Небојша Икодиновић

УВОД У МАТЕМАТИЧКУ ЛОГИКУ

Булове алгебре, Исказна логика, Логика првог реда

Београд
2014

Садржај

Предговор

Књига је написана на основу предавања које је аутор држао у оквиру предмета Увод у математичку логику ...

У Београду, 2014. године Аутор

Булове алгебре

Дефиниција Булове алгебре

Уопштено говорећи, Булове алгебре треба замишљати као структуре чије се операције „понашају“ попут добро познатих скуповних операција, тј. задовољавају иста својства као скуповне операције. Зато најпре наводимо основне примере Булових алгебри, који ће нам уједно бити и полазиште скоро свих даљих разматрања.

ПРИМЕР 1. Нека је U произвољан скуп. Ако партитивни скуп $\mathcal{P}(U)$, тј. скуп свих подскупова скупа U, посматрамо заједно са операцијама:

- *уније*, $\cup : \mathcal{P}(U) \times \mathcal{P}(U) \to \mathcal{P}(U)$, $(X, Y) \mapsto X \cup Y$, $X, Y \in \mathcal{P}(U)$,
- *пресека*, $\cap : \mathcal{P}(U) \times \mathcal{P}(U) \to \mathcal{P}(U)$, $(X, Y) \mapsto X \cap Y$, $X, Y \in \mathcal{P}(U)$ и
- *комплементирања*, ${}^{\mathrm{c}} : \mathcal{P}(U) \to \mathcal{P}(U)$, $X \mapsto X^{\mathrm{c}} = U \setminus X$, $X \in \mathcal{P}(U)$.

и елементима $\emptyset$ и U, који свакако имају посебан статус међу осталим елементима из $\mathcal{P}(U)$, добијамо типичан пример Булове алгебре. Ову Булову алгебру означавамо са $(\mathcal{P}(U), \cup, \cap, {}^{\mathrm{c}}, \emptyset, U)$ (при чему заправо набрајамо све оно што је сачињава).

Већ смо напоменули да ће нас занимати особине наведених операција. Као посебно значајне истичемо следеће познате једнакости[1]:

$\mathbf{A}^{\cup}$	$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$\mathbf{A}^{\cap}$	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$
$\mathbf{K}^{\cup}$	$X \cup Y = Y \cup X$	$\mathbf{K}^{\cap}$	$X \cap Y = Y \cap X$
$\mathbf{D}^{\cup}_{\cap}$	$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$\mathbf{D}^{\cap}_{\cup}$	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
$\mathbf{N}^{\cup}$	$X \cup \emptyset = X$	$\mathbf{N}^{\cap}$	$X \cap U = X$
$\mathbf{C}^{\cup}$	$X \cup X^{\mathrm{c}} = U$	$\mathbf{C}^{\cap}$	$X \cap X^{\mathrm{c}} = \emptyset$

које важе за све $X, Y, Z \in \mathcal{P}(U)$.

[1] Једнакости су означене почетним словом устаљених термина који се користе за одговарајуће особине операција, при чему уз слова стоје и ознаке операција на које се особине односе. У складу са тим и читамо ознаке: $\mathbf{A}^{\cup}$ – асоцијативност уније; $\mathbf{D}^{\cup}_{\cap}$ – дистрибутивност уније према пресеку, $\mathbf{N}^{\cap}$ – неутрални елемент за пресек, $\mathbf{C}^{\cup}$ – однос комплементирања и пресека, итд.

Ове идентитети нису случајно изабрани јер се испоставља да су остали скуповни идентитети последице наведених. За сада наводимо само један пример. Из наведених особина извешћемо идентитет $X \cap X = X$, $X \in \mathcal{P}(U)$.

$$X \cap X \overset{(\mathbf{N}^{\cup})}{=} (X \cap X) \cup \emptyset \overset{(\mathbf{C}^{\cap})}{=} (X \cap X) \cup (X \cap X^{c}) \overset{(\mathbf{D}^{\cap}_{\cup})}{=} X \cap (X \cup X^{c}) \overset{(\mathbf{C}^{\cup})}{=} X \cap U \overset{(\mathbf{N}^{\cap})}{=} X$$

Посебно је важан следећи специјалан случај алгебре $(\mathcal{P}(U), \cup, \cap, ^{c}, \emptyset, U)$. Ако је U једночлан скуп, на пример $U = \{\emptyset\}$, онда је $\mathcal{P}(U) = \{\emptyset, \{\emptyset\}\} = \{\emptyset, U\}$ и операције можемо приказати следећим таблицама.

$\cup$	$\emptyset$	U
$\emptyset$	$\emptyset$	U
U	U	U

$\cap$	$\emptyset$	U
$\emptyset$	$\emptyset$	$\emptyset$
U	$\emptyset$	U

	^{c}
$\emptyset$	U
U	$\emptyset$

Ако $\emptyset$ означимо са 0 и интерпретирамо као *нетачно*, $\{\emptyset\}$ са 1 и интерпретирамо као *тачно*, и преозначимо операције, $\cup$ са $\vee$, $\cap$ са $\wedge$ и ^{c} са $\neg$, добијамо редом таблице познатих логичких операција на скупу $\{0, 1\}$: *дисјункције*, *конјункције* и *негације*.

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

	$\neg$
0	1
1	0

Ознаке операција које користимо за ову специјалну Булову алгебру углавном се користе приликом општих разматрања о Буловим алгебрама. Ми ћемо у наредној дефиницији следити тај принцип, при чему ћемо поменуте ознаке мало стилизовати да би се разликовале од ових које ћемо користити за логичке операције. $\triangleright$

Особине скуповних операција истакнуте у претходном примеру узимамо за *аксиоме* Булових алгебри.

Дефиниција 1. ***Булова алгебра*** *је структура* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *коју чине неки скуп* B*, две бинарне операције*[2] $\curlyvee$, $\curlywedge : B \times B \to B$*, једна унарна* $' : B \to B$ *и два различита елемента* 0 *и* 1 *из* B*, при чему произвољни елементи* x, y, z *из* B *испуњавају следеће услове:*

$\mathbf{A}^{\curlyvee}$ $x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z$ $\quad$ $\mathbf{A}^{\curlywedge}$ $x \curlywedge (y \curlywedge z) = (x \curlywedge y) \curlywedge z$

$\mathbf{K}^{\curlyvee}$ $x \curlyvee y = y \curlyvee x$ $\quad$ $\mathbf{K}^{\curlywedge}$ $x \curlywedge y = y \curlywedge x$

$\mathbf{D}^{\curlyvee}_{\curlywedge}$ $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$ $\quad$ $\mathbf{D}^{\curlywedge}_{\curlyvee}$ $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$

$\mathbf{C}^{\curlyvee}$ $x \curlyvee x' = 1$ $\quad$ $\mathbf{C}^{\curlywedge}$ $x \curlywedge x' = 0$

$\mathbf{N}^{\curlyvee}$ $x \curlyvee 0 = x$ $\quad$ $\mathbf{N}^{\curlywedge}$ $x \curlywedge 1 = x$

Скуп B *се назива домен или скуп носач Булове алгебре* $\mathbf{B}$.

---

[2] На српском језику, бинарне операције Булове алгебре углавном се називају као и одговарајуће скуповне, односно логичке операције: $\curlyvee$ – унија, одн. дисјункција, $\curlywedge$ – пресек, одн. конјункција. На енглеском језику, који се данас сматра универзалним језиком и научне комуникације, поменуте операције имају нова имена: $\curlyvee$ – meet (а не union, одн. disjuntion), $\curlywedge$ – join (а не intersection, одн. conjunction).

Примери Булових алгебри

Пример 2. Са основним примерима Булових алгебри већ смо се упознали. Реч је о такозваним **алгебрама партитивног скупа** $(\mathcal{P}(U), \cup, \cap, {}^c, \emptyset, U)$, где је U било који скуп.

Када је U једночлан скуп, одговарајућу алгебру партитивног скупа називамо **алгебром исказног рачуна**. Узимајући у обзир разматрања и ознаке из претходног примера, алгебру исказног рачуна означавамо са $\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$. Приметимо да се операције Булове алгебре $\mathbf{2}$ могу описати и на још један начин уколико 0 и 1 схватимо као бројеве. Наиме, за $x, y \in \{0,1\}$, имамо да је $x \vee y = \max\{x,y\}$, $x \wedge y = \min\{x,y\}$, (при чему се ослањамо на уобичајени поредак $0 < 1$), као и да је $\neg x = 1 - x$ („$-$“ је знак за одузимање). Дакле, можемо писати и да је $\mathbf{2} = (\{0,1\}, \max, \min, 1-, 0, 1)$, при чему „$1-$“ схватамо као ознаку функције која очекује аргумент здесна. Једнакости из претходне дефиниције у овој нотацији постају:

$\mathbf{A}^{\curlyvee}$ $\max\{x, \max\{y,z\}\} = \max\{\max\{x,y\}, z\}$

$\mathbf{A}^{\curlywedge}$ $\min\{x, \min\{y,z\}\} = \min\{\min\{x,y\}, z\}$

$\mathbf{K}^{\curlyvee}$ $\max\{x,y\} = \max\{y,x\}$ $\mathbf{K}^{\curlywedge}$ $\min\{x,y\} = \min\{y,x\}$

$\mathbf{D}^{\curlyvee}_{\curlywedge}$ $\max\{x, \min\{y,z\}\} = \min\{\max\{x,y\}, \max\{x,z\}\}$

$\mathbf{D}^{\curlywedge}_{\curlyvee}$ $\min\{x, \max\{y,z\}\} = \max\{\min\{x,y\}, \min\{x,z\}\}$

$\mathbf{C}^{\curlyvee}$ $\max\{x, 1-x\} = 1$ $\mathbf{C}^{\curlywedge}$ $\min\{x, 1-x\} = 0$

$\mathbf{N}^{\curlyvee}$ $\max(x, 0) = x$ $\mathbf{N}^{\curlywedge}$ $\min\{x, 1\} = x$

и директно се може проверити да важе за било које $x, y \in \{0,1\}$. Ми ћемо се у наставку повремено ослањати и на ове описе операција алгебре $\mathbf{2}$. $\triangleright$

Пример 3. Занимљив пример Булове алгебре добијамо разматрајући скуп D_n свих природних делилаца неког природног броја n који је производ различитих простих бројева (дакле, n није дељив квадратом неког простог броја). Није тешко показати, користећи елементарна својства најмањег заједничког садржаоца и највећег заједничког делиоца, да је $\mathbf{D}_n = (D_n, \mathrm{nzs}, \mathrm{nzd}, n/, 1, n)$ једна Булова алгебра (комплемент елемента $x \in D_n$ је n/x), тј. да за било које x, y, z важе следеће једнакости:

$\mathbf{A}^{\curlyvee}$ $\mathrm{nzs}(x, \mathrm{nzs}(y,z)) = \mathrm{nzs}(\mathrm{nzs}(x,y), z)$

$\mathbf{A}^{\curlywedge}$ $\mathrm{nzd}(x, \mathrm{nzd}(y,z)) = \mathrm{nzd}(\mathrm{nzd}(x,y), z)$

$\mathbf{K}^{\curlyvee}$ $\mathrm{nzs}(x,y) = \mathrm{nzs}(y,x)$ $\mathbf{K}^{\curlywedge}$ $\mathrm{nzd}(x,y) = \mathrm{nzd}(y,x)$

$\mathbf{D}^{\curlyvee}_{\curlywedge}$ $\mathrm{nzs}(x, \mathrm{nzd}(y,z)) = \mathrm{nzd}(\mathrm{nzs}(x,y), \mathrm{nzs}(x,z))$

$\mathbf{D}^{\curlywedge}_{\curlyvee}$ $\mathrm{nzd}(x, \mathrm{nzs}(y,z)) = \mathrm{nzs}(\mathrm{nzd}(x,y), \mathrm{nzd}(x,z))$

$\mathbf{C}^{\curlyvee}$ $\mathrm{nzs}\left(x, \frac{n}{x}\right) = n$ $\mathbf{C}^{\curlywedge}$ $\mathrm{nzd}\left(x, \frac{n}{x}\right) = 1$

$\mathbf{N}^{\curlyvee}$ $\mathrm{nzs}(x, 1) = x$ $\mathbf{N}^{\curlywedge}$ $\mathrm{nzd}(x, n) = x$

Комплетан доказ наведених једнакости препуштамо читаоцима. Овде наводимо само детаљније упутство. Нека су $p_1, \ldots, p_k$ међусобно различити прости бројеви и нека је $n = p_1 \cdots p_k$. Тада се сваки елемент $x \in D_n$ може записати у облику $x = p_1^{a_1} \cdots p_k^{a_k}$, за неке $a_1, \ldots, a_k \in \{0,1\}$. Ако је $x = p_1^{a_1} \cdots p_k^{a_k}$ и $y = p_1^{b_1} \cdots p_k^{b_k}$, $a_i, b_i \in \{0,1\}$, $i = 1, \ldots, k$, онда је $\mathrm{nzs}(x,y) = p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}$ и $\mathrm{nzd}(x,y) = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}$. Комплемент елемента x јесте $\frac{n}{x} = p_1^{1-a_1} \ldots p_k^{1-a_k}$. Сада је једноставно проверити сваку од наведених једнакости коришћењем одговарајућих једнакости из претходног примера. $\triangleright$

Пример 4. Ако је U било који скуп, Булову алгебру образује и било који непразан подскуп $\mathcal{B}$ од $\mathcal{P}(U)$ који је затворен за унију, пресек и комплемент: ако $X, Y \in \mathcal{B}$, онда $X \cup Y, X \cap Y, X^{c} \in \mathcal{B}$. Приметимо да из затворености скупа $\mathcal{B}$ за наведене операције, следи да $\emptyset, U \in \mathcal{B}$. Булове алгебре добијене на овај начин називају се **поља скупова** или **алгебре скупова**. Уобичајено је да се са $\mathcal{B}$ означава и одговарајућа Булова алгебра, када се подразумева да су њене операције заправо скуповне операције. Алгебра партитивног скупа је специјалан случај поља скупова. Наводимо још неколико примера поља скупова.

Подскуп X од U је *коконачан* (кофинитан) ако је његов комплемент $X^{c} = U \setminus X$ коначан. Скуп свих подскупова од U који су коначни или коконачни представља једно поље скупова, које се назива и **Фрешеова алгебра** или **алгебра коначно-коконачних скупова** и обележава се са $\mathcal{F}(U)$. Није тешко проверити да је скуп $\mathcal{F}(U)$ затворен за унију, пресек и комплемент. Заиста, ако $X, Y \in \mathcal{F}(U)$, да бисмо доказали да $X \cup Y \in \mathcal{F}(U)$ разликујемо следеће случајеве.
1. случај: и X и Y су коначни. Тада је $X \cup Y$ коначан па припада $\mathcal{F}(U)$.
2. случај: и X и Y су коконачни. Тада су $U \setminus X$ и $U \setminus Y$ коначни, па је коначан и њихов пресек $(U \setminus X) \cap (U \setminus Y)$. Према Де Моргановом закону је $(U \setminus X) \cap (U \setminus Y) = U \setminus (X \cup Y)$, одакле закључујемо да је $X \cup Y$ коконачан скуп па припада $\mathcal{F}(U)$.
3. случај: X коначан и Y је коконачан[3]. Како је $U \setminus (X \cup Y) = (U \setminus X) \cap (U \setminus Y) \subseteq U \setminus Y$ и $U \setminus Y$ је коначан скуп, закључујемо да је $X \cup Y$ коконачан, па припада $\mathcal{F}(U)$.
Препуштамо читаоцима да докажу да је $\mathcal{F}(U)$ затворен за пресек и комплемент.

Ако је U коначан скуп, онда је $\mathcal{F}(U) = \mathcal{P}(U)$. Међутим, ако је U бесконачан скуп, онда се Фрешеова алгебра разликује од $\mathcal{P}(U)$. Важно је приметити да је $|\mathcal{F}(U)| = |U|$ уколико је U бесконачан скуп (зашто?), што значи да постоје Булове алгебре било које бесконачне кардиналности[4].

Размотримо и једно поље подскупова скупа реалних бројева $\mathbb{R}$. Под **лево-полузатвореним интервалима** подразумевамо подскупове од $\mathbb{R}$ који су облика $(-\infty, b)$, $b \in \mathbb{R}$, или $[a, b)$, $a, b \in \mathbb{R}$, $a < b$, или $[a, +\infty)$, $a \in \mathbb{R}$, или $(-\infty, +\infty) = \mathbb{R}$. Коначне уније лево-полузатворених интервала образују поље скупова (проверите!). $\triangleright$

Пример 5. Ако су $\mathbf{B}_1 = (B_1, \curlyvee_1, \curlywedge_1, {}'^{1}, 0_1, 1_1)$ и $\mathbf{B}_2 = (B_2, \curlyvee_2, \curlywedge_2, {}'^{2}, 0_2, 1_2)$ две Булове алгебре, на природан начин дефинишемо Булову алгебру над $B_1 \times B_2$. Нека су $\curlyvee$ и $\curlywedge$ бинарне операције на $B_1 \times B_2$ дате редом са:

$$(x_1, x_2) \curlyvee (y_1, y_2) = (x_1 \curlyvee_1 y_1, x_2 \curlyvee_2 y_2) \text{ и } (x_1, x_2) \curlywedge (y_1, y_2) = (x_1 \curlywedge_1 y_1, x_2 \curlyvee_2 y_2),$$

и нека је комплементирање $'$ дефинисано са $(x_1, x_2)' = (x_1'^{1}, x_2'^{2})$. Једноставно се проверава да је $(B_1 \times B_2, \curlyvee, \curlywedge, ', (0_1, 0_2), (1_1, 1_2))$ Булова алгебра. Ова Булова алгебра назива се **производ** алгебри $\mathbf{B}_1$ и $\mathbf{B}_2$, и обележава се са $\mathbf{B}_1 \times \mathbf{B}_2$. На пример, операције Булове алгебре $\mathbf{2} \times \mathbf{2}$ дате су следећим таблицама.

[3]Могли смо претпоставити и да је X коконачан, а Y је коначан и дошли бисмо до истог закључка.

[4]Ствари стоје другачије када су у питању коначне Булове алгебре. Наиме, кардиналност коначне Булове алгебре, као што ћемо видети, може бити само степен броја 2.

$\curlyvee$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,0)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$

$\curlywedge$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

x	x'
$(0,0)$	$(1,1)$
$(0,1)$	$(1,0)$
$(1,0)$	$(0,1)$
$(1,1)$	$(0,0)$

$\triangleright$

Пример 6. Нека је I произвољан непразан скуп. На скупу 2^I, свих функција из I у скуп $2 = \{0,1\}$ који је уређен тако да је $0 < 1$, дефинисаћемо две бинарне операције, $f \sqcup g(x) = \max\{f(x), g(x)\}$ и $f \sqcap g(x) = \min\{f(x), g(x)\}$, и једну унарну операцију, $f'(x) = 1 - f(x)$. Ако су $\mathbf{0}, \mathbf{1} : I \to 2$ функције дефинисане са $\mathbf{0}(x) = 0$ и $\mathbf{1}(x) = 1$, онда је $(2^I, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ Булова алгебра, тј. за произвољне $f, g, h \in 2^I$ важе једнакости:

$\mathbf{A}^{\curlyvee}$ $f \sqcup (g \sqcup h) = (f \sqcup g) \sqcup h$ $\mathbf{A}^{\curlywedge}$ $f \sqcap (g \sqcap h) = (f \sqcap g) \sqcap h$
$\mathbf{K}^{\curlyvee}$ $f \sqcup g = g \sqcup f$ $\mathbf{K}^{\curlywedge}$ $f \sqcap g = g \sqcap f$
$\mathbf{D}^{\curlyvee}_{\curlywedge}$ $f \sqcup (g \sqcap h) = (f \sqcup g) \sqcap (f \sqcup h)$ $\mathbf{D}^{\curlywedge}_{\curlyvee}$ $f \sqcap (g \sqcup h) = (f \sqcap g) \sqcup (f \sqcap h)$
$\mathbf{C}^{\curlyvee}$ $f \sqcup f' = 1$ $\mathbf{C}^{\curlywedge}$ $f \sqcap f' = 0$
$\mathbf{N}^{\curlyvee}$ $f \sqcup \mathbf{0} = f$ $\mathbf{N}^{\curlywedge}$ $f \sqcap \mathbf{1} = f$

Уместо детаљног образложења зашто важе наведене једнакости, упућујемо читаоца на пример 2, уз напомену да, на пример, доказ једнакости $\mathbf{K}^{\curlyvee}$ подразумева доказ да за свако $x \in I$ важи $f \sqcup g(x) = g \sqcup f(x)$, тј. да за свако $x \in I$, важи $\max\{f(x), g(x)\} = \max\{g(x), f(x)\}$ (што је тривијално). $\triangleright$

Изоморфизам Булових алгебри

Иако смо се трудили да дефиницију Булових алгебри илуструјемо што већим бројем различитих примера, међу наведеним Буловим алгебрама постоје оне које су разликују само привидно, што ћемо детаљније објаснити у наредном примеру.

Пример 7. Посматрајмо две „привидно“ различите Булове алгебре: алгебру партитивног скупа $(\mathcal{P}(\{a,b\}), \cup, \cap, ^{c}, \emptyset, \{a,b\})$ и Булову алгебру $(D_6, \mathrm{nzs}, \mathrm{nzd}, 6/\,, 1, 6)$, о којој смо уопштено писали у примеру 3. Приметимо најпре да обе алгебре имају исти број елемената: $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ и $D_6 = \{1,2,3,6\}$. Ако пажљивије погледамо одговарајуће таблице операција, уочићемо да су у суштини истог облика.

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

x	x^{c}
$\emptyset$	$\{a,b\}$
$\{a\}$	$\{b\}$
$\{b\}$	$\{a\}$
$\{a,b\}$	$\emptyset$

nzs	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

nzd	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

x	$6/x$
1	6
2	3
3	2
6	1

Обострано-једнозначну кореспонденцију $\emptyset \leftrightarrow 1, \{a\} \leftrightarrow 2, \{b\} \leftrightarrow 3, \{a,b\} \leftrightarrow 6$ можемо схватити и као преозначавање елемената једне алгебре елементима друге алгебре, при чему то преозначавање „чува“ и таблице операција: када се садржај сваког поља таблице једне алгебре преозначи на поменути начин, добија се одговарајућа таблица друге алгебре. Изложимо ова запажања мало строже. Наиме, наведена кореспонденција јесте заправо једна бијекција $f : \mathcal{P}(\{a,b\}) \to D_6$,

$$f = \begin{pmatrix} \emptyset & \{a\} & \{b\} & \{a,b\} \\ 1 & 2 & 3 & 6 \end{pmatrix}.$$

Чињеница да се преозначавањем свих поља таблице за $\cup$ добија таблица за nzs, једноставно се описује једнакостима $f(x \cup y) = \mathrm{nzs}(f(x), f(y))$, за све $x, y \in \mathcal{P}(\{a,b\})$.

$$\begin{array}{c|ccc} \cup & \cdots & x & \cdots \\ \hline \vdots & & & \\ y & & x \cup y & \\ \vdots & & & \end{array} \quad \stackrel{f}{\longmapsto} \quad \begin{array}{c|ccc} f \circ \cup & \cdots & f(x) & \cdots \\ \hline \vdots & & & \\ f(y) & & f(x \cup y) & \\ \vdots & & & \end{array} \quad = \quad \begin{array}{c|ccc} \mathrm{nzs} & \cdots & f(x) & \cdots \\ \hline \vdots & & & \\ f(y) & & \mathrm{nzs}(f(x), f(y)) & \\ \vdots & & & \end{array}$$

Аналогно долазимо и до једнакости $f(x \cap y) = \mathrm{nzd}(f(x), f(y))$ и $f(x^c) = n/f(x)$. Из управо наведених разлога, дате Булове алгебре идентификујемо као алгебре „истог облика“, тј. као *изоморфне*[5] алгебре. Функција f назива се *изоморфизам* између ових Булових алгебри. Да ли постоји још неки изоморфизам између наведених Булових алгебри? $\triangleright$

Дефиниција 2. $\mathbf{B}_1 = (B_1, \curlyvee_1, \curlywedge_1, {}'^{1}, 0_1, 1_1)$ *и* $\mathbf{B}_2 = (B_2, \curlyvee_2, \curlywedge_2, {}'^{2}, 0_2, 1_2)$ *су* ***изоморфне*** *Булове алгебре ако постоји бијекција* $f : B_1 \xrightarrow[\text{na}]{\text{1-1}} B_2$ *таква да за све* $x, x_1, x_2 \in B_1$ *важи:*

1. $f(x_1 \curlyvee_1 x_2) = f(x_1) \curlyvee_2 f(x_2)$;
2. $f(x_1 \curlywedge_1 x_2) = f(x_1) \curlywedge_2 f(x_2)$;
3. $f(x'^{1}) = f(x)'^{2}$;
4. $f(0_1) = 0_2$;
5. $f(1_1) = 1_2$.

Бијекција која задовољава набројане особине назива се ***изоморфизам***.

Да су $\mathbf{B}_1$ и $\mathbf{B}_2$ изоморфне, означавамо са $\mathbf{B}_1 \cong \mathbf{B}_2$. Ако желимо да истакнемо да је $f : B_1 \xrightarrow[\text{na}]{\text{1-1}} B_2$ изоморфизам одговарајућих Булових алгебри, пишемо $f : \mathbf{B}_1 \cong \mathbf{B}_2$.

[5] Реч *изоморфан* је грчког порекла: изос = неизмењен, сталан, једнак; морфе = облик.

Пример 8. Нека је U коначан скуп који има k елемената, $k \geqslant 2$ и нека је n производ k међусобно различитих простих бројева. Тада су Булове алгебре $(\mathcal{P}(U), \cup, \cap, {}^{c}, \emptyset, U)$ и $\mathbf{D}_n = (D_n, \mathrm{nzs}, \mathrm{nzd}, n/, 1, n)$ изоморфне. Да бисмо то доказали, потребно је уочити изоморфизам међу њима. Ослањајући се на разматрања из примера 3, није тешко открити функцију која ће бити изоморфизам. Нека је $U = \{u_1, \ldots, u_k\}$ и $n = p_1 \cdots p_k$. Дефинишимо функцију $f : \mathcal{P}(U) \to D_n$, на следећи начин:

$$f(A) = p_1^{\chi_A(u_1)} \cdots p_k^{\chi_A(u_k)},$$

где је $\chi_A : U \to \{0, 1\}$ карактеристична функција скупа $A \in \mathcal{P}(U)$. Остављамо читаоцима да докажу да је f тражени изоморфизам. $\triangleright$

Доказе наредне две теореме препуштамо читаоцима.

Теорема 1. *Ако је* $|U| = |V|$, *онда су Булове алгебре* $(\mathcal{P}(U), \cup, \cap, {}^{c}, \emptyset, U)$ *и* $(\mathcal{P}(V), \cup, \cap, {}^{c}, \emptyset, V)$ *изоморфне.*

Упутство. Ако је $|U| = |V|$, онда постоји бијекција $f : U \xrightarrow[\text{na}]{\text{1-1}} V$. Показати да је функција $F : \mathcal{P}(U) \to \mathcal{P}(V)$, дата са $F(X) = f[X] = \{f(x) \mid x \in X\}$, $X \in \mathcal{P}(U)$, тражени изоморфизам.

Теорема 2. *Нека су* $\mathbf{B}_1$, $\mathbf{B}_2$ *и* $\mathbf{B}_3$ *Булове алгебре. Тада је*

- $\mathbf{B}_1 \cong \mathbf{B}_1$;
- *ако је* $\mathbf{B}_1 \cong \mathbf{B}_2$, *онда је* $\mathbf{B}_2 \cong \mathbf{B}_1$;
- *ако је* $\mathbf{B}_1 \cong \mathbf{B}_2$ *и* $\mathbf{B}_2 \cong \mathbf{B}_3$, *онда је* $\mathbf{B}_1 \cong \mathbf{B}_3$.

Упутство. Докази наведених својстава засновани су на следећим чињеницама:

- идентичко пресликавање[6] је изоморфизам;
- инверзна функција изоморфизма такође је изоморфизам;
- композиција два изоморфизма такође је изоморфизам.

Неколико изведених Булових закона

Иако смо на почетку овог поглавља истакли да операције Булове алгебре имају иста својства као скуповне операције, то се не може директно видети на основу изабраних аксиома будући да су изабрана само нека од својстава скуповних операција. На крају одељка ћемо показати да су аксиоме добро

[6] $\mathrm{id} : B_1 \to B_1, \mathrm{id}(x) = x, x \in B_1$

изабране. За сада ћемо само делимично учврстити ово уверење, доказујући нека додатна својства аналогна добро познатим својствима скуповних операција. Доказаћемо пре свега оне законитости које ће нам у наставку значајно олакшати рачун у Буловим алгебрама.

Лема 1. *Нека је* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *Булова алгебра. За произвољне елементе* x *и* y *из* B *важи:*

$[\mathbf{I}^{\curlyvee}]$	$x \curlyvee x = x,$	$[\mathbf{I}^{\curlywedge}]$	$x \curlywedge x = x,$	[*закони идемпотентности*];
$[\mathbf{1}^{\curlyvee}]$	$x \curlyvee 1 = 1,$	$[\mathbf{0}^{\curlywedge}]$	$x \curlywedge 0 = 0;$	
$[\mathbf{A}^{\curlyvee}_{\curlywedge}]$	$x \curlyvee (x \curlywedge y) = x,$	$[\mathbf{A}^{\curlywedge}_{\curlyvee}]$	$x \curlywedge (x \curlyvee y) = x,$	[*закони апсорпције*].

Доказ.[7]

$$\begin{aligned} & x \curlyvee x \\ = \;& (x \curlyvee x) \curlywedge 1 && [\mathbf{N}^{\curlywedge}] \\ = \;& (x \curlyvee x) \curlywedge (x \curlyvee x') && [\mathbf{C}^{\curlyvee}] \\ = \;& x \curlyvee (x \curlywedge x') && [\mathbf{D}^{\curlyvee}_{\curlywedge}] \\ = \;& x \curlyvee 0 && [\mathbf{C}^{\curlywedge}] \\ = \;& x && [\mathbf{N}^{\curlyvee}] \end{aligned}$$

$$\begin{aligned} & x \curlywedge x \\ = \;& (x \curlywedge x) \curlyvee 0 && [\mathbf{N}^{\curlyvee}] \\ = \;& (x \curlywedge x) \curlyvee (x \curlywedge x') && [\mathbf{C}^{\curlywedge}] \\ = \;& x \curlywedge (x \curlyvee x') && [\mathbf{D}^{\curlywedge}_{\curlyvee}] \\ = \;& x \curlywedge 1 && [\mathbf{C}^{\curlyvee}] \\ = \;& x && [\mathbf{N}^{\curlywedge}] \end{aligned}$$

$$\begin{aligned} x \curlyvee 1 &= x \curlyvee (x \curlyvee x') && [\mathbf{C}^{\curlyvee}] \\ &= (x \curlyvee x) \curlyvee x' && [\mathbf{A}^{\curlyvee}] \\ &= x \curlyvee x' && [\mathbf{I}^{\curlyvee}] \\ &= 1 && [\mathbf{N}^{\curlyvee}] \end{aligned}$$

$$\begin{aligned} x \curlywedge 0 &= x \curlywedge (x \curlywedge x') && [\mathbf{C}^{\curlywedge}] \\ &= (x \curlywedge x) \curlywedge x' && [\mathbf{A}^{\curlywedge}] \\ &= x \curlywedge x' && [\mathbf{I}^{\curlywedge}] \\ &= 0 && [\mathbf{N}^{\curlyvee}] \end{aligned}$$

$$\begin{aligned} & x \curlyvee (x \curlywedge y) \\ = \;& (x \curlywedge 1) \curlyvee (x \curlywedge y) && [\mathbf{N}^{\curlywedge}] \\ = \;& x \curlywedge (1 \curlyvee y) && [\mathbf{D}^{\curlywedge}_{\curlyvee}] \\ = \;& x \curlywedge (y \curlyvee 1) && [\mathbf{K}^{\curlywedge}] \\ = \;& x \curlywedge 1 && [\mathbf{1}^{\curlyvee}] \\ = \;& x && [\mathbf{N}^{\curlywedge}] \end{aligned}$$

$$\begin{aligned} & x \curlywedge (x \curlyvee y) \\ = \;& (x \curlyvee 0) \curlywedge (x \curlyvee y) && [\mathbf{N}^{\curlyvee}] \\ = \;& x \curlyvee (0 \curlywedge y) && [\mathbf{D}^{\curlyvee}_{\curlywedge}] \\ = \;& x \curlyvee (y \curlywedge 0) && [\mathbf{K}^{\curlyvee}] \\ = \;& x \curlyvee 0 && [\mathbf{0}^{\curlywedge}] \\ = \;& x && [\mathbf{N}^{\curlyvee}] \end{aligned}$$

□

Наредна теорема је веома корисна приликом доказивања неких закона Булових алгебри. Она заправо тврди да је комплементирање потпуно одређено законима $\mathbf{C}^{\curlyvee}$ и $\mathbf{C}^{\curlywedge}$.

[7] Ако пажљивије анализирамо идентитете леме 1 и њихове доказе, уочићемо извесне аналогије које су последица такозваног *принципа дуалности.* Наиме, ако у неком Буловом идентитету симболе $\curlyvee$, $\curlywedge$, 0 и 1 заменимо редом симболима $\curlywedge$, $\curlyvee$, 1 и 0, добијамо тзв. *дуални идентитет.* Принцип дуалности каже: ако се неки идентитет може извести из аксиома Булових алгебри, онда се може извести и њему дуални идентитет. Образложење је једноставно: свака аксиома Булове алгебре има свој дуал, па ако у доказу неког идентитета, свако позивање на неку аксиому заменимо позивањем на дулану аксиому, добијамо доказ дуалног идентитета.

Теорема 3. [***Теорема о јединствености комплемента***] *Нека је* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *Булова алгебра и* x *и* y *произвољни елементи из* B. *Ако је* $x \curlyvee y = 1$ *и* $x \curlywedge y = 0$, *онда је* $y = x'$.

Доказ. Нека је (1) $x \curlyvee y = 1$ и (2) $x \curlywedge y = 0$.

$$\begin{array}{rcll}
x' & = & x' \curlywedge 1 & [\mathbf{N}^{\curlywedge}] \\
 & = & x' \curlywedge (x \curlyvee y) & [(1)] \\
 & = & (x' \curlywedge x) \curlyvee (x' \curlywedge y) & [\mathbf{D}^{\curlywedge}_{\curlyvee}] \\
 & = & (x \curlywedge x') \curlyvee (x' \curlywedge y) & [\mathbf{K}^{\curlywedge}] \\
 & = & 0 \curlyvee (x' \curlywedge y) & [\mathbf{C}^{\curlywedge}] \\
 & = & (x' \curlywedge y) \curlyvee 0 & [\mathbf{K}^{\curlyvee}] \\
 & = & x' \curlywedge y & [\mathbf{N}^{\curlyvee}]
\end{array}$$

$$\begin{array}{rcll}
y & = & y \curlywedge 1 & [\mathbf{N}^{\curlywedge}] \\
 & = & y \curlywedge (x \curlyvee x') & [\mathbf{C}^{\curlyvee}] \\
 & = & (y \curlywedge x) \curlyvee (y \curlywedge x') & [\mathbf{D}^{\curlywedge}_{\curlyvee}] \\
 & = & (x \curlywedge y) \curlyvee (y \curlywedge x') & [\mathbf{K}^{\curlywedge}] \\
 & = & 0 \curlyvee (y \curlywedge x') & [(2)] \\
 & = & (y \curlyvee x') \curlyvee 0 & [\mathbf{K}^{\curlyvee}] \\
 & = & y \curlywedge x' & [\mathbf{N}^{\curlyvee}] \\
 & = & x' \curlywedge y & [\mathbf{K}^{\curlywedge}]
\end{array}$$

Из доказаних једнакости закључујемо да је $x' = y$. □

Лема 2. *Нека је* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *Булова алгебра. За произвољне елементе* x *и* y *из* B *важи:*

1. $(x')' = x$ [*закони инволуције*];
2. $0' = 1$, $1' = 0$;
3. $(x \curlyvee y)' = x' \curlywedge y'$, $(x \curlywedge y)' = x' \curlyvee y'$ [*Де Морганови закони*].

Доказ. Сви наведени закони су једноставне последице претходне теореме. Као илустрацију наводимо доказ Де Моргановог закона $(x \curlyvee y)' = x' \curlywedge y'$. Према теореми о јединствености комплемента довољно је доказати да за произвољне x и y из B важе једнакости

$$(x \curlyvee y) \curlyvee (x' \curlywedge y') = 1 \text{ и } (x \curlyvee y) \curlywedge (x' \curlywedge y') = 0.$$

Навешћемо само основне кораке доказа ових једнакости:

$$\begin{array}{rl}
 & (x \curlyvee y) \curlyvee (x' \curlywedge y') \\
= & ((x \curlyvee y) \curlyvee x') \curlywedge ((x \curlyvee y) \curlyvee y') \\
 & \vdots \\
= & (y \curlyvee (x \curlyvee x')) \curlywedge (x \curlyvee (y \curlyvee y')) \\
= & (y \curlyvee 1) \curlywedge (x \curlyvee 1) \\
= & 1 \curlywedge 1 \\
= & 1
\end{array}$$

$$\begin{array}{rl}
 & (x \curlyvee y) \curlywedge (x' \curlywedge y') \\
= & (x \curlywedge (x' \curlywedge y')) \curlyvee (y \curlywedge (x' \curlywedge y')) \\
 & \vdots \\
= & (y' \curlywedge (x \curlywedge x')) \curlyvee (x' \curlywedge (y \curlywedge y')) \\
= & (y' \curlywedge 0) \curlyvee (x' \curlywedge 0) \\
= & 0 \curlyvee 0 \\
= & 0
\end{array}$$

□

На основу доказаних идентитета, издвајамо два важна запажања. Прво, рачун са константама 0 и 1 исти је у свакој Буловој алгебри и обавља се у складу са таблицама[8] алгебре **2** наведеним у примеру 1. Друго запажање се односи на примену Де Морганових закона. Наиме, Де Морганов закон је веома користан идентитет којим је успостављена веза међу свим операцијама неке Булове алгебре. Као илустрацију његове примене, показујемо да је бијекција $f : B_1 \overset{\text{1-1}}{\underset{\text{na}}{\rightarrow}} B_2$ изоморфизам Булових алгебри $\mathbf{B}_1 = (B_1, \curlyvee_1, \curlywedge_1, {}'^1, 0_1, 1_1)$ и $\mathbf{B}_2 = (B_2, \curlyvee_2, \curlywedge_2, {}'^2, 0_2, 1_2)$ уколико задовољава услове 1 и 3 дефиниције 2, јер су преостали услови последице ова два:
$f(x_1 \curlywedge_1 x_2) = f\left((x_1'^1 \curlyvee_1 x_2'^1)'^1\right) = (f(x_1)'^2 \curlyvee_2 f(x_2)'^2)'^2 = f(x_1) \curlywedge_2 f(x_2)$;
$f(0_1) = f(x \curlywedge_1 x'^1) = f(x) \curlywedge_2 f(x)'^2 = 0_2$;
$f(1_1) = f(x \curlyvee_1 x'^1) = f(x) \curlyvee_2 f(x)'^2 = 1_2$.
Аналогно се показује да је бијекција $f : B_1 \overset{\text{1-1}}{\underset{\text{na}}{\rightarrow}} B_2$ изоморфизам уколико важе услови 2 и 3 дефиниције 2.

Лема 3. *Нека су* $\mathbf{B}_1 = (B_1, \curlyvee_1, \curlywedge_1, {}'^1, 0_1, 1_1)$ *и* $\mathbf{B}_2 = (B_2, \curlyvee_2, \curlywedge_2, {}'^2, 0_2, 1_2)$ *Булове алгебре. Бијекција* $f : B_1 \overset{\text{1-1}}{\underset{\text{na}}{\rightarrow}} B_2$ *је изоморфизам Булових алгебри* $\mathbf{B}_1$ *и* $\mathbf{B}_2$ *уколико за све* $x, x_1, x_2 \in B_1$ *важи:*

1. $f(x_1 \curlyvee_1 x_2) = f(x_1) \curlyvee_2 f(x_2)$;

2. $f(x'^1) = f(x)'^2$.

Да бисмо једноставније формулисали још једно корисно тврђење, уводимо следеће ознаке: нека x^0 означава x', а x^1 означава x. Поред тога, користићемо уобичајени начин краћег записивања израза $x_1 \curlyvee \cdots \curlyvee x_k$ и $x_1 \curlywedge \cdots \curlywedge x_k$ редом записима $\bigvee\limits_{i=1}^{k} x_i$ и $\bigwedge\limits_{i=1}^{k} x_i$, при чему изостављамо заграде имајући на уму асоцијативност одговарајућих операција.

Лема 4. *Нека је* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *произвољна Булова алгебра. Тада за свако* $n \geqslant 1$ *и произвољне* $x_1, \ldots, x_n \in B$ *важи:*

$$\bigvee_{(a_1,\ldots,a_n)\in 2^n} (x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) = 1.$$

Доказ. Доказ изводимо индукцијом по n.

Ако је $n = 1$, онда је $\bigvee_{a\in 2} x^a = x^0 \curlyvee x^1 = x' \curlyvee x = 1$.

[8]Таблице можемо извести из аксиома $\mathbf{K}^{\curlyvee}$, $\mathbf{K}^{\curlywedge}$, $\mathbf{N}^{\curlyvee}$, $\mathbf{N}^{\curlywedge}$, једнакости $[\mathbf{1}^{\curlyvee}]$, $[\mathbf{0}^{\curlywedge}]$ (лема 1) и једнакости $0' = 1$, $1' = 0$ (лема 2).

Доказ завршавамо следећим низом једнакости, при чему полазимо од једнакости која заправо представља индуктивну претпоставку. Поред тога, користимо и очигледну последицу дистрибутивности: $\left(\bigvee_{i=1}^{k} x_i\right) \curlywedge x = \bigvee_{i=1}^{k} (x_i \curlywedge x)$.

$$
\begin{aligned}
1 &= \bigvee_{(a_1,\ldots,a_n)\in 2^n} (x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) \\
&= \left(\bigvee_{(a_1,\ldots,a_n)\in 2^n} (x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n})\right) \curlywedge (x_{n+1}^0 \curlyvee x_{n+1}^1) \\
&= \bigvee_{(a_1,\ldots,a_n)\in 2^n} \left(x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n} \curlywedge x_{n+1}^0\right) \curlyvee \bigvee_{(a_1,\ldots,a_n)\in 2^n} \left(x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n} \curlywedge x_{n+1}^1\right) \\
&= \bigvee_{(a_1,\ldots,a_n,a_{n+1})\in 2^{n+1}} \left(x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n} \curlywedge x_{n+1}^{a_{n+1}}\right)
\end{aligned}
$$

□

Одељак завршавамо тврђењем које даје својеврсну алгебарску карактеризацију једнакости у Буловим алгебрама.

Лема 5. *Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра. Тада за произвољне $x, y \in B$ важи: $x = y$ акко $(x \curlywedge y) \curlyvee (x' \curlywedge y') = 1$.*

Доказ. ($\rightarrow$) Ако је $x = y$, онда је

$$(x \curlywedge y) \curlyvee (x' \curlywedge y') = (x \curlywedge x) \curlyvee (x' \curlywedge x') = x \curlyvee x' = 1.$$

($\leftarrow$) Претпоставимо да је $(x \curlywedge y) \curlyvee (x' \curlywedge y') = 1$. Тада је

$$
\begin{aligned}
x &= x \curlywedge 1 \\
&= x \curlywedge [(x \curlywedge y) \curlyvee (x' \curlywedge y')] \\
&= (x \curlywedge x \curlywedge y) \curlyvee (x \curlywedge x' \curlywedge y') \\
&= (x \curlywedge y) \curlyvee 0 \\
&= x \curlywedge y
\end{aligned}
\qquad
\begin{aligned}
y &= y \curlywedge 1 \\
&= y \curlywedge [(x \curlywedge y) \curlyvee (x' \curlywedge y')] \\
&= (y \curlywedge x \curlywedge y) \curlyvee (y \curlywedge x' \curlywedge y') \\
&= (x \curlywedge y) \curlyvee 0 \\
&= x \curlywedge y
\end{aligned}
$$

одакле следи да је $x = y$. □

Булови изрази и логички везници

Уопштено говорећи, Булове функције јесу функције дефинисане алгебарским изразима својственим Буловим алгебрама. Иако ћемо се касније детаљније, строже и уопштеније бавити алгебарским изразима, сматрамо да ће бити вишеструко корисно (и за проучавање Булових алгебри и за садржаје наредних поглавља) понешто прецизирати на овом месту. Прецизирајмо најпре појам израза у контексту Булових алгебри, тј. појам *Буловог израза*. Булове изразе градимо као и било коју другу врсту израза: помоћу променљивих, константи (0 и 1) и одговарајућих операција ($\curlyvee$, $\curlywedge$ и $'$), користећи при томе заграде када је потребно. Иако су изрази записани помоћу коначно много поменутих симбола, не желимо да ограничимо број различитих променљивих које се могу појављивати у неком изразу, па зато претпостављамо да нам је на располагању пребројиво много променљивих. Променљиве ћемо означавати малим словима латинице, са или без индекса: $x, y, z, x_1, y_1, z_1, x_2, \ldots$ Булове изразе градимо применом наредних правила коначан број пута[9]:

- свака променљива, као и константа 0 и 1 јесте један Булов израз;
- ако је α Булов израз, онда је и α' Булов израз;
- ако су α и β Булови изрази, онда су и $(\alpha \curlyvee \beta)$ и $(\alpha \curlywedge \beta)$ Булови изрази.

Наводимо неколико примера Булових израза:

$$x, (x \curlywedge 0), x', (1 \curlywedge 0)', ((x \curlyvee y')' \curlywedge z), \ldots$$ [10]

Булове изразе означаваћемо малим грчким словима: α, β, γ, ... Запис $\alpha(x_1, \ldots, x_n)$ користимо када желимо да истакнемо да су све променљиве које се појављују у изразу α неке од променљивих $x_1, \ldots, x_n$. Вредност неког Буловог израза можемо одредити у било којој Буловој алгебри $\mathbf{B}$ ако знаке $\curlyvee$, $\curlywedge$, $'$, 0 и 1 интерпретирамо одговарајућим операцијама, односно константама из $\mathbf{B}$ и ако променљивама доделимо неке вредности из домена те Булове алгебре. Вредност израза $\alpha(x_1, \ldots, x_n)$ у Буловој алгебри $\mathbf{B}$ када се променљивама $x_1, \ldots, x_n$ редом доделе вредности $a_1, \ldots, a_n \in \mathbf{B}$ означавамо са $\alpha^{\mathbf{B}}(a_1, \ldots, a_n)$, при чему ћемо изостављати горњи индекс када се подразумева о којој Буловој алгебри $\mathbf{B}$ је реч.

Пример 9. У наредној табели израчунате су вредности Буловог израза $x' \curlyvee y$ у неким конкретним Буловим алгебрама, за конкретне вредности променљивих.

[9] Дефиниција Буливих израза је индуктивна: најпре су одређени најједноставнији Булови изрази (променљиве и константе су Булови изрази), а затим је описано како се формирају сложенији Булови изрази. Тако, полазећи од најједноставнијих Булових израза помоћу ових правила градимо нове изразе, које даље користимо за изградњу још сложенијих израза.

[10] Потреба за заградама приликом записивања израза је позната. Међутим, да би се поједноставило записивање, уобичајено је да се усвајају разне конвенције о брисању сувишних заграда (тј. оних чије изостављање не утиче на читљивост израза). Ми ове конвенције нећемо наводити, јер ће их читалац свакако уочити у наставку текста.

	$(\mathcal{P}(\{a,b\}), \cup, \cap, ^c, \emptyset, \{a,b\})$	$\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$	$(D_6, \mathrm{nzs}, \mathrm{nzd}, 6/, 1, 6)$	$\cdots$
	$x^c \cup y$	$\neg x \vee y$	$\mathrm{nzs}\left(\frac{n}{x}, y\right)$	$\cdots$
	$x = \{a\}, y = \{b\}$	$x = 0, y = 0$	$x = 2, y = 6$	$\cdots$
	$x^c \cup y = \{b\}$	$\neg x \vee y = 1$	$\mathrm{nzs}\left(\frac{n}{x}, y\right) = 6$	$\cdots$
	$x = \{b\}, y = \{a,b\}$	$x = 1, y = 0$	$x = 3, y = 1$	$\cdots$
	$x^c \cup y = \{a,b\}$	$\neg x \vee y = 0$	$\mathrm{nzs}\left(\frac{n}{x}, y\right) = 3$	$\cdots$

$\triangleright$

Булови закони (идентитети), од који су неки узети за аксиоме, а неки су из њих изведени, јесу заправо једнакости два Булова израза које су увек тачне, коју год Булову алгебру да изаберемо и које год елементе из те алгебре да доделимо променљивама. У наредним тврђењима доказаћемо неке опште резултате који се односе на Булове законе. Пре тога уводимо неколико ознака.

Нека је α било који Булов израз и x променљива. Означимо са $\alpha(x/0)$ (односно $\alpha(x/1)$) израз који се добија из α када сва појављивања променљиве x заменимо константом 0 (односно 1). Очигледно је да уколико се променљива x не појављује у изразу α, онда је $\alpha(x/0) = \alpha(x/1) = \alpha$.

Лема 6. *Ако је α било који Булов израз, онда једнакост*

$$\alpha = (\alpha(x/0) \curlywedge x') \curlyvee (\alpha(x/1) \curlywedge x)$$

важи у било којој Буловој алгебри.

Доказ. Доказ спроводимо индукцијом по сложености израза, што значи да ћемо најпре доказати да тврђење важи за најједноставније Булове изразе (променљиве и константе), а затим да важи и за сложеније, под претпоставком да је тачно за изразе од којих је тај израз састављен.

Ако је α променљива различита од x, или константа 0 или 1, онда је $\alpha(x/0) = \alpha(x/1) = \alpha$, па важи:

$$(\alpha(x/0) \curlywedge x') \curlyvee (\alpha(x/1) \curlywedge x) = (\alpha \curlywedge x') \curlyvee (\alpha \curlywedge x) = \alpha \curlywedge (x \curlyvee x') = \alpha \curlywedge 1 = \alpha.$$

Ако је α променљива x, онда је $\alpha(x/0) = 0$ и $\alpha(x/1) = 1$, па је

$$(\alpha(x/0) \curlywedge x') \curlyvee (\alpha(x/1) \curlywedge x) = (0 \curlywedge x') \curlyvee (1 \curlywedge x) = 0 \curlyvee x = x = \alpha.$$

Нека је α облика θ'. Према индуктивној претпоставци тврђење важи за θ па је $\theta = (\theta(x/0) \curlywedge x') \curlyvee (\theta(x/1) \curlywedge x)$, одакле добијамо:

$$
\begin{aligned}
\alpha &= \theta' = \big((\theta(x/0) \curlywedge x') \curlyvee (\theta(x/1) \curlywedge x)\big)' \\
&= (\theta(x/0)' \curlyvee x) \curlywedge (\theta(x/1)' \curlyvee x') \\
&= \big(\theta(x/0)' \curlywedge \theta(x/1)'\big) \curlyvee \big(\theta(x/0)' \curlywedge x'\big) \curlyvee \big(\theta(x/1)' \curlywedge x\big) \curlyvee \big(x \curlywedge x'\big) \\
&= \big(\theta(x/0)' \curlywedge \theta(x/1)' \curlywedge (x \curlyvee x')\big) \curlyvee \big(\theta(x/0)' \curlywedge x'\big) \curlyvee \big(\theta(x/1)' \curlywedge x\big) \\
&= \big(\theta(x/0)' \curlywedge \theta(x/1)' \curlywedge x\big) \curlyvee \big(\theta(x/0)' \curlywedge \theta(x/1)' \curlywedge x'\big) \curlyvee \\
&\qquad \curlyvee \big(\theta(x/0)' \curlywedge x'\big) \curlyvee \big(\theta(x/1)' \curlywedge x\big) \\
&= (\theta(x/0)' \curlywedge x') \curlyvee (\theta(x/1)' \curlywedge x) \\
&= (\theta'(x/0) \curlywedge x') \curlyvee (\theta'(x/1) \curlywedge x) \\
&= (\alpha(x/0) \curlywedge x') \curlyvee (\alpha(x/1) \curlywedge x).
\end{aligned}
$$

Нека је α облика $\theta_1 \curlyvee \theta_2$. Према индуктивној претпоставци тврђење важи за θ_i, па је $\theta_i = (\theta_i(x/0) \curlywedge x') \curlyvee (\theta_i(x/1) \curlywedge x)$, $i = 1, 2$. Одавде добијамо:

$$
\begin{aligned}
\alpha &= \theta_1 \curlyvee \theta_2 \\
&= (\theta_1(x/0) \curlywedge x') \curlyvee (\theta_1(x/1) \curlywedge x) \curlyvee (\theta_2(x/0) \curlywedge x') \curlyvee (\theta_2(x/1) \curlywedge x) \\
&= \big((\theta_1(x/0) \curlyvee \theta_2(x/0)) \curlywedge x'\big) \curlyvee ((\theta_1(x/1) \curlyvee \theta_2(x/1)) \curlywedge x) \\
&= \big((\theta_1 \curlyvee \theta_2)(x/0) \curlywedge x'\big) \curlyvee ((\theta_1 \curlyvee \theta_2)(x/1) \curlywedge x) \\
&= \big(\alpha(x/0) \curlywedge x'\big) \curlyvee (\alpha(x/1) \curlywedge x)\,.
\end{aligned}
$$

Случај када је α облика $\theta_1 \curlywedge \theta_2$, препуштамо читаоцима. □

Из претходне леме изводимо веома важну теорему познату као *теорема о канонској дисјунктивној нормалној форми.*

Теорема 4. *Ако је $\alpha(x_1, \ldots, x_n)$ Булов израз, онда једнакост*

$$
(KDNF) \qquad \alpha(x_1, \ldots, x_n) = \bigvee_{(a_1,\ldots,a_n)\in 2^n} (\alpha(a_1, \ldots, a_n) \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n})
$$

важи у свакој Буловој алгебри.

Доказ. Доказ изводимо индукцијом по n. Случај $n = 1$ непосредна је последица претходне леме. Претпоставимо да је тврђење тачно за изразе са n променљивих.

$$
\begin{aligned}
& \alpha(x_1, \ldots, x_n, x_{n+1}) \\
= \ & \left(\alpha(x_1, \ldots, x_n, 0) \curlywedge x_{n+1}^0\right) \curlyvee \left(\alpha(x_1, \ldots, x_n, 1) \curlywedge x_{n+1}^1\right) \\
= \ & \left(\bigvee_{(a_1,\ldots,a_n)\in 2^n} (\alpha(a_1, \ldots, a_n, 0) \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) \curlywedge x_{n+1}^0 \right) \curlyvee \\
& \quad \curlyvee \left(\bigvee_{(a_1,\ldots,a_n)\in 2^n} (\alpha(a_1, \ldots, a_n, 1) \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) \curlywedge x_{n+1}^1 \right) \\
= \ & \bigvee_{(a_1,\ldots,a_n,a_{n+1})\in 2^{n+1}} \left(\alpha(a_1, \ldots, a_n, a_{n+1}) \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n} \curlywedge x_{n+1}^{a_{n+1}}\right)
\end{aligned}
$$

□

Израз са десне стране једнакости из претходне теореме назива се *канонска дисјунктивна нормална форма* израза $\alpha(x_1, \ldots, x_n)$. Имајући на уму управо доказану једнакост, закључујемо да је сваки Булов израз суштински одређен својим вредностима на скупу $\{0, 1\}$. Подсећамо да је небитно из које Булове алгебре долазе константе 0 и 1, јер је рачун са њима увек исти и обавља се у складу са таблицама операција алгебре $\mathbf{2}$. Овај закључак истиче централну улогу алгебре $\mathbf{2}$ у теорији Булових алгебри, бар када су у питању Булови закони.

