UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET

Dr Gradimir Vojvodić

PREDAVANJA IZ MATEMATIČKE LOGIKE

Novi Sad, 2007.

Naziv Udžbenika "PREDAVANJA IZ MATEMATIČKE LOGIKE"(I DEO "PREDAVANJA IZ MATEMATIČKE LOGIKE I ALGEBRE")

Autor: Dr Gradimir Vojvodić, redovni profesor Prirodno-matematičkog fakulteta u Novom Sadu

Recenzenti: Dr Miodrag Rašković, redovni profesor Prirodno-matematičkog fakulteta u Kragujevcu
Dr Milan Grulović, redovni profesor Prirodno-matematičkog fakulteta u Novom Sadu

Izdavač: Prirodno-matematički fakultet u Novom Sadu

Glavni i odgovorni urednik pojedinačnog izdanja: Dr Miroslav Vesković, dekan Prirodno-matematičkog fakulteta u Novom Sadu

Štampano u ... primeraka, III dopunjeno i izmenjeno izdanje
(I izdanje, Edicija Univerzitetski udžbenik, broj 68, Novi Sad, 1998.)

Štampa: FUTURA, Novi Sad

Sadržaj

Predgovor

Ovaj tekst obuhvata predavanja iz predmeta Matematička logika. Namenjen je pre svega studentima informatike Prirodno-matematičkog fakulteta u Novom Sadu. Nastao je iz moje knjige "Predavanja iz matematičke logike i algebre"Novi Sad 1998.

Knjiga sadrži 3 poglavlja. Tekst sadrži i brojne primere i urađene zadatke. Sve to treba da omogući brže i lakše usvajanje gradiva. Deo gradiva obrajen je u knjizi G. Vojvodić, B. Šobot: "Zbirka zadataka iz matematičke logike i algebre" Univerzitet u Novom Sadu, PMF Novi Sad, Novi Sad 2003. Takođe, i okviri u kojima su izloženi pojedini delovi teksta, uslovljeni su fondom časova, pa čitaoce koji ih žele proširiti upućujem na literaturu navedenu na kraju knjige. Iz tih knjiga preuzeti su neki zadaci, tvrđenja, kao i neki primeri.

Posebnu zahvalnost dugujem Viktoru Kunčaku, iz čijih beležaka sa mojih predavanja je nastao ovaj tekst. Viktor Kunčak je tehnički obradio tekst, dao brojne korisne sugestije i pažljivo proverio rešenja zadataka. Njegovom zaslugom je proširen odeljak 2.7.7 u odnosu na izvorni tekst predavanja.

Zahvaljujem se recenzentima na korisnim komentarima i primedbama koje su mi ukazali nakon pažljivog čitanja rukopisa.

U Novom Sadu, oktobar 2007. Gradimir Vojvodić

*

Glava 1

Iskazni račun

1.1 Operacije sa iskazima

Iskaz je rečenica koja ima smisla (taj smisao se naziva *sud*) i koja je u pogledu tačnosti ili tačna ili lažna. Da je iskaz tačan obeležavamo sa $\top$, a da je netačan sa $\bot$.

Primer 1.1 Rečenica $2+2=4$ je tačan iskaz. Rečenica $2 \cdot 3 < 5$ je netačan iskaz. Rečenica "Video sam dete sa drugog sprata" nije iskaz, jer je neprecizna. Izjava Epeminida sa ostrva Krita "Svi stanovnici Krita lažu" nije iskaz jer joj ne možemo dodeliti istinitostnu vrednost. Hipoteza Golbaha (C. H. Golbach) ("Svaki paran broj veći ili jednak od četiri može se napisati kao zbir dva prosta broja" jeste iskaz, jer ima istinitosnu vrednost $\top$ ili $\bot$, samo što nam ta istinitosna vrednost nije poznata. $\triangle$

Iskaze ćemo označavati slovima p, q, r, ... Takođe umesto "ako i samo ako" pišemo "akko".

Definicija 1.2

Disjunkcija redom iskaza p i q je iskaz "p ili q", u oznaci $p \vee q$, koji je tačan akko je bar jedan od iskaza p, q tačan.

Konjunkcija redom iskaza p i q je iskaz "p i q", u oznaci $p \wedge q$, koji je tačan akko su oba iskaza p i q tačni.

Implikacija redom iskaza p i q je iskaz "ako p onda q", u oznaci $p \Rightarrow q$, koji je netačan akko je p tačan, a q netačan.

Ekvivalencija redom iskaza p i q je iskaz "p akko q", u oznaci $p \Leftrightarrow q$, koji je tačan akko su ili oba iskaza tačna ili oba iskaza netačna.

Negacija iskaza p je iskaz "ne p", u oznaci $\neg p$, koji je tačan akko je p netačan iskaz.

1.2 Iskazne formule

Neka je $Var = \{p_1, \ldots, p_n, \ldots\}$ prebrojiv (videti odeljak 3.4.3) skup iskaznih slova (promenljive), $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$ logički veznici, a $\top$ i $\bot$ logičke konstante (logičke konstante se mogu, a ne moraju uvoditi kao deo iskaznih formula).

Definicija 1.3

1. Iskazna slova (i logičke konstante) su iskazne formule.
2. Neka su A i B oznake za iskazne formule. Tada su iskazne formule i $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ i $(\neg A)$.
3. Iskazne formule se dobijaju samo konačnom primenom pravila 1 i 2.

Definicija 1.4 Formula D je podformula formule C akko je D formula koja je deo formule C.

Usvajamo sledeći dogovor o brisanju zagrada:

- spoljne zagrade se brišu;
- operacijama dodeljujemo različit prioritet: $\neg$ vezuje najjače, $\wedge$ i $\vee$ slabije, a $\Rightarrow$ i $\Leftrightarrow$ najslabije.

Primer 1.5 $\neg p \vee q \Rightarrow r$ znači $(((\neg p) \vee q) \Rightarrow r)$. $\triangle$

1.3 Iskazna algebra

Definicija 1.6 Neka su $\bot$ i $\top$ dva različita znaka. Uređena šestorka

$$(\{\top, \bot\}, \wedge, \vee, \Rightarrow, \Leftrightarrow, \neg)$$

naziva se iskazna algebra ako su $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ binarne operacije skupa $\{\top, \bot\}$ date tablicama

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

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

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

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

a $\neg$ unarna operacija data sledećom tablicom.

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

Prioritet operacija odgovara prioritetu logičkih veznika u iskaznim formulama. Svako preslikavanje $\{\top, \bot\}^n \rightarrow \{\top, \bot\}$ naziva se n-arna operacija iskazne algebre. Osim navedenih operacija, u iskaznoj algebri se često posmatraju i sledeće dve:

$$x \uparrow y = \neg(x \wedge y) \quad \text{(Šeferova (Sheffer))}$$
$$x \downarrow y = \neg(x \vee y) \quad \text{(Lukasijevičeva (J. Lukasiewicz)).}$$

1.4 Odnos iskaznih formula i iskazne algebre

Iskazne formule interpretiramo u iskaznoj algebri.

Definicija 1.7 Valuacija α je preslikavanje *Var* $\rightarrow \{\top, \bot\}$ koje iskaznim slovima dodeljuje vrednosti iz skupa $\{\bot, \top\}$.

Definicija 1.8 Vrednost formule A u valuaciji α, u oznaci $v_\alpha(A)$, definisana je na sledeći način:

$$
\begin{array}{lll}
v_\alpha(p_i) & = \alpha(p_i), & \text{za iskazno slovo } p_i; \\
v_\alpha(A \wedge B) & = v_\alpha(A) \wedge v_\alpha(B); & \\
v_\alpha(A \vee B) & = v_\alpha(A) \vee v_\alpha(B); & \\
v_\alpha(A \Rightarrow B) & = v_\alpha(A) \Rightarrow v_\alpha(B); & \\
v_\alpha(A \Leftrightarrow B) & = v_\alpha(A) \Leftrightarrow v_\alpha(B); & \\
v_\alpha(\neg A) = \neg v_\alpha(A). & &
\end{array}
$$

Napomena 1.9 Postoji bitna razlika između oznaka $\wedge$, $\vee$, $\Rightarrow$ i $\Leftrightarrow$ koje se javljaju sa leve i desne strane definicije 1.8. U formuli $A \wedge B$ oznaka $\wedge$ se javlja kao *logički veznik*, tj. element azbuke koji se koristi pri izgradnji formula kao nizova simbola, dok sa desne strane $\wedge$ predstavlja *logičku operaciju* kao preslikavanje $\wedge : \{\top, \bot\}^2 \rightarrow \{\top, \bot\}$, koje zbog preglednosti pišemo u infiksnom obliku. $\diamond$

Napomena 1.10 Iz definicije sledi da $v_\alpha(A)$ zavisi samo od vrednosti $\alpha(q_1), \ldots, \alpha(q_k)$ gde su $q_1, \ldots, q_k$ promenljive koje se javljaju u formuli A. Formulu čije su promenljive među promenljivim $q_1, \ldots, q_k$ označavamo sa $A(q_1, \ldots, q_k)$. $\diamond$

Interpretacijom u iskaznoj algebri iskaznoj formuli $A(q_1, \ldots, q_k)$ dodeljujemo funkciju

$$\bar{A} : \{\top, \bot\}^k \rightarrow \{\top, \bot\}$$

za koju važi

$$\bar{A}(x_1, \ldots, x_k) = v_\alpha(A(q_1, \ldots, q_k))$$

gde je α valuacija za koju važi $\alpha(q_i) = x_i$ za $i \in \{1, 2, \ldots k\}$. Ako je data formula $A(q_1, \ldots, q_k)$ i $B_1, \ldots, B_k$ su proizvoljne iskazne formule, tada sa $A(B_1, \ldots, B_k)$ označavamo formulu koja je dobijena od formule $A(q_1, \ldots, q_k)$ zamenom iskaznih slova $q_1, \ldots, q_k$ redom formulama $B_1, \ldots, B_k$. Formula $A(B_1, \ldots, B_k)$ se naziva *instanca* formule $A(q_1, \ldots, q_k)$.

Napomena 1.11 Umesto da formulu označimo sa $A(x)$, a kasnije rezultat zamene promenljive x formulom F označavamo sa $A(F)$, možemo koristiti oznaku $A[x/F]$ za rezultat zamene promenljive x formulom F. Prednost ovakvog zapisa je što za datu formulu A ne moramo znati koje se sve promenljive u njoj javljaju. U tom slučaju $[x/F]$ funkcioniše kao preslikavanje skupa formula u skup formula. Ovo preslikavanje formuli A pridružuje formulu $A[x/F]$ i naziva se *zamena*. U opštem slučaju, ako su $q_1, \ldots, q_n$ proizvoljna međusobno različita iskazna slova, tada definišemo zamenu koja formuli A pridružuje formulu $A[q_1/F_1, \ldots, q_n/F_n]$ u kojoj su sve pojave promenljivih $q_1, \ldots, q_n$ zamenjene redom formulama $F_1, \ldots, F_n$. Definiciju zamene možemo precizirati sledećim jednakostima:

$$\begin{aligned}
q_i[q_1/F_1, \ldots, q_n/F_n] &= F_i \qquad \text{za } 1 \leq i \leq n \\
x[q_1/F_1, \ldots, q_n/F_n] &= x \qquad \text{ako } x \notin \{q_1, \ldots, q_n\} \\
(\neg A)[q_1/F_1, \ldots, q_n/F_n] &= \neg(A[q_1/F_1, \ldots, q_n/F_n]) \\
(A \wedge B)[q_1/F_1, \ldots, q_n/F_n] &= A[q_1/F_1, \ldots, q_n/F_n] \wedge B[q_1/F_1, \ldots, q_n/F_n] \\
(A \vee B)[q_1/F_1, \ldots, q_n/F_n] &= A[q_1/F_1, \ldots, q_n/F_n] \vee B[q_1/F_1, \ldots, q_n/F_n] \\
(A \Rightarrow B)[q_1/F_1, \ldots, q_n/F_n] &= A[q_1/F_1, \ldots, q_n/F_n] \Rightarrow B[q_1/F_1, \ldots, q_n/F_n] \\
(A \Leftrightarrow B)[q_1/F_1, \ldots, q_n/F_n] &= A[q_1/F_1, \ldots, q_n/F_n] \Leftrightarrow B[q_1/F_1, \ldots, q_n/F_n].
\end{aligned}$$

$\diamond$

Definicija 1.12 Formula A je *tautologija*, u oznaci $\models A$, akko za sve valuacije α važi $v_\alpha(A) = \top$.

Tautologije opisuju zakonitosti matematičke logike i zaključivanja uopšte, i upućuju na pravila koja se koriste u dokazivanjima.

Primer 1.13 Sledeća tablica pokazuje da, bez obzira koje vrednosti valuacija dodeljuje promenljivim p i q, vrednost formule $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ je $\top$. Zato je ova formula tautologija.

p	q	$p \Rightarrow q$	$\neg p \vee q$	$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$
$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$

$\triangle$

U nastavku navodimo spisak nekih tautologija.

1. $p \Rightarrow p$
2. $p \vee \neg p$ (zakon isključenja trećeg)
3. $\neg(p \wedge \neg p)$ (zakon neprotivrečnosti)
4. $\neg\neg p \Rightarrow p$ (zakon dvojne negacije)
5. $\neg p \Rightarrow (p \Rightarrow q)$
6. $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$ (zakon kontrapozicije)

7. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
8. $(p \wedge p) \Leftrightarrow p$; $(p \vee p) \Leftrightarrow p$ (zakon idempotencije)
9. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
10. $p \wedge q \Leftrightarrow q \wedge p$ (zakon komutativnosti za $\wedge$ i $\vee$)
11. $p \wedge (p \vee q) \Leftrightarrow p$; $p \vee (p \wedge q) \Leftrightarrow p$ (zakon apsopcije)
12. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ (distributivnost $\wedge$ prema $\vee$)
13. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ (De Morganovi zakoni)
14. $p \Leftrightarrow p$
15. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s)$
16. $(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$
17. $(p \Leftrightarrow q) \wedge (r \Leftrightarrow s) \Rightarrow ((p * r) \Leftrightarrow (q * s))$
    gde je $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ proizvoljan logički veznik
18. $p \wedge (p \Rightarrow q) \Rightarrow q$
19. $(p \Rightarrow q \wedge r) \Leftrightarrow ((p \Rightarrow q) \wedge (p \Rightarrow r))$
20. $(p \vee q \Rightarrow r) \Leftrightarrow ((p \Rightarrow r) \wedge (q \Rightarrow r))$
21. $(p \wedge \neg q \Rightarrow r \wedge \neg r) \Leftrightarrow (p \Rightarrow q)$
22. $(\neg p \Rightarrow r \wedge \neg r) \Rightarrow p$
23. $(p \wedge q \Rightarrow r) \Leftrightarrow (p \wedge \neg r \Rightarrow q)$
24. $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$
25. $p \vee \top \Leftrightarrow \top$; $p \wedge \top \Leftrightarrow p$
26. $(p \vee \bot) \Leftrightarrow p$; $(p \wedge \bot) \Leftrightarrow \bot$
27. $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$
28. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

Tvrđenje 1.14 *Ako* $\models A$ *i* $\models A \Rightarrow B$ *onda* $\models B$.

Dokaz. Neka je α proizvoljna valuacija. Pošto $\models A$, važi $v_\alpha(A) = \top$. Iz $\models A \Rightarrow B$ sledi $v_\alpha(A \Rightarrow B) = \top$. Tada je, prema definiciji 1.8, $(v_\alpha(A) \Rightarrow v_\alpha(B)) = \top$ tj. $(\top \Rightarrow v_\alpha(B)) = \top$. Odatle prema tablici za implikaciju sledi $v_\alpha(B) = \top$. Pošto je α bilo proizvoljno, sledi da za svako α važi $v_\alpha(B) = \top$. Dakle $\models B$. ∎

Sledeće tvrđenje pokazuje da su instance tautologija tautologije.

Tvrđenje 1.15 *Neka je A proizvoljna formula, $q_1, \ldots, q_k$ različite promenljive, a B_1, $\ldots, B_k$ proizvoljne iskazne formule. Tada ako*

$$\models A$$

onda

$$\models A[q_1/B_1, \ldots, q_k/B_k].$$

Dokaz. Neka je α proizvoljna valuacija. Pošto svaka od formula B_i uzima vrednosti iz skupa $\{\top, \bot\}$, posmatrajmo valuaciju α' datu sa $\alpha'(q_i) = v_\alpha(B_i)$. Kako je formula $A[q_1/B_1, \ldots, q_k/B_k]$ dobijena zamenom svih q_i odgovarajućim B_i, važi

$$v_\alpha(A[q_1/B_1, \ldots, q_k/B_k]) = v_{\alpha'}(A)$$

što se može proveriti i indukcijom po broju logičkih veznika u formuli A. Pošto $\models A$, to i za α' važi $v_{\alpha'}(A) = \top$. Zato i $v_\alpha(A[q_1/B_1, \ldots, q_k/B_k]) = \top$. Pošto je α bila proizvoljna valuacija, sledi $\models A[q_1/B_1, \ldots, q_k/B_k]$. ■

Tvrđenje 1.16 *Neka su A i B proizvoljne formule i neka je $F(A)$ formula koja ima kao svoju podformulu formulu A. Tada*

$$\models (A \Leftrightarrow B) \Rightarrow (F(A) \Leftrightarrow F(B))$$

gde je $F(B)$ dobijena od formule $F(A)$ zamenom podformule A formulom B.

Dokaz. Neka je α proizvoljna valuacija.

1. $v_\alpha(A \Leftrightarrow B) = \bot$. Tada na osnovu osobina implikacije direktno sledi

$$v_\alpha((A \Leftrightarrow B) \Rightarrow (F(A) \Leftrightarrow F(B)) = \top.$$

2. $v_\alpha(A \Leftrightarrow B) = \top$. Tada je

$$v_\alpha(A) = v_\alpha(B)$$

pa je

$$v_\alpha(F(A)) = \bar{F}(v_\alpha(A)) = \bar{F}(v_\alpha(B)) = v_\alpha(F(B))$$

gde je $\bar{F}$ funkcija iskaznog računa dobijena interpretacijom svih delova iskazne formule osim formule A. Odatle po definiciji ekvivalencije sledi $v_\alpha(F(A) \Leftrightarrow F(B)) = \top$, pa je i cela implikacija tačna.

■

Napomena 1.17 Prethodni dokaz se može sprovesti i indukcijom po broju logičkih veznika u formuli $F(A)$. $\diamond$

Primer 1.18 Neka je Φ oznaka za formulu $p \wedge (q \wedge r) \Leftrightarrow r \wedge (p \wedge q)$. Pokazaćemo da je Φ tautologija. Označimo prvo sa Ψ tautologiju 9:

$$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r.$$

Ako na tautologiji 10 primenimo zamenu $[p/(p \wedge q), q/r]$ dobijamo formulu

$$(p \wedge q) \wedge r \Leftrightarrow r \wedge (p \wedge q)$$

koja je prema tvrđenju 1.15 takođe tautologija. Prema tvrđenju 1.16 važi

$$\begin{aligned} &\models ((p \wedge q) \wedge r \Leftrightarrow r \wedge (p \wedge q)) \\ &\qquad \Rightarrow ((p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r) \Leftrightarrow r \wedge (p \wedge q))), \end{aligned}$$

pa prema tvrđenju 1.14 dobijamo

$$\models (p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r) \Leftrightarrow r \wedge (p \wedge q))$$

tj. $\models \Psi \Leftrightarrow \Phi$. Neka je α proizvoljna valuacija. Kako je $v_\alpha(\Psi \Leftrightarrow \Phi) = \top$, sledi

$$v_\alpha(\Psi) \Leftrightarrow v_\alpha(\Phi) = \top.$$

Formula Ψ je tautologija, pa $v_\alpha(\Psi) = \top$, odakle dobijamo $v_\alpha(\Phi) = \top$. Pošto je α bila proizvoljna valuacija, sledi $\models \Phi$. Time smo dokazali da je Φ tautologija. $\triangle$

Napomena 1.19 Primenom sličnog postupka kao u prethodnom primeru može se pokazati da istinitosna vrednost $v_\alpha(A)$ formule A ne zavisi od redosleda podformula koje učestvuju u konjunkcijama formule A. Slično važi i za disjunkciju. To nam omogućava da izostavljamo zagrade u formulama kada nam je bitna samo istinitosna vrednost koju one uzimaju pri datoj valuaciji. Tako umesto $(p \wedge (q \wedge r)) \wedge s$ možemo pisati samo $p \wedge q \wedge r \wedge s$. $\diamond$

Primer 1.20 (Interpolaciona lema Krejga za iskazni račun). Neka je $A \vee B$ tautologija. Tada postoji formula C čija se iskazna slova pojavljuju i u A i u B takva da su $A \vee C$ i $\neg C \vee B$ tautologije. (Uputstvo. Dokaz je indukcijom po broju iskazanih slova koje se pojavljuju u A ali ne i u B.) $\triangle$

1.5 Metode za dokazivanje tautologija

1.5.1 Tablična metoda

Istinistosna vrednost date iskazne formule zavisi samo od interpretacije iskaznih slova koje u njoj učestvuju. Iskazna slova uzimaju vrednosti iz skupa $\{\top, \bot\}$. Ako su $q_1, \ldots, q_k$ iskazna slova formula A tada ona mogu uzeti 2^k različitih vrednosti. Ovaj postupak za proveru da li je formula iskaznog računa tautologija se sastoji u proveri istinitosne vrednosti iskazne formule A u svih 2^k slučajeva, što se prikazuje tablicom (primer 1.13).

1.5.2 Svođenje na protivrečnost

Da bismo proverili da li je iskazna formula A tautologija, pretpostavimo da A nije tautologija, tj. da je za neke vrednosti iskaznih slova netačna, i tražimo vrednosti koje iskazna slova moraju imati da bi formula bila netačna. Ukoliko pronadjemo bar jedan takav niz vrednosti za iskazna slova, to je primer koji ukazuje da formula nije tautologija. Ako se dokaže da takve vrednosti ne postoje, onda je pokazano da je ta formula tautologija. Ovaj metod je naročito pogodan ukoliko formula sadrži veliki broj implikacija, jer ako je implikacija $p \Rightarrow q$ netačna, onda p mora biti tačno, a q netačno.

Primer 1.21 Proverimo da li je $\models (p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$. Pretpostavimo suprotno: da je za neke vrednosti p, q, r vrednost formule $\perp$. Tada $v_\alpha(p \Rightarrow (q \Rightarrow r)) = \top$ i $v_\alpha((p \Rightarrow q) \Rightarrow (p \Rightarrow r) = \perp$. Iz poslednje jednakosti sledi $v_\alpha(p \Rightarrow q) = \top$ i $v_\alpha(p \Rightarrow r) = \perp$, pa $\alpha(p) = \top$ i $\alpha(r) = \perp$. Iz $v_\alpha(p \Rightarrow q) = \top$ tada sledi $\alpha(q) = \top$. No tada je $v_\alpha(p \Rightarrow (q \Rightarrow r)) = \perp$ što je kontradikcija. Dakle $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ je tautologija. $\triangle$

1.5.3 Svođenje na konjunktivni oblik

Ovaj metod se zasniva na tautologijama

1. $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$;
2. $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$;
3. $(\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$;
4. $(\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$;
5. $(\neg\neg A) \Leftrightarrow A$;
6. $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$.

Neka je $F_0(q_1, \ldots, q_k; \Leftrightarrow, \Rightarrow, \wedge, \vee, \neg)$ formula čija su iskazna slova $q_1, \ldots, q_k$. Primenom tvrđenja 1.16 i tautologije 1 na sve podformule formule F_0 oblika $A \Leftrightarrow B$ dobijamo formulu $F_1(q_1, \ldots, q_k; \Rightarrow, \wedge, \vee, \neg)$ koja ne sadrži $\Leftrightarrow$, a ekvivalentna je sa F_0 (ima istu istinitosnu vrednost kao i F_0 bez obzira na vrednosti učestvujućih promenljivih). Primenom tvrđenja 1.16 i tautologije 2 na F_1 dobijamo ekvivalentnu formulu $F_2(q_1, \ldots, q_k; \wedge, \vee, \neg)$. Primenom tautologija 3, 4, 5 i tvrđenja 1.16 dobijamo formulu F_3 u kojoj se negacija javlja samo uz iskazna slova. Ako primenjujući tautologiju 6 u formuli F_3 potreban broj puta zamenimo podformule oblika $A \vee (B \wedge C)$ podformulama $(A \vee B) \wedge (A \vee C)$, dobijamo formulu F_4 u obliku

$$M_1 \wedge M_2 \wedge \ldots \wedge M_k$$

gde je svaki M_i oblika $a_{i_1} \vee a_{i_2} \ldots \vee a_{ik_i}$ gde su a_{i_j} iskazna slova ili njihove negacije. Za F_4 kažemo da je u *konjunktivnom obliku*. F_4 je tautologija akko su sve formule M_i tautologije, a to važi akko se u svakoj od formula M_i javlja neko iskazno slovo p zajedno sa svojom negacijom $\neg p$. Pošto su formule F_0 i F_4 ekvivalentne, time utvrđujemo i da li je početna formula tautologija.

Primer 1.22 Dokažimo da je formula $(p \Rightarrow q \wedge \neg q) \Rightarrow \neg p$ tautologija. Svođenjem na konjuktivni oblik dobijamo sledeći niz ekvivalentnih formula.

$$\begin{array}{l}
(p \Rightarrow (q \wedge \neg q)) \Rightarrow \neg p, \\
\neg p \vee (q \wedge \neg q) \Rightarrow \neg p, \\
\neg(\neg p \vee (q \wedge \neg q)) \vee \neg p, \\
(\neg\neg p \wedge \neg(q \wedge \neg q)) \vee \neg p, \\
(p \wedge (\neg q \vee \neg\neg q)) \vee \neg p, \\
(p \wedge (\neg q \vee q)) \vee \neg p, \\
(p \vee \neg p) \wedge (\neg q \vee q \vee \neg p).
\end{array}$$

Poslednja formula je tačna u svim valuacijama, pa je tautologija. Kako je ona ekvivalentna polaznoj formuli, i polazna formula je tautologija. $\triangle$

Primer 1.23 Ispitajmo da li je tautologija formula

$$((p \vee q) \wedge r) \vee (\neg r \wedge p).$$

Svođenjem na konjunktivni oblik dobijamo formulu

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

koja je ekvivalentna sa $(p \vee q \vee \neg r) \wedge (p \vee q) \wedge (r \vee \neg r) \wedge (r \vee p)$. Vidimo da već prva disjunkcija ne sadrži nijedno slovo zajedno sa njegovom negacijom. Zato možemo definisati valuaciju u kojoj je ta disjunkcija netačna:

$$\begin{array}{rcl}
\alpha(p) & = & \perp \\
\alpha(q) & = & \perp \\
\alpha(r) & = & \top
\end{array}$$

Kako je netačna prva disjunkcija, i cela formula je netačna. Tako smo našli valuaciju za koju polazna formula nije tačna, pa ne može biti tautologija. $\triangle$

1.5.4 Diskusija po iskaznom slovu

Diskusija po iskaznom slovu se zasniva na sledećoj posledici definicije tautologije: $F(q_1, \ldots, q_{k-1}, q_k)$ je tautologija akko su obe formule $F(q_1, \ldots, q_{k-1}, \top)$ i $F(q_1, \ldots, q_{k-1}, \perp)$ tautologije.

Primer 1.24 Ukoliko vršimo diskusiju po iskaznom slovu p, dobijamo da je formula $A(p, q, r)$ data sa

$$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$$

tautologija akko

1. $\models (\top \Rightarrow (q \Rightarrow r)) \Rightarrow ((\top \Rightarrow q) \Rightarrow (\top \Rightarrow r))$, što je tačno jer je
$$v_\alpha(\top \Rightarrow C) = v_\alpha(C)$$
za svaku formulu C, a $(q \Rightarrow r) \Rightarrow (q \Rightarrow r)$ je instanca tautologije $p \Rightarrow p$,
2. $\models (\bot \Rightarrow (q \Rightarrow r)) \Rightarrow ((\bot \Rightarrow q) \Rightarrow (\bot \Rightarrow r))$, što je, s obzirom da je
$$v_\alpha(\bot \Rightarrow C) = \top,$$
ekvivalentno sa $\models \top \Rightarrow (\top \Rightarrow \top)$.

$\triangle$

Zadatak 1.25 Neka je $F(q_1, \ldots, q_n; \Leftrightarrow)$ iskazna formula koja sadrži promenljive q_1, $\ldots, q_n$ i ne sadrži druge promenljive, a od logičkih veznika sadrži samo $\Leftrightarrow$. Dokazati da je F tautologija akko se svako iskazno slovo javlja paran broj puta.

Rešenje. Na osnovu istinitosne tablice za logičku operaciju $\Leftrightarrow$ lako se proverava da su formule
$$(A \Leftrightarrow (B \Leftrightarrow C)) \Leftrightarrow ((A \Leftrightarrow B) \Leftrightarrow C)$$
$$(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$$
tautologije. Primetimo takođe da važi $v_\alpha(p \Leftrightarrow p) = \top$ i $(\top \Leftrightarrow x) = x$. Označimo sa p^n formulu
$$\underbrace{p \Leftrightarrow p \Leftrightarrow \cdots \Leftrightarrow p}_{n}.$$
Ako je $n = 2m$ paran broj, tada je
$$v_\alpha(p^{2m}) = \underbrace{v_\alpha(p \Leftrightarrow p) \Leftrightarrow \cdots \Leftrightarrow v_\alpha(p \Leftrightarrow p)}_{m} = \top \Leftrightarrow \cdots \Leftrightarrow \top = \top.$$
Ako je $n = 2m+1$ neparan broj, tada je
$$v_\alpha(p^{2m+1}) = v_\alpha(p^{2m}) \Leftrightarrow v_\alpha(p) = \top \Leftrightarrow \alpha(p) = \alpha(p).$$
Takođe je jasno da za valuaciju za koju važi $\alpha(p) = \top$ važi
$$v_\alpha(p^n) = \top \Leftrightarrow \top \Leftrightarrow \cdots \Leftrightarrow \top = \top.$$

Neka je $F(q_1, \ldots, q_n; \Leftrightarrow)$ proizvoljna formula koja sadrži promenljive $q_1, \ldots, q_n$ i ne sadrži druge promenljive, a od logičkih veznika sadrži samo $\Leftrightarrow$. Tada se primenom asocijativnosti i komutativnosti ekvivalencije i tvrđenja 1.16 formula F može transformisati u njoj ekvivalentnu formulu F':
$$q_1^{k_1} \Leftrightarrow q_2^{k_2} \Leftrightarrow \cdots \Leftrightarrow q_n^{k_n}$$

pri čemu se svaka od promenljivih javlja jednak broj puta u formulama F i F'. (Grupišemo ista iskazna slova u formuli.) Pokazaćemo da je formula F' tautologija ako su svi brojevi $k_1, \ldots, k_n$ parni, a nije tautologija ako je neki od brojeva $k_1, \ldots, k_n$ neparan.

Pretpostavimo da su svi brojevi $k_1, \ldots, k_n$ parni. Tada za svaku valuaciju α imamo

$$v_\alpha(F') = v_\alpha(q_1^{k_1}) \Leftrightarrow \cdots \Leftrightarrow v_\alpha(q_n^{k_n}) = \top \Leftrightarrow \cdots \Leftrightarrow \top = \top,$$

pa je F' tautologija. Pretpostavimo sada da je za $1 \leq i \leq n$ neki k_i neparan. Posmatrajmo valuaciju α datu sa

$$\alpha(p) = \begin{cases} \perp, & \text{ako je } p = q_i \\ \top, & \text{inače.} \end{cases}$$

Tada je

$$\begin{aligned} v_\alpha(F') &= v_\alpha(q_1^{k_1}) \Leftrightarrow \cdots \Leftrightarrow v_\alpha(q_{i-1}^{k_{i-1}}) \Leftrightarrow v_\alpha(q_i^{k_i}) \Leftrightarrow v_\alpha(q_{i+1}^{k_{i+1}}) \Leftrightarrow \cdots \Leftrightarrow v_\alpha(q_n^{k_n}) \\ &= \top \Leftrightarrow \cdots \Leftrightarrow \top \Leftrightarrow \alpha(q_i) \Leftrightarrow \top \Leftrightarrow \cdots \Leftrightarrow \top \\ &= \alpha(q_i) = \perp. \end{aligned}$$

Dakle F' nije tačna za valuaciju α, pa nije ni tautologija. Prema tome, F' je tautologija akko se svaka od promenljivih javlja paran broj puta. Formula F joj je ekvivalentna i svaka od promenljivih se javlja u F i F' isti broj puta, pa je i F tautologija akko se svaka od promenljivih u F javlja paran broj puta. ∎

1.6 Kanonske forme

Videli smo da svakoj iskaznoj formuli $F(q_1, \ldots, q_n)$ interpretacija dodeljuje funkciju $\bar{F}(x_1, \ldots, x_n)$ koja predstavlja n-arnu operaciju iskazne algebre. Pokazaćemo da važi i obrnuto: za svaku funkciju $f : \{\top, \perp\}^n \to \{\top, \perp\}$ postoji iskazna formula F tako da je $\bar{F} = f$. Funkcija f se naziva *istinitosna funkcija*.

Definicija 1.26 Neka je p iskazno slovo, a $\alpha \in \{\top, \perp\}$. Tada je p^α definisano sa

$$\begin{aligned} p^\top &= p \\ p^\perp &= \neg p. \end{aligned}$$

Tvrđenje 1.27 *Neka je $f : \{\top, \perp\}^n \to \{\top, \perp\}$ istinitosna funkcija iskazne algebre. Tada*

$$f(x_1, \ldots, x_n) = \bigvee_{(\alpha_1, \ldots, \alpha_n) \in \{\top, \perp\}^n} (f(\alpha_1, \ldots, \alpha_n) \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}).$$

Dokaz. Neka je $(\beta_1, \ldots, \beta_n) \in \{\top, \bot\}^n$ proizvoljna n-torka vrednosti iz $\{\top, \bot\}$. Tada $\beta_i^{\alpha_i} = \top$ akko $\beta_i = \alpha_i$, pa je

$$\beta_1^{\alpha_1} \wedge \cdots \wedge \beta_n^{\alpha_n} = \begin{cases} \top, & \alpha_1 = \beta_1, \cdots, \alpha_n = \beta_n; \\ \bot, & \text{inače.} \end{cases}$$

Otud

$$\begin{aligned} & \bigvee_{(\alpha_1,\ldots,\alpha_n)\in\{\top,\bot\}^n} (f(\alpha_1, \ldots, \alpha_n) \wedge \beta_1^{\alpha_1} \wedge \cdots \wedge \beta_n^{\alpha_n}) \\ & = \bot \vee \cdots \vee \bot \vee f(\beta_1, \ldots, \beta_n) \vee \bot \cdots \vee \bot \\ & = f(\beta_1, \ldots, \beta_n). \end{aligned}$$

■

Formula koju smo pridružili istinitosnoj funkciji u prethodnom tvrđenju sadrži i znake $\top$ i $\bot$. Odgovarajuću formulu koja ne sadrži $\top$ i $\bot$ dobijamo na sledeći način. Ukoliko funkcija f uvek uzima vrednost $\bot$ tada joj pridružimo formulu $p \wedge \neg p$ za proizvoljno iskazno slovo p. Neka je sada funkcija f takva da bar za jednu uređenu n-torku $(\beta_1, \ldots, \beta_n)$ uzima vrednost $\top$. Prema prethodnom tvrđenju je:

$$f(x_1, \ldots, x_n) = \bigvee_{(\alpha_1,\ldots,\alpha_n)\in\{\top,\bot\}^n} (f(\alpha_1, \ldots, \alpha_n) \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}).$$

Pošto je $\bot \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n} = \bot$, i kako $\bot \vee y = y$ za svako y, vrednost izraza sa desne strane se neće promeniti ukoliko uklonimo sve članove za koje je $f(\alpha_1, \ldots, \alpha_n) = \bot$. Ako je pak $f(\alpha_1, \ldots, \alpha_n) = \top$, tada umesto $\top \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}$ možemo staviti samo $x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}$. Zato je

$$f(x_1, \ldots, x_n) = \bigvee_{f(\alpha_1,\ldots,\alpha_n)=\top} (x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}).$$

Za poslednju formulu kažemo da se nalazi u *disjunktivnoj kanonskoj formi.*

Svaku formulu možemo predstaviti i u konjunktivnoj kanonskoj formi, na sledeći način. Neka je f proizvoljna n-arna istinitosna funkcija. Ako f uvek uzima vrednost $\top$, tada je možemo predstaviti formulom $p \vee \neg p$. Pretpostavimo da f uzima vrednost $\bot$ bar za jednu n-torku $(\beta_1, \ldots, \beta_n)$. Tada je i $f'(x_1, \ldots, x_n) = \neg f(x_1, \ldots, x_n)$ n-arna istinitosna funkcija koja bar za tu istu n-torku uzima vrednost $\top$. Stoga prema tvrđenju 1.27 važi

$$\neg f(x_1, \ldots, x_n) = \bigvee_{(\alpha_1,\ldots,\alpha_n)\in\{\top,\bot\}^n} (\neg f(\alpha_1, \ldots, \alpha_n) \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}).$$

Ukoliko primenimo negaciju na obe strane formule dobijamo:

$$f(x_1, \ldots, x_n) \quad = \bigwedge_{(\alpha_1,\ldots,\alpha_n)\in\{\top,\bot\}^n} \neg(\neg f(\alpha_1, \ldots, \alpha_n) \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n})$$

$$= \bigwedge_{(\alpha_1,\dots,\alpha_n)\in\{\top,\bot\}^n} (f(\alpha_1,\dots,\alpha_n) \vee \neg x_1^{\alpha_1} \vee \cdots \vee \neg x_n^{\alpha_n})$$

$$= \bigwedge_{f(\alpha_1,\dots,\alpha_n)=\bot} (x_1^{\neg\alpha_1} \vee \cdots \vee x_n^{\neg\alpha_n}).$$

Za poslednju formulu kažemo da je u *konjunktivnoj kanonskoj formi*.

Zadatak 1.28 Odrediti sve do na ekvivalenciju iskazne formule A koje sadrže promenljive p i q i ne sadrže druge promenljive, a za koje važi

$$\models p \wedge q \Leftrightarrow p \wedge A.$$

Rešenje. Uslov $\models p \wedge q \Leftrightarrow (p \wedge A)$ važi akko za svaku valuaciju α važi

$$v_\alpha(p \wedge q \Leftrightarrow p \wedge A) = \top$$

što je ekvivalentno sa

$$\alpha(p) \wedge \alpha(q) \Leftrightarrow \alpha(p) \wedge v_\alpha(A) = \top.$$

Za $\alpha(p) = \top$ ovaj uslov se svodi na

$$\alpha(q) \Leftrightarrow v_\alpha(A) = \top,$$

a on je ekvivalentan sa uslovom $v_\alpha(A) = \alpha(q)$. Za $\alpha(p) = \bot$ uslov se svodi na

$$\bot \Leftrightarrow \bot$$

koji trivijalno važi. Prema tome, formula A zadovoljava uslove zadatka akko važi $v_\alpha(A) = \alpha(q)$ za svaku valuaciju za koju je $\alpha(p) = \top$. Istinitosna tablica formule A stoga izgleda ovako.

p	q	A
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	x
$\bot$	$\bot$	y

Pri tome su x i y proizvoljni elementi skupa $\{\top, \bot\}$. Za različite vrednosti x i y dobijamo 4 istinitosne funkcije. Njima odgovaraju 4 neekvivalentne formule:

x	y	A
$\top$	$\top$	$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$
$\top$	$\bot$	$(p \wedge q) \vee (\neg p \wedge q)$
$\bot$	$\top$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
$\bot$	$\bot$	$p \wedge q$

Kako se svakoj formuli A koja zadovoljava uslov zadatka može pridružiti istinitosna funkcija ovakvog oblika, zaključujemo da su to sve do na ekvivalenciju iskazne formule koje zadovoljavaju traženi uslov. ■

Zadatak 1.29 Neka je $A(p_1, \ldots, p_n; \neg, \wedge, \vee)$ iskazna formula čije su sve promenljive među promenljivim $p_1, \ldots, p_n$, a od logičkih veznika sadrži samo $\neg$, $\wedge$ i $\vee$. Neka je $A^* = A(\neg p_1, \ldots, \neg p_n; \neg, \vee, \wedge)$ formula dobijena od formule A tako što su promenljive $p_1, \ldots, p_n$ zamenjene redom formulama $\neg p_1, \ldots, \neg p_n$, a logičkim veznicima $\wedge$ i $\vee$ su međusobno zamenjena mesta. Dokazati da je tada $A^* \Leftrightarrow \neg A$ tautologija.

Rešenje. Formula $A^* \Leftrightarrow \neg A$ je tautologija akko za svaku valuaciju α važi $v_\alpha(A^*) = \neg v_\alpha(A)$. Neka je α proizvoljna valuacija. Pokazaćemo da za svaku formulu A tada važi

$$v_\alpha(A^*) = \neg v_\alpha(A).$$

Tvrđenje dokazujemo indukcijom po broju n logičkih veznika u formuli A.

Za $n = 0$ formula A je oblika p_i za $1 \leq i \leq n$. Tada je A^* oblika $\neg p_i$, pa je direktno po definiciji interpretacije $v_\alpha(\neg p_i) = \neg v_\alpha(p_i)$.

Pretpostavimo da tvrđenje važi za sve formule sa manje od n logičkih veznika. Neka je A proizvoljna formula sa n logičkih veznika. Razlikujemo 3 slučaja.

1. A je $\neg B$ gde je B formula koja ima manje od n logičkih veznika. Tada je A^* oblika $\neg B^*$. Prema induktivnoj hipotezi važi $v_\alpha(B^*) = \neg v_\alpha(B)$, pa $\neg v_\alpha(B^*) = \neg v_\alpha(\neg B)$, što je ekvivalentno sa $v_\alpha(\neg B^*) = v_\alpha(\neg\neg B)$ tj. $v_\alpha(A^*) = v_\alpha(\neg A)$.
2. A je $B \wedge C$ gde su B i C formule koje imaju manje od n logičkih veznika. Tada je A^* oblika $B^* \vee C^*$. Za B i C važi induktivna hipoteza, pa je $v_\alpha(B^*) = \neg v_\alpha(B)$ i $v_\alpha(C^*) = \neg v_\alpha(C)$. Tada prema De Morganovom zakonu dobijamo
$$\begin{aligned} v_\alpha(A^*) &= v_\alpha(B^* \vee C^*) \\ &= v_\alpha(B^*) \vee v_\alpha(C^*) \\ &= \neg v_\alpha(B) \vee \neg v_\alpha(C) \\ &= \neg(v_\alpha(B) \wedge v_\alpha(C)) \\ &= \neg v_\alpha(B \wedge C) \\ &= \neg v_\alpha(A). \end{aligned}$$
3. A je $B \vee C$ gde su B i C formule koje imaju manje od n logičkih veznika. Tada analogno prethodnom slučaju, A^* je $B^* \wedge C^*$. Za B i C važi induktivna hipoteza, pa je $v_\alpha(B^*) = \neg v_\alpha(B)$ i $v_\alpha(C^*) = \neg v_\alpha(C)$. Ponovo prema De Morganovom zakonu dobijamo
$$\begin{aligned} v_\alpha(A^*) &= v_\alpha(B^* \wedge C^*) \\ &= v_\alpha(B^*) \wedge v_\alpha(C^*) \\ &= \neg v_\alpha(B) \wedge \neg v_\alpha(C) \\ &= \neg(v_\alpha(B) \vee v_\alpha(C)) \\ &= \neg v_\alpha(B \vee C) \\ &= \neg v_\alpha(A). \end{aligned}$$

   Time je indukcijski korak završen.

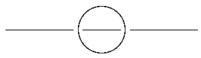
■

1.7 Interpretacije iskaznih formula

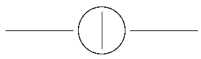
Iskazna algebra Interpretacija iskaznih formula u iskaznoj algebri (definicija 1.8) predstavlja interpretaciju koju ćemo mi najčešće koristiti.

Prekidačka kola U ovoj interpretaciji iskazna slova predstavljamo prekidačima u električnom kolu, a iskazne veznike međusobnim rasporedom prekidača u kolu.

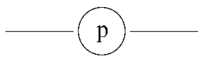
Konstanti $\top$ pridružićemo otvoreni prekidač



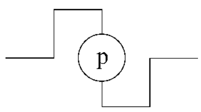
a konstanti $\perp$ prekidač



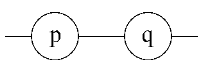
Pri tome pretpostavljamo da horizontalni položaj prekidača omogućava prolaz samo u horizontalnom, a vertikalni samo u vertikalnom smeru. Iskaznom slovu p pridružićemo prekidač



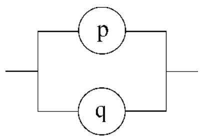
formuli $\neg p$ prekidač



formuli $p \wedge q$ prekidač

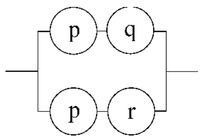


a formuli $p \vee q$ prekidač



Sada se mogu napraviti sheme i za složene iskazna formule.

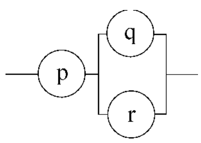
Primer 1.30 Za formulu $(p \wedge q) \vee (p \wedge r)$ odgovarajuća shema (predikačko kolo) je



$\triangle$

U osnovi prvih digitalnih računara su navedena prekidačka kola. Jedan od osnovnih problema izgradnje velikih računskih mašina je takozvani *problem minimizacije*: kako sa što manje upotrebljenih elemenata postići traženi efekat.

Primer 1.31 Za formulu $p \wedge (q \vee r)$ odgovarajuće prekidačko kolo je dato na sledećoj slici.



No, navedena formula je ekvivalentna formuli $(p \wedge q) \vee (p \wedge r)$ čije smo prekidačko kolo konstruisali u primeru 1.30. To znači da prekidačko kolo iz ovog primera predstavlja i formulu $(p \wedge q) \vee (p \wedge r)$ i to sa tri prekidača, za razliku od prethodnog kola u kojem je bilo potrebno 4 prekidača. $\triangle$

Zadatak 1.32 Odrediti prekidačko kolo sa dva prekidača p i q tako da bude otvoreno kada je jedan prekidač otvoren, a drugi zatvoren, a zatvoreno u ostalim slučajevima.

