Diskretna Matematika

Iskazni Račun

Žarko Mijajlović **Zoran Petrović** **Maja Roslavcev**

.
..
...
....
.....
.....
.....
.....
.....
.....

Matematički fakultet
Beograd 2011

Glava 1

Iskazni račun

Matematička logika najčešće se definiše kao nauka koja se bavi izučavanjem logike matematičkim sredstvima. Takvom opisu ove discipline može se prigovoriti s obzirom da se zakoni logike koriste u konstrukcijama matematičkih dokaza. Otuda bi se zaključilo da izučavanje logike treba da prethodi izučavanju matematike. Ovakav tok stvari zapravo je uobičajen u nauci – setimo se odnosa matematike i fizike, na primer. Bilo koji vid savremene fizike pretpostavlja ozbiljnu upotrebu i poznavanje savremene matematike. Štaviše mnoge važne oblasti matematike razvile su se pod uticajem fizike ili radi potreba fizike. Slična situacija u odnosu na matematiku postoji i u nekim drugim savremenim naukama. Ipak to ne pretpostavlja, niti bilo ko očekuje da se neko treba u potpunosti posvetiti izučavanju matematika, a tek potom svojoj osnovnoj nauci. U krajnjoj liniji, aktuelno ljudsko znanje ipak predstavlja samo uzan snop svetlosti na dve strane nepoznatog: mogu se razviti do kraja sve posledice polazeći od poznatih principa. Ili se može potisnuti dublje nejasna i tajanstvena tama u kojoj leže osnove naše nauke.

Upravo koristeći matematički aparat, odnosno koristeći ideograme (simbole za ideje) umesto reči prirodnog jezika, može se baciti sasvim novo svetlo na logičke principe koji se koriste u matematici. Ovakav pristup doneo je više znanja o logici u jednom veku nego što je tog znanja bilo od Aristotelovog vremena do sredine 19. veka kada se pojavilo veliko delo Džordža Bula o iskaznoj algebri.

U ovom poglavlju biće predstavljen klasičan iskazni račun. Ovaj deo matematičke logike je njen najjednostavniji deo, ali već u tom računu mogu se videti ili makar naslutiti koji su to osnovni problemi i metode matematičke logike.

1.1 Iskazne operacije

Iskazni račun, kojeg ćemo kraće označiti pomoću slova **I**, prvi je formalan sistem napravljen radi izučavanja validnih procesa zaključivanja, odnosno deduktivnog zaključivanja. Ovaj sistem uveo je matematičar Džordž Bul (George Boole, irac,

1815-1864) u svom računu klasa, danas teorija poznata pod imenom Bulove algebre.

U zaključivanju polazi se od nekih iskaza koje nazivama pretpostavkama ili premisama i primenom određenih pravila izvođenja izvodimo (dedukujemo) zaključak. Pretpostavke i zaključak su iskazi, dakle određene rečenice kojima se mogu dodeliti istinistosne vrednosti tačno i netačno (lažno). Formalni sistem daje pravila za izgradnju rečenica, pravila izvođenja i način računanja istinitosti rečenica sistema. Sistem je deduktivan ukoliko su njegova pravila izvođenja saglasna sa istinitošću, odnosno ako ispunjavaju uslov *salva veritate*: primenom pravila na istinite pretpostavke proizvode se istiniti zaključci.

U formalnom sistemu razlikujemo sintaksni i semantički deo. Sintaksni deo daje pravila za formiranje ispravnih izraza sistema, u slučaju iskaznog računa to su iskazne formule, i pravila izvođenja sistema. Semantički deo odnosi se na računanje istinitosti i izučavanje svojstva ovog pojma. U slučaju iskaznog računa semantički deo predstavljen je iskaznom algebrom, odnosno iskaznim operacijama na domenu $2 = \{0, 1\}$. Ovde su 1 i 0 redom matematički prepisi za logičkue vrednosti tačno (istinito) i netačno (neistinito, lažno).

Iskazni račun odnosi se u osnovi na mali fragment prirodnog jezika. To su sledeći veznici i jezičke konstrukcije: *i, ili, ne, ako ... onda, ako i samo ako*. U iskaznom računu za te reči uvode se sledeći simboli, nazivi i značenja:

Tablica iskaznih simbola

$\vee$	disjunkcija	... *ili* ...
$\wedge$	konjunkcija	... *i* ...
$\neg$	negacija	*ne* ...
$\Rightarrow$	implikacija	*ako* ... *onda* ...
$\Leftrightarrow$	ekvivalencija	... *ako i samo ako* ...
$\underline{\vee}$	ekskluzivna disjunkcija	*ili* ... *ili* ...

Logičke konstante $\top$ (*te* – univerzalno istinit iskaz) i $\bot$ (*ne-te* – univerzalno lažan iskaz) takođe su delovi izkaznog računa. Dakle jezik iskaznog računa je $L_{\mathbf{I}} = \{\vee, \wedge, \neg, \Rightarrow, \Leftrightarrow, \underline{\vee}, \top, \bot\}$. Kao što se iz tablice vidi, simboli iskaznih operacija $\vee, \wedge, \Rightarrow, \Leftrightarrow, \underline{\vee}$ imaju dva argumentna mesta, odnosno imaju arnost ili dužinu dva, dok je $\neg$ simbol iskazne operacije dužine (arnosti) jedan. Logičke konstante $\top, \bot$ imaju po definiciji dužinu nula. Spomenimo da jezik $L_{\mathbf{I}}$ nije strogo fiksiran. Negde se uzima da se $L_{\mathbf{I}}$ sastoji samo od prvih pet simbola, na drugim mestima uzima se da je $L_{\mathbf{I}} = \{\Rightarrow, \neg\}$, na trećim je $L_{\mathbf{I}} = \{\vee, \wedge, \neg\}$. Ova raznolikost potiče iz činjenice, u koju ćemo se kasnije uveriti, da se za određene izbore ostale iskazne operacije mogu izvesti pomoću onih izabranih u jeziku $L_{\mathbf{I}}$. U izgradnji iskaznih formula pored logičkih veznika učestvuju iskazna (propozicionalna) slova: $p_0, p_1, p_2 \ldots$. To su zaprave promenljive koje predstavljaju elementarne iskaze pomoću kojih se grade složenije iskazne formule. Neka je $\mathcal{P} = \{p_0, p_1, p_2 \ldots\}$. Kao što vidimo $\mathcal{P}$ je prebrojiv skup, mada se u primenama mogu izabrati skupovi druge kardinalnosti, pa i konačne i nepreborijive. Formule iskaznog računa grade se pomoću iskaznih promenljivih i logičkih veznika

na isti način kako se grade termi (algebarski izrazi) nekog algebarskog jezika L. Dakle skup iskaznih formula $\mathcal{F}_\mathcal{P}$ nad skupom promenljivih $\mathcal{P}$ definišemo induktivno na sledeći način:

$$\mathcal{F}_0 = \mathcal{P} \cup \{\top, \bot\}$$

$$\begin{aligned}\mathcal{F}_{n+1} \quad = \mathcal{F}_n \ \cup \quad & \{(\varphi \vee \psi) \colon \varphi, \psi \in \mathcal{F}_n\} \cup \{(\varphi \wedge \psi) \colon \varphi, \psi \in \mathcal{F}_n\} \ \cup \\ & \{\neg\varphi \colon \varphi \in \mathcal{F}_n\} \cup \{(\varphi \Rightarrow \psi) \colon \varphi, \psi \in \mathcal{F}_n\} \ \cup \\ & \{(\varphi \Leftrightarrow \psi) \colon \varphi, \psi \in \mathcal{F}_n\} \cup \{(\varphi \veebar \psi) \colon \varphi, \psi \in \mathcal{F}_n\} \end{aligned} \tag{1.1}$$

$$\mathcal{F}_\mathcal{P} = \bigcup_{i \in N} \mathcal{F}_n = \mathcal{F}_0 \cup \mathcal{F}_1 \cup \mathcal{F}_2 \cup \ldots$$

Shodno ovoj definiciji, φ je formula iskaznog računa nad skupom iskaznih promenljivih $\mathcal{P}$ akko $\varphi \in \mathcal{F}_P$. Kao i u algebri pretpostavljaju se razne konvenicje o jednostavnijem zapisivanju iskaznih formula. Na primer, dopušteno je pisati formule bez krajnjih zagrada: tako, umesto $(p_1 \vee p_2)$ pišemo $p_1 \vee p_2$. Dalje, formula $\varphi_1 \vee \varphi_2 \vee \varphi_3 \vee \ldots \vee \varphi_n$ stoji umesto formule $(\ldots((\varphi_1 \vee \varphi_2) \vee \varphi_3) \ldots \vee \varphi_n)$ i sličan dogovor važi za $\varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \ldots \wedge \varphi_n$. Uverićemo se da je izbor rasporeda zagrada nebitan s obzirom da važe zakoni asocijacije za iskazne operacije disjunkcije i konjunkcije.

Pomoću $p, q, r, s, t, \ldots$ označavaćemo proizvoljna iskazna slova. Dakle, to su metapromenljive čije je domen skup $\mathcal{P}$. Neka svojstva iskaznog računa bitno zavise od izbora skupa promenljivih. S druge strane, u primenama iskaznog računa za skupove promenljivih biraćemo razne skupove simbola. Tako, u našem osnovnom primeru $\mathcal{P} = \{p_0, p_1, p_2 \ldots\}$ prema (1.1) skup iskaznih formula je prebrojiv. Da smo izabrali za $\mathcal{P}$ neprebrojiv skup, tada bi, naravno i skup iskaznih formula bio neprebrojiv skup. Otuda se oznakom $\mathbf{I}_\mathcal{P}$ zapisuje činjenica da je izabrani skup iskaznih promenljivih iskaznog računa upavo $\mathcal{P}$.

Svakom od simbola $\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\veebar$ odgovara redom jedna algebarska operacija domena $\mathbf{2} = \{0, 1\}$: $\vee_\mathbf{I}$, $\wedge_\mathbf{I}$, $\neg_\mathbf{I}$, $\Rightarrow_\mathbf{I}$, $\Leftrightarrow_\mathbf{I}$, $\veebar_\mathbf{I}$. Ove operacije definisane su sledećim tablicama.

$\vee_\mathbf{I}$	0	1
0	0	1
1	1	1

$\wedge_\mathbf{I}$	0	1
0	0	0
1	0	1

p	$\neg_\mathbf{I} p$
0	1
1	0

$\Rightarrow_\mathbf{I}$	0	1
0	1	1
1	0	1

$\Leftrightarrow_\mathbf{I}$	0	1
0	1	0
1	0	1

$\veebar_\mathbf{I}$	0	1
0	0	1
1	1	0

Za logičke konstante $\top, \bot$ uzimamo da je $\top_\mathbf{I} = 1$ i $\bot_\mathbf{I} = 0$. Navedene iskazne operacije nose imena prema odgovarajućim simbolima iz Tablice iskaznih simbola, dok se algebra $\mathbf{2}_\mathbf{I} = (2, \vee_\mathbf{I}, \wedge_\mathbf{I}, \neg_\mathbf{I}, \Rightarrow_\mathbf{I}, \Leftrightarrow_\mathbf{I}, \veebar_\mathbf{I}, 0, 1)$ naziva *iskazna algebra*. Na primer, $\Rightarrow_\mathbf{I}$ je iskazna operacija implikacije ili jednostavno implikacija. Definicione tablice iskaznih operacija takođe se nazivaju *istinitosnim tablicama*

iskaznog računa. Radi jednostavnije notacije indeks $_{\mathbf{I}}$ često se ispušta iz oznaka iskaznih operacija. U zavisnosti od konteksta, znak $\Rightarrow$ označavaće ili simbol iskazne operacije ili samu iskaznu operaciju. Ako se znak $\Rightarrow$ pojavljuje u nekoj iskaznoj formuli, onda je $\Rightarrow$ simbol iskazne operacije. S druge strane, izraz $0 \Rightarrow 1$ je kraći zapis za $0 \Rightarrow_{\mathbf{I}} 1$ i pritom $(0 \Rightarrow 1) = 1$.

Mnoge definicije i dokazi svojstava iskaznih formula izvode se po složenosti formula. Složenost iskazne formule φ je formalan pojam i odslikava strukturu formule φ.

Definicija 1.1 *Složenost iskazne formule je preslikavanje* $\mathrm{sl}\colon \mathcal{F}_{\mathcal{P}} \to N$ *definisano na sledeći način:*

S1 *Ako je* $\varphi \in \mathcal{F}_0$ *onda je* $\mathrm{sl}(\varphi) = 0$.

S2 *Neka je* $\varphi \in \mathcal{F}_{\mathcal{P}}$ *i* $\varphi \notin \mathcal{F}_0$. *Tada je* $\mathrm{sl}(\varphi)$ *najmanji prirodan broj* n *takav da je* $\varphi \in \mathcal{F}_n \backslash \mathcal{F}_{n-1}$.

Primer 1.2 *Ako je* $\varphi = ((p \wedge q) \wedge \neg(q \Rightarrow r))$ *tada* $\mathrm{sl}(p \wedge \neg(q \Rightarrow r)) = 3$:
$p, q, r \in \mathcal{F}_0$, $(p \wedge q)$, $(q \Rightarrow r) \in \mathcal{F}_1$, $\neg(q \Rightarrow r) \in \mathcal{F}_2$, $((p \wedge q) \wedge \neg(q \Rightarrow r)) \in \mathcal{F}_3$.

Struktura formule φ može se prikazati pomoću specijalnog označenog grafa kojeg nazivamo *drvo formule* φ. Drvo formule prati i predstavlja postupak pomoću kojeg je φ izgrađena od svojih potformula.

Drvo formule je konačan parcijalno uređen skup $\mathbf{T} = (T, \leq, \varphi)$ definisan na sledeći način: elementi domena T su potformule formule φ, dok je za $\psi, \theta \in T$, $\psi \leq \theta$ akko je ψ podformula formule θ. Najveći element u $\mathbf{T}$ je φ. Neka je $\mathbf{T}^* = (T, \geq, \varphi)$ dualno uređenje za $\mathbf{T}$. Ključno svojstvo uređenja $\mathbf{T}$ je: $\mathbf{T}^*$ je drvo (stablo), tj. $\mathbf{T}^*$ ima najmanji element (φ) i za $X = \{\sigma \in T\colon \theta \leq \sigma\}$, $(X, \geq)$ je dobro uređen skup za svaki $\theta \in T$. Otuda se izvodi naziv drvo formule.

1.2 Tautologije

Vrednost iskazne formule za date logičke vrednosti promenljivih izračunava se na isti način kao vrednost algebarskog terma u nekoj algebri. Dakle, vrednost iskazne formule induktivnog je karaktera i definiše se indukcijom po složenosti formule. U ovom izračunavanju važno mesto ima pojam *iskazne valuacije*, preslikavanja koje dodeljuje iskaznim promenljivama logičke vrednosti $0, 1$. Iskazna valuacija, ili jednostavno valuacija, je svako preslikavanje $\lambda\colon \mathcal{P} \to 2$, $\mathcal{P}$ je skup iskaznih promenljivih. Ako je $\mathcal{P} = \{p_0, p_1, p_2, \ldots\}$ i $\lambda \in 2^{\mathcal{P}}$, tada

$$\lambda = \begin{pmatrix} p_0 & p_1 & p_2 & \ldots \\ \lambda_0 & \lambda_1 & \lambda_2 & \ldots \end{pmatrix} = \begin{pmatrix} p_i \\ \lambda_i \end{pmatrix}_{i \in N}, \qquad \lambda_i \in \{0, 1\}.$$

Prema tome, $2^{\mathcal{P}} = \{\lambda |\ \lambda\colon \mathcal{P} \to 2\}$ je skup svih iskaznih valuacija. Primetimo da ovaj skup ima moć kontinuuma ukoliko je $\mathcal{P}$ beskonačan prebrojiv skup. Ako je $\mathcal{P}$ konačan i $|\mathcal{P}| = n$, tada $|2^{\mathcal{P}}| = 2^n$.

Definicija 1.3 *Neka je φ iskazna formula i $\lambda \in 2^{\mathcal{P}}$. Vrednost $\varphi[\lambda]$ formule φ za valuaciju λ definišemo na sledeći način:*

V1 *Neka je* $\mathrm{sl}(\varphi) = 0$. *Tada je φ ili neka promenljiva $p \in \mathcal{P}$ ili jedna od logičkih konstanti $\top, \bot$. U prvom slučaju $\varphi[\lambda] = \lambda(p)$. Ako je φ jednaka simbolu $\top$ onda $\varphi[\lambda] = 1$. Ako je φ jednaka simbolu $\bot$ onda $\varphi[\lambda] = 0$.*

V2 *Neka je* $\mathrm{sl}(\varphi) = n, n \in N^+$. *Tada je φ izgrađena od potformula koje imaju složenost manju od n. Naprimer, ako je $\varphi = (\psi \vee \theta)$, tada* $\mathrm{sl}(\psi), \mathrm{sl}(\theta) < n$. *Za φ postoje sledeće mogućnosti:*

$$\begin{array}{lll}
\varphi = (\psi \vee \theta), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \psi[\lambda] \vee_{\mathbf{I}} \theta[\lambda]. \\
\varphi = (\psi \wedge \theta), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \psi[\lambda] \wedge_{\mathbf{I}} \theta[\lambda]. \\
\varphi = (\neg\psi), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \neg_{\mathbf{I}} \psi[\lambda]. \\
\varphi = (\psi \Rightarrow \theta), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \psi[\lambda] \Rightarrow_{\mathbf{I}} \theta[\lambda]. \\
\varphi = (\psi \Leftrightarrow \theta), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \psi[\lambda] \Leftrightarrow_{\mathbf{I}} \theta[\lambda]. \\
\varphi = (\psi \underline{\vee} \theta), & \textit{tada} & \varphi[\lambda] \stackrel{\text{def}}{=} \psi[\lambda] \underline{\vee}_{\mathbf{I}} \theta[\lambda].
\end{array}$$

Neka je dat izbor vrednosti iskaznih promenljivih (nekom valuacijom λ). Shodno prethodnom, ove vrednosti određuju jedinstvenu logičku vrednost svake iskazne formule. Neka je φ iskazna formula. Ako je $\varphi[\lambda] = 1$, tada kažemo da je iskaz φ istinit (tačan, ima logičku vrednost 1, ima istinitosnu vrednost 1) za ovaj izbor (valuacijom λ) vrednosti promenljivih. Slično, ako je $\varphi[\lambda] = 0$, tada kažemo da je za ovaj izbor vrednosti promenljivih iskaz φ neistinit (netačan). S obzirom na definicione tablice iskaznih formula, vidimo da za proizvoljan izbor λ vrednosti iskaznih promenljivih važi:

- Ako je $\varphi = (\psi \vee \theta)$ tada: iskaz φ je istinit akko je bar jedan od iskaza ψ, θ istinit.

