.

Доказ. Проверимо најпре да је $X \subseteq \mathbf{M}$, тј. X домен подмодела од $\mathbf{M}$.

Ако је c симбол константе, из $\mathbf{M} \models \exists y(y = c)$ следи да постоји $b \in X$ такво да је $b = c^{\mathbf{M}}$.

Ако је F операцијски симбол дужине n, и $a_1, \ldots, a_n \in X$, из

$$\mathbf{M} \models \exists y(F(x_1, \ldots, x_n) = y)[a_1, \ldots, a_n]$$

следи да постоји $b \in X$ такво да је $b = F^{\mathbf{M}}(a_1, \ldots, a_n)$.

Дакле, $X \subseteq \mathbf{M}$, па према претходној теореми важи тврђење. $\square$

Теорема 9. [**слаба Левенхајм-Сколемова теорема**] *Нека је* $\mathbf{M}$ *произвољна структура пребројиве сигнатуре* L. *Тада за сваки пребројиви скуп* $X \subseteq M$ *постоји пребројив елементаран подмодел* $\mathbf{A}$ *од* $\mathbf{M}$ *такав да* $X \subseteq A$.

Доказ. Дефинишимо низ пребројивих подскупова $X_0 \subseteq X_1 \subseteq X_2 \subseteq \cdots$ од M.

Нека је $X_0 = X$. Претпоставимо да је дефинисан скуп X_m и нека је $L_m = L \cup X_m$ проста еспанзија сигнатуре L симболима константи који одговарају елементима из X_m; одговарајућу експанзију структуре $\mathbf{M}$ означићемо $\mathbf{M}_m$. Нека је Γ_m скуп свих L_m-реченица које су облика $\exists y\theta(y)$ и које важе у $\mathbf{M}_m$. Оваквих реченица има пребројиво много:

$$\exists y\theta_0(y), \exists y\theta_1(y), \ldots, \exists y\theta_k(y), \ldots$$

и за сваку од њих постоји $a_k \in M$ такво да $\mathbf{M}_m \models \theta[a_k]$. Нека је $X_{m+1} = X_m \cup \{a_k \mid k \geqslant 0\}$; X_{m+1} је пребројив.

Скуп $A = \bigcup_{m\in\mathbb{N}} X_m$ такође је пребројив.

Остаје да проверимо услов претходне последице: за сваку формулу $\theta(\overline{x}, y)$ и све $\overline{a}$ из A:

$$\text{из } \mathbf{M} \models \exists y\theta[\overline{a}] \text{ следи да постоји } b \in A \text{ такав да } \mathbf{M} \models \theta[\overline{a}, b].$$

Нека је $\theta(x_1, \ldots, x_n, y)$ нека L-формула и $a_1, \ldots, a_n \in A$ тако да важи $\mathbf{M} \models \exists y\theta[\overline{a}]$. Очигледно је да постоји природан број m такав да $a_1, \ldots, a_n \in X_m$; уочимо формулу $\theta(\underline{a_1}, \ldots, \underline{a_1}, y)$ сигнатуре L_m. Тада $\mathbf{M}_m \models \exists y\theta(\underline{a_1}, \ldots, \underline{a_1}, y)$, па за неко $a \in M$ важи $\mathbf{M}_m \models \theta(\underline{a_1}, \ldots, \underline{a_1}, y)[a]$, што значи да $a \in X_{m+1} \subseteq A$. Дакле, за $b \in A$ важи $\mathbf{M} \models \theta[\overline{a}, b]$. $\square$

Комӣлеӣне и ω-каӣеӷоричне ӣеорије

Дефиниција 18. *Нека је T произвољна теорија.*

(1) Теорија T је дедуктивно затворена ако садрж све своје последице: $T = \mathrm{Cn}(T) = \{\sigma \mid T \vdash \sigma\}$.

Према теореми потпуности, $T \vdash \sigma$ акко $T \models \sigma$.

(2) Теорија T је комплетна ако је непротивречна и за сваку реченицу σ, или $\sigma \in T$ или $\neg\sigma \in T$ (и наравно не оба).

(3) Теорија T је категорична ако су сви њени модели изоморфни, тј. T има јединствен модел, до на изморфизам.

(4) Теорија T је ω-категорична ако су сви њени пребројиви модели међуосбно изоморфни, тј. T има јединствен пробројив модел, до на изоморфизам.

Лема 19. *Нека је T дедуктивно затворена теорија. Теорија T је комплетна акко сви модели теорије T елементарно еквивалентни.*

Доказ. ($\rightarrow$) Нека је T комплетна теорија, и нека су $\mathbf{A}$ и $\mathbf{B}$ модели теорије T. Ако $\mathbf{A} \not\equiv \mathbf{B}$, онда постоји реченица σ таква да $\mathbf{A} \models \sigma$ и $\mathbf{B} \models \neg\sigma$. Како је T комплетна теорија, или $\sigma \in T$ или $\neg\sigma \in T$. Ако би било $\sigma \in T$, имали бисмо да су у $\mathbf{B}$ тачне обе реченице σ и $\neg\sigma$, што је немогуће. Такође, ако би било $\neg\sigma \in T$, у $\mathbf{A}$ би биле тачне обе реченице σ и $\neg\sigma$, што је немогуће. Дакле, $\mathbf{A} \equiv \mathbf{B}$.

