[1] Опис лиценци Креативне заједнице доступан је на адреси creativecommons.org.rs/?page_id=74.

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET

Boris Šobot

Teorijski osnovi informatike I

- sa zbirkom zadataka -

Novi Sad, 2017.

Naziv udžbenika: ,,Teorijski osnovi informatike I”
Autor: dr Boris Šobot, vanredni profesor
Prirodno-matematičkog fakulteta u Novom Sadu
Recenzenti: dr Miloš Racković, redovni profesor
Prirodno-matematičkog fakulteta u Novom Sadu
dr Milan Vidaković, redovni profesor
Fakulteta tehničkih nauka u Novom Sadu
dr Nebojša Mudrinski, vanredni profesor
Prirodno-matematičkog fakulteta u Novom Sadu
Izdavač: Prirodno-matematički fakultet u Novom Sadu
Univerzitet u Novom Sadu
Glavni i odgovorni urednik pojedinačnog izdanja: dr Milica Pavkov Hrvojević,
dekan Prirodno-matematičkog fakulteta u Novom Sadu

CIP - каталогизација у публикацији
Библиотека Матице српске, Нови Сад

004(075.8)

ШОБОТ, Борис

Teorijski osnovi informatike I [Elektronski izvor] : sa zbirkom zadataka / Boris Šobot. - Novi Sad : Prirodno-matematički fakultet, 2017

Način pristupa (URL): https://www.pmf.uns.ac.rs/studije/epublikacije/matinf/sobot_teorijski_osnovi_informatike.pdf - Nasl. s naslovnog ekrana. - Opis zasnovan na stanju na dan 14. 8. 2017. - Bibliografija. - Registar.

ISBN 978-86-7031-362-0

a) Информатика
COBISS.SR-ID 316452103

Sadržaj

Predgovor

Ova knjiga nastala je prvenstveno kao udžbenik za predmet *Teorijske osnove informatike I*, držan studentima informatike na Prirodno-matematičkom fakultetu u Novom Sadu. Međutim, nadam se da će biti od koristi i drugim informatičarima koji žele da se upoznaju sa nekim matematičkim temama koje su povezane sa računarstvom.

Na početku, želeo bih da navedem nekoliko ključnih reči koje smatram bitnim za izloženi materijal:

- *Razumevanje.* Verujem da učenje matematike ,,napamet" ne vodi ničemu i stoga ova knjiga nije spisak šablona za izračunavanje i konstrukciju raznih objekata. Iako će jedan od ciljeva biti da se čitaocu približi intuitivno shvatanje svakog od uvedenih pojmova, insistiraće se i na preciznom definisanju i dokazivanju. Čitalac će moći po želji da preskoči poneki složeniji dokaz, ali će većina njih ipak biti uključeni (bar kao ideje) kako bi se bolje razumelo ne samo kako, već i zašto nešto radi. Izuzetak će, naravno, biti teoreme čiji dokazi po složenosti znatno prevazilaze nivo ove knjige.

- *Apstrakcija.* Jedan od glavnih razloga zbog kojeg je matematika teška je njena apstraktnost. Glavni pojmovi opisani u ovoj knjizi (relacije, funkcije itd.) dobijeni su izdvajanjem zajedničkih osobina raznih objekata i cilj njihovog uvođenja je da nam pruži jezik koji će nam omogućiti baratanje širokim opsegom takvih objekata. Da bi se prevazišle teškoće nastale apstrakcijom svaka nova definicija propraćena je brojnim primerima koji treba da pomognu čitaocu da razume novi pojam.

- *Povezivanje.* Skoro svaki pojam i tvrđenje koje se pojavljuju u knjizi biće osnova za nove pojmove i tvrđenja. Pored toga, pokušao sam da, gde god je to moguće, gradivo bude povezano s programiranjem i drugim oblastima informatike s kojim će se čitalac sretati kasnije.

Često se postavlja pitanje: da li je, i u kojoj meri, informatičarima potrebno znanje matematike? Verujem da poznavanje pojmova matematičke logike omogućava pogled ,,odgore" na konkretne objekte s kojima se radi u informatici. Ali, pored znanja, bitne su i ideje i način razmišljanja koji se razvija prilikom dokazivanja matematičkih problema. Analogija, koja će često biti korišćena u ovoj knjizi, neophodna je svakom informatičaru da bi umeo da jednom viđene ideje za rešavanje jednog prilagodi i primeni na rešavanje drugih, sličnih problema.

Verovatno ne postoji savršen način za izlaganje ove materije. Detaljna obrada pojmova iz teorije skupova, relacija i funkcija pre iskaznog i predikatskog računa značila bi da se lišavamo mnogih prednosti baratanja iskaznim i predikatskim formulama. S druge strane, poznavanje osnovnih pojmova iz navedenih tema biće potrebno za razumevanje nekih delova gradiva iskaznog i predikatskog

računa. Stoga se u prvoj glavi daje pregled predznanja neophodnih za razumevanje sadržaja koji dolaze kasnije; nekih tema ćemo se dotaći samo nakratko (skupovi, relacije, funkcije), a detaljnije ih izučavati u kasnijim glavama.

U drugoj glavi izložene su osnove iskaznog računa. Akcenat je na tautologijama - najopštijim pravilima matematičkog zaključivanja. Međutim, kroz razne metode dokazivanja tautologija biće predstavljene i najbitnije strategije rešavanja matematičkih problema (svođenje na protivrečnost, rastavljanje na slučajeve itd.) Na nekoliko primera upoznaćemo se i sa intuitivnim pojmom algoritma.

Treća glava predstavlja kratak uvod u predikatski račun. Predikatske formule su osnova za precizno izražavanje u svim oblastima matematike, ali mogu biti od koristi i informatičaru (videti npr. odeljak 3.8). Veliki broj zadataka s konstrukcijom modela formula treba da pomogne čitaocu da nauči da pravilno čita i razume formule. Prilikom konstrukcija nekih od njih biće u izvesnoj meri korišćeno i znanje iz naredne dve glave, pa se čitaocu preporučuje da takve zadatke preskoči i vrati se na njih nakon boljeg upoznavanja s relacijama i funkcijama. U ovoj glavi biće pomenuti i logički programski jezici, koji za osnovu imaju upravo predikatski račun.

Osnovni pojmovi četvrte glave su skupovi i relacije. Posebnu pažnju posvećujemo relacijama poretka i relacijama ekvivalencije. Biće prikazan i način na koji n-arne relacije služe kao osnova za tzv. relacioni model baza podataka.

Funkcije se izučavaju u poslednjoj glavi. Iako se pojmovi funkcija u matematici i programiranju znatno razlikuju, pravilno shvatanje prvog od njih od velikog je značaja za razumevanje drugog. Takođe se uvodi i pojam kardinalnosti skupa i navode osnovne činjenice vezane za pojam beskonačnosti.

Svaka glava sadrži i veliki broj pratećih zadataka. Složeniji zadaci iz ovih tema mogu se naći u [20].

Pomenimo još neka pitanja koja se prirodno postavljaju kada se pristupa pisanju ovakve knjige. Pre svega, kakav nivo formalnosti i preciznosti odabrati? U nekim slučajevima neformalno objašnjenje bolje doprinosi razumevanju izloženog nego striktan dokaz. S druge strane, jedan od ciljeva ovog udžbenika je da uputi čitaoca u pravilno i precizno izvođenje i zapisivanje tvrđenja i dokaza. Stoga sam se odlučio za srednje rešenje: neki dokazi su izloženi precizno (pogotovo ako oni ilustruju ranije uvedene logičke metode dokazivanja) a neki su dati samo kroz ideje.

Što se tiče zapisa, on je većinom standardan. Jedna od specifičnosti je što prilikom ekvivalencijskih transformacija koristimo oznaku $\sim$ umesto $\Leftrightarrow$, kao i $\models$ umesto $\Rightarrow$ u koracima u kojima izvodimo posledice. Time se izbegava dvosmislenost u zapisu: da li $\Leftrightarrow$ predstavlja deo formule koju transformišemo ili relaciju između dve formule? Treba napomenuti da smo iste oznake koristili i u opštijem smislu, prilikom korišćenja dodatnih uslova zadatih u tvrđenju (npr. ako je zadato $A \subseteq B$, tokom izvođenja koristimo $x \in A \models x \in B$) u cilju izbegavanja uvođenja dodatnih oznaka i komplikovanja zapisa.

Na nekoliko mesta u knjizi uključeno je i nekoliko kratkih programskih segmenata. Oni su pisani u programskom jeziku Java, ali isto ili slično izgledaju i u C-u i srodnim jezicima; verujemo da svako ko je upoznat s osnovama programiranja neće imati problema da ih razume.

Želeo bih da se zahvalim recenzentima: dr Milošu Racković, dr Milanu Vidakoviću i dr Nebojši Mudrinskom, na savetima i sugestijama kojima su doprineli poboljšanju ovog teksta. Branislav Šobot je takođe pažljivo pročitao tekst. Zahvalnost dugujem i svim nastavnicima i saradnicima koji su radili na ovom predmetu i njegovim ranijim inkarnacijama. Mnoge ideje o sadržaju i

poneki primer potiču iz sjajne knjige [4] koju preporučujem za dalje čitanje i koja pokriva još neke teme koje ovde nisu obrađene. Na kraju, posebno se zahvaljujem svojoj porodici koja mi uvek pruža bezrezervnu podršku i ljubav koje mi omogućuju da se posvetim svom poslu.

Novi Sad, 16. 5. 2017. Boris Šobot

Glava 1

Uvod

1.1 Skupovi

Pojam skupa u ovoj knjizi nećemo precizno definisati, nego ćemo baratati intuitivnom predstavom o skupovima kao kolekcijama nekih elemenata. Razlog za to je činjenica da je za precizno uvođenje pojma skupa neophodan složen sistem aksioma. Jedan takav sistem, koji je danas u širokoj upotrebi, je Zermelo-Frenkelov (ZF) sistem o kojem zainteresovani čitalac može naći mnogo u knjizi [6].

Ako je x element skupa A, to zapisujemo ovako: $x \in A$. Da x nije element skupa A pišemo $x \notin A$.

Za neke važne skupove koristićemo standardne oznake, koje će se u ostatku knjige podrazumevati. To su: N - skup prirodnih brojeva, Z - skup celih brojeva, Q - skup racionalnih brojeva i R - skup realnih brojeva. Ove skupove možemo formalno zasnovati na nekoliko načina; neki od njih prikazani su u knjigama [19] i [11]. Napomenimo još da se nula nekad smatra prirodnim brojem, a nekada ne; u ovoj knjizi iz praktičnih razloga smatraćemo da $0 \notin N$.

Skupove možemo zadavati na nekoliko načina. Prvi je direktno nabrajanje elemenata u vitičastim zagradama, npr. $\{1, 2, 3\}$. Ovakvo zadavanje ima jedno veliko ograničenje: njime možemo definisati samo konačne skupove. Stoga često koristimo i zapis $\{x \in A : \varphi(x)\}$, gde je A neki već poznati skup; on nam daje podskup skupa A kojeg čine elementi koji zadovoljavaju formulu $\varphi(x)$. Recimo, $\{x \in R : x > 10\}$ označava skup realnih brojeva većih od 10. Naravno, ovakvim zapisom moći ćemo se mnogo slobodnije koristiti kada se upoznamo bolje sa predikatskim formulama.

Ponekad se prethodni zapis skraćuje izostavljanjem skupa A ako je iz konteksta jasno o kojem skupu se radi. Recimo, u zapisu $\{x : 3 \mid x\}$ kojim se definiše skup brojeva deljivih sa 3 obično se podrazumeva da su u pitanju celi brojevi. Ali ovakav zapis može biti dvosmislen, npr. $\{x : x > 10\}$ može biti shvaćeno kao $\{x \in R : x > 10\}$ ili kao $\{x \in N : x > 10\}$. Postoji još jedan razlog zašto ovakvo zadavanje treba izbegavati: ovakvim zapisom može se dobiti i nešto što formalno, prema aksiomama teorije skupova, uopšte nije skup. Tako, kolekcija $\{x : x = x\}$ bi obuhvatala previše elemenata da bi oni mogli ,,stati" u skup. Neprecizna formulacija pojma skupa, po kojoj bi i navedena kolekcija bila skup, početkom prošlog veka je dovela do pojave tzv. Raselovog paradoksa koja je izazvala veliku krizu u matematici, rešenu upravo uvođenjem precizne aksiomatike.

Konačno, skupove možemo zadavati i na treći način. Ako zapišemo $\{t(x) :$

$x \in A\}$, gde je A ponovo neki poznati skup a t izraz (izraze, odnosno termove ćemo takođe precizno definisati u glavi posvećenoj predikatskom računu), dobijamo skup svih vrednosti terma $t(x)$ za $x \in A$. Npr. $\{x^2 : x \in N\}$ je skup svih potpunih kvadrata, odnosno kvadrata prirodnih brojeva.

Možemo zaključiti da se svaki skup može zapisati na više načina. Najbolji način zapisivanja je, naravno, onaj koji je najlakši za razumevanje.

1.2 Relacije

Ako je n prirodan broj, *n-arna relacija* P na skupu A opisuje odnos između n elemenata tog skupa. Sa $P(x_1, x_2, \ldots, x_n)$ označava se da su elementi $x_1, x_2, \ldots, x_n$ u relaciji P.

U ovom, uvodnom odeljku o relacijama bavićemo se samo tzv. unarnim i binarnim relacijama. *Unarne* relacije (za $n = 1$) opisuju osobine koje mogu imati elementi nekog skupa, dakle sa $P(x)$ označavaćemo da je element x u relaciji P. *Binarne* relacije opisuju odnose između parova elementa nekog skupa: sa $P(x, y)$ označavamo da su x i y u relaciji P. Za binarne relacije često koristimo i tzv. infiksni zapis i pišemo xPy umesto $P(x, y)$.

Relacije možemo predstavljati direktnim zadavanjem elemenata koji su u relaciji ili formulom. Za unarne i binarne relacije na konačnim skupovima možemo koristiti i tablicu u kojoj sa $\top$ označimo elemente (ili parove elemenata) koje su u relaciji, a sa $\bot$ one koje nisu. Binarne relacije na konačnom skupu možemo predstavljati i grafički, tzv. grafom relacije (o tome više u odeljku 4.5). Predstavljanje formulama za sada ćemo posmatrati samo intuitivno, pošto ćemo se s njima detaljnije upoznati tek u glavi 3.

Primer 1.1 *(1) Na skupu N definišimo relaciju: $P(x)$ ako je x paran broj. To je jedna unarna relacija i možemo je formulom zapisati ovako: $P(x)$ ako $2 \mid x$. Dakle, važi $P(2)$ ali ne i $P(3)$.*

(2) Slično, na skupu $A = \{-2, -1, 0, 1, 2\}$ možemo definisati unarnu relaciju ovako: $Q(x)$ ako je x pozitivan broj. Ona se može prikazati formulom: $Q(x)$ ako $x > 0$. Kako je skup A konačan, ovu relaciju možemo predstaviti i tablicom:

Q	
-2	$\bot$
-1	$\bot$
0	$\bot$
1	$\top$
2	$\top$

Tablicu čitamo na sledeći način: elementi pored kojih stoji $\top$ su u relaciji Q, a oni pored kojih stoji $\bot$ nisu.

(3) Na proizvoljnom skupu možemo posmatrati relaciju jednakosti $=$. Tako, na skupu $B = \{1, 2, 3\}$ je recimo $= (1, 1)$, što češće pišemo u infiksnoj notaciji kao $1 = 1$; s druge strane nije $2 = 3$. Binarne relacije takođe možemo predstavljati tablicama:

$=$	1	2	3
1	$\top$	$\bot$	$\bot$
2	$\bot$	$\top$	$\bot$
3	$\bot$	$\bot$	$\top$

Tablicu binarne relacije čitamo ovako: ako je u polje u preseku vrste jednog i kolone drugog elementa upisano $\top$, to znači da je prvi od ta dva elementa u relaciji s drugim; u suprotnom oni nisu u relaciji.

(4) Na svakom skupu imamo i relaciju $\neq$. I ova relacija se može prikazati tablicom, npr. na skupu $B = \{1, 2, 3\}$:

$\neq$	1	2	3
1	$\bot$	$\top$	$\top$
2	$\top$	$\bot$	$\top$
3	$\top$	$\top$	$\bot$

(5) Relacija $<$ na skupu N može se zadati ovako: $m < n$ ako postoji $k > 0$ takvo da je $m + k = n$; naravno, parova elemenata koji su u relaciji sada ima beskonačno mnogo: $1 < 2$, $1 < 3$, $2 < 4, \ldots$ pa ovu relaciju ne možemo zadati nabrajanjem elemenata koji su u relaciji niti tablicom.

(6) Slično prethodnom primeru, na skupu N imamo i relaciju $\leq$: $m \leq n$ ako postoji $k \geq 0$ takvo da je $m + k = n$.

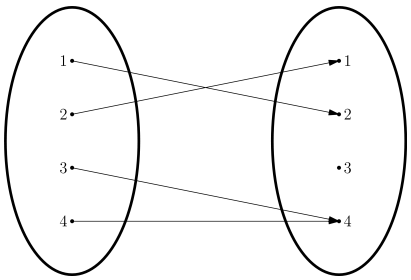
(7) Na skupu N možemo posmatrati i relaciju deljivosti koju takođe zapisujemo infiksno: $x \mid y$ (videti definiciju 1.4).

1.3 Funkcije

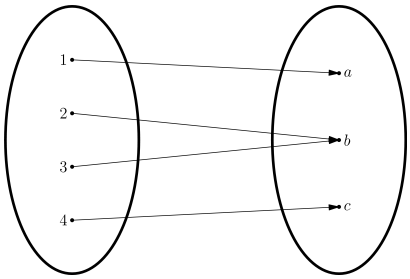
Funkcija f koja preslikava skup A u skup B svakom elementu $a \in A$ pridružuje tačno jedan element $b \in B$ (kažemo: preslikava a u b). To pišemo $f(a) = b$.

Za funkciju f koja preslikava skup A u skup B skup A zovemo *domen*, a skup B *kodomen* te funkcije; tada pišemo $f : A \to B$. Funkcije možemo predstavljati izrazom koji opisuje kako se iz x izračunava $f(x)$, dijagramom, kao i tablicom.

Primer 1.2 *(1) Obeležimo $A = \{1, 2, 3, 4\}$. Jedna funkcija $f : A \to A$ zadata je ovako: $f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 4 \end{pmatrix}$. To znači da se element 1 slika u 2, 2 u 1, a 3 i 4 u 4. Ovo se može prikazati i dijagramom:*



(2) Za $A = \{1, 2, 3, 4\}$ i $B = \{a, b, c\}$ jedna funkcija $g : A \to B$ data je ovako: $g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & b & c \end{pmatrix}$. Primetimo da je dozvoljeno da se različiti elementi domena, 2 i 3, preslikavaju u isti element b kodomena. Evo i dijagrama:



(3) $\begin{pmatrix} 1 & 2 & 3 & 3 \\ a & b & c & d \end{pmatrix}$ *nije funkcija, jer nije dozvoljeno da se jedan element domena (u ovom slučaju 3) preslikava u više različitih elemenata kodomena (c i d).*

Posebna vrsta funkcija su operacije na nekom skupu. *n-arna operacija* na skupu A preslikava n-torke elemenata skupa A u skup A.

Kao i u slučaju relacija, za $n = 1$ dobijamo *unarne*, za $n = 2$ *binarne*, a za $n = 3$ ternarne operacije.

Primer 1.3 *(1) Izrazom $f(x) = x - 1$ zadata je jedna unarna operacija na skupu R (ili na skupu Z). Primetimo da ovo nije operacija na skupu N, jer je $f(1) = 0$, a 0 ne pripada skupu N.*

(2) Izrazi $f(x, y) = x + y$, $g(x, y) = x - y$ i $h(x, y) = x \cdot y$ definišu tri binarne operacije na skupu R. Ali $d(x, y) = \frac{x}{y}$ nije operacija na skupu R, jer nije definisano $d(x, 0)$. Međutim, ona jeste operacija na skupu $R \setminus \{0\}$.

(3) Binarne operacije, slično binarnim relacijama, možemo zadavati tablicama. Za to imamo dva načina, npr. na skupu $\{1, 2, 3\}$ možemo zadati jednu operaciju ovako:

h	1	2	3
1	2	2	1
2	3	2	1
3	2	3	3

x	y	$h(x, y)$
1	1	2
1	2	2
1	3	1
2	1	3
2	2	2
2	3	1
3	1	2
3	2	3
3	3	3

Prvu tablicu čitamo ovako: npr. rezultat operacije $h(2, 3)$ nalazi se u preseku vrste koja odgovara elementu 2 i kolone koja odgovara elementu 3, pa je $h(2, 3) = 1$. U drugoj tablici potražimo vrstu koja odgovara paru $x = 2$, $y = 3$, dakle $h(2, 3) = 1$.

(4) Izrazom $f(x, y, z) = x + y^z$ zadata je jedna ternarna operacija na skupu R.

U izrazu $f(x, y)$ elementi x i y se nazivaju argumenti ili parametri funkcije. Važno je razumeti da, ako je funkcija zadata nekim izrazom (kao u prethodnom primeru), taj izraz samo daje „šemu" za računanje rezultata funkcije. Dakle, ako je $f(x) = x - 1$, onda je, za bilo koju drugu vrednost argumenta y (iz domena funkcije), $f(y) = y - 1$, kao i $f(x + y) = x + y - 1$ (ako je i zbir $x + y$ u domenu funkcije).

1.4 Teorija brojeva

Kako će mnogi primeri u ovoj knjizi biti vezani za pojmove teorije brojeva, u ovom odeljku dajemo kratak pregled neophodnog predznanja. Čitaoca zainteresovanog za ovu oblast upućujemo na knjigu [9].

Kao što znamo, svaki ceo broj a može se podeliti bilo kojim celim brojem $b \neq 0$ i pritom se dobijaju količnik q i ostatak r, takav da $0 \leq r < b$, koji su jedinstveno određeni relacijom $a = bq + r$. Kada je ostatak pri deljenju jednak nuli, kažemo da je broj a deljiv brojem b.

Definicija 1.4 *Broj $a \in Z$ deljiv je brojem $b \in Z$ ($b \neq 0$) ako je $a = bq$ za neko $q \in Z$. To pišemo $b \mid a$ a čitamo takođe i: b deli a.*

U preostalim definicijama ograničićemo se samo na prirodne brojeve, mada se neke od njih mogu formulisati i za cele brojeve uopšte.

Definicija 1.5 *Najveći zajednički delilac prirodnih brojeva a i b je najveći prirodan broj d takav da $d \mid a$ i $d \mid b$. On se označava sa $NZD(a, b)$.*

Najmanji zajednički sadržalac prirodnih brojeva a i b je najmanji prirodan broj s takav da $a \mid s$ i $b \mid s$. On se označava sa $NZS(a, b)$.

Kažemo da su prirodni brojevi a i b uzajamno prosti ako je $NZD(a, b) = 1$, odnosno ako oni nemaju drugih zajedničkih delitelja osim jedinice.

Definicija 1.6 *Prirodan broj $n > 1$ je prost ako nema drugih delitelja osim samog sebe i jedinice; u suprotnom je složen.*

Primetimo da se 1 ne smatra ni prostim ni složenim brojem. Takođe je važno razlikovati pojam prostog broja od pojma uzajamno prostih brojeva: relacija ,,biti prost broj" je unarna - govori samo o osobini jednog broja, dok je relacija ,,brojevi su uzajamno prosti" binarna - govori o međusobnom odnosu dva broja.

Za kraj ovog odeljka dajemo dve teoreme koje će biti korišćene kasnije.

Teorema 1.7 *Iz $n \mid a$ i $n \mid b$ sledi $n \mid a + b$.*

Dokaz. $n \mid a$ i $n \mid b$ znače da je $a = nk$ i $b = nl$ za neke $k, l \in Z$. Tada je $a + b = n(k + l)$, pa i $n \mid a + b$. □

Teorema 1.8 (Osnovna teorema aritmetike) *Svaki prirodan broj $n > 1$ može se na jedinstven način predstaviti kao proizvod prostih činilaca:*

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},$$

gde su, dakle, $p_1, p_2, \dots, p_k$ različiti prosti brojevi a $a_1, a_2, \dots, a_k \in N$.

1.5 Matematička indukcija

Pretpostavimo da želimo da dokažemo neko tvrđenje oblika ,,Za svaki prirodan broj n važi $T(n)$", gde je $T(n)$ neka tvrdnja o broju n. Problem je u tome što prirodnih brojeva ima beskonačno mnogo pa je nemoguće za sve njih direktno proveriti $T(n)$. *Matematička indukcija* je veoma moćan metod za dokazivanje takvih tvrđenja.

Postoji nekoliko oblika matematičke indukcije. Krenimo od najjednostavnijeg:

1. baza indukcije: dokaže se $T(1)$;
2. indukcijska hipoteza: pretpostavimo da, za neko $n \in N$, važi $T(n)$;
3. indukcijski korak: dokažemo, koristeći indukcijsku hipotezu, da važi i $T(n+1)$.

Zašto iz svega ovog sledi da $T(n)$ važi za svako $n \in N$? Za početak, $T(1)$ je dokazano direktno. Kako iz $T(n)$ sledi $T(n+1)$ za svako n, specijalno iz $T(1)$ sledi $T(2)$, dakle i $T(2)$ je tačno. Zatim iz $T(2)$ sledi $T(3)$ i tako dalje, šematski:

$$T(1) \to T(2) \to T(3) \to T(4) \to \dots$$

Baza indukcije (kraće: B.I.) se obično lako proverava, ali se ne sme izostaviti jer je ona „temelj" cele konstrukcije. U indukcijskoj hipotezi (I.H.) ništa se ne dokazuje, već se samo postavlja pretpostavka o tačnosti tvrđenja za neko $n \in N$. Konačno, indukcijski korak (I.K.) je glavni deo metoda, prelaz sa n na $n+1$. Kako je ovo i najsloženiji deo dokaza, pogodno je na početku indukcijskog koraka zapisati kako tačno glasi $T(n+1)$ koje pokazujemo.

Primer 1.9 *Dokažimo da za svako $n \in N$ važi $1+2+\ldots+n = \frac{n(n+1)}{2}$.*

B.I. Za $n = 1$ treba proveriti da li je $1 = \frac{1\cdot 2}{2}$, što je očigledno tačno.

I.H. Pretpostavimo da za neko $n \in N$ važi $1+2+\ldots+n = \frac{n(n+1)}{2}$.

I.K. Dokažimo da tada važi i $1+\ldots+n+(n+1) = \frac{(n+1)(n+2)}{2}$. Najvažnije je uočiti kako iskoristiti indukcijsku hipotezu; u ovom primeru primećujemo da se leva strana jednakosti koju dokazujemo sastoji iz leve strane jednakosti iz I.H. kojoj je dodat još jedan sabirak, $n+1$. Stoga je

$$1+\ldots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

što je i trebalo dokazati.

Napomenimo da ova verzija indukcije ima i razne varijacije, npr. ako tvrđenje dokazujemo samo za prirodne brojeve $n \geq 2$ (recimo zato što ono ne važi za $n = 1$), tada u bazi indukcije dokazujemo $T(2)$ (videti zadatak 3).

Druga varijanta indukcije koristi se kada nam je za dokazivanje indukcijskog koraka potrebno da pretpostavimo da tvrđenje važi za dva (ili više) prethodna prirodna broja:

1. baza indukcije: dokaže se $T(1)$ i $T(2)$;
2. indukcijska hipoteza: pretpostavimo da, za neko $n \in N$, važi $T(n-1)$ i $T(n)$;
3. indukcijski korak: dokažemo, koristeći indukcijsku hipotezu, da važi i $T(n+1)$.

Zašto i ova šema zaista dokazuje da $T(n)$ važi za svako $n \in N$? Za početak, $T(1)$ i $T(2)$ su direktno dokazani. Iz indukcijskog koraka sledi da $T(1)$ i $T(2)$ povlače i $T(3)$, iz $T(2)$ i $T(3)$ sledi i $T(4)$ itd. Naravno, i ovde dokazivanje ne mora početi baš od $n = 1$.

Primer 1.10 *Dokažimo: ako je broj $x + \frac{1}{x}$ ceo, onda je ceo i broj $x^n + \frac{1}{x^n}$ za sve $n \in N$. Da bismo sebi olakšali dokazivanje, krenimo od $n = 0$ (iako se taj slučaj ne traži u zadatku, lakši je za proveru nego $n = 2$).*

B.I. Za $n = 0$ *je* $x^0 + \frac{1}{x^0} = 1 + 1 = 2$*, što je ceo broj.*
Za $n = 1$ *nam je dato u zadatku da je broj* $x^1 + \frac{1}{x^1} = x + \frac{1}{x}$ *ceo.*
I.H. Pretpostavimo da su za neko $n \in N$ *brojevi* $x^{n-1} + \frac{1}{x^{n-1}}$ *i* $x^n + \frac{1}{x^n}$ *celi.*
I.K. Treba dokazati da je i $x^{n+1} + \frac{1}{x^{n+1}}$ *ceo broj. Primetimo da je*

$$\left(x^n + \frac{1}{x^n}\right)\left(x + \frac{1}{x}\right) = x^{n+1} + \frac{1}{x^{n+1}} + x^{n-1} + \frac{1}{x^{n-1}}, \tag{1.1}$$

odnosno $x^{n+1}+\frac{1}{x^{n+1}} = (x^n+\frac{1}{x^n})(x+\frac{1}{x})-(x^{n-1}+\frac{1}{x^{n-1}})$ *pa je, prema indukcijskoj hipotezi, i to ceo broj.*

Ovde nije bilo unapred očigledno da treba koristiti ovu varijantu indukcije, ali kada u indukcijskom koraku stignemo do jednakosti (1.1) vidimo da nam je neophodno da znamo da su i $x^{n-1} + \frac{1}{x^{n-1}}$ *i* $x^n + \frac{1}{x^n}$ *celi da bismo zaključili da je* $x^{n+1} + \frac{1}{x^{n+1}}$ *ceo broj.*

Još nekoliko primera primene matematičke indukcije srešćemo u odeljku 5.6. Specijalno, ovakav vid indukcije prirodno se primenjuje kod rekurzivnih definicija dubine 2 ili više.

Najopštiji vid indukcije, takozvana *totalna indukcija*, izgleda ovako:

1. baza indukcije: dokaže se $T(1)$;

2. indukcijska hipoteza: pretpostavimo da za sve $k < n$ važi $T(k)$;

3. indukcijski korak: dokažemo, koristeći indukcijsku hipotezu, da važi i $T(n)$.

Dakle, ovu verziju indukcije koristimo kada, da bismo dokazali $T(n)$, moramo da znamo da tvrđenje važi za sve prirodne brojeve manje od n. Tipičan primer je oslabljena varijanta Osnovne teoreme aritmetike (teorema 1.8), koju ćemo sada dokazati. U njoj, naime, nećemo dokazivati jedinstvenost opisanog predstavljanja broja n, već samo da to predstavljanje postoji.

Primer 1.11 *Dokažimo da se svaki prirodan broj veći od 1 može predstaviti kao proizvod prostih brojeva.*

B.I. $n = 2$ *je prost, pa se samim tim može predstaviti preko prostih činilaca.*

I.H. Pretpostavimo da se svaki prirodan broj veći od 1 a manji od n može predstaviti kao proizvod prostih činilaca.

I.K. Dokažimo da to važi i za broj n. Ako je on sam prost, kao u bazi indukcije nemamo šta da dokazujemo. U suprotnom, on ima delilac k takav da je $1 < k < n$*. To dalje znači da je* $n = kl$ *za neki ceo broj l i takođe mora biti* $1 < l < n$ *(npr. ako bi bilo* $l = 1$ *to bi značilo da je* $k = n$*). Primenimo indukcijsku hipotezu na k i na l:* $k = p_1p_2 \dots p_r$ *i* $l = q_1q_2 \dots q_s$*, gde su* $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ *prosti. Ali to znači da je* $n = p_1p_2 \dots p_rq_1q_2 \dots q_s$*; dobili smo predstavljanje broja n preko prostih činilaca.*

Treba obratiti pažnju da u prethodnom primeru, gde smo indukcijsku hipotezu primenjivali na brojeve k i l, nismo imali nikakvu informaciju o tome za koliko su k i l manji od n. Baš to je razlog iz kojeg smo morali koristiti totalnu indukciju.

1.6 Zadaci

1. Dokazati da za svako $n \in N$ važi:
   (a) $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$;
   (b) $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.
2. Dokazati da za sve $n \in N$ važi $2^n > n$.
3. Dokazati da za sve prirodne brojeve $n \geq 5$ važi $2^n > n^2$.
4. Dokazati da za sve $n \in N$ važi:
   (a) $8|(3^{2n} - 1)$;
   (b) $17|(3 \cdot 5^{2n+1} + 2^{3n+1})$.
5. Iz table 128×128 isečeno je jedno polje. Dokazati da dobijenu figuru možemo pokriti figurama od tri polja u obliku slova L:

(Figure se ne smeju preklapati a dozvoljeno ih je rotirati. Svaka od figura mora pokriti tačno po 3 polja.)

Glava 2

Iskazni račun

2.1 Iskazne formule

Mnoge rečenice iz svakodnevnog života sadrže neke delove koji mogu biti tačni ili netačni. U matematici je to još češća pojava. Rečenicu koja može biti tačna (tu vrednost označavamo $\top$) ili netačna (to označavamo $\bot$) zovemo *iskaz*.

Primer 2.1 *Neki iskazi su: (a) ,,2+2=4"; (b) ,,Ja imam 19 godina"; (c) ,,Za godinu dana imaću 1000000 dolara". Primetimo da nije neophodno da nam bude poznata tačnost neke rečenice da bi ona bila iskaz.*

Evo još jednog primera: Goldbahova hipoteza tvrdi da se svaki paran prirodan broj veći od 2 može predstaviti kao zbir dva prosta broja. Recimo, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$ *itd. I to je jedan iskaz, iako ne znamo da li je tačan ili ne.*

Od iskaza dalje možemo graditi složenije rečenice pomoću tzv. iskaznih veznika. Sa $\neg$ ćemo označavati negaciju, sa $\wedge$ konjunkciju (u svakodnevnom govoru veznik ,,i"), sa $\vee$ disjunkciju (,,ili"), sa $\Rightarrow$ implikaciju (kojoj odgovara jezička konstrukcija ,,ako... onda...") i sa $\Leftrightarrow$ ekvivalenciju (,,ako i samo ako"). Pre nego što pređemo na formalnije definicije, pogledajmo neke primere.

Primer 2.2 *(a) ,,Učiću ili neću položiti ispit." U ovoj rečenici imamo dva iskaza: sa p ćemo označiti ,,učiću", a sa q ,,položiću ispit" (uvek za iskaze uzimamo najmanje delove rečenice koji imaju vrednost* $\top$ *ili* $\bot$*). Tada ovu rečenicu možemo predstaviti formulom* $p \vee \neg q$.

(b) ,,Ako ne budem učio, neću položiti ispit." Uz iste oznake kao gore, dobijamo formulu $\neg p \Rightarrow \neg q$.

(c) ,,Položiću ispit samo ako budem učio." Ponovo uz iste oznake, imamo formulu $q \Rightarrow p$.

Ako pogledamo bolje, sve tri rečenice iz prethodnog primera govore istu stvar. Jedan od zadataka iskaznog računa je upravo da obezbedi mehanizam za proveru ovakvih zapažanja. Drugi i najvažniji njegov zadatak je da izdvoji najopštije zakone logičkog razmišljanja, koje ćemo zvati tautologije. Kao što ćemo videti, ova dva zadatka su usko povezana jedan s drugim.

Da bismo pristupili rešavanju ovih zadataka, moramo (za početak) znati preciznije kako se grade *iskazne formule*. One se sastoje od tri vrste simbola; to su:

1. iskazna slova: $p, q, r, \ldots$, ili sa indeksima: $p_1, p_2, \ldots$
2. iskazni veznici: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ i
3. zagrade: (i).

Pritom, iskazna slova u formulama zamenjuju iskaze. Međutim, ove ,,sastojke" ne možemo kombinovati na proizvoljan način da bismo dobili formule. Precizan postupak opisan je pomoću sledeća tri pravila.

Definicija 2.3 *1. Iskazna slova su iskazne formule.*

2. Ako su A i B iskazne formule, onda su to i: $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$ i $(A \Leftrightarrow B)$.

3. Iskazne formule mogu se dobiti samo konačnim brojem primena pravila 1 i 2.

Ovakav način definisanja naziva se *rekurzivna definicija*. U ovom slučaju to znači sledeće: prvim pravilom definisane su najjednostavnije formule, a drugo pravilo opisuje kako se od jednostavnijih grade složenije. Treće pravilo nas ograničava precizirajući da ništa ne može biti iskazna formula ako nije dobijena pomoću prva dva pravila, i to samo u konačno mnogo koraka. Više o pojmu rekurzije biće reči u odeljku 5.6.

U ovoj glavi često ćemo umesto ,,iskazna formula" pisati samo ,,formula".

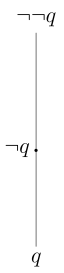
Primer 2.4 *Neke iskazne formule su:*

(1) p. Ona je dobijena direktno iz pravila 1.

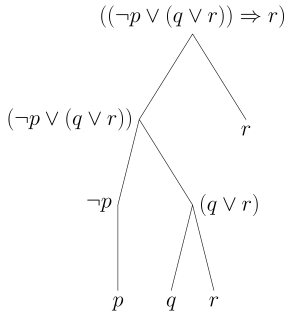
(2) $\neg\neg q$. Do nje dolazimo ovako: prvo, prema pravilu 1 q je formula. Prema pravilu 2 dalje sledi da je i $\neg q$ formula. Ponovnom primenom pravila 2 dobijamo da je i $\neg\neg q$ formula.

(3) $((\neg p \vee (q \vee r)) \Rightarrow r)$. Iz pravila 1 dobijamo da su p, q i r formule. Sada nekoliko puta primenjujemo pravilo 2 i dobijamo redom formule: $\neg p$, $(q \vee r)$, $(\neg p \vee (q \vee r))$ i na kraju $((\neg p \vee (q \vee r)) \Rightarrow r)$.

Svaka formula dobijena u nekom od koraka izgradnje formule F naziva se *podformula* formule F. Npr. za formulu iz dela (3) prethodnog primera podformule su: p, q, r, $\neg p$, $(q \vee r)$, $(\neg p \vee (q \vee r))$ i na kraju sama formula $((\neg p \vee (q \vee r)) \Rightarrow r)$. Da bismo bolje sagledali postupak izgradnje jedne formule, za nju možemo nacrtati tzv. *drvo podformula*. To je ustvari grafički prikaz svih podformula neke formule, gde su ispod svake podformule dobijene pravilom 2 prikazane formule od kojih je ona dobijena. Evo primera drveta podformula za dve formule iz prethodnog primera:



Slika 2.1: Drvo podformula za formulu $\neg\neg q$



Slika 2.2: Drvo podformula za $((\neg p \vee (q \vee r)) \Rightarrow r)$

Kako primene pravila 2 (osim u slučaju negacije) dodaju po jedan par zagrada, ovim postupkom često dobijamo formule sa velikim brojem zagrada, što ih čini teško čitljivim. Da bismo ovo ublažili, uvešćemo nekoliko neformalnih pravila o izostavljanju zagrada.

1. Spoljne zagrade u svakoj formuli se izostavljaju; npr. umesto $((\neg p \vee (q \vee r)) \Rightarrow r)$ pišemo $(\neg p \vee (q \vee r)) \Rightarrow r$.

2. Ako se u formuli meša nekoliko uzastopnih istih veznika $\wedge$ ili $\vee$, zagrade se izostavljaju, npr. umesto $(\neg p \vee (q \vee r)) \Rightarrow r$ pišemo samo $(\neg p \vee q \vee r) \Rightarrow r$. Ovim naravno skraćeni oblik $\neg p \vee q \vee r$ može da predstavlja dve različite formule ali, kao što ćemo videti kasnije, ovo je opravdano time što su te dve formule ekvivalentne.

3. Operacijama $\wedge$ i $\vee$ dodeljujemo veći prioritet u odnosu na $\Rightarrow$ i $\Leftrightarrow$; to znači da, ako se u nekoj formuli mešaju npr. $\wedge$ i $\Rightarrow$, zagrade se podrazumevaju oko konjunkcije. Dakle, umesto $(\neg p \vee q \vee r) \Rightarrow r$ možemo pisati samo $\neg p \vee q \vee r \Rightarrow r$.

Poslednja dva pravila u gornjoj definiciji sasvim su analogna pravilima izostavljanja zagrada u aritmetičkim izrazima. Npr. u izrazu $1 + (2 + 3)$ rezultat će biti isti i ako zagrade stoje drugačije: $(1 + 2) + 3$, odnosno ako računamo prvo zbir $1 + 2$, a onda to saberemo sa 3; stoga se u takvim izrazima zagrade ni ne pišu. Takođe, množenje ima prioritet u odnosu na sabiranje, pa se i u izrazu $1 + (2 \cdot 3)$ zagrade mogu izostaviti.

Za kraj ovog odeljka, prikazaćemo na jednom jednostavnom primeru kako funkcioniše tzv. indukcija po složenosti formule u iskaznom računu. U svakom takvom dokazu koristićemo sledeću oznaku: sa $v(F)$ obeležićemo broj veznika koji se pojavljuju u formuli F; npr. za formulu $F = (p \wedge \neg q) \vee \neg r$ je $v(F) = 4$: ona ima dva veznika negacije i po jedan veznik konjunkcije i disjunkcije. (U ovom tvrđenju privremeno zanemarujemo naš dogovor o izostavljanju zagrada i smatramo da se formule grade striktno po definiciji 2.3.)

Teorema 2.5 *Svaka iskazna formula F ima isti broj levih i desnih zagrada.*

Dokaz. Dokaz sprovodimo indukcijom po broju veznika u formuli F. Obeležimo sa $l(F)$ broj levih, a sa $d(F)$ broj desnih zagrada u F.

B.I. $v(F) = 0$. Tada je formula F samo iskazno slovo, pa je $l(F) = d(F) = 0$.

I.H. Pretpostavimo da svaka formula sa manje od n veznika ima isti broj levih i desnih zagrada.

I.K. Neka je $v(F) = n$. Formula je tada dobijena drugim pravilom iz definicije 2.3, pa može biti jednog od sledećih 5 oblika: $\neg G$, $(G \wedge H)$, $(G \vee H)$, $(G \Rightarrow H)$ ili $(G \Leftrightarrow H)$. Zato posmatramo 5 slučajeva.

1° $F = \neg G$. Tada se sve zagrade formule F nalaze i u formuli G, pa kako G ima $n-1$ veznika, po indukcijskoj hipotezi je $l(G) = d(G)$, te sledi i $l(F) = l(G) = d(G) = d(F)$.

2° $F = (G \wedge H)$. Tada su leve zagrade formule F one koje se javljaju u G, one koje se javljaju u H i još jedna na samom početku formule F. Dakle $l(F) = l(G) + l(H) + 1$. Analogno je i $d(F) = d(G) + d(H) + 1$. Međutim, formule G i H imaju svaka po manje od n veznika (jer ih ukupno imaju $n-1$, pošto veznik konjunkcije između njih ne pripada nijednoj od njih), pa za njih važi indukcijska hipoteza: $l(G) = d(G)$ i $l(H) = d(H)$. Dakle i $l(F) = d(F)$.

Ostala tri slučaja razmatraju se potpuno analogno drugom. □

2.2 Tačnost formula

Sada kada znamo kako se grade formule, vreme je da preciziramo značenje iskaznih veznika. Za svaki od njih imamo po jednu operaciju na skupu $\{\top, \bot\}$ (videti odeljak 1.3 o operacijama), označenu istim simbolom. Operacija $\neg$ je unarna, što znači da deluje na jedan argument, a ostale su binarne (imaju po dva argumenta). Te operacije date su tablicama:

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

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

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

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

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

Ove tablice uglavnom odgovaraju našoj intuiciji, objašnjenje je potrebno možda samo za operaciju $\Rightarrow$. Ona je definisana tako da daje vrednost $\bot$ samo ako je leva strana (pretpostavka) tačna, a desna (zaključak) netačna. Dakle, iz netačne pretpostavke možemo izvesti bilo kakav zaključak (tačan ili netačan). Stoga, prilikom dokazivanja tvrđenja oblika $A \Rightarrow B$ pretpostavljamo da važi A (,,leva strana") i dokazujemo B. S druge strane, kada treba u dokazu da iskoristimo uslov oblika $A \Rightarrow B$ potrebno je prvo proveriti da važi A, iz čega zatim možemo izvesti B.

Naredni primer (preuzet iz knjige [21]) bolje će ilustrovati smisao implikacije.

Primer 2.6 *Dat je špil karata koje na prednjoj strani imaju brojeve od 1 do 10, a pozadina im je plava ili crvena. Na osnovu sledeće informacije:*

Karte sa parnim brojem na prednjoj strani imaju crvenu pozadinu

odrediti šta možemo reći o drugoj strani karata kojima se s jedne strane nalazi:

(a) broj 4;

(b) broj 5;

(c) crvena pozadina;

(d) plava pozadina?

Odgovori:

(a) Kako je broj na ovoj karti paran, njena pozadina mora biti crvena.

(b) Za drugu kartu ne znamo da li je njena pozadina plava ili crvena: karte sa neparnim brojem ne moraju imati plavu pozadinu (jer formula $\neg p \Rightarrow \neg q$ ne znači isto što i formula $p \Rightarrow q$).

(c) Za treću kartu ne znamo da li je broj s njene prednje strane paran ili neparan: karte s crvenom pozadinom ne moraju imati zapisan paran broj (jer formula $q \Rightarrow p$ ne znači isto što i formula $p \Rightarrow q$).

(d) Četvrta karta s prednje strane mora imati neparan broj: kada bi on bio paran, njena pozadina morala bi biti crvena.

Formulu oblika $A \Rightarrow B$ možemo izraziti kao ,,ako A, onda B", ali i kao ,,A samo ako B". Kako je formula $A \Leftrightarrow B$ ekvivalentna sa konjunkcijom formula $A \Rightarrow B$ i $B \Rightarrow A$ (ovo ćemo dokazati kasnije), $A \Leftrightarrow B$ se obično čita kao ,,A ako i samo ako B", a skraćeno se piše i kao ,,A akko B". Takođe, kako $A \Rightarrow B$ znači da je A dovoljan, a $B \Rightarrow A$ da je i potreban uslov za B, $A \Leftrightarrow B$ možemo čitati i kao ,,A je potreban i dovoljan uslov za B".

Sada uvodimo pojam valuacije; intuitivno, ona dodeljuje svakom iskaznom slovu jednu od vrednosti $\top$ ili $\bot$. Formalno, ako sa V označimo skup svih iskaznih slova, *valuacija* je funkcija $\alpha : V \to \{\top, \bot\}$.

Sada, ako su nam vrednosti iskaznih slova zadate nekom valuacijom, možemo izračunati i *vrednost* proizvoljne formule F koristeći gornje tablice; nju označavamo sa $v_\alpha(F)$. To radimo prema sledećim pravilima, prateći definiciju 2.3.

Definicija 2.7 *1. $v_\alpha(F) = \alpha(F)$ ako je F iskazno slovo.*

2. $v_\alpha(\neg A) = \neg v_\alpha(A)$.

3. $v_\alpha(A \wedge B) = v_\alpha(A) \wedge v_\alpha(B)$.

4. $v_\alpha(A \vee B) = v_\alpha(A) \vee v_\alpha(B)$.

5. $v_\alpha(A \Rightarrow B) = v_\alpha(A) \Rightarrow v_\alpha(B)$.

6. $v_\alpha(A \Leftrightarrow B) = v_\alpha(A) \Leftrightarrow v_\alpha(B)$.

Dakle, vrednost se prvo izračuna za najjednostavnije podformule, a to su iskazna slova. Zatim se ona računa za sve složenije podformule, sve do same zadate formule. U praksi se, naravno, zadaju samo vrednosti slova koja učestvuju u formuli koju posmatramo.

Primer 2.8 *Ako je iskaz ,,učiću" netačan ($\alpha(p) = \bot$) a iskaz ,,položiću ispit" tačan ($\alpha(q) = \top$), za formule iz primera 2.2 imamo:*

(a) $v_\alpha(p \vee \neg q) = v_\alpha(p) \vee v_\alpha(\neg q) = \alpha(p) \vee \neg\alpha(q) = \bot \vee \neg\top = \bot \vee \bot = \bot$.

(b) $v_\alpha(\neg p \Rightarrow \neg q) = v_\alpha(\neg p) \Rightarrow v_\alpha(\neg q) = \neg\alpha(p) \Rightarrow \neg\alpha(q) = \neg\bot \Rightarrow \neg\top = \top \Rightarrow \bot = \bot$.

(c) $v_\alpha(q \Rightarrow p) = v_\alpha(q) \Rightarrow v_\alpha(p) = \top \Rightarrow \bot = \bot$.

2.3 Tautologije

Ako nas zanimaju vrednosti neke formule F u svim valuacijama, njih brže računamo tzv. tabličnom metodom. Kolone tablice odgovaraju podformulama formule F, poređane od najjednostavnijih (to su iskazna slova) prema složenijim, od kojih je poslednja sama formula F. Vrste odgovaraju valuacijama (preciznije,

svim kombinacijama vrednosti onih iskaznih slova koja se javljaju u F). Zatim tablicu popunjavamo kolonu po kolonu, računajući vrednosti podformula u svim valuacijama.

Primer 2.9 *Izračunajmo vrednosti formule* $F = p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ *u svim valuacijama.*

p	q	r	$q \wedge r$	$p \wedge q$	$p \wedge (q \wedge r)$	$(p \wedge q) \wedge r$	F
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$

Vidimo da je formula F iz prethodnog primera uvek tačna (u svim valuacijama). Ovakve formule izražavaju najopštije logičke zakone i zato su nam od posebne važnosti.

Definicija 2.10 *Formula* F *je tautologija ako je tačna u svim valuacijama. To zapisujemo ovako:* $\models F$.

Formula F *je kontradikcija ako je netačna u svim valuacijama.*

Tablična metoda je jedan *algoritam* za proveru da li je data formula tautologija. To znači da ona opisuje precizan i efektivno izvodljiv postupak za tu proveru koji se sastoji iz konačnog broja koraka. Neformalno govoreći, algoritam nam daje ,,recept" kako doći do traženog rezultata, u kojem su koraci i njihov redosled jasno definisani. Proučavanje algoritama i njihove efikasnosti od velikog je značaja za svakog programera. Više na tu temu može se naći u knjigama [12] (s programerske) i [1] (s matematičke tačke gledišta).

Međutim, opisani algoritam je veoma neefikasan. Precizirajmo to.

Ako sa n označimo veličinu ulaznih podataka (za problem provere da li je F tautologija možemo uzeti da je to broj različitih iskaznih slova koja se pojavljuju u F) vremenska složenost algoritma može se izraziti kao neka funkcija sa parametrom n. Ako je ta funkcija polinom, kaže se da je problem *polinomne složenosti* i takvi algoritmi smatraju se (relativno) efikasnim. Međutim, uz nešto kombinatornog zaključivanja može se izračunati da, za formulu od n iskaznih slova, tablica koju dobijamo ima 2^n vrsta. To znači da je u pitanju algoritam *eksponencijalne složenosti*, dakle da broj operacija potrebnih za izvršenje algoritma veoma brzo raste sa porastom broja iskaznih slova.

Evo sada nekoliko važnih tautologija koje će nam biti od koristi u nastavku:

1. $p \Leftrightarrow p, p \vee \neg p$
2. $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$ (kontrapozicija)
3. $p \wedge p \Leftrightarrow p; \quad p \vee p \Leftrightarrow p$ (idempotentnost)
4. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r;$ (asocijativnost)
   $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r;$
   $(p \Leftrightarrow (q \Leftrightarrow r)) \Leftrightarrow ((p \Leftrightarrow q) \Leftrightarrow r)$
5. $p \wedge q \Leftrightarrow q \wedge p;$ (komutativnost)
   $p \vee q \Leftrightarrow q \vee p;$
   $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$
6. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r);$ (distributivnost)
   $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

7. $p \wedge (p \vee q) \Leftrightarrow p$; $p \vee (p \wedge q) \Leftrightarrow p$ (apsorpcija)
8. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$; $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ (De Morganovi zakoni)
9. $p \wedge (p \Rightarrow q) \Rightarrow q$ (modus ponens)
10. $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$
11. $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$; $\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$
12. $\neg\neg p \Leftrightarrow p$.

Pomenimo i jednu jednostavnu kontradikciju koja će nam biti od koristi: $p \wedge \neg p$.

S obzirom na neefikasnost tablične metode biće nam potrebni i drugi načini za proveru da li je data formula tautologija. Ovde ćemo opisati još dve metode, kroz koje ćemo se upoznati sa dve tipične ideje koje se koriste u matematičkim dokazima.

Prva od njih je *svođenje na protivrečnost* (svođenje na kontradikciju). Ideja je da pretpostavimo da formula F nije tautologija; to znači da postoji valuacija α za koju $v_\alpha(F) = \bot$. Odatle izvodimo vrednosti raznih podformula formule F, pokušavajući da dobijemo da ista podformula ima i vrednost $\top$ i vrednost $\bot$, što je naravno nemoguće. Ako uspemo u tome, to će značiti da je F tautologija. U suprotnom, možemo pokušati da nađemo vrednosti iskaznih slova, tj. valuaciju u kojoj je F netačna, što bi značilo da ona nije tautologija.

Primer 2.11 *Proverimo da li je* $F = p \wedge (q \vee r) \Rightarrow (p \wedge q) \vee (p \wedge r)$ *tautologija. Pretpostavimo suprotno, da postoji valuacija* α *za koju* $v_\alpha(F) = \bot$. *Odatle zaključujemo da je*

$$v_\alpha(p \wedge (q \vee r)) = \top \tag{2.1}$$
$$v_\alpha((p \wedge q) \vee (p \wedge r)) = \bot. \tag{2.2}$$

Iz (2.2) dalje imamo da je

$$v_\alpha(p \wedge q) = \bot \tag{2.3}$$
$$v_\alpha(p \wedge r) = \bot. \tag{2.4}$$

S druge strane, iz (2.1) imamo

$$\alpha(p) = \top \tag{2.5}$$
$$v_\alpha(q \vee r) = \top. \tag{2.6}$$

Sada iz (2.5) i (2.3) imamo $\alpha(q) = \bot$ *a iz (2.5) i (2.4) da je* $\alpha(r) = \bot$. *Međutim, to znači da je* $v_\alpha(q \vee r) = \bot$, *što je nemoguće zbog (2.6). Dakle,* F *je tautologija.*

Iz rezonovanja primenjenog u prethodnom primeru može se videti da ova metoda nije pogodna za sve formule. Konkretno, ona se primenjuje najbolje na formule oblika $A \Rightarrow B$ ili $A \vee B$, jer ako su one netačne, lako dobijamo vrednosti za A i B.

Sledeća je *metoda diskusije po iskaznom slovu*. U pitanju je, ustvari, rastavljanje na dva slučaja: izaberemo jedno iskazno slovo (npr. p) i posmatramo odvojeno slučaj $\alpha(p) = \top$ a odvojeno slučaj $\alpha(p) = \bot$. Zatim u svakom od njih pokušamo da izračunamo vrednost date formule F. Ako je F tačna u oba slučaja, ona je tautologija; u suprotnom ona to nije.

Primer 2.12 *Dokazaćemo da je* $G = p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ *tautologija diskusijom po slovu* p.

1° $\alpha(p) = \top$. *Tada je*

$$\begin{aligned} v_\alpha(G) &= v_\alpha(p \vee (q \wedge r)) \Leftrightarrow v_\alpha((p \vee q) \wedge (p \vee r)) \\ &= \alpha(p) \vee v_\alpha(q \wedge r) \Leftrightarrow v_\alpha(p \vee q) \wedge v_\alpha(p \vee r) \\ &= \alpha(p) \vee (\alpha(q) \wedge \alpha(r)) \Leftrightarrow (\alpha(p) \vee \alpha(q)) \wedge (\alpha(p) \vee \alpha(r)) \\ &= \top \vee (\alpha(q) \wedge \alpha(r)) \Leftrightarrow (\top \vee \alpha(q)) \wedge (\top \vee \alpha(r)) \\ &= \top \Leftrightarrow \top \wedge \top \\ &= \top \Leftrightarrow \top = \top. \end{aligned}$$

Naime, da bi disjunkcija $A \vee B$ bila tačna dovoljno je da bar jedna od formula A i B bude tačna. Na taj način vidimo da u ovom slučaju $v_\alpha(G)$ ne zavisi od $\alpha(q)$ i $\alpha(r)$, nego je uvek $\top$.

2° $\alpha(p) = \bot$. *Tada je*

$$\begin{aligned} v_\alpha(G) &= \alpha(p) \vee (\alpha(q) \wedge \alpha(r)) \Leftrightarrow (\alpha(p) \vee \alpha(q)) \wedge (\alpha(p) \vee \alpha(r)) \\ &= \bot \vee (\alpha(q) \wedge \alpha(r)) \Leftrightarrow (\bot \vee \alpha(q)) \wedge (\bot \vee \alpha(r)) \\ &= \alpha(q) \wedge \alpha(r) \Leftrightarrow \alpha(q) \wedge \alpha(r) = \top. \end{aligned}$$

Ovde smo u pretposlednjem koraku, recimo pri računanju $\bot \vee \alpha(q)$, zaključivali ovako: ako je $\alpha(q) = \top$ onda je i $\bot \vee \alpha(q) = \top$, a ako $\alpha(q) = \bot$ onda i $\bot \vee \alpha(q) = \bot$. Dakle, $\bot \vee \alpha(q) = \alpha(q)$.

U poslednjem koraku, vrednost $\alpha(q) \wedge \alpha(r) \Leftrightarrow \alpha(q) \wedge \alpha(r)$ mora biti $\top$, jer operacija $\Leftrightarrow$ daje vrednost $\top$ ako su leva i desna strana jednake.

Ako bismo formulu iz prethodnog primera proveravali tablicom, ona bi imala 8 vrsta. To znači da smo svakim od dva posmatrana slučaja „pokrili" po 4 vrste tablice i na taj način značajno skratili računanje. Moglo se, naravno, desiti i da sama vrednost slova p ne bude dovoljna da se izračuna $v_\alpha(G)$; u tom slučaju bi trebalo posmatrati podslučajeve, odnosno ponovo izabrati neko slovo i podeliti razmatranje na dva dela: kada ono ima vrednost $\top$ i kada ima vrednost $\bot$.

Kako izabrati slovo po kojem sprovodimo diskusiju? Najbolje je da to bude slovo od kojeg u najvećoj meri zavisi tačnost formule G. U većini slučajeva to je slovo koje se najviše puta pojavljuje u formuli, ali ne obavezno.

Teorema 2.13 *Ako $\models A$ i $\models A \Rightarrow B$, onda $\models B$.*

Dokaz. Neka su A i $A \Rightarrow B$ tautologije. Da bismo pokazali da je i B tautologija, uzmimo neku valuaciju α i pokažimo da je $v_\alpha(B) = \top$. Iz pretpostavke imamo da je $v_\alpha(A) = v_\alpha(A \Rightarrow B) = \top$. Ali ako bi bilo $v_\alpha(B) = \bot$, to bi sa $v_\alpha(A) = \top$ impliciralo $v_\alpha(A \Rightarrow B) = \bot$, što nije tačno. □

Ponekad, da bismo naglasili koja iskazna slova se javljaju u formuli F, umesto samo F pišemo $F(q_1, q_2, \ldots, q_k)$. Formulu dobijenu zamenom svih pojava slova q_i u F formulom B_i za $i = 1, 2, \ldots, k$ označavamo $F(B_1, B_2, \ldots, B_k)$.

Teorema 2.14 (O zameni) *Neka su $q_1, q_2, \ldots, q_k$ iskazna slova a $F(q_1, q_2, \ldots, q_k)$, $B_1, B_2, \ldots, B_k$ iskazne formule. Ako $\models F(q_1, q_2, \ldots, q_k)$, onda i $\models F(B_1, B_2, \ldots, B_k)$.*

Ideja dokaza. Da bismo dokazali da je $\models F(B_1, B_2, \ldots, B_k)$, uzmimo proizvoljnu valuaciju α. Definišimo pomoću nje novu valuaciju β: za $i = 1, 2, \ldots, k$ neka je $\beta(q_i) = v_\alpha(B_i)$. Kako je F tautologija, ona je tačna u valuaciji β. Ali

$v_\alpha(F(B_1, B_2, \ldots, B_k)) = v_\beta(F(q_1, q_2, \ldots, q_k))$; naime, prilikom izračunavanja vrednosti $v_\alpha(F(B_1, B_2, \ldots, B_k))$ mi ustvari ,,uvlačimo" v_α unutar formule (kao u primeru 2.8), sve dok ono ne bude delovalo na podformule B_i, a onda možemo zameniti svako $v_\alpha(B_i)$ sa $\beta(q_i)$, pa dobijamo vrednost $\top$. □

Primer 2.15 *U primeru 2.9 videli smo da je formula* $F(p, q, r) = p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ *tautologija. Ako u njoj zamenimo* p *sa* $A = p \vee q$ *a* q *sa* $B = q \Rightarrow r \wedge s$, *dobijamo formulu*

$$F(A, B, r) = (p \vee q) \wedge ((q \Rightarrow r \wedge s) \wedge r) \Leftrightarrow ((p \vee q) \wedge (q \Rightarrow r \wedge s)) \wedge r$$

koja je, dakle, takođe tautologija. Na ovaj način možemo iz svake tautologije dobiti još beskonačno mnogo novih, ali to suštinski najčešće nije veliki dobitak, jer ove, izvedene, tautologije ne daju nam suštinski nove logičke zakonitosti.

2.4 Semantičke posledice

Definicija 2.16 *Kažemo da je formula* A *semantička posledica formula* F_1, F_2, $\ldots, F_n$ *ako je u svakoj valuaciji u kojoj su tačne* $F_1, F_2, \ldots, F_n$ *tačna i formula* A. *To označavamo* $F_1, F_2, \ldots, F_n \models A$.

Umesto ,,semantička posledica" obično ćemo pisati samo ,,posledica", jer nećemo uvoditi druge vrste logičkih posledica formula.

Primetimo da, ako je A tautologija, onda je ona posledica praznog skupa formula: $\emptyset \models A$. Odatle potiče i korišćenje iste oznake.

Primer 2.17 *(1)* $p, p \Rightarrow q \models q$. *Neka je* α *valuacija takva da je* $v_\alpha(p) = v_\alpha(p \Rightarrow q) = \top$. *Iz ta dva uslova sledi i* $v_\alpha(q) = \top$. *(Uporediti ovo sa teoremom 2.13.)*

(2) $p \Rightarrow q, q \Rightarrow r \models p \Rightarrow r$. *Neka je* α *valuacija takva da je* $v_\alpha(p \Rightarrow q) = v_\alpha(q \Rightarrow r) = \top$. *Pretpostavimo suprotno, da je* $v_\alpha(p \Rightarrow r) = \bot$. *To znači da je* $v_\alpha(p) = \top$ *i* $v_\alpha(r) = \bot$. *Iz* $v_\alpha(p) = v_\alpha(p \Rightarrow q) = \top$, *kao u prvom primeru, dobijamo i* $v_\alpha(q) = \top$. *Zatim slično odatle i iz* $v_\alpha(q \Rightarrow r) = \top$ *imamo* $v_\alpha(r) = \top$, *kontradikcija.*

(3) $p \Rightarrow q, \neg p \Rightarrow q \models q$. *Neka za valuaciju* α *važi* $v_\alpha(p \Rightarrow q) = v_\alpha(\neg p \Rightarrow q) = \top$. *Ako pretpostavimo da je* $v_\alpha(q) = \bot$, *sledi* $v_\alpha(p) = \bot$ *i* $v_\alpha(\neg p) = \bot$, *što je nemoguće.*

Tokom izvođenja matematičkih dokaza veoma često koristimo razna logička pravila. Evo nekih primera; neka od ovih pravila biće korišćena već u dokazima teorema koje slede.

(1) Mnoga matematička tvrđenja oblika ,,ako p onda q" izvode se *kontrapozicijom*. To znači da ,,pretpostavimo suprotno", odnosno da je q netačno, pa pokušavamo da dobijemo da je i p netačno. Ovo opravdava sledeća činjenica: $\neg q \Rightarrow \neg p \models p \Rightarrow q$.

(2) Srodan način dokazivanja je *svođenje na kontradikciju*. Ako želimo da pokažemo da važi tvrđenje p, pokušamo umesto toga da iz $\neg p$ izvedemo kontradikciju $q \wedge \neg q$. Da je to dovoljno sledi iz $\neg p \Rightarrow q \wedge \neg q \models p$. Upravo smo ovu ideju koristili kao jedan od metoda dokazivanja tautologija.

(3) Često dokaz sprovodimo *rastavljanjem na slučajeve*. Ako obeležimo te slučajeve sa p_1 i p_2 (može ih biti i više, ali radi jednostavnosti uzimamo da ih je dva) i uverimo se da oni ,,pokrivaju" sve mogućnosti, odnosno da važi $p_1 \vee p_2$, onda je dovoljno dokazati da u svakom od tih slučajeva važi željeno tvrđenje q. Ovaj metod posledica je činjenice da $p_1 \vee p_2, p_1 \Rightarrow q, p_2 \Rightarrow q \models q$. Njen specijalan slučaj je i $p \Rightarrow q, \neg p \Rightarrow q \models q$. I ovu ideju smo već koristili, prilikom dokazivanja tautologija metodom diskusije po iskaznom slovu.

(4) Tvrđenje oblika ,,p ako i samo ako q" obično se dokazuje iz dva dela: ,,ako p onda q" i ,,ako q onda p". Ovakvo *razdvajanje na smerove* opravdava pravilo $p \Rightarrow q, q \Rightarrow p \models p \Leftrightarrow q$.

Već u sledeće dve teoreme imaćemo priliku da primenimo pravilo (4): razdvajanje na smerove. Smer ,,sleva na desno" označavaćemo sa ($\Rightarrow$) a smer ,,zdesna nalevo" sa ($\Leftarrow$).

Teorema 2.18 *$F_1, F_2, \ldots, F_n \models B$ ako i samo ako $\models F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B$.*

Dokaz. ($\Rightarrow$) Pretpostavimo da važi $F_1, F_2, \ldots, F_n \models B$. Neka je α proizvoljna valuacija. Posmatrajmo dva slučaja. Prvo, ako je $v_\alpha(F_1) = v_\alpha(F_2) = \ldots = v_\alpha(F_n) = \top$, onda iz pretpostavke imamo $v_\alpha(B) = \top$, pa je i $v_\alpha(F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B) = \top$. S druge strane, ako za bar jednu formulu F_i imamo $v_\alpha(F_i) = \bot$, onda i $v_\alpha(F_1 \wedge F_2 \wedge \ldots \wedge F_n) = \bot$, pa je opet $v_\alpha(F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B) = \top$. Dakle, formula $F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B$ je tautologija.

($\Leftarrow$) Neka je sada $F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B$ tautologija, i neka je α valuacija takva da su u njoj sve formule $F_1, F_2, \ldots, F_n$ tačne. Tada je i $v_\alpha(F_1 \wedge F_2 \wedge \ldots \wedge F_n) = \top$, pa kako je i $v_\alpha(F_1 \wedge F_2 \wedge \ldots \wedge F_n \Rightarrow B) = \top$, tačna je i formula B. □

Teorema 2.19 *$F_1, F_2, \ldots, F_n, A \models B$ ako i samo ako $F_1, F_2, \ldots, F_n \models A \Rightarrow B$.*

Dokaz. ($\Rightarrow$) Pretpostavimo da je $F_1, F_2, \ldots, F_n, A \models B$, i neka je data valuacija α u kojoj su tačne formule $F_1, F_2, \ldots, F_n$. Dokažimo da je u njoj tačna i formula $A \Rightarrow B$. Pretpostavimo suprotno, da je $v_\alpha(A) = \top$ i $v_\alpha(B) = \bot$. Ali tada je to valuacija u kojoj su tačne formule $F_1, F_2, \ldots, F_n$ i A, ali ne i B, što je kontradikcija.

($\Leftarrow$) Obratno, neka je $F_1, F_2, \ldots, F_n \models A \Rightarrow B$. Neka je α valuacija u kojoj su tačne formule $F_1, F_2, \ldots, F_n$ i A. Tada je, po pretpostavci, u njoj tačna i formula $A \Rightarrow B$, pa iz $v_\alpha(A) = v_\alpha(A \Rightarrow B) = \top$ dobijamo $v_\alpha(B) = \top$. □

Kao specijalan slučaj bilo koje od dve prethodne teoreme dobijamo sledeću posledicu.

Posledica 2.20 *$A \models B$ ako i samo ako $\models A \Rightarrow B$.*

2.5 Ekvivalentnost formula

U primeru 2.2 videli smo nekoliko formula za koje možemo reći da izražavaju isto. Sada ćemo to precizno definisati.

Definicija 2.21 *Kažemo da su formule A i B ekvivalentne (pišemo: $A \sim B$) ako za svaku valuaciju α važi $v_\alpha(A) = v_\alpha(B)$.*

Drugim rečima, dve formule su ekvivalentne ako imaju jednake istinitosne tablice.

Teorema 2.22 *$A \sim B$ ako i samo ako $\models A \Leftrightarrow B$.*

Dokaz. ($\Rightarrow$) Pretpostavimo prvo da je $A \sim B$. Tada za svaku valuaciju α imamo $v_\alpha(A) = v_\alpha(B)$, pa je $v_\alpha(A \Leftrightarrow B) = v_\alpha(A) \Leftrightarrow v_\alpha(B) = \top$.