Rešenje. Prvo ćemo sastaviti tablicu odgovarajuće operacije iskazne algebre.

p	q	$f(p,q)$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

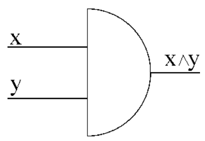
Na osnovu tablice dobijamo iskaznu formulu u disjunktivnoj normalnoj formi

$$(p \wedge \neg q) \vee (\neg p \wedge q),$$

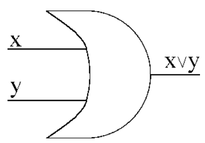
koja se označava sa $p \veebar q$ ili $p \oplus q$ i naziva *isključna disjunkcija*. Ona određuje traženo prekidačko kolo. ∎

Logička kola U konstrukciji digitalnih računara osnovnu ulogu igraju elementi koji se nazivaju *logički sklopovi*. Logički sklopovi imaju jedan ili više ulaza, a preko svojih izlaza realizuju logičke funkcije kao što su $\wedge$, $\vee$ i $\neg$. Ulazi i izlazi se mogu nalaziti u dva stanja, označena obično sa 0 i 1. Njima odgovaraju istinitosne vrednosti $\top$ i $\bot$. Za date vrednosti ulaza logičko kolo daje izlaz koji je u skladu sa logičkom funkcijom koju predstavlja. Primetimo da sada konkretnim objektima interpretiramo same operacije, dok smo kod prekidačkih kola iskazna slova interpretirali kao prekidače. Razlikujemo sledeća tri osnovna sklopa.

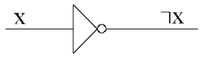
I-sklop je element sa dva ulaza x i y koji na izlazu daje vrednost $x \wedge y$.



ILI-sklop je element sa dva ulaza x i y koji na izlazu daje vrednost $x \vee y$.

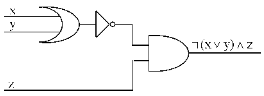


NE-sklop je element sa jednim ulazom x koji na izlazu daje vrednost $\neg x$.



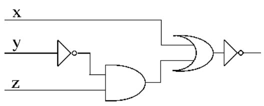
Logičko kolo povezuje konačan broj sklopova. Može imati veći broj ulaza i izlaza.

Primer 1.33 Logičko kolo sa tri ulaza na sledećoj slici realizuje funkciju $\neg(x \vee y) \wedge z$.



△

Primer 1.34 Logičko kolo koje realizuje $\neg(x \vee (\neg y \wedge z))$ prikazano je na sledećoj slici.



△

Prirodne brojeve možemo prikazati u binarnom brojevnom sistemu. Broj $n \in N_0$ tako na jedinstven način možemo prikazati u obliku

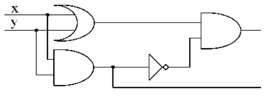
$$a_k a_{k-1} \ldots a_1 a_0$$

gde $a_i \in \{0, 1\}$ za $1 \leq i \leq k$, $a_k \neq 0$ i važi

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0.$$

Tako broj $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ prikazujemo u obliku 1101_2 (donji indeks 2 označava da se radi o binarnom zapisu broja).

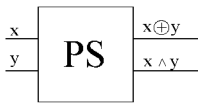
Sledeće logičko kolo realizuje sabiranje dve binarne cifre sa prenosom. Naziva se *polusabirač*.



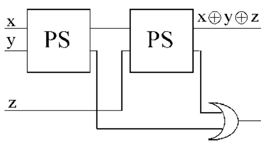
Ponašanje polusabirača je opisano sledećom tabelom. Prvi izlaz daje zbir ulaza x i y po modulu 2, a to je $x \oplus y$ (što se realizuje sa $(x \vee y) \wedge \neg(x \wedge y)$), a drugi izlaz daje konjukciju ulaza $x \wedge y$.

x	y	Izlaz 2	Izlaz 1
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Ceo polusabirač skraćeno obeležavamo kao na slici.



Kada se dva polusabirača povežu kao što je označeno na sledećoj shemi, dobija se *sabirač*.



Sabirač sabira stanja na ulazu x i y, uzimajući u obzir i prenos z. Izlaz sabirača je zbir $x \oplus y \oplus z$ i ukupni prenos prilikom sabiranja. Kada se na odgovarajući način poveže n sabirača dobija se element koji sabira prirodne brojeve iz opsega od 0 do $2^n - 1$ predstavljene u binarnom zapisu.

1.8 Baze iskazne algebre

Tvrđenje 1.35 *Svaka operacija iskazne algebre se može prikazati formulom koja sadrži kao operacijska slova samo jedan od sledeća tri para logičkih operacija:*

$$\begin{array}{ll} 1. & \vee, \quad \neg; \\ 2. & \wedge, \quad \neg; \\ 3. & \Rightarrow, \quad \neg. \end{array}$$

Dokaz. Na osnovu tvrđenja 1.27, svaka operacija iskazne algebre se može predstaviti pomoću logičkih operacija $\wedge$, $\vee$ i $\neg$.

1. Pošto je $p \wedge q = \neg(\neg p \vee \neg q)$, znači da konjunkciju možemo izraziti preko $\vee, \neg$ pa se pomoću ove dve operacije može izraziti svaka operacija iskazne algebre.
2. Analogno prethodnom slučaju, $p \vee q = \neg(\neg p \wedge \neg q)$ pa su i $\wedge, \neg$ dovoljni da se izrazi svaka operacija iskazne algebre.
3. Kako je $p \vee q = \neg p \Rightarrow q$, tvrđenje sledi iz prethodnog slučaja.

■

Definicija 1.36 *Baza iskazne algebre* je minimalni skup operacija iskazne algebre pomoću kojih se mogu izraziti sve ostale operacije iskazne algebre.

Definicija 1.37 *Baza iskaznog računa* je minimalni skup logičkih veznika takav da je svaka formula iskaznog računa ekvivalentna nekoj formuli koja sadrži samo logičke veznike tog skupa.

Ako je skup S, čiji su članovi logičke operacije, baza iskazne algebre, tada za svaku operaciju iskazne algebre f postoji formula F koja sadrži samo logičke veznike koji odgovaraju operacijama iz skupa S, takva da je $f = \bar{F}$ tj. f predstavlja interpretaciju formule F u iskaznoj algebri. Minimalnost skupa S se ogleda u tome da ni za jedno $o \in S$ skup $S \setminus \{o\}$ nije baza iskazne algebre.

Primer 1.38 Skup $\{\neg\}$ nije baza, jer su sve formule koja od logičkih veznika sadrže samo $\neg$ oblika $\neg\neg\cdots\neg p$ za neko iskazno slovo p, a interpretacija tih formula nikada ne može biti npr. funkcija koja uzima vrednost $\top$ za sve vrednosti argumenata. Sa druge strane, skupovi $\{\wedge, \neg\}$, $\{\vee, \neg\}$ i $\{\Rightarrow, \neg\}$ jesu baze, jer se na osnovu tvrđenja 1.35, pomoću njih mogu iskazati sve operacije, a lako se proverava da ni jedan od skupova $\{\wedge\}, \{\vee\}, \{\Rightarrow\}, \{\neg\}$ nije dovoljan da se izraze sve operacije iskazne algebre. $\triangle$

Zadatak 1.39 Pokazati da skup $\{\wedge, \vee\}$ nije baza iskaznog računa.

Rešenje. Primetimo da važi $\top \wedge \top = \top$ kao i $\top \vee \top = \top$. Neka je α valuacija takva da je $\alpha(p) = \top$ za svaku promenljivu p. Pokazaćemo da za svaku formulu F koja od logičkih veznika sadrži samo $\wedge$ i $\vee$ važi $v_\alpha(F) = \top$.

Dokaz sprovodimo indukcijom po broju n logičkih veznika u formuli F. Ako je $n = 0$ tada je formula F oblika p gde je p iskazno slovo. Kako je $\alpha(p) = \top$, sledi $v_\alpha(F) = \top$. Pretpostavimo da tvrđenje važi za sve iskazne formule sa manje od n logičkih veznika i neka je F proizvoljna iskazna formula koja od logičkih veznika sadrži samo $\wedge$ i $\vee$. Razlikujemo dva slučaja.

1. F je $G \wedge H$ gde G i H sadrže manje od n veznika $\wedge$ i $\vee$, pa za njih važi induktivna hipoteza. Zato je $v_\alpha(G) = \top$ i $v_\alpha(H) = \top$. Odatle sledi
$$v_\alpha(F) = v_\alpha(G \wedge H) = v_\alpha(G) \wedge v_\alpha(H) = \top \wedge \top = \top.$$

2. F je $G \vee H$. Tada, analogno prethodnom slučaju, za G i H važi induktivna hipoteza, pa je $v_\alpha(G) = v_\alpha(H) = \top$, odakle sledi
$$v_\alpha(F) = v_\alpha(G \vee H) = v_\alpha(G) \vee v_\alpha(H) = \top \vee \top = \top.$$

Prema tome, sve formule F u kojima učestvuju samo veznici $\wedge$ i $\vee$ imaju osobinu da je $v_\alpha(F) = \top$ za valuaciju za koju je $\alpha(p) = \top$ za sve p. Kako npr. za formulu $\neg p$ važi $v_\alpha(\neg p) = \bot$, sledi da se $\neg p$ ne može prikazati formulama u kojima učestvuju samo $\wedge$ i $\vee$. Prema tome, $\{\wedge, \vee\}$ nije baza. ∎

Zadatak 1.40 Ako je operacija $*$ definisana sa $x * y = \bot$ za sve $x, y \in \{\top, \bot\}$, dokazati:

a) $\{\Rightarrow, *\}$ jeste baza iskazne algebre;

b) $\{\wedge, *\}$ nije baza iskazne algebre.

Rešenje.

a) Kako je
$$\begin{array}{rcl} \neg x & = & x \Rightarrow (x * x) \\ x \vee y & = & (x \Rightarrow y) \Rightarrow y, \end{array}$$
a skup $\{\neg, \vee\}$ je baza, sledi da je i $\{\Rightarrow, *\}$ baza.

b) Pokazaćemo prvo sledeću lemu.

Lema 1.41 *Svaki izraz $A(\bot, \wedge, *)$ izgradjen od operacija $\wedge$ i $*$ i konstante $\bot$ ima vrednost $\bot$.*

Dokaz. Indukcijom po broju n znakova $\wedge$ i $*$. Za $n = 0$ izraz A je konstanta $\perp$. Pretpostavimo da tvrđenja važi za sve izraze sastavljene od manje od n znakova $\wedge$ i $*$, gde je $n > 0$. Neka je A izraz sastavljen od n znakova $\wedge$ i $*$. Tada je A oblika $B \wedge C$ ili $B * C$. Izrazi B i C imaju manje od n znakova $\wedge$ i $*$, pa je njihova vrednost $\perp$. Odatle po definiciji operacija $\wedge$ i $*$ sledi da je vrednost A takođe $\perp$. ■

Sada možemo dokazati tvrđenje zadatka. Pretpostavimo suprotno, da je skup $\{\wedge, *\}$ baza. Tada se operacija $\neg$ može predstaviti izrazom koji sadrži promenljive i znake $\wedge$ i $*$. Tada se vrednost $\neg\perp$ je može predstaviti izrazom koji sadrži konstante $\perp$ i operacije $*$ i $\neg$, pa je po prethodnoj lemi $\neg\perp = \perp$, što je kontradikcija. Dakle $\{\wedge, *\}$ nije baza.

■

Tvrđenje 1.42 *Jedine binarne operacije skupa $\{\top, \perp\}$ pomoću kojih se mogu izraziti sve ostale operacije su $\uparrow$ i $\downarrow$.*

Dokaz. Dokazaćemo prvo da su $\{\uparrow\}$ i $\{\downarrow\}$ baze iskazne algebre. Na osnovu definicije, za $\uparrow$ važi

$$\begin{aligned} p \uparrow p &= \neg(p \wedge p) = \neg p \\ (p \uparrow q) \uparrow (p \uparrow q) &= \neg(p \uparrow q) = \neg\neg(p \wedge q) = p \wedge q \end{aligned}$$

a kako je prema tvrđenju 1.35 skup $\{\wedge, \neg\}$ baza, sledi da je i $\{\uparrow\}$ baza. Analogno, iz

$$\begin{aligned} p \downarrow p &= \neg(p \vee p) = \neg p \\ (p \downarrow q) \downarrow (p \downarrow q) &= \neg(p \downarrow q) = \neg\neg(p \vee q) = p \vee q \end{aligned}$$

i kako je prema tvrđenju 1.35 skup $\{\vee, \neg\}$ baza, sledi da je i $\{\downarrow\}$ baza.

Preostaje da pokažemo da su $\downarrow$ i $\uparrow$ jedine operacije koje čine jednoelementnu bazu. Neka je $h(p, q)$ binarna operacija pomoću koje se mogu prikazati sve ostale. Tada mora biti $h(\top, \top) = \perp$. Ukoliko bi, naime, bilo $h(\top, \top) = \top$, tada bi za svaku funkciju f koja se može predstaviti korišćenjem samo operacije h važilo $f(\top, \top, \ldots \top) = \top$. (Tako na primer za $f(p, q) = h(h(p, q), q)$ važi $f(\top, \top) = h(h(\top, \top), \top) = h(\top, \top) = \top$.) Kako postoje operacije koje za vrednosti iskaznih promenljivih $\top, \top, \ldots, \top$ uzimaju vrednost $\perp$ (takva je na primer $\neg$), mora biti $h(\top, \top) = \perp$.

Analogno zaključujemo $h(\perp, \perp) = \top$. Zato je operacija h određena vrednostima $h(\top, \perp)$ i $h(\perp, \top)$, pa postoje 4 mogućnosti. Operacije koje predstavlja h u svim slučajevima date su u tabeli.

$h(\top, \perp)$	$h(\perp, \top)$	h
$\top$	$\top$	$\uparrow$
$\perp$	$\perp$	$\downarrow$
$\top$	$\perp$	$\neg q$
$\perp$	$\top$	$\neg p$

U poslednja dva slučaja h predstavlja negaciju, pa se tada sa h ne mogu izraziti sve operacije. Dakle $\uparrow$ i $\downarrow$ su jedine mogućnosti. ■

Napomena 1.43 Mogu se posmatrati i operacije veće arnosti (npr. ternarne) sa stanovišta baza iskazne algebre, kao i baze u viševrednosnoj logici (videti [SJ]). ◇

1.9 Tvrđenje kompaktnosti za iskazni račun

Definicija 1.44 Valuacija α je model za formulu A akko je $v_\alpha(A) = \top$. Valuacija α je model za skup formula $\mathcal{F}$ akko za svako $A \in \mathcal{F}$ važi $v_\alpha(A) = \top$.

Tvrđenje 1.45 (Tvrđenje kompaktnosti za iskazni račun) *Ako svaki konačan podskup skupa iskaznih formula $\mathcal{F}$ ima model, onda i $\mathcal{F}$ ima model.*

Dokaz. Neka svaki konačan podskup skupa $\mathcal{F}$ ima model. Dokazaćemo da je model za ceo skup $\mathcal{F}$ valuacija i definisana na sledeći način:

$$i(p_1) = \begin{cases} \top, & \text{ako za svaki konačan podskup skupa } \mathcal{F} \text{ postoji neki model } j \\ & \text{tako da } j(p_1) = \top; \\ \bot, & \text{inače;} \end{cases}$$

$$i(p_{n+1}) = \begin{cases} \top, & \text{ako za svaki konačan podskup skupa } \mathcal{F} \text{ postoji neki model } j \\ & \text{tako da } j(p_1) = i(p_1), \dots, j(p_n) = i(p_n), j(p_{n+1}) = \top; \\ \bot, & \text{inače.} \end{cases}$$

Dakle, $i(p_{n+1})$ se definiše pomoću vrednosti $i(p_1), \dots, i(p_n)$. Kako je zadata vrednost $i(p_1)$, i je dobro definisano. Indukcijom po n pokazaćemo sledeću lemu.

Lema 1.46 *Za svako $n \in N$ važi da svaki konačan podskup skupa $\mathcal{F}$ ima neki model j za koji važi $j(p_1) = i(p_1), \dots, j(p_n) = i(p_n)$.*

Dokaz. Neka je $n = 1$. Ako je $i(p_1) = \top$, tada po definiciji valuacije i tvrđenje važi. Neka je $i(p_1) = \bot$. Pošto nije $i(p_1) = \top$, postoji konačan podskup A koji nema modele j za koje važi $j(p_1) = \top$. Dokazaćemo da tada svaki konačan podskup skupa $\mathcal{F}$ ima neki model j za koji važi $j(p_1) = \bot$. Pretpostavimo suprotno: da neki konačan podskup B nema modele za koje je $j(p_1) = i(p_1) = \bot$. Posmatrajmo skup $A \cup B$. On je takođe konačan podskup skupa $\mathcal{F}$, pa po pretpostavci tvrđenja ima model m. Taj model je istovremeno i model za A i B. Pri tome $m(p_1) \in \{\top, \bot\}$.

1. Ako je $m(p_1) = \top$, tada A ima model m za koji je $m(p_1) = \top$, što je kontradikcija;
2. Ako je $m(p_1) = \bot$, tada B ima model m za koji je $m(p_1) = \bot$, što je kontradikcija.

Dakle u oba slučaja dolazimo do kontradikcije. Zato je pretpostavka da postoji konačan podskup B koji nema modele za koje je $j(p_1) = \bot$ pogrešna, pa svaki konačan podskup ima model m za koji je $m(p_1) = \bot$. Dakle i za $i(p_1) = \bot$ tvrđenje važi.

Pretpostavimo sada da tvrđenje važi za n: Svaki konačan podskup skupa $\mathcal{F}$ ima neki model j tako da

$$\begin{array}{rcl} j(p_1) & = & i(p_1); \\ j(p_2) & = & i(p_2); \\ & \vdots & \\ j(p_n) & = & i(p_n). \end{array} \qquad (*)$$

Dokazujemo da tvrđenje važi za $n+1$ (postupićemo slično kao za $n = 1$). Ako je $i(p_{n+1}) = \top$, tada po definiciji valuacije i tvrđenje važi i za $n+1$. Neka je $i(p_{n+1}) = \bot$. Tada postoji konačan podskup A koji nema ni jedan model j za koji važi $(*)$ i $j(p_{n+1}) = \top$, jer bi u suprotnom bilo $i(p_{n+1}) = \top$. Dokazaćemo da tada svaki konačan podskup ima model j za koji važi $(*)$ i $j(p_{n+1}) = \bot$. Pretpostavimo suprotno: da neki konačan podskup B nema model za koji važi $(*)$ i $j(p_{n+1}) = \bot$. Tada je $A \cup B$ konačan podskup, pa po induktivnoj hipotezi postoji model m tako da važi $(*)$. m je model i za A i za B jer su to podskupovi skupa $A \cup B$. Mora biti $m(p_{n+1}) = \top$ ili $m(p_{n+1}) = \bot$.

1. Ako je $m(p_{n+1}) = \top$, tada A ima model m za koji važi $(*)$ i $m(p_{n+1}) = \top$, što je kontradikcija;
2. Ako je $m(p_{n+1}) = \bot$, tada B ima model m za koji važi $(*)$ i $m(p_{n+1}) = \bot$, što je kontradikcija.

Dakle pretpostavka da neki konačan podskup B nema model za koji važi $(*)$ i $j(p_{n+1}) = \bot$ vodi u kontradikciju, pa svaki konačan podskup skupa $\mathcal{F}$ ima valuciju m za koju važi

$$\begin{array}{rl} j(p_1) & = i(p_1); \\ j(p_2) & = i(p_2); \\ & \vdots \\ j(p_n) & = i(p_n); \\ j(p_{n+1}) = & \bot \quad = i(p_{n+1}). \end{array}$$

Time je dokaz leme završen. ■

Neka je sada $\varphi \in \mathcal{F}$ proizvoljna formula. Ona ima konačan broj promenljivih, neka su to promenljive $p_{k_1}, \ldots, p_{k_n}$. Stavimo $M = \max\{k_1, \ldots, k_n\}$. Tada se sve promenljive formule φ nalaze među promenljivima $p_1, \ldots, p_M$. Pošto je $\{\varphi\}$ konačan podskup skupa $\mathcal{F}$, prema prethodnoj lemi postoji model j za $\{\varphi\}$ takav da $i(p_1) = j(p_1)$, $\ldots, i(p_M) = j(p_M)$. Valuacije i i j se poklapaju za sve vrednosti promenljivih formule φ, pa je $v_i(\varphi) = v_j(\varphi) = \top$. Dakle i je model za φ. Kako je φ bila proizvoljna formula, i je model za ceo skup $\mathcal{F}$. ■

1.10 Hipoteze i posledice. Semantički pristup

Definicija 1.47 Neka je $\mathcal{F}$ skup iskaznih formula i A proizvoljna formula. A je *semantička posledica* skupa formula $\mathcal{F}$ (čije članove nazivamo *hipoteze*), u oznaci $\mathcal{F} \models A$, akko za svaku valuaciju α važi: ako je α model za $\mathcal{F}$, onda je α model i za A.

Primer 1.48 $\{p, p \Rightarrow q, q \Rightarrow r\} \models r$. Naime, ako je α model za $\{p, p \Rightarrow q, q \Rightarrow r\}$ tada je $\alpha(p) = \top$. Takođe $v_\alpha(p \Rightarrow q) = \top$, pa i $\alpha(q) = \top$. Pošto je i $v_\alpha(q \Rightarrow r) = \top$, sledi i $\alpha(r) = \top$. $\triangle$

Primer 1.49 $\{p \vee q, p \Rightarrow q\} \models (p \wedge q) \vee (\neg p \vee q)$ jer za svaku valuaciju α koja je model za skup hipoteza važi $\alpha(q) = \top$, a onda važi i $v_\alpha((p \wedge q) \vee (\neg p \vee q)) = \top$. $\triangle$

Primer 1.50 $\{r, q\} \models p \Rightarrow q$, jer za $\alpha(q) = \top$ važi $v_\alpha(p \Rightarrow q) = \top$. $\triangle$

Primer 1.51 $\{q\} \models p \Rightarrow p$ jer važi i $\emptyset \models p \Rightarrow p$. Uočavamo da je tautologija posledica praznog skupa formula. $\triangle$

Napomena 1.52 Ako je skup $\mathcal{F} = \{A_1, \ldots, A_n\}$ konačan skup, umesto $\mathcal{F} \models A$ pišemo i $A_1, \ldots, A_n \models A$. $\diamond$

Tvrđenje 1.53 $A_1, \ldots, A_n \models A$ *akko* $\models A_1 \wedge \cdots \wedge A_n \Rightarrow A$.

Dokaz. ($\Rightarrow$): Neka je α proizvoljna valuacija. Ako je $v_\alpha(A_i) = \bot$ za neko A_i gde $i \in \{1, 2, \ldots n\}$ tada je $v_\alpha(A_1 \wedge \cdots \wedge A_n) = \bot$, pa je $v_\alpha((A_1 \wedge \cdots \wedge A_n) \Rightarrow A) = \top$. Ukoliko za sve A_i važi $v_\alpha(A_i) = \top$, tada je α model za $\{A_1, \ldots A_n\}$, pa je i $v_\alpha(A) = \top$. Zato je $v_\alpha((A_1 \wedge \ldots \wedge A_n) \Rightarrow A) = \top$. Dakle za svako α važi $v_\alpha((A_1 \wedge \cdots \wedge A_n) \Rightarrow A) = \top$, pa je formula tautologija.

($\Leftarrow$): Neka je α proizvoljna valuacija i neka za sve A_i važi $v_\alpha(A_i) = \top$. Pošto je $v_\alpha((A_1 \wedge \cdots \wedge A_n) \Rightarrow A) = \top$, sledi $(\top \Rightarrow v_\alpha(A)) = \top$, pa je $v_\alpha(A) = \top$. ∎

Tvrđenje 1.54

$$\begin{aligned}\models \quad & (A_1 \wedge \cdots \wedge A_n \Rightarrow A) \Leftrightarrow \\ & (A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_n \Rightarrow A) \cdots)))\end{aligned}$$

Dokaz. Indukcijom po n i diskusijom po $v_\alpha(A_n)$.

Za $n = 1$ formula se svodi na $(A_1 \Rightarrow A) \Leftrightarrow (A_1 \Rightarrow A)$ što je instanca tautologije $p \Leftrightarrow p$.

Pretpostavimo da važi

$$\begin{aligned}\models \quad & (A_1 \wedge \cdots \wedge A_n \Rightarrow A) \Leftrightarrow \\ & (A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_n \Rightarrow A) \cdots))).\end{aligned}$$

Treba dokazati

$$\begin{aligned}\models \quad & (A_1 \wedge \cdots \wedge A_n \wedge A_{n+1} \Rightarrow A) \Leftrightarrow \\ & (A_1 \Rightarrow (A_2 \Rightarrow (\cdots (A_n \Rightarrow (A_{n+1} \Rightarrow A)) \cdots))).\end{aligned}$$

Neka ja α proizvoljna valuacija. Razlikujemo dva slučaja.

1. $v_\alpha(A_{n+1}) = \top$. Tada se formula svodi na

   $$(A_1 \wedge \cdots \wedge A_n \wedge \top \Rightarrow A) \Leftrightarrow (A_1 \Rightarrow (A_2 \Rightarrow (\cdots (A_n \Rightarrow (\top \Rightarrow A)))$$

   odnosno

   $$(A_1 \wedge \cdots \wedge A_n \Rightarrow A) \Leftrightarrow (A_1 \Rightarrow (A_2 \Rightarrow (\cdots (A_n \Rightarrow A) \cdots))).$$

   Vrednost poslednje formule u proizvoljnoj valuaciji, pa i u α, je tačna po induktivnoj hipotezi.
2. $v_\alpha(A_{n+1}) = \bot$. Tada je $v_\alpha(A_1 \wedge \cdots \wedge A_{n+1}) = \bot$, pa $v_\alpha(A_1 \wedge \cdots \wedge A_{n+1} \Rightarrow A) = \top$. Sa druge strane,

   $$\begin{aligned} & v_\alpha(A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_n \Rightarrow (\bot \Rightarrow A)))))) = \\ & \quad = v_\alpha(A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_n \Rightarrow \top)))) \\ & \quad = v_\alpha(A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_{n-1} \Rightarrow \top)))) \\ & \quad \cdots \\ & \quad = \top. \end{aligned}$$

   Obe strane ekvivalencije su tačne, pa je i ekvivalencija tačna.

U oba slučaja vrednost formule je $\top$, pa je formula tautologija. ■

Posledica 1.55 *Jednostavna posledica prethodnih tvrđenja je sledeća:*

$$\begin{aligned} A_1, \ldots, A_n & \models A & \text{akko} \\ & \models (A_1 \Rightarrow (A_2 \Rightarrow (\cdots \Rightarrow (A_n \Rightarrow A) \cdots))) & \text{akko} \\ A_1, \ldots, A_{n-1} & \models A_n \Rightarrow A. & \end{aligned}$$

Primer 1.56

$$\begin{aligned} & \models p \Rightarrow (q \Rightarrow p) & \text{akko} \\ p, q & \models p & \text{akko} \\ q & \models p \Rightarrow p & \text{akko} \\ & \models q \Rightarrow (p \Rightarrow p). & \end{aligned}$$

△

1.11 Formalne teorije

Matematička logika nam omogućuje formalno zasnivanje matematičkih teorija. Reč je o tzv. *formalnim teorijama* kod kojih je do kraja sproveden sintaktički postupak izgrađivanja. One se grade isključivo pomoću simbola i izraza koji su od tih simbola napravljeni, bez pozivanja na "značenje" (semantiku) tih izraza. Svrha ovakvog načina konstruisanja matematičkih teorija je u "čišćenju" teorije od svih primesa jezika koje mogu uneti neodređenost i dvosmislenost, kao i izbegavanju raznih paradoksa.

Definicija 1.57 Formalna teorija je uređena četvorka

$$F_t = (\mathcal{S}, \mathit{For}, \mathit{Ax}, P)$$

gde je

- $\mathcal{S}$ skup osnovnih simbola (azbuka) koji je najviše prebrojiv (videti 3.4.3). Reči su konačni nizovi simbola iz $\mathcal{S}$. Skup svih reči se označava sa $\mathcal{S}^*$.
- *For* $\subseteq \mathcal{S}^*$ skup formula. Dat je efektivan postupak kojim se može utvrditi da li data reč pripada *For* ili ne.
- $\mathit{Ax} \subseteq \mathit{For}$ skup aksioma. Ako je dat efektivan postupak za odlučivanje da li je neka formula aksioma ili ne, kažemo da je teorija *aksiomatska*.
- P konačan skup pravila izvođenja. Svako pravilo izvođenja α je shema oblika

$$\alpha : \frac{A_1, \ldots, A_n}{A}$$

gde $A_1, \ldots, A_n, A$ označavaju formule iz *For*. Kažemo da je A dobijena primenom pravila izvođenja α na formule $A_1, \ldots, A_n$. Pravilo α je relacija arnosti $(n+1)$ na skupu *For*.

Definicija 1.58 Konačan niz formula $B_1, \ldots, B_n$ je izvođenje (dokaz) u formalnoj teoriji F_t akko za svaku formulu B_i, $1 \leq i \leq n$ važi

1. B_i je aksioma, ili
2. B_i se može dobiti iz prethodnih formula niza $B_1, \ldots, B_{i-1}$ primenom nekog od pravila izvođenja iz P.

Formula B je teorema formalne teorije F_t, u oznaci $\vdash_{F_t} B$ akko postoji dokaz $B_1, \ldots, B_{n-1}, B$ u formalnoj teoriji F_t. Skup svih teorema formalne teorije F_t označavamo sa $Th(F_t)$.

Ako je iz konteksta jasno o kojoj se formalnoj teoriji radi, umesto $\vdash_{F_t} B$ pišemo samo $\vdash B$.

Definicija 1.59 Formalna teorija F_t je *odlučiva* akko postoji efektivan postupak kojim se za proizvoljnu formulu može utvrditi da li je teorema formalne teorije F_t (pojam efektivnog postupka ovde nećemo strogo uvoditi).

Definicija 1.60 Neka je $\mathcal{F} \subseteq$ *For* proizvoljan skup formula formalne teorije F_t i neka $A \in$ *For*. A je sintaksna posledica skupa formula $\mathcal{F}$, u oznaci $\mathcal{F} \vdash_{F_t} A$ akko postoji konačan niz $B_1, \ldots, B_n$ formula iz *For* tako da je B_n formula A i za svako B_i, $1 \leq i \leq n$ važi

1. $B_i \in Ax$ ili
2. $B_i \in \mathcal{F}$ ili
3. B_i se može dobiti od prethodnih članova u nizu primenom nekog od pravila izvođenja iz F_t.

Taj konačan niz formula nazivamo izvođenje formule A iz skupa hipoteza $\mathcal{F}$. U nizu formula koji predstavljaju dokaz sa *Ax* označavamo da je formula aksioma, sa *Hyp* da je hipoteza, a sa $\alpha(i_1, \ldots, i_k)$ da je dobijena primenom pravila izvođenja α redom na članove niza sa indeksima $i_1, \ldots, i_k$.

Definicija 1.61 Ako je A proizvoljna azbuka, tada sa a^n označavamo reč $\underbrace{a \ldots a}_{n}$ iz skupa A^*.

Primer 1.62 Neka je data formalna teorija $F_t = (\mathcal{S}, For, Ax, P)$ gde je

$$\begin{aligned} \mathcal{S} &= \{a\} \\ For &= \{a, aa, aaa, \ldots\} \\ Ax &= \{a\} \\ P &= \{\alpha\} \end{aligned}$$

a α je sledeće pravilo izvođenja:

$$\alpha : \frac{w}{waa}$$

za proizvoljnu reč w nad azbukom $\{a\}$ tj.

$$\alpha = \{\, (w, waa) \mid w \in A^* \,\}.$$

Sledeći niz formula je izvođenje formule $aaaaa$:

1.	a	Ax
2.	aaa	$\alpha(1)$
3.	$aaaaa$	$\alpha(2)$

Dokazaćemo sledeće tvrđenje o formalnoj teoriji F_t.

Tvrđenje 1.63 *Reč $w \in \mathcal{S}^*$ je teorema formalne teorije F_t akko w sadrži neparan broj simbola a.*

Dokaz. $\Rightarrow$): Dokazujemo da sve teoreme formalne teorije F_t imaju neparan broj simbola a. Pokazaćemo da za svaki prirodan broj n reč koja ima izvođenje dužine n u formalnoj teoriji F_t ima neparan broj slova a. Dokaz sprovodimo indukcijom po n.

Za $n = 1$ izvođenje se sastoji samo od jedne reči, pa ona mora biti aksioma a. Aksioma a sadrži jedno slovo a, pa tvrđenje važi za $n = 1$.

Pretpostavimo da tvrđenje važi za sve brojeve $k < n$ gde je $n > 1$. Neka formula w ima izvođenje $w_1, \ldots, w_n$ gde je w_n formula w. Tada je w aksioma ili je dobijena primenom pravila α na prethodnu formulu u nizu. Ako je w aksioma, tada je w formula a pa sadrži neparan broj slova. U suprotnom, w je dobijena od reči w_i za neko $1 \leq i \leq n-1$ primenom pravila α, te je w oblika $w_i aa$. Niz $w_1, \ldots, w_{i-1}$ predstavlja izvođenje reči w_i i dužina tog izvođenja je $i < n$. Zato prema induktivnoj hipotezi w_i sadrži neparan broj slova a. Reč w sadrži dva slova više od reči w_i, pa i w sadrži neparan broj slova a. Time je indukcijski korak završen.

$\Leftarrow$): Indukcijom dokazujemo da za svaki neparan broj $2k-1$ gde $k \in N$ postoji izvođenje reči a^{2k-1}.

Ako je $k = 1$, tada je a^{2k-1} formula a, a to je aksioma.

Pretpostavimo da reč dužine a^{2k-1} ima izvođenje $w_1, \ldots, w_n$ gde je w_n formula a^{2k-1}. Tada niz

$$w_1, \ldots, w_k, a^{2k+1}$$

predstavlja izvođenje reči a^{2k+1} jer je a^{2k+1} dobijena primenom pravila α na reč a^{2k-1} koja joj prethodi u nizu. Dakle tvrđenje važi i za $k+1$. Time je i drugi smer dokaza završen. ■ △

Meta jezik je deo "obične" matematike kojim govorimo o objekt jeziku. Prethodno tvrđenje 1.63 pripada meta jeziku, njime su okarakterisane teoreme date formalne teorije.

1.12 Iskazni račun ($\mathcal{L}$) kao formalna teorija

Definicija 1.64 Iskazni račun je formalna teorija $\mathcal{L} = (\mathcal{S}, For, Ax, P)$, gde je

$\mathcal{S}$ $= \{p_1, \ldots, p_n, \ldots, (,), \Rightarrow, \neg\}$ gde je $\{p_1, \ldots, p_n, \ldots\}$ prebrojiv skup iskaznih slova, (i) su zagrade kao pomoćni simboli, a $\Rightarrow$ i $\neg$ su logički veznici.

For je skup formula iskaznog računa (definicija 1.3) koje od logičkih veznika sadrže samo $\Rightarrow$ i $\neg$.

Ax je beskonačan skup dat pomoću sledeće tri shema-aksiome: ako su A, B i C proizvoljne formule iskaznog računa, tada su aksiome

$$\begin{array}{ll} Ax1 & A \Rightarrow (B \Rightarrow A) \\ Ax2 & (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \\ Ax3 & (\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A) \end{array}$$

Nije teško uveriti se da postoji efektivan postupak za proveru da li je data formula aksioma iskaznog računa ili ne. Zato je $\mathcal{L}$ aksiomatska teorija.

$P = \{MP\}$ gde je *MP* pravilo izvođenja *modus ponens* dato sa

$$MP : \frac{A, A \Rightarrow B}{B}$$

Da bismo definiciju formalne teorije učinili što jednostavnijom, definisali smo formule iskaznog računa na jeziku koji od logičkih veznika sadrži samo $\Rightarrow$ i $\neg$. Ostale veznike uvodimo kao skraćene zapise formula koje sadrže samo veznike $\Rightarrow$ i $\neg$:

$A \vee B$ je zamena za $\neg A \Rightarrow B$;
$A \wedge B$ je zamena za $\neg(A \Rightarrow \neg B)$;
$A \Leftrightarrow B$ je zamena za $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Tako na primer $p \vee (q \wedge r)$ predstavlja oznaku za formulu

$$\neg p \Rightarrow \neg(q \Rightarrow \neg r).$$

Lema 1.65 *Za proizvoljnu formulu A važi* $\vdash A \Rightarrow A$.

Dokaz.

1.	$A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$	$Ax1$
2.	$(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$	$Ax2$
3.	$(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$	$MP(1,2)$
4.	$A \Rightarrow (A \Rightarrow A)$	$Ax1$
5.	$A \Rightarrow A$	$MP(4,3)$

■

Tvrđenje 1.66 (Tvrđenje dedukcije za $\mathcal{L}$) *Neka je $\mathcal{F} \subseteq$ For i $A, B \in$ For. Tada $\mathcal{F}, A \vdash B$ akko $\mathcal{F} \vdash A \Rightarrow B$.*

Dokaz. $\Leftarrow$): Neka $\mathcal{F} \vdash A \Rightarrow B$. Tada postoji izvođenje $B_1, \ldots, B_n$ gde je B_n formula $A \Rightarrow B$. Posmatrajmo niz

1.	B_1	
2.	B_2	
...		
n.	$A \Rightarrow B$	
$(n+1)$.	A	*Hyp*
$(n+2)$.	B	$MP(n+1, n)$

On predstavlja izvođenje formule B iz hipoteza $\mathcal{F}, A$ jer prvih n članova predstavljaju izvođenje iz skupa $\mathcal{F}$, pa stoga i iz skupa $\mathcal{F} \cup \{A\}$, član $n+1$ je hipoteza, a formula

$n+2$ se može dobiti primenom pravila *MP* na članove n i $n+1$ koji joj prethode u nizu. Dakle postoji izvođenje formule B iz skupa $\mathcal{F} \cup \{A\}$, pa $\mathcal{F}, A \vdash B$.

$\Rightarrow$): Dokazaćemo da za svaku formulu B važi sledeće tvrđenje: ako postoji izvođenje formule B u n koraka iz hipoteza $\mathcal{F}, A$ tada postoji izvođenje formule $A \Rightarrow B$ iz hipoteza $\mathcal{F}$. Dokaz sprovodimo indukcijom po n.

Za $n = 1$ izvođenje se sastoji samo od formule B, pa ona mora biti aksioma, hipoteza iz $\mathcal{F}$ ili hipoteza A.

1. B je aksioma. Tada je sledeći niz formula izvođenje formule $A \Rightarrow B$ iz skupa $\mathcal{F}$:

1.	B	aksioma
2.	$B \Rightarrow (A \Rightarrow B)$	$Ax2$
3.	$A \Rightarrow B$	*MP*$(1, 2)$

2. B je iz $\mathcal{F}$. Tada je, slično prethodnom slučaju, sledeći niz formula izvođenje formule $A \Rightarrow B$ iz skupa $\mathcal{F}$:

1.	B	*Hyp*
2.	$B \Rightarrow (A \Rightarrow B)$	$Ax2$
3.	$A \Rightarrow B$	*MP*$(1, 2)$

3. B je A. Tada prema lemi 1.65 važi $\vdash A \Rightarrow A$, pa i $\mathcal{F} \vdash A \Rightarrow A$.

Pretpostavimo sada da za svako $k < n$, ako postoji izvođenje formule B dužine k iz $\mathcal{F}, A$, tada postoji i izvođenje formule $A \Rightarrow B$ iz $\mathcal{F}$. Neka postoji izvođenje $B_1, \dots, B_n$ gde je B_n formula B. Tada je po definiciji izvođenja B ili aksioma, ili hipoteza iz $\mathcal{F}$, ili hipoteza A, ili je dobijena primenom pravila *MP* na prethodne članove u nizu. U prva tri slučaja analogno kao u prethodnom razmatranju zaključujemo da postoji izvođenje formule $A \Rightarrow B$ iz $\mathcal{F}$. Preostaje da razmotrimo slučaj kada je B dobijena primenom pravila *MP* na prethodne formule u nizu. Tada izvođenje ima sledeći oblik:

1.	B_1	
2.	B_2	
...		
i.	B_i	
...		
j.	$B_i \Rightarrow B$	
...		
n.	B	*MP*(i, j)

(pri tome nije bitno koja se od formula B_i i $B_i \Rightarrow B$ javlja prva po redu u izvođenju). Prvih i formula čine izvođenje za B_i, a prvih j formula čine izvođenje za $B_i \Rightarrow B$. Kako je $i, j < n$, prema induktivnoj hipotezi postoje izvođenja iz skupa hipoteza $\mathcal{F}$:

$$C_1, \dots, C_p \quad \text{gde je} \quad C_p \text{ formula } A \Rightarrow B_i$$

kao i

$$D_1, \ldots, D_q \quad \text{gde je} \quad D_q \text{ formula } A \Rightarrow (B_i \Rightarrow B).$$

Posmatrajmo niz formula

1.	C_1	
2.	C_2	
...		
p.	$A \Rightarrow B_i$	
$(p+1)$.	D_1	
$(p+2)$.	D_2	
...		
r.	$A \Rightarrow (B_i \Rightarrow B)$	
$(r+1)$.	$(A \Rightarrow (B_i \Rightarrow B)) \Rightarrow ((A \Rightarrow B_i) \Rightarrow (A \Rightarrow B))$	$Ax2$
$(r+2)$.	$(A \Rightarrow B_i) \Rightarrow (A \Rightarrow B)$	*MP*$(r, r+1)$
$(r+3)$.	$A \Rightarrow B$	*MP*$(p, r+2)$

gde je $r = p + q$. Članovi od 1 do p i $p+1$ do r predstavljaju izvođenja iz $\mathcal{F}$, a u preostalim članovima smo koristili samo aksiome $\mathcal{L}$ i pravilo *MP*. Zato je posmatrani niz formula izvođenje formule $A \Rightarrow B$ iz $\mathcal{F}$.

Time smo pokazali da za svako izvođenje formule B iz $\mathcal{F}, A$ postoji izvođenje formule $A \Rightarrow B$ iz $\mathcal{F}$. Dakle $\mathcal{F}, A \vdash B$ povlači $\mathcal{F} \vdash A \Rightarrow B$. ■

Posledica 1.67 $A \vdash A$ *akko* $\vdash A \Rightarrow A$.

Lema 1.68 *Ako su A, B, C proizvoljne iskazne formule, onda*

$$A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C.$$

Dokaz. Na osnovu tvrđenja dedukcije $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$ akko $A \Rightarrow B, B \Rightarrow C, A \vdash C$, a to važi zbog

1.	$A \Rightarrow B$	*Hyp*
2.	A	*Hyp*
3.	B	*MP*$(2, 1)$
4.	$B \Rightarrow C$	*Hyp*
5.	C	*MP*$(3, 4)$.

■

Posledica 1.69 *Prema tvrđenju dedukcije i prethodnom tvrđenju važi*

$$\vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$$

$$\vdash (B \Rightarrow C) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$$

Ako izvođenje $A_1, \ldots, A_n$ sadrži formule oblika $A \Rightarrow B$ i $B \Rightarrow C$ onda lema 1.68 obezbeđuje da se takvo izvođenje može dopuniti do izvođenja koje sadrži i formulu $A \Rightarrow C$. To nam omogućava da lemu 1.68 koristimo kao meta pravilo izvođenja. Primenu ovog meta pravila redom na formule A_i i A_j označavamo sa $T(A_i, A_j)$.

Lema 1.70 *Za sve* $A, B \in$ *For važi* $A, \neg A \vdash B$.

Dokaz. Neka su A i B proizvoljne formule. Tada sledeći niz predstavlja izvođenje formule B iz formula A i $\neg A$:

1.	$\neg A$	*Hyp*
2.	A	*Hyp*
3.	$\neg A \Rightarrow (\neg B \Rightarrow \neg A)$	*Ax*1
4.	$\neg B \Rightarrow \neg A$	*MP*$(1,3)$
5.	$(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$	*Ax*3
6.	$A \Rightarrow B$	*MP*$(4,5)$
7.	B	*MP*$(2,6)$

■

Lema 1.71 *Za sve* $A, B \in$ *For važi*

1. $\vdash \neg\neg A \Rightarrow A$

2. $\vdash A \Rightarrow \neg\neg A$

3. $\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$

Dokaz. Neka su A i B proizvoljne formule.

1. Prema tvrđenju dedukcije, dovoljno je dokazati $\neg\neg A \vdash A$.

1.	$\neg\neg A$	*Hyp*
2.	$\neg\neg A \Rightarrow (\neg A \Rightarrow \neg\neg\neg A)$	posledica leme 1.70 i tvrđenja dedukcije
3.	$\neg A \Rightarrow \neg\neg\neg A$	*MP*$(1,2)$
4.	$(\neg A \Rightarrow \neg\neg\neg A) \Rightarrow (\neg\neg A \Rightarrow A)$	*Ax*3
5.	$\neg\neg A \Rightarrow A$	*MP*$(3,4)$
6.	A	*MP*$(1,5)$

2. Po tvrđenju dedukcije dovoljno je dokazati $A \vdash \neg\neg A$.

1.	A	*Hyp*
2.	$\neg\neg\neg A \Rightarrow \neg A$	prema 1. delu ove leme
3.	$(\neg\neg\neg A \Rightarrow \neg A) \Rightarrow (A \Rightarrow \neg\neg A)$	*Ax*3
4.	$A \Rightarrow \neg\neg A$	*MP*$(2,3)$
5.	$\neg\neg A$	$MP(1,4)$

3. Koristeći tvrđenje dedukcije, dokazujemo $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$.

1.	$A \Rightarrow B$	*Hyp*
2.	$(\neg\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg B \Rightarrow \neg A)$	*Ax*3
3.	$\neg\neg A \Rightarrow A$	po 1. delu ove leme
4.	$\neg\neg A \Rightarrow B$	$T(3,1)$
5.	$B \Rightarrow \neg\neg B$	po 2. delu ove leme
6.	$\neg\neg A \Rightarrow \neg\neg B$	$T(4,5)$
7.	$\neg B \Rightarrow \neg A$	$MP(6,2)$

■

Sledeća lema je direktna posledica aksiome 2 i tvrđenja dedukcije.

Lema 1.72 $A \Rightarrow (B \Rightarrow C) \vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$.

Lema 1.73 *Za sve* $A, B \in For$ *važi* $A \Rightarrow B, \neg A \Rightarrow B \vdash B$.

Dokaz. Neka su A i B proizvoljne formule.

1.	$A \Rightarrow B$	*Hyp*
2.	$\neg A \Rightarrow B$	*Hyp*
3.	$\neg B \Rightarrow \neg A$	iz 1 po lemi 1.71
4.	$\neg B \Rightarrow B$	$T(3,2)$
5.	$\neg B \Rightarrow (B \Rightarrow \neg(B \Rightarrow B))$	po lemi 1.70
6.	$(\neg B \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(B \Rightarrow B))$	iz 5 po lemi 1.72
7.	$\neg B \Rightarrow \neg(B \Rightarrow B)$	$MP(4,6)$
8.	$(\neg B \Rightarrow \neg(B \Rightarrow B)) \Rightarrow ((B \Rightarrow B) \Rightarrow B)$	*Ax*3
9.	$(B \Rightarrow B) \Rightarrow B$	$MP(7,8)$
10.	$B \Rightarrow B$	po lemi 1.65
11.	B	$MP(10,9)$

■

Lema 1.74 *Za sve* $A, B \in For$ *važi*

1. $A, B \vdash A \Rightarrow B$

2. $A, \neg B \vdash \neg(A \Rightarrow B)$

3. $\neg A, B \vdash A \Rightarrow B$

4. $\neg A, \neg B \vdash A \Rightarrow B$

Dokaz.