- Ako je $\varphi = (\psi \wedge \theta)$ tada: iskaz φ je istinit akko su oba iskaza ψ, θ istinita.
- Ako je $\varphi = (\neg\psi)$ tada: iskaz φ je istinit akko je iskaz ψ neistinit.
- Ako je $\varphi = (\psi \Rightarrow \theta)$ tada: iskaz φ je istinit osim ako je iskaz ψ istinit i θ neistinit.
- Ako je $\varphi = (\psi \Leftrightarrow \theta)$ tada: iskaz φ je istinit akko iskazi ψ, θ imaju iste istinitosne vrednosti.
- Ako je $\varphi = (\psi \underline{\vee} \theta)$ tada: iskaz φ je istinit akko je tačno jedan od iskaza ψ, θ istinit, odnosno ψ i θ imaju suprotne logičke vrednosti.

Prethodnom definicijom opisan je jedan semantički model iskaznog računa. Model je zasnovan na iskaznoj algebri $\mathbf{2_I}$ i u njemu važno mesto ima pojam iskazne valuacije. S obzirom da u formuli φ učestvuje svega konačno mnogo promenljivih, za neko n sve one sadržane su u skupu $\{p_0, p_1, \dots p_n\}$. Otuda, notacijom $\varphi(p_0, p_1, \dots, p_n)$ označavamo činjenicu da su sve promenljive koje imaju pojavljivanje u φ neke od promenljivih $p_0, p_1, \dots, p_n$. Neka je $\varphi = \varphi(p_0, p_1, \dots, p_n)$ iskazna formula i neka su λ, μ valuacije koje imaju iste vrednosti na promenljivama $p_0, p_1, \dots, p_n$. Tada $\varphi[\lambda] = \varphi[\mu]$. Drugim rečima vrednost $\varphi[\lambda]$ ne zavisi od vrednosti $\lambda(p_k)$ za $k > n$. Stoga u određivanju vrednosti $\varphi[\lambda]$ možemo pretpostaviti da je λ *skoro konstantna valuacija*, odnosno da je za neko n i sve $k > n$, $\lambda_k = 0$. Označimo sa $\mathcal{P}_\infty$ skup svih skoro konstantnih valuacija. Tada je $\mathcal{P}_\infty$ *prebrojiv* skup i za svako $\mu \in 2^{\mathcal{P}}$ postoji $\lambda \in \mathcal{P}_\infty$ tako da je $\varphi[\lambda] = \varphi[\mu]$. Ako je $\lambda = \langle \lambda_0, \lambda_1, \dots, \lambda_n, 0, 0 \dots \rangle$, umesto $\varphi[\lambda]$ pišemo takođe $\varphi[\lambda_0, \lambda_1, \dots, \lambda_n]$, odnosno $\varphi(\lambda_0, \lambda_1, \dots, \lambda_n)$.

Spomenuli smo da je za dati izbor vrednosti iskaznih promenljivih jedinstveno određena logička vrednost svake iskazne formule. Deo ovog tvrđenja koje se odnosi na jedinstvenost ove vrednosti nije tako očigledan. Naime, možemo postaviti pitanje da li jedan konačan niz znakova može predstavljati dva različita validna izraza iskazne logike. Drugim rečima, da li izgradnjom na opisani način dve različite formule možemo doći do istog niza znakova. Da je to nemoguće tvrdi sledeća teorema koja se odnosi na terme bilo kojeg algebarskog jezika.

Teorema 1.4 *Neka je u term algebarskog jezika L. Tada je u ili promenljiva, ili simbol konstante, ili postoji tačno jedan funkcijski znak F jezika L i jedinstveni termi $t_1, t_2, \dots, t_n$ jezika L, gde je $n = \mathrm{ar}(F)$, tako da je $u = F(t_1, t_2, \dots, t_n)$.*

U slučaju iskaznog računa jezik L sastoji se iz logičkih simbola i logičkih konstanti. Dokaz ove teoreme izostavljamo.

Neka je φ iskazna formula. U izračunavanju logičkih vrednosti formule φ mogu nastati sledeći slučajevi:

Iskaz φ je istinit za sve vrednosti svojih iskaznih slova, tj. za sve valuacije λ, $\varphi[\lambda] = 1$. U tom slučaju za formulu φ kažemo da je *tautologija*. Ako φ nije tautologija, tj. za neku valuaciju λ važi $\varphi[\lambda] = 0$, onda kažemo da je φ *oboriva formula*. Ako je $\neg\varphi$ tautologija, onda iskaz φ nazivamo *kontradikcijom*. Dakle

u tom slučaju za sve valuacije λ važi $\varphi[\lambda] = 0$. Najzad, ako φ nije kontradikcija, za iskaz φ kažemo da je *ispunjiv*.

Najvažniju klasu iskaznih formula čine tautologije (univerzalno istiniti iskazi). Naime ako iskazna logika zaista predstavlja model ispravnog logičkog zaključivanja, onda tautologije predstavljaju logičke zakone. Da je neka iskazna formula tautologija, može se utvrditi tabličnom metodom – izračunavanjem vrednosti formule φ za sve logičke vrednosti njenih promenljivih.

Primer 1.5 *Neka su* $\varphi = ((p \vee \neg q) \Rightarrow r)$, $\psi = ((p \wedge q) \Rightarrow (q \vee r))$ *i* $\theta = ((p \vee q) \wedge \neg r \wedge (p \Rightarrow r) \wedge (q \Rightarrow r))$. *Istintosne tablice ovih formula su:*

p	q	r	φ	ψ	θ
0	0	0	0	1	0
0	0	1	1	1	0
0	1	0	1	1	0
0	1	1	1	1	0
1	0	0	0	1	0
1	0	1	1	1	0
1	1	0	0	1	0
1	1	1	1	1	0

Uvidom u tablicu nalazimo da je formula ψ tautologija, θ je kontradikcija, dok je φ istovremeno i oboriva i ispunjiva.

Tablični metod provere tautologičnosti nije naročito efikasan. Naime, ako je φ zaista tautlogija, potreban broj provera iznosi 2^n gde je n broj različitih iskaznih slova koje se pojavljuju u φ. Dakle, ovaj metod je primenljiv ako φ ima mali broj iskazih slova. Na primer, ako je $n = 100$, broj ovih provera iznosi preko 10^{30}, što je van domašaja i danas najbržih računara. Postoje razne druge metode za proveru tautologičnosti. Ipak, niti jedna od tih metoda u osnovi nije efikasnija od osnovne - tablične metode. Svaka od poznath metoda zahteva takođe eksponencijalno vreme u odnosu na broj uěstvujućih promenljivih. Ne zna se da li postoji postupak koji problem tautologičnosti rešava za svaku iskaznu formulu u polinomijalnom vremenu. Taj problem poznat je pod imenom *Problem zadovoljivosti* i predstavlja centralni otvoren problem teorijskog računarstva, posebno dela koji se odnosi na oblast složenost algoritama.

Postoje bar dva važna razloga koji čine Problem zadovoljivosti tako značajnim. Prvi razlog leži u činjenici da bi bilo koje rešenje ovog problema rešilo status mnogih drugih algoritamskih zadataka iz algebre, diskretne matematike i algoritmike, s obzirom da je njihovo rešavanje direktno vezano za ovaj problem. Drugi razlog nalazi se u praktičnim primenama iskazne algebre i teorije Bulovih algebri u dizajnu logičkih kola koja čine osnovu savremenih digitalnih računara. Logička kola koja se pojavljuju u elektronskim čipovima sadrže i do nekoliko stotina logičkih elemenata. Najčešće neko kolo K na čipu nastalo je redukcijom broja logičkih elemenata projektovanog kola K' za neku određenu

funkciju. Provera da kolo K obavlja istu funkciju svodi se na proveru zadovoljivosti odnosno tautologičnosti neke složene iskazne formule. Naime, ako je φ iskazna formula koja predstavlja kolo K i φ' kolo K', tada kola K i K' izvršavaju istu funkciju ako i samo ako je $\varphi \Leftrightarrow \varphi'$ tautologija.

Primer 1.6 *Navodimo neke važnije tautologije.*

$\bot \Rightarrow p, \quad p \Rightarrow \top.$	
$(p \wedge (p \vee q)) \Leftrightarrow p,$	apsorpcija konjunkcije prema disjunkciji
$(p \vee (p \wedge q)) \Leftrightarrow p,$	apsorpcija disjunkcije prema konjunkciji
$\neg\neg p \Rightarrow p,$	zakon dvostruke negacije.
$p \vee \neg p,$	zakon isključenja trećeg (tertium non datur).
$p \Rightarrow (q \Rightarrow p),$	Pierce-ov zakon.
$(p \wedge (p \Rightarrow q)) \Rightarrow r.$	Modus Ponens.
$(p \wedge q) \Rightarrow p.$	Slabljenje konjunkcije
$p \Rightarrow (p \vee q).$	Uvodjenje disjunkcije
$(p \wedge q) \Rightarrow (q \wedge p),$	komutativnost konjunkcije.
$(p \vee q) \Rightarrow (q \vee p),$	komutativnost disjunkcije.
$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q),$	De Morganov zakon.
$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q),$	De Morganov zakon.
$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q),$	svodjenje implikacije.
$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p)),$	svođenje ekvivalencije na implikaciju.
$(p \underline{\vee} q) \Leftrightarrow \neg(p \Leftrightarrow q),$	svođenje ekskluzivne disjunkcije.
$((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r)),$	asocijativnost disjunkcije.
$((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r)),$	asocijativnost konjunkcije.
$(p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)),$	distributivnost konjunkcije.
$(p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)),$	distributivnost disjunkcije.
$(p \vee q) \wedge (q \vee r) \wedge (r \vee p) \Leftrightarrow$ $(p \wedge q) \vee (q \wedge r) \vee (r \wedge p),$	Dedekindova tautologija.

Svaka tautologija proizvodi nove tautologije supstitucijom promenljivih iskaznim formulama. O tome govori sledeće tvrđenje.

Stav 1.7 *Princip supstitucije za tautologije. Neka je $\varphi(q_1, q_2, \ldots, q_n)$ tautologija i neka su $\psi_1, \psi_2, \ldots, \psi_n$ bilo koje iskazne formule. Tada je iskazna formula $\theta = \varphi(\psi_1, \psi_2, \ldots, \psi_n)$ takođe tautologija.*

Dokaz Neka je λ bilo koja valuacija i neka su $\mu_1 = \psi[\lambda_1]$, $\mu_2 = \psi[\lambda_2]$, ..., $\mu_n = \psi[\lambda_n]$. Tada $\theta[\lambda] = \varphi[\mu_1, \mu_2, \ldots, \mu_n] = 1$. □

Na primer, zamenjujući u Piercevom zakonu q formulom $p \Rightarrow (q \vee r)$, nalazimo da je $p \Rightarrow ((p \Rightarrow (q \vee r)) \Rightarrow p)$ takođe tautologija.

Činjenicu da je iskazna formula φ tautologija zapisujemo pomoću $\models \varphi$. Oznakom $\models$ uvodi se relacija koju nazivamo *relacijom zadovoljenja* ili relacijom istinitosti. Zapis $\models \varphi$ takođe čitamo φ je univerzalno tačna, odnosno φ je univerzalno istinita formula. Na primer, prema Principu supstitucije i na osnovu De Morganovog zakona, za proizvoljne iskazne formule φ i ψ imamo:

$\models \neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$.

Za iskazne formule i relaciju $\models$ važe mnogobrojna pravila. Svako takvo pravilo odslikava neko svojstvo deduktivnog zaključivanja. Pored toga, pomoću njih mogu se proizvesti, odnosno dokazati nove tautologije na osnovu nekog izabranog skupa tautologija.

Primer 1.8 *U sledećem primeru φ, ψ, θ su proizvoljne iskazne formule. Takođe se implictitno koristi Princip supstitucije.*

Modus ponens: Ako $\models \varphi$ i $\models \varphi \Rightarrow \psi$ onda $\models \psi$.
Tranzitivnost implikacije: Ako $\models \varphi \Rightarrow \psi$ i $\models \psi \Rightarrow \theta$ tada $\models \varphi \Rightarrow \theta$.
Pravilo kontrapozicije: Ako $\models \neg\psi \Rightarrow \neg\varphi$ tada $\models \varphi \Rightarrow \psi$.

Dokažimo, na primer, tranzitivnost implikacije. Pretpostavimo da su $\varphi \Rightarrow \psi$ i $\psi \Rightarrow \theta$ tautologije i neka je λ proizvoljna valuacija.
(1) Ako $\varphi[\lambda] = 0$, prema istinitosnoj tablici za implikaciju važi:
$(\varphi \Rightarrow \theta)[\lambda] = (\varphi[\lambda] \Rightarrow_{\mathbf{I}} \theta[\lambda]) = (0 \Rightarrow_{\mathbf{I}} \theta[\lambda]) = 1$.
(2) Pretpostavimo da je $\varphi[\lambda] = 1$. S obzirom da je $\varphi \Rightarrow \psi$ tautologija, važi $(\varphi \Rightarrow \psi)[\lambda] = 1$, tj. $(\varphi[\lambda] \Rightarrow_{\mathbf{I}} \psi[\lambda]) = 1$. Otuda, opet prema istinitosnoj tablici za implikaciju, nalazimo $\psi[\lambda] = 1$. S obzirom da je $\models \psi \Rightarrow \theta$, koristeći $\psi[\lambda] = 1$ na sličan način nalazimo $\theta[\lambda] = 1$. Otuda i s obzirom na pretpostavku $\varphi[\lambda] = 1$, nalazimo $(\varphi \Rightarrow \theta)[\lambda] = 1$.

S obzirom na (1) i (2), za proizvoljnu valuaciju λ važi $(\varphi \Rightarrow \theta)[\lambda] = 1$, tj. $\models \varphi \Rightarrow \theta$. □

Definicija 1.9 *Iskazne formule φ i ψ su (logički) ekvivalentne akko $\models \varphi \Leftrightarrow \psi$. Da su φ i ψ ekvivalentnne, zapisujemo $\varphi \sim \psi$.*

Stav 1.10 *Relacija $\sim$ je relacija ekvivalencije u skupu $\mathcal{F} = \mathcal{F}_{\mathcal{P}}$ svih iskaznih formula. Takođe, relacija $\sim$ saglasna je sa logičkim veznicima, odnosno važi:*
Ako $\varphi_1 \sim \psi_1$ i $\varphi_2 \sim \psi_2$, tada
$\neg\varphi_1 \sim \neg\psi_1$, $(\varphi_1 \vee \varphi_2) \sim (\psi_1 \vee \psi_2)$, $(\varphi_1 \wedge \varphi_2) \sim (\psi_1 \wedge \psi_2)$,
$(\varphi_1 \Rightarrow \varphi_2) \sim (\psi_1 \Rightarrow \psi_2)$, $(\varphi_1 \Leftrightarrow \varphi_2) \sim (\psi_1 \Leftrightarrow \psi_2)$, $(\varphi_1 \veebar \varphi_2) \sim (\psi_1 \veebar \psi_2)$.

Dokaz Tvrđenje neposrednos sledi na osnovu:
Refleksivnost: $\models \varphi \Leftrightarrow \varphi$.
Simetričnost: ako $\models \varphi \Leftrightarrow \psi$ onda $\models \psi \Leftrightarrow \varphi$.
Tranzitivnost: ako $\models \varphi \Leftrightarrow \psi$ i $\models \psi \Leftrightarrow \theta$, onda $\models \varphi \Leftrightarrow \theta$.
Saglasnost: Pretpostavimo $\models \varphi_1 \Leftrightarrow \psi_1$ i $\models \varphi_2 \Leftrightarrow \psi_2$. Tada
$\models \neg\varphi_1 \Leftrightarrow \neg\psi_1$, $\models (\varphi_1 \vee \varphi_2) \Leftrightarrow (\psi_1 \vee \psi_2)$, $\models (\varphi_1 \wedge \varphi_2) \Leftrightarrow (\psi_1 \wedge \psi_2)$,
$\models (\varphi_1 \Rightarrow \varphi_2) \Leftrightarrow (\psi_1 \Rightarrow \psi_2)$, $\models (\varphi_1 \Leftrightarrow \varphi_2) \Leftrightarrow (\psi_1 \Leftrightarrow \psi_2)$,
$\models (\varphi_1 \veebar \varphi_2) \Leftrightarrow (\psi_1 \veebar \psi_2)$. □

Ako su p i q različita iskazna slova, tada ovigledno $p \Leftrightarrow q$ nije tautologija, dakle $p \not\sim q$. Otuda sledi da klasa ekvivalencija ima bar koliko i iskaznih slova. Na primer, pretpostavimo da je $\mathcal{P}$ prebrojiv. Tada je $\mathcal{F}/\sim$ bar prebrojiv skup. S druge strane, iskaznih formula nad najviše prebrojivim skupom iskaznih slova ima prebrojivo mnogo, dakle i $\mathcal{F}$ je najviše prebrojiv skup, pa otuda $|\mathcal{F}| = \aleph_0$.

1.3 Normalne forme iskaznih formula

Neka je $\varphi/_\sim = \{\psi \in \mathcal{F}_\mathcal{P}: \psi \sim \varphi\}$ klasa logičke ekvivalencije iskazne formule φ sa skupom iskaznih slova u $\mathcal{P}$. Dakle $\varphi/_\sim$ je skup svih formula iz $\mathcal{F}_\mathcal{P}$ logički ekvivalentnih φ. Prirodno je pitanje da li se može učiniti nekakav izbor kanonskih predstavnika iz ovih klasa ekvivalencija. Takav izbor postoji i u opisu kanonskih predstavnika učestvuju sledeći pojmovi. S obzirom da logička vrednost formule φ zavisi jedino od učestvujućih iskaznih promenljivih, pretpostavićemo da je $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$, gde je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$ i $n \in N^+$.