Теорема 5. *Нека су α и β произвољни Булови изрази. Закон $\alpha = \beta$ важи у свакој Буловој алгебри акко важи у Буловој алгебри $\mathbf{2}$.*

Доказ. На основу леме 5, уместо једнакости $\alpha = \beta$ можемо посматрати $(\alpha \curlywedge \beta) \curlyvee (\alpha' \curlywedge \beta') = 1$. Другим речима, доказаћемо да за сваки Булов израз θ, закон $\theta = 1$ важи у свакој Буловој алгебри акко важи у Буловој алгебри $\mathbf{2}$.
($\rightarrow$) Тривијално.
($\leftarrow$) Претпоставимо да $\theta = 1$ важи у Буловој алгебри $\mathbf{2}$. Нека су све променљиве које се појављују у изразу θ неке од променљивих $x_1, \ldots, x_n$. Тада за све $(a_1, \ldots, a_n) \in 2^n$, важи $\theta(a_1, \ldots, a_n) = 1$. Ако узмемо у обзир канонску дисјунктивну нормалну форму израза θ, закључујемо да је

$$
\begin{aligned}
\theta(x_1, \ldots, x_n) &= \bigvee_{(a_1,\ldots,a_n)\in 2^n} (\theta(a_1, \ldots, a_n) \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) \\
&= \bigvee_{(a_1,\ldots,a_n)\in 2^n} (1 \curlywedge x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) \\
&= \bigvee_{(a_1,\ldots,a_n)\in 2^n} (x_1^{a_1} \curlywedge \cdots \curlywedge x_n^{a_n}) = 1
\end{aligned}
$$

Последња једнакост доказана је у леми 4. □

Пример 10. Према претходној теореми, да бисмо доказали да у свакој Буловој алгебри важи закон $x \curlyvee (y' \curlywedge (y' \curlyvee x)) = (x' \curlywedge y)'$, довољно је проверити да ли он важи у алгебри $\mathbf{2}$.

x	y	y'	$y' \curlyvee x$	$y' \curlywedge (y' \curlyvee x)$	$x \curlyvee (y' \curlywedge (y' \curlyvee x))$	x'	$x' \curlywedge y$	$(x' \curlywedge y)'$
0	0	1	1	1	1	1	0	1
0	1	0	0	0	0	1	1	0
1	0	1	1	1	1	0	0	1
1	1	0	1	0	1	0	0	1

Упоређујући резултате у одговарајућим колонама, закључујемо да наведени закон важи у Буловој алгебри $\mathbf{2}$. ▷

Теорема 4 има још доста значајних последица. Издвајамо неке од њих. Ако је $\mathbf{B}$ било која Булова алгебра, онда сваки Булов израз $\alpha(x_1, \ldots, x_n)$ одређује једну функцију из B^n у B, односно једну n-арну операцију скупа B: $B^n \ni (a_1, \ldots, a_n) \mapsto \alpha^{\mathbf{B}}(x_1, \ldots, x_n) \in B$. Оваквих функција укупно има 2^{2^n}, јер толико има n-арних операција на скупу $\{0, 1\}$. На пример, ако је $\alpha(x_1, x_2)$ неки Булов израз са две променљиве, онда се функција $(x_1, x_2) \mapsto \alpha^{\mathbf{B}}(x_1, x_2)$, може приказати у следећем облику:

$$\alpha^{\mathbf{B}}(x_1, x_2) = (f(0,0) \curlywedge x_1' \curlywedge x_2') \curlyvee (f(0,1) \curlywedge x_1' \curlywedge x_2) \curlyvee$$
$$\curlyvee (f(1,0) \curlywedge x_1 \curlywedge x_2') \curlyvee (f(1,1) \curlywedge x_1 \curlywedge x_2),$$

где је f једна од следећих 16 бинарних операција скупа $\{0, 1\}$ (ознаке у наредним табелама објаснићемо у примеру 12).

	0	1
0	0	0
1	0	0

$\wedge$	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

	0	1
0	0	1
1	0	0

$\downarrow$	0	1
0	1	0
1	0	0

	0	1
0	0	0
1	1	1

	0	1
0	0	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

$\veebar$	0	1
0	0	1
1	1	0

	0	1
0	1	0
1	1	0

	0	1
0	1	1
1	0	0

$\uparrow$	0	1
0	1	1
1	1	0

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftarrow$	0	1
0	1	0
1	1	1

	0	1
0	0	1
1	1	1

	0	1
0	1	1
1	1	1

Из претходних разматрања закључујемо да посебно значајно место заузимају функције $\alpha^{\mathbf{2}} : 2^n \to 2$, $2^n \ni (x_1, \ldots, x_n) \mapsto \alpha^{\mathbf{2}}(x_1, \ldots, x_n) \in 2$. Свака оваква функција назива се *истинитосна функција* или *n-арни логички везник*. Очигледно, свака функција $f : 2^n \to 2$ се може схватити као један n-арни логички везник, јер постоји Булов израз $\alpha(x_1, \ldots, x_n)$ такав да је $f(x_1, \ldots, x_n) = \alpha^{\mathbf{2}}(x_1, \ldots, x_n)$, за све $x_1, \ldots, x_n \in 2$.

Пример 11. Нека је $f : 2^3 \to 2$, функција (дужине три) дата следећом табелом.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Уочавајући за које вредности аргумената функција f има вредност 1 једноставно налазимо Булов израз $\alpha(x_1, x_2, x_3)$ који одређује ову функцију:

$$\alpha(x_1, x_2, x_3) = (x_1' \curlywedge x_2' \curlywedge x_3) \curlyvee (x_1' \curlywedge x_2 \curlywedge x_3) \curlyvee (x_1 \curlywedge x_2 \curlywedge x_3') \curlyvee (x_1 \curlywedge x_2 \curlywedge x_3).$$

Сређивањем израза са десне стране, добијамо да је

$$\alpha(x_1, x_2, x_3) = (x_1 \curlywedge x_2) \curlyvee (x_1' \curlywedge x_3).$$

Овај Булов израз одређује један важан тернарни везник: **if** x_1 **then** x_2 **else** x_3. $\triangleright$

Пример 12. Наводећи таблице за свих шеснаест бинарних логичких везника, посебним знацима су означени само неки од њих. Поред конјункције ($\wedge$) и дисјункције ($\vee$), истакнути су и следећи везници:

- $\downarrow$ – *нили*, *Лукашијевичева стрелица* (ни $\cdots$ ни $***$);
- $\Leftrightarrow$ – *еквиваленција* ($\cdots$ ако и само ако $***$);
- $\veebar$ – *искључна дисјункција* (или $\cdots$ или $***$, али не оба);
- $\uparrow$ – *ни*, *Шеферова стрелица* (није $\cdots$ или није $***$);
- $\Rightarrow$ – *импликација* (ако $\cdots$, онда $***$; $\cdots$ је довољан услов за $***$);
- $\Leftarrow$ – *обратна импликација* ($\cdots$ ако $***$; $\cdots$ је потребан услов за $***$).

Ови бинарни везници су издвојени због свог значаја у исказној логици, о чему ћемо датаљније писати у наредном поглављу. $\triangleright$

Уређење Булове алгебре

За било који скуп U, инклузија је једно уређење скупа $\mathcal{P}(U)$. Није тешко показати да за произвољне $X, Y \in \mathcal{P}(U)$ важи:

$$X \subseteq Y \text{ акко } X \cup Y = Y \text{ акко } X \cap Y = X.$$

Наведене еквиваленције указују на то како се може дефинисати уређење било које Булове алгебре. Пре него што га дефинишемо, доказаћемо да важи тврђење аналогно другој еквиваленцији.

Лема 7. *Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра. За произвољне елементе x и y из B важи: $x \curlyvee y = y$ акко $x \curlywedge y = x$.*

Доказ. $(\rightarrow)$ Ако је $x \curlyvee y = y$, онда је $x \curlywedge y = x \curlywedge (x \curlyvee y) = x$, при чему последња једнакост важи на основу закона апсорпције.
$(\leftarrow)$ Обрнуто доказујемо потпуно аналогно: ако је $x \curlywedge y = x$, онда је $x \curlyvee y = (x \curlywedge y) \curlyvee y = y$. $\square$

Ако је $(B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра, бинарну релацију $\preccurlyeq$ на B дефинишемо на следећи начин: $x \preccurlyeq y$ акко $x \curlyvee y = y$. При томе, према претходној леми, имамо на уму да је:

$$x \preccurlyeq y \text{ акко } x \curlyvee y = y \text{ акко } x \curlywedge y = x.$$

Лема 8. *Релација $\preccurlyeq$ је релација поретка (уређење) домена Булове алгебре.*

Доказ. (Рефлексивност) За било који елемент x из B важи $x \curlyvee x = x$, тј. $x \preccurlyeq x$.
(Антисиметричност) Претпоставимо да је $x \preccurlyeq y$ и $y \preccurlyeq x$. Тада је $x \curlyvee y = y$ (јер је $x \preccurlyeq y$) и $y \curlyvee x = x$ (јер је $y \preccurlyeq x$), одакле следи $x = y$ због $(\mathrm{K}^{\curlyvee})$.
(Транзитивност) Нека је $x \preccurlyeq y$ и $y \preccurlyeq z$, тј. $x \curlyvee y = y$ и $y \curlyvee z = z$. Тада је: $x \curlyvee z = x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z = y \curlyvee z = z$, тј. $x \preccurlyeq z$. $\square$

Строго уређење одређено релацијом $\preccurlyeq$ означаваћемо са $\prec$.

Лема 9. *У Буловој алгебри $(B, \curlyvee, \curlywedge, ', 0, 1)$, елемент 0 је најмањи, а 1 највећи у односу на $\preccurlyeq$.*

Доказ. За свако $x \in B$ важи: $x \curlyvee 0 = x$, тј. $0 \preccurlyeq x$, и $x \curlyvee 1 = 1$, тј. $x \preccurlyeq 1$. $\square$

Лема 10. *Ако је $(B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра, за било које елементе x, y и z из B важи:*

1.1. $x \preccurlyeq x \curlyvee y$ и $y \preccurlyeq x \curlyvee y$;

1.2. ако је $x \preccurlyeq z$ и $y \preccurlyeq z$, онда је $x \curlyvee y \preccurlyeq z$;

2.1. $x \curlywedge y \preccurlyeq x$ и $x \curlywedge y \preccurlyeq y$;

2.2. ако је $z \preccurlyeq x$ и $z \preccurlyeq y$, онда је $z \preccurlyeq x \curlywedge y$.

Доказ. 1.1. Из једнакости $x \curlyvee (x \curlyvee y) = (x \curlyvee x) \curlyvee y = x \curlyvee y$, следи да је $x \preccurlyeq x \curlyvee y$. Аналогно се доказује да је $y \preccurlyeq x \curlyvee y$.
1.2. Нека је $x \preccurlyeq z$ и $y \preccurlyeq z$, тј. $x \curlyvee z = z$ и $y \curlyvee z = z$. Тада је $(x \curlyvee y) \curlyvee z = x \curlyvee (y \curlyvee z) = x \curlyvee z = z$, односно $x \curlyvee y \preccurlyeq z$.
Тврђења 2.1 и 2.2 аналогно се доказују и доказе препуштамо читаоцима. $\square$

Тврђење 1.1 претходне леме каже да је $x \curlyvee y$ горње ограничење скупа $\{x, y\}$ у односу на $\preccurlyeq$, док 2.1 тврди да је $x \curlyvee y$ и најмање горње ограничење. Другим речима, $x \curlyvee y$ је *супремум* (најмање горње ограничење) скупа $\{x, y\}$, $x \curlyvee y = \sup\{x, y\}$. Аналогно томе, према 2.1 и 2.2, $x \curlywedge y$ је *инфимум* (највеће доње ограничење) скупа $\{x, y\}$, $x \curlywedge y = \inf\{x, y\}$.

Атоми Булове алгебре и репрезентација коначних Булових алгебри

У било којој алгебри партитивног скупа $(\mathcal{P}(U), \cup, \cap, {}^c, \emptyset, U)$, једночлани скупови, тј. синглтони $\{u\}$, $u \in U$, јесу минимални елементи скупа $\mathcal{P}(U) \setminus \{\emptyset\}$ у односу на инклузију, и као такви поседују низ карактеристичних особина. Штавише, они представљају и својеврсни „градивни материјал“ од кога су „састављени“ сви други елементи из $\mathcal{P}(U) \setminus \{\emptyset\}$. Ово запажање донекле поткрепљује чињеница да синглтони репрезентују елементе скупа U, односно да је $\{u\} \subseteq X$ акко $u \in X$, за било које $u \in U$ и било које $X \in \mathcal{P}(U) \setminus \{\emptyset\}$. У произвољној Буловој алгебри сличну улогу имаће тзв. *атоми*, наравно уколико их разматрана алгебра уопште има.

Дефиниција 3. *Елемент a је* ***атом*** *Булове алгебре $\mathbf{B}$, ако је $0 \prec a$ и не постоји елемент $x \in B \setminus \{0\}$ такав да је $x \prec a$. Другим речима, атом је сваки минимални елемент скупа $B \setminus \{0\}$ у односу на $\preccurlyeq$.*

ПРИМЕР 13. Атоми Булове алгебре $(\mathcal{P}(U), \cup, \cap, {}^c, \emptyset, U)$ јесу синглтони $\{u\}$, $u \in U$.

Постоје и Булове алгебре које немају атома. У примеру 4 навели смо да коначне уније лево-полузатворених интервала скупа $\mathbb{R}$ образују једно поље скупова. Ова Булова алгебра нема атома, јер за сваки лево-полузатворени интервал, постоји други такав интевал који је строго садржан у првом. $\triangleright$

У наредној леми издвајамо неке значајне особине атома.

Лема 11. *Нека је $\mathbf{B} = (B, \curlyvee, \curlywedge, {}', 0, 1)$ Булова алгебра и a било који њен атом.*

1. *За сваки елемент $x \in B$ важи $a \curlywedge x = 0$ или $a \curlywedge x = a$. Специјално, ако је a_1 атом у $\mathbf{B}$ различит од a, онда је $a \curlywedge a_1 = 0$.*

2. *Ако је $a \preccurlyeq x_1 \curlyvee x_2 \curlyvee \cdots \curlyvee x_n$, за неке $x_1, x_2, \ldots, x_n \in B$, онда постоји $k \in \{1, \ldots, n\}$ такав да је $a \preccurlyeq x_k$. Специјално, за сваки елемент $x \in B$ важи $a \preccurlyeq x$ или $a \preccurlyeq x'$, али не оба.*

ДОКАЗ. 1. За било који елемент x важи $0 \preccurlyeq a \curlywedge x \preccurlyeq a$, одакле следи да је $a \curlywedge x = 0$ или $a \curlywedge x = a$, јер је a атом, па не може бити $0 \prec a \curlywedge x \prec a$. Нека су a и a_1 различити атоми. Како је a атом, према управо доказаном имамо да је $a \curlywedge a_1 = 0$ или $a \curlywedge a_1 = a$. Пошто је и a_1 атом, добијамо и да је $a \curlywedge a_1 = 0$

или $a \curlywedge a_1 = a_1$. Како је $a \neq 0$, $a_1 \neq 0$ и $a \neq a_1$, закључујемо да мора бити $a \curlywedge a_1 = 0$.
2. Нека је $a \preccurlyeq x_1 \curlyvee x_2 \curlyvee \cdots \curlyvee x_n$. Ако би за свако $k \in \{1, \ldots, n\}$ било $a \not\preccurlyeq x_k$, имали бисмо (према 1) да је $a \curlywedge x_k = 0$. Међутим, тада је

$$a = a \curlywedge (x_1 \curlyvee x_2 \curlyvee \cdots \curlyvee x_n) = (a \curlywedge x_1) \curlyvee (a \curlywedge x_2) \curlyvee \cdots \curlyvee (a \curlywedge x_n) = 0 \curlyvee 0 \curlyvee \cdots \curlyvee 0 = 0,$$

што је немогуће, јер је a атом. Како за било које x важи $a \preccurlyeq 1 = x \curlyvee x'$, према управо доказаном имамо да је $a \preccurlyeq x$ или $a \preccurlyeq x'$. Наравно да не може бити $a \preccurlyeq x$ и $a \preccurlyeq x'$, јер би тада било и $a \preccurlyeq x \curlywedge x' = 0$. □

Дефиниција 4. *Булова алгебра* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *је* ***атомична*** *ако за сваки елемент* $x \in B \setminus \{0\}$ *постоји атом* a *такав да је* $a \preccurlyeq x$.

Пример 14. Алгебре партитивног скупа $(\mathcal{P}(U), \cup, \cap, ^c, \emptyset, U)$, где је U било који скуп, јесу атомичне Булове алгебре.

Коначне уније лево-полузатворених интервала скупа $\mathbb{R}$ образују поље скупова које не може бити атомична Булова алгебра, јер уопште нема атома. ▷

Теорема 6. *Свака коначна Булова алгебра је атомична.*

Доказ. Нека је $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ коначна Булова алгебра (што значи да је B коначан скуп). Претпоставимо да $\mathbf{B}$ није атомична. То значи да постоји елемент $x \in B \setminus \{0\}$ за који не постоји атом a такав да је $a \preccurlyeq x$. Специјално, x није атом, што значи да постоји $x_1 \in B$ такав да је $0 \prec x_1 \prec x$. Такође, ни x_1 није атом, па постоји $x_2 \in B$ да је $0 \prec x_2 \prec x_1$. Очигледно, овај поступак можемо неограничено наставити. Међутим, то није могуће ако је $\mathbf{B}$ коначна Булова алгебра. □

Већ смо рекли да атоми у атомичним Буловим алгебрама у извесном смислу представљају „градивни материјал“ помоћу кога се добијају сви други елементи различити од 0. То се најбоље види на примеру коначних алгебри партитивног скупа. Ако је U коначан скуп, онда је сваки X из $\mathcal{P}(U) \setminus \{\emptyset\}$ заправо унија синглтона (атома) $\{u\}$, $u \in X$. Ово запажање се природно преноси на све коначне Булове алгебре (што ће показати наредна теорема): ако операцију $\curlyvee$ неке коначне Булове алгебре назовемо унијом, онда је сваки елемент x ове алгебре унија атома који се налазе испод њега. Ова аналогија нас наводи на помисао да су коначне Булове алгебре заправо изоморфне са коначним алгебрама скупова.

Теорема 7. *Нека је* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *коначна Булова алгебра и* $A \subseteq B$ *скуп њених атома. Тада су Булове алгебре* $(B, \curlyvee, \curlywedge, ', 0, 1)$ *и* $(\mathcal{P}(A), \cup, \cap, ^c, \emptyset, A)$ *изоморфне.*

ДОКАЗ. Приметимо најпре да је Булова алгебра $\mathbf{B}$ атомична, јер је коначна (теорема 6). Узимајући у обзир разматрање пре формулације теореме, природно је претпоставити да ће тражени изоморфизам представљати функција $f : B \to \mathcal{P}(A)$, дефинисана са $f(x) = \{a \in A \mid a \preccurlyeq x\}$, $x \in B$. То ћемо у наставку и доказати.

f је 1-1 функција. Нека су x_1 и x_2 различити елементи из B. Тада је $x_1 \not\preccurlyeq x_2$ или $x_2 \not\preccurlyeq x_1$ (јер би у супротном елементи морали бити једнаки). Није тешко показати да је тада $x_1 \curlywedge x_2' \neq 0$ или $x_1' \curlywedge x_2 \neq 0$. Заиста, ако би било $x_1 \curlywedge x_2' = 0$ и $x_1' \curlywedge x_2 = 0$, имали бисмо

$$x_1 = x_1 \curlywedge 1 = x_1 \curlywedge (x_2 \curlyvee x_2') = (x_1 \curlywedge x_2) \curlyvee (x_1 \curlywedge x_2') = (x_1 \curlywedge x_2) \curlyvee 0 = x_1 \curlywedge x_2,$$

тј. $x_1 \preccurlyeq x_2$, као и

$$x_2 = x_2 \curlywedge 1 = x_2 \curlywedge (x_1 \curlyvee x_1') = (x_2 \curlywedge x_1) \curlyvee (x_2 \curlywedge x_1') = (x_2 \curlywedge x_1) \curlyvee 0 = x_2 \curlywedge x_1,$$

тј. $x_2 \preccurlyeq x_1$. Уколико је $x_1 \curlywedge x_2' \neq 0$, онда постоји $a \in A$ такав да је $a \preccurlyeq x_1 \curlywedge x_2'$, јер је $\mathbf{B}$ атомична Булова алгебра. Тада је $a \preccurlyeq x_1$, па $a \in f(x_1)$, али је и $a \preccurlyeq x_2'$, па $a \not\preccurlyeq x_2$, тј. $a \notin f(x_2)$. Дакле, $f(x_1) \neq f(x_2)$. Аналогно се добија да из $x_1' \curlywedge x_2 \neq 0$, следи $f(x_1) \neq f(x_2)$.

f је на функција. Нека је $Y \in \mathcal{P}(A)$ произвољан скуп атома. Ако је $Y = \emptyset$, онда је $f(0) = Y$. Претпоставимо да је $Y \neq \emptyset$. Како је B коначан скуп, коначан је и скуп A, па можемо узети да је $Y = \{a_1, \ldots, a_n\}$, за неке $a_1, \ldots, a_n \in A$. Нека је $x = a_1 \curlyvee \cdots \curlyvee a_n$. Доказаћемо да је $f(x) = Y$. С обзиром на то да је $a_i \preccurlyeq x = a_1 \curlyvee \cdots \curlyvee a_n$, за свако $i \in \{1, \ldots, n\}$, закључујемо да је $Y \subseteq f(x)$. Да бисмо доказали и обрнуту инклузију, изабраћемо произвољан атом $a \in f(x)$, тј. атом такав да је $a \preccurlyeq a_1 \curlyvee \cdots \curlyvee a_n$. Тада, према особини 2 леме 11, имамо да је $a \preccurlyeq a_i$, за неко $i \in \{1, \ldots, n\}$. Пошто су и a и a_i атоми, закључујемо да мора бити $a = a_i$, тј. $a \in Y$. Дакле, $f(x) \subseteq Y$.

f је изоморфизам. На основу леме 3, довољно је доказати да за произвољне $x, x_1, x_2 \in B$ важи $f(x_1 \curlyvee x_2) = f(x_1) \cup f(x_2)$ и $f(x') = f(x)^{\mathrm{c}}$.

$$\begin{aligned} f(x_1 \curlyvee x_2) &= \{a \in A \mid a \preccurlyeq x_1 \curlyvee x_2\} \overset{(!)}{=} \{a \in A \mid a \preccurlyeq x_1 \text{ или } a \preccurlyeq x_2\} \\ &= \{a \in A \mid a \preccurlyeq x_1\} \cup \{a \in A \mid a \preccurlyeq x_2\} = f(x_1) \cup f(x_2) \end{aligned}$$

Једнакост (!) важи на основу особине 2 леме 11, као и из чињенице да је $x_1 \curlyvee x_2 = \sup\{x_1, x_2\}$.

$$f(x') = \{a \in A \mid a \preccurlyeq x'\} = \{a \in A \mid a \not\preccurlyeq x\} = A \setminus \{a \in A \mid a \preccurlyeq x\} = f(x)^{\mathrm{c}}$$

Ове једнакости следе из чињенице да за сваки атом a и било који елемент x важи или $a \preccurlyeq x$ или $a \preccurlyeq x'$, али никако оба. $\square$

Последица 1. *Свака коначна Булова алгебра има* 2^n *елемената, за неки природан број* n.

Последица 2. *Изоморфне су сваке две коначне Булове алгебре са истим бројем елемената.*

Стонова теорема репрезентације Булових алгебри

У претходном одељку показали смо да се свака коначна Булова алгебра може схватити као алгебра партитивног скупа неког коначног скупа (прецизније, скупа својих атома). Природно се намеће питање да ли можемо доказати сличан резултат за било коју Булову алгебру. Не можемо очекивати да ће свака Булова алгебра бити изоморфна некој алгебри партитивног скупа, из једноставног разлога, јер постоје пребројиве Булове алгебре[11], док су алгебре партитивног скупа коначне или непребројиве. Ипак, можемо покушати да их опишемо (до на изоморфизам) као поља скупова. Већ на први поглед се види да доказ којим су окарактерисане коначне Булове алгебре не можемо директно уопштити на све Булове алгебре (јер постоје оне које нису атомичне). Ипак нека заједничка нит се може пронаћи. У случају коначних Булових алгебри, сваки њен елемент је схваћен као „скуп" атома, а знамо да је сваки скуп потпуно одређен елементима које садржи. У општем случају, размишљаћемо дуално: елементе неке Булове алгебре $\mathbf{B}$ покушаћемо да репрезентујемо скуповима (подскуповима од B) који садрже тај елемент. Настојаћемо да одредимо колекцију $\mathcal{U} \subseteq \mathcal{P}(B)$ погодну да било који елемент a из B репрезентујемо скупом свих скупова из $\mathcal{U}$ који садрже a, тј. скупом $\{X \in \mathcal{U} \mid a \in X\}$. Притом, потребно је да наведена репрезентација елемената чува операције и константе одговарајућих Булових алгебри – Булове алгебре $\mathbf{B}$ и алгебре партитивног скупа над $\mathcal{P}(\mathcal{U})$. Прецизније, функција $f : B \to \mathcal{P}(\mathcal{U})$, $f(a) = \{X \in \mathcal{U} \mid a \in X\}$, $a \in B$, треба да задовољава следеће услове:

1. $f(a \curlyvee b) = f(a) \cup f(b)$, тј.
   $\{X \in \mathcal{U} \mid a \curlyvee b \in X\} = \{X \in \mathcal{U} \mid a \in X\} \cup \{X \in \mathcal{U} \mid b \in X\}$;
2. $f(a \curlywedge b) = f(a) \cap f(b)$, тј.
   $\{X \in \mathcal{U} \mid a \curlywedge b \in X\} = \{X \in \mathcal{U} \mid a \in X\} \cap \{X \in \mathcal{U} \mid b \in X\}$;
3. $f(a') = f(a)^{\mathrm{c}}$, тј. $\{X \in \mathcal{U} \mid a' \in X\} = \{X \in \mathcal{U} \mid a \in X\}^{\mathrm{c}}$;
4. $f(0) = \emptyset$, тј. $\{X \in \mathcal{U} \mid 0 \in X\} = \emptyset$;

[11] На пример, Фрешеова алгебра $\mathcal{F}(\mathbb{N})$ (алгебра коначно-коконачних скупова) над скупом природних бројева $\mathbb{N}$ је пребројива (видети пример 4).

5. $f(1) = \mathcal{U}$, тј. $\{X \in \mathcal{U} \mid 1 \in X\} = \mathcal{U}$.

Да ли можемо да одредимо (тј. да ли постоји) скуп $\mathcal{U}$ који остварује све наше замисли? Наведени захтеви биће испуњени ако сваки X из $\mathcal{U}$ задовољава следеће услове[12]:

1.1. ако $a \curlyvee b \in X$, онда $a \in X$ или $b \in X$;

1.2. ако $a \in X$, онда за било који $b \in B$, $a \curlyvee b \in X$;

2.1. ако $a \curlywedge b \in X$, онда $a \in X$ и $b \in X$;

2.2. ако $a \in X$ и $b \in X$, онда $a \curlywedge b \in X$;

3. $a' \in X$ акко $a \notin X$;

4. $0 \notin X$;

5. $1 \in X$.

Неки од наведених услова су последице осталих, па се овај списак може скратити.

$$\begin{array}{ccc} 1.2 & \wedge & \underbrace{2.2 \ \wedge \ 3 \ \wedge \ 4} & \wedge & 5 \\ \Downarrow & & \Downarrow & & \\ 2.1 & & 1.1 & & \end{array}$$

Приметимо најпре да је услов 1.2 еквивалентан услову:

$$(*) \qquad \text{ако } a \in X \text{ и } a \preccurlyeq b, \text{ онда } b \in X.$$

Заиста, претпоставимо да важи 1.2, да $a \in X$ и $a \preccurlyeq b$. Како је $b = a \curlyvee b$, одмах добијамо да $b \in X$. Обрнуто, претпоставимо да важи $(*)$, да $a \in X$ и да је $b \in B$ произвољан. Како је $a \preccurlyeq a \curlyvee b$, закључујемо да $a \curlyvee b \in X$. Лако се уочава и да је услов 2.1 последица услова $(*)$. Услов 1.1 последица је услова 2.2, 3 и 4. Заиста, претпоставимо да $a \curlyvee b \in X$, али да $a \notin X$ и $b \notin X$. Тада према услову 3 следи да $a' \in X$ и $b' \in X$, и даље, према 2.2, да $a' \curlywedge b' = (a \curlyvee b)' \in X$. Позивајући се још једном на услов 2.2 добијамо да $(a \curlyvee b) \curlywedge (a \curlyvee b)' = 0 \in X$, што противречи услову 4. Приметимо да се уместо услова 5 може поставити слабији захтев да скуп X буде непразан, и да ће тада из $(*)$ следити 5. Сумирајући претходна разматрања, у наредној дефиницији издвајамо какве бисмо подскупове од B желели да садржи $\mathcal{U}$. Реч је тзв. *ултрафилтерима*.

[12]На основу наведених услова видимо да замисао не можемо остварити за $\mathcal{U} = \mathcal{P}(B)$.

Дефиниција 5. *Нека је* $\mathbf{B}$ *произвољна Булова алгебра. Скуп* $X \subseteq B$ *је* ***ултрафилтер*** *у* $\mathbf{B}$ *уколико важе следећи услови:*

F1 $1 \in F$;

F2 $0 \notin F$;

F3 *ако* $a \in F$ *и* $a \preccurlyeq b$, *онда* $b \in F$;

F4 *ако* $a \in F$ *и* $b \in F$, *онда* $a \curlywedge b \in F$;

F5 $a' \in F$ *акко* $a \notin F$.

Скуп X *је* ***филтер*** *ако задовољава услове* **F1**–**F4**.

Наравно, одмах се намеће питање да ли у свакој Буловој алгебри уопште постоје ултрафилтери. Наредна теорема даје потврдан одговор. Штавише, показаћемо да сваки подскуп од B који има *својство коначног пресека* генерише по један ултрафилтер у $\mathbf{B}$.

Дефиниција 6. *Подскуп* $K \subseteq B$ *има својство коначног пресека, ако за сваки избор коначно много елемената* $x_1, \dots, x_n$ *из* K *важи* $x_1 \curlywedge \cdots \curlywedge x_n \neq 0$.

Теорема 8. [***Теорема о ултрафилтеру***] *За сваки подскуп* $K \subseteq B$ *који има својство коначног пресека, постоји ултрафилтер* F_K *у* $\mathbf{B}$ *који га садржи, тј.* $K \subseteq F_K$.

Доказ теореме је наизглед дугачак, али само зато што ћемо три пута проверавати поједине услове дефиниције 5. Саветујемо читаоцу да најпре прочита доказ прескачући провере поменутих услова.

Доказ. Дефинишимо најпре скуп

$$F = \{x \in B \mid x_1 \curlywedge \cdots \curlywedge x_n \preccurlyeq x, \text{ за неко } n \in \mathbb{N} \text{ и неке } x_1, \dots, x_n \in K\}.$$

Очигледно је $K \subseteq F$. Једноставно је проверити да скуп F задовољава услове F1–F4 претходне дефиниције, док услов F5 не мора задовољавати.

F1 Очигледно $1 \in F$, јер је 1 највећи елемент Булове алгебре.

F2 Пошто K има својство коначног пресека, не постоје $n \in \mathbb{N}$ и $x_1, \dots, x_n \in K$ такви да је $x_1 \curlywedge \cdots \curlywedge x_n \preccurlyeq 0$. Дакле, $0 \notin F$.

F3 Претпоставимо да $a \in F$ и $a \preccurlyeq b$. Из $a \in F$ следи да постоје $n \in \mathbb{N}$ и $x_1, \dots, x_n \in K$ такви да је $x_1 \curlywedge \cdots \curlywedge x_n \preccurlyeq a$. Како је тада и $x_1 \curlywedge \cdots \curlywedge x_n \preccurlyeq b$, следи да $b \in F$.

F4 Ако $a, b \in F$, онда постоје $n, m \in \mathbb{N}$ и $x_1, \dots, x_n, y_1, \dots, y_m \in K$ такви да је $x_1 \curlywedge \cdots \curlywedge x_n \preccurlyeq a$ и $y_1 \curlywedge \cdots \curlywedge y_m \preccurlyeq b$. Из ове две неједнакости добијамо да је $x_1 \curlywedge \cdots \curlywedge x_n \curlywedge y_1 \curlywedge \cdots \curlywedge y_m \preccurlyeq a \curlywedge b$, па $a \curlywedge b \in F$.

Кључну идеју за наставак доказа добијамо ако уочимо да се ултрафилтеру не може додати ниједан нови елемент из B, а да добијени надскуп и даље буде ултрафилтер. Заиста, услов F5 је еквивалентан следећем услову: за сваки елемент $a \in B$, или a или a' припада ултрафилтеру, а никако не могу припадати оба, због услова F2 и F4. Једноставно се уочава да је ултрафилтер максималан, у смислу инклузије, подскуп од B који задовољава услове F1–F4. Дакле, очекивана је примена Цорнове леме[13] (тј. аксиоме избора) у наставку доказа.

Нека је $\mathcal{F} = \{X \subseteq B \mid F \subseteq X \text{ и } X \text{ задовољава услове F1} - \text{F4}\}$. Тада је $\mathcal{F} \neq \emptyset$, јер $F \in \mathcal{F}$. Доказаћемо да уређење $(\mathcal{F}, \subseteq)$ задовољава услов Цорнове леме, тј. да сваки ланац има горње ограничење. Нека је $\mathcal{L} \subseteq \mathcal{F}$ ланац, тј. за произвољне $X_1, X_2 \in \mathcal{L}$ важи $X_1 \subseteq X_2$ или $X_2 \subseteq X_1$. Показаћемо да $X_{\mathcal{L}} \stackrel{\text{def}}{=} \cup\mathcal{L} \in \mathcal{F}$. Пошто за свако $X \in \mathcal{L}$, важи $F \subseteq X$, закључујемо да је $F \subseteq X_{\mathcal{L}}$.

F1 За свако $X \in \mathcal{L}$ важи $0 \notin X$, одакле следи да $0 \notin X_{\mathcal{L}}$.

F2 За свако $X \in \mathcal{L}$ важи $1 \in X$, одакле следи да $1 \in X_{\mathcal{L}}$.

F3 Претпоставимо да $a \in X_{\mathcal{L}}$ и $a \preccurlyeq b$. Из $a \in X_{\mathcal{L}} = \cup\mathcal{L}$, следи да постоји $X \in \mathcal{L}$ тако да је $a \in X$, па пошто X задовољава услов F3, закључујемо да $b \in X$, а самим тим и да $b \in X_{\mathcal{L}}$.

F4 Нека су $a, b \in X_{\mathcal{L}}$ произвољни. Тада постоје $X_1, X_2 \in \mathcal{L}$ такви да $a \in X_1$ и $b \in X_2$. Како је $X_1 \subseteq X_2$ или $X_2 \subseteq X_1$, имамо да $a, b \in X_1$ или $a, b \in X_2$, одакле следи да $a \curlywedge b \in X_1$ или $a \curlywedge b \in X_2$. Који год случај да наступи, биће $a \curlywedge b \in X_{\mathcal{L}}$.

Дакле, $X_{\mathcal{L}} \in \mathcal{F}$. Како је за свако $X \in \mathcal{L}$, $X \subseteq X_{\mathcal{L}}$, закључујемо да је $X_{\mathcal{L}}$ горње ограничење у $(\mathcal{F}, \subseteq)$ ланца $\mathcal{L}$. Према Цорновој леми, постоји максималан елемент F_K у $(\mathcal{F}, \subseteq)$. Остаје још да се покаже да F_K задовољава својство F5 (јер својства F1–F4 тривијално задовољава будући да $F_K \in \mathcal{F}$).

Да бисмо доказали да F_K задовољава својство F5, претпоставићемо супротно, да постоји $z \in B$ такав да $z \notin F_K$ и $z' \notin F_K$. Нека је

$$F_K^z = \{x \in B \mid u \curlywedge z \preccurlyeq x, \text{ за неко } u \in F_K\}.$$

Приметимо најпре да је $F \subseteq F_K \subseteq F_K^z$ и $z \in F_K^z$. Није тешко проверити да F_K^z задовољава услове $\text{F1} - \text{F4}$.

[13]Цорнова лема: Ако у неком парцијално уређеном скупу сваки ланац има горње ограничење (мајоранту), онда у том парцијалном уређењу постоји максималан елемент. Цорнова лема је еквивалентна аксиоми избора.

F1 Очигледно је да $1 \in F_K^z$, јер је $1 \curlywedge z \preccurlyeq 1$ и $1 \in F_K$.

F2 Такође, $0 \notin F_K^z$, јер би у супротном постојао $u \in F_K$ такав да је $u \curlywedge z \preccurlyeq 0$, одакле бисмо имали $u \preccurlyeq z'$, па би морало бити и $z' \in F_K$ супротно претпоставци да $z' \notin F_K$.

F3 Ако $a \in F_K^z$ и $a \preccurlyeq b$, онда постоји $u \in F_K$ такав да је $u \curlywedge z \preccurlyeq a \preccurlyeq b$, па $b \in F_K^z$.

F4 Ако $a, b \in F_K^z$, онда постоје $u_1, u_2 \in F_K$ такви да је $u_1 \curlywedge z \preccurlyeq a$ и $u_2 \curlywedge z \preccurlyeq b$, па како је $(u_1 \curlywedge z) \curlywedge (u_2 \curlywedge z) = (u_1 \curlywedge u_2) \curlywedge z \preccurlyeq a \curlywedge b$ и $u_1 \curlywedge u_2 \in F_K$, следи да $a \curlywedge b \in F_K^z$.

Дакле, $F_K^z \in \mathcal{F}$ и при томе $F_K \subsetneqq F_K^z$, што није могуће јер је F_K максималан.

Да закључимо, F_K је ултрафилтер Булове алгебре $\mathbf{B}$ који садржи скуп K. $\square$

Последица 3. *За сваки елемент $a \in B \setminus \{0\}$, постоји ултрафилтер у $\mathbf{B}$ који га садржи.*

Вратимо се сада на почетак. Нека је $\mathbf{B}$ произвољна Булова алгебра и $\mathcal{U}$ скуп свих ултрафилтера ове алгебре. Сада знамо да функција $f : B \to \mathcal{P}(\mathcal{U})$, $f(a) = \{X \in \mathcal{U} \mid a \in X\}$, $a \in B$, задовољава следеће услове:

1. $f(a \curlyvee b) = f(a) \cup f(b)$;
2. $f(a \curlywedge b) = f(a) \cap f(b)$;
3. $f(a') = f(a)^{\mathrm{c}}$;
4. $f(0) = \emptyset$, тј. $\{X \in \mathcal{U} \mid 0 \in X\} = \emptyset$;
5. $f(1) = \mathcal{U}$, тј. $\{X \in \mathcal{U} \mid 1 \in X\} = \mathcal{U}$.

Штавише, ова функција је и 1-1. Заиста, ако су $a, b \in B$ различити, $a \neq b$, онда је $a' \curlywedge b \neq 0$ или $a \curlywedge b' \neq 0$. У случају да је $a' \curlywedge b \neq 0$, према претходној последици, постоји ултрафилтер $F_{\{a',b\}}$ који садржи и a' и b, а самим тим не садржи a. Дакле, $F_{\{a',b\}} \notin f(a)$ и $F_{\{a',b\}} \in f(b)$, одакле следи да је $f(a) \neq f(b)$. До истог закључка долазимо полазећи од претпоставке $a \curlywedge b' \neq 0$.

Скуп $f[B] = \{f(a) \mid a \in B\} \subseteq \mathcal{P}(\mathcal{U})$ представља једно поље скупова које је изоморфно са $\mathbf{B}$. На овај начин је доказана теорема која је узета за наслов овог одељка.

Теорема 9. [***Стонова теорема репрезентације***] *Свака Булова алгебра изоморфна је неком пољу скупова.*

Ова теорема заправо у потпуности оправдава тврдњу са почетка поглавља да су Буловим алгебрама окарактерисана сва алгебарска својства скуповних операција.

Задаци

1. Због чега структура $\mathbf{D}_n = (D_n, \mathrm{nzs}, \mathrm{nzd}, n/, 1, n)$ није Булова алгебра уколико је n дељив квадратом неког простог броја? Који закони из дефиниције 1 не важе у овој структури?

2. Доказати да подскупови скупа реалних бројева $\mathbb{R}$ који су највише пребројиви или су копребројиви[14] образују једно поље скупова.

3. Нека је $2\mathbb{N}$ скуп парних, $2\mathbb{N}+1$ скуп непарних природних бројева и

$$\mathcal{A} = \{X \subseteq 2\mathbb{N} \mid X \text{ је коначан }\} \cup \{X \subseteq 2\mathbb{N}+1 \mid \mathbb{N} \setminus X \text{ је коначан }\}.$$

Испитати да ли је $\mathcal{A}$ поље скупова.

4. Нека је P скуп простих бројева и $\mathcal{B}$ скуп свих оних и само оних подскупова X од $\mathbb{N}$ за које је $X \cap P = \emptyset$ или $X \cap P = P$. Доказати да је $\mathcal{B}$ поље скупова.

5. Нека је $\mathbb{Z}$ скуп целих бројева и m неки фиксирани цео број. Подскуп X од $\mathbb{Z}$ је m-*периодичан* ако је $X = X + m$, при чему је $X + m \overset{\text{def}}{=} \{x + m \mid x \in X\}$. Очигледно је да су $\emptyset$ и $\mathbb{Z}$ m-периодични. Доказати да је скуп $\mathcal{Z}_m$ свих m-периодичних подскупова од $\mathbb{Z}$ поље скупова.
Напомена. Приметите да је $\mathcal{Z}_0 = \mathcal{P}(\mathbb{Z})$ и $\mathcal{Z}_1 = \{\emptyset, \mathbb{Z}\}$. Одредите $\mathcal{Z}_2$ и $\mathcal{Z}_3$.

6. Доказати да су Булове алгебре $(\mathcal{P}(\{a,b\}), \cup, \cap, ^{\mathrm{c}}, \emptyset, \{a,b\})$ и $\mathbf{2}\times\mathbf{2}$ изоморфне.

7. На скупу $S = \{a, b, c, d\}$ дефинисати (одговарајућим таблицама) две операције $\oplus, \odot : S \times S \to S$ и једну унарну $^* : S \to S$, тако да структура $(S, \oplus, \odot, ^*, a, b)$ буде Булова алгебра.

8. Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра. Доказати да за све $a, b, c \in B$ важи:
(а) $a \curlyvee (a' \curlywedge b) = a \curlyvee b$;
(б) $(a \curlyvee b) \curlywedge (a' \curlyvee c) = (a \curlywedge c) \curlyvee (a'b)$;
(в) $(a \curlywedge b) \curlyvee (b \curlywedge c) \curlyvee (c \curlywedge a) = (a \curlyvee b) \curlywedge (b \curlyvee c) \curlywedge (c \curlyvee a)$.

9. Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра. Доказати следећа тврђења:
(а) ако за неко $x \in B$ важи $a \curlyvee x = b \curlyvee x$ и $a \curlyvee x' = b \curlyvee x'$, онда је $a = b$;
(б) ако за неко $x \in B$ важи $a \curlywedge x = b \curlywedge x$ и $a \curlywedge x' = b \curlywedge x'$, онда је $a = b$.

10. Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра. *Симетрична разлика* елемената x и y из B дефинисана је са $x \triangle y = (x \curlywedge y') \curlyvee (x' \curlywedge y)$. Доказати да за произвољне $x, z, y \in B$ важи:

[14] Подскуп X од $\mathbb{R}$ је *копребројив* ако је његов комплемент $X^{\mathrm{c}} = \mathbb{R} \setminus X$ највише пребројив.

(а) $x \triangle y = y \triangle x$; (б) $x \triangle 0 = x$;
(в) $x \triangle x' = 1$; (г) $x \triangle (y \triangle z) = (x \triangle y) \triangle z$;
(д) $x \curlywedge (y \triangle z) = (x \curlywedge y) \triangle (x \curlywedge z)$; (ђ) $x \triangle x = 0$;
(е) $x \triangle 1 = x'$; (ж) $x = y$ акко $x \triangle y = 0$.

Дефиниција. *Прстен* је структура $(R, +, -, \cdot, 0, 1)$ коју чине неки скуп R, две бинарне операције $+, \cdot : R \times R \to R$, једна унарна $- : R \to R$ и два различита елемента 0 и 1 из R, при чему произвољни елементи x, y, z из R испуњавају следеће услове:

$\mathbf{A}^{+}$ $\quad x + (y + z) = (x + y) + z$;
$\mathbf{K}^{+}$ $\quad x + y = y + x$;
$\mathbf{N}^{+}$ $\quad x + 0 = x$;
$\mathbf{I}^{+}$ $\quad x + (-x) = 0$;
$\mathbf{A}^{\cdot}$ $\quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
$\mathbf{K}^{\cdot}$ $\quad x \cdot y = y \cdot x$;
$\mathbf{N}^{\cdot}$ $\quad x \cdot 1 = x$;
$\mathbf{D}^{\cdot}_{+}$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Прстен $(R, +, -, \cdot, 0, 1)$ је *Булов прстен* ако за свако $x \in B$ важи $x \cdot x = x$.

11. Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра. Доказати да је $(B, \triangle, -, \curlywedge, 0, 1)$ Булов прстен, при чему је $\triangle$ симетрична разлика дефинисана у зад 10, а $-$ је унарна операција дефинисана као идентичко пресликавање, тј. са $-x = x$.

12. Нека је $(R, +, -, \cdot, 0, 1)$ Булов прстен. Доказати да је $(B, \curlyvee, \cdot, ', 0, 1)$ Булова алгебра, при чему је $\curlyvee$ бинарна операција дефинисана са $x \curlyvee y = x + y + (x \cdot y)$, а $'$ унарна операција дефинисана са $x' = 1 + x$.

13. Ако је α било који Булов израз, доказати да једнакост

$$\alpha = (\alpha(x/0) \curlyvee x) \curlywedge (\alpha(x/1) \curlyvee x')$$

важи у било којој Буловој алгебри.
Упутство. Видети лему 6 (страна 19)

14. Ако је $\alpha(x_1, \dots, x_n)$ Булов израз, доказати да једнакост

$$(KKNF) \qquad \alpha(x_1, \dots, x_n) = \bigwedge_{(a_1, \dots, a_n) \in 2^n} \left(\alpha(a_1, \dots, a_n)' \curlyvee x_1^{a_1} \curlyvee \cdots \curlyvee x_n^{a_n}\right)$$

важи у свакој Буловој алгебри. Израз са десне стране једнакости назива се *канонска конјунктивна нормална форма* израза $\alpha(x_1, \dots, x_n)$.
Упутство. Видети лему 4 (страна 20).

ДНФ и КНФ. Булов израз је у *дисјунктивној (конјунктивној) нормалној форми* ако је облика $\bigvee_{i\in I}\bigwedge_{j\in J_i} x_{ij}^{a_{ij}}$ $\left(\bigwedge_{i\in I}\bigvee_{j\in J_i} x_{ij}^{a_{ij}}\right)$, за неке коначне скупове I и J_i, и неке $a_{ij}\in\{0,1\}$, при чему су x_{ij} променљиве. Примери израза у ДНФ су: $x \curlywedge y'$, $(x_1 \curlywedge x_2 \curlywedge x_3) \curlyvee (x_1' \curlywedge x_3)$, итд. Примери израза у КНФ су: $x \curlywedge y'$, $(x_1 \curlyvee x_2 \curlywedge x_3) \curlywedge (x_1' \curlyvee x_3)$, $z \curlyvee z'$ итд.
На основу теореме 4 и задатка 14, закључујемо да се сваки Булов израз може трансформисати у ДНФ и КНФ. Осим директне примене поменутих тврђења, неки израз α можемо трансформисати у днф, односно кнф, спроводећи следеће кораке:
1. док год је могуће примењивати Де Морганове законе (тј. док год се сви комплементи не „спусте“ до променљивих и константи), елиминишићу двоструке комплементе законом инволуције и примењујући одговарајуће једнакости за комплементе константи; у овом кораку израз α се трансформише у израз изграђен од константи, променљивих и комплемената променљивих, при чему се појављују само $\curlyvee$ и $\curlywedge$ (и заграде, наравно);
2. примењивати дистрибутивни закон $\mathbf{D}^{\curlywedge}_{\curlyvee}$ (као и асоцијативност, и комутативност) на израз добијен у претходном кораку, уз одговарајућу елиминацију константи, док год се не добије израз у днф; односно примењивати дистрибутивни закон $\mathbf{D}^{\curlyvee}_{\curlywedge}$ (као и асоцијативност, и комутативност) на израз добијен у претходном кораку, уз одговарајућу елиминацију константи, док год се не добије израз у кнф.

15. Трансформисати израз у днф:
(а) $(x \curlyvee y) \curlywedge (x' \curlyvee y')$; (б) $(x \curlyvee y)' \curlyvee (x \curlywedge y')$; (в) $(x' \curlyvee (y \curlywedge z')')' \curlyvee z'$.

16. Трансформисати израз у кнф:
(а) $(x \curlywedge y) \curlyvee (x' \curlywedge y')$; (б) $(x \curlyvee y)' \curlyvee (x \curlywedge y')$; (в) $(x' \curlyvee (y \curlywedge z')')' \curlyvee z'$.

17. Нека је $(B, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра и $\preccurlyeq$ уређење ове алгебре. Доказати да за све $a, b \in B$ важи:
(а) $a \preccurlyeq b$ акко $b' \preccurlyeq a'$;
(б) ако је $a \preccurlyeq b$, онда за свако $c \in B$ важи $a \curlyvee (b \curlywedge c) = b \curlywedge (a \curlyvee c)$.

Исказна логика

Синтакса и семантика исказне логике

Најпре ћемо неким једноставним примерима илустровати идеје које су у основи исказног рачуна.

Пример 1. Очигледно је да реченице:

1. *Земља се окреће око Сунца или се Земља не окреће око Сунца.*
2. *Број* $1,41$ *јесте решење једначине* $x^2 = 2$ *или* $1,41$ *није решење једначине* $x^2 = 2$.

имају исту структуру „$\cdots$ *или не* $\cdots$“, и да их управо због тога сматрамо тачним без обзира на то да ли је исказ који се налази на месту тачкица тачан или нетачан. Одавде се јасно види значај логичких везника *или* и *не* у структури наведених реченица. Наравно, још много аналогних примера можемо саставити. Анализирајмо даље и следећа два закључивања.

Ако некоме кажемо	*Ако си ти у праву, онда сам ја луд.*
и додамо	*Ја нисам луд.*
саговорник ће знати да смо рекли	*Ти ниси у праву.*

Знамо да важи	*Ако је четвороугао* $ABCD$ *квадрат, онда је* $ABCD$ *правоугаоник.*
и ако уочимо да	*Четвороугао* $ABCD$ *није правоугаоник.*
закључујемо да	*Четвороугао* $ABCD$ *није квадрат.*

Ова два закључивања, иако долазе из потпуно различитих околности, суштински се не разликују.

Претпоставке:	*Ако* $\cdots$, *онда* $***$.
	Не $***$.
Закључак:	*Не* $\cdots$.

И овога пута, исправност наведених закључивања оправдавамо логичким везницима „*Ако* $\cdots$, *онда* $***$“ и „*Не* $***$“ не обазирући се много на смисао реченица које стоје уместо $\cdots$ и $***$. ▷

У исказној логици централно место заузимају тзв. *логички везници*: *и*, *или*, *не*, *ако ..., онда ...*, *ако и само ако*. Помоћу њих градимо сложене исказе полазећи од неких једноставних чији смисао нас не занима, већ је једино важно да ли су они тачни или нетачни. Истинитост сложенијих исказа одређујемо на основу тзв. истинитосних таблица придружених везницима.

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

	$\neg$
0	1
1	0

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

У таблицама су наведене стандардне ознаке за везнике: $\wedge$ – *и*, $\vee$ – *или*, $\neg$ – *не*, $\Rightarrow$ – *ако ..., онда ...*, $\Leftrightarrow$ – *ако и само ако*. Ако неке једноставне исказе означимо словима p, q, r, онда је $(p \wedge q) \Rightarrow r$ пример сложеног исказа (који читамо *ако* p *и* q, *онда* r). Други пример сложеног исказа је $p \vee \neg p$ са којим смо се срели у претходном примеру. Неформално, слова p, q и r се могу замишљати као неки једноставни искази, али пошто нам смисао тих исказа није важан већ само то да ли су тачни или нетачни, сложене исказе схватамо као *алгебарске изразе* прилагођене тзв. *исказној алгебри* $(\{0,1\}, \vee, \wedge, \neg, \Rightarrow, \Leftrightarrow, 0, 1)$. Ова алгебра је проширење Булове алгебре $\mathbf{2}$ двема новим операцијама $\Rightarrow$ и $\Leftrightarrow$. Приметимо да проширење није од неког значаја, јер се додате операције једноставно дефинишу помоћу операција Булове алгебре $\mathbf{2}$:

$$x \Rightarrow y = \neg x \vee y \text{ и } x \Leftrightarrow y = (\neg x \vee y) \wedge (x \vee \neg y), \text{ за све } x, y \in \{0,1\}.$$

Наведене једнакости се директно могу проверити и то препуштамо читаоцима.

Алгебарске изразе, поменуте у претходном пасусу, називамо *исказним формулама* и дефинишемо их као и било коју другу врсту израза[15], тј. као речи записане употребом унапред изабраних симбола и по одређеним правилима. Скуп изабраних симбола називамо *алфабетом* исказне логике.

Исказне формуле

Алфабет исказне логике чине следећи симболи:

- исказна слова којих има пребројиво много; исказна слова означаваћемо малим латиничним словом p које је индексирано природним бројевима; скуп свих исказних слова углавном ћемо означавати са P; дакле $P = \{p_k \mid k \in \mathbb{N}\} = \{p_0, p_1, p_2, p_3, \ldots\}$.
- логички везници: унарни логички везник $\neg$ (негација) и бинарни логички везници $\wedge$ (конјункција), $\vee$ (дисјункција), $\Rightarrow$ (импликација) и $\Leftrightarrow$ (еквиваленција);

[15]аналогно, на пример, Буловим изразима

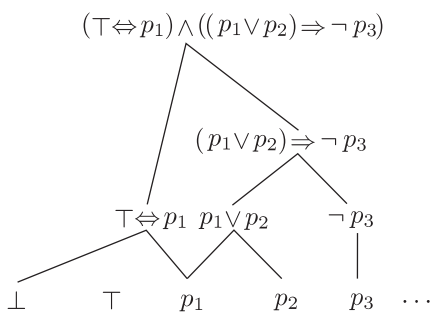
- логичке константе: $\top$ и $\bot$;
- помоћни знаци: лева „(“ и десна заграда „)“.

Дефиниција 1. *Скуп исказних формула* For *jесте најмањи (у смислу инклузије) скуп речи над алфабетом исказне логике такав да важи:*

- $P \cup \{\top, \bot\} \subseteq \mathrm{For}$ *(исказна слова и логичке константе су исказне формуле);*
- *ако* $\alpha \in \mathrm{For}$*, онда* $\neg\alpha \in \mathrm{For}$*;*
- *ако* $\alpha, \beta \in \mathrm{For}$*, онда* $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \Rightarrow \beta), (\alpha \Leftrightarrow \beta) \in \mathrm{For}$.