1.

1.	A	*Hyp*
2.	B	*Hyp*
3.	$B \Rightarrow (A \Rightarrow B)$	Ax1
4.	$A \Rightarrow B$	*MP*$(2,3)$

2.

1.	A	*Hyp*
2.	$\neg B$	*Hyp*
3.	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$	iz $A, A \Rightarrow B \vdash B$ po tvrđenju dedukcije
4.	$(A \Rightarrow B) \Rightarrow B$	*MP*$(1,3)$
5.	$\neg B \Rightarrow \neg(A \Rightarrow B)$	po lemi 1.71
6.	$\neg(A \Rightarrow B)$	*MP*$(2,5)$

3, 4. Po lemi 1.70 važi $\neg A \vdash A \Rightarrow B$, pa tim pre važi $\neg A, B \vdash A \Rightarrow B$ kao i $\neg A, \neg B \vdash A \Rightarrow B$.

■

1.13 Glavna interpretacija iskaznog računa

Glavna interpretacija iskaznog računa $\mathcal{L}$ je interpretacija iskaznih formula u iskaznoj algebri (definicija 1.8). U ovom odeljku govorimo o vezi između sintaksnih svojstava formula (sintaksna posledica, teorema) i semantičkih svojstava formula (tautologija, semantička posledica). Razmatramo tri osnovna problema formalnih teorija: neprotivrečnost, potpunost i odlučivost, a spomenućemo i nezavisnost aksioma.

Tvrđenje 1.75 *Svaka teorema iskaznog računa $\mathcal{L}$ je tautologija (tj. $\vdash_{\mathcal{L}} A$ povlači $\models A$).*

Dokaz. Neposrednom proverom (diskusijom po vrednosti koju u datoj valuaciji uzimaju formule A, B, C) ustanovljavamo da su sve aksiome formalne teorije $\mathcal{L}$ tautologije. Indukcijom po n pokazaćemo da ako postoji dokaz dužine n za formulu A u $\mathcal{L}$, onda je A tautologija.

Za $n = 1$ A je aksioma, pa je tautologija. Pretpostavimo da su za svako $k < n$ sve formule koje imaju dokaz dužine k tautologije. Neka je A proizvoljna formula koja ima dokaz dužine n. Ukoliko je A aksioma, tada je A tautologija. U suprotnom, A je dobijena primenom pravila MP na prethodne članove u nizu:

$$
\begin{array}{rll}
1. & B_1 & \\
2. & B_2 & \\
\dots & & \\
i. & B_i & \\
\dots & & \\
j. & B_i \Rightarrow A & \\
\dots & & \\
 & & \\
n. & A & \qquad MP(i,j)
\end{array}
$$

Formule B_i i $B_i \Rightarrow A$ imaju dokaze dužine manje od n, pa prema induktivnoj hipotezi važi $\models B_i$ i $\models B_i \Rightarrow A$. Prema tvrđenju 1.14, tada važi i $\models A$. ∎

Neka je $p^\top$ oznaka za p a $p^\perp$ oznaka za $\neg p$ gde je p proizvoljno iskazno slovo.

Lema 1.76 (Kalmar (L. Kalmar)) *Neka su $p_1, \dots, p_n$ iskazna slova formule $A(p_1, \dots, p_n)$. Tada za sve vrednosti $\alpha_1, \dots, \alpha_n \in \{\top, \perp\}$ važi:*

$$p_1^{\alpha_1}, \dots, p_n^{\alpha_n} \vdash A^\alpha$$

gde je $\alpha = \bar{A}(\alpha_1, \dots, \alpha_n)$.

Dokaz. Indukcijom po m pokazujemo da tvrđenje važi za sve formule A sa m logičkih veznika $\Rightarrow, \neg$.

Ako je $m = 0$ tada je A neko iskazno slovo p, $\alpha = \alpha_1$, pa se tvrđenje svodi na $p^\alpha \vdash p^\alpha$, što je tačno.

Pretpostavimo da tvrđenje važi za sve formule sa manje od $m > 0$ logičkih veznika. Neka je A proizvoljna formula sa m logičkih veznika. Prema definiciji iskazne formule (definicija 1.64) mogu nastupiti sledeća dva slučaja:

1. A je $\neg B$ za neku formulu B. Tada B ima $m - 1 < m$ logičkih veznika, pa prema induktivnoj hipotezi važi
$$p_1^{\alpha_1}, \dots, p_n^{\alpha_n} \vdash B^\beta$$
gde je $\beta = \bar{B}(\alpha_1, \dots, \alpha_n)$. Razlikujemo dva podslučaja.
   (a) $\beta = \top$. Tada B^β je B, pa $p_1^{\alpha_1}, \dots, p_n^{\alpha_n} \vdash B$. $\alpha = \perp$, pa A^α je $\neg\neg B$. Prema lemi 1.71 $B \vdash \neg\neg B$, pa dobijamo $p_1^{\alpha_1}, \dots, p_n^{\alpha_n} \vdash A^\alpha$.
   (b) $\beta = \perp$. Tada B^β je $\neg B$ tj. A, pa je A^α baš A jer je $\alpha = \top$. Zato već po induktivnoj hipotezi važi $p_1^{\alpha_1}, \dots, p_n^{\alpha_n} \vdash A^\alpha$.

2. A je $B \Rightarrow C$. B i C imaju manje od m logičkih veznika, pa za njih važi induktivna hipoteza. Sva iskazna slova formula B i C su istovremeno i iskazna slova formule A, pa važi
$$p_1^{\alpha_1}, \ldots, p_n^{\alpha_n} \vdash B^\beta, C^\gamma$$
gde je $\beta = \bar{B}(\alpha_1, \ldots, \alpha_n)$, a $\gamma = \bar{C}(\alpha_1, \ldots, \alpha_n)$, tj. $\alpha = (\beta \Rightarrow \gamma)$. Dakle A^α je $B^\beta \Rightarrow C^\gamma$. Preostaje još da se dokaže da $B^\beta, C^\gamma \vdash (B \Rightarrow C)^{\beta \Rightarrow \gamma}$. Zavisno od vrednosti β i γ razlikujemo 4 slučaja, i svi slede iz leme 1.74:

1.	$\beta = \top, \gamma = \top$	svodi se na	$B, C \vdash B \Rightarrow C$
2.	$\beta = \top, \gamma = \bot$	svodi se na	$B, \neg C \vdash \neg(B \Rightarrow C)$
3.	$\beta = \bot, \gamma = \top$	svodi se na	$\neg B, C \vdash B \Rightarrow C$
4.	$\beta = \bot, \gamma = \bot$	svodi se na	$\neg B, \neg C \vdash B \Rightarrow C$

Time smo razmotrili sve mogućnosti pa je induktivni korak završen. ∎

1.13.1 Potpunost iskaznog računa

Tvrđenje 1.77 (Gedela o potpunosti) $\vdash A$ *akko* $\models A$.

Dokaz. Tvrđenje 1.75 predstavlja smer $\Rightarrow$) tvrđenja potpunosti. Dokazujemo smer $\Leftarrow$). Neka $\models A(p_1, \ldots, p_n)$. Tada za sve $\alpha_1, \ldots, \alpha_n$ važi $\bar{A}(\alpha_1, \ldots, \alpha_n) = \top$. Stoga prema lemi 1.76 za sve vrednosti $\alpha_1, \ldots, \alpha_n \in \{\top, \bot\}$ važi $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n} \vdash A$ (jer je $\alpha = \top$). Za $\alpha_n = \top$ dobijamo
$$p_1^{\alpha_1}, \ldots, p_{n-1}^{\alpha_{n-1}}, p_n \vdash A;$$
a za $\alpha_n = \bot$ dobijamo
$$p_1^{\alpha_1}, \ldots, p_{n-1}^{\alpha_{n-1}}, \neg p_n \vdash A.$$
Prema tvrđenju dedukcije (tvrđenje 1.66) tada važi
$$p_1^{\alpha_1}, \ldots, p_{n-1}^{\alpha_{n-1}} \vdash p_n \Rightarrow A$$
$$p_1^{\alpha_1}, \ldots, p_{n-1}^{\alpha_{n-1}} \vdash \neg p_n \Rightarrow A.$$
Kako prema lemi 1.73
$$p_n \Rightarrow A, \neg p_n \Rightarrow A \vdash A$$
dobijamo
$$p_1^{\alpha_1}, \ldots, p_{n-1}^{\alpha_{n-1}} \vdash A.$$
Ponavljajući ovaj postupak još $n-1$ puta dobijamo $\vdash A$. ∎

1.13.2 Odlučivost iskaznog računa

Tvrđenje 1.78 *Iskazni račun je odlučiv.*

Dokaz. Neka je A proizvoljna formula iskaznog računa. Prema prethodnom tvrđenju 1.77 $\vdash A$ akko $\models A$. Kako postoji postupak za proveru da li je $\models A$ (npr. tablicom), sledi da u konačnom broju koraka možemo proveriti da li je formula teorema u $\mathcal{L}$ (ukoliko koristimo tablicu broj koraka je 2^n gde je n broj promenljivih u formuli). ∎

1.13.3 Neprotivrečnost iskaznog računa

Definicija 1.79 Iskazni račun je *neprotivrečan* ako ne postoji par formula $A, \neg A$ tako da $\vdash A$ i $\vdash \neg A$.

Tvrđenje 1.80 *$\mathcal{L}$ je neprotivrečan.*

Dokaz. Pretpostavimo suprotno: da postoje A i $\neg A$ tako da $\vdash A$ i $\vdash \neg A$. Tada, prema tvrđenju potpunosti (1.77) važi $\models A$ i $\models \neg A$, što je u suprotnosti sa definicijom tautologije. ∎

1.13.4 Nezavisnost aksioma

Sistem aksioma formalne teorije je *nezavisan* ako se ni jedna od aksioma ne može dobiti od preostalih koristeći pravila izvođenja te formalne teorije. Sve aksiome iskaznog računa $\mathcal{L}$ su nezavisne. Ovde ćemo pokazati da je $Ax3$ nezavisna od $Ax1$ i $Ax2$. Neka je $S = \{0, 1\}$. Interpretirajmo logičke veznike $\Rightarrow, \neg$ kao operacije na skupu S date sledećim tablicama.

	$\neg$
0	0
1	0

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

Označimo sa $v_\beta(A)$ vrednost formule A pri valuaciji $\beta : \{p_1, p_2, \ldots\} \to S$. Proverom ustanovljavamo da je za sve valuacije β (bez obzira koje vrednosti promenljive formule A uzimale) važi $v_\beta(Ax1) = 0$ i $v_\beta(Ax2) = 0$. Pravilo *MP* čuva svojstvo "imati vrednost nula za sve valuacije" što se takođe neposredno proverava.

Zbog toga sve formule koje su dobijene polazeći od aksioma $Ax1$ i $Ax2$ imaju vrednost 0 u svim valuacijama. Ako međutim posmatramo valuaciju β u kojoj važi $v_\beta(A) = 1$ i $v_\beta(B) = 0$ za aksiomu $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$ dobijamo $v_\beta(Ax3) = 1$. Zbog toga $Ax3$ ne može biti posledica aksioma $Ax1$ i $Ax2$. Sličan postupak se primenjuje i pri dokazivanju nezavisnosti ostalih aksioma, pri čemu se za skup S u nekim slučajevima mora uzeti bar troelementni skup.

Napomena 1.81 Postoje formalni sistemi koji se interpretiraju u višeznačnoj logici, npr. na skupu $\{0, 1, \ldots, n-1\}$ ili čak na podskupu $(0, 1)$ skupa realnih brojeva. ◇

Glava 2

Predikatski račun

Iskazni račun nam omogućava povezivanje iskaza logičkim operacijama i utvrđivanje veza između njih, ali ne omogućava uvid u strukturu iskaza. Osim toga, iskaznim računom nije moguće iskazati značenje reči "svaki" i "neki". Da bi se to omogućilo potreban je složeniji jezik predikatskog (kvantifikatorskog) računa.

Primer 2.1 Neka je $P(x)$ oznaka za "x je tačka" a $Q(x)$ za "x je prava". Tada zapis iskaza "Kroz svake dve različiti tačke prolazi prava." u predikatskom računu glasi:

$$(\forall x)(\forall y)(P(x) \wedge P(y) \wedge x \neq y \Rightarrow (\exists z)(Q(z) \wedge x \in z \wedge y \in z)).$$

△

Kada govorimo o predikatskom računu prvog reda znači da dozvoljavamo kvantifikovanje samo objekata, ne i svojstava objekata.

2.1 Predikatske formule

Predikatske formule se grade od sledećih znakova:

1. $Var = \{v_1, v_2, v_3, \ldots\}$ prebrojiv skup znakova promenljivih koje označavamo i sa $x, y, z, x_1, y_1, z_1, \ldots, x_n, y_n, z_n, \ldots$
2. $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$ logički veznici;
3. $\forall, \exists$ kvantifikatori;
4. $(,)$ pomoćni znaci;
5. $a, b, c, a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ znaci konstanti;
6. $f, g, h, f_1^1, f_1^2, \ldots, f_2^1, f_2^2, \ldots, f_i^j$: operacijska slova; gornji indeks j u f_i^j označava arnost operacijskog slova;
7. $R_1^1, R_1^2, \ldots, R_2^1, R_2^2 \ldots, R_i^j$ relacijska slova; gornji indeks j u R_i^j označava arnost relacijskog slova. Mora postojati bar jedno relacijsko slovo.

Znakovi konstanti, operacijska slova i relacijska slova čine *jezik*. Promenljive, logički veznici, kantifikatori i pomoćni znaci su fiksirani, dok jezik predikatskog računa zavisi od teorije koju želimo njime da aksiomatizujemo.

Znakove konstanti tumačimo kao konkretne objekte, operacijska slova arnosti n kao n-arne operacije nad objektima, a relacijska slova arnosti n kao n-arne relacije nad objektima.

Primer 2.2 Neka je Z skup celih brojeva. Ako f_1^2 tumačimo kao sabiranje celih brojeva, R_1^2 kao jednakost celih brojeva, R_2^2 kao relaciju $<$ nad celih brojevima, a konstantu a_1 kao ceo broj 1 onda formula

$$R_1^2(x,x) \wedge R_2^2(x, f_1^2(x,a_1))$$

predstavlja tvrđenje "$x = x$ i $x < x + 1$". Ova formula je na jeziku $\{a_1, f_1^2, R_1^2, R_2^2\}$. $\triangle$

Definicija 2.3 *Termi* (izrazi) nad datim jezikom dati su sledećim pravilima:

1. Promenljive $x, y, z, \ldots$ i konstante $a, b, c \ldots$ su termi.
2. Ako su $t_1, \ldots, t_j$ termi i f_i^j operacijsko slovo arnosti j, tada je i $f_i^j(t_1, \ldots, t_j)$ term.
3. Termi se dobijaju samo konačnom primenom pravila 1 i 2.

Definicija 2.4 Neka su $t_1, \ldots, t_j$ termi i R_i^j relacijsko slovo arnosti j. Tada je $R_i^j(t_1, \ldots, t_j)$ *elementarna (atomska) formula.*

Definicija 2.5 Formule (nad datim jezikom) su date sledećim pravilima:

1. Elementarne formule su formule.
2. Ako su A i B formule i x promenljiva, tada su formule i $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $\neg A$, $(\forall x)A$ i $(\exists x)A$.
3. Formule se dobijaju samo konačnom primenom pravila 1 i 2.

Pošto kvantifikatori $\forall, \exists$ stoje samo uz promenljive, radi se o računu prvog reda. Postoje i računi višeg reda, u kojima se kavntifikatori odnose i na operacijska i relacijska slova.

Dogovor o brisanju zagrada:

1. spoljne zagrade brišemo;
2. prioritet znakova je sledeći: $\forall, \exists$; $\neg$; $\wedge, \vee$; $\Rightarrow, \Leftrightarrow$.

Definicija 2.6 Neka je x proizvoljna promenljiva i A proizvoljna formula predikatskog računa. Kažemo da je pojavljivanje promenljive x u formuli A *pod dejstvom kvantifikatora* $\forall$ odnosno $\exists$ ukoliko se ono nalazi u podformuli formule A oblika $(\forall x)B$ odnosno $(\exists x)B$. Ukoliko pojavljivanje promenljive x nije ni pod dejstvom ni jednog od kvantifikatora $\exists$, $\forall$, za to pojavljivanje promenljive x kažemo da je *slobodno*. Promenljiva x je *slobodna promenljiva* formule A ukoliko postoji slobodno pojavljivanje promenljive x u formuli A. Rečenica (zatvorena formula) je formula koja nema slobodne promenljive.

Primer 2.7 Posmatrajmo formulu A:

$$(\forall x)(Q(y) \Rightarrow (\exists y)P(x, f(y)))$$

gde su x i y promenljive, Q relacijsko slovo arnosti 1, P relacijsko slovo arnosti 2, a f operacijsko slovo arnosti 1. Prvo i drugo pojavljivanje promenljive x su pod dejstvom kvantifikatora $\forall$. Prvo pojavljivanje promenljive y je slobodno, a drugo je pod dejstvom kvantifikatora $\exists$. Promenljiva y je slobodna promenljiva formule A jer postoji slobodno pojavljivanje promenljive y u formuli A. $\triangle$

Svojstvo "biti slobodna promenljiva" se može definisati i na sledeći način. Neka je V oznaka za skup promenljivih terma t, a $FV(A)$ oznaka za skup svih slobodnih promenljivih formule A. Ako je x proizvoljna promenljiva, a proizvoljna konstanta, f_i^j proivoljno operacijsko slovo arnosti j, R_i^j proizvoljno relacijsko slovo arnosti j, $t_1, \ldots, t_n$ proizvoljni termi, a B i C proizvoljne formule, tada definišemo

$$V(x) = \{x\}$$

$$V(a) = \emptyset$$

$$V(f_i^j(t_1, \ldots, t_j)) = V(t_1) \cup \cdots \cup V(t_j)$$

$$FV(R_i^j(t_1, \ldots, t_j)) = V(t_1) \cup \cdots \cup V(t_j)$$

$$FV(\neg B) = FV(B)$$

$$FV(B \wedge C) = FV(B) \cup FV(C)$$

$$FV(B \vee C) = FV(B) \cup FV(C)$$

$$FV(B \Rightarrow C) = FV(B) \cup FV(C)$$

$$FV(B \Leftrightarrow C) = FV(B) \cup FV(C)$$

$$FV((\forall x)B) = FV(B) \setminus \{x\}$$

$$FV((\exists x)B) = FV(B) \setminus \{x\}$$

Napomena 2.8 (videti napomenu 1.10) Kada formulu A označimo sa $A(y_1, \ldots, y_n)$ tada sa $A(t_1, \ldots, t_n)$ označava formulu dobijenu zamenom redom slobodnih pojavljivanja promenljivih $y_1, \ldots, y_n$ termima $t_1, \ldots, t_n$ (ako se neka od promenljiva y_j ne javlja u formuli A tada je rezultat zamene t_j za y_j polazna formula). Analogne oznake uvodimo za terme: ako je $u(y_1, \ldots, y_n)$ term, tada sa $u(t_1, \ldots, t_n)$ označavamo rezultat zamene svih pojavljivanja promenljivih $y_1, \ldots, y_n$ redom termima $t_1, \ldots, t_n$ (ni u ovom slučaju se ne moraju sve promenljive $y_1, \ldots, y_n$ javiti u u). $\diamond$

Napomena 2.9 Kao i u iskaznom računu (napomena 1.11), možemo uvesti pojam zamene kao preslikavanja formula predikatskog računa u formule predikatskog računa. Prvo definišemo zamenu terma t u termu u umesto promenljive x, uz oznaci $u[x/t]$:

$$\begin{array}{rcl} x[x/t] & = & t \\ y[x/t] & = & y \\ a[x/t] & = & a \\ f_i^j(t_1,\ldots,t_j)[x/t] & = & f_i^j(t_1[x/t],\ldots,t_j[x/t]) \end{array}$$

Navodimo definiciju zamene terma t umesto promenljive x u formuli A, u oznaci $A[x/t]$.

$$\begin{array}{rcl} R_i^j(t_1,\ldots,t_j)[x/t] & = & R_i^j(t_1[x/t],\ldots,t_j[x/t]) \\ ((\forall x)B)[x/t] & = & (\forall x)B \\ ((\forall y)B)[x/t] & = & (\forall y)(B[x/t]) \\ ((\exists x)B)[x/t] & = & (\exists x)B \\ ((\exists y)B)[x/t] & = & (\exists y)(B[x/t]) \\ (\neg B)[x/t] & = & \neg(B[x/t]) \\ (B\wedge C)[x/t] & = & (B[x/t]\wedge C[x/t]) \\ (B\vee C)[x/t] & = & (B[x/t]\vee C[x/t]) \\ (B\Rightarrow C)[x/t] & = & (B[x/t]\Rightarrow C[x/t]) \\ (B\Leftrightarrow C)[x/t] & = & (B[x/t]\Leftrightarrow C[x/t]) \end{array}$$

Pri tome su x i y različite promenljive, a konstanta, t, $t_1,\ldots,t_n$ termi, f_i^j operacijsko slovo, R_i^j relacijsko slovo, a B i C proizvoljne formule. $\diamond$

Napomena 2.10 Negde se za zamenu promenljive x termom t umesto $A[x/t]$ koristi oznaka $A(t)$. $\diamond$

Primer 2.11 Neka je α oznaka za neko R_k^2 i neka su date formule

$$\alpha(x,y)\wedge\alpha(y,z)\Rightarrow\alpha(x,z)$$

$$(\forall x)(\forall y)(\forall z)(\alpha(x,y)\wedge\alpha(y,z)\Rightarrow\alpha(x,z)).$$

Navedene formule možemo tumačiti na više načina.

1. Neka x,y,z uzimaju vrednosti iz skupa Z, a α je relacija jednakosti $(=)$ celih brojeva. Tada prva formula postaje

$$x=y\wedge y=z\Rightarrow x=z.$$

Jasno je da ne možemo govoriti o njenoj tačnosti ako ne zadamo konkretne vrednosti za x, y, z (do ovoga je došlo zbog toga što formula sadrži slobodne promenljive). Proverom ustanovljavamo da ako x, y, z uzmu redom vrednosti 1, 1, 1 dobijamo tačan iskaz. Tačan iskaz dobijamo i kada x, y, z uzmu vrednosti 1, 2, 3. U stvari, lako je uveriti se da bez obzira koje vrednosti uzimale promenljive x, y, z formula se uvek svodi na tačan iskaz.

2. Neka x, y, z takođe uzimaju vrednosti iz skupa Z, ali neka je α relacija nejednakosti ($\neq$). Tada se prva formula svodi na $x \neq y \wedge y \neq z \Rightarrow x \neq z$. Ako x, y, z uzmu vrednosti 1, 2, 3 dobijamo tačan iskaz, ali ako uzmu vrednosti (redom) 1, 2, 1 dobijamo netačan iskaz.

Druga formula ne sadrži slobodne promenljive. Kvantifikator $\forall$ označava da formula koja je pod njegovim dejstvom treba da bude tačna za sve vrednosti promenljivih uz koju kvantifikatori stoje. Zbog toga je druga formula u prvom tumačenju tačna, a u drugom netačna.

Postoji beskonačno interpretacija formula i one se razlikuju prema skupu vrednosti koje uzimaju promenljive kao i tumačenju konstanti, relacijskih i iskaznih slova. Zbog toga je problem ispitivanja tačnosti formule mnogo složeniji nego u iskaznog računu. $\triangle$

2.2 Interpretacija predikatskih formula

Interpretacija predikatskih formula je uređen par $i = (D, \varphi)$ gde je D neprazan skup koji nazivamo domen interpretacije, a φ preslikavanje koje znacima konstanti pridružuje elemente domena D, operacijskim slovima arnosti j funkcije $D^j \rightarrow D$, a relacijskim znacima arnosti j relacije arnosti j nad skupom D tj. podskupove skupa D^j. Za $j = 1$ dobijamo unarne relacije, to su podskupovi skupa D. (Specijalni oblici unarnih relacija su prazna relacija koja odgovara praznom skupu $\emptyset$ i puna relacija koja odgovara skupu D.) Logičke veznike tumačimo kao odgovarajuće logičke operacije. Formuli $(\forall x)A$ dodeljujemo vrednost $\top$ akko za sve vrednosti promenljive x iz skupa D formula A ima vrednost $\top$. Formuli $(\exists x)A$ dodeljujemo vrednost $\top$ akko postoji vrednost koju može uzeti promenljiva x u skupu D tako da formula A ima vrednost $\top$.

Primer 2.12 U prvom slučaju prethodnog primera 2.11 tumačenje formule je odgovaralo interpretaciji $i = (Z, \varphi)$ gde je za $\varphi(\alpha)$ uzeta relacija jednakosti $=$. Tada je $i(\alpha(x, y) \wedge \alpha(y, z) \Rightarrow \alpha(x, z)) = \top$. U drugom slučaju $i = (Z, \varphi)$ gde je za $\varphi(\alpha)$ uzeta relacija $\neq$, pa $i(\alpha(x, y) \wedge \alpha(y, z) \Rightarrow \alpha(x, z))$ može biti $\top$ ili $\perp$ zavisno od vrednosti koje uzimaju x, y i z. $\triangle$

U nastavku ćemo precizirati pojam interpretacije. Vrednost terma u datoj interpretaciji i zavisi ne samo od interpretacije konstanti, već i od vrednosti koje uzimaju promenljive koje učestvuju u termu. Zato uvodimo pojam valuacije.

Definicija 2.13 Valuacija v interpretacije $i = (D, \varphi)$ je preslikavanje *Var* $\to D$ koje promenljivim dodeljuje vrednosti iz D.

Valuacija dodeljuje vrednosti svim promenljivim, ali su za vrednost terma bitne samo one promenljive koje u njemu učestvuju.

Definicija 2.14 Vrednost terma t za valuaciju v interpretacije i, u oznaci $t^i[v]$, data je sledećim pravilima:

1. $a^i[v] = \varphi(a)$ ako je a konstanta;
2. $x^i[v] = v(x)$ ako je x promenljiva;
3. $(f^n_m(t_1, \ldots, t_n))^i[v] = \bar{f}^n_m(t^i_1[v], \ldots, t^i_n[v])$ gde je $\bar{f}^n_m = \varphi(f^n_m)$ funkcija pridružena operacijskom znaku f^n_m, a $t^i_j[v]$ vrednosti terma t_i u valuaciji v interpretacije i (dobijene prethodnom primenom ovih pravila).

Definicija 2.15 Definišemo kada je formula A je tačna u valuaciji v interpretacije i, u oznaci $i \models_v A$.

1. Ako je A elementarna formula $R^n_m(t_1, \ldots, t_n)$, tada
$$i \models_v R^n_m(t_1, \ldots, t_n)$$
akko
$$(t^i_1[v], \ldots, t^i_n[v]) \in \bar{R}^n_m$$
gde je $\bar{R}^n_m = \varphi(R^n_m)$;
2. Ako je A oblika $\neg B$, tada $i \models_v \neg B$ akko ne važi $i \models_v B$;
3. Ako je A oblika $B \Rightarrow C$, tada $i \models_v B \Rightarrow C$ akko iz $i \models_v B$ sledi $i \models_v C$;
4. Ako je A oblika $(\forall x)B$, tada $i \models_v (\forall x)B$ akko za svako $d \in D$ važi $i \models_{v(d/x)} B$;
5. Ako je A oblika $(\exists x)B$, tada $i \models_v (\exists x)B)$ akko postoji $d \in D$ tako da važi $i \models_{v(d/x)} B$.

Pri tome je $v(d/x)$ valuacija interpretacije i data sa

$$v(d/x)(y) = \begin{cases} v(y), & y \neq x; \\ d, & y = x. \end{cases}$$

Ukoliko formula sadrži još neke iskazne veznike, oni se interpretiraju analogno, npr. $i \models_v B \wedge C$ akko $i \models_v B$ i $i \models_v C$. Ukoliko jezik ne sadrži npr. iskazni veznik $\wedge$, tada se $A \wedge B$ uvodi kao skraćenica za $\neg(A \Rightarrow \neg B)$, a lako se dokazuje da važi $i \models_v B \wedge C$ akko $i \models_v B$ i $i \models_v C$. Takođe se $(\exists x)A$ može uvesti kao skraćenica za $\neg(\forall x)\neg A$, pa iz prethodne definicije sledi da je formula $(\exists x)A$ tačna u valuaciji v akko postoji $d \in D$ tako da je A tačna u valuaciji $v(d/x)$.

Definicija 2.16 Formula A je tačna u interpretaciji i, u oznaci $i \models A$ akko za svaku valuaciju v interpretacije i važi $i \models_v A$. Ako je A tačna u interpretaciji i kažemo da je i model formule A.

Definicija 2.17 Formula predikatskog računa A je *valjana*, u oznaci $\models A$, akko je tačna u svim interpretacijama (svaka interpretacija formule A je model za A).

Napomena 2.18 Ako važi $i \models_v A$, pišemo $i_v(A) = \top$, u suprotnom pišemo $i_v(A) = \bot$. To nam omogućava da definiciju interpretacije iskažemo u obliku analognom interpretaciji iskaznih formula. Tako imamo $i_v(C \Rightarrow B) = (i_v(C) \Rightarrow i_v(B))$ gde je sa desne strane "$\Rightarrow$" operacija iskazne algebre.

Slično, umesto $i \models A$ pišemo $i(A) = \top$. Dakle $i(A) = \top$ akko za svaku valuaciju v važi $i_v(A) = \top$. Ako pak za svaku valuaciju v važi $i_v(A) = \bot$, tada pišemo $i(A) = \bot$. $\diamond$

Sledeći primer pokazuje da u opštem slučaju ne mora važiti ni $i(A) = \top$ ni $i(A) = \bot$.

Primer 2.19 Neka je A formula $R_1^2(x, y)$, a interpretacija $i = (Z, \varphi)$ gde je Z skup celih brojeva, a $\varphi(R_1^2)$ relacija $<$ na skupu celih brojeva. Za valuaciju α za koju važi $\alpha(x) = 5$ i $\alpha(y) = 1$ važi $i_\alpha(A) = \bot$ jer nije $5 < 1$. Sa druge strane, za valuaciju β za koju važi $\beta(x) = 1$ i $\beta(y) = 5$ važi $i_\beta(A) = \top$ jer je $1 < 5$. Dakle niti je $i(A) = \top$ niti $i(A) = \bot$, već vrednost formule u interpretaciji i zavisi od valuacije. $\triangle$

Primetimo da formula $R_1^2(x, y)$ nije bila zatvorena, jer su i x i y slobodne promenljive. U nastavku ćemo pokazati da zatvorenim formulama u datoj interpretaciji uvek možemo dodeliti jednu od istinitosnih vrednosti $\top$ ili $\bot$.

Lema 2.20 *Neka je i proizvoljna interpretacija i A proizvoljna formula. Ako se valuacije v i v' poklapaju za sve vrednosti promenljivih koje su slobodne u A tj. ako važi:*

$$x \in FV(A) \text{ povlači } v(x) = v'(x),$$

tada je $i_v(A) = i_{v'}(A)$.

Dokaz. Neka je $i = (D, \varphi)$ proizvoljna interpretacija. Dokaz sprovodimo indukcijom po broju logičkih veznika i kvantifikatora u formuli A.

Ako je A elementarna formula, tada su sve promenljive koje se javljaju u formuli A slobodne. Ako se v i v' poklapaju za sve vrednosti tih promenljivih, iz definicije interpretacije (definicije 2.14 i 2.15) sledi da je $i_v(A) = i_{v'}(A)$.

Pretpostavimo da tvrđenje važi za sve formule sa manje od $n > 0$ logičkih veznika i kvantifikatora i neka je A formula koja sadrži n logičkih veznika i kvantifikatora. Razlikujemo sledeće slučajeve.

1. A je $\neg B$ gde B sadrži $n-1$ logičkih veznika i kvantifikatora. Neka se valuacije v i v' poklapaju za sve slobodne promenljive formule A. Kako je $FV(A) = FV(B)$, a za B važi induktivna hipoteza, dobijamo da je $i_v(B) = i_{v'}(B)$. Odatle po definiciji interpretacije
$$i_v(\neg B) = \neg i_v(B) = \neg i_{v'}(B) = i_{v'}(\neg B),$$
što znači da tvrđenje važi i za A.

2. A je $B \wedge C$ gde B i C imaju manje od n logičkih veznika i kvantifikatora, pa za njih važi induktivna hipoteza. Neka se v i v' poklapaju za sve vrednosti promenljivih iz $FV(A)$. Kako je $FV(A) = FV(B) \cup FV(C)$, valuacije v i v' se poklapaju za sve vrednosti iz $FV(B)$, pa važi $i_v(B) = i_{v'}(B)$. Analogno, $i_v(C) = i_{v'}(C)$. Zato je
$$\begin{aligned} i_v(B \wedge C) &= i_v(B) \wedge i_v(C) \\ &= i_{v'}(B) \wedge i_{v'}(C) \\ &= i_{v'}(B \wedge C) \end{aligned}$$
što znači da tvrđenje važi i za formulu A.

3. Ako je A oblika $B \vee C$, $B \Rightarrow C$ ili $B \Leftrightarrow C$ dokaz je analogan prethodnom slučaju.

4. A je $(\forall x)B$. Tada je $FV(A) = FV(B) \setminus \{x\}$. Neka se v i v' poklapaju za sve promenljive iz $FV(A)$. Tada se v i v' poklapaju za sve promenljive iz $FV(B)$ osim možda promenljive x, pa se za proizvoljno $d \in D$ valuacije $v(d/x)$ i $v'(d/x)$ poklapaju za sve promenljive iz $FV(B)$. Zato je prema induktivnoj hipotezi
$$\begin{aligned} i_v((\forall x)B) = \top &\Leftrightarrow \text{ za sve } d \in D \ i_{v(d/x)}(B) = \top \\ &\Leftrightarrow \text{ za sve } d \in D \ i_{v'(d/x)}(B) = \top \\ &\Leftrightarrow i_{v'}((\forall x)B) = \top. \end{aligned}$$
Dakle $i_v(A) = i_{v'}(A)$.

5. A je $(\exists x)B$. Analogno prethodnom slučaju, ako se v i v' poklapaju za sve promenljive iz $FV(A)$, tada je
$$\begin{aligned} i_v((\exists x)B) = \top &\Leftrightarrow \text{ postoji } d \in D \text{ tako da } i_{v(d/x)}(B) = \top \\ &\Leftrightarrow \text{ postoji } d \in D \text{ tako da } i_{v'(d/x)}(B) = \top \\ &\Leftrightarrow i_{v'}((\exists x)B) = \top, \end{aligned}$$
pa i u ovom slučaju $i_v(A) = i_{v'}(B)$.

Time je dokaz završen. ■

Posledica 2.21 *Ako je A zatvorena formula, i proizvoljna interpretacija, a v i v' proizvoljne valuacije, tada je $i_v(A) = i_{v'}(A) = i(A)$.*

Dokaz. Ako su v i v' proizvoljne valuacije interpretacije i, tada se one poklapaju za sve slobodne promenljive zatvorene formule A jer $FV(A) = \emptyset$. Zato je po prethodnoj lemi 2.20 $i_v(A) = i_{v'}(A)$. Odatle dalje sledi da ako je $i_v(A) = \top$, tada za sve valuacije v' važi $i_{v'}(A) = \top$, pa $i(A) = \top$. Ako je pak $i_v(A) = \bot$, tada za sve valuacije v' važi $i_{v'}(A) = \bot$, pa je $i(A) = \bot$. Prema tome, $i(A) = i_v(A)$. ∎

Iz prethodnih tvrđenja sledi da zatvorene formule u datoj interpretaciji uvek imaju dobro definisanu istinitosnu vrednost iz skupa $\{\top, \bot\}$. Za njih tada važe pravila koja smo definisali za svaku valuaciju pojedinačno: tako je $i(A \wedge B) = i(A) \wedge i(B)$, $i(\neg A) = \neg i(A)$ i analogno za ostale logičke veznike.

Primetimo da je način izgradnje predikatskih formula od elementarnih formula (definicija 2.5) analogan načinu izgradnje iskaznih fomula od iskaznih slova (definicija 1.3). Ukoliko je $A(p_1, \ldots, p_n)$ iskazna fomula, a $B_1, \ldots, B_n$ predikatske formule tada sa $A(B_1, \ldots, B_n)$ označavamo predikatsku formulu dobijenu od $A(p_1, \ldots, p_n)$ tako što su iskazna slova p_j zamenjena odgovarajućim predikatskim formulama B_j, a iskazni veznici $\neg, \wedge, \vee, \Rightarrow$ i $\Leftrightarrow$ odgovarajućim predikatskim veznicima (koje smo ovde označavali istim simbolima $\neg, \wedge, \vee, \Rightarrow$ i $\Leftrightarrow$).

Tvrđenje 2.22 *Neka je iskazna formula $A(p_1, \ldots, p_n)$ tautologija i $B_1, \ldots, B_n$ proizvoljne predikatske formule. Tada je $A(B_1, \ldots, B_n)$ valjana formula, tzv.* izvod tautologije.

Dokaz. Neka je i proizvoljna interpretacija i v proizvoljna valuacija interpretacije i. Tada za svako B_j važi $i_v(B_j) \in \{\top, \bot\}$. Pošto je A tautologija, bez obzira na vrednosti $i_v(B_j)$ važiće $i_v(A(B_1, \ldots, B_n)) = \top$. Kako je v bila proizvoljna valuacija, zaključujemo da je $A(B_1, \ldots, B_n)$ tačna u svim valuacijama interpretacije i, pa je tačna u interpretaciji i. Kako je i proizvoljna interpretacija, znači da je $A(B_1, \ldots, B_n)$ tačna u svim interpretacijama, pa je valjana. ∎

Zadatak 2.23 Odrediti model za formulu $(\forall x)(\beta(x) \Rightarrow \beta(f(x)))$ takav da je

$$D = \{a, b, c\};$$

$$\bar{f} = \begin{pmatrix} a\,b\,c \\ c\,b\,a \end{pmatrix}.$$

Rešenje. Pošto je zadat domen D i interpretacija $\bar{f}$ operacijskog znaka f, treba još odrediti interpretaciju $\bar{\beta}$ operacijskog znaka β. Prema definiciji univerzalnog kvantifikatora treba da važi:

$$\bar{\beta}(a) \Rightarrow \bar{\beta}(f(a))$$
$$\bar{\beta}(b) \Rightarrow \bar{\beta}(f(b))$$
$$\bar{\beta}(c) \Rightarrow \bar{\beta}(f(c))$$

pa po definiciji funkcije f

$$\bar{\beta}(a) \Rightarrow \bar{\beta}(c)$$
$$\bar{\beta}(b) \Rightarrow \bar{\beta}(b)$$
$$\bar{\beta}(c) \Rightarrow \bar{\beta}(a)$$

Jedno od mogućih rešenja je $\bar{\beta} = \{a, c\}$.

Ukoliko $\bar{\beta}(a)$, $\bar{\beta}(b)$, $\bar{\beta}(c)$ posmatramo kao iskazna slova, vidimo da je problem sveden na traženje modela za skup iskaznih formula. U ovom slučaju je D konačan, pa smo dobili konačan broj iskaznih formula. ■

Videli smo da se iz tautologija mogu izvesti valjane formule. Sledeći primer pokazuje da nisu sve valjane formule tog oblika.

Tvrđenje 2.24 *Formula*

$$\neg(\forall x)\alpha(x) \Leftrightarrow (\exists x)\neg\alpha(x)$$

nije izvod tautologije, ali jeste valjana.

Dokaz. Formula je oblika $A \Leftrightarrow B$ gde su A i B dve različite formule bez logičkih veznika. Zato može biti jedino izvod iskazne formule oblika $p \Leftrightarrow q$ za neka dva različita iskazna slova p i q. Kako iskazne formule tog oblika nisu tautologije, sledi da formula nije izvod tautologije.

Prelazimo na dokaz da je formula valjana. Neka je $i = (D, \varphi)$ proizvoljna interpretacija. Razlikujemo dva slučaja.

1. $\varphi(\alpha) = D$ tj. α interpretiramo kao punu relaciju. Neka je v proizvoljna valuacija. Po definiciji interpretacije formule za sve $d \in D$ važi

$$\begin{array}{ll} i \models_{v(d/x)} \alpha(x) & \text{akko} \\ x^i[v(d/x)] \in \varphi(\alpha) & \text{akko} \\ d \in \varphi(\alpha). & \end{array}$$

Pošto je $\varphi(\alpha) = D$, važi $i \models_{v(d/x)} \alpha(x)$ za svako $d \in D$, pa $i \models_v (\forall x)\alpha(x)$. Stoga ne važi $i \models_v \neg(\forall x)\alpha(x)$. Sa druge strane, za proivoljno $e \in D$ imamo

$$\begin{array}{ll} i \models_{v(e/x)} \neg\alpha(x) & \text{akko} \\ \text{ne važi } x^i[v(e/x)] \in \varphi(\alpha) & \text{akko} \\ \text{ne važi } e \in \varphi(\alpha) & \end{array}$$

Pošto je $\varphi(\alpha) = D$ sledi da ni za jedno $e \in D$ ne važi $i \models_{v(e/x)} \neg\alpha(x)$, pa ne važi $i \models_v (\exists x)(\neg\alpha(x))$. Dakle obe strane ekvivalencije su netačne, pa je ekvivalencija tačna. Valuacija v je bila proizvoljna, pa za svaku valuaciju v važi $i \models_v \neg(\forall x)\alpha(x) \Leftrightarrow (\exists x)(\neg\alpha(x))$. Zato je formula tačna u interpretaciji i.

2. $\varphi(\alpha) \neq D$. Tada postoji $d \in D$ tako da $d \notin \varphi(\alpha)$. Neka je v proizvoljna valuacija. Tada, analogno prethodnom slučaju, ne važi $i \models_{v(d/x)} \alpha(x)$, pa ne važi $i \models_v (\forall x)\alpha(x)$. Zato važi $i \models_v \neg(\forall x)\alpha(x)$. Sa druge strane, ne važi $i \models_{v(d/x)} \alpha(x)$, pa važi $i \models_{v(d/x)} \neg\alpha(x)$. Zato važi $i \models_v (\exists x)\neg\alpha(x)$. Sada su obe strane implikacije tačne, a to važi u proizvoljnoj valuaciji v, pa i u ovom slučaju $i \models \neg(\forall x)\alpha(x) \Leftrightarrow (\exists x)(\neg\alpha(x))$.

■

Napomena 2.25 Prethodni rezultat se može uopštiti: za proizvoljnu formulu A važi

$$\neg(\forall x)A \Leftrightarrow (\exists x)\neg A.$$

Dokaz je analogan prethodnom, ali se diskusija vrši po relaciji $\alpha(x)$ datoj sa $\alpha(b)$ akko $\models_{v(b/x)} A$ gde je v proizvoljna valuacija. ◇

Zadatak 2.26 Neka je sa F označena formula

$$(\forall x)\,\neg\alpha(x,x) \ \wedge\ (\forall x)(\exists y)\,\alpha(x,y) \ \wedge\ (\forall x)(\forall y)(\forall z)\,(\alpha(x,y) \wedge \alpha(y,z) \Rightarrow \alpha(x,z)).$$

Pokazati da formula F ima model, ali da je svaki model za F sa beskonačnim domenom.

Rešenje. Neka je $i = (N, \varphi)$ interpretacija formule F gde je N skup prirodnih brojeva, a $\varphi(\alpha) = <$ relacija strogog poretka na skupu prirodnih brojeva. Ni za jedno $d \in N$ ne važi $d < d$, pa važi prvi deo formule F. Drugi deo formule F važi jer za svako $d \in N$ postoji $d+1 \in N$ tako da $d < d+1$. Treći deo formule F je posledica tranzitivnosti relacije $<$. Dakle i je model formule F. Pokazujemo da svaki model formule F ima beskonačan domen.

Neka je $i = (D, \varphi)$ model formule F. Prema definiciji interpretacije, to znači da za relaciju $\bar{\alpha}$ važe sledeća tvrđenja:

1. za svako $d \in D$ nije $\bar{\alpha}(d,d)$
2. za svako $d \in D$ postoji $e \in D$ tako da $\bar{\alpha}(d,e)$
3. za sve $d, e, f \in D$ iz $\bar{\alpha}(d,e)$ i $\bar{\alpha}(e,f)$ sledi $\bar{\alpha}(d,f)$

Pokazaćemo sledeću lemu.

Lema 2.27 *Za svaki prirodan broj n postoji niz $x_1, \ldots, x_n$ elemenata iz D tako da za svako i, j gde je $1 \leq i < j \leq n$ važi $\bar{\alpha}(x_i, x_j)$.*

Dokaz. Za $n = 1$ tvrđenje važi jer je D neprazan skup, pa postoji element $d \in D$. Ako stavimo $x_1 = d$ dobijamo niz dužine 1 za koji trivijalno važi tvrđenje leme.