Definicija 1.11 *Neka je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, $n \in N^+$, iskazna formula. Iskazna funkcija pridružena formuli φ je preslikavanje $\hat{\varphi}: 2^n \to 2$ definisano na sledeći način:*

$$\hat{\varphi}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \varphi[\lambda], \quad \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n), \quad \lambda: \mathcal{P} \to 2.$$

Za preslikavanje $f: 2^n \to 2$, $n \in N^+$, kažemo da je *iskazna funkcija* ukoliko postoji iskazna formula $\varphi(p_1, p_2, \ldots, p_n)$ tako da je $f = \hat{\varphi}$. S obzirom na tablicu iskazne operacije $\Leftrightarrow_1$, vidimo da je za proizvoljne formule $\varphi, \psi \in \mathcal{F}_\mathcal{P}$, $\varphi \sim \psi$ akko $\hat{\varphi} = \hat{\psi}$. Dakle $\varphi/_\sim = \{\psi \in \mathcal{F}_\mathcal{P}: \hat{\psi} = \hat{\varphi}\}$.

Definicija 1.12 *Literali i disjunktivna normalna forma skupa iskaznih promenljivih $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$.*

Literal iskazne promenljive $p \in \mathcal{P}$ je $\neg p$ ili samo slovo p.

Neka su $q_1, q_2, \ldots, q_k \in \mathcal{P}$ različita iskazna slova, i neka su $r_1, r_2, \ldots, r_k$ redom jedan izbor literala ovih iskaznih promenljivih. Formula $\psi = r_1 \wedge r_2 \wedge \ldots \wedge r_k$ naziva se elementarnom konjunkcijom literala nad $\mathcal{P}$. Literali su takođe elementarne konjunkcije. Ako je $k = n$, onda se ψ naziva potpunom elementarnom konjunkcijom (literala nad $\mathcal{P}$).

Neka su $\theta_1, \theta_2, \ldots, \theta_m$ u parovima logički neekvivalentne elementarne konjunkcije nad $\mathcal{P}$. Disjunkcija $\theta = \theta_1 \vee \theta_2 \vee \ldots \vee \theta_m$ naziva se disjunktivnom normalnom formom nad $\mathcal{P}$, skraćeno DNF. Ako je svaka elementarna konjunkcija θ_i potpuna, onda se disjunkcija θ naziva potpunom ili savršenom DNF, kratko SDNF.

Naprimer, neka je $\mathcal{P} = \{p, q, r\}$ skup sastavljen od tri različita iskazna slova. Tada je S skup svih literala nad $\mathcal{P}$, dok je T skup nekih elementarnih konjunkcija nad $\mathcal{P}$:

$$S = \{p, \neg p, q, \neg q, r, \neg r\}, \quad T = \{p, \neg q, p \wedge q, \neg p \wedge r, p \wedge \neg q \wedge r\}.$$

Poslednja konjunkcija u T je potpuna. Formula φ je DNF dok je ψ primer SDNF nad $\mathcal{P}$:

$$\varphi = p \vee (\neg q \wedge r) \quad \psi = (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r)$$

Dakle, u slučaju tročlanog $\mathcal{P}$ ima tačno 6 literala. Ukoliko ne razlikujemo logički ekvivalentne formule, tj. do na logičku ekvivalenciju u istom slučaju ima tačno 26 elementarnih konjunkcija, 8 potpunih elementarnih konjunkcija i 255 SDNF.

Uvedimo sledeću notaciju: $\varphi^1 \stackrel{\text{def}}{=} \varphi$, $\varphi^0 \stackrel{\text{def}}{=} \neg\varphi$, φ je proizvoljna iskazna formula. Ako je $\alpha \in 2^n$, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, i $\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_n)$ je niz iskaznih formula, onda je

$$\varphi^\alpha \stackrel{\text{def}}{=} \bigwedge_{1\le i\le n} \varphi_i^{\alpha_i} \stackrel{\text{def}}{=} \varphi_1^{\alpha_1} \wedge \varphi_2^{\alpha_2} \wedge \ldots \wedge \varphi_n^{\alpha_n}.$$

Ukoliko kontekst dozvoljava, na primer ako je u datom razmatranju n fiksiran broj, umesto $\bigwedge_{1\le i\le n} \varphi_i$ pisaćemo jednostavno $\bigwedge_i \varphi_i$.

Neka je S_θ skup literala od kojih je sagrađena elementarna konjunkcija θ. Tada je θ konjunkcja literala iz S_θ i s obzirmo da važe zakoni asocijacije i komutacije za konjunkciju, možemo pisati $\theta = \bigwedge_{\vartheta\in S_\theta} \vartheta$. Takođe, dve elementarne konjunkcije θ_1 i θ_2 su (logički) ekvivalentne akko $S_{\theta_1} = S_{\theta_2}$. Otuda, nećemo razlikovati elementarne konjunkcije koje imaju iste skupove literale. Radi određenosti, često se pretpostavlja nekakav poredak $\prec$ među iskaznim slovima, na primer leksikografski ili onaj induciran indeksima (slovo p_i prethodi p_j ukoliko je $i < j$). U tom slučaju međusobno ekvivalentne elementarne konjunkcije imaju jedinstvenog predstavnika, to je konjunkcija literala u kojoj se iskazna slova pojavljuju u poretku $\prec$ od manjeg ka većem. U prethodnom primeru $\mathcal{P} = \{p, q, r\}$, izabran je leksikografski poredak slova p, q, r i sve navedene elementarne konjunkcije imaju opisani zapis. Alternativno, elementarna konjunkcija θ može se identifikovati sa skupom S_θ. Prethodne napomene mogu biti od interesa za programsku implementaciju raznih sintaktičkih algoritama iz oblasti logike.

Za skup iskaznih slova $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$, elementarna konjunkcija θ biće potpuna akko je skup $S_\theta \cap \{p, \neg p\}$ jednočlan za svako $p \in \mathcal{P}$, odnosno $\theta = \bigwedge_i p_i^{\alpha_i}$ za neko $\alpha \in 2^n$.

Lema 1.13 *Neka je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, $n \in N^+$, iskazna formula. Tada je φ logički ekvivalentna iskaznoj formuli*
$\psi = (\varphi(p_1, p_2, \ldots, p_{n-1}, \top) \wedge p_n) \vee (\varphi(p_1, p_2, \ldots, p_{n-1}, \bot) \wedge \neg p_n)$.

Dokaz S obzirom da je $\varphi \sim \psi$ akko $\hat{\varphi} = \hat{\psi}$, dovoljno je dokazati $\hat{\varphi} = \hat{\psi}$, dakle da je

$$\hat{\varphi}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{array}{l}(\hat{\varphi}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1) \wedge_{\mathbf{I}} \lambda_n) \vee_{\mathbf{I}} \\ (\hat{\varphi}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 0) \wedge_{\mathbf{I}} \neg_{\mathbf{I}} \lambda_n)\end{array}, \quad \lambda_1, \lambda_2, \ldots, \lambda_n \in \{0, 1\}.$$

Ovaj identitet se trivijalno proverava birajući redom vrednosti $0, 1$ za λ_n. □

Imajući u vidu da je $\top_{\mathbf{I}} = 1$ i $\bot_{\mathbf{I}} = 0$, neposredno se proverava da su, na primer, iskazne formule $\top \Rightarrow \bot$ i $\bot$ logički ekvivalentne, tj. $\models (\top \Rightarrow \bot) \Leftrightarrow \bot$. Isto tako odmah se vidi da su iskazne formule $\top \Rightarrow \top$, $\bot \Rightarrow \bot$, $\bot \Rightarrow \top$ logički ekvivalentne formuli $\top$. Drugim rečima, istinitosna tablica implikacije ugrađena je u iskazni račun u sledećem smislu. Primetimo da je iskazna tablica za implikaciju (definicija funkcije $\Rightarrow_{\mathbf{I}}$) zapravo skup četiri jednakosti: $0 \Rightarrow_{\mathbf{I}} 0 = 1$, $0 \Rightarrow_{\mathbf{I}} 1 = 1$, $1 \Rightarrow_{\mathbf{I}} 0 = 9$, $1 \Rightarrow_{\mathbf{I}} 1 = 1$. Ukoliko se 0 zameni simbolom $\bot$ i 1 simbolom $\top$ i ako se umesto jednakosti uzme logička ekvivalencija, dobićemo

upravo opisane logičke ekvivalencije za implikaciju i logičke konstante $\top, \bot$. Slična činjenica važi i za ostale logičke veznike i ona se predstavlja pomoću *iskaznih tablica*:

$\vee$	$\bot$	$\top$
$\bot$	$\bot$	$\top$
$\top$	$\top$	$\top$

$\wedge$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$

p	$\neg p$
$\bot$	$\top$
$\top$	$\bot$

$\Rightarrow$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$

$\Leftrightarrow$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\top$

$\veebar$	$\bot$	$\top$
$\bot$	$\bot$	$\top$
$\top$	$\top$	$\bot$

Prethodno razmatranje i sledeće tvrđenje pokazuje da je iskazna algbera ugrađena u iskazni račun.

Lema 1.14 *Neka je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, $n \in N^+$, iskazna formula i neka su $\theta_1, \theta_2, \ldots, \theta_n \in \{\top, \bot\}$. Tada je $\varphi(\theta_1, \theta_2, \ldots, \theta_n)$ logički ekvivalentna ili $\top$ ili $\bot$.*

Dokaz Tvrđenje se neposredno dokazuje indukcijom po broju iskaznih slova na osnovu Leme 1.13 i iskaznih tablica za konjunkciju, disjunkciju i negaciju. □

Drugi dokaz prethodne leme može se izvesti indukcijom po složenosti iskazne formule koristeći iskazne tablice logičkih veznika. Logički ekvivalent formule $\varphi(\theta_1, \theta_2, \ldots, \theta_n)$ može se tačno utvrditi. S obzirom da je $\theta_i \in \{\top, \bot\}$, logička vrednost α_i formule θ_i ne zavisi od izbora valuacije iskaznih promenljivih. Neka je $\beta = \hat{\varphi}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ i neka je $\theta = \top$ ako je $\beta = 1$, odnosno $\theta = \bot$ ako je $\beta = 0$. Tada $\varphi \sim \theta$.

Teorema 1.15 (**Teorema o SDNF**) *Neka je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, $n \in N^+$, iskazna formula, $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ i neka je $\Gamma = \{\lambda \in 2^{\mathcal{P}} : \varphi[\lambda] = 1\}$. Ako je $\Gamma \neq \emptyset$, odnosno φ nije kontradikcija, onda je φ logički ekvivalentna formuli*

$$\psi = \bigvee_{\alpha \in \Gamma} \bigwedge_i p_i^{\alpha_i}.$$

Dokaz Dovoljno je dokazati da je $\hat{\varphi} = \hat{\psi}$. Ovu jednakost možemo dokazati, na primer, indukcijom po broju n iskaznih slova koristeći Lemu 1.13. Ovde dajemo jedan direktan dokaz.

Neka je $p \in \mathcal{P}$, λ valuacija promenljivih iz $\mathcal{P}$, $\mu = \lambda(p)$ i $\nu \in \{0, 1\}$. S obzirom na definiciju iskazne formule p^ν, vidimo da je $p^\nu[\lambda] = 1$ akko $\mu = \nu$. Neka je $\theta_\alpha = \bigwedge_i p_i^{\alpha_i}$, $\alpha \in 2^n$. Za datu valuaciju, konjunkcija iskaznih formula ima logičku vrednost 1 akko svaki član konjunkcije ima vrednost 1. Otuda $\theta_\alpha[\lambda] = 1$ akko $\lambda = \alpha$. Shodno ovom razmatarnju imamo:

S obzirom da $\Gamma \neq \emptyset$, disjunkcija ψ postoji i ima bar jedan član. Dalje, neka je $\hat{\varphi}(\lambda) = 1$. Tada $\lambda \in \Gamma$, dakle θ_λ je član disjunkcije $\psi = \bigvee_\alpha \theta_\alpha$ i $\theta_\lambda[\lambda] = 1$. Za datu valuaciju disjunkcija iskaznih formula ima logičku vrednost 1 akko bar

jedan član disjunkcije ima logičku vrednost 1, odakle sledi $\hat{\psi}[\lambda] = 1$. Otuda, ako $\hat{\varphi}(\lambda) = 1$ onda $\hat{\psi}[\lambda] = 1$. Ako $\hat{\varphi}(\lambda) = 0$ tada za sve $\alpha \in \Gamma$ važi $\theta_\alpha[\lambda] = 0$, odakle sledi $\hat{\psi}[\lambda] = 0$. Dakle, ako $\hat{\varphi}(\lambda) = 0$ onda $\hat{\psi}[\lambda] = 0$. S obzirom da je $\hat{\varphi}(\lambda) \in \{0, 1\}$ za sve valuacije λ, sledi $\hat{\varphi}(\lambda) = \hat{\psi}(\lambda)$. □

Primetimo da ako za $\Gamma = \emptyset$ uzmemo da je $\bigvee_{\alpha\in\Gamma} \theta_\alpha \stackrel{\text{def}}{=} \bot$, tada iskaz teoreme važi za proizvoljnu formulu φ. Teorema o SDNF govori o kanonskoj reprezentaciji iskaznih formula i ima više važnih posledica.

Teorema 1.16 (**Teorema funkcionalne potpunosti**) *Neka je* $f\colon 2^n \to 2$, $n \in N^+$, *proizvoljna funkcija. Tada postoji iskazna formula* $\varphi = \varphi(p_1, p_2, \ldots, p_n)$ *tako da je* $f = \hat{\varphi}$.

Dokaz Ukoliko je $f(\lambda_1, \lambda_2, \ldots, \lambda_n) = 0$ za svaki $\lambda \in 2^n$ uzećemo $\varphi = \bot$. Pretpostavimo da je $f(\lambda_1, \lambda_2, \ldots, \lambda_n) = 1$ za neki $\lambda \in 2^n$ i neka je

$$\Gamma = \{\lambda \in 2^n \colon f(\lambda_1, \lambda_2, \ldots, \lambda_n) = 1\}.$$

Tada $\Gamma \neq \emptyset$, dakle disjunkcija $\varphi(p_1, p_2, \ldots, p_n) = \bigvee_{\alpha\in\Gamma} \bigwedge_i p_i^{\alpha_i}$ postoji i ima bar jedan član. S obzirom da za svaki $\lambda \in 2^n$ važi $\hat{\varphi}[\lambda] = 1$ akko $\lambda \in \Gamma$ akko $f(\lambda_1, \lambda_2, \ldots, \lambda_n) = 1$, to je $f = \hat{\varphi}$. □

U savremenom računarstvu digitalni računari se sa matematičkog stanovišta identifikuju sa Turingovom mašinom. Drugim rečima skup Turing-izračunljivih funkcija tačno je skup izračunljivih funkcija pomoću nekog idealnog digitalnog računara, bez obzira na hardversku realizaciju samog računara ili izbor programskog jezika. Pod idejom "idealnog" pretpostavljamo da računar nema fizička ograničenja, kao što su ograničenost memorije ili ograničenost dužine izračunavanja. Stvarni računari, naravno, imaju ta ograničenja i u osnovi svako izračunavanje je konačno i ostvaruje se u domenu konačnih binarnih nizova. U tom pogledu logička kola predstavljaju matematičku osnovu hardverske realizacije savremenih digitalnih računara. S druge strane svako logičko kolo predstvaljeno je nekom iskaznom formulom. Teorema funkcionalne potpunosti iskaznog računa tvrdi da se *zaista* proizvoljna binarna funkcija može realizovati pomoću logičkih kola. Dokaz ove teoreme daje i metod direktne konstrukcije iskazne formule $\varphi(p_1, p_2, \ldots, p_n)$ za datu funkciju $f\colon 2^n \to 2$.

Primer 1.17 *Neka je* $f\colon 2^3 \to 2$ *zadata tablicom:*

p	q	r	f
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Ovde
$\Gamma = \{(0,0,1), (0,1,0), (0,1,1), (1,0,1), (1,1,1)\}$.

$$\begin{aligned}\varphi(p,q,r) = \quad & (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee \\ & (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee \\ & (p \wedge q \wedge r)\end{aligned}$$

Primetimo da postoje jednostavnije iskazne formule koje reprezentuju f. Na primer, formula $\psi = (\neg p \wedge q) \vee r$. Tada $f = \hat{\varphi} = \hat{\psi}$.

Shodno prethodnom, pod iskaznom funkcijom podrazumevaćemo bilo koje preslikavanje $f: 2^n \to 2$. Dakle, 2^{2^n}, $n \in N$ je skup svih iskaznih funkcija koje imaju n promenljivih. Nad ovim skupom mogu se uočiti mnoge zanimljive operacije i relacije. Na primer, za $f, g: 2^n \to 2$ možeo definsati relaciju nejednakosti na sledeći način:

$$f \leq g \qquad \text{akko} \qquad \text{za svako } \alpha \in 2^n \;\; f(\alpha) \leq g(\alpha).$$

Nije teško proveriti da je $(2^{2^n}, \leq)$ parcijalno uređen skup, da ima najmanji element $\mathbf{0}$ (konstantna funkcija čije su sve vrednosti 0) i da ima najveći element $\mathbf{1}$ (konstantna funkcija čije su sve vrednosti 1). Jednostavno se proverava da važi sledeće tvrđenje.

Stav 1.18 *Neka su φ, ψ proizvoljne iskazne formule nad istim skupom iskaznih slova. Tada $\models \varphi \Rightarrow \psi$ akko $\hat{\varphi} \leq \hat{\psi}$.*

□

Neka su φ i θ iskazne formule nad skupom iskaznih slova $\mathcal{P}$ i neka je $p \in \mathcal{P}$. Term $\varphi_p(\theta)$ označava iskaznu formulu dobijenu iz φ supstitucijom formulom θ svakog pojavljivanja u φ iskaznog slova p. Ako se p ne pojavljuje u φ, onda je $\varphi_p(\theta) = \varphi$. Ako su $p_1, p_2, \ldots, p_n \in \mathcal{P}$ različite promenljive, tada je $\varphi_{p_1 p_2 \ldots p_n}(\theta_1, \theta_2, \ldots, \theta_n)$ iskazna formula dobijena iz formule φ simultanom i uniformnom suspstitucijom promenljivih $p_1, p_2, \ldots, p_n$ formulama $\theta_1, \theta_2, \ldots, \theta_n$. Na primer, ako je $\varphi = (p \Rightarrow (q \vee r))$, onda je $\varphi_{pq}(\theta_1, \theta_2) = (\theta_1 \Rightarrow (\theta_2 \vee r))$. Ako je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, vidimo da je $\varphi_{p_1 p_2 \ldots p_n}(\theta_1, \theta_2, \ldots, \theta_n) = \varphi(\theta_1, \theta_2, \ldots, \theta_n)$. Ako je $A = \{p_1, p_2, \ldots, p_n\}$, pretpostavljajući nekakav poredak u skupu promenljivih (na primer leksikografski ili induciran poretkom na indeksima), pisaćemo $\varphi_A(\theta_1, \theta_2, \ldots, \theta_n)$ umesto $\varphi_{p_1 p_2 \ldots p_n}(\theta_1, \theta_2, \ldots, \theta_n)$.