($\Leftarrow$) Obratno, ako je $\models (A \Leftrightarrow B)$, to znači da je, za svaku valuaciju α, $v_\alpha(A \Leftrightarrow B) = v_\alpha(A) \Leftrightarrow v_\alpha(B) = \top$, što je tačno samo ako $v_\alpha(A) = v_\alpha(B)$. □

Na osnovu prethodnog tvrđenja već imamo nekoliko parova ekvivalentnih formula. Naime, u spisku važnih tautologija u prethodnom odeljku većina su oblika $A \Leftrightarrow B$. Tako je, na primer, $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p)$. Takođe dobijamo da je $p \wedge (q \wedge r) \sim (p \wedge q) \wedge r$ i $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$, što opravdava jednu od naših konvencija za izostavljanje zagrada u formulama.

Teorema 2.23 *$A \sim B$ ako i samo ako $A \models B$ i $B \models A$.*

Dokaz. Iz posledice 2.22 dobijamo da $A \sim B$ ako i samo ako $\models A \Leftrightarrow B$. Kako je $A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A)$, sledi da je $A \Leftrightarrow B$ tautologija akko su $A \Rightarrow B$ i $B \Rightarrow A$ tautologije, a ovo je prema teoremi 2.20 ekvivalentno sa $A \models B$ i $B \models A$. □

Teorema 2.24 *Za bilo koje formule A, B i C važi:*

(a) $A \sim A$;

(b) ako $A \sim B$ *onda* $B \sim A$;

(c) ako $A \sim B$ *i* $B \sim C$ *onda* $A \sim C$.

Dokaz. Dokazaćemo samo tvrđenje (c), ostala se ostavljaju čitaocu za laku vežbu. Neka je α proizvoljna valuacija. Tada, prema $A \sim B$ i $B \sim C$, imamo $v_\alpha(A) = v_\alpha(B)$ i $v_\alpha(B) = v_\alpha(C)$. Sledi da je $v_\alpha(A) = v_\alpha(C)$. Pošto to važi za svaku valuaciju α, sledi $A \sim C$. □

Teorema 2.25 *Za proizvoljne formule A_1, A_2, B_1, B_2 iz uslova $A_1 \sim A_2$ i $B_1 \sim B_2$ sledi:*

(a) $\neg A_1 \sim \neg A_2$;

(b) $(A_1 \wedge B_1) \sim (A_2 \wedge B_2)$;

(c) $(A_1 \vee B_1) \sim (A_2 \vee B_2)$;

(d) $(A_1 \Rightarrow B_1) \sim (A_2 \Rightarrow B_2)$;

(e) $(A_1 \Leftrightarrow B_1) \sim (A_2 \Leftrightarrow B_2)$.

Dokaz. Dokažimo opet, ilustracije radi, samo tvrđenje (b). Neka je α proizvoljna valuacija. Iz $A_1 \sim A_2$ i $B_1 \sim B_2$ sledi $v_\alpha(A_1) = v_\alpha(A_2)$ i $v_\alpha(B_1) = v_\alpha(B_2)$. Stoga je

$$v_\alpha(A_1 \wedge B_1) = v_\alpha(A_1) \wedge v_\alpha(B_1) = v_\alpha(A_2) \wedge v_\alpha(B_2) = v_\alpha(A_2 \wedge B_2).$$

Kako to važi za svaku valuaciju, dobijamo $(A_1 \wedge B_1) \sim (A_2 \wedge B_2)$. □

Prethodna dva tvrđenja osnova su za još jedan metod provere da li je data formula tautologija. Naime, ona nam omogućuju da zamenom neke podformule u formuli F njoj ekvivalentnom formulom dobijemo formulu ekvivalentnu sa F. Npr. ako je $F = A_1 \wedge B$ i $A_1 \sim A_2$, možemo zameniti A_1 sa A_2 i dobiti formulu $A_2 \wedge B$ ekvivalentnu sa F. Nadovezivanjem ovakvih koraka, koje zovemo *ekvivalencijske transformacije*, možemo dobiti da su dve tražene formule ekvivalentne.

Ovo u praksi možemo primenjivati na više načina. Prvi je da, ukoliko želimo da dokažemo da je formula oblika $F \Leftrightarrow G$ tautologija, ekvivalencijskim transformacijama svedemo F na G.

Primer 2.26 *Dokažimo* $\models \neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$. *Pritom koristimo ekvivalencijske transformacije koje slede iz tablice važnih tautologija (str. 20).*

$$\begin{aligned} \neg(p \Rightarrow q) &\sim \neg(\neg p \vee q) \\ &\sim \neg\neg p \wedge \neg q \\ &\sim p \wedge \neg q. \end{aligned}$$

Prilikom ekvivalencijskih transformacija često koristimo i teoremu o zameni. Recimo, u prethodnom primeru, kada smo koristili De Morganovo pravilo $\neg(x \vee q) \sim \neg x \wedge \neg q$ na mestu slova x bila je formula $\neg p$ pa smo dobili $\neg(\neg p \vee q) \sim \neg\neg p \wedge \neg q$.

Drugi način primene je da, sprovođenjem određenih transformacija, od formule F koju ispitujemo dobijemo njoj ekvivalentnu za koju je lako proveriti da li je tautologija. Ovom metodu biće posvećen sledeći odeljak.

Veliki broj zadataka u ovoj knjizi počinjaće sa: ,,konstruisati sve (do na ekvivalenciju) iskazne formule takve da...". Smisao izraza ,,do na ekvivalenciju" biće jasan tek pošto budu uvedene relacije ekvivalencije; za sada pomenimo samo da u takvom zadatku treba za svaku iskaznu tablicu koju može imati takva formula konstruisati po jednu formulu. Korišćenjem kanonskih formi (odeljak 2.7) to će biti jednostavno.

2.6 Konjunktivni i disjunktivni oblik

Proveravanje da li je data formula tautologija ekvivalencijskim transformacijama može biti prilično komplikovano, jer treba pravilno proceniti koju transformaciju primeniti u kojem koraku. Međutim, svođenje na konjunktivni oblik to znatno olakšava jer nam precizno opisuje redosled njihovog primenjivanja.

Konjunktivni oblik je formula oblika $C_1 \wedge C_2 \wedge \ldots \wedge C_n$, gde su $C_1, C_2, \ldots, C_n$ formule oblika $p_1 \vee p_2 \vee \ldots \vee p_k \vee \neg q_1 \vee \neg q_2 \vee \ldots \vee \neg q_l$, tzv. *klauze*. Iskazna slova i njihove negacije koje su delovi klauza zovemo *literali*.

Za svaku iskaznu formulu postoji njoj ekvivalentna formula u konjunktivnom obliku. Da bismo to pokazali, prikažimo algoritam za nalaženje te formule. On se sastoji u primenjivanju nekoliko ekvivalencijskih transformacija:

1. eliminacija veznika $\Leftrightarrow$ pomoću pravila $A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A)$;
2. eliminacija veznika $\Rightarrow$ pomoću pravila $A \Rightarrow B \sim \neg A \vee B$;
3. ,,uvlačenje" negacija unutar zagrada uz pomoć De Morganovih pravila: $\neg(A \wedge B) \sim \neg A \vee \neg B$ i $\neg(A \vee B) \sim \neg A \wedge \neg B$;
4. eliminisanje višestrukih negacija pravilom $\neg\neg A \sim A$;
5. primena distributivnosti $\vee$ prema $\wedge$: $A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$.

Pritom se sva navedena pravila primenjuju ,,sleva nadesno", tako da distributivnost služi za ,,ubacivanje" disjukcija unutar zagrada a ,,izvlačenje" konjunkcija napolje. Njena primena je potpuno analogna primeni distributivnosti množenja prema sabiranju u aritmetičkim izrazima: $a(b + c)$ zamenjujemo sa $ab + ac$. Stoga je možemo koristiti i slobodnije, kao u jednakosti $(a+b)(c+d) = ac + ad + bc + bd$; videti poslednji korak primera koji sledi.

Komutativnost i asocijativnost za obe operacije ćemo primenjivati bez posebnog naglašavanja i zamenjivati, recimo, $p \wedge q$ sa $q \wedge p$. I ovo je analogno aritmetičkim transformacijama gde i komutativnost i asocijativnost važe i za sabiranje i za množenje: $a + b = b + a$, $a(b \cdot c) = (a \cdot b)c$ itd.

Na kraju, formula u konjunktivnom obliku je tautologija ako i samo ako svaka klauza sadrži literale p i $\neg p$ za neko iskazno slovo p. Zaista, u svakoj valuaciji svaka klauza je tada tačna (jer sadrži deo $p \vee \neg p$ koji je tačan), a samim tim je tačna i njihova konjunkcija. S druge strane, ako neka klauza ne sadrži takve članove, možemo izabrati valuaciju u kojoj će slova koja se u toj klauzi javljaju negirana imati vrednost $\top$, a ostala vrednost $\bot$. U toj valuaciji ta klauza će biti netačna, a time i cela formula.

Primer 2.27 *Proverićemo da li je formula* $((p \vee q) \wedge (r \vee \neg q)) \vee \neg(p \Rightarrow r)$ *tautologija. Da bismo olakšali praćenje pojedinačnih koraka za svaki od njih naznačićemo koja je ekvivalencijska transformacija korišćena.*

$$\begin{aligned}
& ((p \vee q) \wedge (r \vee \neg q)) \vee \neg(p \Rightarrow r) \\
\overset{2}{\sim} \; & ((p \vee q) \wedge (r \vee \neg q)) \vee \neg(\neg p \vee r) \\
\overset{3}{\sim} \; & ((p \vee q) \wedge (r \vee \neg q)) \vee (\neg\neg p \wedge \neg r) \\
\overset{4}{\sim} \; & ((p \vee q) \wedge (r \vee \neg q)) \vee (p \wedge \neg r) \\
\overset{5}{\sim} \; & (p \vee q \vee p) \wedge (p \vee q \vee \neg r) \wedge (r \vee \neg q \vee p) \wedge (r \vee \neg q \vee \neg r).
\end{aligned}$$

Kako se bar u jednoj od klauza (recimo drugoj) ne javlja isto slovo i sa i bez negacije, formula nije tautologija. Štaviše, možemo naći valuaciju u kojoj će ta klauza (a samim tim i cela formula) biti netačna: $\alpha(p) = \bot$, $\alpha(q) = \bot$ *i* $\alpha(r) = \top$.

Pored ispitivanja tautologičnosti, često je za datu formulu bitno i da li je ona tačna bar u jednoj valuaciji, drugim rečima: da li formula nije kontradikcija? Za takve formule kažemo da su *zadovoljive*, a za valuacije u kojima su one tačne kažemo da su *modeli* tih formula.

Zadovoljivost date formule možemo proveravati svođenjem na *disjunktivni oblik*: $C_1 \vee C_2 \vee \ldots \vee C_n$, gde su $C_1, C_2, \ldots, C_n$ formule oblika $p_1 \wedge p_2 \wedge \ldots \wedge p_k \wedge \neg q_1 \wedge \neg q_2 \wedge \ldots \wedge \neg q_l$. Podformule $C_1, C_2, \ldots, C_n$ i ovde zovemo klauze, a iskazna slova i njihove negacije unutar klauza - literali. I za svođenje na disjunktivni oblik postoji algoritam, veoma sličan svođenju na konjunktivni oblik. Jedina ralika je u poslednjem koraku, koji izgleda ovako:

5'. primena distributivnosti $\wedge$ prema $\vee$: $A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C)$.

Sada je formula zadovoljiva ako bar jedna klauza ne sadrži članove oblika p i $\neg p$. Tada možemo definisati valuaciju u kojoj će slova koja su u tom članu negirana imati vrednost $\bot$, a ostala $\top$, pa će za tu valuaciju data formula biti tačna.

Primer 2.28 *Proverimo sada da li je formula* $F = ((p \vee q) \wedge (r \vee \neg q)) \vee \neg(p \Rightarrow r)$ *iz prethodnog primera barem zadovoljiva. Slično kao u tom primeru dobijamo*

$$\begin{aligned} & ((p \vee q) \wedge (r \vee \neg q)) \vee \neg(p \Rightarrow r) \\ \sim \quad & ((p \vee q) \wedge (r \vee \neg q)) \vee (p \wedge \neg r) \\ \overset{5'}{\sim} \quad & (p \wedge r) \vee (p \wedge \neg q) \vee (q \wedge r) \vee (q \wedge \neg q)) \vee (p \wedge \neg r). \end{aligned}$$

Kako imamo bar jednu klauzu (recimo prvu) u kojoj se ne javlja isto slovo i sa i bez negacije, lako nalazimo valuaciju u kojoj je ta klauza (pa i cela formula) tačna: $\alpha(p) = \top$ *i* $\alpha(r) = \top$ *(bez obzira na vrednost slova q). Dakle, F je zadovoljiva.*

U vezi sa konjunktivnim oblikom formule pomenimo i poznati *problem SAT*. On se sastoji u sledećem: za datu formulu F u konjunktivnom obliku proveriti da li je zadovoljiva. Razlog zbog kojeg je ovaj problem značajan u teoriji algoritama je što, iako je naizgled jednostavan, za njega nije poznat algoritam koji bi ga rešio u polinomnom vremenu. Preciznije, ako sa n označimo broj iskaznih slova koja se pojavljuju u F, ni za jedan poznati algoritam koji rešava problem SAT funkcija složenosti algoritma nije polinomna funkcija od argumenta n.

Štaviše, problem SAT pripada klasi tzv. NP-kompletnih problema. To znači da bi nalaženje algoritma polinomne složenosti koji rešava ovaj problem dalo i pozitivan odgovor na čuveni P=NP problem. (O klasi NP, problemu SAT i raznim drugim, kao i o problemu P=NP može se više naći u knjizi [1].)

2.7 Kanonske forme

Svakoj iskaznoj formuli $F(p_1, \ldots, p_n)$ odgovara istinitosna tablica čiju smo konstrukciju opisali u odeljku 2.3. Tom tablicom ustvari je definisana tzv. istinitosna funkcija $f : \{\top, \bot\}^n \to \{\top, \bot\}$ data sa $f(\alpha_1, \ldots, \alpha_n) = v_\alpha(F)$, gde je $\alpha_i = \alpha(p_i)$. Postavlja se pitanje: da li postoji i obrnut postupak rekonstruisanja formule iz njene istinitosne tablice, tj. nalaženja formule kojoj će odgovarati zadata istinitosna funkcija f? Odgovor je potvrdan.

Za početak, za svako iskazno slovo p obeležimo $p^\top = p$ i $p^\bot = \neg p$.

Disjunktivna kanonska forma (skraćeno: DKF), ili disjunktivna normalna forma istinitosne funkcije f je

$$\bigvee_{f(\alpha_1,\alpha_2,\ldots,\alpha_n)=\top} (p_1^{\alpha_1} \wedge p_2^{\alpha_2} \wedge \ldots \wedge p_n^{\alpha_n}).$$

Drugim rečima, za svaku valuaciju (tj. vrednosti $\alpha_1, \alpha_2, \ldots, \alpha_n$ slova $p_1, p_2 \ldots, p_n$) za koje je $f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \top$ imaćemo po jedan član - klauzu u disjunkciji. U tom članu nalaze se sva slova $p_1, p_2, \ldots, p_n$, ona koja u toj valuaciji imaju vrednost $\bot$ sa negacijom, a ostala bez negacije; njih i ovde zovemo literali.

Konjunktivna kanonska forma (skraćeno: KKF), ili konjunktivna normalna forma istinitosne funkcije f je

$$\bigwedge_{f(\alpha_1,\alpha_2,\ldots,\alpha_n)=\bot} (p_1^{\neg\alpha_1} \wedge p_2^{\neg\alpha_2} \wedge \ldots \wedge p_n^{\neg\alpha_n}).$$

Dakle, sada za svaku valuaciju u kojoj je f netačna imamo po jednu klauzu u konjunkciji. Ovaj put te klauze gradimo tako što kao literale ona slova koja u toj valuaciji imaju vrednost $\bot$ stavljamo bez negacije, a ostala sa negacijom.

Primer 2.29 *Nađimo formule u DKF i KKF čija je istinitosna tablica*

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$

Da bismo konstruisali DKF posmatramo prvu, četvrtu i osmu vrstu tablice. One redom daju klauze $p \wedge q \wedge r$, $p \wedge \neg q \wedge \neg r$ *i* $\neg p \wedge \neg q \wedge \neg r$, *pa je tražena DKF* $(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r)$.

Da bismo konstruisali KKF posmatramo ostalih pet vrsta (u kojima F *treba da bude netačna) i dobijamo formulu* $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r)$.

Zašto ovako dobijene formule zaista imaju zadatu istinitosnu funkciju? Objasnimo to prvo za DKF. Za svaku valuaciju u kojoj formula treba da bude tačna ona će sadržati klauzu konstruisanu tako da bude tačna baš u toj valuaciji (recimo u gornjem primeru za valuaciju u kojoj je $\alpha(p) = \top$, $\alpha(q) = \bot$ i $\alpha(r) = \bot$ ta klauza je $p \wedge \neg q \wedge \neg r$), pa kako je jedna klauza u disjunkciji tačna, i cela formula je tačna. S druge strane, za valuacije u kojima formula ne treba da bude tačna odgovarajuća klauza se ne nalazi u disjunkciji, pa će u svakoj od prisutnih klauza bar jedan literal imati vrednost $\bot$.

Slično je i kod KKF: za svaku valuaciju u kojoj formula treba da bude netačna imamo po jednu klauzu u kojoj će svi literali u toj valuaciji biti netačni, pa će i cela klauza, a samim tim i cela formula biti netačna. U ostalim valuacijama svaka klauza ima bar jedan tačan literal. Ovim smo dokazali sledeće tvrđenje.

Teorema 2.30 *(a) Za svaku istinitosnu funkciju koja nije netačna za sve vrednosti iskaznih slova postoji formula u DKF čija je to istinitosna funkcija.*

(b) Za svaku istinitosnu funkciju koja nije tačna za sve vrednosti iskaznih slova postoji formula u KKF čija je to istinitosna funkcija.

Primer 2.31 *Odredimo DKF i KKF za formulu* $F = \neg(p \Rightarrow q) \Rightarrow q \wedge \neg r$. *Konstruišimo prvo istinitosnu tablicu ove formule.*

p	q	r	$p \Rightarrow q$	$\neg(p \Rightarrow q)$	$\neg r$	$q \wedge \neg r$	F
$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\top$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$

Sada je odgovarajuća DKF:

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

a njena KKF:

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

Obe dobijene formule imaju istu istinitosnu tablicu kao F, dakle ekvivalentne su s njom.

2.8 Baze iskazne algebre

Svakom istinitosnom tablicom zadata je po jedna operacija iskazne algebre, odnosno funkcija $f : \{\top, \bot\}^k \to \{\top, \bot\}$. Svaku takvu operaciju možemo posmatrati kao još jedan dodatni iskazni veznik i koristiti je za formiranje jednog šireg skupa formula. U ovom odeljku ćemo, dakle, pod formulama podrazumevati i one koje su formirane analogno pravilima iz definicije 2.3, ali koristeći i ove dodatne operacije.

Primer 2.32 *Jedan primer unarne iskazne operacije je $\neg$. Neki primeri binarnih su $\wedge, \vee, \Rightarrow$ i $\Leftrightarrow$. Definišimo još neke:*

p	q	$\uparrow$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

p	q	$\downarrow$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

p	q	$\veebar$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Operaciju $\uparrow$ zovemo Šeferova, operaciju $\downarrow$ Lukasijevičeva operacija, a $\veebar$ zovemo ,,ekskluzivno ili". $\downarrow$ izražava rečenične strukture oblika ,,ni... ni...", a $\veebar$ strukture oblika ,,ili... ili...". Iz tablica možemo zaključiti da je $p \uparrow q \sim \neg(p \wedge q)$ i $p \downarrow q \sim \neg(p \vee q)$.

Definicija 2.33 *Kažemo da se operacija $*(p_1, p_2, \ldots, p_k)$ može izraziti preko operacija $f_1, f_2, \ldots, f_n$ ako postoji formula $G(p_1, p_2, \ldots, p_k)$ koja od operacija sadrži samo $f_1, f_2, \ldots, f_n$ i koja je ekvivalentna sa $*(p_1, p_2, \ldots, p_k)$.*

Primer 2.34 *(1) Kako je $p \Rightarrow q \sim \neg p \vee q$, operacija $\Rightarrow$ može se izraziti preko $\neg$ i $\vee$.*

(2) Pošto je $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p)$, $\Leftrightarrow$ se može izraziti preko $\Rightarrow$ i $\wedge$.

Treba obratiti pažnju da $\neg p \vee q \sim p \Rightarrow q$ ne znači da se $\neg$ i $\vee$ mogu izraziti preko $\Rightarrow$. Naime, izražavati možemo samo jednu po jednu operaciju.

Definicija 2.35 *Kažemo da je skup $\{f_1, f_2, \ldots, f_n\}$ operacija iskazne algebre baza iskazne algebre ako se svaka operacija iskazne algebre može izraziti preko $f_1, f_2, \ldots, f_n$.*

Uobičajeno je da se ovoj definiciji doda još jedan uslov: da taj skup bude *minimalan*, odnosno da nijedan njegov podskup s manje operacija nije dovoljan da se izraze sve operacije iskazne algebre. Mi radi pojednostavljenja izostavljamo taj drugi uslov.

Prema teoremi 2.30 za svaku operaciju $*$ iskazne algebre postoji formula u KKF ili DKF čija je istinitosna funkcija zadata sa $*$. Drugim rečima, svaka operacija iskazne algebre može se izraziti preko operacija $\neg$, $\wedge$ i $\vee$. Međutim, iz sledećeg tvrđenja ćemo videti da skup $\{\neg, \wedge, \vee\}$ nije minimalan.

Teorema 2.36 *Svaki od sledećih skupova je baza iskazne algebre:*

(a) $\{\neg, \vee\}$;

(b) $\{\neg, \wedge\}$;

(c) $\{\neg, \Rightarrow\}$.

Dokaz. (a) Operacija $\wedge$ može se izraziti preko $\neg$ i $\vee$ pomoću De Morganovih zakona: $p \wedge q \sim \neg\neg(p \wedge q) \sim \neg(\neg p \vee \neg q)$. Kako za svaku operaciju postoji njoj ekvivalentna formula u kojoj se javljaju samo $\neg$, $\vee$ i $\wedge$, na ovaj način možemo eliminisati $\wedge$ iz te formule i dobiti ekvivalentnu formulu u kojoj se javljaju samo $\neg$ i $\vee$.

(b) Dokaz se izvodi slično kao (a), pri čemu eliminišemo $\vee$ na sledeći način: $p \vee q \sim \neg\neg(p \vee q) \sim \neg(\neg p \wedge \neg q)$.

(c) Kao pod (a), polazeći od KKF ili DKF i koristeći transformacije $p \vee q \sim \neg p \Rightarrow q$ i $p \wedge q \sim \neg(\neg p \vee \neg q) \sim \neg(p \Rightarrow \neg q)$, dobijamo ekvivalentnu formulu u kojoj se javljaju samo $\neg$ i $\Rightarrow$. □

Ispostaviće se da je svaki od skupova iz prethodnog tvrđenja i minimalan. Da bismo to pokazali, treba da proverimo da nijedna od operacija $\neg$, $\wedge$, $\vee$ i $\Rightarrow$ nije sama za sebe dovoljna da se izraze sve operacije. To će slediti iz teoreme 2.40.

Teorema 2.37 *Svaka formula $F(p_1, p_2, \ldots, p_n)$ koja od logičkih veznika sadrži samo $\wedge$, $\vee$, $\Rightarrow$ i $\Leftrightarrow$ ima osobinu očuvavanja $\top$: u valuaciji α u kojoj su sva iskazna slova tačna važi i $v_\alpha(F) = \top$.*

Dokaz. Dokaz sprovodimo indukcijom po broju veznika $v(F)$.

B.I. $v(F) = 0$. U ovom slučaju F je samo iskazno slovo, recimo $F = p_i$. Iz $\alpha(p_i) = \top$ odmah sledi $v_\alpha(F) = \top$.

I.H. Pretpostavimo da tvrđenje važi za sve formule sa manje od n veznika među kojima su samo $\wedge$, $\vee$, $\Rightarrow$ i $\Leftrightarrow$.

I.K. Neka je sada $v(F) = n$. Formula F, pošto se u njoj ne pojavljuje veznik $\neg$, može biti jednog od 4 oblika: $G \wedge H$, $G \vee H$, $G \Rightarrow H$ ili $G \Leftrightarrow H$. Ispitajmo jedan od ovih slučajeva, recimo $F = G \Rightarrow H$, a ostali se proveravaju analogno.

Kako F ima ukupno n veznika, a jedan od njih je veznik implikacije između G i H, svaka od formula G i H ima po manje od n veznika. To po indukcijskoj hipotezi znači da one očuvavaju tačnost. Dakle, za valuaciju α u kojoj je $\alpha(p_1) = \ldots = \alpha(p_n) = \top$ imamo $v_\alpha(F) = v_\alpha(G) \Rightarrow v_\alpha(H) = \top \Rightarrow \top = \top$, pa i F očuvava tačnost. □

Teorema 2.38 *Skup $\{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ nije baza. (Dakle, nijedan njegov podskup nije baza.)*

Dokaz. Pretpostavimo suprotno; to bi značilo da se $\neg$ može izraziti preko operacija tog skupa: $\neg p \sim G(p)$, gde G sadrži samo veznike $\wedge, \vee, \Rightarrow$ i $\Leftrightarrow$. Uzmimo valuaciju α takvu da $\alpha(p) = \top$. Tada je $v_\alpha(\neg p) = \bot$, a prema teoremi 2.37 $v_\alpha(G) = \top$, što je nemoguće. □

Potpuno analogno teoremi 2.37 dokazuje se sledeća teorema.

Teorema 2.39 *Svaka formula $F(p_1, p_2, \ldots, p_n)$ koja od logičkih veznika sadrži samo $\wedge$ i $\vee$ ima osobinu očuvavanja $\bot$: u valuaciji α u kojoj su sva iskazna slova netačna važi i $v_\alpha(F) = \bot$.*

Primetimo da je za dokaz očuvavanja tačnosti bilo suštinski bitno to što $\top \wedge \top = \top \vee \top = \top \Rightarrow \top = \top \Leftrightarrow \top = \top$. Slično, za očuvavanje netačnosti bitno je $\bot \wedge \bot = \bot \vee \bot = \bot$, pa kako je $\bot \Rightarrow \bot = \bot \Leftrightarrow \bot = \top$, ova teorema ne važi za veznike $\Rightarrow$ i $\Leftrightarrow$.

Ako želimo da dokažemo da je i neki skup S iskaznih operacija baza, dovoljno je preko operacija iz S izraziti operacije neke poznate baze B; naime, dalje se preko operacija iz B (a samim tim i preko operacija iz S) mogu izraziti sve ostale operacije. U tu svrhu najčešće se koriste baze iz teoreme 2.36.

Teorema 2.40 *(a) Skupovi* $\{\uparrow\}$ *i* $\{\downarrow\}$ *su baze.*

(b) Jedine binarne istinitosne funkcije $*$ *takve da je* $\{*\}$ *baza su Šeferova i Lukasijevičeva operacija.*

Dokaz. (a) Kako je $\{\neg, \wedge\}$ baza, da bismo dokazali da je $\{\uparrow\}$ baza, dovoljno je preko operacije $\uparrow$ izraziti $\neg$ i $\wedge$:

$$p \uparrow p \sim \neg(p \wedge p) \sim \neg p$$
$$p \wedge q \sim \neg\neg(p \wedge q) \sim \neg(p \uparrow q) \sim (p \uparrow q) \uparrow (p \uparrow q).$$

(Treba primetiti da zbog teoreme 2.24(b) ekvivalentnost formula možemo čitati i zdesna nalevo, pa smo u prvom od dva reda izrazili $\neg$ preko $\uparrow$.)

Analogno se elementi baze $\{\neg, \vee\}$ izražavaju preko $\downarrow$, te je i $\{\downarrow\}$ baza.

(b) Pretpostavimo da je $*$ binarna operacija skupa $\{\top, \bot\}$ takva da je $\{*\}$ baza. Neka je njena istinitosna tablica

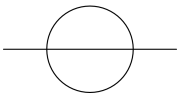
p	q	$p * q$
$\top$	$\top$	a
$\top$	$\bot$	b
$\bot$	$\top$	c
$\bot$	$\bot$	d

Kako se pomoću operacija koje očuvavaju tačnost ne može izraziti $\neg$ (videti dokaz teoreme 2.38), mora biti $a = \bot$. Analogno, ni preko operacije koje očuvavaju netačnost ne može se izraziti $\neg$ (teorema 2.39), pa mora biti $d = \top$. Ostaju još 4 načina kako se može do kraja popuniti gornja tablica, u zavisnosti od vrednosti b i c.

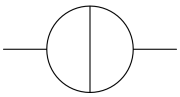
Ako je $b = c = \top$, to je tablica Šeferove, a ako je $b = c = \bot$ Lukasijevičeve operacije. Ostaje da se dokaže da preostale dve operacije, dobijene kombinacijama $b = \top$, $c = \bot$ i $b = \bot$, $c = \top$, ne čine baze. Ako obeležimo te dve operacije sa $*_1$ i $*_2$ redom, vidimo da je $p *_1 q \sim \neg q$ i $p *_2 q \sim \neg p$. Međutim, to su suštinski unarne operacije i nisu dovoljne da bi se preko njih izrazila ijedna od binarnih operacija $\wedge, \vee, \Rightarrow \ldots$ (videti zadatak 41). □

2.9 Primene iskaznih formula

Osnovni elementi *prekidačkih kola* su prekidači. Svaki od njih može biti u dva položaja, uključen i isključen:



Slika 2.3: Uključen prekidač

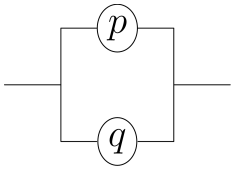


Slika 2.4: Isključen prekidač

Dakle, prekidač je uključen ako kroz njega prolazi struja a isključen u suprotnom. Ovi položaji odgovaraju redom logičkim vrednostima $\top$ i $\bot$ za neko iskazno slovo.

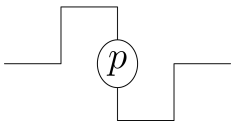
Više prekidača u kolo možemo vezivati redno ili paralelno:

Slika 2.5: Redno vezivanje



Slika 2.6: Paralelno vezivanje

Redno vezivanje odgovara konjunkciji: da bi struja proticala kroz taj deo kola potrebno je da oba prekidača budu uključena. Slično, paralelno vezivanje odgovara disjunkciji: da bi struja proticala dovoljno je da bar jedan od prekidača bude uključen. Negaciju ćemo predstavljati na sledeći način:

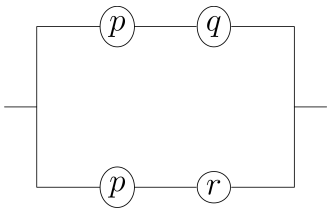


Slika 2.7: ,,Negacija" prekidača

Kroz ovako postavljen prekidač struja će proticati ako i samo ako je prekidač p isključen (ima vrednost $\bot$).

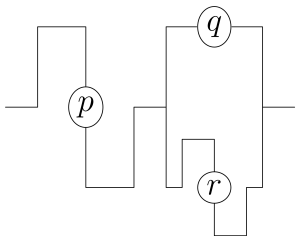
Kako je skup $\{\neg, \wedge, \vee\}$ jedna baza iskazne algebre, jasno je da svaku iskaznu funkciju možemo predstaviti prekidačkim kolom: zapišemo formulu koja odgovara toj funkciji (u kojoj negacije stoje samo uz iskazna slova, što je moguće postići primenom De Morganovih zakona), a nju je potom lako prevesti na prekidačko kolo.

Primer 2.41 *(1) Nacrtajmo prekidačko kolo koje odgovara formuli* $(p \wedge q) \vee (p \wedge r)$. *Prilikom skiciranja prekidačkog kola formulu razbijamo na podformule, od složenijih ka jednostavnijim, slično kao pri crtanju drveta podformula. Dakle, kolo ćemo dobiti paralelnom vezom kola za podformule* $p \wedge q$ *i* $p \wedge r$, *a svako od njih spajanjem rednom vezom odgovarajućih prekidača.*



Slika 2.8: Prekidačko kolo za formulu $(p \wedge q) \vee (p \wedge r)$

(2) Skicirajmo prekidačko kolo za formulu $\neg(p \vee (\neg q \wedge r))$. *Kako negaciju možemo primenjivati samo na pojedinačne prekidače, moramo prvo transformisati formulu:* $\neg(p \vee (\neg q \wedge r)) \sim \neg p \wedge \neg(\neg q \wedge r) \sim \neg p \wedge (q \vee \neg r)$.



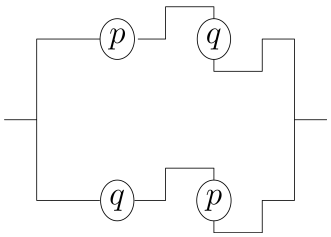
Slika 2.9: Prekidačko kolo za formulu $\neg p \wedge (q \vee \neg r)$

Naravno, mogli smo formulu transformisati i do nekog drugog oblika pa potom skicirati odgovarajuće kolo; ono će, jasno, biti ekvivalentno gornjem (struja će proticati kroz ta dva kola za iste položaje prekidača).

(3) Ako želimo da nacrtamo prekidačko kolo formule $p \underline{\vee} q$ *definisane u primeru 2.32, moramo prvo transformisati tu formulu i dobiti formulu u kojoj se pojavljuju samo veznici* $\neg$, $\wedge$ *i* $\vee$*:*

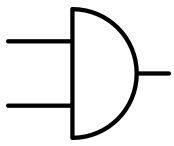
$$\begin{aligned} p \underline{\vee} q &\sim \neg(p \Leftrightarrow q) \\ &\sim \neg((p \Rightarrow q) \wedge (q \Rightarrow p)) \\ &\sim \neg((\neg p \vee q) \wedge (\neg q \vee p)) \\ &\sim (p \wedge \neg q) \vee (q \wedge \neg p), \end{aligned}$$

traženo prekidačko kolo može izgledati ovako:

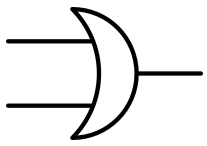


Slika 2.10: Prekidačko kolo za formulu $(p \wedge \neg q) \vee (q \wedge \neg p)$

Logička kola mogu imati nekoliko ulaza, na kojima se mogu pojavljivati vrednosti 0 i 1. Svaki ulaz odgovara po jednom iskaznom slovu u formuli, a vrednosti 0 i 1 odgovaraju vrednostima $\bot$ i $\top$ redom. Da bismo na izlazu dobili traženi rezultat, kombinujemo tri osnovna sklopa: I-sklop, ILI-sklop i NE-sklop, prikazana na sledećim slikama:



Slika 2.11: I-sklop



Slika 2.12: ILI-sklop

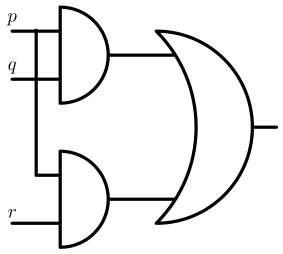
Slika 2.13: NE-sklop

Oni odgovaraju redom iskaznim operacijama konjunkcije, disjunkcije i negacije. Dakle, I-sklop i ILI-sklop imaju po dve, a NE-sklop jednu ulaznu vrednost. I-sklop daje na izlazu 1 ako i samo ako su vrednosti na oba ulaza 1; ILI-sklop daje na izlazu 1 ako i samo ako je bar jedna od ulaznih vrednosti 1 a NE-sklop daje na izlazu vrednost suprotnu onoj na ulazu.

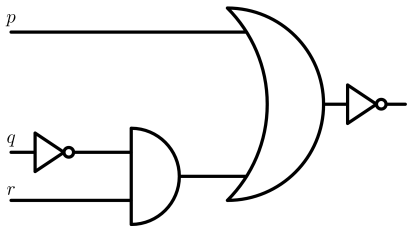
Kao i kod prekidačkih, i pomoću logičkih kola možemo izraziti svaku iskaznu funkciju. Naravno, kako za svaku iskaznu formulu možemo naći mnogo njoj ekvivalentnih formula, postoji jednako mnogo načina da se nacrta odgovarajuće logičko kolo. Za prevođenje formule u logičko kolo nije neophodno da negacije stoje samo ispred iskaznih slova, jer NE-sklop možemo primeniti na signal dobijen prethodnom primenom bilo kakvog dela kola.

Pošto su i $\{\neg, \wedge\}$ i $\{\neg, \vee\}$ baze, ustvari nam nisu neophodni i I-sklop i ILI-sklop, ali kola su znatno preglednija ako možemo da koristimo oba.

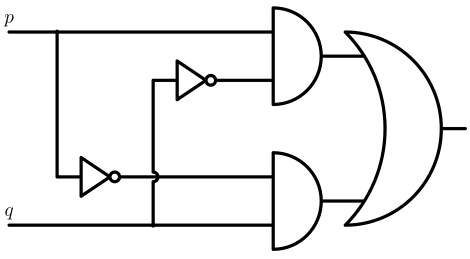
Primer 2.42 *Nacrtajmo logička kola koja odgovaraju formulama iz prethodnog primera. Razlika je u tome što prilikom konstruisanja logičkih kola krećemo od jednostavnijih podformula, pa ih ,,spajamo" sklopovima da bismo stigli do složenijih.*



Slika 2.14: Logičko kolo za formulu $(p \wedge q) \vee (p \wedge r)$



Slika 2.15: Logičko kolo za formulu $\neg(p \vee (\neg q \wedge r))$



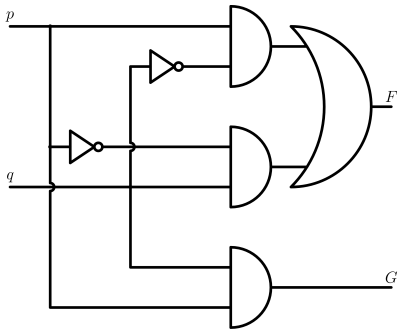
Slika 2.16: Logičko kolo za formulu $p \underline{\vee} q \sim (p \wedge \neg q) \vee (q \wedge \neg p)$

Jedno logičko kolo koje je posebno značajno je tzv. polusabirač; on služi za sabiranje dva binarna jednocifrena broja. On ima dva ulaza (označimo ih sa p i q) i dva izlaza; naime zbir dve binarne cifre može biti i dvocifren zbog mogućeg prenosa. Drugim rečima, ako sa F označimo funkciju koja daje kao rezultat

prvu cifru zdesna u zbiru, a sa G funkciju koja računa drugu cifru (prenos), tablice tih funkcija su:

p	q	G	F
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	0

Vidimo da G odgovara operaciji $\underline{\vee}$ čije smo kolo već skicirali u prethodnom primeru a F operaciji $\wedge$. Dakle, polusabirač možemo konstruisati na sledeći način:



Slika 2.17: Šema polusabirača

Za kraj ove glave pomenimo da je pravilno razumevanje iskaznih formula neophodno i u programiranju. Većina programskih jezika ima u sebi ugrađene osnovne logičke veznike $\neg, \wedge$ i $\vee$ koji su, kao što nam je poznato, dovoljni za izražavanje svake istinitosne funkcije. Npr. u programskom jeziku Java konjunkcija se zapisuje kao `p&&q`, disjunkcija kao `p||q`, a negacija kao `!p`. Ilustrujmo važnost razumevanja osnova iskaznog računa na nekoliko primera.

Primer 2.43 *Prevedimo u Javu sledeće izraze:*

(1) ,,Broj n nije deljiv ni sa 2, ni sa 3, ni sa 5." Deljivost broja n brojem k u Javi proverava se na sledeći način: `n % k == 0`*. Dakle, Java izraz koji bi odgovarao datoj rečenici bio bi*

```
!(n % 2 == 0) && !(n % 3 == 0) && !(n % 5 == 0).
```

Kao što znamo iz De Morganovih zakona, negacija se može i ,,izvući" na početak formule kako bismo dobili jednostavniju formulu:

```
!(n % 2 == 0 || n % 3 == 0 || n % 5 == 0).
```

(2) ,,Broj n nije između 1 i 2, niti između 5 i 6." Odgovarajući izraz u Javi je

```
!(1 < n && n < 2) && !(5 < n && n < 6).
```

(3) ,,n-ta godina je prestupna." Da li je godina prestupna određuje se po sledećim pravilima: (i) ako $400 \mid n$*, godina je prestupna, (ii) inače, ako* $100 \mid n$*, godina nije prestupna, (iii) inače, ako* $4 \mid n$*, godina je prestupna i (iv) u suprotnom, godina nije prestupna. Odgovarajući izraz u Javi je*

```
n % 400 == 0 || (n % 4 == 0 && n % 100 != 0).
```

Napomenimo još da se rezonovanje koje smo koristili u primeru 2.12 koristi i u programskim jezicima; naime ako se, tokom izvršavanja nekog programa, prilikom računanja vrednosti formule oblika $A \vee B$ dobije da je A tačna, vrednost formule B se ni ne računa. Slično, ako se prilikom računanja vrednosti formule oblika $A \wedge B$ dobije da je A netačna, vrednost formule B se opet ne računa, jer je $A \wedge B$ sigurno netačna.

2.10 Zadaci

Iskazne formule i tautologije

1. Zapisati sledeće rečenice pomoću iskaznih formula i nacrtati odgovarajuća drveta podformula:
   (a) Poneo sam kaput i čizme, ali ne i kišobran.
   (b) Ako bude padala kiša, neću ići ni na predavanja ni na vežbe.
   (c) Bez obzira na to da li pada kiša, ja idem na predavanja.
   (d) Ostani samo ako ćeš paziti na času.
2. Izračunati vrednosti formula:
   (a) $(p \Rightarrow q) \Rightarrow (r \wedge \neg s \Rightarrow q)$;
   (b) $\neg(p \wedge q) \Leftrightarrow \neg r \vee \neg s$

   u valuacijama: (1) $\alpha(p) = \top$, $\alpha(q) = \top$, $\alpha(r) = \bot$, $\alpha(s) = \top$; (2) $\beta(p) = \bot$, $\beta(q) = \top$, $\beta(r) = \top$, $\beta(s) = \bot$.
3. Tabličnom metodom dokazati: $\models (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.
4. Metodom svođenja na protivrečnost proveriti da li su tautologije:
   (a) $p \wedge (p \Rightarrow q) \Rightarrow q$;
   (b) $(p \Leftrightarrow \neg q \vee r) \Rightarrow (\neg p \Rightarrow q)$;
   (c) $((((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) \Rightarrow r) \Rightarrow t) \Rightarrow ((t \Rightarrow p) \Rightarrow (s \Rightarrow p))$.
5. Diskusijom po iskaznom slovu proveriti da li su sledeće formule tautologije:
   (a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$;
   (b) $((p \wedge q) \vee r \Rightarrow q) \Leftrightarrow ((\neg p \Rightarrow q) \wedge \neg r)$.
6. Dokazati da su sledeće formule tautologije:
   (a) $(p \vee q \Rightarrow ((p \Leftrightarrow r) \Rightarrow s \wedge r)) \Rightarrow ((p \vee q \Rightarrow (p \Leftrightarrow r)) \Rightarrow (p \vee q \Rightarrow s \wedge r))$.
   (b) $(p \vee q \Leftrightarrow ((p \Leftrightarrow r) \Leftrightarrow s \wedge r)) \Leftrightarrow (((p \Leftrightarrow r) \Leftrightarrow p \vee q) \Leftrightarrow s \wedge r)$.
7. Dokazati da je sledeća formula tautologija:

$$((p \wedge r \Leftrightarrow s \vee t) \Rightarrow (q \Rightarrow (p \vee (s \wedge t)))) \Rightarrow$$
$$(((p \wedge r \Leftrightarrow s \vee t) \Rightarrow q) \Rightarrow ((p \wedge r \Leftrightarrow s \vee t) \Rightarrow (p \vee (s \wedge t)))).$$

8. Dokazati da je formula A kontradikcija ako i samo ako je $\neg A$ tautologija.

Posledice i ekvivalentnost formula

9. Date su rečenice: ,,Ako je hladno, počeo je februar", ,,Ako nije počeo februar, onda je hladno" i ,,Počeo je februar".
   (a) Zapisati ih u obliku iskaznih formula.
   (b) Dokazati da je formula koja odgovara trećoj rečenici posledica ostale dve.
10. Odrediti šta se može zaključiti iz sledećih pretpostavki, obrazložiti i dokazati pravilo po kojem se izvodi zaključak:
   (a) ,,Nije tačno da sunce ne sija".
   (b) ,,Ako sunce sija, teren je otvoren" i ,,Sunce sija".
   (c) ,,Ako sunce sija, teren je otvoren" i ,,Ako je teren otvoren, naći ćemo se tamo u 10 sati".
   (d) ,,Sunce sija ili su tereni zatvoreni" i ,,Tereni nisu zatvoreni".
11. Ako je za formule A, B, C formula $A \Rightarrow (B \Rightarrow C)$ tautologija, dokazati da je i $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$ tautologija.
12. (a) Dva restorana objavila su reklame. Na prvoj piše: ,,Dobra hrana nije jeftina", a na drugoj ,,Jeftina hrana nije dobra". Da li ove dve rečenice govore istu stvar?
   (b) Dva restorana promenila su reklame. Na prvoj sada piše: ,,Dobra hrana je skupa", a na drugoj ,,Skupa hrana je dobra". Da li i ove dve rečenice govore istu stvar?
13. Ekvivalencijskim transformacijama dokazati da je tautologija: $(p \vee q \Rightarrow r) \Leftrightarrow (p \Rightarrow r) \wedge (q \Rightarrow r)$.
14. Svođenjem na konjunktivni oblik ispitati da li su sledeće formule tautologije, a za one koje nisu svođenjem na disjunktivni oblik ispitati da li su zadovoljive:
   (a) $(p \Rightarrow q \wedge \neg q) \Rightarrow \neg p$;
   (b) $((p \vee q) \wedge r) \vee (\neg r \wedge p)$;
   (c) $p \wedge (q \vee \neg p) \wedge ((q \Rightarrow \neg p) \vee \neg q)$.

Kanonske forme

15. Naći formulu u DKF i KKF čija je istinitosna tablica

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$

16. Konstruisati iskaznu formulu $F(p, q, r)$ tako da važi $v_\alpha(F) = \top$ ako i samo ako je $\alpha(p) = \alpha(r)$ ili $\alpha(p) = \alpha(q) = \bot$.

17. Konstruisati iskaznu formulu $F(p,q,r)$ koja je tačna ako i samo ako (a) tačno dva (b) bar dva njena iskazna slova imaju vrednost $\top$.

18. Konstruisati sve do na ekvivalenciju iskazne formule F takve da važi:

    (a) $\models (F \wedge q \Rightarrow \neg p) \Leftrightarrow ((p \Leftrightarrow \neg q) \Rightarrow F)$;

    (b) $\models ((r \Rightarrow \neg q \wedge p) \Rightarrow F) \Rightarrow (F \wedge (p \Rightarrow q) \wedge r)$.

19. Da li postoji iskazna formula $F(p,q)$ takva da je $\models (p \vee q \Rightarrow F) \Leftrightarrow (F \Rightarrow p \wedge r)$?

20. Odrediti sve (do na ekvivalenciju) formule $F(p,q,r)$ takve da formula

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

    bude tautologija.

21. Postoji li formula F takva da je

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

    tautologija?

22. Naći bar dve neekvivalentne iskazne formule F takve da formula

$$(F \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)) \wedge (F \wedge (r \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q))$$

    bude tautologija.

23. Naći bar tri neekvivalentne iskazne formule F takve da sledeća formula bude tautologija:

$$(F \Rightarrow p \vee q) \wedge (F \Rightarrow p \vee r) \wedge (p \Rightarrow F \vee p).$$

24. Odrediti jednu formulu F iskaznog računa u kojoj se pojavljuju samo veznici $\vee$ i $\neg$ takvu da formula

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

    bude tautologija.

25. Naći bar dve neekvivalentne iskazne formule $F(p,q,r)$ takve da važi:

$$p \Rightarrow r \models (q \Rightarrow r) \Rightarrow (p \vee F \Rightarrow r).$$

26. Da li postoji formula F takva da su tautologije formule:

$$(p \wedge q \wedge F) \vee \neg(\neg p \Rightarrow F)$$
$$((p \Leftrightarrow q) \vee F) \wedge (F \Rightarrow \neg p)?$$

27. Naći sve do na ekvivalenciju iskazne formule $F(p,q,r)$ takve da

$$\begin{aligned} p \Rightarrow F &\sim q \Rightarrow \neg p \vee r \\ F \Rightarrow p &\sim (r \Rightarrow q) \Rightarrow p. \end{aligned}$$

28. Da li postoje iskazne formule F i G takve da je formula $p \vee q \Rightarrow (r \wedge F) \vee (\neg r \wedge G)$ tautologija?

29. Odrediti sve (do na ekvivalenciju) formule $F(p,q)$ takve da

$$((F \Rightarrow p) \wedge (q \Rightarrow F)) \vee ((F \Rightarrow q) \wedge (p \Rightarrow F))$$

ne bude tautologija.

Baze

30. Sa T obeležimo operaciju iskazne algebre koja za proizvoljne vrednosti slova daje rezultat $\top$ (jednostavnosti radi, neka ona bude unarna). Dakle, $T(p) = \top$ za $p \in \{\top, \bot\}$. Analogno, neka je B operacija takva da $B(p) = \bot$ za sve $p \in \{\top, \bot\}$. Izraziti:

(a) $\neg$ preko $\Rightarrow, B$;

(b) $\neg$ preko $\underline{\vee}, T$;

(c) $\vee$ preko $\Rightarrow$.

31. Uz oznake kao u prethodnom zadatku, dokažite da su baze:

(a) $\{\Rightarrow, B\}$;

(b) $\{\vee, \underline{\vee}, T\}$.

32. Neka je operacija $\not\Rightarrow$ definisana sa $p \not\Rightarrow q \sim \neg(p \Rightarrow q)$. Dokazati da je $\{T, \not\Rightarrow\}$ baza iskaznog računa.

33. Neka je $\not\Rightarrow$ kao u prethodnom zadatku. Dokazati da je $\{\Rightarrow, \not\Rightarrow\}$ baza iskazne algebre, a zatim prikazati operacije $\wedge$ i $\uparrow$ u bazi $\{\Rightarrow, \not\Rightarrow\}$.

34. Da li je skup $\{\neg, *\}$ baza iskaznog računa, gde je operacija $*$ zadata tablicom:

$*$	$\top$	$\bot$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$

35. Sa π_1 i π_2 označimo prvu i drugu projekciju, tj. operacije iskazne algebre definisane sa $p\pi_1 q = p$ i $p\pi_2 q = q$. Da li je skup $\{\wedge, \vee, \pi_1, \pi_2\}$ baza iskazne algebre?

36. Operacija $*$ iskazne algebre definisana je tablicom

p	q	$p * q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

Dokazati da $\{*, \Leftrightarrow\}$ nije, a $\{*, \neg\}$ jeste baza iskazne algebre.

37. Dokazati da se $\Rightarrow$ ne može izraziti preko $\wedge$ i $\vee$.

38. Dokazati teoremu 2.39.

39. Neka su operacije $\not\Rightarrow$ i B date kao u zadacima 30 i 32. Dokazati da $\{\not\Rightarrow, B\}$ nije baza iskazne algebre.

40. Ako je B operacija iz zadatka 30, dokazati da $\{\wedge, B\}$ nije baza iskazne algebre.

41. Dokazati da $\{*, \&\}$ nije baza, gde

p	q	$p * q$	$p\&q$
$\top$	$\top$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$

42. Nacrtati prekidačka i logička kola koja odgovaraju sledećim formulama:

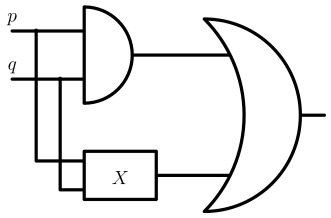
    (a) $(x \vee y) \wedge (\neg x \vee y)$;

    (b) $(x \wedge y) \vee (y \wedge z) \vee \neg z$.

43. (a) Svođenjem na konjuktivni oblik dokazati da je formula $(\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r) \Leftrightarrow p$ tautologija.

    (b) Nacrtati jedno prekidačko kolo koje odgovara formuli $(\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r)$.

44. Nacrtati logička kola koja mogu da stoje na mestu X u dijagramu, tako da taj dijagram odgovara kolu koje na izlazu daje 1 ($\top$) za sve moguće ulaze.



Glava 3

Predikatski račun

3.1 Predikatske formule

Iskazni račun je, zbog svoje jednostavnosti, prilično ograničenih mogućnosti kada je u pitanju izražajnost. Na primer, njime se ne mogu izraziti sledeće rečenice:

(R1) ,,ako je $a > b$ onda nije $b > a$";

(R2) ,,postoji najmanji prirodan broj" ili

(R3) ,,za sve pozitivne realne brojeve x je $x + 1 > x$".

Recimo, prva rečenica bi se kao iskazna formula mogla zapisati ovako: $p \Rightarrow \neg q$. Međutim, tim zapisom se ne može iskazati njen smisao: ona govori o odnosu neka dva broja a i b, koji su ,,izgubljeni" prilikom prevođenja u formulu. Preostale dve rečenice ne bi se ni u toj meri mogle zapisati iskaznim formulama.

Da bismo povećali izražajnost formula posmatraćemo proširenje iskaznog računa, predikatski račun. To proširenje se odnosi na dva aspekta. Prvi je razmatranje strukture iskaza; naime, u iskaznom računu iskaz je bio najmanja jedinica s kojom smo baratali. Sada ćemo uvođenjem relacijskih ($<$), funkcijskih ($+$) i simbola konstanti (0) moći razložiti iskaz; preciznije, datu formulu posmatraćemo na nekom skupu (koji ćemo zvati domen) i na kojem ćemo posmatrati operacije, relacije i konstante. Drugo proširenje ogleda se u uvođenju kvantifikatora, koji će nam omogućiti da izrazimo reči ,,svaki" i ,,postoji". Na taj način gornje rečenice moći ćemo izraziti sledećim formulama:

(R1) $P(a, b) \Rightarrow \neg P(b, a)$;

(Ovde relacijsko slovo P predstavlja relaciju $>$. Dakle, umesto samih iskaznih slova, delove formule $a > b$ i $b > a$ možemo izraziti na način kojim se očuvava njihova struktura.)

(R2) $(\exists x)(\forall y)Q(x, y)$;

(Ovde slovo Q predstavlja relaciju $\leq$, $(\exists x)$ čitamo ,,postoji x" a $(\forall y)$,,za svako y". Dakle, formula izražava da postoji x takav da za sve y važi $x \leq y$.)

(R3) $(\forall x)(P(x, c) \Rightarrow P(f(x), x))$.

(Slovo P ponovo predstavlja relaciju $>$, funkcijsko slovo f funkciju koja x preslikava u $x + 1$, a znak konstante c predstavlja konstantu 0.)

Kao i kod iskaznih, za početak koncentrisaćemo se na pravila za izgradnju *predikatskih formula* (u ovoj glavi reč ,,formule" označavaće predikatske formule). Simboli koji učestvuju u njihovoj izgradnji su:

1. promenljive: $x, y, z, \ldots$, kao i: $x_1, x_2, \ldots$;
2. iskazni veznici: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
3. kvantifikatori: univerzalni $\forall$ i egzistencijalni $\exists$;
4. zagrade: (i) i zarez ,;
5. relacijski simboli: $P, Q, S, \ldots$ kao i $P_1, P_2, \ldots$;
6. funkcijski simboli: $f, g, h, \ldots$ kao i $f_1, f_2, \ldots$ i
7. simboli konstanti: $c, d, e, \ldots$ kao i $c_1, c_2, \ldots$

Posebno ćemo obratiti pažnju na poslednje tri grupe simbola, koje čine *jezik* formule u kojoj se pojavljuju. Svaki relacijski i funkcijski simbol ima svoju fiksiranu arnost - broj argumenata na koje se primenjuje (videti odeljke 1.2 i 1.3). Dakle, isti relacijski simbol ne sme se, recimo, u jednoj formuli pojavljivati i kao unarni i kao binarni.

Naravno, svi ovi simboli ne mogu se na proizvoljan način slagati da bi se dobile formule. Da bismo precizirali postupak izgradnje formula, moramo prvo videti kako se grade *termovi* (izrazi). Kao i u definiciji 2.3 ova pravila biće data rekurzivno: od jednostavnijih ka složenijim termovima i formulama.

Definicija 3.1 *1. Promenljive i simboli konstanti su termovi.*

2. Ako je f n-arni funkcijski simbol a $t_1, t_2, \ldots, t_n$ termovi, onda je term i $f(t_1, t_2, \ldots, t_n)$.

3. Termovi se mogu dobiti samo konačnim brojem primena pravila 1 i 2.

Definicija 3.2 *1. Ako je P n-arni relacijski simbol a $t_1, t_2, \ldots, t_n$ termovi, onda je $P(t_1, t_2, \ldots, t_n)$ predikatska formula.*

2. Ako su A i B predikatske formule a x promenljiva, onda su predikatske formule i: $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $(\forall x)A$ i $(\exists x)A$.

3. Predikatske formule mogu se dobiti samo konačnim brojem primena pravila 1 i 2.

Dakle, najjednostavnije su formule oblika $P(t_1, t_2, \ldots, t_n)$, tzv. atomske formule. One u predikatskim formulama zamenjuju iskaze, ali imaju znatno složeniju strukturu.

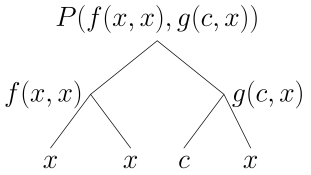
Primer 3.3 *(1) $P(f(x, x), g(c, x))$ je formula. Zaista, c (kao simbol konstante) i x (kao promenljiva) su termovi. Složeniji termovi $f(x, x)$ i $g(c, x)$ dobijaju se iz njih primenom pravila 2 definicije 3.1. Stoga je $P(f(x, x), g(c, x))$ atomska formula.*

(2) $(\exists x)P(f(x), x)$ je takođe formula. x i $f(x)$ su termovi, pa je $P(f(x), x)$ (atomska) formula. Sada primenom pravila 2 definicije 3.2 sledi da je i $(\exists x)P(f(x), x)$ formula.

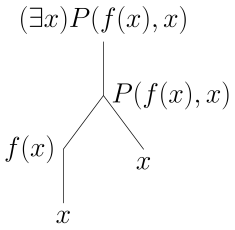
(3) I $(\forall x)(Q(x) \Rightarrow (\exists y)P(x, f(y)))$ *je formula. Naime,* x, y *i* $f(y)$ *su termovi, pa su* $Q(x)$ *i* $P(x, f(y))$ *atomske formule. Sledi da je i* $(\exists y)P(x, f(y))$ *formula, kao i* $(Q(x) \Rightarrow (\exists y)P(x, f(y)))$*. Konačno, dodavanjem kvantifikatora dobijamo formulu* $(\forall x)(Q(x) \Rightarrow (\exists y)P(x, f(y)))$*.*

U predikatskim formulama primenjivaćemo ista pravila za izostavljanje zagrada kao u iskaznim.

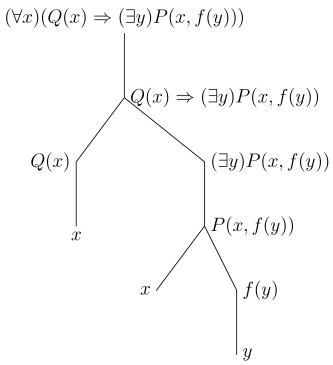
Podformule predikatskih formula definišemo analogno kao kod iskaznih. I one se mogu predstavljati drvetom podformula. Ono se gradi slično kao za iskazne formule, osim što ćemo, da bismo bolje prikazali izgradnju formule, u njega sada uključiti pored podformula i termove koji učestvuju u njenoj izgradnji. Recimo, za formule iz prethodnog primera ta drveta izgledaju ovako:



Slika 3.1: Drvo podformula za $P(f(x,x), g(c,x))$



Slika 3.2: Drvo podformula za $(\exists x)P(f(x), x)$



Slika 3.3: Drvo podformula za $(\forall x)(Q(x) \Rightarrow (\exists y)P(x, f(y)))$

Neka je u nekom koraku izgradnje formule F dobijena njena podformula $(Qx)G(x)$ (Q je neki od kvantifikatora $\forall$ ili $\exists$, a x je promenljiva). Tada kažemo da je formula $G(x)$ *oblast dejstva* kvantifikatora (Qx). U istoj formuli jedna promenljiva može se javljati više puta. Njene pojave koje su u oblasti dejstva nekog kvantifikatora zovemo *vezane*; ostale pojave zovemo *slobodne*. Formula je *zatvorena* ako se u njoj ne javljaju slobodne pojave nijedne promenljive.

U prethodnom primeru (1) sve tri pojave promenljive x su slobodne. U primeru (3) oblast dejstva kvantifikatora $(\exists y)$ je $P(x, f(y))$, a oblast dejstva kvantifikatora $(\forall x)$ ceo ostatak formule $(Q(x) \Rightarrow (\exists y)P(x, f(y)))$. Stoga su u formuli (3) sve pojave obe promenljive vezane, pa je ta formula zatvorena.

Ako želimo da naglasimo da se $x_1, x_2, \ldots, x_n$ (ili neke od njih) pojavljuju u formuli A kao slobodne promenljive, često ćemo umesto samo A pisati $A(x_1, x_2, \ldots, x_n)$. Slično je i s termovima: ako se u termu t pojavljuju promenljive $x_1, x_2, \ldots, x_n$ pisaćemo $t(x_1, x_2, \ldots, x_n)$.

3.2 Interpretacija

Da bi neka predikatska formula imala značenje, neophodno je da je interpretiramo. Interpretacija predikatskih formula odgovara valuaciji iskaznih, ali je znatno složenija. Kao što ćemo videti, svaku formulu možemo interpretirati na više načina.

Da bi formula zaista dobila značenje koje smo joj namenili neophodno je da, pre svega, odredimo skup na kojem ćemo je interpretirati, tzv. domen (recimo, u slučaju formule za (R2) s početka ove glave to je skup prirodnih brojeva N), a zatim da odredimo da relacijsko slovo Q predstavlja relaciju $\leq$. U ovakvoj interpretaciji ta formula je očigledno tačna. Međutim, ako bismo promenili bilo domen, bilo način interpretiranja slova Q, ona bi promenila značenje i mogla bi postati netačna. Recimo, ako umesto N za domen uzmemo Z, ona više nije tačna. Ili, ako umesto $\leq$ interpretiramo Q kao $\geq$, ponovo dobijamo netačno tvrđenje.

Sada ćemo precizno definisati šta smatramo interpretacijom formule.

Definicija 3.4 *Interpretaciju i formule F čine:*

- *domen D - to može biti bilo koji neprazan skup;*
- *po jedna n-arna relacija P^i na skupu D za svaki n-arni relacijski simbol P;*
- *po jedna n-arna operacija f^i na skupu D za svaki n-arni funkcijski simbol f;*
- *po jedan element $c^i \in D$ za svaki simbol konstante c.*

Obično pišemo $i = (D, P^i, \ldots, f^i, \ldots, c^i, \ldots)$, uz dogovor da najpre navodimo domen, zatim relacije, funkcije i na kraju konstante. Međusobni redosled relacija (ili funkcija) biće obično jasan iz konteksta (navodićemo ih po abecednom redosledu slova, npr. $f, g, h \ldots$).

U slučaju formula $F(x_1, x_2, \ldots, x_n)$ koje sadrže slobodne promenljive interpretacija nije uvek dovoljna da bi se izračunala tačnost formule: potrebno je i dodeliti vrednosti slobodnim promenljivima $x_1, x_2, \ldots, x_n$.

Definicija 3.5 *Za term $t(x_1, x_2, \ldots, x_n)$ sa $t^i[a_1, a_2, \ldots, a_n]$ označavaćemo njegovu vrednost u interpretaciji i kada promenljive imaju vrednosti $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$. Prateći definiciju 3.1, vrednost $t^i[a_1, a_2, \ldots, a_n]$ definiše se ovako:*

1. *ako je $t = x_k$ promenljiva, njena vrednost zadata je sa $t^i[a_1, a_2, \ldots, a_n] = a_k$;*
2. *ako je $t = c$ simbol konstante, onda je $t^i[a_1, a_2, \ldots, a_n] = c^i$;*
3. *ako je $t = f(t_1, t_2, \ldots, t_m)$, gde su $t_1, t_2, \ldots, t_m$ termovi a f m-arno funkcijsko slovo, onda je*

$$t^i[a_1, a_2, \ldots, a_n] = f^i(t_1^i[a_1, a_2, \ldots, a_n], \ldots, t_m^i[a_1, a_2, \ldots, a_n]).$$

Drugim rečima, kod složenijih termova oblika $f(t_1, t_2, \ldots, t_m)$ najpre izračunamo vrednosti jednostavnijih termova $t_1, t_2, \ldots, t_m$, a zatim na njih primenimo funkciju f^i.

Definicija 3.6 *Ako je zadata interpretacija i sa domenom D, za formulu $F(x_1, x_2, \ldots, x_n)$ sa slobodnim promenljivim $x_1, x_2, \ldots, x_n$ i za elemente $a_1, a_2, \ldots, a_n \in D$ sa $i \models F[a_1, a_2, \ldots, a_n]$ označićemo da je formula F tačna za vrednosti promenljivih $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$. To definišemo rekurzivno po složenosti formule, prateći definiciju 3.2:*

1. *ako je $F = P(t_1, t_2, \ldots, t_m)$ atomska formula, gde su $t_1, t_2, \ldots, t_m$ termovi a P m-arno relacijsko slovo, onda je $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako $P^i(t_1^i[a_1, a_2, \ldots, a_n], t_2^i[a_1, a_2, \ldots, a_n], \ldots, t_m^i[a_1, a_2, \ldots, a_n])$ (drugim rečima, najpre izračunamo vrednosti termova $t_1, t_2, \ldots, t_m$, a zatim proverimo da li su one u relaciji P^i);*

2. *ako je $F = \neg G$, onda $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako nije $i \models G[a_1, a_2, \ldots, a_n]$;*

3. *ako je $F = G \wedge H$, onda $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako $i \models G[a_1, a_2, \ldots, a_n]$ i $i \models H[a_1, a_2, \ldots, a_n]$;*

4. *ako je $F = G \vee H$, onda $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako $i \models G[a_1, a_2, \ldots, a_n]$ ili $i \models H[a_1, a_2, \ldots, a_n]$;*

5. *ako je $F = G \Rightarrow H$, onda $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako iz $i \models G[a_1, a_2, \ldots, a_n]$ sledi $i \models H[a_1, a_2, \ldots, a_n]$;*

6. *ako je $F = G \Leftrightarrow H$, onda $i \models F[a_1, a_2, \ldots, a_n]$ ako i samo ako važi: $i \models G[a_1, a_2, \ldots, a_n]$ ako i samo ako $i \models H[a_1, a_2, \ldots, a_n]$;*

7. *ako je $F(x_1, \ldots, x_{n-1}) = (\forall x_n)G(x_1, \ldots, x_{n-1}, x_n)$, onda $i \models F[a_1, a_2, \ldots, a_{n-1}]$ ako i samo ako za sve $a_n \in D$ važi $i \models G[a_1, a_2, \ldots, a_n]$;*

8. *ako je $F(x_1, \ldots, x_{n-1}) = (\exists x_n)G(x_1, \ldots, x_{n-1}, x_n)$, onda $i \models F[a_1, a_2, \ldots, a_{n-1}]$ ako i samo ako postoji $a_n \in D$ takvo da važi $i \models G[a_1, a_2, \ldots, a_n]$.*

Dakle, veznici $\neg, \wedge, \vee, \Rightarrow$ i $\Leftrightarrow$ imaju isto značenje kao u iskaznim formulama. Kakvo je značenje formule oblika $(\forall x)G(x)$? Kada dokazujemo da ona važi moramo proveriti da je $G(x)$ tačno za svaku vrednost x iz domena. S druge strane, kada dokazujemo da takva formula nije tačna, dovoljno je da nađemo primer elementa x za koji ne važi $G(x)$.

Definicija 3.7 *Interpretacija i je model formule F ako je $i \models F[a_1, a_2, \ldots, a_n]$ za sve vrednosti $a_1, a_2, \ldots, a_n$ iz domena D interpretacije i. To pišemo $i \models F(x_1, x_2, \ldots, x_n)$.*

Ako je i model za svaku od formula $F_1, F_2, \ldots, F_k$ kažemo i da je i model za skup formula $\{F_1, F_2, \ldots, F_k\}$.

Primer 3.8 *(1a) Posmatrajmo atomsku formulu $F = P(f(x, x), g(c, x))$ najpre u interpretaciji $i_1 = (Z, =, +, \cdot, 2)$. Domen je skup celih brojeva Z. Simbol konstante c interpretira se kao $c^{i_1} = 2$, a funkcijski simboli f i g redom kao sabiranje i množenje. Dakle, za proizvoljnu celobrojnu vrednost $x = a$ termovi $t_1(x) = f(x, x)$ i $t_2(x) = g(c, x)$ imaju redom vrednosti $t_1[a] = a + a$ i $t_2[a] = 2 \cdot a$. Sada tačnost date formule proveravamo ubacujući relaciju $=$ umesto relacijskog slova P: $i_1 \models F[a]$ akko je $a + a = 2 \cdot a$, što je tačno za svako $a \in N$. Dakle, $i_1 \models F$.*

(1b) Na istu formulu F možemo primeniti i drugačiju interpetaciju $i_2 = (Z, =, +, +, 2)$; dakle jedina izmena je to što sada i g interpetiramo kao sabiranje. Sada je, analogno, $i_2 \models F[a]$ akko je $a + a = 2 + a$. Ovo očigledno važi za $a = 2$ ali ne važi za ostale vrednosti $a \in Z$. Sledi da i_2 nije model za F.

(2a) Formulu $G = (\exists x)P(f(x), x)$ posmatrajmo najpre u interpretaciji $i_1 = (R, \leq, f^{i_1})$, gde je $f^{i_1}(x) = x + 1$. Dakle, domen je skup realnih brojeva R, relacijski simbol P interpretiramo kao relaciju $\leq$ a funkcijski simbol f kao operaciju f^{i_1}. Za atomsku formulu $G_1 = P(f(x), x)$ i neko $a \in R$ imamo $i_1 \models G_1[a]$ ako i samo ako je $a + 1 \leq a$. Stoga $i_1 \models G$ ako i samo ako postoji $a \in R$ takvo da je $a+1 \leq a$, što je naravno netačno pa $i_1 \not\models G$.