($\leftarrow$) Претпоставимо да су свака два модела теорије T елементарно еквивалентна, али да T није комплетна, тј. да постоји реченица σ таква да $\sigma \notin T$ или $\neg\sigma \notin T$. Није тешко уочити да су теорије $T \cup \{\sigma\}$ и $T \cup \{\neg\sigma\}$ непротивречне и да, самим тим, имају моделе – нека је $\mathbf{A} \models T \cup \{\sigma\}$ и $\mathbf{B} \models T \cup \{\neg\sigma\}$. Пошто су $\mathbf{A}$ и $\mathbf{B}$ модели теорије T, према петпоставци следи да је $\mathbf{A} \equiv \mathbf{B}$, што је немогуће, јер $\mathbf{A} \models \sigma$ и $\mathbf{B} \models \neg\sigma$. □

Лема 20. *Свака комплетна теорија која има коначан модел је категорична теорија.*

Претходном лемом су заправо окрактерисане све категоричне теорије. Теорије које имају бесконачне моделе, имају моделе и прозвољно велике кардиналности, а самим тим и неизоморфне моделе.

Лема 21. *Нека је T дедуктивно затворена теорија предбројивог језика која има само бесконачне моделе. Ако је T ω-категорична, онда је комплетна.*

Доказ. Претпоставимо да T није комплетна. Тада постоје модели $\mathbf{A}$ и $\mathbf{B}$ теорије T, који нису елементарно еквивалентни. Према слабој Левенхајм-Сколемовој теореми постоје пребројиви модели $\mathbf{A}'$ и $\mathbf{B}'$ такви да је $\mathbf{A}' \equiv \mathbf{A}$ и $\mathbf{B}' \equiv \mathbf{B}$. Из ω-категоричности теорије T следи да је $\mathbf{A}' \cong \mathbf{B}'$, па је самим тим и $\mathbf{A}' \equiv \mathbf{B}'$, што је немогуће. □

У доказу наредне теореме биће приказан један веома важан метод који ћемо касније више пута користити.

back-and-forth, или цик-цак метод

Теорема 10. *Теорија густих линеарних уређења са крајњим тачкама је ω-категорична.*

Доказ. Теорију T_{DLOE} густих линеарних уређења са крајњим тачкама чине следеће реченице:

Dense Linear Orders with End points

- $\forall x \forall y\, (x < y \Rightarrow \neg y < x)$
- $\forall x\, \neg x < x$
- $\forall x \forall y\, (x < y \vee y < x \vee x = y)$
- $\forall x \forall y \forall z\, (x < y \wedge y < z \Rightarrow x < z)$
- $\forall x \forall y\, (x < y \Rightarrow \exists z\, (x < z \wedge z < y))$
- $\exists x \forall y\, (x = y \vee x < y)$
- $\exists x \forall y\, (x = y \vee y < x)$

Нека су $\mathbf{A} = (A, <^{\mathbf{A}})$ и $\mathbf{B} = (B, <^{\mathbf{B}})$ два пребројива модела теорије T_{DLOE}. Елементе сваког од скупова A и B поређајмо у низ (без понављања):

$$A:\ a_1, a_2, a_3, a_4, \ldots \quad \text{и} \quad B:\ b_1, b_2, b_3, b_4, \ldots,$$

тако да су a_1 и a_2 редом најмањи и највећи елемент у $\mathbf{A}$, а b_1 и b_2 најмањи и највећи елемент у $\mathbf{B}$.

Функцију f између A и B конструисаћемо корак-по-корак. У сваком кораку конструишемо f-слике за два елемента из A.
Корак 1. $f(a_1) = b_1, f(a_2) = b_2$.
Корак n. I део: Нека је A_n скуп свих елемената из A за које су дефинисане f-слике у претходним корацима. Нека је a_i први елемент низа из A који не припада A_n. Како је скуп A_n коначан скуп, постоје a' и a'' из A_n такви да измењу њих нема других елемената из A_n, али a_i јесте између њих ($a' <^{\mathbf{A}} a_i <^{\mathbf{A}} a''$ или $a'' <^{\mathbf{A}} a_i <^{\mathbf{A}} a'$). Нека је b било који елемент из B који се налази између $f(a')$ и $f(a'')$. Ставимо да је $f(a_i) = b$.

II део: Нека је B_n скуп свих елемената из B који су слике елемената из $A_n \cup \{a_i\}$. Нека је b_j први елемент низа из B који не припада B_n. Како је скуп B_n коначан скуп, постоје b' и b'' из B_n такви да измењу њих нема других елемената из B_n, али b_j јесте између њих ($b' <^{\mathbf{B}} b_j <^{\mathbf{B}} b''$ или $b'' <^{\mathbf{B}} b_j <^{\mathbf{B}} b'$). Нека је a било који елемент из A који се налази између елемената чије су слике b' и b''. Ставимо $f(a) = b_j$.

На описани начин, дефинисана је функција f између A и B, која је 1-1 и на, и која чува уређење; дакле $f : \mathbf{A} \cong \mathbf{B}$. □

Последица 8. *T_{DLOE} је комплетна теорија.*

Доказ. Према Леми 21 довољно је уочити да T_{DLOE} има само бесконачне моделе. □

Напомена 1. *Према претходној последици, $([0,1]_{\mathbb{Q}}, <)$ је једини, до на изоморфизам, пребројиви модел теорије T_{DLOE}. Приметимо да је $([0,1], <)$ непребројиви модел теорије T_{DLOE}, и да је*

$[0,1]_{\mathbb{Q}}$ скуп свих рационалних бројева јединичног интервала

$$([0,1], <) \equiv ([0,1]_{\mathbb{Q}}, <),$$

али је наравно $([0,1], <) \not\cong ([0,1]_{\mathbb{Q}}, <)$.