Primer 1.19 *Neka je φ iskazna formula i p iskazno slovo. Tada postoji formula θ tako da je $\models \theta \Leftrightarrow \varphi_p(\theta)$ akko $\models \varphi_p(\bot) \Rightarrow \varphi_p(\top)$.*

Dokaz Pretpostavimo da je $\models \theta \Leftrightarrow \varphi_p(\theta)$. Prema Lemi 1.14 tada važi

$$\theta \sim (\varphi_p(\top) \wedge \theta) \vee (\varphi_p(\bot) \wedge \neg\theta) \tag{1.2}$$

Otuda sledi $\theta \sim (\varphi_p(\top) \wedge \theta)$ i $(\varphi_p(\bot) \wedge \neg\theta) \sim \bot$, odakle $\models \theta \Rightarrow \varphi_p(\top)$ i $\models \varphi_p(\bot) \Rightarrow \theta$, tj. $\models \varphi_p(\bot) \Rightarrow \varphi_p(\top)$. Radi dokaza druge strane tvrđenja, pretpostavimo uslov $\models \varphi_p(\bot) \Rightarrow \varphi_p(\top)$ i neka je θ bilo koja od formula $\varphi_p(\bot), \varphi_p(\top)$. Tada važi $\theta \sim (\varphi_p(\top) \wedge \theta)$ i $(\varphi_p(\bot) \wedge \neg\theta) \sim \bot$, dakle važi i ekvivalencija 1.2, tj. $\models \theta \Leftrightarrow \varphi_p(\theta)$. □

Za iskaznu formulu φ, neka P_φ označava skup iskaznih slova koja se javljaju u φ. Na primer, ako je $\varphi = ((p \vee q) \Rightarrow r))$, tada $P_\varphi = \{p, q, r\}$.

Teorema 1.20 (**Teorema interpolacije**) *Neka su φ i ψ iskazne formule nad skupom iskaznih promeljivih $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$. Ako $\models \varphi \Rightarrow \psi$ tada postoji iskazna formula θ takva da je $\models \varphi \Rightarrow \theta$, $\models \theta \Rightarrow \psi$ i $P_\theta \subseteq P_\varphi \cap P_\psi$.*

Dokaz Pretpostavimo $\models \varphi \Rightarrow \psi$. Neka je A skup svih iskaznih slova koja se javljaju samo u φ. Ako je $A = \emptyset$ očigledno možemo uzeti da je $\theta = \varphi$. Pretpostavimo da je $A \neq \emptyset$ u neka je $A = \{p_1, p_2, \ldots, p_n\}$. Dalje, uzmimo $X = \{\top, \bot\}^n$ i neka $\vartheta = (\vartheta_1, \vartheta_2, \ldots, \vartheta_n)$ označava bilo koji član skupa X. Dokazaćemo da formula

$$\theta = \bigvee_{\vartheta \in X} \varphi_A(\vartheta_1, \vartheta_2, \ldots, \vartheta_n)$$

zadovoljava iskaz Teoreme. Najpre primetimo da je očigledno $P_\theta \subseteq P_\varphi \cap P_\psi$. Neka je p proizvoljno iskazno slovo iz A, recimo p_n i neka su λ i μ valuacije promenljivih iz $\mathcal{P}$ koje se razlikuju samo u p: $\lambda(p) = 1$ i $\mu(p) = 0$. S obzirom da se p ne pojavljuje u formuli ψ, to je $\psi[\lambda] = \psi[\mu]$. Kako je

$$\varphi \sim (\varphi_p(\top) \wedge p) \vee (\varphi_p(\bot) \wedge \neg p)$$

i prema pretpostavci $\hat{\varphi} \leq \hat{\psi}$, važi

$$\varphi_p(\top)[\lambda] = \varphi[\lambda] \leq \psi[\lambda], \qquad \varphi_p(\bot)[\lambda] = \varphi[\mu] \leq \psi[\mu],$$
$$\varphi_p(\top)[\mu] = \varphi[\lambda] \leq \psi[\lambda], \qquad \varphi_p(\bot)[\mu] = \varphi[\mu] \leq \psi[\mu].$$

S obzirom na proizvoljnost izbora valuacije λ (i μ), sledi

$\models \varphi_p(\top) \Rightarrow \psi$, $\models \varphi_p(\bot) \Rightarrow \psi$, odakle $\models (\varphi_p(\top) \vee \varphi_p(\bot)) \Rightarrow \psi$. Primenjujući isti postupak na formule $\varphi_p(\top) \vee \varphi_p(\bot)$ (umesto na φ) i ψ i promenljivu $q = p_{n-1}$, nalazimo

$$\models (\varphi_{pq}(\top, \top) \vee \varphi_{pq}(\top, \bot) \vee \varphi_{pq}(\bot, \top) \vee \varphi_{pq}(\bot, \bot)) \Rightarrow \psi,$$

i dalje na promenljive $p_{n-2}, \ldots, p_1$, dobijamo

$$\models \bigvee_{\vartheta \in X} \varphi_A(\vartheta_1, \vartheta_2, \ldots, \vartheta_n) \Rightarrow \psi,$$

tj. $\models \theta \Rightarrow \psi$.

Dokazujemo da je $\models \varphi \Rightarrow \theta$. Neka je λ proizvoljna valuacija promenljivih iz $\mathcal{P}$. Ako je $\varphi[\lambda] = 0$ onda očigledno $\varphi[\lambda] \leq \psi[\lambda]$. Pretpostavimo $\varphi[\lambda] = 1$ i neka je $\vartheta'_i = \top$ ako je $\lambda[p_i] = 1$, odnosno $\vartheta'_i = \bot$ ako je $\lambda[p_i] = 0$, $1 \leq i \leq n$. Tada $\varphi_A(\vartheta'_1, \vartheta'_2, \ldots, \vartheta'_n)[\lambda] = 1$, stoga $\bigvee_{\vartheta \in X} \varphi_A(\vartheta_1, \vartheta_2, \ldots, \vartheta_n)[\lambda] = 1$, s obzirom da je $(\vartheta'_1, \vartheta'_2, \ldots, \vartheta'_n) \in X$. Dakle, $\varphi[\lambda] = 1$ povlači $\theta[\lambda] = 1$, odnosno $\varphi[\lambda] \leq \theta[\lambda]$, tj. $\models \varphi \Rightarrow \theta$. □

Jedna od kritika klasičnog iskaznog računa odnosi se na nerelevantnost implikacije. Naime, prema ovoj kritici ako je formula $\varphi \Rightarrow \psi$ istinit iskaz u nekom logičkom sistemu, onda bi iskazi φ i ψ trebalo da se odnose na isti subjekt. U slučaju klasičnog iskaznog računa, koji se predstavlja u ovoj knjizi, možemo uzeti da je subjekt reprezentovan nekim iskaznim slovom. U slučaju tautologija $(p \wedge \neg p) \Rightarrow q$ ili $p \Rightarrow (q \vee \neg q)$, vidimo da relevantnost u opisanom smislu zaista nije zastupljena. Eliminacija ovog problema motivisala je razvoj drugih formalnih sistema (logika) u kojima glavno mesto ima implikacija. Ipak, sledeće tvrđenje daje jedan odgovor na ovu kritiku. Istovremeno ono pokazuje da su navedeni primeri zapravo i jedini slučajevi nerelevantnosi tautologija vida $\varphi \Rightarrow \psi$.

Teorema 1.21 (**Teorema relevantnosti**) *Neka su φ i ψ iskazne formule nad istim skupom iskaznih slova. Ako je $\models \varphi \Rightarrow \psi$, φ nije kontradikcija i ψ nije tautologija, onda φ i ψ imaju zajedničko iskazno slovo.*

Dokaz Prema teoremi interpolacije postoji formula θ tako da su formule $\varphi \Rightarrow \theta$ i $\theta \Rightarrow \psi$ tautologije i $P_\theta \subseteq P_\varphi \cap P_\psi$. Otuda, ako pretpostavimo $P_\varphi \cap P_\psi = \emptyset$ onda je i $P_\theta = \emptyset$, tj. θ ne sadrži iskazna slova. Dakle, prema Lemi 1.14, θ je tautologija ili kontradikcija, pa možemo uzeti da je je $\theta \in \{\top, \bot\}$. Ako je $\theta = \bot$, onda, uzimajući u obzir da je $\models \varphi \Rightarrow \theta$, sledi da je φ kontradikcija, suprotno pretpostavci teoreme. Slično, s obzirom da je $\theta \Rightarrow \psi$, ako je $\theta = \top$ onda je ψ tautologija, takođe suprotno pretpostavci teoreme. Dakle $P_\theta \neq \emptyset$ $\square$.

1.4 Princip dualnosti

Radi bolje preglednosti, za iskaznu operaciju negacije koristićemo sledeću notaciju: $\bar{x} \stackrel{\text{def}}{=} \neg_{\mathbf{I}} x$. Naprimer, De Morganovi obrasci u novoj notaciji glase:

$$\overline{(x \vee_{\mathbf{I}} y)} = \bar{x} \wedge_{\mathbf{I}} \bar{y}, \quad \overline{(x \wedge_{\mathbf{I}} y)} = \bar{x} \vee_{\mathbf{I}} \bar{y}.$$

Isti primer pokazuje da između konjunkcije i disjunkcije postoji veza koju opisujemo kao *dualnost*. Slična veza postoji i za neke druge parove iskaznih funkcija. Ovaj pojam ima važno mesto u ispitivanju svojstava iskaznih funkcija. Sledećom definicijom uvodimo operator dualnosti f^*.

Definicija 1.22 *Ako je $f\colon 2^n \to 2$, tada $f^*(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \bar{f}(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$. Iskazne funkcije $f, g\colon 2^n \to 2$ su dualne ukoliko za svaki $\alpha \in 2^n$ važi jednakost $f(\alpha_1, \alpha_2, \ldots, \alpha_n) = g^*(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

U sledećem tvrđenju iskazana su osnovna svojstva operatora * i relacije dualnosti. Prema istom tvrđenju konjunkcija i disjunkcija su uzajamno dulane, zatim ekskluzivna disjunkcija i ekvivalencija su uzajamno dualne i negacija je dualna samoj sebi.

Stav 1.23 *Neka su $f, g\colon 2^n \to 2$, $n \in N^+$. Tada*

1° $\top^* = \bot, \quad \bot^* = \top, \quad x^* = x, \quad \bar{x}^* = \bar{x}, \quad f^{**} = f.$

2° *Relacija dualnosti je simetrična relacija u skupu svih iskaznih funkcija n promenljivih.*

3° $(f \vee_{\mathbf{I}} g)^* = f^* \wedge_{\mathbf{I}} g^*, \ (f \wedge_{\mathbf{I}} g)^* = f^* \vee_{\mathbf{I}} g^*, \ (f \Rightarrow_{\mathbf{I}} g)^* = \overline{(g^* \Rightarrow_{\mathbf{I}} f^*)},$
$(f \veebar_{\mathbf{I}} g)^* = f^* \Leftrightarrow_{\mathbf{I}} g^*, \ (f \Leftrightarrow_{\mathbf{I}} g)^* = f^* \veebar_{\mathbf{I}} g^*$

Dokaz Tvrđenje je neposredna posledica identiteta $\bar{\bar{x}} = x$:

1° $f^{**}(x_1, x_2, \ldots, x_n) = \bar{\bar{f}}(\bar{\bar{x}}_1, \bar{\bar{x}}_2, \ldots, \bar{\bar{x}}_n) = f(x_1, x_2, \ldots, x_n).$

2° Ako je $g = f^*$, tada $f = f^{**} = g^*$.

3° $(f \vee_{\mathbf{I}} g)^* = \overline{(f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \vee_{\mathbf{I}} g(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n))} =$
$\bar{f}(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \wedge_{\mathbf{I}} \bar{g}(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) = f^* \wedge_{\mathbf{I}} g^*.$

$\square$

Relacija dualnosti i operator * u vezi su sa sledećim izomorfizmom. Neka su $\mathbf{B}_2 = (2, \vee_{\mathbf{I}}, \wedge_{\mathbf{I}}, \neg_{\mathbf{I}}, \Leftrightarrow_{\mathbf{I}}, \underline{\vee}_{\mathbf{I}}, 0, 1)$ i $\mathbf{B}_2^* = (2, \wedge_{\mathbf{I}}, \vee_{\mathbf{I}}, \neg_{\mathbf{I}}, \underline{\vee}_{\mathbf{I}}, \Leftrightarrow_{\mathbf{I}}, 1, 0)$. Za algebru $\mathbf{B}_2^*$ kažemo da je dualna algebri $\mathbf{B}_2$. Shodno prethodnom, neposredno se proverava da je preslikavanje $\mathbf{h}: x \to \bar{x}$, $x \in 2$, izomorfizam ovih algebri. Kao posledicu dobijamo sledeće tvrđenje.

Teorema 1.24 (**Princip dualnosti**) *Neka je $\varphi = \varphi(\vee, \wedge, \underline{\vee}, \Leftrightarrow, \neg, \top, \bot)$ rečenica predikatskog računa prvog reda nad jezikom iskazne algebre*

$$L = \{\vee, \wedge, \underline{\vee}, \Leftrightarrow, \neg, \top, \bot\}$$

i neka je $\varphi^* = \varphi(\wedge, \vee, \Leftrightarrow, \underline{\vee}, \neg, \bot, \top)$, formula dobijena iz φ uzajamnom razmenom mesta simbola $\vee$ i $\wedge$, zatim $\underline{\vee}$ i $\Leftrightarrow$ i najzad $\top$ i $\bot$ u formuli φ. Uz prirodnu interpretaciju simbola jezika L u algebri $\mathbf{B}_2$ (simbol disjunkcije $\vee$ interpretiran iskaznom operacijom disjunkcije $\vee_{\mathbf{I}}$, itd.), φ istinita je u $\mathbf{B}_2$ akko je φ^* istinita u $\mathbf{B}_2$.

Dokaz Tvrđenje je neposredna posledica činjenice da je $\mathbf{h}: \mathbf{B}_2 \simeq \mathbf{B}_2^*$. Strog dokaz izvodi se indukcijom po složenosti formule φ. O takvim dokazima biće više reči u poglavlju o predikatskom računu. □

Uz pomoć principa dualnosti ne samo da možemo dokazivati nova tvrđenja, već možemo uvoditi i nove pojmove. Jedan važan primer takve primene Principa dualnosti je izgradnja pojmova konjunktivne normalne forme i SKNF (savršene konjunktivne normalne forme). Ovi pojmovi nastaju potpunom dualizacijom definicija i tvrđenja koji se odnose na disjunktivnu normalnu formu i SDNF, dakle najvećeg dela prethodnog poglavlja. Na primer, Definicija 1.12 posle dualizacije izgleda

Definicija 1.25 *Literali i konjunktivna normalna forma skupa iskaznih promenljivih $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$.*

Literal iskazne promenljive $p \in \mathcal{P}$ je $\neg p$ ili samo slovo p.

Neka su $q_1, q_2, \ldots, q_k \in \mathcal{P}$ različita iskazna slova, i neka su $r_1, r_2, \ldots, r_k$ jedan izbor literala ovih iskaznih promenljivih. Formula $\psi = r_1 \vee r_2 \vee \ldots \vee r_k$ naziva se elementarnom disjunkcijom literala nad $\mathcal{P}$. Literali su takođe elementarne disjunkcije. Ako je $k = n$, onda se ψ naziva potpunom elementarnom disjunkcijom (literala nad $\mathcal{P}$).

Neka su $\theta_1, \theta_2, \ldots, \theta_m$ u parovima logički neekvivalentne elementarne disjunkcije nad $\mathcal{P}$. Konjunkcija $\theta = \theta_1 \wedge \theta_2 \wedge \ldots \wedge \theta_m$ naziva se konjunktivnom normalnom formom nad $\mathcal{P}$, skraćeno KNF. Ako je svaka elementarna disjunkcija θ_i potpuna, onda se konjunkcija θ naziva potpunom ili savršenom KNF, kratko SKNF.

Primenom Principa dualnosti na Teoremu 1.15 dobija se sledeće tvrđenje o SKNF. U iskazu ove teoreme koristimo pojmove i notaciju uvedenu kod dokaza Teoreme o SDNF. U postupku dualizacije treba biti pažljiv, na primer, definicija za p^α posle dualizacije menja se u $p^1 = \neg p$ i $p^0 = p$, setimo se da je $\mathbf{h}(1) = 0$,

$\mathbf{h}(0) = 1$ i da je $\mathbf{h}(\bar{x}) = \bar{x}$. Ipak, radi uniformnosti izlaganja zadržaćemo definiciju za p^α iz prethodnog poglavlja, s tim da ćemo donekle izmeniti dualni oblik teoreme o SDNF, odnosno iskaz teoreme o SKNF.

Teorema 1.26 (**Teorema o SKNF**) *Neka je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$, $n \in N^+$, iskazna formula, $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ i neka je $\Gamma = \{\lambda \in 2^{\mathcal{P}} : \varphi[\lambda] = 0\}$. Ako je $\Gamma \neq \emptyset$, odnosno φ nije tautologija, onda je φ logički ekvivalentna formuli*

$$\psi = \bigwedge_{\alpha\in\Gamma} \bigvee_i p_i^{\bar{\alpha}_i}.$$

Ako za $\Gamma = \emptyset$ uzmemo $\bigwedge_{\alpha\in\Gamma} \theta_\alpha \stackrel{\text{def}}{=} \top$, tada iskaz teoreme važi za proizvoljnu formulu φ. Često ćemo pretpostavljati ovu definiciju i koristiti, na primer, ovaj prošireni oblik Teoreme o SKNF.