(2b) Posmatrajmo sada formulu G iz (2a) u drugoj interpretaciji $i_2 = (Z, =, f^{i_2})$, gde je $f^{i_2}(x) = x^2$. Za $G_1 = P(f(x), x)$ i $a \in Z$ je $i_2 \models G_1[a]$ ako i samo ako je $a^2 = a$. Sledi da $i_2 \models G$ ako i samo ako postoji $a \in Z$ takvo da je $a^2 = a$, što je tačno: $a = 1$ je takvo a. Dakle $i_2 \models G$.

(3) Za formulu $H = (\forall x)(Q(x) \Rightarrow (\exists y)P(x, f(y)))$ jedna moguća interpretacija je $i = (N, =, Q^i, f^i)$, gde $f^i(x) = x + 1$ a $Q^i(x)$ ako i samo ako je $x > 1$. Obeležimo $H_1 = P(x, f(y))$, $H_2 = (\exists y)P(x, f(y))$ i $H_3 = Q(x) \Rightarrow (\exists y)P(x, f(y))$. Vidimo da, za $a, b \in N$, $i \models H_1[a, b]$ ako i samo ako je $a = b + 1$, pa $i \models H_2[a]$ akko postoji $b \in N$ takvo da je $a = b + 1$. Dalje, $i \models H_3[a]$ znači: ako je $a > 1$ onda postoji $b \in N$ takvo da je $a = b + 1$. Konačno, $i \models H$ znači: za svako $a \in N$, ako je $a > 1$ onda postoji $b \in N$ takvo da je $a = b + 1$ pa zaključujemo da $i \models H$.

Kao što možemo videti iz prethodnog primera (1b), postoji interpretacija za koju ne možemo reći ni da je data formula tačna u njoj niti da je netačna. Razlog za to je postojanje slobodnih promenljivih u formuli $P(f(x, x), g(c, x))$; dakle tačnost formule može zavisiti od vrednosti tih promenljivih. Međutim, kada slobodnih promenljivih nema, formula je u svakoj interpretaciji ili tačna ili netačna (precizan dokaz ove činjenice nećemo izvoditi.)

Teorema 3.9 *Neka je A zatvorena formula. Za svaku interpretaciju i važi $i \models A$ ili $i \models \neg A$.*

Napomenimo da u specijalnom slučaju, kada ne sadrži relacije, interpretacija i postaje tzv. algebarska struktura. One se izučavaju npr. u knjizi [11].

3.3 Valjane formule

Definicija 3.10 *Formula F je valjana ako je tačna u svakoj svojoj interpretaciji. To označavamo $\models F$.*

Naravno, nije slučajno što se koristi ista oznaka kao za tautologije u iskaznom računu, jer valjane formule u predikatskom računu igraju ulogu koju su u iskaznom igrale tautologije: to su opšti zakoni logičkog mišljenja. Iz sledeće teoreme, slične teoremi zamene, sledi da su tautologije u nekom smislu specijalni slučajevi valjanih formula; $A(B_1, B_2, \ldots, B_n)$ ponovo označava formulu dobijenu iz $A(p_1, p_2, \ldots, p_n)$ zamenom svih pojava slova p_1 formulom B_1, svih pojava p_2 formulom B_2 itd.

Teorema 3.11 *Ako je $A(p_1, p_2, \ldots, p_n)$ tautologija, i $B_1, B_2, \ldots, B_n$ predikatske formule, onda je $A(B_1, B_2, \ldots, B_n)$ valjana (tzv. izvod tautologije).*

Ideja dokaza. Koristimo istu ideju kao u teoremi 2.14. Neka su $x_1, x_2, \ldots,$ x_k slobodne promenljive koje se javljaju u formuli $A(B_1, B_2, \ldots, B_n)$ (označimo tu formulu sa $F(x_1, x_2, \ldots, x_k)$). Dalje, neka je data proizvoljna interpretacija i i vrednosti $a_1, a_2, \ldots, a_k$ za promenljive $x_1, x_2, \ldots, x_k$ redom. Definišimo valuaciju α na sledeći način: neka je, za svako $j = 1, 2, \ldots, k$, $\alpha(p_j)$ vrednost formule $B_j[a_1, a_2, \ldots, a_k]$ u interpretaciji i. Sada se vrednost $F[a_1, a_2, \ldots, a_k]$ u toj interpretaciji izračunava kao $v_\alpha(A(p_1, p_2, \ldots, p_n))$, a ona je tačna jer je A tautologija. □

Primer 3.12 *Kako je* $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ *tautologija, ako zamenimo iskazna slova* p *i* q *redom formulama* $(\forall x)(\exists y)P(x, y)$ *i* $(\exists x)\neg Q(x)$*, dobijamo valjanu formulu* $\neg((\forall x)(\exists y)P(x, y) \vee (\exists x)\neg Q(x)) \Leftrightarrow \neg(\forall x)(\exists y)P(x, y) \wedge \neg(\exists x)\neg Q(x)$.

Međutim, daleko od toga da su izvodi tautologija jedine valjane formule. Štaviše, one nam ne daju neke suštinski nove zakone koje nismo imali već u iskaznom računu. Međutim, one nam omogućuju da zakone koji su važili već u iskaznoj logici koristimo i u predikatskoj, što ćemo veoma često i činiti.

Evo i spiska nekoliko najvažnijih valjanih formula koje nisu izvodi tautologija:

1. $\neg(\forall x)A \Leftrightarrow (\exists x)\neg A$
2. $\neg(\exists x)A \Leftrightarrow (\forall x)\neg A$
3. $(\forall x)(A \wedge B) \Leftrightarrow (\forall x)A \wedge (\forall x)B$
4. $(\exists x)(A \vee B) \Leftrightarrow (\exists x)A \vee (\exists x)B$
5. $(\forall x)A \vee (\forall x)B \Rightarrow (\forall x)(A \vee B)$
6. $(\exists x)(A \wedge B) \Rightarrow (\exists x)A \wedge (\exists x)B$
7. $(\forall x)(\forall y)A \Leftrightarrow (\forall y)(\forall x)A$
8. $(\exists x)(\exists y)A \Leftrightarrow (\exists y)(\exists x)A$
9. $(\exists x)(\forall y)A \Rightarrow (\forall y)(\exists x)A$

Pored gore pomenutih, sledeće formule su valjane ako se promenljiva x ne pojavljuje u B:

10. $(\forall x)A \vee B \Leftrightarrow (\forall x)(A \vee B)$
11. $(\forall x)A \wedge B \Leftrightarrow (\forall x)(A \wedge B)$
12. $(\exists x)A \vee B \Leftrightarrow (\exists x)(A \vee B)$
13. $(\exists x)A \wedge B \Leftrightarrow (\exists x)(A \wedge B)$

Gornji spisak ustvari ne daje konkretne formule, već šeme valjanih formula. To znači da, ako u bilo kojoj od njih umesto A i B stavimo proizvoljne predikatske formule, dobićemo valjanu formulu.

Formule 1 i 2 biće nam veoma bitne prilikom negiranja formula, videti odeljak 3.5. Formule 3 i 4 tvrde da se kvantifikator $\forall$ „slaže" s veznikom $\wedge$, a $\exists$ sa $\vee$, što ćemo često koristiti u dokazima. Formule 10-13 koristićemo prilikom prevođenja formula u preneksni oblik u jednom od narednih odeljaka.

Teorema 3.13 *Za svaku formulu* $A(x, y_1, y_2, \ldots, y_n)$ *i svaku interpretaciju* i *važi:* $i \models A(x, y_1, y_2, \ldots, y_n)$ *ako i samo ako* $i \models (\forall x)A(x, y_1, y_2, \ldots, y_n)$.

Dokaz. $i \models A(x, y_1, y_2, \ldots, y_n)$ znači da za sve $a, b_1, b_2, \ldots, b_n$ iz domena D interpretacije i važi $i \models A[a, b_1, b_2, \ldots, b_n]$. S druge strane, $i \models (\forall x)A(y_1, y_2, \ldots, y_n)$ znači da za sve $b_1, b_2, \ldots, b_n \in D$ važi $i \models (\forall x)A[b_1, b_2, \ldots, b_n]$, što je tačno ako i samo ako za svako $a \in D$ i sve $b_1, b_2, \ldots, b_n \in D$ imamo $i \models A[a, b_1, b_2, \ldots, b_n]$. Ove dve tvrdnje su očigledno ekvivalentne. □

Prethodna teorema tvrdi da se dodavanjem univerzalnog kvantifikatora na početak formule (ili njegovim uklanjanjem) ne menja tačnost formule u bilo kojoj

interpretaciji. Stoga se često pri formulisanju tvrđenja na početku izostavlja deo ,,za sve... važi". Npr. zadatak 8 prethodne glave mogao je glasiti i ovako: ,,Dokazati da za svaku formulu A važi: A je kontradikcija ako i samo ako je $\neg A$ tautologija".

S druge strane, prethodna teorema nam omogućava da od svake formule napravimo zatvorenu formulu dodavanjem po jednog univerzalnog kvantifikatora za svaku slobodnu promenljivu i da tačnost dobijene formule u svakoj interpretaciji bude ista kao i tačnost polazne formule. To je bitno zbog toga što mnoga tvrđenja važe samo za zatvorene formule; jedno od njih je sledeća teorema.

Teorema 3.14 *Zatvorena formula A je valjana ako i samo ako $\neg A$ nema model.*

Dokaz. Formula A je valjana ako i samo ako je tačna u svakoj interpretaciji odnosno, prema teoremi 3.9, ako i samo ako ne postoji interpretacija u kojoj je $\neg A$ tačna, tj. model za $\neg A$. □

Većina primera s kojima ćemo raditi su zatvorene formule pa ćemo na njih moći da primenimo prethodno tvrđenje. S druge strane, prema teoremi 3.13 umesto bilo koje formule koja nije zatvorena mogli bismo posmatrati njeno ,,zatvorenje" dobijeno dodavanjem kvantifikatora $(\forall x)$ za svaku slobodnu promenljivu x, pa ovo i nije veliko ograničenje.

Kako dakle pokazujemo da data formula F nije valjana? Iz teoreme 3.14 sledi da je dovoljno konstruisati bar jedan model za $\neg F$; to ćemo često zvati i *kontramodel* formule F. Recimo, možemo primetiti da neke od formula sa našeg spiska valjanih formula nisu u obliku ekvivalencije već samo implikacije, te se prirodno postavlja pitanje da li su i ,,obratne" implikacije takođe valjane formule. Ovde dokazujemo za jednu od njih da to nije slučaj, a ostale se ostavljaju čitaocu za vežbu.

Primer 3.15 *Dokažimo da formula $F = (\forall x)(A(x) \vee B(x)) \Rightarrow (\forall x)A(x) \vee (\forall x)B(x)$ nije valjana, nalazeći model za $\neg F$. Za domen kontramodela i ove formule uzmimo skup N, a relacijska slova A i B interpretirajmo kao sledeće unarne relacije:*

$A^i(x)$ ako i samo ako je x paran broj;

$B^i(x)$ ako i samo ako je x neparan broj.

Formula $(\forall x)(A(x) \vee B(x))$ je tačna u toj interpretaciji ako i samo ako za svaki $x \in N$ važi da je x paran ili da je neparan; dakle $i \models (\forall x)(A(x) \vee B(x))$. S druge strane, formula $(\forall x)A(x) \vee (\forall x)B(x)$ je tačna ako i samo ako je svaki $x \in N$ paran ili je svaki $x \in N$ neparan; očigledno $i \not\models (\forall x)A(x) \vee (\forall x)B(x)$. Dakle, $i \models \neg F$.

Prilikom konstrukcije modela za date formule imamo dve moguće strategije. Prva je da tražimo model na nekom malom domenu (obično sa 2 do 4 elementa) a relacije i funkcije predstavljamo tablicama. Zadate formule zadovoljavamo jednu po jednu, popunjavajući deo po deo tih tablica.

Druga strategija je da, kao u prethodnom primeru, koristimo poznate relacije na skupovima N, Z, $R, \ldots$ Pogodno je, pre biranja polazne interpretacije, najpre pregledati zadate formule kako bismo krenuli od one koja, za početak, zadovoljava što više formula, a potom je po potrebi prilagoditi ostalim. Kod obe strategije od suštinskog značaja je pravilno čitanje formula.

Nešto je teže pitanje: kako dokazati da neka formula F jeste valjana? Pošto za svaku formulu imamo beskonačno mnogo različitih interpretacija, nije moguće

u svakoj od njih proveriti tačnost formule F. Stoga ćemo u tu svrhu koristiti metod svođenja na protivrečnost: pretpostaviti suprotno, da postoji kontramodel i, a zatim računati tačnost raznih formula u interpretaciji i, pokušavajući da dobijemo da neka formula istovremeno i važi i ne važi u i. Ilustrujmo ovo na primeru formule 9 sa našeg spiska valjanih formula.

Primer 3.16 *Obeležimo* $F = (\exists x)(\forall y)A(x,y) \Rightarrow (\forall y)(\exists x)A(x,y)$ *i dokažimo da je* $\models F$. *Pretpostavimo da postoji kontramodel* $i = (D, A^i)$ *za* F. *U njemu bi tada bila tačna negacija formule* F, *odnosno imali bismo*

$$i \models (\exists x)(\forall y)A(x,y) \tag{3.1}$$
$$i \models \neg(\forall y)(\exists x)A(x,y). \tag{3.2}$$

Iz (3.1) sledi da postoji $m \in D$ *takav da*

$$\text{za sve } y \in D \text{ važi } A^i(m,y). \tag{3.3}$$

Dalje, iz (3.2) sledi da nije za sve elemente $y \in D$ *tačno* $(\exists x)A^i(x,y)$. *Dakle postoji* $n \in D$ *takav da ne postoji* $x \in D$ *za koji* $A^i(x,n)$, *odnosno da*

$$\text{za svaki } x \in D \text{ ne važi } A^i(x,n). \tag{3.4}$$

Sada iz (3.3) za $y = n$ *dobijamo da važi* $A^i(m,n)$, *a iz (3.4) za* $x = m$ *dobijamo da ne važi* $A^i(m,n)$, *kontradikcija.*

Najčešća strategija kod ovakvih dokaza je, dakle, da krenemo od formula koje počinju kvantifikatorom $\exists$. One nam daju konkretan element domena (za koji potom uvodimo posebnu oznaku $m, n \ldots$) na koji zatim možemo primenjivati formule koje počinju kvantifikatorom $\forall$. Baratanje formulama u ovakvim dokazima značajno će nam olakšati uvođenje ekvivalentnosti formula, posebno pravila za pomeranje negacija unutar formula.

3.4 Semantičke posledice

Pojmovi semantičkih posledica i ekvivalentnosti predikatskih formula definišu se analogno kao za iskazne formule. Dakle, grubo govoreći, A je posledica formula $F_1, F_2, \ldots, F_k$ ako uvek kada su one tačne mora biti tačna i formula A.

Definicija 3.17 *Formula* A *je semantička posledica formula* $F_1, F_2, \ldots, F_k$ *ako za svaku interpretaciju* i *i sve vrednosti* $a_1, a_2, \ldots, a_n \in D$ *slobodnih promenljivih koje se javljaju u* $F_1, F_2, \ldots, F_k, A$, *ako* $i \models F_1[a_1, a_2, \ldots, a_n], i \models F_2[a_1, a_2, \ldots, a_n], \ldots, i \models F_k[a_1, a_2, \ldots, a_n]$, *onda* $i \models A[a_1, a_2, \ldots, a_n]$. *To pišemo ovako:* $F_1, F_2, \ldots, F_k \models A$.

Naravno, prethodna definicija se pojednostavljuje kada su formule o kojima se govori zatvorene; ona tada glasi: za svaku interpretaciju i, ako $i \models F_1$, $i \models F_2, \ldots, i \models F_k$, onda i $i \models A$. Napomenimo da je u upotrebi i nešto drugačija definicija semantičkih posledica u predikatskom računu, koja se s našom poklapa u slučaju zatvorenih formula.

Primer 3.18 *Dokažimo* $(\exists x)P(x), (\forall x)(P(x) \Rightarrow Q(x)) \models (\exists x)Q(x)$. *Neka je* $i = (D, P^i, Q^i)$ *interpretacija takva da* $i \models (\exists x)P(x)$ *i* $i \models (\forall x)(P(x) \Rightarrow Q(x))$. *To znači da postoji* $a \in D$ *takav da* $P^i(a)$. *Dalje, za svako* $x \in D$ *iz* $P^i(x)$ *sledi* $Q^i(x)$, *pa i za* $x = a$: *kako je* $P^i(a)$ *sledi da važi i* $Q^i(a)$. *Dakle, našli smo element* $a \in D$ *takav da* $Q^i(a)$, *pa* $i \models (\exists x)Q(x)$.

Naredna teorema je analogna teoremi 2.19.

Teorema 3.19 *$F_1, F_2, \ldots, F_k, A \models B$ ako i samo ako $F_1, F_2, \ldots, F_k \models A \Rightarrow B$.*

Dokaz. ($\Rightarrow$) Neka su $x_1, x_2, \ldots, x_n$ slobodne promenljive koje se pojavljuju u datim formulama. Pretpostavimo da je $F_1, F_2, \ldots, F_n, A \models B$, i neka je data interpretacija i sa domenom D i elementi $a_1, a_2, \ldots, a_n \in D$ tako da $i \models F_i[a_1, a_2, \ldots, a_n]$ za $i = 1, 2, \ldots, k$. Dokažimo da $i \models (A \Rightarrow B)[a_1, a_2, \ldots, a_n]$. U suprotnom, važi $i \models A[a_1, a_2, \ldots, a_n]$ ali ne i $i \models B[a_1, a_2, \ldots, a_n]$. Kako je i model za $F_1, F_2, \ldots, F_n$ i A, prema pretpostavci mora biti i $i \models B[a_1, a_2, \ldots, a_n]$, kontradikcija.

($\Leftarrow$) Pretpostavimo sada da $F_1, F_2, \ldots, F_n \models A \Rightarrow B$ i neka je data interpretacija i sa domenom D i elementi $a_1, a_2, \ldots, a_n \in D$ tako da $i \models F_i[a_1, a_2, \ldots, a_n]$ za $i = 1, 2, \ldots, n$ i $i \models A[a_1, a_2, \ldots, a_n]$. Ako ne bi bilo $i \models B[a_1, a_2, \ldots, a_n]$, sledilo bi $i \not\models (A \Rightarrow B)[a_1, a_2, \ldots, a_n]$, kontradikcija. □

Posledica 3.20 *Za sve formule A i B važi: $A \models B$ ako i samo ako $\models A \Rightarrow B$.*

Teorema 3.21 *Neka su $F_1, F_2, \ldots, F_n, A$ formule i A je zatvorena. Tada $F_1, F_2, \ldots, F_n \models A$ ako i samo ako skup formula $\{F_1, F_2, \ldots, F_n, \neg A\}$ nema model.*

Dokaz. ($\Rightarrow$) Neka je $F_1, F_2, \ldots, F_n \models A$. Pretpostavimo suprotno, da postoji model i za skup formula $\{F_1, F_2, \ldots, F_n, \neg A\}$. Kako $i \models F_1$, $i \models F_2$, ..., $i \models F_n$, sledi da $i \models A$. Ali i $i \models \neg A$, što je nemoguće.

($\Leftarrow$) Pretpostavimo sada da skup $\{F_1, F_2, \ldots, F_n, \neg A\}$ nema model. Neka je i model za skup $\{F_1, F_2, \ldots, F_n\}$. Kako je A zatvorena, iz teoreme 3.9 i pretpostavke da i ne može biti model za $\neg A$ sledi $i \models A$. □

Pokažimo primerom da se uslov zatvorenosti formule A ne može izostaviti.

Primer 3.22 *Posmatrajmo formule $F = (\exists x)P(x)$ i $A = P(y)$. Tada ne postoji model i za skup formula $\{F, \neg A\}$, jer bi $i \models (\exists x)P(x)$ značilo da postoji element a domena takav da $P^i(a)$, a $i \models \neg P(y)$ bi značilo da za sve vrednosti a ne sme biti $P^i(a)$.*

S druge strane, ne važi $F \models A$, jer možemo konstruisati interpretaciju $i = (N, P^i)$, gde $P^i(n)$ znači „n je paran broj", u kojoj $i \models F$ ali ne važi recimo $i \models A[1]$.

U dokazima ćemo često, polazeći od neke formule F_1 formirati niz formula $F_1, F_2, \ldots, F_n$ takvih da $F_1 \models F_2$, $F_2 \models F_3, \ldots, F_{n-1} \models F_n$ (svaka sledeća formula je posledica prethodne) i na taj način zaključiti da $F_1 \models F_n$. Prilikom takvih dokazivanja od koristi će nam biti sledeće dve teoreme.

Teorema 3.23 *Ako $A \models B$, tada je:*

(a) $C \wedge A \models C \wedge B$;

(b) $C \vee A \models C \vee B$;

(c) $(\forall x)A \models (\forall x)B$;

(d) $(\exists x)A \models (\exists x)B$.

Dokaz. Neka su $x, y_1, y_2, \ldots, y_n$ slobodne promenljive koje se javljaju u formulama A, B i C.

(a) Neka je data interpretacija i sa domenom D i elementi $a, b_1, b_2, \ldots, b_n \in D$ tako da $i \models (C \wedge A)[a, b_1, b_2, \ldots, b_n]$. To znači da $i \models C[a, b_1, b_2, \ldots, b_n]$ i $i \models A[a, b_1, b_2, \ldots, b_n]$, a iz ovog drugog i pretpostavke $A \models B$ sledi i $i \models B[a, b_1, b_2, \ldots, b_n]$. Dakle, $i \models (C \wedge B)[a, b_1, b_2, \ldots, b_n]$.

(b) Neka su opet dati i i $a, b_1, b_2, \ldots, b_n$ tako da $i \models (C \vee A)[a, b_1, b_2, \ldots, b_n]$. To znači da $i \models C[a, b_1, b_2, \ldots, b_n]$ ili $i \models A[a, b_1, b_2, \ldots, b_n]$. U prvom slučaju direktno sledi $i \models (C \vee B)[a, b_1, b_2, \ldots, b_n]$, a u drugom, koristeći $A \models B$ dobijamo $i \models B[a, b_1, b_2, \ldots, b_n]$, pa $i \models (C \vee B)[a, b_1, b_2, \ldots, b_n]$.

(c) Neka su dati i i $b_1, b_2, \ldots, b_n$ takvi da $i \models (\forall x)A[b_1, b_2, \ldots, b_n]$ (nije potrebno zadati vrednost za x jer ona nije slobodna promenljiva u formuli $(\forall x)A$). Tada za svako $a \in D$ važi $i \models A[a, b_1, b_2, \ldots, b_n]$, pa zbog $A \models B$ sledi $i \models B[a, b_1, b_2, \ldots, b_n]$; dakle $i \models (\forall x)B[b_1, b_2, \ldots, b_n]$.

(d) Dokaz je analogan dokazu pod (c). □

Treba obratiti pažnju na činjenicu da analogna verzija prethodne teoreme za veznik $\neg$ ne važi (kao ni za veznike $\Rightarrow$ i $\Leftrightarrow$), dakle iz $A \models B$ ne sledi $\neg A \models \neg B$. To pokazuje sledeći primer.

Primer 3.24 *Neka je $A = (\forall x)P(x)$ i $B = (\exists x)P(x)$. Lako se dokazuje da $A \models B$, ali nije tačno da $\neg A \models \neg B$. Zaista, uzmimo interpretaciju $i = (N, P^i)$, gde $P^i(x)$ važi ako i samo ako je x paran broj. Tada $i \models \neg(\forall x)P(x)$, jer nije svaki prirodan broj paran, ali ne i $i \models \neg(\exists x)P(x)$, jer nije tačno da ne postoji paran prirodan broj.*

Definicija 3.25 *Kažemo da je term t slobodan za promenljivu x u formuli F ako se uvrštavanjem t na mesto promenljive x u F ne dobijaju nove vezane pojave nekih promenljivih.*

Primer 3.26 *(1) Term $t = \sqrt{2} + 1$ slobodan je za x u formuli $2x = x + x$. Naime, t ni ne sadrži promenljive, pa njegovim uvrštavanjem na mesto promenljive x ne možemo dobiti nove vezane promenljive.*

(2) Term y nije slobodan za promenljivu x u formuli $F = (\forall y)P(x, y)$, jer ubacivanjem y na mesto x u toj formuli dobijamo formulu $(\forall y)P(y, y)$ sa jednom novom vezanom pojavom promenljive y. Iz istih razloga ni term $f(x, y)$ nije slobodan za x u F.

Ako je term t slobodan za x u $A(x)$ (dodajemo x u zagradu da bismo naglasili njegovo pojavljivanje u formuli A), sa $A(t)$ ćemo označavati formulu dobijenu njegovim uvrštavanjem u $A(x)$ na mesto svih pojava promenljive x.

Teorema 3.27 *Ako je t term slobodan za promenljivu x u formuli A, onda važi:*

(a) $(\forall x)A(x) \models A(t)$;

(b) $A(t) \models (\exists x)A(x)$.

Dokaz. Radi jednostavnijeg zapisa dokazaćemo teoremu za slučaj kada je x jedina slobodna promenljiva u formuli A, a t ne sadrži promenljive.

(a) Pretpostavimo suprotno, da postoji interpretacija i sa domenom D takva da $i \models (\forall x)A(x)$, ali nije $i \models A(t)$. Označimo $a = t^i$ (vrednost terma t u interpretaciji i). Tada $i \not\models A[a]$, pa samim tim i $i \not\models (\forall x)A(x)$.

(b) Pretpostavimo sada da za interpretaciju i važi da je $i \models A(t)$. Tada za $a = t^i$ važi i $i \models A[a]$, odnosno $i \models (\exists x)A(x)$. □

Smisao prethodne teoreme je u sledećem: ako neka osobina važi za sve elemente x domena, onda umesto x možemo zameniti bilo koji konkretan element tog skupa; takođe, ako nađemo konkretan element domena za koji važi neka osobina, odatle možemo izvesti formulu koja tvrdi da takav element postoji.

Primer 3.28 *(a) Term* $t = \sqrt{2} + 1$ *slobodan je za* x *u formuli* $2x = x + x$, *pa prema teoremi 3.27(a)* $(\forall x)(2x = x + x)$ *ima za posledicu* $2(\sqrt{2} + 1) = (\sqrt{2} + 1) + (\sqrt{2} + 1)$.

(b) Term $t = 5/2$ *je slobodan za* x *u formuli* $2 \cdot x = 5$, *pa prema teoremi 3.27(b)* $2 \cdot (5/2) = 5$ *ima za posledicu* $(\exists x)(2 \cdot x = 5)$.

3.5 Ekvivalentnost formula

Definicija 3.29 *Kažemo da su formule* A *i* B *ekvivalentne (pišemo:* $A \sim B$*) ako za svaku interpretaciju* i *(sa domenom* D*) i sve vrednosti* $a_1, a_2, \ldots, a_n \in D$ *slobodnih promenljivih koje se javljaju u* A *i* B *važi*

$$i \models A[a_1, a_2, \ldots, a_n] \text{ ako i samo ako } i \models B[a_1, a_2, \ldots, a_n].$$

Iz ove i definicije 3.17 direktno sledi sledeće tvrđenje.

Teorema 3.30 $A \sim B$ *ako i samo ako* $A \models B$ *i* $B \models A$.

Teorema 3.31 $A \sim B$ *ako i samo ako* $\models A \Leftrightarrow B$.

Dokaz. Koristeći prethodnu teoremu i teoremu 3.20 imamo:

$$\begin{array}{lll} A \sim B & \text{akko} & A \models B \text{ i } B \models A \\ & \text{akko} & \models A \Rightarrow B \text{ i } \models B \Rightarrow A \\ & \text{akko} & \models A \Leftrightarrow B \end{array}$$

što je i trebalo dokazati. □

Teorema 3.32 *Iz uslova* $A_1 \sim A_2$ *i* $B_1 \sim B_2$ *sledi:*

(a) $\neg A_1 \sim \neg A_2$;

(b) $(A_1 \wedge B_1) \sim (A_2 \wedge B_2)$;

(c) $(A_1 \vee B_1) \sim (A_2 \vee B_2)$;

(d) $(A_1 \Rightarrow B_1) \sim (A_2 \Rightarrow B_2)$;

(e) $(A_1 \Leftrightarrow B_1) \sim (A_2 \Leftrightarrow B_2)$;

(f) $(\forall x)A_1 \sim (\forall x)A_2$;

(g) $(\exists x)A_1 \sim (\exists x)A_2$.

Dokaz. Tačke (b), (c), (f) i (g) lako se izvode korišćenjem teoreme 3.23. Dokažimo, recimo, tačku (g). Iz $A_1 \sim A_2$, na osnovu teoreme 3.30, sledi $A_1 \models A_2$ i $A_2 \models A_1$, pa prema 3.23 i $(\exists x)A_1 \models (\exists x)A_2$ i $(\exists x)A_2 \models (\exists x)A_1$. Ali to, opet prema teoremi 3.30, znači $(\exists x)A_1 \sim (\exists x)A_2$.

Dokažimo još i tačku (d), a ostale se pokazuju analogno. Neka je $i \models (A_1 \Rightarrow B_1)[a_1, a_2, \ldots, a_n]$ za neku interpretaciju i sa domenom D i neke vrednosti $a_1, a_2, \ldots, a_n \in D$ i pretpostavimo da ne važi $i \models (A_2 \Rightarrow B_2)[a_1, a_2, \ldots, a_n]$. Tada $i \models A_2[a_1, a_2, \ldots, a_n]$ ali $i \not\models B_2[a_1, a_2, \ldots, a_n]$. Iz $A_1 \sim A_2$ i $B_1 \sim B_2$ dobijamo da $i \models A_1[a_1, a_2, \ldots, a_n]$ ali $i \not\models B_1[a_1, a_2, \ldots, a_n]$, što je nemoguće zbog $i \models (A_1 \Rightarrow B_1)[a_1, a_2, \ldots, a_n]$, kontradikcija. □

Sada, kao i kod iskaznih formula, možemo sprovoditi *ekvivalencijske transformacije*.

Jedna od važnih primena ekvivalentnosti predikatskih formula je uprošćavanje negacija tih formula. Potreba za tim se često javlja, recimo kod dokaza svođenjem na kontradikciju: kada pretpostavljamo suprotno, moramo biti sposobni da formulišemo šta tačno znači to ,,suprotno".

Za uprošćavanje negacija koristimo sledeće ekvivalencijske transformacije:

$$\begin{aligned}
\neg(\forall x)A &\sim (\exists x)\neg A \\
\neg(\exists x)A &\sim (\forall x)\neg A \\
\neg(A \wedge B) &\sim \neg A \vee \neg B \\
\neg(A \vee B) &\sim \neg A \wedge \neg B \\
\neg(A \Rightarrow B) &\sim A \wedge \neg B \\
\neg\neg A &\sim A.
\end{aligned}$$

Primer 3.33 *U primeru 2.17 dokazivali smo $p \Rightarrow q, q \Rightarrow r \models p \Rightarrow r$, što znači: za svaku valuaciju α, ako $v_\alpha(p \Rightarrow q) = v_\alpha(q \Rightarrow r) = \top$, onda $v_\alpha(p \Rightarrow r) = \top$. Primetimo da je ovo tvrđenje oblika $(\forall\alpha)(A \wedge B \Rightarrow C)$. Prema gornjim pravilima negacija ovog tvrđenja ekvivalentna je sa*

$$\neg(\forall\alpha)(A \wedge B \Rightarrow C) \sim (\exists\alpha)\neg(A \wedge B \Rightarrow C) \sim (\exists\alpha)(A \wedge B \wedge \neg C).$$

Zato smo u tom dokazu, pretpostavljajući suprotno, zaključili da postoji valuacija α takva da $v_\alpha(p \Rightarrow q) = v_\alpha(q \Rightarrow r) = \top$, ali $v_\alpha(p \Rightarrow r) = \bot$.

Napomenimo još da, pošto iz našeg spiska valjanih formula sledi da važi $(\forall x)(\forall y)A \sim (\forall y)(\forall x)A$ i $(\exists x)(\exists y)A \sim (\exists y)(\exists x)A$, to znači da je redosled više uzastopnih kvantifikatora iste vrste nebitan. Stoga se često zapis skraćuje i piše samo $(\forall x, y)A$ ili $(\exists x, y)A$.

3.6 Račun sa jednakošću

Za mnoge funkcije, relacije i konstante koje se često koriste postoje standardne oznake. Tipičan primer je relacija jednakosti koju označavamo sa $=$, pa korišćenje oznake $P(x, y)$ umesto $x = y$ može učiniti formulu znatno teže čitljivom. Stoga uvodimo specijalni relacijski simbol $=$ i dogovaramo se da će u svakoj interpretaciji njemu odgovarati relacija jednakosti na domenu.

Izdvojićemo neke značajne osobine relacije jednakosti. Za sve terme $t_1, t_2, \ldots, t_n, t'_1, t'_2, \ldots, t'_n$, za svako n-arno relacijsko slovo P i svako n-arno funkcijsko slovo f mora da važi:

(J1) $t_1 = t_1$,

(J2) $t_1 = t_2 \Rightarrow t_2 = t_1$,

(J3) $t_1 = t_2 \wedge t_2 = t_3 \Rightarrow t_1 = t_3$,

(J4) $t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_n = t_n' \Rightarrow (P(t_1, t_2, \ldots, t_n) \Rightarrow P(t_1', t_2', \ldots, t_n'))$,

(J5) $t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_n = t_n' \Rightarrow f(t_1, t_2, \ldots, t_n) = f(t_1', t_2', \ldots, t_n')$.

Osobine (J1)–(J3) kažu da jednakost mora biti relacija ekvivalencije (videti odeljak 4.9). Evo primera koji ilustruje šta izražavaju preostale dve osobine.

Primer 3.34 *U interpretaciji* $(N, >, +, \cdot, 1, 2)$ *očigledno važi* $1+1 = 2$ *i* $1 \cdot 1 = 1$. *Zbog toga relacija* $1 + 1 > 1 \cdot 1$ *mora važiti ako i samo ako važi* $2 > 1$ *(ovde su nam* $t_1 = 1 + 1$, $t_1' = 2$, $t_2 = 1 \cdot 1$ *i* $t_2 = 1$ *termovi* $a >$ *relacijsko slovo* P *iz uslova (J4)). Slično, mora važiti i* $(1 + 1) \cdot (1 \cdot 1) = 2 \cdot 1$ *(gde* $\cdot$ *stoji na mestu* f *iz uslova (J5)).*

Uobičajeno je da se umesto $\neg x = y$ koristi kraći zapis $x \neq y$.

Kada na raspolaganju imamo i simbol jednakosti možemo predikatskim formulama izraziti razne kardinalne osobine modela (tj. osobine koje se tiču broja elemenata).

Primer 3.35 *(1) Formula čiji svi modeli imaju bar 2 elementa:*

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

(2) Formula čiji modeli imaju bar 3 elementa:

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

(3) Formulu čiji modeli imaju najviše 2 elementa možemo dobiti negiranjem prethodne formule i srediti je ekevivalencijskim transformacijama:

$$\begin{aligned} & \neg(\exists x)(\exists y)(\exists z)(x \neq y \wedge x \neq z \wedge y \neq z) \\ \sim \quad & (\forall x)(\forall y)(\forall z)\neg(x \neq y \wedge x \neq z \wedge y \neq z) \\ \sim \quad & (\forall x)(\forall y)(\forall z)(x = y \vee x = z \vee y = z). \end{aligned}$$

(4) Formulu čiji modeli imaju tačno 2 elementa možemo dobiti kao konjunkciju formula (1) i (3) ili nešto kraće direktno:

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

Kao i u slučaju relacije jednakosti ponekad ćemo, ako posmatramo neku formulu samo u jednoj interpretaciji, gde relacijska i funkcijska slova predstavljaju neke fiksirane relacije i funkcije, koristiti standardne oznake za njih. To se odnosi, pre svega, na relacije $\leq, \geq, <, >$ i operacije $+$ i $\cdot$. Npr. ako ne postoji opasnost od zabune, formule sa početka ove glave možemo zapisivati ovako:

(R1) $a > b \Rightarrow \neg(b > a)$;

(R2) $(\exists x)(\forall y)x \leq y$;

(R3) $(\forall x)(x > 0 \Rightarrow x + 1 > x)$.

3.7 Ograničeni kvantifikatori

Neka je P neka binarna relacija. Tada često pišemo:

$$(\forall xPy)A \quad \text{umesto} \quad (\forall x)(xPy \Rightarrow A)$$
$$(\exists xPy)A \quad \text{umesto} \quad (\exists x)(xPy \wedge A).$$

Ove skraćenice najčešće se koriste za relacije poretka (videti odeljak 4.10) ili pri radu sa skupovima, za relacijski simbol $\in$. Na primer, $(\exists x \leq y)x^2 = y$ je skraćeno od $(\exists x)(x \leq y \wedge x^2 = y)$ a $(\forall x \in N)x+1 > x$ je skraćeni zapis formule $(\forall x)(x \in N \Rightarrow x + 1 > x)$.

Značajna osobina ovih skraćenica je to što se na njih mogu primeniti neke od bitnih ekvivalencijskih transformacija, što ćemo pokazati u narednoj teoremi (uporediti sa spiskom valjanih formula u odeljku 3.3).

Teorema 3.36 *(a)* $\neg(\forall xPy)A \sim (\exists xPy)\neg A$;

(b) $\neg(\exists xPy)A \sim (\forall xPy)\neg A$;

(c) $(\forall xPy)(A \wedge B) \sim (\forall xPy)A \wedge (\forall xPy)B$;

(d) $(\exists xPy)(A \vee B) \sim (\exists xPy)A \vee (\exists xPy)B$.

Dokaz. (a) Ekvivalencijskim transformacijama dobijamo:

$$\neg(\forall xPy)A \sim \neg(\forall x)(xPy \Rightarrow A) \sim (\exists x)(xPy \wedge \neg A) \sim (\exists xPy)\neg A.$$

(b) Analogno kao pod (a),

$$\neg(\exists xPy)A \sim \neg(\exists x)(xPy \wedge A) \sim (\forall x)(xPy \Rightarrow \neg A) \sim (\forall xPy)\neg A.$$

(c)
$$\begin{aligned}(\forall xPy)(A \wedge B) &\sim (\forall x)(xPy \Rightarrow A \wedge B)\\ &\sim (\forall x)(\neg xPy \vee (A \wedge B))\\ &\sim (\forall x)((\neg xPy \vee A) \wedge (\neg xPy \vee B))\\ &\sim (\forall x)((xPy \Rightarrow A) \wedge (xPy \Rightarrow B))\\ &\sim (\forall x)(xPy \Rightarrow A) \wedge (\forall x)(xPy \Rightarrow B)\\ &\sim (\forall xPy)A \wedge (\forall xPy)B.\end{aligned}$$

(d) Ovaj deo možemo dokazati analogno delu (c) ili kombinovanjem rezultata (a), (b) i (c):

$$\begin{aligned}(\exists xPy)(A \vee B) &\sim \neg\neg(\exists xPy)(A \vee B)\\ &\sim \neg(\forall xPy)\neg(A \vee B)\\ &\sim \neg(\forall xPy)(\neg A \wedge \neg B)\\ &\sim \neg((\forall xPy)\neg A \wedge (\forall xPy)\neg B)\\ &\sim \neg(\forall xPy)\neg A \vee \neg(\forall xPy)\neg B\\ &\sim (\exists xPy)\neg\neg A \vee (\exists xPy)\neg\neg B\\ &\sim (\exists xPy)A \vee (\exists xPy)B.\end{aligned}$$

Još jedan standardan skraćeni zapis je kvantifikator ,,postoji tačno jedan":

$$(\exists_1 x)A(x) \text{ umesto } (\exists x)(A(x) \wedge (\forall y \neq x)\neg A(y)).$$

Na primer, formula $(\forall x \in N)(\exists_1 y)y = x + 1$ označava da svaki prirodan broj ima tačno jednog sledbenika.

3.8 Dokazivanje ispravnosti algoritma

Jedna od važnih primena predikatskog računa u računarstvu je dokazivanje ispravnosti datog algoritma. Naime, ono što želimo da dokažemo da neki algoritam radi često je najzgodnije zapisati u obliku predikatske formule.

Posmatrajmo npr. standardni algoritam za nalaženje najvećeg elementa u nizu. Neka je dat niz realnih brojeva dužine n; obeležimo ih sa `x[1],x[2], ...,x[n]`.

Ideja pronalaženja najvećeg elementa je sledeća: uvedemo pomoćnu promenljivu `max`, koja će u svakom koraku sadržati najveću vrednost u do sada proverenom delu niza. Stavimo joj početnu vrednost na prvi element niza, a zatim za svaki od preostalih elemenata `x[i]`, ako je on veći od `max`, dodelimo `max = x[i]`. Dakle, algoritam bi izgledao ovako:

```
max = x[1];
for(i = 2; i <= n; i++)
{
   if(x[i] > max)
   {
        max = x[i];
   }
}
```

Postavlja se pitanje: kako dokazati da ovaj algoritam radi, odnosno da promenljiva `max` na kraju izvršavanja zaista ima vrednost najvećeg člana niza? Kako je u osnovi algoritma jedna petlja, pokazaćemo matematičkom indukcijom da nakon svakog koraka petlje `max` ima vrednost najvećeg člana u do tada obrađenom delu niza (koji obuhvata prvih i članova). Ovakve rečenice pogodno je, radi lakše manipulacije, zapisati u obliku predikatskih formula. Dakle, ako sa $\texttt{max}_i$ označimo vrednost promenljive `max` nakon i-tog izvršavanja for-ciklusa, za naš algoritam treba dokazati dve stvari:

(a) $(\forall i \leq n)(\forall j \leq i)\texttt{max}_i \geq \texttt{x[j]}$ i

(b) $(\forall i \leq n)(\exists j \leq i)\texttt{max}_i = \texttt{x[j]}$.

Dokaz sprovodimo indukcijom po i (s tim što se ona završava kada je $i = n$, umesto da ,,pokrije" sve prirodne brojeve).

B.I. Za $i = 1$ je $\texttt{max}_1$=`x[1]`, pa i (a) i (b) očigledno važe.

I.H. Pretpostavimo su formule (a) i (b) tačne za neku vrednost i.

I.K. Dokažimo da su one tačne i za $i + 1$. Posmatrajmo dva slučaja.

1° Ako je `x[i+1]`>$\texttt{max}_i$, onda je $\texttt{max}_{i+1} =$ `x[i+1]` pa odmah imamo da važi (b). Kako po indukcijskoj hipotezi važi $\texttt{max}_i \geq$ `x[j]` za sve $j \leq i$, sledi da je $\texttt{max}_{i+1} \geq$ `x[j]` za sve $j \leq i + 1$, dakle važi i (a).

2° U suprotnom, $\texttt{max}_i \geq$ `x[i+1]` pa vrednost `max` ostaje ista: $\texttt{max}_{i+1} = \texttt{max}_i$. Po indukcijskoj hipotezi je $\texttt{max}_i \geq$ `x[j]` za $j \leq i$, pa zbog $\texttt{max}_i \geq$ `x[i+1]` to važi i za $j \leq i + 1$. Takođe, po indukcijskoj hipotezi postoji $j \leq i$ takvo da $\texttt{max}_i =$ `x[j]`, pa i $\texttt{max}_{i+1} =$ `x[j]`.

3.9 Preneksni oblik

Primetimo da je za značenje formule potpuno nebitno koje promenljive se u njoj pojavljuju. Naime, svejedno je da li kažemo ,,za svaki prirodan broj x je $x \geq 1$" ili ,,za svaki prirodan broj y je $y \geq 1$". Ovo ćemo precizirati u sledećoj teoremi, koju nećemo dokazivati.

Teorema 3.37 *(a)* $(\forall x)A(x) \sim (\forall y)A(y)$;

(b) $(\exists x)A(x) \sim (\exists y)A(y)$.

Definicija 3.38 *Kažemo da je formula F u preneksnom obliku ako je*

$$F = (Q_1 x_1)(Q_2 x_2)\dots(Q_n x_n)G,$$

gde su $Q_1, Q_2, \dots, Q_n$ kvantifikatori, $x_1, x_2, \dots, x_n$ promenljive, a G formula bez kvantifikatora.

Dakle, formula je u preneksnom obliku ako su svi njeni kvantifikatori ,,izvučeni" na početak. Primetimo da to znači i da cela formula G pripada oblasti dejstva svakog od tih kvantifikatora.

Teorema 3.39 *Za svaku formulu F postoji njoj ekvivalentna formula F^P u preneksnom obliku.*

Dokaz. Opisaćemo algoritam za nalaženje formule F^P. Zahvaljujući teoremi 3.13 možemo pretpostaviti da je F zatvorena formula (u suprotnom, možemo prvo za svaku njenu slobodnu promenljivu x dodati $(\forall x)$ na početak i tako dobiti formulu ekvivalentnu sa F).

Polazeći od F i primenjujući ekvivalencijske transformacije doći ćemo do F^P. Ti koraci su redom sledeći:

1. eliminisanje veznika $\Leftrightarrow$ koristeći $A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A)$;

2. eliminisanje veznika $\Rightarrow$ koristeći $A \Rightarrow B \sim \neg A \vee B$;

3. dok god postoje dva kvantifikatora koji deluju na istu promenljivu, preimenujemo sve pojave te promenljive u oblasti dejstva jednog od njih u neku novu promenljivu (koja se do sada nije javljala u formuli); ovo nam omogućuje teorema 3.37;

4. ,,uvlačenje" negacija koristeći $\neg(\forall x)A \sim (\exists x)\neg A(x)$, $\neg(\exists x)A \sim (\forall x)\neg A(x)$, $\neg(A \wedge B) \sim \neg A \vee \neg B$ i $\neg(A \vee B) \sim \neg A \wedge \neg B$;

5. ,,izvlačenje" kvantifikatora korišćenjem formula

$$\begin{aligned}
(\forall x)A \vee B &\sim (\forall x)(A \vee B)\\
(\forall x)A \wedge B &\sim (\forall x)(A \wedge B)\\
(\exists x)A \vee B &\sim (\exists x)(A \vee B)\\
(\exists x)A \wedge B &\sim (\exists x)(A \wedge B).
\end{aligned}$$

   Prema našem spisku valjanih formula (odeljak 3.3) ove transformacije smemo vršiti ako se promenljiva x ne pojavljuje u formuli B, ali to se neće desiti pošto je cela formula na kojoj radimo zatvorena i u koraku 3 smo izvršili preimenovanje za slučaj da je još neki kvantifikator delovao na x.

Nakon ,,pripremnih" koraka 1-4 dobijamo formulu u kojoj se javljaju samo veznici $\neg$, $\wedge$ i $\vee$ i sve negacije stoje uz atomske formule. Korak 5 omogućava nam da iz takve formule dobijemo preneksni oblik. □

Primer 3.40 *Prevedimo sledeće tri formule u preneksni oblik.*

(1)
$$\begin{aligned} & (\forall x)P(x) \wedge (\exists y)Q(y) \\ \sim\ & (\forall x)(P(x) \wedge (\exists y)Q(y)) \\ \sim\ & (\forall x)(\exists y)(P(x) \wedge Q(y)). \end{aligned}$$

(2)
$$\begin{aligned} & (\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall y)Q(y) \\ \sim\ & \neg(\forall x)(P(x) \vee Q(x)) \vee (\forall y)Q(y) \\ \sim\ & (\exists x)\neg(P(x) \vee Q(x)) \vee (\forall y)Q(y) \\ \sim\ & (\exists x)(\neg P(x) \wedge \neg Q(x)) \vee (\forall y)Q(y) \\ \sim\ & (\exists x)(\forall y)((\neg P(x) \wedge \neg Q(x)) \vee Q(y)). \end{aligned}$$

(3)
$$\begin{aligned} & (\exists y)P(y,y) \Leftrightarrow (\forall x)P(x,x) \\ \sim\ & ((\exists y)P(y,y) \Rightarrow (\forall x)P(x,x)) \wedge ((\forall x)P(x,x) \Rightarrow (\exists y)P(y,y)) \\ \sim\ & (\neg(\exists y)P(y,y) \vee (\forall x)P(x,x)) \wedge (\neg(\forall x)P(x,x) \vee (\exists y)P(y,y)) \\ \sim\ & ((\forall y)\neg P(y,y) \vee (\forall x)P(x,x)) \wedge ((\exists x)\neg P(x,x) \vee (\exists y)P(y,y)) \\ \sim\ & (\forall y)(\forall x)(\neg P(y,y) \vee P(x,x)) \wedge (\exists x)(\exists y)(\neg P(x,x) \vee P(y,y)) \\ \sim\ & (\forall y)(\forall x)(\exists x)(\exists y)((\neg P(y,y) \vee P(x,x)) \wedge (\neg P(x,x) \vee P(y,y))). \end{aligned}$$

Iz prethodnog primera možemo videti da, čak i ako formula na početku nije sadržala više kvantifikatora koji deluju na istu promenljivu, nakon eliminisanja veznika $\Leftrightarrow$ takvi kvantifikatori se mogu pojaviti. Stoga nam je zaista neophodan korak preimenovanja promenljivih.

Čitalac bi, gledajući gornji primer, mogao doći do pogrešnog zaključka da redosled kvantifikatora nije bitan, npr. u delu (1) mogli smo prvo ,,izvući" i kvantifikator $(\exists y)$. Ovde je to slučaj samo zato što su kvantifikatori delovali na promenljive koje se nisu ,,mešale" u formuli, tj. formula je izražavala osobine x i y nezavisno jednu od druge, a ne njihov međusobni odnos. Kroz zadatke s modelima videćemo važnost redosleda kvantifikatora.

3.10 Skolemizacija

Neka je F formula u preneksnom obliku. *Skolemizacija* te formule dobija se eliminacijom jednog po jednog svih kvantifikatora $\exists$ sleva nadesno i pritom:

- ako ispred $(\exists x)$ nema drugih kvantifikatora, sve pojave x u formuli zamenjujemo nekim novim znakom konstante (dakle, nekim koji se prethodno nije pojavljivao u formuli);
- ako ispred $(\exists x)$ stoji $(\forall y_1)(\forall y_2)\ldots(\forall y_k)$, sve pojave x u formuli zamenjujemo sa $f(y_1, y_2, \ldots, y_k)$, gde je f neki novi funkcijski simbol.

Formulu dobijenu na taj način označićemo sa F^S.

Primer 3.41 *(1) Ako je $F = (\exists x)P(x, f(x))$, onda $F^S = P(c, f(c))$.*

(2) Ako je $G = (\forall x)(\exists y)P(x, f(y))$, onda je $G^S = (\forall x)P(x, f(g(x)))$.

(3) Ako je $H = (\exists x_1)(\forall x_2)(\exists x_3)(\forall x_4)(\exists x_5)B(x_1, x_2, x_3, x_4, x_5)$, pošto u formuli imamo tri kvantifikatora $\exists$, skolemizaciju sprovodimo u tri koraka:

$$\begin{aligned} & (\forall x_2)(\exists x_3)(\forall x_4)(\exists x_5)B(c, x_2, x_3, x_4, x_5) \\ & (\forall x_2)(\forall x_4)(\exists x_5)B(c, x_2, f(x_2), x_4, x_5) \\ & (\forall x_2)(\forall x_4)B(c, x_2, f(x_2), x_4, g(x_2, x_4)) = H^S. \end{aligned}$$

Važno je napomenuti da formula F^S dobijena skolemizacijom nije ekvivalentna polaznoj formuli F; one čak nemaju ni isti jezik. U sledećoj teoremi dokazaćemo da za njih važi nešto slabiji uslov od ekvivalentnosti. Pre nego što pređemo na nju videćemo na primeru o čemu ona govori.

Primer 3.42 *Neka je dat skup formula* $\{F_1, F_2\}$*, gde* $F_1 = (\exists x)(\forall y)P(x,y)$ *i* $F_2 = (\forall y)(\exists x)P(y,x)$*. Nije teško videti da je* $(N, \leq)$ *jedan model ovog skupa formula: prva od njih tvrdi da postoji* $a \in N$ *koji je manji ili jednak od svih prirodnih brojeva (to je* $a = 1$*), a druga da za svaki prirodan broj* y *postoji prirodan broj veći ili jednak od njega (to je npr.* $y + 1$*).*

Formule dobijene od datih skolemizacijom su $F_1^S = (\forall y)P(c,y)$ *i* $F_2^S = (\forall y)P(y, f(y))$*. Model za skup* $\{F_1^S, F_2^S\}$ *možemo lako naći dopunjavanjem interpretacije* $(N, \leq)$ *tako što ćemo znak konstante* c *interpretirati kao* $c^i = 1$*, a funkcijsko slovo* f *kao funkciju* $f^i(y) = y + 1$*. Sada je* $(N, \leq, 1, f^i)$ *model za* $\{F_1^S, F_2^S\}$*, jer prva od tih formula tvrdi da je broj 1 manji ili jednak od svih prirodnih brojeva, a druga da je za svaki broj* $y \in N$ *broj* $y + 1$ *veći ili jednak od njega.*

Dakle, skolemizacijom formula suština je ostala nepromenjena, samo smo obogatili jezik formule precizirajući koji je to element manji ili jednak od svih i*, za svako* y*, koje je to* x *veće ili jednako od* y*.*

Teorema 3.43 *(a) Neka je* F *formula u preneksnom obliku. Tada* F *ima model ako i samo ako* F^S *ima model.*

(b) Neka su $F_1, F_2, \ldots, F_n$ *formule u preneksnom obliku. Tada skup formula* $\{F_1, F_2, \ldots, F_n\}$ *ima model ako i samo ako skup* $\{F_1^S, F_2^S, \ldots, F_n^S\}$ *ima model.*

Ideja dokaza. Daćemo samo ideju dokaza pod (a) u slučaju kada skolemizacija ima samo jedan korak, tj. eliminiše se samo jedan kvantifikator. Neka je i model za F sa domenom D.

($\Rightarrow$) Ako je $F = (\exists x)G$, prilikom skolemizacije pojave x su zamenjene nekim simbolom konstante c. To što $i \models F$ znači da postoji $a \in D$ takvo da $i \models G[a]$. Proširićemo interpretaciju i tako što ćemo dodati $c^i = a$.

Dalje, ako je $F = (\forall y_1)(\forall y_2)\ldots(\forall y_k)(\exists x)G$, x je prilikom skolemizacije zamenjeno sa $f(y_1, y_2, \ldots, y_k)$. To što $i \models F$ znači da za bilo koje $b_1, b_2, \ldots, b_k \in D$ postoji $a \in D$ takvo da $i \models G[b_1, \ldots, b_k, a]$. Proširićemo interpretaciju i tako što ćemo dodati funkciju f^i definisanu ovako: $f(b_1, b_2, \ldots, b_k) = a$, i tako za sve k-torke $b_1, b_2, \ldots, b_k \in D$.

Interpretacija koju smo na ovaj način dobili biće model za formulu F^S.

($\Leftarrow$) Obratno, ako je i model za F^S, model za F dobićemo ako iz i izostavimo interpretacije svih slova dodatih prilikom skolemizacije. □

Skolemizacija bi trebalo da nam pomogne u razumevanju značaja redosleda kvantifikatora: formula oblika $(\exists x)(\forall y)G$ tvrdi da postoji jedno x u domenu koje za sve y zadovoljava uslov G dok formula oblika $(\forall y)(\exists x)G$ tvrdi da se, ako nam je dato y, postoji x koje zadovoljava uslov G. U ovom drugom slučaju pri skolemizaciji zamenjujemo x sa $f(y)$ jer x zavisi od vrednosti y.

3.11 Rezolucija

Pretpostavimo da treba da napišemo program na računaru koji će za zadate formule $F_1, F_2, \ldots, F_n, A$ proveriti da li važi $F_1, F_2, \ldots, F_n \models A$ (ili, u specijalnom slučaju, da li $\models A$). Ako je formula A zatvorena, prema teoremi 3.21

treba ustvari proveriti da li postoji model za skup formula $\{F_1, F_2, \ldots, F_n, \neg A\}$. Tome je namenjen tzv. postupak rezolucije. Ono u čemu se rezolucija razlikuje od metoda proveravanja valjanosti objašnjenih u odeljku 3.3 je to što je u pitanju postupak koji se može automatizovati; drugim rečima moguće je napisati računarski program koji bi na datom skupu formula sproveo postupak rezolucije.

Neka je, dakle, zadat skup formula $\{F_1, F_2, \ldots, F_n\}$ za koji proveravamo ima li model. Pre samog sprovođenja rezolucije treba izvršiti nekoliko pripremnih koraka. Oni se sastoje u sledećem:

1. svaku od formula $F_1, F_2, \ldots, F_n$ prevesti u preneksni oblik;
2. izvršiti skolemizaciju svake od njih;
3. preimenovati promenljive tako da ne deluju dva kvantifikatora na istu (čak ni u različitim formulama);
4. ukloniti univerzalne kvantifikatore i
5. prevesti svaku od formula u konjunktivni oblik, po potpuno istim pravilima kao za iskazne formule (odeljak 2.6).

Na ovaj način za svaku od datih formula F možemo naći formulu F' bez kvantifikatora u konjunktivnom obliku tako da se ista promenljiva ne javlja u više formula.

Prema teoremi 3.39 prevođenjem u preneksni oblik dobijamo formule ekvivalentne polaznim. Iz teoreme 3.43 vidimo da skup formula dobijen Skolemizacijom ima model ako i samo ako polazni skup ima model. Preimenovanje promenljivih je takođe ekvivalencijska transformacija (teorema 3.37). Uklanjanjem kvantifikatora $\forall$ sve interpretacije koje su bili modeli za polaznu formulu ostaju i modeli za dobijenu formulu bez kvantifikatora (teorema 3.13). Konačno, pri svođenju na konjunktivni oblik opet se koriste samo ekvivalencijske transformacije. Sve ovo ukratko znači da polazni skup formula $\{F_1, F_2, \ldots, F_n\}$ ima model ako i samo ako skup formula $\{F_1', F_2', \ldots, F_n'\}$ dobijen posle opisanih 5 koraka ima model.

Ilustrujmo sve do sada opisano na jednom primeru.

Primer 3.44 *Pretpostavimo da želimo da proverimo da li je* $(\forall x)(P(x) \Rightarrow (\exists y)Q(x,y)), (\exists x)P(x) \models (\exists x)(\exists y)Q(x,y)$. *Kako su sve navedene formule zatvorene, treba ustvari proveriti da li skup* $\{F_1, F_2, F_3\}$ *ima model, gde* $F_1 = (\forall x)(P(x) \Rightarrow (\exists y)Q(x,y))$, $F_2 = (\exists x)P(x)$ *i* $F_3 = \neg(\exists x)(\exists y)Q(x,y)$. *Pratimo gore opisane korake:*

1. $F_1 \sim (\forall x)(\neg P(x) \vee (\exists y)Q(x,y)) \sim (\forall x)(\exists y)(\neg P(x) \vee Q(x,y)) = F_1^P$;
   $F_2 = F_2^P$ *i*
   $F_3 \sim (\forall x)(\forall y)\neg Q(x,y) = F_3^P$;
   dakle dobili smo preneksni oblik za svaku od formula.
2. *Izvršimo skolemizaciju svake od formula:*
   $F_1^S = (\forall x)(\neg P(x) \vee Q(x, f(x)))$;
   $F_2^S = P(c)$ *i*
   $F_3^S = F_3^P$.
3. *Promenljiva* x *se javlja i u prvoj i u trećoj formuli pa ćemo njene pojave u trećoj preimenovati u novu promenljivu* z. *Na taj način dobijamo formulu* $(\forall z)(\forall y)\neg Q(z,y)$.

4. *Uklanjanjem univerzalnih kvantifikatora dobijamo skup formula* $\{\neg P(x) \vee Q(x, f(x)), P(c), \neg Q(z, y)\}$.

5. *Svaka od ovih formula je već u konjunktivnom obliku. Svaka ima samo po jednu klauzu, pa smo dobili klauze* $\neg P(x) \vee Q(x, f(x)), P(c)$ *i* $\neg Q(z, y)$.

Podsetimo se, za skup iskaznih formula kažemo da je zadovoljiv ako ima model, odnosno valuaciju u kojoj su sve njegove formule tačne.

Teorema 3.45 (Erbran) *Za svaki skup S klauza predikatskog računa postoji skup iskaznih klauza HS takav da S ima model ako i samo ako je skup HS zadovoljiv.*

Dokaz teoreme Erbrana može se naći u knjizi [18] (tvrđenje 2.61). Ona nam omogućuje da predikatske klauze zamenimo iskaznim i da postupak nastavimo sa skupom iskaznih klauza. Kako je precizan postupak te zamene sadržan u dokazu teoreme, mi ćemo se zadovoljiti samo saznanjem da je to u principu moguće uraditi.

Ostaje da se proveri da li dobijeni skup iskaznih formula ima model. Kažemo da je klauza D *rezolventa* klauza C_1 i C_2 ako postoji iskazno slovo p takvo da se p nalazi u C_1 (kao literal): $C_1 = p \vee C_1'$, $\neg p$ se nalazi u C_2: $C_2 = \neg p \vee C_2'$ i $D = C_1' \vee C_2'$. Dakle, D se dobija „spajanjem" klauza C_1 i C_2 i izbacivanjem literala p i $\neg p$. *Rezolucija* je postupak izvođenja u kojem polazimo od formula datog skupa i u svakom koraku dodajemo rezolvente.

Teorema 3.46 *Ako je D rezolventa klauza C_1 i C_2, onda $C_1, C_2 \models D$.*

Dokaz. Neka je $C_1 = p \vee C_1'$, $C_2 = \neg p \vee C_2'$ i $D = C_1' \vee C_2'$. Treba, dakle, dokazati da $p \vee C_1', \neg p \vee C_2' \models C_1' \vee C_2'$.

Neka je α valuacija takva da $v_\alpha(p \vee C_1') = v_\alpha(\neg p \vee C_2') = \top$. Posmatrajmo dva slučaja:

1° $\alpha(p) = \bot$. Tada mora biti $v_\alpha(C_1') = \top$;

2° $\alpha(p) = \top$. Tada mora biti $v_\alpha(C_2') = \top$.

U oba slučaja mora biti $v_\alpha(C_1' \vee C_2') = \top$, što je i trebalo dokazati. □

Ako je $C_1 = p$ i $C_2 = \neg p$, njihova rezolventa nema nijedan literal pa ćemo je zvati praznom klauzom. Izvođenje prazne klauze približno odgovara dolasku do kontradikcije, pa važi sledeća teorema (koju nećemo dokazivati).

Teorema 3.47 *Skup iskaznih klauza nema model ako i samo ako se rezolucijom od njega može izvesti prazna klauza.*

Primer 3.48 *Pretpostavimo da smo primenom teoreme Erbrana došli do skupa iskaznih klauza $\{q, \neg p \vee \neg q \vee r, \neg r \vee \neg q \vee p, r \vee p, \neg r\}$. Pokušajmo metodom rezolucije da izvedemo praznu klauzu. Za početak, rezolventa klauza $r \vee p$ i $\neg r$ je p, pa nju dodajemo našem skupu. Dalje, rezolventa klauza p i $\neg p \vee \neg q \vee r$ je $\neg q \vee r$, pa dodajemo i nju. Rezolventa te klauze i klauze q je r. Konačno, rezolventa klauza r i $\neg r$ je prazna klauza. Sledi da polazni skup nije zadovoljiv.*

Kao što je napomenuto na početku ove glave, važna osobina metoda rezolucije je to što je to algoritamski metod, dakle može se pretvoriti u računarski program. Npr. kada nam je dat konačan skup iskaznih klauza (kao u prethodnom primeru) imamo samo konačan broj parova klauza na koje možemo primeniti rezoluciju, pa možemo efektivno ispitati da li se iz tog skupa može izvesti prazna klauza.

Metod rezolucije je u osnovi programskog jezika *Prolog*. On se razlikuje od većine drugih jezika jer je deklarativni, a ne imperativni jezik - ne sastoji se od niza naredbi koje se izvršavaju, tj. programer samo navodi šta treba rešiti, ali ne i kako.

Program u Prologu sastoji se iz činjenica i pravila. Činjenicama se ustvari zadaju relacije na nekom skupu elemenata. Pravila se zadaju u obliku implikacija pri čemu se umesto $\Rightarrow$ piše $:-$ i čita zdesna nalevo (umesto $p \Rightarrow q$ pišemo q`:-`p). Pritom možemo koristiti i konjunkciju (koja se piše kao `,`) i negaciju (`not`). Kao što znamo, $\{\neg, \wedge\}$ je jedna baza iskaznog računa, pa su nam ta dva veznika i dovoljna. Kvantifikatori se ne koriste, što je prema teoremi 3.13 isto kao da su sve promenljive kvantifikovane univerzalnim kvantifikatorom.

Evo jednog programa u Prologu.

```
otac(aca,branko).
otac(aca,dragana).
otac(branko,eva).
otac(branko,goca).
majka(dragana,ivana).
majka(dragana,jovan).
deda(X,Y) :- otac(X,Z),otac(Z,Y).
deda(X,Y) :- otac(X,Z),majka(Z,Y).
```

Prvih šest redova programa predstavljaju činjenice. Njima se zadaju četiri para elemenata koji su u relaciji `otac` i dva para koji su u relaciji `majka`. Preostala dva reda su pravila. Prvo od njih, recimo, kaže da, ako je `X` otac osobe `Z` a `Z` otac osobe `Y`, onda je `X` deda osobe `Y`. `X,Y,Z` su promenljive i, kao što je gore rečeno, podrazumeva se da pravila važe za sve moguće vrednosti promenljivih.

Nakon činjenica i pravila možemo zadati i upit, npr.

```
?-deda(aca,goca).
```

Prolog sada proverava da li je ovo posledica gornjih činjenica i pravila, i to upravo metodom rezolucije.

U praksi primena rezolucije je nešto drugačija nego što je gore opisano; za početak ona se sprovodi direktno na predikatskim formulama, bez prevođenja na iskazne, ali je to značajno složeniji postupak.

3.12 Zadaci

Formule i interpretacije

1. Za svaku od formula:

   (a) $F_1 = P(f(a,a),a)$,

   (b) $F_2 = (\exists x)P(f(x,x),a)$,

   (c) $F_3 = (\forall x)(\exists y)P(f(x,y),a)$,

   (d) $F_4 = (\exists x)((\exists y)(P(f(x,y),a) \Rightarrow P(x,a))$

   nacrtati drvo podformula.

2. Ispitati tačnost formule $(\forall x)P(x,x)$, u interpretaciji $i = (R, P^i)$, gde je R skup realnih brojeva i: (a) P^i je $=$; (b) P^i je $\leq$; (c) P^i je $<$.

3. Ispitati tačnost formula iz zadatka 1 u sledećim interpretacijama:

(a) $i_1 = (Z, =, +, 1)$;

(b) $i_2 = (N, =, \cdot, 1)$;

(c) $i_3 = (R, =, \cdot, 0)$.

4. Data je formula $(\forall x)P(f(x, y), x)$. Da li je interpretacija $(R, =, \cdot)$ model te formule?

5. Konstruisati predikatske formule koje bi u odgovarajućim interpretacijama imale sledeća značenja:

   (a) „x je paran broj" za interpretacije: $i_1 = (N, |, 2)$, $i_2 = (N, =, \cdot, 2)$, $i_3 = (N, =, +)$.

   (b) „Neki brojevi nisu parni" za interpretaciju $(N, =, +)$.

   (c) „$x = \sqrt{y}$" za interpretacije: $i_1 = (R, =, \sqrt{\ })$, $i_2 = (R, =, Q^{i_2}, \cdot)$, gde Q^{i_2} ako i samo ako je x pozitivan.

   (d) „Postoji najmanji broj" za $i_1 = (N, \leq)$ i $i_2 = (N, =, <)$.

   (e) „x je prost broj" za interpretacije: $i_1 = (N, =, |, 1)$, $i_2 = (N, =, |)$.

   (f) „x i y su uzajamno prosti" za interpretacije: $i_1 = (N, =, NZD, 1)$, $i_2 = (N, =, |, 1)$, $i_3 = (N, =, \cdot, 1)$.

6. Prevesti u preneksni oblik formulu

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

7. Izvršiti skolemizaciju formula:

   (a) $(\exists x)(\forall y)P(x, y)$;

   (b) $(\forall x)(\exists y)Q(x, y)$;

   (c) $(\exists u)(\forall x)(\exists y)(\exists v)(\forall z)(\exists t)(P(u, x, y) \wedge P(v, x, z) \Rightarrow P(y, z, t))$;

   (d) $(\exists x)(\exists z)(\forall y)(\exists t)(\forall u)(\exists v)(P(x, y) \wedge P(x, f(z, t, u)) \Rightarrow P(v, v))$.

8. Izvršiti skolemizaciju formule dobijene u zadatku 6.

9. Dat je `BubbleSort` algoritam za sortiranje elemenata datog niza brojeva `x[1],x[2],...,x[n]` od najvećeg ka najmanjem:

```
for(i = n-1; i >= 1; i--)
{
    for(j = 1; j <= i; j++)
    {
            if(x[j] < x[j+1])
            {
                Zameni(x[j],x[j+1]);
            }
    }
}
```

   (`Zameni(a,b)` je, naravno, deo programa koji zamenjuje vrednosti `a` i `b`.) Dokazati ispravnost ovog algoritma, tj. pokazati da će nakon njegovog izvršenja elementi niza zaista biti poređani od najvećeg ka najmanjem.

10. Naći što jednostavniji oblik za negaciju date formule:

(a) $(\forall x)(P(x) \Rightarrow Q(x, c))$;

(b) $(\exists x)(\forall y)xy = y$;

(c) $(\forall x)(\forall y)(x < y \Rightarrow (\exists z)(x < z \wedge z < y))$.