Pretpostavimo da tvrđenje važi za n: postoji niz $x_1, \ldots, x_n$ elemenata iz D tako da za svako i, j gde $1 \leq i < j \leq n$ važi $\bar{\alpha}(x_i, x_j)$. Prema tvrđenju 2, postoji element $e \in D$ tako da $\bar{\alpha}(x_n, e)$. Stavimo $x_{n+1} = e$. Pokazujemo da za svako i, j gde $1 \leq i < j \leq n+1$ važi $\bar{\alpha}(x_i, x_j)$. Neka su i, j gde $1 \leq i < j \leq n+1$ proizvoljni. Ako je $j \leq n$, tada po induktivnoj hipotezi važi $\alpha(x_i, x_j)$. Neka je $j = n+1$ i $1 \leq i \leq n$. Ako je $i = n$ tada po konstrukciji elementa x_{n+1} važi $\bar{\alpha}(x_i, x_j)$. Ako je $i < n$, tada po induktivnoj hipotezi važi $\bar{\alpha}(x_i, x_n)$. Kako po konstrukciji elementa x_{n+1} važi $\bar{\alpha}(x_n, x_{n+1})$, po tvrđenju 3 sledi $\bar{\alpha}(x_i, x_{n+1})$. Time je dokaz leme završen. ∎

Primetimo da je niz $x_1, \ldots, x_n$ iz prethodne leme niz različitih elemenata, jer ako je $1 \leq i < j \leq n$ tada je $\bar{\alpha}(x_i, x_j)$, a to po tvrđenju 1 povlači $x_i \neq x_j$. Sada je lako dokazati da je skup D beskonačan: pretpostavimo suprotno, da D ima n elemenata za neki prirodan broj n. Kako postoji skup od $n+1$ različitih elemenata skupa D, dobijamo kontradikciju. Dakle D mora biti beskonačan. Time smo pokazali da svaka interpretacija i koja je model za F ima beskonačan domen D. ∎

2.3 Neke valjane formule

Valjane formule predstavljaju zakonitosti mišljenja. Neke njihove oblike proučavao je još Aristotel u vidu silogizama. U nastavku navodimo spisak često korišćenih valjanih formula [SP].

$$\neg(\forall x)A \Leftrightarrow (\exists x)\neg A \tag{2.1}$$
$$\neg(\exists x)A \Leftrightarrow (\forall x)\neg A \tag{2.2}$$
$$(\forall x)(A \wedge B) \Leftrightarrow (\forall x)A \wedge (\forall x)B \tag{2.3}$$
$$(\exists x)(A \vee B) \Leftrightarrow (\exists x)A \vee (\exists x)B \tag{2.4}$$
$$(\forall x)A \vee (\forall x)B \Rightarrow (\forall x)(A \vee B) \tag{2.5}$$
$$(\exists x)(A \wedge B) \Rightarrow (\exists x)A \wedge (\exists x)B \tag{2.6}$$
$$(\forall x)(A \Rightarrow B) \Rightarrow ((\forall x)A \Rightarrow (\forall x)B) \tag{2.7}$$
$$(\forall x)(\forall y)A \Leftrightarrow (\forall y)(\forall x)A \tag{2.8}$$
$$(\exists x)(\exists y)A \Leftrightarrow (\exists y)(\exists x)A \tag{2.9}$$
$$(\exists x)(\forall y)A \Rightarrow (\forall y)(\exists x)A \tag{2.10}$$

Sledeće valjane formule važe ako x nije slobodna promenljiva u formuli B.

$$(\forall x)(A \vee B) \Leftrightarrow (\forall x)A \vee B \tag{2.11}$$
$$(\exists x)(A \wedge B) \Leftrightarrow (\exists x)A \wedge B \tag{2.12}$$
$$(\forall x)(A \Rightarrow B) \Leftrightarrow ((\exists x)A \Rightarrow B) \tag{2.13}$$
$$(\forall x)(B \Rightarrow A) \Leftrightarrow (B \Rightarrow (\forall x)A) \tag{2.14}$$

Konstrukcijom odgovarajuće interpretacije može se pokazati da u formulama 2.5, 2.6 i 2.7 ne važi suprotan smer. Pokažimo to za formulu 2.5. Neka je formula A elementarna formula $\alpha(x)$ i B elementarna formula $\beta(x)$. Posmatramo interpretaciju čiji je domen skup prirodnih brojeva, α se interpretira kao unarna relacija "biti paran", a β kao unarna relacija "biti neparan". Tada je desna strana formule tačna, jer je svaki prirodan broj paran ili neparan, a leva netačna jer niti su svi prirodni brojevi parni, niti su svi prirodni brojevi neparni. Zato na ovom modelu *ne važi* implikacija

$$(\forall x)(\alpha(x) \vee \beta(x)) \Rightarrow (\forall x)\alpha(x) \vee (\forall x)\beta(x),$$

pa ne važi ni ekvivalencija. Dakle formula

$$(\forall x)(\alpha(x) \vee \beta(x)) \Leftrightarrow (\forall x)\alpha(x) \vee (\forall x)\beta(x)$$

nije valjana, jer smo pronašli interpretaciju u kojoj nije tačna.

2.4 Neka jednostavna svojstva valjanih formula

Tvrđenje 2.28 *Ako važi* $\models A$ *i važi* $\models A \Rightarrow B$ *onda važi* $\models B$.

Dokaz. Neka $\models A$ i $\models A \Rightarrow B$. Neka je i proizvoljna interpretacija i v proizvoljna valuacija te interpretacije. Kako $\models A \Rightarrow B$, sledi $i \models_v A \Rightarrow B$, što po definiciji znači da iz $i \models_v A$ sledi $i \models_v B$. Kako $\models A$, važi $i \models_v A$, pa $i \models_v B$. Dakle za proizvoljnu interpretaciju i i proizvoljnu valuaciju v važi $i \models_v B$. Zato $\models B$. ∎

Tvrđenje 2.29 $\models A$ *akko* $\models (\forall x)A$.

Dokaz. $\Rightarrow$): Neka $\models A$. Neka je $i = (D, \varphi)$ proizvoljna interpretacija i v proizvoljna valuacija. Po definiciji interpretacije važi

$$i \models_v (\forall x)A \tag{$*$}$$

akko za svako $d \in D$ važi

$$i \models_{v(d/x)} A \tag{$**$}$$

Neka je d proizvoljno. Preslikavanje $v(d/x)$ je valuacija interpretacije i, a važi $\models A$, pa važi $(**)$. Kako je d bilo proizvoljno, važi i $(*)$. Pošto to važi za svaku interpretaciju i, sledi $\models (\forall x)A$.

$\Leftarrow$): Neka je $\models (\forall x)A$. Tada po definiciji, za svaku interpretaciju $i = (D, \varphi)$, svaku valuaciju v i svako $d \in D$ važi $i \models_{v(d/x)} A$. Uzimajući specijalno $d = v(x)$ dobijamo da za svako i i svako v važi $i \models_{v(v(x)/x)} A$, tj. $i \models_v A$. Dakle $\models A$. ∎

Tvrđenje 2.30 (Tvrđenje zamene) *Neka $\models A \Leftrightarrow B$ i neka je $F(A)$ proizvoljna formula koja sadrži kao podformulu formulu A. Ako sa $F(B)$ označimo rezultat zamene nekih pojava podformule A formulom B, tada $\models F(A) \Leftrightarrow F(B)$.*

Dokaz. Neka je i proizvoljna interpretacija i v proizvoljna valuacija. Pošto $\models A \Leftrightarrow B$ sledi $i \models_v A \Leftrightarrow B$, pa $i_v(A) = i_v(B)$. Kako se $F(A)$ od $F(B)$ razlikuje samo po zameni nekih pojava podformule A formulom B, sledi $i_v(F(A)) = i_v(F(B))$ (ovo se može proveriti i indukcijom po složenosti formule F). Odatle $i \models_v F(A) \Leftrightarrow F(B)$. Kako su i i v proizvoljni, sledi $\models F(A) \Leftrightarrow F(B)$. ■

Definicija 2.31 Term t je *nezavisan (slobodan)* za promenljivu x u formuli A akko zamenom t za slobodne pojave promenljive x nijedna promenljiva terma t ne postaje vezana u $A[x/t]$.

Tvrđenje 2.32 *Neka je i proizvoljna interpretacija i v proizvoljna valuacija interpretacije i. Neka je A proizvoljna formula, i t term slobodan za promenljivu x u formuli A. Tada važi $i_v(A[x/t]) = i_{v'}(A)$ gde je $v' = v(t^i[v]/x)$ (sintaksna zamena i zamena u valuaciji su ekvivalentne).*

Dokaz. Neka je $i = (D, \varphi)$ proizvoljna interpretacija i v proizvoljna valucija interpretacije i. Dokazaćemo prvo sledeću lemu.

Lema 2.33 *Ako su u i t termi tada za svaku valuaciju v važi $u[x/t]^i[v] = u^i[v']$ gde je $v' = v(t^i[v]/x)$.*

Dokaz. Neka je v proizvoljna valuacija. Tvrđenje ćemo dokazati indukcijom po broju operacijskih slova u termu u. Ako term nema operacijskih slova, tada je on promenljiva ili konstanta.

1. u je promenljiva. Ukoliko je $u = x$, tada je

$$(x[x/t])^i[v] = t^i[v] = x^i[v(t^i[v]/x)].$$

   Ukoliko je $u = y \neq x$, tada je

$$(y[x/t])^i[v] = y^i[v] = v(y) = v'(y) = y^i[v'].$$

2. $u = a$ je konstanta. U tom slučaju važi

$$a[x/t]^i[v] = a^i[v] = \varphi(a) = a^i[v'].$$

Pretpostavimo da tvrđenje važi za sve terme sa manje od k operacijskih slova. Neka je u proizvoljan term sa k operacijskih slova. Tada je $u = f_m^n(s_1, \ldots, s_n)$ gde termi s_j

za $1 \leq j \leq n$ imaju manje od k operacijskih slova, pa za njih važi indukcijska hipoteza. Zato važi

$$\begin{aligned}
&(f_m^n(s_1,\ldots,s_n)[x/t])^i[v] = \\
&\quad = (f_m^n(s_1[x/t],\ldots,s_n[x/t])^i[v] \\
&\quad = \varphi(f_m^n)((s_1[x/t])^i[v],\ldots,(s_n[x/t])^i[v]) && \text{(definicija vrednosti terma)} \\
&\quad = \varphi(f_m^n)(s_1^i[v'],\ldots,s_n^i[v']) && \text{(indukcijska hipoteza)} \\
&\quad = (f_m^n(s_1,\ldots,s_n))^i[v'] && \text{(definicija vrednosti terma).}
\end{aligned}$$

Time je lema dokazana. ■

Dokaz samog tvrđenja sprovodimo indukcijom po broju logičkih veznika u formuli A. Ako A nema logičkih veznika, tada je A neka elementarna formula $R_m^n(s_1,\ldots,s_n)$, pa za proizvoljnu valuaciju v i $v' = v(t^i[v]/x)$ važi:

$$\begin{aligned}
&i_v(R_m^n(s_1,\ldots,s_n)[x/t]) \\
&\quad = i_v(R_m^n(s_1[x/t],\ldots,s_n[x/t])) \\
&\quad = \varphi(R_m^n)((s_1[x/t])^i[v],\ldots,(s_n[x/t])^i[v]) \\
&\qquad\quad \text{(po definiciji vrednosti terma)} \\
&\quad = \varphi(R_m^n)(s_1^i[v'],\ldots,s_n^i[v']) \\
&\qquad\quad \text{(po prethodnoj lemi)} \\
&\quad = i_{v'}(R_m^n(s_1,\ldots,s_n)).
\end{aligned}$$

Pretpostavimo da tvrđenje važi za sve formule sa manje od $k > 0$ logičkih veznika i sve valuacije interpretacije i. Neka je A formula sa k logičkih veznika, t term slobodan za promenljivu x u formuli A, v proizvoljna valuacija i $v' = v(b/x)$ za $b = t^i[v]$. Prema definiciji formule, mogu nastupiti sledeći slučajevi.

1. A je $\neg C$. Tada je t slobodan za x i u C, pa važi:

$$\begin{aligned}
i_v((\neg C)[x/t]) &= i_v(\neg(C[x/t])) \\
&= \neg i_v(C[x/t]) \\
&= \neg i_{v'}(C) \quad \text{(po induktivnoj hipotezi)} \\
&= i_{v'}(\neg C).
\end{aligned}$$

2. A je $(C \Rightarrow D)$. Tada je t slobodan za x i u C i D, pa važi:

$$\begin{aligned}
i_v((C \Rightarrow D)[x/t]) &= i_v(C[x/t] \Rightarrow D[x/t]) \\
&= i_v(C[x/t]) \Rightarrow i_v(D[x/t]) \\
&= i_{v'}(C) \Rightarrow i_{v'}(D) \\
&\qquad \text{(induktivna hipoteza)} \\
&= i_{v'}(C \Rightarrow D).
\end{aligned}$$

3. Slučajevi kada je A oblika $C \wedge D$, $C \vee D$ i $C \Leftrightarrow D$ se razmatraju analogno prethodnom slučaju.
4. A je $(\forall x)C$. Tada x nije slobodno u A, pa važi:

$$i_v(((\forall x)C)[x/t]) = i_v((\forall x)C) = i_{v'}((\forall x)C)$$

jer se v i v' razlikuju samo po vrednosti za x, a po lemi 2.20 vrednost valuacije za x ne utiče na vrednost formule.
5. Slučaj kada je A oblika $(\exists x)C$ se razmatra analogno prethodnom slučaju.
6. A je $(\forall y)C$, za $y \neq x$. Razlikujemo dva podslučaja.

   (a) y se javlja u termu t. Ukoliko bi x bilo slobodno u C, tada bi zamenom t umesto x u formulu A promenljiva y postala vezana, pa t ne bi bio slobodan za x u A. Kako je po pretpostavci t slobodan za x u A, x se ne javlja slobodno u C (pa ni u A). Zato kao i u prethodnom slučaju tvrđenje važi.
   (b) y se ne javlja u termu t. Tada je t slobodan za x u C, pa

$$i \models_v (((\forall y)C)[x/t])$$

akko

$$i \models_v ((\forall y)(C[x/t]))$$

akko (po definiciji interpretacije)

$$\text{za svako } d \in D \text{ važi } i \models_{v(d/y)} C[x/t]$$

akko (prema induktivnoj hipotezi)

$$\text{za svako } d \in D \text{ važi } i \models_{v(d/y)(t^i[v(d/y)]/x)} C$$

akko (jer se y ne javlja u t, pa $t^i[v(d/y)] = t^i[v]$)

$$\text{za svako } d \in D \text{ važi } i \models_{v(d/y)(b/x)} C$$

akko (jer $x \neq y$)

$$\text{za svako } d \in D \text{ važi } i \models_{v(b/x)(d/y)} C$$

akko (po definiciji interpretacije)

$$i \models_{v'} (\forall y)C.$$

■

Tvrđenje 2.34 *Neka je A proizvoljna formula i t term slobodan za x u A. Tada je formula*

$$(\forall x)A \Rightarrow A[x/t]$$

valjana.

Dokaz. Neka je $i = (D, \varphi)$ proizvoljna interpretacija i v valuacija u i. Neka važi $i \models_v (\forall x)A$. Tada za svako $d \in D$ važi

$$i \models_{v(d/x)} A \qquad (*)$$

Pošto je t slobodan za x u A, prema prethodnom tvrđenju važi $i \models_v A[x/t]$ akko $i \models_{v'} A$ gde je $v' = v(t^i[v]/x)$. Stavljajući u $(*)$ $d = t^i[v]$ dobijamo $i \models_{v'} A$. Dakle $i \models_v A[x/t]$. Stoga $i \models_v (\forall x)A \Rightarrow A[x/t]$. Kako su i i v bili proizvoljni, sledi $\models (\forall x)A \Rightarrow A[x/t]$. ∎

Sledeći primer pokazuje da se u prethodnom tvrđenju zahtev da je term t slobodan za x u A ne sme izostaviti.

Primer 2.35 Posmatrajmo formulu $(\forall x)A$ gde je A formula $(\exists y)\alpha(x, y)$. Ako u A zamenimo promenljivu x termom y, dobijamo formulu $(\exists y)\alpha(y, y)$. Formula $(\forall x)A \Rightarrow A[x/t]$ se tada svodi na

$$(\forall x)(\exists y)\alpha(x, y) \Rightarrow (\exists y)\alpha(y, y).$$

Interpretirajmo ovu formulu na skupu prirodnih brojeva i uzmimo za relaciju α relaciju strogog poretka $<$. Tada pretpostavka formule važi, jer za svaki prirodan broj n postoji broj m tako da $n < m$, ali zaključak ne važi jer ne postoji prirodan broj n tako da je $n < n$. Prema tome, formula *nije valjana.* Do ovoga je došlo zbog toga što je promenljiva y zamenom za x postala vezana, što znači da term y nije slobodan za promenljivu x u formuli A. △

2.5 Predikatski račun kao formalna teorija

Predikatski račun prvog reda se može zadati kao formalna teorija

$$\mathcal{K} = (\mathcal{S}, For, Ax, P)$$

gde je

- $\mathcal{S}$ azbuka sastavljena od promenljivih, konstanti, operacijskih i relacijskih slova, logičih veznika $\Rightarrow$ i $\neg$ i znakova $\forall$, (,) (odeljak 2.1);
- *For* formule koje se grade na način opisan u 2.1 pri čemu se kao logički veznici koriste samo $\neg$ i $\Rightarrow$ a od kvantifikatora samo $\forall$;
- *Ax* skup aksioma datih pomoću sledećih 5 shema-aksioma:

  1. $A \Rightarrow (B \Rightarrow A)$

2. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
3. $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$
4. $(\forall x)(A \Rightarrow B(x)) \Rightarrow (A \Rightarrow (\forall x)B)$, ako x nije slobodna promenljiva formule A;
5. $(\forall x)A(x) \Rightarrow A(t)$ gde je t proizvoljan term slobodan za x u formuli $A(x)$.

Primetimo da sheme-aksiome 1–3 odgovaraju shema-aksiomama formalne teorije iskaznog računa $\mathcal{L}$.

$P = \{MP, GEN\}$ skup pravila izvođenja:

$$MP: \quad \frac{A, A \Rightarrow B}{B}$$

$$GEN: \quad \frac{A}{(\forall x)A}$$

Pojmovi teoreme i sintaksne posledice se za predikatski račun uvode kao i za svaku formalnu teoriju (definicija 1.58).

Tvrđenje 2.36 (O izvodu teorema iskaznog računa $\mathcal{L}$) *Ako* $\vdash_{\mathcal{L}} A(q_1, \ldots, q_n)$ *onda* $\vdash_{\mathcal{K}} A(B_1, \ldots, B_n)$ *gde je* $A(B_1, \ldots, B_n)$ *formula predikatskog računa dobijena zamenom iskaznih slova* $q_1, \ldots, q_n$ *redom predikatskim formulama* $B_1, \ldots, B_n$.

Dokaz. Neka $\vdash_{\mathcal{L}} A(q_1, \ldots, q_n)$. Tada postoji dokaz $A_1, \ldots, A_k$ u $\mathcal{L}$ tako da je A_k formula $A(q_1, \ldots, q_n)$. Zamenimo u tom dokazu promenljive $q_1, \ldots, q_n$ redom formulama $B_1, \ldots, B_n$ predikatskog računa. Ostale promenljive koje se javljaju u formulama dokaza $A_1, \ldots, A_k$ zamenimo proizvoljnim formulama predikatskog računa tako da iste promenljive zamenimo istim formulama. Pokazaćemo da je dobijen niz formula $B_1, \ldots, B_k$ je dokaz u $\mathcal{K}$. Neka je B_i proizvoljna formula niza $B_1, \ldots, B_k$. Pošto je A_i formula u dokazu $A_1, \ldots, A_k$, ona je ili aksioma u $\mathcal{L}$ ili je dobijena primenom *MP* na prethodne formule u nizu. Ako je A_i aksioma u $\mathcal{L}$, tada je B_i aksioma u $\mathcal{K}$ jer za svaku shemu-aksiomu u $\mathcal{L}$ postoji odgovarajuća shema u $\mathcal{K}$. Ako je A_i dobijena primenom *MP* na formule A_r i A_s za $r, s < i$ tada se i B_i može dobiti primenom *MP* u predikatskom računu na formule B_r i B_s. Dakle sve formule niza B_i su ili aksiome teorije $\mathcal{K}$, ili dobijene primenom *MP* na prethodne u nizu, pa je $B_1, \ldots, B_k$ dokaz u $\mathcal{K}$. Zato je B_k tj. $A(B_1, \ldots, B_n)$ teorema predikatskog računa $\mathcal{K}$. ■

Tvrđenje 2.37 (Gedela o potpunosti) $\vdash_{\mathcal{K}} A$ *akko* $\models A$.

Dokaz. $\Rightarrow$): Indukcijom po dužini izvođenja za A. Ako je A instanca shema-aksioma 1, 2 ili 3, tada je ona izvod tautologije, pa važi $\models A$. Ako je A aksioma 4, tada $\models A$ prema valjanoj formuli 2.14 (odeljak 2.3). Ako je A instanca aksiome 5, tada prema tvrđenju 2.34 važi $\models A$. Dakle aksiome su valjane formule. Ukoliko A ima izvođenje dužine 1, tada je A aksioma, pa je valjana. Pretpostavimo da su sve formule koje imaju izvođenje dužine manje od n valjane. Neka je A proizvoljna formula koja ima izvođenje dužine n. Tada je ona aksioma, dobijena primenom pravila *MP*, ili dobijena primenom pravila *GEN* na prethodne formule u nizu.

1. Ukoliko je A aksioma, tada prema prethodnom razmatranju važi $\models A$.
2. Ukoliko je A dobijena primenom pravila *MP* na formule B i $B \Rightarrow A$ tada B i $B \Rightarrow A$ imaju izvođenje dužine manje od n, pa prema induktivnoj hipotezi važi $\models B$ i $\models B \Rightarrow A$. Prema tvrđenju 2.28 tada $\models A$.
3. Ukoliko je A dobijena primenom pravila *GEN* tada je A oblika $(\forall x)B$ gde je B jedna od prethodnih formula u nizu. B ima izvođenje dužine manje od n, pa po induktivnoj hipotezi $\models B$. Tada prema tvrđenju 2.29 važi $\models (\forall x)B$ tj. $\models A$.

$\Leftarrow$): Videti [EM]. ∎

Tvrđenje 2.38 *$\mathcal{K}$ nije odlučiva formalna teorija.*

Dokaz. Videti npr. [EM]. ∎

Tvrđenje 2.39 *$\mathcal{K}$ je neprotivrečan (ne postoji formula A tako da su A i $\neg A$ teoreme predikatskog računa $\mathcal{K}$).*

Dokaz. Definišemo "brišuću funkciju" f koja preslikava formule predikatskog računa $\mathcal{K}$ u formule iskaznog računa $\mathcal{L}$. Različitim relacijskim slovima R_i^j ćemo pridružiti različita iskazna slova p_k. To možemo uraditi jer relacijskih simbola ima najviše prebrojivo mnogo, a iskaznih slova ima prebrojivo mnogo. Sada definišemo

$$\begin{aligned} f(R_i^j(t_1,\ldots,t_j)) &= p_k \\ f((\forall x)A) &= f(A) \\ f(A \Rightarrow B) &= (f(A) \Rightarrow f(B)) \\ f(\neg A) &= \neg f(A). \end{aligned}$$

Lema 2.40 *Ako $\vdash_{\mathcal{K}} A$ tada $\vdash_{\mathcal{L}} f(A)$.*

Dokaz. Dokaz sprovodimo indukcijom po dužini izvođenja n za formulu A. Neka je A formula predikatskog računa. Ukoliko je A instanca $Ax1$, $Ax2$ ili $Ax3$ tada je $f(A)$ instanca $Ax1$, $Ax2$ odnosno $Ax3$ iskaznog računa. Ukoliko je A instanca $Ax4$, tada je ona oblika $(\forall x)(B \Rightarrow C) \Rightarrow (B \Rightarrow (\forall x)C)$, pa je $f(A) = (f(B) \Rightarrow f(C)) \Rightarrow (f(B) \Rightarrow f(C))$ po definiciji preslikavanja f, a to je teorema u $\mathcal{L}$ na osnovu tvrđenja 1.65. Ako je A

instanca $Ax5$ tada je ona oblika $(\forall x)B(x) \Rightarrow B(t)$. Kako zamenom terma t umesto promenljive x menjamo samo unutrašnju strukturu elementarnih formula unutar formule B, a ona se funkcijom f zanemaruje, imamo $f(A) = f(B \Rightarrow B)$, što je teorema u $\mathcal{L}$.

Ako je $n = 1$, tada je A aksioma, pa prema prethodnom razmatranju $\vdash_{\mathcal{L}} f(A)$. Pretpostavimo da tvrđenje važi za svako $k < n$, gde je $n > 1$. Neka postoji izvođenja $A_1, \ldots, A_n$ za formulu A u $\mathcal{K}$. Tada je A aksioma ili dobijena primenom pravila izvođenja na prethodne u nizu. Ukoliko je A aksioma, tada na osnovu prethodnog razmatranja $\vdash_{\mathcal{L}} f(A)$. Ukoliko je A dobijena primenom *MP* na prethodne formule u nizu, tada postoje formule B i $B \Rightarrow A$ koje imaju dokaz dužine manje od n. Za njih važi induktivna hipoteza, pa $\vdash_{\mathcal{L}} f(B \Rightarrow A)$ i $\vdash_{\mathcal{L}} f(B)$. No kako je $f(B \Rightarrow A) = (f(B) \Rightarrow f(A))$, primenom pravila *MP* za $\mathcal{L}$ sledi $\vdash_{\mathcal{L}} f(A)$. Ukoliko je A dobijena pravilom *GEN* tada je ona oblika $(\forall x)B$ i B ima izvođenje dužine manje od n, pa je $\vdash_{\mathcal{L}} f(B)$. Kako je $f(A) = f(B)$, trivijalno dobijamo $\vdash_{\mathcal{L}} f(A)$. Time je dokaz leme završen. ∎

Pretpostavimo sada da $\vdash_{\mathcal{K}} A$ i $\vdash_{\mathcal{K}} \neg A$. Tada $\vdash_{\mathcal{L}} f(A)$ i $\vdash_{\mathcal{L}} f(\neg A)$ tj. $\vdash_{\mathcal{L}} \neg f(A)$. No to je u suprotnosti sa neprotivrečnošću iskaznog računa $\mathcal{L}$ (tvrđenje 1.80). Dakle $\mathcal{K}$ je neprotivrečan. ∎

Tvrđenje 2.41 (Tvrđenje dedukcije za $\mathcal{K}$) *Ako je $\mathcal{F}$ skup formula predikatskog računa i A* zatvorena *formula, tada*

$$\mathcal{F}, A \vdash_{\mathcal{K}} B \text{ akko } \mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow B.$$

Dokaz. Ako $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow B$, tada primenom *MP* direktno dobijamo $\mathcal{F}, A \vdash_{\mathcal{K}} B$. Dokazujemo suprotan smer: ako $\mathcal{F}, A \vdash_{\mathcal{K}} B$ onda i $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow B$. Dokaz sprovodimo indukcijom po dužini izvođenja n formule B iz formula $\mathcal{F}$, A. Ukoliko je B aksioma ili iz $\mathcal{F}$, tada primenom $Ax1$ imamo $\vdash_{\mathcal{K}} A \Rightarrow B$. Ukoliko je B baš A tada je $A \Rightarrow A$ izvod tautologije, pa je teorema u $\mathcal{K}$. Za $n = 1$ su to jedine mogućnosti, pa tvrđenje važi za $n = 1$. Neka je $n > 1$ i neka tvrđenje važi za svako $k < n$. Neka je B proizvoljna formula takva da postoji izvođenje iz $\mathcal{F} \cup \{A\}$ u n koraka. Mogu nastupiti sledeći slučajevi.

1. B je aksioma, $B \in \mathcal{F}$ ili B je A. Tada na osnovu prethodnog razmatranja $\vdash_{\mathcal{K}} A \Rightarrow B$.
2. B je dobijena primenom pravila *MP* na prethodne formule u nizu, neka su to formule C i $C \Rightarrow B$. Tada $\mathcal{F}, A \vdash_{\mathcal{K}} C$ i $\mathcal{F}, A \vdash_{\mathcal{K}} C \Rightarrow B$ i pri tome su izvođenja dužine manje od n. Prema induktivnoj hipotezi, tada $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow C$ i $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow (C \Rightarrow B)$. Prema $Ax3$ važi

$$\vdash_{\mathcal{K}} (A \Rightarrow (C \Rightarrow B)) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow B)).$$

Odatle primenom dva puta pravila *MP* dobijamo $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow B$.

3. B je dobijena primenom pravila *GEN*. Tada je B oblika $(\forall x)C$ gde je C jedna od prethodnih formula u nizu. Za C važi induktivna hipoteza, pa $\mathcal{F} \vdash_{\mathcal{K}} A \Rightarrow C$. Tada postoji izvođenje iz $\mathcal{F}$ formule $A \Rightarrow C$, neka je to $D_1, \ldots, D_k$. Posmatrajmo niz

$$\begin{array}{rll} 1. & D_1 & \\ 2. & D_2 & \\ \vdots & & \\ k. & A \Rightarrow C & \\ (k+1). & (\forall x)(A \Rightarrow C) & GEN(k) \\ (k+2). & (\forall x)(A \Rightarrow C) \Rightarrow (A \Rightarrow (\forall x)C) & Ax4 \\ (k+3). & A \Rightarrow (\forall x)C & MP(k+1, k+2) \end{array}$$

On predstavlja izvođenja formule $A \Rightarrow B$ iz $\mathcal{F}, A$. Aksiomu 4 smo smeli primeniti jer je A zatvorena formula, pa x nije slobodna promenljiva u A.

■

Napomena 2.42 Prethodno tvrđenje se može uopštiti. Uočimo da smo u 3. slučaju induktivnog koraka koristili samo činjenicu da x nije slobodna promenljiva u formuli A. Zbog toga je dovoljno pretpostaviti da važi $\mathcal{F}, A \vdash_{\mathcal{K}} B$ i pri tome u izvođenju za B nema primene pravila generalizacije po promenljivima koje su slobodne u formuli A. $\diamond$

2.6 Specijalni predikatski račun prvog reda

Azbuka specijalnog predikatskog računa prvog reda sadrži neke od konstanti predikatskog računa (ali ne mora ni jednu), neka operacijska slova predikatskog računa (ali ne mora ni jedno) i bar jedno relacijsko slovo. Formule se formiraju prema pravilima za izgradnju formula predikatskog računa. Skup aksioma se sastoji od aksioma $Ax1$–$Ax5$ predikatskog računa i specijalnih aksioma. Specijalne aksiome predstavljaju proizvoljan podskup skupa formula. Pravila izvođenja su *MP* i *GEN*.

Model za specijalni predikatski račun prvog reda je interpretacija i formula predikatskog računa u kojoj su tačne specijalne aksiome. Pošto su aksiome samog predikatskog računa ($Ax1$–$Ax5$) valjane, one su u svakoj interpretaciji tačne. Pošto pravila izvođenja *MP* i *GEN* čuvaju svojstvo "biti tačan na modelu", sledi da su i sve teoreme koje možemo izvesti u specijalnom predikatskom računu prvog reda tačne u i.

Zavisno od izbora operacijskih i relacijskih slova, konstanti i specijalnih aksioma postoje različiti specijalni predikatski računi. Oni predstavljaju proširenje računa $\mathcal{K}$ i koriste se za aksiomatizaciju matematičkih teorija. Prvi stepen u proširivanju predikatskog računa je aksiomatizacija relacije jednakosti. Tako dobijamo *predikatski račun prvog* *reda sa jednakošću.* Među relacijskim slovima arnosti 2 ističemo znak R_1^2, i radi preglednijeg zapisa formulu oblika $R_1^2(t_1, t_2)$ pišemo kao $t_1 \approx t_2$. Uvodimo sledeće specijalne aksiome (zadate u obliku shema).

$$t_1 \approx t_1$$
$$t_1 \approx t_2 \Rightarrow t_2 \approx t_1$$
$$t_1 \approx t_2 \wedge t_2 \approx t_3 \Rightarrow t_1 \approx t_3$$
$$t_1 \approx t_1' \wedge \cdots \wedge t_n \approx t_n' \Rightarrow f_i^n(t_1, \ldots, t_n) \approx f_i^n(t_1', \ldots, t_n')$$
$$t_1 \approx t_1' \wedge \cdots \wedge t_n \approx t_n' \Rightarrow (R_i^n(t_1, \ldots, t_n) \Rightarrow R_i^n(t_1', \ldots, t_n'))$$

Pri tome su $t_1, \ldots, t_n$ i $t_1', \ldots, t_n'$ proizvoljni termi, f_i^n proizvoljno operacijsko slovo i R_i^n proizvoljno relacijsko slovo, a podrazumevamo da su sve promenljive koje se javljaju u shemama univerzalno kvantifikovane.

Definicija 2.43 Model $i = (D, \varphi)$ predikatskog računa sa jednakošću naziva se *normalan* akko se relacijsko slovo $\approx$ interpretira kao jednakost. *Jednakosno valjane* formule su formule koje su tačne u svim normalnim modelima.

Napomena 2.44 Možemo uočiti tri različita oblika u kojima se javlja jednakost. Prvi oblik je relacijsko slovo $\approx$ arnosti 2 kao *sintaksni objekat* koji ulazi u sastav formula kao nizova simbola. Drugi oblik je jednakost koja predstavlja interpretaciju relacijskog simbola $\approx$. Najzad, u meta teoriji se javlja relacija $\equiv$ kojom se označava identičnost dva objekata. Kako je obično iz konteksta jasno o kojoj jednakosti je reč, koristićemo simbol $=$ u sva tri slučaja. $\diamond$

Tvrđenje 2.45 *Ako A proizvoljna formula i promenljiva y slobodna za x u formuli A, tada su sledeće formule jednakosno valjane:*

$$\begin{array}{ll} 1. & x = y \Rightarrow (A \Rightarrow A[x/y]) \\ 2. & (\forall x)(x = y \Rightarrow A) \Leftrightarrow A[x/y] \\ 3. & (\exists x)(x = y \wedge A) \Leftrightarrow A[x/y] \end{array}$$

U poslednje dve formule "eliminišuše kvantifikatori, tj. dodaje se ekvivalentna formula bez kvantifikatora.

Dokaz.

1. Neka je i proizvoljna interpretacija i v proizvoljna valuacija te interpretacije. Treba da pokažemo da je formula tačna na i za valuaciju v. Razlikujemo dva slučaja.

   (a) $v(x) \neq v(y)$. Tada je $i_v(x = y) = \perp$, pa je cela implikacija tačna.

(b) $v(x) = v(y)$. Pošto je y slobodan za x u A, prema tvrđenju 2.32 važi $i_v(A[x/y]) = i_{v'}(A)$ gde je $v' = v(v(y)/x) = v$, pa je $i_v(A(y)) = i_v(A(x))$. Zbog toga je i $i_v(A \Leftrightarrow A[x/y]) = \top$, pa je implikacija tačna.

2. Neka je i proizvoljna intepretacija i v proizvoljna valuacija te interpretacije. Treba da pokažemo da je formula tačna u valuaciji v. Prema definiciji interpretacije

$$i_v((\forall x)(x = y \Rightarrow A)) = \top \qquad (*)$$

važi akko za svako $d \in D$ za $v' = v(d/x)$ važi

$$i_{v'}(x = y \Rightarrow A) = \top. \qquad (**)$$

Ako je $d \neq v(y)$ tada je $i_v(x = y) = \perp$, pa implikacija važi. Stoga će $(*)$ važiti akko $(**)$ važi za $d = v(y)$, imamo dakle

$$i_v((\forall x)(x = y \Rightarrow A)) = i_{v'}(x = y \Rightarrow A)$$

gde $v' = v(v(y)/x)$. Prema tvrđenju 2.32 važi

$$i_v(A[x/y]) = i_{v(v(y)/x)}(A) = i_{v'}(A).$$

Pošto je $i_{v'}(x = y) = \top$, sledi

$$\begin{aligned} i_v((\forall x)(x = y \Rightarrow A)) &= i_{v'}(x = y \Rightarrow A) \\ &= \top \Rightarrow i_{v'}(A) \\ &= i_{v'}(A) \\ &= i_v(A[x/y]) \end{aligned}$$

pa je cela ekvivalencija tačna.

3. Primenom valjanih formula (2.3) i tautologija na polaznu formulu dobijamo:

$$\begin{aligned} (\exists x)(x = y \wedge A) \Leftrightarrow A[x/y] &\quad \text{akko} \\ \neg(\exists x)(x = y \wedge A) \Leftrightarrow \neg A[x/y] &\quad \text{akko} \\ (\forall x)(\neg x = y \vee \neg A) \Leftrightarrow \neg A[x/y] &\quad \text{akko} \\ (\forall x)(x = y \Rightarrow \neg A) \Leftrightarrow \neg A[x/y]. & \end{aligned}$$

Poslednja formula je posledica 2. dela ovog tvrđenja.

■

Ograničeni kvantifikatori Ako je R proizvoljna relacija za koju po dogovoru pišemo xRy umesto $R(x,y)$ tada je

$$(\forall xRy)A \quad \text{skraćeni zapisa za} \quad (\forall x)(xRy \Rightarrow A),$$

a

$$(\exists xRy)A \quad \text{skraćeni zapisa za} \quad (\exists x)(xRy \wedge A).$$

$(\forall xRy)$ i $(\exists xRy)$ se nazivaju ograničeni kvantifikatori. Neke od valjanih formula se prenose i na ograničene kvantifikatore.

Primer 2.46 Primenom definicije ograničenih kvantifikatora i valjanih formula, dobijamo:

$$\begin{aligned} \neg(\forall xRy)A &\Leftrightarrow \neg(\forall x)(xRy \Rightarrow A) \\ &\Leftrightarrow (\exists x)\neg(xRy \Rightarrow A) \\ &\Leftrightarrow (\exists x)(xRy \wedge \neg A) \\ &\Leftrightarrow (\exists xRy)\neg A \end{aligned}$$

$\triangle$

Ograničeni kvantifikatori se najčešće primenjuju uz relacije $\in$ i $\leq$.

Da bismo iskazali da postoje dva različita objekta koja imaju dato svojstvo, potreban nam je predikatski račun sa jednakošću. Tada činjenicu "postoje (bar) dva različita objekta koja imaju svojstvo A" označavamo formulom

$$(\exists x)(\exists y)(x \neq y \wedge A(x) \wedge A(y)).$$

Analogno se može konstruisati formula koja odgovara svojstvu "postoji k međusobno različitih objekta koji imaju svojstvo A". Tako se u izvesnoj meri može predikatskim računom govoriti o prirodnim brojevima, ali je takav način težak za rad, pa se brojevi uglavnom uvode posebnim konstantama i operacijskim slovima.

Iskaz "postoji tačno jedan objekat koji ima svojstvo A", u oznaci $(\exists_1 x)A(x)$, definišemo kao skraćeni oblik formule

$$(\exists x)(A(x) \wedge (\forall y)(A(y) \Rightarrow y = x))$$

ili njoj ekvivalentne

$$(\exists x)(\forall y)(A(y) \Leftrightarrow y = x).$$

2.7 Tvrdjenje Erbrana

2.7.1 Semantička posledica

Slično kao u iskaznom računu definišemo pojam semantičke posledice. Ukoliko je formula predikatskog računa A tačna u interpretaciji i kažemo da je i model za A.

Definicija 2.47 Interpretacija i je model *skupa formula* $\mathcal{A}$ predikatskog računa akko je i model za svaku formulu skupa $\mathcal{A}$.

Definicija 2.48 $\mathcal{A} \models B$ akko je svaka interpretacija koja je model za $\mathcal{A}$ model i za B.

Tvrđenje 2.49 *Neka je $\mathcal{A}$ skup zatvorenih formula predikatskog računa prvog reda i B zatvorena formula. Tada $\mathcal{A} \models B$ akko skup $\mathcal{A} \cup \{\neg B\}$ nema model.*

Dokaz. $\Rightarrow$): Neka $\mathcal{A} \models B$. Neka je i proizvoljna interpretacija. Ako i nije model za $\mathcal{A}$ onda nije model ni za $\mathcal{A} \cup \{\neg B\}$. Ako i jeste model za $\mathcal{A}$, onda je i model i za B, pa i nije model za $\neg B$, pa opet i nije model za $\mathcal{A} \cup \{\neg B\}$.

$\Leftarrow$): Neka skup $\mathcal{A} \cup \{\neg B\}$ nema model. Neka je i model za $\mathcal{A}$. Pošto i nije model za $\mathcal{A} \cup \{\neg B\}$, mora biti $i(\neg B) = \bot$. Tada je $i(B) = \top$. Kako je i bila proizvoljna interpretacija, važi $\mathcal{A} \models B$. ∎

Posledica prethodnog tvrđenja je da je zatvorena formula B valjana akko skup $\{\neg B\}$ nema model. Time je problem ispitivanja semantičke posledice i valjanosti sveden na egzistenciju modela skupa formula. Zahtev da je B zatvorena formula ne predstavlja ograničenje, jer uvek možemo posmatrati univerzalno zatvorenje formule B, u oznaci $\forall B$, koje se dobija dopisivanjem ispred formule B kvantifikatora $\forall x$ za svaku promenljivu x koja je slobodna u B. Iz tvrđenja 2.29 sledi da je valjanost formula B i $\forall B$ ekvivalentna.

2.7.2 Ekvivalentnost formula

Definicija 2.50 Formula A je ekvivalentna formuli B, u oznaci $A \sim B$, akko za svaku interpretaciju i i svaku valuaciju v te interpretacije važi $i_v(A) = i_v(B)$.

Iz definicije sledi $A \sim B$ akko $\models A \Leftrightarrow B$. Relacija $\sim$ je relacija ekvivalencije na skupu formula. Ona je i saglasna sa logičkim operacijama i kvantifikovanjem, što za posledicu ima sledeće tvrđenje.

Tvrđenje 2.51 *Ako formula $C(A)$ sadrži kao podformulu formulu A i važi $A \sim B$, tada je i $C(A) \sim C(B)$ gde je $C(B)$ dobijena od $C(A)$ zamenom podformule A formulom B.*

Dokaz. Neka važi $A \sim B$. Indukcijom po broju logičkih veznika u formuli C pokazaćemo da tada i $C(A) \sim C(B)$. Uočimo prvo da ako je $C = A$ tada je $C(B) = B$, pa se $C(A) \sim C(B)$ svodi na $A \sim B$, što po pretpostavci važi. Ako je C bez logičkih veznika, tada je ona elementarna formula, pa kako sadrži formulu A mora biti baš $C = A$. Zato u tom slučaju tvrđenje važi. Pretpostavimo da tvrđenje važi za sve formule sa manje od $n > 0$ logičkih veznika. Neka je $C(A)$ proizvoljna formula sa n logičkih veznika koja sadrži A. Prema prethodnom razmatranju, dovoljno je posmatrati slučaj kada $C(A)$ nije A. Prema definiciji formule, razlikujemo sledeće slučajeve.

1. $C(A)$ je $\neg F(A)$. Tada je $C(B)$ oblika $\neg F(B)$, pa po induktivnoj hipotezi važi $F(A) \sim F(B)$. Neka je i proizvoljna interpretacija i v proizvoljna valuacija. Tada
$$\begin{aligned} i_v(C(A)) &= i_v(\neg F(A)) \\ &= \neg i_v(F(A)) \\ &= \neg i_v(F(B)) \\ &= i_v(\neg F(B)) \\ &= i_v(C(B)). \end{aligned}$$
Dakle $C(A) \sim C(B)$.
2. $C(A)$ je $F \Rightarrow E(A)$ ili $F(A) \Rightarrow E$. Neka je npr. $C(A)$ oblika $F \Rightarrow E(A)$ (drugi slučaj se razmatra analogno). Tada je po induktivnoj hipotezi $E(A) \sim E(B)$. Neka je i proizvoljna interpretacija i v proizvoljna valuacija. Tada
$$\begin{aligned} i_v(C(A)) &= i_v(F \Rightarrow E(A)) \\ &= i_v(F) \Rightarrow i_v(E(A)) \\ &= i_v(F) \Rightarrow i_v(E(B)) \\ &= i_v(F \Rightarrow E(B)) \\ &= i_v(C(B)), \end{aligned}$$
pa važi $C(A) \sim C(B)$.
3. $C(A)$ je oblika $E \wedge F$, $E \vee F$ ili $E \Leftrightarrow F$. Ovi slučajevi su analogni prethodnom.
4. $C(A)$ je $(\forall x)E(A)$. Neka je $i = (D, \varphi)$ proizvoljna interpretacija i v proizvoljna valuacija. Neka je $d \in D$ proizvoljno i neka je $v' = v(d/x)$. Po induktivnoj hipotezi $E(A) \sim E(B)$, pa važi $i_{v'}(E(A)) = i_{v'}(E(B))$. Zato imamo
$$\begin{aligned} i_v(C(A)) = \top \quad &\text{akko} \quad i_v((\forall x)E(A)) = \top \\ &\text{akko} \quad \text{za svako } d \in D \text{ važi } i_{v'}(E(A)) = \top \\ &\text{akko} \quad \text{za svako } d \in D \text{ važi } i_{v'}(E(B)) = \top \\ &\text{akko} \quad i_v((\forall x)E(B)) = \top \\ &\text{akko} \quad i_v(C(B)) = \top, \end{aligned}$$
tj. $i_v(C(A)) = i_v(C(B))$. Prema tome, $C(A) \sim C(B)$.

5. $C(A)$ je $(\exists x)E(A)$. Ovaj slučaj je analogan prethodnom.

■

Ovo tvrđenje nam omogućava da formuli čija nas valjanost zanima proizvoljne podformule zamenjujemo njima ekvivalentnim, a da se valjanost formule ne menja. Takav postupak nazivamo ekvivalencijska transformacija.

2.7.3 Preneksni oblik formule

Za formulu A kažemo da je u *preneksnom obliku* ako je ona oblika

$$(Q_1 y_1)(Q_2 y_2)\dots(Q_n y_n)B$$

gde su $y_1, \dots, y_n$ različite promenljive, $Q_1, \dots, Q_n$ kvantifikatori, a B je formula bez kvantifikatora. Za B kažemo da je *matrica* formule A.

Tvrđenje 2.52 (O preneksnom obliku) *Za svaku formulu A predikatskog računa prvog reda postoji njoj ekvivalentna formula A' koja je u preneksnom obliku.*

Dokaz. Opisaćemo postupak kojim se svaka formula predikatskog računa pretvara u njoj ekvivalentnu formulu koja sadrži samo veznike $\wedge$, $\vee$ i $\neg$ i nalazi se u preneksnom obliku. Pri tome primenjujemo ekvivalencijske transformacije (navedene ekvivalencije treba primenjivati s leva na desno).

1. Uklanjaju se veznici $\Leftrightarrow$ i $\Rightarrow$ primenom formula
   (a) $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$ i
   (b) $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$.

   Posle primene ovog koraka formula sadrži samo veznike $\wedge$, $\vee$ i $\neg$.
2. Vrši se reimenovanje vezanih promenljivih tako da uz svaki kvantifikator stoji različita promenljiva, formulama
   (a) $(\forall x)A(x) \Leftrightarrow (\forall y)A(y)$ i
   (b) $(\exists x)A(x) \Leftrightarrow (\exists y)A(y)$

   gde je y nova promenljiva.
3. Kvantifikatori se pomeraju s desna na levo pomoću formula
   (a) $\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$;
   (b) $\neg(\forall x)A(x) \Leftrightarrow (\exists x)\neg A(x)$;
   (c) $\neg\neg A \Leftrightarrow A$;
   (d) $(C \vee (\forall x)A(x)) \Leftrightarrow (\forall x)(C \vee A(x))$;

(e) $(C \vee (\exists x)A(x)) \Leftrightarrow (\exists x)(C \vee A(x))$;

(f) $((\forall x)A(x) \vee C) \Leftrightarrow (\forall x)(A(x) \vee C)$;

(g) $((\exists x)A(x) \vee C) \Leftrightarrow (\exists x)(A(x) \vee C)$;

(h) $(C \wedge (\forall x)A(x)) \Leftrightarrow (\forall x)(C \wedge A(x))$;

(i) $(C \wedge (\exists x)A(x)) \Leftrightarrow (\exists x)(C \wedge A(x))$;

(j) $((\forall x)A(x) \wedge C) \Leftrightarrow (\forall x)(A(x) \wedge C)$;

(k) $((\exists x)A(x) \wedge C) \Leftrightarrow (\exists x)(A(x) \wedge C)$;

pri čemu promenljiva x nije slobodna u formuli C (ovaj uslov uvek možemo ostvariti primenom transformacija iz prethodnog koraka). Ako formula nije u preneksnom obliku tada uvek možemo primeniti bar jednu od transformacija iz ove grupe, dovoljno je posmatrati kontekst u kom se kvantifikator javlja da bismo odredili koju formulu možemo primeniti. Sa druge strane, primenom svake od ovih transformacija zbir brojeva simbola koji se nalaze levo od kvantifikatorā se smanjuje. Kako je taj broj konačan, zaključujemo da primenom ovih pravila u konačnom broju koraka dolazimo do formule u obliku $(Q_1 y_1)\dots(Q_n y_n)\,B$. Primenom valjane formule $(\forall x)A \Leftrightarrow A$ za $x \notin FV(A)$ dobijamo formulu u preneksnom obliku.