Последица 9. *Теорија густих линеарних уређења без крајњих тачака је ω-категорична и комплетна.*

Скица доказа. Теорију T_{DLO} густих линеарних уређења без крајњих тачака чине следеће реченице:

- $\forall x \forall y \, (x < y \Rightarrow \neg y < x)$
- $\forall x \, \neg x < x$
- $\forall x \forall y \, (x < y \vee y < x \vee x = y)$
- $\forall x \forall y \forall z \, (x < y \wedge y < z \Rightarrow x < z)$
- $\forall x \forall y \, (x < y \Rightarrow \exists z \, (x < z \wedge z < y))$
- $\forall x \exists y \, x < y$
- $\forall x \exists y \, y < x$

Сваки модел за T_{DLO} се може проширити до модела за T_{DLOE} додавањем најмањег и највећег елемента. Ако би постојали пребројиви неизоморфни модели за T_{DLO}, могли би се проширити до неизоморфних пребројивих модела за T_{DLOE}. □

Последица 10. $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$

Својство ω-категоричности неке теорије дефинисали смо семантички, ослањајући се на моделе те теорије. Постоје и другачије карактеризације, међу којима издвајамо један синтаксни услов.

Дефиниција 19. *Ако је T нека теорија, за формуле α и β кажемо да су T-еквивалентне, у означи $\alpha \equiv_T \beta$, ако је $T \vdash \alpha \Leftrightarrow \beta$.*

Теорема 11. *Нека је T комплетна теорија. Ако, до на T-еквивалентност, постоји само коначно много формула са n-слободних промењљивих, за свако n, онда је T ω-категорична.*

ДОКАЗ. Претпоставимо да за свако n постоји, до на T-еквивалентност, само коначно много формула са n слободних промењивих; окупимо их у скуп:

$$\mathcal{F}_n(\overline{x}) = \{\theta_1(\overline{x}), \ldots, \theta_n(\overline{x})\},$$

при чему је $\overline{x} = (x_1, \ldots, x_n)$.

Докажимо да је T ω-категорична теорија. Нека су $\mathbf{A}$ и $\mathbf{B}$ пребројиви модели теорије T, при чему су елементи сваког од скупова A и B поређајмо у низ (без понављања). Конструисаћемо изоморфизам f између $\mathbf{A}$ и $\mathbf{B}$ цик-цак методом. Приметимо најпре да, пошто је T комплетна теорија, за сваку реченицу φ важи: $\mathbf{A} \models \varphi$ акко $\mathbf{B} \models \varphi$.

Нека је $A_0 = B_0 = \emptyset$. Претпоставимо да су у n-том кораку дефинисани коначни подскупови $A_n \subseteq A$ и $B_n \subseteq B$, $|A_n| = |B_n| = n$, такви да за сваку формулу $\varphi(x_1, \ldots, x_n)$ важи:

$$\mathbf{A} \models \varphi(a_1, \ldots, a_n) \text{ акко } \mathbf{B} \models \varphi(b_1, \ldots, b_n),$$

где су $a_1, \ldots, a_n$ и $b_1, \ldots, b_n$ низови елемената из A и B поређани у редоследом којим је дефинисана функција f.
КОРАК $n+1$.

Случај када је n паран број. Нека је a први елемент из A који се не појављује у A_n. Постоји, до на T-еквивалентност, само коначно много формула са $n+1$ слободном промењивом. Нека је $\phi(x_1, \ldots, x_n, y)$ конјункција свих формула $\theta_i(\overline{x}, y)$ из $\mathcal{F}_{n+1}(\overline{x}, y)$ таквих да $\mathbf{A} \models \theta_i[a_1, \ldots, a_n, a]$. Тада $\mathbf{A} \models \exists y \phi[a_1, \ldots, a_n]$. Према индуктивној претпоставци, $\mathbf{B} \models \exists y \phi[b_1, \ldots, b_n]$. Нека је $b \in B$ такав да $\mathbf{B} \models \phi[b_1, \ldots, b_n, b]$.

Случај када је n непаран број. Нека је b први елемент из B који се не појављује у B_n. Постоји, до на T-еквивалентност, само коначно много формула са $n+1$ слободном промењивом. Нека је $\psi(x_1, \ldots, x_n, y)$ конјункција свих формула $\theta_i(\overline{x}, y)$ из $\mathcal{F}_{n+1}(\overline{x}, y)$ таквих да $\mathbf{B} \models \theta_i[b_1, \ldots, b_n, b]$. Тада $\mathbf{B} \models \exists y \psi[b_1, \ldots, b_n]$. Према индуктивној претпоставци, $\mathbf{A} \models \exists y \phi[a_1, \ldots, a_n]$. Нека је $a \in B$ такав да $\mathbf{A} \models \phi[a_1, \ldots, a_n, a]$.

У сваком од наведених случајева, ставимо да је $f(a) = b$, $A_{n+1} = A_n \cup \{a\}$ и $B_{n+1} = B_n \cup \{b\}$.

Није тешко уочити да је овако дефинисана функција f тражени изоморфизам. □

Тачан је и обрат претходне теореме, али доказ те чињенице изостављамо.

Теорема 12. [***Рил-Нарцевски***] *Комплетна теорија T је ω-категорична акко за свако n постоји само коначно много формула са n-слободних промењивих, до на T-еквивалентност.*

Случајни графови

Теорија графова је теорија сигнатуре $\{R\}$ (при чему је R један бинарни релацијски симбол):

$$T_G : \ \forall x \, \neg R(x,x), \ \forall x \forall y \, (R(x,y) \Leftrightarrow R(y,x)).$$

Приметимо да је укупан број ивица графа над $V = \{v_1, \dots, v_n\}$, $n \geqslant 1$, једнак $\binom{n}{2} = \dfrac{n(n-1)}{2} = e(n)$.