Modeli

11. Dokazati da sledeća formula nije valjana:

$$(\forall x)(P(x) \Rightarrow Q(x)) \Rightarrow \neg((\exists x)P(x) \wedge (\exists x)\neg Q(x)).$$

12. Naći model za sledeći skup formula: $\{(\forall x)(P(x) \Rightarrow \neg Q(x)),\ (\exists x)S(x),$ $(\forall x)(S(x) \Rightarrow P(x)), (\exists x)(S(x) \wedge \neg Q(x))\}$.

13. Data je formula

$$\neg(\forall x)(P(x) \Rightarrow (\forall y)(P(y) \Rightarrow (Q(x) \Rightarrow \neg Q(y)) \vee (\forall z)P(z)))$$

(a) naći jedan model formule

(b) dokazati da nije valjana.

14. Dokazati da nije valjana formula:

$$(\exists x)(P(x) \wedge \neg Q(x)) \wedge (\exists x)(Q(x) \wedge \neg S(x)) \Rightarrow (\forall x)(S(x) \Rightarrow P(x)).$$

15. Naći model za skup formula

$$\{(\forall x)(P(x) \wedge Q(x) \Rightarrow S(x)), (\forall x)(T(x) \Rightarrow S(x)),$$
$$(\exists x)(P(x) \wedge \neg Q(x)), (\exists x)(Q(x) \wedge \neg P(x)), (\exists x)(S(x) \wedge \neg T(x))\}.$$

16. Dokazati da sledeća formula nije valjana:

$$(\exists x)(\forall y)P(x, y) \wedge (\exists x)\neg P(x, x) \wedge$$
$$(\exists x)(\exists y)(x \neq y \wedge P(x, x) \wedge P(y, y)) \Rightarrow (\forall x)(\exists y)\neg P(y, x).$$

17. Dokazati da sledeća formula nije valjana:

$$(\exists x)(\forall y)P(x, y) \wedge (\exists x)(\forall y)P(y, x) \Rightarrow (\forall x)P(x, x).$$

18. Da li je valjana formula

$$(\forall x)P(x, x) \wedge (\forall x)(\exists y)\neg P(x, y) \wedge$$
$$(\forall x)(\exists y)\neg P(y, x) \Rightarrow (\forall x)(\forall y)(P(x, y) \vee P(y, x))?$$

19. Dokazati da nije valjana formula:

$$(\forall x)(\forall y)(P(x, y) \Rightarrow Q(y, x)) \Rightarrow (\forall x)Q(x, x) \vee$$
$$(\forall x)(\forall y)(\neg P(x, y) \vee \neg Q(x, y)).$$

20. Dokazati da sledeća formula nije valjana:

$$(\exists x)(\exists y)P(x, y) \wedge$$
$$(\forall x)(\forall y)(P(x, y) \Leftrightarrow (\exists z)(P(x, z) \wedge P(z, y))) \Rightarrow (\exists x)P(x, x).$$

21. Naći model za sledeći skup formula:

$$\{(\forall x)P(x,x), (\forall x)(\forall y)(P(x,y) \Leftrightarrow (\exists z)(P(x,z) \wedge P(z,y))),$$
$$(\exists x)(\forall y)P(y,x)\}.$$

22. Dokazati da sledeća formula nije valjana:

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

23. Dokazati da sledeća predikatska formula nije valjana:

$$(\forall x)(\forall y)(\exists z)(A(x,y) \wedge B(x,z) \wedge B(y,z)) \Rightarrow$$
$$(\forall x)(\exists y)(\forall z)(A(x,y) \wedge B(y,z) \wedge B(x,z)).$$

24. Dokazati da nije valjana formula:

$$(\forall x)(\forall y)(P(x,y) \Leftrightarrow P(y,x)) \Rightarrow$$
$$(\forall x)P(x,x) \vee (\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z)).$$

25. Naći model za sledeći skup formula:

$$\{(\forall x)\neg P(x,x), (\forall x)(\forall y)(\exists z)(P(x,z) \wedge P(y,z)),$$
$$(\exists x)(\exists y)(x \neq y \wedge \neg P(x,y) \wedge \neg P(y,x)),$$
$$(\forall x)(\forall y)\neg(P(x,y) \wedge P(y,x))\}.$$

26. Naći model za sledeći skup formula:

$$\{(\forall x)\neg P(x,x), (\forall x)(\exists y)P(x,y), (\forall x)(\exists y)P(y,x),$$
$$(\exists x)(\exists y)(x \neq y \wedge \neg P(x,y) \wedge \neg P(y,x)),$$
$$(\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z))\}.$$

27. Dokazati da nije valjana formula:

$$(\forall x)P(x,x) \wedge (\forall x)(\forall y)(P(x,y) \wedge P(y,x) \Rightarrow x = y)$$
$$\wedge(\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z))$$
$$\Rightarrow (\forall x)(\forall y)(\forall z)(P(x,y) \vee P(y,z) \vee P(z,x)).$$

28. Dat je skup predikatskih formula $\{(\forall x)P(x,x), (\forall x)(\forall y)(x \neq y \Rightarrow P(x,y) \vee P(y,x)), (\forall x)(\exists y)(x \neq y \wedge P(x,y)\}$. Za svaku od formula tog skupa naći interpretaciju u kojoj ona nije tačna, a tačne su ostale dve.

29. Data je formula $(\forall x)(P(x) \Rightarrow P(f(x)))$.

    (a) Dokazati da ona nije valjana.

    (b) Da li se može naći model te formule sa domenom $A = \{a,b,c\}$ takav da bude $f^i : \begin{pmatrix} a & b & c \\ c & b & b \end{pmatrix}$?

30. (a) Dokazati da formula $(\forall x)(\forall y)(P(x,y) \Rightarrow P(f(x),f(y)))$ nije valjana.

    (b) Naći model za datu formulu sa domenom $A = \{a,b,c\}$ takav da f bude interpretirano funkcijom $f^i : \begin{pmatrix} a & b & c \\ b & b & a \end{pmatrix}$.

31. Dokazati da nije valjana formula

$$(\exists x)P(x) \Rightarrow (\exists x)(P(f(x)) \wedge \neg P(x)) \vee (\forall x)P(f(x)).$$

32. Naći model za sledeći skup formula:

$$\{(\exists x)\neg P(x,x), (\forall x)(\forall y)(\exists z)(P(x,y) \Rightarrow P(x,z) \wedge P(z,y)),$$
$$(\forall x)P(f(x),x)\}.$$

33. Proveriti da li je valjana formula:

$$(\forall x)(\forall y)P(f(x,y),y) \vee (\forall x)(\forall y)P(x,f(x,y)).$$

34. Naći model za dati skup formula $\{(\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z)),$
$\neg(\forall x)(\forall y)(P(x,y) \wedge P(y,x) \Rightarrow x = y), (\forall x)(\forall y)(P(x,y) \Rightarrow P(f(y),f(x)))\}$.

35. Da li je valjana formula

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

36. Naći model za skup formula

$$\{(\forall x)(P(x) \Leftrightarrow \neg P(f(x))),$$
$$(\forall x)(\forall y)(x \neq y \Rightarrow f(x) \neq f(y)), (\forall x)(\exists y)f(x) = y\}.$$

37. Naći model za sledeći skup formula:

    (a) $\{(\forall x)(\exists y)(P(x,y) \wedge (\forall z)(z \neq y \Rightarrow \neg P(x,z))), (\forall y)(\exists x)P(x,y)\}$;

    (b) $\{(\exists x)(\forall y)P(x,y), (\exists x)(\forall y)P(y,x), (\forall x)P(x,f(x)), (\exists x)(f(x) \neq x)\}$.

Valjane formule

38. Dokazati da je valjana formula

$$(\forall x)(\forall y)(P(x) \wedge \neg P(y) \Rightarrow Q(x)) \wedge (\exists x)(P(x) \wedge \neg Q(x)) \Rightarrow (\forall x)P(x).$$

39. Dokazati da je valjana sledeća formula:

$$(\forall x)(\exists y)(A(x) \Rightarrow B(y)) \wedge (\forall x)(\exists y)(B(x) \Rightarrow C(y))$$
$$\Rightarrow (\forall x)(\exists y)(A(x) \Rightarrow C(y)).$$

40. Dokazati da je sledeća formula valjana:

$$(\forall x)(P(x) \Rightarrow \neg Q(x)) \wedge (\exists x)S(x) \wedge$$
$$(\forall x)(S(x) \Rightarrow P(x)) \Rightarrow (\exists x)(S(x) \wedge \neg Q(x)).$$

41. Da li je valjana sledeća formula:

$$((\exists x)(\neg P(x) \wedge Q(x)) \Rightarrow (\exists x)S(x)) \wedge (\forall x)(P(x) \Leftrightarrow \neg Q(x))$$
$$\wedge(\forall x)(P(x) \vee Q(x) \Rightarrow \neg S(x)) \Rightarrow (\forall x)P(x)?$$

42. Dokazati da je valjana formula

$$(\forall x)(\exists y)P(x,y) \wedge (\forall x)(\forall y)(P(x,y) \wedge \neg Q(y,x) \Rightarrow P(y,x)) \\ \Rightarrow (\forall x)(\exists y)P(y,x) \vee (\exists x)(\exists y)Q(x,y).$$

43. Data je formula

$$(\forall z)((\forall x)(A(x) \Rightarrow B(x,z)) \Rightarrow ((\exists y)A(y) \Rightarrow (\exists y)B(y,z))).$$

(a) Naći njen preneksni oblik.

(b) Da li je ona valjana?

44. Dokazati da je valjana formula:

$$(\forall x)(\forall y)(Q(x,y) \Rightarrow P(x,y)) \wedge (\forall x)(\exists y)\neg P(x,y) \wedge \\ (\forall x)(\forall y)(P(x,x) \Rightarrow P(x,y)) \Rightarrow (\forall x)\neg Q(x,x).$$

45. Dokazati da je valjana sledeća formula

$$(\forall x)(\exists y)A(x,y) \wedge (\forall y)(\exists z)B(y,z) \\ \Rightarrow (\forall x)(\exists y)(\exists z)(A(x,y) \wedge B(y,z)).$$

46. Dokazati da su valjane formule:

(a) $(\forall x)(\forall y)(P(x,y) \Rightarrow Q(y,x)) \wedge (\forall x)(\exists y)(\exists z)(P(x,y) \wedge P(z,x)) \Rightarrow (\forall x)(\exists y)(\exists z)(Q(x,y) \wedge Q(z,x))$;

(b) $(\forall x)(\forall y)(P(x,y) \vee Q(x,y)) \wedge (\forall x)(\forall y)(P(x,y) \Leftrightarrow Q(y,x)) \Rightarrow (\forall x)(P(x, x) \wedge Q(x,x))$;

(c) $(\forall x)((\forall y)P(x,y) \Rightarrow Q(x)) \wedge (\forall x)((\exists y)P(y,x) \Rightarrow Q(x)) \wedge (\exists x)\neg Q(x) \Rightarrow (\exists x)(\exists y)(\neg P(x,y) \wedge \neg P(y,x))$.

47. Dokazati da je sledeća formula valjana:

$$(\forall x)P(x,f(x)) \Rightarrow (\exists x)P(x,x) \vee (\forall x)(\exists y)(P(x,y) \wedge \neg P(x,x)).$$

48. Dokazati da je sledeća formula valjana:

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

Glava 4

Skupovi i relacije

4.1 Skupovi

Tokom proučavanja skupova obilato ćemo koristiti znanje stečeno u prethodnim glavama. Neke od dokaza izvodićemo koristeći pravila oblika $F \models G$ i $F \sim G$ iz iskaznog i predikatskog računa. S druge strane, ponekad ćemo, radi lakšeg dokazivanja ili boljeg razumevanja dokaze izvoditi manje formalno.

Skupove ćemo posmatrati kao kolekcije nekih elemenata. Osnovni jezik teorije skupova sadrži samo jedan binarni relacijski simbol $\in$; sa $x \in A$ označavamo da element x pripada skupu A. Važno je pritom ne razdvajati striktno elemente od skupova, jer i skupovi mogu biti elementi drugih skupova (pogledati definiciju partitivnog skupa). Umesto $\neg(x \in A)$ uglavnom ćemo pisati $x \notin A$.

Tokom rada sa skupovima uvodićemo i druge, izvedene, relacijske i funkcijske simbole. Prvi od njih je jednakost skupova. Za dva skupa reći ćemo da su jednaki ako imaju iste elemente. Ovo se precizira sledećom definicijom.

Definicija 4.1 *Za skupove A i B definišemo: $A = B$ ako važi $(\forall x)(x \in A \Leftrightarrow x \in B)$. Umesto $\neg(A = B)$ pisaćemo $A \neq B$.*

Primer 4.2 *Isti skup obično možemo zapisati na različite načine:*

(1) $\{1, 1\} = \{1\}$ *(dakle, isti element ne može više puta pripadati istom skupu).*

(2) $\{1, 2\} = \{2, 1\}$ *(dakle, unutar skupa ne postoji nikakav podrazumevani poredak).*

(3) Podsećamo se iz odeljka 1.1 da skupove možemo zadavati i kao skupove elemenata koji zadovoljavaju neku predikatsku formulu, npr. $\{n \in Z : n^2 - n - 2 = 0\} = \{-1, 2\}$. Sada kad smo se upoznali s formulama ovaj način zadavanja ćemo često koristiti.

(4) $\{n \in N : n^2 - n - 2 = 0\} = \{2\}$. *Obratimo pažnju da, ako izmenimo skup iz kojeg biramo elemente (npr. uzmemo N umesto Z) skup elemenata koji zadovoljavaju datu formulu više ne mora biti isti.*

(5) Podsetimo se i trećeg načina zadavanja elemenata, preko oblika elemenata, npr. $\{n \in Z : (\exists m \in Z) n = m^2\} = \{m^2 : m \in Z\}$. U zapisu s desne strane navedeno je da skup sadrži sve kvadrate celih brojeva (sve brojeve ,,oblika" m^2).

Uvođenje relacije jednakosti skupova je primer računa sa jednakošću opisanog u odeljku 3.6. Dokažimo da ovako uvedena relacija jednakosti skupova zadovoljava uslove (J1)-(J5). Ustvari, kako jezik teorije skupova nema nijedno funkcijsko slovo i ima samo jedno relacijsko slovo $\in$, uslov (J5) nemamo, a uslov (J4) treba dokazati samo za relaciju $\in$.

Teorema 4.3 *Za sve skupove A, B, C važi:*

(a) $A = A$;

(b) ako $A = B$ onda $B = A$;

(c) ako $A = B$ i $B = C$, onda i $A = C$;

(d) ako $a = b$, $A = B$ i $a \in A$, onda $b \in B$.

Dokaz. (a) Formula $(\forall x)(x \in A \Leftrightarrow x \in A)$ je očigledno tačna za svaki skup A.

(b) Formule $(\forall x)(x \in A \Leftrightarrow x \in B)$ i $(\forall x)(x \in B \Leftrightarrow x \in A)$ su ekvivalentne, pa iz $A = B$ sledi $B = A$.

(c) Pretpostavimo da za svaki element x važi $x \in A \Leftrightarrow x \in B$ i $x \in B \Leftrightarrow x \in C$. Odatle sledi da je $x \in A \Leftrightarrow x \in C$ za sve x pa $A = C$.

(d) $A = B$ znači $(\forall x)(x \in A \Leftrightarrow x \in B)$. Za $x = a = b$ dobijamo $a \in A \Leftrightarrow b \in B$, pa kako je $a \in A$, sledi i $b \in B$. □

Definicija 4.4 *Kažemo da je skup A podskup skupa B ako $(\forall x)(x \in A \Rightarrow x \in B)$. To obeležavamo $A \subseteq B$. Takođe, kažemo da je A pravi podskup skupa B ako je $A \subseteq B$ i $A \neq B$; to pišemo $A \subset B$.*

Primer 4.5 *Obeležimo sa $2N$ skup parnih prirodnih brojeva. Tada*

$$2N \subset N \subset Z \subset Q \subset R \subset C.$$

Da bismo utvrdili da su sve inkluzije striktne, potrebno je da nađemo element jednog skupa koji ne pripada drugom. Npr. $N \subset Z$ jer $-1 \in Z$ ali $-1 \notin N$.

Teorema 4.6 *$A = B$ ako i samo ako $A \subseteq B$ i $B \subseteq A$.*

Dokaz.

$$\begin{aligned} A \subseteq B \wedge B \subseteq A &\sim (\forall x)(x \in A \Rightarrow x \in B) \wedge (\forall x)(x \in B \Rightarrow x \in A) \\ &\sim (\forall x)((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \\ &\sim (\forall x)(x \in A \Leftrightarrow x \in B) \\ &\sim A = B \end{aligned}$$

čime je dokaz završen. □

Prethodna teorema je veoma značajna jer je koristimo u većini slučajeva kada dokazujemo da su dva skupa A i B jednaka, tako što to dokazivanje razdvojimo na dva dela (dve inkluzije): $A \subseteq B$ i $B \subseteq A$. Te delove dokaza obeležavaćemo sa $(\subseteq)$ i $(\supseteq)$, kao pri razdvajanju na smerove. Naravno, iz dokaza se vidi da je ovo samo posledica opštijeg pravila $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p)$ i „slaganja" univerzalnog kvantifikatora s veznikom $\wedge$ (valjana formula 3 s našeg spiska iz odeljka 3.3).

Primer 4.7 *(1) Definišimo* $A = \{n \in N : (\exists k \in N_0)n = 2k+1\} = \{2k+1 : k \in N_0\}$ *i* $B = \{n \in N : (\exists k \in N_0)n = 4k+1\} = \{4k+1 : k \in N_0\}$. *Vidimo da važi* $B \subseteq A$, *jer svaki broj* $4k+1 \in B$ *možemo zapisati kao* $2 \cdot 2k+1$, *pa on pripada i skupu* A. *S druge strane, nije* $A \subseteq B$ *jer recimo* $3 \in A$, *ali* $3 \notin B$. *Prema prethodnoj teoremi sledi* $A \neq B$.

(2) Neka je sada $A = \{2k+2 : k \in Z\}$ *i* $B = \{2k : k \in Z\}$. *Da bismo dokazali da je* $A = B$ *pokažimo posebno* $A \subseteq B$ *i* $B \subseteq A$. *Svaki element* $2k+2 \in A$ *možemo zapisati i kao* $2(k+1)$ *pa, kako i* $k+1 \in Z$, *on pripada i skupu* B. *Obratno, svaki element* $2k \in B$ *može se zapisati i kao* $2(k-1)+2$, *pa on pripada i skupu* A. *Dakle* $A = B$.

Teorema 4.8 *Za sve skupove* A, B, C *važi:*

(a) $A \subseteq A$;

(b) ako $A \subseteq B$ *i* $B \subseteq A$ *onda i* $A = B$;

(c) ako $A \subseteq B$ *i* $B \subseteq C$, *onda i* $A \subseteq C$.

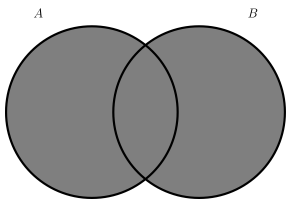
Dokaz. (a) Formula $(\forall x)(x \in A \Rightarrow x \in A)$ je očigledno tačna za svaki skup A.
(b) Ovo sledi iz teoreme 4.6.
(c) Pretpostavimo da za svaki element x važi $x \in A \Rightarrow x \in B$ i $x \in B \Rightarrow x \in C$. Odatle sledi $x \in A \Rightarrow x \in C$. □

Prazan skup možemo definisati ovako: $\emptyset = \{x \in N : x \neq x\}$. Kako je $x \neq x$ netačno za svako x, sledi da nije $x \in \emptyset$ ni za jedno x. Primetimo da je $\emptyset \subseteq A$ za svaki skup A.

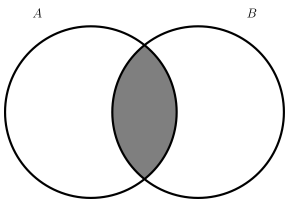
4.2 Operacije nad skupovima

Definicija 4.9 *Definisaćemo četiri binarne operacije nad skupovima. To su, redom: unija, presek, razlika i simetrična razlika skupova.*
$A \cup B = \{x : x \in A \vee x \in B\}$;
$A \cap B = \{x : x \in A \wedge x \in B\}$;
$A \setminus B = \{x : x \in A \wedge x \notin B\}$;
$A \triangle B = \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$.

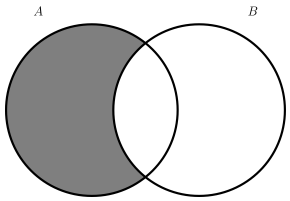
Uobičajeno je da se ove operacije nad skupovima prikazuju tzv. Venovim dijagramima:



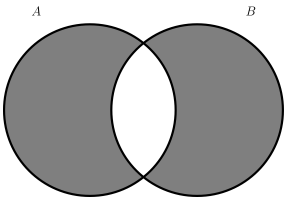
Slika 4.1: Dijagram skupa $A \cup B$



Slika 4.2: Dijagram skupa $A \cap B$



Slika 4.3: Dijagram skupa $A \setminus B$



Slika 4.4: Dijagram skupa $A \triangle B$

Primer 4.10 *(1) Definišimo* $A = \{a, b, c\}$ *i* $B = \{c, d\}$. *Tada je* $A \cup B = \{a, b, c, d\}$, $A \cap B = \{c\}$, $A \setminus B = \{a, b\}$, $B \setminus A = \{d\}$ *i* $A \triangle B = \{a, b, d\}$.

(2) Neka je $A = (0, 5)$ *i* $B = [2, 7]$ *(dakle, A je otvoreni, a B zatvoreni interval realnih brojeva). Tada* $A \cup B = (0, 7]$, $A \cap B = [2, 5)$, $A \setminus B = (0, 2)$, $B \setminus A = [5, 7]$ *i* $A \triangle B = (0, 2) \cup [5, 7]$. *Opštije, možemo zaključiti da je* $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Iz definicija direktno sledi da za sve skupove A i B važi: $A \subseteq A \cup B$, $B \subseteq A \cup B$, $A \cap B \subseteq A$ i $A \cap B \subseteq B$. Ove osobine ćemo takođe često koristiti.

Definicija 4.11 *Kažemo da su skupovi A i B disjunktni ako je* $A \cap B = \emptyset$, *tj. ako nemaju zajedničkih elemenata.*

Teorema 4.12 *Za sve skupove* A, B *i* C *važi:*

(a) $A \cup A = A$ *i* $A \cap A = A$;

(b) $A \cup B = B \cup A$ *i* $A \cap B = B \cap A$;

(c) $A \cup (B \cup C) = (A \cup B) \cup C$ *i* $A \cap (B \cap C) = (A \cap B) \cap C$;

(d) $A \cup (A \cap B) = A$ *i* $A \cap (A \cup B) = A$;

(e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *i* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

(f) $A \cup \emptyset = A$ *i* $A \cap \emptyset = \emptyset$.

Dokaz. Sve jednakosti navedene u teoremi dokazuju se na isti način (osim dela (f)), direktno iz poznatih pravila o ekvivalentnosti iskaznih formula, pa ćemo dokazati samo neke od njih.

(b) Za svako x imamo:

$$\begin{aligned} x \in A \cup B &\sim x \in A \vee x \in B \\ &\sim x \in B \vee x \in A \\ &\sim x \in B \cup A. \end{aligned}$$

Pritom smo koristili poznato pravilo $p \vee q \sim q \vee p$.

(e) Za svako x važi:

$$\begin{aligned} x \in A \cap (B \cup C) &\sim x \in A \wedge x \in B \cup C \\ &\sim x \in A \wedge (x \in B \vee x \in C) \\ &\sim (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\sim x \in A \cap B \vee x \in A \cap C \\ &\sim x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Ovde smo koristili pravilo $p \wedge (q \vee r) \sim (p \wedge q) \vee (p \vee r)$.

(f) Za svako x:

$$\begin{aligned} x \in A \cup \emptyset &\sim x \in A \vee x \in \emptyset \\ &\sim x \in A, \end{aligned}$$

jer je $x \in \emptyset$ uvek netačno. □

Osobine opisane u prethodnoj teoremi nazivamo istim imenima kao i odgovarajuća pravila iskaznog računa koja koristimo u njihovim dokazima. Tako, pravilo (a) je idempotentnost, (b) je komutativnost, (c) asocijativnost, (d) apsorpcija a (e) distributivnost.

Sledeću teoremu koristićemo često u dokazima.

Teorema 4.13 *Za sve skupove A, B i C važi:*

(a) $A \cup B \subseteq C$ ako i samo ako $A \subseteq C$ i $B \subseteq C$;

(b) $A \subseteq B \cap C$ ako i samo ako $A \subseteq B$ i $A \subseteq C$.

Dokaz. (a)

$$\begin{aligned} A \cup B \subseteq C &\sim (\forall x)(x \in A \cup B \Rightarrow x \in C) \\ &\sim (\forall x)(x \in A \vee x \in B \Rightarrow x \in C) \\ &\sim (\forall x)(\neg(x \in A \vee x \in B) \vee x \in C) \\ &\sim (\forall x)((\neg x \in A \wedge \neg x \in B) \vee x \in C) \\ &\sim (\forall x)((\neg x \in A \vee x \in C) \wedge (\neg x \in B \vee x \in C)) \\ &\sim (\forall x)((x \in A \Rightarrow x \in C) \wedge (x \in B \Rightarrow x \in C)) \\ &\sim (\forall x)(x \in A \Rightarrow x \in C) \wedge (\forall x)(x \in B \Rightarrow x \in C) \\ &\sim A \subseteq C \wedge B \subseteq C \end{aligned}$$

(U dokazu smo koristili činjenicu da se kvantifikator $\forall$ „slaže" s veznikom $\wedge$, videti napomenu nakon spiska valjanih formula u odeljku 3.3.)

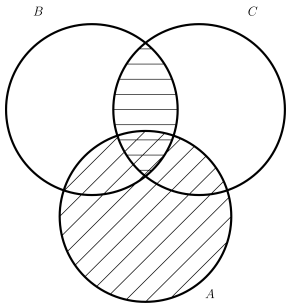
(b) Dokaz izvodimo u dva dela.

($\Rightarrow$) Neka je $A \subseteq B \cap C$. Pošto je $B \cap C \subseteq B$, sledi da je $A \subseteq B$. Analogno je i $A \subseteq C$.

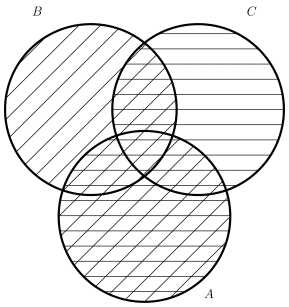
($\Leftarrow$) Neka je sada $A \subseteq B$ i $A \subseteq C$. Za svaki element $x \in A$ prvi uslov povlači da je $x \in B$ a drugi da je $x \in C$; dakle $x \in B \cap C$. Ali to znači da je $A \subseteq B \cap C$. □

Primer 4.14 *Operacija $\setminus$ nije ni komutativna ni asocijativna: ako je npr. $A = \{1\}$, $B = \{1, 2\}$ i $C = \{1, 2, 3\}$, onda je $A \setminus B = \emptyset$ a $B \setminus A = \{2\}$. Takođe je $(A \setminus B) \setminus C = \emptyset \setminus C = \emptyset$ dok je $A \setminus (B \setminus C) = A \setminus \emptyset = \{1\}$.*

Da bi se bolje razumele jednakosti iz teoreme 4.12 može biti od koristi skicirati Venove dijagrame tih skupova. Ilustrujmo npr. distributivnost $\cup$ prema $\cap$. Na prvom dijagramu skup A je šrafiran na jedan način a $B \cap C$ na drugi te je rezultujući skup njihova unija; na drugom je $(A \cup B)$ šrafiran na jedan a $(A \cup C)$ na drugi način i rezultujući skup je njihov presek:



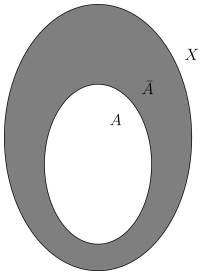
Slika 4.5: Dijagram skupa $A \cup (B \cap C)$



Slika 4.6: Dijagram skupa $(A \cup B) \cap (A \cup C)$

Ponekad se za uniju ili presek skupova koristi skraćeni zapis: $\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \ldots \cup A_n$ i $\bigcap_{k=1}^{n} A_k = A_1 \cap A_2 \cap \ldots \cap A_n$. Ovakav način zapisivanja je posebno značajan jer se može koristiti i za unije i preseke beskonačno mnogo skupova, npr. $\bigcup_{k=1}^{\infty} A_k$. On je analogan zapisu suma i proizvoda: $\sum_{k=1}^{n} a_k = a_1 + a_2 + \ldots + a_n$ i $\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Definicija 4.15 *Neka je $A \subseteq X$. Komplement skupa A u odnosu na skup X definišemo ovako: $\bar{A} = X \setminus A$.*



Slika 4.7: Dijagram skupa $\bar{A}$

Napomenimo da se nekada za komplement koriste i druge oznake, npr. A' ili A^c. Sa svakim od navedenih zapisa treba biti oprezan ako iz konteksta nije jasno u odnosu na koji nadskup se računa komplement, jer to može dovesti do zabune. Recimo, neka je $A = N$. Komplement ovog skupa u odnosu na $X = N_0$ je $\bar{N} = \{0\}$, a u odnosu na $X = Z$ je $\bar{N} = \{x \in Z : x \leq 0\}$.

Teorema 4.16 *(a) $\overline{(\overline{A})} = A$. (b) Ako je $A \subseteq B$, onda $\bar{B} \subseteq \bar{A}$.*

Dokaz. Neka se komplementi računaju u odnosu na skup X (tj. $\overline{A} = X \setminus A$).

(a)
$$\begin{aligned} x \in \overline{\overline{A}} &\sim x \in X \wedge \neg(x \in \bar{A}) \\ &\sim x \in X \wedge \neg(x \in X \wedge \neg x \in A) \\ &\sim x \in X \wedge (\neg x \in X \vee x \in A) \\ &\sim (x \in X \wedge \neg x \in X) \vee (x \in X \wedge x \in A) \\ &\sim x \in X \wedge x \in A \\ &\sim x \in A \end{aligned}$$

(Poslednja ekvivalencija važi jer je $A \subseteq X$.) Kao što vidimo, u svakom koraku dokaza deo $x \in X$ se samo prepisuje, pa da bismo pojednostavili ovakve dokaze

(sa komplementima) ubuduće ćemo $x \in \overline{A}$ zamenjivati samo sa $x \notin A$, a $x \in X$ ćemo podrazumevati. Tako bi prethodni dokaz glasio

$$\begin{aligned} x \in \overline{\overline{A}} &\sim \neg(x \in \bar{A}) \\ &\sim \neg\neg x \in A \\ &\sim x \in A. \end{aligned}$$

(b) Pretpostavimo da je $A \subseteq B$, odnosno $x \in A \Rightarrow x \in B$ za sve x. Odatle sledi (kontrapozicijom) $\neg x \in B \Rightarrow \neg x \in A$ pa imamo

$$\begin{aligned} x \in \overline{B} &\sim \neg x \in B \\ &\models \neg x \in A \\ &\sim x \in \overline{A}. \end{aligned}$$

Postoji drugi način da se definiše operacija $\setminus$: $A \setminus B = A \cap \overline{B}$ (pritom se komplement računa u odnosu na bilo koji skup koji sadrži $A \cup B$). Dakle, iako za operaciju $\setminus$ ne važe osobine navedene u teoremi 4.12, izražavajući je na ovaj način preko operacija preseka i komplementa možemo u dokazima koristiti neke od njih.

4.3 Predstavljanje skupova u računarstvu

Neki programski jezici imaju poseban skupovni tip podataka, ali ne svi. Kako se skupovi najjednostavnije predstavljaju u memoriji računara? Da bismo predstavili neki skup A, moramo ga posmatrati kao podskup nekog većeg skupa X, i u memoriji rezervisati niz bitova koji će imati po jedan element za svaki $x \in X$. Sada, za $x \in A$ odgovarajući bit će imati vrednost 1, a za $x \in \overline{A}$ vrednost 0. Čitalac neka uporedi ovo sa definicijom karakteristične funkcije skupa A (primer 5.4).

Skupovima predstavljenim na ovaj način možemo manipulisati pomoću bitovskih operacija. U Javi, recimo, imamo bitovsko ,,i" u oznaci &, bitovsko ,,ili" u oznaci | kao i bitovsko ,,ekskluzivno ili" (`XOR`). Oni funkcionišu kao i ,,obična" konjunkcija, disjunkcija, odnosno $\veebar$, ali deluju na odgovarajuće pojedinačne bitove.

Primer 4.17 *Binarni zapisi 00101110 i 01111001 mogu predstavljati skupove, npr. podskupove skupa* $\{1, 2, \ldots, 8\}$*, konkretno* $\{3, 5, 6, 7\}$ *i* $\{2, 3, 4, 5, 8\}$*. Rezultati izvršavanja bitovskih operacija nad njima bili bi sledeći:*

$$\begin{aligned} 00101110 \;\&\; 01111001 &= 00101000 \\ 00101110 \mid 01111001 &= 01111111 \\ 00101110 \;\texttt{XOR}\; 01111001 &= 01010111. \end{aligned}$$

Možemo primetiti da, ako ti nizovi bitova predstavljaju skupove, onda ove tri operacije odgovaraju upravo skupovnim operacijama $\cap$*,* $\cup$ *i* $\triangle$*:*

$$\begin{aligned} \{3, 5, 6, 7\} \cap \{2, 3, 4, 5, 8\} &= \{3, 5\} \\ \{3, 5, 6, 7\} \cup \{2, 3, 4, 5, 8\} &= \{2, 3, 4, 5, 6, 7, 8\} \\ \{3, 5, 6, 7\} \triangle \{2, 3, 4, 5, 8\} &= \{2, 4, 6, 7, 8\}. \end{aligned}$$

4.4 Direktni proizvod i partitivni skup

Definicija 4.18 *Uređeni par elemenata a i b definišemo ovako:*

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Suština prethodne definicije je da uvede objekat koji bi u sebi ,,sadržao" dva jednostavnija objekta, a i b, ali tako da je njihov redosled određen (da se zna koji od ta dva elementa je prvi a koji drugi). Ovo ne možemo postići neuređenim parom, odnosno skupom $\{a, b\}$, jer je $\{a, b\} = \{b, a\}$. Dakle, osnovna osobina uređenog para je da je $(a, b) \neq (b, a)$. Sledeća teorema dokazuje nešto jaču osobinu.

Teorema 4.19 *$(a, b) = (c, d)$ ako i samo ako $a = c$ i $b = d$.*

Dokaz. ($\Leftarrow$) Ako je $a = c$ i $b = d$ onda iz definicije uređenog para direktno sledi $(a, b) = (c, d)$.

($\Rightarrow$) Neka je $(a, b) = (c, d)$, tj. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Ova jednakost skupova znači da imamo dve mogućnosti:

1° $\{a\} = \{c\}$ i $\{a, b\} = \{c, d\}$. Iz prve jednakosti sledi $a = c$, a koristeći to iz druge dobijamo $b = d$.

2° $\{a\} = \{c, d\}$ i $\{a, b\} = \{c\}$. Iz prve jednakosti sledi $a = c = d$, a iz druge $c = a = b$, pa dobijamo $a = b = c = d$. □

Koristeći definiciju uređenog para možemo definisati i uređene n-torke elemenata za proizvoljno $n \in N$. One se definišu rekurzivno: ako su već definisane uređene n-torke, uređenu $(n + 1)$-torku definišemo sa

$$(a_1, a_2, a_3, \ldots, a_{n+1}) = ((a_1, a_2, \ldots, a_n), a_{n+1}).$$

Npr. za $n = 3$ je $(a, b, c) = ((a, b), c)$. I za n-torke važi tvrđenje analogno teoremi 4.19.

Teorema 4.20 *$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ ako i samo ako $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.*

Dokaz. Teoremu dokazujemo matematičkom indukcijom.

B.I. Za $n = 2$ ovo je teorema 4.19.

I.H. Pretpostavimo da tvrđenje važi za neko $n \geq 2$.

I.K. $(a_1, a_2, \ldots, a_n, a_{n+1}) = (b_1, b_2, \ldots, b_n, b_{n+1})$, odnosno $((a_1, a_2, \ldots, a_n), a_{n+1}) = ((b_1, b_2, \ldots, b_n), b_{n+1})$, prema teoremi 4.19 važi ako i samo ako je $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ i $a_{n+1} = b_{n+1}$. Ali po indukcijskoj hipotezi $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ je ekvivalentno sa $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. □

Uređene n-torke koristili smo, između ostalog, u glavi 3 (mada ne pod tim imenom): svaka interpretacija neke formule je jedna uređena n-torka čiji prvi član je domen, a ostali su relacije, funkcije i konstante za svaki simbol jezika te formule. Mi ubuduće nećemo nigde koristiti samu definiciju uređenog para (ili n-torke) već samo prethodne dve teoreme.

Definicija 4.21 *Direktan proizvod skupova A i B je skup*

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Opštije, možemo definisati i direktan proizvod više skupova:

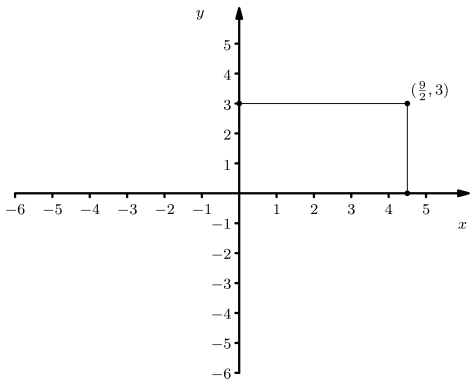
$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \text{ za } i = 1, 2, \ldots, n\}.$$

Ako su svi skupovi A_i jednaki, pišemo $A^n = \underbrace{A \times A \times \ldots \times A}_{n}$.

Iz definicije uređene n-torke vidimo da je $A \times B \times C$ ustvari skup $(A \times B) \times C$. Mogli smo definisati ovaj skup i kao $A \times (B \times C)$, videti zadatak 46(b).

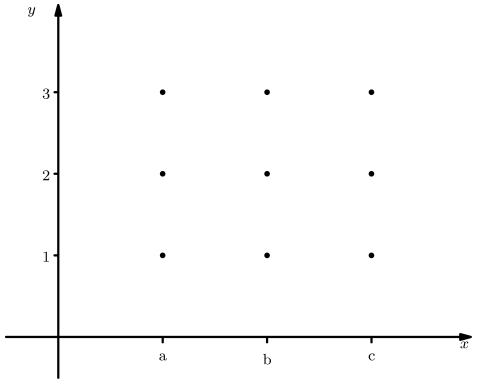
Primer 4.22 *(1) Koordinatni sistem u ravni je ustvari skup uređenih parova (x, y) realnih brojeva, tj. skup R^2. U ravni se izaberu dve normalne prave (x-osa i y-osa) i uspostavi se korespondencija njihovih tačaka sa skupom realnih brojeva; dakle, svakoj tački dodeli se po jedan realan broj. Zatim se svaka tačka ravni projektuje na te ose i pridružuju joj se brojevi x i y koji odgovaraju dobijenim projekcijama. Brojeve x i y zovemo prva, odnosno druga koordinata para (x, y); ove nazive ćemo koristiti i u slučaju uređenih parova u drugim direktnim proizvodima.*

Tako, tačka označena na slici projektuje se na tačku $\frac{9}{2}$ na x-osi i tačku 3 na y-osi, te su njene koordinate $(\frac{9}{2}, 3)$.



Slika 4.8: Koordinatni sistem

(2) I drugi direktni proizvodi mogu se prikazivati u vidu koordinatnog sistema. Npr. skup $\{a, b, c\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$ možemo prikazati na sledeći način:



Definicija 4.23 *Partitivni skup skupa A je skup svih podskupova skupa A:* $P(A) = \{B : B \subseteq A\}$.

Primer 4.24 *(1) Neka je* $A = \{1, 2, 3\}$. *Tada*

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

(2) Neka je $A = \emptyset$. *Tada* $P(A) = \{\emptyset\}$, *jer je jedini podskup praznog skupa on sam.*

(3) Ako je $A = \{\{1, 2\}\}$, *ovaj skup ima samo jedan element, a to je* $\{1, 2\}$. *Stoga je* $P(A) = \{\emptyset, \{\{1, 2\}\}\}$.

Na prvi pogled može se činiti neobičnim da skupovi budu elementi drugih skupova. Međutim, pri aksiomatskom zasnivanju teorije skupova svi objekti sa kojima se manipuliše su skupovi, dakle svaki element nekog skupa je drugi skup. To, između ostalog, znači da se svi prirodni brojevi uvode kao neki skupovi; u odeljku 5.8 videćemo kako se to postiže.

4.5 Relacije

Sada ćemo dati formalnu definiciju pojma relacije.

Definicija 4.25 *n-arna relacija na skupovima $A_1, A_2, \ldots, A_n$ je podskup skupa $A_1 \times A_2 \times \ldots \times A_n$.*

Relacije arnosti 1 (za $n = 1$) zovemo unarne. Unarna relacija na skupu A je ustvari podskup skupa A. Dakle, njome izražavamo neko svojstvo koje poseduju neki od elemenata skupa A (oni koji su „u relaciji").

Mi ćemo najčešće baratati binarnim relacijama, koje dobijamo za $n = 2$. Binarna relacija na skupovima A i B izražava neki odnos između elemenata iz A i elemenata iz B. U specijalnom slučaju, kada su skupovi A i B jednaki, tj. kada je $\rho \subseteq A^2$ za neki skup A, kažemo samo da je ρ binarna relacija na skupu A.

Relacije arnosti veće od 2 ćemo ređe susretati. Pomenimo još da se relacije arnosti 3 nazivaju ternarne.

Oznake koje ćemo koristiti za relacije su najčešće velika slova $P, Q, S, \ldots$ Za binarne relacije često koristimo i grčka slova $\rho, \sigma, \tau, \theta, \ldots$ i infiksni zapis. To znači da ćemo umesto $(x, y) \in \rho$ ili $\rho(x, y)$ često pisati $x \rho y$, kao što je uobičajeno za neke poznate relacije: $x \leq y$, $x \mid y$ itd.

Primer 4.26 *(1) $\emptyset$ i A^n su „ekstremni" primeri n-arnih relacija: prva je takva da nijedna n-torka elemenata nije u relaciji, a druga je takva da je svaka n-torka u relaciji.*

(2) Na svakom skupu A imamo i relaciju jednakosti, koju ćemo takođe zvati i „dijagonala" i označavati $\triangle_A = \{(a, a) : a \in A\}$. Pored standardne oznake $=$ uvodimo i ovu dodatnu oznaku da bismo izbegli neugodne izraze tipa $\rho ==$ (ako želimo da zapišemo da je relacija ρ jednaka sa $=$).

U ovom i nekim narednim primerima indekse ćemo koristiti da naglasimo skup na kojem posmatramo relaciju: treba primetiti da relacija $\triangle_A$ jednakosti na skupu $A = \{1, 2, 3\}$ i relacija $\triangle_N$ na skupu prirodnih brojeva ne sadrže iste uređene parove: $(4, 4) \in \triangle_N$ *ali* $(4, 4) \notin \triangle_A$.

Odakle potiče naziv ,,dijagonala"? To će se videti ako relaciju $\triangle_A$ predstavimo tablicom:

$\triangle_A$	1	2	3
1	$\top$	$\bot$	$\bot$
2	$\bot$	$\top$	$\bot$
3	$\bot$	$\bot$	$\top$

Sada, pošto je svaki element u relaciji samo sa samim sobom, u tablici se na dijagonali nalazi $\top$, a na ostalim mestima $\bot$.

(3) Na skupu tačaka u ravni definišimo jednu ternarnu relaciju: $I(x, y, z)$ ako su x, y i z kolinearne i tačka y se nalazi između x i z. Za nju važi recimo formula $(\forall x)(\forall y)(\forall z)(I(x, y, z) \Rightarrow I(z, y, x))$, koja kaže da, ako je y između tačaka x i z, onda je i između z i x.

(4) Neka je A skup muškaraca a B skup žena. Relaciju P na skupu $A \cup B$ definišimo ovako: $P(x, y)$ ako je x dete osobe y.

(5) Neka je i dalje A skup muškaraca a B skup žena. Relaciju $Q \subseteq A \times B \times (A \cup B)$ definišimo sa: $Q(x, y, z)$ ako je x otac, a y majka osobe z. Važi $(\forall x)(\forall y)(\forall z)(Q(x, y, z) \Rightarrow P(z, x) \wedge P(z, y))$, jer ta formula kaže da, ako je x otac a y majka osobe z, onda z mora biti dete i osobe x i osobe y.

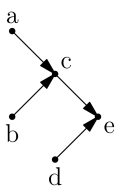
(6) Evo jednog primera ternarne relacije na skupu N: definišimo da važi $S(x, y, z)$ ako je $x + y < z$.

Primeri na koji ćemo posebno obratiti pažnju su grafovi. Razlog je činjenica da mnogi značajni algoritmi rešavaju upravo probleme na grafovima. Evo definicija nekoliko osnovnih pojmova.

Definicija 4.27 *Orijentisani graf (ili digraf) je uređeni par (V, E), gde je E binarna relacija na skupu V; drugim rečima $E \subseteq \{(u, v) : u, v \in V\}$. Elemente skupa V zovemo čvorovi, a elemente skupa E grane.*

Grafovima obično predstavljamo veze između nekih objekata. Npr. čvorovi mogu biti gradovi a grane avio linije između njih. Grane u digrafovima su usmerene, tj. razlikujemo granu (u, v) od čvora u do čvora v od grane (v, u) od v do u. Grafovi su pogodni zbog svog slikovitog predstavljanja: čvorove možemo predstaviti tačkama, a grane strelicama koje ih spajaju. Ako npr. A, B i P imaju značenje kao u primeru (4) gore, $(A \cup B, P)$ je jedan digraf. Ovakve strukture su pogodne recimo za predstavljanje rezultata nekog turnira, pri čemu bi V bio skup takmičara, a postojanje grane (u, v) značilo bi da je takmičar u pobedio u partiji protiv takmičara v.

Primer 4.28 *Neka je $V = \{a, b, c, d, e\}$ ponovo neki skup osoba, takav da su a i b roditelji osobe c, a c i d roditelji osobe e. Ovoj situaciji odgovara skup grana $E = \{(a, c), (b, c), (c, e), (d, e)\}$. Digraf (V, E) može se predstaviti kao na slici:*



Nešto kasnije uvešćemo i (neorijentisane) grafove koji predstavljaju posebnu vrstu relacija.

4.6 Operacije nad binarnim relacijama

Kako su relacije na nekom skupu A posebna vrsta skupova, nad njima možemo primenjivati skupovne operacije: $\cup, \cap$ i $\setminus$. Sve osobine tih operacija dokazane u teoremama 4.12 i 4.13 važe i pri radu sa relacijama. Kada posmatramo relaciju ρ na skupu A, njen komplement uvek računamo u odnosu na punu relaciju A^2, pa nemamo dvosmislenost oznake $\bar{\rho}$ kao pri radu sa skupovima uopšte.

Definišimo i dve operacije koje se primenjuju samo na binarnim relacijama.

Definicija 4.29 *Inverzna relacija relacije ρ označava se ρ^{-1} i definiše ovako:*

$$\rho^{-1} = \{(y, x) : (x, y) \in \rho\}.$$

Kompozicija relacija ρ i σ označava se sa $\rho \circ \sigma$ i definiše kao

$$\rho \circ \sigma = \{(x, y) : (\exists z)((x, z) \in \rho \wedge (z, y) \in \sigma)\}.$$

Primer 4.30 *(1) Neka je $A = \{1, 2, 3\}$, $\rho = \{(2, 1)\}$ i $\sigma = \{(1, 1), (1, 3), (2, 3)\}$. Tada je:*

$\rho \cup \sigma = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$;

$\rho \cap \sigma = \emptyset$;

$\bar{\rho} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$;

$\bar{\sigma} = \{(1, 2), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$;

$\rho^{-1} = \{(1, 2)\}$;

$\sigma^{-1} = \{(1, 1), (3, 1), (3, 2)\}$;

$\rho \circ \sigma = \{(2, 1), (2, 3)\}$;

$\sigma \circ \rho = \emptyset$.

Vidimo da pri konstrukciji $\rho \circ \sigma$ tražimo u kojim parovima (x, z) iz ρ se isti element z pojavljuje na drugoj koordinati kao u nekim parovima (z, y) iz σ na prvoj; tada par (x, y) pripada kompoziciji. Tako, $(2, 1) \in \rho$ i $(1, 3) \in \sigma$ povlači da $(2, 3) \in \rho \circ \sigma$.

(2) Za relaciju $<_Z$ imamo: $<_Z^{-1} = >_Z$ i $\overline{<_Z} = \geq_Z$.

(3) Ako je P relacija iz tačke (4) primera 4.26, tada je:

$P^{-1}(x, y)$ ako i samo ako je x roditelj osobe y;

$P \circ P(x, y)$ ako i samo ako je x dete neke osobe koja je dete osobe y, dakle ako je x unuk ili unuka osobe y.

Iz tačke (1) gornjeg primera vidimo da operacija $\circ$ nije komutativna, odnosno da ne mora važiti $\rho \circ \sigma = \sigma \circ \rho$.

U narednim teoremama dajemo pregled važnih osobina operacija nad relacijama koje ćemo često koristiti u nastavku.

Teorema 4.31 *Ako je ρ binarna relacija na skupu A, onda važi:*

(a) $(\rho^{-1})^{-1} = \rho$;

(b) $(\bar{\rho})^{-1} = \overline{\rho^{-1}}$;

(c) $\rho \circ \triangle_A = \triangle_A \circ \rho = \rho$.

Dokaz. Kao i pri radu sa skupovima uopšte, da bismo pokazali da su dve relacije jednake potrebno je dokazati da imaju iste elemente. Međutim, kako su elementi binarnih relacija uređeni parovi, treba pokazati da svaki uređeni par pripada prvoj relaciji ako i samo ako pripada drugoj.

(a)
$$\begin{aligned}(x,y) \in (\rho^{-1})^{-1} &\sim (y,x) \in \rho^{-1} \\ &\sim (x,y) \in \rho.\end{aligned}$$

(b)
$$\begin{aligned}(x,y) \in (\bar{\rho})^{-1} &\sim (y,x) \in \bar{\rho} \\ &\sim (y,x) \in A^2 \wedge (y,x) \notin \rho \\ &\sim (x,y) \in A^2 \wedge (x,y) \notin \rho^{-1} \\ &\sim (x,y) \in \overline{\rho^{-1}}.\end{aligned}$$

U prethodnom dokazu, ekvivalentnost formula $(y,x) \notin \rho$ i $(x,y) \notin \rho^{-1}$ sledi iz činjenice da iz $F \sim G$ sledi $\neg F \sim \neg G$.

(c) Dokažimo da je $\rho \circ \triangle_A = \rho$, a jednakost $\triangle_A \circ \rho = \rho$ dokazuje se analogno.

$$\begin{aligned}(x,y) \in \rho \circ \triangle_A &\sim (\exists z)((x,z) \in \rho \wedge (z,y) \in \triangle_A) \\ &\sim (\exists z)((x,z) \in \rho \wedge z = y) \\ &\sim (\exists z)(x,y) \in \rho \\ &\sim (x,y) \in \rho.\end{aligned}$$

Da iz formule u drugom redu sledi naredna posledica je pravila (J4) za relaciju $\in$ dokazanog u teoremi 4.3(d). Obratno, iz formule u trećem redu sledi prethodna na osnovu teoreme 3.27(b). Četvrta ekvivalencija sledi iz pravila $(\exists z)F \sim F$, koje očigledno važi ako se z ne pojavljuje u formuli F. □

Teorema 4.32 *Ako su ρ i σ binarne relacije, onda važi:*

(a) $(\rho \cup \sigma)^{-1} = \rho^{-1} \cup \sigma^{-1}$;

(b) $(\rho \cap \sigma)^{-1} = \rho^{-1} \cap \sigma^{-1}$;

(c) $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$.

Dokaz. (a)
$$\begin{aligned}(x,y) \in (\rho \cup \sigma)^{-1} &\sim (y,x) \in \rho \cup \sigma \\ &\sim (y,x) \in \rho \vee (y,x) \in \sigma \\ &\sim (x,y) \in \rho^{-1} \vee (x,y) \in \sigma^{-1} \\ &\sim (x,y) \in \rho^{-1} \cup \sigma^{-1}.\end{aligned}$$

(b) se pokazuje analogno.

(c)
$$\begin{aligned}(x,y) \in (\rho \circ \sigma)^{-1} &\sim (y,x) \in \rho \circ \sigma \\ &\sim (\exists z)((y,z) \in \rho \wedge (z,x) \in \sigma) \\ &\sim (\exists z)((x,z) \in \sigma^{-1} \wedge (z,y) \in \rho^{-1}) \\ &\sim (x,y) \in \sigma^{-1} \circ \rho^{-1}\end{aligned}$$

čime je dokaz završen. □

Teorema 4.33 *Ako su ρ, σ i τ binarne relacije, onda važi $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$.*

Dokaz.

$$\begin{aligned}
(x,y) \in \rho \circ (\sigma \circ \tau) &\sim (\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma \circ \tau) \\
&\sim (\exists z)((x,z) \in \rho \wedge (\exists t)((z,t) \in \sigma \wedge (t,y) \in \tau)) \\
&\sim (\exists z)(\exists t)((x,z) \in \rho \wedge ((z,t) \in \sigma \wedge (t,y) \in \tau)) \\
&\sim (\exists t)(\exists z)(((x,z) \in \rho \wedge (z,t) \in \sigma) \wedge (t,y) \in \tau) \\
&\sim (\exists t)((\exists z)((x,z) \in \rho \wedge (z,t) \in \sigma) \wedge (t,y) \in \tau) \\
&\sim (\exists t)((x,t) \in \rho \circ \sigma) \wedge (t,y) \in \tau) \\
&\sim (x,y) \in (\rho \circ \sigma) \circ \tau
\end{aligned}$$

što je i trebalo dokazati. □

Teorema 4.34 *Iz $\rho \subseteq \sigma$ sledi:*

(a) $\rho^{-1} \subseteq \sigma^{-1}$;

(b) $\rho \circ \tau \subseteq \sigma \circ \tau$;

(c) $\tau \circ \rho \subseteq \tau \circ \sigma$.

Dokaz. (a) $\rho \subseteq \sigma$ znači da svaki uređeni par koji je u ρ mora pripadati i relaciji σ. Koristeći to dobijamo:

$$\begin{aligned}
(x,y) \in \rho^{-1} &\sim (y,x) \in \rho \\
&\models (y,x) \in \sigma \\
&\sim (x,y) \in \sigma^{-1}.
\end{aligned}$$

(b)
$$\begin{aligned}
(x,y) \in \rho \circ \tau &\sim (\exists z)((x,z) \in \rho \wedge (z,y) \in \tau) \\
&\models (\exists z)((x,z) \in \sigma \wedge (z,y) \in \tau) \\
&\sim (x,y) \in \sigma \circ \tau.
\end{aligned}$$

(c) Analogno dokazu (b) □

4.7 Projekcije i baze podataka

Definisaćemo još neke operacije nad relacijama. One se, sasvim analogno, mogu definisati i za relacije koje nisu binarne, ali mi ćemo se, jednostavnosti radi, zadržati na binarnim.

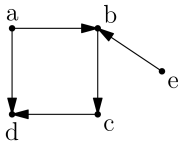
Definicija 4.35 *Neka je $\rho \subseteq X \times Y$ binarna relacija. Njena prva projekcija je*

$$\pi_1(\rho) = \{x \in X : (\exists y \in Y)(x,y) \in \rho\},$$

a druga projekcija:

$$\pi_2(\rho) = \{y \in Y : (\exists x \in X)(x,y) \in \rho\}.$$

Primer 4.36 *Neka je (V,E) orijentisani graf, gde $V = \{a,b,c,d,e\}$ i $E = \{(a,b),(a,d),(b,c),(c,d),(e,b)\}$. Prva projekcija relacije E je $\pi_1(E) = \{a,b,c,e\}$ - skup čvorova iz kojih izlazi bar jedna grana, a druga projekcija: $\pi_2(E) = \{b,c,d\}$ - skup čvorova do kojih vodi bar jedna grana.*



Relacije su blisko vezane sa bazama podataka. Naime, jedan od tipičnih načina organizacije baze podataka je tzv. relacioni model, po kojem su podaci organizovani u tabele. Međutim, tabela sa n kolona nije ništa drugo do n-arna relacija.

Primer 4.37 *Pretpostavimo da želimo u bazi da sačuvamo podatke o predmetima, profesorima, asistentima i studentima. Jedan način da se to učini je pomoću dve tabele: u jednoj (nazvanoj PROFESORI) bi bili podaci o tome koji profesor predaje koji predmet a u drugoj (nazvanoj STUDENTI), pošto za isti predmet može biti zaduženo više asistenata, bili bi podaci o tome koji student sluša koji predmet i kod kojeg asistenta. To bi moglo izgledati ovako:*

K	P
$Analiza$	$Todorovic$
$Teor.\ osn.\ inf.$	$Sobot$
$Algebra$	$Mirkovic$
$Programiranje$	$Radovic$

S	K	A
$Petar$	$Analiza$	$Brankovic$
$Petar$	$Teor.\ osn.\ inf.$	$Vukovic$
$Petar$	$Programiranje$	$Petrovic$
$Milos$	$Analiza$	$Brankovic$
$Milos$	$Teor.\ osn.\ inf.$	$Simovic$
$Milos$	$Programiranje$	$Petrovic$
$Lazar$	$Programiranje$	$Markovic$
$Lazar$	$Algebra$	$Nikolic$

To znači da imamo 4 skupa s kojima radimo: skup predmeta $K = \{Analiza, TOI, Algebra, Prog\}$*, skup profesora* $P = \{Todorovic, Sobot, Mirkovic, Radovic\}$*, skup asistenata* $A = \{Brankovic, Vukovic, Petrovic, Simovic, Markovic, Nikolic\}$ *i skup studenata* $S = \{Petar, Milos, Lazar\}$ *(u realnoj bazi, naravno, količina podataka bila bi znatno veća). Ali gornje dve tabele su ustvari dve relacije: PROFESORI je binarna relacija* $\rho \subseteq K \times P$*, a STUDENTI ternarna relacija* $\sigma \subseteq S \times K \times A$*. Elementi prve od njih su uređeni parovi (npr.* $(Analiza, Todorovic), (TOI, Sobot), \ldots$*) a elementi druge uređene trojke (npr.* $(Petar, Analiza, Brankovic), (Petar, TOI, Vukovic), \ldots$*).*

Za rad s bazama podataka konstruisani su specijalizovani jezici, kao što je SQL (Structured Query Language). Oni omogućavaju pretraživanje po bazi i izdvajanje željenih podataka. To se vrši postavljanjem upita (query (eng.) = upit).

Recimo da želimo da dobijemo spisak svih kurseva u bazi podataka. To bismo pomoću SQL-a dobili upitom

```
SELECT K FROM PROFESORI
```

Prethodni upis u potpunosti odgovara operaciji prve projekcije: iz relacije ρ izdvajamo skup svih prvih koordinata.

Ako sada želimo da saznamo koje sve kurseve i kod kojeg asistenta sluša student $Petar$, to bismo pomoću SQL-a dobili upitom

```
SELECT K,A FROM STUDENTI
WHERE S=Petar
```

Primetimo da ovakvi upiti imaju dosta sličnosti sa predikatskim formulama kojima bismo izdvajali odgovarajući skup uređenih parova predmeta i asistenata: $\{(k, a) : (Petar, k, a) \in \rho\}$.

Moguće je i kombinovati podatke iz više tabela. Ako, na primer, želimo spisak svih profesora i asistenata kod kojih *Petar* sluša kurseve, to možemo dobiti ovakvim upitom:

```
SELECT P,A FROM PROFESORI,STUDENTI
WHERE S=Petar
```

Ovakvo ,,spajanje" tabela je veoma slično kompoziciji relacija, pa bismo traženi skup mogli ovako definisati: $\{(p, a) : (\exists k)((Petar, k, a) \in \rho \wedge (k, p) \in \sigma)\}$.

4.8 Specijalne binarne relacije

Definicija 4.38 *Binarna relacija ρ na skupu A je:*

- *refleksivna ako* $(\forall x)(x, x) \in \rho$;
- *irefleksivna ako* $(\forall x)\neg(x, x) \in \rho$;
- *simetrična ako* $(\forall x)(\forall y)((x, y) \in \rho \Rightarrow (y, x) \in \rho)$;
- *antisimetrična ako* $(\forall x)(\forall y)((x, y) \in \rho \wedge (y, x) \in \rho \Rightarrow x = y)$;
- *tranzitivna ako* $(\forall x)(\forall y)(\forall z)((x, y) \in \rho \wedge (y, z) \in \rho \Rightarrow (x, z) \in \rho)$.

Primer 4.39 *(1) Jedan primer refleksivne relacije na skupu $A = \{a, b, c\}$ je relacija ρ data tablicom*

ρ	a	b	c
a	$\top$	$\bot$	$\bot$
b	$\top$	$\top$	$\bot$
c	$\top$	$\bot$	$\top$

Možemo primetiti da, ako je relacija zadata tablicom, refleksivnost je lako proveriti: ona znači da se na celoj glavnoj dijagonali tablice (onoj koja ide od gornjeg levog do donjeg desnog ugla) nalaze simboli $\top$. Još neki primeri refleksivnih relacija: $=$, $\leq$, $\geq$ (na bilo kom skupu na kojem ove relacije imaju smisla).

(2) Primer irefleksivne relacije na istom skupu A je relacija σ data tablicom

σ	a	b	c
a	$\bot$	$\bot$	$\top$
b	$\top$	$\bot$	$\bot$
c	$\top$	$\bot$	$\bot$

Irefleksivnost je jednako lako proveriti: ona znači da se na celoj glavnoj dijagonali nalaze simboli $\bot$. Još neki primeri irefleksivnih relacija: $<$, $>$.

(3) Jedna simetrična relacija na A je relacija τ data tablicom

τ	a	b	c
a	$\top$	$\top$	$\top$
b	$\top$	$\bot$	$\bot$
c	$\top$	$\bot$	$\bot$

I simetričnost se na lak način proverava preko tablice: ona važi ako i samo ako se na svaka dva polja tablice koja su simetrična u odnosu na glavnu dijagonalu nalaze isti simboli; recimo vidimo da $(a, b) \in \tau$, pa mora biti i $(b, a) \in \tau$. To je i razlog zbog kojeg se ova osobina naziva simetričnost. Još neki primeri simetričnih relacija: $=$, $\perp$ (normalnost pravih u geometriji).

(4) Evo i jedne antisimetrične relacije:

θ	a	b	c
a	$\top$	$\perp$	$\top$
b	$\top$	$\top$	$\perp$
c	$\perp$	$\perp$	$\perp$

Kako je $(\forall x)(\forall y)((x, y) \in \rho \wedge (y, x) \in \rho \Rightarrow x = y) \sim (\forall x)(\forall y)(x \neq y \Rightarrow \neg((x, y) \in \rho \wedge (y, x) \in \rho))$, antisimetričnost je ispunjena ako i samo ako se ni na koja dva polja tablice van glavne dijagonale koja su simetrična u odnosu na tu dijagonalu ne nalaze simboli $\top$; recimo vidimo da $(b, a) \in \theta$, pa ne sme biti i $(a, b) \in \theta$. Još neki primeri antisimetričnih relacija: $=$, $\leq$, $\geq$, $<$, $>$.

(5) Tranzitivnost se, nažalost, ne može na lak način proveriti iz tablice. Neki primeri tranzitivnih relacija su: $=$, $\leq$, $\geq$, $<$ i $>$.

Primetimo da uslov za antisimetričnost nije negacija uslova za simetričnost. Dakle, ako relacija nije simetrična to ne znači da je antisimetrična. Recimo, relacija σ iz dela (2) prethodnog primera nije ni simetrična (jer $b\sigma a$ ali ne i $a\sigma b$) ni antisimetrična (jer $a\sigma c$ i $c\sigma a$ ali $a \neq c$). Slično, ni irefleksivnost nije negacija refleksivnosti: relacija θ iz gornjeg primera nije ni refleksivna ni irefleksivna.

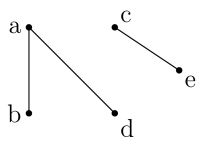
Definicija 4.40 *Graf je uređeni par (V, E), gde je $E \subseteq \{\{u, v\} : u, v \in V \wedge u \neq v\}$ (ova struktura se često naziva i prost graf). Elemente skupa V zovemo čvorovi, a elemente skupa E grane.*

Razlika između grafova i digrafova (definicija 4.27) je u tome što grane grafova nisu orijentisane: one su neuređeni parovi. Stoga su grafovi pogodni za predstavljanje simetričnih relacija. Pri zapisu grana se obično umesto $(x, y) \in E$ i $(y, x) \in E$ (kao kod orijentisanih grafova) pišemo samo $\{x, y\} \in E$ ili još kraće $xy \in E$; zbog simetričnosti redosled navođenja čvorova jedne grani nije bitan.

Grafovima obično predstavljamo veze između nekih objekata. Npr. čvorovi mogu biti osobe, a grane poznanstva između njih; tu važi simetričnost: ako jedna osoba poznaje drugu onda i druga poznaje prvu. Drugi primer: čvorovi mogu biti gradovi a grane direktni putevi između njih.

Relacije koje se predstavljaju grafovima su obično refleksivne ili irefleksivne; i u slučaju refleksivnosti često se grane koje spajaju čvorove s njima samima radi jednostavnijeg crteža ne prikazuju.

Primer 4.41 *Neka je $V = \{a, b, c, d, e\}$ neki skup osoba, pri čemu a poznaje b i d, c poznaje e, a ostale osobe se međusobno ne poznaju. Kako je poznanstvo simetrična relacija, odgovarajući skup grana je $\{ab, ad, ce\}$, i graf (V, E) može se predstaviti kao na slici.*



Iskoristimo ovaj primer da još jednom ukažemo na značaj redosleda kvantifikatora u predikatskim formulama. Formula

$$F_1 = (\forall x)(\exists y)P(x, y),$$

recimo, za ovaj graf tvrdi da iz svakog čvora izlazi bar po jedna grana, što je očigledno tačno. S druge strane, formula

$$F_2 = (\exists y)(\forall x)P(x, y)$$

tvrdi za postoji čvor spojen granama sa svim čvorovima, što nije tačno.

Za svaku od osobina iz definicije 4.38 daćemo još po jedan ekvivalentan uslov. Nakon toga ćemo u daljim dokazivanjima koristiti paralelno definicije ili ove ekvivalentne uslove, u zavisnosti od toga šta nam je pogodnije.

Teorema 4.42 *Neka je ρ binarna relacija na skupu A.*

(a) ρ je refleksivna ako i samo ako je $\triangle_A \subseteq \rho$.

(b) ρ je irefleksivna ako i samo ako je $\rho \cap \triangle_A = \emptyset$.

(c) ρ je simetrična ako i samo ako je $\rho^{-1} \subseteq \rho$ ako i samo ako je $\rho^{-1} = \rho$.

(d) ρ je antisimetrična ako i samo ako je $\rho \cap \rho^{-1} \subseteq \triangle_A$.

(e) ρ je tranzitivna ako i samo ako je $\rho \circ \rho \subseteq \rho$.

Dokaz. (a) Uslov $\triangle_A \subseteq \rho$ znači da svaki uređeni par koji je u relaciji $\triangle_A$ pripada i relaciji ρ. Ali $\triangle_A$ sadrži upravo parove oblika (x, x) za $x \in A$ pa taj uslov kaže da svi takvi parovi moraju biti u ρ, tj. da je ρ refleksivna.

(b) Uslov $\rho \cap \triangle_A = \emptyset$ znači da nijedan uređeni par ne sme pripadati i relaciji $\triangle_A$ i relaciji ρ. Drugim rečima, parovi oblika (x, x) za $x \in A$ ne smeju pripadati relaciji ρ, a to je irefleksivnost.

(c)
$$\begin{aligned} \rho^{-1} \subseteq \rho &\sim (\forall x)(\forall y)((x, y) \in \rho^{-1} \Rightarrow (x, y) \in \rho) \\ &\sim (\forall x)(\forall y)((y, x) \in \rho \Rightarrow (x, y) \in \rho), \end{aligned}$$

a to je baš uslov simetričnosti. Uz to, ako važi $\rho^{-1} \subseteq \rho$, prema teoremi 4.34(a) je i $(\rho^{-1})^{-1} \subseteq \rho^{-1}$ odnosno, po teoremi 4.31(a), $\rho \subseteq \rho^{-1}$, što nam daje $\rho^{-1} = \rho$.

(d)

$$\begin{aligned} \rho \cap \rho^{-1} \subseteq \triangle_A &\sim (\forall x)(\forall y)((x, y) \in \rho \cap \rho^{-1} \Rightarrow (x, y) \in \triangle_A) \\ &\sim (\forall x)(\forall y)((x, y) \in \rho \wedge (x, y) \in \rho^{-1} \Rightarrow (x, y) \in \triangle_A) \\ &\sim (\forall x)(\forall y)((x, y) \in \rho \wedge (y, x) \in \rho \Rightarrow x = y), \end{aligned}$$

što je baš uslov antisimetričnosti.

(e) ($\Rightarrow$) Pretpostavimo prvo da je ρ tranzitivna. Ako $(x, y) \in \rho \circ \rho$, to znači da postoji z takvo da $(x, z) \in \rho$ i $(z, y) \in \rho$, pa zbog tranzitivnosti i $(x, y) \in \rho$.

($\Leftarrow$) Obratno, pretpostavimo da je $\rho \circ \rho \subseteq \rho$. Da bismo dokazali da je ρ tranzitivna, pretpostavimo da za neke x, y, z važi $(x, y) \in \rho$ i $(y, z) \in \rho$. To znači da $(x, z) \in \rho \circ \rho$, pa po pretpostavci i $(x, z) \in \rho$. $\square$

4.9 Relacije ekvivalencije

Osobine binarnih relacija o kojima je bilo reči u prethodnom odeljku dobijaju poseban značaj ako se kombinuju. Prva značajna kombinacija je sledeća.