Скуп исказних формула jе *индуктивно дефинисан.* Најпре су уведене најједноставније исказне формуле: свако исказно слово и свака логичка константа представља једну исказну формулу. Затим је прецизирано како се формирају сложеније исказне формуле: полазећи од најједноставнијих исказних формула, помоћу наведених правила градимо нове формуле, које даље користимо за изградњу још сложенијих формула. Притом, исказне формуле се могу градити само на овај начин, што је последица захтева да For буде најмањи скуп речи са наведеним особинама (*Скуп исказних формула* For *jесте најмањи скуп . . .*).

Верујемо да су читаоцима познате уобичајене конвенције о брисању заграда, па их овде нећемо све наводити. Истичемо само договор о приоритету логичких везника: $\neg$ је везник највећег приоритета, за њим следе $\vee$ и $\wedge$ који су подједнаког приоритета, а за њима $\Rightarrow$ и $\Leftrightarrow$, такође једнаког приоритета.



На илустрацији изнад јасно се могу уочити нивои сложености исказних формула. Сложеност исказних формула „мерићемо“ функцијом која свакој формули додељује један природан број схваћен као сложеност те формуле. Иако је боље било да сложеност формула дефинишемо заједно са самим формулама, тј. да је уведемо у оквиру претходне дефиниције, уводимо је новом дефиницијом.

Дефиниција 2. *Сложеност исказне формуле је природан број који тој формули додељује функција* $\mathrm{s} : \mathrm{For} \to \mathbb{N}$ *дата са:*

- $\mathrm{s}\,(p) = \mathrm{s}\,(\top) = \mathrm{s}\,(\bot) = 0, p \in P$,

- $\mathbf{s}(\neg\alpha) = \mathbf{s}(\alpha) + 1$,
- $\mathbf{s}(\alpha * \beta) = \max\{\mathbf{s}(\alpha), \mathbf{s}(\beta)\} + 1, * \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.

Ако је $\mathbf{s}(\theta) > 0$ формулу θ називамо сложеном исказном формулом. Ако је θ сложена исказна формула, онда је она или негација неке друге исказне формуле, тј. $\theta = \neg\theta_1$, за неку формулу θ_1 (мање сложености), или је $\theta = \theta_1 * \theta_2$, за неке формуле θ_1 и θ_2 (мање сложености) и неки везник $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.

Дефинишимо још две корисне функције чији су домени For, пре свега да бисмо још једном истакли дефиниције индуктивног карактера.

За задату формулу α, интуитивно је јасно како бисмо одредили скуп $P(\alpha)$ свих исказних слова која се појављују у формули α. Строга дефиниција функције $\alpha \mapsto P(\alpha)$ јесте индуктивна:

- $P(p) = \{p\}, p \in P$;
- $P(\top) = P(\bot) = \emptyset$;
- $P(\neg\alpha) = P(\alpha)$;
- $P(\alpha * \beta) = P(\alpha) \cup P(\beta), * \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.

Аналогно уводимо скуп $\mathrm{F}(\alpha)$ свих *потформула* формуле α, тј. скуп свих подречи од α који су такође исказне формуле. Функција $\alpha \mapsto \mathrm{F}(\alpha)$ дата је са:

- $\mathrm{F}(p) = \{p\}, p \in P$;
- $\mathrm{F}(\top) = \{\top\}, \mathrm{F}(\bot) = \{\bot\}$;
- $\mathrm{F}(\neg\alpha) = \mathrm{F}(\alpha) \cup \{\neg\alpha\}$;
- $\mathrm{F}(\alpha * \beta) = \mathrm{F}(\alpha) \cup \mathrm{F}(\beta) \cup \{\alpha * \beta\}, * \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.

Пример 2. На основу дефиниција функција $\alpha \mapsto P(\alpha)$ и $\alpha \mapsto \mathrm{F}(\alpha)$, за сваку формулу α једноставно „израчунавамо“ скуп исказних слова која се у њој појављују, као и скуп њених потформула.

$$\begin{aligned}
P(p_1 \wedge \neg(p_2 \Rightarrow p_3)) &= P(p_1) \cup P(\neg(p_2 \Rightarrow p_3)) \\
&= \{p_1\} \cup P(p_2 \Rightarrow p_3) \\
&= \{p_1\} \cup P(p_2) \cup P(p_3) \\
&= \{p_1\} \cup \{p_2\} \cup \{p_3\} \\
&= \{p_1, p_2, p_3\}
\end{aligned}$$

$$\begin{array}{rl} & \mathrm{F}(p_1 \wedge \neg(p_2 \Rightarrow p_3)) \\ = & \mathrm{F}(p_1) \cup \mathrm{F}(\neg(p_2 \Rightarrow p_3)) \cup \{p_1 \wedge \neg(p_2 \Rightarrow p_3)\} \\ = & \{p_1\} \cup \mathrm{F}(p_2 \Rightarrow p_3) \cup \{\neg(p_2 \Rightarrow p_3)\} \cup \{p_1 \wedge \neg(p_2 \Rightarrow p_3)\} \\ = & \{p_1\} \cup \mathrm{F}(p_2) \cup \mathrm{F}(p_3) \cup \{p_2 \Rightarrow p_3\} \cup \{\neg(p_2 \Rightarrow p_3)\} \cup \{p_1 \wedge \neg(p_2 \Rightarrow p_3)\} \\ = & \{p_1\} \cup \{p_2\} \cup \{p_3\} \cup \{p_2 \Rightarrow p_3\} \cup \{\neg(p_2 \Rightarrow p_3)\} \cup \{p_1 \wedge \neg(p_2 \Rightarrow p_3)\} \\ = & \{p_1, p_2, p_3, p_2 \Rightarrow p_3, \neg(p_2 \Rightarrow p_3), p_1 \wedge \neg(p_2 \Rightarrow p_3)\} \end{array}$$

$\triangleright$

У наредној леми истичемо нека очигледна тврђења која се односе на уведене функције.

Лема 1. *За сваку исказну формулу α важи:*

- *скупови $P(\alpha)$ и $\mathrm{F}(\alpha)$ су коначни;*
- $\alpha \in \mathrm{F}(\alpha)$*;*
- $P(\alpha) \subseteq \mathrm{F}(\alpha)$.

ДОКАЗ. Без обзира на очигледност наведених тврђења, доказаћемо једно од њих, пре свега да бисмо илустровали доказе *индукцијом по сложености формуле*, које ћемо у наставку често користити (наравно, са мање детаља него овога пута). Доказаћемо да је за свако α, скуп $P(\alpha)$ коначан.

БИ Нека је $\mathrm{s}(\alpha) = 0$. Тада је α исказно слово или логичка константа, па је $P(\alpha)$ једночлан или празан скуп, а самим тим и коначан.

ИК [ИП] Претпоставимо да је n природан број такав да је за сваку формулу θ сложености не веће од n, $\mathrm{s}(\theta) \leqslant n$, скуп $P(\theta)$ коначан.

Нека је α формула сложености $n+1$, $\mathrm{s}(\alpha) = n+1$. Тада је α облика $\neg\theta$, где је θ нека формула сложености не веће од n или је α облика $\theta_1 * \theta_2$, $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, где су θ_1 и θ_2 неке формуле сложености не веће од n. У првом случају је $P(\alpha) = P(\theta)$, па по индуктивној претпоставци [ИП] следи да је $P(\alpha)$ коначан скуп. У другом случају је $P(\alpha) = P(\theta_1) \cup P(\theta_2)$, а како су по индуктивној претпоставци скупови $P(\theta_1)$ и $P(\theta_2)$ коначни, такав мора бити и скуп $P(\alpha)$.

Доказе преосталих тврђења препуштамо читацима. $\square$

Истинитосне вредности исказних формула

Уопште, ако је неки алгебарски израз састављен од променљивих и константи и операција које се појављују у некој конкретној алгебарској структури, онда се вредност тог израза може израчунати када се променљивама доделе конкретне вредности из домена те структуре. Притом, додељивање конкретних вредности променљивама назива се *валуација*[16]. Све ово важи и за исказне формуле, тј. алгебарске изразе који одговарају исказној алгебри.

Дефиниција 3. *Валуација је свака функција која скуп исказних слова пресликава у скуп* $\{0,1\}$*, тј.* $v : P \to \{0,1\}$.

Ако је задата валуација, онда свакој формули одговара тачно једна истинитосна вредност. Другим речима, свака валуација $v : P \to \{0,1\}$ се природно проширује до функције чији је домен скуп свих исказних формула.

Дефиниција 4. *Екстензија (проширење) валуације* $v : P \to \{0,1\}$ *на скуп свих исказних формула јесте функција* $\widehat{v} : \mathrm{For} \to \{0,1\}$ *дата са:*

- $\widehat{v}(p) = v(p)$;
- $\widehat{v}(\top) = 1, \widehat{v}(\bot) = 0$;
- $\widehat{v}(\neg\alpha) = \neg\widehat{v}(\alpha)$, *при чему* $\neg$ *са леве стране једнакости представља симбол за логички везник, а* $\neg$ *са десне стране одговарајућу интерпретацију поменутог везника, тј. унарну операцију* $\neg$ *скупа* $\{0,1\}$;
- $\widehat{v}(\alpha * \beta) = \widehat{v}(\alpha) * \widehat{v}(\beta)$, $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, *при чему* $*$ *са леве стране једнакости представља симбол за логички везник, а* $*$ *са десне стране одговарајућу бинарну операцију скупа* $\{0,1\}$.

Није тешко уочити да свака валуација има јединствено проширење на скуп For. Ако узмемо у обзир уобичајени поредак на скупу $\{0,1\}$ $(0 < 1)$, закључујемо и да је:

- $\widehat{v}(\alpha \wedge \beta) = \min\{\widehat{v}(\alpha), \widehat{v}(\beta)\}$;
- $\widehat{v}(\alpha \vee \beta) = \max\{\widehat{v}(\alpha), \widehat{v}(\beta)\}$;
- $\widehat{v}(\alpha \Rightarrow \beta) = 1$ акко $\widehat{v}(\alpha) \leqslant \widehat{v}(\beta)$;
- $\widehat{v}(\alpha \Leftrightarrow \beta) = 1$ акко $\widehat{v}(\alpha) = \widehat{v}(\beta)$.

[16] evaluatio – одређивање вредности нечега

ПРИМЕР 3. Нека је дата формула $p_2 \wedge (\neg p_7 \Rightarrow p_8)$ и валуација $v : P \to \{0,1\}$:

$$v(p_i) = \begin{cases} 1, & i \text{ је паран број}, \\ 0, & i \text{ је непаран број}. \end{cases}$$

Тада је

$$\begin{aligned} \widehat{v}(p_2 \wedge (\neg p_7 \Rightarrow p_8)) &= \widehat{v}(p_2) \wedge \widehat{v}(\neg p_7 \Rightarrow p_8) = v(p_2) \wedge (\widehat{v}(\neg p_7) \Rightarrow \widehat{v}(p_8)) \\ &= v(p_2) \wedge (\neg \widehat{v}(p_7) \Rightarrow v(p_8)) = v(p_2) \wedge (\neg v(p_7) \Rightarrow v(p_8)) \\ &= 1 \wedge (\neg 0 \Rightarrow 1) \\ &= 1. \end{aligned}$$

Дакле, истинитосна вредност формуле при датој валуацији једнака је 1. ▷

Очигледно је да истинитосна вредност неке формуле зависи само од истинитосних вредности које су додељене словима која се у тој формули појављују. Ову чињеницу строго доказујемо у наредној леми.

Лема 2. *Нека су v_1 и v_2 две валуације. Тада за сваку формулу α важи: ако је $v_1(p) = v_2(p)$, за свако $p \in P(\alpha)$, онда је $\widehat{v_1}(\alpha) = \widehat{v_2}(\alpha)$.*

ДОКАЗ. Доказ изводимо индукцијом по сложености формуле α.
Нека је α исказно слово p. Тада је $P(\alpha) = \{p\}$, па је $v_1(p) = v_2(p)$. Према дефиницији 4 имамо да је $\widehat{v_1}(p) = v_1(p) = v_2(p) = \widehat{v_2}(p)$.
Нека је α логичка константа $\top$. Пошто екстензија било које валуације формули $\top$ додељује вредност 1 имамо да је $\widehat{v_1}(\top) = 1 = \widehat{v_2}(\top)$. Аналогно поступамо ако је α логичка константа $\bot$.
Нека је α формула облика $\neg\theta$, за неку формулу θ. Ако је $\widehat{v_1}(p) = \widehat{v_2}(p)$, за $p \in P(\alpha)$, с обзиром на то да је $P(\alpha) = P(\theta)$, према индуктивној претпоставци закључујемо да је $\widehat{v_1}(\theta) = \widehat{v_2}(\theta)$. Дакле,

$$\widehat{v_1}(\alpha) = \widehat{v_1}(\neg\theta) = \neg\widehat{v_1}(\theta) = \neg\widehat{v_2}(\theta) = \widehat{v_2}(\neg\theta) = \widehat{v_2}(\alpha).$$

Нека је α формула облика $\theta_1 * \theta_2$, за неке формуле θ_1 и θ_2, и $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.
Ако је $\widehat{v_1}(p) = \widehat{v_2}(p)$, $p \in P(\alpha) = P(\theta_1) \cup P(\theta_2)$, према индуктивној претпоставци је $\widehat{v_1}(\theta_1) = \widehat{v_2}(\theta_1)$ и $\widehat{v_1}(\theta_2) = \widehat{v_2}(\theta_2)$. Дакле,

$$\widehat{v_1}(\alpha) = \widehat{v_1}(\theta_1 * \theta_2) = \widehat{v_1}(\theta_1) * \widehat{v_1}(\theta_2) = \widehat{v_2}(\theta_1) * \widehat{v_2}(\theta_2) = \widehat{v_2}(\theta_1 * \theta_2) = \widehat{v_2}(\alpha).$$

Овим је тврђење у потпуности доказано. □

Према претходној леми, да бисмо одредили истинитосну вредност неке формуле α за неку валуацију v довољно је узети у обзир само рестрикцију валуације v на скуп $P(\alpha)$. Другим речима, довољно је да знамо само које су истинитосне вредности додељене словима из $P(\alpha)$. Ако се у формули α појављује n слова, тј. ако је $|P(\alpha)| = n$, онда постоји укупно 2^n функција из $P(\alpha)$ у $\{0, 1\}$. Ако израчунамо истинитосне вредносте формуле α за сваку од ових 2^n функција, практично смо одредили истинитосне вредности формуле α при било којој валуацији исказних слова. Оваква израчунавања најједноставније приказујемо у облику таблице познате под називом *истинитосна таблица*. У наредном примеру описаћемо уобичајени начин формирања истинитосне таблице неке формуле.

Пример 4. Истинитосна таблица формуле α такве да $|P(\alpha)| = n$, има $2^n + 1$ врста и $|\mathrm{F}(\alpha)|$ колона. У пољима прве врсте наводе се потформуле од α тако да гледано слева на десно не опадају њихове сложености. Тада ће у првих n поља прве врсте бити уписана исказна слова која се појављују у α. Поља испод исказних слова попуњавамо истинитосним вредностима (0 и 1) тако да у првих 2^{n-1} поља испод првог слова уписујемо 0, а у преосталих 2^{n-1} поља уписујемо 1, затим у првих 2^{n-2} поља испод другог слова уписујемо 0, у следећих 2^{n-2} поља уписујемо 1, па у наредних 2^{n-2} поља поново 0, и најзад у преостала поља друге колоне 1, и тако даље, до n-те колоне у којој почев одозго наизменично попуњавамо поља са 0 и 1. Након тога слева надесно попуњавамо колону по колону узимајући у обзир потформулу која је наведена на врху колоне и одговарајуће вредности из колона лево од ње.

Формирајмо истинитосну таблицу формуле $p_1 \wedge \neg(p_2 \Rightarrow p_3)$ чије смо скупове исказних слова и потформула одредили („израчунали“) у примеру 2.

p_1	p_2	p_3	$p_2 \Rightarrow p_3$	$\neg(p_2 \Rightarrow p_3)$	$p_1 \wedge \neg(p_2 \Rightarrow p_3)$
0	0	0	1	0	0
0	0	1	1	0	0
0	1	0	0	1	0
0	1	1	1	0	0
1	0	0	1	0	0
1	0	1	1	0	0
1	1	0	0	1	1
1	1	1	1	0	0

Формирање истинитосних таблица је прилично заморно, и ми ћемо их користити искључиво у једноставним случајевима да бисмо објаснили неке нове појмове. Непрактичност истинитосних таблица најбоље уочавамо при покушају да формирамо таблицу формуле која има много исказних слова. На пример, нека је α нека исказна формула у којој се појављује 25 исказних слова. Да бисмо проценили величину њене истинитосне таблице, искористићемо најгрубљу могућу процену броја њених потформула: $|\mathrm{F}(\alpha)| \geqslant |P(\alpha)| = 25$. Истинитосна таблица ове формуле имаће више од $(2^{25} + 1) \cdot 25 = 838860825$ поља. Ако бисмо сваке секунде попуњавали једно њено поље, онда бисмо целу табелу комплетирали за више од 26 година. $\triangleright$

Задовољиве формуле и таутологије

Дефиниција 5. *Кажемо да је валуација v* **модел** *(реализација) формуле α и пишемо $v \models \alpha$, ако је $\widehat{v}(\alpha) = 1$. Наравно, ако је $\widehat{v}(\alpha) = 0$, онда v није модел за α и пишемо $v \not\models \alpha$.*

Дефиниција 6. *Исказна формула α је*

- ***задовољива*** *ако има модел, тј. постоји валуација v таква да је $v \models \alpha$;*
- ***таутологија*** *ако је свака валуација њен модел, тј. за сваку валуацију v важи $v \models \alpha$. Да је α таутологија означавамо са $\models \alpha$ (остављајући празно место са леве стране знака $\models$ чиме указујемо да се ту може уписати било која валуација).*

ПРИМЕР 5. Да је формула $\neg p_1 \Rightarrow \neg(p_2 \Rightarrow \neg p_1)$ задовољива једноставно уочавамо формирањем њене истинитосне таблице.

p_1	p_2	$\neg p_1$	$p_2 \Rightarrow \neg p_1$	$\neg(p_2 \Rightarrow \neg p_1)$	$\neg p_1 \Rightarrow \neg(p_2 \Rightarrow \neg p_1)$
0	0	1	1	0	0
0	1	1	1	0	0
1	0	0	1	0	1
1	1				

Дату формулу задовољава свака валуација v таква да је $v(p_1) = 1$, $v(p_2) = 0$. Приметимо да попуњавање таблице можемо прекинути када у последњем пољу неке врсте добијемо вредност 1. Као што смо већ истакли, употреба истинитосних таблица је неефикасна и практично је корисна само у неким једноставним случајевима.

Формирање истинитосне таблице свакако бисмо избегавали у случају да треба испитати задовољивост формуле

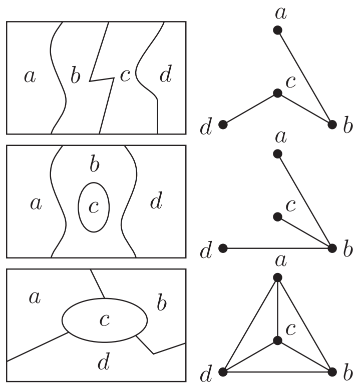
$$(p_1 \vee \neg p_2 \vee p_3) \wedge (p_2 \vee p_4 \vee p_5) \wedge (\neg p_1 \vee \neg p_3 \vee \neg p_5) \wedge (\neg p_1 \vee p_2 \vee p_4) \vee (\neg p_1 \vee p_3 \vee p_5).$$

Наведена формула јесте задовољива, а читаоцима остављамо да открију које истинитосне вредности треба доделити словима која се у формули појављују. $\triangleright$

ПРИМЕР 6. Многи (практични) проблеми[17] еквивалентни су проблему испитивања задовољивости исказних формула[18]. Као илустрацију ове тврдње наводимо један једноставан пример.

[17] налажење оптималног решења неких проблема, шифровање (заштита) података, теоријско рачунарство итд.

[18] Проблем задовољивости исказних формула краће се назива и САТ-проблем (енг. satisfiability – задовољивост). Препоручујемо читаоцу да се путем интернета детаљније информише о овом проблему и његовом значају у математици нашег доба.



За сваку од мапа наведених на сликама десно, треба одредити најмањи број различитих боја потребних да се обоје области a, b, c, d тако да било које две суседне области не буду обојене истом бојом. Читаоцима препуштамо решавање постављеног проблема, уз препоруку да се детаљније упознају, путем интернета, са чувеном *теоремом о четири боје*. Ми ћемо укратко описати како се ови проблеми своде на проблем задовољивости одговарајућих исказних формула.

Приметимо најпре да је за решавање постављеног проблема једино важно колико има области и које две су суседне, па је природно мапе репрезентовати графовима чији чворови одговарају областима и при чему су два чвора спојена ивицом акко су одговарајуће области суседне. Уопште, сваку мапу можемо репрезентовати паром (G, E), где је G неки непразан скуп и $E \subseteq G \times G$ ирефлексивна и симетрична бинарна релација скупа G. На основу ове репрезентације, проблем да ли се нека мапа може обојити у k боја тако да су сваке две суседне области обојене различитим бојама, сводимо на проблем да ли је одговарајући граф (G, E) k-обојив, што значи да ли се G може разбити на k дисјунктних подскупова $C_i \neq \emptyset$, $i = 1, \ldots, k$ ($G = C_1 \cup \cdots \cup C_k$, $C_i \cap C_j = \emptyset$, $1 \leqslant i < j \leqslant k$)[19] тако да суседни чворови нису обојени истом бојом, тј. за све различите a и b из C_i важи $(a, b) \notin E$. Другачије речено, граф (G, E) је k-обојив ако постоји функција $f : G \to \{1, 2, \ldots, k\}$ таква да за све $a, b \in G$, из $(a, b) \in E$ следи $f(a) \neq f(b)$.

Ако је G коначан скуп, бојење графа (G, E) у k боја можемо описати и једном формулом исказног рачуна. Сваком пару $(a, i) \in G \times \{1, \ldots, k\}$ придружимо једно исказно слово $p_{a,i}$. Тада за било који чвор a из G, формула $\alpha_a = \bigvee_{1 \leqslant i \leqslant k} p_{a,i}$ значи да је a обојен бар једном од k датих боја, док формула $\beta_a = \bigwedge_{1 \leqslant i < j \leqslant k} \neg(p_{a,i} \wedge p_{a,j})$ означава да a није обојен двема бојама. За свака два различита чвора a и b из G, формула $\gamma_{a,b} = \bigwedge_{1 \leqslant i \leqslant k} \neg(p_{a,i} \wedge p_{b,i})$ значи да a и b нису обојени истом бојом. Нека је

$$\delta^k_{(G,E)} = \bigwedge_{a \in G} \alpha_a \wedge \bigwedge_{a \in G} \beta_a \wedge \bigwedge_{(a,b) \in E} \gamma_{a,b}.$$

Тврдимо да је граф (G, E) је k-обојив акко је формула $\delta^k_{(G,E)}$ задовољива.

$(\to)$ Ако је граф (G, E) k-обојив, онда постоји функција $f : G \to \{1, 2, \ldots, k\}$ таква да за све $a, b \in G$, из $(a, b) \in E$ следи $f(a) \neq f(b)$. Користећи функцију f дефинишимо валуацију $v : \{p_{a,i} \mid (a, i) \in G \times \{1, \ldots, k\}\} \to \{0, 1\}$ на следећи начин:

$$v(p_{a,i}) = \begin{cases} 1, & f(a) = i, \\ 0, & f(a) \neq i. \end{cases}$$

Није тешко уочити да $v \models \delta^k_{(G,E)}$.

[19] Скуп C_i представља елементе из G који су обојени бојом i.

($\leftarrow$) Претпоставимо да је $\delta^k_{(G,E)}$ задовољива формула, тј. да постоји валуација $v : \{p_{a,i} \mid (a,i) \in G \times \{1,\ldots,k\}\} \to \{0,1\}$ таква да $v \models \delta^k_{(G,E)}$. Нека је

$$f = \{(a,i) \mid v(p_{a,i}) = 1\} \subseteq G \times \{1,2,\ldots,k\}.$$

Из $v \models \alpha_a$ и $v \models \beta_a$, за свако a из G, следи да је f једна функционална релација, тј. да $f : G \to \{1,2,\ldots,k\}$. Из $v \models \gamma_{a,b}$, за све a и b из G такве да $(a,b) \notin E$, следи да је f једно k-бојење графа (G,E). $\triangleright$

На основу дефиниције 6 једноставно закључујемо да нека формула није задовољива ако и само ако је њена негација таутологија. Самим тим, проблем испитивања да ли је нека формула таутологија значајан и у свим контекстима поменутим у претходном примеру. Поред тога, таутологије у извесном смислу репрезентују и *законе мишљења*, о чему ћемо писати касније.

Пример 7. Докажимо да је $\models p_1 \wedge (p_1 \Rightarrow p_2) \Rightarrow p_2$. Формирањем истинитосне таблице једноставно проверавамо да дата формула јесте таутологија.

p_1	p_2	$p_1 \Rightarrow p_2$	$p_1 \wedge (p_1 \Rightarrow p_2)$	$p_1 \wedge (p_1 \Rightarrow p_2) \Rightarrow p_2$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Да је дата формула таутологија можемо доказати на још један начин, тзв. методом свођења на противречност. Претпоставимо да дата формула није таутологија, тј. да постоји валуација v таква да је $\widehat{v}(p_1 \wedge (p_1 \Rightarrow p_2) \Rightarrow p_2) = 0$. Тада мора бити (1) $\widehat{v}(p_1 \wedge (p_1 \Rightarrow p_2)) = 1$ и (2) $\widehat{v}(p_2) = 0$. Из (1) следи да је $\widehat{v}(p_1) = 1$ и $\widehat{v}(p_1 \Rightarrow p_2) = 1$. Из последње једнакости добијамо да је $\widehat{v}(p_1) = 1$ и $\widehat{v}(p_2) = 1$. На овај начин, долазимо до контрадикције, јер није могуће да буде $\widehat{v}(p_2) = 0$ и $\widehat{v}(p_2) = 1$. Дакле, дата формула јесте таутологија. $\triangleright$

Пример 8. Ако су α и β било које исказне формуле, онда је $\models \alpha \wedge (\alpha \Rightarrow \beta) \Rightarrow \beta$. Ово тврђење једноставно доказујемо методом свођења на противречност, поступајући као у претходном примеру. $\triangleright$

Претходна два примера илуструју следеће опште тврђење: *ако у таутологији исказна слова истовремено заменимо било којим формулама тако што свако слово мењамо увек истом формулом, онда ће добијена формула такође бити таутологија*. Пре него што строго докажемо наведено тврђење, индукцијом по сложености формуле α дефинишемо формулу $\alpha(p/\theta)$ која се добија из α истовременом заменом свих појављивања слова p у формули α формулом θ:

- ако је α логичка константа или исказно слово q различито од p, онда је $\alpha(p/\theta) \overset{\text{def}}{=} \alpha$;

- ако је α исказно слово p, онда је $\alpha(p/\theta) \stackrel{\text{def}}{=} \theta$;
- ако је $\alpha = \neg\varphi$, за неку формулу φ, онда је $\alpha(p/\theta) \stackrel{\text{def}}{=} \neg(\varphi(p/\theta))$;
- ако је $\alpha = \varphi * \psi$, за неке формуле φ и ψ и $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, онда је $\alpha(p/\theta) \stackrel{\text{def}}{=} \varphi(p/\theta) * \psi(p/\theta)$.

Уведимо још једну ознаку. Ако је $v : P \to \{0,1\}$ валуација, $p \in P$ и $i \in \{0,1\}$, онда са $v(p/i)$ означавамо валуацију која свим исказним словима додељује исте вредности као и v, осим слову p коме додељује вредност i. Другим речима, $v(p/i) : P \to \{0,1\}$ при чему је:

$$v(p/i)(x) = \begin{cases} v(x), & x \neq p, \\ i, & x = p. \end{cases}$$

Лема 3. *Нека су α и θ произвољне формуле и p било које исказно слово. Тада за сваку валуацију v важи $\widehat{v}(\alpha(p/\theta)) = \widehat{w}(\alpha)$, где је $w = v(p/\widehat{v}(\theta))$.*

Доказ. Доказ изводимо индукцијом по сложености формуле α.

Ако је α логичка константа или исказно слово q различито од p, онда је $\alpha(p/\theta) \stackrel{\text{def}}{=} \alpha$. Пошто $p \notin P(\alpha)$, према леми 2 имамо да је $\widehat{v}(\alpha(p/\theta)) = \widehat{v}(\alpha) = \widehat{w}(\alpha)$.

Нека је α исказно слово p. Тада је $\alpha(p/\theta) = \theta$, па је $\widehat{v}(\alpha(p/\theta)) = \widehat{v}(\theta)$. Поред тога, имамо да је $\widehat{w}(\alpha) = \widehat{w}(p) = w(p) = v(p/\widehat{v}(\theta))(p) = \widehat{v}(\theta)$, па је тврђење у овом случају доказано.

Претпоставимо да је $\alpha = \neg\varphi$, за неку формулу φ. У овом случају користимо индуктивну претпоставку према којој је $\widehat{v}(\varphi(p/\theta)) = \widehat{w}(\varphi)$, па је

$$\widehat{v}(\alpha(p/\theta)) = \neg\widehat{v}(\varphi(p/\theta)) = \neg\widehat{w}(\varphi) = \widehat{w}(\alpha).$$

Читаоцима препуштамо случај када је $\alpha = \varphi * \psi$, за неке формуле φ и ψ и $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$. □

Последица 1. *Ако је $\models \alpha$, онда је $\models \alpha(p/\theta)$, за било које слово p и било коју формулу θ.*

Доказ. Нека је v произвољна валуација. Треба да докажемо да $v \models \alpha(p/\theta)$. Према претходној леми је $\widehat{v}(\alpha(p/\theta)) = \widehat{w}(\alpha)$, где је $w = v(p/\widehat{v}(\theta))$. Како је α таутологија, имамо да је $\widehat{w}(\alpha) = 1$, па је и $\widehat{v}(\alpha(p/\theta)) = 1$, тј. $v \models \alpha(p/\theta)$. □

У наставку, ослањаћемо се на претходну последицу без експлицитног позивања на њу. На пример, ако знамо да је $\models (p_1 \vee p_2) \vee p_3 \Leftrightarrow p_1 \vee (p_2 \vee p_3)$, подразумеваћемо и да је $\models (\alpha \vee \beta) \vee \gamma \Leftrightarrow \alpha \vee (\beta \vee \gamma)$, за било које формуле α, β, γ.

Подугачак је списак таутологија које већ познајемо јер их добијамо на основу Булових закона о којима је било речи у претходном поглављу. Већ смо више пута истакли да исказне формуле можемо посматрати и као алгебарске изразе, као и да је истинитосна вредност формуле при задатој валуацији заправо вредност израза у исказној алгебри при тој валуацији. Будући да је исказна алгебра једноставно проширење Булове алгебре **2**, директно добијамо таутологије набројане у наредној леми.

Лема 4. *За било које формуле α, β, γ, следеће формуле су таутологије:*

($\mathbf{A}^{\vee}$) $\alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$;	($\mathbf{A}^{\wedge}$) $\alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge \gamma$;
($\mathbf{K}^{\vee}$) $\alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$;	($\mathbf{K}^{\wedge}$) $\alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$;
($\mathbf{D}^{\vee}_{\wedge}$) $\alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$;	($\mathbf{D}^{\wedge}_{\vee}$) $\alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$;
($\mathbf{C}^{\vee}$) $\alpha \vee \neg\alpha \Leftrightarrow \top$;	($\mathbf{C}^{\wedge}$) $\alpha \wedge \neg\alpha \Leftrightarrow \bot$;
($\mathbf{N}^{\vee}$) $\alpha \vee \bot \Leftrightarrow \alpha$;	($\mathbf{N}^{\wedge}$) $\alpha \wedge \top \Leftrightarrow \alpha$.

Ако узмемо у обзир и Булове законе доказане у лемама 1 и 2 претходног поглавља, добијамо још таутологија.

Лема 5. *За било које формуле α, β, γ, следеће формуле су таутологије:*

$\alpha \vee \alpha \Leftrightarrow \alpha$;	$\alpha \wedge \alpha \Leftrightarrow \alpha$;	[*закони идемпотентности*]
$\alpha \vee \top \Leftrightarrow \top$;	$\alpha \wedge \bot \Leftrightarrow \bot$;	
$\alpha \vee (\alpha \wedge \beta) \Leftrightarrow \alpha$;	$\alpha \wedge (\alpha \vee \beta) \Leftrightarrow \alpha$;	[*закони апсорпције*]
$\neg\neg\alpha \Leftrightarrow \alpha$;		[*закони двојне негације*]
$\neg(\alpha \vee \beta) \Leftrightarrow \neg\alpha \wedge \neg\beta$;	$\neg(\alpha \wedge \beta) \Leftrightarrow \neg\alpha \vee \neg\beta$.	[*Де Морганови закони*]

Линденбаумова алгебра

Све таутологије набројане у претходне две леме говоре о еквиваленцији неких формула, и као такве посебно су важне за проучавање исказне логике. Зато истичемо нека општа запажања. Ако је $\models \alpha \Leftrightarrow \beta$, онда се α и β семантички не разликују у смислу да за сваку валуацију v важи $\widehat{v}(\alpha) = \widehat{v}(\beta)$, па кажемо да су α и β *семантички еквивалентне*[20]. Уместо $\models \alpha \Leftrightarrow \beta$, краће се пише $\alpha \equiv \beta$. Није тешко уочити да је $\equiv$ релација еквиваленције на скупу свих формула:

(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 (очигледно је да из $\models \alpha \Leftrightarrow \beta$ следи $\models \beta \Leftrightarrow \alpha$);

[20]Изрази α и β имају исте вредности за све вредности промењљивих из $\{0, 1\}$

(T) 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 $\models \alpha \Leftrightarrow \gamma$).

Нека је $\|\alpha\| = \{\varphi \in \mathrm{For} \mid \alpha \equiv \varphi\}$ класа еквиваленције одређена формулом α у односу на релацију $\equiv$, тј. скуп свих формула које су семантички еквивалентне формули α. Наравно, $\|\alpha\| = \|\beta\|$ акко $\alpha \equiv \beta$. Означимо са B_P скуп свих класа еквиваленције одређених исказним формулама са словима из скупа P, $B_P = \{\|\alpha\| \mid \alpha \in \mathrm{For}\}$. На овом скупу дефинишемо две бинарне операције $\curlyvee$ и $\curlywedge$, и једну унарну $'$ на следећи начин:

$$\|\alpha\| \curlyvee \|\beta\| = \|\alpha \vee \beta\|,\ \|\alpha\| \curlywedge \|\beta\| = \|\alpha \wedge \beta\|,\ \|\alpha\|' = \|\neg\alpha\|.$$

Није тешко проверити да су операције добро дефинисане:

($\curlyvee$) ако је $\|\alpha\| = \|\alpha_1\|$ и $\|\beta\| = \|\beta_1\|$, онда је $\|\alpha\| \curlyvee \|\beta\| = \|\alpha_1\| \curlyvee \|\beta_1\|$, што директно следи из тврђења које се једноставно доказује: ако је $\alpha \equiv \beta$ и $\alpha_1 \equiv \beta_1$, онда је $\alpha \vee \alpha_1 \equiv \beta \vee \beta_1$;

($\curlywedge$) ако је $\|\alpha\| = \|\alpha_1\|$ и $\|\beta\| = \|\beta_1\|$, онда је $\|\alpha\| \curlywedge \|\beta\| = \|\alpha_1\| \curlywedge \|\beta_1\|$, што директно следи из следећег тврђења: ако је $\alpha \equiv \beta$ и $\alpha_1 \equiv \beta_1$, онда је $\alpha \wedge \alpha_1 \equiv \beta \wedge \beta_1$;

($'$) ако је $\|\alpha\| = \|\alpha_1\|$, онда је $\|\alpha\|' = \|\alpha_1\|'$, што следи из следећег тврђења: ако је $\alpha \equiv \alpha_1$, онда је $\neg\alpha \equiv \neg\alpha_1$.

Означимо $\|\bot\|$ са 0 и $\|\top\|$ са 1. Приметимо да је:

- α таутологија акко је $\|\alpha\| = 1$;
- α задовољива акко је $\|\alpha\| \neq 0$.

Тада је $\mathbf{B}_P = (B_P, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра, тј. за произвољне формуле α, β, γ важи:

$\mathbf{A}^{\curlyvee}$	$\|\alpha\| \curlyvee (\|\beta\| \curlyvee \|\gamma\|) = (\|\alpha\| \curlyvee \|\beta\|) \curlyvee \|\gamma\|$	$\mathbf{A}^{\curlywedge}$	$\|\alpha\| \curlywedge (\|\beta\| \curlywedge \|\gamma\|) = (\|\alpha\| \curlywedge \|\beta\|) \curlywedge \|\gamma\|$
$\mathbf{K}^{\curlyvee}$	$\|\alpha\| \curlyvee \|\beta\| = \|\beta\| \curlyvee \|\alpha\|$	$\mathbf{K}^{\curlywedge}$	$\|\alpha\| \curlywedge \|\beta\| = \|\beta\| \curlywedge \|\alpha\|$
$\mathbf{D}^{\curlyvee}_{\curlywedge}$	$\|\alpha\| \curlyvee (\|\beta\| \curlywedge \|\gamma\|) = (\|\alpha\| \curlyvee \|\beta\|) \curlywedge (\|\alpha\| \curlyvee \|\gamma\|)$	$\mathbf{D}^{\curlywedge}_{\curlyvee}$	$\|\alpha\| \curlywedge (\|\beta\| \curlyvee \|\gamma\|) = (\|\alpha\| \curlywedge \|\beta\|) \curlyvee (\|\alpha\| \curlywedge \|\gamma\|)$
$\mathbf{C}^{\curlyvee}$	$\|\alpha\| \curlyvee \|\alpha\|' = 1$	$\mathbf{C}^{\curlywedge}$	$\|\alpha\| \curlywedge \|\alpha\|' = 0$
$\mathbf{N}^{\curlyvee}$	$\|\alpha\| \curlyvee 0 = \|\alpha\|$	$\mathbf{N}^{\curlywedge}$	$\|\alpha\| \curlywedge 1 = \|\alpha\|$

Доказ наведених особина препуштамо читаоцима. Уместо упутства, наводимо доказ особине $\mathbf{A}^{\curlyvee}$.

$$\begin{aligned} \|\alpha\| \curlyvee (\|\beta\| \curlyvee \|\gamma\|) &= \|\alpha \vee (\beta \vee \gamma)\| \\ &= \|(\alpha \vee \beta) \vee \gamma\| \quad [\text{јер је } \alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma] \\ &= (\|\alpha\| \curlyvee \|\beta\|) \curlyvee \|\gamma\| \end{aligned}$$

Булова алгебра $\mathbf{B}_P$ назива се *Линденбаумова алгебра* исказне логике. Уређење Линденбаумове алгебре дефинише се као и у свакој другој Буловој алгебри (страна 23): $\|\alpha\| \preccurlyeq \|\beta\|$ акко $\|\alpha\| \curlyvee \|\beta\| = \|\beta\|$, односно $\|\alpha \vee \beta\| = \|\beta\|$. Није тешко уочити да важи: $\alpha \vee \beta \equiv \beta$ акко $\models \alpha \Rightarrow \beta$. Дакле, $\|\alpha\| \preccurlyeq \|\beta\|$ акко $\models \alpha \Rightarrow \beta$.

Нормалне форме

Свака исказна формула $\alpha(p_1, \ldots, p_n)$ дефинише један n-арни логички везник[21]: $f_\alpha : 2^n \to 2$, при чему је за $(a_1, \ldots, a_n) \in 2^n$, $f_\alpha(a_1, \ldots, a_n)$ истинитосна вредност формуле α за валуацију v такву да је $v(p_i) = a_i$, $1 \leqslant i \leqslant n$, тј. $f_\alpha(a_1, \ldots, a_n) = \widehat{v}(\alpha)$ (подсећамо на лему 2). Заправо, f_α је функција дефинисана истинитосном таблицом формуле α. Очигледно, две семантички еквивалентне формуле $\alpha(p_1, \ldots, p_n)$ и $\beta(p_1, \ldots, p_n)$ одређују исти n-арни логички везник. На основу резултата из претходног поглавља (страна 20) имамо и да за било које $(x_1, \ldots, x_n) \in 2^n$ важи

$$f_\alpha(x_1, \ldots, x_n) = \bigvee_{(a_1, \ldots, a_n) \in 2^n} (f_\alpha(a_1, \ldots, a_n) \wedge x_1^{a_1} \wedge \cdots \wedge x_n^{a_n})$$

где x^0 означава $\neg x$, а x^1 означава x. Одавде директно изводимо следећи закључак.

Лема 6. *Свака задовољива формула $\alpha(p_1, \ldots, p_n)$ семантички је еквивалентна исказној формули*

$$\text{(KDNF)} \qquad \bigvee_{\widehat{v}(\alpha)=1} \left(p_1^{v(p_1)} \wedge \cdots \wedge p_n^{v(p_n)}\right),$$

при чему је број дисјунката последње формуле једнак броју уређених n-торки $(a_1, \ldots, a_n) \in 2^n$, таквих да за валуацију v, $v(p_i) = a_i$, $1 \leqslant i \leqslant n$, важи $\widehat{v}(\alpha) = 1$ (из претпоставке да је α задовољива формула, следи да постоји бар једна оваква валуација).

Формула (KDNF) из претходне леме назива се *канонска дисјунктивна нормална форма* формуле α. Често се по договору узима да је формула $\perp$ канонска дисјунктивна нормална форма незадовољиве формуле. Аналогно долазимо и до следећег закључка (видети задатак 14 на страни 34).

[21] тј. један n-арну операцију скупа $2 = \{0, 1\}$ (видети страну 22)

Лема 7. *Свака формула $\alpha(p_1, \dots, p_n)$ која није таутологија семантички је еквивалентна исказној формули*

$$\text{(KKNF)} \qquad \bigwedge_{\widehat{v}(\alpha)=0} \left(p_1^{v(\neg p_1)} \vee \dots \vee p_n^{v(\neg p_n)}\right),$$

при чему је број конјуката последње формуле једнак броју уређених n-торки $(a_1, \dots, a_n) \in 2^n$, таквих да за валуацију v, $v(p_i) = a_i$, $1 \leqslant i \leqslant n$, важи $\widehat{v}(\alpha) = 0$ (из претпоставке да α није таутологија, следи да постоји бар једна оваква валуација).

Формула (KKNF) из претходне леме назива се *канонска конјунктивна нормална форма* формуле α. По договору се узима да је формула $\top$ канонска конјунктивна нормална форма таутологије. Грубо говорећи, канонске нормалне форме неке формуле јесу заправо описи истинитосне таблице те формуле. Ако је дата истинитосна таблица формуле, онда из њих директно читамо и канонске нормалне форме те формуле (видети пример 11 на страни 23). Такође, ако познајемо канонску дисјунктивну или конјунктивну нормалну форму формуле, онда једноставно конструишемо и њену таблицу. Пошто је формирање истинитосних таблица неефикасно (подсећамо на коментаре из примера 4 овог поглавља), углавном се трага за нормалним формама које нису канонске.

Дефиниција 7. *Формула је у дисјунктивној (конјунктивној) нормалној форми ако је облика $\bigvee_{i \in I} \bigwedge_{j \in J_i} p_{ij}^{a_{ij}}$ $\left(\bigwedge_{i \in I} \bigvee_{j \in J_i} p_{ij}^{a_{ij}}\right)$, за неке коначне скупове I и J_i, и неке $a_{ij} \in \{0, 1\}$, при чему су p_{ij} исказна слова.*

Примери формула у днф су: $p_1 \wedge \neg p_2$, $(p_1 \wedge p_2 \wedge p_3) \vee (\neg p_1 \wedge p_3)$, итд. Примери формула у кнф су: $p_1 \wedge \neg p_2$, $(p_1 \vee p_2 \wedge p_3) \wedge (\neg p_1 \vee p_3)$, $p_0 \vee \neg p_0$ итд. Очигледно, свака исказна формула је семантички еквивалентна некој формули која је у днф, као и некој формули која је у кнф. У наредном примеру описаћемо једноставан поступак како се могу добити ове форме.

ПРИМЕР 9. Дисјунктивну (конјунктивну) нормалну форму неке формуле једноставно налазимо спроводећи следећи поступак:

1. елиминисати везник $\Leftrightarrow$ користећи семантичку еквиваленцију: $\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$;
2. елиминисати везник $\Rightarrow$ користећи семантичку еквиваленцију: $\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$;
3. док год је могуће примењивати Де Морганове законе (тј. док год се све негације не „спусте“ до исказних слова и логичких константи), $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$ и $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$;

4. елиминисати вишеструке негације и негације константи користећи логичке еквиваленције:
$\neg\neg\alpha \equiv \alpha$, $\neg\bot \equiv \top$ и $\neg\top \equiv \bot$;

5. на формулу добијену у претходном кораку примењивати семантичке еквиваленције које произлазе из дистрибутивног $\mathbf{D}^{\wedge}_{\vee}$ (односно $\mathbf{D}^{\vee}_{\wedge}$), асоцијативног и комутативног закона, уз одговарајућу елиминацију константи, док год се не добије израз у днф (односно кнф).

Наравно, редослед корака можемо по потреби модификовати и прилагодити га датој ситуацији. Поред тога, форме добијене претходним поступком можемо додатно поједноставити применом семантичких еквиваленција: $\alpha\vee\alpha \equiv \alpha$, $\alpha\wedge\alpha \equiv \alpha$, $\alpha\vee\neg\alpha \equiv \top$, $\alpha \wedge \neg\alpha \equiv \bot$ итд.

Нађимо описаним поступком нормалне форме формуле $\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3)$.

ДНФ		КНФ	
	$\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3)$		$\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3)$
$\equiv$	$\neg\neg(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$	$\equiv$	$\neg\neg(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$
$\equiv$	$\neg p_1 \vee p_2 \vee (\neg p_1 \wedge p_3)$	$\equiv$	$(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$
		$\equiv$	$(\neg p_1 \vee p_2 \vee \neg p_1) \wedge (\neg p_1 \vee p_2 \vee p_3)$
		$\equiv$	$(\neg p_1 \vee p_2) \wedge (\neg p_1 \vee p_2 \vee p_3)$

Добијене нормалне форме прилично су информативне. Тако, из днф једноставно налазимо валуацију која задовољава дату формулу (на пример, било која валуација за коју је $p_1 \mapsto 0$), а из кнф валуацију која је не задовољава (на пример, $p_1 \mapsto 1, p_2 \mapsto 0$). Препуштамо читаоцима да пронађу још неке валуације које (не) задовољавају дату формулу. $\triangleright$

У претходном примеру смо видели да је днф неке формуле погодна да се утврди да ли је нека формула задовољива, а кнф помаже да се открије да формула није таутологија. У општем случају, днф формуле није погодна да се испита да ли је формула таутологија, док кнф није погодна за испитивање задовољивости формуле[22].

Пример 10. Без много детаља, показаћемо како се проблем задовољивости неке формуле у кнф може свести на проблем испитивања да ли неки граф има тзв. Хамилтонов циклус. Нека је $\mathbf{G} = (G, E)$, $E \subseteq G \times G$, неки коначан граф, $G = \{v_1, v_2, \ldots, v_k\}$. Хамилтонов циклус графа $\mathbf{G}$ јесте пут који кроз сваки чвор пролази тачно једанпут и завршава се тамо одакле је почео, тј. пермутација чворова $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ таква да $(v_{i_1}, v_{i_2}), \ldots, (v_{i_{k-1}}, v_{i_k}), (v_{i_k}, v_{i_1}) \in E$.

Нека је α формула у кнф, при чему се свако исказно слово у сваком конјункту појављује највише једном. Описаћемо како се конструише граф $\mathbf{G}_\alpha$ такав да важи

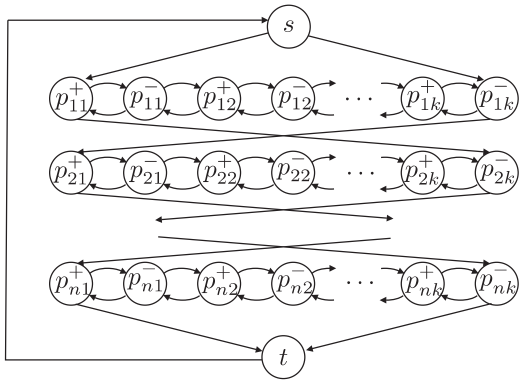
$(*)$ $\qquad$ α је задовољива формула акко $\mathbf{G}_\alpha$ садржи Хамилтонов циклус.

[22] Трагање за **ефикасним** поступком за испитивање да ли је задовољива формула у конјунктивној нормалној форми представља важну област истраживања. Наравно постоји и могућност да такав поступак не постоји.

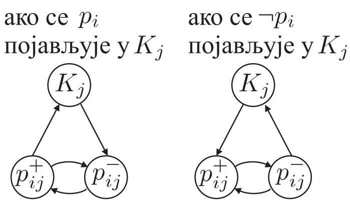
Претпоставимо да се у α појављује n исказних слова, $p_1, \dots, p_n$ и да α има k конјуката, $K_1, \dots, K_k$. Дакле, α је облика $K_1 \wedge \dots \wedge K_k$, и свако K_j је облика $p_{j_1}^{a_{j_1}} \vee \dots \vee p_{j_\ell}^{a_{j_\ell}}$, за неке $a_{j_1}, \dots, a_{j_\ell} \in \{0,1\}$ и неке различите $j_1, \dots, j_\ell \in \{1, \dots, n\}$.

Граф $\mathbf{G}_\alpha$ садржи $2nk+k+2$ чвора који су повезани као што је описано у наставку.

Сваком слову p_i, $i = 1, \dots, n$ одговара $2k$ чворова које ћемо означавати са p_{ij}^+ и p_{ij}^-, $j = 1, \dots, k$. Поред ових чворова додајемо још два чвора s и t. Наведене чворове повезујемо као на наредној слици.



Нацртаној слици додајемо још k чворова означених са $K_1, \dots, K_k$, при чему сваки K_j повезујемо са p_{ij}^+ и p_{ij}^- само ако се слово p_i појављује у конјункту K_j водећи рачуна да ли се у K_j појављује p_i или $\neg p_i$. Нове ивице цртамо у складу са наредном илустрацијом.



Препуштамо читаоцима да се увере у тачност тврђења $(*)$. Препоручујемо да најпре формирате одговарајуће графове неких једноставних формула од којих једна јесте задовољива (као на пример, $p_1 \wedge \neg p_2$), а једна није (на пример, $p_1 \wedge \neg p_2 \wedge (\neg p_1 \vee p_2)$), а затим и потражите Хамилтонове циклусе у тим графовима. $\triangleright$

Потпуни системи везника

Није тешко закључити на основу досадашњих разматрања да смо у алфабет исказне логике, поред исказних слова и помоћних симбола, могли да ставимо само знаке за дисјункцију, конјункцију и негацију. Уопште, сматрајући логичке константе $\top$ и $\bot$ логичким везницима дужине 0, ако са $\mathcal{C}$ означимо неки коначан скуп логичких везника, скуп формула $\mathrm{For}(\mathcal{C})$ над алфабетом $\mathcal{A}(\mathcal{C}) = P \cup \{(,)\} \cup \mathcal{C}$ (који садржи исказна слова из P, леву и десну заграду и знаке за везнике из $\mathcal{C}$) дефинишемо на очекивани начин: $\mathrm{For}(\mathcal{C})$ је најмањи скуп речи над алфабетом $\mathcal{A}(\mathcal{C})$ такав да важи:

- исказна слова из P и логички везници дужине 0, уколико су у $\mathcal{C}$, припадају $\mathrm{For}(\mathcal{C})$;
- ако је $F \in \mathcal{C}$ логички везник дужине $n \geqslant 1$ и $\alpha_1, \ldots, \alpha_n \in \mathrm{For}(\mathcal{C})$, онда $F(\alpha_1, \ldots, \alpha_n) \in \mathrm{For}(\mathcal{C})$.

Приметимо да је раније дефинисан скуп исказних формула For једнак $\mathrm{For}(\{\bot, \top, \neg, \vee, \wedge, \Rightarrow, \Leftrightarrow\})$.

Било која валуација $v : P \to \{0,1\}$ природно се проширује до функције $\widehat{v} : \mathrm{For}(\mathcal{C}) \to \{0,1\}$: $\widehat{v}(p) = v(p)$, $\widehat{v}(\bot) = 0$, $\widehat{v}(\top) = 1$ (ако $\bot, \top \in \mathcal{C}$),

$$\widehat{v}(F(\alpha_1, \ldots, \alpha_n)) = F(\widehat{v}(\alpha_1), \ldots, \widehat{v}(\alpha_n)),\ F \in \mathcal{C} \setminus \{\top, \bot\}.$$

Самим тим, свака формула $\alpha(p_1, \ldots, p_n)$ из $\mathrm{For}(\mathcal{C})$, на природан начин, одређује један n-арни логички везник који ћемо означити са f_α.

Дефиниција 8. *Скуп логичких везника $\mathcal{C}$ је **потпун**, ако за сваку функцију $f : 2^n \to 2$, постоји формула $\alpha(p_1, \ldots, p_n) \in \mathrm{For}(\mathcal{C})$ таква да је $f = f_\alpha$.*

Као што смо видели, пример потпуног система везника јесте $\{\neg, \vee, \wedge\}$. То значи да се, приликом проучавања исказне логике, можемо ограничити само на формуле скупа $\mathrm{For}(\{\neg, \vee, \wedge\})$. У том случају, $\bot$ уводимо као скраћење формуле $p \wedge \neg p$, за неко исказно слово p, $\top$ као скраћење за $\neg\bot$, $\alpha \Rightarrow \beta$ као скраћење за $\neg\alpha \vee \beta$, и најзад $\alpha \Leftrightarrow \beta$ као скраћење за $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, односно $(\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha)$.

Ако се сетимо Де Моргановог закона, једноставно уочавамо да је и $\{\neg, \vee\}$ потпун систем везника, те да се могу узети у обзир само формуле из $\mathrm{For}(\{\neg, \vee\})$, при чему би се, на пример, $\alpha \wedge \beta$ схватило као скраћење за $\neg(\neg\alpha \vee \neg\beta)$.

У литератури се често под исказним формулама подразумевају само формуле скупа $\mathrm{For}(\{\neg, \Rightarrow\})$, што је оправдано чињеницом да је $\{\neg, \Rightarrow\}$ потпун систем везника. При томе се подразумевају следећа скраћења:
$\top$ за $p \Rightarrow p$, где је p неко исказно слово,
$\bot$ за $\neg\top$, тј. $\neg(p \Rightarrow p)$,
$\alpha \vee \beta$ за $\neg\alpha \Rightarrow \beta$,
$\alpha \wedge \beta$ за $\neg(\alpha \Rightarrow \neg\beta)$,
$\alpha \Leftrightarrow \beta$ за $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, тј. $\neg((\alpha \Rightarrow \beta) \Rightarrow \neg(\beta \Rightarrow \alpha))$.

Приметимо најзад, да се можемо ограничити и на скуп $\mathrm{For}(\{\bot, \Rightarrow\})$, јер $\neg\alpha$ можемо схватити као скраћење формуле $\alpha \Rightarrow \bot$.