Primer 1.27 *Neka je $f : 2^3 \to 2$ zadata tablicom:*

p	q	r	f
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Ovde
$\Gamma = \{(0,0,0), (1,0,0), (1,1,0)\}$.
$\varphi(p,q,r) = (p \vee q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r)$
Primetimo da postoje jednostavnije iskazne formule u KNF koje reprezentuju f. Na primer, formula $\psi = (\neg p \vee r) \wedge (q \vee r)$. Tada $f = \hat{\varphi} = \hat{\psi}$.

Primer 1.28 Iskazna funkcija $f : 2^n \to 2$ je *pozitivna* ako $f(1, 1, \ldots, 1) = 1$. Iskazna formula φ je *pozitivna* ako u izgradnji formule φ od logičkih simbola učestvuju jedino $\top$, konjunkcija, disjunkcija i implikacija. S obzirom da je $1 \wedge_{\mathbf{I}} 1 = 1$, $1 \vee_{\mathbf{I}} 1 = 1$ i $1 \Rightarrow_{\mathbf{I}} 1 = 1$, ako je $\varphi = \varphi(p_1, p_2, \ldots, p_n)$ pozitivna iskazna formula, onda je očigledno $f(x_1, x_2, \ldots, x_n) = \hat{\varphi}(x_1, x_2, \ldots, x_n)$ pozitivna iskazna funkcija. Dokazaćemo da je svaka pozitivna iskazna funkcija f reprezentovana nekom pozitivnom iskaznom formulom φ, tj. $f = \hat{\varphi}$.

Neka je $\Gamma = \{\alpha \in 2^n : f(\alpha) = 0\}$. Ako je $\Gamma = \emptyset$, izaberimo $\varphi = \top$ i tada $f = \hat{\varphi}$. Pretpostavimo da je $\Gamma \neq \emptyset$ i neka je $\theta = \bigwedge_{\alpha\in\Gamma} \bigvee_i p_i^{\bar{\alpha}_i}$ i

$$S_\alpha = \{j : \alpha_j = 0, 1 \leq j \leq n\}, \quad T_\alpha = \{j : \alpha_j = 1, 1 \leq j \leq n\}, \quad \alpha \in \Gamma.$$

Prema pretpostavci $(1, 1, \ldots, 1) \notin \Gamma$, dakle za $\alpha \in \Gamma$ postoji $1 \leq j \leq n$ tako da $\alpha_j = 0$, tj. $S_\alpha \neq \emptyset$. Otuda, slovo p_j ima pozitivno pojavljivanje u formuli $\theta_\alpha = \bigvee_i p_i^{\bar{\alpha}_i}$, tj. p_j je disjunkt formule θ_α, prema tome disjunkcija $\bigvee_{j\in S_\alpha} p_j$ je neprazna. Stoga je $\varphi_\alpha = \bigwedge_{j\in T_\alpha} p_j \Rightarrow \bigvee_{j\in S_\alpha} p_j$ pozitivna formula i $\hat{\varphi}_\alpha = \hat{\theta}_\alpha$. Dakle i formula $\varphi = \bigwedge_{\alpha\in\Gamma} \varphi_\alpha$ je pozitivna i $f = \hat{\theta} = \hat{\varphi}$. □

Odavde imamo sledeću zanimljivu posledicu. Neka je θ proizvoljna iskazna formula i $f = \hat{\theta}$. Tada je očigledno ili f ili $\neg_{\mathbf{I}} f$ pozitivna iskazna funkcija. Shodno prethodnom primeru postoji pozitivna iskazna formula φ takva da je $\hat{\theta} = f = \hat{\varphi}$ ili $\hat{\theta} = f = \hat{\psi}$, $\psi = \neg\varphi$. Dakle proizvoljna iskazna formula θ logički je ekvivalentna nekoj formuli φ izgrađenoj jedino pomoću nekog broja logičkih simbola $\top$, $\vee$, $\wedge$ i $\Rightarrow$ i najviše jedne negacije. Primetimo da je $\top$ logički ekvivalentna formuli $p_1 \Rightarrow p_1$, te se u izgradnji formule φ simbol $\top$ može eliminisati.

1.5 Baze iskazne algebre

Prema Teoremi o SDNF, svaka iskazna funkcija izraziva je pomoću operacija disjunkcije, konjunkcije i negacije. S obzirom na De Morganove tautologije, proizilazi da je svaka iskazna funkcija izraziva samo pomoću disjunkcije i negacije, odnosno pomoću konjunkcije i negacije. Otuda, skupove iskaznih funkcija $\{\vee_{\mathbf{I}}, \neg_{\mathbf{I}}\}$ i $\{\wedge_{\mathbf{I}}, \neg_{\mathbf{I}}\}$ nazivamo *bazama* iskazne algebre.

Shodno prethodnom opisu, pod bazom iskazne algebre podrazumevamo bilo koji skup iskaznih funkcija pomoću kojih primenom operatora supstitucije možemo dobiti *sve* iskazne funkcije, bilo kojeg broja promenljivih. Sledeće pojmove iz algebre koristićemo za formalnu definiciju baze iskazne algebre. Neka je D domen, tj. neprazan skup. *Ime* alegebarske operacije f domena D je simbol operacije F iste dužine (arnosti) kao i operacija f. Uzimamo da je f interpretacija simbola F. Slično, ime konstante $a \in D$ je simbol konstante c koji se interpretira elementom a. Za ime nekog skupovnog objekta a koristićemo oznaku $\check{a}$. Ako je $\mathbf{A}$ algebra algebarskog jezika L i $t = t(x_1, x_2, \ldots, x_n)$ term (algebarski izraz) jezika L, tada se preslikavnje $f\colon A^n \to A$, definisano pomoću $f(a_1, a_2, \ldots, a_n) = t^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$, $a_1, a_2, \ldots, a_n \in A$, naziva term-preslikavanjem algebre $\mathbf{A}$. Na primer, polinomno preslikavanje nad nekim poljem je term preslikavanje.

Definicija 1.29 *Neka je $S = \{g_1, g_2, \ldots, g_n\}$ skup nekih iskaznih funkcija i $L = \{\check{g}_1, \check{g}_2, \ldots, \check{g}_n\}$ skup imena ovih operacija. S je baza iskazne algebre akko je svaka iskazna funkcija term preslikavanje algebre $\mathbf{2}_S = (2, g_1, g_2, \ldots, g_n)$. Ako je S baza i niti jedan pravi podskup od S nije baza, onda kažemo da je S minimalna ili glavna baza iskazne algebre.*

Dakle, koristeći oznake iz prethodne definicije, S je baza iskazne algebre akko za svaku iskaznu funkciju f postoji algebarski term $t = t(x_1, x_2, \ldots, x_n)$ jezika L tako da je $f(a_1, a_2, \ldots, a_n) = t^{\mathbf{2}_S}(a_1, a_2, \ldots, a_n)$, $a_1, a_2, \ldots, a_n \in 2$. Pojam baze prenosi se na prirodan način na bilo koji skup iskaznih funkcija. Neka je $\mathcal{F}$ skup nekih iskaznih funkcija. Skup S nekih iskaznih funkcija je baza za $\mathcal{F}$ ako je svaka funkcija iz $\mathcal{F}$ izraziva u smislu prethodne definicije pomoću preslikavanja iz S. Sledeće tvrđenje daje koristan kriterijum za utvrđivanje da li je neki skup iskaznih funkcija baza iskazne algebre.

Stav 1.30 *Neka je U baza za neki skup $\mathcal{F}$ iskaznih funkcija i neka je V baza za U. Tada je V baza za $\mathcal{F}$.*

Dokaz Neka je $f \in \mathcal{F}$ i neka je t term jezika U tako da je $f = t^{\mathbf{2}_U}$. Neka su $\check{u}_1, \check{u}_2, \ldots, \check{u}_n$ simboli jezika U koji se javljaju u t. S obzirom da je V baza za U, postoje termi $v_1, v_2, \ldots, v_n$ jezika V takvi da je $u_i = v_i^{\mathbf{2}_V}$. Supstitucijom redom simbola $\check{u}_i$ u termu t pomoću terma v_i, $1 \leq i \leq n$, dobijamo term-reprezentaciju preslikavanja f u bazi V.

Nešto formalniji dokaz ove teoreme može se izvesti indukcijom po složenosti terma t. □

Posledica 1.31 *Neka je S baza iskazne algebre. Tada je $S^* = \{f^* : f \in S\}$ takođe baza iskazne algebre.*

Dokaz Neka je $f \in S$. Tada $f = f^{**}$ i $f^* \in S^*$, pa tvrđenje sledi prema prethodnoj teoremi. □

Primer 1.32 Jednočlane baze iskazne algebre. *Neka su $x \uparrow y$ i $x \downarrow y$ funkcije definisane tablicama:*

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

Šeferova funkcija

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

Lukašijevičeva funkcija

Vidimo da je $x \uparrow y = \neg_{\mathbf{I}}(x \wedge_{\mathbf{I}} y)$, $x \downarrow y = \neg_{\mathbf{I}}(x \vee_{\mathbf{I}} y)$. Takoje $\neg_{\mathbf{I}} x = x \uparrow x$ i $x \vee_{\mathbf{I}} y = (x \uparrow x) \uparrow (y \uparrow y)$. S obzirom da je $\{\neg_{\mathbf{I}}, \vee_{\mathbf{I}}\}$ baza iskazne algebre, prema Tvrđenju 1.30 skup $\{\uparrow\}$ je takođe baza iskazne algebre. Dalje,

$$(x \uparrow y)^* = \overline{\neg_{\mathbf{I}}(\bar{x} \wedge \bar{y})} = \neg_{\mathbf{I}}(x \vee_{\mathbf{I}} y) = x \downarrow y,$$

dakle, $\{\downarrow\}$ je takođe baza iskazne algebre. Šeferova i Lukašijevičeva funkcija imaju posebno mesto u iskaznoj algebri. Dokazaćemo da su $\{\downarrow\}$ i $\{\uparrow\}$ jedine jednočlane baze iskazne algebre. Neka je $*$ binarna iskazna operacija i pretpostavimo da je $\{*\}$ baza iskazne algebre. Pretpostavimo da je $0 * 0 = 0$. Tada je $t(0, 0, \ldots, 0) = 0$ za proizvoljan term $t(x)$ jezika $\{\check{*}\}$, dakle u tom slučaju funkcija $\bar{x}$ nije predstavljiva operacijom $*$ (jer $\bar{0} = 1$). Dakle $0 * 0 = 1$. Na sličan način nalazimo $1 * 1 = 0$. Neka su $\alpha = 0 * 1$ i $\beta = 1 * 0$. Ako je $\alpha = 0$ i $\beta = 1$, onda je $x * y = \bar{x}$ i u tom slučaju jedine funkcije koje se mogu proizvesti pomoću $*$ su x i $\bar{x}$, dakle $*$ ne može činiti jednočlanu bazu. Ako je $\alpha = 0$ i $\beta = 1$, tada je $x * y = \bar{y}$ i kao u prethodnom slučaju $\{*\}$ nije baza. Prema tome ostaje jedino $\alpha = \beta = 0$ ili $\alpha = \beta = 1$, a to su Lukašijevičeva, odnosno Šeferova funkcija. □

Postoji tačno 46 glavnih baza iskazne algebre u kojima su sve operacije unarne ili binarne. Kao što smo videli ima tačno dve jednočlane baze. Postoji 34 dvočlanih glavnih baza od kojih se 10 sastoji od jende unarne i jedne binarne operacije, dok ostalih 24 imaju dve binarne operacije. Najzad, ima 10 tročlanih glavnih baza od kojih 4 sa jednom unarnom i dve binarne operacije, dok su u ostalih 6 sve tri operacije binarne.

Primer 1.33 Prema Primeru 1.28 skup $S = \{\vee_{\mathbf{I}}, \wedge_{\mathbf{I}}, \Rightarrow_{\mathbf{I}}\}$ je jedna baza za klasu pozitivnih iskaznih funkcija. Prema Principu dualnosti, skup $S^* = \{\wedge_{\mathbf{I}}, \vee_{\mathbf{I}}, g\}$, gde $g(x, y) = \bar{x} \wedge_{\mathbf{I}} y$, predstavlja bazu skupa svih iskaznih funkcija f koje zadovoljavaju uslov $f(0, 0, \ldots, 0) = 0$.

Primer 1.34 *Klasa iskaznih funkcija $\mathcal{F}$ generisanih pomoću $S' = \{\wedge_{\mathbf{I}}, \underline{\vee}_{\mathbf{I}}\}$.* Radi jednostavnije notacije, operacije $\wedge_{\mathbf{I}}$ i $\underline{\vee}_{\mathbf{I}}$ označićemo redom sa $\cdot$ i $+$. Dakle $x \cdot y = x \wedge_{\mathbf{I}} y$, $x \underline{\vee}_{\mathbf{I}} y = x + y$. Tada ove operacije zadovoljavaju aksiome komutativog prstena sa jedinicom u kojem važe zakon idempotencije, $x^2 = x$, i zakon involucije za sabiranje, $x + x = 0$. Neka je $f \in \mathcal{F}$. Tada se u f javlja bar jedna od operacija $+$, $\cdot$, dakle f je funkcija nekih promenljivih $x_1, x_2, \ldots, x_n$, $n \geq 1$, i $f(x_1, x_2, \ldots, x_n)$ postaje polinomna funkcija ovih promenljivih nad prstenom $(\{0, 1\}, +, \cdot, 0)$. S obzirom na pomenute zakone idempotencije i involucije postoji jedinstven $\Gamma \subseteq \mathbf{P}(\{1, 2, \ldots, n\})$, tako da važi:

$$f(x_1, x_2, \ldots, x_n) = \sum_{\alpha \in \Gamma} x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_k} \tag{1.3}$$

gde za $\alpha \in \Gamma$ važi $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, $1 \leq k \leq n$, $\alpha_1 < \alpha_2 < \ldots < \alpha_k$. Primetimo da ako $\Gamma = \emptyset$ onda $f = 0$. Ako je $v \in S$, onda $v(0, 0) = 0$, odakle sledi da za sve $f \in \mathcal{F}$ važi $f(0, 0, \ldots, 0) = 0$, te f pripada klasi iskaznih funkcija iz prethodnog primera. Otuda takođe sledi da je slobodan član u f jednak nuli, pa kako je za $\alpha = \emptyset$, $\prod_{j \in \alpha} x_j = 1$, to $\emptyset \notin \Gamma$. Vidimo da se $\mathcal{F}$ ne menja ukoliko se skup S' dopuni funkcijom $\vee_{\mathbf{I}}$, jer $x \vee_{\mathbf{I}} y = x + y + xy$. Kako je $\bar{x}y = y + xy$, za S^* iz prethodnog primera važi $S^* \subseteq \mathcal{F}$, dakle svaka iskazna funkcija f koja zadovoljava $f(0, 0, \ldots, 0) = 0$ pripada $\mathcal{F}$. Najzad, ako je f polinom 1.3, $\emptyset \notin \Gamma$, onda $f(0, 0, \ldots, 0) = 0$. Dakle, $\mathcal{F}$ je tačno skup iskaznih funkcija koje zadovoljavaju uslov $f(0, 0, \ldots, 0) = 0$, odnosno binarnih funkcija predstavljivih pomoću polinoma 1.3 kod kojih $\emptyset \notin \Gamma$.

Primer 1.35 *Klasa iskaznih funkcija $\mathcal{T}$ generisanih pomoću $S'' = \{\neg_{\mathbf{I}}, \underline{\vee}_{\mathbf{I}}\}$.* Neka je kao u prethodnom primeru $x + y = x \underline{\vee}_{\mathbf{I}} y$ i $\bar{x} = \neg_{\mathbf{I}} x$. Sa $+_N$ označićemo sabiranje u skupu prirodnih brojeva radi razlikovanja od novouvedene operacije sabiranja. Pretpostavimo da je $f(x_1, x_2, \ldots, x_n) \in \mathcal{T}$, tj. $f = \hat{\varphi}$ za neku iskaznu formulu φ izgrađenu jedino od iskaznih veznika $\neg$ i $\underline{\vee}$ i promenljivih $x_1, x_2, \ldots, x_n$, $n \geq 1$. Neka je λ_i broj pojavljivanja promenljive x_i, $1 \leq i \leq n$, i μ broj pojavljivanja simbola $\neg$ u φ. Najzad, neka je $\lambda_i' = \lambda_i \pmod 2$, $\lambda_i' \in \{0, 1\}$, tj. λ_i' je ostatak od $\lambda_i \bmod 2$, i neka je $\mu' = \mu \pmod 2$, $\mu' \in \{0, 1\}$. Indukcijom po složenosti formule φ dokazujemo da je $f = \mu' + \lambda_1' x_1 + \lambda_2' x_2 + \ldots + \lambda_n' x_n$. Ovde $0 \cdot x = 0$ i $1 \cdot x = x$. U dokazu koristićemo činjenicu da je ovako uvedena operacija $+$ zapravo operacija $+_2$, sabiranje po modulu 2 u $\{0, 1\}$, i da je $(\{0, 1\}, +_2, 0)$ komutativna grupa.

Slučaj $\mathrm{sl}\,\varphi = 1$. Razlikujemo sledeće slučajeve:

a. $\varphi = \neg x$. Tada $f = \hat{\varphi} = \bar{x} = 1 + x$, dakle tvrđenje važi.

b. $\varphi = x \underline{\vee} y$. Tada $f = \hat{\varphi} = x + y$, dakle tvrđenje i u ovom slučaju važi.