Definicija 4.43 *Binarna relacija ρ je relacija ekvivalencije ako je refleksivna, simetrična i tranzitivna.*

Primer 4.44 *(1) Relacija jednakosti $\triangle_A$ na svakom skupu A je relacija ekvivalencije:*

R: za svako $x \in A$ važi $x = x$.

S: ako je $x = y$, onda je i $y = x$.

T: ako je $x = y$ i $y = z$, onda i $x = z$.

Ustvari, postoji veliki broj relacija izvedenih iz jednakosti koje u izvesnom smislu ,,preuzimaju" od nje ove tri osobine, pa su i same relacije ekvivalencije. Npr. relacije ,,imati istu boju očiju" ili ,,biti jednake visine" na skupu svih ljudi, ili ,,imati jednaku poslednju cifru" na skupu N. Čitaocu ostavljamo da sam proveri da su one relacije ekvivalencije.

(2) Za bilo koji skup A puna relacija A^2, koja se sastoji iz svih uređenih parova elemenata skupa A, je relacija ekvivalencije:

R: za svako $x \in A$ važi $(x, x) \in A^2$.

S: ako je $(x, y) \in A^2$, onda i $(y, x) \in A^2$.

T: ako je $(x, y) \in A^2$ i $(y, z) \in A^2$, onda i $(x, z) \in A^2$.

(I leve i desne strane implikacija kod simetričnosti i tranzitivnosti su tačne za sve elemente.)

(3) Relacija ρ na skupu $S = \{1, 2, 3, 4, 5, 6\}$ data je sa $\rho = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4), (5, 5), (5, 6), (6, 5), (6, 6)\}$. Nju možemo prikazati i tablicom:

ρ	1	2	3	4	5	6
1	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
2	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
3	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
4	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
5	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$
6	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$

Ona je relacija ekvivalencije. Zaista, refleksivnost važi jer $(1, 1), (2, 2), \ldots, (6, 6) \in \rho$. Simetričnost takođe: kako je $(1, 2) \in \rho$, treba proveriti da i $(2, 1) \in \rho$, i slično za sve ostale parove. Konačno, proveravamo i tranzitivnost: kako je $(1, 3) \in \rho$ i $(3, 2) \in \rho$, treba proveriti $(1, 2) \in \rho$, i slično za ostale parove.

(4) Neka je A bilo koji skup. Na skupu $P(A)$ svih njegovih podskupova relacija jednakosti skupova je relacija ekvivalencije prema teoremi 4.3.

(5) Neka je F skup svih iskaznih formula. Relacija ekvivalentnosti formula $\sim$ na skupu F je relacija ekvivalencije prema teoremi 2.24. Slično tome, može se pokazati da je i relacija ekvivalentnosti $\sim$ na skupu predikatskih formula relacija ekvivalencije.

Teorema 4.45 *Neka je ρ binarna relacija na skupu A. Sledeći uslovi su ekvivalentni:*

(a) ρ je relacija ekvivalencije;

(b) $\triangle_A \subseteq \rho$, $\rho^{-1} \subseteq \rho$ i $\rho \circ \rho \subseteq \rho$;

(c) $\triangle_A \subseteq \rho$, $\rho^{-1} = \rho$ i $\rho \circ \rho = \rho$.

Dokaz. (a)⇔(b) Prema teoremi 4.42 refleksivnost je ekvivalentna sa $\triangle_A \subseteq \rho$, simetričnost sa $\rho^{-1} \subseteq \rho$ a tranzitivnost sa $\rho \circ \rho \subseteq \rho$.

(c)⇒(b) Ovo sledi direktno, jer je jednakost skupova ,,jača" od podskupa.

(b)⇒(c) Iz teoreme 4.42 imamo da iz $\rho^{-1} \subseteq \rho$ sledi $\rho^{-1} = \rho$, pa treba samo još dokazati $\rho \circ \rho = \rho$. Kako nam je već dato $\rho \circ \rho \subseteq \rho$, treba još pokazati $\rho \subseteq \rho \circ \rho$. Iz teoreme 4.31 imamo $\rho = \rho \circ \triangle_A$ a iz teoreme 4.34, pošto je $\triangle_A \subseteq \rho$, sledi $\rho \circ \triangle_A \subseteq \rho \circ \rho$. Konačno, $\rho \subseteq \rho \circ \rho$. □

Prethodna teorema daje dve kombinacije uslova ekvivalentne sa (a); pritom (b) sadrži naizgled slabije a (c) jače uslove. To znači da, kada dokazujemo da je ρ relacija ekvivalencije, dovoljno je dokazati uslove iz (b), a kada već znamo da je ρ relacija ekvivalencije i treba to da iskoristimo, možemo primenjivati i uslove iz (c).

Definicija 4.46 *Neka je ρ relacija ekvivalencije na skupu S. Klasa ekvivalencije elementa $x \in S$ je*

$$[x]_\rho = \{s \in S : x \rho s\}.$$

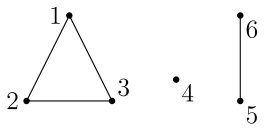
(Ona se nekad obeležava i sa x/ρ. Ako je jasno o kojoj relaciji ρ je reč, možemo pisati samo $[x]$.) Skup svih klasa ekvivalencije

$$S/\rho = \{[x]_\rho : x \in S\}$$

naziva se količnički skup (ili faktor skup).

Dakle, u istoj klasi ekvivalencije se nalaze elementi koji su međusobno u relaciji.

Primer 4.47 *(1) Navedimo klase ekvivalencije relacije ρ iz tačke (3) prethodnog primera: $[1] = [2] = [3] = \{1, 2, 3\}$, $[4] = \{4\}$ i $[5] = \{5, 6\}$. Podela na klase najbolje se vidi s grafa:*



Količnički skup je $S/\rho = \{[1], [4], [5]\}$. Kako je $[1] = [2]$, taj skup ne pišemo više puta, već izaberemo ,,predstavnika" tj. jedan element tog skupa, u ovom slučaju 1.

(2) Za relaciju $\triangle_A$ na skupu $A = \{1, 2, 3, 4\}$ klase ekvivalencije su: $[1] = \{1\}$, $[2] = \{2\}$, $[3] = \{3\}$ i $[4] = \{4\}$, a količnički skup $A/\triangle_A = \{[1], [2], [3], [4]\}$.

(3) Za relaciju A^2 na skupu $A = \{1, 2, 3, 4\}$ svi elementi su u istoj klasi ekvivalencije: $[1] = [2] = [3] = [4] = \{1, 2, 3, 4\}$, a količnički skup je $A/A^2 = \{[1]\}$.

(4) Za relaciju $\sim$ ekvivalentnosti iskaznih formula svaku klasu čine međusobno ekvivalentne formule. Npr. jednu klasu čine sve tautologije, drugu sve kontradikcije, treću formule p, $p \wedge p$, $p \vee (p \wedge q) \ldots$ Tih klasa ima beskonačno mnogo, jer broj iskaznih slova u formulama može biti proizvoljno veliki. Dakle, u zadacima tipa ,,konstruisati sve (do na ekvivalenciju) iskazne formule takve da..." mi smo, ustvari, iz svake klase ekvivalencije birali po jednu formulu–predstavnika.

Teorema 4.48 *Neka je ρ relacija ekvivalencije na skupu S.*

(a) Ako je $x \rho y$, onda $[x]_\rho = [y]_\rho$;

(b) inače, $[x]_\rho \cap [y]_\rho = \emptyset$.

Dokaz. (a) Neka je $x \rho y$. Dokažimo $[x]_\rho \subseteq [y]_\rho$, a obratna inkluzija $[y]_\rho \subseteq [x]_\rho$ se dokazuje analogno.

Neka $s \in [x]_\rho$. To znači da $x \rho s$. Iz $x \rho y$ sledi $y \rho x$ zbog simetričnosti, a odatle i iz $x \rho s$ dalje sledi $y \rho s$ iz tranzitivnosti. Dakle, $s \in [y]_\rho$.

(b) Pretpostavimo suprotno, da nije $x \rho y$ ali je $[x]_\rho \cap [y]_\rho \neq \emptyset$. To znači da postoji $s \in [x]_\rho \cap [y]_\rho$, dakle $x \rho s$ i $y \rho s$. Iz simetričnosti dobijamo $s \rho y$, a iz tranzitivnosti $x \rho y$, što je u suprotnosti s pretpostavkom. Dakle, mora biti $[x]_\rho \cap [y]_\rho = \emptyset$. □

Glavni razlog zbog kojeg su relacije ekvivalencije bitne je upravo način na koji one dele skup S na klase ekvivalencije: te klase se ili poklapaju ili su disjunktne, i zajedno čine ceo skup S. Takve podele skupova na podskupove zvaćemo *particije*. Mi ćemo, jednostavnosti radi, definisati samo konačne particije (tj. podele na konačno mnogo podskupova), ali treba naglasiti da naredna teorema važi (praktično s istim dokazom) i u slučaju beskonačnih particija.

Definicija 4.49 *Familija $F = \{A_1, A_2, \ldots, A_n\} \subseteq P(S) \setminus \{\emptyset\}$ je konačna particija skupa S ako:*
(1) $A_1 \cup A_2 \cup \ldots \cup A_n = S$;
(2) ako $A_i \neq A_j$ onda je $A_i \cap A_j = \emptyset$.

Teorema 4.50 (O reprezentaciji) *(a) Ako je ρ relacija ekvivalencije sa konačno mnogo klasa na skupu S, onda je S/ρ konačna particija skupa S.*
(b) Ako je $\{A_1, A_2, \ldots, A_n\}$ konačna particija skupa S i definišemo relaciju

$$x \rho y \Leftrightarrow (\exists i)(x \in A_i \wedge y \in A_i), \tag{4.1}$$

onda je ρ relacija ekvivalencije i njene klase ekvivalencije su skupovi $A_1, A_2, \ldots, A_n$.

Dokaz. (a) Za početak, sve klase ekvivalencije su neprazni skupovi, jer svakoj klasi $[x]_\rho$ pripada bar jedan element, x. Dokažimo da su ispunjeni uslovi (1) i (2) definicije 4.49.

(1) Kako je $[x]_\rho \subseteq S$ za svaku klasu S, imamo da je i unija svih klasa podskup skupa S (po teoremi 4.13(a)). Obratno, ako $x \in S$, onda $x \in [x]_\rho$, pa svaki element iz S pripada i uniji klasa ekvivalencije relacije ρ.

(2) Prema teoremi 4.48 različite klase ekvivalencije moraju biti disjunktne.

(b) Dokazujemo prvo da je ρ relacija ekvivalencije.

R: Za svako $x \in S$ zbog uslova (1) imamo da postoji i takvo da $x \in A_i$, pa je $x\rho x$.

S:
$$\begin{aligned} x\rho y &\sim (\exists i)(x \in A_i \wedge y \in A_i) \\ &\sim (\exists i)(y \in A_i \wedge x \in A_i) \\ &\sim y\rho x. \end{aligned}$$

T: $x\rho y$ znači da postoji i takvo da $x, y \in A_i$, a $y\rho z$ da postoji j takvo da $y, z \in A_j$. Međutim, kako $y \in A_i$ i $y \in A_j$ dobijamo da $A_i \cap A_j \neq \emptyset$, što po uslovu (2) znači da je $A_i = A_j$. Dakle, postoji i takvo da $x, z \in A_i$, pa $x\rho z$.

Ostaje da dokažemo da, ako $x \in A_i$, onda je $[x]_\rho = A_i$.

($\subseteq$) Ako $s \in [x]_\rho$, to znači da $x\rho s$, tj. s pripada istom skupu particije kao i x: $s \in A_i$.

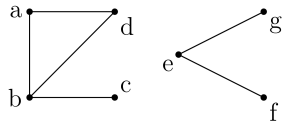
($\supseteq$) Ako $s \in A_i$, onda po definiciji relacije ρ imamo $x\rho s$, odnosno $s \in [x]_\rho$.□

Dakle, svakoj relaciji ekvivalencije na skupu S odgovara neka particija skupa S i obratno: iz svake particije možemo „rekonstruisati" odgovarajuću relaciju ekvivalencije. U prethodnom primeru već smo videli kako od relacije ekvivalencije dobijamo odgovarajuću particiju, npr. za relaciju ρ iz tačke (1) dobili smo particiju $\{\{1,2,3\},\{4\},\{5,6\}\}$. Naredni primer ilustruje deo (b) prethodne teoreme.

Primer 4.51 *Neka je data particija* $\{\{1\},\{3\},\{2,4,5\}\}$ *skupa* $\{1,2,3,4,5\}$. *Prateći definiciju (4.1) popunjavamo tablicu za odgovarajuću relaciju ekvivalencije:*

ρ	1	2	3	4	5
1	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
2	$\bot$	$\top$	$\bot$	$\top$	$\top$
3	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
4	$\bot$	$\top$	$\bot$	$\top$	$\top$
5	$\bot$	$\top$	$\bot$	$\top$	$\top$

Primer 4.52 *Neka je* (V, E) *graf takav da* $V = \{a, b, c, d, e, f, g\}$ *i* $E = \{ab, ad, bc, bd, ef, eg\}$*:*



Šetnja u grafu je niz čvorova u kojem su susedni čvorovi spojeni granama, npr. bad *je jedna šetnja u datom grafu. Definišimo na skupu* V *relaciju:* $x\sigma y$ *ako i samo ako je* $x = y$ *ili postoji šetnja od* x *do* y*. Iz definicije je jasno da je ona refleksivna. Ako postoji šetnja od* x *do* y*, onda postoji i šetnja od* y *do* x *(koja prolazi istim granama), pa je* σ *simetrična. Ako postoje šetnje od* x *od* y *i od* y *do* z*, njihovim spajanjem dobijamo šetnju od* x *do* z *pa je* σ *i tranzitivna.*

Dakle, σ *je relacija ekvivalencije. Njene klase ekvivalencije su tzv. komponente povezanosti grafa; u našem primeru to su* $C_1 = \{a, b, c, d\}$ *i* $C_2 = \{e, f, g\}$*. Dakle,* $\{C_1, C_2\}$ *je particija koja odgovara relaciji* σ*.*

Pretpostavimo sada da je V *neki skup osoba, a* E *skup prijateljstava među njima (dakle,* $xy \in E$ *znači da su osobe* x *i* y *prijatelji). Ako saopštimo neku informaciju jednoj od tih osoba* x *i pretpostavimo da će svaka osoba koja sazna informaciju nju preneti svojim prijateljima, koje osobe će saznati tu informaciju? Upravo one koje su u istoj komponenti povezanosti pomenute particije kao* x*.*

4.10 Relacije poretka

Definicija 4.53 *Binarna relacija ρ je relacija poretka ako je refleksivna, antisimetrična i tranzitivna. Ako je ρ relacija poretka na skupu A, par (A, ρ) naziva se parcijalno uređenje.*

Dakle, prema terminologiji prethodne glave, parcijalno uređenje je model za formule koje definišu refleksivnost, antisimetričnost i tranzitivnost (definicija 4.8).

Kao što im i ime kaže, relacije poretka uspostavljaju neki poredak na skupu na kojem su definisane.

Primer 4.54 *(1) Najpoznatiji primeri relacija poretka su $\leq$ i $\geq$ (na bilo kom od skupova N, Z, Q, R). Proverimo to npr. za relaciju $\leq_R$:*

R: za svako $x \in R$ je $x \leq x$;

AS: ako je $x \leq y$ i $y \leq x$, onda mora biti $x = y$;

T: ako je $x \leq y$ i $y \leq z$, onda je i $x \leq z$.

(2) Ako je A proizvoljan skup, relacija $\subseteq$ na skupu $P(A)$ je relacija poretka, što je dokazano u teoremi 4.8.

(3) Relacija deljivosti $|$ na skupu N je relacija poretka. Proverimo to:

R: Za svaki $x \in N$ je $x \mid x$, jer $x = 1 \cdot x$.

AS: Ako $x \mid y$ i $y \mid x$, to znači da je $x \leq y$ i $y \leq x$, pa je $x = y$.

T: Ako $x \mid y$ i $y \mid z$, onda je, po definiciji deljivosti, $y = kx$ i $z = ly$ za neke cele brojeve k i l, pa je $z = klx$, tj. $x \mid z$.

Primetimo da relacija deljivosti na skupu Z nije relacija poretka. Zaista, ona nije antisimetrična: $2 \mid -2$ i $-2 \mid 2$, ali $2 \neq -2$.

Dakle, $(N, \leq_N)$, $(R, \geq_R)$, $(P(A), \subseteq)$ i $(N, |)$ su primeri parcijalnih uređenja.

Definicija 4.55 *Binarna relacija ρ je relacija strogog poretka ako je irefleksivna, antisimetrična i tranzitivna.*

Teorema 4.56 *Ako je ρ irefleksivna i tranzitivna, ona je i antisimetrična.*

Dokaz. Neka važi $x\rho y$ i $y\rho x$. Iz tranzitivnosti sledi $x\rho x$, što je nemoguće zbog irefleksivnosti. Dakle, ni za koja dva elementa ne može važiti $x\rho y$ i $y\rho x$, pa je antisimetričnost trivijalno ispunjena. □

Prethodna teorema dozvoljava nam da prilikom provere da li je neka relacija relacija strogog poretka ispitamo samo irefleksivnost i tranzitivnost.

Primer 4.57 *(1) Najpoznatiji primeri relacija strogog poretka su $<$ i $>$ (na bilo kom od skupova N, Z, Q, R). I to je jednostavno proveriti (recimo za $<_R$):*

IR: ni za jedno $x \in R$ nije $x < x$;

T: ako je $x < y$ i $y < z$, onda je i $x < z$.

(2) Ako je A proizvoljan skup, relacija $\subset$ na skupu $P(A)$ je relacija strogog poretka. Njena irefleksivnost je očigledna, a tranzitivnost (ustvari njen nešto jači oblik) će biti dokazana u zadatku 12.

(3) Relacija data sa

$$P(x, y) \Leftrightarrow x \text{ je potomak osobe } y$$

na skupu svih osoba je relacija poretka. Proverimo to:

IR: Nijedna osoba nije sama sebi potomak.

T: Ako je x potomak osobe y a y potomak osobe z onda je, jasno, i x potomak osobe z.

(4) ASCII kod je tabela koja skupu znakova tastature (proširenom za još neke korisne znakove) pridružuje redne brojeve od 0 *do* 127 *(ili, u slučaju proširenog koda, od* 0 *do* 255*). Na taj način se na skupu tih znakova uvodi jedna relacija strogog poretka: $x < y$ ako i samo ako je redni broj znaka x u ASCII kodu manji od rednog broja znaka y. Npr. redni broj slova* `'A'` *je* 65 *a slova* `'B'` - 66*, pa je* `'A'<'B'`*. Uopšte, velika slova imaju uzastopne redne brojeve i to po abecednom redu; ista je situacija i s malim slovima i ciframa. Ova relacija je uključena u većinu programskih jezika i omogućuje laku proveru da li je neki znak* `x` *slovo pomoću izraza*

```
('A'<=x && x<='Z') || ('a'<=x && x<='z').
```

Sledeće dve teoreme slične su teoremi 4.45, pa su i dokazi slični. Navodimo samo delove dokaza koji se razlikuju, a detalje ostavljamo čitaocu.

Teorema 4.58 *Neka je ρ binarna relacija na skupu A. Sledeći uslovi su ekvivalentni:*

(a) ρ je relacija poretka.

(b) $\triangle_A \subseteq \rho$, $\rho \cap \rho^{-1} \subseteq \triangle_A$ i $\rho \circ \rho \subseteq \rho$.

(c) $\triangle_A \subseteq \rho$, $\rho \cap \rho^{-1} = \triangle_A$ i $\rho \circ \rho = \rho$.

Dokaz. Jedino što treba dokazati je implikacija (b)⇒(c), preciznije da važi $\rho \cap \rho^{-1} = \triangle_A$. Kako je $\rho \cap \rho^{-1} \subseteq \triangle_A$ već dato u (b), treba pokazati drugu inkluziju. Ali imamo da je $\triangle_A \subseteq \rho$ pa samim tim i $\triangle_A^{-1} \subseteq \rho^{-1}$ (teorema 4.34(a)). Kako je $\triangle_A^{-1} = \triangle_A$, to znači da je $\triangle_A \subseteq \rho \cap \rho^{-1}$ (prema teoremi 4.13(b)). □

Teorema 4.59 *Neka je ρ binarna relacija na skupu A. Sledeći uslovi su ekvivalentni:*

(a) ρ je relacija strogog poretka.

(b) $\triangle_A \cap \rho = \emptyset$ i $\rho \circ \rho \subseteq \rho$.

(c) $\triangle_A \cap \rho = \emptyset$, $\rho \cap \rho^{-1} = \emptyset$ i $\rho \circ \rho \subseteq \rho$.

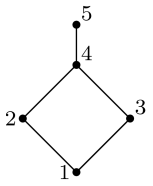
Dokaz. Ponovo treba dokazati samo deo (b)⇒(c), preciznije da je $\rho \cap \rho^{-1} = \emptyset$. Međutim, iz teoreme 4.56 znamo da iz irefleksivnosti i tranzitivnosti sledi antisimetričnost, odnosno $\rho \cap \rho^{-1} \subseteq \triangle_A$. Ali to znači da $\rho \cap \rho^{-1} = \rho \cap \rho^{-1} \cap \triangle_A = \emptyset$ jer je već $\triangle_A \cap \rho = \emptyset$. □

Jedna zgodna osobina relacija poretka (i relacija strogog poretka) na bilo kom skupu A je to što se one mogu predstavljati grafički, tzv. *Haseovim dijagramima*. Na takvom dijagramu elementi skupa A predstavljaju se tačkama od kojih su neke povezane linijama. Dva različita elementa $x, y \in A$ su u relaciji ako i samo ako se od x do y može doći krećući se po linijama isključivo od dole nagore.

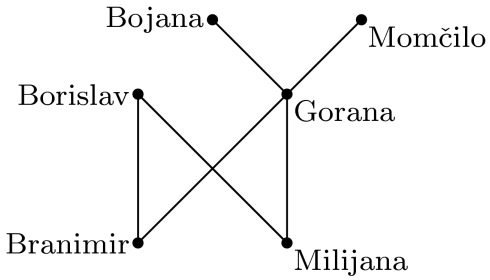
Primer 4.60 *(1) Neka je* $\rho = \{(1,1),(1,2),(1,3),(1,4),(1,5),(2,2),(2,4),(2,5),(3,3),(3,4),(3,5),(4,4),(4,5),(5,5)\}$ *relacija na skupu* $\{1,2,3,4,5\}$. *Pogodnije je ovu relaciju predstaviti tablicom:*

ρ	1	2	3	4	5
1	$\top$	$\top$	$\top$	$\top$	$\top$
2	$\bot$	$\top$	$\bot$	$\top$	$\top$
3	$\bot$	$\bot$	$\top$	$\top$	$\top$
4	$\bot$	$\bot$	$\bot$	$\top$	$\top$
5	$\bot$	$\bot$	$\bot$	$\bot$	$\top$

Iz tablice lako proveravamo da je ρ *refleksivna i antisimetrična, a takođe je i tranzitivna. Ona se dijagramom predstavlja na sledeći način:*

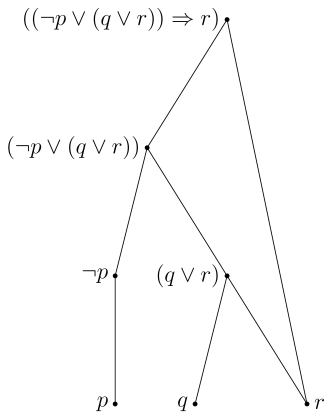


(2) Neka je P *relacija iz dela (3) prethodnog primera, ali samo na skupu* {*Bojana, Branimir, Borislav, Gorana, Milijana, Momčilo*}, *i neka su uz to Branimir i Milijana deca Borislava i Gorane, a Gorana dete Bojane i Momčila. Tada je (ako skratimo imena na Boj,Br,Bor,G,Mi,Mo)* $P = \{(Br,Bor),\ (Br,G),(Br,Boj),(Br,Mo),(Mi,Bor),(Mi,G),(Mi,Boj),(Mi,Mo),(G,Boj),(G,Mo)\}$, *što na dijagramu izgleda ovako:*



Dijagram ove relacije obično se naziva genealoško stablo.

(3) Na skupu iskaznih (ili predikatskih) formula možemo definisati relaciju: $F\rho G$ *ako je* F *podformula formule* G. *To je jedna relacija poretka. Ako umesto skupa svih formula posmatramo samo podformule neke fiksirane formule* H, *Haseov dijagram te relacije je vrlo sličan drvetu podformula; jedina razlika je u tome što, ako se ista podformula pojavljuje više puta u* H, *u drvetu podformula je crtamo više puta a na dijagramu samo jednom. Recimo, za poslednju formulu iz primera 2.4 dijagram bi izgledao ovako:*



Definicija 4.61 *Neka je (A, ρ) parcijalno uređenje. Element $a \in A$ naziva se:*

- *najveći ako* $(\forall x \in A) x \rho a$;
- *najmanji ako* $(\forall x \in A) a \rho x$;
- *maksimalan ako* $(\forall x \in A)(x \neq a \Rightarrow \neg a \rho x)$;
- *minimalan ako* $(\forall x \in A)(x \neq a \Rightarrow \neg x \rho a)$.

Iako su u svakodnevnom govoru to sinonimi, u matematici razlikujemo pojmove najvećeg i maksimalnog elementa. Najveći element je ujedno i maksimalan, ali obratno ne mora da važi. U delu (1) primera 4.60 element 1 je najmanji a 5 najveći. U delu (2) istog primera Branimir i Milijana su minimalni, ali ne i najmanji elementi: ispod njih nema drugih elemenata ali nijedan od njih nije potomak svih ostalih. Bojana, Borislav i Momčilo su maksimalni ali nijedan od njih nije najveći.

Naziv *parcijalno uređenje* koristi se da bi se naglasilo da mogu da postoje i elementi x i y koji nisu uporedivi, tj. takvi da ne važi ni $x \rho y$ ni $y \rho x$ (parcijalno znači delimično). Od posebnog su značaja uređenja u kojima nemamo takvih, neuporedivih, elemenata.

Definicija 4.62 *Parcijalno uređenje (A, ρ) naziva se linearno (totalno) uređenje (ili kraće: lanac) ako*

$$(\forall x, y \in A)(x \rho y \vee y \rho x). \tag{4.2}$$

Definicije analogne prethodnim dvema mogu se uvesti i za stroga uređenja; jedina razlika je u tome što zbog irefleksivnosti možemo tražiti samo da npr. najmanji element bude u relaciji sa svim ostalim (ne i sa samim sobom).

Primer 4.63 *(1) $(N, \leq)$ i $(R, \geq)$ su primeri linearnih uređenja. Zaista, za svaka dva realna broja x i y važi $x \geq y$ ili $y \geq x$. U uređenju $(N, \leq)$ element 1 je najmanji a maksimalnih elemenata nema. Nazivi iz definicije 4.61 prilagođeni su baš ovom uređenju. To može biti zbunjujuće: npr. u uređenju $(N, \geq)$ 1 je najveći element. U $(R, \leq)$ nema ni minimalnih ni maksimalnih elemenata.*

(2) Ako je $A = \{a, b, c\}$, $(P(A), \subseteq)$ nije linearno uređenje. Elementi $\{a\}$ i $\{b\}$ skupa $P(A)$ su neuporedivi: niti je $\{a\} \subseteq \{b\}$ niti $\{b\} \subseteq \{a\}$. Ovo uređenje ima i najmanji element ($\emptyset$) i najveći (A).

(3) $(N, |)$ *takođe nije linearno uređenje, jer ne važi ni* $2 \mid 3$ *ni* $3 \mid 2$. *I u njemu je* 1 *najmanji element, a maksimalnih nema.*

(4) Abecedni poredak na skupu svih slova abecede je jedno linearno uređenje. Iz njega se može izvesti i tzv. leksikografsko uređenje $\leq_{lex}$ *na skupu svih reči. To je uređenje koje se koristi u rečnicima i enciklopedijama: dve reči se porede tako što im se porede najpre prva slova, ako su ona jednaka porede se druga itd. Tako je npr.* $MATEMATIKA \leq_{lex} MATRICA$, *jer su prva tri slova jednaka, a* E *je ispred* R *u abecednom poretku.*

Linearna uređenja su posebno bitna u programiranju. Naime, jedan od bitnih problema je sortiranje datog skupa prema nekom linearnom uređenju i za to postoji mnoštvo različitih algoritama. Npr. ako sortiramo cele brojeve, koristimo poredak $\leq_Z$. Za sortiranje reči najčešće se koristi leksikografski poredak; koliko je on bitan postaje jasno ako se razmisli koliko bi trajalo traženje neke reči u rečniku ako u njemu reči ne bi bile sortirane.

Za sortiranje možemo koristiti i relaciju koja nije antisimetrična (već samo refleksivna i tranzitivna); naime, u slučaju kada i $x\rho y$ i $y\rho x$ svejedno je da li će prilikom sortiranja x biti postavljen ispred ili iza y.

Pomenimo i problem sortiranja parova (ili n-torki) elemenata po jednoj koordinati. Npr. ako nam je dat niz parova oblika $(osoba, visina)$ (recimo, kao struktura u Javi) i želimo da ih sortiramo po visini, tu je ustvari na snazi relacija opisana u narednoj teoremi.

Teorema 4.64 *Neka je* ρ *relacija poretka na skupu* A. *Ako na skupu* $A \times B$ *definišemo relaciju:*

$$(a_1, b_1)\sigma(a_2, b_2) \Leftrightarrow a_1 \rho a_2,$$

tada je ona refleksivna i tranzitivna. Ako ρ *zadovoljava uslov (4.2), onda i* σ *zadovoljava taj uslov.*

Dokaz. R: Za svaki par (a, b) važi $(a, b)\sigma(a, b)$ jer $a\rho a$.

T: Ako $(a_1, b_1)\sigma(a_2, b_2)$ i $(a_2, b_2)\sigma(a_3, b_3)$, to znači da $a_1\rho a_2$ i $a_2\rho a_3$, pa kako je ρ tranzitivna, imamo i $a_1\rho a_3$, dakle $(a_1, b_1)\sigma(a_3, b_3)$.

L: Ako su $(a_1, b_1), (a_2, b_2) \in A \times B$ i ρ je linearno uređenje, onda važi $a_1\rho a_2$ ili $a_2\rho a_1$. U prvom slučaju je $(a_1, b_1)\sigma(a_2, b_2)$, a u drugom $(a_2, b_2)\sigma(a_1, b_1)$. □

Drugi problem s kojim se programeri često susreću je pretraživanje elemenata linearno uređenog skupa. Naravno, postoje i slučajevi kada elementi skupa koji pretražujemo nisu linearno uređeni, što onda značajno komplikuje pretragu.

Primetimo da se relacije $\leq$ i $<$ (npr. na skupu N) razlikuju samo po tome da li su elementi u relaciji sa samima sobom: $\leq$ je refleksivna a $<$ irefleksivna relacija. Isti je slučaj i s relacijama $\subseteq$ i $\subset$. Naredna teorema pokazuje da je to opšte pravilo: relacije poretka i relacije strogog poretka uvek se javljaju u takvim parovima.

Teorema 4.65 *(a) Ako je* ρ *relacija strogog poretka na skupu* A, *onda je* $\rho \cup \triangle_A$ *relacija poretka na skupu* A.

(b) Ako je ρ *relacija poretka na skupu* A, *onda je* $\rho \setminus \triangle_A$ *relacija strogog poretka na skupu* A.

Dokaz. (a) Obeležimo $\sigma = \rho \cup \triangle_A$.

R: Očigledno $\triangle_A \subseteq \sigma$.

AS: Neka $(x,y) \in \sigma$ i $(y,x) \in \sigma$. Ako bar jedan od ovih parova pripada relaciji $\triangle_A$, to odmah znači da je $x = y$. U suprotnom, $(x,y) \in \rho$ i $(y,x) \in \rho$ pa, kako je ρ antisimetrična, opet $x = y$.

T: Neka $(x,y) \in \sigma$ i $(y,z) \in \sigma$. Posmatrajmo četiri slučaja:

1° $(x,y) \in \rho$ i $(y,z) \in \rho$. Tada, zbog tranzitivnosti ρ, i $(x,z) \in \rho$, dakle i $(x,z) \in \sigma$.

2° $(x,y) \in \rho$ i $(y,z) \in \triangle_A$. Tada je $y = z$, pa iz $(x,y) \in \rho$ opet imamo $(x,z) \in \rho$ pa i $(x,z) \in \sigma$.

3° $(x,y) \in \triangle_A$ i $(y,z) \in \rho$. Analogno slučaju 2°.

4° $(x,y) \in \triangle_A$ i $(y,z) \in \triangle_A$. To znači da je $x = y$ i $y = z$, pa $(x,z) \in \triangle_A$, odakle $(x,z) \in \sigma$.

(b) Obeležimo $\tau = \rho \setminus \triangle_A$.

IR: Očigledno $\triangle_A \cap \tau = \emptyset$.

T: Neka $(x,y) \in \tau$ i $(y,z) \in \tau$. To znači da $(x,y), (y,z) \in \rho$ ali $(x,y), (y,z) \notin \triangle_A$. Kako je ρ tranzitivna imamo $(x,z) \in \rho$. Treba još pokazati da $(x,z) \notin \triangle_A$. Ali u suprotnom $x = z$, pa zbog antisimetričnosti relacije ρ iz $(x,y), (y,x) \in \rho$ imali bismo $x = y$, što je nemoguće jer $(x,y) \notin \triangle_A$. □

U kakvom su odnosu relacije $\leq$ i $\geq$? One su jedna drugoj inverzne ($\leq^{-1}$ je relacija $\geq$). I ovo je opšte pravilo: inverzna relacija svake relacije poretka je i sama relacija poretka; isto važi i za relacije strogog poretka.

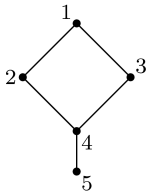
Teorema 4.66 *(a) Ako je ρ relacija poretka na skupu A, onda je i ρ^{-1} relacija poretka na skupu A.*

(b) Ako je ρ relacija strogog poretka na skupu A, onda je i ρ^{-1} relacija strogog poretka na skupu A.

Dokaz. (a) Ako je ρ refleksivna, antisimetrična i tranzitivna, isto važi i za ρ^{-1} prema zadacima 33, 36 i 37.

(b) Ako je ρ irefleksivna i tranzitivna, isto važi i za ρ^{-1} prema zadacima 34 i 37. □

Pritom, Haseov dijagram relacije ρ^{-1} dobija se okretanjem ,,naopačke" dijagrama relacije ρ; npr. dijagram relacije inverzne relaciji iz dela (1) primera 4.60 izgledao bi ovako:



4.11 Zatvorenja relacija

Ako neka binarna relacija nema neku od osobina refleksivnosti, simetričnosti ili tranzitivnosti, ponekad nam je korisno da znamo koje elemente moramo da joj dodamo da bi zadovoljavala tu osobinu. O tome govori sledeća definicija.

Definicija 4.67 *Neka je ρ binarna relacija na skupu A.*

Refleksivno zatvorenje relacije ρ je najmanja refleksivna relacija ρ_R takva da $\rho \subseteq \rho_R$.

Simetrično zatvorenje relacije ρ je najmanja simetrična relacija ρ_S takva da $\rho \subseteq \rho_S$.

Tranzitivno zatvorenje relacije ρ je najmanja tranzitivna relacija ρ_T takva da $\rho \subseteq \rho_T$.

Napomenimo da u gornjoj definiciji reč ,,najmanja" znači: najmanja u odnosu na poredak $\subseteq$ (ustvari, kad poredimo neke skupove, obično se i podrazumeva da ih poredimo relacijom $\subseteq$). Dakle, npr. za relaciju ρ_S se traži: (a) da $\rho \subseteq \rho_S$; (b) da bude simetrična i (c) da bude najmanja takva, tj. da za svaku simetričnu relaciju σ takvu da $\rho \subseteq \sigma$ važi $\rho_S \subseteq \sigma$.

Nije teško zaključiti da je, da bismo od ρ napravili refleksivnu relaciju, neophodno da joj dodamo sve parove oblika (x, x) za $x \in A$. Stoga je refleksivno zatvorenje relacije ρ: $\rho_R = \rho \cup \triangle_A$.

Primer 4.68 *(1) Refleksivno zatvorenje relacije $<_N$ je relacija $\leq_N$; primetimo da smo u teoremi 4.65(a) od relacije strogog poretka konstruisali relaciju poretka upravo tako što smo napravili njeno refleksivno zatvorenje.*

(2) Refleksivno zatvorenje relacije $\subset$ je relacija $\subseteq$.

(3) Ako je sama relacija ρ već refleksivna, njeno refleksivno zatvorenje je ona sama: ne treba joj ništa dodati da bi postala refleksivna. Npr. za relaciju $\triangle_A$ refleksivno zatvorenje je sama relacija $\triangle_A$. Isti zaključak važi i za simetrično i tranzitivno zatvorenje.

Konstruisanje simetričnog zatvorenja je takođe jednostavno: da bismo od ρ napravili simetričnu relaciju, neophodno da joj dodamo sve parove oblika (y, x) za $(x, y) \in \rho$. Drugim rečima, simetrično zatvorenje relacije ρ je $\rho_S = \rho \cup \rho^{-1}$.

Primer 4.69 *(1) Simetrično zatvorenje relacije $<_N$ je relacija $\neq_N$. Naime, ako je $x < y$ ili $y < x$, to ustvari znači da $x \neq y$.*

(2) Na skupu Z definišimo relaciju ρ: $x \rho y \Leftrightarrow x - y = 1$. Njeno simetrično zatvorenje tada je dato formulom $x \rho_S y \Leftrightarrow |x - y| = 1$.

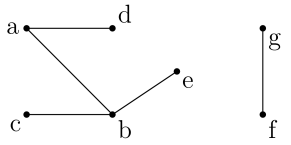
Konstrukcija tranzitivnog zatvorenja znatno je složenija. Pokažimo to na primeru: neka je data relacija $\rho = \{(1, 2), (2, 3), (3, 4)\}$ na skupu $\{1, 2, 3, 4\}$. Ona nije tranzitivna i da bismo je načinili takvom moramo joj, zbog parova $(1, 2)$ i $(2, 3)$ dodati i par $(1, 3)$, a zbog parova $(2, 3)$ i $(3, 4)$ i par $(2, 4)$. Međutim, dobijena relacija i dalje nije tranzitivna, jer sada zbog parova $(1, 3)$ i $(3, 4)$ moramo ubaciti i par $(1, 4)$.

Kao što vidimo, konstruisanje tranzitivnog zatvorenja mora se odvijati u nekoliko koraka. Definišimo $\rho_1 = \rho$ i $\rho_{n+1} = \rho_n \cup (\rho_n \circ \rho)$ za $n \in N$. Tranzitivno zatvorenje relacije ρ je tada

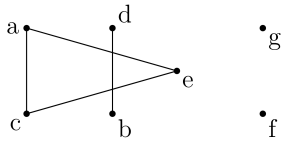
$$\rho_T = \bigcup_{n \in N} \rho_n. \tag{4.3}$$

U mnogim slučajevima (npr. uvek kada je ρ relacija na nekom konačnom skupu) opisani postupak se završava u konačno mnogo koraka; npr. ako je $\rho_3 = \rho_4$, ni u narednim koracima neće se dodavati više uređenih parova pa je ρ_3 traženo tranzitivno zatvorenje.

Primer 4.70 *(1) Neka graf (V, E) sadrži informacije o avio linijama između gradova neke države; dakle, čvorovi (elementi skupa V) su gradovi, a $uv \in E$ ako postoji direktna linija između gradova u i v. Radi jednostavnosti smatraćemo da je E refleksivna relacija (tj. da je svaki grad povezan sa samim sobom). Pitanje da li se može stići od u do v je pitanje da li $uv \in E_T$. Prikažimo ovo na konkretnom grafu: neka je $V = \{a, b, c, d, e, f, g\}$ i $E = \{ab, ad, bc, be, fg\}$ (podsetimo se, kod grafova pišemo ab umesto parova (a, b) i (b, a)).*

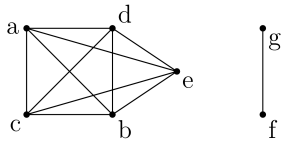


U prvom koraku na E dodajemo parove iz $E \circ E$ koji već nisu u E a to su ac, bd, ce i ae. Dobijena relacija $E_2 = E \cup (E \circ E)$ sadrži informacije o tome između kojih gradova se može stići sa najviše jednim presedanjem:



U sledećem koraku dodajemo i parove iz $E_3 = E_2 \circ E$: cd i de. Dobijena relacija prikazuje od kojeg do kojeg grada možemo stići uz najviše dva presedanja.

U trećem koraku trebalo bi dodati i parove iz $E_3 \circ E$ koji se već nisu javljali u E_3, ali takvih nema. To znači da smo stigli do tranzitivnog zatvorenja $E_T = E_3$:



(2) Ako na skupu svih ljudi $Q(x, y)$ znači: x je dete osobe y, onda $Q_T(x, y)$ znači: x je potomak osobe y. Dakle, tranzitivno zatvorenje relacije Q je relacija P iz tačke (3) primera 4.57.

4.12 Zadaci

Skupovi

1. Nabrojati elemente sledećih skupova:
   (a) $A = \{2n^2 + 3 : n \in \{1, 2, 3\}\}$;
   (b) $B = \{x^2 : x \in Z \wedge -3 \leq x \leq 2\}$;
   (c) $C = \{(n + 1) - n : n \in N\}$;
   (d) $D = Z \cap (1, 5]$.

2. Zapisati sledeće skupove formulama:
   (a) $A = \{-5, -4, -3, -2, -1, 0, 1, 2\}$;
   (b) $B = \{1, 3, 5, 7, 9, 11\}$;
   (c) $C = \{\sqrt{2} - 1, \sqrt{2}, \sqrt{2} + 1, \sqrt{2} + 2\}$.
3. Koliko elemenata ima skup:
   (a) $\{\{0, 1\}, \{1, 2\}\}$;
   (b) $\{\emptyset\}$;
   (c) $\{\emptyset, 1, \{2, 3\}\}$?
4. Da li je $A \subseteq B$, $B \subseteq A$ i $A = B$, ako:
   (a) $A = \{2n^2 + 3 : n \in N\}$, $B = \{4n^2 + 3 : n \in N\}$;
   (b) $A = \{6n - 1 : n \in N\}$, $B = \{n \in N : n$ je prost$\}$;
   (c) $A = \{n \in N : 2 \leq n \leq 9\}$, $B = \{n \in N : 3 < n^2 < 100\}$.
5. Dati su skupovi $A = \{4k : k \in N\}$ i $B = \{k^2 : k \in N \wedge 2 \mid k\}$.
   (a) Da li je $B \subseteq A$?
   (b) Da li je $A = B$?
6. Odrediti $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \triangle B$, $A \times B$ i $P(A)$ ako:
   (a) $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$;
   (b) $A = \{\{1\}, 2\}$, $B = \{1\}$.
7. Odrediti $A \cup B$, $A \cap B$ i $A \setminus B$ ako:
   (a) $A = \{2n : n \in N\}$, $B = \{3n : n \in N\}$;
   (b) $A = \{2n : n \in N\}$, $B = \{4n : n \in N\}$.
8. Dokazati da za svaki podskup A skupa X važi: (a) $A \cup \bar{A} = X$; (b) $A \cap \bar{A} = \emptyset$.
9. Dokazati:
   (a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$;
   (b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
10. Dokazati:
    (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
    (b) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
11. Dokazati:
    (a) $A = (A \cap B) \cup (A \setminus B)$;
    (b) $A \cup B = (A \cap B) \cup (A \triangle B)$.
12. Dokazati: ako je $A \subseteq B$ i $B \subset C$, onda je $A \subset C$.
13. Dokazati:
    (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

14. Dokazati da je, za proizvoljne skupove A, B i C, jedan od sledećih skupova podskup drugog:

    (a) $((A \cap B) \setminus C) \cup ((B \cap C) \setminus A)$ i $(A \cup C) \cap B$;

    (b) $(A \setminus (B \cup C)) \cup (B \setminus (A \cup C))$ i $(A \cup B) \setminus C$.

15. Neka su A i B disjunktni skupovi. Da li mora važiti i: (a) $P(A) \cap P(B) = \emptyset$; (b) $A^2 \cap B^2 = \emptyset$?

16. (a) Dokazati da za neprazne i različite skupove A i B važi $P(A) \cup P(B) \subseteq P(A \cup B)$.

    (b) Pokazati primerom da ne mora da važi jednakost.

Relacije

17. Ispisati elemente sledećih relacija:

    (a) $\rho = \{(x, y) \in N^2 : y \leq 6 \wedge x + 1 < y\}$;

    (b) $\sigma = \{(x, y) \in R^2 : x \in Z \cap [1, 3] \wedge x = y^2\}$;

    (c) $\tau = \{(x, y) \in (P(\{1, 2\})^2 : x \subseteq y\}$;

    (d) $\mu = \{(x, y, z) \in \{1, 2, 3, 4, 5, 6\}^3 : xy = z\}$;

    (e) $\theta = \{(x, y, z) \in N^3 : x < y < z < 5\}$.

18. Za date relacije ρ i σ na skupu A odrediti $\rho \cup \sigma$, $\rho \cap \sigma$, $\bar{\rho}$, ρ^{-1}, $\rho \circ \sigma$ i $\sigma \circ \rho$:

    (a) $A = \{a, b, c\}$, $\rho = \{(a, a), (a, c)\}$ i $\sigma = \{(a, a), (a, b), (c, b)\}$;

    (b) $A = R$, $\rho = \leq_R$ i $\sigma = \geq_R$.

19. Orijentisani graf (V, E) dat je skupom čvorova $V = \{a, b, c, d, e\}$ i skupom grana $E = \{(a, b), (a, d), (b, c), (c, d), (e, b)\}$. Naći E^{-1}, $E \circ E$ i $(E \circ E) \circ E$.

20. Odrediti $\pi_1(\rho)$ i $\pi_2(\rho)$ ako:

    (a) $X = \{A, B, C\}$, $Y = \{1, 2, 3, 4\}$, $\rho = \{(A, 1), (A, 2), (C, 2)\}$;

    (b) $X = Y = R$, $\rho = \{(x, y) \in R^2 : x^2 + y^2 = 1\}$.

21. Dokazati da za relacije $\rho, \sigma \subseteq X \times Y$ važi:

    (a) $\rho \subseteq \pi_1(\rho) \times \pi_2(\rho)$;

    (b) $\pi_1(\rho \cup \sigma) = \pi_1(\rho) \cup \pi_1(\sigma)$;

    (c) $\pi_1(\rho \cap \sigma) \subseteq \pi_1(\rho) \cap \pi_1(\sigma)$; pokazati da jednakost ne važi uvek.

22. Ako su ρ, σ i τ binarne relacije, dokazati da važi:

    (a) $\rho \circ (\sigma \cup \tau) = \rho \circ \sigma \cup \rho \circ \tau$;

    (b) $(\sigma \cup \tau) \circ \rho = \sigma \circ \rho \cup \tau \circ \rho$;

    (c) $\rho \circ (\sigma \cap \tau) \subseteq \rho \circ \sigma \cap \rho \circ \tau$;

    (d) $(\sigma \cap \tau) \circ \rho \subseteq \sigma \circ \rho \cap \tau \circ \rho$.

    Pokazati primerima da pod (c) i (d) ne mora važiti jednakost.

23. Ako su ρ, σ, τ binarne relacije na skupu A i za sve $x, y, z \in A$ važi

$$(x, y) \in \rho \wedge (x, z) \in \rho \Rightarrow y = z,$$

dokazati da je $\rho \circ (\sigma \cap \tau) = (\rho \circ \sigma) \cap (\rho \circ \tau)$.

24. Ako su ρ, σ i τ relacije na nekom skupu takve da je $\rho \subseteq \sigma \cap \tau$, dokazati da je $(\rho \circ \tau) \cup (\sigma \circ \rho) \subseteq \sigma \circ \tau$.

25. Neka je θ binarna relacija na skupu X. Za $Y \subseteq X$ definišimo $\theta[Y] = \{x \in X : (\exists y \in Y) x \theta y\}$. Neka su A i B podskupovi skupa X.

    (a) Dokazati da je $\theta[A \cap B] \subseteq \theta[A] \cap \theta[B]$.

    (b) Primerom pokazati da u zadatku (a) ne mora da važi jednakost.

26. Za binarnu relaciju ρ na skupu A kažemo da je *neograničena* ako važi: $(\forall x \in A)(\exists y \in A)(x, y) \in \rho$. Ako su ρ i σ neograničene relacije na skupu A, dokazati da su i $\rho \cup \sigma$ i $\rho \circ \sigma$ neograničene.

27. Dokazati: $\rho^{-1} \circ \overline{(\rho \circ \sigma)} \subseteq \overline{\sigma}$ i dati primer kada ne važi jednakost.

28. Dokazati: $(\rho \circ \sigma) \cap \tau \subseteq (\rho \circ \rho^{-1}) \circ \tau$ i dati primer kada ne važi jednakost.

29. Ako $\rho \circ \sigma \subseteq \rho$ i $\rho \circ \sigma^{-1} \subseteq \rho$, dokazati: $\rho \cap (\tau \circ \sigma) = (\rho \cap \tau) \circ \sigma$.

30. Ako su ρ, σ i τ binarne relacije na skupu celih brojeva Z i operacija $*$ definisana ovako:

$$\rho^* = \{(x, y) \in Z^2 : (x + 1, y + 1) \in \rho\},$$

dokazati da je $(\rho \cup (\sigma \circ \tau))^* = \rho^* \cup (\sigma^* \circ \tau^*)$.

Specijalne binarne relacije

31. Ispitati da li su sledeće relacije refleksivne, irefleksivne, simetrične, antisimetrične, tranzitivne:

    (a) na skupu karata za igranje: $x \rho y \Leftrightarrow$ karta x ima isti broj kao y;

    (b) na skupu polja šahovske table: $x \sigma y \Leftrightarrow$ skakač može stići jednim skokom od x do y;

    (c) na skupu svih ljudi: $x \tau y \Leftrightarrow x$ ima oči iste boje kao y;

    (d) na skupu svih ljudi: $x \omega y \Leftrightarrow x$ ima zajedničkog potomka sa y;

    (e) na skupu svih ljudi: $x \theta_1 y \Leftrightarrow x$ je brat osobe y;

    (f) na skupu svih muškaraca: $x \theta_2 y \Leftrightarrow x$ je brat osobe y.

32. Dati primer relacije koja je:

    (a) refleksivna i simetrična, ali ne i tranzitivna;

    (b) refleksivna i tranzitivna, ali ne i simetrična;

    (c) simetrična i tranzitivna, ali ne i refleksivna;

    (d) refleksivna, ali ne simetrična ni tranzitivna;

    (e) simetrična, ali ne refleksivna ni tranzitivna;

    (f) tranzitivna, ali ne refleksivna ni simetrična.

33. Dokazati: ako su ρ i σ refleksivne relacije na skupu A, onda su i $\rho \cup \sigma$, $\rho \cap \sigma$, ρ^{-1} i $\rho \circ \sigma$ refleksivne.

34. Neka su ρ i σ irefleksivne relacije na skupu A.

    (a) Dokazati da su i $\rho \cup \sigma$, $\rho \cap \sigma$ i ρ^{-1} irefleksivne;

    (b) pokazati primerom da $\rho \circ \sigma$ ne mora biti irefleksivna.

35. Neka su ρ i σ simetrične relacije na skupu A.

    (a) Dokazati da su i $\rho \cup \sigma$, $\rho \cap \sigma$ i ρ^{-1} simetrične;

    (b) dokazati da je $\rho \circ \sigma$ je simetrična ako i samo ako važi $\rho \circ \sigma = \sigma \circ \rho$.

36. Neka su ρ i σ relacije na skupu A.

    (a) Ako je ρ je antisimetrična, dokazati da su i $\rho \cap \sigma$ i ρ^{-1} antisimetrične;

    (b) Ako su ρ i σ antisimetrične, pokazati primerima da $\rho \cup \sigma$ i $\rho \circ \sigma$ ne moraju biti antisimetrične.

37. Neka su ρ i σ tranzitivne relacije na skupu A.

    (a) Dokazati da su i $\rho \cap \sigma$ i ρ^{-1} tranzitivne;

    (b) pokazati primerom da $\rho \cup \sigma$ i $\rho \circ \sigma$ to ne moraju biti.

38. Dokazati: ako su ρ i σ relacije na skupu A, $\rho \subseteq \sigma$ i σ refleksivna i tranzitivna, onda je $\rho \circ \sigma \circ \rho \subseteq \sigma \circ \rho \circ \sigma$.

39. Ako je ρ refleksivna, a σ tranzitivna relacija na skupu X i važi $\rho \subseteq \sigma$, dokazati da je $\sigma \circ \rho \circ \sigma = \sigma$.

40. Ako su ρ i σ simetrične relacije skupa A i $\rho \circ \sigma \subseteq \sigma \circ \rho$, dokazati da je $\rho \circ \sigma = \sigma \circ \rho$.

41. Ako je ρ tranzitivna relacija takva da važi $\rho^{-1} \circ \rho \subseteq \rho$, dokazati da je i $\rho \circ \rho^{-1}$ tranzitivna.

42. Dokazati: ako su ρ i σ tranzitivne relacije na skupu A takve da je $\sigma \circ \rho \subseteq \triangle_A$, dokazati da je i $\rho \circ \sigma$ tranzitivna.

43. Neka je $n \in N$ fiksiran, a $\sigma_n \subseteq N \times N$ relacija definisana sa:

$$(x, y) \in \sigma_n \Leftrightarrow x + n \leq y.$$

    Dokazati:

    (a) σ_n je tranzitivna;

    (b) $m \leq n$ ako i samo ako $\sigma_n \subseteq \sigma_m$;

    (c) $\sigma_m \circ \sigma_n \subseteq \sigma_{m+n}$.

Relacije ekvivalencije

44. Naći relaciju ekvivalencije koja odgovara datoj particiji i nacrtati njen graf:

    (a) $\{\{a, b, c, d\}\}$;

    (b) $\{\{a, c\}, \{b, d\}\}$;

(c) $\{\{a,b\},\{c\},\{d\}\}$.

45. Dokazati da su sledeće relacije relacije ekvivalencije i opisati klase ekvivalencije:

(a) paralelnost pravih;

(b) podudarnost duži;

(c) relacija $\equiv_m$ na skupu N definisana sa:

$$a \equiv_m b \text{ ako i samo ako } m \mid (a-b)$$

(ova relacija naziva se *kongruencija po modulu m* i jedna je od najvažnijih u teoriji brojeva);

(d) relacija ρ na skupu R definisana sa: $a\rho b$ ako i samo ako $a-b \in Q$;

(e) relacija $\sim$ na skupu Z definisana sa: $x \sim y$ ako i samo ako $x+y \in P$, gde je P skup svih parnih brojeva.

46. Da li relacija $\perp$ na skupu svih pravih u ravni relacija ekvivalencije?

47. Dat je skup $X = \{$Arsenije,Borivoje,Cana,Dubravka,Eustahije,Flora$\}$ radnika u nekom preduzeću.

(a) Dokazati da je relacija data sa:

$$x\rho y \text{ ako i samo ako } x \text{ i } y \text{ rade u istoj prostoriji}$$

relacija ekvivalencije.

(b) Poznato je da: 1) Asenije radi u istoj prostoriji sa Canom; 2) Cana, Dubravka i Flora sve rade u različitim prostorijama i 3) Florin sto se u jednoj od prostorija nalazi između Borivojevog i Eustahijevog. Odrediti relaciju ρ i njene klase ekvivalencije.

48. Da li je relacija σ na R^2 definisana sa:

$$(a,b)\sigma(c,d) \Leftrightarrow a-b=c-d$$

relacija ekvivalencije?

49. Dokazati da je relacija ρ na skupu R^2 relacija ekvivalencije, gde je

$$(x,y)\rho(z,t) \Leftrightarrow x+y=z+t \wedge x^2+y^2=z^2+t^2.$$

50. Dokazati: ako su ρ, σ i τ binarne relacije na skupu A i ρ relacija ekvivalencije, onda važi $\rho \cap (\sigma \circ (\rho \cap \tau)) \subseteq (\rho \cap \sigma) \circ \tau$.

51. Ako su ρ i σ relacije ekvivalencije na skupu A, dokazati da je i $\rho \cap \sigma$ relacija ekvivalencije.

52. Neka je ρ refleksivna i tranzitivna relacija na skupu A. Dokazati da je $\rho \cap \rho^{-1}$ relacija ekvivalencije na skupu A.

53. Neka je ρ neograničena binarna relacija na skupu A (videti zadatak 26). Dokazati da je ρ relacija ekvivalencije ako i samo ako je $\rho \circ \rho^{-1} = \rho$.

54. Dokazati da je relacija ρ na skupu A relacija ekvivalencije ako i samo ako je $(\rho \circ \rho^{-1}) \cup \triangle_A = \rho$.

55. Neka su ρ i σ relacije ekvivalencije skupa A. Dokazati da je $\rho\circ\sigma\circ\rho$ relacija ekvivalencije ako i samo ako je $\sigma\circ\rho\circ\sigma\subseteq\rho\circ\sigma\circ\rho$.

56. Neka su ρ i σ relacije ekvivalencije. Dokazati:

    (a) $\rho\cup\sigma$ je relacija ekvivalencije ako i samo ako $\rho\cup\sigma=\rho\circ\sigma$;

    (b) $\rho\circ\sigma$ je relacija ekvivalencije ako i samo ako $\rho\circ\sigma=\sigma\circ\rho$.

Relacije poretka

57. Neka je D_n skup delitelja broja n.

    (a) Nacrtati Haseove dijagrame parcijalnih uređenja $(D_n,|)$ za $n=6,8,9,20,24$.

    (b) Za kakvo n je $(D_n,|)$ linearno uređenje?

58. (a) Nacrtati Haseove dijagrame parcijalnih uređenja $(P(A),\subseteq)$ za $A=\{1\},\{1,2\},\{1,2,3\}$.

    (b) Za kakvo A je $(P(A),\subseteq)$ linearno uređenje?

59. Na skupu N prirodnih brojeva definisana je relacija:

$$m\rho n\Leftrightarrow \text{ cifra jedinica broja } m \text{ je manja od cifre jedinica broja } n.$$

    (a) Dokazati da je ρ relacija strogog poretka.

    (b) Skicirati njen Haseov dijagram na skupu $\{1,6,10,20,21,101,199\}$.

60. Na skupu N prirodnih brojeva definisana je relacija:

$$m\rho n\Leftrightarrow \text{ zbir cifara broja } m \text{ je manji od zbira cifara broja } n.$$

    (a) Dokazati da je ρ relacija strogog poretka.

    (b) Skicirati njen Haseov dijagram na skupu $\{1,10,11,20,21,101,199\}$.

61. Na skupu $\{1,2\}\times P(\{a,b\})$ definisana je relacija:

$$(m,X)\rho(n,Y) \text{ ako i samo ako } m\leq n \text{ i } X\supseteq Y.$$

    (a) Dokazati da je ρ relacija poretka.

    (b) Skicirati njen Haseov dijagram.

62. Za neprazan podskup A skupa N sa $\min(A)$ označimo njegov najmanji element. Na skupu $P(N)\setminus\{\emptyset\}$ definisana je relacija ρ na sledeći način: $A\rho B$ ako i samo ako $\min(A)\leq\min(B)$.

    (a) Da li je ρ relacija poretka?

    (b) Da li je $(P(N),\rho)$ linearno uređenje?

63. Naći sve binarne relacije skupa prirodnih brojeva N koje su istovremeno i relacije ekvivalencije i relacije poretka na N.

64. Neka je ρ binarna relacija na skupu A, σ binarna relacija na skupu B, a τ relacija na $A\times B$ definisana sa

$$(x,y)\tau(u,v) \text{ akko } x\rho u\wedge y\sigma v.$$

    Dokazati:

(a) ako su ρ i σ relacije ekvivalencije, i τ je relacija ekvivalencije;

(b) ako su ρ i σ relacije poretka, i τ je relacija poretka.

(c) ako su ρ i σ relacije strogog poretka, i τ je relacija strogog poretka.

65. Ako su ρ i σ relacije poretka na skupu A, dokazati da je i $\rho \cap \sigma^{-1}$ relacija poretka.

66. Neka su ρ i σ relacije strogog poretka na skupu A. Dokazati da je $\rho \cup \sigma$ relacija strogog poretka skupa A ako i samo ako važi

$$(\rho \circ \sigma) \cup (\sigma \circ \rho) \subseteq \rho \cup \sigma. \tag{4.4}$$

67. Dokazati da je parcijalno uređen skup (A, ρ) linearno uređen ako i samo ako $\rho \cup \rho^{-1} = A^2$.

68. Neka su ρ i σ linearna uređenja skupa A. Dokazati da je $\rho \circ \sigma$ linearno uređenje ako i samo ako je $\rho = \sigma$.

69. Neka su $<_N$ i $>_N$ standardne relacije striktnog uređenja na skupu prirodnih brojeva N. Ispitati u kakvom su odnosu $>_N \circ <_N$ i $<_N \circ >_N$ (da li je jedna od njih podskup druge).

70. Neka je S skup svih iskaznih formula i $\sim$ relacija ekvivalentnosti formula. Na skupu $S/\sim$ definisana je relacija $\leq$ ovako:

$$[A] \leq [B] \text{ ako i samo ako } \models (A \Rightarrow B).$$

Dokazati da je $(S/\sim, \leq)$ parcijalno uređenje.

Zatvorenja relacija

71. Naći refleksivno, simetrično i tranzitivno zatvorenje sledećih relacija:

(a) $\rho = \{(1,2),(2,1),(2,3),(3,4)\}$ na skupu $\{1,2,3,4\}$.

(b) $\triangle_N$;

(c) $\leq_N$;

(d) $<_N$.

72. Na skupu $A = \{a,b,c,d\}$ data je relacija $\rho = \{(a,b),(b,b),(b,d),(c,d)\}$.

(a) Naći refleksivno zatvorenje ρ' relacije ρ.

(b) Da li je ρ' relacija poretka? Ako jeste, skicirati njen Haseov dijagram.

73. 12 ljudi, označenih brojevima od 1 do 12, raspoređeno je na sedišta u tri reda na sledeći način:

1	2	3	4
5	6	7	8
9	10	11	12

Definišemo relaciju ρ na skupu $\{1,2,\ldots,12\}$: $x \rho y$ ako i samo ako x sedi u istom redu kao y i desno od njega (ne obavezno neposredno).

(a) Da li je ρ tranzitivna? Naći njeno tranzitivno zatvorenje ρ_T.

(b) Da li je ρ_T simetrična? Naći njeno simetrično zatvorenje ρ_S.

(c) Da li je ρ_S refleksivna? Naći njeno refleksivno zatvorenje ρ_R.

(d) Da li je ρ_R relacija ekvivalencije? Opisati tu relaciju rečima.

74. Naći tranzitivna zatvorenja sledećih relacija na skupu polja šahovske table, pokazati da su to relacije ekvivalencije i naći njihove klase ekvivalencije:

(a) $x\rho y \Leftrightarrow$ skakač može stići jednim skokom od x do y;

(b) $x\rho y \Leftrightarrow$ lovac može stići jednim potezom od x do y.

Glava 5

Funkcije i kardinalnost skupova

5.1 Funkcije

Definicija 5.1 *Funkcija (preslikavanje) skupa A u skup B, u oznaci $f : A \to B$, je podskup skupa $A \times B$ takav da*

$$(\forall a \in A)(\exists_1 b \in B)(a, b) \in f. \tag{5.1}$$

Kao što se vidi iz definicije, funkcije su ustvari binarne relacije koje zadovoljavaju još jedan dodatni uslov (5.1). Skup A naziva se domen, a skup B kodomen funkcije f. Naravno, umesto $(a, b) \in f$ uglavnom se koristi zapis $f(a) = b$.

Primetimo da, pošto smo funkciju definisali kao skup uređenih parova, njen kodomen nije time precizno određen. Npr. funkcija zadata sa $f(x) = x^2$ za $x \in R$ je ustvari skup $\{(x, x^2) : x \in R\}$, ali se pritom za kodomen može uzeti ceo skup R ali i njegov podskup $\{x \in R : x \geq 0\}$.

Definicija 5.2 *Funkcije $f : A^n \to A$ (čiji je domen neki stepen kodomena A) nazivamo n-arne operacije skupa A.*

Operacije su osnovni predmet izučavanja algebre koja, između ostalog, proučava njihove osobine poput komutativnosti, asocijativnosti i sl. koje su takođe pominjane i u ovoj knjizi.

Ako funkciju $f : A \to B$, kao skup uređenih parova, predstavimo u koordinatnom sistemu koji prikazuje proizvod $A \times B$, dobijamo *grafik* funkcije.

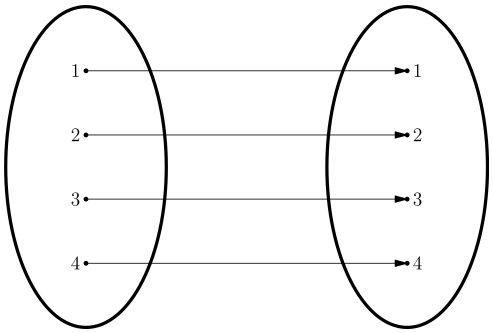
Definicija 5.3 *Funkcija $f : A \to B$ je:*

- *1-1 (injekcija) ako $(\forall x, y \in A)(f(x) = f(y) \Rightarrow x = y)$;*
- *„na" (sirjekcija) ako $(\forall b \in B)(\exists a \in A) f(a) = b$;*
- *bijekcija ako je 1-1 i „na".*

Uslov 1-1 je možda lakše razumeti ako ga zapišemo kontrapozicijom: iz $x \neq y$ sledi $f(x) \neq f(y)$, dakle: različiti elementi domena moraju se slikati u različite elemente kodomena. Ipak, oblik koji smo dali u definiciji je najpogodniji za praktičnu proveru.

Veoma je bitno uočiti da uslovi 1-1 i ,,na" zajedno ustvari traže da uslov (5.1) (koji mora biti ispunjen za svaku funkciju) važi i kada se ,,zamene" uloge domena i kodomena, tj. da za svako $b \in B$ postoji tačno jedno $a \in A$ za koje $f(a) = b$.

Primer 5.4 *(1) Za bilo koji skup A identičko preslikavanje skupa A je $i_A : A \to A$ definisano ovako: $i_A(x) = x$ za sve $x \in A$. Npr. za $A = \{1, 2, 3, 4\}$ ta funkcija izgleda ovako:*

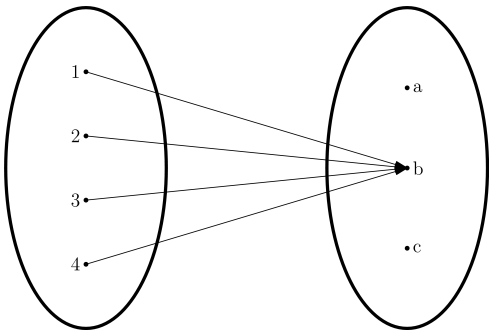


Posmatran kao skup uređenih parova, ovaj skup je ustvari isto što i relacija koju smo zvali dijagonala: $i_A = \{(x, x) : x \in A\}$. To je ujedno i najjednostavniji primer bijekcije na bilo kojem skupu; proverimo da je to zaista bijekcija:

1-1: iz $f(x) = f(y)$ po definiciji preslikavanja f imamo $x = y$;

,,na": za svako $a \in A$ postoji element koji se u njega slika: sam taj element, tj. $f(a) = a$.

(2) Za bilo koja dva skupa A i B možemo izabrati jedan element $b \in B$ i definisati konstantno preslikavanje $f : A \to B$ ovako: $f(x) = b$ za sve $x \in A$. Npr. ako je $A = \{1, 2, 3, 4\}$ i $B = \{a, b, c\}$ to preslikavanje izgleda ovako:

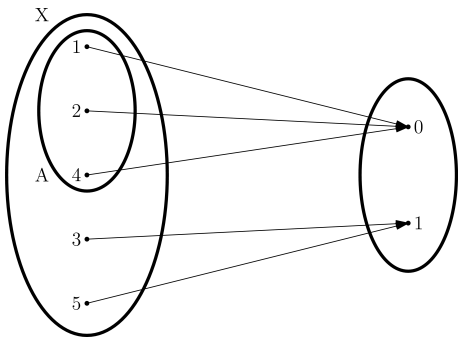


Ovo preslikavanje može biti 1-1 samo u slučaju da A ima samo 1 element. Ono može biti ,,na" samo u slučaju da B ima samo 1 element (b).

(3) Za svaki podskup A nekog skupa X možemo definisati odgovarajuću karakterističnu funkciju $\chi_A : X \to \{0, 1\}$ na sledeći način:

$$\chi_A(x) = \begin{cases} 0, & \text{ako } x \in A \\ 1, & \text{ako } x \notin A. \end{cases}$$

Ako je, recimo, $X = \{1, 2, 3, 4, 5\}$ i $A = \{1, 2, 4\}$, dijagram te funkcije je:



Karakteristične funkcije skupova igraju veoma važnu ulogu u teoriji algoritama (videti [1], str. 44). χ_A može biti 1-1 samo ako i A i $\overline{A}$ imaju najviše po 1 element. S druge strane, ona je ,,na" ako i A i $\overline{A}$ imaju bar po jedan element.

(4) Realni nizovi koji se izučavaju u matematičkoj analizi su ustvari funkcije $x : N \to R$, samo što se umesto $x(n)$ češće koristi oznaka x_n za n-ti član niza.

(5) Operacije iskazne algebre $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ su binarne, a $\neg$ unarna operacija na skupu $\{\top, \bot\}$.

(6) Najveći zajednički delilac (NZD) i najmanji zajednički sadržalac (NZS) su dve binarne operacije na skupu N (ili na skupu $Z \setminus \{0\}$).