■

Primer 2.53 Nađimo preneksni oblik formule

$$(\forall x)\alpha(x) \Rightarrow (\exists y)\beta(y).$$

Primenom postupka opisanog u prethodnom tvrđenju, dobijamo redom sledeće formule:

$\neg(\forall x)\alpha(x) \vee (\exists y)\beta(y)$

$(\exists x)\neg\alpha(x) \vee (\exists y)\beta(y)$

$(\exists x)(\neg\alpha(x) \vee (\exists y)\beta(y))$

$(\exists x)(\exists y)(\neg\alpha(x) \vee \beta(y))$

Poslednja formula se nalazi u preneksnom obliku. $\triangle$

Napomena 2.54 Posmatrajmo formulu u preneksnom obliku

$$(Q_1 y_1)(Q_2 y_2)\dots(Q_n y_n)B$$

gde je B formula bez kvantifikatora. B se sastoji od elementarnih formula povezanih logičkim veznicima. U odeljku 1.5.3 navedene su tautologije kojima se proizvoljna iskazna formula transformiše u njoj ekvivalentnu koja se nalazi u konjunktivnoj normalnoj formi. Analogno tom postupku, primenjujući izvode istih tautologija možemo naći formulu B' koja je ekvivalentna formuli B i nalazi se u konjunktivnoj kanonskoj formi:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

gde su $C_1, \ldots, C_n$ formule oblika

$$L_1 \vee L_2 \vee \cdots \vee L_k$$

pri čemu su L_i elementarne formule ili njihove negacije. Formule L_i se nazivaju *literali*, a formule C_i *klauze*. Ponekad je pogodno klauze prikazati u obliku implikacije:

$$L_{i_1} \wedge L_{i_2} \cdots \wedge L_{i_s} \Rightarrow L_{j_1} \vee L_{j_2} \vee \ldots \vee L_{j_t}$$

koja se dobija grupisanjem negiranih elementarnih formula sa leve strane, a nenegiranih elementarnih formula sa desne strane implikacije. $\diamond$

Identiteti i kvazi-identiteti Kvazi-identitet je formula oblika

$$(\forall x_1)(\forall x_2)\cdots(\forall x_n)(t_1 = t'_1 \wedge \cdots \wedge t_k = t'_k \Rightarrow u = v)$$

gde su $t_1, \ldots, t_k, t'_1, \ldots, t'_k$, u i v termi. Identitet je formula oblika

$$(\forall x_1)(\forall x_2)\cdots(\forall x_n)(u = v)$$

gde su u i v termi. Identiteti i kvazi-identiteti igraju veliku ulogu u algebri.

2.7.4 Skolemizacija

Neka je formula A u preneksnom obliku:

$$(Q_1 y_1)(Q_2 y_2)\cdots(Q_n y_n)B$$

gde je B formula bez kvantifikatora, a $y_1, \ldots, y_n$ su različite promenljive. Neka su Q_1, $\ldots, Q_{i-1}$ univerzalni kvantifikatori, a Q_i egzistencijalni. Tada formula ima oblik

$$(\forall y_1)\cdots(\forall y_{i-1})(\exists y_i)(Q_{i+1}y_{i+1})\cdots(Q_n y_n)B. \tag{2.15}$$

Neka je f_i^j funkcijsko slovo koje se ne pojavljuje u jeziku kojim je izgrađena formula A. Posmatramo formulu A':

$$(\forall y_1)\cdots(\forall y_{i-1})(Q_{i+1}y_{i+1})\cdots(Q_n y_n)B[y_i/f_j^{i-1}(y_1,\ldots,y_{i-1})]$$

koja ne sadrži promenljivu y_i, a sve pojave y_i su u B zamenjene termom $f_i^j(y_1,\ldots,y_{i-1})$. Ukoliko je $i = 1$ tada promenljivu y_i zamenjujemo novim simbolom konstante. Ovakav postupak ponavljamo dok ne eliminišemo sve egzistencijalne kvantifikatore. Tako dobijamo *otvorenu formulu* formule A, u oznaci A^S. Postupak transformacije A u A^S naziva se skolemizacija (T. Skolem).

Primer 2.55 Navodimo primere nekih formula i odgovarajućih otvorenih formula.

A	A^S
$(\exists x)R(x, f(x))$	$R(a, f(a))$
$(\forall x)(\exists y)R(x, f(y))$	$(\forall x)R(x, f(f_1(x)))$
$(\exists x_1)(\forall x_2)(\exists x_3)(\exists x_4)$ $(P(x_1, x_2) \Rightarrow Q(x_3, x_4))$	$(\forall x_2)(P(a, x_2) \Rightarrow Q(f_2(x_2), f_3(x_2)))$
$(\exists x_1)(\forall x_2)(\exists x_3)(\forall x_4)(\exists x_5)$ $B(x_1, x_2, x_3, x_4, x_5)$	$(\forall x_2)(\forall x_4)B(a, x_2, f_4(x_2), f_5(x_2, x_4))$

Pri tome je a nova oznaka konstante, a f_1, f_2, f_3, f_4 i f_5 nova funkcijska slova. △

Tvrđenje 2.56 *Neka je formula A u preneksnom obliku (2.15). Tada A ima model akko A' ima model.*

Dokaz. Neka je C oznaka za

$$(Q_{i+1}y_{i+1}) \cdots (Q_n y_n)B.$$

a t oznaka za term $f_j^{i-1}(y_1, \ldots, y_{i-1})$ gde je f_j^{i-1} novo funkcijsko slovo.

$\Rightarrow$): Neka je L skup oznaka konstanti, funkcijskih i relacijskih simbola pomoću kojih je izgrađena formula A i neka je $i = (D, \varphi)$ model za A. Tada prema definiciji interpretacije za svaku valuaciju v i za svako $d_1, \ldots, d_{i-1} \in D$ postoji odgovarajuće $d_i \in D$ tako da važi

$$i \models_{v_1} C \tag{2.16}$$

gde je $v_1 = v(d_1/y_1, \ldots, d_i/y_i)$. Tada (prema aksiomi izbora, videti odeljak 3.1) postoji funkcija F takva da $F(d_1, \ldots, d_{i-1}) = d_i$ za svaki niz $d_1, \ldots, d_{i-1}$. Proširimo L novim simbolom f_j^{i-1} i definišimo interpretaciju $i' = (D, \varphi')$ gde je $\varphi'(r) = \varphi(r)$ za $r \in L$, a $\varphi'(f_j^{i-1}) = F$. Pokazaćemo da je i' model za A'.

Neka je v' proizvoljna valuacija interpretacije i'. Prema definiciji interpretacije

$$i' \models_{v'} A'$$

akko za sve $d_1, \ldots, d_{i-1} \in D$ važi

$$i' \models_{v_1'} C[y_i/t] \tag{2.17}$$

gde je $v_1' = v'(d_1/y_1, \ldots, d_{i-1}/y_{i-1})$. Neka su $d_1, \ldots, d_{i-1} \in D$ proizvoljni. Tada je term t slobodan za promenljivu y_i u formuli C jer C ne sadrži kvantifikatore koji stoje uz promenljive $y_1, \ldots, y_{i-1}$. Zato prema tvrđenju 2.32 sledi da (2.17) važi akko

$$i' \models_{v_2'} C \tag{2.18}$$

gde je

$$\begin{aligned} v_2' &= v_1'(t^{i'}[v']/y_i) \\ &= v_1'(F(d_1, \ldots, d_{i-1})/y_i) \\ &= v_1'(d_i/y_i) \\ &= v'(d_1/y_1, \ldots, d_i/y_i). \end{aligned}$$

No s obzirom da C ne sadrži novouvedeno slovo f_j^{i-1}, (2.18) važi akko važi

$$i \models_{v_2'} C,$$

a to sledi iz (2.16) uzimajući $v = v'$. Dakle za svako v' važi $i' \models_{v'} A'$, pa je i' model za A'.

$\Leftarrow$): Neka je $i' = (D, \varphi')$ model za formulu A' i v' proizvoljna valuacija. Tada po definiciji interpretacije za sve $d_1, \ldots, d_{i-1}$ važi

$$i' \models_{v_1'} C[y_i/t]$$

gde je $v_1' = v'(d_1/y_1, \ldots, d_{i-1}/y_{i-1})$. Prema tvrđenju zamene, pošto je t slobodan za y_i u C, važi

$$i' \models_{v_2'} C \tag{2.19}$$

gde je $v_2' = v_1'(t^{i'}[v_1']) = v'(d_1/y_1, \ldots, d_i/y_i)$ za $d_i = t^{i'}[v_1']$. Dakle za proizvoljno d_1, $\ldots, d_{i-1}$ postoji d_i tako da važi (2.19), pa važi

$$i' \models_{v'} (\forall y_1) \cdots (\forall y_{i-1})(\exists y_i) C$$

tj. $i' \models_{v'} A$. Dakle i' je tada model i za A. ■

Tvrđenje 2.57 (Skolem) *Skup formula $\mathcal{F}$ predikatskog računa prvog reda ima model akko skup $\mathcal{F}^S$ ima model gde je $\mathcal{F}^S = \{ A^S \mid A \in \mathcal{F} \}$.*

Dokaz. Primenom prethodnog tvrđenja na sve egzistencijalne kvantifikatore formule A zaključujemo da A ima model akko A^S ima model. Ako imamo proizvoljan skup formula $\mathcal{F}$, tada on ima model akko ima model $\mathcal{F}^S$, gde je $\mathcal{F}^S$ skup elemenata koji su dobijeni skolemizacijom elemenata iz $\mathcal{F}$ tako da za svaku formulu uvodimo različita funkcijska slova i konstante. ■

Primer 2.58 Odredimo otvorenu formulu formule

$$(\forall x)(\exists y)(\forall z)\,(\alpha(x, y) \Rightarrow (\exists u)(\exists v)(\beta(u, z) \wedge \gamma(v))).$$

Prvo formulu dovodimo u preneksni oblik: svedemo sve logičke veznike na $\wedge$, $\vee$ i $\neg$:

$$(\forall x)(\exists y)(\forall z)\,(\neg\alpha(x, y) \vee (\exists u)(\exists v)(\beta(u, z) \wedge \gamma(v)))$$

a zatim izvučemo kvantifikatore $(\exists u)$ i $(\exists v)$:

$$(\forall x)(\exists y)(\forall z)(\exists u)(\exists v)(\neg\alpha(x,y) \vee (\beta(u,z) \wedge \gamma(v))).$$

Elinimišemo kvantifikator $\exists y$ tako što umesto y zamenjujemo term $f(x)$ gde je f novo funkcijsko slovo arnosti 1:

$$(\forall x)(\forall z)(\exists u)(\exists v)(\neg\alpha(x,f(x)) \vee (\beta(u,z) \wedge \gamma(v)))$$

zatim pomoću funkcijsko slova g arnosti 2 eliminišemo $(\exists u)$ tako što umesto u zamenjujemo $g(x,z)$:

$$(\forall x)(\forall z)(\exists v)(\neg\alpha(x,f(x)) \vee (\beta(g(x,z),z) \wedge \gamma(v)))$$

a zatim eliminišemo i v:

$$(\forall x)(\forall z)(\neg\alpha(x,f(x)) \vee (\beta(g(x,z),z) \wedge \gamma(h(x,z)))).$$

Matricu formule možemo dovesti u konjunktivnu normalnu formu, pa dobijamo formulu:

$$(\forall x)(\forall z)((\neg\alpha(x,f(x)) \vee \beta(g(x,z),z)) \wedge (\neg\alpha(x,f(x)) \vee \gamma(h(x,z)))).$$

$\triangle$

2.7.5 Tvrđenje Erbrana

Videli smo da se problem ispitivanja da li $\mathcal{A} \models B$ svodi na egzistenciju modela skupa formula (tvrđenje 2.49). Prema tvrđenju 2.52 dovoljno je posmatrati formule u preneksnom obliku, a prema tvrđenju 2.57 dovoljno je posmatrati preneksne formule bez egzistencijalnih kvantifikatora. Prema tvrđenju 2.29 možemo izostaviti i sve univerzalne kvantifikatore. Tako dobijamo formule bez kvantifikatora koje od logičkih veznika sadrže samo $\wedge$, $\vee$ i $\neg$. Primenom izvoda tautologija iz 1.5.3, formule možemo dovesti u oblik

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

pri čemu su formule C_i oblika

$$L_1 \vee L_2 \vee \cdots \vee L_k$$

a L_j su elementarne formule ili njihove negacije (videti napomenu 2.54). Lako se proverava da za proizvoljnu interpretaciju m važi:

$$m \models A \wedge B \quad \text{akko} \quad m \models A \text{ i } m \models B.$$

Zbog toga možemo sve formule rastaviti na klauze, pa je početni problem ispitivanja semantičke posledice sveden na egzistenciju modela skupa klauza. U nastavku ćemo pokazati da je pri proveri egzistencije modela dovoljno posmatrati specijalne modele koji su prebrojivi.

Primer 2.59 Pretpostavimo da nas zanima da li važi

$$\{(\forall x)(P(x) \Rightarrow (\exists y)Q(x,y)),\ (\exists x)P(x)\} \models (\exists x)(\exists y)Q(x,y).$$

Prema tvrđenju 2.49 to važi akko nema model skup

$$\mathcal{F} = \{(\forall x)(P(x) \Rightarrow (\exists y)Q(x,y)),\ (\exists x)P(x),\ \neg(\exists x)(\exists y)Q(x,y)\}.$$

Eliminisanjem $\Rightarrow$ i spuštanjem znaka $\neg$ dobijamo

$$\{(\forall x)(\neg P(x) \vee (\exists y)Q(x,y)),\ (\exists x)P(x), (\forall x)(\forall y)\neg Q(x,y)\}.$$

Posle izvlačenja kvantifikatora dobijamo formule u preneksnom obliku:

$$\{(\forall x)(\exists y)(\neg P(x) \vee Q(x,y)),\ (\exists x)P(x),\ (\forall x)(\forall y)\neg Q(x,y)\},$$

posle skolemizacije

$$\{(\forall x)(\neg P(x) \vee Q(x,f(x))),\ P(a),\ (\forall x)(\forall y)\neg Q(x,y)\},$$

a uklanjanjem univerzalnih kvantifikatora:

$$\{\neg P(x) \vee Q(x,f(x)),\ P(a),\ \neg Q(x,y)\}.$$

U ovom jednostavnom slučaju nismo morali primeniti svođenje na konjunktivnu normalnu formu jer su formule već u obliku klauza. $\triangle$

Neka je $\mathcal{F}$ proizvoljan skup klauza nad jezikom $L = R \cup F \cup C$, gde je R skup relacijskih slova, F skup operacijskih slova, a C skup znakova konstanti. Skup svih terma nad jezikom L koji ne sadrže promenljive zvaćemo *Erbranov univerzum* (J. Herbrand), i označavati sa *HU*. Skup *HU* se dakle gradi od znakova konstanti i funkcijskih znakova. Ukoliko L ne sadrži ni jednu konstantu, tada uvodimo jednu konstantu a. (Ona ne utiče na egzistenciju modela, jer je domen svake interpretacije po definiciji neprazan, pa ćemo uvek moći da je interpretiramo.) Možemo dakle definisati

$$\begin{aligned}
HU_0 &= C \\
HU_{n+1} &= HU_n \cup \{\, f_i^j(t_1,\dots,t_j) \mid t_1,\dots,t_j \in HU_n, f_i^j \in F \,\} \\
HU &= \bigcup_{n \in N_0} HU_n.
\end{aligned}$$

Erbranov univerzum će igrati ulogu domena prebrojivog modela.

Skup *Erbranovih atoma*, u oznaci *HA*, je skup elementarnih formula nad jezikom L koje ne sadrže promenljive. Dakle

$$HA = \{R_i^j(t_1,\dots,t_j) \mid R_i^j \in R, \quad t_1,\dots,t_j \in HU\}.$$

Posmatraćemo i *Erbranov sistem*, u oznaci *HS* koji predstavlja instance formula skupa $\mathcal{F}$ koje ne sadrže promenljive:

$$\begin{aligned} HS = \{ \ & A(t_1,\ldots,t_n) \mid t_1,\ldots,t_n \in HU, \quad A(y_1,\ldots,y_n) \in \mathcal{F}, \\ & y_1,\ldots,y_n \text{ su sve promenljive formule } A\} \end{aligned}$$

Primer 2.60 Za skup formula $\mathcal{F}$ iz prethodnog primera dobijamo:

$$\begin{aligned} L \ &= R \cup F \cup C \\ & R = \{P, Q\}, \quad F = \{f\}, \quad C = \{a\} \\ HU &= \{a, f(a), f(f(a)), \ldots\} \\ HA &= \{P(a), P(f(a)), \ldots \\ & Q(a,a), Q(a, f(a)), Q(f(a), a), \ldots\} \\ HS \ &= \{\neg P(a) \vee Q(a, f(a)), \neg P(f(a)) \vee Q(f(a), f(f(a))), \ \ldots, \\ & P(a), \\ & \neg Q(a,a), \neg Q(a, f(a)) \ldots\} \end{aligned}$$

$\triangle$

Tvrđenje 2.61 *Neka je $\mathcal{F}$ skup predikatskih klauza. Sledeći uslovi su ekvivalentni:*

1. *$\mathcal{F}$ ima model;*
2. *$\mathcal{F}$ ima model sa domenom HU;*
3. *HS posmatran kao skup iskaznih formula ima model ako se kao iskazna slova posmatraju elementi HA.*

Dokaz. ($1 \Rightarrow 3$): Neka je $M = (D, \varphi)$ model za $\mathcal{F}$. Konstruišemo iskazni model za skup *HS* posmatran kao skup iskaznih formula izgrađenih od promenljivih iz *HA*. Pošto je skup *HA* najviše prebrojiv, postoji preslikavanje $\Phi : HA \rightarrow \{p_1, p_2, \ldots\}$ koje različitim Erbranovim atomima pridružuje različita iskazna slova. Definišemo preslikavanje $\bar{\Phi}$ koje preslikava predikatske formule bez promenljivih u iskazne formule (atomi se posmatraju kao jedinstveni simboli, a predikatski veznici kao odgovarajući iskazni):

$$\begin{aligned} \bar{\Phi}(A) &= \Phi(A) \quad \text{ako je } A \text{ Erbranov atom;} \\ \bar{\Phi}(\neg A) &= \neg\bar{\Phi}(A); \\ \bar{\Phi}(A \vee B) &= \bar{\Phi}(A) \vee \bar{\Phi}(B). \end{aligned}$$

Definišemo valuaciju α za koju ćemo pokazati da je iskazni model za *HS*. Ako iskazno slovo p nije slika ni jedne formule iz *HS*, tada vrednost $\alpha(p)$ stavimo proizvoljnu (te vrednosti ne igraju nikakvu ulogu). Ako je $\bar{\Phi}(A) = p$ za neku formulu $A \in HA$, tada je A jedinstvena, i u tom slučaju stavimo $\alpha(p) = M(A)$. Pokazaćemo da za svaku klauzu A na jeziku L koja ne sadrži promenljive važi $v_\alpha(\bar{\Phi}(A)) = M(A)$. Iz definicije interpretacije sledi da za elementarne formule važi:

$$\begin{aligned} v_\alpha(\bar{\Phi}(R_i^j(t_1,\ldots,t_j))) &= v_\alpha(\Phi(R_i^j(t_1,\ldots,t_j))) \\ &= \alpha(\Phi(R_i^j(t_1,\ldots,t_j))) \\ &= M(R_i^j(t_1,\ldots,t_j)). \end{aligned}$$

Stoga važi i

$$\begin{aligned} v_\alpha(\bar{\Phi}(\neg A)) &= v_\alpha(\neg\bar{\Phi}(R_i^j(t_1,\ldots,t_j))) \\ &= \neg v_\alpha(\bar{\Phi}(R_i^j(t_1,\ldots,t_j))) \\ &= \neg M(R_i^j(t_1,\ldots,t_j)) \\ &= M(\neg R_i^j(t_1,\ldots,t_j)), \end{aligned}$$

što znači da tvrđenje važi za sve literale. Zato za proizvoljnu klauzu $L_1 \vee \cdots \vee L_n$ važi

$$\begin{aligned} v_\alpha(\bar{\Phi}(L_1 \vee \cdots \vee L_n)) &= v_\alpha(\bar{\Phi}(L_1) \vee \cdots \vee \bar{\Phi}(L_n)) \\ &= v_\alpha(\bar{\Phi}(L_1)) \vee \cdots \vee v_\alpha(\bar{\Phi}(L_n)) \\ &= M(L_1) \vee \cdots \vee M(L_n) \\ &= M(L_1 \vee \cdots \vee L_n). \end{aligned}$$

Specijalno, za klauzu $A \in$ *HS* dobijamo $v_\alpha(\bar{\Phi}(A)) = M(A)$. Formule iz *HS* su dobijene zamenom slobodnih promenljivih termima koji su slobodni za te promenljive (pošto formule iz $\mathcal{F}$ nemaju kvantifikatore), a sve formule iz $\mathcal{F}$ su po pretpostavci tačne u interpretaciji M, pa prema tvrđenju 2.34 sledi $M(A) = \top$. Dakle $v_\alpha(\bar{\Phi}(A)) = \top$, pa je α model za A. A je bila proizvoljna formula iz *HS*, pa je α iskazni model za skup formula $\{\bar{\Phi}(A) \mid A \in HS\}$.

($3 \Rightarrow 2$): Neka skup *HS* ima iskazni model α sa iskaznim promenljivima iz *HA* tj. neka postoji preslikavanje $\bar{\Phi}$ definisano kao u prethodnom slučaju, koje preslikava formule bez promenljivih nad jezikom L u formule iskaznog računa tako da $\{\bar{\Phi}(A) \mid A \in HS\}$ ima iskazni model. Konstruišemo model $H = (HU, \rho)$ gde je *HU* Erbranov univerzum, a ρ je definisano na sledeći način:

$$\begin{aligned} \rho(c) &= c \quad \text{ako} \quad c \in C \\ \rho(f_k^j) &= \bar{f}_k^j \text{ gde je } \bar{f}_k^j(t_1,\ldots,t_j) = f_k^j(t_1,\ldots,t_j) \\ & \quad \text{za sve } t_1,\ldots,t_j \in HU \\ \rho(R_k^j) &= \bar{R}_k^j \quad \text{gde} \quad \bar{R}_k^j(t_1,\ldots,t_j) \text{ akko } \alpha(\bar{\Phi}(R_k^j(t_1,\ldots,t_j))) = \top. \end{aligned}$$

Neka je $A(y_1,\ldots,y_n) \in \mathcal{F}$ proizvoljna formula pri čemu su $y_1,\ldots,y_n$ sve promenljive formule A. Neka je v proizvoljna valuacija interpretacije H. Treba da dokažemo $H \models_v A$. Označimo

$$A_H = A(v(y_1),\ldots,v(y_n)).$$

Formula A_H je dobijena je zamenom svih slobodnih promenljivih formule A termima $v(y_1), \ldots, v(y_n)$. Dakle $A_H \in$ *HS*. Zato A_H nema promenljivih i njena tačnost u interpretaciji H ne zavisi od valuacije. Neka je stoga v_1 neka valuacija interpretacije H. Kako A nema kvantifikatore, svi termi su slobodni za sve promenljive, pa prema tvrđenju 2.32 važi

$$H \models_{v_1} A_H \quad \text{akko} \quad H \models_{v_2} A$$

gde je $v_2 = v_1(v(y_1)/y_1, \ldots, v(y_n)/y_n)$. Valuacije v_2 i v se poklapaju za sve vrednosti promenljivih koje učestvuju u formuli A, pa važi

$$H \models_{v_2} A \quad \text{akko} \quad H \models_v A.$$

Pošto izbor valuacije v_1 ne utiče na tačnost A_H, imamo

$$H \models A_H \quad \text{akko} \quad H \models_{v_1} A_H \quad \text{akko} \quad H \models_v A.$$

Pokazaćemo da važi $H(A_H) = v_\alpha(\bar{\Phi}(A_H))$. Uočimo prvo da za elementarnu formulu $R_k^j(t_1, \ldots, t_j) \in$ *HS* prema konstrukciji interpretacije H važi:

$$\begin{array}{rl} H \models R_k^j(t_1, \ldots, t_j) & \text{akko} \quad \bar{R}_k^j(t_1^H, \ldots, t_j^H) \\ & \text{akko} \quad \bar{R}_k^j(t_1, \ldots, t_j) \\ & \text{akko} \quad v_\alpha(\bar{\Phi}(R_k^j(t_1, \ldots, t_j))) = \top. \end{array}$$

Dakle $H(R_k^j(t_1, \ldots, t_j)) = v_\alpha(\bar{\Phi}(R_k^j(t_1, \ldots, t_j)))$. Odatle sledi i

$$\begin{array}{rcl} H(\neg R_k^j(t_1, \ldots, t_j)) & = & \neg H(R_k^j(t_1, \ldots, t_j)) \\ & = & \neg v_\alpha(\bar{\Phi}(R_k^j(t_1, \ldots, t_j))) \\ & = & v_\alpha(\neg \bar{\Phi}(R_k^j(t_1, \ldots, t_j))) \\ & = & v_\alpha(\bar{\Phi}(\neg R_k^j(t_1, \ldots, t_j))), \end{array}$$

što znači da tvrđenje važi za sve literale, pa i za proizvoljnu klauzu $L_1 \vee \cdots \vee L_n$ važi

$$\begin{array}{rcl} H(L_1 \vee \cdots \vee L_n) & = & H(L_1) \vee \cdots \vee H(L_n) \\ & = & v_\alpha(\bar{\Phi}(L_1)) \vee \cdots \vee v_\alpha(\bar{\Phi}(L_n)) \\ & = & v_\alpha(\bar{\Phi}(L_1) \vee \cdots \vee \bar{\Phi}(L_n)) \\ & = & v_\alpha(\bar{\Phi}(L_1 \vee \cdots \vee L_n)). \end{array}$$

Kako je formula A_H klauza, dobijamo $H(A_H) = v_\alpha(\bar{\Phi}(A_H)) = \top$, jer je $A_H \in$ *HS*, a α je model za *HS*. Dakle pokazali smo:

$$H_v(A) = H(A_H) = v_\alpha(\bar{\Phi}(A_H)) = \top.$$

Kako je v bila proizvoljna valuacija, zaključujemo $H(A) = \top$. A je bila proizvoljna formula iz $\mathcal{F}$, pa je H model za $\mathcal{F}$.

($2 \Rightarrow 1$): Ovaj smer važi jer je model sa domenom *HU* jedan model za $\mathcal{F}$. ∎

Primer 2.62 Preslikavanja Φ koje odgovara prethodnom primeru ima oblik

$$\Phi = \begin{pmatrix} P(a) & P(f(a)) & \dots & Q(a,a) & Q(a,f(a)) & Q(f(a),f(f(a)))\dots \\ p_1 & p_2 & & q_1 & q_2 & q_3 \end{pmatrix},$$

a skup *HS* posmatran kao skup iskaznih formula je

$$\begin{aligned} \bar{\Phi}(HS) &= \{\neg p_1 \vee q_2, \neg p_2 \vee q_3, \dots, \\ & \quad p_1, \dots, \\ & \quad \neg q_1, \neg q_2, \dots\} \end{aligned}$$

Sada vidimo da polazni skup nema model, jer ako je α model za p_1 i za $\neg q_2$, tada ne može biti model za $\neg p_1 \vee q_2$. Tako smo utvrdili da važi:

$$\{(\forall x)(P(x) \Rightarrow (\exists y)Q(x,y)),\ (\exists x)P(x)\} \models (\exists x)(\exists y)Q(x,y).$$

$\triangle$

2.7.6 Neke posledice tvrđenja Erbrana

Tvrđenjem Erbrana se problem utvrđivanja semantičke posledice (pa i valjanosti formule) svodi na ispitivanje egzistencije iskaznog modela prebrojivog skupa formula. Neka je $\mathcal{S} = \{A_1, A_2, \dots\}$ prebrojiv skup *iskaznih* formula. Prema tvrđenju kompaktnosti, skup $\mathcal{S}$ ima model akko svaki njegov konačan podskup ima model. Posmatrajmo niz konačnih skupova:

$$\begin{aligned} S_1 &= \{A_1\} \\ S_2 &= \{A_1, A_2\} \\ S_3 &= \{A_1, A_2, A_3\} \\ &\vdots \end{aligned}$$

Ako svaki konačan podskup skupa $\mathcal{S}$ ima model, onda i svaki član ovog niza ima model. Obrnuto, ako svaki član ovog niza ima model, onda za proizvoljan konačan podskup $\mathcal{P}$ skupa $\mathcal{S}$ možemo naći član ovog niza koji sadrži $\mathcal{P}$, pa i $\mathcal{P}$ ima model. Iz toga sledi da postoji sledeći postupak koji za svaki skup iskaznih formula koji nema model utvrđuje da taj skup nema model: redom se generišu skupovi $\mathcal{S}_1, \mathcal{S}_2, \dots$ i za svaki od tih skupova se proverava da li ima model (na primer tako što se ispitaju sve moguće vrednosti koje valuacija može dodeliti konačnom broju promenljivih koje učestvuju u formulama tog skupa). Ukoliko neki skup $\mathcal{S}_i$ nema model, tada ni ceo skup $\mathcal{S}$ nema model. Obrnuto, ako skup $\mathcal{S}$ nema model, tada će se sigurno u nekom trenutku vremena pronaći podskup $\mathcal{S}_i$ koji nema model, pa će se to konstatovati.

Opisan postupak omogućava da se utvrdi da je data formula valjana. Ako je formula valjana, tada odgovarajući skup iskaznih formula nema model, pa će se to u konačnom broju koraka opisanim postupkom utvrditi. Ali ako formula nije valjana, tada se nikad neće pronaći konačan podskup koji nema model. Tada proces provere da li je formula valjana ne mora da se završi u konačnom broju koraka. To je posledica neodlučivosti predikatskog računa.

2.7.7 Postupak rezolucije

Postupak za proveru valjanosti formule opisan u prethodnom odeljku je vrlo neefikasan. Efikasniji postupak od opisanog je postupak *rezolucije* (videti npr. [HLCP], [JR], [PHIP]). To je jedan od postupaka koji se primenjuju u automatskim dokazivačima teorema, a ograničeni oblik rezolucije primenjuje se kao osnovni mehanizam izvršavanja programa u programskom jeziku Prolog.

Definisaćemo prvo postupak rezolucije u iskaznom računu. Primenom postupka koji je opisan u odeljku 1.5.3, svaka formula iskaznog računa se može napisati u obliku

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

gde su C_i formule oblika

$$L_1 \vee L_2 \vee \cdots \vee L_k$$

pri čemu su L_j iskazna slova ili njihove negacije. Kao i u predikatskom računu, formule L_j nazivamo literali, a formule C_j klauze. Iz asocijativnosti, komutativnosti i idempotentnosti logičke operacije $\vee$ sledi da za istinitosnu vrednost klauze nije bitan redosled literala kao i da se višestruke pojave istog literala mogu izostaviti. Zato klauzu možemo posmatrati kao konačan skup literala

$$\{L_1, L_2, \ldots, L_k\}.$$

Analogno tome, svaku formulu koja predstavlja konjukciju klauza možemo posmatrati kao konačan skup klauza

$$\{C_1, C_2, \ldots, C_n\}.$$

U ovakvoj reprezentaciji, unija dva skupa literala odgovara disjunkciji odgovarajućih klauza. Zato je prirodno da skup $\emptyset$ predstavlja iskaz $\perp$ (kontradikciju). Njega takođe smatramo klauzom i nazivamo *prazna klauza*.

Primer 2.63 Konjunktivna normalna forma formule $(p \Rightarrow q) \vee (r \Rightarrow s)$ je klauza $\neg p \vee q \vee \neg r \vee s$. Zato ovu formulu možemo predstaviti skupom

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

$\triangle$

Ako je $L = q$ iskazno slovo, tada $\bar{L}$ označava literal $\neg q$, a ako je $L = \neg q$, tada $\bar{L}$ označava literal q.

Ako drugačije nije naglašeno, pod klauzama ćemo u nastavku podrazumevati njihove reprezentacije pomoću skupova. Pojmovi interpretacije se na prirodan način sa iskaznih formula prenose i na skupove kojima se te formule predstavljaju.

Sada smo u prilici da definišemo postupak rezulucije u iskaznom računu.

Definicija 2.64 Neka su C_1 i C_2 iskazne klauze. Klauza D je *rezolventa* klauza C_1 i C_2 akko postoji literal L tako da $L \in C_1$, $\bar{L} \in C_2$ i

$$D = (C_1 \setminus \{L\}) \cup (C_2 \setminus \{\bar{L}\}).$$

Primer 2.65 Skup $C_1 = \{\neg p, q\}$ predstavlja formulu $p \Rightarrow q$, a skup $C_2 = \{\neg q, r\}$ formulu $q \Rightarrow r$. Kao $q \in C_1$ i $\neg q \in C_2$, iskazna rezolventa klauza C_1 i C_2 je

$$(\{\neg p, q\} \setminus \{q\}) \cup (\{\neg q, r\} \setminus \{\neg q\}) = \{\neg p\} \cup \{r\} = \{\neg p, r\}$$

a to je klauza koja odgovara formuli $p \Rightarrow r$. $\triangle$

Tvrđenje 2.66 *Neka je $\mathcal{F}$ proizvoljan skup klauza, $C_1, C_2 \in \mathcal{F}$ i neka je D rezolvent klauza C_1 i C_2. Tada $\mathcal{F} \models D$.*

Dokaz. Neka je D rezolvent klauza C_1 i C_2 takav da za literal L važi $L \in C_1$, $\bar{L} \in C_2$ i $D = (C_1 \setminus \{L\}) \cup (C_2 \setminus \{\bar{L}\})$. Neka je α proizvoljna valuacija u kojoj su tačne sve formule skupa $\mathcal{F}$. Razlikujemo dva slučaja.

1. $v_\alpha(L) = \bot$. Pošto je $v_\alpha(C_1) = \top$, mora biti $v_\alpha(C_1 \setminus \{L\}) = \top$. Zato je i $v_\alpha(D) = \top$.

2. $v_\alpha(L) = \top$. Tada je $v_\alpha(\bar{L}) = \bot$, a kako je $v_\alpha(C_2) = \top$, mora biti $v_\alpha(C_2 \setminus \{\bar{L}\}) = \top$. Zato je opet $v_\alpha(D) = \top$.

U svakom slučaju je $v_\alpha(D) = \top$. Kako je α bila proizvoljna valuacija u kojoj su tačne sve formule iz $\mathcal{F}$, sledi $\mathcal{F} \models D$. ∎

Definicija 2.67 *Izvođenje* klauze D iz skupa klauza $\mathcal{F}$ je konačan niz klauza $C_1, C_2, \ldots, C_n$ gde $C_n = D$ i za svako C_k za $1 \leq k \leq n$ važi $C_k \in \mathcal{F}$ ili je C_k rezolventa klauza C_i i C_j za $1 \leq i, j < k$.

Svaki model za skup formula $\mathcal{F}$ je model i za sve formule koje su semantičke posledice skupa $\mathcal{F}$. Ako primenom pravila rezolucije utvrdimo da je prazna klauza posledica skupa formula $\mathcal{F}$, sledi da ni skup $\mathcal{F}$ nema model, jer prazna klauza nema model.

Primenom tvrđenja kompaktnosti za iskazni račun (tvrđenje 1.45) može se pokazati da važi i obrnuto: ako skup formula $\mathcal{F}$ nema model, tada postoji izvođenje prazne klauze iz $\mathcal{F}$ (videti [HLCP]). Posledica toga je sledeće tvrđenje:

Tvrđenje 2.68 *Skup klauza $\mathcal{F}$ nema model akko postoji izvođenje prazne klauze iz skupa $\mathcal{F}$.*

Primer 2.69 Pokažimo postupkom rezolucije da važi

$$\{q,\ p \wedge q \Rightarrow r,\ r \wedge q \Rightarrow p,\ \neg r \Rightarrow p\} \models \{r\}.$$

Ako pretpostavke pretvorimo u klauze i dodamo polaznom skupu negaciju formule r, dobijamo skup S čiji su članovi:

1. $\{q\}$
2. $\{\neg p, \neg q, r\}$
3. $\{\neg r, \neg q, p\}$
4. $\{r, p\}$
5. $\{\neg r\}$.

Sledeći niz klauza predstavlja izvođenje prazne klauze iz skupa S primenom iskazne rezolucije:

6.	$\{\neg p, r\}$	iz $1, 2$
7.	$\{\neg p\}$	iz $5, 6$
8.	$\{r\}$	iz $4, 7$
9.	$\emptyset$	iz $8, 5$

$\triangle$

Tvrđenje 2.68 daje postupak za proveru da li dati skup iskaznih formula ima model. Ako je dat skup *predikatskih* formula, tada bismo mogli postepeno generisati Erbranov sistem i proveravati da li postoji izvođenje prazne klauze iz do sada generisanog skupa. Pokazuje se, međutim, da je to moguće izbeći ako se postupak rezolucije definiše direktno nad *predikatskim* klauzama. Analogno iskaznim klauzama, i predikatske klauze predstavljamo skupovima literala.

Primer 2.70 Neka je F formula

$$(\forall x)(\forall y)\,(\alpha(x,y) \Rightarrow \beta(x) \wedge \gamma(y)).$$

Posle izostavljanja univerzalnih kvantifikatora i eliminacije implikacije, dobijamo formulu

$$\neg\alpha(x,y) \vee (\beta(x) \wedge \gamma(y)).$$

Primenom distributivnosti formulu svodimo na konjunktivnu normalnu formu

$$(\neg\alpha(x,y) \vee \beta(x)) \ \wedge\ (\neg\alpha(x,y) \vee \gamma(y)).$$

Zato formulu F možemo predstaviti skupom klauza

$$\{\,\{\neg\alpha(x,y), \beta(x)\},\ \{\neg\alpha(x,y), \gamma(y)\}\,\}.$$

$\triangle$

Osnovna ideja rezolucije u predikatskom računu je da se koristi predikatska klauza C da bi se predstavio (potencijalno beskonačan) skup svih instanci koje C generiše u Erbranovom sistemu *HS*. Nalaženje rezolventi predikatskih formula C i D tako zamenjuje nalaženje iskaznih rezolventi svih instanci formula C i D. Pre nego što uvedemo pojam rezolucije za predikatske formule uvešćemo pojam zamene i unifikacije.

Prema napomeni 2.9 zamenu možemo tumačiti kao funkciju koja preslikava skup predikatskih formula u skup predikatskih formula. Zamena se primenjuje na klauzu tako što se primeni na svaki njen literal, a na skup klauza tako što se primeni na svaku od klauza u skupu. Primenu zamene θ na formulu ili skup formula A označavamo sa $A\theta$.

Ako su θ i σ dve zamene, tada se može definisati kompozicija zamena $\theta\sigma$ tako da za svaku formulu A važi
$$A(\theta\sigma) = (A\theta)\sigma.$$

Primer 2.71 Neka su date zamene

$$\begin{aligned} \theta &= [x/f(a), y/g(z,a)] \\ \sigma &= [z/h(b)]. \end{aligned}$$

Kompozicija ovih zamena je

$$\theta\sigma = [x/f(a), y/g(h(b),a), z/h(b)].$$

U ovom slučaju su promenljive koje se javljaju u θ i σ različite, pa se rezultat kompozicije lako nalazi. U opštem slučaju treba voditi računa o zajedničkim promenljivim da bi kompozicija imala traženo svojstvo $A(\theta\sigma) = (A\theta)\sigma$ za svaku formulu A. $\triangle$

Definicija 2.72 Zamena θ je *unifikator* formula A i B akko važi

$$A\theta = B\theta$$

Primer 2.73 Unifikator formule $A = \alpha(f(x), a)$ i $B = \alpha(f(g(b)), y)$ je zamena $\theta = [x/g(b), y/a]$, jer je
$$A\theta = B\theta = \alpha(f(g(b)), a).$$

Zamena $\sigma = [x/y]$ je unifikator formula $A = \alpha(f(a), x)$ i $B = \beta(f(a), y)$. Unifikator ovih formula je i $\sigma' = [x/a, y/a]$ kao i $\sigma'' = [x/f(a), y/f(a)]$. Primećujemo da formule A i B imaju beskonačno mnogo unifikatora. Tako je za svaku zamenu $\eta = [y/t]$ kompozicija $\sigma\eta$ unifikator za A i B. $\triangle$

Definicija 2.74 Zamena θ je *najopštiji unifikator* formula A i B ako je θ unifikator formula A i B, i za svaki unifikator σ formula A i B postoji zamena τ tako da

$$\sigma = \theta\tau.$$

Može se pokazati da svake dve formule imaju najopštiji unifikator i da se on može efektivno odrediti.

Primer 2.75 Za formule $A = \alpha(f(a), x)$ i $B = \beta(f(a), y)$ iz prethodnog primera najopštiji unifikator je $\sigma = [x/y]$. Unifikator $\bar{\sigma} = [y/x]$ je takođe jedan najopštiji unifikator za A i B. Dakle najopštiji unifikator nije jedinstven. Može se, međutim, pokazati da se najopštiji unifikatori mogu dobiti jedan od drugog reimenovanjem promenljivih (videti [JL]). $\triangle$

Analogno kao kod rezolucije iskaznih formula, sa $\bar{L}$ označavamo predikatski literal $\neg L$ ako je L elementarna formula, odnosno L' ako je $L = \neg L'$ negacija elementarne formule.

Definicija 2.76 Neka su C_1 i C_2 dve klauze koje nemaju zajedničke promenljive, a $L_1 \in C_1$ i $L_2 \in C_2$ proizvoljni literali takvi da L_1 i $\bar{L}_2$ imaju najopštiji unifikator θ. Tada je *binarna rezolventa* klauza C_1 i C_2 klauza

$$(C_1\theta \setminus \{L_1\theta\}) \cup (C_2\theta \setminus \{L_2\theta\}).$$

Primer 2.77 Neka su date klauze

$$C_1 = \{\alpha(x), \beta(x)\} C_2 = \{\neg\alpha(a), \gamma(y)\}.$$

Literali $\alpha(x)$ i $\alpha(a)$ imaju najopštiji unifikator $\theta = [x/a]$, pa je binarna rezolventa klauza C_1 i C_2 klauza

$$\{\beta(x)[x/a]\} \cup \{\gamma(y)[x/a]\} = \{\beta(a), \gamma(y)\}.$$

$\triangle$

Napomena 2.78 Ukoliko dve klauze imaju zajedničke promenljive, tada se promenljive u jednoj od klauza mogu reimenovati da bi se dobile klauze bez zajedničkih promenljivih. Reimenovanjem se dobija ekvivalentna klauza, jer nas zanima samo da li klauze važe u datoj interpretaciji, što znači da se sve promenljive ponašaju kao da su univerzalno kvantifikovane. $\diamond$

Definicija 2.79 Neka je C proizvoljna klauza i $L_1, L_2 \in C$ dva proizvoljna literala te klauze koja imaju najopštiji unifikator θ. Tada se $C\theta$ naziva *faktor klauze* C.

Primer 2.80 Pošto je $\theta = [x/f(y)]$ najopštiji unifikator literala $\alpha(x)$ i $\alpha(f(y))$, klauza $\{\alpha(f(y)), \neg\beta(f(y))\}$ je faktor klauze $\{\alpha(x), \alpha(f(y)), \neg\beta(x)\}$. $\triangle$

Definicija 2.81 Neka su C_1 i C_2 proizvoljne klauze. Neka je D_1 klauza C_1 ili proizvoljan njen faktor, a D_2 klauza C_2 ili proizvoljan njen faktor. Tada se svaka binarna rezolventa klauza D_1 i D_2 naziva *rezolventom* klauza C_1 i C_2.

Sledeća definicija određuje pravilo rezolucije za predikatske formule.

Definicija 2.82 Neka je $\mathcal{F}$ proizvoljan skup klauza. Tada je

$$\begin{array}{rcl} R(\mathcal{F}) & = & \mathcal{F} \cup \{D \mid (\exists C_1, C_2 \in \mathcal{F})\ D \text{ je rezolventa klauza } C_1 \text{ i } C_2\} \\ R^0(\mathcal{F}) & = & \mathcal{F} \\ R^{n+1}(\mathcal{F}) & = & R(R^n(\mathcal{F})) \\ R^*(\mathcal{F}) & = & \bigcup_{n \in N_0} R^n \end{array}$$

Dakle $R(\mathcal{F})$ se dobija tako što se skupu $\mathcal{F}$ dodaju sve rezolvente klauza iz $\mathcal{F}$. Iteriranjem ovog postupka dobija se $R^*(\mathcal{F})$. Značaj postupka rezolucije ogleda se u sledećem tvrđenju.

Tvrđenje 2.83 (Tvrđenje rezolucije za predikatski račun) *Skup klauza $\mathcal{F}$ nema model akko $\emptyset \in R^*(\mathcal{F})$.*

Da bismo ustanovili da li skup $\mathcal{F}$ ima model generišemo redom skupove $R(\mathcal{F})$, $R^2(\mathcal{F})$, $R^3(\mathcal{F})$, itd. Ako neki od skupova $R^k(\mathcal{F})$ sadrži $\emptyset$, skup $\mathcal{F}$ nema model. Obrnuto, ako skup $\mathcal{F}$ nema model, tada postoji $R^k(\mathcal{F})$ koji sadrži $\emptyset$. U slučaju da $\mathcal{F}$ ima model, ovaj postupak ne mora da se završi. Osim toga, broj klauza se u svakom sledećem koraku eksponencijalno povećava, pa je algoritam neefikasan. Zbog toga se u programima za automatsko dokazivanje teorema primenjuju različita poboljšanja osnovnog postupka rezolucije, ali se u opštem slučaju ne može eliminisati problem završavanja algoritma kada $\mathcal{F}$ ima model niti problem neefikasnosti koji u praktičnoj primeni (zbog ograničenja vremena i resursa računara) sprečava nalaženje prazne klauze čak i kada ona pripada skupu $R^*(\mathcal{F})$.