Пун граф са n чворова, тј. граф чија су свака два чвора повезана ивицом, назива се n-клик.

Нека је $\mathcal{G}_n$ скуп свих графова са n чворова, а $\mathcal{G}_n(\varphi)$ скуп свих графова из $\mathcal{G}_n$ у којима важи φ. Тада је

$$P_n(\varphi) = \frac{|\mathcal{G}_n(\varphi)|}{|\mathcal{G}_n|}$$

вероватноћа да *случајно изабрани*, одн *случајно генерисани* граф са n чворова задовољава реченицу φ.

На пример, ако је α формула $\forall x \forall y \, (x \neq y \Rightarrow R(x,y))$ ('свака два чвора су повезана'), онда је

$$P_n(\alpha) = \frac{1}{2^{e(n)}} = \frac{1}{2^{\frac{n(n-1)}{2}}} \to 0, \, n \to \infty,$$

док је

$$P_n(\neg\alpha) = \frac{2^{e(n)} - 1}{2^{e(n)}} \to 1, \, n \to \infty.$$

Ако је β формула

$$\exists x \exists y \, (R(x,y) \wedge \forall u \forall v \, (R(u,v) \Rightarrow (u = x \wedge v = y) \vee (u = y \wedge v = x)))$$

('граф има тачно једну ивицу'), онда је

$$P_n(\beta) = \frac{e(n)}{2^{e(n)}} \to 0, \, n \to \infty, \text{ и } P_n(\neg\beta) = \frac{2^{e(n)} - e(n)}{2^{e(n)}} \to 1, \, n \to \infty.$$

[**0-1 закон за графове**] За сваку $\{R\}$-реченицу θ важи

$$\lim_{n\to\infty} P_n(\theta) = 0 \text{ или } \lim_{n\to\infty} P_n(\theta) = 1.$$

Претходну теорему можемо формулисати и на следећи начин: једна од реченица, θ или $\neg\theta$ *скоро сигурно* важи у сваком коначном графу са великим бројем елемената. Из 0-1-закона за графове следи, на пример, да не постоји $\{R\}$-реченица којом се тврди да граф има паран број ивица.

У доказу 0-1-закона за графове користимо следеће $\{R\}$-реченице. За било које $m \in \mathbb{N}$ нека је ρ_m реченица:

$$\forall x_1 \cdots \forall x_m \forall y_1 \cdots \forall y_m \left(\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{m} x_1 \neq y_j \Rightarrow \exists z \left(\bigwedge_{i=1}^{m} R(x_i, z) \wedge \bigwedge_{j=1}^{m} (z \neq y_j \wedge \neg R(z, y_j)) \right) \right).$$

Реченица ρ_m тврди: за свака два дисјунктна скупа чворова $X = \{x_1, \dots, x_m\}$ и $Y = \{y_1, \dots, y_m\}$ ($X \cap Y = \emptyset$) постоји чвор z који не припада $X \cup Y$ такав да је повезан ивицом са сваким чвором из X и није повезан ни са једним чвором из Y. Ако је $m_1 \leqslant m_2$, онда $\rho_{m_2} \Rightarrow \rho_{m_1}$.

Ако је $n \leqslant m$, онда је $P_n(\rho_m) = 0$. Није лако прецизно одредити $P_n(\rho_m)$ ако је $n > m$. Да бисмо одредили $\lim\limits_{n\to\infty} P_n(\rho_m)$, проценићемо број $P_n(\rho_m)$ ако је $n > 2m$. Замислимо да на случајан начин генеришемо граф са n чворова. За сваки пар чворова v_i и v_j ($i \neq j$) бацамо фер новчић: ако падне грб, повезујемо v_i и v_j ивицом, а ако падне писмо, v_i и v_j не повезујемо ивицом. Нека је $X = \{x_1, \dots, x_m\}$ и $Y = \{y_1, \dots, y_m\}$ пар дисјунктних скупова чворова. За чвор $z \notin X \cup Y$ кажемо да *раздваја* пар X, Y ако је z повезан са сваким чвором из X, и није повезан ни са једним чвором из Y. Вероватноћа да z раздваја пар X, Y једнака је $\frac{1}{2^{2m}}$. Постоји укупно $n - 2m$ чворова који се могу изабрати за z, па вероватноћа да ниједан од њих не раздваја X, Y једнака је

$$\left(1 - \frac{1}{2^{2m}}\right)^{n-2m}.$$

Наравно, потребно је посматрати све могуће изборе парова дисјунктних скупова X, Y. Будућа да је

- $\binom{n}{2m}$ број могућих избора за $X \cup Y$;
- $\binom{2m}{m}$ број могућих избора за X

следи да могућих избора парова дисјунктних скупова X, Y има $\binom{n}{2m} \cdot \binom{2m}{m}$. Приметимо да је:

$$\binom{n}{2m} \cdot \binom{2m}{m} = \frac{n!}{(n-2m)! \cdot (2m)!} \cdot \frac{(2m)!}{m! \cdot m!} < \frac{n^{2m}}{(m!)^2} \leqslant n^{2m}.$$

одакле следи,

$$P_n(\neg\rho_m) \leqslant n^{2m} \cdot \left(1 - \frac{1}{2^{2m}}\right)^{n-2m} \to 0,\ n \to \infty.$$

Лема 22. $\lim\limits_{n\to\infty} P_n(\rho_m) = 1$

Теорију случајних графова T_{RG} чине следеће аксиоме:

- $\forall x\, \neg R(x, x)$
- $\forall x \forall y\, (R(x, y) \Leftrightarrow R(y, x))$
- $\varphi_{\geqslant m}$, тј. $\exists x_1 \cdots \exists x_m \bigwedge_{i<j} x_i \neq x_j$, за све $m \geqslant 1$ (приметимо, $\varphi_{\geqslant 1} \Leftarrow \varphi_{\geqslant 2} \Leftarrow \varphi_{\geqslant 3} \Leftarrow \cdots$)
- ρ_m за све $m \geqslant 1$ (приметимо, $\rho_1 \Leftarrow \rho_2 \Leftarrow \rho_3 \Leftarrow \cdots$)

Лема 23. *Теорија T_{RG} има модел.*

Доказ. Нека је T_0 коначан подскуп од T_{RG}. Докажимо да T_0 има модел. Нека је m_0 највећи природан број такав да $\rho_{m_0} \in T_0$. Из $\lim\limits_{n\to\infty} P_n(\rho_m) = 1$ следи да постоји довољно велико n_0, веће од сваког n таквог да $\varphi_{\geqslant n}$ припада T_0, тако да је $P_{n_0}(\rho_{m_0}) > 0$, што значи да скуп

$$\{\forall x\, \neg R(x,x),\, \forall x \forall y\, (R(x,y) \Leftrightarrow R(y,x)),\, \rho_1,\ldots,\rho_{m_0}, \varphi_{\geqslant 1},\ldots,\varphi_{\geqslant n_0}\}$$

има модел, одакле следи да и T_0 има модел. Према теореми компактности следи да T_{RG} има модел. □

Теорема 13. *Теорија T_{RG} је ω-категорична.*

Доказ. Нека су $\mathbf{A} = (A, R^{\mathbf{A}})$ и $\mathbf{B} = (B, R^{\mathbf{B}})$ пребројиви модели теорије T_{RG}. Изоморфизам f између $\mathbf{A}$ и $\mathbf{B}$ дефинишемо цик-цак методом. Елементе сваког од скупова A и B поређајмо у низ (без понављања). Нека је $f(a_1) = b_1$. Претпоставимо да су после n корака дефинисане f-вредности елемената из $A_n = \{a_1,\ldots,a_n\}$ и нека је $f(a_i) = b_i$, при чему је $B_n = \{b_1,\ldots,b_n\}$.
Корак $n+1$.

Случај када је n паран број. Нека је a први елемент из A такав да $a \notin A_n$. Пошто $\mathbf{B} \models \rho_m$, за произвољно велико m, постоји $b \in B$ такав да за свако $a_i \in A_n$ важи:

$$R^{\mathbf{B}}(f(a_i), b) \text{ акко } R^{\mathbf{A}}(a_i, a).$$

Случај када је n непаран број. Нека је b први елемент из B такав да $b \notin B_n$. Пошто $\mathbf{A} \models \rho_m$, за произвољно велико m, постоји $a \in A$ такав да за свако $a_i \in A_n$ важи:

$$R^{\mathbf{B}}(f(a_i), b) \text{ акко } R^{\mathbf{A}}(a_i, a).$$

У сваком случају стављамо да је $f(a) = b$, $A_{n+1} = A_n \cup \{a\}$ и $B_{n+1} = B_n \cup \{b\}$.

Није тешко уочити да је овако дефинисана функција f тражени изоморфизам. □

Дефиниција 20. *Јединствени (до на изоморфизам) пребројиви модел теорије T_{RG} назива се случајни граф.*

Теорема 14. *Сваки коначан граф се може утопити у било који модел теорије T_{RG}.*

Доказ. Нека је $\mathbf{G} = (G, R^{\mathbf{G}})$ коначни граф и $\mathbf{M} \models T_{RG}$. Да се $\mathbf{G}$ може утопити у $\mathbf{M}$ показујемо индукцијом по броју елемената скупа G.

Ако је $|G| = 1$, тврђење је очигледно тачно. Претпоставимо да се сваки граф са n чворова може утопити у $\mathbf{M}$.

Нека је G граф који има $n+1$ елемент, $G = \{v_1, \ldots, v_n, v_{n+1}\}$. Нека је $G' = \{v_1, \ldots, v_n\}$ подграф од $\mathbf{G}$ и $f : \mathbf{G}' \hookrightarrow \mathbf{M}$ утапање. Пошто $\mathbf{M} \models \rho_m$, за произвољно велико m постоји чвор a у M такав да

$$R^{\mathbf{M}}(f(v_i), a) \text{ акко } R^{\mathbf{G}}(v_i, v_{n+1}),\ i = 1, \ldots, n.$$

Дакле, $\mathbf{G}$ се може утопити у $\mathbf{M}$. □

Теорема 15. *Теорија T_{RG} је комплетна теорија.*

Комплетност теорије T_{RG} следи из чињенице да T_{RG} има само бесконачне моделе.

Теорема 16. [***0-1 закон за графове***] *За сваку реченицу θ сигнатуре $\{R\}$ важи*

$$\lim_{n\to\infty} P_n(\theta) = 0 \text{ или } \lim_{n\to\infty} P_n(\theta) = 1.$$

Доказ. Према доказаним тврђењима, за сваку реченицу φ такву да $T_{RG} \vdash \varphi$ важи $\lim\limits_{n\to\infty} P_n(\varphi) = 1$. Пошто је T_{RG} комплетна теорија, за сваку реченицу θ важи $T_{RG} \vdash \theta$ или $T_{RG} \vdash \neg\theta$, дакле следи

$$\lim_{n\to\infty} P_n(\theta) = 1 \text{ или } \lim_{n\to\infty} P_n(\neg\theta) = 1.$$

□

Претходни резултат важи за сваку сигнатуру која садржи само релацијске симболе.