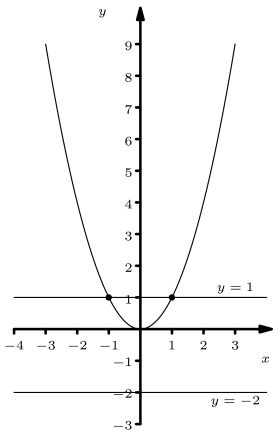
(7) Ako je $A = \{1, 2, 3\}$, skupovi $f = \{(1, 2), (1, 3), (2, 3), (3, 1)\}$ i $g = \{(1, 2)\}$ uopšte nisu funkcije sa domenom A. Naime, f ,,preslikava" element 1 u dva različita elementa, a g ne preslikava element 2 nigde, što nije dozvoljeno po uslovu (5.1).

Ako je domen funkcije neki direktan proizvod, onda ona ima više argumenata; to važi recimo za binarne operacije. Tada, umesto $f((x, y))$ (jer su elementi domena uređeni parovi), da bismo pojednostavili zapis pišemo samo $f(x, y)$.

Funkcije na realnim brojevima najelegantnije se predstavljaju grafikom, a posebna prednost takvog prikazivanja je to što sa grafika možemo i ,,pročitati" da li je funkcija 1-1 i ,,na". Naime, f će biti 1-1 ako i samo ako svaka horizontalna prava u koordinatnom sistemu (prava oblika $y = a$ za neku konstantu a) seče grafik funkcije f u najviše jednoj tački. Slično, f je ,,na" ako i samo ako svaka horizontalna prava seče grafik u bar jednoj tački.

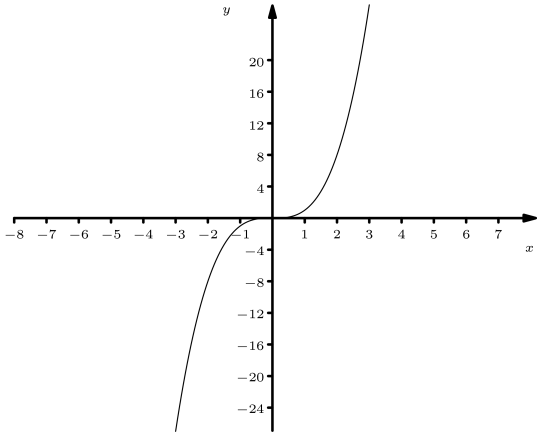
Slično tome, grafik svake funkcije mora svaku vertikalnu pravu preseći u tačno jednoj tački (da bi bio ispunjen uslov (5.1)).

Primer 5.5 *(1) Neka je $f : R \to R$ zadata sa $f(x) = x^2$. Sa grafika vidimo da f nije ni 1-1 (jer prava $y = 1$ seče grafik u dve tačke) ni ,,na" (jer ga prava $y = -2$ ne seče ni u jednoj tački:*



Zašto je ovakvo rezonovanje dobro? To što prava $y = 1$ seče grafik u dve tačke znači da postoje dve različite vrednosti $x_1, x_2 \in R$ koje se slikaju u 1: $f(1) = f(-1) = 1$. To što prava $y = -2$ ne seče grafik nijednom znači da ne postoji nijedan $a \in R$ takav da je $f(a) = -2$.

(2) Posmatrajmo sada grafik funkcije $g : R \to R$ zadate sa $g(x) = x^3$:



Vidimo da svaka horizontalna prava seče grafik funkcije g u tačno jednoj tački, što znači da je g bijekcija. Dokažimo da je zaista tako:

1-1: Iz $g(x) = g(y)$, odnosno $x^3 = y^3$, sledi (primenom 3. korena) da je $x = y$. (Zašto ovo nismo mogli uraditi i za funkciju f iz prošlog primera? Zato što bi korenovanje jednakosti $x^2 = y^2$ dalo samo $|x| = |y|$, pa ne mora važiti $x = y$!)

,,na": Za svako $b \in R$ možemo naći element $a = \sqrt[3]{b}$ takav da je $g(a) = b$. (Zašto ni ovo nije ,,radilo" za funkciju f? Zato što ne smemo primenjivati kvadratni koren na negativne brojeve.)

Svaki programski jezik ima u sebi ugrađen veliki broj funkcija i (specijalno) operacija. Funkcije se u programiranju najčešće primenjuju u istom zapisu kao i u matematici: iza imena funkcije u zagradi se nabrajaju argumenti. Za operacije (pre svega binarne) obično se koristi infiksna notacija, i uobičajeno je da se operacijama nazivaju sve funkcije koje se zapisuju infiksno (čak i ako se ne uklapaju u našu definiciju 5.2).

Primer 5.6 *(1) Neka je $f : R \to Z$ funkcija koja svaki ceo broj preslikava u najbliži ceo broj manji ili jednak od njega. U matematici se ona obično označava sa $f(x) = \lfloor x \rfloor$, dok je u programskom jeziku Java označena sa* `floor(x)`.

(2) U Javi se logičke vrednosti $\top$ i $\bot$ predstavljaju kao 1 i 0. Jedna binarna operacija u Javi je npr. $==: R \to \{0, 1\}$ definisana sa

$$(x == y) = \begin{cases} 1, & \text{ako } x = y \\ 0, & \text{ako } x \neq y, \end{cases}$$

i ona služi za proveru da li su neke dve vrednosti jednake. Ovo je na prvi pogled pomalo neobično jer o jednakosti obično ne razmišljamo kao o operaciji, ali za programiranje je pogodno. Slično ovome, svaku n-arnu relaciju P na skupu A možemo predstaviti i kao operaciju koja preslikava A^n u $\{0, 1\}$: uređene n-torke preslikamo u 1 ako one pripadaju relaciji P a u 0 inače.

(3) Operacija dodavanja jedinice na neki ceo broj, $++ : Z \to Z$ je jedna unarna operacija.

(4) ASCII kod opisan u primeru 4.57 je ustvari jedna bijekcija između skupa $\{n \in Z : 0 \leq n \leq 255\}$ i jednog skupa znakova.

Napomenimo da definicija funkcije data u (5.1) ima izvesne nedostatke. Naime, da li smatramo različitim funkciju $f : R \to R$ datu sa $f(x) = x^2$ i funkciju $g : R \to R^+ \cup \{0\}$ datu sa $g(x) = x^2$? Posmatrani kao skupovi oni su jednaki, ali ove funkcije imaju neke različite osobine, npr. f nije „na" a g jeste (jer su im kodomeni različiti). Iz ovog razloga preciznija definicija funkcije bi bila da je to uređena trojka (A, B, f), gde su A i B domen i kodomen, a $f : A \to B$. Međutim, mi ćemo se jednostavnosti radi držati gornje definicije i po potrebi naglašavati na kojem domenu i kodomenu posmatramo funkciju.

5.2 Parcijalne funkcije, restrikcije funkcija

Pomenimo još i pojam parcijalne funkcije, veoma značajan u teoriji rekurzija. *Parcijalna funkcija* na skupu A je funkcija definisana na nekom podskupu X skupa A. Drugim rečima, ona nije definisana na svim elementima skupa A. Formalno, ona je tada funkcija sa domenom X, ali iz praktičnih razloga nekad se naziva i parcijalna funkcija na skupu A.

Primer 5.7 *(1) Na skupu A svih ljudi definišimo funkciju*

$$f(x) = \text{broj računa osobe } x \text{ u banci.}$$

Kako ne mora svaka osoba imati otvoren račun u banci, ovo je parcijalna funkcija na A.

(2) Kako računari mogu raditi samo sa ograničenim (dakle, konačnim) skupovima brojeva, svaka operacija nad celim ili realnim brojevima koja se izvodi na računaru samo je parcijalna. Tako, tip celih brojeva `int` *u Javi obuhvata samo brojeve iz skupa $X = \{-2147483648, \ldots, 2147483647\}$, pa je čak i operacija celobrojnog sabiranja samo parcijalna - definisana samo na parovima čiji zbir se nalazi u navedenom opsegu.*

Već smo se sretali sa funkcijama na različitim skupovima definisanim na isti način. Npr. operacija sabiranja $+_N$ na skupu N i operacija sabiranja $+_Z$ na skupu Z funkcionišu jednako (za prirodne brojeve), ali strogo govoreći to nisu iste funkcije, jer npr. $((2,-1),1) \in +_Z$ ali $((2,-1),1) \notin +_N$, drugim rečima operacija $+_N$ nije definisana van skupa prirodnih brojeva. U sledećoj definiciji preciziraćemo odnos ovakvih funkcija.

Definicija 5.8 *Ako je $f : A \to B$ funkcija i $X \subseteq A$, restrikcija funkcije f na skup X je funkcija $f \restriction_X : X \to B$ definisana sa $f \restriction_X (x) = f(x)$ za sve $x \in X$.*

Primer 5.9 *(1) Ako je data funkcija $f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$, onda je njena restrikcija na skup $\{1,2,3\}$ funkcija $f \restriction_{\{1,2,3\}} : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}$.*

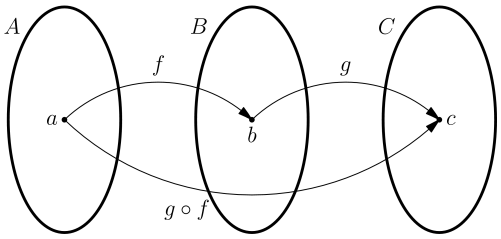
(2) Operacija $+_N$ je restrikcija operacije $+_Z$ na skup N^2, a $+_Z$ je opet restrikcija operacije $+_R$ na skup Z^2. Kao što smo već naveli u delu (2) prethodnog primera, svaka operacija koja se izvodi na računaru samo je restrikcija odgovarajuće matematičke operacije. Dakle, operaciju celobrojnog sabiranja u Javi možemo posmatrati kao restrikciju operacije $+_Z$ na skup X definisan u tom primeru.

(3) Neka je $f : R \to R$ data sa $f(x) = x^2$ i $g = f \restriction_{R^+}$, gde je R^+ skup pozitivnih realnih brojeva. Dakle, i f i g su funkcije koje kvadriraju, ali f ima za domen ceo skup R dok je g definisana samo na R^+. Već smo videli u primeru 5.4 da f nije 1-1. Međutim, $f \restriction_{R^+}$ jeste, jer za pozitivne realne brojeve iz $x^2 = y^2$ sledi $x = y$. Dakle, ove funkcije je bitno razlikovati jer su i neke njihove značajne osobine različite.

5.3 Kompozicija funkcija

Definicija 5.10 *Ako su $f : A \to B$ i $g : B \to C$ funkcije, njihova kompozicija je funkcija $g \circ f : A \to C$ definisana sa $g \circ f(x) = g(f(x))$ za sve $x \in A$.*

Iz gornjeg primera vidimo da ne možemo praviti kompoziciju bilo koje dve funkcije: neophodno je da kodomen prve bude jednak domenu druge (ili, opštije, bar da bude njegov podskup).



Slika 5.1: Kompozicija funkcija

Kako smo funkcije definisali kao specijalne relacije, napomenimo da se (iako to nije očigledno) definicija kompozicije funkcija potpuno slaže sa kompozicijom relacija. Naime, ako $f(a) = b$ i $g(b) = c$, njihova kompozicija je definisana tako da $g \circ f(a) = c$ (slika). Zapisujući ove funkcije kao skupove uređenih parova (tj. binarne relacije), prethodna rečenica dobija sledeći oblik: ako $(a,b) \in f$

i $(b,c) \in g$, onda $(a,c) \in g \circ f$, što je upravo način na koji smo definisali kompoziciju relacija. Jedina razlika je u redosledu f i g u toj kompoziciji. Razlog zbog kojeg se kod kompozicije funkcija uglavnom koristi ovaj neobični redosled (da se funkcija koja se prva primenjuje piše s desne strane) je to što se tada u zapisu $g \circ f(x) = g(f(x))$ ne menja redosled, što je dosta praktično, posebno kod komplikovanijih izraza.

Primer 5.11 *(1) Neka su date $f : R \to R$ i $g : R \to R$ ovako: $f(x) = x^2$ i $g(x) = 2x + 1$. Tada je*

$$g \circ f(x) = g(f(x)) = g(x^2) = 2x^2 + 1$$

$$f \circ g(x) = f(g(x)) = f(2x + 1) = (2x + 1)^2.$$

Primetimo da dobijene kompozicije nisu jednake, npr. $g \circ f(1) = 3$ a $f \circ g(1) = 9$. Dakle, u opštem slučaju ne važi komutativnost, tj. ne mora biti $g \circ f = f \circ g$.

(2) Neka je $A = \{1,2,3,4\}$ i unarne operacije f i g na A su date sa $f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ i $g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 4 \end{pmatrix}$. Tada je $g \circ f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 4 \end{pmatrix}$ i $f \circ g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 3 \end{pmatrix}$.

Za narednih nekoliko teorema potrebno je razjasniti: šta, za neke dve funkcije f i g, znači da su jednake ($f = g$)? Za početak, potrebno je da one imaju jednake domene. Pored toga, pošto su funkcije ustvari skupovi uređenih parova, u skladu sa definicijom 4.1 potrebno je da one sadrže iste uređene parove, tj. da za svaki element x njihovog domena važi $f(x) = g(x)$.

Pošto smo videli da se kompozicija funkcija definiše u skladu sa definicijom relacija, nije iznenađujuće da osobine ove operacije i dalje važe. Tako smo videli u prethodnom primeru da kompozicija funkcija nije komutativna. Sledeća teorema analogna je teoremi 4.33.

Teorema 5.12 *Ako $f : A \to B$, $g : B \to C$ i $h : C \to D$, onda je $(h \circ g) \circ f = h \circ (g \circ f)$.*

Dokaz. Da bismo dokazali da su funkcije $(h \circ g) \circ f$ i $h \circ (g \circ f)$ jednake, treba da dokažemo da one svaki element x svog domena A preslikavaju u isti element kodomena.

$$(h \circ g) \circ f(x) = h \circ g(f(x)) = h(g(f(x)))$$
$$h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x)))$$

Kao što vidimo, oba preslikavanja funkcionišu tako što se primeni najpre f, zatim g i na kraju h. □

Takođe, kako je identičko preslikavanje i_A ustvari isti skup kao $\triangle_A$, prirodno je da važi i sledeće tvrđenje, analogno teoremi 4.31(c).

Teorema 5.13 *Ako $f : A \to B$, onda je $f \circ i_A = i_B \circ f = f$.*

Dokaz. Dokažimo da je $f \circ i_A = f$. Za svako $x \in A$ je

$$f \circ i_A(x) = f(i_A(x)) = f(x).$$

Potpuno analogno se dokazuje i $i_B \circ f = f$. □

Podsetimo se još jednom da je neophodno da kodomen prve funkcije bude podskup domena druge da bi se uopšte mogla definisati kompozicija tih funkcija; to je razlog zbog kojeg se u prvoj kompoziciji u prethodnoj teoremi pojavljuje i_A a u drugoj i_B.

Teorema 5.14 *Neka $f : A \to B$ i $g : B \to C$.*

(a) Ako su f i g 1-1, onda je i $g \circ f$ 1-1.

(b) Ako su f i g „na", onda je i $g \circ f$ „na".

(c) Ako je $g \circ f$ 1-1, onda je i f 1-1.

(d) Ako je $g \circ f$ „na", onda je i g „na".

Dokaz. (a) Pretpostavimo da je $g \circ f(x) = g \circ f(y)$ za neke $x, y \in A$. To znači da je $g(f(x)) = g(f(y))$, pa kako je g 1-1, sledi $f(x) = f(y)$. Pošto je i f 1-1, dobijamo $x = y$.

(b) Neka je dat proizvoljan element $c \in C$. Kako je g „na", postoji $b \in B$ takav da $g(b) = c$. Pošto je i f „na", postoji i $a \in A$ takav da $f(a) = b$. Ali tada $g \circ f(a) = g(f(a)) = g(b) = c$.

(c) Pretpostavimo da je $g \circ f$ 1-1. Da bismo dokazali da je i f 1-1, uzmimo $x, y \in A$ takve da je $f(x) = f(y)$. Ali tada je i $g(f(x)) = g(f(y))$, pa pošto je $g \circ f$ 1-1, sledi $x = y$.

(d) Neka je $c \in C$ proizvoljan element. Kako je $g \circ f$ „na", postoji $a \in A$ takav da $g \circ f(a) = c$. Ali to znači da je $g(f(a)) = c$, odnosno $f(a)$ je element skupa B koji se funkcijom g slika u c. □

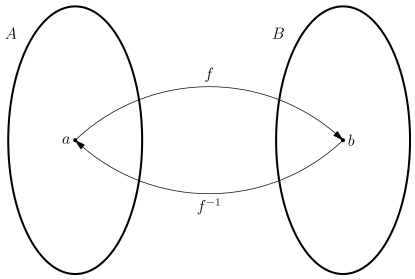
Primer 5.15 *Pokažimo primerom da nije moguće dokazati više od onog što je pokazano u delovima (c) i (d) prethodne teoreme: da je moguće da $g \circ f$ bude 1-1 ali da g nije 1-1, kao i da je moguće da $g \circ f$ bude „na", a da f nije „na". Definišimo $A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$ i funkcije $f : \begin{pmatrix} a \\ b_1 \end{pmatrix}$ i $g : \begin{pmatrix} b_1 & b_2 \\ c & c \end{pmatrix}$. Tada je funkcija $g \circ f : \begin{pmatrix} a \\ c \end{pmatrix}$ očigledno bijekcija, ali g nije 1-1, a f nije „na".*

5.4 Inverzna funkcija

Definicija 5.16 *Inverzno preslikavanje za funkciju $f : A \to B$ je funkcija $g : B \to A$ takva da je $g \circ f = i_A$ i $f \circ g = i_B$.*

Prethodna definicija znači ustvari da g radi „suprotno" od f: ako je $f(a) = b$, onda je $g(b) = a$. Naime, tada je

$$g \circ f(a) = g(f(a)) = g(b) = a \tag{5.2}$$
$$f \circ g(b) = f(g(b)) = f(a) = b. \tag{5.3}$$



Slika 5.2: Inverzna funkcija

Važno je naglasiti da ne postoji za svaku funkciju f njena inverzna funkcija; to ćemo precizirati u teoremi 5.18.

Primer 5.17 *(1) Neka je $f : R \to R$ data sa $f(x) = x+1$. Za njenu inverznu funkciju g mora da važi $g(x+1) = x$ za sve $x \in R$. Da bismo odredili tu funkciju obeležimo $t = x + 1$; tada je $x = t - 1$ pa je $g(t) = t - 1$ za sve $t \in R$.*

(2) Neka je $f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$. Kako je $f(1) = 2$, za njenu inverznu funkciju g mora važiti $g(2) = 1$. Analognim razmatranjem za ostale elemente dobijamo $g : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$.

(3) Neka je sada $f(x) = x^2$. Ako bi g bila njena inverzna funkcija, zbog $f(2) = f(-2) = 4$ element 4 morao bi se funkcijom g slikati i u 2 i u -2, što nije dozvoljeno po definiciji funkcije. Takođe, kako se funkcijom f nijedan $x \in R$ ne preslikava u -1, funkcijom g element -1 ne može se slikati ni u jedan $x \in R$, što takođe nije dozvoljeno po definiciji (5.1).

Kao što možemo zaključiti već iz poslednje tačke gornjeg primera, da bi f imala inverznu funkciju neophodno je da bude 1-1 i ,,na". Sledeća teorema pokazuje da je to i dovoljno.

Teorema 5.18 *(a) Za funkciju $f : A \to B$ postoji inverzna ako i samo ako je f bijekcija;*

(b) ako inverzna funkcija za f postoji, ona je jedinstvena.

Dokaz. (a) ($\Rightarrow$) Pretpostavimo prvo da f ima inverznu funkciju g. Po definiciji to znači da je $g \circ f = i_A$ i $f \circ g = i_B$. Kako je i_A 1-1 funkcija, prema teoremi 5.14(c) mora i f biti 1-1. Pošto je i_B ,,na", prema teoremi 5.14(d) mora i f biti ,,na".

($\Leftarrow$) Pretpostavimo sada da je f bijekcija. To znači da za svaki $b \in B$ postoji jedinstven element $a \in A$ takav da je $f(a) = b$; definišimo $g(b) = a$ za sve takve b i a. Kao što smo videli u (5.2) i (5.3) to upravo znači da je $g \circ f = i_A$ i $f \circ g = i_B$.

(b) Pretpostavimo da postoji još jedna funkcija $g_1 : B \to A$ takva da je $g_1 \circ f = i_A$ i $f \circ g_1 = i_B$. Tada imamo, koristeći teoreme 5.12 i 5.13:

$$g_1 = g_1 \circ i_B = g_1 \circ (f \circ g) = (g_1 \circ f) \circ g = i_A \circ g = g,$$

što je i trebalo dokazati. □

Ubuduće ćemo, znajući da je inverzna funkcija za f (ako postoji) jedinstvena, tu funkciju označavati sa f^{-1}.

Teorema 5.19 *Ako je f bijekcija, onda je i f^{-1} bijekcija i važi $(f^{-1})^{-1} = f$.*

Dokaz. Dokažimo da je i f inverzna funkcija za f^{-1}, pa će to po prethodnoj teoremi značiti da je i f^{-1} bijekcija. Ali to sledi direktno iz uslova da je f^{-1} inverzna za f: $f^{-1} \circ f = i_A$ i $f \circ f^{-1} = i_B$. □

Teorema 5.20 *Ako su $f : A \to B$ i $g : B \to C$ bijekcije, onda je i $g \circ f$ bijekcija i važi $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dokaz. Ako dokažemo da je $f^{-1} \circ g^{-1}$ inverzna funkcija za $g \circ f$, iz teoreme 5.18 će slediti da je $g \circ f$ bijekcija. Ali to sledi iz

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ i_B \circ f \\ &= f^{-1} \circ f \\ &= i_A\end{aligned}$$

i

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ i_B \circ g^{-1} \\ &= g \circ g^{-1} \\ &= i_C\end{aligned}$$

čime je dokaz završen. □

Važnu primenu pojmovi bijekcije i inverzne funkcije nalaze u *kriptovanju*. Naime, prilikom slanja poruka često je neophodno šifrovati poruku da je ne bi mogao pročitati niko osim onog kome je ona namenjena. Jedan prirodan način da se to učini je da se na svaki simbol u poruci primeni neka funkcija f. Npr. možemo primeniti funkciju koja svako slovo preslikava u sledeće slovo abecede, osim poslednjeg, koje se preslikava u prvo: $f : \begin{pmatrix} a & b & \dots & y & z \\ b & c & \dots & z & a \end{pmatrix}$ Npr. primenom ove funkcije reč ,,logika" postaje ,,mphjlb".

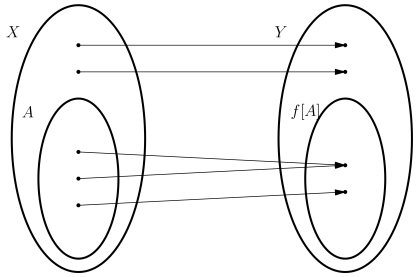
Da bi dešifrovao poruku primalac mora znati inverznu funkciju f^{-1}. Primenjujući je, on rekonstruiše originalnu poruku slovo po slovo. Kao što vidimo, funkcija za šifrovanje mora biti bijekcija (da bi imala inverznu funkciju).

Naravno, funkcija f za kriptovanje mora biti znatno složenija da bi učinila dešifrovanje što težim za onog ko ne zna f^{-1}. U tu svrhu često se koriste rezultati teorije grupa; neke informacije o tome mogu se naći u [20]. Kodomen funkcije f čak ne mora biti skup simbola: moguće je jedan simbol zameniti sa više simbola prilikom šifrovanja, što dodatno otežava dešifrovanje onome ko ne zna f^{-1}.

5.5 Direktna i inverzna slika

Definicija 5.21 *Neka je $f : X \to Y$ funkcija, $A \subseteq X$ i $B \subseteq Y$. Direktna slika skupa A je skup*

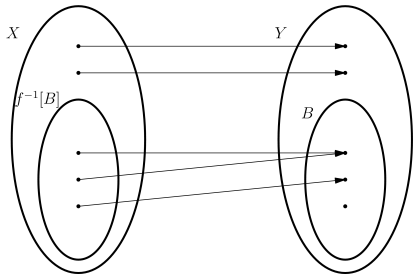
$$f[A] = \{y \in Y : (\exists a \in A) f(a) = y\} = \{f(a) : a \in A\}.$$



Slika 5.3: Direktna slika skupa A

Inverzna slika skupa B je skup

$$f^{-1}[B] = \{x \in X : f(x) \in B\}.$$



Slika 5.4: Inverzna slika skupa B

Direktna slika $f[X]$ celog domena obično se naziva *rang funkcije* f. Primetimo da je $f : X \to Y$ „na" ako i samo ako je $f[X] = Y$, tj. rang funkcije f je ceo kodomen Y.

Primer 5.22 *(1) Neka je $f : R \to R$ data sa $f(x) = 2x$. Njen rang, skup $f[R]$ je ceo skup R jer je f „na" funkcija. Direktna slika skupa N je $f[N] = \{2n : n \in N\}$ - skup parnih prirodnih brojeva.*

(2) Neka je sada $g : R \to R$ data sa $g(x) = x^2$. Njen rang je $g[R] = \{x \in R : x \geq 0\} = R^+ \cup \{0\}$. Inverzna slika skupa R je $g^{-1}[R] = R$, ali je i $g^{-1}[R^+ \cup \{0\}] = R$.

Važno je razlikovati oznaku za inverznu sliku skupa $f^{-1}[B]$ od inverzne funkcije f^{-1}, mada su te oznake slične. Pomenimo još jednom da inverzna funkcija ne postoji uvek (samo ako je f bijekcija), a inverznu sliku skupa možemo računati za svaku funkciju f.

Neke osobine direktne i inverzne slike skupa biće dokazane u zadatku 31. Dokazi za inverznu sliku će biti znatno jednostavniji jer u njenoj definiciji ne učestvuje nijedan kvantifikator. Takođe, upravo će prisustvo kvantifikatora $\exists$ biti razlog zbog kojeg u nekim osobinama nemamo jednakost već samo inkluziju (preciznije, razlog je „neslaganje" kvantifikatora $\exists$ sa veznikom $\wedge$).

5.6 Rekurzija

Za funkciju f sa domenom N kažemo da je definisana *rekurzivno* ako su joj, počevši od nekog n, vrednosti $f(n)$ zadate preko prethodnih vrednosti $f(k)$ za $k < n$. Obično su, uz ovakvu rekurentnu formulu, zadati i početni uslovi:

vrednosti $f(n)$ za prvih nekoliko prirodnih brojeva n koje omogućavaju da se, krenuvši od njih, izračuna $f(n)$ za bilo koje n.

Za funkcije definisane rekurzivno prirodan način dokazivanja njihovih osobina je matematička indukcija. Zaista, ako uporedimo ,,strategiju" definisanja neke funkcije rekurzivno (najpre $f(1)$ a zatim se svaka sledeća vrednost izražava preko prethodnih) primećujemo veliku sličnost sa ,,strategijom" indukcije (najpre dokazati tvrđenje $T(1)$, a zatim, uz pretpostavku da su dokazana $T(k)$ za $k < n$, dokazati i $T(n)$).

Primer 5.23 *(1) Funkcija $f : N \to N$ zadata je početnim uslovom $f(1) = 2$ i rekurentnom formulom $f(n+1) = f(n) + 2$ (za $n \geq 1$). Iz ove definicije možemo izračunati $f(n)$ za svako n; npr.*

$$\begin{aligned} f(2) &= f(1) + 2 = 4 \\ f(3) &= f(2) + 2 = 6 \\ f(4) &= f(3) + 2 = 8 \end{aligned}$$

i tako dalje. Nije teško zaključiti da je ustvari $f(n) = 2n$ za sve $n \in N$, što možemo i dokazati indukcijom:

B.I. Za $n = 1$ je direktno zadato $f(1) = 2 = 2 \cdot 1$.

I.H. Pretpostavimo da je $f(n) = 2n$ za neko $n \in N$.

I.K. Dokažimo da je i $f(n+1) = 2(n+1)$. Zaista, iz rekurentne formule je, uz korišćenje indukcijske hipoteze, $f(n+1) = f(n)+2 = 2n+2 = 2(n+1)$.

(2) Neka je funkcija $g : N \to N$ zadata sa $g(1) = 1$ i $g(n+1) = 3g(n)$ za $n \geq 1$. Slično kao u prvom primeru imamo

$$\begin{aligned} g(2) &= 3g(1) = 3 \\ g(3) &= 3g(2) = 9 \\ g(4) &= 3g(3) = 27 \end{aligned}$$

pa možemo dokazati indukcijom da je $g(n) = 3^{n-1}$.

(3) Fibonačijev niz je funkcija $F : N \to N$ zadata početnim uslovima $F(1) = 1$ i $F(2) = 1$ i rekurentnom relacijom $F(n+1) = F(n) + F(n-1)$ za $n \geq 2$. Tako imamo

$$\begin{aligned} F(3) &= F(2) + F(1) = 2 \\ F(4) &= F(3) + F(2) = 3 \\ F(5) &= F(4) + F(3) = 5 \end{aligned}$$

i tako dalje. Ovo je primer funkcije za koju je nešto teže naći opšti izraz za $F(n)$. Metod za rešavanje ovakvih rekurentnih formula opisan je u [8].

Primetimo da, recimo, formule $F(n+1) = F(n) + F(n-1)$ i $F(n) = F(n-1) + F(n-2)$ daju istu rekurentnu vezu, te uz jednake početne uslove definišu istu funkciju.

Rekurzivne funkcije predmet su proučavanja teorije rekurzija, oblasti koja pripada i matematičkoj logici i teorijskom računarstvu. Njoj je posvećen veliki deo knjige [1].

Pojam rekurzije je znatno opštiji od ovog koji smo ovde opisali. Ustvari, već u ovoj knjizi videli smo neke drugačije rekurzivne definicije. Npr. videli smo u

definiciji tranzitivnog zatvorenja (4.3) da se rekurzija može koristiti i za definisanje relacija. Takođe, rekurzija se ne mora sprovoditi samo na skupu prirodnih brojeva: podsetimo se definicija koje opisuju građenje iskaznih (definicija 2.3) i predikatskih formula (definicija 3.2). Potom, kada smo dokazivali neke osobine tako definisanih pojmova, takođe smo se koristili matematičkom indukcijom, ali njenom opštijom verzijom - totalnom indukcijom (videti npr. teoreme 2.5 i 2.37).

Naravno, rekurzija je od velikog značaja i u programiranju, gde je mnoge probleme prirodno rešavati rekurzivno. Navedimo kao primer rekurzivnu funkciju u Javi za računanje n-tog Fibonačijevog broja.

```
int Fibonaci(int n)
  {
  if(n==1 || n==2)
    return 1;
  else
    return Fibonaci(n-1)+Fibonaci(n-2);
  }
```

Ovakav način računanja Fibonačijevih brojeva je, s jedne strane, prirodan jer direktno sledi njihovu rekurzivnu definiciju, ali je s druge strane veoma neefikasan.

5.7 Kardinalnost skupova

Definicija 5.24 *Za skupove A i B kažemo da su ekvipotentni (i pišemo $A \sim B$) ako postoji bijekcija $f : A \to B$.*

Strogo gledano, kolekcija C svih skupova nije skup: ako bi postojao skup koji sadrži sve skupove, on bi sadržao i sebe kao element, što je nemoguće. Stoga ni $\sim$ nije relacija, jer je ona definisana na C. Međutim, ovakvi problemi su daleko izvan okvira ove knjige, pa ćemo ubuduće o $\sim$ govoriti kao o relaciji.

Teorema 5.25 *$\sim$ je relacija ekvivalencije nad skupovima.*

Dokaz. R: Svaki skup A je ekvipotentan samom sebi, jer je $i_A : A \to A$ bijekcija.

S: Ako je $A \sim B$, to znači da postoji bijekcija $f : A \to B$. Ali tada je, prema teoremi 5.19, i $f^{-1} : B \to A$ bijekcija, pa važi i $B \sim A$.

T: Ako je $A \sim B$ i $B \sim C$, tj. ako su $f : A \to B$ i $g : B \to C$ bijekcije, po teoremi 5.20 i $g \circ f : A \to C$ je bijekcija, pa $A \sim C$. □

Dakle, relacija $\sim$ deli sve skupove na klase ekvivalencije. U istoj klasi nalaze se skupovi koji su međusobno ekvipotentni.

Definicija 5.26 *Klasa ekvivalencije skupa A za relaciju ekvipotentnosti $\sim$ naziva se kardinalnost (kardinalni broj) skupa A.*

Kardinalnost skupa A označavamo sa $|A|$ (umesto $[A]_\sim$ kao za druge relacije ekvivalencije). Umesto $A \sim B$ češće se piše $|A| = |B|$ i čita: skupovi A i B su iste kardinalnosti.

Intuitivno, dva skupa su iste kardinalnosti ako imaju isti broj elemenata. Za konačne skupove pitanje da li su dva skupa iste kardinalnosti obično se najlakše rešava prebrojavanjem i upoređivanjem. Npr. skupovi $A = \{1, 2, 3\}$

i $B = \{3, 4, 5\}$ imaju po 3 elementa pa je $|A| = |B|$; nije teško konstruisati ni bijekciju između njih: $f : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \end{pmatrix}$. Međutim, za beskonačne skupove (a i za neke konačne, definisane na složeniji način) to da su iste kardinalnosti proverava sa uspostavljanjem bijekcije između njih.

Definicija 5.27 *Za skupove A i B definišemo $|A| \leq |B|$ (čitamo: skup A ima kardinalnost manju ili jednaku od kardinalnosti skupa B) ako postoji 1-1 funkcija $f : A \to B$. Takođe, $|A| < |B|$ ako $|A| \leq |B|$ ali ne i $|A| = |B|$.*

Primetimo da je relacija $\leq$ definisana nad kardinalnim brojevima. Kada neku relaciju ili funkciju definišemo na nekom količničkom skupu, neophodno je pokazati da je definicija dobra. Šta to znači? Ako je $|A| \leq |B|$ i skup A_1 pripada istoj klasi kao skup A (tj. $|A| = |A_1|$), a skup B_1 istoj klasi kao skup B (tj. $|B| = |B_1|$), da li mora biti i $|A_1| \leq |B_1|$, odnosno da li je definicija relacije $\leq$ nezavisna od izbora predstavnika za klase?

To što je $|A| \leq |B|$ znači da postoji bijekcija $f : A \to B$. Dalje, to što $|A| = |A_1|$ i $|B| = |B_1|$ znači da postoje bijekcije $g : A_1 \to A$ i $h : B \to B_1$. Međutim, kako je prema teoremi 5.14(a) kompozicija 1-1 funkcija takođe 1-1, i $h \circ f \circ g : A_1 \to B_1$ je 1-1 funkcija, pa sledi $|A_1| \leq |B_1|$.

Sledeća teorema daje drugi, ekvivalentan način na koji smo mogli definisati relaciju $\leq$.

Teorema 5.28 *$|A| \leq |B|$ ako i samo ako postoji „na" funkcija $g : B \to A$.*

Dokaz. ($\Rightarrow$) Neka je $|A| \leq |B|$, odnosno postoji 1-1 funkcija $f : A \to B$. Fiksirajmo jedan element $a_0 \in A$ i definišimo funkciju $g : B \to A$ ovako: za svako $b \in B$, ako postoji $a \in A$ takvo da je $f(a) = b$, onda je $g(b) = a$ za neko takvo a; u suprotnom neka je $g(b) = a_0$.

g jeste funkcija jer je f 1-1, pa ni za jedno $b \in B$ ne postoje dva različita elementa koja se slikaju u b. Ova funkcija je „na" jer za svako $a \in A$ važi $g(f(a)) = a$.

($\Leftarrow$) Neka je $g : B \to A$ „na". Definišimo funkciju $f : A \to B$ ovako: za svako $a \in A$, pošto je g „na", postoji bar jedan element $b \in B$ takav da $g(b) = a$; neka je $f(a)$ bilo koji od tih elemenata.

Treba dokazati da je f 1-1. Pretpostavimo suprotno, da je $f(a_1) = f(a_2) = b$ za neki $b \in B$. Ali tada bi b funkcijom g trebalo da se preslikava i u a_1 i u a_2, što je nemoguće. □

U dokazu prethodne teoreme u jednom koraku smo, između nekoliko mogućnosti za $f(a)$, birali jednu. Time smo koristili tzv. aksiomu izbora, jednu od najinteresantnijih i najviše proučavanih aksioma teorije skupova. Mnogo više o njoj moguće je naći u knjizi [6].

Sledeća teorema, čiji dokaz se može naći u [18] ili [6], tvrdi da, ako postoje i 1-1 funkcija i „na" funkcija iz A u B, onda postoji i bijekcija između ta dva skupa.

Teorema 5.29 (Šreder-Bernštajn) *Ako je $|A| \leq |B|$ i $|B| \leq |A|$, onda je $|A| = |B|$.*

Teorema 5.30 *$\leq$ je relacija poretka nad kardinalnim brojevima.*

Dokaz. R: Za svaki skup A imamo 1-1 funkciju $i_A : A \to A$ pa je $|A| \leq |A|$.

AS: Sledi iz teoreme Šreder-Bernštajna.

T: Ako je $|A| \leq |B|$ i $|B| \leq |C|$, odnosno postoje 1-1 funkcije $f : A \to B$ i $g : B \to C$, onda je, prema teoremi 5.14(a), i $g \circ f : A \to C$ 1-1 funkcija, odnosno $|A| \leq |C|$. □

Napomenimo još da se može pokazati da za svaka dva skupa A i B važi $|A| \leq |B|$ ili $|B| \leq |A|$, tj. da je relacija $\leq$ nad kardinalnim brojevima linearno uređenje. Evo i ideje dokaza: izaberimo jedan element a_1 skupa A i jedan element b_1 skupa B. Zatim izaberemo još po jedan element $a_2 \in A$ i $b_2 \in B$, tako da oni budu različiti od prvih izabranih. Ovo nastavljamo sve dok u jednom od skupova ne ponestane elemenata; ako je to recimo skup A, onda je funkcija koja preslikava svaki a_i u b_i (izabran u istom koraku) 1-1 funkcija iz A u B, tj. $|A| \leq |B|$.

5.8 Beskonačnost

U raznim oblastima matematike prirodni brojevi zadaju se na razne načine. Kako su u teoriji skupova jedini objekti s kojima se radi skupovi, i prirodni brojevi se u teoriji skupova definišu kao neki skupovi, i to na sledeći način:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \end{aligned}$$

itd. svaki prirodan broj uvodi se kao skup svih prirodnih brojeva manjih od njega: $n + 1 = \{0, 1, \ldots, n\}$. Tako je svaki prirodan broj n ustvari jedan skup sa tačno n elemenata, pa prirodne brojeve možemo uzeti za predstavnike svojih klasa ekvivalencije za relaciju $\sim$. Stoga umesto $|A| = |n|$ obično pišemo samo $|A| = n$, što znači: skup A ima tačno n elemenata.

Definicija 5.31 *Skup A je konačan ako je $|A| = n$ za neki prirodan broj n; u suprotnom je beskonačan.*

Dokazivanje da je skup konačan u većini slučajeva je jednostavno, konstrukcijom bijekcije iz prethodne definicije. Npr. skup $\{a, b, c, d\}$ je konačan jer je $|A| = 4$, drugim rečima možemo konstruisati bijekciju $f : \begin{pmatrix} 0 & 1 & 2 & 3 \\ a & b & c & d \end{pmatrix}$. Ali na taj način ne možemo dokazati da je skup beskonačan, jer ne možemo isprobati sve funkcije sa svim domenima oblika $\{0, 1, \ldots, n-1\}$. Sledeća teorema je uobičajen način za dokazivanje da je dati skup beskonačan; njen dokaz takođe se može naći u knjizi [18].

Teorema 5.32 *Skup A je beskonačan ako i samo ako postoji bijekcija između A i nekog njegovog pravog podskupa.*

Primer 5.33 *(1) Pokažimo da je skup N beskonačan, tako što ćemo konstruisati bijekciju između njega i njegovog pravog podskupa $N \setminus \{1\}$. To će biti funkcija data sa $f(x) = x + 1$ i lako se proverava da je $f : N \to N \setminus \{1\}$ zaista bijekcija. Ilustrujmo ovu ideju kroz priču o tzv. Hilbertovom hotelu: pretpostavimo da imamo hotel sa beskonačno mnogo soba obeleženih prirodnim brojevima $1, 2, \ldots$ Sve sobe su popunjene ali pojavio*

se još jedan gost. Kako smestiti i njega? Zamolićemo gosta iz sobe 1 *da pređe u sobu* 2*, gosta iz sobe* 2 *da pređe u sobu* 3 *itd. čime će se soba* 1 *osloboditi za novog gosta, ali svi stari gosti su i dalje smešteni.*

(2) Ako obeležimo $N_0 = N \cup \{0\}$*, slično se pokazuje da je* $f : N \to N_0$ *data sa* $f(x) = x - 1$ *bijekcija, pa je i* N_0 *beskonačan. Nije teško dokazati da, opštije, dodavanje ili oduzimanje konačno mnogo elemenata ne može da naruši beskonačnost nekog skupa.*

(3) Konstruišimo sada bijekciju između Z *i* N*, pa kako je* $N \subset Z$*, slediće da je i* Z *beskonačan. To će biti funkcija* $f : Z \to N$ *definisana sa*

$$f(x) = \begin{cases} 2x, & \text{ako je } x > 0 \\ -2x + 1, & \text{inače.} \end{cases}$$

Dakle, ,,taktika" koju koristimo je da pozitivne cele brojeve slikamo u parne prirodne, a ostale u neparne. Na sličan način možemo pokazati i da je, ako sa $2N$ *označimo skup parnih prirodnih brojeva, funkcija* $f : N \to 2N$ *data sa* $f(x) = 2x$ *bijekcija. Ovakva situacija, u kojoj jedan skup ima beskonačno mnogo elemenata koji ne pripadaju drugom a ipak su iste kardinalnosti karakteristična je za beskonačne skupove. Kako bi, dakle, postupio upravnik Hilbertovog hotela iz dela (1) ovog primera kada bi mu se pojavilo beskonačno mnogo novih gostiju odjednom? Zamolio bi gosta iz sobe* 1 *da pređe u sobu* 2*, gosta iz sobe* 2 *da pređe u sobu* 4*, gosta iz sobe* 3 *da pređe u sobu* 6 *itd. Na taj način oslobođeno je beskonačno mnogo soba (sve sa neparnim brojevima) i svi gosti mogu biti smešteni.*

Činjenica koja na prvi pogled zvuči neobično je da uopšte ima više različitih beskonačnosti, odnosno da postoje dva beskonačna skupa koja nisu iste kardinalnosti. To će slediti iz sledeće teoreme.

Teorema 5.34 (Kantor) *Za svaki skup* A *važi* $|A| < |P(A)|$.

Dokaz. Pre svega, lako je videti da $|A| \leq |P(A)|$, jer je funkcija $f : A \to P(A)$ zadata sa $f(a) = \{a\}$ 1-1.

Da bismo dokazali da nije $|A| \geq |P(A)|$ treba, prema teoremi 5.28, pokazati da ne postoji ,,na" funkcija $g : A \to P(A)$ (dakle, ne samo da funkcija f koju smo mi definisali nije ,,na", nego da takva uopšte ne postoji). Pretpostavimo suprotno, da postoji takva ,,na" funkcija g. Definišimo $S = \{a \in A : a \notin g(a)\}$; ova definicija ima smisla jer je, za svaki $a \in A$, $g(a)$ neki podskup skupa A. Kako je g ,,na" i $S \in P(A)$, postoji element $a \in A$ takav da je $g(a) = S$. Ali tada

$$\begin{aligned} a \in S &\sim a \notin g(a) \\ &\sim a \notin S, \end{aligned}$$

što je očigledno nemoguće. □

Definicija 5.35 *Za skup* A *kažemo da je prebrojiv ako je* $|A| = |N|$*. Za beskonačan skup koji nije prebrojiv kažemo da je neprebrojiv.*

Kardinalni broj $|N|$ najmanji je među beskonačnim kardinalnim brojevima. Drugim rečima (videti definiciju 5.27), za svaki beskonačan skup X može se konstruisati 1-1 funkcija $f : N \to X$, odnosno niz $\langle f_n : n \in N \rangle$ različitih elemenata skupa X.

Sada, polazeći od skupa $X_1 = N$, prema Kantorovoj teoremi možemo konstruisati skup $X_2 = P(X_1)$ koji je striktno veće kardinalnosti. Primenjujući još jednom Kantorovu teoremu dobijamo da skup $X_3 = P(X_2)$ ima još veću kardinalnost. Nastavljajući ovaj postupak zaključujemo da postoji beskonačno mnogo ,,različitih beskonačnosti".

Primer 5.36 *Dokažimo da je* $|N| \leq |Q| \leq |Z^2| \leq |N|$*, što će značiti, zbog tranzitivnosti i antisimetričnosti relacije* $\leq$*, da je* $|N| = |Q| = |Z^2|$*, odnosno da su skupovi* Z^2 *i* Q *prebrojivi.*

$|N| \leq |Q|$ *je očigledno, jer je preslikavanje* $i : N \to Q$ *definisano sa* $i(x) = x$ *za sve* $x \in N$ *1-1.*

$|Q| \leq |Z^2|$*: definišimo funkciju* $f : Q \to Z^2$ *ovako: ako je* $\frac{p}{q} \in Q$ *skraćeni razlomak (tj.* $NZD(p,q) = 1$*), onda je* $f(\frac{p}{q}) = (p,q)$*. Ovo preslikavanje je 1-1 jer bi* $f(\frac{p_1}{q_1}) = f(\frac{p_2}{q_2})$ *značilo da je* $(p_1, q_1) = (p_2, q_2)$*, odakle sledi* $p_1 = p_2$ *i* $q_1 = q_2$*, pa i* $\frac{p_1}{q_1} = \frac{p_2}{q_2}$*.*

$|Z^2| = |Z|$*: poređajmo sve parove* $(x, y) \in Z^2$ *u niz na sledeći način:* $(0,0)$*,* $(-1,0)$*,* $(0,-1)$*,* $(0,1)$*,* $(1,0)$*,* $(-2,0)$*,* $(-1,-1)$*,* $(-1,1), \ldots$ *Drugim rečima, u nizu se prvo javljaju parovi* (x, y) *takvi da je zbir* $|x| + |y| = 0$*, zatim oni za koje je* $|x| + |y| = 1$ *itd.; parovi sa istim zbirom koordinata porede se najpre po prvoj koordinati a zatim po drugoj. Sada neka je* $g(x, y)$ *redni broj para* (x, y) *u ovom nizu.* g *je injekcija između skupova* Z^2 *i* N*.*

Konačno, pomenućemo bez dokaza teoremu iz koje (zajedno sa Kantorovom teoremom) sledi da je skup realnih brojeva R neprebrojiv.

Teorema 5.37 $|R| = |P(N)|$.

5.9 Zadaci

1-1 i ,,na" funkcije

1. Neka je $A = \{1,2,3,4\}$, $B = \{1,2,3\}$ i $C = \{1,2,3,4,5\}$. Koje od sledećih funkcija su 1-1, a koje ,,na":

   (a) $f : A \to B$ data sa $f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 3 \end{pmatrix}$;

   (b) $g : A \to C$ data sa $g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 5 \end{pmatrix}$;

   (c) $h : A \to A$ data sa $h : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

2. Koje od sledećih funkcija su 1-1, a koje ,,na":

   (a) $f : R \to R$ definisana sa $f(x) = 2x - 1$;

   (b) $f_1 : Z \to Z$ definisana sa $f(x) = 2x - 1$;

   (c) $g : R \to R$ definisana sa $g(x) = x^2 - 6x - 10$;

   (d) $h : R \to R$ definisana sa $h(x) = \begin{cases} 3x & x < 0 \\ x^3 & x \geq 0 \end{cases}$

   (e) $k : Z^2 \to Z$ definisana sa $k(x, y) = x + y$;

   (f) $k_1 : N^2 \to N$ definisana sa $k_1(x, y) = x + y$;

(g) $NZD : N^2 \to N$;

(h) $NZS : N^2 \to N$;

(i) $m : P(N) \setminus \{\emptyset\} \to N$ definisana sa $m(A) = \min(A)$.

3. Za koje od funkcija iz prethodna dva zadatka postoje inverzne funkcije? Odrediti te inverzne funkcije.

4. Funkcije $f : R \to R$, $g : R \to R^+$ i $h : R^+ \to R^+$ (R^+ je skup pozitivnih realnih brojeva) date su sa $f(x) = x^3$, $g(x) = e^{-x}$ i $h(x) = \frac{1}{x}$. Da li je $h \circ g \circ f : R \to R^+$ bijekcija?

5. Ako je $f : R \to R$ bijekcija, dokazati da je i funkcija $g : R \to R$ definisana sa $g(x) = 2f(x) + 3$ bijekcija.

6. Funkcije $f : N \to N$ i $g : N \to N$ definisane su ovako: $f(n)$ je zbir cifara broja n, a $g(n) = n + 1$.

   (a) Izračunati $g \circ f(999)$ i $f \circ g(999)$.

   (b) Proveriti da li je $g \circ f$ 1-1.

7. Dati su skup pisaca $A = \{andric, pavlovic, pekic, selenic\}$, skup knjiga $B = \{avlija, besnilo, cuprija, ocevi, ubistvo, zid\}$ i skup brojeva $C = \{200, 250, 270, 300, 450, 500\}$, kao i funkcije $f : B \to A$ koja svaku knjigu preslikava u ime njenog pisca:

$$f : \begin{pmatrix} avlija & besnilo & cuprija & ocevi & ubistvo & zid \\ andric & pekic & andric & selenic & selenic & pavlovic \end{pmatrix}$$

   i $g : B \to C$ koja svaku knjigu preslikava u broj stranica:

$$g : \begin{pmatrix} avlija & besnilo & cuprija & ocevi & ubistvo & zid \\ 200 & 500 & 450 & 250 & 270 & 300 \end{pmatrix}$$

   (a) Koja od funkcija f i g ima inverznu funkciju? Obrazložiti i naći tu inverznu funkciju.

   (b) Koja od funkcija $f \circ g$, $f \circ g^{-1}$, $g \circ f$, $f^{-1} \circ g$ je dobro definisana (ima smisla)? Odrediti tu funkciju.

8. Neka su m i n prirodni brojevi i A neki skup od m slova. Reč dužine n nad A je n-torka $x_1x_2 \dots x_n$, gde $x_1, x_2, \dots, x_n \in A$. (Npr. ako je $A = \{a, b, c\}$, reči dužine 2 nad A su *aa,ab,ac,ba,bb,bc,ca,cb* i *cc*.) Neka je B skup svih reči dužine n nad A a funkcija $f : B \to A$ definisana ovako: $f(x_1x_2 \dots x_n) = x_1$. (Npr. za $n = 4$ je $f(abba) = a$.)

   (a) Za koje vrednosti m i n je funkcija f „na”?

   (b) Za koje vrednosti m i n je funkcija f 1-1?

   Odgovore obrazložiti.

9. Dati su skupovi: (1) $A = \{1, 2, 3, 4\}$ i $B = \{1, 2, 3, 4, 5, 6, 7\}$; (2) $A = \{1, 2, 3, 4, 5, 6\}$ i $B = \{1, 2, 3, 4, 5\}$.

   (a) Da li postoji 1-1 funkcija $f : A \to B$?

   (b) Da li je svaka funkcija $f : A \to B$ 1-1?

   (c) Da li postoji „na” funkcija $f : A \to B$?

(d) Da li je svaka funkcija $f : A \to B$ „na"?

10. Dokazati bez primene teoreme 5.18 da za funkciju $f : A \to B$, ako f^{-1} postoji onda i ona mora biti bijekcija.

11. Dokazati bez primene teoreme 5.18 da, ako su $f : A \to B$ i $g : B \to C$ bijekcije, i $g \circ f$ mora biti bijekcija.

12. Ako su $f : A \to B$ i $g : B \times C \to D$ bijekcije, dokazati da je i funkcija $h : A \times C \to D$ data sa $h(a, c) = g(f(a), c)$ bijekcija.

13. Ako su $f : A \to C$ i $g : B \to D$ bijekcije, dokazati da je i $h : C \times B \to A \times D$ data sa $h(x, y) = (f^{-1}(x), g(y))$ bijekcija.

14. Ako su $f : A \to A$ i $g : B \to B$ bijekcije i $A \cap B = \emptyset$, dokazati da je i $h : A \cup B \to A \cup B$ definisana sa $h(x) = \begin{cases} f(x), & \text{ako } x \in A \\ g(x), & \text{ako } x \in B \end{cases}$ bijekcija.

15. Neka su $f : X \to Y$ i $g : Y \to Z$ funkcije. Dokazati da je $g \circ f$ 1-1 ako i samo ako je f 1-1 i

$$(\forall y_1, y_2 \in f[X])(g(y_1) = g(y_2) \Rightarrow y_1 = y_2). \tag{5.4}$$

16. Ako su $f : A \to B, g : B \to C$ i $h : C \to D$ funkcije i $h \circ g \circ f$ bijekcija, koje od funkcija f, g, h moraju biti 1-1, a koje „na"? Dati primere kada ostale ne zadovoljavaju ta svojstva.

17. Ako $f : X \to Y$ i $g : Y \to Z$, i g i $g \circ f$ su bijekcije, pokazati da je i f bijekcija.

18. Ako su $f : A \to B$ i $h : C \to D$ bijekcije i $g : B \to C$ funkcija takva da je $h \circ g \circ f$ bijekcija, dokazati da je i g bijekcija.

19. Kažemo da je $f : A \to A$ „2-1" funkcija ako za svaki element $a \in A$ skup $f^{-1}[\{a\}] = \{x \in A : f(x) = a\}$ ima 1 ili 2 elementa, tj. u svaki element iz A slika se bar jedan, a najviše dva elementa iz A. Dokazati: ako je $f \circ f$ „2-1" funkcija, onda je i f „2-1" funkcija.

20. Za funkciju $f : X \to Y$ kažemo da je *netrivijalna* ako je $|f[X]| > 1$, tj. ako se ne slikaju svi elementi iz X u isti element iz Y. Ako je f „na" a g netrivijalna, dokazati da i $g \circ f$ mora biti netrivijalna.

21. Neka je $A \neq \emptyset$ neki skup i funkcija $f : A \to A^2$ zadata ovako: $f(a) = (a, a)$ za sve $a \in A$. Kakve uslove treba da zadovoljava skup A da bi f bila (a) 1-1; (b) „na"? Obrazložiti.

22. Neka A neprazan skup i preslikavanje $f : P(A)^2 \to P(A)^2$ definisano ovako: $f(X, Y) = (X \cup Y, X \setminus Y)$. Da li je f (a) 1-1; (b) „na"?

23. Neka je $A = \{a, b, c\}$ i $B = \{b, c, d\}$. Ako je $f : P(A) \times P(B) \to \{0, 1, 2, 3\}$ funkcija definisana sa $f(X, Y) = |X \cap Y|$, ispitati da li je ona 1-1, „na", bijekcija.

Funkcije i relacije

24. (a) Ako je $f : A \to B$ funkcija, dokazati da je relacija $\sim$ definisana sa $x \sim y \Leftrightarrow f(x) = f(y)$ relacija ekvivalencije. ($\sim$ se naziva jezgro preslikavanja f.)

(b) Ako je $\sim$ relacija ekvivalencije na skupu A, prirodno preslikavanje $g : A \to A/\sim$ definiše se sa $g(x) = [x]_\sim$. Dokazati da je ono „na".

25. (a) Ako je (A, ρ) parcijalno uređenje, a $f : B \to A$ 1-1 funkcija, pokazati da i (B, σ) mora biti parcijalno uređenje, gde je

$$x\sigma y \Leftrightarrow f(x)\rho f(y)$$

za $x, y \in B$.

(b) Ako je (A, ρ) linearno uređenje, da li i (B, σ) mora biti linearno?

(c) Ako je (B, σ) linearno uređenje, da li i (A, ρ) mora biti linearno?

26. Neka je ρ relacija na skupu A, $f : A \to B$ „na" funkcija a relacija σ na B je definisana formulom

$$b_1\sigma b_2 \Leftrightarrow (\exists a_1, a_2 \in A)(f(a_1) = b_1 \wedge f(a_2) = b_2 \wedge a_1\rho a_2) \tag{5.5}$$

za $b_1, b_2 \in B$.

(a) Ako je (A, ρ) linearno uređenje, da li i (B, σ) mora biti linearno uređenje?

(b) Ako je ρ relacija ekvivalencije na skupu A i važi

$$f(x) = f(y) \Rightarrow x\rho y, \tag{5.6}$$

dokazati da je σ relacija ekvivalencije na B.

27. Neka je $(A, \leq_A)$ linearno uređen, $(B, \leq_B)$ parcijalno uređen skup, a $f : A \to B$ bijekcija koja čuva poredak: $x \leq_A y \Rightarrow f(x) \leq_B f(y)$ za $x, y \in A$. Dokazati da i f^{-1} čuva poredak, tj. $x \leq_B y \Rightarrow f^{-1}(x) \leq_A f^{-1}(y)$ za $x, y \in B$.

28. Na skupu F_N svih funkcija koje slikaju skup N u sebe definisana je relacija ρ: $f\rho g \Leftrightarrow (\forall n \in N)f(n) \leq g(n)$. Dokazati da je ρ relacija poretka i da (F_N, ρ) nije linearno uređenje.

Direktna i inverzna slika

29. Neka je $X = \{1, 2, 3, 4\}$, $Y = \{1, 2, 3, 4, 5\}$, $A = \{1, 2, 3\}$, $B = \{3, 4\}$ i $f : X \to Y$ data sa $f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}$. Odrediti $f[A]$, $f[B]$, $f^{-1}[A]$ i $f^{-1}[B]$.

30. Neka je $g : R \to R$ data sa $g(x) = x^2$. Odrediti $g[R]$, $g[(1, 2)]$, $g^{-1}[[0, 1]]$ i $g^{-1}[(1, 2)]$. (U ovom zadatku $(a, b) = \{x \in R : a < x < b\}$ označava otvoreni interval a ne uređeni par elemenata a i b; slično, $[a, b]$ je zatvoreni interval.)

31. Neka $f : X \to Y$, $g : Y \to Z$, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$. Dokazati:

(a) $f[\emptyset] = \emptyset$ i $f^{-1}[\emptyset] = \emptyset$;

(b) ako $A \subseteq B$ onda $f[A] \subseteq f[B]$;

(c) ako $C \subseteq D$ onda $f^{-1}[C] \subseteq f^{-1}[D]$;

(d) $f[A \cup B] = f[A] \cup f[B]$;

(e) $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;

(f) $f[A \cap B] \subseteq f[A] \cap f[B]$;

(g) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;

(h) $g \circ f[A] = g[f[A]]$;

(i) $(g \circ f)^{-1}[E] = f^{-1}[g^{-1}[E]]$.

32. Neka $f : X \to Y$, $g : Y \to Z$, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$. Dokazati:

(a) $f[A] \setminus f[B] \subseteq f[A \setminus B]$;

(b) $f^{-1}[C \setminus D] = f^{-1}[C] \setminus f^{-1}[D]$;

(c) ako je f 1-1, onda pod (a) važi jednakost;

(d) pokazati primerom da jednakost ne važi uvek pod (a).

33. Ako je $f : X \to Y$ 1-1 funkcija, a A i B su podskupovi skupa X takvi da je $A \cap B = \emptyset$, dokazati da je i $f[A] \cap f[B] = \emptyset$.

34. Neka je $f : X \to Y$ a A i B su podskupovi skupa Y. Dokazati da je $f^{-1}(A \triangle B) = f^{-1}(A) \triangle f^{-1}(B)$.

35. Neka $f : X \to Y$ i $A \subseteq X$.

(a) Dokazati: $A \subseteq f^{-1}[f[A]]$.

(b) Ako je f 1-1, dokazati da pod (a) važi jednakost.

(c) Pokazati primerom da jednakost ne važi uvek.

36. Neka $f : X \to Y$ i $A \subseteq Y$.

(a) Dokazati: $f[f^{-1}[A]] \subseteq A$.

(b) Ako je f „na", dokazati da pod (a) važi jednakost.

(c) Pokazati primerom da jednakost ne važi uvek.

37. Ako je $f : X \to Y$ 1-1 funkcija, dokazati da je i $g : P(X) \to P(Y)$ data sa $g(A) = f[A]$ 1-1 funkcija.

38. Neka je $\pi_1 : R^2 \to R$ prva projekcija (zadata sa $\pi_1(x, y) = x$).

(a) Da li je ona 1-1?

(b) Da li je „na"?

(c) Ako je $A = \{(x, y) : 0 \leq x \leq 1 \leq y \leq 2\}$, naći skup $\pi[A]$.

39. Funkcija $f : R \to R$ definisana je ovako:

(1) $f(x) = \begin{cases} -x + 1, & \text{ako je } x < 0 \\ \frac{1}{x+1}, & \text{ako je } x \geq 0. \end{cases}$

(2) $f(x) = \begin{cases} x, & \text{ako je } x < 0 \\ 0, & \text{ako je } 0 \leq x \leq 1 \\ x^2 - 1, & \text{ako je } x > 1. \end{cases}$

(a) Ispitati da li je f 1-1 i da li je „na".

(b) Da li postoji f^{-1}? Ako postoji naći je.

(c) Odrediti $f[(-1, 1)]$ i $f^{-1}[(-1, 1)]$.

Rekurzija i kardinalnost

40. Funkcija $f : N \to Z$ zadata je rekurzivno: $f(1) = 2$ i $f(n+1) = 2f(n) - 1$ za $n \in N$. Dokazati da je $f(n) = 2^{n-1} + 1$ za sve $n \in N$.

41. Naći opšti izraz za funkciju zadatu rekurzivno:

    (a) $f(0) = 3$ i $f(n+1) = f(n) + 2$ za $n > 0$;

    (b) $g(1) = 2$ i $g(n+1) = 3g(n) + 2$ za $n > 1$.

42. (a) Niz je zadat rekurentnom vezom $a_{n+1} = 3a_n - 2a_{n-1}$ i početnim uslovima $a_0 = 2$, $a_1 = 3$. Dokazati da je $a_n = 2^n + 1$.

    (b) Niz je zadat rekurentnom vezom $a_{n+1} = 4(a_n - a_{n-1})$ i početnim uslovima $a_0 = 0$, $a_1 = 2$. Dokazati da je $a_n = n \cdot 2^n$.

43. Definisati rekurzijom sledeće funkcije:

    (a) $f(n) = n!$;

    (b) $g(n) = n^2$.

    Napisati rekurzivne funkcije u Javi za računanje $f(n)$ i $g(n)$.

44. (a) Dokazati: ako je $|X| = |Y| = n$, $f : X \to Y$ je 1-1 funkcija ako i samo ako je „na".

    (b) Pokazati primerima da to ne važi ako su X i Y beskonačni skupovi iste kardinalnosti.

45. Skup A je konačan, a $f : A \to A$ je bijekcija takva da je $f^{-1} = f$ i nema fiksnih tačaka, tj. ni za jedno $a \in A$ ne važi $f(a) = a$. Dokazati da skup A ima paran broj elemenata.

46. Dokazati:

    (a) $|A \times B| = |B \times A|$;

    (b) $|A \times (B \times C)| = |(A \times B) \times C|$.

47. Neka je $|A| = |C|$ i $|B| = |D|$. Dokazati da je $|A \times B| = |C \times D|$.

48. Dokazati:

    (a) $|R| = |(-\frac{\pi}{2}, \frac{\pi}{2})|$;

    (b) $|(0,1)| = |(a,b)|$ za bilo koje brojeve $a, b \in R$ takve da je $a < b$;

    (c) $|(0,1)| = |[0,1]|$.

Glava 6

Rešenja zadataka

6.1 Uvod

1. (a) Dokažimo traženu jednakost indukcijom po n.

   B.I. Za $n = 1$ ona se svodi na $1^2 = \frac{1\cdot 2\cdot 3}{6}$, što je tačno.

   I.H. Pretpostavimo da je $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ za neko n.

   I.K. Treba pokazati da tvrđenje važi i za broj $n+1$, odnosno da je $1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$. Ali prema I.H. je

$$\begin{aligned}(1^2 + 2^2 + \ldots + n^2) + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(2n^2 + n + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}.\end{aligned}$$

   (Prilikom rastavljanja izraza $2n^2 + 7n + 6$ na oblik $(n+2)(2n+3)$ od pomoći je, naravno, to što znamo šta treba da dobijemo pa ustvari treba samo proveriti da li je $(n+2)(2n+3) = 2n^2 + 7n + 6$. Metode rastavljanja polinoma neće biti razmatrane u ovoj knjizi; zainteresovanog čitaoca upućujemo na knjigu [8].)

   (b) Dokažimo i ovu jednakost indukcijom po n.

   B.I. Za $n = 1$ treba proveriti da li je $1^3 = \left(\frac{1\cdot 2}{2}\right)^2$, što je tačno.

   I.H. Pretpostavimo da je $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ za neko n.

   I.K. Treba pokazati da je $1^3 + 2^3 + \ldots + n^3 + (n+1)^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$. Koristeći I.H. dobijamo

$$(1^3 + 2^3 + \ldots + n^3) + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$$

$$\begin{aligned} &= \frac{(n+1)^2}{4}(n^2+4(n+1)) \\ &= \frac{(n+1)^2}{4}(n+2)^2 \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2. \end{aligned}$$

2. Dokažimo zadatak indukcijom po n.

   B.I. Za $n=1$ je $2^1 > 1$.

   I.H. Pretpostavimo da je $2^n > n$ za neko $n \in N$.

   I.K. Dokažimo da je i $2^{n+1} > n+1$. Množeći nejednakost iz I.H. sa 2 dobijamo $2^{n+1} > 2n$, a očigledno je $2n \geq n+1$ za $n \geq 1$.

3. Dokažimo nejednakost indukcijom po n. Kako ona važi samo za $n \geq 5$, baza indukcije biće nam $n=5$.

   B.I. Za $n=5$ je $2^5 = 32 > 5^2 = 25$.

   I.H. Pretpostavimo da je $2^n > n^2$ za neko $n \geq 5$.

   I.K. Dokažimo da je i $2^{n+1} > (n+1)^2$. Množeći opet nejednakost iz I.H. sa 2 dobijamo $2^{n+1} > 2n^2$, pa treba još proveriti da li je $2n^2 \geq (n+1)^2$. Ova nejednakost se svodi na $n^2 - 2n - 1 \geq 0$. Ispitivanjem znaka ove kvadratne funkcije lako možemo videti da ta nejednakost važi za $n \geq 5$. Dokažimo ipak, vežbe radi, i nju indukcijom po n (što će značiti da je dokazano i glavno tvrđenje zadatka).

   B.I. Za $n=5$ je $5^2 - 2 \cdot 5 - 1 = 14 \geq 0$.

   I.H. Neka je $n^2 - 2n - 1 \geq 0$ za neko $n \geq 5$.

   I.K. Treba još dokazati da je i $(n+1)^2 - 2(n+1) - 1 \geq 0$, odnosno $n^2 - 2 \geq 0$. Ali to očigledno važi za $n \geq 5$.

4. (a) B.I. Za $n=1$ je $8 \mid 3^2 - 1$.

   I.H. Neka $8|(3^{2n}-1)$ za neko n.

   I.K. Dokažimo $8|(3^{2n+2}-1)$. Zapišimo $3^{2n+2} - 1 = 3^2 \cdot 3^{2n} - 1 = 8 \cdot 3^{2n} + (3^{2n} - 1)$. Kako su oba sabirka deljiva sa 8, prema teoremi 1.7 je i $3^{2n+2} - 1$ deljivo sa 8.

   (b) Kako traženi uslov važi i za $n=0$ a to se znatno lakše proverava nego slučaj $n=1$, uzećemo $n=0$ za bazu indukcije.

   B.I. Za $n=0$ važi $17|(3 \cdot 5 + 2)$.

   I.H. Neka važi $17|(3 \cdot 5^{2n+1} + 2^{3n+1})$ za neko n.

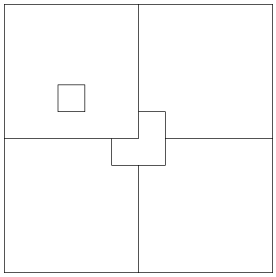
   I.K. Dokažimo da je i $17|(3 \cdot 5^{2n+3} + 2^{3n+4})$. Zapišimo $3 \cdot 5^{2n+3} + 2^{3n+4} = 5^2 \cdot 3 \cdot 5^{2n+1} + 2^3 \cdot 2^{3n+1} = 17 \cdot 3 \cdot 5^{2n+1} + 8(3 \cdot 5^{2n+1} + 2^{3n+1})$. Prvi sabirak je očigledno deljiv sa 17, a drugi po I.H. te je i njihov zbir deljiv sa 17.

5. Pokažimo indukcijom po n da se za svako $n \in N$ tabla $2^n \times 2^n$ iz koje je izbačeno jedno polje može pokriti opisanim figurama. Za $n=7$ dobićemo da to onda važi i za tablu 128×128 (bez jednog polja).

   B.I. Za $n=1$ tabla 2×2 bez jednog polja i sama jeste figura opisana u zadatku.

   I.H. Pretpostavimo da se, za neko $n \in N$, tabla $2^n \times 2^n$ bez jednog polja može pokriti figurama opisanim u zadatku.

I.K. Podelimo tablu $2^{n+1} \times 2^{n+1}$ na četiri kvadrata dimenzija $2^n \times 2^n$. Iz jednog od njih izbačeno je jedno polje pa se on prema I.H. može pokriti opisanim figurama. Postavimo sada jednu figuru u centar table tako da pokriva po jedno polje iz svakog od preostala tri dela (kao na slici). Tako dobijamo još tri kvadrata $2^n \times 2^n$ sa po jednim izbačenim poljem, pa se po I.H. i oni mogu prekriti. Na taj način prekrili smo celu tablu $2^{n+1} \times 2^{n+1}$ bez jednog polja.



6.2 Iskazni račun

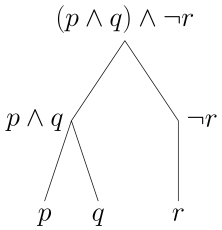
1. (a) Obeležimo sa p iskaz ,,poneo sam kaput", sa q: ,,poneo sam čizme" a sa r: ,,poneo sam kišobran". Zadata rečenica tada se može zapisati kao formula $p \wedge q \wedge \neg r$. (Veznik ,,ali" suštinski označava isto što i veznik ,,i".)