Пример 11. Испитајмо да ли је $\{\top, \Rightarrow\}$ потпун систем везника. Да бисмо доказали да је наведени скуп везника потпун, довољно је формулама које одговарају том скупу везника представити све функције које репрезентују везнике неког потпуног система. Или, наспупрот овоме, пронаћи истинитосну функцију коју није могуће представити формулом из $\mathrm{For}(\{\top, \Rightarrow\})$. Будући да знамо да негација и импликација образују потпун систем везника, испитајмо да ли се функција $\neg : 2 \to 2$, $\neg 0 = 1$, $\neg 1 = 0$ може представити неком формулом $\alpha(p) \in \mathrm{For}(\{\top, \Rightarrow\})$. Покушаји да се пронађе жељена формула[23] неуспешно се завршавају јер таква формула не постоји. Да бисмо то и доказали, треба да уочимо каква може бити истинитосна функција одређена формулом $\alpha(p)$. Није тешко приметити да могу да наступе две случаја, или је $\alpha(p) \equiv \top$ или је $\alpha(p) \equiv p$. Доказ изводимо индукцијом по сложености формуле.

Ако је $\alpha(p)$ сложености нула, онда је $\alpha(p)$ заправо исказно слово p и наше је тврђење очигледно тачно.

Претпоставимо да је тврђење тачно за све формуле сложености мање од n, за неко $n > 0$, и нека је $\alpha(p)$ сложености n. Тада је $\alpha(p)$ облика $\varphi(p) \Rightarrow \psi(p)$. Позивајући се на индуктивну претпоставку разликујемо четири случаја.
1. случај: $\varphi(p) \equiv \top$ и $\psi(p) \equiv \top$. Тада је $\alpha(p) \equiv (\top \Rightarrow \top) \equiv \top$;
2. случај: $\varphi(p) \equiv p$ и $\psi(p) \equiv \top$. Тада је $\alpha(p) \equiv (p \Rightarrow \top) \equiv \top$;
3. случај: $\varphi(p) \equiv \top$ и $\psi(p) \equiv p$. Тада је $\alpha(p) \equiv (\top \Rightarrow p) \equiv p$;
4. случај: $\varphi(p) \equiv p$ и $\psi(p) \equiv p$. Тада је $\alpha(p) \equiv (p \Rightarrow p) \equiv \top$.

Дакле, ако $\alpha(p) \in \mathrm{For}(\{\top, \Rightarrow\})$, онда је или $\alpha(0) = \alpha(1) = 1$, или је $\alpha(0) = 0$ и $\alpha(1) = 1$, што значи да се негација не може представити оваквим формулама. $\triangleright$

Семантичка последица

Појам семантичке последице најпре ћемо илустровати примером.

Пример 12. Докажимо да из $\models \alpha$ и $\models \alpha \Rightarrow \beta$, следи да је и $\models \beta$. Нека је v произвољна валуација. Тада $v \models \alpha$ и $v \models \alpha \Rightarrow \beta$, тј. $\widehat{v}(\alpha) = 1$ и $\widehat{v}(\alpha \Rightarrow \beta) = 1$. Из последње две једнакости једноставно закључујемо да мора бити и $\widehat{v}(\beta) = 1$, тј. $v \models \beta$.

Приметимо да смо доказали и општије тврђење: *за сваку валуацију v, из $v \models \alpha$ и $v \models \alpha \Rightarrow \beta$ следи да $v \models \beta$*. Другим речима, ако су при некој валуацији тачне формуле α и $\alpha \Rightarrow \beta$, при истој валуацији мора бити тачна и формула β. Природно је сматрати да је β својеврсна последица формула α и $\alpha \Rightarrow \beta$. $\triangleright$

Као што је наговештено у претходном примеру, занимаће нас када је нека формула последица (закључак) неког скупа претпоставки (премиса). Иначе, извлачење закључка из неког скупа претпоставки јесте мисаона радња, тзв. *дедуктивно закључивање*, којој се посвећује велика пажња још од традиционалне логике па све до савремене математичке логике. Давно је формулисан општи услов који мора испуњавати свако дедуктивно закључивање. Услов је познат под називом salva veritate и гласи *приликом извођења закључака не сме*

[23] $\top \Rightarrow p, p \Rightarrow \top, p \Rightarrow (\top \Rightarrow p), (p \Rightarrow \top) \Rightarrow p, \ldots$

се наносити штета истинитости, односно ако су премисе истините, онда је и закључак истинит.

Дефиниција 9. *Валуација v задовољава скуп исказних формула Γ, $\Gamma \subseteq \mathrm{For}_{\mathcal{L}}$, или v је модел скупа Γ, у ознаци $v \models \Gamma$, ако $v \models \gamma$, за свако $\gamma \in \Gamma$.*

Дефиниција 10. *Нека је Γ неки скуп исказних формула ($\Gamma \subseteq \mathrm{For}_{\mathcal{L}}$) и α нека формула. Формула α је* ***семантичка последица*** *скупа Γ, у ознаци $\Gamma \models \alpha$, ако за сваку валуацију $v : P \to \{0,1\}$, из $v \models \Gamma$ следи $v \models \alpha$.*

Скуп Γ у претходној дефиницији може бити било какав скуп формула (коначан или бесконачан). Семантичка последица $\models$ јесте заправо релација која повезује скуп формула са неком формулом, $\models \subseteq \mathcal{P}(\mathrm{For}) \times \mathrm{For}$.

Да бисмо поједноставили записивање, уместо $\{\gamma_1, \dots, \gamma_k\} \models \alpha$ (тј. у случају да је Γ коначан скуп $\{\gamma_1, \dots, \gamma_k\}$), писаћемо $\gamma_1, \dots, \gamma_k \models \alpha$. Такође, уместо $\Gamma \cup \{\gamma\} \models \alpha$, писаћемо краће $\Gamma, \gamma \models \alpha$. Приметимо и да $\emptyset \models \alpha$ значи да је α таутологија, тј. $\models \alpha$.

Пример 13. Из претходног примера закључујемо да је $p_1, p_1 \Rightarrow p_2 \models p_2$.

Да је $p_1 \Rightarrow p_3, p_2 \Rightarrow p_3 \models p_1 \vee p_2 \Rightarrow p_3$ можемо доказати као у претходном примеру, или формирати истинитосну таблицу и уочити да када год су обе формуле $p_1 \Rightarrow p_3$ и $p_2 \Rightarrow p_3$ тачне, тада је тачна и формула $p_1 \vee p_2 \Rightarrow p_3$.

p_1	p_2	p_3	$p_1 \Rightarrow p_3$	$p_2 \Rightarrow p_3$	$p_1 \vee p_2$	$p_1 \vee p_2 \Rightarrow p_3$
0	0	0	**1**	**1**	0	**1**
0	0	1	**1**	**1**	0	**1**
0	1	0	1	0	1	0
0	1	1	**1**	**1**	1	**1**
1	0	0	0	1	1	0
1	0	1	**1**	**1**	1	**1**
1	1	0	0	0	1	0
1	1	1	**1**	**1**	1	**1**

Препуштамо читаоцима да образложе наредне чињенице:

- $p_1 \models p_2 \Rightarrow p_1$;
- $p_1, \neg p_2 \Rightarrow \neg p_1 \models p_2$;
- $p_1, \neg p_1 \models p_2$;
- $p_1 \vee \neg p_1 \models p_1 \Rightarrow p_1$;
- $p_1, \neg p_1 \vee (p_2 \Rightarrow \neg p_1) \models \neg(p_1 \Rightarrow p_2)$.

$\triangleright$

У наредној теореми издвајамо неке очигледне особине семантичке последице.

Теорема 1. *Нека је Γ произвољан скуп формула и α нека формула.*

1. *Ако $\alpha \in \Gamma$, онда $\Gamma \models \alpha$.*

2. *Ако $\Gamma \models \alpha$ и $\Gamma \subseteq \Delta$, онда $\Delta \models \alpha$.*

3. *Ако $\Gamma \models \alpha$ и $\models \tau$, онда $\Gamma \setminus \{\tau\} \models \alpha$.*

4. *Ако је $\models \alpha$, онда $\Gamma \models \alpha$, за сваки скуп формула Γ.*

5. *Ако $\Gamma \models \bot$, онда $\Gamma \models \alpha$, за сваку формулу α.*

Доказ. Докази наведених тврђења веома су једноставни, па доказујемо, примера ради, само 3 и 5, а остала тврђења остављамо читаоцима.

3. Нека је $\Gamma \models \alpha$ и $\models \tau$. Да бисмо доказали да је $\Gamma \setminus \{\tau\} \models \alpha$, претпостављамо да је v валуација таква да $v \models \Gamma \setminus \{\tau\}$ и настојимо да докажемо да $v \models \alpha$. Пошто је τ таутологија по претпоставци, мора бити $v \models \tau$. Из $v \models \tau$ и $v \models \Gamma \setminus \{\tau\}$, следи да $v \models \Gamma = \{\tau\} \cup (\Gamma \setminus \{\tau\})$, па због $\Gamma \models \alpha$, закључујемо да $v \models \alpha$.

5. Да је $\Gamma \models \bot$ заправо значи да скуп Γ нема модел, тј. да не постоји валуација v таква да $v \models \Gamma$. Одавде тривијално следи да свака валуација која задовољава Γ мора задовољавати и било коју формулу α, тј. да $\Gamma \models \alpha$. $\square$

Теорема компактности

Сада ћемо доказати једну од најзначајнијих теорема овог поглавља. Између осталог, њен значај се огледа и у бројним применама не само у математичкој логици, већ и у осталим математичким дисциплинама.

Теорема 2. [***Теорема компактности***] *Нека је $\Gamma \subseteq \mathrm{For}_{\mathcal{L}}$. Ако за сваки коначан подскуп Γ' скупа Γ постоји валуација v таква да $v \models \Gamma'$, онда постоји и валуација w таква да $w \models \Gamma$.*

Дајемо два доказа теореме компактности.

Доказ I. Означимо са $\mathcal{V}$ скуп свих валуација,

$$\mathcal{V} = \{0,1\}^P = \{v \mid v : P \to \{0,1\}\}.$$

Нека је $\mathcal{P}_{\mathrm{fin}}(\Gamma)$ скуп свих коначних подскупова од Γ. Претпоставку теореме формулисаћемо у следећем облику:

$$(\mathbb{P}) \qquad \text{за свако } \Gamma' \in \mathcal{P}_{\mathrm{fin}}(\Gamma) \text{ постоји } v \in \mathcal{V} \text{ тако да } v \models \Gamma'.$$

Тражену валуацију w дефинисаћемо тако што ћемо редом словима p_1, p_2, p_3, $\ldots$ додељивати вредности из $\{0,1\}$. Одредимо најпре истинитосну вредност слова p_1. Да бисмо се определили коју вредност треба да доделимо слову p_1, поделимо све валуације у два дисјунктна скупа:

$$\mathcal{V}_0 = \{v \in \mathcal{V} \mid v(p_1) = 0\} \text{ и } \mathcal{V}_1 = \{v \in \mathcal{V} \mid v(p_1) = 1\}.$$

Очигледно је $\mathcal{V}_0 \cup \mathcal{V}_1 = \mathcal{V}$ и $\mathcal{V}_0 \cap \mathcal{V}_1 = \emptyset$. Доказаћемо да мора бити истинито бар једно (можда и оба) од следећа два тврђења:

($\mathbb{P}_0$) за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_0$ тако да $v \models \Gamma'$

или

($\mathbb{P}_1$) за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_1$ тако да $v \models \Gamma'$.

Претпоставимо супротно, да није тачно ($\mathbb{P}_0$) нити је тачно ($\mathbb{P}_1$). Тада, пошто ($\mathbb{P}_0$) није тачно, важи

(не-$\mathbb{P}_0$) постоји $\Gamma_0 \in \mathcal{P}_{\text{fin}}(\Gamma)$ тако да за свако $v \in \mathcal{V}_0$ важи $v \not\models \Gamma_0$.

Како и ($\mathbb{P}_1$) није тачно, важи и

(не-$\mathbb{P}_1$) постоји $\Gamma_1 \in \mathcal{P}_{\text{fin}}(\Gamma)$ тако да за свако $v \in \mathcal{V}_1$ важи $v \not\models \Gamma_1$.

Нека је $\Gamma' = \Gamma_0 \cup \Gamma_1$. Скуп Γ' је коначан подскуп од Γ, па према претпоставци ($\mathbb{P}$) постоји нека валуација $v' \in \mathcal{V}$ таква да $v' \models \Gamma'$. Приметимо да $v' \models \Gamma_0$ и $v' \models \Gamma_1$. Очигледно, или $v' \in \mathcal{V}_0$ или $v' \in \mathcal{V}_1$. У оба случаја, долазимо до контрадикције:

- ако $v' \in \mathcal{V}_0$, онда $v' \models \Gamma_0$ противречи тврдњи (не-$\mathbb{P}_0$),
- ако $v' \in \mathcal{V}_1$, онда $v' \models \Gamma_1$ противречи тврдњи (не-$\mathbb{P}_1$).

Из добијених контрадикција, закључујемо да је тачно ($\mathbb{P}_0$) или је тачно ($\mathbb{P}_1$). Нека је

$$w(p_1) = i_1 = \begin{cases} 0, & \text{ако је } (\mathbb{P}_0) \text{ тачно,} \\ 1, & \text{иначе.} \end{cases}$$

Да бисмо се определили коју вредност треба да доделимо слову p_2, поступамо слично. Поделимо све валуације скупа $\mathcal{V}_{i_1}$ на два дисјунктна скупа:

$$\mathcal{V}_{i_1 0} = \{v \in \mathcal{V}_{i_1} \mid v(p_2) = 0\} \text{ и } \mathcal{V}_{i_1 1} = \{v \in \mathcal{V}_{i_1} \mid v(p_2) = 1\}.$$

Тада је $\mathcal{V}_{i_1} = \mathcal{V}_{i_10} \cup \mathcal{V}_{i_11}$ и $\mathcal{V}_{i_10} \cap \mathcal{V}_{i_11} = \emptyset$. Подсећамо да је тачно следеће тврђење

$(\mathbb{P}_{i_1})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_1}$ тако да $v \models \Gamma'$.

Као и раније закључујемо да мора бити тачно бар једно од следећа два тврђења:

$(\mathbb{P}_{i_10})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_10}$ тако да $v \models \Gamma'$

или

$(\mathbb{P}_{i_11})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_11}$ тако да $v \models \Gamma'$.

Доказ да је тачно бар једно од тврђења $(\mathbb{P}_{i_10})$ или $(\mathbb{P}_{i_11})$ спроводи се као у претходном кораку. Нека је

$$w(p_2) = i_2 = \begin{cases} 0, & \text{ако је } (\mathbb{P}_{i_10}) \text{ тачно,} \\ 1, & \text{иначе.} \end{cases}$$

Дефиниција валуације w се даље одвија на очекивани начин: да бисмо одредили $w(p_3)$, све валуације скупа $\mathcal{V}_{i_1i_2}$ делимо на два дисјунктна скупа итд.

Уопште, ако је валуација w дефинисана за сва слова $p_1, p_2, \ldots, p_n$, при чему је $w(p_k) = i_k$, $k = 1, \ldots, n$, онда дефинишемо $w(p_{n+1})$ тако што скуп валуација $\mathcal{V}_{i_1i_2\ldots i_n}$ разбијамо на $\mathcal{V}_{i_1i_2\ldots i_n0} = \{v \in \mathcal{V}_{i_1i_2\ldots i_n} \mid v(p_{n+1}) = 0\}$ и $\mathcal{V}_{i_1i_2\ldots i_n1} = \{v \in \mathcal{V}_{i_1i_2\ldots i_n} \mid v(p_{n+1}) = 1\}$. Даље, на основу тврдње

$(\mathbb{P}_{i_1i_2\ldots i_n})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_1i_2\ldots i_n}$ тако да $v \models \Gamma'$

доказујемо да је тачно бар једно од тврђења:

$(\mathbb{P}_{i_1i_2\ldots i_n0})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_1i_2\ldots i_n0}$ тако да $v \models \Gamma'$

или

$(\mathbb{P}_{i_1i_2\ldots i_n1})$ за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_1i_2\ldots i_n1}$ тако да $v \models \Gamma'$.

Описаним поступком, за свако исказно слово p_k након k корака дефинисана је истинитосна вредност $w(p_k) = i_k$, па је индуктивно дефинисана и читава валуација $w : P \to \{0, 1\}$.

Да ли је w тражена валуација? Приметимо најпре да за свако n:

- ако $v \in \mathcal{V}_{i_1i_2\ldots i_n}$, онда је $v(p_k) = i_k$, $k = 1, 2, \ldots, n$,
- $w \in \mathcal{V}_{i_1i_2\ldots i_n}$.

Нека је $\gamma \in \Gamma$ произвољна формула. Пошто је $P(\gamma)$ коначан скуп, постоји природан број $n > 0$ такав да је $P(\gamma) \subseteq \{p_1, p_2, \ldots, p_n\}$. Тврђење $(\mathbb{P}_{i_1 i_2 \ldots i_n})$ каже да за свако $\Gamma' \in \mathcal{P}_{\text{fin}}(\Gamma)$ постоји $v \in \mathcal{V}_{i_1 i_2 \ldots i_n}$ тако да је $v \models \Gamma'$, па специјално, за $\Gamma' = \{\gamma\}$ постоји $v \in \mathcal{V}_{i_1 i_2 \ldots i_n}$ тако да је $v \models \gamma$. Пошто $w \in \mathcal{V}_{i_1 i_2 \ldots i_n}$ и $w(p_k) = v(p_k) = i_k$, $k = 1, 2, \ldots, n$, имамо да је $w(p) = v(p)$, за свако $p \in P(\gamma)$, одакле, према леми 2, следи да $w \models \gamma$. □

Наводимо још један доказ теореме компактности. Овај доказ је нешто општији јер је у њему претпоставка о пребројивости скупа исказних слова неважна, па је на тај начин доказано да теорема компактности важи и у случају да алфабет садржи непребројиво много исказних слова.

Доказ II. Претпоставимо да је сваки коначан подскуп од Γ задовољив. Тада скуп $\overline{\Gamma} = \{\|\gamma\| \mid \gamma \in \Gamma\}$ у Линденбаумовој алгебри $\mathbf{B}_P$ има својство коначног пресека. Заиста, ако су $\|\gamma_1\|, \ldots, \|\gamma_n\|$ произвољни елементи из $\overline{\Gamma}$, онда је $\|\gamma_1\| \curlywedge \cdots \curlywedge \|\gamma_n\| = \|\gamma_1 \wedge \cdots \wedge \gamma_n\| \neq 0$, јер су скуп $\{\gamma_1, \ldots, \gamma_n\}$, а самим тим и формула $\gamma_1 \wedge \cdots \wedge \gamma_n$ задовољиви.

Према теореми о ултрафилтеру (страна 30), постоји ултрафилтер U Булове алгебре $\mathbf{B}_P$ такав да $\overline{\Gamma} \subseteq U$. Нека је $v_U : P \to \{0, 1\}$ валуација дефинисана са:

$$v_U(p) = \begin{cases} 1, & \|p\| \in U, \\ 0, & \|p\| \notin U. \end{cases}$$

Доказаћемо да $v_U \models \Gamma$, тако што ћемо доказати да за сваку формулу α важи:

$$(*) \qquad \widehat{v_U}(\alpha) = 1 \text{ акко } \|\alpha\| \in U.$$

Тврђење $(*)$ доказујемо индукцијом по сложености формуле α.

Ако је α исказно слово, $(*)$ важи по дефиницији валуације v_U. Уколико је α логичка константа $\top$ или $\bot$, $(*)$ важи јер $1 = \|\top\| \in U$ и $0 = \|\bot\| \notin U$.

Нека је α формула $\neg\theta$.

$$\begin{array}{rll} \widehat{v_U}(\alpha) = 1 & \text{акко} & \widehat{v_U}(\theta) = 0 \\ & \text{акко} & \|\theta\| \notin U \quad [\text{инд. претпоставка}] \\ & \text{акко} & \|\theta\|' \in U \quad [\text{особина } \mathbf{F5} \text{ страна 30}] \\ & \text{акко} & \|\neg\theta\| = \|\alpha\| \in U \end{array}$$

Нека је α формула $\theta_1 \wedge \theta_2$.

$$\begin{array}{rll} \widehat{v_U}(\alpha) = 1 & \text{акко} & \widehat{v_U}(\theta_1) = 1 \text{ и } \widehat{v_U}(\theta_2) = 1 \\ & \text{акко} & \|\theta_1\| \in U \text{ и } \|\theta_2\| \in U \quad [\text{инд. претпоставка}] \\ & \text{акко} & \|\theta_1\| \curlywedge \|\theta_2\| \in U \quad [\text{особине } \mathbf{F3} \text{ и } \mathbf{F4} \text{ страна 30}] \\ & \text{акко} & \|\theta_1 \wedge \theta_2\| = \|\alpha\| \in U \end{array}$$

Ово је довољно за доказ тврђења (∗), јер је $\|\alpha \vee \beta\| = \|\neg(\neg\alpha \wedge \neg\beta)\|$, $\|\alpha \Rightarrow \beta\| = \|\neg(\alpha \wedge \neg\beta)\|$ и $\|\alpha \Leftrightarrow \beta\| = \|\neg(\alpha \wedge \neg\beta) \wedge \neg(\neg\alpha \wedge \beta)\|$. □

Теорема 3. $\Gamma \models \alpha$ *акко постоји коначан подскуп* Γ_0 *од* Γ *такав да* $\Gamma_0 \models \alpha$.

ДОКАЗ. ($\leftarrow$) Тривијално.

($\rightarrow$) Нека је $\Gamma \models \alpha$. Ако постоји коначан подскуп Γ_0 од Γ за који не постоји валуација v таква да $v \models \Gamma_0$, онда тривијално важи $\Gamma_0 \models \alpha$.

Претпоставимо зато да за сваки коначан подскуп Γ_0 од Γ постоји валуација v таква да $v \models \Gamma_0$. У овом случају, претпоставимо и да не важи оно што треба доказати, тј. да за сваки коначан подскуп Γ_0 од Γ важи $\Gamma_0 \not\models \alpha$. Тада, за сваки коначан подскуп Γ_0 од Γ постоји валуација v таква да $v \models \Gamma_0 \cup \{\neg\alpha\}$. Дакле, за сваки коначан подскуп Γ' од $\Gamma \cup \{\neg\alpha\}$ постоји валуација v таква да $v \models \Gamma'$. Према теореми компактности следи да постоји валуација w таква да $w \models \Gamma \cup \{\neg\alpha\}$ што није могуће због $\Gamma \models \alpha$. □

Приметимо да су претходне две теореме еквивалентне. Доказали смо да из теореме 2 следи теорема 3. Лако се види да је тачно и обрнуто: ако у теореми 3, за α узмемо $\perp$, добијамо теорему 2. Зато се и теорема 3 назива теоремом компактности.

У наредним примерима, доказаћемо неколико важних математичких тврђења применом теореме компактности.

ПРИМЕР 14. **Бојење графа.** Сетимо се примера 6 (страна 45) у коме смо проблем бојења неког коначног графова свели на проблем задовољивости одговарајуће исказне формуле. Аналогно томе, проблем бојења било ког (можда бесконачног) графа (G, E) у k боја[24] сводимо на проблем задовољивости скупа формула[25]

$$\Gamma^k_{(G,E)} = \{\alpha_a \mid a \in G\} \cup \{\beta_a \mid a \in G\} \cup \{\gamma_{a,b} \mid (a,b) \in E\}.$$

Поступајући као у примеру 6, закључујемо да важи следећа теорема.

Теорема. Граф (G, E) је k-обојив акко скуп $\Gamma^k_{(G,E)}$ има модел.

Подграф графа (G, E) јесте граф $(G_0, E \cap G_0^2)$, за било који подскуп $G_0 \subseteq G$.

Теорема. Граф (G, E) је k-обојив акко је сваки његов коначан подграф k-обојив.

ДОКАЗ. ($\rightarrow$) Доказ ове импликације је тривијалан. Нека је (G, E) k-обојив, тј. нека постоји функција $f : G \to \{1, 2, \ldots, k\}$ таква да за све $a, b \in G$, из $(a, b) \in E$ следи $f(a) \neq f(b)$. Тада је за било који (не само коначан) подскуп $G_0 \subseteq G$, подграф

[24] Граф (G, E) је k-обојив ако постоји функција $f : G \to \{1, 2, \ldots, k\}$ таква да за све $a, b \in G$, из $(a, b) \in E$ следи $f(a) \neq f(b)$.

[25] Подсећамо да $\alpha_a = \bigvee_{1 \leqslant i \leqslant k} p_{a,i}$ значи да је a обојен бар једном од k датих боја, $\beta_a = \bigwedge_{1 \leqslant i < j \leqslant k} \neg(p_{a,i} \wedge p_{a,j})$ означава да a није обојен двема бојама и $\gamma_{a,b} = \bigwedge_{1 \leqslant i \leqslant k} \neg(p_{a,i} \wedge p_{b,i})$ значи да a и b нису обојени истом бојом.

$(G_0, E \cap G_0^2)$ такође k-обојив и одговарајуће бојење је одређено рестрикцијом функције f на G_0, тј. функцијом $f \restriction G_0 : G_0 \to \{1, 2, \ldots, k\}$.

($\leftarrow$) Претпоставимо да је k-обојив сваки коначан подграф графа (G, E). Доказаћемо да је скуп $\Gamma^k_{(G,E)}$ задовољив, одакле ће према претходној теореми следити жељени закључак. Задовољивост скупа $\Gamma^k_{(G,E)}$ доказаћемо применом теореме компактности. Нека је Γ_0 неки коначан подскуп од $\Gamma^k_{(G,E)}$. Означимо са G_0 скуп свих чворова из G који су индекси формула из Γ_0. Очигледно је скуп G_0 коначан и важи:

$$\Gamma_0 \subseteq \Gamma^k_{(G_0, E \cap G_0^2)} = \{\alpha_a \mid a \in G_0\} \cup \{\beta_a \mid a \in G_0\} \cup \{\gamma_{a,b} \mid (a, b) \in E \cap G_0^2\}.$$

Како је по претпоставци граф $(G_0, E \cap G_0^2)$ k-обојив, закључујемо да је скуп $\Gamma^k_{(G_0, E \cap G_0^2)}$ задовољив, а самим тим задовољив је и скуп Γ_0. $\triangleright$

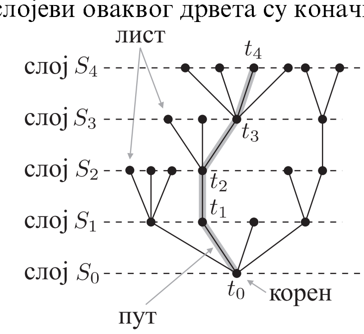
ПРИМЕР 15. **Кенигова лема.** Укратко ћемо описати врсту структура на које се односи Кенигова лема. Уређен скуп $(T, \preccurlyeq)$ је **дрво** уколико

1. постоји $\preccurlyeq$-најмањи елемент скупа T, који се назива *корен* дрвета – означимо га са t_0,
2. за свако t из T почетни сегмент $(\cdot, t] = \{x \in T : x \preccurlyeq t\}$ је добро уређен релацијом $\preccurlyeq$.

Ако је T коначан скуп кажемо да је дрво $(T, \preccurlyeq)$ коначно, а у супротном да је бесконачно. Елементе скупа T називамо *чворовима* дрвета $(T, \preccurlyeq)$. Кажемо да је t' *следбеник* чвора t ако је $t \prec t'$ (тј. $t \preccurlyeq t'$ и $t \neq t'$). Чвор t' је *непосредни следбеник* чвора t ако је $t \prec t'$ и не постоји чвор s такав да је $t \prec s \prec t'$. Није тешко видети да чвор или нема следбенике и у том случају га називамо *лист*, или има непосредне следбенике и тада кажемо да је то *унутрашњи чвор* дрвета. *Слојеве дрвета* дефинишемо индуктивно: $S_0 = \{t_0\}$ и S_{k+1} је скуп свих непосредних следбеника чворова са слоја S_k, $k \in \mathbb{N}$. Ми ћемо се у наставку ограничити само на дрвета за која је $T = \cup_{n \in \mathbb{N}} S_n$, тј. она чији се сваки чвор налази у неком слоју S_n, $n \in \mathbb{N}$.

Уколико сваки чвор дрвета има коначно много непосредних следбеника то дрво називамо *дрветом са коначним гранањем.* Сви слојеви оваквог дрвета су коначни.

Дрво $(T, \preccurlyeq)$ цртамо тако што најпре нацртамо његов корен, а затим изнад њега доцртавамо његове непосредне следбенике, тако да они буду распоређени колинеарно, и сваки доцртани чвор спајамо са t_0. Након тога, додајемо непосредне следбенике свих непосредних следбеника корена дрвета трудећи се да сви они (друго колено корена) буду колинеарни итд.



Није тешко уочити да сваки чвор t који није корен дрвета има само једног непосредног претходника, као и да постоји коначан низ чворова који повезује t са кореном t_0, тј. постоје $t_m, \ldots, t_1, t_0$, за неко $m \geqslant 1$, такви да је $t_m = t$ и $t_{i-1} \prec t_i$, $1 \leqslant i \leqslant m$. Овај низ назива се *пут* од чвора t до корена t_0.

Кенигова лема: У сваком бесконачном дрвету $(T, \preccurlyeq)$ са коначним гранањем постоји низ $t : \mathbb{N} \to T$ такав да је t_0 корен дрвета и $t_i \prec t_{i+1}$, за свако $i \in \mathbb{N}$, односно постоји бесконачан пут.

ДОКАЗ. За сваки чвор дрвета $(T, \preccurlyeq)$ увешћемо по једно исказно слово: $p_t, t \in T$. Нека $\Gamma_{(T,\preccurlyeq)}$ садржи следеће формуле:

- $\bigvee_{t \in S_k} p_t, k \in \mathbb{N}$,
- $\neg(p_t \wedge p_s), t, s \in S_k, t \neq s, k \in \mathbb{N}$,
- $p_t \Rightarrow p_s, t, s \in T, t \preccurlyeq s$.

Доказаћемо да је произвољно изабран коначан подскуп $\Gamma_0 \subseteq \Gamma_{(T,\preccurlyeq)}$ задовољив. Нека је $k_{\max}$ највећи природан број такав да се на слоју $S_{k_{\max}}$ појављује чвор који је индекс неког исказног слова у формулама из Γ_0. Очигледно је да овакав природан број постоји. Ако је $k_{\max} = 0$, тада је $\Gamma_0 = \{p_{t_0}\}$ па је овај скуп тривијално задовољен. Претпоставимо да је $k_{\max} \geqslant 1$. Означимо са Γ скуп формула

- $\bigvee_{t \in S_k} p_t, k \leqslant k_{\max}$,
- $\neg(p_t \wedge p_s), t, s \in S_k, t \neq s, k \leqslant k_{\max}$,
- $p_t \Rightarrow p_s, t, s \in \bigcup_{k \leqslant k_{\max}} S_k, t \preccurlyeq s$.

Очигледно је $\Gamma_0 \subseteq \Gamma$. Нека је $t_{\max}$ произвољан чвор (са највишег) нивоа $S_{k_{\max}}$. Тада постоји низ чворова $t_{\max}, t_{\max-1}, \ldots, t_0$ (по један на сваком нивоу $S_i, i \leqslant k_{\max}$) такав да је $t_{i-1} \prec t_i$, $1 \leqslant i \leqslant k_{\max}$. Дефинишимо валуацију $v : \{p_t \mid t \in T\} \to \{0, 1\}$:

$$v(p_a) = \begin{cases} 1, & t = t_i, \text{ за неко } i \in \{0, \ldots, \max\}, \\ 0, & \text{иначе.} \end{cases}$$

Није тешко закључити да $v \models \Gamma$, па тиме и $v \models \Gamma_0$. Према теореми компактности и скуп $\Gamma_{(T,\preccurlyeq)}$ је задовољив, тј. постоји валуација $v : \{p_t \mid t \in T\} \to \{0, 1\}$ таква да $v \models \Gamma_{(T,\preccurlyeq)}$. Пошто за свако $k \in \mathbb{N}, v \models \bigvee_{t \in S_k} p_t$ и за све $t, s \in S_k, t \neq s, v \models \neg(p_t \wedge p_s)$, закључујемо да за свако $k \in \mathbb{N}$ постоји тачно један чвор $t_k \in S_k$ такав да је $v(p_{t_k}) = 1$. За све остале чворове дрвета, $t \in T \setminus \{t_k \mid k \in \mathbb{N}\}$ важи $v(p_t) = 0$. Уочени низ чворова је тражени, јер за све $t, s \in T, t \preccurlyeq s$, имамо да $v \models p_t \Rightarrow p_s$. $\triangleright$

ПРИМЕР 16. **Холова теорема спаривања.** Нека је S неки скуп и $\mathcal{S} = \{S_i \mid i \in I\}$ фамилија (не нужно различитих) подскупова од S. *Систем различитих представника* фамилије $\mathcal{S}$ јесте свака 1-1 функција $f : I \to S$ таква да је $f(i) \in S_i$, за свако $i \in I$. На пример, ако је $S = \mathbb{N}$ и $S_n = \{n, n+1\}$, $n \in \mathbb{N}$, онда је идентична функција $\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$, $\mathrm{id}_{\mathbb{N}}(n) = n$, $n \in \mathbb{N}$, један систем различитих представика. Холова теорема спаривања одговара на питање када за коначну фамилију подскупова неког скупа S постоји систем различитих представника.

Холова теорема спаривања: Нека је S било који скуп и $n \geqslant 1$. За коначан низ $S_1, \ldots, S_n$ подскупова од S постоји систем различитих представника акко

($\mathbf{H}_n$) за свако $k \in \{1, \ldots, n\}$ и сваки избор k индекса $1 \leqslant i_1, \ldots, i_k \leqslant n$, важи $|S_{i_1} \cup \cdots \cup S_{i_k}| \geqslant k$.

Доказ. Ако за коначан низ $S_1, \ldots, S_n$ подскупова од S постоји систем различитих представника, онда очигледно важи $(\mathbf{H}_n)$. Обрнуто доказујемо индукцијом. Ако је $n = 1$, тврђење тривијално важи. Претпоставимо да тврђење важи за сваки природан број који није већи од неког n, $n \geqslant 1$. Нека је $S_1, \ldots, S_n, S_{n+1}$ низ подскупова скупа S такав да важи $(\mathbf{H}_{n+1})$. Разликујемо два случаја.
1. случај. За свако $k \in \{1, \ldots, n\}$ и све $1 \leqslant i_1, \ldots, i_k \leqslant n$, важи $|S_{i_1} \cup \cdots \cup S_{i_k}| > k$. Изаберимо из S_{n+1} било који елемент a. Нека је $S_i' = S_i \setminus \{a\}$, $i = 1, \ldots, n$. Тада за коначан низ $S_1', \ldots, S_n'$ важи услов $(\mathbf{H}_n)$, па по индуктивној претпоставци постоји систем различитих представника, тј. функција $f : \{1, \ldots, n\} \xrightarrow{1\text{-}1} S$, таква да $f(i) \in S_i'$. Проширење $\widehat{f} : \{1, \ldots, n, n+1\} \xrightarrow{1\text{-}1} S$ дато са $\widehat{f}(i) = f(i)$, $i = 1, \ldots, n$, и $f(n+1) = a$, јесте систем различитих представника за $S_1, \ldots, S_n, S_{n+1}$.
2. случај. Постоји $k \in \{1, \ldots, n\}$ такав да за неке индексе $1 \leqslant i_1, \ldots, i_k \leqslant n$, важи $|S_{i_1} \cup \cdots \cup S_{i_k}| = k$. Пошто низ подскупова $S_{i_1}, \ldots, S_{i_k}$ има мање од $n+1$ чланова, према индуктивној претпоставци постоји функција $f_1 : \{1, \ldots, k\} \xrightarrow{1\text{-}1} S$, таква да $f_1(j) \in S_{i_j}$, $j = 1, \ldots, k$. Нека је $S' = S_{i_1} \cup \cdots \cup S_{i_k}$ и $S_\ell' = S_\ell \setminus S'$, за $\ell \notin \{i_1, \ldots, i_k\}$. Скупова S_ℓ', $\ell \notin \{i_1, \ldots, i_k\}$, има укупно $n+1-k$, и образују један нови низ $S_{\ell_1}', \ldots, S_{\ell_{n+1-k}}'$ подскупова од S. За овај низ важи $(\mathbf{H}_{n+1-k})$. Заиста, за свако $m \in \{1, \ldots, n+1-k\}$ и било које индексе $1 \leqslant s_1, \ldots, s_m \leqslant n+1-k$ важи

$$m + k \leqslant |S_{\ell_{s_1}} \cup \cdots \cup S_{\ell_{s_m}} \cup S'| = |S_{\ell_{s_1}}' \cup \cdots \cup S_{\ell_{s_m}}'| + k,$$

одакле следи да је $|S_{\ell_{s_1}}' \cup \cdots \cup S_{\ell_{s_m}}'| \geqslant m$. Према индуктивној претпоставци, постоји функција $f_2 : \{\ell_1, \ldots, \ell_{n+1-k}\} \xrightarrow{1\text{-}1} S$ таква да $f_2(\ell) \in S_\ell$, $\ell \in \{\ell_1, \ldots, \ell_{n+1-k}\}$. Није тешко дефинисати помоћу функција f_1 и f_2 систем различитих представника полазног низа $S_1, \ldots, S_n, S_{n+1}$. $\square$

Применом теореме компактности једноставно доказујемо теорему познату као **бесконачна верзија Холове теореме**. Нека је S било који скуп и $S_1, \ldots, S_n, \ldots$ низ <u>коначних</u>[26] подскупова од S. За овај низ постоји систем различитих представника акко

$(\mathbf{H})$ за свако $k \geqslant 1$ и сваки избор k индекса $1 \leqslant i_1, \ldots, i_k \leqslant n$, важи $|S_{i_1} \cup \cdots \cup S_{i_k}| \geqslant k$.

За свако $n \geqslant 1$ и сваки елемент $x \in S_n$ уведимо по једно исказно слово $p_{n,x}$. Нека Γ садржи следеће формуле:

- $\neg(p_{m,x} \wedge p_{n,x})$, $m, n \geqslant 1$, $m \neq n$ и $x \in S_m \cap S_n$;
- $\neg(p_{n,x} \wedge p_{n,y})$, $n \geqslant 1$, $x, y \in S_n$, $x \neq y$;
- $\bigvee_{x \in S_n} p_{n,x}$, $n \geqslant 1$.

Треба доказати да постоји валуација $v : \{p_{n,x} \mid n \geqslant 1, x \in S_n\} \to \{0, 1\}$ која задовољава све формуле скупа Γ. Оваква валуација нам даје систем различитих представника $f : \mathbb{N}^+ \to S$, који дефинишемо следећом еквиваленцијом: $f(n) = x$ акко $v(p_{n,x}) = 1$. Остављамо читаоцу да провери коректност овакве дефиниције. Поред тога, за вежбу остављамо и доказ да поменута валуација уопште постоји. $\triangleright$

[26] Да ли се ова претпоставка може изоставити?

Синтаксна последица

Поред важних својстава семантичке последице које смо навели у претходном одељку, ова релација има низ специфичних особина које се односе на логичке везнике. У наредној теореми наводимо једну такву особину за импликацију.

Лема 8. *Нека је* $\Gamma \subseteq \mathrm{For}$ *и* $\alpha \in \mathrm{For}$. *Ако* $\Gamma, \alpha \models \beta$, *онда* $\Gamma \models \alpha \Rightarrow \beta$.

Доказ. Претпоставимо да је $\Gamma, \alpha \models \beta$. Нека је v произвољна валуација таква да $v \models \Gamma$. Доказаћемо да мора важити и $v \models \alpha \Rightarrow \beta$. Разликујемо два случаја.

Први случај: $\widehat{v}(\alpha) = 0$. Тада директно на основу таблице за импликацију закључујемо да мора бити $\widehat{v}(\alpha \Rightarrow \beta) = 1$, тј. $v \models \alpha \Rightarrow \beta$.

Други случај: $\widehat{v}(\alpha) = 1$. Тада $v \models \Gamma, \alpha$, па због $\Gamma, \alpha \models \beta$ мора бити и $v \models \beta$, тј. $\widehat{v}(\beta) = 1$. Из $\widehat{v}(\alpha) = 1$ и $\widehat{v}(\beta) = 1$, следи $\widehat{v}(\alpha \Rightarrow \beta) = 1$, тј. $v \models \alpha \Rightarrow \beta$. □

Претходна лема заправо одсликава начин на који доказујемо импликацију из неких претпоставки. Ако желимо да докажемо да из претпоставки Γ следи $\alpha \Rightarrow \beta$, прво ћемо формулу α прикључити претпоставкама Γ и затим настојати да докажемо β.

Пример 17. Докажимо да је формула $\varphi \Rightarrow (\psi \Rightarrow \varphi)$ таутологија, тј. да је ова формула семантичка последица празног скупа формула, $\models \varphi \Rightarrow (\psi \Rightarrow \varphi)$. Према претходној леми, довољно је доказати да важи $\varphi \models \psi \Rightarrow \varphi$, односно након још једног позивања на исту лему, да је $\varphi, \psi \models \varphi$. Ово последње је једноставна последица тврдње коју смо већ доказали (теорема 1): ако нека формула припада скупу претпоставки, онда је та формула и семантичка последица тог скупа.

Аналогно доказујемо, на пример: $\models \varphi \Rightarrow \varphi$, $\models \varphi \Rightarrow (\psi \Rightarrow (\theta \Rightarrow \psi))$ итд. ▷

На основу претходног примера видимо да се тврђење леме 8 може схватити и као правило за доказивање импликације које ћемо записати у следећем облику:

$$\frac{\Gamma, \alpha \models \beta}{\Gamma \models \alpha \Rightarrow \beta} \, (\Rightarrow_{\mathrm{U}}).$$

Наведено правило називамо *правило увођења импликације* и означавамо га са $(\Rightarrow_{\mathrm{U}})$. Правило каже: ако смо доказали да је $\Gamma, \alpha \models \beta$, онда закључујемо и да је $\Gamma \models \alpha \Rightarrow \beta$. У истом примеру смо користили још једно правило: ако нека формула припада скупу претпоставки, онда је та формула и семантичка последица тог скупа. Ово правило ћемо назвати *аксиомом* и скраћено га записати у облику

$$\frac{}{\Gamma, \alpha \models \alpha} \, (\mathrm{ax}).$$

Изнад хоризонталне црте ништа није наведено јер закључак $\Gamma, \alpha \models \alpha$ непосредно изводимо.

Пример 18. Доказ из претходног примера, да је $\models \varphi \Rightarrow (\psi \Rightarrow \varphi)$, можемо записати и на следеће начине:

$$\dfrac{\dfrac{\dfrac{}{\varphi, \psi \models \varphi}(\mathrm{ax})}{\varphi \models \psi \Rightarrow \varphi}(\Rightarrow_{\mathrm{U}})}{\models \varphi \Rightarrow (\psi \Rightarrow \varphi)}(\Rightarrow_{\mathrm{U}})$$

или

1. $\varphi, \psi \models \varphi$ (ax)
2. $\varphi \models \psi \Rightarrow \varphi$ из 1. применом $(\Rightarrow_{\mathrm{U}})$
3. $\models \varphi \Rightarrow (\psi \Rightarrow \varphi)$ из 2. применом $(\Rightarrow_{\mathrm{U}})$.

Приметимо да у наведеном доказу не помињемо никакве валуације, већ само анализирамо структуру формула. $\triangleright$

Након претходних разматрања природно је поставити питање да ли је могуће увођењем сличних правила за остале логичке везнике потпуно окарактерисати појам семантичке последице. У наставку ћемо увести нову релацију којом се успоставља веза између неког скупа формула Γ и неке формуле α, при чему ћемо узимати у обзир само структуре формула из Γ, односно структуру формуле α. Пошто се у дефиницији ове нове релације неће помињати валуације, већ ће бити важни само записи одговарајућих формула, називаћемо је релацијом *синтаксне последице* и означавати са $\vdash$ (знак $\vdash$ читамо „рампа“). Запис $\Gamma \vdash \alpha$ називамо *секвентом*.

Природна дедукција

Дефиниција 11. *Формула α је синтаксна последица скупа формула Γ, ако се секвент $\Gamma \vdash \alpha$ може добити применом следећих правила коначан број пута.*

Аксиома

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

Слабљење

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

Увођење импликације

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

Елиминација импликације

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

Увођење конјункције

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

Елиминација конјункције

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

Увођење дисјункције

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

Елиминација дисјункције

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

Увођење негације

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

Елиминација негације

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

Класична противречност

$$\frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}\ (\bot_c)$$

Анализирајмо правила из претходне дефиниције. Свако правило чине:

- скуп (могуће и празан) секвената које називамо *премисе правила* и који су записани изнад хоризонталне линије и

- један секвент који називамо *закључак правила* и који је записан испод хоризонталне линије.

Поред хоризонталне линије, која раздваја премисе и закључак правила, стоји сугестивна ознака правила. Свако правило схватамо на следећи начин: *ако су доказане премисе правила, онда се из њих директно изводи и закључак правила.*

Правило (ax) већ смо коментарисали. Правило (slab) назива се *слабљење* јер изражава следеће: *ако је доказив секвент* $\Gamma \vdash \varphi$, *онда је* φ *последица и ослабљеног скупа претпоставки* $\Gamma \cup \{\varphi\}$, односно *при додавању нових претпоставки све последице изведене без те нове претпоставке јесу последице и новог, ширег скупа претпоставки.* Сваком логичком везнику одговарају две врсте правила.

- Свако *правило увођења* омогућава доказивање секвената чији је закључак формула која као главни има одређени логички везник. Тако, правило $(\Rightarrow_{\mathrm{U}})$ говори о томе када је импликација $\varphi \Rightarrow \psi$ последица неких претпоставки Γ, правило $(\wedge_{\mathrm{U}})$ када је конјункција $\varphi \wedge \psi$ последица неких претпоставки Γ, итд.

- Свако *правило елиминације* омогућава коришћење формула које имају као главни одређени логички знак. Тако, правило $(\Rightarrow_{\mathrm{E}})$ говори о томе како се у доказима користи чињеница да је импликација $\varphi \Rightarrow \psi$ последица неких претпоставки Γ, док правила $(\wedge^{\mathrm{l}}_{\mathrm{E}})$ и $(\wedge^{\mathrm{d}}_{\mathrm{E}})$ говоре о томе како се у доказима користи чињеница да је конјункција $\varphi \wedge \psi$ последица неких претпоставки Γ итд.

Последње наведено правило означено је са $(\bot_c)$ и назива се *правило класичне противречности.* Ово правило одговара уобичајеном начину доказивања у математици које започињемо речима „претпоставимо супротно ...“. Заиста, да бисмо доказали да је φ последица претпоставки Γ, довољно је да скупу Γ придружимо $\neg\varphi$ и изведемо контрадикцију. Посебно истичемо да се правила $(\neg_{\mathrm{U}})$ и $(\bot_c)$ битно разликују, јер прво говори о томе када су негације формула последице неких претпоставки, а друго, слободније речено, даје један општи метод извођења секвената.

Сва правила можемо читати (схватити) на два начина:

– *одозго надоле*: ако смо доказали хипотезе правила, можемо доказати и секвент који се налази испод хоризонталне линије; овако читамо правило када треба написати доказ неког секвента (СИНТЕЗА);

– *одоздо нагоре*: да бисмо доказали секвент који је закључак правила, довољно је доказати хипотезе правила; овако читамо правило када трагамо за доказом неког секвента (АНАЛИЗА).

Приметимо најзад да се у наведеним правилима не помиње еквиваленција. Иако смо могли да додамо одговарајућа правила и за овај везник, једноставније је да усвојимо договор да формула $\varphi \Leftrightarrow \psi$ буде скраћени запис за $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$. Слично томе, нека је $\top$ скраћени запис за $\neg\bot$.

Дефиниција 12. *Формула σ је доказива, тј. јесте теорема исказне логике, у ознаци $\vdash \sigma$, ако је доказив секвент $\emptyset \vdash \sigma$.*

ПРИМЕР 19. Докажимо да је $\neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)$ теорема исказне логике, тј. да је $\vdash \neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)$. Најпре наводимо одговарајућу анализу, тј. описујемо како размишљамо при трагању за доказом наведеног секвента. Као што смо већ нагласили, размишљамо „уназад“ читајући правила одоздо нагоре и бирајући она правила која нам одговарају.

АНАЛИЗА. Да бисмо доказали секвент $\vdash \neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)$, у складу са наведеним правилима анализирамо („растављамо“) формуле са десне стране:

1. према напомени испред дефиниције 12, секвент $\vdash \neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)$ биће доказан, ако докажемо секвент $\vdash (\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \wedge ((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)$;

2. како је формула са десне стране последњег секвента конјункција, тражимо правило које доказује конјункције; то је $(\wedge_{\mathrm{U}})$, па закључујемо да ћемо жељену конјункцију доказати ако докажемо $\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \bot)$ и $\vdash (\alpha \Rightarrow \bot) \Rightarrow \neg\alpha$;

3. да бисмо доказали секвент $\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \bot)$

   3.1. тражимо правило које доказује импликације; то је $(\Rightarrow_{\mathrm{U}})$ и закључујемо да треба доказати $\neg\alpha \vdash \alpha \Rightarrow \bot$,

   3.2. а према истом правилу, последњи секвент ће бити доказан ако докажемо $\neg\alpha, \alpha \vdash \bot$;

   3.3. према правилу $(\neg_{\mathrm{E}})$ последњи секвент добијамо из секвената $\neg\alpha, \alpha \vdash \alpha$ и $\neg\alpha, \alpha \vdash \neg\alpha$ које добијамо применом правила (ax);

4. да бисмо доказали секвент $\vdash (\alpha \Rightarrow \bot) \Rightarrow \neg\alpha$

   4.1. према правилу $(\Rightarrow_{\mathrm{U}})$ потребно је доказати $\alpha \Rightarrow \bot \vdash \neg\alpha$;

4.2. уочавајући правило $(\neg_{\mathrm{U}})$, које даје негације, закључујемо да ћемо последњи секвент доказати ако докажемо $\alpha \Rightarrow \bot, \alpha \vdash \bot$;

4.3 да бисмо доказали последњи секвенет тражимо правило које нам каже како да користимо импликације; то је $(\Rightarrow_{\mathrm{E}})$, па према овом правилу треба доказати секвенте $\alpha \Rightarrow \bot, \alpha \vdash \alpha$ и $\alpha \Rightarrow \bot, \alpha \vdash \alpha \Rightarrow \bot$ које добијамо применом правила (ax).

Анализу завршавамо када стигнемо до правила (ax) које нема премисе. На основу анализе није тешко саставити тражени доказ, тј. извршити *синтезу*.

Синтеза

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\alpha, \alpha \vdash \neg\alpha}\,\text{(ax)} \quad \dfrac{}{\neg\alpha, \alpha \vdash \alpha}\,\text{(ax)}}{\neg\alpha, \alpha \vdash \bot}\,(\neg_{\mathrm{E}})}{\neg\alpha \vdash \alpha \Rightarrow \bot}\,(\Rightarrow_{\mathrm{U}})}{\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \bot)}\,(\Rightarrow_{\mathrm{U}}) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \Rightarrow \bot, \alpha \vdash \alpha \Rightarrow \bot}\,\text{(ax)} \quad \dfrac{}{\alpha \Rightarrow \bot, \alpha \vdash \alpha}\,\text{(ax)}}{\alpha \Rightarrow \bot, \alpha \vdash \bot}\,(\Rightarrow_{\mathrm{E}})}{\alpha \Rightarrow \bot \vdash \neg\alpha}\,(\neg_{\mathrm{U}})}{\vdash (\alpha \Rightarrow \bot) \Rightarrow \neg\alpha}\,(\Rightarrow_{\mathrm{U}})$$

$$\dfrac{\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \bot) \qquad \vdash (\alpha \Rightarrow \bot) \Rightarrow \neg\alpha}{\vdash \neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)}\,(\wedge_{\mathrm{U}})$$

Иако је извођење жељеног секвента приказано као дрво, што је доста илустративно, уобичајеније и једноставније је доказ записати линеарно у нумерисаним редовима, при чему се у сваком реду наводи како је одговарајући секвент добијен. У наставку ћемо користити овај други начин записивања.

1.	$\neg\alpha, \alpha \vdash \neg\alpha$	(ax)
2.	$\neg\alpha, \alpha \vdash \alpha$	(ax)
3.	$\neg\alpha, \alpha \vdash \bot$	из 1 и 2 према $(\neg_{\mathrm{E}})$
4.	$\neg\alpha \vdash \alpha \Rightarrow \bot$	из 3 према $(\Rightarrow_{\mathrm{U}})$
5.	$\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \bot)$	из 4 према $(\Rightarrow_{\mathrm{U}})$
6.	$\alpha \Rightarrow \bot, \alpha \vdash \alpha \Rightarrow \bot$	(ax)
7.	$\alpha \Rightarrow \bot, \alpha \vdash \alpha$	(ax)
8.	$\alpha \Rightarrow \bot, \alpha \vdash \bot$	из 6 и 7 према $(\Rightarrow_{\mathrm{E}})$
9.	$\alpha \Rightarrow \bot \vdash \neg\alpha$	из 8 према $(\neg_{\mathrm{U}})$
10.	$\vdash (\alpha \Rightarrow \bot) \Rightarrow \neg\alpha$	из 9 према $(\Rightarrow_{\mathrm{U}})$
11.	$\vdash (\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \wedge ((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)$	из 5 и 10 према $(\wedge_{\mathrm{U}})$

$\triangleright$

Пример 20. Доказаћемо да је $\vdash (\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta) \Rightarrow (\gamma \Rightarrow \alpha \vee \beta)$. Саветујемо читаоцима, пре него што наставе са читањем, да по угледу на претходни пример обаве одговарајућу анализу.

Синтеза

1.	$(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma \vdash (\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta)$	(ax)
2.	$(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \alpha \vdash \gamma \Rightarrow \alpha$	(ax)
3.	$(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \alpha \vdash \gamma$	(ax)

4. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \alpha \vdash \alpha$ из 2 и 3 према $(\Rightarrow_{\mathrm{E}})$
5. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \alpha \vdash \alpha \vee \beta$ из 4 према $(\vee^{\mathrm{l}}_{\mathrm{U}})$
6. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \beta \vdash \gamma \Rightarrow \beta$ (ax)
7. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \beta \vdash \gamma$ (ax)
8. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \beta \vdash \beta$ из 6 и 7 према $(\Rightarrow_{\mathrm{E}})$
9. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma, \gamma \Rightarrow \alpha \vdash \alpha \vee \beta$ из 8 према $(\vee^{\mathrm{d}}_{\mathrm{U}})$
10. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta), \gamma \vdash \alpha \vee \beta$ из 1, 5 и 9 према $(\vee_{\mathrm{E}})$
11. $(\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta) \vdash \gamma \Rightarrow \alpha \vee \beta$ из 10 према $(\Rightarrow_{\mathrm{U}})$
12. $\vdash (\gamma \Rightarrow \alpha) \vee (\gamma \Rightarrow \beta) \Rightarrow (\gamma \Rightarrow \alpha \vee \beta)$ из 11 према $(\Rightarrow_{\mathrm{U}})$

$\triangleright$

ПРИМЕР 21. Насупрот претходном примеру, овога пута ћемо извршити анализу која претходи доказу секвента $\vdash \neg(\alpha \wedge \beta) \Rightarrow \neg\alpha \vee \neg\beta$ препуштајући читаоцима синтезу.

АНАЛИЗА

1. Да бисмо доказали жељени секвент, довољно је, према правилу $(\Rightarrow_{\mathrm{U}})$, доказати $\neg(\alpha \wedge \beta) \vdash \neg\alpha \vee \neg\beta$.