Neka je $n > 1$ prirodan broj. Pretpostavimo induktivnu hipotezu, da je tvrđenje istinito za sve iskazne formule ψ, $\mathrm{sl}\,\psi < n$. Neka je φ iskazna formula, $\mathrm{sl}\,\varphi = n$. Dokazujemo da odgovarajući identitet važi za $\hat{\varphi}$. Razlikujemo sledeće skučajeve:

a. $\varphi = \neg\psi$. U ovom slučaju broj pojavljivanja nekog iskaznog slova x u φ i ψ je isti, dok za broj ν simbola $\neg$ u ψ važi $\mu = \nu +_N 1$, dakle $\mu' = \bar{\nu}' +_2 1 = \nu' + 1$. Prema induktivnoj hipotezi $\hat{\psi} = \nu' + \lambda'_1 x_1 + \lambda'_2 x_2 + \ldots + \lambda'_n x_n$, jer $\mathrm{sl}\,\psi < \mathrm{sl}\,\varphi$. S obzirom da je $\bar{u} = 1 + u$, imamo $f = \hat{\varphi} = 1 + \hat{\psi}$, dakle

$$f = 1 + \nu' + \lambda'_1 x_1 + \lambda'_2 x_2 + \ldots + \lambda'_n x_n = \mu' + \lambda'_1 x_1 + \lambda'_2 x_2 + \ldots + \lambda'_n x_n.$$

b. $\varphi = \theta \underline{\vee} \vartheta$. Tada $\mathrm{sl}\,\theta, \mathrm{sl}\,\vartheta < \mathrm{sl}\,\varphi$, te prema induktivnoj hipotezi imamo:

$$\hat{\theta} = \rho' + \alpha'_1 x_1 + \alpha'_2 x_2 + \ldots + \alpha'_n x_n, \quad \hat{\vartheta} = \sigma' + \beta'_1 x_1 + \beta'_2 x_2 + \ldots + \beta'_n x_n,$$

gde je $\xi' = \xi \,(\mathrm{mod}\, 2)$, $\xi' \in 2$, ξ je neka od vrednosti $\rho, \sigma, \alpha_i, \beta_i$, $1 \leq i \leq n$, $2 = \{0, 1\}$. Ovde su ρ i σ broj pojavljivanja simbola $\neg$ redom u θ i ϑ, dok su α_i, β_i broj pojavljivanja promenljive x_i redom u θ i ϑ. Kako je $x + x = 0$, to za $\alpha, \beta \in \{0, 1\}$ važi $\alpha x + \beta x = (\alpha + \beta)x$ (setimo se da $+$ označava operaciju $+_2$). Dalje, preslikavanje $' \colon Z \to 2$ je homomorfizam aditivne grupe celih brojeva u grupu $(2, +_2, 0)$, dakle za $m, n \in N$ važi $m' + n' = (m + n)'$. Otuda,

$$\begin{aligned} f = \quad & \hat{\varphi} = \hat{\theta} \underline{\vee}_{\mathbf{I}} \hat{\vartheta} = \hat{\theta} + \hat{\vartheta} = \\ & (\rho' + \sigma') + (\alpha'_1 + \beta'_1)x_1 + (\alpha'_2 + \beta'_2)x_2 + \ldots (\alpha'_n + \beta'_n)x_n = \\ & (\rho + \sigma)' + (\alpha_1 + \beta_1)' x_1 + (\alpha_2 + \beta_2)' x_2 + \ldots (\alpha_n + \beta_n)' x_n = \\ & \mu' + \lambda'_1 x_1 + \lambda'_2 x_2 + \ldots + \lambda'_n x_n. \end{aligned}$$

Direktna posledica upravo opisane reprezentacije formula skupa $\mathcal{T}$ je sledeći opis tautologija iz tog skupa: Neka je φ iskazna formula u kojoj od iskaznih veznika učestvuju jedino simbol negacije i simbol ekskluzivavne disjunkcije. Tada je φ tautologija akko svako iskazno slovo u φ ima paran broj pojavljivanja (dakle $\lambda'_i = 0$) i simbol negacije ima neparan broj pojavljivanja (dakle $\mu' = 1$). Primetimo da je ovim tvrđenjem dat algoritam kojim se u polinomijalnom vremenu (linearan u odnosu na dužinu formule φ) proverava da li je formula φ opisanog tipa tautlogija.

1.6 Iskazne teorije

Neka je $\mathcal{P}$ skup iskaznih slova. Bilo koji skup $\mathcal{T}$ iskaznih formula sa iskaznim slovima u $\mathcal{P}$ naziva se *iskaznom teorijom* nad $\mathcal{P}$. U tom slučaju formule iz $\mathcal{T}$ nazivaju se *aksiomama* teorije $\mathcal{T}$. Teorija $\mathcal{T}$ može imati konačan ili beskonačan skup aksioma; u prvom slučaju $\mathcal{T}$ se naziva *konačno-aksiomatskom* teorijom. Ako je $\mathcal{P}$ najviše prebrojiv skup, tada svih reči (konačnih nizova) nad $\mathcal{P}$ i logičkim veznicima ima prebrojivo mnogo, dakle svaka teorija nad $\mathcal{P}$ ima najviše pebrojiv skup aksioma. U opštem slučaju ako je k beskonačan kardinalni broj i $|\mathcal{P}| = k$ tada je $|\mathcal{T}| \leq k$. Ova činjenica proizilazi iz jednakosti $k^2 = k$ koja važi za beskonačne krardinalne brojeve k.

Primer 1.36 **1**. $\mathcal{T} = \{\neg p, p \Rightarrow (q \vee r), r \Rightarrow p\}$. *Ova teorija ima tri aksiome:* $\neg p, p \Rightarrow (q \vee r), r \Rightarrow p$, *dakle* $\mathcal{T}$ *je konačno-aksiomatska.* $\mathcal{T}$ *je iskazna teorija nad bilo kojim skupom* $\mathcal{P}$ *iskaznih slova koji sadrži iskazne promenljive* p, q, r. **2**. *Neka je* $\mathcal{P} = \{p_i \colon i \in N\}$, $\mathcal{T} = \{p_i \Rightarrow p_{i+1} \colon i \in N\}$, N *je skup prirodnih brojeva. Teorija* $\mathcal{T}$ *ima beskonačan skup aksioma:* $p_0 \Rightarrow p_1$, $p_1 \Rightarrow p_2, \ldots$.

Sledećim definicijama uvode se ključne osobine iskaznih teorija. U svim slučajevima, do kraja ovog odeljka, $\mathcal{T}$ je iskazna teorija nad skupom iskaznih slova $\mathcal{P}$.

Definicija 1.37 *Valuacija μ domena $\mathcal{P}$ je model teorije $\mathcal{T}$ akko je svaka formula $\varphi \in \mathcal{T}$ zadovoljena valuacijom μ. Činjenicu da je μ model teorije $\mathcal{T}$ zapisujemo pomoću $\mu \models \mathcal{T}$.*

Definicija 1.38 *Teorija $\mathcal{T}$ je semantički neprotivurečna akko $\mathcal{T}$ ima model. Ako $\mathcal{T}$ nema model, tada kažemo da je $\mathcal{T}$ protivurečna teorija.*

Shodno prethodnoj definiciji, $\mu \models \mathcal{T}$ akko $\bigwedge_{\varphi\in\mathcal{T}} \varphi[\mu] = 1$. Ako je $\mathcal{T} = \{\psi\}$, tada $\mu \models \mathcal{T}$ akko $\psi[\mu] = 1$. Neka je $\mathcal{P} = \{p, q, r\}$ u Primeru 1.37.1. Modele μ teorije $\mathcal{T}$ iz tog primera određujemo na sledeći način: Kako je $(\neg p)[\mu] = 1$, to je $\mu[p] = 0$. Dalje, $(r \Rightarrow p)[\mu] = 1$ te s obzirom na već utvrđenu vrednost $\mu[p] = 0$ imamo $\mu[r] = 0$. Najzad, kako je $\mu[p] = 0$, to je $(p \Rightarrow (q \vee r))[\mu] = 1$ za bilo koju vrednost iskazne promenljive q. Dakle skup svih modela teorije $\mathcal{T}$ je $\{(0, 0, 0), (0, 1, 0)\}$ uz leksikografski poredak slova p, q, r. U Primeru 1.37.2. sve modele teorije $\mathcal{T}$ čine beskonačni nizovi

$$(1, 1, 1, 1, \ldots),\ \ (0, 1, 1, 1, \ldots),\ \ (0, 0, 1, 1, \ldots),\ \ (0, 0, 0, 1, \ldots),\ \ \ldots.$$

Dakle, u ovom slučaju skup modela teroije $\mathcal{T}$ je beskonačan prebrojiv skup.

U oba prethodna primera razmatrane teorije su očigledno neprotivurečne. Primetimo da ako je $\mathcal{T}$ neka teorija i postoji formula θ tako da $\theta, \neg\theta \in \mathcal{T}$, onda je $\mathcal{T}$ protivurečna teorija. Jedno od glavnih pitanja u ovoj oblasti su kriterijumi (semantičke) neprotivurečnosti teorija. Ako je $\mathcal{T}$ teorija sa konačnim skupom aksioma, tada je $\mathcal{T}$ semantički neprotivurečna akko postoji valuacija koja realizuje formulu $\psi = \bigwedge_{\varphi\in\mathcal{T}}$. Otuda spomenuti kriterijumi imaju smisla jedino za teorije sa beskonačnim skupom aksioma. O samim kriterijumima biće reči nešto kasnije.

Mnoge logičke zagonetke i drugi matematički zadaci mogu se rešiti postavljanjem odgovarajućeg iskaznog modela i sprovođenjem računa u iskaznoj algebri. Sledeći primer je takve vrste.

Primer 1.39 U jednom selu desilo se ubistvo. Stanovnici sela podeljeni su u dva klana, klan Belih i klan Crnih. Poznato je da (R_1) dva stanovnika u međusobnom razgovoru govore istinu jedino ako su pripadnici istih klanova, u suprotnom njihovi iskazi su lažni. Takođe se zna (R_2) da je ubica tačno jedna od osoba A, B, C, D, E. U sudnici osumnjičeni su u međusobnom suočavanju pred sudijom izjavili:

θ_1: Osoba A osobi B: *D je pripadnik klana Belih akko je C ubica.*
θ_2: Osoba B osobi C: *Ja pripadam klanu Crnih ili D pripada klanu Crnih.*
θ_3: Osoba C osobi D: *Ubica je osoba A ili osoba B.*
θ_4: Osoba D osobi E: *Ako je C pripadnik klana Belih onda sam je ubica.*
θ_5: Osoba E osobi A: *B je pripadnik klana Belih.*

Sudija je čuo takođe jednu od sledećih rečenica koju je osoba B izrekla osobi A:

φ_1: *Bar jedna od osoba C, D je pripadnik klana Belih.*
φ_2: *C i D su pripadnici klana Belih.*
φ_3: *C je pripadnik klana Belih.*
φ_4: *D je pripadnik klana Belih.*

Sudija je na osnovu ovih iskaza i činjenica R_1 i R_2 zaključio ko je ubica.

Pitanja: Ko je ubica? Kojim klanovima pripadaju osobe A, B, C, D, E? Koji od iskaza $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ je sudija čuo?

Rešenje Neka a, b, c, d, e redom označavaju iskaze da A, B, C, D, E pripadaju klanu Belih i neka p, q, r, s, t redom označavaju iskaze da je A, B, C, D, E ubica. Tada, na primer, $r \Rightarrow a$ predstavlja iskaz: "*ako je C ubica onda je A pripadnik klana belih*". Neka su X, Y dve različite osobe i neka su x, y iskazi koji se odnose na njihovu pripadnost klanu Belih. Tada formula $\psi = (x \wedge y) \vee (\neg x \wedge \neg y)$ iskazuje da su X, Y pripadnici istog klana. Formula ψ je logički ekvivalentna $x \Leftrightarrow y$, pa možemo uzeti da je $\psi = (x \Leftrightarrow y)$. Tada prema uslovu R_1, sledi da je:

$\theta_1 = (a \Leftrightarrow b) \Leftrightarrow (d \vee r)$, i slično, $\theta_2 = (b \Leftrightarrow c) \Leftrightarrow (\neg b \vee \neg d)$,
$\theta_3 = (c \Leftrightarrow d) \Leftrightarrow (p \vee q)$, $\theta_4 = (d \Leftrightarrow e) \Leftrightarrow (c \Rightarrow s)$, $\theta_5 = (e \Leftrightarrow a) \Leftrightarrow b$.

Neka je $S_1 = \{\theta_1, \theta_2, \theta_3, \theta_4, \theta_5\}$. Rešenje zadatka, valuacija α koja između ostalog dodeljuje vrednosti promenljivima a, b, c, d, e, tada jeste model skupa S_1. Prema uslovu R_2, za isto α, koja između ostalog dodeljuje vrednsoti i promenljivama p, q, r, s, t, disjunkcija $p \vee q \vee r \vee s \vee t$ takodje jeste tačna i za različite $u, v \in \{p, q, r, s, t\}$ mora biti $(u \wedge v)[\alpha] = 0$. Dakle α je model i skupa

$$S_2 = \{p \vee q \vee r \vee s \vee t\} \cup \{\neg(u \wedge v) |\ u, v \in \{p, q, r, s, t\}, u \neq v\}.$$

Neka je $\psi_1 = \bigwedge S_1 = \bigwedge_{\theta \in S_1} \theta$, $\psi_2 = \bigwedge S_2$ i $\psi = \psi_1 \wedge \psi_2$. Prema prethodnom, mora biti $\psi[\alpha] = 1$. Ako je $\bigvee_{\beta \in \Gamma} \psi_\beta$ SDNF formule ψ, tada α pripada Γ. SDNF formule ψ, tj. skup Γ može imati više od jednog člana, dok s druge strane, prema uslovu zadatka sudija je uz pomoć neke od rečenica φ_1, φ_2, φ_3, φ_4 došao do jednoznačnog rešenja, odnosno jedinstvene valuacije α. Dakle rešenje, valuacija α, dobija se iz one formule $\psi \wedge \varphi_i$, $i = 1, 2, 3, 4$, čija SDNF ima tačno jedan član, odnosno koja ima tačno jedan model. Ovim je zadatak u osnovi rešen, dovoljno je odrediti SDNF formula $\psi \wedge \varphi_i$, što se može uraditi u konačno mnogo koraka. S druge strane broj promenljivih u tom računu je 10, i u direktnom izračunavanju broj računskih operacija postaje veoma veliki. Ipak, uz pojednostavljenu notaciju i primenu algebre zadatak se relativno lako rešava.

Neka $x + y$, xy i $\bar{x}$ imaju ista značenja kao u primerima 1.34 i 1.35 (ekskluzivna disjunkcija, konjunkcija i negacija). U algebri $\mathbf{2} = (\mathbf{2}, +, \cdot, \bar{}, \mathbf{0}, \mathbf{1})$ važi $\bar{x} = 1 + x$, $x + x = 0$, $x^2 = x$, $x \Leftrightarrow y = 1 + x + y$, $x \vee y = x + y + xy$. Otuda $\theta_1 = 1$ akko $1 + a + b = 1 + d + r$, akko $a + b + d + r = 0$, zatim $\theta_2 = 1$ akko $1 + b + c = \bar{b} + \bar{d} + \bar{b}\bar{d}$ akko $1 + b + c = 1 + b + 1 + d + (1 + b)(1 + d)$ akko $b + c + bd = 0$, zatim $\theta_3 = 1$ akko $1 + c + d = p + q + pq$ akko $c + d + p + q = 1$ jer $pq = 0$, itd. Dakle valuacija α biće rešenje sledećeg sitema jednačina nad $\mathbf{2}$:

$a+b+d+r = 0$, $b+c+bd = 0$, $c+d+p+q = 1$, $c+d+e+cs = 0$, $a+b+e = 1$

odnosno, sabiranjem prve i poslednje jednačine, zatim treće i četvrte,

$$a+b+e = 1,\ e+d+r = 1,\ b+c+bd = 0,\ c+d+p+q = 1,\ e+p+q+cs = 1 \quad (1.4)$$

Iz poslednjeg dela uslova zadatka nalazimo:

$$\begin{array}{lll} \varphi_1: & a+b+c+d+cd=1, & \varphi_2: a+b+cd=1, \\ \varphi_3: & a+b+c=1, & \varphi_4: a+b+d=1 \end{array} \tag{1.5}$$

Množenjem poslednje jednačine u 1.4 sa p, q, r, s, t nalazimo

$$ep=0,\ \ eq=0,\ \ er=r,\ \ et=t,\ \ es+cs=0. \tag{1.6}$$

Pretpostaviom $s=1$. Tada $p=q=r=t=0$ te iz dve poslednje jednačine u 1.4 nalazimo $c+d=1, e+c=1$, odakle $e+d=0$, pa iz druge jednačine u 1.4 sledi $r=1$, kontradikcija. Dakle $s=1$. Pretpostavimo $e=0$. Tada iz poslednje jednačine u 1.4 sledi $p+q=1$, odakle $p=1$ ili $q=1$, te $r=0$. Tada iz 1.4 sledi $d=1, c=1$ i na osnovu $b+c+bd=0$ sledi $c=0$, kontradikcija.

Dakle, $s=0, e=1$ i prema 1.6 takođe $p=0, q=0$. Tada sistem 1.4 postaje

$$a+b=0,\ \ d+r=0,\ \ b+c+bd=0,\ \ c+d=1 \tag{1.7}$$

Sada rešavamo sistem 1.7 zajedno sa svakom od jednačina $\varphi_1, \varphi_2, \varphi_3, \varphi_4$:

(1.7)+φ_1: $a+b=0,\ d+r=0,\ b+c+bd=0,\ c+d=1,\ cd=0.$

Ovaj sistem ima bar dva rešenja, u jednom je $a=1, b=0$, dok je u drugom $a=0, b=1$. Prema uslovu zadatka rešenje mora biti jedinstveno, dakle ovaj slučaj nije moguć.

(1.7)+φ_2: $a+b=0,\ d+r=0,\ b+c+bd=0,\ c+d=1,\ cd=1$

Iz poslednje jednačine sledi $c=1, d=1$ što je u kontradikciji sa $c+d=1$. Dakle ovaj slučaj nije moguć.

(1.7)+φ_3: $a+b=0,\ d+r=0,\ b+c+bd=0,\ c+d=1,\ a+b+c=1$

Iz ovog sistema neposredno sledi $c=1$, $d=0$, $b=1$, $a=1$, $r=0$, što uz $e=1$, $s=0$, $p=0$, $q=0$, daje $t=0$. Dakle ovaj sistem ima tačno jedno rešenje, čime je zadatak rešen. Ipak razmotrimo i poslednji slučaj

(1.7)+φ_4: $a+b=0,\ d+r=0,\ b+c+bd=0,\ c+d=1,\ a+b+d=1$

U ovom sistemu sledi $d=1, c=0$, $a=1, b=0$; $a=0, b=1$ itd, dakle sistem ima bar dva rešenja te ovaj slučaj kao i u (1.7)+φ_1 nije moguć.