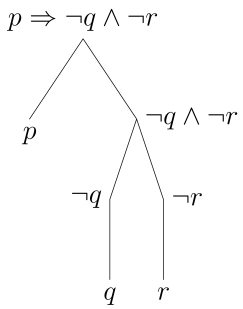
   (b) Obeležimo sa p: ,,padaće kiša", sa q: ,,ići ću na predavanja" a sa r: ,,ići ću na vežbe". Odgovarajuća formula je $p \Rightarrow \neg q \wedge \neg r$.

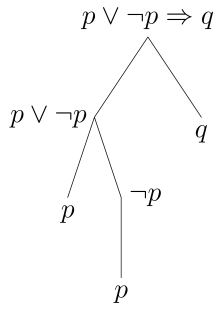
   (c) Ako su p i q kao u prethodnom primeru, dobijamo formulu $p \vee \neg p \Rightarrow q$.

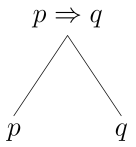
   (d) Obeležimo sa p: ,,ostaćeš" a sa q ,,pazićeš na času". Tada se zadata rečenica može zapisati formulom $p \Rightarrow q$.

   Konstruišimo i drvo podformula za svaku od dobijenih formula. (Prvu od njih posmatraćemo kao $(p \wedge q) \wedge \neg r$; naravno, da smo zagrade rasporedili drugačije dobili bismo nešto drugačije drvo.)









2. (a) Obeležimo $F = (p \Rightarrow q) \Rightarrow (r \wedge \neg s \Rightarrow q)$. Prema pravilima za računanje vrednosti formula je

$$\begin{aligned} v_\alpha(F) &= v_\alpha(p \Rightarrow q) \Rightarrow v_\alpha(r \wedge \neg s \Rightarrow q) \\ &= (v_\alpha(p) \Rightarrow v_\alpha(q)) \Rightarrow (v_\alpha(r \wedge \neg s) \Rightarrow v_\alpha(q)) \\ &= (\alpha(p) \Rightarrow \alpha(q)) \Rightarrow (\alpha(r) \wedge \neg\alpha(s) \Rightarrow \alpha(q)) \\ &= (\top \Rightarrow \top) \Rightarrow (\bot \wedge \neg\top \Rightarrow \top) \\ &= \top \Rightarrow (\bot \Rightarrow \top) \\ &= \top \Rightarrow \top = \top. \end{aligned}$$

Slično je

$$\begin{aligned} v_\beta(F) &= (\beta(p) \Rightarrow \beta(q)) \Rightarrow (\beta(r) \wedge \neg\beta(s) \Rightarrow \beta(q)) \\ &= (\bot \Rightarrow \top) \Rightarrow (\top \wedge \neg\bot \Rightarrow \top) \\ &= \top \Rightarrow (\top \Rightarrow \top) \\ &= \top \Rightarrow \top = \top. \end{aligned}$$

(b) Obeležimo $G = \neg(p \wedge q) \Leftrightarrow \neg r \vee \neg s$.

$$\begin{aligned} v_\alpha(G) &= \neg(\alpha(p) \wedge \alpha(q)) \Leftrightarrow \neg\alpha(r) \vee \neg\alpha(s) \\ &= \neg(\top \wedge \top) \Leftrightarrow \neg\bot \vee \neg\top \\ &= \neg\top \Leftrightarrow \top \vee \bot \\ &= \bot \Leftrightarrow \top = \bot. \end{aligned}$$

$$\begin{aligned} v_\beta(G) &= \neg(\beta(p) \wedge \beta(q)) \Leftrightarrow \neg\beta(r) \vee \neg\beta(s) \\ &= \neg(\bot \wedge \top) \Leftrightarrow \neg\top \vee \neg\bot \\ &= \neg\bot \Leftrightarrow \bot \vee \top \\ &= \top \Leftrightarrow \top = \top. \end{aligned}$$

3. Označimo datu formulu sa F i formirajmo tablicu:

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$	F
$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$

Kako formula F ima vrednost $\top$ u svim valuacijama, sledi da je ona tautologija.

4. (a) Pretpostavimo da data formula (označimo je sa F) nije tautologija. To znači da postoji valuacija α takva da je $v_\alpha(F) = \bot$. Odatle dobijamo da je $v_\alpha(p \wedge (p \Rightarrow q)) = \top$ i $v_\alpha(q) = \bot$. Iz prve jednakosti dalje zaključujemo $v_\alpha(p) = \top$ i $v_\alpha(p \Rightarrow q) = \top$. Međutim, iz $v_\alpha(p) = \top$ i $v_\alpha(q) = \bot$ dobijamo $v_\alpha(p \Rightarrow q) = \bot$, kontradikcija.

   (b) Označimo $G = (p \Leftrightarrow \neg q \vee r) \Rightarrow (\neg p \Rightarrow q)$. Ako G ne bi bila tautologija, postojala bi valuacija α takva da $v_\alpha(G) = \bot$. Odatle sledi $v_\alpha(p \Leftrightarrow \neg q \vee r) = \top$ i $v_\alpha(\neg p \Rightarrow q) = \bot$. Iz drugog uslova dobijamo $\alpha(p) = \alpha(q) = \bot$. To nam, zajedno s prvim uslovom, daje $v_\alpha(\neg q \vee r) = \bot$, što je nemoguće zbog $\alpha(q) = \bot$, kontradikcija.

   (c) Obeležimo $H = ((((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) \Rightarrow r) \Rightarrow t) \Rightarrow ((t \Rightarrow p) \Rightarrow (s \Rightarrow p))$ i pretpostavimo suprotno, da postoji valuacija α takva da $v_\alpha(H) = \bot$. Odatle sledi

$$v_\alpha((((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) \Rightarrow r) \Rightarrow t) = \top \tag{6.1}$$
$$v_\alpha((t \Rightarrow p) \Rightarrow (s \Rightarrow p)) = \bot. \tag{6.2}$$

   Iz uslova (6.2) dobijamo $v_\alpha(t \Rightarrow p) = \top$ i $v_\alpha(s \Rightarrow p) = \bot$, pa je iz drugog od ova dva uslova $\alpha(s) = \top$, $\alpha(p) = \bot$ a zatim iz prvog $\alpha(t) = \bot$. To zajedno sa (6.1) daje $v_\alpha(((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) \Rightarrow r) = \bot$, dakle $v_\alpha((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) = \top$ i $\alpha(r) = \bot$. Kako je $v_\alpha(\neg r \Rightarrow \neg s) = \neg\bot \Rightarrow \neg\top = \bot$, mora biti $v_\alpha(p \Rightarrow q) = \bot$, što je nemoguće jer $\alpha(p) = \bot$. Dakle, H je tautologija.

5. (a) Označimo datu formulu sa F i radimo diskusijom po r.

   1° $\alpha(r) = \top$. Tada je

$$\begin{aligned} v_\alpha(F) &= v_\alpha((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow v_\alpha(p \Rightarrow r) \\ &= v_\alpha(p \Rightarrow q) \wedge v_\alpha(q \Rightarrow r) \Rightarrow v_\alpha(p \Rightarrow r) \\ &= (\alpha(p) \Rightarrow \alpha(q)) \wedge (\alpha(q) \Rightarrow \alpha(r)) \Rightarrow (\alpha(p) \Rightarrow \alpha(r)) \\ &= (\alpha(p) \Rightarrow \alpha(q)) \wedge (\alpha(q) \Rightarrow \top) \Rightarrow (\alpha(p) \Rightarrow \top) \\ &= (\alpha(p) \Rightarrow \alpha(q)) \wedge \top \Rightarrow \top = \top. \end{aligned}$$

   2° $\alpha(r) = \bot$. Tada, slično kao gore, imamo

$$\begin{aligned} v_\alpha(F) &= (\alpha(p) \Rightarrow \alpha(q)) \wedge (\alpha(q) \Rightarrow \bot) \Rightarrow (\alpha(p) \Rightarrow \bot) \\ &= (\alpha(p) \Rightarrow \alpha(q)) \wedge \neg\alpha(q) \Rightarrow \neg\alpha(p). \end{aligned}$$

   Kako u ovom slučaju $v_\alpha(F)$ zavisi i od vrednosti slova p i q, možemo nastaviti diskusijom po p i posmatrati podslučajeve.

   2.1° $\alpha(p) = \top$. Tada $v_\alpha(F) = (\top \Rightarrow \alpha(q)) \wedge \neg\alpha(q) \Rightarrow \bot = \alpha(q) \wedge \neg\alpha(q) \Rightarrow \bot = \bot \Rightarrow \bot = \top$; ovde smo koristili činjenicu da je $v_\alpha(q \wedge \neg q) = \bot$ za obe moguće vrednosti q.

   2.2° $\alpha(p) = \bot$. Tada $v_\alpha(F) = (\bot \Rightarrow \alpha(q)) \wedge \neg\alpha(q) \Rightarrow \top = \top$ bez obzira na vrednost $\alpha(q)$.

   Kako je F tačna u svim valuacijama, ona je tautologija.

   (b) Označimo $G = ((p \wedge q) \vee r \Rightarrow q) \Leftrightarrow ((\neg p \Rightarrow q) \wedge \neg r)$. Sprovodimo diskusiju po slovu q.

1° $\alpha(q) = \top$.

$$\begin{aligned} v_\alpha(G) &= ((\alpha(p) \wedge \alpha(q)) \vee \alpha(r) \Rightarrow \alpha(q)) \Leftrightarrow ((\neg\alpha(p) \Rightarrow \alpha(q)) \wedge \neg\alpha(r)) \\ &= ((\alpha(p) \wedge \top) \vee \alpha(r) \Rightarrow \top) \Leftrightarrow ((\neg\alpha(p) \Rightarrow \top) \wedge \neg\alpha(r)) \\ &= \top \Leftrightarrow (\top \wedge \neg\alpha(r)) \\ &= \top \wedge \neg\alpha(r) = \neg\alpha(r). \end{aligned}$$

Kako vrednost formule zavisi i od vrednosti slova r, treba posmatrati podslučajeve u zavisnosti od $\alpha(r)$. Ali već za $\alpha(r) = \top$ dobijamo $v_\alpha(F) = \neg\top = \bot$, pa F nije tautologija. Nema potrebe da ispitujemo ostale slučajeve.

6. (a) Ako obeležimo $A = p \vee q$, $B = p \Leftrightarrow r$ i $C = s \wedge r$, data formula je

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

Prema teoremi o zameni (teorema 2.14) dovoljno je dokazati da je formula

$$F = (a \Rightarrow (b \Rightarrow c)) \Rightarrow ((a \Rightarrow b) \Rightarrow (a \Rightarrow c))$$

tautologija, pa će i data formula (dobijena od nje zamenom slova a, b, c redom formulama A, B, C) biti tautologija. Dokažimo $\models F$ metodom svođenja na protivrečnost. Dakle, pretpostavimo suprotno, da postoji valuacija α za koju je $v_\alpha(F) = \bot$. Tada je

$$v_\alpha(a \Rightarrow (b \Rightarrow c)) = \top \tag{6.3}$$
$$v_\alpha((a \Rightarrow b) \Rightarrow (a \Rightarrow c)) = \bot. \tag{6.4}$$

Iz (6.4) sledi $v_\alpha(a \Rightarrow b) = \top$ i $v_\alpha(a \Rightarrow c) = \bot$. Iz ovog drugog imamo $\alpha(a) = \top$ i $\alpha(c) = \bot$, a iz prvog zatim $v_\alpha(b) = \top$. Međutim, tada je $v_\alpha(a \Rightarrow (b \Rightarrow c)) = \bot$, što je kontradikcija sa (6.3). Dakle, F je tautologija.

(b) Ako obeležimo $A = p \vee q$, $B = p \Leftrightarrow r$ i $C = s \wedge r$, data formula je

$$F = (A \Leftrightarrow (B \Leftrightarrow C)) \Leftrightarrow ((B \Leftrightarrow A) \Leftrightarrow C).$$

Prema teoremi o zameni dovoljno je dokazati da je formula

$$G = (a \Leftrightarrow (b \Leftrightarrow c)) \Leftrightarrow ((b \Leftrightarrow a) \Leftrightarrow c)$$

tautologija, pa će i F biti tautologija. Dokažimo $\models G$ metodom diskusije po iskaznom slovu b.

1° $\alpha(b) = \top$. Tada je

$$\begin{aligned} v_\alpha(G) &= (\alpha(a) \Leftrightarrow (\top \Leftrightarrow \alpha(c))) \Leftrightarrow ((\top \Leftrightarrow \alpha(a)) \Leftrightarrow \alpha(c)) \\ &= (\alpha(a) \Leftrightarrow \alpha(c)) \Leftrightarrow (\alpha(a) \Leftrightarrow \alpha(c)) = \top. \end{aligned}$$

2° $\alpha(b) = \bot$. Tada

$$\begin{aligned} v_\alpha(G) &= (\alpha(a) \Leftrightarrow (\bot \Leftrightarrow \alpha(c))) \Leftrightarrow ((\bot \Leftrightarrow \alpha(a)) \Leftrightarrow \alpha(c)) \\ &= (\alpha(a) \Leftrightarrow \neg\alpha(c)) \Leftrightarrow (\neg\alpha(a) \Leftrightarrow \alpha(c)). \end{aligned}$$

Sprovedimo u ovom slučaju dalju diskusiju po a.

2.1° $\alpha(a) = \top$. Tada je $v_\alpha(G) = (\top \Leftrightarrow \neg\alpha(c)) \Leftrightarrow (\bot \Leftrightarrow \alpha(c)) = \neg\alpha(c) \Leftrightarrow \neg\alpha(c) = \top$.

2.2° $\alpha(a) = \bot$. Tada je $v_\alpha(G) = (\bot \Leftrightarrow \neg\alpha(c)) \Leftrightarrow (\top \Leftrightarrow \alpha(c)) = \alpha(c) \Leftrightarrow \alpha(c) = \top$.

Kako je $v_\alpha(G) = \top$ za sve valuacije α, G je tautologija.

7. Na osnovu teoreme o zameni dovoljno je dokazati da je formula

$$F = (a \Rightarrow (q \Rightarrow b)) \Rightarrow ((a \Rightarrow q) \Rightarrow (a \Rightarrow b))$$

tautologija, jer se data formula iz nje dobija zamenom redom iskaznih slova a i b formulama $p \wedge r \Leftrightarrow s \vee t$ i $p \vee (s \wedge t)$. Ovo je već dokazano u delu (a) prethodnog zadatka.

8. Koristeći definicije tautologija i kontradikcija imamo:

$$\begin{array}{lll} A \text{ je kontradikcija} & \text{akko} & \text{za svaku valuaciju } \alpha,\ v_\alpha(A) = \bot \\ & \text{akko} & \text{za svaku valuaciju } \alpha,\ v_\alpha(\neg A) = \top \\ & \text{akko} & \neg A \text{ je tautologija.} \end{array}$$

9. (a) Obeležimo iskaze; p: ,,hladno je" i q: ,,počeo je februar". Tada su tražene formule: $p \Rightarrow q$, $\neg q \Rightarrow p$ i q.

(b) Da bismo dokazali da $p \Rightarrow q, \neg q \Rightarrow p \models q$ pretpostavimo suprotno, da za neku valuaciju α važi:

$$v_\alpha(p \Rightarrow q) = \top \tag{6.5}$$
$$v_\alpha(\neg q \Rightarrow p) = \top \tag{6.6}$$
$$v_\alpha(q) = \bot. \tag{6.7}$$

Iz (6.5) i (6.7) sledi da je $\alpha(p) = \bot$, a iz (6.6) i (6.7) da je $\alpha(p) = \top$, kontradikcija.

10. (a) Ako obeležimo sa p iskaz ,,sunce sija", datu rečenicu možemo zapisati kao $\neg\neg p$. Iz nje se može izvesti zaključak ,,sunce sija", a pravilo koje pritom koristimo je $\neg\neg p \models p$. Dokažimo ga: ako za neku valuaciju α važi $v_\alpha(\neg\neg p) = \top$, onda je $v_\alpha(\neg p) = \bot$, pa je $v_\alpha(p) = \top$. (Ovo pravilo sledi i iz ekvivalentnosti $\neg\neg p \sim p$ koju dobijamo iz tablice tautologija iz odeljka 2.3 i teoreme 2.22.)

(b) Uz p kao pod (a) obeležimo sa q iskaz ,,teren je otvoren". Iz datih rečenica možemo izvesti zaključak ,,teren je otvoren" po pravilu $p, p \Rightarrow q \models q$, koje smo već dokazali u primeru 2.17.

(c) Uz oznake iz (b), uvedimo i oznaku r za iskaz ,,naći ćemo se tamo u 10 sati". Zaključak je: ,,ako sunce sija, naći ćemo se tamo u 10 sati" po pravilu $p \Rightarrow q, q \Rightarrow r \models p \Rightarrow r$, takođe dokazanom u primeru 2.17.

(d) Označimo sa p iskaz ,,sunce sija" a sa q: ,,tereni su zatvoreni". Iz datih rečenica možemo izvesti zaključak ,,sunce sija" po pravilu $p \vee q, \neg q \models p$. Dokažimo ovo pravilo. Neka je α valuacija takva da je $v_\alpha(p \vee q) = v_\alpha(\neg q) = \top$. Tada je $\alpha(q) = \bot$ pa mora biti $\alpha(p) = \top$.

11. I način. Pretpostavimo suprotno, da postoji valuacija α za koju je $v_\alpha((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) = \bot$. Tada je $v_\alpha(A \Rightarrow B) = \top$ i $v_\alpha(A \Rightarrow C) = \bot$. Iz drugog uslova dobijamo $v_\alpha(A) = \top$ i $v_\alpha(C) = \bot$. Dalje, iz $v_\alpha(A \Rightarrow B) = \top$

i $v_\alpha(A) = \top$ sledi $v_\alpha(B) = \top$. Konačno, dobijamo $v_\alpha(A \Rightarrow (B \Rightarrow C)) = v_\alpha(A) \Rightarrow (v_\alpha(B) \Rightarrow v_\alpha(C)) = \top \Rightarrow (\top \Rightarrow \bot) = \bot$, kontradikcija.

II način. U zadatku 6 dokazano je da je $\models (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$. Prema posledici 2.20 sledi da je $A \Rightarrow (B \Rightarrow C) \models (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$. To znači da, kad god je formula $A \Rightarrow (B \Rightarrow C)$ tačna, i $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$ je tačna. Dakle, ako je $A \Rightarrow (B \Rightarrow C)$ tautologija, i $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$ mora biti tautologija.

12. (a) Ako sa p označimo iskaz ,,hrana je dobra" a sa q: ,,hrana je jeftina", prva reklama može se predstaviti formulom $p \Rightarrow \neg q$, a druga formulom $q \Rightarrow \neg p$. Proverimo tabličnom metodom da li su ove dve formule ekvivalentne:

p	q	$\neg p$	$\neg q$	$p \Rightarrow \neg q$	$q \Rightarrow \neg p$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$

Kako te formule imaju iste vrednosti u svim valuacijama, one su ekvivalentne. Dakle, dve reklame izražavaju istu stvar.

(b) Uz oznake p: ,,hrana je dobra" i q: ,,hrana je skupa", prva reklama može se sada predstaviti formulom $p \Rightarrow q$, a druga formulom $q \Rightarrow p$. Konstruišimo njihove istinitosne tablice:

p	q	$p \Rightarrow q$	$q \Rightarrow p$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$

Kao što vidimo, postoje valuacije u kojima ove dve formule nemaju iste vrednosti, pa one nisu ekvivalentne.

13. Imamo da je:

$$\begin{aligned} p \vee q \Rightarrow r &\sim \neg(p \vee q) \vee r \sim (\neg p \wedge \neg q) \vee r \\ &\sim (\neg p \vee r) \wedge (\neg q \vee r) \sim (p \Rightarrow r) \wedge (q \Rightarrow r). \end{aligned}$$

14. (a)
$$\begin{aligned} (p \Rightarrow q \wedge \neg q) \Rightarrow \neg p &\sim \neg(\neg p \vee (q \wedge \neg q)) \vee \neg p \\ &\sim (p \wedge \neg(q \wedge \neg q)) \vee \neg p \\ &\sim (p \wedge (\neg q \vee q)) \vee \neg p \\ &\sim (p \vee \neg p) \wedge (\neg q \vee q \vee \neg p). \end{aligned}$$

Kako se u svakoj od dobijene dve klauze u konjunktivnom obliku javlja bar jedno iskazno slovo i sa i bez negacije, polazna formula je tautologija.

(b)
$$\begin{aligned} &((p \vee q) \wedge r) \vee (\neg r \wedge p) \\ \sim\ &(p \vee q \vee \neg r) \wedge (p \vee q) \wedge (r \vee \neg r) \wedge (r \vee p). \end{aligned}$$

U prvoj klauzi ne javlja se nijedno slovo i sa i bez negacije, pa možemo konstruisati valuaciju u kojoj formula nije tačna: $\alpha(p) = \alpha(q) = \bot$, $\alpha(r) = \top$. Dakle, ona nije tautologija.

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

U prvoj od klauza u disjunktivnom obliku ne javlja se isto slovo i sa i bez negacije, pa možemo konstruisati valuaciju u kojoj će formula biti tačna: $\alpha(p) = \alpha(r) = \top$ (vrednost $\alpha(q)$ možemo birati proizvoljno). Dakle, ona je zadovoljiva.

(c)
$$\begin{aligned} & p \wedge (q \vee \neg p) \wedge ((q \Rightarrow \neg p) \vee \neg q) \\ \sim \quad & p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p \vee \neg q). \\ \sim \quad & p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p). \end{aligned}$$

Iz prve klauze (koja se sastoji samo iz jednog literala) vidimo da je za valuaciju $\alpha(p) = \bot$ formula netačna, pa nije tautologija.

$$\begin{aligned} & p \wedge (q \vee \neg p) \wedge ((q \Rightarrow \neg p) \vee \neg q) \\ \sim \quad & p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p) \\ \sim \quad & (p \wedge q \wedge \neg q) \vee (p \wedge q \wedge \neg p) \vee (p \wedge \neg p \wedge \neg q) \vee (p \wedge \neg p \wedge \neg p). \end{aligned}$$

U svakoj klauzi nalazi se bar po jedno slovo i sa i bez negacije, pa formula nije zadovoljiva; dakle ona je kontradikcija.

15. Disjunktivna kanonska forma koja odgovara datoj tablici je $(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r)$, a konjunktivna: $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee \neg r)$.

16. Iz zadatih uslova dobijamo istinitosnu tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$

Odgovarajuća DKF je

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

a KKF:

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

17. (a) Iz zadatih uslova dobijamo istinitosnu tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\bot$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Jedna formula kojoj odgovara ova tablica (dobijena pomoću DKF) je $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$.

(b) Iz zadatih uslova dobijamo istinitosnu tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Jedna formula kojoj odgovara ova tablica je $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$.

18. (a) Obeležimo $G = (F \wedge q \Rightarrow \neg p) \Leftrightarrow ((p \Leftrightarrow \neg q) \Rightarrow F)$. Diskusijom po p izražavamo $v_\alpha(G)$ preko $v_\alpha(F)$:

1° $\alpha(p) = \top$. $v_\alpha(G) = (v_\alpha(F) \wedge \alpha(q) \Rightarrow \neg\top) \Leftrightarrow ((\top \Leftrightarrow \neg\alpha(q)) \Rightarrow v_\alpha(F)) = \neg(v_\alpha(F) \wedge \alpha(q)) \Leftrightarrow (\neg\alpha(q) \Rightarrow v_\alpha(F))$. Nastavljamo diskusijom po q:

1.1°. $\alpha(q) = \top$. $v_\alpha(G) = \neg(v_\alpha(F) \wedge \top) \Leftrightarrow (\neg\top \Rightarrow v_\alpha(F)) = \neg v_\alpha(F) \Leftrightarrow \top = \neg v_\alpha(F)$.

1.2°. $\alpha(q) = \bot$. $v_\alpha(G) = \neg(v_\alpha(F) \wedge \bot) \Leftrightarrow (\neg\bot \Rightarrow v_\alpha(F)) = \neg\bot \Leftrightarrow (\top \Rightarrow v_\alpha(F)) = \top \Leftrightarrow v_\alpha(F) = v_\alpha(F)$.

2° $\alpha(p) = \bot$. $v_\alpha(G) = (v_\alpha(F) \wedge \alpha(q) \Rightarrow \neg\bot) \Leftrightarrow ((\bot \Leftrightarrow \neg\alpha(q)) \Rightarrow v_\alpha(F)) = \top \Leftrightarrow (\alpha(q) \Rightarrow v_\alpha(F)) = \alpha(q) \Rightarrow v_\alpha(F)$. Daljom diskusijom po q dobijamo opet dva podslučaja:

2.1°. $\alpha(q) = \top$. $v_\alpha(G) = \top \Rightarrow v_\alpha(F) = v_\alpha(F)$.

2.2°. $\alpha(q) = \bot$. $v_\alpha(G) = \bot \Rightarrow v_\alpha(F) = \top$.

Sada, u slučajevima u kojima je $v_\alpha(G) = v_\alpha(F)$ (to su 1.2° i 2.1°), da bi G bila tautologija, neophodno je da F ima vrednost $\top$. Slično, kada je $v_\alpha(G) = \neg v_\alpha(F)$ (slučaj 1.1°) moramo staviti $v_\alpha(F) = \bot$. Konačno, u slučaju 2.2° je $v_\alpha(G) = \top$ nezavisno od vrednosti formule F pa tada vrednost za F možemo izabrati proizvoljno. Dakle, za F dobijamo sledeću tablicu:

p	q	F
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top/\bot$

Dakle, postoje dve (do na ekvivalenciju) formule F takve da je G tautologija: jednu dobijamo ako u poslednjoj vrsti tablice izaberemo $\top$ a drugu ako izaberemo $\bot$. KKF za prvu je $\neg p \vee \neg q$ a DKF za drugu: $(p \wedge \neg q) \vee (\neg p \wedge q)$.

(b) Obeležimo datu formulu sa H. Sprovodeći diskusiju po iskaznom slovu r dobijamo dva slučaja:

1° $\alpha(r) = \top$: za ovakve valuacije je $v_\alpha(H) = (\neg\alpha(q) \wedge \alpha(p) \Rightarrow v_\alpha(F)) \Rightarrow (v_\alpha(F) \wedge (\alpha(p) \Rightarrow \alpha(q)))$. Sada opet primenjujemo diskusiju po iskaznom slovu, ovog puta q:

1.1° $\alpha(q) = \top$: sada je $v_\alpha(H) = \top \Rightarrow v_\alpha(F)$, pa za ovakve valuacije mora biti $v_\alpha(F) = \top$;

1.2° $\alpha(q) = \bot$: u ovom slučaju je $v_\alpha(H) = (\alpha(p) \Rightarrow v_\alpha(F)) \Rightarrow (v_\alpha(F) \wedge \neg\alpha(p))$, pa nastavljamo diskusijom po p:

1.2.1° $\alpha(p) = \top$: $v_\alpha(H) = v_\alpha(F) \Rightarrow \bot = \neg v_\alpha(F)$ pa mora važiti $v_\alpha(F) = \bot$;

1.2.2° $\alpha(p) = \bot$: $v_\alpha(H) = \top \Rightarrow v_\alpha(F) = v_\alpha(F)$ i mora biti $v_\alpha(F) = \top$;

2° $\alpha(r) = \bot$: sada dobijamo $v_\alpha(H) = v_\alpha(F) \Rightarrow \bot = \neg v_\alpha(F)$, pa za ovakve valuacije $v_\alpha(F) = \bot$.

Kao pod (a). pomoću dobijenih podataka možemo konstruisati istinitosnu tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$

a zatim i traženu formulu u DNF:

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

19. Obeležimo $G = (p \vee q \Rightarrow F) \Leftrightarrow (F \Rightarrow p \vee r)$.

I način. Radimo diskusijom po p.

1° $\alpha(p) = \top$.

$$\begin{aligned} v_\alpha(G) &= (\top \vee \alpha(q) \Rightarrow v_\alpha(F)) \Leftrightarrow (v_\alpha(F) \Rightarrow \top \wedge \alpha(r)) \\ &= (\top \Rightarrow v_\alpha(F)) \Leftrightarrow (v_\alpha(F) \Rightarrow \alpha(r)) \\ &= v_\alpha(F) \Leftrightarrow (v_\alpha(F) \Rightarrow \alpha(r)). \end{aligned}$$

Posmatramo podslučajeve prema vrednosti r:

1.1° $\alpha(r) = \top$. $v_\alpha(G) = v_\alpha(F) \Leftrightarrow \top = v_\alpha(F)$.

1.2° $\alpha(r) = \bot$. $v_\alpha(G) = v_\alpha(F) \Leftrightarrow \neg v_\alpha(F) = \bot$.

Vidimo da u ovoj valuaciji ni za kakvu vrednost F ne možemo dobiti $v_\alpha(G) = \top$.

II način. Ako bi postojala formula $F(p, q, r)$ takva da zadata formula G bude tautologija, onda bi za svaku valuaciju α moralo biti $v_\alpha(G) = \top$. Koristeći pravila $v_\alpha(F) \Rightarrow \bot = \neg v_\alpha(F)$ i $\top \Rightarrow v_\alpha(F) = v_\alpha(F)$ pokušajmo da pronađemo valuaciju α za koju važi $v_\alpha(p \vee q) = \top$ i $v_\alpha(p \wedge r) = \bot$. Vidimo da je to zadovoljeno npr. za valuaciju $\alpha : \begin{pmatrix} p & q & r \\ \top & \top & \bot \end{pmatrix}$ pa konačno imamo:

$$\begin{aligned} v_\alpha(G) &= (v_\alpha(p \vee q) \Rightarrow v_\alpha(F)) \Leftrightarrow (v_\alpha(F) \Rightarrow v_\alpha(p \wedge r)) \\ &= (\top \Rightarrow v_\alpha(F)) \Leftrightarrow (v_\alpha(F) \Rightarrow \bot) \\ &= v_\alpha(F) \Leftrightarrow \neg v_\alpha(F) = \bot. \end{aligned}$$

Dakle formula F sa traženim osobinama ne postoji.

20. Obeležimo datu formulu sa G. Radićemo diskusijom po iskaznom slovu q.

    1° $\alpha(q) = \top$: tada je $v_\alpha(G) = (v_\alpha(F) \Rightarrow \alpha(p)) \wedge (v_\alpha(F) \wedge \alpha(r) \Leftrightarrow \alpha(r))$. Vidimo da za $\alpha(p) = \bot$ mora biti $v_\alpha(F) = \bot$. Slično, za $\alpha(r) = \top$ mora biti $v_\alpha(F) = \top$. Sledi da u valuaciji $\alpha : \begin{pmatrix} p & q & r \\ \bot & \top & \top \end{pmatrix}$ ne postoji vrednost F za koju je G tačna.

21. Obeležimo zadatu formulu sa G. Radimo diskusijom po q.

    1° $\alpha(q) = \top$. Tada je $v_\alpha(G) = v_\alpha(F) \Leftrightarrow \alpha(p) \vee \alpha(r) \vee (\alpha(p) \wedge \alpha(r)) = v_\alpha(F) \Leftrightarrow \alpha(p) \vee \alpha(r)$ (koristili smo apsorpciju). Dakle, u ovom slučaju $v_\alpha(F) = \alpha(p) \vee \alpha(r)$, tj. F je tačna akko bar jedno od slova p i r ima vrednost $\top$.

    2° $\alpha(q) = \bot$. Tada je $v_\alpha(G) = \alpha(p) \wedge \alpha(r) \wedge v_\alpha(F) \Leftrightarrow \alpha(r) \wedge \alpha(p)$.

    2.1° Ako je $\alpha(p) = \top$, onda $v_\alpha(G) = \alpha(r) \wedge v_\alpha(F) \Leftrightarrow \alpha(r)$, pa za $\alpha(r) = \top$ mora biti $v_\alpha(F) = \top$, a za $\alpha(r) = \bot$ $v_\alpha(F)$ je proizvoljno.

    2.2° Ako je $\alpha(p) = \bot$, uvek je $v_\alpha(G) = \top$, pa je $v_\alpha(F)$ opet proizvoljno.

    Popunjavamo istinitosnu tablicu za F:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top/\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top/\bot$
$\bot$	$\bot$	$\bot$	$\top/\bot$

    Kako nam je dovoljno samo jedno rešenje, izaberimo kombinaciju koja će nam dati najjednostavnije:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$

    Dakle, jedna od formula koje zadovoljavaju dati uslov je $F = p \vee \neg q \vee r$.

22. Obeležimo datu formulu sa G. Radićemo diskusijom po iskaznom slovu q:

    1° $\alpha(q) = \top$: tada $v_\alpha(G) = v_\alpha(F) \wedge v_\alpha(r) \Rightarrow (v_\alpha(p) \Rightarrow v_\alpha(r))$. Nastavljamo diskusijom po r:

    1.1° $\alpha(r) = \top$: tada $v_\alpha(G) = \top$, pa $v_\alpha(F)$ može biti bilo $\top$ bilo $\bot$;

    1.2° $\alpha(r) = \bot$: opet $v_\alpha(G) = \top$ bez obzira na $v_\alpha(F)$;

    2° $\alpha(q) = \bot$: tada $v_\alpha(G) = (v_\alpha(F) \Rightarrow (v_\alpha(p) \Rightarrow v_\alpha(r))) \wedge (v_\alpha(F) \wedge \neg v_\alpha(r) \Rightarrow \neg v_\alpha(p) \wedge \neg v_\alpha(r))$. Nastavimo još jednom diskusijom po r:

2.1° $\alpha(r) = \top$: još jednom je $v_\alpha(G) = \top$ bez obzira na $v_\alpha(F)$, pa je $v_\alpha(F)$ proizvoljno;

2.2° $\alpha(r) = \bot$: sada $v_\alpha(G) = (v_\alpha(F) \Rightarrow \neg v_\alpha(p)) \wedge (v_\alpha(F) \Rightarrow \neg v_\alpha(p)) = v_\alpha(F) \Rightarrow \neg v_\alpha(p)$. Za $\alpha(p) = \top$ dobijamo $v_\alpha(G) = \neg v_\alpha(F)$, tj. $v_\alpha(F) = \bot$, a za $\alpha(p) = \bot$ je $v_\alpha(G) = \top$ bez obzira na $v_\alpha(F)$.

Sve u svemu, dobijamo tablicu

p	q	r	F
$\top$	$\top$	$\top$	$\top/\bot$
$\top$	$\top$	$\bot$	$\top/\bot$
$\top$	$\bot$	$\top$	$\top/\bot$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top/\bot$
$\bot$	$\top$	$\bot$	$\top/\bot$
$\bot$	$\bot$	$\top$	$\top/\bot$
$\bot$	$\bot$	$\bot$	$\top/\bot$

Vidimo da postoji $2^7 = 128$ formula do na ekvivalenciju koje zadovoljavaju dati uslov. Evo dve najjednostavnije (dobijene redom pomoću DKF i KKF): $F_1(p,q,r) = p \wedge q \wedge r$ i $F_2(p,q,r) = \neg p \vee q \vee r$. (Za F_1 uzeli smo da je samo $F(\top,\top,\top) = \top$, a u ostalim valuacijama vrednost $v_\alpha(F) = \bot$, a za F_2 da je samo $F(\top,\bot,\bot) = \bot$, a u svim ostalim slučajevima $v_\alpha(F) = \top$.)

23. Obeležimo datu formulu sa G. Radimo diskusijom po iskaznom slovu p.

1° Ako je $\alpha(p) = \top$, onda je $v_\alpha(G) = (v_\alpha(F) \Rightarrow \top \vee \alpha(q)) \wedge (v_\alpha(F) \Rightarrow \top \vee \alpha(r)) \wedge (\top \Rightarrow v_\alpha(F) \vee \top) = \top \wedge \top \wedge \top = \top$, dakle G je tačna nezavisno od F.

2° Ako je $\alpha(p) = \bot$, onda je $v_\alpha(G) = (v_\alpha(F) \Rightarrow \bot \vee \alpha(q)) \wedge (v_\alpha(F) \Rightarrow \bot \vee \alpha(r)) \wedge (\bot \Rightarrow v_\alpha(F) \vee \bot) = (v_\alpha(F) \Rightarrow \alpha(q)) \wedge (v_\alpha(F) \Rightarrow \alpha(r)) \wedge \top = (v_\alpha(F) \Rightarrow \alpha(q)) \wedge (v_\alpha(F) \Rightarrow \alpha(r))$. Ako bar jedno od iskaznih slova q i r ima vrednost $\bot$ (npr. $\alpha(q) = \bot$) važi $v_\alpha(G) = (v_\alpha(F) \Rightarrow \bot) \wedge (v_\alpha(F) \Rightarrow \alpha(r)) = \neg v_\alpha(F) \wedge (v_\alpha(F) \Rightarrow \alpha(r))$, pa mora biti $v_\alpha(F) = \bot$. U suprotnom, ako je $\alpha(q) = \alpha(r) = \top$, imamo $v_\alpha(G) = (v_\alpha(F) \Rightarrow \top) \wedge (v_\alpha(F) \Rightarrow \top) = \top \wedge \top = \top$, ponovo nezavisno od F. Dakle, dobijamo tablicu

p	q	r	G	F
$\top$	$\top$	$\top$	$\top$	$\top/\bot$
$\top$	$\top$	$\bot$	$\top$	$\top/\bot$
$\top$	$\bot$	$\top$	$\top$	$\top/\bot$
$\top$	$\bot$	$\bot$	$\top$	$\top/\bot$
$\bot$	$\top$	$\top$	$\top$	$\top/\bot$
$\bot$	$\top$	$\bot$	$\neg F$	$\bot$
$\bot$	$\bot$	$\top$	$\neg F$	$\bot$
$\bot$	$\bot$	$\bot$	$\neg F$	$\bot$

Pošto za 5 valuacija imamo po dve mogućnosti za vrednost F, ukupno imamo $2^5 = 32$ formula F (do na ekvivalenciju) za koje je G tautologija. Neke od njih su (u DKF): $F_1 = p \wedge q \wedge r$, $F_2 = p \wedge q \wedge \neg r$ i $F_3 = p \wedge \neg q \wedge r$.

24. Obeležimo $G = (F \Leftrightarrow p \wedge q) \Rightarrow (r \wedge F)$. Radimo diskusijom po r:

1° $\alpha(r) = \top$. Tada je $v_\alpha(G) = (v_\alpha(F) \Leftrightarrow \alpha(p) \wedge \alpha(q)) \Rightarrow v_\alpha(F)$. Za valuacije u kojima je $\alpha(p) \wedge \alpha(q) = \top$, odnosno $\alpha(p) = \alpha(q) = \top$ imamo

$v_\alpha(G) = v_\alpha(F) \Rightarrow v_\alpha(F) = \top$, pa F može imati proizvoljnu vrednost. Ako bar jedno od slova p i q ima vrednost $\bot$, tada je $v_\alpha(G) = \neg v_\alpha(F) \Rightarrow v_\alpha(F) = v_\alpha(F)$, pa mora biti $v_\alpha(F) = \top$.

2° $\alpha(r) = \bot$. Tada je $v_\alpha(G) = (v_\alpha(F) \Leftrightarrow \alpha(p) \wedge \alpha(q)) \Rightarrow \bot = \neg(v_\alpha(F) \Leftrightarrow \alpha(p) \wedge \alpha(q))$, pa mora biti $v_\alpha(F) = \neg(\alpha(p) \wedge \alpha(q))$.

Tako dobijamo tablicu za F:

p	q	r	F
$\top$	$\top$	$\top$	$\top/\bot$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$

Jedna formula koja sadrži samo veznike $\neg$ i $\vee$ (dobijena pomoću KNF) je $F = \neg p \vee \neg q \vee r$.

Napomena. U opštem slučaju, ako se traži formula u kojoj figurišu samo veznici $\vee$ i $\neg$, možemo konstruisati bilo KKF bilo DKF, pa eliminisati veznik $\wedge$ (videti odeljak o bazama).

25. Obeležimo $G = p \Rightarrow r$ i $H = (q \Rightarrow r) \Rightarrow (p \vee F \Rightarrow r)$.

I rešenje. Formulu F treba konstruisati tako da za sve valuacije α u kojima je $v_\alpha(G) = \top$ bude i $v_\alpha(H) = \top$. Sprovodimo diskusiju po iskaznom slovu r:

1° $\alpha(r) = \top$. U ovom slučaju je $v_\alpha(G) = \alpha(p) \Rightarrow \top = \top$ i $v_\alpha(H) = (\alpha(q) \Rightarrow \top) \Rightarrow (\alpha(p) \vee v_\alpha(F) \Rightarrow \top) = \top \Rightarrow \top = \top$, pa je traženi uslov ispunjen za sve formule F.

2° $\alpha(r) = \bot$. Sada je $v_\alpha(G) = \alpha(p) \Rightarrow \bot = \neg\alpha(p)$ i $v_\alpha(H) = (\alpha(q) \Rightarrow \bot) \Rightarrow (\alpha(p) \vee v_\alpha(F) \Rightarrow \bot) = \neg\alpha(q) \Rightarrow \neg(\alpha(p) \vee v_\alpha(F))$. $v_\alpha(G) = \top$ važi samo ako je $\alpha(p) = \bot$, i u tom slučaju treba obezbediti da bude $v_\alpha(H) = \top$. Za $\alpha(q) = \top$ tada imamo $v_\alpha(H) = \bot \Rightarrow \neg v_\alpha(F) = \top$ bez obzira na vrednost formule F, a za $\alpha(q) = \bot$ je $v_\alpha(H) = \top \Rightarrow \neg v_\alpha(F) = \neg v_\alpha(F)$ pa mora biti $v_\alpha(F) = \bot$. Tako dobijamo tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\top/\bot$
$\top$	$\top$	$\bot$	$\top/\bot$
$\top$	$\bot$	$\top$	$\top/\bot$
$\top$	$\bot$	$\bot$	$\top/\bot$
$\bot$	$\top$	$\top$	$\top/\bot$
$\bot$	$\top$	$\bot$	$\top/\bot$
$\bot$	$\bot$	$\top$	$\top/\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Dakle, jednu moguću formulu dobijamo ako u prvih 7 vrsta stavimo $\top$ kao vrednost za F, pa pomoću KKF dobijamo

$$F_1 = p \vee q \vee r,$$

a drugu ako recimo stavimo vrednost $\top$ u prvoj vrsti a $\bot$ u svim ostalim, pa nam DKF daje

$$F_2 = p \wedge q \wedge r.$$

II rešenje. Prema poznatoj teoremi $G \models H$ važi ako i samo ako je $\models G \Rightarrow H$. Obeležimo $A = G \Rightarrow H$ i dalje nastavljamo, analogno prvom rešenju, diskusijom po r:

1° $\alpha(r) = \top$. $v_\alpha(A) = (\alpha(p) \Rightarrow \top) \Rightarrow ((\alpha(q) \Rightarrow \top) \Rightarrow (\alpha(p) \vee v_\alpha(F) \Rightarrow \top)) = \top \Rightarrow (\top \Rightarrow \top) = \top$.

2° $\alpha(r) = \bot$. $v_\alpha(A) = (\alpha(p) \Rightarrow \bot) \Rightarrow ((\alpha(q) \Rightarrow \bot) \Rightarrow (\alpha(p) \vee v_\alpha(F) \Rightarrow \bot)) = \neg\alpha(p) \Rightarrow (\neg\alpha(q) \Rightarrow \neg(\alpha(p) \vee v_\alpha(F)))$. Razmatramo podslučajeve:

2.1° $\alpha(p) = \top$. $v_\alpha(A) = \bot \Rightarrow (\neg\alpha(q) \Rightarrow \neg(\top \vee v_\alpha(F))) = \top$.

2.2° $\alpha(p) = \bot$. $v_\alpha(A) = \top \Rightarrow (\neg\alpha(q) \Rightarrow \neg(\bot \vee v_\alpha(F))) = \neg\alpha(q) \Rightarrow \neg v_\alpha(F)$. Konačno, razmatramo i vrednosti za q.

$2.2.1^\circ$ $\alpha(q) = \top$. $v_\alpha(A) = \bot \Rightarrow \neg v_\alpha(F) = \top$.

$2.2.2^\circ$ $\alpha(q) = \bot$. $v_\alpha(A) = \top \Rightarrow \neg v_\alpha(F) = \neg v_\alpha(F)$, pa u ovom slučaju mora biti $v_\alpha(F) = \bot$.

Konačno, dobijamo tabelu kao u I rešenju i iz nje tražene formule.

26. Obeležimo $G = (p \wedge q \wedge F) \vee \neg(\neg p \Rightarrow F)$ i $H = ((p \Leftrightarrow q) \vee F) \wedge (F \Rightarrow \neg p)$. Radimo diskusijom po p.

1° $\alpha(p) = \top$. $v_\alpha(G) = (\alpha(q) \wedge v_\alpha(F)) \vee \bot = \alpha(q) \wedge v_\alpha(F)$. S druge strane je $v_\alpha(H) = (\alpha(q) \vee v_\alpha(F)) \wedge \neg v_\alpha(F) = (\alpha(q) \wedge \neg v_\alpha(F)) \vee (v_\alpha(F) \wedge \neg v_\alpha(F)) = \alpha(q) \wedge \neg v_\alpha(F)$. Za $\alpha(q) = \bot$ je $v_\alpha(H) = \bot$ bez obzira na vrednost F.

Dakle, H nije tautologija ni za jednu formulu F. (Nema potrebe da ispitujemo slučaj $\alpha(p) = \bot$.)

27. I rešenje. Prema teoremi 2.22 zadati uslovi su ekvivalentni s tim da formule $G = (p \Rightarrow F) \Leftrightarrow (q \Rightarrow \neg p \vee r)$ i $H = (F \Rightarrow p) \Leftrightarrow ((r \Rightarrow q) \Rightarrow p)$ budu tautologije. Sprovedimo diskusiju po iskaznom slovu p.

1° $\alpha(p) = \top$. Tada $v_\alpha(G) = v_\alpha(F) \Leftrightarrow (\alpha(q) \Rightarrow \alpha(r))$ i $v_\alpha(H) = \top \Leftrightarrow \top = \top$, pa mora biti $v_\alpha(F) = \alpha(q) \Rightarrow \alpha(r)$.

2° $\alpha(p) = \bot$. Tada je $v_\alpha(G) = \top \Leftrightarrow (\alpha(q) \Rightarrow \top) = \top$ i $v_\alpha(H) = \neg v_\alpha(F) \Leftrightarrow \neg(\alpha(r) \Rightarrow \alpha(q))$, pa mora biti $v_\alpha(F) = \alpha(r) \Rightarrow \alpha(q)$. Dobijamo sledeću tablicu:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$

Dakle, $F = (\neg p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r)$ je jedina (do na ekvivalenciju) formula koja zadovoljava dati uslov.

II rešenje. Pomoću zadatih uslova popunjavamo sledeću tablicu:

p	q	r	$p \Rightarrow F$	$\neg p \Rightarrow \neg F$	F
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$

Pritom četvrtu kolonu popunjavamo koristeći prvi od datih uslova (računajući $v_\alpha(q \Rightarrow \neg p \vee r)$), a petu koristeći drugi (računajući $v_\alpha((r \Rightarrow q) \Rightarrow p)$). Šesta kolona popunjava se pomoću sledećih razmatranja:

-iz $v_\alpha(p) = \top$ i $v_\alpha(p \Rightarrow F) = \top$ sledi $v_\alpha(F) = \top$;

-iz $v_\alpha(p) = \top$ i $v_\alpha(p \Rightarrow F) = \bot$ sledi $v_\alpha(F) = \bot$;

-iz $v_\alpha(p) = \bot$ i $v_\alpha(\neg p \Rightarrow \neg F) = \top$ sledi $v_\alpha(F) = \bot$;

-iz $v_\alpha(p) = \bot$ i $v_\alpha(\neg p \Rightarrow \neg F) = \bot$ sledi $v_\alpha(F) = \top$.

Pomoću KKF sada dobijamo jedino rešenje (do na ekvivalenciju): $F = (\neg p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r)$.

28. Obeležimo datu formulu sa H. Radimo diskusijom po r:

1° $\alpha(r) = \top$. Tada je $v_\alpha(H) = \alpha(p) \vee \alpha(q) \Rightarrow (\top \wedge v_\alpha(F)) \vee (\bot \wedge v_\alpha(G)) = \alpha(p) \vee \alpha(q) \Rightarrow v_\alpha(F)$. To znači da je H tačna ako u svim ovakvim valuacijama u kojima bar jedno od slova p i q ima vrednost $\top$ i F ima vrednost $\top$.

2° $\alpha(r) = \bot$. Tada je $v_\alpha(H) = \alpha(p) \vee \alpha(q) \Rightarrow (\bot \wedge v_\alpha(F)) \vee (\top \wedge v_\alpha(G)) = \alpha(p) \vee \alpha(q) \Rightarrow v_\alpha(G)$. To znači da je H tačna ako u svim ovakvim valuacijama u kojima bar jedno od slova p i q ima vrednost $\top$ i G ima vrednost $\top$.

Dakle, takve formule F i G postoje. Najjednostavniji način da ih konstruišemo je da obe budu tautologije, npr. $F = p \vee \neg p$ i $G = q \vee \neg q$.

29. Obeležimo datu formulu sa A. Na uobičajeni način popunjavamo tablicu:

p	q	A
$\top$	$\top$	F
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\neg F$

pri čemu prve dve kolone označavaju razne valuacije za p i q, a treća vrednost $v_\alpha(A)$ izraženu preko $v_\alpha(F)$ za te valuacije. Dakle, treba da važi $F(\top, \top) = \bot$ ili $F(\bot, \bot) = \top$ da A ne bi bila tautologija. Mogućnosti da se popuni tablica su sledeće:

p	q	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_10	F_{11}	F_{12}
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

Njima odgovaraju sledeće formule (dobijene pomoću DKF):

$$\begin{aligned}
F_1 &= (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)\\
F_2 &= (p \wedge \neg q) \vee (\neg p \wedge q)\\
F_3 &= (p \wedge \neg q) \vee (\neg p \wedge \neg q)\\
F_4 &= (\neg p \wedge q) \vee (\neg p \wedge \neg q)\\
F_5 &= p \wedge \neg q\\
F_6 &= \neg p \wedge q\\
F_7 &= \neg p \wedge \neg q\\
F_8 &= \neg p \wedge p \text{ (kontradikcija)}\\
F_9 &= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)\\
F_{10} &= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)\\
F_{11} &= (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)\\
F_{12} &= (p \wedge q) \vee (\neg p \wedge \neg q).
\end{aligned}$$

30. (a) Direktno se proverava (npr. crtanjem istinitosne tablice) da je $\neg p \sim p \Rightarrow B(p)$.

    (b) $\neg p \sim p \veebar T(p)$.

    (c) Koristeći, između ostalog, distributivnost, apsorpciju i De Morganove zakone imamo:

$$\begin{aligned}
p \vee q &\sim (p \vee q) \wedge (q \vee \neg q)\\
&\sim (p \wedge q) \vee (p \wedge \neg q) \vee q \vee (q \wedge \neg q)\\
&\sim (p \wedge \neg q) \vee q\\
&\sim (\neg\neg p \wedge \neg q) \vee q\\
&\sim \neg(\neg p \vee q) \vee q\\
&\sim \neg(p \Rightarrow q) \vee q\\
&\sim (p \Rightarrow q) \Rightarrow q.
\end{aligned}$$

31. (a) Prema prethodnom zadatku $\neg$ možemo izraziti preko date dve operacije. Kako je $\{\Rightarrow, \neg\}$ baza, sledi da je i $\{\Rightarrow, B\}$ baza.

    (b) Iz prethodnog zadatka ponovo sledi da pomoću datih operacija možemo dobiti negaciju. Pošto je $\{\vee, \neg\}$ baza, i dati skup je baza.

32. Važi: $\neg p \sim T(p) \not\Rightarrow p$, pa se $\neg$ može izraziti preko T i $\not\Rightarrow$. Sada je lako izraziti i $\Rightarrow$:

$$p \Rightarrow q \sim \neg(p \not\Rightarrow q) \sim T(p) \not\Rightarrow (p \not\Rightarrow q)$$

    pa, kako je $\{\neg, \Rightarrow\}$ baza, sledi da je i $\{T, \not\Rightarrow\}$ baza.

33. $x \Rightarrow (x \not\Rightarrow x) \sim x \Rightarrow B(x) \sim \neg x$, pa se negacija može izraziti preko elemenata datog skupa. Kako je $\{\neg, \Rightarrow\}$ baza iskazne algebre, to je i $\{\Rightarrow, \not\Rightarrow\}$.

    $x \not\Rightarrow y \sim \neg(x \Rightarrow y) \sim x \wedge \neg y$ odakle $x \wedge y \sim x \not\Rightarrow \neg y \sim x \not\Rightarrow (y \Rightarrow (y \not\Rightarrow y))$ – izrazili smo $\wedge$ preko date baze. Takođe, $x \uparrow y \sim \neg(x \wedge y) \sim x \Rightarrow \neg y \sim x \Rightarrow (y \Rightarrow (y \not\Rightarrow y))$.

34. Direktno se proverava da je $p * q \sim \neg p \wedge q$, pa je $p \wedge q \sim \neg\neg p \wedge q \sim \neg p * q$. Kako je $\{\neg, \wedge\}$ baza i $\wedge$ se može izraziti preko $\neg$ i $*$, i $\{\neg, *\}$ je baza.

35. Analogno teoremi 2.37 možemo pokazati da sve operacije iz datog skupa očuvavaju $\top$ (tj. za $* \in \{\wedge, \vee, \pi_1, \pi_2\}$ važi $\top * \top = \top$) pa kao u teoremi 2.38 zaključujemo da se preko njih ne može izraziti negacija. Dakle, dati skup nije baza.

36. Primetimo da je $p \Rightarrow q \sim q * p$, pa kako je $\{\Rightarrow, \neg\}$ baza iskazne algebre, sledi da je to i $\{*, \neg\}$. S druge strane, i $*$ i $\Leftrightarrow$ očuvavaju $\top$, pa se postupkom opisanim u teoremi 2.38 pokazuje da se preko njih ne može izraziti $\neg$.

37. Neka je α valuacija takva da je $\alpha(p) = \bot$. Dokaz sprovodimo indukcijom po broju veznika $\wedge$ i $\vee$ u formuli F.

    B.I. $v(F) = 0$. Tada $F = p$, pa je $v_\alpha(F) = \bot$.

    I.H. Neka tvrđenje važi za sve formule sa manje od n veznika koji su svi $\wedge$ i $\vee$.

    I.K. Neka je $v(F) = n$. Imamo dva slučaja. 1° $F = G \wedge H$. Svaka od formula G i H ima manje od n veznika pa za njih važi indukcijska hipoteza, odakle dobijamo $v_\alpha(G) = v_\alpha(H) = \bot$. Sledi da je i $v_\alpha(F) = v_\alpha(G) \wedge v_\alpha(H) = \bot \wedge \bot = \bot$. 2° $F = G \vee H$ - analogno slučaju 1°.

38. Prema teoremi 2.39 svaka formula u kojoj se javljaju samo veznici $\wedge$ i $\vee$ očuvava $\bot$. Pretpostavimo da se $\Rightarrow$ može izraziti preko $\wedge$ i $\vee$: $p \Rightarrow q \sim A(p, q)$, gde A sadrži samo veznike $\wedge$ i $\vee$. Za valuaciju α takvu da je $\alpha(p) = \alpha(q) = \bot$ je, zbog očuvavanja $\bot$, $v_\alpha(A) = \bot$, a s druge strane $v_\alpha(p \Rightarrow q) = \top$, kontradikcija.

39. Analogno teoremi 2.39 možemo dokazati da svaka formula $F(p)$ u kojoj se javljaju samo veznici $\not\Rightarrow$ i B očuvava $\bot$. Pokažimo da se $\neg$ ne može izraziti preko $\not\Rightarrow$ i B. Pretpostavimo da može, tj. da je $\neg p \sim F(p)$ za neku formulu F koja sadrži samo $\not\Rightarrow$ i B. Ali za valuaciju α takvu da je $\alpha(p) = \bot$ imamo $v_\alpha(\neg p) = \top$ a zbog očuvavanja $\bot$ je $v_\alpha(F) = \bot$, kontradikcija.

40. Analogno teoremi 2.39 svaka formula $A(p)$ u kojoj se javljaju samo veznici $\wedge$ i B i iskazno slovo p očuvava $\bot$. Stoga, ako bi $\{\wedge, B\}$ bila baza, onda bi se negacija mogla prikazati pomoću $\wedge$ i B: $\neg p \sim A(p)$ za neku formulu A koja sadrži samo $\wedge$ i B. Za valuaciju α takvu da je $\alpha(p) = \bot$ bi važilo $v_\alpha(A) = \bot$ i $v_\alpha(\neg p) = \top$ što je nemoguće pa $\{\wedge, B\}$ nije baza.

41. Iz tablice možemo zaključiti da je $p * q \sim q$ i $p \& q \sim \neg p$. Dakle, oba veznika su u suštini unarna, pa ćemo dokazati da se pomoću njih može izraziti samo jedan mali skup operacija iskazne algebre. Konkretno, dokažimo da je svaka formula $F(p, q)$ u kojoj se pojavljuju samo ova dva veznika ekvivalentna sa nekom od sledećih: p, q, $\neg p$ ili $\neg q$. Dokaz sprovodimo indukcijom po složenosti formule F:

    B.I. $v(F) = 0$. Tada je $F = p$ ili $F = q$, pa tvrđenje važi.

    I.H. Pretpostavimo da tvrđenje važi za sve formule sa manje od n veznika $*$ i $\&$.

    I.K. Neka je $v(F) = n$. Imamo dva slučaja:

    1° $F = G * H$, gde su G i H formule sa manje od n veznika. Tada je $F \sim H$, pa kako je H po indukcijskoj hipotezi ekvivalentna nekoj od formula $p, q, \neg p$ ili $\neg q$, isto važi i za F.

    2° $F = G \& H$. U ovom slučaju je $F \sim \neg G$, pa ponovo primenjujući indukcijsku hipotezu dobijamo da je G ekvivalentna nekoj od formula

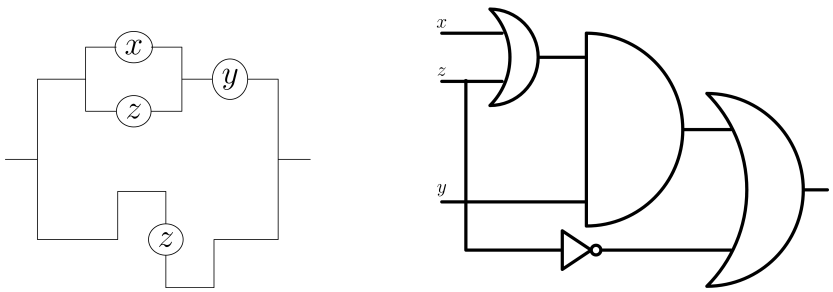
$p, q, \neg p$ ili $\neg q$, odakle sledi da je F ekvivalentno nekoj od formula $\neg p, \neg q, p$ ili q redom.

Dakle, nijedna od operacija $\wedge, \vee, \Rightarrow, \Leftrightarrow \ldots$ ne može se izraziti preko date dve operacije.

42. (a) Transformišimo najpre formulu: $(x \vee y) \wedge (\neg x \vee y) \sim (x \wedge \neg x) \vee y \sim y$. Dakle, tražena kola su:

(Za logičko kolo nije potreban nijedan sklop; ulaz se samo prosledi na izlaz.)

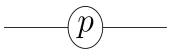
(b) Kako je $(x \wedge y) \vee (y \wedge z) \vee \neg z \sim ((x \vee z) \wedge y) \vee \neg z$, tražena kola su:



43. (a)
$$\begin{aligned}
& (\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r) \Leftrightarrow p \\
\sim\ & ((\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r) \Rightarrow p) \wedge (p \Rightarrow (\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r)) \\
\sim\ & (\neg((\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r)) \vee p) \wedge (\neg p \vee ((\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r))) \\
\sim\ & (\neg((p \vee r) \wedge (p \vee \neg r)) \vee p) \wedge (\neg p \vee ((p \vee r) \wedge (p \vee \neg r))) \\
\sim\ & ((\neg p \wedge \neg r) \vee (\neg p \wedge r)) \vee p) \wedge (\neg p \vee ((p \vee r) \wedge (p \vee \neg r))) \\
\sim\ & (\neg p \vee \neg p \vee p) \wedge (\neg p \vee r \vee p) \wedge (\neg r \vee \neg p \vee p) \wedge \\
& \wedge (\neg r \vee r \vee p) \wedge (\neg p \vee p \vee r) \wedge (\neg p \vee p \vee \neg r).
\end{aligned}$$

Kako svaka klauza sadrži bar jedno slovo i sa i bez negacije, data formula je tautologija.

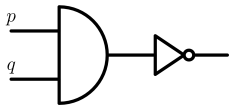
(b) Iz (a) vidimo da je $(\neg p \Rightarrow r) \wedge (\neg p \Rightarrow \neg r) \sim p$, pa je prekidačko kolo veoma jednostavno:



44. Treba da nađemo formulu X takvu da $(p \wedge q) \vee X$ bude tautologija. Dakle, mora biti $v_\alpha(X) = \top$ za sve valuacije α takve da $\alpha(p \wedge q) = \bot$. To znači da tablica za X izgleda ovako:

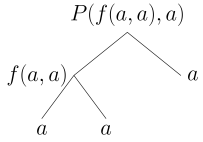
p	q	X
$\top$	$\top$	$\top/\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

Jedna od formula koje to zadovoljavaju je $\neg p \vee \neg q \sim \neg(p \wedge q)$, a odgovarajuće kolo je:

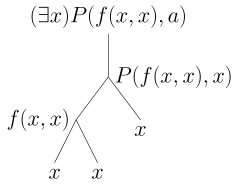


6.3 Predikatski račun

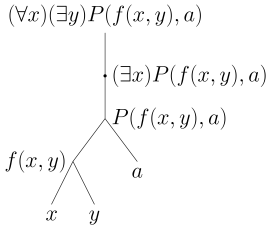
1. Tražena drveta izgledaju ovako:



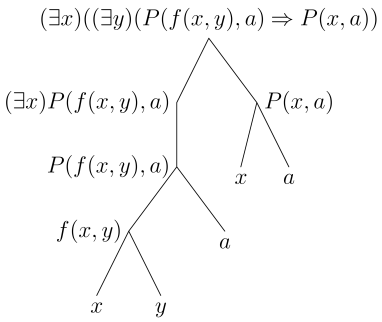
Slika 6.1: Drvo podformula za $P(f(a,a),a)$



Slika 6.2: Drvo podformula za $(\exists x)P(f(x,x),a)$



Slika 6.3: Drvo podformula za $(\forall x)(\exists y)P(f(x,y),a)$



Slika 6.4: Drvo podformula za $(\exists x)((\exists y)(P(f(x,y),a) \Rightarrow P(x,a))$

2. (a) Neka je $i_1 = (R, =)$ data interpretacija. Tada $i_1 \models (\forall x)P(x,x)$ znači da za sve $a \in R$ važi $i_1 \models P(x,x)[a]$, odnosno, kada P interpretiramo kao jednakost a na mesto x zamenimo a, da za sve $a \in R$ važi $a = a$, što je tačno.

   (b) Neka je $i_2 = (R, \leq)$. $i_2 \models (\forall x)P(x,x)$ znači da za sve $a \in R$ važi $a \leq a$, što je takođe tačno.

   (c) Konačno, neka je $i_3 = (R, <)$. $i_3 \models (\forall x)P(x,x)$ sada znači da za sve $a \in R$ važi $a < a$, što nije tačno.

3. (a) $i_1 \models F_1$ znači da je $1 + 1 = 1$ (relacijsko slovo P interpretira se kao jednakost, funkcijsko slovo f kao sabiranje a znak konstante a kao 1); to naravno nije tačno.

   $i_2 \models F_1$ znači da je $1 \cdot 1 = 1$, što jeste tačno.

   $i_3 \models F_1$ znači da je $0 \cdot 0 = 0$, što je takođe tačno.

   (b) $i_1 \models F_2$ znači da postoji $x \in Z$ takvo da je $x + x = 1$, što nije tačno.

   $i_2 \models F_2$ znači da postoji $x \in N$ takvo da je $x \cdot x = 1$, što je tačno.

$i_3 \models F_2$ znači da postoji $x \in R$ takvo da je $x \cdot x = 0$, što je opet tačno.

(c) $i_1 \models F_3$ znači da za svako $x \in Z$ postoji $y \in Z$ takvo da je $x + y = 1$, što je tačno.

$i_2 \models F_3$ znači da za svako $x \in N$ postoji $y \in N$ takvo da je $x \cdot y = 1$, što nije tačno: za $x = 2$ ne postoji takvo y.

$i_3 \models F_3$ znači da za svako $x \in R$ postoji $y \in R$ takvo da je $x \cdot y = 0$. To je tačno: za bilo koje $x \in R$ možemo uzeti $y = 0$.

(d) $i_1 \models F_4$ znači da postoji $x \in Z$ takvo da, ako postoji $y \in Z$ takvo da je $x + y = 1$, onda je $x = 1$. Kako za sve $x \in Z$ postoji $y \in Z$ takvo da je $x + y = 1$, formula nije tačna u interpretaciji i_1.

$i_2 \models F_4$ znači da postoji $x \in N$ takvo da, ako postoji $y \in N$ takvo da je $x \cdot y = 1$, onda je $x = 1$. Zaista, takvo $y \in N$ može postojati samo za $x = 1$, pa je formula tačna u interpretaciji i_2.

$i_3 \models F_4$ znači da postoji $x \in R$ takvo da, ako postoji $y \in R$ takvo da je $x \cdot y = 0$, onda je $x = 0$. Opet za sve $x \in R$ postoji $y = 0$ takvo da je $x \cdot y = 0$, pa formula nije tačna u interpretaciji i_3.

4. Ako je $i = (R, =, \cdot)$, $i \models (\forall x)P(f(x, y), x)$ važi ako je, za sve $x \in R$, $x \cdot y = x$. Ali tačnost ove formule zavisi od vrednosti slobodne promenljive y: ako je $y = 1$ ona je tačna, dok je za ostale vrednosti $y \in R$ netačna. Zaključujemo da i nije model date formule, jer ona nije tačna u interpretaciji i za sve vrednosti slobodnih promenljivih.

5. (a) „x je paran broj" je najlakše izraziti formulom u obliku $2 \mid x$. Dakle, tražena formula u jeziku interpretacije i_1 je recimo $P(a, x)$ (P je u datoj interpretaciji relacija deljivosti a a konstanta 2).

   Drugi način da izrazimo da je x paran je da postoji y takvo da $x = 2y$, dakle formulom $(\exists y)P(x, f(a, y))$ u jeziku i_2 (P je sada relacija jednakosti, f je množenje a a opet konstanta 2).

   Konačno, ako umesto množenja i konstante 2 na raspolaganju imamo samo sabiranje, deo formule $x = 2y$ možemo zameniti sa $x = y+y$, dakle u jeziku i_3 cela formula glasi $(\exists y)(P(x, f(y, y)))$.

   (b) Uzimajući u obzir rešenje zadatka (a), jedna moguća formula za datu rečenicu je $(\exists x)\neg(\exists y)(P(x, f(y, y)))$.

   (c) Za i_1 direktno dobijamo formulu $P(x, f(y))$.

   Da bismo prešli na jezik interpretacije i_2 možemo $x = \sqrt{y}$ zameniti sa $x \cdot x = y$ uz dodatni uslov da je x pozitivan; dakle formula bi glasila $P(f(x, x), y) \wedge Q(x)$.

   (d) Najmanji broj je onaj koji je manji ili jednak od svih. U jeziku interpretacije i_1 formula bi glasila $(\exists x)(\forall y)P(x, y)$, a u jeziku interpretacije i_2: $(\exists x)(\forall y)(\neg P(x, y) \Rightarrow Q(x, y))$ (tj. x je manji od svih ostalih prirodnih brojeva).

   (e) Broj je prost ako su svi njegovi delioci jednaki jedinici ili njemu samom. Stoga je u jeziku i_1 tražena formula $(\forall y)(Q(y, x) \Rightarrow P(y, a) \vee P(y, x))$ (P se interpretira kao $=$ a Q kao $|$).

   Da bismo eliminisali jedinicu treba da je izrazimo preko ostalih elemenata jezika. Možemo iskoristiti činjenicu da je broj 1 jedini element skupa N koji deli sve druge. Tako dobijamo formulu $(\forall y)(Q(y, x) \Rightarrow (\forall z)Q(y, z) \vee P(y, x))$.

(f) U interpretaciji i_1 formula je $NZD(x,y)=1$, odnosno $P(f(x,y),a)$. Da bismo prešli na i_2 treba operaciju NZD zameniti relacijom deljivosti, dakle formula treba da izrazi da x i y nemaju drugih zajedničkih delilaca osim 1: $(\forall z)(Q(z,x)\wedge Q(z,y)\Rightarrow P(z,a))$. Da bismo ovo preveli u jezik interpretacije i_3 treba da eliminišemo deljivost pomoću operacije množenja (definicija 1.4); dobijamo:

$$(\forall z)((\exists s)P(f(z,s),x)\wedge(\exists t)P(f(z,t),y)\Rightarrow P(z,a)).$$

Napomena. (1) Primetimo da, kada konstruišemo formulu koja nešto govori o $x,y,\ldots$, tada $x,y,\ldots$ treba da se u njoj javljaju kao slobodne promenljive. Ako formula izražava neko opšte pravilo (koje se ne tiče konkretnih elemenata domena), ona nema slobodne promenljive.

(2) Prikazana rešenja, naravno, nisu jedinstvena; čitalac može pokušati da nađe i druge načine zapisivanja datih rečenica pomoću formula.