2. Прво шта нам пада на памет јесте да тражимо правило које доказује дисјункције[27], али према правилу $(\perp_{\mathrm{c}})$ можемо трагати и за доказом секвента $\neg(\alpha \wedge \beta), \neg(\neg\alpha \vee \neg\beta) \vdash \perp$. Због једноставнијег записивања, означимо са Γ скуп који садржи формуле $\neg(\alpha \wedge \beta)$ и $\neg(\neg\alpha \vee \neg\beta)$.

3. Да бисмо доказали $\Gamma \vdash \perp$, није тешко закључити да је довољно доказати $\Gamma \vdash \alpha \wedge \beta$ или $\Gamma \vdash \neg\alpha \vee \neg\beta$. Покушајмо да докажемо овај последњи.

4. Према правилима $(\vee^{\mathrm{l}}_{\mathrm{U}})$ и $(\vee^{\mathrm{d}}_{\mathrm{U}})$, секвент $\Gamma \vdash \neg\alpha \vee \neg\beta$ ће бити доказан ако докажемо $\Gamma \vdash \neg\alpha$ или $\Gamma \vdash \neg\beta$. Покушајмо да докажамо секвент $\Gamma \vdash \neg\alpha$.

5. Секвнет $\Gamma \vdash \neg\alpha$ добијамо применом правила $(\neg_{\mathrm{U}})$ на секвент $\Gamma, \alpha \vdash \perp$.

6. Трагање за доказом секвента $\Gamma, \alpha \vdash \perp$ наводи нас на правило $(\neg_{\mathrm{E}})$, а пошто са леве стране рампе имамо три формуле, уочавамо да на разне начине можемо покушати да докажемо овај секвент. Један од тих покушаја јесте трагање за доказом секвента $\Gamma, \alpha \vdash \neg\alpha \vee \neg\beta$.

7. За доказ последњег секвента природно се намеће примена једног од правила $(\vee^{\mathrm{l}}_{\mathrm{U}})$ и $(\vee^{\mathrm{d}}_{\mathrm{U}})$. Покушајмо да докажемо секвент $\Gamma, \alpha \vdash \neg\beta$. Овај секвент ћемо добити из $\Gamma, \alpha, \beta \vdash \perp$ применом правила $(\neg_{\mathrm{U}})$.

8. Секвент $\Gamma, \alpha, \beta \vdash \perp$ се једноставно добија из $\Gamma, \alpha, \beta \vdash \neg(\alpha \wedge \beta)$ (ax) и из секвента $\Gamma, \alpha, \beta \vdash \alpha \wedge \beta$ добијеног двоструком применом правила (ax) и једном применом $(\wedge_{\mathrm{U}})$.

Пошто очекујемо да ће се пажљив читалац осетити превареним понуђеном анализом, покушаћемо неким додатним објашњењима да се оправдамо. Наиме, наведена анализа обилује недетерминистичким упутствима, тј. упутствима после којих се може

[27]Саветујемо читаоцу да покуша и са овом стратегијом након што прочита ону која је овде изложена.

кренути различитим правцима, што је јасно и истакнуто у анализи. Опредељујући се за по једну алтернативу у сваком оваквом кораку, ми смо успешно завршили анализу на основу које је једноставно конструисати одговарајући синтетички доказ. Природно се намеће питање шта би се догодило да смо у једном тренутку кренули неким другим путем. Постоји више могућих одговора: доказ би се знатно закомпликовао или пак поједноставио, или бисмо се „заглавили“ увиђајући да изабраним правацем не можемо стићи до жељеног краја. Саветујемо читаоцу да крене неким различитим правцима назначеним у нашој анализи и открије шта га све на изабраним путевима чека. Ово је уједно и најбољи начин да се јача интуиција, подстиче машта и стиче искуство, што су неопходне вештине не само за доказивање секвената већ за бављење математиком уопште. $\triangleright$

ПРИМЕР 22. Потражимо доказ секвента $\vdash \alpha \vee \neg\alpha$ препуштајући читаоцима синтезу.

АНАЛИЗА. Није тешко уочити да нас до жељеног секвента не могу довести правила $(\vee^{\mathrm{l}}_{\mathrm{U}})$ или $(\vee^{\mathrm{d}}_{\mathrm{U}})$. Покушајмо, имајући на уму правило $(\perp_{\mathrm{c}})$ да докажемо $\neg(\alpha\vee\neg\alpha) \vdash \perp$. Последњи секвент добићемо ако успемо да докажемо $\neg(\alpha\vee\neg\alpha) \vdash \alpha\vee\neg\alpha$ $(\neg_{\mathrm{E}})$. Према $(\vee^{\mathrm{d}}_{\mathrm{U}})$, покушаћемо да докажемо $\neg(\alpha \vee \neg\alpha) \vdash \neg\alpha$, односно, узимајући у обзир $(\neg_{\mathrm{U}})$, $\neg(\alpha \vee \neg\alpha), \alpha \vdash \perp$. Овај секвент добијамо из $\neg(\alpha \vee \neg\alpha), \alpha \vdash \alpha \vee \neg\alpha$ $(\mathrm{ax}) + (\vee^{\mathrm{l}}_{\mathrm{U}})$ и $\neg(\alpha \vee \neg\alpha), \alpha \vdash \neg(\alpha \vee \neg\alpha)$ (ax). $\triangleright$

На крају, издвајамо и једну општу особину релације $\vdash$, тј. тврђење аналогно теореми компактности.

Лема 9. $\Gamma \vdash \alpha$ *акко постоји коначан подскуп* Γ_0 *од* Γ, *такав да* $\Gamma_0 \vdash \alpha$.

ДОКАЗ. $(\rightarrow)$ За доказ секвента $\Gamma \vdash \alpha$ значајне су само оне формуле из Γ које су активиране правилом (ax). С обзиром на то да правило (ax) може бити примењено само коначно много пута, следи да и „активних“ формула има само коначно много. Ако са Γ_0 означимо скуп свих активних формула, закључујемо да мора бити и $\Gamma_0 \vdash \alpha$.

$(\leftarrow)$ Тривијално. $\square$

Извођење секвената знатно олакшава и скраћује коришећење тзв. *изведених правила*. У наредној леми издвојено је неколико таквих правила.

Лема 10. (1) $\dfrac{\Gamma, \alpha \vdash \beta \quad \Gamma \vdash \alpha}{\Gamma \vdash \beta}(\mathrm{cut})$[28] (2) $\dfrac{}{\Gamma, \alpha, \neg\alpha \vdash \perp}(\neg_{\mathrm{L}})$[29] (3) $\dfrac{\Gamma \vdash \perp}{\Gamma \vdash \alpha}(\perp_{\mathrm{i}})$[30]

[28] енгл. cut – сечење

[29] Индекс L указује на то да се правило односи на негацију са **леве** стране рампе

[30] Индекс i указује на тзв. **интуиционистичку логику**. Природна дедукција ове логике уместо правила $(\perp_{\mathrm{c}})$ (које се избације) подразумева правило $(\perp_{\mathrm{i}})$, док су сва остала правила дозвољена.

Доказ.
(1)

1. $\Gamma, \alpha \vdash \beta$ [претпоставка]
2. $\Gamma \vdash \alpha \Rightarrow \beta$ из 1 према $(\Rightarrow_{\mathrm{U}})$
3. $\Gamma \vdash \alpha$ [претпоставка]
4. $\Gamma \vdash \beta$ из 3 према $(\Rightarrow_{\mathrm{E}})$

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, \alpha \vdash \beta}}{\Gamma \vdash \alpha \Rightarrow \beta}(\Rightarrow_{\mathrm{U}}) \qquad \dfrac{\vdots}{\Gamma \vdash \alpha}}{\Gamma \vdash \beta}(\Rightarrow_{\mathrm{E}})$$

(2)

1. $\Gamma, \alpha, \neg\alpha \vdash \alpha$ (ax)
2. $\Gamma, \alpha, \neg\alpha \vdash \neg\alpha$ (ax)
3. $\Gamma, \alpha, \neg\alpha \vdash \bot$ из 1, 2 према $(\neg_{\mathrm{E}})$

(3)

1. $\Gamma \vdash \bot$ [претпоставка]
2. $\Gamma, \neg\alpha \vdash \bot$ из 1 према (slab)
3. $\Gamma \vdash \alpha$ из 2 према $(\bot_{\mathrm{c}})$

$\square$

Хилбертов систем за дедукцију

Постоје и други начини да се уведе појам синтаксне последице. Један од њих је тзв. *Хилбертов формални систем* који чине следеће схеме аксиома:

$(\mathbf{H1})$	$\varphi \Rightarrow (\psi \Rightarrow \varphi)$,	$(\mathbf{H2})$	$(\varphi \Rightarrow (\psi \Rightarrow \theta)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \theta))$,
$(\mathbf{H3})$	$\varphi \wedge \psi \Rightarrow \varphi$,	$(\mathbf{H4})$	$\varphi \wedge \psi \Rightarrow \psi$,
$(\mathbf{H5})$	$\varphi \Rightarrow (\psi \Rightarrow \varphi \wedge \psi)$,	$(\mathbf{H6})$	$\varphi \Rightarrow \varphi \vee \psi$,
$(\mathbf{H7})$	$\psi \Rightarrow \varphi \vee \psi$,	$(\mathbf{H8})$	$(\varphi \Rightarrow \theta) \Rightarrow ((\psi \Rightarrow \theta) \Rightarrow (\varphi \vee \psi \Rightarrow \theta))$,
$(\mathbf{H9})$	$\neg\varphi \Rightarrow (\varphi \Rightarrow \bot)$,	$(\mathbf{H10})$	$(\varphi \Rightarrow \bot) \Rightarrow \neg\varphi$,
$(\mathbf{H11})$	$\bot \Rightarrow \varphi$,	$(\mathbf{H12})$	$\varphi \vee \neg\varphi$,

и правило $\mathbf{MP}$ познато као *модус поненс*:

$(\mathbf{MP})$ ψ је непосредна последица формула φ и $\varphi \Rightarrow \psi$, што краће записујемо у облику

$$\frac{\varphi \quad \varphi \Rightarrow \psi}{\psi}(\mathbf{MP}),$$

при чему су φ, ψ, θ произвољне исказне формуле.

Дефиниција 13. $\Gamma \vdash_{\mathbf{H}} \varphi$ *ако и само ако постоји коначан низ формула* φ_1, φ_2, $\ldots, \varphi_n$ *са следећим својствима:*

1. φ_n *је формула* φ*;*

2. *свака формула* φ_k, $1 \leqslant k \leqslant n$, *задовољава један од следећих услова:*

2.1. φ_i *је аксиома, или*

2.2. $\varphi_i \in \Gamma$, *или*

2.3. φ_i *је добијена применом правила* $\mathbf{MP}$ *на неке две одговарајуће формуле које претходе овој формули у наведеном низу.*

Пример 23. Доказ да је $\vdash_{\mathbf{H}} \neg\alpha \Leftrightarrow (\alpha \Rightarrow \bot)$ представља следећи низ:

1. $\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)$ аксиома $\mathbf{H9}$
2. $(\alpha \Rightarrow \bot) \Rightarrow \neg\alpha$ аксиома $\mathbf{H10}$
3. $(\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \Rightarrow (((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha) \Rightarrow (\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \wedge ((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha))$ аксиома $\mathbf{H5}$[31]
4. $((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha) \Rightarrow (\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \wedge ((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)$ из 1, 3 према $\mathbf{MP}$
5. $(\neg\alpha \Rightarrow (\alpha \Rightarrow \bot)) \wedge ((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)$ из 2, 4 према $\mathbf{MP}$

$\triangleright$

Теорема 4. $\Gamma \vdash \alpha$ *акко* $\Gamma \vdash_{\mathbf{H}} \alpha$.

Доказ да је Хилбертов систем за дедукцију еквивалентан природној дедукцији спроводи се индукцијом по дужини извођења секвената у једном, одн. другом систему. Доказ изостављамо.

Теорема потпуности

У досадашњим разматрањима није било тешко уочити да релација сематичке последице ($\models$) и релација синтаксне последице ($\vdash$) поседују низ заједничких особина, без обзира на то што су дефинисане на потпуно различите начине (па су и докази тих заједничких особина потпуно различити). Као илустрацију ове тврдње наводимо следећу лему.

Лема 11. *Ако су* α, β, γ *произвољне формуле, тада*

1. $\alpha, \beta \models \gamma$ *акко* $\models \alpha \wedge \beta \Rightarrow \gamma$;
2. $\alpha, \beta \vdash \gamma$ *акко* $\vdash \alpha \wedge \beta \Rightarrow \gamma$.

Доказ. (1) ($\rightarrow$) Претпоставимо да је $\alpha, \beta \models \gamma$. Нека је v произвољна валуација. Ако је $\widehat{v}(\alpha \wedge \beta) = 0$, онда мора бити и $\widehat{v}(\alpha \wedge \beta \Rightarrow \gamma) = 1$, тј. $v \models \alpha \wedge \beta \Rightarrow \gamma$. Ако је $\widehat{v}(\alpha \wedge \beta) = 1$, онда је $\widehat{v}(\alpha) = 1$ и $\widehat{v}(\beta) = 1$, тј. $v \models \alpha, \beta$, па према претпоставци $v \models \gamma$, односно $\widehat{v}(\gamma) = 1$. Најзад, из $\widehat{v}(\alpha \wedge \beta) = 1$ и $\widehat{v}(\gamma) = 1$, закључујемо да је $\widehat{v}(\alpha \wedge \beta \Rightarrow \gamma) = 1$, тј. $v \models \alpha \wedge \beta \Rightarrow \gamma$.
($\leftarrow$) Претпоставимо да је $\models \alpha \wedge \beta \Rightarrow \gamma$. Нека је v валуација таква да је $v \models \alpha, \beta$, тј. $\widehat{v}(\alpha) = \widehat{v}(\beta) = 1$. Како је тада и $\widehat{v}(\alpha \wedge \beta) = 1$, а по претпоставци је $\widehat{v}(\alpha \wedge \beta \Rightarrow \gamma) = 1$, закључујемо да мора бити и $\widehat{v}(\gamma) = 1$, тј. $v \models \gamma$.

[31] $\underbrace{(\neg\alpha \Rightarrow (\alpha \Rightarrow \bot))}_{\varphi} \Rightarrow (\underbrace{((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)}_{\psi} \Rightarrow \underbrace{(\neg\alpha \Rightarrow (\alpha \Rightarrow \bot))}_{\varphi} \wedge \underbrace{((\alpha \Rightarrow \bot) \Rightarrow \neg\alpha)}_{\psi})$

(2) $(\rightarrow)$ Претпоставимо да је $\alpha, \beta \vdash \gamma$.

1. $\alpha, \beta \vdash \gamma$	[претпоставка]
2. $\alpha \wedge \beta, \alpha, \beta \vdash \gamma$	(slab)
3. $\alpha \wedge \beta, \alpha \vdash \beta \Rightarrow \gamma$	из 2 према $(\Rightarrow_{\mathrm{U}})$
4. $\alpha \wedge \beta \vdash \alpha \Rightarrow (\beta \Rightarrow \gamma)$	из 3 према $(\Rightarrow_{\mathrm{U}})$
5. $\alpha \wedge \beta \vdash \alpha \wedge \beta$	(ax)
6. $\alpha \wedge \beta \vdash \alpha$	из 5 према $(\wedge_{\mathrm{E}}^{\mathrm{l}})$
7. $\alpha \wedge \beta \vdash \beta$	из 5 према $(\wedge_{\mathrm{E}}^{\mathrm{d}})$
8. $\alpha \wedge \beta \vdash \beta \Rightarrow \gamma$	из 4, 6 према $(\Rightarrow_{\mathrm{E}})$
9. $\alpha \wedge \beta \vdash \gamma$	из 8, 7 према $(\Rightarrow_{\mathrm{E}})$
10. $\vdash \alpha \wedge \beta \Rightarrow \gamma$	из 9 према $(\Rightarrow_{\mathrm{U}})$

$(\leftarrow)$ Претпоставимо да је $\vdash \alpha \wedge \beta \Rightarrow \gamma$.

1. $\vdash \alpha \wedge \beta \Rightarrow \gamma$	[претпоставка]
2. $\alpha, \beta \vdash \alpha \wedge \beta \Rightarrow \gamma$	из 1 према $2 \times$ (slab)
3. $\alpha, \beta \vdash \alpha$	(ax)
4. $\alpha, \beta \vdash \beta$	(ax)
5. $\alpha, \beta \vdash \alpha \wedge \beta$	из 3, 4 према $(\wedge_{\mathrm{U}})$
6. $\alpha, \beta \vdash \gamma$	из 2, 5 према $(\Rightarrow_{\mathrm{E}})$.

$\square$

Математичком индукцијом једноставно се показује и следеће тврђење.

Лема 12. *Ако су $\alpha_1, \ldots, \alpha_n, \beta$ произвољне формуле, тада*

1. $\alpha_1, \ldots, \alpha_n \models \beta$ *акко* $\models \alpha_1 \wedge \cdots \wedge \alpha_n \Rightarrow \beta$;
2. $\alpha_1, \ldots, \alpha_n \vdash \beta$ *акко* $\vdash \alpha_1 \wedge \cdots \wedge \alpha_n \Rightarrow \beta$.

Сетимо се да је наша полазна намера приликом увођења појма синтаксне последице ($\vdash$) била да на један други начин, независно од валуација, окарактеришемо семантичку последицу ($\models$). Да смо у томе успели доказују теореме у овом поглављу. Најпре ћемо формулисати све важне теореме овог одељка, прокоментарисати њихов однос, а затим и сваку од њих доказати.

Наиме, желимо да докажемо следећу теорему

$$(\bigstar) \qquad \Gamma \vdash \alpha \text{ акко } \Gamma \models \alpha.$$

Од посебног значаја је и њена директна последица

$$(\star) \qquad \vdash \alpha \text{ акко } \models \alpha.$$

Иако се чини да је ова последица слабија од наведене теореме, теорема $(\star)$, заједно са теоремом компактности и лемом 9, имплицира $(\bigstar)$. Приметимо најпре да из ($\star$) једноставно доказујемо, применом леме 12, да за сваки коначан скуп формула Γ важи: $\Gamma \vdash \alpha$ акко $\Gamma \models \alpha$. Заиста, ако је Γ коначан скуп[32], онда

$$\Gamma \vdash \alpha \text{ акко } \vdash \bigwedge \Gamma \Rightarrow \alpha \overset{(\star)}{\text{ акко }} \models \bigwedge \Gamma \Rightarrow \alpha \text{ акко } \Gamma \models \alpha.$$

Уколико је Γ бесконачан скуп, тада се морамо позвати на теорему компактности и лему 9.

$$\begin{aligned} \Gamma \vdash \alpha \quad & \text{акко} \quad \Gamma_0 \vdash \alpha \text{ за неки коначан } \Gamma_0 \subseteq \Gamma \text{ [према леми 9]} \\ & \text{акко} \quad \Gamma_0 \models \alpha \text{ за неки коначан } \Gamma_0 \subseteq \Gamma \\ & \text{акко} \quad \Gamma \models \alpha \text{ [према теореми компактности]} \end{aligned}$$

У наставку, најпре ћемо доказати тзв. **теорему сагласности**: ако је $\Gamma \vdash \alpha$, онда је $\Gamma \models \alpha$. Специјално, ако је $\vdash \alpha$, онда је $\models \alpha$. Још једна последица теореме сагласности је занимљива; реч је о тзв. **теореми о непротивречности**: ако скуп Γ има модел ($\Gamma \not\models \perp$), онда се из Γ не може извести контрадикција ($\Gamma \nvdash \perp$), тј. Γ је *непротивречан* (*конзистентан*) скуп.

Након доказа теореме сагласности, остаје да докажемо и њен обрат тзв. **теорему јаке потпуности**: из $\Gamma \models \alpha$, следи $\Gamma \vdash \alpha$. Уобичајено је да се уместо теореме јаке потпуности доказује једна њена варијанта тзв. **теорема о постојању модела**: Ако је Γ непротивречна теорија ($\Gamma \nvdash \perp$), онда има модел ($\Gamma \not\models \perp$), тј. постоји валуација која задовољава све формуле из Γ. Наредна лема успоставља везу између ове две теореме.

Лема 13. *Следећа два тврђења су еквивалентна:*

(1) *за сваку формулу* α, *из* $\Gamma \models \alpha$, *следи* $\Gamma \vdash \alpha$*;*

(2) *из* $\Gamma \nvdash \perp$, *следи* $\Gamma \not\models \perp$.

Доказ. $(1) \rightarrow (2)$ Тривијално.
$(2) \rightarrow (1)$ Претпоставимо да важи (2) и да је $\Gamma \models \alpha$. Претпоставимо и, супротно ономе што треба доказати, да је $\Gamma \nvdash \alpha$. Тада $\Gamma, \neg\alpha \nvdash \perp$, јер бисмо у супротном имали

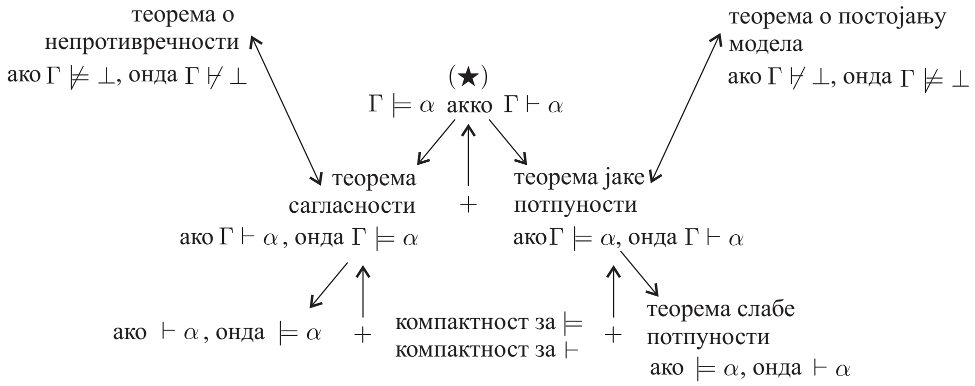
$$\frac{\Gamma, \neg\alpha \vdash \perp}{\Gamma \vdash \alpha}(\perp_c).$$

На основу (2), закључујемо да $\Gamma, \neg\alpha \not\models \perp$, тј. да постоји валуација v таква да $v \models \Gamma, \neg\alpha$, што је у супротности са $\Gamma \models \alpha$. Дакле, $\Gamma \vdash \alpha$. □

Као што смо већи истакли, теорема јаке потпуности, због теореме компактности, биће последица **теореме слабе потпуности**: из $\models \alpha$, следи $\vdash \alpha$.

[32] Ако је $\Gamma = \{\gamma_1, \dots, \gamma_n\}$, онда је $\bigwedge \Gamma$ формула $\gamma_1 \wedge \cdots \wedge \gamma_n$.

Следе обећани докази свих поменутих теорема. Након теореме сагласности доказаћемо независно све три теореме: теорему слабе потпуности, теорему о постојању модела и теорему јаке потпуности. Разлог је тај што сваки доказ доноси неке корисне идеје и специфичан приступ. Узимајући у обзир претходна разматрања, доказивањем ове три теореме заправо доказујемо теорему (★) на три начина.



Теорема сагласности

Теорема 5. [***Теорема сагласности***] *Ако је* $\Gamma \vdash \alpha$*, онда је* $\Gamma \models \alpha$.

Доказ. Ако је секвент $\Gamma \vdash \alpha$ доказив, онда одговарајуће извођење можемо представити као коначан низ секвената $\Gamma_1 \vdash \alpha_1, \ldots, \Gamma_n \vdash \alpha_n$, за неко $n \geqslant 1$, при чему је $\Gamma_n = \Gamma$ и $\alpha_n = \alpha$ и сваки секвент $\Gamma_k \vdash \alpha_k$, $1 \leqslant k \leqslant n$, добијен је или применом правила (ax) или применом неког другог правила на секвенте који му претходе у низу. Важно је приметити да је тада доказив и сваки секвент наведеног низа и да његово извођење дају секвенти који му претходе у низу. Под дужином извођења неког секвента подразумевамо дужину низа којим је то извођење представљено.

Доказ теореме сагласности изводимо индукцијом по дужини извођења за $\Gamma \vdash \alpha$.

Претпоставимо да је дужина извођења за $\Gamma \vdash \alpha$ једнака 1. Нека је v валуација таква да је $v \models \Gamma$. Треба да докажемо да је тада и $v \models \alpha$. Из претпоставке да је дужина извођења за $\Gamma \vdash \alpha$ једнака 1, закључујемо да је $\Gamma \vdash \alpha$ добијен применом правила (ax), тј. да $\alpha \in \Gamma$. Дакле, ако $v \models \Gamma$, онда у овом случају тривијално следи да $v \models \alpha$.

Претпоставимо да је тврђење које желимо да докажемо тачно за све природне бројеве мање од неког n, $n > 1$. Нека је дужина извођења секвента $\Gamma \vdash \alpha$ једнака n. Претпоставимо да је v валуација таква да $v \models \Gamma$. Разликоваћемо случајеве у зависности од тога којим правилом је добијен последњи секвент $\Gamma \vdash \alpha$.

(slab) Ако је $\Gamma \vdash \alpha$ добијен применом правила (slab), онда му у извођењу претходи секвент облика $\Gamma \setminus \{\gamma\} \vdash \alpha$, за неку формулу γ. Из $v \models \Gamma$, следи да $v \models \Gamma \setminus \{\gamma\}$, а како је дужина доказа за $\Gamma \setminus \{\gamma\} \vdash \alpha$ мања од n, према индуктивној претпоставци закључујемо да је $v \models \alpha$.

($\Rightarrow_{\mathrm{U}}$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\Rightarrow_{\mathrm{U}}$), онда α мора бити облика $\varphi \Rightarrow \psi$, за неке формуле φ и ψ. Поред тога, у одговарајућем извођењу секвенту $\Gamma \vdash \varphi \Rightarrow \psi$ (тј. $\Gamma \vdash \alpha$), претходи секвент $\Gamma, \varphi \vdash \psi$. Уколико $v \models \varphi$, онда $v \models \Gamma, \varphi$, па према индуктивној претпоставци следи да $v \models \psi$, а самим тим и $v \models \varphi \Rightarrow \psi$, тј. $v \models \alpha$. Уколико $v \not\models \varphi$, онда одмах добијамо да $v \models \varphi \Rightarrow \psi$, тј. $v \models \alpha$.

Препоручујемо читаоцу да доказ самостално комплетира и да на крају сопствени доказ упореди са наставком доказа датим овде.

($\Rightarrow_{\mathrm{E}}$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\Rightarrow_{\mathrm{E}}$), онда му претходе секвенти $\Gamma \vdash \varphi$ и $\Gamma \vdash \varphi \Rightarrow \alpha$, за неку формулу φ. Пошто $v \models \Gamma$, према индуктивној претпоставци добијамо да $v \models \varphi$ и $v \models \varphi \Rightarrow \alpha$, одакле једноставно добијамо $v \models \alpha$.

($\wedge_{\mathrm{U}}$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\wedge_{\mathrm{U}}$), онда α мора бити облика $\varphi \wedge \psi$, за неке формуле φ и ψ. Поред тога, у одговарајућем извођењу, секвенту $\Gamma \vdash \varphi \wedge \psi$ (тј. $\Gamma \vdash \alpha$) претходе секвенти $\Gamma \vdash \varphi$ и $\Gamma \vdash \psi$. Из $v \models \Gamma$, према индуктивној претпоставци следи да $v \models \varphi$ и $v \models \psi$, а самим тим и $v \models \varphi \wedge \psi$, тј. $v \models \alpha$.

($\wedge_{\mathrm{E}}^{\mathrm{l}}$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\wedge_{\mathrm{E}}^{\mathrm{l}}$), онда му претходи секвент $\Gamma \vdash \alpha \wedge \varphi$, за неку формулу φ. Пошто $v \models \Gamma$, према индуктивној претпоставци добијамо да $v \models \alpha \wedge \varphi$, одакле следи да $v \models \alpha$.

($\wedge_{\mathrm{E}}^{\mathrm{d}}$) Аналогно претходном случају.

($\vee_{\mathrm{U}}^{\mathrm{l}}$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\vee_{\mathrm{U}}^{\mathrm{l}}$), онда α мора бити облика $\varphi \vee \psi$, за неке формуле φ и ψ. У одговарајућем извођењу, секвенту $\Gamma \vdash \varphi \vee \psi$ (тј. $\Gamma \vdash \alpha$) претходи секвент $\Gamma \vdash \varphi$. Из $v \models \Gamma$, према индуктивној претпоставци следи да $v \models \varphi$, одакле добијамо $v \models \varphi \vee \psi$, тј. $v \models \alpha$.

($\vee_{\mathrm{U}}^{\mathrm{d}}$) Аналогно претходном случају.

($\vee_E$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\vee_E$), онда му претходе секвенти $\Gamma \vdash \varphi \vee \psi$, $\Gamma, \varphi \vdash \alpha$ и $\Gamma, \psi \vdash \alpha$, за неке формуле φ и ψ. Из $v \models \Gamma$ према индуктивној претпоставци следи да $v \models \varphi \vee \psi$, тј. $v \models \varphi$ или $v \models \psi$, па самим тим $v \models \Gamma, \varphi$ или $v \models \Gamma, \psi$. Било који од ова два случаја да наступи, позивањем на индуктивну претпоставку добијамо да $v \models \alpha$.

($\neg_U$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\neg_U$), онда је α облика $\neg\varphi$, за неку формулу φ. У одговарајућем извођењу, секвенту $\Gamma \vdash \neg\varphi$ (тј. $\Gamma \vdash \alpha$) претходи секвент $\Gamma, \varphi \vdash \bot$. Ако би за валуацију v такву да $v \models \Gamma$ било и $v \models \varphi$, према индуктивној претпоставци имали бисмо $v \models \bot$, што није могуће. Дакле, $v \not\models \varphi$, па $v \models \neg\varphi$, тј. $v \models \alpha$.

($\neg_E$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\neg_E$), онда је α заправо логичка константа $\bot$ и у одговарајућем извођењу наведеном секвенту претходе секвенти $\Gamma \vdash \varphi$ и $\Gamma \vdash \neg\varphi$, за неку формулу φ. У овом случају треба показати да не постоји валуација која задовољава све формуле из Γ. Ако би постојала валуација v таква да је $v \models \Gamma$, онда бисмо према индуктивној претпоставци имали да $v \models \varphi$ и $v \models \neg\varphi$, што није могуће.

($\bot_c$) Ако је $\Gamma \vdash \alpha$ добијен применом правила ($\bot_c$), онда у одговарајућем извођењу овом секвенту претходи $\Gamma, \neg\alpha \vdash \bot$. Ако би за валуацију v такву да $v \models \Gamma$ било и $v \not\models \alpha$, тј. $v \models \neg\alpha$, према индуктивној претпоставци имали бисмо $v \models \bot$, што није могуће. Дакле, $v \models \alpha$.

$\square$

Теорема слабе потпуности

Теорему слабе потпуности изводимо као последицу наредне две леме.

Лема 14. *Ако $\lhd$ означава једну од релација $\models$ (семантичку последицу) или $\vdash$ (синтаксну последицу), онда важи:*

($D_\neg^\neg$) $\Gamma \lhd \neg\neg\alpha$ *акко* $\Gamma \lhd \alpha$;

($D_\vee$) $\Gamma \lhd \alpha \vee \beta$ *акко* $\Gamma, \neg\alpha \lhd \beta$;

($D_\vee^\neg$) $\Gamma \lhd \neg(\alpha \vee \beta)$ *акко* $\Gamma \lhd \neg\alpha$ *и* $\Gamma \lhd \neg\beta$;

($D_\wedge$) $\Gamma \lhd \alpha \wedge \beta$ *акко* $\Gamma \lhd \alpha$ *и* $\Gamma \lhd \beta$;

($D_\wedge^\neg$) $\Gamma \lhd \neg(\alpha \wedge \beta)$ *акко* $\Gamma, \alpha \lhd \neg\beta$;

($D_\Rightarrow$) $\Gamma \lhd \alpha \Rightarrow \beta$ *акко* $\Gamma, \alpha \lhd \beta$;

($D^{\neg}_{\Rightarrow}$) $\Gamma \lhd \neg(\alpha \Rightarrow \beta)$ *акко* $\Gamma \lhd \alpha$ *и* $\Gamma \lhd \neg\beta$;

($D_{\Leftrightarrow}$) $\Gamma \lhd \alpha \Leftrightarrow \beta$ *акко* $\Gamma, \alpha \lhd \beta$ *и* $\Gamma, \beta \lhd \alpha$;

($D^{\neg}_{\Leftrightarrow}$) $\Gamma \lhd \neg(\alpha \Leftrightarrow \beta)$ *акко* $\Gamma, \neg\alpha \lhd \beta$ *и* $\Gamma, \neg\beta \lhd \alpha$;

($L^{\neg}_{\neg}$) $\Gamma, \neg\neg\alpha \lhd \varphi$ *акко* $\Gamma, \alpha \lhd \varphi$;

($L_{\vee}$) $\Gamma, \alpha \vee \beta \lhd \varphi$ *акко* $\Gamma, \alpha \lhd \varphi$ *и* $\Gamma, \beta \lhd \varphi$;

($L^{\neg}_{\vee}$) $\Gamma, \neg(\alpha \vee \beta) \lhd \varphi$ *акко* $\Gamma\neg\alpha, \neg\beta \lhd \varphi$;

($L_{\wedge}$) $\Gamma, \alpha \wedge \beta \lhd \varphi$ *акко* $\Gamma, \alpha, \beta \lhd \varphi$;

($L^{\neg}_{\wedge}$) $\Gamma, \neg(\alpha \wedge \beta) \lhd \varphi$ *акко* $\Gamma, \neg\alpha \lhd \varphi$ *и* $\Gamma, \neg\beta \lhd \varphi$;

($L_{\Rightarrow}$) $\Gamma, \alpha \Rightarrow \beta \lhd \varphi$ *акко* $\Gamma, \neg\alpha \lhd \varphi$ *и* $\Gamma, \beta \lhd \varphi$;

($L^{\neg}_{\Rightarrow}$) $\Gamma, \neg(\alpha \Rightarrow \beta) \lhd \varphi$ *акко* $\Gamma, \alpha, \neg\beta \lhd \varphi$;

($L_{\Leftrightarrow}$) $\Gamma, \alpha \Leftrightarrow \beta \lhd \varphi$ *акко* $\Gamma, \alpha, \beta \lhd \varphi$ *и* $\Gamma, \neg\alpha, \neg\beta \lhd \varphi$;

($L^{\neg}_{\Leftrightarrow}$) $\Gamma, \neg(\alpha \Leftrightarrow \beta) \lhd \varphi$ *акко* $\Gamma, \neg\alpha, \beta \lhd \varphi$ *и* $\Gamma, \alpha, \neg\beta \lhd \varphi$.

Доказ. Докази свих наведених тврђења представљају корисну вежбу, те их остављамо читаоцу. Примера ради, наводимо само доказ тврђења ($D_{\vee}$). Треба да докажемо:

$$(1) \quad \Gamma \models \alpha \vee \beta \text{ акко } \Gamma, \neg\alpha \models \beta \quad \text{и} \quad (2) \quad \Gamma \vdash \alpha \vee \beta \text{ акко } \Gamma, \neg\alpha \vdash \beta.$$

Докажимо (1).

($\rightarrow$) Претпоставимо да је $\Gamma \models \alpha \vee \beta$. Нека је v произвољна валуација таква да $v \models \Gamma, \neg\alpha$. Из $v \models \Gamma$ и $\Gamma \models \alpha \vee \beta$ закључујемо да $v \models \alpha \vee \beta$, тј. $\widehat{v}(\alpha \vee \beta) = 1$. Из $v \models \neg\alpha$, следи да је $\widehat{v}(\alpha) = 0$. Како је $\widehat{v}(\alpha \vee \beta) = 1$ и $\widehat{v}(\alpha) = 0$, добијамо да је $\widehat{v}(\beta) = 1$, тј. $v \models \beta$.

($\leftarrow$) Претпоставимо да је $\Gamma, \neg\alpha \models \beta$. Нека је v произвољна валуација таква да $v \models \Gamma$. Разликујемо два случаја: $\widehat{v}(\alpha) = 1$ или $\widehat{v}(\alpha) = 0$. Ако је $\widehat{v}(\alpha) = 1$, онда мора бити и $\widehat{v}(\alpha \vee \beta) = 1$, тј. $v \models \alpha \vee \beta$. Ако је $\widehat{v}(\alpha) = 0$, онда $v \models \Gamma, \neg\alpha$, па због $\Gamma, \neg\alpha \models \beta$, закључујемо да је $v \models \beta$, тј. $\widehat{v}(\beta) = 1$, одакле добијамо $\widehat{v}(\alpha \vee \beta) = 1$, односно $v \models \alpha \vee \beta$.

Докажимо (2).

($\rightarrow$) Претпоставимо да је $\Gamma \vdash \alpha \vee \beta$.

1. $\Gamma \vdash \alpha \vee \beta$	[претпоставка]
2. $\Gamma, \neg\alpha \vdash \alpha \vee \beta$	из 1. према (slab)

3. $\Gamma, \neg\alpha, \alpha \vdash \beta$ $\quad(\neg_\mathrm{L}) + (\bot_\mathrm{i})$
4. $\Gamma, \neg\alpha, \beta \vdash \beta$ $\quad(\mathrm{ax})$
5. $\Gamma, \neg\alpha \vdash \beta$ $\quad$ из 2, 3, 4 према $(\vee_\mathrm{E})$

($\leftarrow$) Претпоставимо да је $\Gamma, \neg\alpha \vdash \beta$.

1. $\Gamma, \neg\alpha \vdash \beta$ $\quad$ [претпоставка]
2. $\Gamma, \neg\alpha, \neg(\alpha \vee \beta) \vdash \beta$ $\quad$ из 1. према (slab)
3. $\Gamma, \neg\alpha, \neg(\alpha \vee \beta) \vdash \alpha \vee \beta$ $\quad$ из 2. према $(\vee_\mathrm{U}^\mathrm{d})$
4. $\Gamma, \neg\alpha, \neg(\alpha \vee \beta) \vdash \neg(\alpha \vee \beta)$ $\quad(\mathrm{ax})$
5. $\Gamma, \neg\alpha, \neg(\alpha \vee \beta) \vdash \bot$ $\quad$ из 3, 4 према $(\neg_\mathrm{E})$
6. $\Gamma, \neg(\alpha \vee \beta) \vdash \alpha$ $\quad$ из 5 према $(\bot_\mathrm{c})$
7. $\Gamma, \neg(\alpha \vee \beta) \vdash \alpha \vee \beta$ $\quad$ из 6 према $(\vee_\mathrm{U}^\mathrm{l})$
8. $\Gamma, \neg(\alpha \vee \beta) \vdash \neg(\alpha \vee \beta)$ $\quad(\mathrm{ax})$
9. $\Gamma, \neg(\alpha \vee \beta) \vdash \bot$ $\quad$ из 7, 8 према $(\neg_\mathrm{E})$
10. $\Gamma \vdash \alpha \vee \beta$ $\quad$ из 9 према $(\bot_\mathrm{c})$

$\square$

На основу особина наведених у претходној леми, закључујемо да се испитивање да ли је формула θ теорема (таутологија) исказног рачуна, односно да ли је $\vdash \theta$ ($\models \theta$), може свести на „систем“ веома једноставних проблема облика:

$$p_{i_1}^{a_1}, \ldots, p_{i_m}^{a_m} \vdash p_j^{a_j} \qquad (p_{i_1}^{a_1}, \ldots, p_{i_m}^{a_m} \models p_j^{a_j}),$$

где су $p_{i_1}, \ldots, p_{i_m}, p_j$ нека исказна слова, $a_{i_1}, \ldots, a_{i_m}, a_j \in \{0, 1\}$, при чему p^0 означава $\neg p$, а p^1 означава p, за било које исказно слово p. Ово запажање илуструјемо у наредном примеру.

Пример 24. Особине наведене у претходној леми можемо посматрати као правила помоћу којих се неки секвент може „сводити“ на секвенте у којима учествују формуле све мање сложености.

Докажимо, на поменути начин, да је $\vdash (p_0 \Rightarrow p_1 \vee p_2) \Rightarrow (p_0 \wedge \neg p_2 \Rightarrow \neg(p_0 \Rightarrow \neg p_1))$.

$\vdash (p_0 \Rightarrow p_1 \vee p_2) \Rightarrow (p_0 \wedge \neg p_2 \Rightarrow \neg(p_0 \Rightarrow \neg p_1))$

акко $p_0 \Rightarrow p_1 \vee p_2 \vdash p_0 \wedge \neg p_2 \Rightarrow \neg(p_0 \Rightarrow \neg p_1)$ $\quad(\mathrm{D}_\Rightarrow)$

акко $p_0 \Rightarrow p_1 \vee p_2, p_0 \wedge \neg p_2 \vdash \neg(p_0 \Rightarrow \neg p_1)$ $\quad(\mathrm{D}_\Rightarrow)$

акко $p_0 \Rightarrow p_1 \vee p_2, p_0 \wedge \neg p_2 \vdash p_0$,
$p_0 \Rightarrow p_1 \vee p_2, p_0 \wedge \neg p_2 \vdash \neg\neg p_1$ $\quad(\mathrm{D}_\Rightarrow^\neg)$

акко $p_0 \Rightarrow p_1 \vee p_2, p_0 \wedge \neg p_2 \vdash p_0$,
$p_0 \Rightarrow p_1 \vee p_2, p_0 \wedge \neg p_2 \vdash p_1$ $\quad(\mathrm{D}_\neg^\neg)$

акко $p_0 \Rightarrow p_1 \vee p_2, p_0, \neg p_2 \vdash p_0$,
$p_0 \Rightarrow p_1 \vee p_2, p_0, \neg p_2 \vdash p_1$ $\quad(\mathrm{L}_\wedge)$

акко $\neg p_0, p_0, \neg p_2 \vdash p_0$,
$p_1 \vee p_2, p_0, \neg p_2 \vdash p_0$,
$\neg p_0, p_0, \neg p_2 \vdash p_1$,
$p_1 \vee p_2, p_0, \neg p_2 \vdash p_1$ $\quad(\mathrm{L}_\Rightarrow)$

акко $\neg p_0, p_0, \neg p_2 \vdash p_0,$
$p_1, p_0, \neg p_2 \vdash p_0,$
$p_2, p_0, \neg p_2 \vdash p_0,$
$\neg p_0, p_0, \neg p_2 \vdash p_1,$
$p_1, p_0, \neg p_2 \vdash p_1$
$p_2, p_0, \neg p_2 \vdash p_1$ $(\mathrm{L}_\vee)$

У датом извођењу, полазни секвент је сведен на „систем" секвената у којима се појављују само исказна слова и негације исказних слова. Очигледно је да се сви секвенти „система" могу извести, па је на тај начин доказан и полазни секвент. ▷

Лема 15. *Ако су* $p_{i_1}, \ldots, p_{i_m}, p_j$ *нека исказна слова и* $a_{i_1}, \ldots, a_{i_m}, a_j \in \{0, 1\}$, *тада су следећа тврђења еквивалентна:*

(1) $p_{i_1}^{a_1}, \ldots, p_{i_m}^{a_m} \vdash p_j^{a_j}$*;*

(2) $p_{i_1}^{a_1}, \ldots, p_{i_m}^{a_m} \models p_j^{a_j}$*;*

(3) постоји $k \in \{1, \ldots, m\}$ *такав да је* $p_j = p_{i_k}$ *и* $a_j = a_k$ *или постоје* $k, \ell \in \{1, \ldots, m\}$, $k \neq \ell$, *такви да је* $p_{i_k} = p_{i_\ell}$ *и* $a_k \neq a_\ell$*.*

Доказ. $(1) \to (2)$ Директно из теореме сагласности.
$(2) \to (3)$ Ако постоје $k, \ell \in \{1, \ldots, m\}$, $k \neq \ell$, такви да је $p_{i_k} = p_{i_\ell}$ и $a_k \neq a_\ell$, тврђење је доказано. Претпоставимо зато да овакви k и ℓ не постоје. У том случају, ако би слово p_j било различито од сваког слова $p_{i_1}, \ldots, p_{i_m}$, онда би за валуацију v такву да је $v(p_{i_k}) = a_k$ (приметимо да ако међу словима $p_{i_1}, \ldots, p_{i_m}$ има истих, онда и „изложиоци" тих слова морају бити једнаки) и $v(p_j) = 1 - a_j$, важило $v \models p_{i_k}^{a_k}$, $1 \leqslant k \leqslant m$, и $v \not\models p_j^{a_j}$, супротно тврђењу (2). Дакле, слово p_j мора бити једнако неком слову p_{i_k}, $1 \leqslant k \leqslant m$. Самим тим, због (2), мора бити и $a_j = a_k$.
$(3) \to (1)$ Ако постоји $k \in \{1, \ldots, m\}$ такав да је $p_j = p_{i_k}$ и $a_j = a_k$, онда према правилу (ax) важи (1) $\ldots, p_j^{a_j}, \ldots \vdash p_j^{a_j}$. Ако постоје $k, \ell \in \{1, \ldots, m\}$, $k \neq \ell$, такви да је $p_{i_k} = p_{i_\ell}$ и $a_k \neq a_\ell$, онда према правилу $(\neg_\mathrm{L})$ следи $\ldots, p_{i_k}, \ldots, \neg p_{i_k}, \ldots, \vdash \bot$, одакле применом правила $(\bot_\mathrm{i})$ закључујемо да важи (1). □

Последица претходне две леме је теорема слабе потпуности.

Теорема 6. [***Теорема слабе потпуности***] *Ако* $\models \alpha$, *онда* $\vdash \alpha$*.*

Теорема о постојању модела

Теорема 7. [***Теорема о постојању модела***] *Ако је неки скуп формула непротивречан, онда има модел (тј. постоји валуација која задовољава све формуле тог скупа).*

Идеја доказа. Нека је Γ непротивречан скуп формула, тј. $\Gamma \nvdash \perp$. Треба да докажемо да постоји валуација $v : P \to \{0,1\}$ таква да $v \models \Gamma$, тј. $\widehat{v}(\gamma) = 1$, за све $\gamma \in \Gamma$. Другим речима, ако је $\chi_\Gamma : \mathrm{For} \to \{0,1\}$ карактеристична функција подскупа $\Gamma \subseteq \mathrm{For}$, онда треба показати да постоји валуација v таква да је $\chi_\Gamma(\alpha) \leqslant \widehat{v}(\alpha)$, за сваку формулу α. Најважнија досетка у доказу теореме потпуности јесте посматрати функцију $\widehat{v} : \mathrm{For} \to \{0,1\}$ као карактеристичну функцију неког подскупа од For. Наиме, свака валуација v одређује један непротивречан скуп $\Delta_v = \{\alpha \in \mathrm{For} \mid \widehat{v}(\alpha) = 1\}$. Поред тога, скуп Δ_v је и максималан (у смислу инклузије) непротивречан скуп формула јер му се не може додати ниједна формула а да се сачува непротивречност. Заиста, ако је δ било која формула која не припада Δ_v, онда је $\Delta_v \cup \{\delta\}$ противречан скуп: из $\delta \notin \Delta_v$, следи да је $\widehat{v}(\delta) = 0$, па је $\widehat{v}(\neg\delta) = 1$, и сходно томе $\neg\delta \in \Delta_v$, што даље значи да δ и $\neg\delta$ припадају $\Delta_v \cup \{\delta\}$ одакле закључујемо да је овај скуп противречан. Од суштинске важности за доказ теореме потпуности биће обрат: ако је Δ максимално непротивречан скуп, онда постоји валуација v таква да је $\Delta = \Delta_v$. Карактеристична функција било ког максимално непротивречног скупа јесте екстензија неке валуације. Основна идеја доказа теореме потпуности сада је јасна: проширити скуп Γ до неког максимално непротивречног скупа Δ.

Дефиниција 14. *Непротивречан скуп формула Γ је максимално непротивречан уколико не постоји прави надскуп овог скупа који је непротивречан.*

Лема 16. *Ако је Δ максимално непротивречан скуп, онда постоји валуација v таква да је $\Delta = \{\alpha \in \mathrm{For} \mid \widehat{v}(\alpha) = 1\}$, тј. таква да је њена екстензија $\widehat{v} : \mathrm{For} \to \{0,1\}$ једнака карактеристичној функцији $\chi_\Delta : \mathrm{For} \to \{0,1\}$.*

Доказ леме. Нека је Δ максимално непротивречан скуп.

Приметимо најпре да за сваку формулу α важи или $\alpha \in \Delta$ или $\neg\alpha \in \Delta$ (и, наравно, никако оба). Заиста, ако би за неку формулу α било $\alpha \notin \Delta$ и $\neg\alpha \notin \Delta$, због максималне непротивречности скупа Δ имали бисмо $\Delta, \alpha \vdash \perp$ и $\Delta, \neg\alpha \vdash \perp$, а самим тим и

$$\dfrac{\dfrac{\Delta, \alpha \vdash \perp}{\Delta \vdash \neg\alpha}(\neg_{\mathrm{U}}) \qquad \dfrac{\Delta, \neg\alpha \vdash \perp}{\Delta \vdash \alpha}(\perp_{\mathrm{c}})}{\Delta \vdash \perp}(\neg_{\mathrm{E}}),$$

што је супротно непротивречности скупа Δ.

Тражена валуација се може „прочитати“ из скупа Δ. Нека је $v_\Delta : P \to \{0,1\}$ рестрикција карактеристичне функције $\chi_\Delta : \mathrm{For} \to \{0,1\}$ на скуп исказних слова P, $v_\Delta = \chi_\Delta \restriction_P$, то јест:

$$v_\Delta(p) = \begin{cases} 1, & p \in \Delta, \\ 0, & \neg p \in \Delta. \end{cases}$$

Треба да докажемо да је $\widehat{v_\Delta} = \chi_\Delta$, тј. да је $\widehat{v_\Delta}(\alpha) = \chi_\Delta(\alpha)$, за сваку исказну формулу α. Последња једнакост је очигледно тачна ако је α исказно слово или логичка константа $\bot$. Остаје још да се докаже да за произвољне формуле φ и ψ важи:

$$\begin{array}{ll}
(1) & \chi_\Delta(\neg\varphi) = \neg\chi_\Delta(\varphi) = 1 - \chi_\Delta(\varphi) \\
(2) & \chi_\Delta(\varphi \wedge \psi) = \chi_\Delta(\varphi) \wedge \chi_\Delta(\psi) = \min\{\chi_\Delta(\varphi), \chi_\Delta(\psi)\} \\
(3) & \chi_\Delta(\varphi \vee \psi) = \chi_\Delta(\varphi) \vee \chi_\Delta(\psi) = \max\{\chi_\Delta(\varphi), \chi_\Delta(\psi)\} \\
(4) & \chi_\Delta(\varphi \Rightarrow \psi) = \chi_\Delta(\varphi) \Rightarrow \chi_\Delta(\psi)
\end{array}$$

Ове једнакости су у складу са дефиницијом екстензије неке валуације и самим тим доказују жељено тврђење. Будући да је χ_Δ карактеристична функција скупа Δ, наведене једнакости можемо формулисати и у следећем облику:
(1) $\neg\varphi \in \Delta$ акко $\varphi \notin \Delta$,
(2) $\varphi \wedge \psi \in \Delta$ акко $\varphi \in \Delta$ и $\psi \in \Delta$,
(3) $\varphi \vee \psi \in \Delta$ акко $\varphi \in \Delta$ или $\psi \in \Delta$,
(4) $\varphi \Rightarrow \psi \in \Delta$ акко из $\varphi \in \Delta$, следи да $\psi \in \Delta$.
Пре него што докажемо сва наведена тврђења, доказаћемо још једно значајно својство максимално непротивречних скупова:
(0) $\varphi \in \Delta$ акко $\Delta \vdash \varphi$.
<u>Доказ тврђења (0).</u> Ако $\varphi \in \Delta$, онда је јасно да мора бити $\Delta \vdash \varphi$. Да бисмо доказали и обрнуто, претпоставимо да $\Delta \vdash \varphi$ и $\varphi \notin \Delta$. Због максималне непротивречности скупа Δ имамо да $\Delta, \varphi \vdash \bot$, а самим тим и $\Delta \vdash \neg\varphi$, применом правила $(\neg_{\mathrm{U}})$. Међутим тада је

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

што није могуће због непротивречности скупа Δ.
<u>Доказ тврђења (1).</u> $(\rightarrow)$ Ако $\neg\varphi \in \Delta$, онда због непротивречности скупа Δ не може φ припадати овом скупу јер бисмо у супротном имали:

$$\frac{\dfrac{}{\Delta \vdash \neg\varphi}(\mathrm{ax}) \quad \dfrac{}{\Delta \vdash \varphi}(\mathrm{ax})}{\Delta \vdash \bot}(\neg_{\mathrm{E}}).$$

$(\leftarrow)$ Ако $\varphi \notin \Delta$, онда због максималне непротивречности скупа имамо да $\Delta, \varphi \vdash \bot$, а самим тим и

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

Према тврђењу (0) имамо да $\neg\varphi \in \Delta$.
<u>Доказ тврђења (2).</u> $(\rightarrow)$ Ако $\varphi \wedge \psi \in \Delta$, онда $\Delta \vdash \varphi \wedge \psi$ и

$$\frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \varphi}(\wedge_{\mathrm{E}}^{\mathrm{l}}), \quad \text{као и} \quad \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \psi}(\wedge_{\mathrm{E}}^{\mathrm{d}}),$$

па према тврђењу (0) следи $\varphi \in \Delta$ и $\psi \in \Delta$.
$(\leftarrow)$ Ако $\varphi \in \Delta$ и $\psi \in \Delta$, онда $\Delta \vdash \varphi$ и $\Delta \vdash \psi$, па и

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

одакле према (0) следи да $\varphi \wedge \psi \in \Delta$.
Доказ тврђења (3). $(\rightarrow)$ Претпоставимо да $\varphi \vee \psi \in \Delta$, али да $\varphi \notin \Delta$ и $\psi \notin \Delta$. Тада због максималне непротивречности закључујемо да $\Delta \vdash \neg\varphi$ и $\Delta \vdash \neg\psi$. Међутим, тада имамо

$$\frac{\Delta \vdash \varphi \vee \psi \qquad \dfrac{\dfrac{}{\Delta, \varphi \vdash \varphi} \quad \dfrac{\Delta \vdash \neg\varphi}{\Delta, \varphi \vdash \neg\varphi}}{\Delta, \varphi \vdash \bot} \qquad \dfrac{\dfrac{}{\Delta, \psi \vdash \psi} \quad \dfrac{\Delta \vdash \neg\psi}{\Delta, \psi \vdash \neg\psi}}{\Delta, \psi \vdash \bot}}{\Delta \vdash \bot},$$

што је у супротности са непротивречношћу скупа Δ.
$(\leftarrow)$ Ако $\varphi \in \Delta$, онда $\Delta \vdash \varphi$, па имамо и

$$\frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi}(\vee_{\mathrm{U}}^{\mathrm{l}}),$$

одакле према (0) следи да $\varphi \vee \psi \in \Delta$. Аналогно, применом правила $(\vee_{\mathrm{U}}^{\mathrm{d}})$ закључујемо да из $\psi \in \Delta$ следи да $\varphi \vee \psi \in \Delta$.
Доказ тврђења (4). $(\rightarrow)$ Ако $\varphi \Rightarrow \psi \in \Delta$ и $\varphi \in \Delta$, онда имамо да $\Delta \vdash \varphi \Rightarrow \psi$ и $\Delta \vdash \varphi$, па и

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

одакле према (0) следи да $\psi \in \Delta$.
$(\leftarrow)$ Разликујемо два случаја. Ако $\varphi \notin \Delta$, онда због максималности скупа Δ важи $\Delta, \varphi \vdash \bot$, па имамо

$$\dfrac{\dfrac{\dfrac{\Delta, \varphi \vdash \bot}{\Delta, \varphi, \neg\psi \vdash \bot}}{\Delta, \varphi \vdash \psi}}{\Delta \vdash \varphi \Rightarrow \psi}.$$

Ако $\varphi \in \Delta$, онда и $\psi \in \Delta$, а тиме и $\Delta \vdash \psi$, па

$$\dfrac{\dfrac{\Delta \vdash \psi}{\Delta, \varphi \vdash \psi}}{\Delta \vdash \varphi \Rightarrow \psi}.$$

У оба случаја према (0) следи да $\varphi \Rightarrow \psi \in \Delta$. $\square$

Доказ теореме 7. Према претходним разматрањима, тражени модел добијамо ако конструишемо максимално непротивречно проширење скупа Γ. То ћемо учинити тако што ћемо све исказне формуле поређати у низ и редом за сваку појединачно испитивати да ли се може додати жељеном максимално непротивречном проширењу.