Елиминација квантификатора

Дефиниција 21. *Теорија T допушта елиминацију квантификатора ако за сваку формулу $\varphi(x_1,\dots,x_n)$ постоји формула без квантификатора $\psi(x_1,\dots,x_n)$ таква да $T \vdash \varphi(x_1,\dots,x_n) \Leftrightarrow \psi(x_1,\dots,x_n)$.*

Модел $\mathbf{M}$ допушта елиминацију квантификатора ако $\mathrm{Th}(\mathbf{M})$ допушта елиминацију квантификатора.

Теорема 17. *Теорија T допушта елиминацију квантификатора акко за сваку формулу облика $\exists y \bigwedge_{i=1}^{n} \lambda_i(x_1,\dots,x_n,y)$, где је $\lambda_i(x_1,\dots,x_n,y)$ неки литерал, постоји формула без квантификатора $\psi(x_1,\dots,x_n)$ таква да*

$$T \vdash \exists y \bigwedge_{i=1}^{n} \lambda_i(x_1,\dots,x_n,y) \Leftrightarrow \psi(x_1,\dots,x_n).$$

Доказ. ($\Leftarrow$) Нека је $\varphi(\overline{x})$ произвољна формула у пренекс нормалној форми

$$\mathrm{Q}_1 y_1 \cdots \mathrm{Q}_m y_m \theta(\overline{x},\overline{y}),\ \mathrm{Q}_i \in \{\forall,\exists\},\ i = 1,m.$$

Најпре елиминишемо Q_m.

Ако је $\mathrm{Q}_m = \exists$, онда је

$$\begin{aligned}
\exists y_m \theta(\overline{x},\overline{y}) &\Leftrightarrow \exists y_m \theta(\overline{x},\overline{y}) \\
&\Leftrightarrow \exists y_m \bigvee_i \bigwedge_j \lambda_{ij}(\overline{x},\overline{y}) \\
&\Leftrightarrow \bigvee_i \exists y_m \bigwedge_j \lambda_{ij}(\overline{x},\overline{y}) \\
&\Leftrightarrow \bigvee_i \psi_i(\overline{x},y_1,\dots,y_{m-1}),
\end{aligned}$$

где је $\psi_i(\overline{x},y_1,\dots,y_{m-1})$ одговарајућа формула без квантификатора.

Ако је $\mathrm{Q}_m = \forall$, онда је

$$\begin{aligned}
\forall y_m \theta(\overline{x},\overline{y}) &\Leftrightarrow \neg\exists y_m \neg\theta(\overline{x},\overline{y}) \\
&\Leftrightarrow \neg\exists y_m \bigvee_i \bigwedge_j \lambda'_{ij}(\overline{x},\overline{y}) \\
&\Leftrightarrow \neg \bigvee_i \exists y_m \bigwedge_j \lambda'_{ij}(\overline{x},\overline{y}) \\
&\Leftrightarrow \neg \bigvee_i \psi'_i(\overline{x},y_1,\dots,y_{m-1}),
\end{aligned}$$

где је $\psi'_i(\overline{x},y_1,\dots,y_{m-1})$ одговарајућа формула без квантификатора. $\square$

Лема 24. *Нека су* $\mathbf{A}$ *и* $\mathbf{M}$ *две* L*-структуре и* $E_{\mathbf{A}}$ *скуп свих реченица језика* L_A *које су тачне у* $(\mathbf{A}, a)_{a\in A}$*. Постоји проста експанзија структуре* $\mathbf{M}$ *која је модел теорије* $E_{\mathbf{A}}$ *акко се* $\mathbf{A}$ *може елементарно утопити у* $\mathbf{M}$.

Лема 25. *Нека су* $\mathbf{A}$ *и* $\mathbf{B}$ *модели комплетне теорије* T*. Тада постоји модел* $\mathbf{M}$ *такав да се и* $\mathbf{A}$ *и* $\mathbf{B}$ *могу елементарно утопити у* $\mathbf{M}$.

ДОКАЗ. Нека је T комплетна L-теорија, $\mathbf{A}$ и $\mathbf{B}$ њени модели и:

$E_{\mathbf{A}}$ скуп свих реченица језика L_A које су тачне у $(\mathbf{A}, a)_{a\in A}$,

$E_{\mathbf{B}}$ скуп свих реченица језика L_B које су тачне у $(\mathbf{B}, b)_{b\in B}$.

Докажимо да је $E_{\mathbf{A}} \cup E_{\mathbf{B}}$ непротивречна теорија сигнатуре $L \cup \{\underline{a} \mid a \in A\} \cup \{\underline{b} \mid b \in B\}$, при чему су $\{\underline{a} \mid a \in A\}$ и $\{\underline{b} \mid b \in B\}$ дисјунктни скупови нових симбола константи.

Претпоставимо да је $E_{\mathbf{A}} \cup E_{\mathbf{B}}$ противречна теорија. Тада постоји $\beta \in E_{\mathbf{B}}$ таква да $E_{\mathbf{A}}, \beta \vdash \bot$, тј. $E_{\mathbf{A}} \vdash \neg\beta$. Формула β је облика $\beta_0(\overline{b})$, где је $\beta_0(\overline{x})$ нека L-формула и $\overline{b}$ коначан низ елемената из B. Пошто су $\mathbf{A}$ и $\mathbf{B}$ елементарно еквивалентни, β_0 није реченица, тј. има бар једну слободну променљиву.