Prema prethodnom imamo: Osoba E je ubica ($t=1$), A, B, C, E su pripadnici klana Belih ($a=b=c=e=1$), D je pripadnik klana Crnih ($d=0$) i sudija je čuo rečenicu φ_3 (sistem (1.7)+φ_3). □

Formula φ nad $\mathcal{P}$ je *semantička posledica* teorije T akko svaki model teorije $\mathcal{T}$ realizuje φ, tj. ako je $\mu \in 2^{\mathcal{P}}$ tada $\bigwedge_{\theta\in\mathcal{T}} \theta[\mu] = 1$ povlači $\varphi[\mu] = 1$. Da je φ semantička posledica teorije $\mathcal{T}$ zapisujemo $\mathcal{T} \models \varphi$. Odmah vidimo da $\mathcal{T}$ ima model akko $\mathcal{T} \not\models \bot$, odnosno $\mathcal{T}$ nema model akko $\mathcal{T} \models \bot$. Ako je $\mathcal{T} = \{\theta_1, \theta_2, \ldots, \theta_n\}$, umesto $\mathcal{T} \models \varphi$ pišemo takođe $\theta_1, \theta_2, \ldots, \theta_n \models \varphi$. Ako je $\mathcal{T}' = \mathcal{T} \cup \{\psi\}$, tada umesto $\mathcal{T}' \models \varphi$ takođe pišemo $\mathcal{T}, \psi \models \varphi$. U sledećem tvrđenju opisuju se neka svojstva relacije $\models$.

Stav 1.40 *Neka su $\mathcal{T}, \mathcal{S}$ iskazne teorije nad skupom iskaznih slova $\mathcal{P}$ i neka su φ, ψ iskazne formule nad $\mathcal{P}$. Tada:*

1. *Ako $\mathcal{T}, \psi \models \varphi$ tada $\mathcal{T} \models \psi \Rightarrow \varphi$.* **2.** *$\bigwedge_{\theta \in \mathcal{S}} \mathcal{T} \models \theta$ i $\mathcal{S} \models \varphi$ povlači $\mathcal{T} \models \varphi$.*

3. *Ako $\mathcal{S} \subseteq \mathcal{T}$ i $\mathcal{S} \models \varphi$ onda $\mathcal{T} \models \varphi$.* **4.** *$\mathcal{T} \models \varphi$ i $\mathcal{T} \models \varphi \Rightarrow \psi$ povlači $\mathcal{T} \models \psi$.*

Dokaz 1. Pretpostavimo (1) $\mathcal{T}, \psi \models \varphi$ i neka je μ model teorije $\mathcal{T}$. Ako je $\psi[\mu] = 1$, tada je μ model teorije $\mathcal{T} \cup \{\psi\}$ te prema (1) sledi $\varphi[\mu] = 1$, tj. $(\psi \Rightarrow \varphi)[\mu] = 1$. Ako je $\psi[\mu] = 0$ onda opet $(\psi \Rightarrow \varphi)[\mu] = 1$, dakle $\mathcal{T} \models \psi \Rightarrow \varphi$.
Ostala tvrđenja 2-4 dokazuju se na sličan način. □

Teorema kompaktnosti je centralno svojstvo iskaznog računa. Ova teorema daje netrivijalan kriterijum za semantičku konzistentnost beskonačnih iskaznih teorija. Teoremu je dokazao A. Malcev 1936. Spomenimo da logika u to vreme nije bila sasvim prepoznata kao matematička disciplina, o čemu svedoči i tada njen dosta popularan naziv "metamatematika". Tek se radovima Gödela, Tarskog i Malceva između dva svetska rata matematička logika utemeljuje kao oblast matematike. Malcev je ovom novom statusu logike doprineo mnogobrojnim primenama Teoreme kompaktnosi u algebri. U ovoj knjizi dajemo nekoliko dokaza Teoreme kompaktnosti. Svaki dokaz predstavljaće primer povezanosti logike i neke druge matematičke oblasti. Prvi dokaz teoreme kompaktnosti zasnovan je na sledećem ekvivalentu aksiome izbora u okviru ZF sistema teorije skupova.

Teorema 1.41 (**Zornova lema**) *Neka je $\mathbf{A} = (A, \leq)$ parcijalno uređen skup u kojem svaki neprazan lanac ima gornju granicu. Tada $\mathbf{A}$ ima maksimalan element.*

Podsetimo se da je $L \subseteq A$ *lanac* u $\mathbf{A}$ ako i samo ako za sve $x, y \in L$ važi $x \leq y$ ili $y \leq x$. Element $b \in A$ je maksimalan element u $\mathbf{A}$ akko $\bigwedge_{x \in A} b \not\leq x$.

Teorema 1.42 (**Teorama kompaktnosti**) *Neka je $\mathcal{T}$ iskazna teorija nad skupom iskaznih promenljivih $\mathcal{P}$. Ako svaki konačan podskup teorije $\mathcal{T}$ ima model, tada $\mathcal{T}$ ima model.*

Dokaz Pretpostavimo da je $\mathcal{T}$ iskazna teorija nad skupom iskaznih promenljivih $\mathcal{P}$ i neka svaki konačan podskup teorije $\mathcal{T}$ ima model. Dokazujemo da teorija $\mathcal{T}$ ima model.

Neka je $\mathbf{A} = (A, \subseteq)$, gde je A skup svih raširenja $\mathcal{S}$ nad $\mathcal{P}$ teorije $\mathcal{T}$ koja imaju osobinu KN (*konačne netportivurečnosti*): *svaki konačan podskup teorije $\mathcal{S}$ ima model*. Očigledno je $A \neq \emptyset$ (jer $\mathcal{T} \in A$) i $\mathbf{A}$ je parcijalno uređen skup. Neka je $L \subseteq A$ bilo koji neprazan lanac i neka je $\mathcal{L} = \bigcup L$. Dokazujemo da $\mathcal{L}$ ima svojstvo KN. Neka je $\mathcal{S} \subseteq \mathcal{L}$ konačan. Ako je $\mathcal{S}$ prazan skup, onda je svaka valuacija promenljivih $\mathcal{P}$ model za $\mathcal{S}$. Pretpostavimo da je $\mathcal{S} \neq \emptyset$ i neka je $\mathcal{S} = \{\theta_1, \theta_2, \ldots, \theta_n\}$. Kako je $\mathcal{S} \subseteq \mathcal{L}$, postoje $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n \in L$ tako da je $\theta_i \in \mathcal{S}_i$, $i = 1, 2, \ldots, n$. S obzirom da je L lanac u odnosu na $\subseteq$, postoji najveći član u $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n\}$. Dakle za neki $\mathcal{K} \in \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n\}$ važi $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n \subseteq \mathcal{K}$, pa $\mathcal{S} \subseteq \mathcal{K}$ i $\mathcal{K}$ ima svojstvo KN. Otuda $\mathcal{S}$ ima model,

dakle $\mathcal{L}$ ima svojstvo KN. Takođe $\mathcal{T} \subseteq \mathcal{L}$, stoga $\mathcal{L} \in A$. Ovim smo dokazali da je $\mathcal{L}$ gornja granica u $\mathbf{A}$ lanca L. Prema tome ispunjeni su uslovi Zornove leme, pa postoji neki maksimalan (u odnosu na $\subseteq$) element u $\mathbf{A}$, neka je to $\mathcal{M}$. Dokazujemo da $\mathcal{M}$ ima sledeća svojstva:

(1) Ako je φ iskazna formula nad $\mathcal{P}$ tada $\varphi \in \mathcal{M}$ ili $\neg\varphi \in \mathcal{M}$.
(2) Ako su φ, ψ iskazne formule nad $\mathcal{P}$ i $\varphi \vee \psi \in \mathcal{M}$, tada $\varphi \in \mathcal{M}$ ili $\psi \in \mathcal{M}$.

Dokažimo, na primer, svojstvo (1). Pretpostavimo suprotno, da $\varphi, \neg\varphi \notin \mathcal{M}$. Tada je $\mathcal{M}$ pravi podskup skupova $\mathcal{M} \cup \{\varphi\}$ i $\mathcal{M} \cup \{\neg\varphi\}$, te zbog maksimalnosti $\mathcal{M}$ u $\mathbf{A}$, postoje konačni skupovi $S_1, S_2 \subseteq \mathcal{M}$ takvi da su $S_1 \cup \{\varphi\}$ i $S_2 \cup \{\neg\varphi\}$ protivrečne teorije. Prema tome, $S_1, \varphi \models \bot$ i $S_2, \neg\varphi \models \bot$, tj. $S_1 \models \varphi \Rightarrow \bot$ i $S_2 \models \neg\varphi \Rightarrow \bot$, odakle $S_1 \models \neg\varphi$ i $S_2 \models \varphi$. Otuda $S_1 \cup S_2 \models \varphi \wedge \neg\varphi$, tj. $S_1 \cup S_2$ je protivurečna teorija. S druge strane $S_1 \cup S_2$ je konačan podskup teorije $\mathcal{M}$ koja ima svojstvo KN (jer pripada $\mathbf{A}$), te je $S_1 \cup S_2$ neprotivurečna teorija, što je u kontradikciji sa iskazom u prethodnoj rečenici. Prema tome $\mathcal{M}$ zaista ima svojstvo (1). Na sličan način se dokazuje da $\mathcal{M}$ ima i svojstvo (2).

Teorija $\mathcal{M}$ ima svojstvo KN, pa za formulu φ ne može biti $\{\varphi, \neg\varphi\} \subseteq \mathcal{M}$. Dakle, za svaku formulu φ, tačno jedna od formula $\varphi, \neg\varphi$ pripada $\mathcal{M}$. S obzriom na ovu napomenu, sledeća definicija valuacije μ promenljivih iz $\mathcal{P}$ je korektna. Neka je $p \in \mathcal{P}$. Ako je $p \in \mathcal{M}$ tada $\mu(p) = 1$. Ako je $\neg p \in \mathcal{M}$ tada uzimamo $\mu(p) = 0$. Indukcijom po složenosti formule dokazujemo da μ zadovoljava sve formule $\varphi \in \mathcal{M}$, preciznije,

(3) *Za proizvoljnu iskaznu formulu φ važi $\varphi[\mu] = 1$ akko $\varphi \in \mathcal{M}$.*

Neka $\mathrm{sl}(\varphi) = 0$ i neka je $\varphi \in \mathcal{M}$. Tada je φ neko iskazno slovo $p \in \mathcal{P}$. Prema izboru valuacije μ, vidimo da je $\mu(p) = 1$ akko $p \in \mathcal{M}$, dakle i $\varphi[\mu] = \mu(p) = 1$. S obzirom da $\{\neg, \vee\}$ čini bazu iskaznog računa, možemo pretpostaviti da su iskazne formule izgrađene jedino od veznika $\neg, \vee$. Neka je $\varphi \in \mathcal{M}$ i neka je $\mathrm{sl}(\varphi) = n + 1$, $n \in N$. Razlikujemo sledeće slučajeve:

a. $\varphi = \neg\psi$. S obzirom da tačno jedna od formula $\psi, \neg\psi$ pripada $\mathcal{M}$, i kako $\neg\psi \in \mathcal{M}$, to $\psi \notin \mathcal{M}$. S obzirom da je $\mathrm{sl}(\psi) < \mathrm{sl}(\varphi)$, prema induktovnoj hipotezi važi $\psi[\mu] = 0$. Dakle $\varphi[\mu] = 1$.

b. $\varphi = (\psi \vee \theta)$. Dakle $(\psi \vee \theta) \in \mathcal{M}$, pa $\psi \in \mathcal{M}$ ili $\theta \in \mathcal{M}$, recimo da je $\psi \in \mathcal{M}$. S obzirom da je $\mathrm{sl}(\psi) < \mathrm{sl}(\varphi)$, prema induktivnoj hipotezi $\psi[\mu] = 1$, dakle i $\varphi[\mu] = 1$.

Prema Teoremi potpune indukcije tvrđenje (3) važi, dakle $\mu \models \mathcal{M}$. S obzirom da je $\mathcal{T} \subseteq \mathcal{M}$, to je onda i $\mu \models \mathcal{T}$, dakle $\mathcal{T}$ je neprotivurečna teorija. □

Sledeći primer predstavlja uvod u drugi dokaz ove teoreme, zasnovan na topološkim metodama. Istovremeno, njime se daju obrisi infinitarnog iskaznog računa.

Primer 1.43 Beskonačni iskazni račun je proširenje klasičnog iskaznog računa u kojem se javljaju formule beskonačne dužine. Ne ulazeći u precizan opis ovih logika, definisaćemo beskonačne konjunkcije i beskonačne disjunkcije običnih iskaznih formula nad nekim skupom iskaznih promenljivih $\mathcal{P}$.

Neka je je X poizvoljan skup (dakle može biti i beskonačan) nekih iskaznih formula nad $\mathcal{P}$. Tada je $\bigwedge X$ uopštena konjunkcija, dok je $\bigvee X$ uopštena disjunkcija formula iz skupa X. Ako je X beskonačan skup, tada ove formule takođe nazivamo beskonačnom konjunkcijom, odnosno beskonačnom disjunkcijom. Umesto $\bigwedge X$ takođe koristimo zapis $\bigwedge_{\varphi\in X}\varphi$, dok $\bigvee X$ zapisujemo pomoću $\bigvee_{\varphi\in X}\varphi$. Ako je X indeksiran skup, na primer, $X=\{\varphi_0,\varphi_1,\varphi_2,\ldots\}$, tada $\bigvee X$ zapisujemo takođe pomoću $\bigvee_{n\in N}\varphi_n$. Slična notacija važi i za uopštene konjunkcije. Ako je X konačan skup, vidimo da se onda pojam uopštene disjunkcije poklapa sa pojmom obične disjunkcije, i da slično važi za uopštenu konjunkciju.

Logičku vrednost ovih formula definišemo na sledeći način. Neka su $\psi=\bigvee X$ i $\theta=\bigwedge X$ uopštena disjunkcija odnosno uopštena konjunkcija, i neka je μ valuacija promenljivih iz $\mathcal{P}$. Tada $\psi[\mu]=1$ akko *bar za jednu* formulu $\varphi\in X$ važi $\varphi[\mu]=1$, dok je $\theta[\mu]=1$ akko za *svaku* formulu $\varphi\in X$ važi $\varphi[\mu]=1$. Uopštena formula je tautologija akko ona ima vrednost 1 za sve valuacije promenljivih $\mathcal{P}$. Ukoliko je $X=\emptyset$, primetimo da je tada $\bigwedge X$ tautologija, dok je $\bigvee X$ kontradikcija. Sledeće tvrđenje kazuje da se svojstvo tautologičnsoti za uopštene disjunkcije reflektuje na neku konačnu podformulu.

Teorema 1.43a (Teorema refleksije) Neka je $\bigvee X$ uopštena tautologija. Tada postoji konačan $Y\subseteq X$ takav da je $\bigvee Y$ tautologija.

Dokaz. Neka je $\bigvee X$ uopštena tautologija i pretpostavimo suprotno, da ne postoji konačan $Y\subseteq X$ takav da je $\bigvee Y$ tautologija. Neka je $X'=\{\neg\varphi\colon \varphi\in X\}$. Tada svaki konačan podskup skupa X' ima model, te prema Teoremi kompaktnosti, X' ima model. Ali u tom slučaju $\bigvee X$ nije (uopštena) tautologija, što je kontradikcija pretpostavci. □

Napomena 1.43b Isto tako jednostavno iz Teoreme refleksije sledi Teorema kompaktnosti. Zaista, pretpostavimo Teoremu refleksije za formule nad promenljivama $\mathcal{P}$ i neka je X skup formula nad $\mathcal{P}$ sa svojstvom KN. Pretpostavimo da X nema model. U tom slučaju za $X'=\{\neg\varphi\colon \varphi\in X\}$, uopštena formula $\bigvee X'$ je tautologija. Onda prema Teoremi refleksije postoji konačan $Y'\subseteq X'$ takav da je $\bigvee Y'$ tautologija. Ali tada je $Y=\{\varphi\colon \neg\varphi\in Y'\}$ podskup skupa X i Y nema model, što je kontradikcija pretpostavci da X ima svojstvo KN. □ ♢

Podsetimo se da je topološki prostor $\mathcal{X}=(\mathcal{X},\tau)$ određen svojim domenom (nosačem) X i familijom τ svih njegovih otvorenih skupova. Prostor $\mathcal{X}$ je *kompaktan* ukoliko je svaki njegov otvoren pokrivač reducibilan na konačan podpokrivač. Drugim rečima, ako je $\{S_i\colon i\in I\}$ neka familija otvorenih skupova prostora $\mathcal{X}$ i važi $X=\bigcup_{i\in I}S_i$, tada postoji konačan $J\subseteq I$ tako da je $\bigcup_{j\in J}S_j=X$. U drugom dokazu Teoreme kompaktnosti koristićemo sledeće tvrđenje iz opšte topologije koje se odnosi na proizvod topoloških prostora.