Како је скуп исказних формула пребројив, све исказне формуле можемо поређати у низ: $\varphi_0, \varphi_1, \varphi_2, \ldots$ Формуле ћемо постепено додавати дефинишући низ Γ_n, $n \in \mathbb{N}$, на следећи начин:

$$\Gamma_0 = \Gamma$$
$$\Gamma_{n+1} = \begin{cases} \Gamma_n, & \text{ако } \Gamma_n, \varphi_n \vdash \bot, \\ \Gamma_n \cup \{\varphi_n\}, & \text{ако } \Gamma_n, \varphi_n \nvdash \bot. \end{cases}$$

Очигледно је $\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \Gamma_3 \subseteq \cdots$. Приметимо да је за свако $n \in \mathbb{N}$ скуп Γ_n непротивречан, тј. важи $\Gamma_n \nvdash \bot$. Ово једноставно доказујемо математичком индукцијом. Ако је $n = 0$, тврђење је тачно по претпоставци. Претпоставимо да је $\Gamma_n \nvdash \bot$. Да бисмо доказали да је $\Gamma_{n+1} \nvdash \bot$, разликујемо два случаја.
1. случај: $\Gamma_n, \varphi_n \vdash \bot$. Тада је $\Gamma_{n+1} = \Gamma_n$, па је тврђење тачно по индуктивној претпоставци.
2. случај: $\Gamma_n, \varphi_n \nvdash \bot$. Тада је $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$, па је и у овом случају $\Gamma_{n+1} \nvdash \bot$.

Нека је $\Gamma^* = \bigcup_{k \in \mathbb{N}} \Gamma_k$. Докажимо да је и Γ^* непротивречан скуп. Претпоставимо супротно да $\Gamma^* \vdash \bot$. Тада постоји коначан подскуп $\Gamma' \subseteq \Gamma^*$, такав да $\Gamma' \vdash \bot$. Пошто је Γ' коначан и $\Gamma' \subseteq \Gamma^* = \bigcup_{k \in \mathbb{N}} \Gamma_k$, постоји природан број n такав да је $\Gamma' \subseteq \bigcup_{k \leqslant n} \Gamma_k = \Gamma_n$. Међутим, тада $\Gamma_n \vdash \bot$ што није могуће.

Скуп Γ^* је и *дедуктивно затворен*, тј. за сваку формулу φ важи: $\Gamma^* \vdash \varphi$ акко $\varphi \in \Gamma^*$. Заиста, нека је φ произвољна формула и $\Gamma^* \vdash \varphi$. Тада је $\varphi = \varphi_k$, за неки природан број k. Ако $\varphi \notin \Gamma^*$, онда $\Gamma_k, \varphi_k \vdash \bot$, одакле према правилу $(\neg_{\mathrm{U}})$ следи $\Gamma_k \vdash \neg\varphi_k$, па тиме и $\Gamma^* \vdash \neg\varphi_k$. Како је $\Gamma^* \vdash \varphi_k$, према правилу $(\neg_{\mathrm{E}})$ добијамо $\Gamma^* \vdash \bot$, што је супротно доказаној непротивречности скупа Γ^*. Обрнуто је тривијално тачно.

Остаје још да покажемо да је Γ^* максимално непротивречан. Ако је $\Gamma^* \subsetneq \Delta$, доказаћемо да је Δ противречан скуп. Нека је $\varphi \in \Delta \setminus \Gamma^*$. Тада постоји $n \in \mathbb{N}$ такав да је $\varphi = \varphi_n$, и при томе $\Gamma_n, \varphi_n \vdash \bot$, јер $\varphi \notin \Gamma^*$. Одавде следи, применом правила $(\neg_{\mathrm{U}})$, да $\Gamma_n \vdash \neg\varphi$, па тиме и $\Delta \vdash \neg\varphi$, јер је $\Gamma_n \subseteq \Gamma^* \subseteq \Delta$. Пошто $\varphi \in \Delta$ имамо да $\Delta \vdash \varphi$, а одавде добијамо

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

Дакле, Γ^* је максимално непротивречан скуп.

Према претходној леми постоји валуација v таква да је $\chi_{\Gamma^*} = \widehat{v}$. Како је $\Gamma \subseteq \Gamma^*$, имамо да је $\chi_\Gamma(\alpha) \leqslant \chi_{\Gamma^*}(\alpha) = \widehat{v}(\alpha)$, за сваку формулу α. Дакле, $v \models \Gamma$. $\square$

Теорема јаке потпуности

Директан доказ теореме јаке потпуности изводимо користећи идеје из другог доказа теореме компактности (страна 61).

Теорема 8. [***Теорема јаке потпуности***] *Ако је* $\Gamma \models \alpha$, *онда је* $\Gamma \vdash \alpha$.

Доказ. Доказаћемо да из $\Gamma \nvdash \alpha$, следи да $\Gamma \not\models \alpha$.

Претпоставимо да је $\Gamma \nvdash \alpha$. Тада је и $\Gamma \nvdash \bot$ (јер из $\Gamma \vdash \bot$, према правилу $(\bot_{\mathrm{i}})$ следи и $\Gamma \vdash \alpha$). На скупу свих формула For дефинишимо релацију $\sim_\Gamma$:

$$\alpha \sim_\Gamma \beta \text{ акко } \Gamma \vdash \alpha \Leftrightarrow \beta.$$

Није тешко доказати да је $\sim_\Gamma$ реалција еквиваленције (задатак 35). Означимо са $|\alpha| = \{\varphi \in \mathrm{For} \mid \alpha \sim_\Gamma\}$ класу еквиваленције одређену формулом α. На скупу $B_P(\Gamma)$, дефинишимо две бинарне операције $\curlyvee$ и $\curlywedge$, и једну унарну $'$:

$$|\alpha| \curlyvee |\beta| = |\alpha \vee \beta|,\ |\alpha| \curlywedge |\beta| = |\alpha \wedge \beta|,\ |\alpha|' = |\neg\alpha|.$$

Операције су добро дефинисане (задатак 36) и $\mathbf{B}_P(\Gamma) = (B_P, \curlyvee, \curlywedge, ', |\bot|, |\top|)$ је Булова алгебра (задатак 32). Приметимо да је $|\neg\alpha| \neq |\bot|$. Заиста, ако би било $|\neg\alpha| = |\bot|$, тј. $\Gamma \vdash \neg\alpha \Leftrightarrow \bot$, имали бисмо $\Gamma \vdash \neg\alpha \Rightarrow \bot$ и $\Gamma \vdash \bot \Rightarrow \neg\alpha$, према правилима $(\wedge^{\mathrm{l}}_{\mathrm{E}})$ и $(\wedge^{\mathrm{d}}_{\mathrm{E}})$. Како је $\Gamma \vdash (\neg\alpha \Rightarrow \bot) \Rightarrow \alpha$ (доказати), применом правила $(\Rightarrow_{\mathrm{E}})$ закључујемо да је $\Gamma \vdash \alpha$, што је супротно полазној претпоставци. Дакле, $|\neg\alpha| \neq |\bot|$, па према теореми о ултрафилтеру (страна 30) постоји ултрафилтер U у $\mathbf{B}_P(\Gamma)$ који садржи $|\neg\alpha|$. Дефинишимо валуацију $v : P \to \{0, 1\}$ на следећи начин:

$$v_U(p) = \begin{cases} 1, & |p| \in U, \\ 0, & |p| \notin U. \end{cases}$$

Као у доказу II теореме компактности (страна 61), доказује се да за сваку формулу α важи:

$$\widehat{v_U}(\alpha) = 1 \text{ акко } |\alpha| \in U.$$

За свако $\gamma \in \Gamma$, важи $|\gamma| = |\top|$, тј. $\Gamma \vdash \gamma \Leftrightarrow \neg\bot$.

1. $\Gamma, \gamma, \bot \vdash \bot$ (ax)
2. $\Gamma, \gamma \vdash \neg\bot$ из 1 према $(\bot_{\mathrm{c}})$
3. $\Gamma \vdash \gamma \Rightarrow \neg\bot$ из 2 према $(\Rightarrow_{\mathrm{U}})$

4. $\Gamma \vdash \gamma$ — (ax), јер $\gamma \in \Gamma$
5. $\Gamma, \neg\bot \vdash \gamma$ — из 4 према (slab)
6. $\Gamma \vdash \neg\bot \Rightarrow \gamma$ — из 5 према $(\Rightarrow_{\mathrm{U}})$
7. $\Gamma \vdash (\gamma \Rightarrow \neg\bot) \wedge (\neg\bot \Rightarrow \gamma)$ — из 3, 6 према $(\wedge_{\mathrm{U}})$

Дакле, за свако $\gamma \in \Gamma$, $|\gamma| = |\top| \in B_P(\Gamma)$, па $v \models \Gamma$. Такође, из $|\neg\alpha| \in U$ следи да $v \not\models \alpha$, одакле закључујемо да $\Gamma \not\models \alpha$. $\square$

Задаци

1. Одредити сложеност и скуп потформула формуле:
(а) $\neg(\neg p_1 \Rightarrow p_2)$;
(б) $\neg(\neg p_1 \Rightarrow p_2) \vee p_1$;
(в) $(\neg(\neg p_0 \Leftrightarrow \neg(p_1 \Rightarrow \bot))) \Rightarrow p_1$.

2. Доказати да је својство „бити потформула“ транзитивно: ако $\alpha \in \mathrm{Pot}(\beta)$ и $\beta \in \mathrm{Pot}(\gamma)$, онда $\alpha \in \mathrm{Pot}(\gamma)$.

3. Доказати да је $|\mathrm{Pot}(\alpha)| \leqslant 2^{\mathrm{sl}(\alpha)} - 1$, за било коју формулу α.

4. Одредити $(p \Rightarrow q)[p/q]$, $(p \Rightarrow q)[p/q][q/p]$ и $(p \Rightarrow q)[q/p][p/q]$, ако су p и q нека исказна слова.

5. Наћи, уколико постоје, бар један модел у коме важи формула

$$(p \Rightarrow q) \wedge (p_1 \Rightarrow q_1) \Rightarrow ((p \Rightarrow p_1) \Rightarrow (q \Rightarrow q_1))$$

и бар један модел у коме ова формула не важи.

6. Испитати да ли су следеће формуле задовољиве:
(а) $((p_1 \Rightarrow p_2) \Rightarrow \neg(p_2 \Rightarrow p_1)) \Leftrightarrow (p_1 \Leftrightarrow p_2)$; (б) $((p_1 \Rightarrow p_2) \Rightarrow p_2) \Rightarrow p_2$;
(в) $p_1 \Leftrightarrow (p_2 \Leftrightarrow (p_1 \Leftrightarrow (p_2 \Leftrightarrow p_1)))$; (г) $p_1 \vee \neg p_2 \Rightarrow \neg p_1 \vee p_2$;
(д) $(p_1 \vee \neg p_2) \wedge (\neg p_1 \vee p_3) \wedge (p_2 \vee \neg p_3)$;
(ђ) $((p_1 \Rightarrow p_2) \Rightarrow p_1) \Leftrightarrow (p_2 \Rightarrow (p_2 \Rightarrow p_1))$;
(е) $((p_1 \Rightarrow p_2 \vee p_3) \Rightarrow (\neg p_2 \Rightarrow \neg p_3)) \Rightarrow \neg p_2$.

7. Одредити формулу $\alpha(p_1, p_2, p_3)$ тако да за сваку валуацију v, $\widehat{v}(\alpha) = 1$ акко при валуацији v тачно два од слова p_1, p_2, p_3 добијају вредност 1.

8. Одредити формулу $\alpha(p_1, p_2, p_3)$ тако да је њена истинитосна вредност при било којој валуацији једнака вредности коју при тој валуацији добија већина (мањина) слова p_1, p_2, p_3.

9. Посматрајмо скуп $P_{15} = \{p_0, p_1, \ldots, p_{14}\}$ који садржи петнаест исказних слова чији су индекси схваћени као елементи домена групе $(\mathbb{Z}_{15}, +_{15})$. Наћи валуацију v, ако постоји, која задовољава следећи скуп формула

$$\{p_0\} \cup \{p_i \Rightarrow p_{-i} \mid i \in \mathbb{Z}_{15}\} \cup \{p_i \wedge p_j \Rightarrow p_{i+_{15}j} \mid i, j \in \mathbb{Z}_{15}\}.$$

Напомена. $-i$ је супротан елементу i у посматраној групи.

10. Ако $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow, \Leftarrow, \veebar\}$, испитати да ли је $p_1 * (p_2 * p_1)$ задовољива формула, и ако јесте да ли је таутологија.

11. Ако $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow, \Leftarrow, \veebar\}$, испитати да ли је $(p_2 * p_1) * \neg(p_1 * p_2)$ задовољива формула, и ако јесте да ли је таутологија.

12. Доказати да је формула $((p_1 \Rightarrow p_2) \Rightarrow p_3) \Rightarrow ((p_3 \Rightarrow p_1) \Rightarrow (p_4 \Rightarrow p_1))$ таутологија.

13. Знак „?“ заменити формулом најмање могуће сложености тако да добијене формуле буду таутологије.

$p \wedge \bot \Leftrightarrow ?$ $\quad$ $p \wedge \top \Leftrightarrow ?$ $\quad$ $p \vee \bot \Leftrightarrow ?$ $\quad$ $p \vee \top \Leftrightarrow ?$

$(p \Rightarrow \bot) \Leftrightarrow ?$ $\quad$ $(p \Rightarrow \top) \Leftrightarrow ?$ $\quad$ $(\bot \Rightarrow p) \Leftrightarrow ?$ $\quad$ $(\top \Rightarrow p) \Leftrightarrow ?$

$(p \Leftrightarrow \bot) \Leftrightarrow ?$ $\quad$ $(p \Leftrightarrow \top) \Leftrightarrow ?$

14. Испитати да ли су следеће формуле таутологије:
(а) $(p \Rightarrow \neg p) \Leftrightarrow \neg p$;
(б) $p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$;
(в) $p \Rightarrow ((q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)))$;
(г) $(p \wedge q \Rightarrow r) \Rightarrow ((p \vee r \Rightarrow p) \Rightarrow (q \Rightarrow p))$;
(д) $((p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s) \wedge \neg(r \vee s)) \Rightarrow ((r \Rightarrow p) \wedge (s \Rightarrow q))$.

15. Доказати да за све формуле $\alpha, \beta, \gamma, \delta$ важи:
(а) ако је $\models \alpha \vee \beta$ и $\models \neg\alpha \vee \gamma$, онда је $\models \beta \vee \gamma$;
(б) ако је $\models \alpha \vee \beta$, $\models \alpha \Rightarrow \gamma$ и $\models \beta \Rightarrow \delta$, онда је $\models \gamma \vee \delta$;
(б) ако је $\models \neg\alpha \vee \beta$ и $\models \neg\beta \vee \neg\gamma$, онда је $\models \alpha \Rightarrow \neg\gamma$.

16. Нека су α и β исказне формуле које немају ниједно заједничко исказно слово ($P(\alpha) \cap P(\beta) = \emptyset$). Доказати да су следећи услови еквивалентни:
(а) $\alpha \Rightarrow \beta$ је таутологија;
(б) бар једна од формула $\neg\alpha$ или β је таутологија.

17. Када сабирамо два броја у бинарном систему која имају највише две цифре, рецимо ab и cd, добијамо резултат са највише три цифре, pqr. На пример, $11 + 01 = 100$. Користећи стандардне логичке везнике, изразити p, q, r у функцији a, b, c, d.

18. Нека је $P = \{p_1, \dots, p_n\}$ коначан скуп исказних слова. На скупу свих валуација 2^P дефинисана је бинарна релација $\ll$ на следећи начин:

$$u \ll v \text{ акко за свако } p \in P,\ u(p) \leqslant v(p).$$

(а) Доказати да је $\ll$ релација поретка на 2^P. Да ли је овај поредак линеаран?

(б) Формула α је *растућа* ако за све $u, v \in 2^P$, из $u \ll v$, следи $\widehat{u}(\alpha) \leqslant \widehat{v}(\alpha)$. Ако формула α није растућа, да ли њена негација $\neg\alpha$ мора бити растућа?

(в) Доказати да је α растућа формула акко је α таутологија или је $\neg\alpha$ таутологија или постоји формула θ која не садржи ниједан од везника $\neg$, $\Rightarrow$ и $\Leftrightarrow$ и која је еквивалента са α.

19. Ако је $\alpha \equiv \beta$, доказати да је тада и $\alpha(p/\theta) \equiv \beta(p/\theta)$, за било које слово p и било коју формулу θ.

20. Одредити формулу у дисјунктивној (конјунктивној) нормалној форми која је семантички еквивалентна формули:

(1) $((p_1 \Rightarrow p_2) \Rightarrow (p_3 \Rightarrow \neg p_1)) \Rightarrow (\neg p_2 \Rightarrow \neg p_3)$;

(2) $\neg(p_1 \wedge (p_2 \vee p_3)) \Rightarrow ((p_1 \wedge p_2) \vee p_3)$.

21. Сеф има n брава и може бити отворен само ако су откључане све браве. Пет особа a, b, c, d и e добило је кључеве неких брава. Могуће је да више особа добије кључеве за исту браву. Наћи најмањи број n и одговарајућу расподелу кључева међу поменутим особама тако да сеф може бити отворен само у случају да су присутне особе a и b, или особе a, b и d, или особе b, d и e.

22. Одредити формулу $\alpha(p_1, p_2)$ тако да буде:

(а) $(\alpha \wedge p_2 \Rightarrow \neg p_1) \Rightarrow ((p_1 \Rightarrow \neg p_2) \Rightarrow \alpha)$;

(б) $((p_3 \Rightarrow (\neg p_2 \Rightarrow p_1)) \Rightarrow \alpha) \Rightarrow (\alpha \wedge (p_1 \Rightarrow p_2) \wedge p_3)$.

23. Одредити формулу $\alpha(p_1, p_2, p_3)$ тако да буде:

(а) $p_1 \wedge \alpha \equiv p_1 \wedge p_2$ и $p_1 \vee \alpha \equiv p_1 \vee p_3$;

(б) $p_3 \Rightarrow \alpha \equiv p_3 \Rightarrow (p_1 \vee p_2)$ и $\alpha \Rightarrow p_3 \equiv \neg(p_1 \vee p_2) \Rightarrow p_3$;

(в) $p_1 \Rightarrow \alpha \equiv p_2 \Rightarrow (\neg p_1 \vee p_3)$ и $(p_3 \Rightarrow p_2) \Rightarrow p_1 \equiv \neg p_1 \Rightarrow \neg\alpha$.

24. Имајући у виду значење формуле $(\alpha \wedge \beta) \vee (\neg\alpha \wedge \gamma)$ можемо је записати и у облику if-формуле: $\mathrm{if}\,\alpha\,\mathrm{then}\,\beta\,\mathrm{else}\,\gamma$. Скуп if-формула дефинишемо као најмањи скуп такав да важи:

• исказна слова и логичке константе $\top$ и $\bot$ су if-формуле,

• ако су α, β и γ if-формуле, онда је if-формула и if ... then ... else ....

(а) Доказати да је свака исказна формуле еквивалентна некој if-формули.

(б) Доказати да су еквивалентне следеће формуле

$$\mathrm{if}\ (\mathrm{if}\ p\ \mathrm{then}\ q\ \mathrm{else}\ r)\ \mathrm{then}\ q_1\ \mathrm{else}\ r_1$$

и

$$\text{if } p \text{ then } (\text{if } q \text{ then } q_1 \text{ else } r_1) \text{ else } (\text{if } r \text{ then } q_1 \text{ else } r_1).$$

(в) Кажемо да је if-формула *проста* уколико је услов (формула која се налази између if и then) исказно слово. Доказати да је свака if-формула еквивалентна некој простој if-формули.

(г) Кажемо да је if-формула *нормална* ако је проста и ако су све њене if-потформуле облика if p then α else β, при чему је p исказно слово које се не појављује ни у α нити у β. Доказати да је свака if-формула еквивалентна некој нормалној if-формули.

25. Аристотел, који се сматра творцем логике, у једној од свој књига је написао „Није могуће извести тачан закључак из контрадикторних претпоставки“. Поједини логичари каснијег доба наведену реченицу су схватили на следећи начин

$$(*) \qquad \text{ако је } \alpha \models \beta \text{ и } \neg\alpha \models \beta, \text{ онда је } \models \neg\beta.$$

Доказати да, уколико $\models$ означава семнатичку последицу, тврдња $(*)$ није тачна.

26. Доказати да за све формуле $\alpha, \beta, \gamma, \delta$ важи:

(а) $\alpha \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow \gamma), \beta \Rightarrow \gamma, \alpha \models \gamma$;

(б) $\alpha \Rightarrow (\beta \vee \gamma), \beta \Rightarrow \neg\alpha \models \alpha \Rightarrow \gamma$.

27. Ако је Γ неки скуп формула, онда са $\mathrm{C}_{\models}(\Gamma)$ означавамо скуп свих формула које су семантичке последице од Γ. Доказати да за произвољне $\Gamma, \Delta \subseteq \mathrm{For}$ важи:

(а) $\Gamma \subseteq \mathrm{C}_{\models}(\Gamma)$;

(б) $\mathrm{C}_{\models}(\mathrm{C}_{\models}(\Gamma)) \subseteq \mathrm{C}_{\models}$;

(в) ако је $\Gamma \subseteq \Delta$, онда је $\mathrm{C}_{\models}(\Gamma) \subseteq \mathrm{C}_{\models}(\Delta)$;

(г) $\mathrm{C}_{\models}(\Gamma) \subseteq \bigcup_{\Sigma \in \mathcal{P}_{\mathrm{fin}}(\Gamma)} \mathrm{C}_{\models}(\Sigma)$, где је $\mathcal{P}_{\mathrm{fin}}(\Gamma)$ скуп свих коначних подскупова од Γ.

28. Скупови формула Γ_1 и Γ_2 су *еквивалентни* ако је $\mathrm{C}_{\models}(\Gamma_1) = \mathrm{C}_{\models}(\Gamma_2)$ (видети претходни задатак). Испитати да ли су еквивалентни следећи скупови формула:

(а) $\{p_1, p_2, p_3\}$ и $\{p_1, p_1 \Rightarrow p_2, (p_1 \Rightarrow p_2) \Rightarrow p_3\}$;

(б) $\{p_1, p_2, p_3\}$ и $\{p_1, p_1 \Rightarrow p_2, p_1 \Rightarrow (p_2 \Rightarrow p_3)\}$;

(в) $P = \{p_n \mid n \in \mathbb{N}\}$ и $Q = \{p_0\} \cup \{p_n \Rightarrow p_{n+1} \mid n \in \mathbb{N}\}$;

(г) $P = \{p_n \mid n \in \mathbb{N}\}$ и $R = \{p_0, p_1\} \cup \{p_n \wedge p_{n+1} \Rightarrow p_{n+2} \mid n \in \mathbb{N}\}$.

29. Скуп формула Γ, $\Gamma \subseteq \mathrm{For}$ је *независтан* ако за сваку формулу $\gamma \in \Gamma$ важи $\Gamma \setminus \{\gamma\} \not\models \gamma$.

(а) Испитати који су од следећих скупова (p, q, r су исказна слова) независни:

• $\{p \Rightarrow q, q \Rightarrow r, r \Rightarrow p\}$;
• $\{p \Rightarrow q, q \Rightarrow r, p \Rightarrow r\}$;
• $\{p \vee q, p \Rightarrow r, q \Rightarrow r, \neg p \Rightarrow q \vee r\}$
• $\{p, q, p \Rightarrow r, r \Rightarrow q\}$.

(б) Да ли је празан скуп независтан? Наћи потребан и довољан услов да скуп који садржи само једну формулу буде независтан.

(в) Доказати да сваки коначан скуп формула садржи бар један еквивалентан (видети претходни задатак) независтан подскуп.

(г) Доказати да је скуп формула независтан акко је независтан сваки његов коначан подскуп.

(д) Да ли бесконачан скуп

$$\{p_1, p_1 \wedge p_2, p_1 \wedge p_2 \wedge p_3, \ldots, p_1 \wedge p_2 \wedge \cdots \wedge p_n, \ldots\}$$

садржи еквивалентан независтан подскуп? Да ли постоји било какав независтан скуп формула еквивалентан овом скупу?

(ђ) Доказати да за сваки пребројив скуп формула постоји бар један независтан скуп који му је еквивалентан.

30. Ако је T скуп исказних формула такав да за сваку валуацију v постоји формула φ из T таква да $v \models \varphi$, онда постоји коначно много формула из T таквих да је дисјункција тих формула таутологија.

31. Доказати теорему компактности применом Кенигове леме.
Упутство. Погледати доказ I теореме компактности и пример 15.

32. Доказати:

($\mathbf{A}^{\vee}$) $\vdash \alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$;	($\mathbf{A}^{\wedge}$) $\vdash \alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge \gamma$;
($\mathbf{K}^{\vee}$) $\vdash \alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$;	($\mathbf{K}^{\wedge}$) $\vdash \alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$;
($\mathbf{D}^{\vee}_{\wedge}$) $\vdash \alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$;	($\mathbf{D}^{\wedge}_{\vee}$) $\vdash \alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$;
($\mathbf{C}^{\vee}$) $\vdash \alpha \vee \neg\alpha \Leftrightarrow \top$;	($\mathbf{C}^{\wedge}$) $\vdash \alpha \wedge \neg\alpha \Leftrightarrow \bot$;
($\mathbf{N}^{\vee}$) $\vdash \alpha \vee \bot \Leftrightarrow \alpha$;	($\mathbf{N}^{\wedge}$) $\vdash \alpha \wedge \top \Leftrightarrow \alpha$.

33. Доказати:

(а) $\alpha \Rightarrow \beta, \alpha \Rightarrow \gamma \vdash \alpha \Rightarrow (\beta \wedge \gamma)$;	(б) $\alpha \Rightarrow \beta, \alpha \wedge \beta \Rightarrow \gamma \vdash \alpha \Rightarrow \gamma$;
(в) $\alpha \Rightarrow (\beta \Rightarrow \gamma) \vdash \alpha \wedge \beta \Rightarrow \gamma$;	(г) $\alpha \Rightarrow (\beta \wedge \gamma) \vdash (\alpha \Rightarrow \beta) \wedge (\alpha \Rightarrow \beta)$;
(д) $\alpha, \alpha \Leftrightarrow \beta \vdash \beta$;	(ђ) $\alpha \wedge \beta \vdash \neg(\alpha \Rightarrow \neg\beta)$;
(е) $\neg(\alpha \Rightarrow \beta) \vdash \neg\beta$;	(ж) $\alpha \Rightarrow \beta \vdash \neg\beta \Rightarrow \neg\alpha$;
(з) $\neg\beta \Rightarrow \neg\alpha \vdash \alpha \Rightarrow \beta$;	(и) $\alpha \Rightarrow \beta \vdash \neg(\alpha \wedge \neg\beta)$;
(ј) $\alpha \Rightarrow \beta \vdash \neg\alpha \vee \beta$;	(к) $\alpha \vee \beta, \neg\alpha \vdash \beta$.

34. Доказати да се следећа *лева* правила извођења могу користити при доказивању.

$$\frac{\Gamma, \alpha, \beta \vdash \gamma}{\Gamma, \alpha, \alpha \Rightarrow \beta \vdash \gamma} \Rightarrow_{\mathrm{L}} \qquad \frac{\Gamma, \alpha, \beta \vdash \gamma}{\Gamma, \alpha \wedge \beta \vdash \gamma} \wedge_{\mathrm{L}} \qquad \frac{\Gamma, \alpha \vdash \gamma \quad \Gamma, \beta \vdash \gamma}{\Gamma, \alpha \vee \beta \vdash \gamma} \vee_{\mathrm{L}}$$

35. Доказати:

(а) $\Gamma \vdash \alpha \Leftrightarrow \alpha$;

(б) ако је $\Gamma \vdash \alpha \Leftrightarrow \beta$, онда је $\Gamma \vdash \beta \Leftrightarrow \alpha$;

(в) ако је $\Gamma \vdash \alpha \Leftrightarrow \beta$ и $\Gamma \vdash \beta \Leftrightarrow \gamma$, онда је $\Gamma \vdash \alpha \Leftrightarrow \gamma$.

36. Ако је $\Gamma \vdash \alpha \Leftrightarrow \alpha_1$ и $\Gamma \vdash \beta \Leftrightarrow \beta_1$, доказати да је:

(а) $\Gamma \vdash \neg\alpha \Leftrightarrow \neg\alpha_1$; (б) $\Gamma \vdash \alpha \wedge \alpha_1 \Leftrightarrow \beta \wedge \beta_1$; (в) $\Gamma \vdash \alpha \vee \alpha_1 \Leftrightarrow \beta \vee \beta_1$.

37. Правила извођења такозване *минималне* логике су сва правила класичне логике, **осим** правила $(\bot_c)$, које је избачено. Са $\Gamma \vdash_m \varphi$ означавамо чињеницу да се секвент $\Gamma \vdash \varphi$ може доказати применом само правила минималне логике.

(а) Доказати да се у минималној логици могу користити и следећа правила:

$$\frac{\Gamma, \alpha \Rightarrow \beta \vdash \alpha}{\Gamma, \alpha \Rightarrow \beta \vdash \beta} (\Rightarrow'_{\mathrm{E}}), \quad \frac{\Gamma, \neg\alpha \vdash \alpha}{\Gamma, \neg\alpha \vdash \bot} (\neg'_{\mathrm{E}}), \quad \frac{\Gamma, \alpha \vdash \neg\alpha}{\Gamma, \alpha \vdash \bot} (\neg''_{\mathrm{E}}).$$

(б) Доказати:

(1) $\vdash_m \alpha \Rightarrow \neg\neg\alpha$; (2) $\vdash_m \neg\neg\neg\alpha \Rightarrow \neg\alpha$;

(3) $\vdash_m \neg\neg(\alpha \wedge \beta) \Rightarrow (\neg\neg\alpha \wedge \neg\neg\beta)$; (4) $\vdash_m \neg\neg(\alpha \Rightarrow \beta) \Rightarrow (\neg\neg\alpha \Rightarrow \neg\neg\beta)$;

(5) $\vdash_m \neg(\alpha \vee \beta) \Leftrightarrow (\neg\alpha \wedge \neg\beta)$;

38. Правила извођења *интуиционистичке* логике су сва правила класичне логике, **осим** правила $(\bot_c)$, које је замењено правилом $(\bot_{\mathrm{i}})$,

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \alpha} (\bot_{\mathrm{i}}).$$

Са $\Gamma \vdash_i \varphi$ означавамо чињеницу да се секвент $\Gamma \vdash \varphi$ може доказати применом само правила интуиционистичке логике.

Доказати

(а) $\vdash_i (\neg\neg\alpha \Rightarrow \neg\neg\beta) \Rightarrow \neg\neg(\alpha \Rightarrow \beta)$;

(б) $\vdash_i \neg\neg((\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta))$;

(в) $\vdash_i \neg\neg(((\alpha \Rightarrow \beta) \Rightarrow \alpha) \Rightarrow \alpha)$;

(г) $\vdash_i \neg\neg((\alpha \wedge \beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma) \vee (\beta \Rightarrow \gamma))$;

(д) $\vdash_i \neg\neg((\alpha \Rightarrow \beta \vee \gamma) \Rightarrow (\alpha \Rightarrow \beta) \vee (\alpha \Rightarrow \gamma))$;

(ђ) $\vdash_i \neg\neg((\alpha \Rightarrow \beta) \vee (\beta \Rightarrow \alpha))$.

Логика првог реда

Синтакса и семантика логике првог реда

Неформално говорећи, исказна логика се бави структуром реченица узимајући у обзир само начин на који су неки једноставни искази повезани логичким везницима, док је значење тих полазних исказа потпуно неважно. Логика првог реда нам омогућава да разматрамо и смисао полазних исказа. Пре него што детаљно опишемо поменуту логику, наводимо два примера у којима ћемо покушати да објаснимо неке полазне идеје у развоју логике првог реда.

ПРИМЕР 1. Природни језици нису погодни за прецизно изражавање смисла исказа. Да ли реченица *Сваки момак воли једну девојку* значи да (1) *Постоји једна девојка коју воли сваки момак* или да (2) *За сваког момка се може пронаћи једна девојка коју он воли*?

Потреба да се елиминишу двосмислености природног језика довела је, између осталог, до увођења **формалних језика**[33]. Сваки формални језик уводимо према унапред утврђеним правилима. Најпре бирамо алфабет, тј. скуп неких симбола који је погодан за изражавање одређених својстава, а затим, на стандардизован начин градимо реченице као коначне низове изабраних симбола које изражавају жељена својства. Као и у природним језицима, неће сваки низ изабраних симбола бити нека реченица.

Алфабет логике првог реда поред логичких везника ($\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$) садржи и квантификаторе $\forall$ – *сваки* и $\exists$ – *неки*, променљиве $x, y, z, x_1, y_1, z_1, x_2, \ldots$ и помоћне знаке: зарез и заграде.

Да бисмо могли формално да запишемо реченице са почетка примера, потребно је да неким симболима означимо и особине *бити момак* и *бити девојка*, као и однос *волети*. Наведене особине можемо схватити као две унарне релације на скупу људи: нека је M скуп свих момака и D скуп свих девојака. Изјаву „*x је момак*" записаћемо краће $M(x)$, а изјаву „*x је девојка*" записаћемо краће $D(x)$. Однос *волети* схватамо као бинарну релацију међу људима. Ако ову релацију означимо са V, онда $V(x, y)$ значи „*x воли y*".

[33]Данас најпознатији примери формалних језика су свакако програмски језици.

Реченицама (1) и (2) редом одговарају следеће реченице нашег формалног језика:

$$\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y,x))) \text{ и } \forall x(M(x) \Rightarrow \exists y(D(y) \wedge V(x,y))),$$

Веома је корисно полазним симболима прикључити и знак једнакости $=$. Наводимо један пример реченице са овим знаком

(3) $$\exists x(M(x) \wedge \exists y \exists z(D(y) \wedge D(z) \wedge y \neq z \wedge V(x,y) \wedge V(x,z))),$$

при чему је $y \neq z$ скраћење за $\neg\, y = z$. Није тешко превести ову реченицу на српски: *постоји момак који воли две различите девојке.* Препуштамо читаоцима да преведу на српски и следеће две реченице:
(4) $\exists x(D(x) \wedge \forall y(M(y) \Rightarrow \neg V(x,y)))$ и
(5) $\exists x(M(x) \wedge \exists y(D(y) \wedge V(x,y) \wedge \forall z(D(z) \wedge V(x,z) \Rightarrow y = z)))$.

Наравно, важно је правилно преводити и са српског на формални језик, па за вежбу дајемо две реченице на српском:

- *сваког момка воли бар једна девојка и бар једна девојка га не воли*,
- *свака девојка воли сваког момка који њу воли.*

Снага уведеног формалног језика лежи у томе што наведене реченице (1)–(5) можемо посматрати у потпуно другачијим контекстима. Навешћемо три математичка контекста.

Контекст 1. Ако говоримо о простим и сложеним природним бројевима, и релацији дељивости међу природним бројевима, можемо користити потпуно исти алфабет с тим што овога пута имамо на уму сасвим другачије значење симбола M, D и V: $M(x)$ нека значи „*x је прост број*", $D(x)$ значи „*x је сложен број*" и $V(x,y)$ значи „*x дели y*". У овом контексту реченица (1) $\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y,x)))$ значи *постоји сложен број који је дељив сваким простим бројем.* Реченица (2) $\forall x(M(x) \Rightarrow \exists y(D(y) \wedge V(x,y)))$ значи *за сваки прост број постоји сложен број који је дељив тим простим бројем.* Када смо говорили о момцима и девојкама, истинитост реченица (1) и (2) је била дискутабилна, али у овом другом контексту реченица (1) није тачна, док реченица (2) јесте. Нас ће занимати искључиво контексти налик овом другом. Препуштамо читаоцима да интерпретирају реченице (3)–(5) у овом новом контексту, и испитају њихову истинитост.

Контекст 2. Наводимо још један контекст потпуно другачији од претходна два. Нека $M(x)$ значи „*x је тачка*", $D(x)$ значи „*x је права*" и $V(x,y)$ да „*x припада y*". Погледајмо сада како се, на пример, може записати позната аксиома планиметрије: *за сваке две различите тачке x и y постоји права z која их садржи*:

(6) $$\forall x \forall y\,(M(x) \wedge M(y) \wedge x \neq y \;\Rightarrow\; \exists z\,(D(z) \wedge V(x,z) \wedge V(y,z)).$$

Није тешко формално записати и остале аксиоме припадања. Наравно можемо формализовати и неке додатне захтеве:

(7) Сваки објекат је тачка или права – $\forall x\,(M(x) \vee D(x))$;

(8) Ниједан објекат није и тачка и права – $\neg\exists x\,(M(x) \wedge D(x))$.

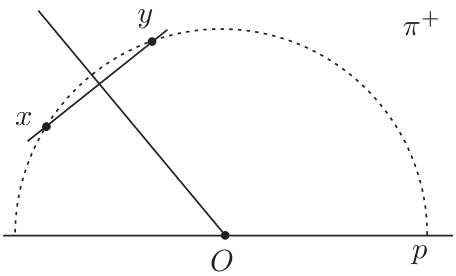
Ако са $u \parallel y$ краће означимо изјаву $\neg\exists w(M(w) \wedge V(w,u) \wedge V(w,y))$ (тј. тврдњу да u и v немају заједничких тачака), и слично за $v \parallel y$, размотримо следећу реченицу:

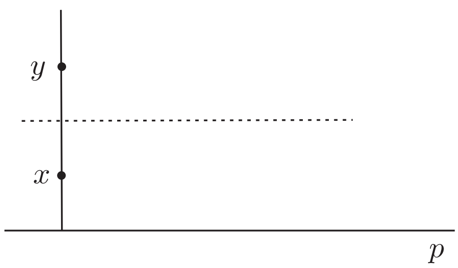
$$(9) \quad \forall x \forall y\, (M(x) \wedge D(y) \wedge \neg V(x,y) \Rightarrow \\ \Rightarrow \exists u \exists v\, (u \neq v \wedge D(u) \wedge D(v) \wedge u \parallel y \wedge v \parallel y)).$$

Ова реченица тврди да *за сваку тачку и сваку праву која не садржи уочену тачку, постоје две различите праве које садрже ту тачку и немају заједничких тачака са уоченом правом.* Скоро свако ће, имајући на уму уобичајено (еуклидско) схватање појмова тачка и права, одмах рећи да реченица (9) није тачна. Наравно, у неком другом контексту ова реченица може бити тачна. Посебно је занимљиво то што се полазни симболи могу инерпретирати тако да (9) буде тачно заједно са свим аксиомама еуклидске геометрије, осим наравно аксиоме паралелности.

Контекст 3. Заборавимо на тренутак на значење које смо дали симболима M, D и V у претходном контексту, само зато да бисмо им дали ново значење.

Замислимо праву p која лежи у еуклидској равни π и уочимо једну од отворених полуравни које она одређује π^+. Нека сада $M(x)$ значи „*тачка x припада π^+*“, а $D(x)$ значи „*x је полукруг у π^+ са центром на p или је полуправа нормална на p и са почетком на p која лежи у π^+*“. Такође, нека $V(x,y)$ значи „*x припада y*“. Размотримо сада шта нам тврди реченица (6): *за све тачке x и y из π^+ постоји полукруг са центром на p који пролази кроз тачке x и y или постоји полуправа нормална на p која садржи тачке x и y.*





Да бисмо се уверили да је ова реченица тачна, довољно је конструисати симетралу дужи $\overline{xy}$ и наћи њен пресек O са p. Очигледно ће круг $k(O, \overline{OX})$ имати тражено својство. У случају да је дуж $\overline{xy}$ нормална на p можемо сматрати да је центар „у бесконачности“ и да се круг „дегенерише“ у нормалу.

Препуштамо читаоцима да се увере да је тачна и реченица (9).

Било који контекст. Приметимо да можемо формулисати (у нашем формалном језику) доста реченица које ће бити тачне у било ком контексту. Наводимо неколико примера таквих реченица:

- $\exists x M(x) \vee \neg\exists x M(x)$,
- $\forall x\, (D(x) \vee \neg D(x))$,
- $\exists x \forall y\, V(x,y) \Rightarrow \forall y \exists x\, V(x,y)$,
- $\neg\exists x D(x) \Rightarrow \forall x\, \neg D(x)$, итд.

У наставку ће нам посебно бити важне управо овакве реченице, тзв. **ваљане формуле**. $\triangleright$

Пример 2. Скуп заједно са неким операцијама које су на њему дефинисане и неким изабраним константама, представља веома важну врсту структура. Свака Булова алгебра, рецимо $\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$, представља један пример овакве структуре. Таква је и структура $\mathbf{Z} = (\mathbb{Z}, +, \cdot, -, 0, 1)$, при чему је $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ скуп целих бројева, $+$ и $\cdot$ сабирање и множење целих бројева, а $-$ унарна операција *супротан елемент*. Иако су две наведене структуре истог типа, тј. чине их две бинарне операције, једна унарна и две константе, оне имају сасвим различита својства.

Да бисмо изразили својства ових структура користићемо алфабет сличан оном из претходног примера заједно са знаком једнакости, осим што ћемо уместо M, D и V користити симболе за наведене операције и константе. Нека су F и G бинарни операцијски симболи, U унарни операцијски симбол, а c и e два симбола константи. Ове симболе различито интерпретирамо у наведеним структурама, као што је то приказано у наредној табели.

	$F(x,y)$ значи	$G(x,y)$ значи	$U(x)$ значи	c значи	e значи
у $\mathbf{2}$	$x \vee y$	$x \wedge y$	$\neg x$	0	1
у $\mathbf{Z}$	$x + y$	$x \cdot y$	$-x$	0	1

Посматрајмо сада формулу $\forall x \forall y\, (F(x,y) = F(y,x))$. Ова формула интерпретирана у структури $\mathbf{2}$ тврди да за све $x, y \in \{0,1\}$ важи $x \vee y = y \vee x$. Иста формула интерпретирана у $\mathbf{Z}$ тврди да за све $x, y \in \mathbb{Z}$ важи $x + y = y + x$. Наравно, у обе структуре дата формула је тачна, јер су одговарајуће операције комутативне.

Наводимо и једну формулу која је тачна у $\mathbf{2}$, али није тачна у $\mathbf{Z}$. Једна таква формула је $\forall x\, (G(x, U(x)) = c)$. Она је тачна у $\mathbf{2}$ јер је $x \wedge \neg x = 0$, за свако $x \in \{0,1\}$. Насупрот томе, није тачно да за свако $x \in \mathbb{Z}$ важи $x \cdot (-x) = 0$ (заправо једнакост неће важити за сваки $x \in \mathbb{Z} \setminus \{0\}$).

Препуштамо читаоцима да пронађу пример формуле која је тачна у $\mathbf{Z}$, а није тачна у $\mathbf{2}$, као и пример формуле која није тачна ни у једној од наведених структура. $\triangleright$

У претходним примерима наговештено је какве математичке структуре настоји да опише логика првог реда и на који начин.

Какве математичке структуре описује логика првог реда?

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 $R \subseteq M^n$.[34] 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

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

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

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 $\mathrm{ar} : \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L} \to \mathbb{N}$ која сваком знаку $S \in \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L}$ придружује неки природан број $\mathrm{ar}(S)$, тзв. *дужину* („*арност*“) знака S.

Како се у логици првог реда описују операцијско-релацијске структуре?

За врсту структура које желимо да описујемо опредељујемо се избором одговарајућег језика $\mathcal{L} = \mathrm{Rel}_\mathcal{L} \cup \mathrm{Fun}_\mathcal{L} \cup \mathrm{Const}_\mathcal{L}$. Симболе језика називамо и *нелогичким симболима*. Поред ових симбола, у логици првог реда користе се и следећи *логички симболи*:

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

Логички и нелогички симболи представљају алфабет на коме састављамо описе изабране врсте структура. У овим описима централну улогу имају *изрази* (*терми*) и *формуле*.

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

Дефиниција 1. *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* $t_1, \ldots, t_{\mathrm{ar}(F)} \in \mathrm{Term}_{\mathcal{L}}$, *онда* $F(t_1, \ldots, t_{\mathrm{ar}(F)}) \in \mathrm{Term}_{\mathcal{L}}$

Дефиниција 2. *Скуп **атомичних (елементарних) формула** језика $\mathcal{L}$, у ознаци $\mathrm{At}_{\mathcal{L}}$, јесте скуп који поред $\perp$ и $\top$ садржи још само*

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

Дефиниција 3. *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* $\exists x\alpha \in \mathrm{For}_{\mathcal{L}}$.

Приметимо да су дефиниције израза и формула индуктивне, и да су скупови израза и формула различити за различите изборе садржаја језика $\mathcal{L}$. Сложеност израза и формула уводи се потпуно аналогно као у случају исказних формула (видети страну 39), али се овога пута нећемо тиме бавити већ ћемо се ослањати само на интуитивно поимање сложености израза и формула.

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.

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 аналогно функцији којом смо исказним формулама дељивали скуп исказних слова која се у њој појављују (видети страну 40), па зато строгу дефиницију функције V изостављамо.

Мало више пажње посветићемо појављивањима променљивих у формулама. 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.

Пример 3. Нека је $\mathrm{Rel}_{\mathcal{L}} = \{\leqslant\}$, $\mathrm{ar}(\leqslant) = 2$, $\mathrm{Fun}_{\mathcal{L}} = \{+, \cdot\}$, $\mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$. На наредној слици у датој формули повезане су променљиве на које делују одговарајући квантификатори, док стрелице показују слободна појављивања променљивих.

$$\exists y\big(\forall x(x + y = x + z) \vee \forall y(y \cdot y = z) \Rightarrow \neg y \leqslant x \vee y + x = 0\big) \wedge \neg z \leqslant y$$

$\triangleright$

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:

- $\mathrm{Fr}(\bot) = \mathrm{Fr}(\top) = \emptyset$;
- $\mathrm{Fr}(u = v) = V(u) \cup V(v)$, $u, v \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(R(t_1, \ldots, t_{\mathrm{ar}(R)})) = V(t_1) \cup \cdots \cup V(t_{\mathrm{ar}(R)})$,
  $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \ldots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(\neg\alpha) = \mathrm{Fr}(\alpha)$;
- $\mathrm{Fr}(\alpha * \beta) = \mathrm{Fr}(\alpha) \cup \mathrm{Fr}(\beta)$, $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$;
- $\mathrm{Fr}(\forall x\alpha) = \mathrm{Fr}(\exists x\alpha) = \mathrm{Fr}(\alpha) \setminus \{x\}$, $x \in \mathrm{Var}$.

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

Дефиниција 4. *Формула σ је* ***реченица*** *језика $\mathcal{L}$ ако нема слободних променљивих, 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

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

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 $\mathrm{ar}(R)$-арну релацију скупа M, тј. $\mathcal{I}_M(R) \subseteq M^{\mathrm{ar}(R)}$, сваком $F \in \mathrm{Fun}_{\mathcal{L}}$ придружује једну $\mathrm{ar}(F)$-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 $S^{\mathbf{M}}$.

Пример 4. 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[35], 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 $1^{\mathbf{X}} = b$). $\triangleright$

[35] 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.

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

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

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

- $\bot^{\mathbf{M}}[\mu] = 0$, $\top^{\mathbf{M}}[\mu] = 1$;
- $(u = v)^{\mathbf{M}}[\mu] = 1$ акко $u^{\mathbf{M}}[\mu] = v^{\mathbf{M}}[\mu]$, $u, v \in \mathrm{Term}_{\mathcal{L}}$;
- $\big(R(t_1, \dots, t_{\mathrm{ar}(R)})\big)^{\mathbf{M}}[\mu] = 1$ акко $R^{\mathbf{M}}(t_1^{\mathbf{M}}[\mu], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[\mu])$, тј.[36]
  $(t_1^{\mathbf{M}}[\mu], \dots, t_{\mathrm{ar}(R)}^{\mathbf{M}}[\mu]) \in R^{\mathbf{M}}$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \dots, t_{\mathrm{ar}(R)} \in \mathrm{Term}_{\mathcal{L}}$;
- $(\neg\alpha)^{\mathbf{M}}[\mu] = \neg\, \alpha^{\mathbf{M}}[\mu]$;
- $(\alpha * \beta)^{\mathbf{M}}[\mu] = \alpha^{\mathbf{M}}[\mu] * \beta^{\mathbf{M}}[\mu]$, $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$;
- $(\forall x\alpha)^{\mathbf{M}}[\mu] = \min\{\alpha^{\mathbf{M}}[\mu(x/a)] \mid a \in M\}$;
- $(\exists x\alpha)^{\mathbf{M}}[\mu] = \max\{\alpha^{\mathbf{M}}[\mu(x/a)] \mid a \in M\}$;

где је $\mu(x/a)$ валуација која промењивама додељује исте вредности као и валуација μ, осим промењивој x којој додељује вредност a, или прецизније $\mu(x/a) : \mathrm{Var} \to M$ и $\mu(x/a)(v) = \begin{cases} \mu(v), & v \neq x, \\ a, & v = x. \end{cases}$

На вредност израза у неком моделу утичу само вредности промењивих које се појављују у том изразу. Слично томе, на истинитосну вредност формуле у неком моделу утичу само вредности слободних промењивих те формуле.

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

Лема 1. *Нека је* $\mathbf{M}$ *произвољан модел језика* $\mathcal{L}$ *и* $\mu_1, \mu_2 : \mathrm{Var} \to M$ *две валуације.*

- *За сваки израз* $t \in \mathrm{Term}_{\mathcal{L}}$*, ако је* $\mu_1(v) = \mu_2(v)$*, за све* $v \in V(t)$*, онда је* $t^{\mathbf{M}}[\mu_1] = t^{\mathbf{M}}[\mu_2]$.

- *За сваку формулу* $\alpha \in \mathrm{For}_{\mathcal{L}}$*, ако је* $\mu_1(v) = \mu_2(v)$*, за све* $v \in \mathrm{Fr}(\alpha)$*, онда је* $\alpha^{\mathbf{M}}[\mu_1] = \alpha^{\mathbf{M}}[\mu_2]$.

Доказ претходне леме (индукцијом по сложености израза t, односно формуле α) препуштамо читаоцима, уз напомену да је аналоган доказу одговарајуће леме наведене на страни 43.

Из претходне леме закључујемо да је при одређивању вредности израза t у моделу $\mathbf{M}$ за валуацију $\mu : \mathrm{Var} \to M$ значајна само рестрикција $\mu \restriction_{V(t)}$. 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 по једна рестрикција $\nu = \begin{pmatrix} x_1 & \cdots & x_n \\ a_1 & \cdots & a_n \end{pmatrix}$. Наведени разлози оправдавају употребу ознаке $t^{\mathbf{M}}[\vec{a}]$ за вредност израза t у моделу $\mathbf{M}$ за $\vec{a} \in M^n$. Исто важи и за формуле. При неком подразумеваном уређењу променљивих $\mathrm{Fr}(\alpha) = \{x_1, \ldots, x_n\}$, сваким $\vec{a} = (a_1, \ldots, a_n) \in M^n$ одређена је једна рестрикција било које валуације, па са $\alpha^{\mathbf{M}}[\vec{a}]$ означавамо истинитосну вредност формуле α у моделу $\mathbf{M}$ за $\vec{a} \in M^n$.

Дефиниција 5. *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 5. Овај пример је наставак примера 4, 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 $\exists z(0 \leqslant z \land z \neq 0 \land x + z \leqslant y \land x + z \neq y)$ (подсећамо да, за изразе t_1 и t_2, записом $t_1 \neq t_2$ скраћујемо формулу $\neg t_1 = t_2$). 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 променљивих 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 $\mathbf{Z} \not\models \varphi[5, 5]$.

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 $\mathbf{X} \models \varphi[a, b]$? $\rhd$

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 μ_1 и μ_2 важи $t^{\mathbf{M}}[\mu_1] = t^{\mathbf{M}}[\mu_2]$). Другим речима, вредност затвореног израза t потпуно је одређена само изабраним моделом $\mathbf{M}$ и ту вредност означавамо са $t^{\mathbf{M}}$. Аналогно, ако је $\mathrm{Fr}(\alpha) = \emptyset$, тј. ако је α реченица, њена истинитосна вредност 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 $\mathbf{M} \models \alpha$.

ПРИМЕР 6. Посматрајмо исти језик и моделе овог језика као у претходном примеру, односно у примеру 4.

Нека је σ реченица $\exists x \forall y (x \leqslant y)$. Није тешко видети да $\mathbf{R} \not\models \sigma$, јер у скупу реалних бројева не постоји најмањи елемент у односу на уређење $\leqslant$. Такође, $\mathbf{Z} \not\models \sigma$. Међутим, σ важи у $\mathbf{X}$: $a \lhd a$, $a \lhd b$, $a \lhd c$.

Реченица $\forall y \exists x (x \leqslant y)$ важи у све три структуре. Препоручујемо читаоцу да одреди што више реченица језика $\mathcal{L}$ које ће важити у неким од посматраних структура, али не и у свим. $\rhd$

Модели и контрамодели реченица, односно теорија

У примеру 6 испитивали смо да ли су у задатом моделу неког језика $\mathcal{L}$ (не)тачне реченице језика $\mathcal{L}$, пре свега да бисмо илустровали дефиницију релације задовољења. Веома је важан и обрнути проблем: ако је дата реченица неког језика $\mathcal{L}$, одредити, ако уопште постоји, структуру језика $\mathcal{L}$ у којој је та реченица тачна, односно структуру у којој није тачна.

Дефиниција 6. ***Модел*** *реченице $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ јесте свака структура језика $\mathcal{L}$ у којој је та реченица тачна. Кажемо да је реченица* ***задовољива*** *ако има бар један модел.* ***Контрамодел*** *реченице $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ јесте свака структура језика $\mathcal{L}$ у којој та реченица није тачна.*

ПРИМЕР 7. Нека је $\mathrm{Rel}_{\mathcal{L}} = \{R\}$, $\mathrm{ar}(R) = 2$. Одредимо, ако постоје, модел и контрамодел реченице $\forall x (\neg R(x, x) \land \exists y R(x, y))$.

Да бисмо одредили модел дате реченице, треба да изаберемо неки скуп M и бинарну релацију $R^{\mathbf{M}} \subseteq M \times M$, тако да $\mathbf{M} = (M, R^{\mathbf{M}}) \models \forall x (\neg R(x, x) \land \exists y R(x, y))$. Наравно, на располагању нам стоје сви скупови „овога (математичког) света“ и на сваком од њих све бинарне релације. Нереално би било очекивати да постоји неки универзални савет како изабрати жељени скуп (и, у овом случају, бинарну релацију на њему). Искуство и интуиција су углавном најјачи адути при решавању оваквих проблема. Тако, искуство и интуиција у вези са структурама бројева помажу нам да уочимо да ће било који од скупова бројева $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ или $\mathbb{R}$, заједно са одговарајућим строгим уређењем представљати жељени модел. На пример,

$$(\mathbb{R}, <) \models \forall x(\neg R(x,x) \wedge \exists y R(x,y)),$$

јер који год реални број x да изаберемо, знамо да је $x \not< x$, као и да постоји реални број y такав да је $x < y$.[37]

Ако се мало дуже задржимо на задатој реченици[38] уочићемо још њених модела. Наводимо само два, остављајући читаоцима да пронађу још неке:

- отворени интервал $(0,1)$ (подскуп од $\mathbb{R}$) заједно са одговарајућим строгим уређењем задовољава дату реченицу;
- скуп $X = \{1,2,3\}$ заједно са релацијом $\lhd = \{(1,2),(2,3),(3,1)\}$ задовољава дату реченицу.