Како се симболи константи који одговарају елементима низа $\overline{b}$ не појављују у формулама теорије $E_{\mathbf{A}}$, закључујемо да важи $E_{\mathbf{A}} \vdash \forall\overline{x}\neg\beta_0(\overline{x})$. Дакле, $\mathbf{A} \models \neg\exists\overline{x}\beta_0(\overline{x})$, одакле следи $\mathbf{B} \models \neg\exists\overline{x}\beta_0(\overline{x})$, што је немогуће, јер $\beta_0(\overline{b}) \in E_{\mathbf{B}}$, тј. $\mathbf{B} \models \beta_0(\overline{b})$.

Нека је $(\mathbf{M}, \underline{a}^{\mathbf{M}}, \underline{b}^{\mathbf{M}})_{a\in A, b\in B} \models E_{\mathbf{A}} \cup E_{\mathbf{B}}$. Није тешко показати да су функције:

$f : A \to M, f(a) = \underline{a}^{\mathbf{M}}, a \in A$ и

$g : B \to M, g(b) = \underline{b}^{\mathbf{M}}, b \in B$

тражена елементарна утапања, $f : \mathbf{A} \prec \mathbf{M}$ и $g : \mathbf{B} \prec \mathbf{M}$. $\square$

Теорема 18. *Нека је* T *комплетна теорија. За сваку формулу* $\varphi(\vec{x})$ *следећи услови су еквивалентни:*

(1) $\varphi(x_1, \ldots, x_n)$ *је* T*-еквивалентно некој формули без квантификатора.*

(2) Ако $\mathbf{M} \models T$ *и* n*-торке* $\overline{a}, \overline{b}$ *елемената из* M *задовољавају исте атомске реченице, онда важи:* $\mathbf{M} \models \varphi[\overline{a}]$ *акко* $\mathbf{M} \models \varphi[\overline{b}]$.

ДОКАЗ. (1) $\Rightarrow$ (2) Очигледно.

(2) $\Rightarrow$ (1) Нека је $\overline{c}$ n-торка нових симбола константи, $L' = L \cup \{c_1, \ldots, c_n\}$ и Δ скуп свих L'-реченица без квантификатора које су последице теорије $T \cup \{\varphi(\overline{c})\}$. Дакле, за свако $\psi \in \Delta$ важи $T, \varphi(\overline{c}) \vdash \psi$, тј. $T \vdash \varphi(\overline{c}) \Rightarrow \psi$. Приметимо да је Δ затворено за конјункције. Довољно је показати да за неко $\psi_0 \in \Delta$ важи

$T \vdash \psi_0 \Rightarrow \varphi(\bar{c})$. Ова чињеница ће бити последица Теореме компактности ако докажемо да $T \cup \Delta \vdash \varphi(\bar{c})$.

Претпоставимо супротно, да је $T \cup \Delta \cup \{\neg\varphi(\bar{c})\}$ непротивречно; нека је $\mathbf{A}' \models T \cup \Delta \cup \{\neg\varphi(\bar{c})\}$. Означимо Δ' скуп свих L'-реченица без квантификатора које су тачне у $\mathbf{A}'$. Очигледно је $\Delta \subseteq \Delta'$ и Δ' је затворено за конјункције. Теорија $T \cup \Delta' \cup \{\varphi(\bar{c})\}$ је непротивречна. Заиста, ако би постојао коначан скуп $\{\delta_1, \ldots, \delta_m\} \subseteq \Delta'$, такав да $T, \delta_1, \ldots, \delta_m, \varphi(\bar{c}) \vdash \bot$, имали бисмо $T, \varphi(\bar{c}) \vdash \neg \bigwedge_{i=1}^m \delta_i$. Ако са δ означимо $\bigwedge_{i=1}^m \delta_i$, онда $\neg\delta \in \Delta \subseteq \Delta'$, што није могуће. Нека је $\mathbf{B}' \models T \cup \Delta' \cup \{\varphi(\bar{c})\}$.

Ако је $\mathbf{A}' = (\mathbf{A}, a_1, \ldots, a_n)$ и $\mathbf{B}' = (\mathbf{B}, b_1, \ldots, b_n)$, L-структуре $\mathbf{A}$ и $\mathbf{B}$ су модели комплетне теорије T, па према претходној леми постоји L-структура $\mathbf{M}$ и елементарна утапања $f : \mathbf{A} \prec \mathbf{M}$ и $g : \mathbf{B} \prec \mathbf{M}$. Јасно, $\mathbf{M} \models T$ и n-торке $f\bar{a} = (fa_1, \ldots, fa_n)$ и $g\bar{b} = (gb_1, \ldots, gb_n)$, елемената из M, задовољавају исте атомичне формуле. Заиста, нека је $\lambda(\bar{x})$ произвољан литерал сигнатуре L. Из $\mathbf{M} \models \lambda[f\bar{a}]$ следи $\mathbf{A} \models \lambda[\bar{a}]$, тј. $\mathbf{A}' = (\mathbf{A}, \bar{a}) \models \lambda(\bar{c})$. Дакле, $\lambda(\bar{c}) \in \Delta'$, па $\mathbf{B}' = (\mathbf{B}, \bar{b}) \models \lambda(\bar{c})$, тј. $\mathbf{B} \models \lambda[\bar{b}]$, одакле следи $\mathbf{M} \models \lambda[g\bar{b}]$. Међутим:

- Из $\mathbf{A}' = (\mathbf{A}, \bar{a}) \models \neg\varphi(\bar{c})$ следи $\mathbf{A} \models \neg\varphi[\bar{a}]$, па и $\mathbf{M} \models \neg\varphi[f\bar{a}]$.
- Из $\mathbf{B}' = (\mathbf{B}, \bar{b}) \models \varphi(\bar{c})$ следи $\mathbf{B} \models \varphi[\bar{b}]$, па и $\mathbf{M} \models \varphi[g\bar{a}]$.