Teorema 1.44 (Teorema kompakntosti, Tihonov) *Neka je $\{\mathcal{X}|_i\colon i\in I\}$ familija kompaktnih topoloških prostora. Tada je topološki proizvod $\prod_{i\in I}\mathcal{X}_i$ ovih prostora takođe kompaktan.*

Pogledajmo bliže strukturu prostora $\mathbf{2}^{\mathcal{P}}$. U izgradnji tog prostora biramo diskretnu topologiju na $\{0,1\}$, tj. $\tau=\{\emptyset,\{0\},\{1\},\{0,1\}\}$. Kako je domen ovog

prostora konačan, onda je on očigledno kompaktan. Neka je za iskazno slovo p, $X_p = \mathbf{2} = (2, \tau)$. Tada je prema teoremi Tihonova $\mathbf{2}^{\mathcal{P}} = \prod_{p\in\mathcal{P}} X_p$ kompaktan prostor. Tačke (elementi) u ovom prostoru su sva preslikavanja iz $\mathcal{P}$ u 2, tj. valuacije promenljivih iz $\mathcal{P}$. Prema definiciji topološkog proizvoda, topologija na $\mathbf{2}^{\mathcal{P}}$ je najmanja topologija takva da su projekcijske funkcije $\pi_p\colon \mu \mapsto \mu(p)$, $\mu \in 2^{\mathcal{P}}$, neprekidne. Otuda konačni preseci skupova

$$B_p = \pi_p^{-1}(1) = \{\mu \in 2^{\mathcal{P}}\colon \mu(p) = 1\}, \quad \bar{B}_p = \pi_p^{-1}(0) = \{\mu \in 2^{\mathcal{P}}\colon \mu(p) = 0\}$$

čine bazu prostora $2^{\mathcal{P}}$. Dakle, elementi baze prostora $2^{\mathcal{P}}$ su skupovi

$$B_\alpha = \{\mu \in 2^{\mathcal{P}}\colon \alpha \subseteq \mu\}$$

gde je α valuacija nekog konačnog podskupa skupa $S \subseteq \mathcal{P}$. Drugim rečima, elementi skupa B_α su sve ekstenzije konačne funkcije α, odnosno sve valuacije domena $\mathcal{P}$ sa istom restrikcijom α. Ako je $S = \{p_1, p_2, \ldots, p_n\}$ tada je

$$B_\alpha = \bigcap_{i\le i\le n} B_{p_i} \quad \text{i} \quad B_\alpha^c = \bigcup_{i\le i\le n} \bar{B}_{p_i}$$

Otuda sledi da je ne samo B_α, već i B_α^c takođe otvoren skup, tj. B_α je otvoreno-zatvoren skup. Dakle prostor $\mathbf{2}^{\mathcal{P}}$ ima bazu koja se sastoji od otvoreno-zatvorenih skupova. Ako je $\mathcal{P}$ beskonačan i prebrojiv, tada se prostor $\mathbf{2}^{\mathcal{P}}$ naziva Kantorov prostor. Za proizvoljno $\mathcal{P}$, dakle i u neprebrojivom slučaju, taj prostor nazivamo uopšten Kantorov prostor. Nekad se koristi i termin *dijadski prostor*. Konačni dijadski prostori nisu tako interesantni jer je tada $\mathbf{2}^{\mathcal{P}}$ diskretan. Sledeće zanimljivo tvrđenje koristićemo u drugom dokazu teoreme kompaktnosti.

Stav 1.45 *Neka je θ iskazna formula jezika $\mathcal{P}$ i neka je $\hat{\theta}\colon 2^{\mathcal{P}} \to 2$ pridružena iskazna funkcija. Tada je $\hat{\theta}$ neprekidna funkcija iz prostora $\mathbf{2}^{\mathcal{P}}$ u (diskretan) prostor $\mathbf{2}$.*

Dokaz Dovoljno je dokazati da je $\hat{\theta}^{-1}[X]$ otvoren skup u $\mathbf{2}^{\mathcal{P}}$ ako je X otvoren skup u $\mathbf{2}$, tj. za $X \in \tau$, $\tau = \{\emptyset, 2, \{0\}, \{1\}\}$. Zaista, $\hat{\theta}^{-1}[\emptyset] = \emptyset$ i $\hat{\theta}^{-1}[2] = 2^{\mathcal{P}}$ su otvoreni podskupovi prostora $\mathbf{2}^{\mathcal{P}}$. Dalje, neka je $S = \{p_1, p_2, \ldots, p_n\}$ skup svih iskaznih slova koja se javljaju u formuli θ i neka je $\Gamma = \{\alpha \in 2^S\colon \hat{\theta}[\alpha] = 1\}$. Dakle Γ je konačan skup. Ako je $X = \{1\}$, tada

$$\hat{\theta}^{-1}[X] = \{\mu \in 2^{\mathcal{P}}\colon \hat{\theta}[\mu] = 1\} = \{\mu \in 2^{\mathcal{P}}\colon \bigvee_{\alpha\in\Gamma} \alpha \subseteq \mu\} = \bigcup_{\alpha\in\Gamma} B_\alpha.$$

Dakle, $\hat{\theta}^{-1}[X]$ je (konačna) unija baznih skupova B_α, te je $\hat{\theta}^{-1}[X]$ otvoren skup u $\mathbf{2}^{\mathcal{P}}$. Slično, ako je $X = \{0\}$, biramo $\Gamma' = \{\alpha \in 2^S\colon \hat{\theta}[\alpha] = 0\}$. Tada je

$$\hat{\theta}^{-1}[X] = \{\mu \in 2^{\mathcal{P}}\colon \hat{\theta}[\mu] = 0\} = \{\mu \in 2^{\mathcal{P}}\colon \bigvee_{\alpha\in\Gamma'} \alpha \subseteq \mu\} = \bigcup_{\alpha\in\Gamma'} B_\alpha,$$

tj. i u ovom slučaju $\hat{\theta}^{-1}[X]$ je (konačna) unija baznih skupova, tj. otvoren skup. Dakle $\hat{\theta}$ je neprekidno preslikavanje iz prostora $\mathbf{2}^{\mathcal{P}}$ u prostor $\mathbf{2}$. □

Primetimo, uz uvedene oznake u dokazu, da je $\hat{\theta}^{-1}[X]$ konačna unija zatvorenih (baznih) skupova, dakle $\hat{\theta}^{-1}[X]$ je otvoreno-zatvoren skup. Ako je $\alpha \in 2$ i $X = \{\alpha\}$, umesto $\hat{\theta}^{-1}[X]$ pisaćemo takođe $\hat{\theta}^{-1}[\alpha]$.

Primer 1.46 *Neka je $\mathcal{S}$ iskazna teorija nad skupom iskaznih slova $\mathcal{P}$ i neka je $\mathcal{S}$ zatvorena za konačne disjunkcije: ako $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \in \mathcal{S}$ tada $\bigvee_{1\leq i\leq n} \vartheta_i \in \mathcal{S}$, $n \in N^+$. Tada važi:*

$$\text{Ako} \quad \bigwedge_{\mu\in 2^{\mathcal{P}}} \bigvee_{\vartheta\in\mathcal{S}} \hat{\vartheta}[\mu] = 1 \quad \text{onda} \quad \bigvee_{\vartheta\in\mathcal{S}} \bigwedge_{\mu\in 2^{\mathcal{P}}} \hat{\vartheta}[\mu] = 1.$$

Dokaz. Pretpostavimo da važi $\bigwedge_{\mu\in 2^{\mathcal{P}}} \bigvee_{\vartheta\in\mathcal{S}} \hat{\vartheta}[\mu] = 1$. Tada $2^{\mathcal{P}} = \bigcup_{\vartheta\in\mathcal{S}} \hat{\vartheta}^{-1}[1]$ i prema prethodnom tvrđenju $\hat{\vartheta}^{-1}[1]$ je otvoren skup u $\mathbf{2}^{\mathcal{P}}$. Dakle,

$$\mathcal{U} = \{\hat{\vartheta}^{-1}[1]\colon \vartheta \in \mathcal{S}\}$$

je otvoren pokrivač prostora $2^{\mathcal{P}}$. Zbog kompakntosti prostora $\mathbf{2}^{\mathcal{P}}$, $\mathcal{U}$ sadrži konačan potpokrivač, tj. postoji $n \in N^+$, postoje $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \in \mathcal{S}$ tako da je $2^{\mathcal{P}} = \bigcup_{1\leq i\leq n} \hat{\vartheta}^{-1}[1]$, te za $\vartheta = \bigvee_{1\leq i\leq n} \vartheta_i$ važi $\vartheta \in \mathcal{S}$ i $\bigwedge_{\mu\in 2^{\mathcal{P}}} \hat{\vartheta}[\mu] = 1$. □

Drugi dokaz Teoreme kompaktnosti za iskazni račun. U ovom dokazu pozvaćemo se na Napomenu 1.43b, prema kojoj iz teoreme refleksije sledi teorema kompaktnosti. Dakle, neka je X skup iskaznih formula nad $\mathcal{P}$ i pretpostavimo da je $\bigvee X$ tautologija. Tada je $2^{\mathcal{P}} = \bigcup_{\varphi\in X} \hat{\varphi}^{-1}[1]$. Funkcije $\hat{\varphi}$ su neprekidne, te je $\{\hat{\varphi}^{-1}[1]\colon \varphi \in X\}$ *otvoren* pokrivač prosora $2^{\mathcal{P}}$. S obzirom da je ovaj prostor kompaktan, onda postoje $\varphi_1, \varphi_2, \ldots, \varphi_n \in X$ takvi da je

$$2^{\mathcal{P}} = \hat{\varphi}_1^{-1}[1] \cup \ldots \cup \hat{\varphi}_n^{-1}[1],$$

tj. $\varphi_1 \vee \ldots \vee \varphi_n$ je tautologija i $\{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ je konačan podskup od X. □

U drugom dokazu Teoreme kompaktnosti koriste se slabiji uslovi (metamatematičke pretpostavke) iz teorije skupova nego što je to slučaj u prvom. Naime, prvi dokaz zasnovan je na Zornovoj lemi, dok je drugi dokaz zasnovan na svojstvu kompaktnosti prostora $\mathbf{2}^{\mathcal{P}}$. U okviru teorije skupova bez aksime izbora (sistem ZF), Zornova lema je ekvivalentna Aksiomi izbora i takođe Aksioma izbora uz aksiome teorije ZF za posledicu ima svojstvo kompaktnosti prostora $\mathbf{2}^{\mathcal{P}}$. S druge strane, Aksioma izbora se ne može dokazati samo na osnovu sistema ZF i svojstva kompaktnosti prostora $\mathbf{2}^{\mathcal{P}}$. Može se takođe dokazati u ZF da je Teorema kompaktnosti za iskazni račun ekvivalentna iskazu da je $\mathbf{2}^{\mathcal{P}}$ kompaktan prostor.

Postoje mnogobrojne primene teoreme kompaktnosti. U nekim primenama ključno mesto imaće činjenica da se valuacije skupa iskaznih slova $\mathcal{P}$ mogu smatrati *tačkama* Kantorovog prostora $2^{\mathcal{P}}$.

Primer 1.47 Produženje parcijalnog uređenja do linearnog uređenja. Parcijalno uređen skup je svaka struktura $\mathbf{A} = (A, \leq)$, gde je relacija $\leq$ domena

A refleksivna, tranzitivna i antisimetrična. Ako je pritom relacija $\leq$ i linearna, tj. zadovoljava uslov $\bigwedge_{a,b\in A}(a \leq b \vee b \leq a)$, tada kažemo da je $\mathbf{A}$ linearno uređen skup. Uređenje $(A, \preceq)$ je proširenje (produženje) uređenja $(A, \leq)$ ukoliko je $\leq \subseteq \preceq$, tj. $a \leq b$ povlači $a \preceq b$, $a, b \in A$. Dokazaćemo da se svako parcijalno uređenje može proširiti do linearnog uređenja.

Lema 1.47a Neka je $\mathbf{A} = (A, \leq)$ konačan parcijalno uređen skup. Tada se $\mathbf{A}$ može proširiti do linearno uređenog skupa.

Dokaz Dokaz izvodimo potpunom indukcijom po broju n elemenata domena A parcijalnog uređenja. Ako je $n = 1$, nema šta da se dokazuje. Neka je $|A| = n \geq 2$ i pretpostavimo (induktivna hipoteza) da tvrđenje važi za sve parcijalno uređene skupove koji imaju manje od n elemenata. S obzirom da je A konačan, postoji maksimalan element u $\mathbf{A}$, neka je to b. Neka je $B = A\backslash\{b\}$ i neka je $\leq'$ restrikcija uređenja $\leq$ na B, tj. $\leq' = \leq \cap B^2$. Tada je $(B, \leq')$ parcijalno uređen skup i $|B| < |A|$. Otuda, prema induktivnoj hipotezi, postoji linearno uređenje $(B, \preceq')$ koje širi $(B, \leq)$. Tada je $\preceq = \preceq' \cup \{(x, b) \colon x \in A\}$ linearno uređenje koje proširuje parcijalno uređenje $\leq$. □

Lema 1.47b Neka je $\mathbf{A} = (A, \leq_{\mathbf{A}})$ beskonačan parcijalno uređen skup. Tada se $\mathbf{A}$ može proširiti do linearno uređenog skupa.

Dokaz Dokaz koji sledi zasnovan je na primeni Teoreme kompaktnosti. U tu svrhu uvedimo skup iskaznih slova $\mathcal{P} = \{p_{ab} \colon a, b \in A\}$, neka $\leq$ označava određenu binarna relacija domena A i uvedimo sledeće iskazne teorije:

$\mathcal{T}_1 = \{p_{ab} \colon a, b \in A,\ a \leq b\}$, $\mathcal{T}_2 = \{p_{aa} \colon a \in A\}$,
$\mathcal{T}_3 = \{(p_{ab} \wedge p_{bc}) \Rightarrow a_{ac} \colon a, b, c \in A\}$, $\mathcal{T}_4 = \{\neg p_{ab} \vee \neg p_{ba} \colon a, b \in A,\ a \neq b\}$,
$\mathcal{T}_5 = \{p_{ab} \vee p_{ba} \colon a, b \in A\}$.

Neka je μ proizvoljna valuacija iskaznih promenljivih $\mathcal{P}$. Neposredno se proverava da je:

- $\mu \models \mathcal{T}_1$ akko μ "modelira" uređenje $\mathbf{A}$, tj. μ je karakteristična funkcija grafa relacije $\leq_{\mathbf{A}}$: $\mu(p_{ab}) = 1$ akko $a \leq_{\mathbf{A}} b$, $a, b \in A$. Drugim rečima, μ je model teorije $\mathcal{T}_1$ akko se relacije $\leq_{\mathbf{A}}$ i $\leq$ poklapaju.

- $\mu \models \mathcal{T}_2 \cup \mathcal{T}_3 \cup T_4$ akko μ inducira parcijalno uređenje na domenu A, tj. μ je karakteristična funkcija grafa nekog parcijalnog uređenja $\leq$ na A. Uređenje $\leq$ uvodi se pomoću: $a \leq b$ akko $\mu(p_{ab}) = 1$, $a, b \in A$. Ovde, teorija $\mathcal{T}_2$ reprezentuje svojstvo refleksivnosti, $\mathcal{T}_3$ tranzitivnosti i $\mathcal{T}_4$ svojstvo antisimetričnosti relacije $\leq$.

- $\mu \models \mathcal{T}_2 \cup \mathcal{T}_3 \cup T_4 \cup \mathcal{T}_5$ akko μ "modelira" linearno uređenje na domenu A. Ovde, teorija $\mathcal{T}_5$ modelira svojstvo linearnosti relacije $\leq$.

Neka je $\mathcal{T}_{\mathbf{A}} = \{p_{ab} \colon a, b \in A,\ a \leq_{\mathbf{A}} b\}$, i neka je $\mathcal{T} = \mathcal{T}_{\mathbf{A}} \cup \mathcal{T}_2 \cup \mathcal{T}_3 \cup \mathcal{T}_4 \cup \mathcal{T}_5$. Izaberimo neprazan konačan $\mathcal{S} \subseteq \mathcal{T}$ i neka je B skup svih konstanti iz A koje se pojavljuju kao indeksi u iskaznim slovima p_{ab}. S obzirom da je $\mathcal{S}$ konačan to je i B neprazan konačan podskup od A. Neka je $\leq_{\mathbf{B}}$ restrikcija uređenja $\leq_{\mathbf{A}}$ na

domen B, tada je $\mathbf{B} = (B, \leq_{\mathbf{B}})$ konačan parcijalno uređen skup. Prema Lemi 1.47a postoji linearno uređenje $(B, \preceq_{\mathbf{B}})$ koje produžuje $\mathbf{B}$. Neka je ν valuacija iskaznih promenljivih $\mathcal{P}$ definisana sa $\nu(p_{ab}) = 1$ akko $a \preceq_{\mathbf{B}} b$, $a, b \in B$. Tada je shodno prethodnim napomenama o teorijama $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_5$, valuacija ν model teorije $\mathcal{S}$. Dakle svaki konačan podskup teorije $\mathcal{T}$ ima model, te prema Teoremi kompaktnosti i teorija $\mathcal{T}$ ima model, neka je to μ. Neka je relacija $\preceq_{\mathbf{A}}$ domena A definisana na sledeći način: $a \preceq_{\mathbf{A}} b$ akko $\mu(p_{ab}) = 1,\ a, b \in A$. Tada je $(A, \preceq_{\mathbf{A}})$ linearno uređenje koje produžuje parcijalno uređenje $(A, \leq_{\mathbf{A}})$. Proverimo, na primer, da $\preceq_{\mathbf{A}}$ zaista produžuje $\leq_{\mathbf{A}}$: Neka su $a, b \in A$ i pretpostavimo da je $a \leq_{\mathbf{A}} b$. Tada $p_{ab} \in \mathcal{T}_1$, dakle $p_{ab} \in \mathcal{T}$. S obzirom da je μ model teorije $\mathcal{T}$, to je onda $\mu(p_{ab}) = 1$, odakle $a \preceq_{\mathbf{A}} b$. Na sličan način se dokazuje da je $\preceq_{\mathbf{A}}$ zaista linearno uređenje domena A. □

Posledica 1.47c Neka je $\mathbf{A} = (A, \leq)$ parcijalno uređen skup. Tada se $\mathbf{A}$ može proširiti do linearno uređenog skupa.

Posledica 1.47d Svaki neprazan skup A se može linearno urediti.

Dokaz Neka je $\leq$ najmanje parcijalno uređenje domena A, tj. za $a, b \in A$ neka je $a \leq b$ akko $a = b$. Tada tvrđenje sledi prema prethodnoj posledici. □

Kao što je napomenuto, iz Teoreme kompaktnosti ne sledi Aksioma izvora. Ipak, neke slabije forme Aksiome izbora mogu se izvesti.

Posledica 1.47e Iz Teoreme kompaktnosti sledi Aksioma izbora za familije nepraznih konačnih skupova.

Dokaz Neka je $\mathcal{S}$ familija nepraznih konačnih skupova i neka je $A = \cup\mathcal{S}$. Prema prethodnoj posledici, na osnovu Teoreme kompaktnosti postoji linearno uređenje $\leq$ domena A. Funkciju izbora f za familiju $\mathcal{S}$ definišemo pomoću $f(X) = b$ akko b je najmanji element skupa X u odnosu na uređenje $\leq$, $X \in \mathcal{S}$. Tada $\bigwedge_{X \in \mathcal{S}} f(X) \in X$. Ova definicija je korektna s obzirom da je svaki $X \in \mathcal{S}$ neprazan i konačan (te ima najmanji element). □