Слично поступамо и при тражењу контрамодела реченице $\forall x(\neg R(x,x) \wedge \exists y R(x,y))$. Није тешко уочити да ће било који од скупова бројева $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ или $\mathbb{R}$, заједно са одговарајућим уређењем представљати контрамодел дате реченице. На пример,

$$(\mathbb{R}, \leqslant) \not\models \forall x(\neg R(x,x) \wedge \exists y R(x,y)),$$

јер који год реални број x да изаберемо, знамо да је $x \leqslant x$. $\triangleright$

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

- $\forall x R(x,x)$,
- $\forall x \forall y (R(x,y) \wedge R(y,x) \Rightarrow x = y)$,
- $\forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow R(x,y))$,

[37] Често је корисно запис $(\mathbb{R}, <) \models \forall x(\neg R(x,x) \wedge \exists y R(x,y))$ превести на формулу теорије скупова $(\forall x \in \mathbb{R})(\neg x < x \wedge \exists y \in \mathbb{R}\,(x < y))$, где су $\mathbb{R}$ и $<$ познате „скуповне константе“. Ми овакве преводе нећемо наводити, али препоручујемо читаоцу да се повремено и њима послужи.

[38] Увек је пожељно приликом решавања оваквих проблема потражити што више различитих модела задате формуле, јер се на тај начин стиче искуство и јача интуиција.

- $\forall x \forall y (R(x,y) \vee R(y,x))$.

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. $\triangleright$

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 9. **Теорија група.** Још од раног школовања упознајемо се са особинама стуктуре $(\mathbb{Z}, +, -, 0)$, где је „+“ сабирање целих бројева, „−“ унарна операција *супротни елемент*, и 0 константа. Временом схватимо да су неке особине посебно важне и да из њих произлазе многе друге. Доста пута смо имали прилике у уџбеницима да сретнемо посебно издвојене следеће особине:

- $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$,
- $\forall x (x + 0 = x)$,
- $\forall x (x + (-x) = 0)$.

Исте особине издвајамо и за $(\mathbb{Q}, +, -, 0)$, $(\mathbb{R}, +, -, 0)$, $(\mathbb{C}, +, -, 0)$. Затим их препознајемо и у случају структура $(\mathbb{Q} \setminus \{0\}, \cdot, ^{-1}, 1)$, $(\mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1)$, $(\mathbb{C} \setminus \{0\}, \cdot, ^{-1}, 1)$, без обзира на нове ознаке: $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$, $\forall x (x \cdot 1 = x)$ $\forall x (x \cdot x^{-1} = 1)$.

Чим се упознамо са појмом бијекције, схватимо да је за било који скуп X, композиција две бијекције $f : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$ и $g : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$ такође једна бијекција $f \circ g : X \to X$, да је идентичко пресликавање бијекција, $\mathrm{id}_X : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$, и да за сваку бијекцију $f : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$ постоји инверзна $f^{-1} : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$, и да притом важе познати закони: $f \circ (g \circ h) = (f \circ g) \circ h$, $f \circ \mathrm{id}_X = f$, $f \circ f^{-1} = \mathrm{id}_X$, за било које бијекције $f, g, h : X \overset{1\text{-}1}{\underset{\text{na}}{\rightarrow}} X$.

Што дубље улазимо у математику, наилазимо на све више структура које задовољавају поменуте законитости. Значај оваквих структура намеће и потребу, али и жељу, да истражујемо све такве структуре. Уочавајући какав је тип структура којима желимо да се бавимо, бирамо језик $\mathcal{L}_{\mathrm{GR}} = \{*, ^{-1}, e\}$ (при чему је, наравно, могуће изабрати и неке друге симболе), $\mathrm{Fun}_{\mathcal{L}_{\mathrm{GR}}} = \{*, ^{-1}\}$, $\mathrm{ar}(*) = 2$; $\mathrm{ar}(^{-1}) = 1$, $\mathrm{Cons}_{\mathcal{L}_{\mathrm{GR}}} = \{e\}$ и на њему формулишему теорију

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

Теорија T_{GR} назива се *теорија група*, а њени модели су *групе*. Овим се отвара један нови свет математичких објеката који по разноврсности далеко превазилази набројане полазне примере. $\triangleright$

Пример 10. **Теорија уређених поља.** Нека је $\mathcal{L}_{\mathrm{OF}} = \{\leqslant, +, -, \cdot, 0, 1\}$, 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 11. **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 $\mathrm{Th}(\mathbf{M}) = \{\sigma \in \mathrm{Sent}_{\mathcal{L}} \mid \mathbf{M} \models \sigma\}$. ▷

Када смо у претходним примерима помињали различите моделе, пре свега смо мислили на моделе који нису тривијално различити, тј. на моделе који нису изоморфни. Појам изоморфизма нека два модела истог језика уводимо аналогно као у случају Булових алгебри (видети страну 11).

Дефиниција 8. *Модели* $\mathbf{A}$ *и* $\mathbf{B}$, *истог језика* $\mathcal{L}$, ***изоморфни*** *су ако постоји бијекција* $f : A \xrightarrow[\text{на}]{1\text{-}1} B$ *таква да:*

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

$$R^{\mathbf{A}}(a_1, \ldots, a_n) \text{ акко } R^{\mathbf{B}}(f(a_1), \ldots, f(a_n));$$

2. *ако* $F \in \mathrm{Fun}_{\mathcal{L}}$, $\mathrm{ar}(F) = n$, *онда за све* $a_1, \ldots, a_n \in A$,

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

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

Бијекција која задовољава набројане особине назива се ***изоморфизам****.*

Да су $\mathbf{A}$ и $\mathbf{B}$ изоморфни модели, означавамо са $\mathbf{A} \cong \mathbf{B}$. Ако желимо да истакнемо да је $f : A \overset{1\text{-}1}{\underset{\text{на}}{\to}} B$ изоморфизам одговарајућих Булових алгебри, пишемо $f : \mathbf{B}_1 \cong \mathbf{B}_2$.

Није тешко доказати да изоморфни модели задовољавају исте реченице, тј. да су теорије ових модела[39] једнаке.

Лема 2. *Ако је* $\mathbf{A} \cong \mathbf{B}$, *онда је* $\mathrm{Th}(\mathbf{A}) = \mathrm{Th}(\mathbf{B})$.

Пример 12. Да ли међу моделима $(\mathbb{R}, <)$, $((0,1), <)$, $(\mathbb{N}, <)$ и $(\mathbb{Z}, <)$, где је $<$ уобичајено строго уређење одговарајућег домена, има оних које су изоморфне?

Очигледно је, на пример, да $(\mathbb{R}, <) \ncong (\mathbb{N}, <)$, јер као што знамо не постоји бијекција међу доменима ових модела.

Бијекција међу доменима модела $(\mathbb{N}, <)$ и $(\mathbb{Z}, <)$ постоји, али ниједна од њих не може бити изоморфизам. Ово једноставно показујемо, применом претходне леме, када уочимо реченицу која је тачна у једном моделу и није тачна у другом. На пример, $(\mathbb{Z}, <) \models \forall x \exists y\, (y < x)$, али $(\mathbb{N}, <) \not\models \forall x \exists y\, (y < x)$. Дакле, $(\mathbb{Z}, <) \ncong (\mathbb{N}, <)$.

Модели $(\mathbb{R}, <)$ и $((0,1), <)$ јесу изоморфни. Функција $f : \mathbb{R} \to (0,1)$, дефинисана са $f(x) = \dfrac{1}{2} + \dfrac{1}{\pi}\mathrm{arctg}\, x$, $x \in \mathbb{R}$, јесте бијекција и важи: $x < y$ акко $f(x) < f(y)$. Дакле, $f : (\mathbb{R}, <) \cong ((0,1), <)$. $\triangleright$

Ваљане формуле

У уводном примеру 1 (страна 95) већ смо наговестили значај реченица које су тачне у било ком моделу одговарајућег језика.

Дефиниција 9. *Формула* $\alpha \in \mathrm{For}_{\mathcal{L}}$ *је* ***ваљана*** *ако за сваки модел* $\mathbf{M}$ *и сваку валуацију* $\mu : \mathrm{Var} \to M$ *важи* $\mathbf{M} \models \alpha[\mu]$. *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* $\mathcal{L}$.

[39] Теорија модела $\mathbf{M}$ језика $\mathcal{L}$ јесте теорија $\mathrm{Th}(\mathbf{M}) = \{\sigma \in \mathrm{Sent}_{\mathcal{L}} \mid \mathbf{M} \models \sigma\}$.

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 $\forall x_1 \ldots \forall x_n \alpha(x_1,\ldots,x_n)$. Да бисмо се у то уверили, претпоставимо да је формула α ваљана и докажимо да је тада ваљана и формула $\forall x\alpha$, где је x произвољна променљива, одакле ће очиглено следити наведена тврдња.

Нека је $\mathbf{M}$ произвољан модел одговарајућег језика и $\mu : \mathrm{Var} \to M$ произвољна валуација. Пошто је α ваљана формула, имамо да за свако $a \in M$ важи $\mathbf{M} \models \alpha[\mu(x/a)]$, јер $\mathbf{M} \models \alpha[\nu]$, за сваку валуацију ν, па специјално и за валуације $\mu(x/a)$, $a \in M$. Према дефиницији релације задовољења (тј. функције која додељује истинитосне вредности формулама), из $\mathbf{M} \models \alpha[\mu(x/a)]$, за све $a \in M$, следи да $\mathbf{M} \models \alpha[\mu]$. Важи и обрнуто, ако је $\forall x\alpha$ ваљана формула, онда је ваљана и формула α. Ако произвољно изаберемо модел $\mathbf{M}$ и валуацију $\mu : \mathrm{Var} \to M$, тада ће из $\mathbf{M} \models \forall x\alpha[\mu]$, следити да $\mathbf{M} \models \alpha[\mu(x/a)]$, за било које $a \in M$, па специјално и за $a = \mu(x)$, што значи да ће бити и $\mathbf{M} \models \alpha[\mu]$.

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. Нека је $\tau(p_1,\ldots,p_n)$ таутологија и $\underline{\tau}$ формула добијена тако што су слова $p_1,\ldots,p_n$ редом замењена формулама $\alpha_1,\ldots,\alpha_n \in \mathrm{For}_{\mathcal{L}}$. Тада ће за произвољан модел $\mathbf{M}$ и било коју валуацију μ важити $\underline{\tau}^{\mathbf{M}}[\mu] = \widehat{v}(\tau)$, где је $\widehat{v}$ валуација исказних слова таква да је $v(p_i) = \alpha_i^{\mathbf{M}}[\mu]$, $i = 1,\ldots,n$, одакле следи жељено тврђење.

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 $\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$).

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

У ваљаност прве формуле једноставно се уверавамо:

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

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 ($\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$):

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

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

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 $\mathbf{N} \not\models \forall xU(x) \vee \forall xV(x)$, тј. $\mathbf{N} \not\models \forall x(U(x) \vee V(x)) \Rightarrow \forall xU(x) \vee \forall xV(x)$. Такође, $\mathbf{N} \not\models \exists xU(x) \wedge \exists xV(x) \Rightarrow \exists x(U(x) \wedge V(x))$.

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 $\mathbf{N} \not\models \forall y\exists xR(x,y) \Rightarrow \exists x\forall yR(x,y)$

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

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

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 μ важи:

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

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 $\alpha^{\mathbf{M}}[\mu(x/t^{\mathbf{M}}[\mu])] = \alpha(x/t)^{\mathbf{M}}[\mu]$, за било који модел $\mathbf{M}$ и валуацију μ.

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.

Пренекс нормална форма

У претходном поглављу, видели смо да нормалне форме исказних формула (страна 51) могу бити веома корисне. Трансформације исказних формула у неку нормалну форму обављали смо ослањајући се на семантичку еквивалентност исказних формула. Ову врсту еквивалентности природно преносимо и на формуле логике првог реда.

Формуле α и β неког језика $\mathcal{L}$ јесу *семантички еквивалентне*, у ознаци $\alpha \equiv \beta$ ако је $\models \alpha \Leftrightarrow \beta$. Неке од ваљаних формула које смо до сада уочили говоре управо о семантичкој еквивалентности одређених формула:

- $\forall x(\alpha \wedge \beta) \equiv \forall x\alpha \wedge \forall x\beta$ и $\exists x(\alpha \vee \beta) \equiv \exists x\alpha \vee \exists x\beta$,
- $\forall x(\alpha \vee \beta) \equiv \alpha \vee \forall x\beta$ и $\exists x(\alpha \wedge \beta) \equiv \alpha \wedge \exists x\beta$, ако x **није** слободна променљива формуле α,
- $\neg\forall x\alpha \equiv \exists x\neg\alpha$ и $\neg\exists x\alpha \equiv \forall x\neg\alpha$;
- $\forall x\alpha \equiv \forall y\alpha[x/y]$ и $\exists x\alpha \equiv \exists y\alpha[x/y]$.

Ове еквиваленције заједно са неким које смо већ користили у исказној логици, омогућавају нам да све квантификаторе неке формуле „извучемо напред“ тј. да формулу трансформишемо у тзв. *пренекс нормалну форму*.

Дефиниција 10. *Формула α је у **пренекс нормалној форми** уколико је облика $Q_1x_1 \ldots Q_nx_n\theta$, где је сваки Q_i неки квантификатор, а θ је формула без квантификатора ($Q_1x_1 \ldots Q_nx_n$ се назива префикс формуле α). Префикс може бити празан, па се и свака формула без квантификатора сматра формулом у пренекс нормалној форми.*

Лема 3. *Свака формула је еквивалентна формули која је у пренекс нормалној форми.*

Доказ леме скицираћемо у наредном примеру.

Пример 13. 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 атомичних 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. $\triangleright$

Пример 14. 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. $\triangleright$

Семантичка последица

Појам семантичке последице за логику првог реда уводимо потпуно аналогно као у случају исказне логике.

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* $\mu : \mathrm{Var} \to M$,

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

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 15. 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]

$\triangleright$

Све особине семантичке последице наведене у леми 1 за исказну логику важе и у случају логике првог реда, па их овом приликом нећемо ни наводити. Такође важи и теорема компактности. Као и у случају исказне логике, реч је о веома важној теореми са бројним применама.

Теорема компактности

Теорема 1. [***Теорема компактности***] *Ако сваки коначан подскуп неке теорије има модел, онда и та теорија има модел.*

Идеја доказа. Доказ ћемо спровести под претпоставком да је одговарајући језик $\mathcal{L}$ пребројив, па је самим тим и скуп формула пребројив. Нека је Γ произвољна теорија на пребројивом језику. Пошто је тада скуп Γ пребројив, све реченице из Γ можемо поређати у низ: $\gamma_0, \gamma_1, \gamma_2, \ldots$. Ако сваки коначан подскуп од Γ има модел, онда за сваки природан број n постоји модел $\mathbf{M}_n$ такав да $\mathbf{M}_n \models \{\gamma_0, \ldots, \gamma_n\}$. Добијени низ модела $\mathbf{M}_n$, $n \in \mathbb{N}$ можемо схватити као низ све бољих апроксимација траженог модела теорије Γ, јер повећавањем индекса n модели $\mathbf{M}_n$ задовољавају све више реченица теорије Γ. Много је важније приметити да свака реченица из Γ важи у скоро свим моделима наведеног низа, тј. у свим осим евентуално у коначно много њих ($\mathbf{M}_n \models \gamma_k$, за $n \geqslant k$, док γ_k не мора важити у моделима $\mathbf{M}_n$ за $n < k$). Заправо, модел теорије Γ биће у одређеном смислу гранична вредност низа модела $\mathbf{M}_n$, $n \in \mathbb{N}$.

Да бисмо што једноставније објаснили идеју конструкције модела теорије Γ, замислимо да је за сваки модел $\mathbf{M}_n$, $n \in \mathbb{N}$, задужена по једна особа која само у свом моделу проверава (не)истинитост реченица језика $\mathcal{L}$ и даје нам одговор *да* или *не* на питање *да ли је тачна нека одређена реченица*. Када свима поставимо исто питање поменутог облика, свака особа на свој начин интерпретира симболе полазног језика (па тиме и другачије разуме наше питање), проверава истинитост те реченице у свом моделу и саопштава нам одговарајући одговор[40]. Наравно, можемо питати и да ли је тачна нека формула са слободним променљивама, при чему свакој особи тада морамо прецизирати које вредности из домена свог модела треба да додели тим променљивама. Како домени модела могу бити различити, ако желимо свима истовремено да прецизирамо коју вредност треба доделити некој променљивој, потребно је да задамо низ $f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} M_n$ такав да $f(n) \in M_n$, $n \in \mathbb{N}$, при чему ће особа задужена за $\mathbf{M}_n$ узимати у обзир само члан $f(n)$. Као што је и очекивано, на свако питање (поменуте врсте) можемо добити различите одговоре, па узимајући их све у обзир, формирамо бинарни низ $r : \mathbb{N} \to \{0, 1\}$, при чему $r(n) = 1$ значи да је особа задужена за $\mathbf{M}_n$ дала одговор *да*, а $r(n) = 0$ да је та особа дала одговор *не*. Испоставља се да уколико „профилтрирамо“ све одговоре, тј. усвојимо добру стратегију тумачења одговора, стратегију помоћу које бисмо на основу низа *да–не* одговора бирали одговор „већине“, онда можемо сматрати да имамо својеврстан модел полазне теорије. Шта значи *већина* прецизираћемо тако што ћемо увести колекцију *великих* подскупова од $\mathbb{N}$. Наиме, колекцију $\mathcal{U}$ подскупова од $\mathbb{N}$ сматраћемо колекцијом *великих подскупова* од $\mathbb{N}$ уколико важе следећа својства:

1. $\mathbb{N} \in \mathcal{U}$, тј. $\mathbb{N}$ је велики подскуп од $\mathbb{N}$;

2. ако је $V \subseteq X$ и $V \in \mathcal{U}$, онда $X \in \mathcal{U}$, тј. надскуп великог скупа је велики скуп;

---

[40] На пример, ако полазни језик садржи бинарни релацијски симбол R свим особама можемо поставити питање *да ли је тачно* $\forall x \exists y R(x, y)$. Особа која је задужена за $\mathbf{M}_n$ провераваће да ли за сваки $x \in M_n$ постоји $y \in M_n$ такав да је $R^{\mathbf{M}_n}(x, y)$.

3. ако $U \in \mathcal{U}$ и $V \in \mathcal{U}$, онда $U \cap V \in \mathcal{U}$, тј. пресек два велика скупа јесте велики скуп;

4. за сваки скуп $X \subseteq \mathbb{N}$, или $X \in \mathcal{U}$ или $X^c \in \mathcal{U}$ и оба нису у $\mathcal{U}$, тј. било који подскуп од $\mathbb{N}$ или је велики или је његов комплемент велики, и при томе оба не могу истовремено бити велики;

5. ако је $K \subseteq \mathbb{N}$ било који коначан скуп и $U \in \mathcal{U}$, онда $U \setminus K \in \mathcal{U}$, тј. ако из великог скупа избацимо коначно много елемената, добијени скуп је и даље велики.

Наведене захтеве није тешко оправдати у контексту за који су нама потребни велики скупови. А контекст је следећи: ако је $r : \mathbb{N} \to \{0, 1\}$ низ одговора које смо добили на неко питање, онда је потребно да измеримо „величину“ скупова $D = \{n \in \mathbb{N} \mid r(n) = 1\}$ и $N = \{n \in \mathbb{N} \mid r(n) = 0\}$, тј. да испитамо да ли $D \in \mathcal{U}$ или $N \in \mathcal{U}$, чиме одређујемо одговор већине – назовимо га *релевантним одговором*. Релевантан одговор је „*да*“ ако $D \in \mathcal{U}$, односно „*не*“ ако $N \in \mathcal{U}$. Услов 1 значи да уколико за све $\mathbf{M}_n$, $n \in \mathbb{N}$, добијемо исти одговор, онда тај одговор прихватамо као релевантан. Други услов је такође природан и веома је близак са модус поненсом. Трећи услов можемо тумачити и на следећи начин: ако смо прихватили као потврдне одговоре на нека два питања, онда морамо прихватити као потврдан одговор на конјункцију тих питања. Четврти услов омогућава да какав год низ одговора да добијемо увек можемо да издвојимо релевантан одговор. Пети услов каже да коначно много одговора не може утицати на релевантан одговор.

Да постоји колекција подскупова од $\mathbb{N}$ таква да важе услови 1–5 показаћемо касније (лема 4)[41]. Пре тога укратко описујемо како добијамо модел теорије Г. Узимајући у обзир то да свакој промењљивој додељујемо једну функцију $f : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} M_n$ такву да $f(n) \in M_n$, $n \in \mathbb{N}$, природно је да изградњу жељеног модела започенемо скупом M свих оваквих функција. Даље, ако свим особама поставимо питање да ли су нека два елемента $f, g \in M$ једнака[42], свака особа ће у свом моделу $\mathbf{M}_n$ проверавати да ли је $f(n) = g(n)$. За нас су f и g једнаки ако $\{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}$. Дакле, иако f и g не морају бити заиста једнаки, ми их сматрамо једнаким на основу добијених одговора. Ово нас даље доводи до тога да елементе скупа M идентификујемо у складу са скупом $\mathcal{U}$. Поменуто изједначавање низова из M уводимо дефиницијом релације еквиваленције $\sim$ на следећи начин:

$$f \equiv_{\mathcal{U}} g \ \text{акко} \ \{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}.$$

[41] Реч је о једној врсти ултрафилтера Булове алгебре над $\mathcal{P}(\mathbb{N})$.

[42] Питање да ли су елементи $f, g \in M$ једнаки исто је као питање да ли је тачна формула $x = y$ за валуацију $x \mapsto f$, $y \mapsto g$.

Ако са $\langle f \rangle$ означимо класу еквиваленције одређену елементом $f \in M$, имамо да је

$$(*) \qquad \langle f \rangle = \langle g \rangle \ \text{акко} \ \{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}.$$

На скупу $M^* = M/\equiv_{\mathcal{U}}$, свих класа еквиваленције, градимо жељени модел, тј. интерпретирамо одговарајући језик. Релацијски симбол $R \in \mathrm{Rel}_{\mathcal{L}}$, $\mathrm{ar}(R) = m$, интерпретирамо по узору на $(*)$:

$$R^{\mathbf{M}^*}(\langle f_1 \rangle, \dots, \langle f_m \rangle) \ \text{акко} \ \{n \in \mathbb{N} \mid R^{\mathbf{M}_n}(f_1(n), \dots, f_m(n))\} \in \mathcal{U}.$$

Функцијски симбол $F \in \mathrm{Fun}_{\mathcal{L}}$, $\mathrm{ar}(F) = m$, интерпретирамо на следећи начин: ако $\langle f_1 \rangle, \dots, \langle f_m \rangle \in M^*$, онда је вредност $F^{\mathbf{M}^*}(\langle f_1 \rangle, \dots, \langle f_m \rangle)$ једнака класи еквиваленције одређеној низом $n \mapsto F^{\mathbf{M}_n}(f_1(n), \dots, f_m(n))$, што ћемо краће записивати $F^{\mathbf{M}^*}(\langle f_1 \rangle, \dots, \langle f_m \rangle) = \langle F^{\mathbf{M}_n}(f_1(n), \dots, f_m(n)) \rangle$. Најзад, симбол константе $c \in \mathrm{Const}_{\mathcal{L}}$ интерпретирамо као класу еквиваленције низа $n \mapsto c^{\mathbf{M}_n}$, тј. $c^{\mathbf{M}^*} = \langle c^{\mathbf{M}_n} \rangle$. Овако добијени модел јесте модел полазне теорије Γ.

Много је тврдњи у претходном излагању које нисмо доказали. У наставку ћемо доказивати постепено све што је пропуштено, али пре тога наводимо један пример.

Пример 16. Посматрајмо језик уређених поља проширен једним новим симболом константе $\mathcal{L} = \{\leqslant, +, -, \cdot, 0, 1, c\}$ и следећу теорију на овом језику:

$$\Gamma = T_{\mathrm{FO}} \cup \{c + c < 1, c + c + c < 1, c + c + c + c < 1, c + c + c + c + c < 1, \dots\},$$

при чему је T_{FO} теорија уређених поља[43]. Посматрајмо сада низ модела $\mathbf{M}_n = (\mathbb{Q}, \leqslant, +, -, \cdot, 0, 1, 1/(n+1))$, $n \in \mathbb{N}$, при чему су у сваком моделу симболи $\leqslant, +, -, \cdot, 0, 1$ интерпретирани на скупу рационалних бројева $\mathbb{Q}$ на уобичајени начин, док је симбол константе c у сваком моделу различито интерпретиран: $c^{\mathbf{M}_n} = \dfrac{1}{n+1}$, $n \in \mathbb{N}$. Приметимо да низ $\mathbf{M}_n$, $n \in \mathbb{N}$, „постепено“ задовољава све више реченица теорије Γ. Изградимо, на горе описани начин, модел $\mathbf{M}^*$ који ће задовољавати све реченице скупа Γ. Како је скуп $\mathbb{Q}$ домен сваког модела датог низа, унија свих домена је такође $\mathbb{Q}$. Нека је $\mathcal{U}$ нека колекција подскупова од $\mathbb{N}$ таква да важе услови 1–5. Жељени модел ће бити $\mathbf{M}^* = \mathbb{Q}^{\mathbb{N}}/\mathcal{U}$, где је $\mathbb{Q}^{\mathbb{N}}$ скуп свих низова рационалних бројева. Да $\mathbf{M}^*$ задовољава све формуле из T_{FO} препуштамо читаоцима да образложе након нашег образложења зашто су задовољене остале реченице скупа Γ. На пример, на питање *да ли је тачна реченица* $c + c + c + c < 1$, све особе задужене за моделе $\mathbf{M}_n$, $n \in \mathbb{N}$, рачунаће збир $c + c + c + c$ на свој начин:

$$\langle \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}, \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + \frac{1}{3}, \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}, \frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5}, \dots \rangle,$$

[43]Формула $c + c < 1$ је скраћење формуле $c + c \leqslant 1 \wedge \neg\, c + c = 0$, и слично за остале.

а затим ће испитивати да ли су добијени збирови мањи од 1:

$$\langle 2, \frac{4}{3}, 1, \frac{4}{5}, \frac{2}{3}, \frac{4}{7}, \frac{1}{2}, \ldots \rangle \overset{?}{<} \langle 1, 1, 1, 1, 1, 1, 1, \ldots \rangle,$$

и дати одговарајуће одговоре:

$$(\textit{не}, \textit{не}, \textit{не}, \textit{да}, \textit{да}, \textit{да}, \textit{да}, \ldots).$$

Ми ћемо као релевантан одговор прихватити *да*, јер су, осим прва три, сви остали одговори потврдни. Дакле, реченица $c + c + c + c < 1$ важи у $\mathbf{M}^*$ (подсећамо да је $1^{\mathbf{M}^*} = \langle 1, 1, 1, 1, \ldots \rangle$ и $c^{\mathbf{M}^*} = \langle \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots \rangle$). Није тешко закључити да ће модел $\mathbf{M}^*$ заправо задовољавати сваку реченицу $\underbrace{c + \cdots + c}_{n \text{ пута}} < 1$, $n \geqslant 2$. ▷

Следе обећани докази свих тврдњи наведених у излагању идеје доказа теореме компактности.

Лема 4. *Постоји колекција $\mathcal{U}$ подскупова од $\mathbb{N}$ таква да важе услови 1–5.*

Доказ. Нека је $\mathcal{F}$ колекција свих коконачних подскупова од $\mathbb{N}$, тј. подскупова чији су комплементи коначни: $\mathcal{F} = \{X \in \mathcal{P}(\mathbb{N}) \mid \mathbb{N} \setminus X \text{ је коначан скуп}\}$. Није тешко проверити да овај скуп има својство коначног пресека. Заиста, ако су $F_1, \ldots, F_n \in \mathcal{F}$ произвољни, тада је $F_1 \cap \cdots \cap F_n = \mathbb{N} \setminus ((\mathbb{N} \setminus F_1) \cup \cdots \cup (\mathbb{N} \setminus F_n))$, па како је скуп $(\mathbb{N} \setminus F_1) \cup \cdots \cup (\mathbb{N} \setminus F_n)$ коначан, скуп $F_1 \cap \cdots \cap F_n$ мора бити непразан. Према теореми о ултрафилтеру (страна 30), у Буловој алгебри $(\mathcal{P}(\mathbb{N}), \cup, \cap, ^{\mathrm{c}}, \emptyset, \mathbb{N})$ постоји ултрафилтер $\mathcal{U}$ који садржи $\mathcal{F}$. Дакле, $\mathcal{U}$ задовољава услове 1–4. Остаје још да проверимо да $\mathcal{U}$ задовољава услов 5. Нека је $K \subseteq \mathbb{N}$ произвољан коначан подскуп и $U \in \mathcal{U}$. Тада $K^{\mathrm{c}} \in \mathcal{F} \subseteq \mathcal{U}$, па према услову 3 следи да $U \setminus K = U \cap K^{\mathrm{c}} \in \mathcal{U}$. □

Дефиниција 12. *Колекција подскупова од $\mathbb{N}$ која задовољава услове 1–5 назива се неглавни ултрафилтер над $\mathbb{N}$.*

У описаној конструкцији модела теорије Γ пошли смо од скупа M који садржи само функције $f : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} M_n$ такве да $f(n) \in M_n$, $n \in \mathbb{N}$. Овај скуп се назива и (уопштени) Декартов производ и обележава се са $\prod_{n \in \mathbb{N}} M_n$. Затим је на овом скупу дефинисана релација $\equiv_{\mathcal{U}}$ на следећи начин:

$$f \equiv_{\mathcal{U}} g \text{ акко } \{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U},$$

где је $\mathcal{U}$ неки неглавни ултрафилтер над $\mathbb{N}$.

Лема 5. *Релација $\equiv_{\mathcal{U}}$ скупа $\prod_{n \in \mathbb{N}} M_n$ је релација еквиваленције.*

Доказ. (P) За свако $f \in \prod_{n\in\mathbb{N}} M_n$, важи $\{n \in \mathbb{N} \mid f(n) = f(n)\} = \mathbb{N} \in \mathcal{U}$, одакле следи да је $f \equiv_{\mathcal{U}} f$.
(C) Нека је $f \equiv_{\mathcal{U}} g$, за неке $f, g \in \prod_{n\in\mathbb{N}} M_n$. Тада $\{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}$, а како је $\{n \in \mathbb{N} \mid f(n) = g(n)\} = \{n \in \mathbb{N} \mid g(n) = f(n)\}$, закључујемо да $\{n \in \mathbb{N} \mid g(n) = f(n)\} \in \mathcal{U}$, односно $g \equiv_{\mathcal{U}} f$.
(T) Претпоставимо да је $f \equiv_{\mathcal{U}} g$ и $g \equiv_{\mathcal{U}} h$, за неке $f, g, h \in \prod_{n\in\mathbb{N}} M_n$. Тада је $X = \{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}$ и $Y = \{n \in \mathbb{N} \mid g(n) = h(n)\} \in \mathcal{U}$. Како је $X \cap Y \in \mathcal{U}$ и $X \cap Y \subseteq \{n \in \mathbb{N} \mid f(n) = h(n)\}$, закључујемо да $\{n \in \mathbb{N} \mid f(n) = h(n)\} \in \mathcal{U}$, тј. $f \equiv_{\mathcal{U}} h$. $\square$

На количничком скупу $M^* = \prod_{n\in\mathbb{N}} M_n/ \equiv_{\mathcal{U}}$, или краће записано $M^* = \prod_{\mathcal{U}} M_n$, језик $\mathcal{L}$ интерпретиран је на следећи начин:

- ако $R \in \mathrm{Rel}_{\mathcal{L}}$, $\mathrm{ar}(R) = m$, онда
$$R^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle) \text{ акко } \{n \in \mathbb{N} \mid R^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))\} \in \mathcal{U}.$$
- ако $F \in \mathrm{Fun}_{\mathcal{L}}$, $\mathrm{ar}(F) = m$, онда
$$F^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle) = \langle F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))\rangle,$$
при чему је $\langle F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))\rangle$ класа еквиваленције одређена низом $n \mapsto F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))$.
- ако $c \in \mathrm{Const}_{\mathcal{L}}$, онда је $c^{\mathbf{M}^*} = \langle c^{\mathbf{M}_n}\rangle$, при чему је $\langle c^{\mathbf{M}_n}\rangle$ класа еквиваленције одређена низом $n \mapsto c^{\mathbf{M}_n}$.

Лема 6. *Интерпретације релацијских и функцијских симбола језика $\mathcal{L}$ на скупу M^* добро су дефинисане.*

Доказ. Добра дефинисаност интерпретација релацијских и функцијских симбола значи да:

1) из $\langle f_1\rangle = \langle g_1\rangle, \ldots, \langle f_m\rangle = \langle g_m\rangle$ следи
$$R^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle) \text{ акко } R^{\mathbf{M}^*}(\langle g_1\rangle, \ldots, \langle g_m\rangle),$$
2) из $\langle f_1\rangle = \langle g_1\rangle, \ldots, \langle f_m\rangle = \langle g_m\rangle$ следи
$$F^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle) = F^{\mathbf{M}^*}(\langle g_1\rangle, \ldots, \langle g_m\rangle).$$

Нека је $\langle f_1\rangle = \langle g_1\rangle, \ldots, \langle f_m\rangle = \langle g_m\rangle$. Тада је $f_1 \equiv_{\mathcal{U}} g_1, \ldots, f_m \equiv_{\mathcal{U}} g_m$, што значи да $X_i = \{n \in \mathbb{N} \mid f(n) = g(n)\} \in \mathcal{U}$, $i = 1, \ldots, m$, па и $X_1 \cap \cdots \cap X_m \in \mathcal{U}$.

Докажимо еквиваленцију из 1. Претпоставимо да $R^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle)$. Тада $X = \{n \in \mathbb{N} \mid R^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))\} \in \mathcal{U}$, па $X \cap X_1 \cap \cdots \cap X_m \in \mathcal{U}$. Ако $n \in X \cap X_1 \cap \cdots \cap X_m$, имамо да је $R^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))$, $f_1(n) = g_1(n)$, $\ldots$, $f_m(n) = g_m(n)$, па важи и $R^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))$. Дакле,

$$X \cap X_1 \cap \cdots \cap X_m \subseteq \{n \in \mathbb{N} \mid R^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))\},$$

па $\{n \in \mathbb{N} \mid R^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))\} \in \mathcal{U}$, тј. $R^{\mathbf{M}^*}(\langle g_1\rangle, \ldots, \langle g_m\rangle)$. Аналогно се доказује да из $R^{\mathbf{M}^*}(\langle g_1\rangle, \ldots, \langle g_m\rangle)$ следи $R^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle)$.

Докажимо једнакост из 2. Ако $n \in X_1 \cap \cdots \cap X_m$, онда је $f_1(n) = g_1(n)$, $\ldots$, $f_m(n) = g_m(n)$, па је и $F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n)) = F^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))$. Дакле,

$$X_1 \cap \cdots \cap X_m \subseteq \{n \in \mathbb{N} \mid F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n)) = F^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))\},$$

одакле следи да

$$\{n \in \mathbb{N} \mid F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n)) = F^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))\} \in \mathcal{U},$$

тј. $\langle F^{\mathbf{M}_n}(f_1(n), \ldots, f_m(n))\rangle = \langle F^{\mathbf{M}_n}(g_1(n), \ldots, g_m(n))\rangle$. Дакле,

$$F^{\mathbf{M}^*}(\langle f_1\rangle, \ldots, \langle f_m\rangle) = F^{\mathbf{M}^*}(\langle g_1\rangle, \ldots, \langle g_m\rangle).$$

□

Конструисани модел $\mathbf{M}^*$ назива се *ултрапроизвод* модела $\mathbf{M}_n$, $n \in \mathbb{N}$. Остаје још да се покаже да овај модел задовољава жељену теорију. То ће бити једноставна последица следећег тврђења познатог као Лошова лема.

Лема 7. *1. За сваки терм $t \in \mathrm{Term}_{\mathcal{L}}$ и све $f_1, \ldots, f_k \in M$, при чему је $k = |V(t)|$, важи:*

$$t^{\mathbf{M}^*}[\langle f_1\rangle, \ldots, \langle f_k\rangle] = \langle t^{\mathbf{M}_n}[f_1(n), \ldots, f_k(n)]\rangle.$$

2. За сваку формулу $\alpha \in \mathrm{For}_{\mathcal{L}}$ и све $f_1, \ldots, f_k \in M$, при чему је $k = |\mathrm{Fr}(\alpha)|$, важи:

$$\mathbf{M}^* \models \alpha[\langle f_1\rangle, \ldots, \langle f_k\rangle] \text{ акко } \{n \in \mathbb{N} \mid \mathbf{M}_n \models \alpha[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U}.$$

Доказ. 1. Доказ изводимо индукцијом по сложености израза t.

Ако је t промењљива x, за валуацију $x \mapsto \langle f\rangle \in M^*$, имамо да је $t^{\mathbf{M}^*}[\langle f\rangle] = \langle f\rangle = \langle t^{\mathbf{M}_n}[f(n)]\rangle$, па тврђење очигледно важи. Ако је t симбол константе c, онда је $t^{\mathbf{M}^*} = c^{\mathbf{M}^*} = \langle c^{\mathbf{M}_n}\rangle = \langle t^{\mathbf{M}_n}\rangle$, па и у овом случају важи тврђење.

Претпоставимо да тврђење важи за све изразе сложености мање од n. Нека је t израз сложености n. Тада је t облика $F(t_1,\dots,t_m)$, за неко $F \in \mathrm{Fun}_{\mathcal{L}}$, $\mathrm{ar}(F)=m$, и неке изразе $t_1,\dots,t_m$ сложености мање од n. Нека је $k = |\mathrm{V}(t)|$. Тада је:

$$\begin{aligned}
& t^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle] \\
= \; & F^{\mathbf{M}^*}\left(t_1^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle],\dots,t_m^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle]\right) \\
= \; & F^{\mathbf{M}^*}\left(\langle t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle,\dots,\langle t_m^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle\right) \\
= \; & \left\langle F^{\mathbf{M}_n}\left(t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)],\dots,t_m^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\right)\right\rangle \\
= \; & \langle t^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle
\end{aligned}$$

2. Доказ изводимо индукцијом по сложености формуле φ.

Ако је α атомична формула облика $t_1 = t_2$, $t_1, t_2 \in \mathrm{Term}_{\mathcal{L}}$:

$$\mathbf{M}^* \models t_1 = t_2[\langle f_1\rangle,\dots,\langle f_k\rangle]$$

акко $t_1^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle] = t_2^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle]$
[према дефиницији релације задовољења]
акко $\langle t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle = \langle t_2^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle$
[према тврђењу под 1]
акко $\{n \in \mathbb{N} \mid t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)] = t_2^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\} \in \mathcal{U}$
[према дефиницији релације еквиваленције]
акко $\{n \in \mathbb{N} \mid \mathbf{M}_n \models t_1 = t_2[f_1(n),\dots,f_k(n)]\} \in \mathcal{U}$
[према дефиницији релације задовољења].

Ако је α атомична формула облика $R(t_1,\dots,t_m)$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $\mathrm{ar}(R) = m$, $t_1,\dots,t_m \in \mathrm{Term}_{\mathcal{L}}$:

$$\mathbf{M}^* \models R(t_1,\dots,t_m)[\langle f_1\rangle,\dots,\langle f_k\rangle]$$

акко $R^{\mathbf{M}^*}\left(t_1^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle],\dots,t_m^{\mathbf{M}^*}[\langle f_1\rangle,\dots,\langle f_k\rangle]\right)$
[према дефиницији релације задовољења]
акко $R^{\mathbf{M}^*}\left(\langle t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle,\dots,\langle t_m^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\rangle\right)$
[према тврђењу под 1]
акко $\{n \in \mathbb{N} \mid R^{\mathbf{M}_n}\left(t_1^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)],\dots,t_m^{\mathbf{M}_n}[f_1(n),\dots,f_k(n)]\right)\} \in \mathcal{U}$
[према дефиницији релације $R^{\mathbf{M}^*}$]
акко $\{n \in \mathbb{N} \mid \mathbf{M}_n \models R(t_1,\dots,t_m)[f_1(n),\dots,f_k(n)]\} \in \mathcal{U}$
[према дефиницији релације задовољења].

Ако је α облика $\neg\theta$, онда

$$\begin{array}{ll}
& \mathbf{M}^* \models \neg\theta[\langle f_1\rangle, \ldots, \langle f_k\rangle] \\
\text{акко } \mathbf{M}^* \not\models \theta[\langle f_1\rangle, \ldots, \langle f_k\rangle] & \text{[према дефиницији релације задовољења]} \\
\text{акко } \{n \in \mathbb{N} \mid \mathbf{M}_n \models \theta[f_1(n), \ldots, f_k(n)]\} \notin \mathcal{U} & \\
& \text{[према индуктивној претпоставци]} \\
\text{акко } \{n \in \mathbb{N} \mid \mathbf{M}_n \not\models \theta[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} & [X \notin \mathcal{U} \text{ акко } X^c \in \mathcal{U}] \\
\text{акко } \{n \in \mathbb{N} \mid \mathbf{M}_n \models \neg\theta[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} & \\
& \text{[према дефиницији релације задовољења].}
\end{array}$$

Ако је α облика $\varphi \wedge \psi$, онда

$$\begin{array}{ll}
& \mathbf{M}^* \models \varphi \wedge \psi[\langle f_1\rangle, \ldots, \langle f_k\rangle] \\
\text{акко} & \mathbf{M}^* \models \varphi[\langle f_1\rangle, \ldots, \langle f_k\rangle] \text{ и } \mathbf{M}^* \models \psi[\langle f_1\rangle, \ldots, \langle f_k\rangle] \\
& \qquad \text{[према дефиницији релације задовољења]} \\
\text{акко} & \{n \in \mathbb{N} \mid \mathbf{M}_n \models \varphi[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} \\
& \qquad \text{и } \{n \in \mathbb{N} \mid \mathbf{M}_n \models \psi[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} \\
& \qquad \text{[према индуктивној претпоставци]} \\
\text{акко} & \{n \in \mathbb{N} \mid \mathbf{M}_n \models \varphi[f_1(n), \ldots, f_k(n)]\} \cap \\
& \qquad \cap \{n \in \mathbb{N} \mid \mathbf{M}_n \models \psi[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} \\
& \qquad [X \cap Y \in \mathcal{U} \text{ акко } X \in \mathcal{U} \text{ и } Y \in \mathcal{U}] \\
\text{акко} & \{n \in \mathbb{N} \mid \mathbf{M}_n \models \varphi[f_1(n), \ldots, f_k(n)] \text{ и } \mathbf{M}_n \models \psi[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} \\
& \qquad \text{[према дефиницији пресека два скупа]} \\
\text{акко} & \{n \in \mathbb{N} \mid \mathbf{M}_n \models \varphi \wedge \psi[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U} \\
& \qquad \text{[према дефиницији релације задовољења].}
\end{array}$$

Нека је α облика $\exists x\theta(x, x_1, \ldots, x_k)$.

Претпоставимо прво да $\mathbf{M}^* \models \exists x\theta[\langle f_1\rangle, \ldots, \langle f_k\rangle]$. Тада постоји $f \in M$, такав да $\mathbf{M}^* \models \theta[\langle f\rangle, \langle f_1\rangle, \ldots, \langle f_k\rangle]$, па према индуктивној претпоставци: $\{n \in \mathbb{N} \mid \mathbf{M}_n \models \theta[f(n), f_1(n), \ldots, f_k(n)]\} \in \mathcal{U}$, одакле следи и

$$\{n \in \mathbb{N} \mid \mathbf{M}_n \models \exists x\theta[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U}.$$

Докажимо и обрнуто. Нека је $X = \{n \in \mathbb{N} \mid \mathbf{M}_n \models \exists x\theta[f_1(n), \ldots, f_k(n)]\} \in \mathcal{U}$. За свако $n \in X$, нека је a_n елемент из M_n такав да $\mathbf{M}_n \models \theta[a_n, f_1(n), \ldots, f_k(n)]$. Дефинишимо низ $f \in M$ на следећи начин:

$$f(n) = \begin{cases} a_n, & n \in X, \\ \text{било који елемент из } M_n, & n \notin X. \end{cases}$$

Тада $\{n \in \mathbb{N} \mid \mathbf{M}_n \models \theta[f(n), f_1(n), \ldots, f_k(n)]\} \in \mathcal{U}$, па према индуктивној претпоставци $\mathbf{M}^* \models \theta[\langle f \rangle, \langle f_1 \rangle, \ldots, \langle f_k \rangle]$, а тиме и $\mathbf{M}^* \models \exists x \theta[\langle f_1 \rangle, \ldots, \langle f_k \rangle]$. $\square$

Теорема компактности пружа велике могућности примене у различитим областима математике, у шта смо се уверили још у случају исказне логике. Поред тога, доказ који смо навели описује и једну веома значајну конструкцију којом се изграђују важне структуре првог реда.

Пример 17. Ако нека теорија T има моделе произвољно велике коначне кардиналности, доказаћемо да тада мора имати и бесконачан модел.

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 $\mathbf{M}^* \models \gamma_{n+1}$. $\triangleright$

У наставку наводимо неколико примена које представљају полазиште неких важних и узбудљивих области математичке логике, али и математике уопште.

Пример 18. 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 $\mathcal{L}_{\mathrm{A}} = \{\leqslant, s, +, \cdot, 0\}$[44] 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.

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[45]. 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

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

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

[45] Наведени терми се називају *нумерали*.

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: $\overline{n_1} < c$, $\overline{n_2} < c$, $\ldots$, $\overline{n_k} < c$, 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 $f : N \xrightarrow[\text{na}]{\text{1-1}} M$, 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 $\mathbf{N}$.

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

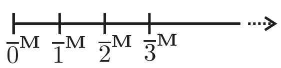
$$\overline{0} < \overline{1} \wedge \forall x(\overline{0} < x \Rightarrow (\overline{1} = x \vee \overline{1} < x))$$

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

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

$$\vdots$$

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:

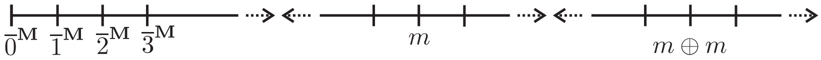


Међутим, скуп M садржи и елемент m који се налази „иза“ (у смислу уређења $\preccurlyeq$) свих елемената $\overline{0}^{\mathbf{M}}, \overline{1}^{\mathbf{M}}, \overline{2}^{\mathbf{M}}, \ldots$ Како стандардни модел $\mathbf{N}$ задовољава реченицу

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

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. Заинтересованог читаоца упућујемо на ??. $\triangleright$

Пример 19. 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.). У наредном примеру, детаљније ћемо проучити једно неархимедско поље које има важну улогу у нестандардној анализи. $\triangleright$

Пример 20. Сетимо се поља које смо добили у примеру 16. Да подсетимо, тада смо полазећи од неког неглавног ултрафилтера $\mathcal{U}$, конструисали уређено поље чији је домен $\mathbb{Q}^{\mathbb{N}}/\mathcal{U}$, где је $\mathbb{Q}^{\mathbb{N}}$ скуп свих низова рационалних бројева. Ово поље се означава са ${}^*\mathbb{Q}$ и назива се *поље хиперрационалних бројева*. Очигледно је да ${}^*\mathbb{Q}$ садржи копију рационалних бројева, јер се сваки $q \in \mathbb{Q}$ може идентификовати са $\langle q, q, q, \ldots \rangle$. Као што смо видели у поменутом примеру, поље ${}^*\mathbb{Q}$ има још доста елемената. Већ смо истакли елемент $\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots \rangle$, који ћемо сада означити са ε, и видели да важи[46]: $0 \leqslant \varepsilon < \dfrac{1}{n}$, за било који природан број n. Елемент $x \in {}^*\mathbb{Q}$, такав да је

$$|x| < \frac{1}{n}, \text{ за било који природан број } n,$$

називамо *инфинитезималом*. Дакле, ε је инфинитезимала различита од нуле. Будући да ${}^*\mathbb{Q}$ има инфинитезимале које нису једнаке нули, закључујемо да ово уређено поље није архимедско. Поред тога, ${}^*\mathbb{Q}$ има и тзв. *бесконачне елементе*: како је ε инфинитезимала различита од нуле, онда је $\varepsilon^{-1} = \langle 2, 3, 4, 5, \ldots \rangle$ бесконачно велики елемент, што значи да је већи од сваког $n \in \mathbf{N}$. Коначни елементи су они који нису бесконачни, тј. они који су мањи од неког природног броја n. На пример, инфинитезимале су коначни елементи. Приликом проучавања неархимедских поља, од посебног значаја је релација *бесконачно блиско* дефинисана на следећи начин: $x \approx y$ акко је $x - y$

[46] $\langle 0, 0, 0, 0, \ldots \rangle < \langle \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots \rangle < \langle \frac{1}{n}, \frac{1}{n}, \frac{1}{n}, \frac{1}{n}, \ldots \rangle$

инфинитезимала. Није тешко показати да је $\approx$ релација еквиваленције на ${}^*\mathbb{Q}$. Занимљиво је да класе еквиваленције у односу на $\approx$ које одређују *коначни елеменати*, заједно са уређењем и операцијама дефинисаним на одговарајући начин, образују заправо архимедско поље изоморфно уређеном пољу реалних бројева. Дакле, описану конструкцију можемо схватити као још једну изградњу структуре реалних бројева (поред познатих конструкција заснованих на Кошијевим низовима, Дедекиндовим пресецима, или Вајерштрасовим редовима).

Аналогно пољу $\mathbb{Q}^{\mathbb{N}}/\mathcal{U}$, изграђује се и *поље хиперреалних бројева* $\mathbb{R}^{\mathbb{N}}/\mathcal{U}$. У овом веома „богатом“ пољу могу се проучавати разни концепти класичне анализе чиме се ми нећемо бавити. Упућујемо заинтересованог читаоца на ??. $\triangleright$

ПРИМЕР 21. **Ремзијева теорема.** За било које $k \geqslant 1$, нека је $[S]^k = \{X \subseteq S \mid |X| = k\}$ скуп свих коначних подскупова од S који имају k елемената и које ћемо краће звати k-подскуповима. Сваку функцију $\pi : [S]^k \overset{\text{na}}{\to} \{1, \ldots, r\}$, за неко $r \geqslant 1$, називаћемо *бојењем k-подскупова од S у r боја*. Скуп $H \subseteq S$ је *хомоген* за бојење π ако су сви елементи из $[H]^k$ обојени истом бојом, тј. ако је $\pi \restriction [H]^k$ константна функција.

Бесконачна верзија Ремзијеве теореме. Нека су k и r позитивни природни бројеви и S бесконачан подскуп од $\mathbb{N}$. Ако $\pi : [S]^k \overset{\text{na}}{\to} \{1, \ldots, r\}$, онда постоји бесконачан скуп $H \subseteq \mathbb{N}$ хомоген за π.

ДОКАЗ. Теорема тривијално важи ако је $r = 1$. Претпоставимо зато да је $r > 1$. Доказ изводимо индукцијом по k.

Ако је $k = 1$ ($[S]^1 = S$), теорема важи на основу једне варијанте Дирихлеовог принципа: ако је сваки елемент из S обојен једном од коначно много боја, онда мора постојати боја којом је обојено бесконачно много елемената из S, јер S има бесконачно много елемената, а боја је коначно много.

Да би индуктивни корак био јаснији, размотрићемо и случај $k = 2$. Дакле, нека $\pi : [S]^2 \overset{\text{na}}{\to} \{1, \ldots, r\}$. Означимо са x_0 минимални елемент скупа S и посматрајмо све парове $\{x_0, x\}$, $x \in S$. Сви овакви парови обојени су једном од r боја, па постоји боја r_0, $1 \leqslant r_0 \leqslant r$, којом је обојено бесконачно много њих. Овај закључак је заправо позивање на случај $k = 1$. Посматрајмо сада скуп $S_0 = \{x \in S \setminus \{x_0\} \mid \pi(\{x_0, x\}) = r_0\}$. Нека је $x_1 = \min S_0$. Изводимо нови закључак: постоји боја r_1, $1 \leqslant r_1 \leqslant r$, којом је обојено бесконачно много парова који садрже x_1. Уочавамо дакле нови бесконачан скуп $S_1 = \{x \in S_0 \setminus \{x_1\} \mid \pi(\{x_1, x\}) = r_1\}$ и његов најмањи елемент $x_2 = \min S_1$, итд. Настављајући овај поступак, добијамо низ боја $r_0, r_1, r_2 \ldots$ и опадајући низ бесконачних скупова $S_0 \supset S_1 \supset S_2 \supset \ldots$ таквих да за свако $i \geqslant 0$, S_{i+1} садржи парове чији је један члан $x_{i+1} = \min S_i$ и који су сви обојени бојом r_{i+1}. Како је $r_0, r_1, r_2 \ldots$ низ бројева из $\{1, \ldots, r\}$, према већ поменутој варијанти Дирихлеовог принципа, постоји бесконачан скуп индекса $I \subseteq \mathbb{N}$, такав да су сви r_i, $i \in I$, једнаки неком r', $1 \leqslant r' \leqslant r$. Дефинишимо најзад и жељени хомогени скуп: $H = \{x_i \mid i \in I\}$. Није тешко показати да је овај скуп заиста хомоген за π. Нека је $x_i \neq x_j$, $i, j \in I$. Без губљења општости можемо претпоставити да је $x_i < x_j$. Сви парови из S_i садрже x_i и обојени су бојом $r_i = r'$. Међу њима мора се налазити и пар $\{x_i, x_j\}$, јер је $S_i \supset S_j \ni x_j$. Дакле, сви парови из H обојени су бојом r'.

Претпоставимо да је теорема тачна за неко $k \geqslant 2$. Нека $\pi : [S]^{k+1} \overset{\text{na}}{\to} \{1, \ldots, r\}$. Конструишемо индуктивно низ непразних подскупова $S_0, S_1, S_2, \ldots$ од S, низ функција $\pi_0, \pi_1, \pi_2, \ldots$ и низ $r_1, r_2, \ldots$ елемената скупа $\{1, \ldots, r\}$, на следећи начин. Нека је $S_0 = S$ и $\pi_0 = \pi$. Ако смо дефинисали скупове $S_0, \ldots, S_n$, а ако је $x_{n+1} = \min S_n$, функцију $\pi_{n+1} : [S_n \setminus \{x_{n+1}\}]^k \to \{1, \ldots, r\}$ дефинишемо са:

$$\pi_{n+1}(\{y_1, \ldots, y_k\}) = \pi(\{x_{n+1}, y_1, \ldots, y_k\}),\ \{y_1, \ldots, y_k\} \in [S_n \setminus \{x_{n+1}\}]^k.$$

Према индуктивној хипотези, постоји бесконачан скуп $S_{n+1} \subseteq S_n \setminus \{x_{n+1}\}$ хомоген за π_{n+1}, тј. за неко r_{n+1}, $1 \leqslant r_{n+1} \leqslant r$, рестрикција $\pi_{n+1} \restriction [X_{n+1}]^k$ је константна функција и свим елементима из $[X_{n+1}]^k$ додељује вредност r_{n+1}.