Zadatak 2.84 Dokazati da je valjana formula

$$\varphi = (\forall x)(\exists y)\alpha(x,y)\ \wedge\ (\forall y)(\exists z)\beta(y,z)\ \Rightarrow (\forall x)(\exists y)(\exists z)(\alpha(x,y) \wedge \beta(y,z))$$

Rešenje. Prema tvrđenju 2.49 važi $\emptyset \models \varphi$ akko skup $\emptyset \cup \{\neg\varphi\}$ nema model, tj. $\models \varphi$ akko $\{\neg\varphi\}$ nema model. Formula $\neg\varphi$ je ekvivalentna sa

$$(\forall x)(\exists y)\alpha(x,y)\ \wedge\ (\forall y)(\exists z)\beta(y,z)\ \wedge\ (\exists x)(\forall y)(\forall z)(\neg\alpha(x,y) \vee \neg\beta(y,z)).$$

Zato skup $\{\neg\varphi\}$ nema model akko nema model skup

$$\{(\forall x)(\exists y)\alpha(x,y),\ (\forall y)(\exists z)\beta(y,z),\ (\exists x)(\forall y)(\forall z)(\neg\alpha(x,y) \vee \neg\beta(y,z))\}.$$

Sve formule ovog skupa su u preneksnom obliku, pa možemo primeniti skolemizaciju. Ako pri tome treću klauzu napišemo u obliku skupa, dobijamo skup:

$$\{\alpha(x, f(x)),\ \beta(y, g(y)),\ \{\neg\alpha(a,y), \neg\beta(y,z)\}\}.$$

Sledeći niz formula je izvođenje prazne klauze:

1.	$\alpha(x, f(x))$	*Hyp*
2.	$\beta(y, g(y))$	*Hyp*
3.	$\neg\alpha(a, y), \neg\beta(y, z)$	*Hyp*
4.	$\neg\beta(f(a), z)$	iz $1, 3$ za $\theta = [x/a, y/f(a)]$
5.	$\emptyset$	iz $2, 4$ za $\theta = [y/f(a), z/g(f(a))]$

Dakle prazna klauza je posledica skupa formula, pa skup nema model, što znači da je φ valjana formula. ■

Rezolucija u Prologu Prolog je deklarativni programski jezik koji baziran na predikatskom računu prvog reda. Program u Prologu predstavlja skup klauza oblika

$$\{\neg B_1, \neg B_2, \ldots, \neg B_n\}$$

ili oblika

$$\{G, \neg B_1, \neg B_2, \ldots, \neg B_n\}$$

gde su G, B_1, $\ldots$, B_n elementarne formule. Ovakve klauze se nazivaju *Hornovske klauze*. Osnovna aktivnost Prolog sistema je da utvrdi da li zadata formula φ (koja se naziva upit) predstavlja posledicu zadatog skupa klauza $\mathcal{F}$ (koji se naziva program). Ova provera se vrši tako što se proverava da li se iz skupa $\mathcal{F} \cup \{\neg\varphi\}$ može izvesti prazna klauza. Specijalni oblik Hornovskih klauza pojednostavljuje postupak rezolucije. U standardnim Prolog sistemima je, međutim, postupak rezolucije u cilju efikasnosti toliko pojednostavljen da za njega više ne važi tvrđenje 2.83. Pored toga, specijalan oblik Hornovskih formula predstavlja ograničenje u praktičnom radu, pa se javlja potreba za uvođenjem negiranih formula umesto elementarnih formula B_1, B_2, $\ldots$, B_n. Implementiranje negacije predstavlja poseban problem (videti [JL]), i način na koji je ona implementirana u standardnim Prolog sistemima nije u skladu sa logičkim pravilima zaključivanja (videti [MR]).

Glava 3

Teorija skupova

3.1 Teorija skupova

Osnivač *naivne teorije skupova*, kojom ćemo se mi ovde baviti, je nemački matematičar Georg Kantor. On je, kao i Dedekind (J. Dedekind), Bul (G. Boole), Peano (G. Peano), i mnogi drugi matematičari u 19. i početkom 20. veka, radio na otklanjanju nepreciznosti matematičkog jezika i uvođenju univerzalnog jezika u matematiku. Kantorova teorija još uvek nije imala precizirana pravila izvođenja, a imala je sledeće tri aksiome.

$Ax1$ *Za svako svojstvo postoji skup elemenata koji imaju to svojstvo.*
Pojam *svojstva* bio je prihvatan intuitivno, a skup S elemenata koji imaju svojstvo P se označavao sa

$$S = \{x \mid P(x)\}.$$

$Ax2$ *Dva skupa su jednaka akko imaju jednake elemente.*

$Ax3$ (Aksioma izbora) *Ako je data proizvoljna familija nepraznih skupova, tada postoji preslikavanje f koje svakom skupu familije pridružuje jedan njegov element.*

Bertrand Rasel je 1902. godine pokazao da $Ax1$ vodi u sledeću protivrečnost. Pošto je $x \notin x$ jedno svojstvo, prema $Ax1$ bi postojao skup $M = \{x \mid x \notin x\}$. Važi $M \in M$ ili $M \notin M$. Ukoliko $M \in M$, tada po definiciji skupa M važi $M \notin M$. Ukoliko pak $M \notin M$, tada $M \in M$. Dobijamo dakle $M \in M$ akko $M \notin M$, što je kontradikcija.

Jedan od načina izbegavanja ovog paradoksa je uvođenje pojma *klase*. Tako se postupa u Nojman-Bernajs (P. Bernays) - Gedelovoj aksiomatizaciji teorije skupova (NBG). Polazni pojam u ovakvom načinu aksiomatizacije je klasa, a za klasu A kažemo da je skup akko postoji klasa B tako da $A \in B$. Tada se dozvoljava egzistencija objekta M koji sadrži sve one skupove x za koje važi $x \notin x$. Pošto pretpostavka da je M skup, prema Raselovom razmatranju, vodi u kontradikciju, sledi da M nije skup. Takva klasa se naziva *prava klasa*.

Drugi način aksiomatizacije je Zermelo (E. Zermelo)-Frenkelova (A. Fraenkel) teorija skupova (ZF). Ovde se ne uvodi pojam klase, ali se ne dozvoljava kreiranje proizvoljnog skupa

$$S = \{x \mid P(x)\}$$

već samo skupa

$$S = \{x \in U \mid P(x)\}$$

gde je U proizvoljan postojeći skup.

Postoje i drugi načini aksiomatizacije.

Kada govorimo o *univerzalnom skupu*, tada posmatramo proizvoljan, ali fiksiran skup koji sadrži sve elemente kojima se u datom kontekstu bavimo. (Kasnije ćemo pokazati da se ne može prihvatiti postojanje "skupa svih skupova", zbog toga je svaki skup univerzalan samo u datom kontekstu.)

Aksiom izbora ima neobične posledice. O tome videti u [SV].

3.1.1 Jednakost skupova

Za osnovnu relaciju među skupovima uzimamo relaciju pripadanja elementa x skupu A, u oznaci $x \in A$. Negaciju formule $x \in A$ označavamo sa $x \notin A$. Ostale relacije među skupovima definišemo.

Definicija 3.1

$$A = B \overset{\text{def}}{\Longleftrightarrow} (\forall x)(x \in A \Leftrightarrow x \in B)$$

Tvrđenje 3.2 *Važe sledeće formule*

1. $A = A$;
2. $A = B \Rightarrow B = A$;
3. $A = B, B = C \Rightarrow A = C$.

Dokaz. Ova svojstva su posledica osobina ekvivalencije.

1.
$$\begin{array}{ll} x \in A \Leftrightarrow x \in A & \text{(izvod tautologije } p \Leftrightarrow p\text{)} \\ (\forall x)(x \in A \Leftrightarrow x \in A) & \text{(generalizacija).} \end{array}$$

2.
$$\begin{aligned} A = B &\Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \\ &\Leftrightarrow (\forall x)(x \in B \Leftrightarrow x \in A) \\ &\Leftrightarrow B = A. \end{aligned}$$

3.

$$\begin{aligned} A = B \wedge B = C &\Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \wedge (\forall x)(x \in B \Leftrightarrow x \in C) \\ &\Leftrightarrow (\forall x)((x \in A \Leftrightarrow x \in B) \wedge (x \in B \Leftrightarrow x \in C)) \\ &\Rightarrow (\forall x)(x \in A \Leftrightarrow x \in C) \\ &\Leftrightarrow A = C. \end{aligned}$$

■

Ovde smo znak $=$ uveli kao oznaku za navedenu formulu, a ne kao poseban relacijski simbol. Može se pokazati da tako uvedena relacija ima osobine koje se zahtevaju od relacije jednakosti (odeljak 2.6). Pošto smo pokazali da je $=$ relacija ekvivalencije, trebalo bi još pokazati saglasnost sa relacijom $\in$:

$$A = B \wedge C = D \Rightarrow A \in C \Leftrightarrow B \in D.$$

Napomena 3.3 (videti [SP]) U opštem slučaju, prilikom definisanja novih pojmova kao skraćenica postojećih konstrukcija, od definicije se zahteva da bude *otklonjiva* i *nekreativna*. Time se obezbeđuje da se sve što se može izraziti korišćenjem uvedenih pojmova, može izraziti i bez njih, kao i da se sve što se može dokazati korišćenjem definicija uvedenih pojmova, može se dokazati i bez njih. Prema prethodnoj definiciji, formula

$$A = B \wedge B = C$$

je samo skraćenica za formulu

$$(\forall x)(x \in A \Leftrightarrow x \in B) \ \wedge \ (\forall x)(x \in B \Leftrightarrow x \in C).$$

Neka je T proizvoljno tvrđenje koje sadrži znak $=$ kao jednakost skupova i D dokaz tog tvrđenja. Ako u tvrđenju T svaku pojavu $A = B$ zamenimo sa $(\forall x)(x \in A \Leftrightarrow x \in B)$, dobijamo tvrđenje T' u kojem se ne javlja jednakost skupova. Ako u dokazu D izvršimo istu zamenu, dobijamo dokaz D' koji takođe ne sadrži jednakost skupova. Otklonjivost i nekreativnost definicije jednakosti skupova obezbeđuje da uvek možemo eliminisati znak $=$ u tvrđenju i njegovom dokazu i da dobijen D' jeste korektan dokaz tvrđenja T'. Tako definicija ne utiče na teoriju koju razmatramo, već samo olakšava rad i skraćuje pisanje. ◇

3.1.2 Podskup skupa

Definicija 3.4

$$A \subseteq B \overset{\text{def}}{\Longleftrightarrow} (\forall x)(x \in A \Rightarrow x \in B)$$

Tvrđenje 3.5 *Važe sledeće formule*

1. $A \subseteq A$*;*

2. $A \subseteq B, B \subseteq A \Rightarrow A = B$*;*

3. $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$*.*

Dokaz. Ova tvrđenja su posledica osobina implikacije.

1. Sledi iz $x \in A \Rightarrow x \in A$ generalizacijom.

2.
$$\begin{aligned} A \subseteq B \wedge B \subseteq A &\Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B) \wedge (\forall x)(x \in B \Rightarrow x \in A) \\ &\Leftrightarrow (\forall x)((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \\ &\Rightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \\ &\Leftrightarrow A = B. \end{aligned}$$

3.
$$\begin{aligned} A \subseteq B \wedge B \subseteq C &\Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B) \wedge (\forall x)(x \in B \Rightarrow x \in C) \\ &\Leftrightarrow (\forall x)((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in C)) \\ &\Rightarrow (\forall x)(x \in A \Rightarrow x \in C) \\ &\Leftrightarrow A \subseteq C. \end{aligned}$$

■

3.1.3 Razlika skupova i prazan skup

Definicija 3.6

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

Ako je $A \subseteq U$ onda $U \setminus A$ nazivamo komplement skupa A u odnosu na U. Pišemo i $C_U A$ ili samo A' ukoliko je jasno o kojem skupu U se radi.

Definicija 3.7 Neka je X proizvoljan skup. *Prazan skup*, u oznaci $\emptyset$, je skup $X \setminus X$.

Tvrđenje 3.8 *Prazan skup je jedinstven.*

Dokaz. Neka su $X \setminus X$ i $Y \setminus Y$ prazni skupovi i a proizvoljno. Tada

$$\begin{aligned} a \in X \setminus X &\Leftrightarrow a \in X \wedge a \notin X \\ &\Leftrightarrow \perp \\ &\Leftrightarrow a \in Y \wedge a \notin Y \\ &\Leftrightarrow a \in Y \setminus Y. \end{aligned}$$

Odatle po definiciji jednakosti skupova sledi $X \setminus X = Y \setminus Y$. ■

Tvrđenje 3.9 *Neka je X proizvoljan skup. Tada $\emptyset \subseteq X$.*

Dokaz.

$$\begin{aligned} \emptyset \subseteq X &\Leftrightarrow (\forall x)(x \in \emptyset \Rightarrow x \in X) \\ &\Leftrightarrow (\forall x)(\perp \Rightarrow x \in X) \\ &\Leftrightarrow \perp \Rightarrow (\forall x)(x \in X) \\ &\Leftrightarrow \top. \end{aligned}$$

■

Tvrđenje 3.10 *Neka $A, B \subseteq X$. Tada*

1. *$X \setminus (X \setminus A) = A$;*
2. *$A \subseteq B \Leftrightarrow (X \setminus B) \subseteq (X \setminus A)$.*

Dokaz.

1.
$$\begin{aligned} x \in X \setminus (X \setminus A) &\Leftrightarrow x \in X \wedge x \notin (X \setminus A) \\ &\Leftrightarrow x \in X \wedge \neg x \in X \setminus A \\ &\Leftrightarrow x \in X \wedge \neg(x \in X \wedge x \notin A) \\ &\Leftrightarrow x \in X \wedge (x \notin X \vee x \in A) \\ &\Leftrightarrow (x \in X \wedge x \notin X) \vee (x \in X \wedge x \in A) \\ &\Leftrightarrow x \in X \wedge x \in A \\ &\Leftrightarrow x \in A. \end{aligned}$$

2.
$$\begin{aligned} A \subseteq B &\Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B) \\ &\Leftrightarrow (\forall x)(x \notin B \Rightarrow x \notin A) \\ &\Leftrightarrow (\forall x)(x \in X \wedge x \notin B \Rightarrow x \in X \wedge x \notin A) \\ &\Leftrightarrow (\forall x)(x \in X \setminus B \Rightarrow x \in X \setminus A) \\ &\Leftrightarrow X \setminus B \subseteq X \setminus A. \end{aligned}$$

Kod treće ekvivalencije pravac $(\Rightarrow)$ je posledica tautologije

$$p \Rightarrow q \Rightarrow (p \wedge r \Rightarrow q \wedge r)$$

a pravac $(\Leftarrow)$ činjenice da su A i B podskupovi skupa X.

■

Definicija 3.11 Skup A je *pravi podskup* skupa X, u oznaci $A \subset X$ akko $A \subseteq X$ i $A \neq X$.

Definicija 3.12 *Partitivni skup* skupa A, u oznaci $\mathcal{P}(A)$, je skup svih podskupova skupa X:

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Pošto za svaki skup A važi $\emptyset \subseteq A$ i $A \subseteq A$, važi i $\emptyset \in \mathcal{P}(A)$ i $A \in \mathcal{P}(A)$.

3.1.4 Operacije sa skupovima

Pored razlike i komplementa uvodimo još i

Unija dva skupa

$$A \cup B = \{x \mid x \in A \vee x \in B\},$$

Presek dva skupa

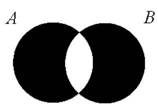
$$A \cap B = \{x \mid x \in A \wedge x \in B\},$$

Simetrična razlika dva skupa

$$A \bigtriangleup B = (A \setminus B) \cup (B \setminus A).$$

Za skupove A i B kažemo da su *disjunktni* akko $A \neq \emptyset$, $B \neq \emptyset$ i $A \cap B = \emptyset$.

Za prikaz skupova koristimo Ojler (L. Euler)-Veneove (J. Venne) dijagrame. Tako simetričnoj razlici skupova A i B odgovara osenčeni deo slike.



Neka je X proizvoljan skup, a Y' oznaka za $X \setminus Y$. Tada se

$$(\mathcal{P}(X), \cup, \cap, {}', \emptyset, X)$$

naziva *Bulova algebra skupova*. Ona zadovoljava sledeće osobine:

1. $A \cup A = A$
2. $A \cup B = B \cup A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$
4. $A'' = A$
5. $(A \cup B)' = A' \cap B'$
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
7. $A \cup (B \cap B') = A$

Bulova algebra skupova zadovoljava niz zakonitosti.

- Ako je F formula sa operacijama $\cap$, $\cup$ i $\setminus$ nad skupovima, dualnom formulom F^* nazivamo formulu koja je dobijena od F tako što su $\cap$ i $\cup$ zamenili mesta. Može se pokazati da su dualne formule tačnih jednakosti opet tačne jednakosti među skupovima. Dovoljno je iz osobina 1–7 izvesti njima dualne osobine 1'–7'. Tako prema osobini 5 važi $(A' \cup B')' = A'' \cap B''$, a kako prema osobini 4 važi $A'' = A$ i $B'' = B$, sledi
$$(A' \cup B')' = A \cap B,$$
odakle primenom osobine 4 dobijamo
$$A' \cup B' = (A \cap B)'$$
a to je dualna osobina osobini 5.
- Sva tvrđenja koja važe za $\cup$, $\cap$ i $\setminus$ se mogu izvesti iz navedenih 7. Pokažimo da važi $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
$$\begin{aligned} A \setminus (B \cap C) &= A \cap (B \cap C)' \\ &= A \cap (B' \cup C') \\ &= (A \cap B') \cup (A \cap C') \\ &= (A \setminus B) \cup (A \setminus C) \end{aligned}$$
- Skup tvrđenja 1–7 je minimalan: ni jedno od navedenih 7 tvrđenja nije posledica preostalih 6.
- Jedna od posledica navedenih formula je i $A \cap (A \cup B) = A$.
- Za relaciju $\subseteq$ važi $A \subseteq B \Leftrightarrow A \cap B = A$. To nam omogućava da nejednakosti sa skupovima svedemo na jednakosti, i obrnuto.
- Sve ove osobine važe i za iskaznu algebru. Apstrakcijom strukture
$$(\mathcal{P}(A), \cup, \cap, ', \emptyset, A)$$
nastaju Bulove algebre.

3.1.5 Familija skupova

Familija skupova je preslikavanje nekog skupa indeksâ u neki skup skupova. Familiju označavamo sa

$$\{A_i \mid i \in I\}$$

gde je I skup indeksā, a A_i slika elementa $i \in I$.

Unija familije skupova je data sa

$$\bigcup_{i\in I} A_i = \{x \mid (\exists i \in I)(x \in A_i)\}$$

a presek familije skupova sa

$$\bigcap_{i\in I} A_i = \{x \mid (\forall i \in I)(x \in A_i)\}.$$

Zadatak 3.13 Neka je $A \neq \emptyset$. Dokazati

$$\mathcal{P}(\cap A) = \cap\{\mathcal{P}(Y) \mid Y \in A\}.$$

Rešenje. Prema definiciji jednakosti skupova pokazaćemo da za svako X važi

$$X \in \mathcal{P}(\cap A) \Leftrightarrow X \in \cap\{\mathcal{P}(Y) \mid Y \in A\}.$$

Pri tome primenjujemo definiciju skupovnih operacija:

$$\begin{array}{rcl}
X \in \mathcal{P}(\cap A) & \Leftrightarrow & X \subseteq \cap A \\
& \Leftrightarrow & (\forall t)(t \in X \Rightarrow t \in \cap A) \\
& \Leftrightarrow & (\forall t)(t \in X \Rightarrow (\forall Z)(Z \in A \Rightarrow t \in Z)) \\
& \Leftrightarrow & (\forall t)(\forall Z)(t \in X \Rightarrow (Z \in A \Rightarrow t \in Z)) \\
& \Leftrightarrow & (\forall Z)(\forall t)(t \in X \Rightarrow (Z \in A \Rightarrow t \in Z)) \\
& \Leftrightarrow & (\forall Z)(\forall t)(Z \in A \Rightarrow (t \in X \Rightarrow t \in Z)) \\
& \Leftrightarrow & (\forall Z)(Z \in A \Rightarrow (\forall t)(t \in X \Rightarrow t \in Z)) \\
& \Leftrightarrow & (\forall Z)(Z \in A \Rightarrow X \subseteq Z) \\
& \Leftrightarrow & (\forall Z)(Z \in A \Rightarrow X \in \mathcal{P}(Z)) \\
& \Leftrightarrow & (\forall Y)(Y \in A \Rightarrow X \in \mathcal{P}(Y)) \\
& \Leftrightarrow & X \in \cap\{\mathcal{P}(Y) \mid Y \in A\}.
\end{array}$$

■

3.1.6 Uređen par

Definicija *uređenog para* (a, b) elemenata a i b prema Vineru (N. Winer) i Kuratovskom (C. Kuratowski) je

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Osnovni smisao ovakve definicije je sledeće tvrđenje.

Tvrđenje 3.14 $(a, b) = (c, d)$ *akko* $a = c$ *i* $b = d$.

Dokaz. Ako je $a = c$ i $b = d$ tada tvrđenje trivijalno važi. Obrnuto, neka je $(a, b) = (c, d)$. Tada po definiciji uređenog para i jednakosti skupova

$$(\forall x)(x \in \{\{a\}, \{a, b\}\} \Leftrightarrow x \in \{\{c\}, \{c, d\}\}),$$

pa po definiciji dvočlanog skupa

$$(\forall x)(x = \{a\} \vee x = \{a, b\} \Leftrightarrow x = \{c\} \vee x = \{c, d\}).$$

Stavljajući $x = \{a\}$ leva strana jednakosti postaje tačna, pa je i desna strana tačna, što znači

$$\{a\} = \{c\} \ \vee \ \{a\} = \{c, d\}.$$

U oba slučaja važi $a = c$. Dalje se uslov jednakosti svodi na

$$(\forall x)(x = \{a\} \vee x = \{a, b\} \Leftrightarrow x = \{a\} \vee x = \{a, d\}).$$

Stavljajući u prethodnoj formuli $x = \{a, b\}$ dobijamo

$$\{a, b\} = \{a\} \vee \{a, b\} = \{a, d\} \tag{$*$}$$

a za $x = \{a, d\}$

$$\{a, d\} = \{a\} \vee \{a, d\} = \{a, b\}. \tag{$**$}$$

Ukoliko važi $a = b$, tada iz $(**)$ sledi

$$\{a, d\} = \{a\}$$

pa je i $d = a = b = c$. Ukoliko važi $a \neq b$, tada ne važi $\{a, b\} = \{a\}$, pa iz $(*)$ sledi da mora važiti $\{a, b\} = \{a, d\}$. Zato je $b = d$. U svakom slučaju $a = c$ i $b = d$. ∎

Kao posledicu prethodnog tvrđenja imamo $(a, b) = (b, a)$ akko $a = b$. Dakle uređeni par razlikuje redosled elemenata.

Definicija 3.15 Uređena n-torka se definiše pomoću uređenog para:

$$(a_1) = a_1$$
$$(a_1, \dots, a_{n-1}, a_n) = ((a_1, \dots, a_{n-1}), a_n).$$

Definicija 3.16 Neka su A i B proizvoljni skupovi. *Dekartov proizvod* (R. Descartes) skupova A i B, u oznaci $A \times B$ je definisan sa

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Ako je $A = \emptyset$ ili $B = \emptyset$ tada iz definicije sledi $A \times B = \emptyset$.

Dekartov proizvod konačnog broja skupova $A_1, \ldots, A_n$ se uvodi na sledeći način:

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}.$$

U opštem slučaju važi $A \times B \neq B \times A$, pa $\times$ nije komutativna operacija nad skupovima. Koristimo i oznaku

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n}.$$

3.2 Relacije

Definicija 3.17 *Binarna relacija* (korespondencija) skupova A i B je proizvoljan podskup $\rho \subseteq A \times B$. $\rho \subseteq A \times A$ je *binarna relacija skupa* A (binarna relacija na skupu A). Ako je ρ relacija skupova A i B tada umesto $(a, b) \in \rho$ pišemo i $a\,\rho\,b$.

Mogu se posmatrati i relacije veće arnosti. Tako za $\rho \subseteq A \times B \times C$ kažemo da je ternarna relacija (redom) skupova A, B i C. $\rho \subseteq A$ je unarna relacija skupa A.

Definicija 3.18 *Preslikavanje* (funkcija) skupa A u skup B je binarna relacija f skupova A i B za koju važi:

$$(\forall a \in A)(\exists_1 b \in B)(a, b) \in f.$$

Ako je f preslikavanje skupa A u skup B tada pišemo $f : A \to B$, a umesto $(a, b) \in f$ pišemo i $f(a) = b$. Skup A nazivamo *domen*, a skup B *kodomen* preslikavanja f.

Definicija 3.19 *Operacija arnosti* n na skupu A je proizvoljno preslikavanje $o : A^n \to A$.

Operaciju arnosti 1 nazivamo *unarna*, a operaciju arnosti 2 *binarna* operacija.

Primer 3.20 Operacija promene znaka je preslikavanje $R_e \to R_e$ koje realnom broju x pridružuje realan broj $-x$. Operacija sabiranja realnih brojeva je preslikavanje $R_e^2 \to R_e$ koje uređenom paru (x, y) pridružuje realan broj $x + y$. Operacija množenja realnih brojeva je takođe binarna operacija koja uređenom paru realnih brojeva (x, y) pridružuje realan broj xy. U cilju preglednijeg zapisa, binarne operacije često pišemo u *infiksnom obliku*: ako je $o : A^2 \to A$ binarna operacija i $x, y \in A$, tada element $o(x, y)$ označavamo $x\,o\,y$. $\triangle$

3.2.1 Značajne binarne relacije skupa A

Posebno su od interesa relacije koje imaju neke od sledećih osobina.

1. ρ je *refleksivna* relacija na skupu A akko
$$(\forall x \in A)(x \,\rho\, x).$$

2. ρ je *simetrična* relacija na skupu A akko
$$(\forall x, y \in A)(x \,\rho\, y \Rightarrow y \,\rho\, x).$$

3. ρ je *tranzitivna* relacija na skupu A akko
$$(\forall x, y, z \in A)(x \,\rho\, y \wedge y \,\rho\, z \Rightarrow x \,\rho\, z).$$

4. ρ je *antisimetrična* relacija na skupu A akko
$$(\forall x, y \in A)(x \,\rho\, y \wedge y \,\rho\, x \Rightarrow x = y).$$

Primer 3.21 Neka je $A = \{1, 2, 3\}$ i $\rho = \{(1, 2), (2, 1)\}$. ρ je binarna relacija na skupu A. Neposrednom proverom ustanovljavamo da ρ nije refleksivna, jeste simetrična, nije tranzitivna i nije antisimetrična. $\triangle$

Dve specijalne binarne relacije svakog skupa A su *prazna relacija* $\emptyset$ i *puna relacija* A^2.

Definicija 3.22 Binarna relacija ρ je *relacija ekvivalencije* na skupu A akko je ρ refleksivna, simetrična i tranzitivna na skupu A (RST).

Relaciju ekvivalencije često obeležavamo znakom $\sim$.

Definicija 3.23 Binarna relacija ρ je *relacija poretka* na skupu A akko je ρ refleksivna, antisimetrična i tranzitivna na skupu A (RAT).

Relaciju poretka obično obeležavamo sa $\leq$.

3.2.2 Tvrđenje reprezentacije relacija ekvivalencije

Definicija 3.24 Neka je $A \neq \emptyset$ proizvoljan skup. *Particija skupa* A je skup $\pi \subseteq \mathcal{P}(A)$ za koji važi:

1. $X \in \pi \Rightarrow X \neq \emptyset$;
2. $A = \bigcup_{X \in \pi} X$;
3. $X, Y \in \pi \Rightarrow X = Y \vee X \cap Y = \emptyset$.

Primer 3.25 Neka je R_e skup realnih, a Z skup celih brojeva. Skup

$$\pi = \{\, [k, k+1) \mid k \in Z \,\}$$

je jedna particija skupa R_e. $\triangle$

Definicija 3.26 Neka je $\sim$ relacija ekvivalencije na skupu A. *Koset* (klasa) elementa $a \in A$ je skup

$$a/_{\sim} = \{b \in A \mid b \sim a\}$$

(koristimo i oznake C_a ili $\bar{a}$ ako se zna o kojoj se relaciji radi). *Količnički (faktor) skup* skupa A po relaciji $\sim$ je skup

$$A/_{\sim} = \{a/_{\sim} \mid a \in A\}.$$

Primer 3.27 Neka je $A = \{1, 2, \dots, 10\}$ i neka

$$x \equiv y \pmod 3 \quad \Leftrightarrow \quad 3 \mid x - y.$$

$\equiv$ je relacija ekvivalencije. Njene klase su sledeće:

$$\begin{aligned} 1/_{\equiv} = 4/_{\equiv} = 7/_{\equiv} = 10/_{\equiv} &= \{1, 4, 7, 10\} \\ 2/_{\equiv} = 5/_{\equiv} = 8/_{\equiv} &= \{2, 5, 8\} \\ 3/_{\equiv} = 6/_{\equiv} = 9/_{\equiv} &= \{3, 6, 9\}. \end{aligned}$$

Primećujemo da klase nemaju isti broj elemenata. Ovde je

$$A/_{\equiv} = \{1/_{\equiv}, 2/_{\equiv}, 3/_{\equiv}\}.$$

$\triangle$

Tvrđenje 3.28 *Neka je $\sim$ relacija ekvivalencije na skupu A. Tada $x \sim y$ akko $x/_{\sim} = y/_{\sim}$.*

Dokaz.
($\Rightarrow$): Neka je $x \sim y$. Neka je $z \in x/_{\sim}$. Tada $z \sim x$. Kako $x \sim y$, iz tranzitivnosti sledi $z \sim y$, pa $z \in y/_{\sim}$. Kako je z bilo proizvoljno, zaključujemo $x/_{\sim} \subseteq y/_{\sim}$. Analognim razmatranjem dobijamo $y/_{\sim} \subseteq x/_{\sim}$. Zbog toga $x/_{\sim} = y/_{\sim}$.
($\Leftarrow$): Neka $x/_{\sim} = y/_{\sim}$. Pošto $x \sim x$, sledi $x \in x/_{\sim}$, tj. $x \in y/_{\sim}$. Zato $x \sim y$. $\blacksquare$

Tvrđenje 3.29 *Neka je $\sim$ proizvoljna relacija ekvivalencije na skupu A, a $x/_\sim$ i $y/_\sim$ dve proizvoljne klase ekvivalencije. Tada važi tačno jedno od tvrđenja*

1. $x/_\sim = y/_\sim$;
2. $x/_\sim \cap y/_\sim = \emptyset$.

Dokaz. Ako je $x/_\sim \cap y/_\sim = \emptyset$, tada nije $x/_\sim = y/_\sim$ jer bi u suprotnom bilo

$$\emptyset = x/_\sim \cap x/_\sim = x/_\sim,$$

što je nemoguće jer iz $x \sim x$ sledi $x \in x/_\sim$.

Ako je $x/_\sim \cap y/_\sim \neq \emptyset$, tada postoji z tako da $z \in x/_\sim$ i $z \in y/_\sim$. Za z važi $z \sim x$ i $z \sim y$. Odatle prema simetričnosti i tranzitivnosti sledi $x \sim y$. Prema prethodnom tvrđenju tada $x/_\sim = y/_\sim$. ∎

Tvrđenje 3.30 *Neka je $\sim$ relacija ekvivalencije skupa A. Tada je količnički skup $A/_\sim$ particija skupa A.*

Dokaz. Neka je $\sim$ relacija ekvivalencije skupa A. Treba da dokažemo da su klase neprazne, disjunktne i da je njihova unija ceo skup A.

1. Neka je $x/_\sim \in A/_\sim$ proizvoljno. Pošto $x \sim x$, sledi $x \in x/_\sim$. Zato $x/_\sim \neq \emptyset$.
2. Prema prethodnom tvrđenju važi ili $x/_\sim = y/_\sim$ ili $x/_\sim \cap y/_\sim = \emptyset$.
3. Pošto za svaku klasu $x/_\sim$ važi $x/_\sim \subseteq A$, važi i

   $$\bigcup_{x \in A} x/_\sim \subseteq A.$$

   Kako važi $\{x\} \subseteq x/_\sim$ za svaki $x \in A$, sledi

   $$A = \bigcup_{x \in A} \{x\} \subseteq \bigcup_{x \in A} x/_\sim.$$

   Iz ove dve nejednakosti dobijamo

   $$\bigcup_{x \in A} x/_\sim = A.$$

∎

Tvrđenje 3.31 *Neka je A neprazan skup i π particija skupa A. Tada je relacija $\sim$, definisana sa*

$$x \sim y \Leftrightarrow (\exists C \in \pi)(x \in C \land y \in C),$$

relacija ekvivalencije na skupu A (i važi $A/_{\sim} = \pi$).

Dokaz. Dokazujemo da je $\sim$ refleksivna, simetrična i tranzitivna.

(R): Neka je $x \in A$ proizvoljan. Pošto je π particija, postoji skup $C \in \pi$ tako da važi $x \in C$. Tada $x \in C$ i $x \in C$, pa $x \sim x$.

(S): Neka $x \sim y$. Tada za neko $C \in \pi$ važi $x \in C$ i $y \in C$. Dakle važi $y \in C$ i $x \in C$, pa $y \sim x$.

(T): Neka $x \sim y$ i $y \sim z$. Tada postoji $C \in \pi$ tako da $x, y \in C$ i postoji $D \in \pi$ tako da $y, z \in D$. Pošto važi $y \in C$ i $y \in D$, sledi $C \cap D \neq \emptyset$. Prema definiciji particije tada mora važiti $C = D$. Zbog toga $x \in C$ i $z \in C$, pa $x \sim z$.

■

Tvrđenjem 3.30 smo pokazali da za svaku relaciju ekvivalencije na A možemo konstruisati particiju skupa A, a tvrđenjem 3.31 da za svaku particiju skupa A možemo konstruisati relaciju ekvivalencije skupa A. Sada ćemo pokazati da su ove dve konstrukcije uzajamno inverzne.

Neka je $\sim$ relacija ekvivalencije skupa A. Tada je $A/_{\sim}$ jedna particija skupa A. Neka je $\equiv$ relacija ekvivalencije određena ovom particijom:

$$x \equiv y \Leftrightarrow (\exists C \in A/_{\sim})(x, y \in C).$$

Pokazaćemo $x \equiv y \Leftrightarrow x \sim y$. Neka je prvo $x \equiv y$. Tada postoji $C \in A/_{\sim}$ tako da $x, y \in C$. Po definiciji skupa $A/_{\sim}$ važi $C = z/_{\sim}$ za neko $z \in A$. Pošto $x \in z/_{\sim}$, sledi $x \sim z$, a pošto $y \in z/_{\sim}$, sledi $y \sim z$. Iz simetričnosti i tranzitivnosti relacije $\sim$, tada sledi $x \sim y$. Dakle, $x \equiv y$ povlači $x \sim y$. Obrnuto, neka je $x \sim y$. Tada je $x/_{\sim} = y/_{\sim}$, pa $x, y \in x/_{\sim}$. Kako $x/_{\sim} \in A/_{\sim}$, sledi $x \equiv y$. Dakle $x \equiv y$ akko $y \sim x$.

Time smo pokazali da primenom prethodne dve konstrukcije od relacije ekvivalencije dolazimo do iste relacije ekvivalencije. Treba još pokazati da polazeći od proizvoljne particije primenom dva puta ovog postupka dolazimo do iste particije. Neka je π proizvoljna particija skupa A i $\sim$ odgovarajuća relacija ekvivalencije na skupu A:

$$x \sim y \Leftrightarrow (\exists C \in \pi)(x, y \in C).$$

Neka je $A/_{\sim}$ particija skupa A koju određuje relacija $\sim$. Pokazaćemo $\pi = A/_{\sim}$. Dokažimo prvo sledeće: Ako je $X \in \pi$ i $y \in X$, tada je $X = y/_{\sim}$. Neka je $z \in X$ proizvoljan. Tada $z, y \in X$, pa $z \sim y$, iz čega sledi $z \in y/_{\sim}$. Zato je $X \subseteq y/_{\sim}$. Neka sada $z \in y/_{\sim}$. Tada $z \sim y$, pa postoji $C \in \pi$ tako da $z, y \in C$. Kako $y \in C$ i $y \in X$, sledi $X \cap C \neq \emptyset$, pa po definiciji particije $X = C$. To znači da $z \in X$. Time smo pokazali i $y/_\sim \subseteq X$, pa $X = y/_\sim$.

Sada možemo dokazati $\pi = A/_\sim$. Neka je $X \in \pi$ proizvoljan. Kako je $X \neq \emptyset$, postoji $y \in X$. Prema prethodnom razmatranju tada $X = y/_\sim$, a $y/_\sim \in A/_\sim$, pa $X \in A/_\sim$. Zato je $\pi \subseteq A/_\sim$. Obrnuto, neka $y/_\sim \in A/_\sim$. Kako je $\bigcup_{X \in \pi} X = A$, postoji $X \in \pi$ tako da $y \in X$. Tada je $X = y/_\sim$, pa $y/_\sim \in \pi$. Zato je i $A/_\sim \subseteq \pi$, pa je $\pi = A/_\sim$.

Prethodna tvrđenja čine *tvrđenje o reprezentaciji*. Ona pokazuju da se jedan u osnovi isti objekat može predstaviti na dva načina: kao relacija ekvivalencije i kao particija skupa.

Primer 3.32 Neka je N^2 skup svih uređenih parova prirodnih brojeva. Definišimo na njemu relaciju $\sim$ sa

$$(a, b) \sim (c, d) \Leftrightarrow a + d = c + b.$$

Pokazaćemo da je $\sim$ relacija ekvivalencije na skupu N^2.

(R): $(a, b) \sim (a, b) \Leftrightarrow a + b = a + b$ a to važi.

(S): Neka $(a, b) \sim (c, d)$. Tada $a+d = c+b$, pa $c+b = a+d$, što znači $(c, d) \sim (a, b)$.

(T): Neka $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$. Tada $a + d = c + b$ i $c + f = e + d$. Sabiranjem ovih jednakosti dobijamo

$$a + d + c + f = c + b + e + d$$

odakle sledi $a + f = e + b$, što znači $(a, b) \sim (e, f)$.

Klasa ekvivalencije elementa (a, b) je

$$\begin{aligned} (a, b)/_\sim &= \{(c, d) \mid a + d = c + b\} \\ &= \{(c, d) \mid a - b = c - d\} \end{aligned}$$

Tako je, na primer,

$$(4, 7)/_\sim = \{(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), \ldots\}.$$

Količnički skup $N^2/_\sim$ je particija skupa N^2:

$$N^2/_\sim = \{(a, b)/_\sim \mid (a, b) \in N^2\}$$

Može se pokazati da svakom celom broju $z \in Z$ odgovara tačno jedna klasa $(a, b)/_\sim$ takva da je $a - b = z$, i obrnuto, pa postoji bijekcija između Z i $N^2/_\sim$. $\triangle$

3.2.3 Tranzitivni proizvodi

Primer 3.33 Neka je $A = \{1, 2, 3, 4\}$,

$$\begin{aligned} \alpha &= \{(1,1), (1,2), (2,3), (1,3)\}, \text{ i} \\ \beta &= \{(2,3), (3,1), (2,1)\}. \end{aligned}$$

Proverom ustanovljavamo da su relacije α i β tranzitivne i antisimetrične. Međutim, relacija $\alpha \cup \beta$ nije tranzitivna, jer $(3,1) \in \alpha \cup \beta$ i $(1,3) \in \alpha \cup \beta$, ali ne važi $(3,3) \in \alpha \cup \beta$. $\alpha \cup \beta$ nije ni antisimetrična, jer $(2,3) \in \alpha \cup \beta$ i $(3,2) \in \alpha \cup \beta$. $\triangle$

Neka je α netranzitivna relacija. Postavlja se pitanje kako proširiti α tako da se dobije tranzitivna relacija.

Definicija 3.34 Neka je $F = \{\alpha_i \mid i \in I\}$ familija relacija na A. *Tranzitivni proizvod* familije F je relacija τ data sa

$$\begin{aligned} a\,\tau\,b \quad \Leftrightarrow \quad & (\exists a_1, \ldots, a_k \in A)(\exists \beta_0, \beta_1, \ldots, \beta_k \in F) \\ & (a\,\beta_0\,a_1 \wedge a_1\,\beta_1\,a_2 \wedge \cdots \wedge a_k\,\beta_k\,b). \end{aligned}$$

pri čemu je $k \in \{0, 1, 2, \ldots\}$.

Tvrđenje 3.35 *Tranzitivni proizvod τ familije relacija F je (1) tranzitivna relacija na A; (2) za svaki $\alpha_i \in F$ važi $\alpha_i \subseteq \tau$; (3) ako je ρ tranzitivna relacija na A takva da $\alpha_i \subseteq \rho$ za sve $\alpha_i \in F$, onda $\tau \subseteq \rho$ (dakle τ je najmanja tranzitivna relacija koja sadrži sve relacije iz F).*

Dokaz.

1. Pokazaćemo da je τ tranzitivna. Neka $a\,\tau\,b$ i $b\,\tau\,c$. Tada po definiciji relacije τ važi

$$\begin{gathered} (\exists a_1, \ldots, a_k \in A)(\exists \beta_0, \beta_1, \ldots, \beta_k \in F) \\ (a\,\beta_0\,a_1 \wedge a_1\,\beta_1\,a_2 \wedge \cdots \wedge a_k\,\beta_k\,b) \\ (\exists b_1, \ldots, b_l \in A)(\exists \gamma_0, \gamma_1, \ldots, \gamma_l \in F) \\ (b\,\gamma_0\,b_1 \wedge b_1\,\gamma_1\,b_2 \wedge \cdots \wedge b_l\,\gamma_l\,c) \end{gathered}$$

   Prema tome, važi:

$$\begin{aligned} & (\exists a_1, \ldots, a_k, b_1, \ldots, b_l \in A)(\exists \beta_0, \beta_1, \ldots, \beta_k, \gamma_0, \gamma_1, \ldots, \gamma_l \in F) \\ & \quad (a\,\beta_0\,a_1 \wedge \cdots \wedge a_k\,\beta_k\,b \wedge b\,\gamma_0\,b_1 \wedge \cdots \wedge b_l\,\gamma_l\,c), \end{aligned}$$

   što po definiciji znači $a\,\tau\,c$.

2. Pokazaćemo da τ sadrži sve relacije $\alpha_i \in F$. Neka je $\alpha_i \in F$ proizvoljno i neka su $a, b \in A$ proizvoljni elementi takvi da $a\,\alpha_i\,b$. Tada po definicije relacije τ za $k = 0$ i $\beta_0 = \alpha_i$ dobijamo $a\,\tau\,b$.

3. Neka je ρ tranzitivna relacija i za svako $\alpha_i \in F$ važi $\alpha_i \subseteq \rho$. Neka su a i b proizvoljni elementi za koje važi $a\,\tau\,b$. Tada

$$(\exists a_1, \ldots, a_k \in A)(\exists \beta_0, \beta_1, \ldots, \beta_k \in F)(a\,\beta_0\,a_1 \wedge a_1\,\beta_1\,a_2 \wedge \cdots \wedge a_k\,\beta_k\,b).$$

Pošto $\alpha_i \subseteq \rho$, važi

$$(a\,\rho\,a_1 \wedge a_1\,\rho\,a_2 \wedge \cdots a_k\,\rho\,b).$$

Odatle primenom tranzitivnosti relacije ρ, zaključujemo $a\,\rho\,b$. Dakle $\tau \subseteq \rho$.

■

Ako je $F = \{\alpha\}$ onda τ nazivamo tranzitivno zatvorenje relacije α i pišemo $\tau = \alpha^*$.

Tvrđenje 3.36 *Ako je neko $\alpha_i \in F$ refleksivna relacija, onda je i τ refleksivna.*

Dokaz. Neka je $a \in A$. Pošto je α_i refleksivna, važi $a\,\alpha_i\,a$. τ sadrži α_i, pa važi $a\,\tau\,a$. Dakle i τ je refleksivna. ■

Tvrđenje 3.37 *Neka je svaka od relacija $\alpha_i \in F$ simetrična. Tada je i τ simetrična.*

Dokaz. Neka $a\,\tau\,b$. Tada

$$(a\,\beta_0\,a_1 \wedge a_1\,\beta_1\,a_2 \wedge \cdots \wedge a_k\,\beta_k\,b).$$

za neke elemente $a_1, \ldots, a_k$ i relacije $\beta_0, \beta_1, \ldots, \beta_k \in F$. Pošto su sve relacije simetrične, važi i

$$(b\,\beta_k\,a_k \wedge \cdots \wedge a_2\,\beta_1\,a_1 \wedge a_1\,\beta_0\,a),$$

što po definiciji znači $b\,\tau\,a$. ■

Posledica 3.38 *Neka je F familija relacija ekvivalencije na A. Tada je τ najmanja relacija ekvivalencije koja sadrži sve relacije iz F.*

Tvrđenje 3.39 *Neka je $F = \{\, \alpha_i \mid i \in I\}$ familija relacija ekvivalencije na A. Tada je $\bigcap_{i\in I} \alpha_i$ relacija ekvivalencije na A.*

Dokaz. Neka je $\alpha = \bigcap_{i\in I} \alpha_i$.

(R) $(x,x) \in \alpha$ akko $(\forall i \in I)(x,x) \in \alpha_i$, a to je tačno jer su sve α_i refleksivne.

(S) $(x,y) \in \alpha$ akko $(\forall i \in I)(x,y) \in \alpha_i$ akko $(\forall i \in I)(y,x) \in \alpha_i$ akko $(y,x) \in \alpha$.

(T) $(x,y) \in \alpha \wedge (y,z) \in \alpha \Leftrightarrow (\forall i \in I)(x,y) \in \alpha_i \wedge (\forall i \in I)(y,z) \in \alpha_i \Leftrightarrow (\forall i \in I)((x,y) \in \alpha_i \wedge (y,z) \in \alpha_i) \Rightarrow (\forall i \in I)(x,z) \in \alpha_i \Leftrightarrow (x,z) \in \alpha$.

■

Zadatak 3.40 Dokazati

$$(\alpha \cap \beta)^* \subseteq \alpha^* \cap \beta^* \subseteq \alpha^* \cup \beta^* \subseteq (\alpha \cup \beta)^*.$$

Rešenje.

1. Neka $(x, y) \in (\alpha \cap \beta)^*$. To znači da postoji konačan niz $a_0, \ldots, a_n$ elemenata iz A tako da $a_0 = x$, $a_n = y$ i za svako $i \in \{0, 1, \ldots, n-1\}$ važi $(a_i, a_{i+1}) \in \alpha \cap \beta$. Tada za svako $i \in \{0, 1, \ldots, n-1\}$ važi $(a_i, a_{i+1}) \in \alpha$, pa $(x, y) \in \alpha^*$. Analogno, za svako $i \in \{0, 1, \ldots, n-1\}$ važi $(a_i, a_{i+1}) \in \beta$, pa $(x, y) \in \beta^*$. Zato $(x, y) \in \alpha^* \cap \beta^*$. Time je prva inkluzija pokazana.