Ова два услова противрече претпоставци (2). □

Претходна теорема даје један критеријум за утврђивање да ли је дата формула T-еквивалентна формули без квантификатора, када је T комплетна теорија.

Теорема 19. *Нека је T комплетна теорија коначне релационе сигнатуре. Тада су следећи услови еквивалентни:*

(1) T допушта елиминацију квантификатора.

(2) За сваки модел $\mathbf{M}$ теорије T, ако n-торке $\bar{a}$ и $\bar{b}$ елемената из M задовољавају исте атомске формуле, онда за свако $a \in M$ постоји $b \in M$ такво да $(\bar{a}, a)$ и $(\bar{b}, b)$ задовољавају исте атомске формуле.

Доказ. $(1) \Rightarrow (2)$ Нека је $\mathbf{M}$ произвољан модел теорије T, $\bar{a}$ и $\bar{b}$ n-торке елемената из M које задовољавају исте атомске формуле и $a \in M$ произвољно изабран.

Како L садржи само коначно много релацијских симбола, постоји само коначно много атомских формула са слободним променљивама $x_1, \ldots, x_n, x$. Нека је $\alpha(x_1, \ldots, x_n, x)$ конјункција свих литерала таквих да $\mathbf{M} \models \alpha[\bar{a}, a]$. Из претпоставке (1) следи да постоји формула без квантификатора $\theta(x_1, \ldots, x_n)$ таква да

$$T \vdash \exists x \alpha(x_1, \ldots, x_n, x) \Leftrightarrow \theta(x_1, \ldots, x_n),$$

а самим тим и $\mathbf{M} \models \theta[\overline{a}]$. Пошто $\overline{a}$ и $\overline{b}$ задовољавају исте атомске формуле, закључујемо да $\mathbf{M} \models \theta[\overline{b}]$, односно $\mathbf{M} \models \exists x\alpha(\overline{x}, x)[\overline{b}]$. Ово последње значи да постоји $b \in B$ такав да $\mathbf{M} \models \alpha[\overline{b}, b]$.

(2) $\Rightarrow$ (1) Довољно је доказати да T допушта елеминицају квантификатора за формуле облика $\exists x\varphi(\overline{x}, x)$, где је $\varphi(\overline{x}, x)$ формула без квантификатора.

Нека је $\mathbf{M} \models T$ и нека су $\overline{a}$ и $\overline{b}$ n-торке елемената из M које задовољавају исте атомичне формуле. Тада

$$\mathbf{M} \models \exists x\varphi(\overline{x}, x)[\overline{a}] \text{ акко } \mathbf{M} \models \exists x\varphi(\overline{x}, x)[\overline{b}],$$

па је према претходној теореми, $\exists x\varphi(\overline{x}, x)$ T-еквивалентно формули без квантификатора. □

Последица 11. *Нека је T комплетна теорија коначне релационе сигнатуре. T допушта елиминацију квантификатора акко услов (2) претходне теореме важи за неки модел $\mathbf{M}$ теорије T.*

Пример 32. Нека је T теорија густих линеарних уређења са крајњим тачкама. Подсећамо да је T комплетна теорија. Докажимо да T не допушта елиминацију квантификатора.

Елементи 0 и $1/10$ модела $[0,1]_{\mathbb{Q}}$ задовољавају исте атомичне формуле (са једном слободном променљивом x: $x < x$ и $x = x$). Међутим, не постоји a из $[0,1]_{\mathbb{Q}}$ такав да $(0, a)$ и $(1/10, 1/100)$ задовољавају исте атомичне формуле. Према претходној теореми, T не дозвољава елиминацију квантификатора.

Специјално, $\exists y(y < x)$ није T-еквивалентно формули без квантификатора.

Теорема 20. *Теорија густих линеарних уређења без крајњих тачака допушта елиминацију квантификатора.*

Доказ. Према претходној последици, довољно је доказати услов (2) за $(\mathbb{Q}, <)$. Нека су $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$ n-торке рационалних бројева које задовољавају исте атомске формуле. Ако, без губљења општости, претпоставимо да је $a_1 < a_2 < \ldots < a_n$, онда је и $b_1 < b_2 < \ldots < b_n$. Треба доказати да за било који $a \in \mathbb{Q}$, постоји $b \in \mathbb{Q}$ такав да $(a_1, \ldots, a_n, a)$ и $(b_1, \ldots, b_n, b)$ задовољавају исте атомске формуле. Разликујемо четири случаја:

1. Ако је $a = a_i$, за неко $i \in \{1, \ldots, n\}$, онда узимамо да је $b = b_i$;

2. Ако је $a < a_i$, за свако $i \in \{1, \ldots, n\}$, онда узимамо да је b рационалан број мањи од свих $b_1, \ldots, b_n$;

3. Ако је $a_i < a$, за свако $i \in \{1, \ldots, n\}$, онда узимамо да је b рационалан број већи од свих $b_1, \ldots, b_n$;

4. Ако је $a_i < a < a_{i+1}$, за неко $i \in \{1, \dots, n-1\}$, онда узимамо да је b рационалан број између b_1 и b_{i+1}.

□

Теорема 21. *Теорија T_{RG} допушта елиминацију квантификатора.*

Доказ. Нека је (G, E) случајни граф. Према аксиоми ρ_m, за довољно велико m, за све n-торке $\overline{a}$ и $\overline{b}$ елемената из G које задовољавају исте атомске формуле и произвољно изабран $a \in G$ постоји $b \in G$ такав да $(\overline{a}, a)$ и $(\overline{b}, b)$ задовољавају исте атомске реченице. □