Како је $r_1, r_2 \ldots$ низ бројева из $\{1, \ldots, r\}$, постоји бексоначан скуп индекса $I \subseteq \mathbb{N}$, такав да су сви r_i, $i \in I$, једнаки неком r', $1 \leqslant r' \leqslant r$. Тада је скуп $H = \{x_i \mid i \in I\}$ хомоген за π. □

Приметимо да се у формулацији претходне теореме може претпоставити да је S било који бесконачан скуп.

Да бисмо једноставније формулисали коначну варијанту Ремзијеве теореме, за позитивне природне бројеве m и r, нека је $\mathbf{m} = \{1, \ldots, m\}$ и $\mathbf{r} = \{1, \ldots, r\}$.

Коначна верзија Ремзијеве теореме. Нека су r, k и n позитивни природни бројеви и $n \geqslant k$. Тада постоји природан број $m \geqslant n$, такав да за свако бојење $\pi : [\mathbf{m}]^k \overset{\text{na}}{\to} \mathbf{r}$ постоји скуп $H \subseteq \mathbf{m}$, $|H| = n$, који је хомоген за π.

Доказ. Претпоставимо супротно, тј. да за свако $m \geqslant n$, постоји бојење $\pi : [\mathbf{m}]^k \overset{\text{na}}{\to} \mathbf{r}$ за које не постоји скуп $H \subseteq \mathbf{m}$, $|H| = n$, хомоген за π.

Формираћемо једну теорију језика $\mathcal{L} = \{B_1, \ldots, B_r\}$, који садржи r релацијских симбола дужине k, $\mathrm{ar}(B_i) = k$, $1 \leqslant i \leqslant r$. Нека је α конјункција следеће три реченице:

– $\forall x_1 \cdots \forall x_k \left(B_i(x_1, \ldots, x_k) \Rightarrow \bigwedge\limits_{1 \leqslant i < j \leqslant k} x_i \neq x_j \right)$,

– $\forall x_1 \cdots \forall x_k \left(B_i(x_1, \ldots, x_k) \Rightarrow \bigwedge\limits_{p \in P_k} B_i(x_{p(1)}, \ldots, x_{p(k)}) \right)$, где је P_k скуп свих пермутација скупа $\{1, \ldots, k\}$,

– $\forall x_1 \cdots \forall x_k \left(\bigwedge\limits_{1 \leqslant i < j \leqslant k} x_i \neq x_j \Rightarrow \bigvee\limits_{1 \leqslant i \leqslant r} B_i(x_1, \ldots, x_k) \right)$.

Ако је $\beta_i(x_1, \ldots, x_n)$ формула $\bigvee\limits_{1 \leqslant j_1 < \ldots < j_k \leqslant n} B_i(x_{j_1}, \ldots, x_{j_k})$, означимо са β реченицу

$$\forall x_1 \cdots \forall x_n \left(\bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j \Rightarrow \bigvee_{1 \leqslant i < j \leqslant r} (\beta_i(x_1, \ldots, x_n) \wedge \beta_j(x_1, \ldots, x_n)) \right).$$

Најзад, нека је γ_ℓ, $\ell \geqslant 1$, реченица $\exists x_1 \cdots \exists x_\ell \bigwedge\limits_{1 \leqslant i < j \leqslant \ell} x_i \neq x_j$.

Докажимо да теорија $T = \{\alpha, \beta, \gamma_1, \gamma_2, \gamma_3, \ldots\}$ има модел. Нека је T_0 произвољан коначан подскуп од T. Тада постоји природан број $m \geqslant n$ такав да је $T_0 \subseteq T_0' = \{\alpha, \beta, \gamma_1, \ldots, \gamma_m\}$. Према нашој полазној претпоставци, постоји бојење $\pi : [\mathbf{m}]^k \overset{\text{na}}{\to} \mathbf{r}$ за које не постоји скуп $H \subseteq \mathbf{m}$, $|H| = n$, хомоген за π. За $i \in \{1, \ldots, r\}$, нека $B_i^{\mathbf{m}} \subseteq \mathbf{m}^k$ садржи само уређене k-торке међусобно различитих елемената $x_1, \ldots, x_k \in \mathbf{m}$ такве да је $\pi(\{x_1, \ldots, x_k\}) = i$. Тада је $(\mathbf{m}, B_1^{\mathbf{m}}, \ldots, B_r^{\mathbf{m}}) \models T_0'$. Према теореми компактности, и скуп T има модел. Нека је $\mathbf{M} = (M, B_1^{\mathbf{M}}, \ldots, B_r^{\mathbf{M}}) \models T$. Приметимо најпре да скуп

M мора бити бесконачан. Дефинишимо функцију $\pi : [M]^k \to \mathbf{r}$ на следећи начин:

$$\pi(\{x_1, \dots, x_k\}) = i \text{ акко } B_i^{\mathbf{M}}(x_1, \dots, x_k), \text{ за међусобно различите } x_1, \dots, x_k \in M.$$

Читаоцима препуштамо проверу да је π добро дефинисана на-функција. Према бесконачној варијанти Ремзијеве теореме постоји бесконачан скуп $H \subseteq M$ који је хомоген за π. Свакако из овог скупа можемо издвојити n међусобно различитих елемената $h_1, \dots, h_n$ од којих се не могу формирати два скупа са по k елемената који ће бити различитих боја, што противречи чињеници да $\mathbf{M} \models \beta$. ▷

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 15 (на страни 115). Тада смо доказали 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. Потпуно исту ситуацију смо имали на пример у првом поглављу када смо доказивали леме 1 и 2 (на странама 14 и 15). Списак правила која смо користили за извођење секвената у исказној логици, проширујемо новим правилима која се односе на квантификаторе и знак једнакости. Овога пута синтаксна последица јесте релација којом се успоставља однос између скупа формула логике првог реда Γ и неке формуле α.

Дефиниција 13. *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

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

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 14. *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 22. $\vdash \forall x\alpha \vee \forall x\beta \Rightarrow \forall x(\alpha \vee \beta)$

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 $(\Rightarrow_{\mathrm{U}})$

$\triangleright$

Пример 23. $\vdash \exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$

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 $(\Rightarrow_{\mathrm{U}})$

$\triangleright$

Пример 24. $\vdash \forall x_1 \forall x_2(x_1 = x_2 \Rightarrow x_2 = x_1)$

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)

$\triangleright$

Пример 25. $\vdash \forall x_1 \forall x_2 \forall x_3(x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$

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 $(=\mathrm{E})$
$\alpha[x/x_3]$ 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)

$\triangleright$

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 8. $$\frac{}{\Gamma, r = s \vdash t[x/r] = t[x/s]}\ (=_c)$$

Доказ.

1. $\Gamma, r = s \vdash r = s$ (ax)
2. $\Gamma, r = s \vdash t = t$ $(=_U)$
3. $\Gamma, r = s \vdash t[x/r] = t[x/s]$ из 1, 2 према $(=_E)$.

□

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 26. 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 $(\forall_E)$, односно $\mathrm{Inv}_f \vdash (f(x) = y)[x/f(y)]$
3. $\mathrm{Inv}_f \vdash \exists x (f(x) = y)$ из 2 према $(\exists_U)$
4. $\mathrm{Inv}_f \vdash \forall y \exists x (f(x) = y)$ из 3 према $(\forall_U)$, односно $\mathrm{Inv}_f \vdash \mathrm{Sur}_f$
5. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(x) = f(y)$ (ax)
6. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(x)) = f(f(y))$ $(=_c)$
7. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(x)) = x$ из 1 према $(\forall_E)$ и (slab)
8. $\mathrm{Inv}_f, f(x) = f(y) \vdash f(f(y)) = y$ из 1 према $(\forall_E)$ и (slab)
9. $\mathrm{Inv}_f, f(x) = f(y) \vdash x = y$ из 6, 7, 8 према $2 \times (=_E)$
10. $\mathrm{Inv}_f \vdash \forall x \forall y (f(x) = f(y) \Rightarrow x = y)$ из 9 према $(\Rightarrow_U) + 2 \times (\forall_U)$, односно $\mathrm{Inv}_f \vdash \mathrm{Inj}_f$
11. $\mathrm{Inv}_f \vdash \mathrm{Bij}_f$ из 4, 10 према $(\wedge_U)$

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 $(\wedge_U)$.

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 $(\exists_{\mathrm{E}}), (\mathrm{ax})$. Једнакост (iii) је последица претпоставке $f(x) = f(y)$ $(=_{\mathrm{c}})$.
f је на-функција? Ако је y произвољно, доказаћемо да постоји x тако да је $f(x) = y$ $(\forall_{\mathrm{U}})$. Нека је $x = f(y)$ $(\exists_{\mathrm{U}})$. Пошто је f инволуција, добијамо да је $f(f(y)) = y$, $(\exists_{\mathrm{E}}), (\mathrm{ax})$. $\triangleright$

ПРИМЕР 27. **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:

$$\frac{\Gamma, \varphi, \psi \vdash \theta}{\Gamma, \varphi \wedge \psi \vdash \theta}(\wedge_{\mathrm{L}}) \quad \frac{\Gamma, \varphi, \psi \vdash \theta}{\Gamma, \varphi, \varphi \Rightarrow \psi \vdash \theta}(\Rightarrow_{\mathrm{L}}) \quad \frac{\Gamma, \forall x\varphi, \varphi[x/t] \vdash \theta}{\Gamma, \forall x\varphi \vdash \theta}(\forall_{\mathrm{L}})$$

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

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 $(\Rightarrow_{\mathrm{U}})$, $(\wedge_{\mathrm{L}})$ и $(\perp_{\mathrm{c}})$, 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 $\overline{\varepsilon}$ терм $|\ell - \ell'|/2$. Тада према правилу $(\forall_{\mathrm{L}})$ примењеном три пута, претходни секвент сводимо на

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

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

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

   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:

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

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

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

6. Активирањем формуле Lema_3 при супституцијама $[x/|\ell - \ell'|]$, $[y/f(z)]$, $[z_1/\ell]$ и $[z_2/\ell']$ (подсећамо да је $\overline{\varepsilon}$ 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. $\triangleright$

Пример 28. 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. $\triangle cab = \triangle bac \Rightarrow \angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$,

активирањем γ_4 правилом $(\forall_{\mathrm{E}})$ при $[x/c]$, $[y/a]$, $[z/b]$, $[u/b]$, $[v/a]$, $[w/c]$

14. $\angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$ — из 12, 13 према $(\Rightarrow_{\mathrm{E}})$
15. $\angle abc = \angle acb$ — из 14 према $(\wedge^{\mathrm{l}}_{\mathrm{E}})$ и $(\wedge^{\mathrm{d}}_{\mathrm{E}})$.

$\triangleright$

Пример 29. 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[47]:

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

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 $(=_{\mathrm{T}})$

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

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 $T_{\mathrm{GR}} \vdash \forall x \forall y((x * y) * y^{-1} = x)$. $\triangleright$

Теорема потпуности

Сва разматрања о теореми потпуности исказне логике (страна 74) односе се и на логику првог реда, па их овом приликом нећемо понављати. Чињеницу да и за логику првог реда важи

$$\Gamma \vdash \alpha \text{ акко } \Gamma \models \alpha$$

изводимо из *теореме сагласносте* и *теореме о постојању модела*.

Теорема 2. [***Теорема сагласности***] *Ако* $\Gamma \vdash \alpha$*, онда* $\Gamma \models \alpha$.

Доказ. Доказ наведене теореме аналоган је доказу теореме сагласности за исказну логику (теорема 5, на страни 77). Зато ћемо изоставити сва разматрања која се односе на правила која смо користили и у исказној логици, и посветити се само правилима која се односе на кватификаторе и једнакост. Подсећамо да доказ спроводимо индукцијом по дужини извођења за $\Gamma \vdash \alpha$.

Ако је дужина извођења за $\Gamma \vdash \alpha$ једнака 1, онда је овај секвент добијен или правилом (ax) или правилом $(=_{\mathrm{U}})$. И у једном и другом случају једноставно изводимо закључак да је $\Gamma \models \alpha$.

Претпоставимо да је тврђење тачно за све секвенте чија је дужина извођења мања од неког n, $n > 1$ и да је дужина извођења секвента $\Gamma \vdash \alpha$ једнака n. Нека је $\mathbf{M}$ модел одговарајућег језика и μ валуација променљивих у M такви да је $\mathbf{M}, \mu \models \Gamma$. Разликоваћемо неколико случајева у зависности од тога којим правилом је добијен последњи секвент $\Gamma \vdash \alpha$. Као што смо већ истакли, разматраћемо само случајеве када је последњи секвент $\Gamma \vdash \alpha$ добијен неким од правила која се односе на кватификаторе и једнакост.

Ако је $\Gamma \vdash \alpha$ добијено применом правила $(\forall_{\mathrm{U}})$, онда је формула α облика $\forall x \theta$, где је x променљива која није слободна у формулама из Γ. Тада, за било које $a \in M$ важи $\mathbf{M}, \mu(x/a) \models \Gamma$. Уоченом секвенту претходи секвент $\Gamma \vdash \theta$, па према индуктивној претпоставци следи да за свако $a \in M$ важи $\mathbf{M}, \mu(x/a) \models \theta$, одакле закључујемо да $\mathbf{M}, \mu \models \forall x \theta$.

Ако је $\Gamma \vdash \alpha$ добијено применом правила $(\forall_{\mathrm{E}})$, онда је формула α облика $\theta[x/t]$, при чему уоченом секвенту претходи секвент $\Gamma \vdash \forall x \theta$. Према индуктивној претпоставци следи да за свако $a \in M$ важи $\mathbf{M}, \mu(x/a) \models \theta$. Специјално, важи и $\mathbf{M}, \mu(x/t^{\mathbf{M}}[\mu]) \models \theta$, одакле следи $\mathbf{M}, \mu \models \theta[x/t]$.

Ако је $\Gamma \vdash \alpha$ добијено применом правила $(\exists_{\mathrm{U}})$, онда је формула α облика $\exists x\theta$, при чему уоченом секвенту претходи секвент $\Gamma \vdash \theta[x/t]$. Према индуктивној претпоставци следи да $\mathbf{M}, \mu \models \theta[x/t]$, тј. $\mathbf{M}, \mu(x/t^{\mathbf{M}}[\mu]) \models \theta$. Одавде директно добијамо да $\mathbf{M}, \mu \models \exists x\theta$.

Ако је $\Gamma \vdash \alpha$ добијено применом правила $(\exists_{\mathrm{E}})$, онда овом секвенту претходе секвенти $\Gamma \vdash \exists x\theta$ и $\Gamma, \theta \vdash \alpha$, при чему је x променљива која није слобдна у формулама скупа $\Gamma \cup \{\alpha\}$. Према индуктивној претпоставци имамо да $\mathbf{M}, \mu \models \exists x\theta$, тј. за неко $a \in M$ важи $\mathbf{M}, \mu(x/a) \models \theta$. Пошто се x не појављује слободно у формулама скупа Γ, закључујемо и да је $\mathbf{M}, \mu(x/a) \models \Gamma$. Позивајући се још једном на индуктивну претпоставку, добијамо да $\mathbf{M}, \mu(x/a) \models \alpha$. Како x није слободна променљива формуле α, следи да $\mathbf{M}, \mu \models \alpha$.

Ако је $\Gamma \vdash \alpha$ добијено применом правила $(=_{\mathrm{E}})$, онда је формула α облика $\theta[x/u]$, и уоченом секвенту претходе секвенти $\Gamma \vdash \theta[x/t]$ и $\Gamma \vdash t = u$. Према индуктивној претпоставци следи $\mathbf{M}, \mu \models \theta[x/t]$ и $\mathbf{M}, \mu \models t = u$, односно $\mathbf{M}, \mu(x/t^{\mathbf{M}}[\mu]) \models \theta$ и $t^{\mathbf{M}}[\mu] = u^{\mathbf{M}}[\mu]$. Одавде непосредно добијамо да $\mathbf{M}, \mu(x/u^{\mathbf{M}}[\mu]) \models \theta$, тј. $\mathbf{M}, \mu \models \theta[x/u]$. $\square$

Пре него што докажемо да важи и обрат претходне теореме, наводимо једну „техничку“ лему познату под називом *лема о новој константи*.

Лема 9. *Нека је c симбол константе који се не појављује у формулама скупа $\Gamma \cup \{\alpha\}$. Ако је $\Gamma \vdash \alpha[x/c]$, онда је $\Gamma \vdash \forall x\alpha$.*

Скица доказа. Нека је $\Gamma[x/c] = \{\gamma[x/c] \mid \gamma \in \Gamma\}$. Најпре треба уочити да важи једно опште тврђење:

$(*)$ из $\Gamma[x/c] \vdash \alpha[x/c]$, следи да $\Gamma[x/t] \vdash \alpha[x/t]$, за било који терм t.

Тврђење $(*)$ се доказује индукцијом по дужини извођења секвента $\Gamma[x/c] \vdash \alpha[x/c]$ (при чему свуда c замењујемо са t).

Претпоставимо да се симбол константе c не појављује у формулама скупа $\Gamma \cup \{\alpha\}$, и да је $\Gamma \vdash \alpha[x/c]$. Може се претпоставити и да је x променљива која није слободна у формулама скупа Γ. На основу тврђења $(*)$ једноставно добијамо (када за t узмемо x) и да је $\Gamma \vdash \alpha$. Како x није слободна у формулама из Γ, применом правила $(\forall_{\mathrm{U}})$, добијамо $\Gamma \vdash \forall x\alpha$. $\square$

Теорема 3. *Свака непротивречна теорија има модел.*

Идеја доказа. Доказ изводимо *Хенкиновом методом константи*. Основна идеја је да проширимо језик тако да добијемо богат скуп израза без промењивих довољан да се од њега може конструисати жељени модел. Као у случају исказне логике, и полазну теорију ћемо проширити, колико год је могуће, тако да из тог проширења можемо „прочитати“ модел. Нека је T непротивречна теорија језика $\mathcal{L}$. Најпре се конструише нова теорија $T^* \supseteq T$ у проширењу $\mathcal{L}^* \supseteq \mathcal{L}$, тако да је:

- $T \subseteq T^*$,
- T^* је комплетна теорија, тј. за сваку реченицу φ, или $T^* \vdash \varphi$ или $T^* \vdash \neg\varphi$,
- за сваку формулу $\varphi(x)$ језика $\mathcal{L}^*$ која има једну слободну променљиву, постоји симбол константе (означимо га са) c_φ језика $\mathcal{L}^*$ такав да $T^* \vdash \exists x\varphi(x) \Rightarrow \varphi[x/c_\varphi]$.

Након тога, дефинише се модел $\mathbf{M}$ теорије T^*.

- Домен модела је скуп $M = E/\sim$, где је E скуп свих израза језика $\mathcal{L}^*$ који не садрже променљиве, а $\sim$ релација еквиваленције на E дефинисана са: $t_1 \sim t_2$ акко $T^* \vdash t_1 = t_2$. Означимо са $\langle t \rangle$ класу еквиваленције одређену елементом t.
- Ако $R \in \mathrm{Rel}_{\mathcal{L}^*}$, $\mathrm{ar}(R) = n$, онда је:
$$R^{\mathbf{M}}(\langle t_1 \rangle, \ldots, \langle t_n \rangle) \text{ акко } T^* \vdash R(t_1, \ldots, t_n).$$
- Ако $F \in \mathrm{Fun}_{\mathcal{L}^*}$, $\mathrm{ar}(F) = n$, онда је $F^{\mathbf{M}}(\langle t_1 \rangle, \ldots, \langle t_n \rangle) = \langle F(t_1, \ldots, t_n) \rangle$.
- Ако $c \in \mathrm{Const}_{\mathcal{L}^*}$, онда је $c^{\mathbf{M}} = \langle c \rangle$.

Овако дефинисана структура језика $\mathcal{L}^*$ јесте модел теорије T^*, а тиме и модел теорије T.

Доказ. Дефинисаћемо индуктивно низ језика $\mathcal{L}_n$, $n \in \mathbb{N}$ и низ теорија T_n, $n \in \mathbb{N}$ (T_n је теорија језика $\mathcal{L}_n$): $\mathcal{L}_0 = \mathcal{L}$ и $T_0 = T$,

- $\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{c_\varphi \mid \varphi \in \mathrm{For}_{\mathcal{L}_n}, |\mathrm{Fr}(\varphi)| = 1\}$, при чему други скуп представља скуп нових симбола константи којих нема у $\mathcal{L}_n$;
- $T_{n+1} = T_n \cup \{\exists x\varphi(x) \Rightarrow \varphi[x/c_\varphi] \mid \varphi \in \mathrm{For}_{\mathcal{L}_n}, |\mathrm{Fr}(\varphi)| = 1\}$

Нека је $\mathcal{L}^* = \cup_{n\in\mathbb{N}}\mathcal{L}_n$ и $\overline{T} = \cup_{n\in\mathbb{N}}T_n$.

Доказаћемо неколико важних помоћних тврђења.

1. За сваку формулу $\varphi(x) \in \mathrm{For}_{\mathcal{L}^*}$, $x \in Var$, постоји константа $c \in \mathcal{L}^*$, таква да $T \vdash \exists x\varphi(x) \Rightarrow \varphi[x/c]$.

Заиста, ако $\varphi(x) \in \mathrm{For}_{\mathcal{L}^*}$, онда постоји $n \in \mathbb{N}$, такав да $\varphi \in \mathrm{For}_{\mathcal{L}_n}$, па скуп T_{n+1} садржи формулу $\exists x\varphi(x) \Rightarrow \varphi[x/c_\varphi]$, при чему је c_φ одговарајући симбол константе из $\mathcal{L}_{n+1}$. Како је $T_{n+1} \subseteq \overline{T}$ и $\mathcal{L}_{n+1} \subseteq \mathcal{L}^*$, закључујемо да тврђење важи.

2. Скуп $\overline{T}$ је непротивречан.

Довољно је доказати да је за свако $n \in \mathbb{N}$, скуп T_n непротивречан. Доказ да је T_n, $n \in \mathbb{N}$, низ непротивречних теорија, спроводимо математичком индукцијом.

Теорија $T_0 = T$ непротивречна је по претпоставци теореме.

Претпоставимо да је T_n непротивречна теорија за неко $n \in \mathbb{N}$. Да бисмо доказали да је тада и T_{n+1} непротивречна теорија, претпоставићемо супротно: нека је T_{n+1} противречна теорија, тј. $T_{n+1} \vdash \bot$. Тада постоји коначно много формула $\varphi_1(x_1), \ldots, \varphi_k(x_k)$ са једном слободном променљивом записаних на језику $\mathcal{L}_n$, тако да

$$T_n, \exists x_1 \varphi_1(x_1) \Rightarrow \varphi_1[x_1/c_{\varphi_1}], \ldots, \exists x_k \varphi_k(x_k) \Rightarrow \varphi_k[x_k/c_{\varphi_k}] \vdash \bot.$$

Одавде добијамо:

$T_n \vdash \bigwedge_{1 \leqslant i \leqslant k}(\exists x_i \varphi_i(x_i) \Rightarrow \varphi_i[x_i/c_{\varphi_i}]) \Rightarrow \bot$

[Према леми 12 из претходног поглавља (страна 75)]

$T_n \vdash \forall y_1 \cdots \forall y_k \left(\bigwedge_{1 \leqslant i \leqslant k}(\exists x_i \varphi_i(x_i) \Rightarrow \varphi_i[x_i/y_i]) \Rightarrow \bot\right)$

[Према леми 9, јер се константе c_{φ_i} не појављују у реченицама из T_n. Променљиве $y_1, \ldots, y_k$ бирамо тако да се ниједна од њих не појављује слободно у формулама $\varphi_i(x_i)$, $i = 1, \ldots, k$.]

$T_n \vdash \exists y_1 \cdots \exists y_k \bigwedge_{1 \leqslant i \leqslant k}(\exists x_i \varphi_i(x_i) \Rightarrow \varphi_i[x_i/y_i]) \Rightarrow \bot$

[$\vdash \forall y(\varphi \Rightarrow \bot) \Leftrightarrow (\exists y \varphi \Rightarrow \bot)$]

$T_n \vdash \bigwedge_{1 \leqslant i \leqslant k}(\exists x_i \varphi_i(x_i) \Rightarrow \exists y_i \varphi_i[x_i/y_i]) \Rightarrow \bot$

[$\vdash \exists y_1 \exists y_2(\varphi_1(y_1) \wedge \varphi_2(y_2)) \Leftrightarrow \exists y_1 \varphi_1(y_1) \wedge \exists y_2 \varphi_2(y_2)$, и ако y није слободно у φ, онда $\vdash \exists y(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \exists y \psi)$]

$T_n \vdash \bot$.

[$\vdash \exists x_i \varphi_i(x_i) \Rightarrow \exists y_i \varphi_i[x_i/y_i]$ (преименовање везаних променљивих)]

Долазимо до контрадикције са индуктивном претпоставком да је T_n непротивречан скуп. Дакле, T_{n+1} такође је непротивречан.

Приметимо да је језик $\mathcal{L}^*$ пребројив, па је пребројив и скуп реченица на овом језику. Све реченице језика $\mathcal{L}^*$ поређаћемо у низ $\sigma_0, \sigma_1, \sigma_2, \ldots$

Дефинисаћемо индуктивно низ теорија $\overline{T}_n$, $n \in \mathbb{N}$: $\overline{T}_0 = \overline{T}$ и

$$\overline{T}_{n+1} = \begin{cases} T_n \cup \{\sigma_n\}, & T_n, \sigma_n \nvdash \bot, \\ T_n, & T_n, \sigma_n \vdash \bot. \end{cases}$$

Нека је $T^* = \cup_{n \in \mathbb{N}} \overline{T}_n$.

3. Теорија T^* је непротивречна и комплетна.

Доказе непротивречности и комплетности препуштамо читаоцима[48].

Приметимо такође да се у тврђењу **1**, уместо T, може писати и T^*.

Остаје још да конструишемо жељени модел. Нека је M скуп свих затворених израза језика $\mathcal{L}^*$ и $\sim$ бинарна релација скупа M дефинисана са

$$t \sim s \text{ акко } T^* \vdash t = s,\ t, s \in M.$$

4. Релација $\sim$ је релација еквиваленције на E. То се једноставно доказује применом $(=_{\mathrm{U}})$ и секвената изведених у примерима 24 и 25.

Нека је $M^* = E/\sim$. Са $\langle t \rangle$ означавамо класу еквиваленције одређену изразом t. На скупу M^* интерпретирамо језик $\mathcal{L}^*$ на следећи начин:

- ако $R \in \mathrm{Rel}_{\mathcal{L}^*}$, $\mathrm{ar}(R) = n$, онда је:

$$R^{\mathbf{M}^*}(\langle t_1 \rangle, \ldots, \langle t_n \rangle) \text{ акко } T^* \vdash R(t_1, \ldots, t_n);$$

- ако $F \in \mathrm{Fun}_{\mathcal{L}^*}$, $\mathrm{ar}(F) = n$, онда је $F^{\mathbf{M}^*}(\langle t_1 \rangle, \ldots, \langle t_n \rangle) = \langle F(t_1, \ldots, t_n) \rangle$;
- ако $c \in \mathrm{Const}_{\mathcal{L}^*}$, онда је $c^{\mathbf{M}^*} = \langle c \rangle$.

5. Интерпретације релацијских и функцијских симбола језика $\mathcal{L}^*$ на скупу M^* добро су дефинисане.

Добра дефинисаност интерпретација релацијских и функцијских симбола значи да:

1) из $\langle t_1 \rangle = \langle s_1 \rangle, \ldots, \langle t_m \rangle = \langle s_m \rangle$, следи

$$R^{\mathbf{M}^*}(\langle t_1 \rangle, \ldots, \langle t_m \rangle) \text{ акко } R^{\mathbf{M}^*}(\langle s_1 \rangle, \ldots, \langle s_m \rangle),$$

2) из $\langle t_1 \rangle = \langle s_1 \rangle, \ldots, \langle t_m \rangle = \langle s_m \rangle$, следи

$$F^{\mathbf{M}^*}(\langle t_1 \rangle, \ldots, \langle t_m \rangle) = F^{\mathbf{M}^*}(\langle s_1 \rangle, \ldots, \langle s_m \rangle).$$

Нека је $\langle t_1 \rangle = \langle s_1 \rangle, \ldots, \langle t_m \rangle = \langle s_m \rangle$. Тада је $t_1 \sim s_1, \ldots, t_m \sim s_m$, што значи да $T^* \vdash t_i = s_i$, $i = 1, \ldots, m$.

Докажимо најпре екиваленцију из 1). Нека је $R^{\mathbf{M}^*}(\langle t_1 \rangle, \ldots, \langle t_m \rangle)$. Тада $T^* \vdash R(t_1, \ldots, t_m)$. Ако m пута применимо правило $(=_{\mathrm{E}})$, добијамо да $T^* \vdash R(s_1, \ldots, s_m)$, одакле следи $R^{\mathbf{M}^*}(\langle s_1 \rangle, \ldots, \langle s_m \rangle)$. Аналогно се доказује обратна импликација.

Докажимо једнакост из 2). Ако на $T^* \vdash F(x_1, \ldots, x_m) = F(x_1, \ldots, x_m)$ $(=_{\mathrm{U}})$, при чему су $x_1, \ldots, x_m$ међусобно различите променљиве и $\mathrm{ar}(F) = m$, m

[48] Видети доказ теореме потпуности за исказну логику.

пута применимо правило $(=_\mathrm{E})$, добијамо $T^* \vdash F(t_1,\dots,t_m) = F(s_1,\dots,s_m)$, одакле следи да је $\langle F(t_1,\dots,t_m)\rangle = \langle F(s_1,\dots,s_m)\rangle$, што даље значи да је $F^{\mathbf{M}^*}(\langle t_1\rangle,\dots,\langle t_m\rangle) = F^{\mathbf{M}^*}(\langle s_1\rangle,\dots,\langle s_m\rangle)$.

Остаје још да се покаже да конструисани модел задовољава жељену теорију. То ће бити једноставна последица следећих тврђења.

6. За сваки терм $t \in \mathrm{Term}_\mathcal{L}$ и све $a_1,\dots,a_k \in M$, при чему је $k = |V(t)|$, важи[49]:

$$t^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle] = \langle t[a_1,\dots,a_k]\rangle.$$

Доказ изводимо индукцијом по сложености израза t.

Ако је t променљива x, за валуацију $x \mapsto \langle a\rangle \in M^*$, имамо да је $t^{\mathbf{M}^*}[\langle a\rangle] = \langle a\rangle = \langle t[a]\rangle$, па тврђење очигледно важи. Ако је t симбол константе c, онда је $t^{\mathbf{M}^*} = c$, па и у овом случају важи тврђење.

Претпоставимо да тврђење важи за све изразе сложености мање од n. Нека је t израз сложености n. Тада је t облика $F(t_1,\dots,t_m)$, за неко $F \in \mathrm{Fun}_\mathcal{L}$, $\mathrm{ar}(F) = m$, и неке изразе $t_1,\dots,t_m$ сложености мање од n. Нека је $k = |\mathrm{V}(t)|$. Тада је:

$$\begin{array}{rl} & t^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ = & F^{\mathbf{M}^*}\left(t_1^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle],\dots,t_m^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle]\right) \\ = & F^{\mathbf{M}^*}\left(\langle t_1[a_1,\dots,a_k]\rangle,\dots,\langle t_m[a_1,\dots,a_k]\rangle\right) \\ = & \langle F\left(t_1[a_1,\dots,a_k],\dots,t_m[a_1,\dots,a_k]\right)\rangle \\ = & \langle t[a_1,\dots,a_k]\rangle \end{array}$$

7. За сваку формулу $\alpha \in \mathrm{For}_\mathcal{L}$ и све $a_1,\dots,a_k \in M$, при чему је $k = |\mathrm{Fr}(\alpha)|$, важи:

$$\mathbf{M}^* \models \alpha[\langle a_1\rangle,\dots,\langle a_k\rangle] \text{ акко } T^* \vdash \alpha[a_1,\dots,a_k].$$

Доказ изводимо индукцијом по сложености формуле φ.

Ако је α атомична формула облика $t_1 = t_2$, $t_1, t_2 \in \mathrm{Term}_\mathcal{L}$:

$$\begin{array}{rl} & \mathbf{M}^* \models \alpha[\langle a_1\rangle,\dots,\langle a_m\rangle] \\ \text{акко} & t_1^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle] = t_2^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ \text{акко} & \langle t_1[a_1,\dots,a_k]\rangle = \langle t_2[a_1,\dots,a_k]\rangle \\ \text{акко} & T^* \vdash t_1[a_1,\dots,a_k] = t_2[a_1,\dots,a_k]. \end{array}$$

[49]Са $t[a_1,\dots,a_k]$ означавамо израз добијен из t заменом свих његових променљивих $x_1,\dots,x_k$ редом изразима $a_1,\dots,a_k$.

Ако је α атомична формула облика $R(t_1,\dots,t_m)$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $\mathrm{ar}(R) = m$, $t_1,\dots,t_m \in \mathrm{Term}_{\mathcal{L}}$:

$$\begin{array}{ll} & \mathbf{M}^* \models R(t_1,\dots,t_m)[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ \text{акко} & R^{\mathbf{M}^*}\left(t_1^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle],\dots,t_m^{\mathbf{M}^*}[\langle a_1\rangle,\dots,\langle a_k\rangle]\right) \\ \text{акко} & R^{\mathbf{M}^*}(\langle t_1[a_1,\dots,a_k]\rangle,\dots,\langle t_m[a_1,\dots,a_k]\rangle) \\ \text{акко} & T^* \vdash R(t_1[a_1,\dots,a_k],\dots,t_m[a_1,\dots,a_k]) \\ \text{акко} & T^* \vdash R(t_1,\dots,t_m)[a_1,\dots,a_k]. \end{array}$$

Ако је α облика $\neg\theta$, онда

$$\begin{array}{ll} & \mathbf{M}^* \models \neg\theta[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ \text{акко} & \mathbf{M}^* \not\models \theta[\langle a_1\rangle,\dots,\langle a_k\rangle] \quad \text{[према дефиницији релације задовољења]} \\ \text{акко} & T^* \nvdash \theta[a_1,\dots,a_k] \quad \text{[према индуктивној претпоставци]} \\ \text{акко} & T^* \vdash \neg\theta[a_1,\dots,a_k] \quad [T^* \text{ је комплетна}] \\ \text{акко} & T^* \vdash \alpha[a_1,\dots,a_k]. \end{array}$$

Ако је α облика $\varphi \wedge \psi$, онда

$$\begin{array}{ll} & \mathbf{M}^* \models \varphi\wedge\psi[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ \text{акко} & \mathbf{M}^* \models \varphi[\langle a_1\rangle,\dots,\langle a_k\rangle] \text{ и } \mathbf{M}^* \models \psi[\langle a_1\rangle,\dots,\langle a_k\rangle] \\ & \qquad\qquad\qquad\qquad \text{[према дефиницији релације задовољења]} \\ \text{акко} & T^* \vdash \varphi[a_1,\dots,a_k] \text{ и } T^* \vdash \psi[a_1,\dots,a_k] \\ & \qquad\qquad\qquad\qquad \text{[према индуктивној претпоставци]} \\ \text{акко} & T^* \vdash \varphi\wedge\psi[a_1,\dots,a_k] \\ & \qquad\qquad\qquad\qquad \text{[према правилима } (\wedge_{\mathrm{U}}),\ (\wedge_{\mathrm{E}}^{\mathrm{l}}),\ (\wedge_{\mathrm{E}}^{\mathrm{d}})] \\ \text{акко} & T^* \vdash \alpha[a_1,\dots,a_k]. \end{array}$$

Нека је α облика $\exists x\theta(x,x_1,\dots,x_k)$.

Претпоставимо да је $\mathbf{M}^* \models \alpha[\langle a_1\rangle,\dots,\langle a_m\rangle]$. Тада постоји елемент $a \in M$, такав да је $\mathbf{M}^* \models \theta[\langle a\rangle,\langle a_1\rangle,\dots,\langle a_m\rangle]$, па према индуктивној претпоставци $T^* \vdash \theta[a,a_1,\dots,a_m]$. Применом правила $(\exists_{\mathrm{U}})$ имамо $T^* \vdash \exists x\theta[x,a_1,\dots,a_m]$, односно $T^* \vdash \alpha[a_1,\dots,a_m]$.

Претпоставимо да $T^* \vdash \alpha[a_1,\dots,a_m]$, односно $T^* \vdash \exists x\theta[x,a_1,\dots,a_m]$. Према тврђењу **1**, постоји симбол константе c језика $\mathcal{L}^*$, такав да

$$T^* \vdash \exists x\theta[x,a_1,\dots,a_m] \Rightarrow \theta[c,a_1,\dots,a_m],$$

одакле, према ($\Rightarrow_{\mathrm{E}}$), следи $T^* \vdash \theta[c, a_1, \ldots, a_m]$. Према индуктивној претпоставци је $\mathbf{M}^* \models \theta[\langle c\rangle, \langle a_1\rangle, \ldots, \langle a_m\rangle]$, па $\mathbf{M}^* \models \exists x\theta[x, \langle a_1\rangle, \ldots, \langle a_m\rangle]$, односно $T^* \vdash \alpha[a_1, \ldots, a_k]$. $\square$

Поглавље завршавамо неким једноставним применама теореме

$$(\bigstar) \qquad \Gamma \vdash \alpha \text{ акко } \Gamma \models \alpha.$$

Пример 30. Применом наведене теореме једноставно се доказује да одређена формула није последица неког скупа претпоставки. То ћемо илустровати једним примером. Посматрајмо теорију група T_{GR} и докажимо да се закон комутативности, тј. формула $\forall x\forall y(x*y = y*x)$ <u>не може</u> извести из T_{GR}. Да бисмо доказали да $T_{\mathrm{GR}} \nvdash \forall x\forall y(x*y = y*x)$, довољно је доказати да $T_{\mathrm{GR}} \not\models \forall x\forall y(x*y = y*x)$, за шта је довољно да конструишемо групу чија бинарна операција није комутативна. Ко је бар мало упознат са теоријом група, одмах ће се сетити примера такве групе. Једна од њих је група $(S_3, \circ, {}^{-1}, \sigma_1)$, где је S_3 скуп свих пермутација (бијекција) скупа $\{1,2,3\}$ чију су елементи:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Да група није комутативна показују једнакости:

$$\tau_3 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3, \ \tau_2 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_2.$$

Аналогно се показује да се чувени пети постулат (тј. аксиома паралелности) не може доказати из осталих аксиома еуклидске геометрије. У примеру са почетка овог поглавља грубо смо описали модел у коме аксиома паралелности не важи, али се могу „реализовати“ све остале аксиоме еуклидске геометрије. Много више детаља о овом моделу читалац може пронаћи у ??. $\triangleright$

Задаци

1. Нелогички део језика предикатске логике првог реда чине следећи симболи: $\mathrm{Rel}_{\mathcal{L}} = \{R, S\}$, $\mathrm{Fun}_{\mathcal{L}} = \{F, G\}$, $\mathrm{Const}_{\mathcal{L}} = \{e\}$, при чему је $\mathrm{ar}(R) = \mathrm{ar}(F) = 2$, $\mathrm{ar}(S) = \mathrm{ar}(G) = 1$.

(i) Који је од следећих низова симбола израз, који формула, а који ни једно ни друго: $F(G(x), G(y))$; $S(F(x, G(e)))$; $R(x, S(x))$; $R(e, e)$; $\forall y R(x, e)$; $\forall x\exists y R(x, y)$; $\forall x(R(x, G(y)) \Rightarrow F(x, y))$?

(ii) Дати језик је интерпретиран на скуповима $\mathbb{Z}$, $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$ и $X = \{a, b, c\}$.

Интерпретација на $\mathbb{Z}$:

$R^{\mathbf{Z}} = \leqslant$ (уређење целих бројева),
$S^{\mathbf{Z}} =$ „*бити позитиван*“ $= \{1, 2, 3, 4, \ldots\}$,
$F^{\mathbf{Z}} = +$ (сабирање целих бројева),
$G^{\mathbf{Z}} = g$, при чему је $g : \mathbb{Z} \to \mathbb{Z}$ и $g(x) = -x$, $x \in \mathbb{Z}$,
$e^{\mathbf{Z}} = 0$.

Интерпретација на $\mathbb{N}$:

$R^{\mathbf{N}} = |$ (дељивост природних бројева),
$S^{\mathbf{N}} =$ „*бити прост*“ $= \{2, 3, 5, 7, 11, \ldots\}$,
$F^{\mathbf{N}} = \cdot$ (множење природних бројева),
$G^{\mathbf{N}} = h$, при чему је $h : \mathbb{N} \to \mathbb{N}$ и $h(x) = 2x + 1$, $x \in \mathbb{N}$,
$e^{\mathbf{N}} = 1$.

Интерпретација на $\mathcal{P}(\mathbb{N})$:

$R^{\mathbf{P}(\mathbb{N})} = \subseteq$ (подскуп),
$S^{\mathbf{P}(\mathbb{N})} =$ „*бити коначан*“,
$F^{\mathbf{P}(\mathbb{N})} = \cap$ (пресек скупова),
$G^{\mathbf{P}(\mathbb{N})} = {}^c$ (комплемент скупа у односу на $\mathbb{N}$, ${}^c : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ и $x^c = \mathbb{N} \setminus x$),
$e^{\mathbf{P}(\mathbb{N})} = \emptyset$.

Интерпретација на X:

$R^{\mathbf{X}} = \{(a, c), (b, c), (c, c), (a, b)\}$,
$S^{\mathbf{X}} = \{a, c\}$,
$F^{\mathbf{X}} = *$, при чему је $*$ бинарна операција дефинисана таблицом

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

,

$G^{\mathbf{X}} = \ell$, при чему је $\ell : X \to X$ дато са $\ell = \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix}$,
$e^{\mathbf{X}} = c$.

(а) Одредити вредности израза $F(F(x, e), G(y))$, $G(F(x, x))$ и испитати тачност формуле $S(F(x, x)) \Rightarrow R(G(x), G(y))$ у
– $\mathbf{Z}$ при валуацији промењљивих $\mu : x \mapsto -2$, $y \mapsto 1$;
– $\mathbf{N}$ при валуацији промењљивих $\mu : x \mapsto 2$, $y \mapsto 1$;
– $\mathbf{P}(\mathbf{N})$ при валуацији промењљивих $\mu : x \mapsto \{1, 2\}$, $y \mapsto \{2, 3\}$;
– $\mathbf{X}$ при валуацији промењљивих $\mu : x \mapsto a$, $y \mapsto b$.

(б) Испитати тачност реченица $\exists x \forall y R(x, y)$, $\forall x S(x) \vee \forall x \neg S(x)$, $\exists x \neg S(x)$, $\neg S(G(e)))$, $\forall x \forall y (S(x) \wedge S(y) \Rightarrow S(F(x, y)))$, $\forall x \forall y (R(x, y) \Rightarrow R(G(y), G(x)))$,

$\forall x(S(x) \Rightarrow \exists y R(x, F(x,y)))$, $\forall x \forall y(R(x,y) \vee R(y,x))$ редом у моделима $\mathbf{Z}$, $\mathbf{N}$, $\mathbf{P}(\mathbb{N})$, $\mathbf{X}$.

(в) Реченицама датог језика изразити следећа својства структуре $\mathbf{N}$.

– *Производ два проста броја није прост број.*

– *Сваки прост број већи од* 2 *је непаран.*

(г) Реченицама датог језика изразити следећа својства структуре $\mathbf{P}(\mathbb{N})$.

– *Комплемент коначног скупа није коначан скуп.*

– *Пресек два коначна скупа је коначан скуп.*

– *Постоји скуп који није коначан и чији комплемент није коначан.*

2. За сваку од наредних реченица језика из претходног задатка наћи, ако је то могуће, бар један модел и бар један контрамодел.

- $\forall x S(x) \wedge \forall x R(x,x) \Rightarrow \forall x(S(x) \wedge R(x,x))$,
- $\forall x \neg R(x,x) \vee \forall x R(x,x)$,
- $\exists x S(x) \vee \exists x R(x,x) \Rightarrow \exists (S(x) \vee R(x,x))$,
- $\forall x(\neg R(x,x) \vee R(x,x))$.
- $\forall x S(x) \wedge \forall x R(x,x) \Rightarrow \forall x(S(x) \wedge R(x,x))$,
- $\exists x(R(x,x) \Rightarrow S(x))$,
- $\forall x \neg R(x,x)$,
- $\exists x S(x) \vee \exists x R(x,x) \Rightarrow \exists x(S(x) \vee R(x,x))$,
- $\forall x(\neg R(x,x) \vee R(x,x))$,
- $\forall x \exists y(S(x) \vee S(y)) \Leftrightarrow \forall x \forall y(\neg S(x) \wedge \neg S(y))$.

3. Језик $\mathcal{L} = \{*, \star, a, b\}$ ($\mathrm{Fun}_{\mathcal{L}} = \{*, \star\}$, $\mathrm{ar}(*) = \mathrm{ar}(\star) = 2$, $\mathrm{Const}_{\mathcal{L}} = \{a, b\}$) интерпретиран је на више начина.

На скупу $\mathbb{Z}$, операцијски знаци $*$ и $\star$ су интерпретирани стандардним операцијама $+$ и $\cdot$, редом, а симболи константи a и b са 0 и 1, редом.

На скупу $\mathbb{Z} \times \mathbb{Z}$, операцијски знаци $*$ и $\star$ су интерпретирани редом операцијама $\oplus$ и $\odot$, при чему је

$$(k,\ell) \oplus (m,n) = (k+m, \ell+n) \text{ и } (k,\ell) \odot (m,n) = (k \cdot m - \ell \cdot n, k \cdot n + \ell \cdot m),$$

а симболи константи a и b са $(0,0)$ и $(1,0)$, редом.

На $\mathrm{M}_2(\mathbb{Z})$ – скупу свих квадратних матрица типа 2×2 над $\mathbb{Z}$ (тј. свих квадратних „шема“ облика $\begin{bmatrix} k & \ell \\ m & n \end{bmatrix}$) операцијски знаци $*$ и $\star$ су интерпретирани редом операцијама $\boxplus$ и $\boxdot$, при чему је

$$\begin{bmatrix} k & \ell \\ m & n \end{bmatrix} \boxplus \begin{bmatrix} k' & \ell' \\ m' & n' \end{bmatrix} = \begin{bmatrix} k+k' & \ell+\ell' \\ m+m' & n+n' \end{bmatrix}$$

и

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

а симболи константи a и b са $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ и $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, редом.

Означимо добијене структуре са

$\mathbf{A} = (\mathbb{Z}, +, \cdot, 0, 1)$,

$\mathbf{B} = (\mathbb{Z} \times \mathbb{Z}, \oplus, \odot, (0,0), (1,0))$ и

$\mathbf{C} = \left(\mathrm{M}_2(\mathbb{Z}), \boxplus, \boxdot, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$.

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

4. Да ли постоји формула α језика $\mathcal{L}_{\mathrm{FO}}$ таква да за свако уређено поље $\mathbf{F}$ важи: $\mathbf{F} \models \alpha$ акко је $\mathbf{F}$ архимедско поље (видети пример 19)?

5. За формулу α неког језика $\mathcal{L}$, нека је

$A_\alpha = \{n \in \mathbb{N} \mid$ постоји модел $\mathbb{M}$ над скупом са n елемената такав да $\mathbf{M} \models \alpha\}$.

За сваки од наредних скупова $A \subseteq \mathbb{N}$ одредити (ако постоји) формулу α, бирајући притом и одговарарјући језик $\mathcal{L}$, тако да $A_\alpha = A$.

- $A = \mathbb{N} \setminus \{0\}$;
- $A = \{1, \ldots, n\}$, $n \geqslant 1$;
- $A = \{n\}$, $n \geqslant 1$;
- $A = \mathbb{N} \setminus \{0, 1, \ldots, n\}$, $n \geqslant 1$;
- $A = \{n \in \mathbb{N} \mid n \equiv 2\,(\mathrm{mod} 3)\}$;
- $A = \{n^2 \mid n \in \mathbb{N}\}$;
- $A = \{n \in \mathbb{N} \mid n$ није прост број$\}$.

6. Доказати:

(а) $\alpha \Rightarrow \forall x \beta \equiv \forall x(\alpha \Rightarrow \beta)$ ако x није слободно у α;

(б) $\exists x \alpha \Rightarrow \beta \equiv \forall x(\alpha \Rightarrow \beta)$ ако x није слободно у β;

(в) $\exists x(\alpha \Rightarrow \beta) \Leftrightarrow (\forall x \alpha \Rightarrow \exists x \beta)$.

7. Нека су $\circ, *$ два бинарна операцијска симбола, а $\lhd, <$ два бинарна релацијска симбола. Дате су следеће формуле:

α_1 $\quad \forall x \forall u \forall v(x \lhd u \circ v \Leftrightarrow \forall y(x < y \Rightarrow (y \lhd u \Rightarrow y \lhd v)))$;

α_2 $\quad \forall x, u, v(x \lhd u * v \Leftrightarrow x \lhd u \vee x \lhd v)$;

α_3 $\quad \forall x \forall y \forall z(x < y \wedge x < z \Rightarrow y < z \vee z < y)$;

α_4 $\quad \forall x \forall y \forall u(x \lhd u \wedge x < y \Rightarrow y \lhd u)$;

$\alpha \quad \forall x \forall u \forall v(x \lhd (u \circ v) * (v \circ u))$.
Доказати $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \models \alpha$.

8. Ако су U и V унарни релацијски симболи и f унарни операцијски симбол, доказати:
(а) $\vdash \exists x \forall y(U(x) \Rightarrow U(y))$;
(б) $\vdash \exists x \forall y(U(y) \Rightarrow U(x))$;
(в) $\vdash \exists x \forall y(((U(y) \Rightarrow U(x)) \Rightarrow U(x)) \Rightarrow U(y))$;
(г) $\vdash \exists x \forall y((V(y) \Rightarrow U(x)) \Rightarrow (V(x) \Rightarrow U(y)))$;
(д) $\vdash \exists x \forall y(((U(f(x)) \Rightarrow U(f(y))) \Rightarrow U(x)) \Rightarrow U(y))$.

9. Ако су α, β и γ произвољне предикатске формуле, доказати да је:
(а) $\vdash \forall x(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \forall x \beta)$ уколико x није слободна промењива у формули α;
(б) $\vdash \exists x(\alpha \Rightarrow \beta) \Rightarrow (\forall x \alpha \Rightarrow \exists x \beta)$.

10. Доказати да се следећа *лева* правила извођења могу користити при доказивању.

$$\frac{\Gamma, \forall x \alpha, \alpha(x := t) \vdash \gamma}{\Gamma, \forall x \alpha \vdash \gamma}\ (\forall_{\mathrm{L}})$$

$$\frac{\Gamma, \alpha \vdash \gamma \quad x \text{ није слободно у формулама из } \Gamma \text{ и у } \gamma}{\Gamma, \exists x \alpha \vdash \gamma}\ (\exists_{\mathrm{L}})$$

Пеанова аритметика (првог реда), у ознаци $\mathbf{PA}$, 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 $\quad \forall x \neg 0 = s(x)$,
PA2 $\quad \forall x \forall y(s(x) = s(y) \Rightarrow x = y)$,
PA3 $\quad \forall x(x + 0 = x)$,
PA4 $\quad \forall x \forall y(x + s(y) = s(x + y))$,
PA5 $\quad \forall x(x \cdot 0 = 0)$,
PA6 $\quad \forall x \forall y(x \cdot s(y) = (x \cdot y) + x)$,
PA7 $\quad \forall x \forall y(x \leqslant y \Leftrightarrow \exists z(z + x = y))$,
PA8 $\quad (\varphi(0) \wedge \forall x(\varphi(x) \Rightarrow \varphi(s(x)))) \Rightarrow \forall x \varphi(x)$.

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

11. Доказати:
(а) $\mathbf{PA} \vdash \forall x \forall y(x + y = y + x)$,
(*Упутство.* Доказати најпре да је $\mathbf{PA} \vdash \forall y(0 + y = y + 0)$.)
(б) $\mathbf{PA} \vdash \forall x(x \leqslant x)$,
(в) $\mathbf{PA} \vdash \forall x \forall y(x \leqslant y \wedge y \leqslant x \Rightarrow x = y)$,

(г) $\mathbf{PA} \vdash \forall x \forall y \forall z (x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z)$,
(д) $\mathbf{PA} \vdash \forall x (x \leqslant 0 \Rightarrow x = 0)$,
(ђ) $\mathbf{PA} \vdash \forall x \forall y (x \leqslant S(y) \Rightarrow x \leqslant y \vee x = s(y))$,
(е) $\mathbf{PA} \vdash \forall x \forall y (x \leqslant y \vee y)$,
(ж) $\mathbf{PA} \vdash \exists x \alpha(x) \Rightarrow \exists x (\alpha(x) \wedge \forall y (y < x \Rightarrow \neg \alpha(y)))$, за сваку формулу α.

12. На скупу $\mathbf{M} = \{0\} \times \mathbf{N} \cup \{1, 2\} \times \mathbf{Z}$ 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 $\mathbf{M}$ важе све аксиоме Пеанове аритметике, осим аксиоме индукције **PA8**. Такође, доказати:

• $\mathbf{M} \not\models \forall x \forall y (x + y = y + x)$;

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

Литература

[1] **Božić**, **Ivić**, **Jovanović**, **Kapetanović**, **Mihaljinec**, **Mijajlović**, **Prešić**, **Rašković**, **Rosenzweig**, **Šami**, **Šeper**, **Šikić**, **Ugrin-Šparac**, *Brojevi*, Školska knjiga, Zagreb, 1985.

[2] **R. David**, **K. Nour**, **C. Raffali**, *Introduction à la logique – Théorie de la démonstration*, Dunod, Paris, 2003.

[3] **H. -D. Ebbinghaus**, **J. Flum**, **W. Thomas**, *Mathematical Logic*, Springer-Verlang, New York Inc., 1994.

[4] **S. Givant**, **P. Halmos**, *Introduction to Boolean algebras*, Springer, New York INC., 2009.

[5] **J. Harison**, *Handbook of Practical logic and Automated Reasoning*, Cambridge University Press, New York, 2009.

[6] **A. Kron**, *Logika*, Univerzitet u Beogradu, Beograd, 1998.

[7] **И. А. Лавров, Л. Л. Максимова**, *Задачи по теории множеств, математической логике и теории алгоритмов*, Наука, Москва, 1984.

[8] **P. Janičić**, *Matematička logika u računarstvu*, Matematički fakultet, Beograd, 2005.

[9] **Ž. Mijajlović**, *Algebra 1*, Milgor, Beograd, Moskva, 1993.

[10] **Ž. Mijajlović**, *An Introduction to Model Theory*, University of Novi Sad, Faculty of Science, Novi Sad, 1987.

[11] **Ž. Mijajlović**, **Z. Marković**, **K. Došen**, *Hilbertovi problemi i logika*, Zavod za udžbenike i nastavna sredstva, Beograd, 1986.

[12] **J. D. Monk**, *Mathematical Logic*, Springer-Verlang, 1976.

[13] **A. Perović**, **A. Jovanović**, **B. Veličković**, *Teorija skupova*, Matematički fakultet, Beograd, 2007.

[14] **Z. Petrović**, **Ž. Mijajlović**, *Matematička logika, elementi teorije skupova*, Zavod za udžbenike, Beograd, 2012.

[15] **W. Rautenberg**, *A Concise Introduction to Mathematical Logic*, Springer, Berlin, 2005.

[16] **M. Rašković**, **N. Ikodinović**, *Priče o velikim i malim brojevima, o brojanju, merenju, zaključivanju ...*, Zavod za udžbenike, Beograd, 2009.

[17] **S. Vujošević**, *Matematička logika (o mogućnostima formalnog metoda)*, CID, Podgorica, 1996.