2. Druga inkluzija trivijalno važi jer
$$\alpha^* \cap \beta^* \subseteq \alpha^* \subseteq \alpha^* \cup \beta^*.$$

3. Neka $(x, y) \in \alpha^* \cup \beta^*$. Tada $(x, y) \in \alpha^*$ ili $(x, y) \in \beta^*$. Neka je npr. $(x, y) \in \alpha^*$ (drugi slučaj se pokazuje analogno). Tada postoji konačan niz $a_0, a_1, \ldots, a_n$ elemenata skupa A tako da $a_0 = x$, $a_n = y$ i za svako $i \in \{0, 1, \ldots, n-1\}$ važi $(a_i, a_{i+1}) \in \alpha$. Zato za svako $i \in \{0, 1, \ldots, n-1\}$ važi i $(a_i, a_{i+1}) \in \alpha \cup \beta$, što znači da $(x, y) \in (\alpha \cup \beta)^*$.

■

3.2.4 Algebra binarnih relacija

Definicija 3.41 Neka je A proizvoljan skup. Skup svih binarnih relacija skupa A označavamo sa
$$R(A) = \{ \alpha \mid \alpha \subseteq A^2 \}.$$
Dijagonalna relacija skupa A, u oznaci Δ_A, je relacija
$$\Delta_A = \{ (x, x) \mid x \in A \}.$$
Inverzna relacija relacije α, u oznaci α^{-1}, je relacija
$$\alpha^{-1} = \{ (x, y) \mid (y, x) \in \alpha \}.$$
Proizvod relacija $\alpha, \beta \in R(A)$, u oznaci $\alpha \circ \beta$, je relacija
$$(\alpha \circ \beta) = \{ (x, y) \mid (\exists z)((x, z) \in \alpha \wedge (z, y) \in \beta) \}.$$
Struktura
$$(R(A), \cup, \cap, {}', \circ, {}^{-1}, \emptyset, \Delta_A, A^2)$$
se naziva *algebra binarnih relacija*.

Primer 3.42 Neka je $A = \{1, 2, 3\}$, $\alpha = \{\,(1,1),\ (1,2)\,\}$ i $\beta = \{\,(1,2),\ (1,3),\ (2,3)\,\}$. Tada je $\alpha \circ \beta = \{\,(1,2),\ (1,3)\,\}$, a $\beta \circ \alpha = \emptyset$. Vidimo da množenje relacija nije komutativna operacija. $\triangle$

Poljski matematičar i logičar Alfred Tarski je pedesetih godina ovog veka pokazao da algebra binarnih relacija zadovoljava beskonačno pravilnosti koje nisu posledica jedne drugih. To otežava proces apstrakcije algebre binarnih relacija. Obično se izdvajaju neke pravilnosti koje se smatraju najvažnijim i izvode se njihove posledice. Tako nastaju Klinijeve, relacione i dinamičke algebre.

Tvrđenje 3.43 *Neka su $\alpha, \beta, \gamma \subseteq A^2$ proizvoljne. Tada važi:*

1. $\alpha \circ (\beta \cup \gamma) = (\alpha \circ \beta) \cup (\alpha \circ \gamma)$; $\qquad (\beta \cup \gamma) \circ \alpha = (\beta \circ \alpha) \cup (\gamma \circ \alpha)$
2. $\alpha \circ (\beta \cap \gamma) \subseteq (\alpha \circ \beta) \cap (\alpha \circ \gamma)$; $\qquad (\beta \cap \gamma) \circ \alpha \subseteq (\beta \circ \alpha) \cap (\gamma \circ \alpha)$.

Dokaz.

1.
$$\begin{aligned}
&(x,y) \in \alpha \circ (\beta \cup \gamma)\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in (\beta \cup \gamma))\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land ((t,y) \in \beta \lor (t,y) \in \gamma))\\
\Leftrightarrow\ & (\exists t \in A)(((x,t) \in \alpha \land (t,y) \in \beta) \lor\\
& \qquad\qquad ((x,t) \in \alpha \land (t,y) \in \gamma))\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \beta) \lor\\
& \quad (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \gamma)\\
\Leftrightarrow\ & (x,y) \in (\alpha \circ \beta) \lor (x,y) \in (\alpha \circ \gamma)\\
\Leftrightarrow\ & (x,y) \in (\alpha \circ \beta) \cup (\alpha \circ \gamma).
\end{aligned}$$

2.
$$\begin{aligned}
&(x,y) \in \alpha \circ (\beta \cap \gamma)\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \beta \cap \gamma)\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \beta \land (t,y) \in \gamma)\\
\Leftrightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \beta \land (x,t) \in \alpha \land (t,y) \in \gamma)\\
\Rightarrow\ & (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \beta) \land\\
& \quad (\exists t \in A)((x,t) \in \alpha \land (t,y) \in \gamma)\\
\Leftrightarrow\ & (x,y) \in \alpha \circ \beta \land (x,y) \in \alpha \circ \gamma\\
\Leftrightarrow\ & (x,y) \in (\alpha \circ \beta) \cap (\alpha \circ \gamma).
\end{aligned}$$

■

Primer 3.44 Pokažimo da ne važi obrnut smer 2. dela prethodnog tvrđenja. Neka je $A = \{1, 2, 3, 4\}$ i neka je

$$\begin{array}{rcl} \alpha & = & \{(1,3),(1,4)\} \\ \beta & = & \{(3,2)\} \\ \gamma & = & \{(4,2)\} \end{array}$$

Tada je

$$\begin{array}{rcl} \beta \cap \gamma & = & \emptyset \\ \alpha \circ (\beta \cap \gamma) & = & \emptyset \end{array}$$

ali je

$$\begin{array}{rcl} \alpha \circ \beta & = & \{(1,2)\} \\ \alpha \circ \gamma & = & \{(1,2)\} \end{array}$$

pa je $(\alpha \circ \beta) \cap (\alpha \circ \gamma) = \{(1,2)\}$, što znači da je leva strana pravi podskup desne strane. $\triangle$

Tvrđenje 3.45 *Neka $\alpha, \beta, \gamma \subseteq A^2$. Tada važi:*

1. $(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}$
2. $(\alpha \cup \beta)^{-1} = \alpha^{-1} \cup \beta^{-1}$
3. $(\alpha \cap \beta)^{-1} = \alpha^{-1} \cap \beta^{-1}$
4. $(\alpha^{-1})^{-1} = \alpha$
5. $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$
6. $\alpha \subseteq \beta \Rightarrow \alpha \circ \gamma \subseteq \beta \circ \gamma$
7. $\alpha \subseteq \beta \Rightarrow \gamma \circ \alpha \subseteq \gamma \circ \beta$
8. $(\alpha^{-1})' = (\alpha')^{-1}$
9. $\Delta_A \circ \alpha = \alpha \circ \Delta_A = \alpha$.

Dokaz. Pokazaćemo samo tvrđenja 1 i 6, ostala se takođe pokazuju jednostavno.

1.
$$\begin{array}{rcl} (x,y) \in (\alpha \circ \beta)^{-1} & \Leftrightarrow & (y,x) \in \alpha \circ \beta \\ & \Leftrightarrow & (\exists t \in A)((y,t) \in \alpha \wedge (t,x) \in \beta) \\ & \Leftrightarrow & (\exists t \in A)((t,y) \in \alpha^{-1} \wedge (x,t) \in \beta^{-1}) \\ & \Leftrightarrow & (x,y) \in \beta^{-1} \circ \alpha^{-1} \end{array}$$

6. Ako primenimo tvrđenje 3.43, dobijamo:

$$\begin{aligned}\alpha \subseteq \beta \;&\Leftrightarrow\; \beta = \alpha \cup \beta\\ &\Rightarrow\; \beta \circ \gamma = (\alpha \cup \beta) \circ \gamma\\ &\Leftrightarrow\; \beta \circ \gamma = (\alpha \circ \gamma) \cup (\beta \circ \gamma)\\ &\Leftrightarrow\; \alpha \circ \gamma \subseteq \beta \circ \gamma.\end{aligned}$$

■

Zadatak 3.46 Neka $\rho, \sigma, \gamma \subseteq A^2$. Dokazati da važi:

$$(\rho \circ \sigma) \cap \gamma \subseteq \rho \circ (\sigma \cap (\rho^{-1} \circ \gamma))$$

i pokazati da inkluzija može biti stroga.

Rešenje. Pokažimo prvo da važi inkluzija:

$$\begin{aligned}&(x, y) \in (\rho \circ \sigma) \cap \gamma\\ &\quad\Leftrightarrow (x, y) \in \rho \circ \sigma \;\wedge\; (x, y) \in \gamma\\ &\quad\Leftrightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma) \;\wedge\; (x, y) \in \gamma\\ &\quad\Leftrightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma \wedge (x, y) \in \gamma)\\ &\quad\Leftrightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma \wedge (x, z) \in \rho \wedge (x, y) \in \gamma)\\ &\quad\Leftrightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma \wedge (z, x) \in \rho^{-1} \wedge (x, y) \in \gamma)\\ &\quad\Rightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma \wedge (z, y) \in \rho^{-1} \circ \gamma)\\ &\quad\Rightarrow (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma \cap (\rho^{-1} \circ \gamma))\\ &\quad\Rightarrow (x, y) \in \rho \circ (\sigma \cap (\rho^{-1} \circ \gamma))\end{aligned}$$

Preostaje da se pokaže da inkluzija može biti stroga. Neka je $A = \{1, 2\}$ i neka su relacije date sa

$$\begin{aligned}\rho &= \{(1, 1), (2, 1)\}\\ \sigma &= \{(1, 1)\}\\ \gamma &= \{(2, 1)\}\end{aligned}$$

Tada je

$$(\rho \circ \sigma) \cap \gamma = \{(1, 1), (2, 1)\} \cap \{(2, 1)\} = \{(2, 1)\},$$

dok je

$$\begin{aligned}\rho \circ (\sigma \cap (\rho^{-1} \circ \gamma)) &= \rho \circ (\{(1, 1)\} \cap \{(1, 1)\})\\ &= \{(1, 1), (2, 1)\} \circ \{(1, 1)\}\\ &= \{(1, 1), (2, 1)\} \neq \{(2, 1)\}.\end{aligned}$$

■

3.2.5 Relacije ekvivalencije

Tvrđenje 3.47 *$\alpha \subseteq A^2$ je relacija ekvivalencije akko $\Delta_A \subseteq \alpha$, $\alpha^{-1} \subseteq \alpha$ i $\alpha \circ \alpha \subseteq \alpha$.*

Dokaz.
($\Rightarrow$): Neka je α relacija ekvivalencije na A. Pošto je α refleksivna, važi $(x, x) \in \alpha$ za svako $x \in A$, pa $\Delta_A \subseteq \alpha$. Neka $(x, y) \in \alpha^{-1}$. Tada $(y, x) \in \alpha$. α je simetrična, pa $(x, y) \in \alpha$. Dakle $\alpha^{-1} \subseteq \alpha$. Neka je sada $(x, y) \in \alpha \circ \alpha$. Tada postoji $z \in A$ tako da $(x, z) \in \alpha$ i $(z, y) \in \alpha$. Pošto je α tranzitivna, važi $(x, y) \in \alpha$. Dakle $\alpha \circ \alpha \subseteq \alpha$.

($\Leftarrow$): Neka za relaciju α važi $\Delta_A \subseteq \alpha$, $\alpha^{-1} \subseteq \alpha$ i $\alpha \circ \alpha \subseteq \alpha$. Neka je $x \in A$ proizvoljno. $(x, x) \in \Delta_A$, pa iz $\Delta_A \subseteq \alpha$ sledi $(x, x) \in \alpha$; dakle α je refleksivna. Neka $(x, y) \in \alpha$. Tada $(y, x) \in \alpha^{-1}$. Stoga $(y, x) \in \alpha$, pa je α simetrična. Neka $(x, y) \in \alpha$ i $(y, z) \in \alpha$. Tada $(x, z) \in \alpha \circ \alpha$, pa $(x, z) \in \alpha$. Dakle α je tranzitivna. ∎

Napomena 3.48 Primetimo da smo svaku osobinu relacije dokazali nezavisno, pa važi

- α je refleksivna na skupu A akko $\Delta_A \subseteq \alpha$;
- α je simetrična na skupu A akko $\alpha^{-1} \subseteq \alpha$;
- α je tranzitivna na skupu A akko $\alpha \circ \alpha \subseteq \alpha$.

◇

Tvrđenje 3.49 *$\alpha \subseteq A^2$ je relacija ekvivalencije na A akko $\Delta_A \subseteq \alpha$, $\alpha^{-1} = \alpha$ i $\alpha \circ \alpha = \alpha$.*

Dokaz. Ako za $\alpha \subseteq A^2$ važi $\Delta_A \subseteq \alpha$, $\alpha^{-1} = \alpha$ i $\alpha \circ \alpha = \alpha$, tim pre važi i $\Delta_A \subseteq \alpha$, $\alpha^{-1} \subseteq \alpha$ i $\alpha \circ \alpha \subseteq \alpha$, pa je prema prethodnom tvrđenju α relacija ekvivalencije. Dokazujemo suprotan smer. Neka je α relacija ekvivalencije. Prema prethodnom tvrđenju važi $\Delta_A \subseteq \alpha$, $\alpha^{-1} \subseteq \alpha$ i $\alpha \circ \alpha \subseteq \alpha$. Treba još dokazati $\alpha \subseteq \alpha^{-1}$ i $\alpha \subseteq \alpha \circ \alpha$. Neka $(x, y) \in \alpha$. α je simetrična, pa $(y, x) \in \alpha$, što znači $(x, y) \in \alpha^{-1}$. Zato $\alpha^{-1} = \alpha$. Pošto je α refleksivna, važi $\Delta_A \subseteq \alpha$. Množenjem ove nejednakosti sa α dobijamo $\alpha = \alpha \circ \Delta_A \subseteq \alpha \circ \alpha$. Dakle važi $\alpha \circ \alpha = \alpha$. ∎

Tvrđenje 3.50 *Neka su α i β relacije ekvivalencije na skupu A. Tada je proizvod $\alpha \circ \beta$ relacija ekvivalencije na skupu A akko $\alpha \circ \beta = \beta \circ \alpha$.*

Dokaz. Neka su α i β relacije ekvivalencije na A.

($\Rightarrow$): Neka je $\alpha \circ \beta$ relacija ekvivalencije. Iz simetričnosti relacija α, β i $\alpha \circ \beta$ sledi

$$\alpha \circ \beta = (\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1} = \beta \circ \alpha.$$

($\Leftarrow$): Neka je $\alpha \circ \beta = \beta \circ \alpha$. Pošto su α i β refleksivne, važi $\Delta_A \subseteq \alpha$ i $\Delta_A \subseteq \beta$. Množenjem ovih nejednakosti dobijamo

$$\Delta_A = \Delta_A \circ \Delta_A \subseteq \alpha \circ \beta,$$

što znači da je i $\alpha \circ \beta$ refleksivna. Pošto je $\alpha \circ \beta = \beta \circ \alpha$, imamo

$$(\alpha \circ \beta)^{-1} = (\beta \circ \alpha)^{-1} = \alpha^{-1} \circ \beta^{-1} = \alpha \circ \beta,$$

pa je $\alpha \circ \beta$ simetrična. Takođe važi

$$\alpha \circ \beta \circ \alpha \circ \beta = \alpha \circ \alpha \circ \beta \circ \beta = \alpha \circ \beta,$$

pa je $\alpha \circ \beta$ tranzitivna. Dakle $\alpha \circ \beta$ je relacija ekvivalencije. ■

Tvrđenje 3.51 *Neka su α, β relacije ekvivalencija na A. Tada $\alpha, \beta \subseteq \alpha \circ \beta$. Ako je γ relacija ekvivalencije takva da $\alpha \subseteq \gamma$ i $\beta \subseteq \gamma$, tada $\alpha \circ \beta \subseteq \gamma$.*

Dokaz. Neka su α i β relacije ekvivalencija na A. Iz $\Delta_A \subseteq \beta$ množenjem sa leve strane sa α dobijamo

$$\alpha = \alpha \circ \Delta_A \subseteq \alpha \circ \beta,$$

a množenjem nejednakosti $\Delta_A \subseteq \alpha$ sa β sa desne strane dobijamo

$$\beta = \Delta_A \circ \beta \subseteq \alpha \circ \beta.$$

Dakle $\alpha \circ \beta$ sadrži obe relacije α i β. Neka je γ relacija ekvivalencije takva da $\alpha \subseteq \gamma$ i $\beta \subseteq \gamma$. Iz $\alpha \subseteq \gamma$ sledi

$$\alpha \circ \gamma \subseteq \gamma \circ \gamma,$$

a iz $\beta \subseteq \gamma$ sledi

$$\alpha \circ \beta \subseteq \alpha \circ \gamma.$$

Iz prethodne dve nejednakosti dobijamo

$$\alpha \circ \beta \subseteq \gamma \circ \gamma.$$

■

Zadatak 3.52 Neka je R refleksivna i tranzitivna relacija skupa A. Dokazati da je $R \cap R^{-1}$ relacija ekvivalencije skupa A.

Rešenje. Neka je $R \subseteq A^2$ refleksivna i tranzitivna. Neka je $\Delta = \{(x, x) \mid x \in A\}$. Tada važi $\Delta \subseteq R$ i $R \circ R \subseteq R$. Pokazujemo da da je $R \cap R^{-1}$ refleksivna, simetrična i tranzitivna. Primenjujemo tvrđenja 3.43, 3.45 i 3.47.

(R) Iz $\Delta \subseteq R$ sledi $\Delta^{-1} \subseteq R^{-1}$, a pošto je $\Delta^{-1} = \Delta$, sledi $\Delta \subseteq R^{-1}$. Kako $\Delta \subseteq R$, sledi

$$\Delta \subseteq R \cap R^{-1},$$

što znači da je $R \cap R^{-1}$ refleksivna.

(S) Kako je

$$(R \cap R^{-1})^{-1} = R^{-1} \cap (R^{-1})^{-1} = R^{-1} \cap R = R \cap R^{-1},$$

relacija $R \cap R^{-1}$ je simetrična.

(T) Primetimo prvo da iz $R \circ R \subseteq R$ sledi $(R \circ R)^{-1} \subseteq R^{-1}$, a to znači da

$$R^{-1} \circ R^{-1} \subseteq R^{-1}.$$

Odatle sledi:

$$\begin{aligned}
&(R \cap R^{-1}) \circ (R \cap R^{-1}) \\
&\quad \subseteq R \circ R \cap R \circ R^{-1} \cap R^{-1} \circ R \cap R^{-1} \circ R^{-1} \\
&\quad \subseteq R \circ R \cap R^{-1} \circ R^{-1} \\
&\quad \subseteq R \cap R^{-1}
\end{aligned}$$

što znači da je relacija R tranzitivna.

■

3.2.6 Relacije poretka

Definicija 3.53 Ako je α relacija poretka na skupu A, tada (A, α) nazivamo *parcijalno uređen skup*.

Lema 3.54 *Relacija $\alpha \subseteq A^2$ je antisimetrična akko $\alpha \cap \alpha^{-1} \subseteq \Delta_A$.*

Dokaz. Primetimo da za $x \in A$ važi $x = y$ akko $(x, y) \in \Delta_A$. Zato važi:

$$\begin{aligned}
&(\forall x, y \in A)((x, y) \in \alpha \wedge (y, x) \in \alpha \Rightarrow x = y) \\
\Leftrightarrow &(\forall x, y \in A)((x, y) \in \alpha \wedge (x, y) \in \alpha^{-1} \Rightarrow (x, y) \in \Delta_A) \\
\Leftrightarrow &(\forall x, y \in A)((x, y) \in \alpha \cap \alpha^{-1} \Rightarrow (x, y) \in \Delta_A) \\
\Leftrightarrow &\alpha \cap \alpha^{-1} \subseteq \Delta_A.
\end{aligned}$$

■

Tvrđenje 3.55 *$\alpha \subseteq A^2$ je relacija poretka na skupu A akko $\Delta_A \subseteq \alpha$, $\alpha \cap \alpha^{-1} \subseteq \alpha$ i $\alpha \circ \alpha \subseteq \alpha$.*

Dokaz. Prema napomeni 3.48, α je refleksivna akko $\Delta_A \subseteq \alpha$ i tranzitivna akko $\alpha \circ \alpha \subseteq \alpha$. Prema prethodnom tvrđenju, α je antisimetrična akko $\alpha \cap \alpha^{-1} \subseteq \alpha$. Odatle direktno sledi traženo tvrđenje. ■

Tvrđenje 3.56 *$\leq \subseteq A^2$ je relacija poretka na skupu A akko je $\leq^{-1}$ relacija poretka na skupu A.*

Dokaz. Koristeći prethodno tvrđenje pokazaćemo da se refleksivnost, antisimetričnost i tranzitivnost slažu sa operacijom $^{-1}$.

1. $\leq$ je refleksivna akko $\Delta_A \subseteq \leq$ akko $\Delta_A^{-1} \subseteq \leq^{-1}$ akko $\Delta_A \subseteq \leq^{-1}$ akko je $\leq^{-1}$ refleksivna.
2. $\leq$ je antisimetrična akko $\leq \cap \leq^{-1} \subseteq \Delta_A$ akko $\leq^{-1} \cap (\leq^{-1})^{-1} \subseteq \Delta_A$ akko je $\leq^{-1}$ antisimetrična.
3. $\leq$ je tranzitivna akko $\leq \circ \leq \subseteq \leq$ akko $(\leq \circ \leq)^{-1} \subseteq \leq^{-1}$ akko $\leq^{-1} \circ \leq^{-1} \subseteq \leq^{-1}$ akko je $\leq^{-1}$ tranzitivna.

■

Ako je $\leq$ relacija poretka tada $\leq^{-1}$ obeležavamo sa $\geq$.

Definicija 3.57 Relacija poretka $\leq$ je relacija *totalnog poretka* (linearno uređenje) akko važi

$$(\forall x, y \in A)(x \leq y \vee y \leq x).$$

Ako je $\leq$ relacija totalnog poretka na skupu A, tada $(A, \leq)$ nazivamo totalno uređen skup (lanac).

Primer 3.58 Ako je N skup prirodnih brojeva, a $\leq$ uobičajen poredak nad prirodnim brojevima, tada je $(N, \leq)$ lanac. Ako je A skup sa bar dva elementa, tada parcijalno uređen skup $(\mathcal{P}(A), \subseteq)$ nije lanac. Ako je $|$ relacija deljivosti prirodnih brojeva, tada $(N, |)$ jeste parcijalno uređen skup, ali takođe nije lanac. $\triangle$

U nastavku ćemo podrazumevati da je $(A, \leq)$ proizvoljan parcijalno uređen skup.

Definicija 3.59 Element $a \in A$ se naziva *gornje ograničenje* skupa $S \subseteq A$ akko

$$(\forall x \in S)(x \leq a).$$

$a \in A$ je *donje ograničenje* skupa $S \subseteq A$ akko

$$(\forall x \in S)(a \leq x).$$

Najveći element skupa S je element $a \in S$ koji je gornje ograničenje skupa S, ukoliko takav element postoji.
Najmanji element skupa S je element $a \in S$ koji je donje ograničenje skupa S, ukoliko takav element postoji.

Lema 3.60 *Ako skup $S \subseteq A$ ima najveći (najmanji) element, tada je taj element jedinstven.*

Dokaz. Neka su a_1 i a_2 dva najveća elementa skupa S. Tada $a_1 \leq a_2$ i $a_2 \leq a_1$, pa po antisimetričnosti relacije $\leq$ sledi $a_1 = a_2$. Jedinstvenost najmanjeg elementa se dokazuje analogno. ∎

Definicija 3.61 Neka je $S \subseteq A$ proizvoljan skup. Ako skup gornjih ograničenja skupa S ima najmanji element a, tada se a naziva *supremum skupa* S.

Ne mora svaki skup $S \subseteq A$ imati supremum. Egzistenciju supremuma u $(R_e, \leq)$ gde je R_e skup realnih brojeva, a $\leq$ uobičajeno uređenje realnih brojeva, garantuje *aksioma neprekidnosti*.

Definicija 3.62 Neka je $S \subseteq A$ proizvoljan. Element $a \in S$ je *maksimalni element* skupa S akko

$$(\forall x \in S)(a \leq x \Rightarrow x = a).$$

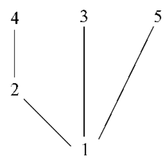
Element $a \in S$ je minimalan element skupa S akko $(\forall x \in S)(x \leq a \Rightarrow x = a)$

Lema 3.63 *Ako $S \subseteq A$ ima najveći element a, onda je a jedini maksimalni element skupa S.*

Dokaz. Neka je a najveći element skupa S. Neka za $x \in S$ važi $a \leq x$. Pošto je a najveći, važi i $x \leq a$. Odatle sledi $x = a$. Dakle a jeste maksimalni. Neka je $m \in S$ proizvoljan maksimalni element skupa S. Pošto $m \in S$, sledi $m \leq a$. Pošto je m maksimalan, sledi $m = a$. Dakle a je jedinstven maksimalni element. ∎

Definicija 3.64 Parcijalno uređen skup $(A, \leq)$ je *dobro uređen* akko svaki neprazan podskup skupa A ima najmanji element.

Primer 3.65 Neka je dat parcijalno uređen skup $(\{1, 2, 3, 4, 5\}, |)$, gde je $|$ relacija deljivosti prirodnih brojeva. Za predstavljanje parcijalno uređenog skupa pogodan je *Haseov dijagram* relacije.



Uočavamo da su 4, 3 i 5 maksimalni elementi a 1 najmanji (pa stoga i minimalni) element. △

Zadatak 3.66 Neka je R refleksivna i tranzitivna relacija skupa S. Definišimo relaciju ρ ovako: $x\,\rho\,y$ akko $x\,R\,y$ i $y\,R\,x$.

a) Dokazati da je ρ relacija ekvivalencije na S.

b) Na količnik skupu $S/_\rho$ definišimo relaciju $\leq$ ovako:

$$x/_\rho \leq y/_\rho \Leftrightarrow x\,R\,y.$$

Dokazati da je $\leq$ dobro definisana i da je relacija poretka na $S/_\rho$.

Rešenje.

a) Primetimo da je $\rho = R \cap R^{-1}$. Zato je prema zadatku 3.52 relacija ρ relacija ekvivalencije na skupu S.

b) Da bismo pokazali da je $\leq$ dobro definisana relacija, treba da dokažemo da odnos dve klase $C_1, C_2 \in S/_\rho$ ne zavisi od predstavnika x i y takvih da $C_1 = x/_\rho$ i $C_2 = y/_\rho$. Neka je stoga $x/_\rho = x'/_\rho$ i $y/_\rho = y'/_\rho$. Tada je $x\,\rho\,x'$ i $y\,\rho\,y'$, što po definiciji znači

$$x\,R\,x', \qquad x'\,R\,x \qquad\qquad y\,R\,y', \qquad y'\,R\,y.$$

Treba da dokažemo da $x\,R\,y$ akko $x'\,R\,y'$. Neka je $x\,R\,y$. Relacija R je tranzitivna, pa

$$x'\,R\,x\,R\,y\,R\,y'$$

što znači $x'\,R\,y'$. Analogno, neka je $x'\,R\,y'$. Tada

$$x\,R\,x'\,R\,y'\,R\,y,$$

pa $x\,R\,y$. Dakle bez obzira da li odabrali predstavnike x i y ili x' i y', odnos elemenata $x/_\rho$ i $y/_\rho$ se ne menja, što znači da je relacija dobro definisana.

Preostaje da se pokaže da je $\leq$ relacija poretka.

(R) Po definiciji relacije $\leq$ važi $x/_\rho \leq x/_\rho$ akko $x\,R\,x$, a to važi jer je R refleksivna relacija.

(AS) Neka je $x/_\rho \leq y/_\rho$ i $y/_\rho \leq x/_\rho$. Tada je $x\,R\,y$ i $y\,R\,x$, što znači $x\rho y$, a to povlači $x/_\rho = y/_\rho$.

(T) Neka je $x/_\rho \leq y/_\rho$ i $y/_\rho \leq z/_\rho$. Tada je $x\,R\,y$ i $y\,R\,z$, a R je tranzitivna, pa $x\,R\,z$, što znači da i $x/_\rho \leq z/_\rho$.

■

Zadatak 3.67 Neka su ρ i σ relacije ekvivalencije skupa A. Dokazati da je $\rho\cup\sigma$ relacija ekvivalencije akko $\rho\cup\sigma=\rho\circ\sigma$.

Rešenje.

$\Rightarrow$): Neka je $\rho\cup\sigma$ relacija ekvivalencije na skupu A. Pošto je σ relacija ekvivalencije na skupu A, važi $\Delta\subseteq\sigma$ odakle množenjem sa leve strane sa ρ dobijamo $\rho\circ\Delta\subseteq\rho\circ\sigma$, a odatle sledi

$$\rho\subseteq\rho\circ\sigma. \qquad (*)$$

Analogno, pošto je ρ relacija ekvivalencije na skupu A važi $\Delta\subseteq\rho$, pa množenjem zdesna sa σ dobijamo $\Delta\circ\sigma\subseteq\rho\circ\sigma$, a odatle sledi

$$\sigma\subseteq\rho\circ\sigma. \qquad (**)$$

Iz $(*)$ i $(**)$ sledi

$$\rho\cup\sigma\subseteq\rho\circ\sigma.$$

Treba još pokazati obrnutu inkluziju. Kako su ρ, σ i $\rho\cup\sigma$ po pretpostavci relacije ekvivalencije i važi $\rho\subseteq\rho\cup\sigma$ i $\sigma\subseteq\rho\cup\sigma$, prema tvrđenju 3.51 važi

$$\rho\circ\sigma\subseteq\rho\cup\sigma.$$

Time smo pokazali $\rho\cup\sigma=\rho\circ\sigma$.

$\Leftarrow$): Neka je $\rho\cup\sigma=\rho\circ\sigma$. Kako su ρ i σ relacije ekvivalencije, važi:

$$\begin{aligned}\sigma\circ\rho &= \sigma^{-1}\circ\rho^{-1}\\ &= (\rho\circ\sigma)^{-1}\\ &= (\rho\cup\sigma)^{-1}\\ &= \rho^{-1}\cup\sigma^{-1}\\ &= \rho\cup\sigma\\ &= \rho\circ\sigma.\end{aligned}$$

Proizvod relacija ekvivalencije ρ i σ komutira, pa prema tvrđenju 3.50 sledi da je $\rho\circ\sigma$ relacija ekvivalencije. Dakle $\rho\cup\sigma$ je relacija ekvivalencije. ■

3.3 Preslikavanja (funkcije)

Definicija 3.68 Neka su A i B proizvoljni skupovi. Relacija $f\subseteq A\times B$ je *preslikavanje* skupa A u skup B akko

$$(\forall a\in A)(\exists_1 b\in B)(a,b)\in f$$

Napomena 3.69 Ako je $A=\emptyset$ tada je jedina relacija skupova A i B relacija $\emptyset$ i ona je funkcija. Ako je $A\neq\emptyset$ i $B=\emptyset$ tada je jedina relacija skupova A i B relacija $\emptyset$, ali ona nije funkcija skupa A u skup B. $\diamond$

Iz prethodne napomene vidimo da je za proveru da li je relacija funkcija potrebno znati i skupove A i B. Zato u definiciju funkcije uključujemo i A i B.

Definicija 3.70 Preslikavanje F skupa A u skup B je uređena trojka (A, B, f), gde su A i B proizvoljni skupovi, a f relacija skupova A i B za koju važi

$$(\forall a \in A)(\exists_1 b \in B)(a, b) \in f.$$

Relacija f se naziva graf funkcije F.

Iz prethodne definicije sledi i uslov jednakosti funkcija. Ako su $F = (A, B, f)$ i $G = (C, D, g)$ funkcije, tada je $F = G$ akko $A = C$, $B = D$ i $f = g$. Primetimo da je uslov $f = g$ ekvivalentan konjunkciji uslova $A = C$ i $(\forall a \in A) f(a) = g(a)$.

Ako je $F = (A, B, f)$ funkcija, pišemo $f : A \to B$. Ako je $f(a) = b$ pišemo $a \mapsto b$.

3.3.1 Neke vrste preslikavanja

Definicija 3.71 Preslikavanje $f : A \to B$ je 1-1 (injekcija) akko

$$(\forall x, y \in A)(f(x) = f(y) \Rightarrow x = y).$$

Preslikavanje $f : A \to B$ je na (sirjekcija) akko

$$(\forall b \in B)(\exists a \in A) f(a) = b.$$

Preslikavanje $f : A \to B$ je *bijekcija* akko je f 1-1 i na.

Primer 3.72 Neka je $\alpha \subseteq A^2$ proizvoljna relacija skupa A. Tada možemo definisati funkciju $f_\alpha : A^2 \to \{\top, \bot\}$ tako da važi

$$f_\alpha(a, b) = \top \quad \Leftrightarrow \quad a\, \alpha\, b.$$

Umesto $f_\alpha(a, b) = \top$ pišemo skraćeno i $\alpha(a, b) = \top$. $\triangle$

Primer 3.73 Neka je $f : \{1, 2\} \to A \cup B$ i neka $f(1) \in A$ i $f(2) \in B$. Ako je npr. $f(1) = a$ i $f(2) = b$, gde $a \in A$ i $b \in B$, tada pišemo

$$f = \begin{pmatrix} 1\,2 \\ a\,b \end{pmatrix}$$

ili skraćeno samo $f = (a, b)$ jer su 1 i 2 fiksirani elementi za svako preslikavanje $f : \{1, 2\} \to A \cup B$. Dakle funkciju f možemo posmatrati kao uređen par, a lako se vrši uopštavanje na uređenu n-torku. (To će se kasnije pokazati značajnim za uopštenje pojma Dekartovog proizvoda.) $\triangle$

Definicija 3.74 *Identičko preslikavanje* skupa A je preslikavanje $1_A : A \to A$ definisano sa $1_A(a) = a$ za svako $a \in A$.

Definicija 3.75 Reč nad azbukom A je preslikavanje $f : \{1, 2, \dots n\} \to A$.

Definicija 3.76 Niz elemenata iz skupa A je preslikavanje $f : \{1, 2, \dots\} \to A$.

Definicija 3.77 Skup svih preslikavanja domena A u kodomen B označavamo B^A tj.:

$$B^A = \{f | f : A \to B\}$$

Posebno, ako je $A = \emptyset$, onda $B^\emptyset$, pišemo B^0 i taj skup je jednočlan skup, to je $\{\emptyset\}$. Takoje, ako je $A = \emptyset$ i $B = \emptyset$, tada je $B^A = \{\emptyset\}$.

3.3.2 Kompozicija preslikavanja

Definicija 3.78 Neka su $f : A \to B$ i $g : B \to C$ preslikavanja. Kompozicija preslikavanja f i g je preslikavanje $g \circ f : A \to C$ definisano sa: $(g \circ f)(a) = g(f(a))$ za svako $a \in A$.

Napomena 3.79 Ako su $F = (A, B, f)$ i $G = (B, C, g)$ preslikavanja tada je $G \circ F = (A, C, f \circ g)$. Kompozicija funkcija dakle odgovara kompoziciji njihovih grafova, ali u obrnutom redosledu. Kada govorimo o kompoziciji funkcija tada podrazumevamo $G \circ F$. $\diamond$

Ako je $h = g \circ f$, kažemo da dijagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

komutira.

Ako postoji $g \circ f$, tada ne mora postojati $f \circ g$, a čak i ako postoji, može biti $f \circ g \neq g \circ f$.

Primer 3.80 Neka su funkcije $f, g : R_e \to R_e$ definisane sa

$$\begin{aligned} f(x) &= 2x + 3 \\ g(x) &= x^2 + 2. \end{aligned}$$

Tada je $(f \circ g)(x) = f(g(x)) = 2x^2 + 7$, a $(g \circ f)(x) = g(f(x)) = 4x^2 + 12x + 11$. $\triangle$

Lema 3.81 *Neka je $f : A \to B$ funkcija i 1_A jedinično preslikavanje skupa A. Tada $f = f \circ 1_A$ i $f = 1_B \circ f$.*

Dokaz. Pošto $1_A : A \to A$ i $f : A \to B$, kompozicija $f \circ 1_A$ postoji, i važi $f \circ 1_A : A \to B$. Ako je $a \in A$, tada je

$$(f \circ 1_A)(a) = f(1_A(a)) = f(a).$$

Stoga prema definiciji jednakosti funkcija $f \circ 1_A = f$.

Pošto je $f : A \to B$ i $1_B : B \to B$, kompozicija $1_B \circ f$ postoji i važi $1_B \circ f : A \to B$. Ako je $a \in A$, tada je

$$(1_B \circ f)(a) = 1_B(f(a)) = f(a),$$

pa prema definiciji jednakosti funkcija važi $1_B \circ f = f$. ∎

Tvrđenje 3.82 *Neka $f : A \to B$, $g : B \to C$ i $h : C \to D$. Tada*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Dokaz. Po definiciji kompozicije $g \circ f : A \to C$, pa $h \circ (g \circ f) : A \to D$. Kako $h \circ g : B \to D$, sledi $(h \circ g) \circ f : A \to D$. Preostaje da proverimo jednakost vrednosti funkcija. Neka je $a \in A$ proizvoljno. Tada

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) = h(g(f(a))), \\ ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) = h(g(f(a))). \end{aligned}$$

Pošto su i vrednosti funkcija jednake, zaključujemo da su i funkcije jednake. ∎

Tvrđenje 3.83 *Neka $f : A \to B$ i $g : B \to C$. Tada*

1. *Ako su f i g* 1-1, *onda je i $g \circ f$* 1-1*;*
2. *Ako su f i g* na, *onda je i $g \circ f$* na.

Dokaz.

1. Neka su f i g 1-1. Neka za $x, y \in A$ važi $(g \circ f)(x) = (g \circ f)(y)$. Tada

   $$g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y) \Rightarrow x = y,$$

   pa je $g \circ f$ takođe 1-1.
2. Neka su f i g na i neka je $c \in C$ proizvoljan. Pošto je g na, postoji $b \in B$ tako da $g(b) = c$. Pošto je f na, postoji $a \in A$ tako da $f(a) = b$. Tada je

   $$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

   Kako je c bio proizvoljan, $g \circ f$ je na.

∎

Posledica 3.84 *Ako su $f : A \to B$ i $g : B \to C$ bijekcije, tada je i $g \circ f : A \to C$ bijekcija.*

3.3.3 Inverzno preslikavanje

Definicija 3.85 Preslikavanje $f^* : B \to A$ je inverzno preslikanje za $f : A \to B$ akko važi

$$\begin{aligned} f^* \circ f &= 1_A \quad \text{i} \\ f \circ f^* &= 1_B. \end{aligned}$$

Tvrđenje 3.86 *Ako preslikavanje f ima inverzno preslikavanje, onda je to inverzno preslikavanje jedinstveno.*

Dokaz. Neka su $f_1, f_2 : B \to A$ inverzna preslikavanja preslikavanja f. Tada je

$$f_1 = f_1 \circ 1_B = f_1 \circ (f \circ f_2) = (f_1 \circ f) \circ f_2 = 1_A \circ f_2 = f_2.$$

■

Za jedinstveno inverzno preslikavanje preslikavanja f koristimo oznaku f^{-1}.

Tvrđenje 3.87 *Neka je $f : A \to B$. Tada f ima inverzno preslikavanje akko je f bijekcija.*

Dokaz.

($\Rightarrow$): Neka f ima inverzno preslikavanje f^{-1}. Prvo dokazujemo da je f 1-1. Neka je $f(x) = f(y)$. Tada važi:

$$\begin{aligned} f^{-1}(f(x)) = f^{-1}(f(y)) &\Rightarrow (f^{-1} \circ f)(x) = (f^{-1} \circ f)(y) \\ &\Rightarrow 1_A(x) = 1_A(y) \\ &\Rightarrow x = y. \end{aligned}$$

Treba još dokazati da je f na. Neka je $b \in B$ proizvoljan. Stavimo $a = f^{-1}(b)$. Tada je

$$f(a) = f(f^{-1}(b)) = (f \circ f^{-1})(b) = 1_B(b) = b,$$

pa je f na.

($\Leftarrow$): Neka je $f = (A, B, \rho)$ bijektivno preslikavanje. Dokazaćemo da je g, dato sa $g = (B, A, \rho^{-1})$ gde je ρ^{-1} inverzna relacija relacije ρ, inverzno preslikavanje preslikavanja f. Dokazaćemo prvo da je g preslikavanje sa domenom B. Neka je $b \in B$ proizvoljan. Pošto je f na, postoji $a \in A$ tako da $f(a) = b$, pa $(a, b) \in \rho$. Stoga $(b, a) \in \rho^{-1}$. Dokazujemo da je a jedinstveno. Pretpostavimo da važi $(b, a_1) \in \rho^{-1}$ i $(b, a_2) \in \rho^{-1}$. Tada $(a_1, b) \in \rho$ i $(a_2, b) \in \rho$, pa $f(a_1) = f(a_2) = b$. Pošto je f 1-1, sledi $a_1 = a_2$. Dakle ρ^{-1} je graf funkcije, pa je g funkcija.

Preostaje da se pokaže da je $g = f^{-1}$, tj. da važi

$$\begin{aligned} g \circ f &= 1_A \\ f \circ g &= 1_B. \end{aligned}$$

Vidimo da se domeni i kodomeni slažu, pa je dovoljno proveriti vrednosti funkcija. Neka je $a \in A$ proizvoljno i neka je $(g \circ f)(a) = g(f(a)) = a'$. Tada postoji $b \in A$ tako da $f(a) = b$ i $g(b) = a'$. Tada je $(a, b) \in \rho$ i $(b, a') \in \rho^{-1}$, pa $(a', b) \in \rho$. Pošto je ρ graf 1-1 funkcije, sledi $a = a'$. Zato je $(g \circ f)(a) = a = 1_A(a)$, čime je prvo tvrđenje pokazano. Neka sada za proizvoljno $b \in B$ važi $(f \circ g)(b) = f(g(b)) = b'$. Tada postoji $a \in A$ tako da važi $g(b) = a$ i $f(a) = b'$. Tada $(a, b') \in \rho$ i $(b, a) \in \rho^{-1}$, pa $(a, b) \in \rho$. Pošto je ρ graf funkcije, sledi $b = b'$. Dakle $(f \circ g)(b) = b = 1_B(b)$. Pošto je b bilo proizvoljno, sledi $f \circ g = 1_B$. ∎

Tvrđenje 3.88 *Neka su $f : A \to B$ i $g : B \to C$ bijekcije. Tada $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dokaz. Kako $g \circ f : A \to C$, sledi $(g \circ f)^{-1} : C \to A$. Iz $f^{-1} : B \to A$ i $g^{-1} : C \to B$ sledi $f^{-1} \circ g^{-1} : C \to A$. Kako važi

$$f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ 1_B \circ f = f^{-1} \circ f = 1_A,$$

i

$$g \circ f \circ f^{-1} \circ g^{-1} = g \circ 1_B \circ g^{-1} = g \circ g^{-1} = 1_C,$$

a kako je $(g \circ f)^{-1}$ jedinstveno, sledi $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ∎

Tvrđenje 3.89 *Neka je $f : A \to B$ i $g : B \to C$. Tada*

1. *Ako je $g \circ f$ 1-1, onda je f 1-1;*
2. *Ako je $g \circ f$ na, onda je g na.*

Dokaz.

1. Pretpostavimo da f nije 1-1. Tada postoje $a_1, a_2 \in A$, tako da $a_1 \neq a_2$, i $f(a_1) = f(a_2)$. Tada je $g(f(a_1)) = g(f(a_2))$, tj. $(g \circ f)(a_1) = (g \circ f)(a_2)$, pa $g \circ f$ nije 1-1. Odatle kontrapozicijom sledi traženo tvrđenje.

2. Pretpostavimo da g nije na. Tada postoji $c \in C$ tako da za svako $b \in B$ važi $g(b) \neq c$. Neka je $a \in A$ proizvoljno. Kako $f(a) \in B$, sledi $g(f(a)) \neq c$. Zato $(g \circ f)(a) \neq c$ za svako a, pa $g \circ f$ nije na. Odatle kontrapozicijom dobijamo traženo tvrđenje.

∎

Primer 3.90 Pokažimo da u prethodnom tvrđenju ne važe suprotni smerovi.

a) Neka je $A = \{1, 2\}$, $B = \{3, 4\}$, $C = \{5\}$ i neka je

$$f = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$
$$g = \begin{pmatrix} 3 & 4 \\ 5 & 5 \end{pmatrix}$$

Preslikavanje f jeste 1-1, ali $g \circ f$ nije jer je

$$(g \circ f)(1) = g(f(1)) = g(3) = 5 = g(4) = g(f(2)) = (g \circ f)(2).$$

b) Neka je $A = \{5\}$, $B = \{3, 4\}$, $C = \{1, 2\}$ i neka je

$$g = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$$
$$f = \begin{pmatrix} 5 \\ 4 \end{pmatrix}.$$

Preslikavanje g jeste na, ali $g \circ f$ nije, jer je $(g \circ f)(x) \neq 1$ za svako $x \in A$.

△

Tvrđenje 3.91 *Ako je f bijekcija, tada je i f^{-1} bijekcija.*

Dokaz. Neka je f bijekcija. Tada važi

$$f^{-1} \circ f = 1_A;$$
$$f \circ f^{-1} = 1_B.$$

Pošto je 1_A bijekcija, pa i na, prema prethodnom tvrđenju sledi da je f^{-1} na. Pošto je 1_B bijekcija, pa i 1-1, prema prethodnom tvrđenju f^{-1} je 1-1. Dakle f^{-1} je bijekcija. ∎

Sledi tvrđenje o reprezentaciji relacija ekvivalencije putem funkcija.

Tvrđenje 3.92 *Relacija $\sim \subseteq A^2$ je relacija ekvivalencije akko za neki skup B i neku funkciju $f : A \to B$ važi*

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Dokaz.

($\Rightarrow$): Neka je $\sim$ relacija ekvivalencije. Definišimo $f : A \to A/_\sim$ sa $f(x) = x/_\sim$. Tada prema tvrđenju 3.28 važi

$$x \sim y \Leftrightarrow x/_\sim = y/_\sim$$

a to je i trebalo dokazati.

($\Leftarrow$): Neka postoji $f : A \to B$ tako da važi $x \sim y \Leftrightarrow f(x) = f(y)$. Tada $f(x) = f(x)$, pa $x \sim x$, što znači da je $\sim$ refleksivna. Neka je $x \sim y$. Tada $f(x) = f(y)$, zato $f(y) = f(x)$, što znači $y \sim x$, stoga je $\sim$ simetrčna. Neka je $x \sim y$ i $y \sim z$. Tada je $f(x) = f(y)$ i $f(y) = f(z)$, zato $f(x) = f(z)$, a to povlači $x \sim z$. Stoga je $\sim$ i tranzitivna, pa je relacija ekvivalencije. ■

Napomena 3.93 Za dato preslikavanje f relacija ekvivalencije $\sim$ se naziva *jezgro preslikavanja*. Za datu relaciju ekvivalencije $\sim$ funkcija $x \mapsto x/_\sim$ se naziva *prirodno preslikavanje*. ◇

Zadatak 3.94 Neka je $E \neq \emptyset$ proizvoljan skup i $A, B \subseteq E$. Neka je preslikavanje $f : \mathcal{P}(E) \to \mathcal{P}(A) \times \mathcal{P}(B)$ definisano sa

$$f(X) = (X \cap A, X \cap B).$$

Dokazati: f je 1-1 akko $E = A \cup B$.

Rešenje.

$\Rightarrow$): Pretpostavimo da $E \neq A \cup B$. Kako je $A \cup B \subseteq E$, postoji element $e \in E$ tako da $e \notin A \cup B$ tj. $e \notin A$ i $e \notin B$. Tada je

$$f(\emptyset) = (\emptyset, \emptyset) = f(\{e\}),$$

što znači da f nije 1-1. Prema tome, ako f jeste 1-1, mora biti $E = A \cup B$.

$\Leftarrow$): Neka je $E = A \cup B$. Neka su $X, Y \in \mathcal{P}(E)$ proizvoljni elementi takvi da je $f(X) = f(Y)$. Tada je

$$((X \cap A), (X \cap B)) = ((Y \cap A), (Y \cap B))$$

pa je $X \cap A = Y \cap A$ i $X \cap B = Y \cap B$. Zato je

$$(X \cap A) \cup (X \cap B) = (Y \cap A) \cup (Y \cap B)$$

što se primenom distributivnosti svodi na

$$X \cap (A \cup B) = Y \cap (A \cup B),$$

pa iz $A \cup B = E$ sledi $X = Y$. Time smo pokazali da f jeste 1-1. ■

Zadatak 3.95 Neka je $(A, \leq)$ dobro uređen skup i $f : A \to A$ preslikavanje za koje važi

$$x < y \Rightarrow f(x) < f(y).$$

Dokazati da za svako $a \in A$ važi $a \leq f(a)$.

Dokaz. Pretpostavimo suprotno: postoji $a \in A$ tako da $a > f(a)$. Neka je

$$S = \{x \in A \mid x > f(x)\}.$$

Pošto $a \in S$, skup S je neprazan, pa ima najmanji element a^*. Kako $a^* \in S$, važi $a^* > f(a^*)$. Prema pretpostavljenoj osobini funkcije f važi

$$f(a^*) < a^* \Rightarrow f(f(a^*)) < f(a^*).$$

Zato $f(a^*) > f(f(a^*))$, pa po definiciji skupa S sledi $f(a^*) \in S$. Ali a^* je najmanji element skupa S, pa važi $a^* \leq f(a^*)$, što je kontradikcija. ■

3.3.4 Neke definicije

Definicija 3.96 Neka je $f : A \to B$ i neka $\emptyset \neq X \subset A$. Tada se preslikavanje $f|_X : X \to B$ definisano sa $f|_X(a) = f(a)$ za $a \in X$ naziva *restrikcija* funkcije f nad skupom X.

Definicija 3.97 Neka je $f : A \to B$. Prošireno preslikavanje $f : \mathcal{P}(A) \to \mathcal{P}(B)$ (direktna slika) definisano je sa

$$f(X) = \{\, f(a) \mid a \in X \,\}.$$

gde je $X \subseteq A$. *Inverzna slika* skupa $Y \subseteq B$ je data sa

$$f^{-1}(Y) = \{\, a \mid f(a) \in Y \,\}.$$

Tvrđenje 3.98 *Neka je $f : S \to T$. Tada za $A, B \subseteq S$ važi:*

1. $f(A \cup B) = f(A) \cup f(B)$;
2. $f(A \cap B) \subseteq f(A) \cap f(B)$;
3. $A \subseteq B \Rightarrow f(A) \subseteq f(B)$.

Dokaz.

1.
$$\begin{aligned}
&y \in f(A \cup B)\\
&\quad \Leftrightarrow (\exists x)(x \in A \cup B \land y = f(x))\\
&\quad \Leftrightarrow (\exists x)((x \in A \lor x \in B) \land y = f(x))\\
&\quad \Leftrightarrow (\exists x)((x \in A \land y = f(x)) \lor (x \in B \land y = f(x)))\\
&\quad \Leftrightarrow (\exists x)(x \in A \land y = f(x)) \lor (\exists x)(x \in B \land y = f(x))\\
&\quad \Leftrightarrow y \in f(A) \lor y \in f(B)\\
&\quad \Leftrightarrow y \in f(A) \cup f(B).
\end{aligned}$$

2.
$$\begin{aligned}
&y \in f(A \cap B)\\
&\Leftrightarrow (\exists x)(x \in A \cap B \wedge y = f(x))\\
&\Leftrightarrow (\exists x)((x \in A \wedge x \in B) \wedge y = f(x))\\
&\Leftrightarrow (\exists x)((x \in A \wedge y = f(x)) \wedge (x \in B \wedge y = f(x)))\\
&\Rightarrow (\exists x)(x \in A \wedge y = f(x)) \wedge (\exists x)(x \in B \wedge y = f(x))\\
&\Leftrightarrow y \in f(A) \wedge y \in f(B)\\
&\Leftrightarrow y \in f(A) \cap f(B).
\end{aligned}$$

3. Neka $A \subseteq B$. Tada $A \cup B = B$. Prema 1. delu tvrđenja

$$f(B) = f(A \cup B) = f(A) \cup f(B),$$

pa $f(A) \subseteq f(B)$.

■

Tvrđenje 3.99 *Neka $f : S \to T$ i neka $A, B \subseteq T$. Tada*

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Dokaz.

1.
$$\begin{aligned}
x \in f^{-1}(A \cup B) &\Leftrightarrow f(x) \in A \cup B\\
&\Leftrightarrow f(x) \in A \vee f(x) \in B\\
&\Leftrightarrow x \in f^{-1}(A) \vee x \in f^{-1}(B)\\
&\Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B).
\end{aligned}$$

2.
$$\begin{aligned}
x \in f^{-1}(A \cap B) &\Leftrightarrow f(x) \in A \cap B\\
&\Leftrightarrow f(x) \in A \wedge f(x) \in B\\
&\Leftrightarrow x \in f^{-1}(A) \wedge f^{-1}(B)\\
&\Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B).
\end{aligned}$$

■

Zadatak 3.100 Za element $x \in A$ kažemo da je fiksna tačka funkcije $f : A \to A$ akko $f(x) = x$. Neka je S skup svih fiksnih tačaka funkcije f. Ako je $g : A \to A$ funkcija takva da je $f \circ g = g \circ f$ dokazati da je $g(S) \subseteq S$.

Rešenje. Neka je $x \in g(S)$ proizvoljan element. Tada postoji $s \in S$ tako da $x = g(s)$. Kako $s \in S$, važi $f(s) = s$. Kako je $g \circ f = f \circ g$, sledi

$$\begin{aligned} x &= g(s) \\ &= g(f(s)) \\ &= (g \circ f)(s) \\ &= (f \circ g)(s) \\ &= f(g(s)) \\ &= f(x). \end{aligned}$$

Dakle, x je fiksna tačka funkcije f, pa $x \in S$. Kako je x bio proizvoljan element iz $g(S)$, sledi $g(S) \subseteq S$. ∎

3.4 Kardinalni i ordinalni brojevi

3.4.1 Prirodni brojevi

Prirodni brojevi se u teoriji skupova uvode kao skupovi posebnog oblika. Aksiome garantuju egzistenciju skupa $\emptyset$ koji predstavlja broj 0, kao i egzistenciju sledbenika S^+ svakog prirodnog broja S.

Definicija 3.101

$$\begin{aligned} 0 &= \emptyset \\ S^+ &= S \cup \{S\} \end{aligned}$$

Tako dobijamo $1 = \{0\}$, $2 = 1 \cup \{1\} = \{0, 1\}$, $3 = 2 \cup \{2\} = \{0, 1, 2\}$ itd. Skup prirodnih brojeva je $N = \{1, 2, 3, \ldots\}$, a skup prirodnih brojeva sa nulom je $N_0 = N \cup \{0\}$.

3.4.2 Kardinalni brojevi

Definicija 3.102 Skupovi A i B su *ekvipotentni*, u oznaci $A \sim B$, akko postoji bijekcija skupa A na skup B.

Tvrđenje 3.103 $\sim$ *ima osobine relacije ekvivalencije: refleksivnost, simetričnost i tranzitivnost.*

Dokaz.

(R): Za svaki skup A jedinično preslikavanje 1_A je bijekcija skupa A na skup A. Zato je $A \sim A$.

(S): Neka je $A \sim B$. Tada postoji bijekcija $f : A \to B$. Pošto je f bijekcija, postoji $f^{-1} : B \to A$. Zbog toga je $B \sim A$.

(T): Neka je $A \sim B$ i $B \sim C$. Tada postoje bijekcije $f : A \to B$ i $g : B \to C$. Prema posledici 3.84 tada je $g \circ f : A \to C$ bijekcija, pa je $A \sim C$.

■

Napomena 3.104 Ako posmatramo proizvoljan skup skupova U, tada je $\sim$ relacija ekvivalencije na U. $\diamond$

Definicija 3.105 *Kardinalni broj* skupa A, u oznaci $|A|$ ili card A je klasa svih skupova ekvipotentnih sa A. Pisaćemo

$$|A| = A/_{\sim}.$$

Iz definicije kardinalnog broja sledi $A \sim B$ akko $|A| = |B|$. Za konačne skupove kardinalni broj identifikujemo sa brojem elemenata skupa.

Definicija 3.106 Skup A je *konačan* akko je prazan ili $A \sim \{1, 2, \ldots n\}$ za neki $n \in N$. Skup A je beskonačan akko nije konačan.

Tvrđenje 3.107 *Skup N je beskonačan.*

Dokaz. Pretpostavimo da je N konačan. Tada za neko $n \in N$ postoji bijekcija $f : \{1, 2, \ldots, n\} \to N$. Onda postoji

$$M = \max_{x \in \{1, \ldots n\}} f(x),$$

i važi $M \in N$. Tada takođe $M + 1 \in N$. Primetimo da za svaki $k \in \{1, 2, \ldots n\}$ važi $f(k) < M + 1$. Odatle sledi

$$M + 1 = f(f^{-1}(M + 1)) < M + 1,$$

što je kontradikcija. ■

Tvrđenje 3.108 *Svaki beskonačan skup se može bijektivno preslikati u svoj pravi podskup.*

Dokaz. Neka je S beskonačan skup. Tada postoji element $a_1 \in S$. Posmatrajmo skup $S\backslash\{a_1\}$. Ukoliko bi taj skup bio prazan, skup S bi imao samo jedan element, pa bi bio konačan. Zato postoji $a_2 \in S\backslash\{a_1\}$. Dalje posmatramo skup $S\backslash\{a_1, a_2\}$. Ako bi on bio prazan, tada bi postojala bijekcija skupa S u skup $\{1, 2\}$, zato postoji $a_3 \in S\backslash\{a_1, a_2\}$. Nastavljajući tako razmatranje dolazimo do niza elemenata $a_1, a_2, \ldots$ koji pripadaju skupu S. Svi ti elementi su različiti jer $a_i \in S\backslash\{a_1, a_2, \ldots a_{i-1}\}$. Neka je $P = S\backslash\{a_1, a_2, \ldots\}$. Definišemo funkciju $f : S \to S\backslash\{a_1\}$ na sledeći način:

$$f(x) = \begin{cases} a_{i+1}, & x = a_i; \\ x, & x \in P. \end{cases}$$

Pokazaćemo da je f bijekcija. Neka su $x \neq y$ proizvoljni elementi iz S. Razlikujemo sledeće slučajeve.

1. $x = a_i$ i $y = a_j$. Tada je $f(x) = a_{i+1}$ i $f(y) = a_{j+1}$. Kako je $x \neq y$, sledi $i \neq j$. Stoga i $i + 1 \neq j + 1$, pa kako su elementi niza različiti, važi $a_{i+1} \neq a_{j+1}$.
2. $x = a_i$ i $y \in P$. Tada $f(x) = a_{i+1}$ i $f(y) = y \in P$, pa kako $a_{i+1} \notin P$, sledi $a_{i+1} \neq y$.
3. $x \in P$ i $y = a_i$. Analogno prethodnom slučaju dobijamo $f(x) = x \neq a_{i+1} = f(y)$
4. $x \in P$ i $y \in P$. Tada $f(x) = x \neq y = f(y)$.

U svakom slučaju $x \neq y \Rightarrow f(x) \neq f(y)$, pa je f 1-1. Preostaje da se pokaže da je f na. Neka je $x \in S\backslash\{a_1\}$ proizvoljan. Ako je $x = a_i$ tada je $i \in \{2, 3, \ldots\}$, pa $a_{i-1} \in \{a_1, a_2, \ldots\}$. Zato $f(a_{i-1}) = a_i$. Ako je pak $x \in P$, tada $f(x) = x$. Dakle f je i na, pa je bijekcija skupa S u njegov pravi podskup $S\backslash\{a_1\}$. ∎

Tvrđenje 3.109 *Svaki skup koji se može bijektivno preslikati u svoj pravi podskup je beskonačan.*

Dokaz. Neka je S skup koji se može bijektivno preslikati u svoj pravi podskup P i neka je $f : S \to P$ bijekcija. Skup $S\backslash P$ je neprazan, pa postoji $a_1 \in S\backslash P$. Definišimo (beskonačan) niz $a_1, a_2, \ldots$ sa $a_{n+1} = f(a_n)$. Pokazaćemo da su svi elementi niza različiti, tako što ćemo indukcijom pokazati da su za svako n elementi $\{a_1, \ldots, a_n\}$ različiti. Za $n = 1$ tvrđenje trivijalno važi. Pretpostavimo da tvrđenje važi za n i posmatrajmo skup $\{a_1, \ldots, a_n, a_{n+1}\}$. Treba da pokažemo da je a_{n+1} različit od ostalih elemenata. Kako je $a_{n+1} = f(a_n)$ važi $a_{n+1} \in P$, pa kako $a_1 \in S \setminus P$, sledi $a_1 \neq a_{n+1}$. Ako je $i > 1$, tada po induktivnoj hipotezi važi $a_{i-1} \neq a_n$, pa kako je f bijekcija, važi $f(a_{i-1}) \neq f(a_n)$, tj. $a_i \neq a_{n+1}$. Time je dokaz indukcijom završen. Dakle skup $\{a_1, a_2, \ldots\}$ je beskonačan. Kako S sadrži beskonačan podskup, i S je beskonačan. ∎

Iz prethodna dva tvrđenja sledi da je skup beskonačan akko se može bijektivno preslikati u svoj pravi podskup. Ovo svojstvo se zato ponekad uzima i za definiciju beskonačnog skupa.

Primer 3.110 Ako je N skup prirodnih brojeva, a $2N$ skup parnih prirodnih brojeva, tada je $f(n) = 2n$ bijekcija skupova N i $2N$. Kako je $2N \subset N$, skup N mora biti beskonačan. $\triangle$

Tvrđenje 3.111 (Šreder-Bernštajn) *(Schröder, Bernstein) Neka za skupove A, A_1 i B važi $A_1 \subseteq B \subseteq A$ i $A \sim A_1$. Tada $A \sim B$.*

Dokaz. Uzmimo da je pretpostavka tvrđenja ispunjena tj. da je $A_1 \subseteq B \subseteq A$ i $A \sim A_1$. Tada postoji bijekcija $f : A \to A_1$. Restrikcija te bijekcije na skup B je injekcija sa B u A_1. Dakle, postoji podskup skupa A_1 na koji bijekcija preslikava skup B. Ako označimo taj podskup sa B_1, tada imamo:

$$A \supseteq B \supseteq A_1 \supseteq B_1$$

gde je $A \sim A_1, B \sim B_1$.

Dalje na osnovu $B \supseteq A_1$ i $B \sim B_1$ zaključujemo da postoji podskup skupa B_1 na koji bijekcija f preslikava skup A_1. Ako označimo taj podskup sa A_2, imamo $A_1 \sim A_2$. Tako smo došli do

$$A \supseteq B \supseteq A_1 \supseteq B_1 \supseteq A_2$$

gde je $A \sim A_1$, $A_1 \sim A_2$ i $B \sim B_1$. Nastavljajući ovaj postupak dobijamo da postoje ekvivalentni skupovi $A_1, A_2, A_3, \ldots$ i ekvivalentni skupovi $B_1, B_2, B_3, \ldots$ tako da je

$$A \supseteq B \supseteq A_1 \supseteq B_1 \supseteq A_2 \supseteq B_2 \supseteq \ldots$$

i da bijekcija f preslikava A_i na A_{i+1}, a B_i na B_{i+1}. Neka je P skup dat sa

$$P = A \cap B \cap A_1 \cap B_1 \cap A_2 \cap B_2 \cap \ldots$$

Tada je

$$\begin{aligned} A &= (A \setminus B) \cup (B \setminus A_1) \cup (A_1 \setminus B_1) \cup \ldots \cup P \\ B &= (B \setminus A_1) \cup (A_1 \setminus B_1) \cup (B_1 \setminus A_2) \cup \ldots \cup P. \end{aligned}$$

Primetimo da je

$$(A_n \setminus B_n) \sim (A_{n+1} \setminus B_{n+1}).$$

Naime, bijekcija f preslikava $A_n \setminus B_n$ na $A_{n+1} \setminus B_{n+1}$ jer A_n preslikava na A_{n+1}, a B_n na B_{n+1}.

Definišimo funkciju $g : A \to B$ ovako:

$$g(x) = \begin{cases} f(x) & \text{ako je } x \in A_i \setminus B_i \text{ ili } x \in A \setminus B \\ x & \text{ako je } x \in B_i \setminus A_{i+1} \text{ ili } x \in P \end{cases}$$

Funkcija g je bijekcija skupa A na skup B. ∎

Definicija 3.112 $|A| \leq |B|$ akko postoji 1-1 preslikavanje skupa A u skup B.

Napomena 3.113 Može se pokazati da rezultat poređenja ne zavisi od izbora predstavnika A i B klasa $|A|$ i $|B|$. $\diamond$

Definicija 3.114 $|A| < |B|$ akko $|A| \leq |B|$ i $|A| \neq |B|$.

Tvrđenje 3.115 (O ekvivalenciji) *Ako je skup A ekvivalentan sa podskupom skupa B i skup B ekvivalentan sa podskupom skupa A, tada su skupovi A i B ekvivalentni.*

Dokaz. Neka je $A_1 \subseteq A$, $B_1 \subseteq B$, $A \sim B_1$ i $B \sim A_1$. Tada postoje bijekcije $f : A \to B_1$ i $g : B \to A_1$. Restrikcija bijekcije g na skup B_1 je bijekcija, pa je $B_1 \sim g(B_1)$. Odatle dobijamo $A \sim B_1 \sim g(B_1)$. Kako je $B_1 \subseteq B$, sledi $g(B_1) \subseteq g(B) = A_1$. Dakle važi $g(B_1) \subseteq A_1 \subseteq A$ i $A \sim g(B_1)$, pa prema tvrđenju Šreder-Bernštajna (3.111), sledi $A \sim A_1$. Pošto $A_1 \sim B$, važi $A \sim B$. ∎

Tvrđenje 3.116 $\leq$ *ima svojstva relacije poretka: refleksivnost, antisimetričnost i tranzitivnost.*

Dokaz.

(R): Neka je A proizvoljan skup. Pošto je 1_A 1-1 preslikavanje skupa A u skup A, važi $|A| \leq |A|$.

(AS): Neka je $|A| \leq |B|$ i $|B| \leq |A|$. Tada postoji 1-1 preslikavanje f skupa A u skup B i 1-1 preslikavanje g skupa B u skup A. Zato je

$$A \sim f(A) \subseteq B \text{ i}$$
$$B \sim g(B) \subseteq A.$$

Odatle prema prethodnom tvrđenju o ekvivalenciji sledi $A \sim B$, što znači $|A| = |B|$.

(T): Neka je $|A| \leq |B|$ i $|B| \leq |C|$. Tada postoji 1-1 preslikavanje $f : A \to B$ i 1-1 preslikavanje $g : B \to C$. Prema tvrđenju 3.83 preslikavanje je $g \circ f : A \to C$ takođe 1-1, što znači da je $|A| \leq |C|$.

∎

Zadatak 3.117 Neka je $|A| = |C|$ i $|B| = |D|$. Dokazati da je $|A \times B| = |C \times D|$.

Rešenje. Pošto je $|A| = |C|$, postoji bijekcija $f : A \to C$, a pošto je $|B| = |D|$, postoji bijekcija $g : B \to D$. Definišimo preslikavanje $f \times g : A \times B \to C \times D$ na sledeći način:

$$(f \times g)((a, b)) = (f(a), g(b)).$$

Pokazaćemo da je $f \times g$ bijekcija.

Neka je $(f \times g)((a, b)) = (f \times g)((a', b'))$. Tada je $(f(a), g(b)) = (f(a'), g(b'))$, pa je

$$\begin{aligned} f(a) &= f(a') \\ g(b) &= g(b'). \end{aligned}$$

Preslikavanje f je 1-1, pa $a = a'$, a g takođe, pa $b = b'$, što znači da je $(a, b) = (a', b')$, pa $f \times g$ jeste 1-1.

Neka je $(c, d) \in C \times D$ proizvoljan. Kako je f na, postoji $a \in A$ tako da $f(a) = c$. Kako je g na, postoji $b \in B$ tako da $f(b) = d$. Tada je

$$(f \times g)((a, b)) = (f(a), g(b)) = (c, d).$$

Time smo pokazali da je $f \times g$ i na, pa je bijekcija. Dakle postoji bijekcija između skupova $A \times B$ i $C \times D$, pa je $|A \times B| = |C \times D|$. ∎

Napomena 3.118 Tvrđenje prethodnog zadatka nam omogućava da definišemo množenje kardinalnih brojeva na sledeći način:

$$|A||B| = |A \times B|.$$

Kardinalni brojevi su klase ekvivalencije međusobno ekvivalentnih skupova. Kako je rezultat množenja definisan preko predstavnika klasa, potrebno je dokazati da rezultat množenja ne zavisi od izbora predstavnika, a to upravo pokazuje prethodni zadatak.

Slično se mogu uvesti i sabiranje i stepenovanje kardinalnih brojeva.

Tako $|A|+|B| = |(1\times A)\cup(2\times B)|$. Ako su A i B disjunktni tada je $|A|+|B| = |A\cup B|$. Stepenovanje kardinalnih brojeva definiše se sa $|A|^{|B|} = |A^B|$. ⋄

Zadatak 3.119 Neka je A proizvoljan skup i $\mathcal{P}(A)$ njegov partitivni skup. Ako sa 2^A označimo skup svih preslikavanja $f : A \to \{0, 1\}$, dokazati da je $|\mathcal{P}(A)| = 2^A$.

Rešenje. Definišemo preslikavanje $G : \mathcal{P}(A) \to 2^A$ na sledeći način. Ako je $X \subseteq A$, tada skupu X pridružujemo preslikavanje $G(X) : A \to \{0, 1\}$ dato sa

$$G(X)(a) = \begin{cases} 1, & a \in X \\ 0, & a \notin X. \end{cases}$$

Pokazaćemo da je preslikavanje G bijekcija.

1-1): Neka je $G(X) = G(Y)$. Funkcije $G(X)$ i $G(Y)$ su jednake, pa za sve argumenta $a \in A$ važi $G(X)(a) = G(Y)(a)$. Tada važi

$$\begin{aligned} a \in X &\Leftrightarrow G(X)(a) = 1 \\ &\Leftrightarrow G(Y)(a) = 1 \\ &\Leftrightarrow a \in Y. \end{aligned}$$

Prema definiciji jednakosti skupova, sledi $X = Y$.

na): Neka je $f : A \to \{0, 1\}$ proizvoljna funkcija. Neka je

$$X = \{a \in A \mid f(a) = 1\}.$$

Pokazaćemo da je $G(X) = f$. Neka je $a \in A$ proizvoljan. Ako je $G(X)(a) = 1$, tada po definiciji preslikavanja G važi $a \in X$, što po definiciji skupa X znači da je $f(a) = 1$. Ako je $G(X)(a) = 0$, tada $a \notin X$, pa nije $f(a) = 1$, a kako $f(a) \in \{0, 1\}$, mora biti $f(a) = 0$. Dakle $G(X)(a) = f(a)$ za svako $a \in A$, pa $G(X) = f$.

■

Primer 3.120 (Princip Dirihlea) Svako injektivno preslikavanje konačnog skupa u samom sebe je i sirjektivno (ti bijekcija). △

Dokaz. Neka je $f : A \to A$ injektivno preslikavanje konačnog skupa A u samog sebe. Za svako $a \in A$ formirajmo $f^2(a), f^3(a), \ldots, f^m(a)$. Kako je A konačan skup, to za svako $a \in A$ postoje nenegativni brojevi $m, n \in N$, tako da je $f^m(a) = f^n(a)$. Neka je npr. $m > n$, onda je $m = n + k$ za neko $k \in N$. Tada iz $f^m(a) = f^n(a)$ sledi $f^{n+k}(a) = f^n(a)$, odnosno $f^n(f^k(a)) = f^n(a)$. Kako je f injektivno to je $f^k(a) = a$ pa je $f(f^{k-1}(a)) = a$. Dakle, za svako $a \in A$ postoji $a' = f^{k-1}(a) \in A$ tako da je $f(a') = a$, tj. f je sirjektivno. ■

3.4.3 Prebrojivi i neprebrojivi skupovi

Neka je $\aleph_0 = |N|$ gde je N skup prirodnih brojeva, i $c = |R_e|$ gde je R_e skup realnih brojeva.

Definicija 3.121 Skup P je *prebrojiv* akko $|P| = \aleph_0$.

Iz definicije sledi da je skup P prebrojiv akko postoji bijekcija $f : N \to P$, tj. akko se elementi skupa P mogu poređati u beskonačan niz tako da se svaki element skupa P u nizu javlja tačno jednom.

Primer 3.122 Skup parnih brojeva $2N = \{2, 4, 6, 8, \ldots\}$ je prebrojiv. △

Tvrđenje 3.123 *Neka su $A = \{a_1, a_2, \ldots\}$ i $B = \{b_1, b_2, \ldots\}$ prebrojivi skupovi. Tada je i $A \cup B$ prebrojiv.*

Dokaz. Primetimo da je $A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots\}$. Tako smo poređali elemente skupa $A \cup B$ u niz, pa je $A \cup B$ prebrojiv. ■

Skup celih brojeva $Z = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ je takođe prebrojiv.

Tvrđenje 3.124 *Ako su $A = \{a_1, a_2, \ldots\}$ i $B = \{b_1, b_2, \ldots\}$ prebrojivi skupovi, tada je i $A \times B$ prebrojiv.*

Dokaz. Uređene parove (a_i, b_j) skupa $A \times B$ možemo poređati prema zbiru indeksâ $i + j$:

$$\begin{array}{lll} (a_1, b_1), & & \\ (a_1, b_2), & (b_2, a_1), & \\ (a_1, b_3), & (a_2, b_2), & (a_3, b_1), \\ \vdots & & \end{array}$$

Pošto se svaki element skupa $A \times B$ tačno jednom javlja u nizu, skup $A \times B$ je prebrojiv. ■

Iz prethodnog tvrđenja sledi da je i $N \times N$ prebrojiv skup. Posmatrajmo skup pozitivnih racionalnih brojeva

$$Q^+ = \{ \frac{p}{q} \mid p, q \in N, \mathrm{NZD}(p, q) = 1 \}.$$

Preslikavanje $n \mapsto \frac{n}{1}$ je 1-1 preslikavanje skupa N u skup Q^+, pa je $\aleph_0 \leq |Q^+|$. Takođe je $Q^+ \sim Q'$ gde je

$$Q' = \{ (p, q) \mid p, q \in N, \mathrm{NZD}(p, q) = 1 \}.$$

Kako je $Q' \subseteq N \times N$, sledi $|Q'| \leq |N \times N|$. Dakle važi

$$\aleph_0 \leq |Q^+| \leq \aleph_0,$$

pa je $|Q^+| = \aleph_0$, što znači da je Q^+ prebrojiv.

Tvrđenje 3.125 (Kantor) $|A| < |\mathcal{P}(A)|$.

Dokaz. Prvo dokazujemo $|A| \leq |\mathcal{P}(A)|$. Neka je preslikavanje $f : A \to \mathcal{P}(A)$ dato sa $f(a) = \{a\}$ za $a \in A$. Ako je $f(a_1) = f(a_2)$, tada $\{a_1\} = \{a_2\}$, pa $a_1 = a_2$. Zato je f 1-1, iz čega sledi $|A| \leq |\mathcal{P}(A)|$.

Treba još pokazati da je $|\mathcal{P}(A)| \neq |A|$. Neka je $f : A \to \mathcal{P}(A)$ funkcija i neka je $B = \{ x \in A \mid x \notin f(x)\}$. Dakle $B \in \mathcal{P}(A)$. Pretpostavimo da postoji $a \in A$ tako da $f(a) = B$. Tada važi $a \in B$ ili $a \notin B$. Ako je $a \in B$, tada po definiciji skupa B sledi $a \notin f(a) = B$. Ako pak $a \notin B$, tada $a \in f(a)$, pa po definiciji skupa B važi $a \in B$. Dakle $a \in B$ akko $a \notin B$, što je kontradikcija. Stoga je pretpostavka da postoji $a \in A$ tako da $f(a) = B$ pogrešna. Zato f nije na, pa ne može biti bijekcija. Pošto ne postoji bijekcija skupa A u skup $\mathcal{P}(A)$, a postoji 1-1 preslikavanje, sledi $|A| < |\mathcal{P}(A)|$. ■

Posledica 3.126 *Ne postoji skup svih skupova.*

Dokaz. Pretpostavimo da je U skup sa svojstvom da za sve skupove A važi $A \in U$. Tada za svaki skup skupova B važi $B \subseteq U$. Specijalno dobijamo $\mathcal{P}(U) \subseteq U$. Odatle sledi $|\mathcal{P}(U)| \leq |U|$ jer je preslikavanje $f : \mathcal{P}(U) \to U$, dato sa $f(x) = x$, 1-1 preslikavanje. Prema prethodnom tvrđenju Kantora, sledi $|U| < |\mathcal{P}(U)|$. Odatle sledi

$$|\mathcal{P}(U)| \leq |U| < |\mathcal{P}(U)|,$$

što je kontradikcija. ■

Tvrđenje 3.127 (Tvrđenje Kantora o neprebrojivosti intervala)
Neka je $(0,1) = \{ x \in R_e \mid 0 < x < 1\}$. *Tada je* $(0,1)$ *beskonačan skup koji nije prebrojiv.*

Dokaz. Pokažimo najpre da je skup $(0,1)$ beskonačan. Preslikavanje $f : N \to (0,1)$ dato sa

$$f(n) = \frac{1}{n+1}$$

je injektivno jer iz $\frac{1}{n+1} = \frac{1}{m+1}$ sledi $m = n$. Zato je $\aleph_0 \leq |(0,1)|$, pa je $(0,1)$ beskonačan skup.

Pokazujemo da $(0,1)$ nije prebrojiv. Koristićemo činjenicu da postoji bijekcija između skupa realnih brojeva intervala $(0,1)$ i njihovih decimalnih razvoja koji sadrže konačan broj cifara 0. Decimalni razvoj broja između $(0,1)$ je niz cifara iz skupa $\{0,1,\ldots,9\}$ koji određuju odgovarajući konvergentan beskonačni red. Za svaki realan broj iz $(0,1)$ postoji njegov decimalni razvoj, ali su npr. 0.50000... i 0.49999... dva različita decimalna razvoja koja odgovaraju istom realnom broju. Ukoliko eleminišemo brojeve oblika $0.c_1c_2\ldots c_k0000\ldots$ tada svakom realnom broju iz $(0,1)$ odgovara tačno jedan decimalni zapis. Pređimo na dokaz tvrđenja.

Pretpostavimo suprotno: svi decimalni zapisi brojeva iz $(0,1)$ se mogu poređati u niz:

$$\begin{aligned} x_1 &= 0.a_1b_1c_1\ldots \\ x_2 &= 0.a_2b_2c_2\ldots \\ x_3 &= 0.a_3b_3c_3\ldots \\ &\vdots \end{aligned}$$

Neka je $x = 0.abcd\ldots$ gde je $a = 1$ ako je $a_1 \neq 1$, a $a = 2$ ako je $a_1 = 1$; $b = 1$ ako je $b_2 \neq 1$, a $b = 2$ ako je $b_2 = 1$; $c = 1$ ako je $c_3 \neq 1$, a $c = 2$ ako je $c_3 = 1$ itd. Tako formiran decimalni zapis odgovara broju iz $(0,1)$ i on ne sadrži cifru 0. Sa druge strane, taj zapis se razlikuje od zapisa svakog broja iz navedenog niza bar po jednoj decimalnoj cifri. Zato x ne može biti ni jedan od brojeva $x_1, x_2, \ldots$, što je kontradikcija sa pretpostavkom da smo decimalne zapise poređali u niz. Dakle brojeve iz $(0,1)$ odnosno njihove decimalne zapise nije moguće poređati u niz, pa ih nema prebrojivo mnogo. ∎

Prema prethodnom tvrđenju važi $\aleph_0 < c$. Može se pokazati da važi $\mathcal{P}(N) \sim (0,1) \sim R_e$. Postavlja se pitanje da li postoji kardinalni broj k tako da važi

$$\aleph_0 < k < c.$$

Koen (P. Cohen) je 1963. godine pokazao da se to ne može izvesti iz uobičajenih aksioma teorije skupova.

Zadatak 3.128 Pokazati da je skup svih zatvorenih intervala realnih brojeva čije su granice racionalni brojevi prebrojiv.

Rešenje. Skup S svih zatvorenih intervala realnih brojeva čije su granice racionalni brojevi je oblika

$$S = \{[p,q] \mid p,q \in Q\}.$$

Definišimo preslikavanje $f : S \to Q^2$ sa

$$f([p,q]) = (p,q)$$

gde je sa (p,q) označen uređen par racionalnih brojeva p i q. Ako je $f([p,q]) = f([p',q'])$ tada je $(p,q) = (p',q')$, pa je $p = p'$ i $q = q'$, što povlači $[p,q] = [p',q']$. Prema tome, preslikavanje $f : S \to Q^2$ je 1-1. Zato je

$$|S| \leq |Q^2|$$

tj. $|S| \leq \aleph_0$. Sa druge strane, neka je preslikavanje $g : N \to S$ dato sa $g(n) = [0,n]$. Ako je $g(n) = g(n')$, tada je $[0,n] = [0,n']$ pa je $n = n'$. Dakle i g je 1-1, pa je

$$|N| \leq |S|$$

tj. $\aleph_0 \leq |S|$. Dobijamo $\aleph_0 \leq |S| \leq \aleph_0$, odakle sledi $|S| = \aleph_0$, što je i trebalo dokazati. ∎

Zadatak 3.129 Za funkciju $f : R_e \to R_e$ gde je R_e skup realnih brojeva kažemo da ima *lokalni minimum* u tački $x_0 \in R_e$ akko postoji otvoreni interval $(a,b) \subseteq R_e$ tako da $x_0 \in (a,b)$ i za svako $x \in (a,x_0) \cup (x_0,b)$ važi $f(x) > f(x_0)$. Dokazati da funkcija $f : R_e \to R_e$ gde je R_e skup realnih brojeva može imati najviše prebrojivo mnogo lokalnih minimuma.

Rešenje. U dokazu ćemo iskoristiti prethodni zadatak i činjenicu da između svaka dva realna broja postoji racionalan broj.

Neka je E skup svih lokalnih minimuma funkcije $f : R_e \to R_e$. Neka je S skup svih zatvorenih intervala čije su granice racionalni brojevi (iz prethodnog zadatka). Definišemo preslikavanje $H : E \to S$ na sledeći način. Neka je $x_0 \in E$ lokalni ekstremum funkcije f. Tada postoji otvoreni interval (a, b) takav da $x_0 \in (a, b)$ i za sve $x \in (a, x_0) \cup (x_0, b)$ važi $f(x) > f(x_0)$. Između tačaka a i x_0 postoji racionalan broj, označimo ga sa p. Između tačaka x_0 i b postoji racionalan broj, označimo ga sa q. Tada za sve $x \in [p, q] \setminus \{x_0\}$ važi $f(x) > f(x_0)$. Za svako x_0 postoji bar jedan takav interval $[p, q]$, neka je $H : E \to S$ proizvoljno preslikavanje koje svakom $x_0 \in R_e$ pridružuje jedan fiksirani interval $[p, q] = H(x_0)$. Pokažimo da je H 1-1.

Neka su $x_0, x_1 \in E$, $x_0 \neq x_1$ tačke lokalnog minimuma. Pretpostavimo da je $H(x_0) = H(x_1) = [p, q]$. Prema konstrukciji intervala $[p, q]$, a pošto $x_1 \in [p, q] \setminus \{x_0\}$, sledi $f(x_1) > f(x_0)$. Analogno, iz $x_0 \in [p, q] \setminus \{x_1\}$, sledi $f(x_0) > f(x_1)$, što je kontradikcija. Dakle mora biti $H(x_0) \neq H(x_1)$.

Time smo pokazali da je $H : E \to S$ 1-1, što znači $|E| \leq |S|$, a prema prethodnom zadatku je $|S| = \aleph_0$, pa dobijamo da skup E ima najviše prebrojivo mnogo elemenata. ■

Zadatak 3.130 Dokazati da je skup R_e ekvipotentan sa intervalom $(0, 1)$.

Rešenje. Dovoljno je uočiti da je funkcija

$$f(x) = \frac{e^x}{1 + e^x}$$

bijekcija skupa R_e u skup $(0, 1)$. ■

3.4.4 Ordinalni brojevi

Definicija 3.131 Parcijalno uređen skup $(S_1, \leq_1)$ je sličan parcijalno uređenom skupu $(S_2, \leq_2)$ akko postoji bijekcija $f : S_1 \to S_2$ za koju važi

$$(\forall a, b \in S_1)(a \leq_1 b \Leftrightarrow f(a) \leq_2 f(b)).$$

Može se pokazati da je i sličnost refleksivna, simetrična i tranzitivna nad parcijalnim porecima.

Definicija 3.132 *Dobro uređen* skup je struktura $(S, \leq)$ takva da je $(S, \leq)$ parcijalno uređen skup, i svaki neprazan podskup skupa S ima najmanji element.

Lema 3.133 *Svaki dobro uređen skup je totalno uređen.*

Dokaz. Neka je $(S, \leq)$ dobro uređen skup i neka su $a, b \in S$ proizvoljni. Skup $\{a, b\}$ je neprazan, pa ima najmanji element. Ako je a najmanji element, tada $a \leq b$. Ako je b najmanji element, tada $b \leq a$. U svakom slučaju $a \leq b \vee b \leq a$, što znači da je $(S, \leq)$ totalno uređen skup. ■

Definicija 3.134 Neka je $(S, \leq)$ dobro uređen skup. *Ordinalni broj* skupa $(S, \leq)$, u oznaci ord S, je klasa dobro uređenih skupova koji su slični skupu $(S, \leq)$.

Neka je $\leq$ uobičajena relacija poretka na prirodnim brojevima. Po definiciji stavljamo

$$\begin{aligned} 1 &= \text{ord}\,(\{1\}, \leq) \\ 2 &= \text{ord}\,(\{1, 2\}, \leq) \\ 3 &= \text{ord}\,(\{1, 2, 3\}, \leq) \\ &\vdots \\ \omega &= \text{ord}\,(\{1, 2, \ldots\}, \leq) \end{aligned}$$

Ako je S podskup skupa prirodnih brojeva, tada umesto $(S, \leq)$ pišemo i samo S pri čemu podrazumevamo uobičajenu relaciju poretka na prirodnim brojevima. Kada skup $\{a_1, a_2, \ldots a_m\}$ posmatramo kao dobro uređen skup, tada podrazumevamo $a_1 \leq a_2 \leq \cdots \leq a_m$.

Definicija 3.135 Neka je $(S, \leq)$ dobro uređen skup. *Inicijalni segment* I_a je dobro uređen skup $(I_a, \leq)$ gde je

$$I_a = \{\, x \mid x \in S, x < a \,\}.$$

Ako su $\alpha = \text{ord}\, A$ i $\beta = \text{ord}\, B$ ordinalni brojevi, tada je ordinalni broj α *manji* od ordinalnog broja β, u oznaci $\alpha < \beta$, akko je A sličan nekom inicijalnom segmentu skupa B.

Primer 3.136 ord $\{1, 2, 3\}$ $<$ ord $\{1, 2, 3, 4, 5\}$ jer je skup $\{1, 2, 3\}$ sličan inicijalnom segmentu I_4 skupa $\{1, 2, 3, 4, 5\}$. △

Može se pokazati da je relacija $<$ dobro definisana nad ordinalnim brojevima i da ima osobine relacije poretka.

Definicija 3.137 Neka su $\alpha = \text{ord}\,(A, \leq_A)$ i $\beta = \text{ord}\,(B, \leq_B)$, $A \cap B = \emptyset$, proizvoljni ordinalni brojevi. *Zbir ordinalnih brojeva* α i β, u oznaci $\alpha + \beta$ je ord $(C, \leq_C)$, gde je $C = A \cup B$, a relacija $\leq_C$ definisana sa

$$\begin{aligned} a_1 \leq_C a_2 \Leftrightarrow a_1 \leq_A a_2, &\quad a_1, a_2 \in A; \\ b_1 \leq_C b_2 \Leftrightarrow b_1 \leq_B b_2, &\quad b_1, b_2 \in B; \\ a \leq_C b, &\quad a \in A, b \in B. \end{aligned}$$

Primer 3.138 Kako je $\omega = \{1, 2, \ldots\}$ i $m = \{a_1, a_2, \ldots\ a_m\}$, važi

$$\begin{aligned} m + \omega &= \{a_1, a_2, \ldots, a_m; 1, 2, \ldots\} = \omega \\ \omega + m &= \{1, 2, \ldots, a_1, a_2, \ldots, a_m\} > \omega. \end{aligned}$$

Dakle sabiranje ordinalnih brojeva nije komutativno. △

Bibliografija

[KK] K. Krivine: *Aksiomatička teorija skupova*, Školska knjiga, Zagreb, 1978.

[MSP] M. i S. Prešić: *Uvod u matematičku logiku, teorija i zadaci*, Matematički institut, Beograd, 1979.

[SP] S. Prešić: *Elementi matematičke logike*, Matematička biblioteka, Beograd, 1968.

[SV] S. Vujošević: *Matematička logika*, CID, Podgorica, 1996.

[EM] E. Mendelson: *Introduction to Mathematical Logic*, D. Van Nostrand Company, New York - Toronto - London - Melbourne, 1964.

[PH] P. Halmos: *Naive set theory*, New York, 1963.

[MJ] M. Jocković: *Veštačka inteligencija*, "Filip Višnjić" - Institut za filozofiju i društvenu teoriju, Beograd, 1994.

[JR] J. Robinson: *A Machine-oriented Logic Based on the Resolution Principle*, JACM, 12, 23-41, 1965.

[HLCP] H. Lewis, C. Papadimitriou: *Elements of the Theory of Computation*, Prentice-Hall International, Inc., 1981.

[PHIP] P. Hotomski, I. Pevac: *Matematički problemi veštačke inteligencije u oblasti automatskog dokazivanja teorema*, Naučna knjiga, Beograd, 1988.

[JL] J. Lloyd: *Foundations of Logic Programming*, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1984.

[MR] M. Radovan: *Programiranje u prologu*, Informator, Zagreb, 1987.

[SJ] S. Jablonskii: *Vvedenie v diskretnuju matematiku*, Nauka, Moskva, 1979.

[MK] A. Mostowski, K. Kuratovski: *Set Theory*, PWN, Warszawa, 1976.

[GCBT] G. Čupona, B. Trpenovski: *Predavanja po algebre* II, Skopje, 1976.

[AM] A. I. Maljcev: *Algebraic Systems*, Springer Verlag, Berlin, Heidelberg, New York, 1973.

[DJK] Đ. Kurepa: *Viša algebra I, II*, Zavod za izdavanje udžbenika, Beograd, 1971.

[AK] A. Kron: *Elementarna teorija skupova*, Matematički institut, Beograd, 1992.

[MC] S. R. Madarász, S. Crvenković: *Relacione algebre*, Matematički institut, Beograd, 1992.

[ZM] Ž. Mijajlović: *Algebra I*, Milgor, Beograd - Moskva, 1993.

[SM84] S. Milić: *Elementi algebre*, Institut za matematiku, Novi Sad, 1984.

[SM] S. Milić: *Elementi matematičke logike i teorije skupova*, Institut za matematiku, Novi Sad, 1981.

[GV] G. Vojvodić: *Algebra*, Institut za matematiku, Novi Sad, 1992.

[GV1] G. Vojvodić: *Predavanja iz matematičke logike i algebre*, Univerzitet u Novom Sadu, Novi Sad, 1998.

[GV2] G. Vojvodić: *Predavanja iz matematičke logike i algebre*, Univerzitet u Novom Sadu, Novi Sad, 2000.

[VDE] V. Devide: *Matematička logika I*, Matematički institut, Beograd, 1964.

[KK] G. Kreisel, J. L. Krivine: *Elements of Mathematical Logic: Model Theory*, North Holland, Amsterdam, 1967.

[BJ] B. Janeva: *Voved vo teorijata na množestvata i matematičata logika*, PMF, Skopje, 1996.

[RD] R. Doroslovački: *Elementi opšte i linearne algebre*, FTN, Novi Sad, 1997.

[MR] M. Radić: *Algebra I, II*, Školska knjiga, Zagreb, 1989.

[EP] J. Eršov, E. Paljutin, *Matematičeskaja logika*, Nauka, Moskva, 1979.

[OK] Z. Ognjanović, N. Krdžavac: *Uvod u teorisko računarstvo*, Beograd - Kragujevac, 2004.

[SB] S. Burris: *Logic for mathematics and computer science*, Univ. Waterlo, Prentice Hall, 1998.

[VS] G. Vojvodić, B. Šobot: *Zbirka zadataka iz matematičke logike i algebre*, Un iverzitet u Novom Sadu, 2003.

[KU] Kag, M., Ulam, S.: *PMatematika i logika*, Školska knjiga Zagreb, 1997.

[SL] S. Lipshitz: *Set theory*, Schaum's outline series McGrouw - Hill, 1964.

[VT] V. Trostnikov: *Što su konstruktivni postupci u matematici*, MM Školska knjiga, Zagreb, 1983.

[SH] S. Hedman: *A first course in Logic*, Oxford, 2004.

Indeks