6.
$$\begin{aligned}
&(\forall x)(\exists y)P(x,y)\Rightarrow\neg((\exists x)Q(x)\vee(\forall x)(\forall y)\neg P(x,y))\\
\sim\ &\neg(\forall x)(\exists y)P(x,y)\vee\neg((\exists x)Q(x)\vee(\forall x)(\forall y)\neg P(x,y))\\
\sim\ &(\exists x)(\forall y)\neg P(x,y)\vee(\neg(\exists x)Q(x)\wedge\neg(\forall x)(\forall y)\neg P(x,y))\\
\sim\ &(\exists x)(\forall y)\neg P(x,y)\vee((\forall x)\neg Q(x)\wedge(\exists x)(\exists y)P(x,y))\\
\sim\ &(\exists x)(\forall y)\neg P(x,y)\vee((\forall z)\neg Q(z)\wedge(\exists u)(\exists v)P(u,v))\\
\sim\ &(\exists x)(\forall y)\neg P(x,y)\vee(\forall z)(\exists u)(\exists v)(\neg Q(z)\wedge P(u,v))\\
\sim\ &(\exists x)(\forall y)(\forall z)(\exists u)(\exists v)(\neg P(x,y)\vee(\neg Q(z)\wedge P(u,v))).
\end{aligned}$$

7. Skolemizacijom dobijamo formule:

(a) $(\forall y)P(a,y)$;

(b) $(\forall x)Q(x,f(x))$;

(c) eliminišući najpre u dobijamo

$$(\forall x)(\exists y)(\exists v)(\forall z)(\exists t)(P(a,x,y)\wedge P(v,x,z)\Rightarrow P(y,z,t)),$$

eliminišući y:

$$(\forall x)(\exists v)(\forall z)(\exists t)(P(a,x,f(x))\wedge P(v,x,z)\Rightarrow P(f(x),z,t)),$$

eliminišući v:

$$(\forall x)(\forall z)(\exists t)(P(a,x,f(x))\wedge P(g(x),x,z)\Rightarrow P(f(x),z,t))$$

i konačno eliminišući t:

$$(\forall x)(\forall z)(P(a,x,f(x))\wedge P(g(x),x,z)\Rightarrow P(f(x),z,h(x,z))).$$

(d) Analogno kao pod (c) dobijamo formulu

$$(\forall y)(\forall u)(P(a,y)\wedge P(a,f(b,g(y),u))\Rightarrow P(h(y,u),h(y,u))).$$

8. Kao u prethodnom zadatku skolemizacijom dobijamo formulu

$$(\forall y)(\forall z)(\neg P(a,y)\vee(\neg Q(z)\wedge P(f(y,z),g(y,z)))).$$

9. Osnovna ideja algoritma `BubbleSort` je da, zamenjujući uzastopne elemente niza, nakon prvog prolaza kroz niz (za `i=n-1`) najmanji element bude postavljen na poslednju poziciju, nakon drugog prolaza (za `i=n-2`) sledeći najmanji na pretposlednju itd. tako da se, kada `i` stigne do 1, svi elementi nalaze na svojim mestima. Dakle, ako sa $\texttt{x[j]}^i$ označimo vrednost `j`-tog elementa niza nakon `i`-tog prolaza kroz niz (brojeći unazad), treba dokazati

   (a) $(\forall i \leq n-1)(\forall j > i)\texttt{x[j-1]}^i > \texttt{x[j]}^i$

   (b) $(\forall i \leq n-1)(\forall j \leq i)\texttt{x[j]}^i > \texttt{x[i+1]}^i$.

   Dokaz, paralelno za (a) i (b), sprovodimo indukcijom po i, ali „unazad", od $i = n-1$ do $i = 1$.

   B.I. Neka je prvo $i = n-1$ i neka se najmanji element na početku nalazi na mestu `x[k]`. Tada će, za `j=k`, biti `x[j]<x[j+1]`, pa će ta dva elementa biti zamenjena. Potom će i za sve veće vrednosti `j` biti `x[j]<x[j+1]`, te će najmanji element biti zamenjen redom sa svim iza njega i na kraju dospeti na poslednje mesto: $\texttt{x[n]}^{n-1}$ će biti najmanji element niza, a to je upravo ono što govore formule (a) i (b) za $i = n-1$.

   I.H. Pretpostavimo su formule (a) i (b) tačne za neku vrednost i.

   I.K. Dokažimo da su one tačne i za $i-1$. Neka se najmanji od elemenata $\texttt{x[j]}^i$ (za `j`$\leq$`i`) nalazi na k-toj poziciji. Tada će, za sve `k`$\leq$`j`$\leq$`i-1` taj element biti zamenjen sa svim elementima $\texttt{x[k+1]}^i, \ldots, \texttt{x[i]}^i$ te će se naći na poziciji `x[i]`. Stoga je taj element, $\texttt{x[i]}^{i-1}$, manji od svih $\texttt{x[j]}^{i-1}$ za $j \leq i-1$ pa je ispunjeno (b). Pošto se elementi na pozicijama `x[i+1]`,...,`x[n]` u ovom prolazu nisu menjali, prema I.H. imamo $\texttt{x[i]}^{i-1} > \texttt{x[i+1]}^{i-1} > \ldots > \texttt{x[n]}^{i-1}$ pa važi i (a).

10. (a)
$$\begin{aligned} \neg(\forall x)(P(x) \Rightarrow Q(x,c)) &\sim (\exists x)\neg(P(x) \Rightarrow Q(x,c)) \\ &\sim (\exists x)(P(x) \wedge \neg Q(x,c)). \end{aligned}$$

    (b)
$$\begin{aligned} \neg(\exists x)(\forall y)xy = y &\sim (\forall x)\neg(\forall y)xy = y \\ &\sim (\forall x)(\exists y)xy \neq y. \end{aligned}$$

    (c)
$$\begin{aligned} & \neg(\forall x)(\forall y)(x < y \Rightarrow (\exists z)(x < z \wedge z < y)) \\ \sim\ & (\exists x)\neg(\forall y)(x < y \Rightarrow (\exists z)(x < z \wedge z < y)) \\ \sim\ & (\exists x)(\exists y)\neg(x < y \Rightarrow (\exists z)(x < z \wedge z < y)) \\ \sim\ & (\exists x)(\exists y)(x < y \wedge \neg(\exists z)(x < z \wedge z < y)) \\ \sim\ & (\exists x)(\exists y)(x < y \wedge (\forall z)\neg(x < z \wedge z < y)) \\ \sim\ & (\exists x)(\exists y)(x < y \wedge (\forall z)(\neg x < z \vee \neg z < y)). \end{aligned}$$

    U nekim od zadataka koji slede biće pogodnije da na kraju disjunkciju transformišemo u implikaciju, pa tako na kraju možemo dobiti i

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

11. Obeležimo datu formulu sa F i nađimo model za njenu negaciju, tj. za

$$\neg F \sim \underbrace{(\forall x)(P(x) \Rightarrow Q(x))}_{\varphi_1} \wedge \underbrace{(\exists x)P(x)}_{\varphi_2} \wedge \underbrace{(\exists x)\neg Q(x)}_{\varphi_3}.$$

Možemo uzeti npr. $D = \{a, b\}$ i relacije

P^i	a	b
	$\top$	$\bot$

i

Q^i	a	b
	$\top$	$\bot$

Tada je (D, P^i, Q^i) traženi model. Zaista, $i \models \varphi_1$ zato što za sve elemente modela (dakle, i za $x = a$ i za $x = b$) važi: ako $P^i(x)$, onda i $Q^i(x)$. φ_2 važi za $x = a$, a φ_3 za $x = b$.

12. Dovoljan nam je model sa samo jednim elementom: neka je $D = \{a\}$, a relacije P^i, Q^i i S^i date tablicama:

P^i	a
	$\top$

Q^i	a
	$\bot$

i

S^i	a
	$\top$

(D, P^i, Q^i, S^i) je model za dati skup formula.

13. (a) Pogodno je datu formulu F prvo transformisati u preneksni oblik koristeći ekvivalencijske transformacije. Dobijamo da je

$$F \sim (\exists x)(\exists y)(\exists z)(P(x) \wedge P(y) \wedge Q(x) \wedge Q(y) \wedge \neg P(z))$$

Model formule je $(\{a, b\}, P^i, Q^i)$, gde su P^i i Q^i date tablicama

P^i	a	b
	$\top$	$\bot$

i

Q^i	a	b
	$\top$	$\top$

(F je zadovoljena za $x = y = a$ i $z = b$.)

(b) Imamo da je

$$\neg F \sim (\forall x)(P(x) \Rightarrow (\forall y)(P(y) \Rightarrow (Q(x) \Rightarrow \neg Q(y)) \vee (\forall z)P(z))).$$

Lak način da obezbedimo da implikacija bude zadovoljena je da se pobrinemo da njena leva strana bude netačna, tj. da ne važi $P^i(x)$ ni za jedan element x domena. Stoga je jedan kontramodel $(\{a, b\}, P^i, Q^i)$, gde

P^i	a	b
	$\bot$	$\bot$

i

Q^i	a	b
	$\top$	$\top$

14. Označimo datu formulu sa F. Tražimo model za $\neg F$. Pošto je

$$\neg F \sim (\exists x)(P(x) \wedge \neg Q(x)) \wedge (\exists x)(Q(x) \wedge \neg S(x)) \wedge (\exists x)(S(x) \wedge \neg P(x)),$$

jedan model bi mogao biti (N, P^i, Q^i, S^i), gde $P^i(x)$ akko je x paran, $Q^i(x)$ akko je x deljiv sa 3 i $S^i(x)$ akko je x deljiv sa 5. Podformule formule $\neg F$ tada redom tvrde da: postoji paran prirodan broj koji nije deljiv s 3, postoji prirodan broj koji je deljiv s 3 ali ne i sa 5 i, konačno, da postoji prirodan broj koji je deljiv s 5 ali nije paran.

15. I rešenje. Jedan mogući model je (N, P^i, Q^i, T^i, S^i), gde je: $P^i(x)$ akko je x paran, $Q^i(x)$ akko je x deljiv sa 3, $T^i(x)$ akko je x deljiv sa 12 i $S^i(x)$ akko je x deljiv sa 6.

II rešenje. Druga mogućnost: domen je $\{a, b\}$ i

P^i	
a	$\top$
b	$\bot$

Q^i	
a	$\bot$
b	$\top$

T^i	
a	$\bot$
b	$\top$

S^i	
a	$\top$
b	$\top$

16. Tražimo model za negaciju date formule, odnosno model koji zadovoljava
$\varphi_1 = (\exists x)(\forall y)P(x,y)$
$\varphi_2 = (\exists x)\neg P(x,x)$
$\varphi_3 = (\exists x)(\exists y)(x \neq y \wedge P(x,x) \wedge P(y,y))$
$\varphi_4 = (\exists x)(\forall y)P(y,x)$.
Domen će biti skup $\{a,b,c\}$, a relacija P^i data tablicom:

P^i	a	b	c
a	$\bot$	$\top$	$\top$
b	$\bot$	$\top$	$\bot$
c	$\top$	$\top$	$\top$

Naime, zbog φ_1 bar u jednoj vrsti tablice moraju se nalaziti samo $\top$. Slično, zbog φ_4 bar u jednoj koloni moraju se nalaziti samo $\top$. Na dijagonali zbog φ_2 mora biti bar jedno $\bot$, a zbog φ_3 bar dva $\top$.

17. Treba dokazati da negacija date formule
$$\neg F \sim (\exists x)(\forall y)P(x,y) \wedge (\exists x)(\forall y)P(y,x) \wedge (\exists x)\neg P(x,x)$$
ima model, odnosno konstruisati interpretaciju i takvu da $i \models F_1$, $i \models F_2$ i $i \models F_3$, gde $F_1 = (\exists x)(\forall y)P(x,y)$, $F_2 = (\exists x)(\forall y)P(y,x)$ i $F_3 = (\exists x)\neg P(x,x)$.
I rešenje. Razmotrimo najpre interpretaciju $(Z,\leq)$. Prva od formula traži da Z ima najmanji element, što će biti tačno ako domen Z zamenimo sa N (tada je 1 taj najmanji element). Druga formula kaže da postoji najveći element; ovo ne važi ni za jedan od skupova N, Z, $R,\ldots$ ali će biti ispunjeno ako domen ,,ograničimo" odgore i uzmemo, recimo, $D = \{1,2,\ldots,10\}$. Konačno, treća formula kaže da nisu svi elementi u relaciji sa samim sobom. Da bismo nju zedovoljili umesto $\leq$ uzmimo relaciju $<$. Konačno, dobijamo jedan mogući model: $(\{1,2,\ldots,10\},<)$.
II rešenje. Model može biti $i = (\{a,b\},P^i)$, gde je P^i zadato tablicom:

P^i	a	b
a	$\top$	$\top$
b	$\top$	$\bot$

Tada $i \models F_1$ jer je element a u relaciji i sa a i sa b, $i \models F_2$ jer su s elementom a u relaciji oba elementa domena i konačno $i \models F_3$ jer b nije u relaciji sa sobom.

18. Dokazaćemo da data formula (obeležimo je sa F) nije valjana tako što ćemo naći model njene negacije. Imamo
$$\neg F \sim (\forall x)P(x,x) \wedge (\forall x)(\exists y)\neg P(x,y) \wedge$$
$$(\forall x)(\exists y)\neg P(y,x) \wedge (\exists x)(\exists y)(\neg P(x,y) \wedge \neg P(y,x)).$$
I rešenje. Definišimo model (D,P^i) ovako: neka je $D = \{a,b\}$ i relacija P^i data tablicom:

P^i	a	b
a	$\top$	$\bot$
b	$\bot$	$\top$

II rešenje. Uzmimo relaciju jednakosti na proizvoljnom skupu od bar dva elementa, dakle model može biti npr. $(N,=)$.

19. Označimo datu formulu sa F. Tražimo model za $\neg F$. Pošto je

$$\neg F \sim (\forall x)(\forall y)(P(x,y) \Rightarrow Q(y,x)) \wedge (\exists x)\neg Q(x,x) \wedge (\exists x)(\exists y)(P(x,y) \wedge Q(x,y)),$$

jedan model bi mogao biti $(N, <, \neq)$.

20. Negacija date formule je ekvivalentna sa

$$\underbrace{(\exists x)(\exists y)P(x,y)}_{\varphi_1} \wedge \underbrace{(\forall x)(\forall y)(P(x,y) \Leftrightarrow (\exists z)(P(x,z) \wedge P(z,y)))}_{\varphi_2} \wedge \underbrace{(\forall x)\neg P(x,x)}_{\varphi_3}$$

Jedan model za $\{\varphi_1, \varphi_2, \varphi_3\}$ je $(Q, <)$. Dokažimo to. φ_1 tvrdi da je relacija neprazna, a φ_3 da je irefleksivna (tj. da nijedan element nije u relaciji sam sa sobom, videti definiciju 4.38), što je očigledno. Što se tiče φ_2, implikacija zdesna nalevo važi zbog tranzitivnosti relacije $<$, a obrnuta zato što između svaka dva elementa $x, y \in Q$ takva da $x < y$ postoji bar još jedan, recimo $\frac{x+y}{2}$ (za skup koji ima tu osobinu kaže se da je gust).

21. Jedan model je $(R^+, \geq)$, gde je R^+ skup pozitivnih realnih brojeva. Naime, prva formula važi jer je $\geq$ refleksivna relacija (svaki element domena je u relaciji sa sobom), druga zato što je skup R gust (između svaka dva realna broja postoji bar još jedan), a treća jer R^+ ima najmanji element (koji je manji ili jednak od svakog).

22. I rešenje. Dovoljno je naći model za negaciju date formule, tj. za

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

To će biti npr. $(R^+, <)$, gde je R^+ skup pozitivnih realnih brojeva.

II rešenje. Za domen uzmemo proizvoljan skup X, a P^i definišemo tako da je $P^i(a,b)$ netačno za sve $a, b \in X$, odnosno svaka dva elementa nisu u relaciji.

23. Ako formiramo negaciju date formule dobijamo da treba naći model za skup formula $\{\varphi_1, \varphi_2\}$, gde

$$\begin{aligned} \varphi_1 &= (\forall x)(\forall y)(\exists z)(A(x,y) \wedge B(x,z) \wedge B(y,z)) \\ \varphi_2 &= (\exists x)(\forall y)(\exists z)(\neg A(x,y) \vee \neg B(y,z) \vee \neg B(x,z)). \end{aligned}$$

Uzmimo npr. $D = \{a, b\}$, a A^i i B^i neka su zadate tablicama:

A^i	a	b
a	$\top$	$\top$
b	$\top$	$\top$

B^i	a	b
a	$\top$	$\bot$
b	$\top$	$\top$

(D, A^i, B^i) je model za dati skup formula. Zaista, za proizvoljne $x, y \in D$ možemo uzeti $z = a$ i φ_1 će biti ispunjeno. Što se tiče φ_2, ako uzmemo $x = a$ i, bez obzira na vrednost y, $z = b$, neće biti ispunjeno $B^i(x,z)$.

24. Dovoljno je da nađemo model za negaciju date formule, tj. za skup formula

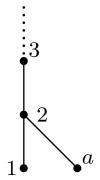
$$\{\underbrace{(\forall x)(\forall y)(P(x,y) \Leftrightarrow P(y,x))}_{\varphi_1}, \underbrace{(\exists x)\neg P(x,x)}_{\varphi_2},$$
$$\underbrace{(\exists x)(\exists y)(\exists z)(P(x,y) \wedge P(y,z) \wedge \neg P(x,z))}_{\varphi_3}\}.$$

U tu svrhu uzmimo npr. $D = \{a, b\}$ i relaciju

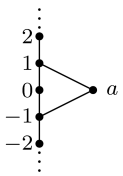
P^i	a	b
a	$\bot$	$\top$
b	$\top$	$\bot$

Traženi model je (D, P^i). Naime, φ_1 kaže da je P^i simetrična relacija, a φ_2 da nije refleksivna. φ_3, koja tvrdi da P^i nije tranzitivna, biće ispunjena za $x = a$, $y = b$ i $z = a$. (Detaljnija objašnjenja ovih značajnih osobina relacija mogu se naći u odeljku 4.8.)

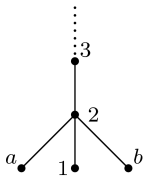
25. $(N, <)$ je model za prvu, drugu i četvrtu formulu datog skupa. Da bismo našli model i za treću treba da modifikujemo ovu interpretaciju tako da sadrži dva neuporediva elementa (tj. takva da nijedan nije manji od drugog). Neka $a \notin N$ i $D = N \cup \{a\}$. Definišimo relaciju P^i na skupu D tako da $P^i(a, n)$ za sve $n \in N \setminus \{1\}$, a da $P^i(m, n)$ važi akko $m < n$ za $m, n \in N$. Dakle, skupu N dodali smo novi element a koji je „ispod" svih njegovih elemenata osim jedinice, sa kojom nije uporediv (videti sliku). Nakon ovakve modifikacije moramo proveriti da su ostale formule i dalje zadovoljene. P^i je irefleksivna, za svaka dva elementa skupa D postoji gornje ograničenje, postoje dva elementa (1 i a) koji nisu uporedivi i za svaka dva elementa bar jedan nije manji od drugog. Dakle, (D, P^i) je model za dati skup formula.



Slika 6.5: Dijagram uz zadatak 25



Slika 6.6: Dijagram uz zadatak 26



Slika 6.7: Dijagram uz zadatak 27

26. Neka je Z skup celih brojeva i $a \notin Z$. Neka je $D = Z \cup \{a\}$. Slično prethodnom zadatku, definišimo relaciju P^i na skupu D tako da a bude ispod svih n za $n \in N$ i iznad svih negativnih brojeva $-n$ za $n \in N$, a $P^i(m, n)$ akko $m < n$ za $m, n \in Z$ (slika). (D, P^i) je traženi model. Zaista, P^i je irefleksivna i tranzitivna, svaki element ima prethodnika i sledbenika, a 0 i a nisu uporedivi.

27. Tražimo model za skup formula $\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, gde

$$\begin{aligned}
\varphi_1 &= (\forall x)P(x,x)\\
\varphi_2 &= (\forall x)(\forall y)(P(x,y) \wedge P(y,x) \Rightarrow x = y)\\
\varphi_3 &= (\forall x)(\forall y)(\forall z)(P(x,y) \wedge P(y,z) \Rightarrow P(x,z))\\
\varphi_4 &= (\exists x)(\exists y)(\exists z)(\neg P(x,y) \wedge \neg P(y,z) \wedge \neg P(z,x)).
\end{aligned}$$

Jedan model će biti (N_1, P^i), gde $N_1 = N \cup \{a, b\}$, $a, b \notin N$, a relacija P^i na D definisana tako da i a i b budu ispod svih prirodnih brojeva osim 1 a $P^i(m, n)$ važi akko je $m \leq n$ za $m, n \in N$. Dakle, skupu N dodali smo dva elementa koja nisu uporediva sa 1, a manji su od svih ostalih prirodnih brojeva (slika).

28. Model za prvu i drugu formulu datog skupa koji ne ispunjava treću je npr. $(\{a, b\}, P^i)$, gde je P^i data tablicom

P^i	a	b
a	$\top$	$\top$
b	$\bot$	$\top$

Model za prvu i treću, ali ne i drugu možemo dobiti analogno zadatku 25: domen je skup $D = N \cup \{a\}$, a relaciju P^i dobijamo tako što a definišemo da bude u relaciji sa svim elementima skupa D (uključujući i sebe) osim jedinice.

Interpretacija u kojoj su tačne samo druga i treća formula je $(N, <)$.

29. (a) Uočimo sledeću interpretaciju: $i = (N, P^i, f^i)$ gde $P^i(n)$ akko $2|n$ i $f^i(x) = x+1$. Tada $i \models \neg(\forall x)(P(x) \Rightarrow P(f(x)))$, odnosno $i \models (\exists x)(P(x) \wedge \neg P(f(x)))$. Naime, postoji $n \in N$ za koje $2|n$ i $2 \nmid (n+1)$; to je npr. $n = 2$.

(b) Za model $i = (A, P^i, f^i)$ treba još da definišemo relaciju P^i. Treba da važi:

$$i \models (\forall x)(P(x) \Rightarrow P(f(x)))$$

odnosno za svako $y \in A$ ako $P^i(y)$ onda $P^i(f^i(y))$.

Kada poslednji uslov ispišemo za svako $y \in A$ dobijamo:

za $y = a$: $\quad P^i(a) \Rightarrow P^i(c)$
za $y = b$: $\quad P^i(b) \Rightarrow P^i(b)$
za $y = c$: $\quad P^i(c) \Rightarrow P^i(b)$.

Uzimajući sve to u obzir, dobijamo jednu od mogućih interpretacija relacijskog slova P:

P^i	a	b	c
	$\bot$	$\top$	$\bot$

30. (a) Za kontramodel možemo uzeti interpretaciju sa domenom N u kojoj P interpretiramo kao relaciju deljivosti $|$, a f kao relaciju sledbenika: $f^i(x) = x + 1$. Tada, npr. za $x = 2$ i $y = 4$, imamo $2 \mid 4$ ali $3 \nmid 5$.

(b) Jedna mogućnost bi bila da P interpretiramo tako da svaka dva elementa iz A budu u relaciji. Implikacija iz formule je tada trivijalno zadovoljena.

31. Treba da nađemo model za $\neg F \sim (\exists x)P(x) \wedge (\forall x)(P(f(x)) \Rightarrow P(x)) \wedge (\exists x)\neg P(f(x))$, tj. za formule $F_1 = (\exists x)P(x)$, $F_2 = (\forall x)(P(f(x)) \Rightarrow P(x))$ i $F_3 = (\exists x)\neg P(f(x))$.

I rešenje. Jedan model je (Z, P^i, f^i), gde $P^i(x)$ akko je x parno i $f^i(x) = x + 2$. F_1 je ispunjeno za bilo koje parno x, a F_3 za bilo koje neparno x (jer je tada i $x + 2$ neparno). F_2 kaže da za sve $x \in Z$, ako je $x + 2$ parno, onda je i x parno, što je tačno.

II rešenje. Uzmimo za domen $D = \{a, b\}$, i definišimo

$$f^i : \begin{pmatrix} a & b \\ a & b \end{pmatrix} \text{ i } \begin{array}{c|c} P^i & \\ \hline a & \top \\ b & \bot \end{array}$$

F_1 je ispunjeno za $x = a$, a F_3 za $x = b$ (tada je i $f(x) = b$). F_2 očigledno važi i za $x = a$ i za $x = b$.

32. I rešenje. Jedan model datog skupa formula je $(R, <, f^i)$, gde je $f^i(x) = x - 1$. Uzimamo $<$, a ne $\leq$ zbog prve formule, R a ne N zbog druge.

II rešenje. Drugi, konačan model, mogao bi biti (M, P^i, f^i), gde $M = \{a, b\}$,

$$\begin{array}{c|cc} P^i & a & b \\ \hline a & \bot & \top \\ b & \top & \top \end{array} \text{ i } f^i = \begin{pmatrix} a & b \\ b & b \end{pmatrix}.$$

Druga formula je zadovoljena jer za bilo koje $x, y \in M$ možemo uzeti $z = b$ i data implikacija će važiti. Slično, kako je $f(x) = b$ za obe vrednosti $x \in M$, zadovoljena je i treća formula.

33. Dokazaćemo da data formula F nije valjana ako nađemo model za

$$\neg F \sim (\exists x)(\exists y)\neg P(f(x, y), y) \wedge (\exists x)(\exists y)\neg P(x, f(x, y)).$$

Za domen uzmimo skup prirodnih brojeva, P interpretirajmo kao standardnu relaciju $<$, a f kao množenje. Jasno je da postoje dva realna broja (npr. $x = y = \frac{1}{2}$) čiji je proizvod manji od y, i da postoje dva prirodna broja (npr. $x = y = 3$) čiji je proizvod veći od x.

34. I rešenje. Uzmimo model (D, P^i, f^i), gde je $D = \{a, b\}$, P^i data tablicom

$$\begin{array}{c|cc} P^i & a & b \\ \hline a & \top & \top \\ b & \top & \top \end{array}$$

i $f^i : \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ (mada smo f^i mogli definisati proizvoljno).

II rešenje. Jedan mogući model je $(D_n, |, f^i)$, gde je $D_n = \{x \in Z : x \mid n\}$ skup svih delitelja nekog fiksiranog prirodnog broja n, $|$ relacija deljivosti, a $f^i(x) = \frac{n}{x}$. Naime, relacija deljivosti na skupu Z je tranzitivna (dakle, prva formula je tačna) a nije antisimetrična (pa je tačna i druga), videti primer 4.54. Treća formula u ovoj interpretaciji kaže da za sve $x, y \in Z$ iz $x \mid y$ sledi $\frac{n}{y} \mid \frac{n}{x}$. Zaista, ako je $y = kx$ i $n = ly$, onda je $\frac{n}{y} = l$ i $\frac{n}{x} = kl$ pa $\frac{n}{y} \mid \frac{n}{x}$.

35. Obeležimo $M = \{1, 2, \ldots, 10\}$. Jedan model negacije tražene formule je (M, P^i, f^i), gde $P^i(x, y)$ akko je $x > 5$ za $x, y \in M$ i $f^i(x) = x$ za sve $x \in M$. Naime, on zadovoljava svaku od formula:

1) $(\exists x)(\forall y)P(x, y)$: $x = 10$ je element takav da $x > 5$ za sve $y \in M$;

2) $(\forall x)(\forall y)(P(x, y) \Rightarrow P(f(x), f(y)))$: pošto je $f^i(x) = x$, iz $P^i(x, y)$ trivijalno sledi $P^i(f(x), f(y))$ za sve $x, y \in M$;

3) $(\exists x)(\forall y)\neg P(x, y)$: $x = 1$ je element takav da ne važi $x > 5$ bez obzira na vrednost $y \in M$.

36. Iz druge i treće formule se vidi da interpretacija slova f mora biti neka bijekcija (videti definiciju 5.3) a iz prve da interpretacija P^i slova P treba da bude takva da je svaki element u relaciji P^i akko njegova slika nije. Traženi model može biti npr. $(Z \setminus \{0\}, f^i, P^i)$, gde je $f^i(x) = -x$ i $P^i(x)$ akko $x > 0$. (Izbacujemo nulu jer za nju ne bi važila prva formula; to možemo jer funkcija f^i nijedan ceo broj različit od nule ne slika u nulu pa je f^i operacija na skupu $Z \setminus \{0\}$.)

37. (a) Neka je (D, P^i) traženi model, i $F_1 = (\forall x)(\exists y)(P(x,y) \wedge (\forall z)(z \neq y \Rightarrow \neg P(x,z)))$, $F_2 = (\forall y)(\exists x)P(x,y)$. Tada formula F_1 kaže da je P^i ustvari funkcija iz skupa D u samog sebe (videti definiciju 5.1). Formula F_2 kaže da je ta funkcija „na" (za svaki element $y \in D$ postoji $x \in D$ koji se u njega slika). Evo dva moguća modela:

    (Z, P^i), gde $P^i(x,y)$ akko je $y = x + 1$;

    (R, P^i), gde $P^i(x,y)$ akko je $y = 2x$.

    (b) Obeležimo formule $F_1 = (\exists x)(\forall y)P(x,y)$, $F_2 = (\exists x)(\forall y)P(y,x)$, $F_3 = (\forall x)P(x, f(x))$ i $F_4 = (\exists x)(f(x) \neq x)$. Ukoliko želimo da nam P^i bude neka relacija poretka, F_1 kaže da ona treba da ima najmanji element a F_2 da treba da ima i najveći (videti definiciju 4.61).

    I rešenje. Uzmimo za domen $D = \{1,2,3,4\}$, a P^i neka bude $\leq$. F_3 kaže da za sve $x \in D$ mora biti $x \leq f^i(x)$, a F_4 da f^i ne sme biti identičko preslikavanje. Dakle, možemo uzeti npr. $f^i : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 4 \end{pmatrix}$.

    II rešenje: $([0,1], \geq, f^i)$, gde je $[0,1]$ zatvoreni interval brojeva između 0 i 1 a $f^i(x) = x^2$.

38. Ako data formula ne bi bila valjana, postojao bi model (M, P^i, Q^i) za njenu negaciju. Taj model bi dakle zadovoljavao sledeće formule:

    $F_1 = (\forall x)(\forall y)(P(x) \wedge \neg P(y) \Rightarrow Q(x))$

    $F_2 = (\exists x)(P(x) \wedge \neg Q(x))$ i

    $F_3 = (\exists x)\neg P(x)$.

    Iz F_2 zaključujemo da postoji $m \in M$ takvo da važi $P^i(m)$ i ne važi $Q^i(m)$.
    Iz F_3 zaključujemo da postoji $n \in M$ takvo da ne važi $P^i(n)$.
    Iz F_1: za sve $x, y \in M$ važi: ako $P^i(x)$ i nije $P^i(y)$, onda i $Q^i(x)$. Za $x = m, y = n$ dobijamo, pošto $P^i(m)$ i nije $P^i(n)$, da važi i $Q^i(m)$. Dobili smo da istovremeno $Q^i(m)$ i nije $Q^i(m)$, kontradikcija.

39. Obeležimo datu formulu sa F i dokažimo da $\neg F$ nema model. Za početak,

$$\neg F \sim (\forall x)(\exists y)(A(x) \Rightarrow B(y)) \wedge$$
$$(\forall x)(\exists y)(B(x) \Rightarrow C(y)) \wedge (\exists x)(\forall y)(A(x) \wedge \neg C(y)).$$

    Pretpostavimo suprotno, tj. da za neku interpretaciju $i = (D, A^i, B^i, C^i)$ važi:

    (1) $i \models (\forall x)(\exists y)(A(x) \Rightarrow B(y))$

    (2) $i \models (\forall x)(\exists y)(B(x) \Rightarrow C(y))$ i

    (3) $i \models (\exists x)(\forall y)(A(x) \wedge \neg C(y))$.

    Iz (3) sledi da postoji $a \in D$ takvo da za sve $y \in D$ važi $A^i(a) \wedge \neg C^i(y)$, odakle sledi da važi $A^i(a)$ i

$$\text{za sve } y \in D \text{ važi } \neg C^i(y). \tag{6.8}$$

Kako formula (1) tvrdi da $(\exists y)(A(x) \Rightarrow B(y))$ važi za sve $x \in D$, na mesto x možemo staviti bilo koji element domena. Uzimajući $x = a$, dobijamo da postoji $b \in D$ takvo da $A^i(a) \Rightarrow B^i(b)$, što sa $A^i(a)$ daje $B^i(b)$. Konačno, iz (2), uzimajući $x = b$ dobijamo da postoji $c \in D$ takvo da $B^i(b) \Rightarrow C^i(c)$, što sa $B^i(b)$ daje $C^i(c)$, a iz (6.8) za $y = c$ sledi da nije $C^i(c)$. Kontradikcija.

40. Pretpostavimo suprotno, da postoji model za negaciju date formule, tj. interpretacija $i = (D, P^i, Q^i, S^i)$ za koju važi:

(1) $i \models (\forall x)(P(x) \Rightarrow \neg Q(x))$

(2) $i \models (\exists x)S(x)$

(3) $i \models (\forall x)(S(x) \Rightarrow P(x))$

(4) $i \models (\forall x)(S(x) \Rightarrow Q(x))$

Iz (2) sledi da postoji $a \in D$ takvo da $S^i(a)$. Iz (3) i (4) imamo redom (za $x = a$): $S^i(a) \Rightarrow P^i(a)$ i $S^i(a) \Rightarrow Q^i(a)$, što sa $S^i(a)$ daje $P^i(a)$ i $Q^i(a)$. Konačno, (1) uz $x = a$ daje $P^i(a) \Rightarrow \neg Q^i(a)$ pa, uzimajući u obzir i $P^i(a)$ važi $\neg Q^i(a)$, a to sa $Q^i(a)$ daje kontradikciju.

41. Pretpostavimo da data formula nije valjana, tj. da skup formula

$$\{\underbrace{(\exists x)(\neg P(x) \wedge Q(x)) \Rightarrow (\exists x)S(x)}_{\varphi_1}, \underbrace{(\forall x)(P(x) \Leftrightarrow \neg Q(x))}_{\varphi_2},$$
$$\underbrace{(\forall x)(P(x) \vee Q(x) \Rightarrow \neg S(x))}_{\varphi_3}, \underbrace{(\exists x)\neg P(x)}_{\varphi_4}\}$$

ima model (D, P^i, Q^i, S^i). Iz formule φ_4 zaključujemo da tada postoji $m \in D$ takav da nije $P^i(m)$. Dalje, iz φ_2 imamo da za sve $x \in D$ važi $P(x)$ akko ne važi $Q(x)$. Za $x = m$ to, sa ranije dokazanim $\neg P^i(m)$, daje da važi $Q^i(m)$. Odatle sledi da važi $\neg P^i(m) \wedge Q^i(m)$, pa D zadovoljava $(\exists x)(\neg P(x) \wedge Q(x))$. Formula φ_1 kaže da, ako i to zadovoljava, onda zadovoljava i $(\exists x)S(x)$. Neka je $n \in D$ takav da važi $S^i(n)$. Iz formule φ_3 imamo: za sve $x \in D$ $P^i(x) \vee Q^i(x) \Rightarrow \neg S^i(x)$, odnosno kontrapozicijom: $S^i(x) \Rightarrow \neg P^i(x) \wedge \neg Q^i(x)$. Za $x = n$ sledi da nije ni $P^i(n)$ ni $Q^i(n)$. Ako sada primenimo φ_2 za $x = n$ dobijamo, pošto ne važi $Q^i(n)$, da mora važiti $P^i(n)$, što je kontradikcija. Dakle, data formula je valjana.

42. Pretpostavimo da data formula F nije valjana, odnosno da

$$\neg F \sim \underbrace{(\forall x)(\exists y)P(x,y)}_{\varphi_1} \wedge \underbrace{(\forall x)(\forall y)(P(x,y) \wedge \neg Q(y,x) \Rightarrow P(y,x))}_{\varphi_2}$$
$$\wedge \underbrace{(\exists x)(\forall y)\neg P(y,x)}_{\varphi_3} \wedge \underbrace{(\forall x)(\forall y)\neg Q(x,y)}_{\varphi_4}$$

ima model (D, P^i, Q^i). Iz φ_3 dobijamo da postoji element $a \in D$ takav da

$$\text{za sve } y \in D \text{ ne važi } P^i(y,a). \tag{6.9}$$

Iz φ_1, za $x = a$, dobijamo da postoji $b \in D$ takvo da $P^i(a,b)$.

Iz φ_4, za $x = b$ i $y = a$, dobijamo da ne važi $Q^i(b,a)$.

Konačno, iz φ_2 za $x = a$ i $y = b$: ako $P^i(a,b)$ i nije $Q^i(b,a)$, onda važi $P^i(b,a)$. Koristeći gore dokazano dobijamo $P^i(b,a)$. Međutim, iz (6.9) za $y = b$ sledi da nije $P^i(b,a)$, kontradikcija.

43. (a)
$$\begin{aligned}
& (\forall z)((\forall x)(A(x) \Rightarrow B(x,z)) \Rightarrow ((\exists y)A(y) \Rightarrow (\exists y)B(y,z))) \\
\sim\ & (\forall z)((\forall x)(\neg A(x) \vee B(x,z)) \Rightarrow (\neg(\exists y)A(y) \vee (\exists u)B(u,z))) \\
\sim\ & (\forall z)(\neg(\forall x)(\neg A(x) \vee B(x,z)) \vee ((\forall y)\neg A(y) \vee (\exists u)B(u,z))) \\
\sim\ & (\forall z)((\exists x)(A(x) \wedge \neg B(x,z)) \vee ((\forall y)\neg A(y) \vee (\exists u)B(u,z))) \\
\sim\ & (\forall z)((\exists x)(A(x) \wedge \neg B(x,z)) \vee (\forall y)(\neg A(y) \vee (\exists u)B(u,z))) \\
\sim\ & (\forall z)((\exists x)(A(x) \wedge \neg B(x,z)) \vee (\forall y)(\exists u)(\neg A(y) \vee B(u,z))) \\
\sim\ & (\forall z)(\forall y)((\exists x)(A(x) \wedge \neg B(x,z)) \vee (\exists u)(\neg A(y) \vee B(u,z))) \\
\sim\ & (\forall z)(\forall y)(\exists x)((A(x) \wedge \neg B(x,z)) \vee (\exists u)(\neg A(y) \vee B(u,z))) \\
\sim\ & (\forall z)(\forall y)(\exists x)(\exists u)((A(x) \wedge \neg B(x,z)) \vee \neg A(y) \vee B(u,z))
\end{aligned}$$

(b) Kako je svaka formula ekvivalentna svom preneksnom obliku, ona je valjana ako i samo ako je njen preneksni oblik valjana formula. Pretpostavimo da ona nije valjana, odnosno da njena negacija

$$(\exists z)(\exists y)(\forall x)(\forall u)((A(x) \Rightarrow B(x,z)) \wedge A(y) \wedge \neg B(u,z))$$

ima model (D, A^i, B^i). To znači da postoje $m, n \in D$ takvi da za sve $x, u \in D$ važi:

(1) $A^i(x) \Rightarrow B^i(x,m)$

(2) $A^i(n)$

(3) $\neg B^i(u,m)$.

Zato to važi i za $x = u = n$, pa iz (1) dobijamo $A^i(n) \Rightarrow B^i(n,m)$, što sa (2) daje $B^i(n,m)$. Međutim, iz (3) dobijamo $\neg B^i(n,m)$, kontradikcija.

44. Pretpostavimo suprotno, da postoji model $i = (D, P^i, Q^i)$ u kojem važi negacija date formule, tj.

(1) $i \models (\forall x)(\forall y)(Q(x,y) \Rightarrow P(x,y))$

(2) $i \models (\forall x)(\exists y)\neg P(x,y)$

(3) $i \models (\forall x)(\forall y)(P(x,x) \Rightarrow P(x,y))$

(4) $i \models (\exists x)Q(x,x)$.

Iz (4) sledi da postoji $m \in D$ takvo da $Q^i(m,m)$. Iz (1) za $x = y = m$ sledi da, ako $Q^i(m,m)$, onda i $P^i(m,m)$. Dakle, važi $P^i(m,m)$. Iz (2) za $x = m$ dobijamo da postoji $n \in D$ takvo da ne važi $P^i(m,n)$. Konačno, iz (3) za $x = m, y = n$ dobijamo da, ako $P^i(m,m)$, onda i $P^i(m,n)$. Zaključujemo da važi $P^i(m,n)$, kontradikcija.

45. Pretpostavimo da $\neg F$ ima model (D, A^i, B^i). Na takvom modelu su tačne sledeće formule:

$F_1 = (\forall x)(\exists y)A(x,y)$

$F_2 = (\forall y)(\exists z)B(y,z)$ i

$F_3 = (\exists x)(\forall y)(\forall z)(A(x,y) \Rightarrow \neg B(y,z))$.

Neka je $a \in D$ element takav da

$$\text{za sve } y, z \in D, \text{ ako } A^i(a,y) \text{ onda ne važi } B^i(y,z), \tag{6.10}$$

dobijen iz F_3. Iz F_1 za $x = a$ dobijamo da postoji $b \in D$ takvo da $A^i(a,b)$. Dalje, iz F_2 za $y = b$ nalazimo $c \in D$ takvo da je $B^i(b,c)$. Najzad, iz (6.10) za $y = b$ i $z = c$ sledi: ako $A^i(a,b)$, onda nije $B^i(b,c)$, kontradikcija. Dakle, $\neg F$ nema model pa $\models F$.

46. (a) Ako data formula ne bi bila valjana, postojao bi model (M, P^i, Q^i) za njenu negaciju. Taj model bi dakle zadovoljavao sledeće formule:

$F_1 = (\forall x)(\forall y)(P(x,y) \Rightarrow Q(y,x))$

$F_2 = (\forall x)(\exists y)(\exists z)(P(x,y) \wedge P(z,x))$ i

$F_3 = (\exists x)(\forall y)(\forall z)\neg(Q(x,y) \wedge Q(z,x))$.

Iz F_3 zaključujemo da postoji $m \in M$ takvo da

$$\text{za sve } y, z \in M \text{ nije istovremeno } Q^i(m,y) \text{ i } Q^i(z,m). \tag{6.11}$$

Iz F_2: za svako $x \in M$ postoje $y, z \in M$ takvi da važi $P^i(x,y)$ i $P^i(z,x)$. Za $x = m$ dobijamo da postoje $n, k \in M$ takvi da $P^i(m,n)$ i $P^i(k,m)$. Iz F_1: za sve $x, y \in M$ važi: ako $P^i(x,y)$, onda i $Q^i(y,x)$. Za $x = m, y = n$ dobijamo, pošto $P^i(m,n)$, da važi i $Q^i(n,m)$ a za $x = k, y = m$, pošto $P^i(k,m)$, da važi i $Q^i(m,k)$. Iz (6.11) za $y = k, z = n$ dobijamo da ne važi istovremeno $Q^i(m,k)$ i $Q^i(n,m)$, što je kontradikcija.

(b) Negacija date formule ekvivalentna je sa

$$\begin{aligned}(\forall x)(\forall y)(P(x,y) \vee Q(x,y)) \wedge (\forall x)(\forall y)(P(x,y) \Leftrightarrow Q(y,x))\\ \wedge(\exists x)(P(x,x) \Rightarrow \neg Q(x,x)).\end{aligned}$$

Pretpostavimo da ona ima model $i = (D, P^i, Q^i)$. Iz $i \models (\exists x)(P(x,x) \Rightarrow \neg Q(x,x))$ vidimo da postoji $m \in D$ takvo da, ako $P^i(m,m)$, onda nije $Q^i(m,m)$. Iz $i \models (\forall x)(\forall y)(P(x,y) \vee Q(x,y))$ za $x = y = m$ dobijamo da važi $P^i(m,m)$ ili $Q^i(m,m)$. Posmatrajmo dva slučaja.

1° Ako $P^i(m,m)$, $i \models (\forall x)(\forall y)(P(x,y) \Leftrightarrow Q(y,x))$ za $x = y = m$ nam daje da i $Q^i(m,m)$, a iz ranije dokazanog sledi da nije $Q^i(m,m)$, kontradikcija.

2° Ako $Q^i(m,m)$, iz iste formule za $x = y = m$ dobijamo da ipak važi i $P^i(m,m)$ pa kao pod 1° dolazimo do kontradikcije.

(c) Pretpostavimo suprotno, da data formula (označimo je sa F) nije valjana, tj. da postoji model $i = (D, P^i, Q^i)$ za

$$\begin{aligned}\neg F \quad \sim \quad & (\forall x)((\forall y)P(x,y) \Rightarrow Q(x)) \wedge (\forall x)((\exists y)P(y,x) \Rightarrow Q(x))\\ & \wedge(\exists x)\neg Q(x) \wedge (\forall x)(\forall y)(\neg P(x,y) \Rightarrow P(y,x)).\end{aligned} \tag{6.12}$$

Označimo

$F_1 = (\forall x)((\forall y)P(x,y) \Rightarrow Q(x))$,

$F_2 = (\forall x)((\exists y)P(y,x) \Rightarrow Q(x))$,

$F_3 = (\exists x)\neg Q(x)$ i

$F_4 = (\forall x)(\forall y)(\neg P(x,y) \Rightarrow P(y,x))$.

Kako $i \models F_3$, postoji $m \in D$ takvo da nije $Q^i(m)$. Iz $i \models F_1$ i $i \models F_2$ kontrapozicijom dobijamo $i \models (\forall x)(\neg Q(x) \Rightarrow (\exists y)\neg P(x,y))$ i $i \models (\forall x)(\neg Q(x) \Rightarrow (\forall y)\neg P(y,x))$. Uzimajući u oba slučaja $x = m$, iz prve od tih formula dobijamo da postoji $n \in D$ takvo da ne važi $P^i(m,n)$, a iz druge da za sve $y \in D$ ne važi $P^i(y,m)$, pa za $y = n$ ne važi ni $P^i(n,m)$. Ali iz $i \models F_4$ za $x = m$, $y = n$ dobijamo da iz $\neg P^i(m,n)$ sledi $P^i(n,m)$, kontradikcija.

47. Pretpostavimo suprotno, da data formula (označimo je sa F) nije valjana, odnosno da postoji model $i = (D, P^i, f^i)$ za

$$\neg F \sim (\forall x)P(x, f(x)) \wedge (\forall x)\neg P(x, x) \wedge (\exists x)(\forall y)(P(x, y) \Rightarrow P(x, x)).$$

Obeležimo njene podformule sa $F_1 = (\forall x)P(x, f(x))$, $F_2 = (\forall x)\neg P(x, x)$ i $F_3 = (\exists x)(\forall y)(P(x, y) \Rightarrow P(x, x))$. Iz $i \models F_3$ imamo da postoji $m \in D$ takvo da

$$\text{za sve } y \in D, \text{ ako } P^i(m, y), \text{ onda } P^i(m, m). \tag{6.13}$$

$i \models F_1$ znači da, za $x = m$, važi $P^i(m, f(m))$, a $i \models F_2$ (opet za $x = m$) da nije $P^i(m, m)$. Ali iz (6.13) za $y = f(m)$ dobijamo da, ako $P^i(m, f(m))$, onda $P^i(m, m)$, što je nemoguće.

48. Pretpostavimo suprotno, da data formula F nije valjana. To znači da postoji model $i = (D, P^i, Q^i, f^i)$ za njenu negaciju, odnosno za formule

$$\begin{aligned} F_1 &= (\forall x)(\exists y)P(x, f(y)) \\ F_2 &= (\forall x)(\forall y)(\exists z)(P(x, y) \Rightarrow Q(x, z)) \\ F_3 &= (\forall x)(\forall y)(Q(x, y) \Rightarrow Q(x, f(y))) \\ F_4 &= (\exists x)(\forall y)\neg Q(x, f(y)). \end{aligned}$$

Iz F_4 sledi da postoji $m \in D$ takvo da

$$\text{za sve } y \in D \text{ ne važi } Q^i(m, f^i(y)). \tag{6.14}$$

Iz F_1 dobijamo da za svako $x \in D$ postoji $y \in D$ takvo da je $P^i(x, f^i(y))$. Za $x = m$ postoji neko $n \in D$ takvo da $P^i(m, f^i(n))$.

Iz F_2: za sve $x, y \in D$ postoji $z \in D$ takvo da, ako $P^i(x, y)$ onda $Q^i(x, z)$. Za $x = m$ i $y = f^i(n)$ postoji $k \in D$ takvo da, ako $P^i(m, f^i(n))$, onda $Q^i(m, k)$. Kako odranije imamo $P^i(m, f^i(n))$, sledi $Q^i(m, k)$.

Iz F_3: za sve $x, y \in D$, ako $Q^i(x, y)$ onda i $Q^i(x, f^i(y))$. Za $x = m$ i $y = k$, kako je $Q^i(m, k)$, dobijamo i $Q^i(m, f^i(k))$. Međutim, iz (6.14) za $y = k$ imamo da ne važi $Q^i(m, f^i(k))$, kontradikcija.

6.4 Skupovi i relacije

1. $A = \{5, 11, 21\}$, $B = \{0, 1, 4, 9\}$, $C = \{1\}$, $D = \{2, 3, 4, 5\}$.

2. Svaki od datih skupova može se, naravno, zapisati na mnogo načina. Evo nekih mogućnosti:

   (a) $A = \{x \in Z : -5 \leq x \leq 2\}$;

   (b) $B = \{x \in N : x \leq 11 \wedge 2 \nmid x\} = \{2n - 1 : n \in N \wedge n \leq 6\}$;

   (c) $C = \{\sqrt{2} + x : x \in Z \wedge -1 \leq x \leq 2\}$.

3. (a) 2 elementa (to su $\{0, 1\}$ i $\{1, 2\}$).

   (b) 1 element ($\emptyset$).

   (c) 3 elementa.

4. (a) Pošto je $5 = 2 \cdot 1^2 + 3$, sledi da $5 \in A$. Međutim, za sve elemente skupa B imamo $4n^2 + 3 \geq 4 + 3 = 7$, pa $5 \notin B$. Dakle, nije $A \subseteq B$.

   S druge strane, $7 = 4 \cdot 1^2 + 3 \in B$ a, osim broja 5, za sve elemente skupa A je $2n^2 + 3 \geq 2 \cdot 4 + 3 = 11$. Dakle, $7 \notin A$ pa nije ni $B \subseteq A$. Sledi da nije ni $A = B$.

   (b) Kako $35 = 6 \cdot 6 - 1 \in A$ a 35 nije prost, sledi da nije $A \subseteq B$.

   Pošto $2 \in B$ a $2 \notin A$, dobijamo da nije ni $B \subseteq A$, dakle ni $A = B$.

   (c) Lako dobijamo da je $A = B = \{2, 3, 4, 5, 6, 7, 8, 9\}$. Samim tim je i $A \subseteq B$ i $B \subseteq A$.

5. (a) Svaki element skupa B je oblika k^2 za neki paran broj k. Dakle, $k = 2m$ za neko $m \in N$ pa je $k^2 = 4m^2$ odakle $k^2 \in A$. Sledi da $B \subseteq A$.

   (b) Kako $8 = 4 \cdot 2 \in A$ a $8 \notin B$, sledi da nije $A = B$.

6. (a) $A \cup B = \{1, 2, 3, 4\}$, $A \cap B = \{2, 3\}$, $A \setminus B = \{1\}$, $B \setminus A = \{4\}$, $A \triangle B = \{1, 4\}$, $A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$ i $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

   (b) $A \cup B = \{1, 2, \{1\}\}$, $A \cap B = \emptyset$, $A \setminus B = \{\{1\}, 2\}$, $B \setminus A = \{1\}$, $A \triangle B = \{1, 2, \{1\}\}$, $A \times B = \{(\{1\}, 1), (2, 1)\}$ i $P(A) = \{\emptyset, \{\{1\}\}, \{2\}, \{\{1\}, 2\}\}$.

   Napomena. Kad god je, kao pod (b), $A \cap B = \emptyset$, biće $A \setminus B = A$, $B \setminus A = B$ i $A \triangle B = A \cup B$.

7. (a) $A \cup B = \{x \in N : 2 \mid x \vee 3 \mid x\}$, $A \cap B = \{x \in N : 2 \mid x \wedge 3 \mid x\} = \{x \in N : 6 \mid x\} = \{6n : n \in N\}$ i $A \setminus B = \{x \in N : 2 \mid x \wedge 3 \nmid x\}$.

   (b) $A \cup B = \{2n : n \in N\}$, $A \cap B = \{4n : n \in N\}$ i $A \setminus B = \{x \in N : 2 \mid x \wedge 4 \nmid x\} = \{4n - 2 : n \in N\}$.

   Napomena. Kad god je, kao pod (b), $B \subseteq A$, uvek je $A \cup B = A$ i $A \cap B = B$.

8. (a) Za sve $x \in X$ važi:

$$\begin{aligned} x \in A \cup \bar{A} &\sim x \in A \vee x \in \bar{A} \\ &\sim x \in A \vee x \notin A \\ &\sim x \in X \end{aligned}$$

   (Naime, formula u pretposlednjem redu je oblika $p \vee \neg p$, pa je tačna za sve $x \in X$.)

   (b)

$$\begin{aligned} x \in A \cap \bar{A} &\sim x \in A \wedge x \in \bar{A} \\ &\sim x \in A \wedge x \notin A \\ &\sim x \in \emptyset \end{aligned}$$

   (Formula u pretposlednjem redu netačna je za sve $x \in X$.)

9. (a)

$$\begin{aligned} x \in \overline{A \cup B} &\sim \neg x \in A \cup B \\ &\sim \neg(x \in A \vee x \in B) \\ &\sim x \notin A \wedge x \notin B \\ &\sim x \in \bar{A} \wedge x \in \bar{B} \\ &\sim x \in \bar{A} \cap \bar{B} \end{aligned}$$

   (b) Analogno dokazu (a).

10. (a) $$\begin{aligned} x \in A \cup (B \cap C) &\sim x \in A \vee x \in B \cap C \\ &\sim x \in A \vee (x \in B \wedge x \in C) \\ &\sim (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\sim x \in A \cup B \wedge x \in A \cup C \\ &\sim x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

(b) $$\begin{aligned} x \in A \setminus (B \cup C) &\sim x \in A \wedge \neg(x \in B \cup C) \\ &\sim x \in A \wedge \neg(x \in B \vee x \in C) \\ &\sim x \in A \wedge (x \notin B \wedge x \notin C) \\ &\sim (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\ &\sim x \in A \setminus B \wedge x \in A \setminus C \\ &\sim x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

U prvom koraku smo umesto $x \notin B \cup C$ pisali $\neg(x \in B \cup C)$ kako bismo tu formulu dalje mogli transformisati De Morganovim zakonima. Naglasimo, takođe, da četvrti korak nije primena distrubutivnosti (jer se i unutar i van zagrade nalaze konjunkcije) već idempotentnosti i asocijativnosti: ,,duplirali" smo deo $x \in A$ a zatim, kako je jedini veznik u formuli $\wedge$, zagrade rasporedili na najpogodniji način.

11. (a) Dokaz je znatno lakše izvesti polazeći od desne strane jednakosti jer je ona složenija pa nam je jasno kako da je ,,raspišemo".

$$\begin{aligned} x \in (A \cap B) \cup (A \setminus B) &\sim x \in A \cap B \vee x \in A \setminus B \\ &\sim (x \in A \wedge x \in B) \vee (x \in A \wedge x \notin B) \\ &\sim x \in A \wedge (x \in B \vee x \notin B) \\ &\sim x \in A \end{aligned}$$

(b) Iz idempotentnosti unije i definicije operacije $\triangle$ imamo:

$$\begin{aligned} (A \cap B) \cup (A \triangle B) &= ((A \cap B) \cup (A \cap B)) \cup ((A \setminus B) \cup (B \setminus A)) \\ &= ((A \cap B) \cup (A \setminus B)) \cup ((A \cap B) \cup (B \setminus A)) \\ &= A \cup B. \end{aligned}$$

(Koristili smo rezultat dokazan pod (a).)

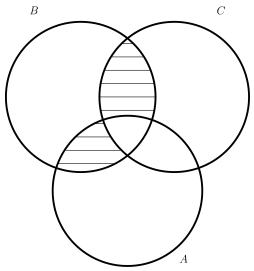
12. Iz teoreme 4.8(c) znamo da iz $A \subseteq B$ i $B \subseteq C$ sledi $A \subseteq C$. Treba još dokazati da uz jači uslov $B \subset C$ sledi $A \subset C$. Pretpostavimo suprotno, da je $A = C$. Ali to bi, zbog $B \subset C$, značilo da je $B \subset A$, što je nemoguće ($A \subseteq B$ i $B \subseteq A$ znače da je $A = B$, kontradikcija sa $B \subset A$).

13. (a) Kako su elementi direktnih proizvoda dva skupa uređeni parovi, treba dokazati da svaki uređeni par pripada skupu s leve strane ako i samo ako pripada skupu s desne strane.

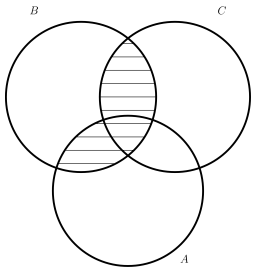
$$\begin{aligned} (x, y) \in A \times (B \cup C) &\sim x \in A \wedge y \in B \cup C \\ &\sim x \in A \wedge (y \in B \vee y \in C) \\ &\sim (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\ &\sim ((x, y) \in A \times B) \vee ((x, y) \in A \times C) \\ &\sim (x, y) \in (A \times B) \cup (A \times C) \end{aligned}$$

(b) Analogno dokazu (a).

14. (a) Ako skiciramo Venove dijagrame navedenih skupova, vidimo da je $((A \cap B) \setminus C) \cup ((B \cap C) \setminus A) \subseteq (A \cup C) \cap B$:



Slika 6.8: Dijagram skupa $((A \cap B) \setminus C) \cup ((B \cap C) \setminus A)$



Slika 6.9: Dijagram skupa $(A \cup C) \cap B$

Dokažimo to.

I način. Za svako x važi

$$\begin{aligned} & x \in ((A \cap B) \setminus C) \cup ((B \cap C) \setminus A) \\ \sim \quad & x \in (A \cap B) \setminus C \vee x \in (B \cap C) \setminus A \\ \sim \quad & (x \in A \wedge x \in B \wedge x \notin C) \vee (x \in B \wedge x \in C \wedge x \notin A) \\ \sim \quad & ((x \in A \wedge x \notin C) \vee (x \in C \wedge x \notin A)) \wedge x \in B \\ \models \quad & (x \in A \vee x \in C) \wedge x \in B \\ \sim \quad & x \in (A \cup C) \cap B. \end{aligned}$$

(U pretposlednjem redu smo koristili pravilo $p \wedge q \models p$.)

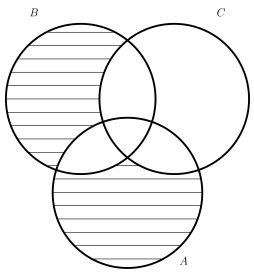
II način. Dovoljno je dokazati da $(A \cap B) \setminus C \subseteq (A \cup C) \cap B$ i $(B \cap C) \setminus A \subseteq (A \cup C) \cap B$, pa će prema teoremi 4.13 i unija skupova s leve strane biti sadržana u $(A \cup C) \cap B$. Imamo:

$$(A \cap B) \setminus C \subseteq A \cap B \subseteq (A \cup C) \cap B$$

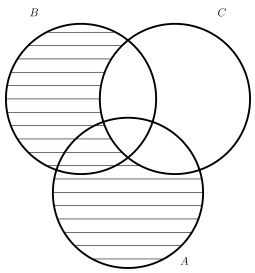
i

$$(B \cap C) \setminus A \subseteq B \cap C \subseteq (A \cup C) \cap B.$$

(b) Ako skiciramo opet Venove dijagrame navedenih skupova, vidimo da je $(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \subseteq (A \cup B) \setminus C$:



Slika 6.10: Dijagram skupa $(A \setminus (B \cup C)) \cup (B \setminus (A \cup C))$



Slika 6.11: Dijagram skupa $(A \cup B) \setminus C$

Dokažimo to.

I način. Za svako x važi

$$\begin{aligned}
& x \in (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \\
\sim\ & x \in (A \setminus (B \cup C)) \vee x \in (B \setminus (A \cup C)) \\
\sim\ & (x \in A \wedge \neg x \in B \cup C) \vee (x \in B \wedge \neg x \in A \cup C) \\
\sim\ & (x \in A \wedge \neg(x \in B \vee x \in C)) \vee (x \in B \wedge \neg(x \in A \vee x \in C)) \\
\sim\ & (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \\
\sim\ & ((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)) \wedge x \notin C \\
\models\ & (x \in A \vee x \in B) \wedge x \notin C \\
\sim\ & x \in (A \cup B) \setminus C.
\end{aligned}$$

II način. Dovoljno je dokazati da $(A\setminus(B\cup C)) \subseteq (A\cup B)\setminus C$ i $(B\setminus(A\cup C)) \subseteq (A\cup B)\setminus C$, pa će i unija skupova s leve strane biti sadržana u $(A\cup B)\setminus C$. Imamo:

$$(A \setminus (B \cup C)) \subseteq A \setminus C \subseteq (A \cup B) \setminus C$$

i

$$(B \setminus (A \cup C)) \subseteq B \setminus C \subseteq (A \cup B) \setminus C.$$

15. (a) Ne. Štaviše, nikad ne važi $P(A)\cap P(B) = \emptyset$, jer uvek $\emptyset \in P(A)\cap P(B)$.

(b) Da. Pretpostavimo suprotno, da je $A \cap B = \emptyset$, ali postoji element $(x, y) \in A^2 \cap B^2$. Tada $(x, y) \in A^2$ znači $x, y \in A$ a $(x, y) \in B^2$ znači $x, y \in B$, pa skupovi A i B ne bi bili disjunktni.

16. (a) Neka je $X \in P(A) \cup P(B)$. To znači da $X \in P(A)$ ili $X \in P(B)$, odnosno $X \subseteq A$ ili $X \subseteq B$. Ali kako $A \subseteq A \cup B$ i $B \subseteq A \cup B$, u oba slučaja iz tranzitivnosti relacije $\subseteq$ dobijamo da $X \subseteq A \cup B$, odnosno $X \in P(A \cup B)$.

(b) Primer kada jednakost ne važi: $A = \{1\}$, $B = \{2\}$. Tada je $A \cup B = \{1, 2\}$, pa je skup $\{1, 2\}$ u $P(A \cup B)$, ali nije ni u $P(A)$ ni u $P(B)$.

17. (a) $\rho = \{(1,3),(1,4),(1,5),(1,6),(2,4),(2,5),(2,6),(3,5),(3,6),(4,6)\}$.

(b) $\sigma = \{(1,1),(1,-1),(2,\sqrt{2}),(2,-\sqrt{2}),(3,\sqrt{3}),(3,-\sqrt{3})\}$.

(c) $\tau = \{(\emptyset,\emptyset),(\emptyset,\{1\}),(\emptyset,\{2\}),(\emptyset,\{1,2\}),(\{1\},\{1\}),(\{1\},\{1,2\}),(\{2\},\{2\}),(\{2\},\{1,2\}),(\{1,2\},\{1,2\})\}$.

(d) $\mu = \{(1,1,1),(1,2,2),(1,3,3),(1,4,4),(1,5,5),(1,6,6),(2,1,2),(2,2,4),(2,3,6),(3,1,3),(3,2,6),(4,1,4),(5,1,5),(6,1,6)\}$.

(e) $\theta = \{(1,2,3),(1,2,4),(1,3,4),(2,3,4)\}$.

18. (a) $\rho \cup \sigma = \{(a,a),(a,c),(a,b),(c,b)\}$

$\rho \cap \sigma = \{(a,a)\}$

$\bar{\rho} = \{(a,b),(b,a),\ (b,b),(b,c),(c,a),(c,b),(c,c)\}$

$\rho^{-1} = \{(a,a),(c,a)\}$

$\rho \circ \sigma = \{(a,a),(a,b)\}$

$\sigma \circ \rho = \{(a,a),(a,c)\}$.

(b) $\leq_R \cup \geq_R = R^2$

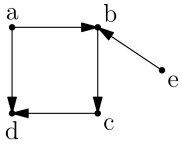
$\leq_R \cap \geq_R = \triangle_R$

$\overline{\leq_R} = >_R$

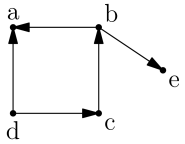
$\leq_R^{-1} = \geq_R$

$\leq_R \circ \geq_R = \leq_R \circ \geq_R = R^2$; obrazložimo ovaj poslednji rezultat: za svaki uređeni par $(x, y) \in R^2$ postoji $z \in R$ koje je veće i od x i od y; stoga $(x, z) \in \leq_R$ i $(z, y) \in \geq_R$ pa $(x, y) \in \leq_R \circ \geq_R$. Analogno i $(x, y) \in \leq_R \circ \geq_R$.

19. $E^{-1} = \{(b, a), (d, a), (c, b), (d, c), (b, e)\}$, $E \circ E = \{(a, c), (b, d), (e, c)\}$ i $(E \circ E) \circ E = \{(a, d), (e, d)\}$. Ovde E^{-1} predstavlja skup grana orijentisanog grafa dobijenog obrtanjem smera svih grana u polaznom orijentisanom grafu.

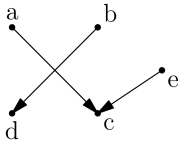


Slika 6.12: Orijentisani graf (V, E)

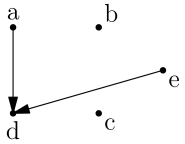


Slika 6.13: Orijentisani graf (V, E^{-1})

Relacija $E \circ E = \{(c, a), (c, e), (d, b)\}$ prikazuje između kojih čvorova postoje putevi dužine 2 (koji se sastoje od 2 grane), a $(E \circ E) \circ E = \{(d, a), (d, e)\}$ između kojih postoje putevi dužine 3:



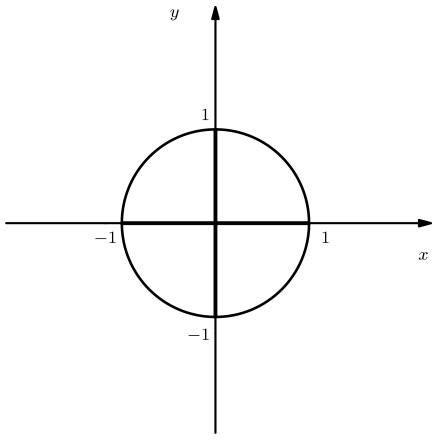
Slika 6.14: Orijentisani graf $(V, E \circ E)$



Slika 6.15: Orijentisani graf $(V, (E \circ E) \circ E)$

20. (a) $\pi_1(\rho) = \{A, C\}$ i $\pi_2(\rho) = \{1, 2\}$.

(b) Skup ρ sadrži tačke koordinatnog sistema koje se nalaze na kružnici s centrom u koordinatnom početku poluprečnika 1 (zaista, uslov $x^2 + y^2 = 1$ prema Pitagorinoj teoremi kaže da je rastojanje tačke (x, y) od koordinatnog početka jednako 1). Stoga je $\pi_1(\rho) = [-1, 1]$ i $\pi_2(\rho) = [-1, 1]$:



21. (a) Neka $(x,y) \in \rho$. Tada $x \in \pi_1(\rho)$ i $y \in \pi_2(\rho)$ pa $(x,y) \in \pi_1(\rho) \times \pi_2(\rho)$.

(b)
$$\begin{aligned} x \in \pi_1(\rho \cup \sigma) &\sim (\exists y)(x,y) \in \rho \cup \sigma \\ &\sim (\exists y)((x,y) \in \rho \vee (x,y) \in \sigma) \\ &\sim (\exists y)(x,y) \in \rho \vee (\exists y)(x,y) \in \sigma \\ &\sim x \in \pi_1(\rho) \vee x \in \pi_1(\sigma) \\ &\sim x \in \pi_1(\rho) \cup \pi_1(\sigma) \end{aligned}$$

(Koristili smo činjenicu da se kvantifikator $\exists$ „slaže" s veznikom $\vee$, videti opet napomenu nakon spiska valjanih formula iz odeljka 3.3.)

(c)
$$\begin{aligned} x \in \pi_1(\rho \cap \sigma) &\sim (\exists y)(x,y) \in \rho \cap \sigma \\ &\sim (\exists y)((x,y) \in \rho \wedge (x,y) \in \sigma) \\ &\models (\exists y)(x,y) \in \rho \wedge (\exists y)(x,y) \in \sigma \\ &\sim x \in \pi_1(\rho) \wedge x \in \pi_1(\sigma) \\ &\sim x \in \pi_1(\rho) \cap \pi_1(\sigma) \end{aligned}$$

Da bismo konstruisali primer za koji jednakost ne važi, za njega treba da, u jedinom koraku u kojem ne važi ekvivalencija, leva strana ne bude posledica desne. Dakle, treba da postoje y_1 za koje $(x,y_1) \in \rho$ i y_2 za koje $(x,y_2) \in \sigma$, ali ne i element y za koji su oba uslova ispunjena. Dakle, (za $x = 1$, $y_1 = 2$ i $y_2 = 3$) uzmimo $\rho = \{(1,2)\}$ i $\sigma = \{(1,3)\}$. Tada je $\pi_1(\rho) = \pi_1(\sigma) = \{1\}$ pa je $\pi_1(\rho) \cap \pi_1(\sigma) = \{1\}$, ali $\rho \cap \sigma = \emptyset$ pa i $\pi_1(\rho \cap \sigma) = \emptyset$.

22. (a)
$$\begin{aligned} &(x,y) \in \rho \circ (\sigma \cup \tau) \\ \sim\ &(\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma \cup \tau) \\ \sim\ &(\exists z)((x,z) \in \rho \wedge ((z,y) \in \sigma \vee (z,y) \in \tau)) \\ \sim\ &(\exists z)(((x,z) \in \rho \wedge (z,y) \in \sigma) \vee ((x,z) \in \rho \wedge (z,y) \in \tau)) \\ \sim\ &(\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma) \vee (\exists z)((x,z) \in \rho \wedge (z,y) \in \tau) \\ \sim\ &(x,y) \in \rho \circ \sigma \vee (x,y) \in \rho \circ \tau \\ \sim\ &(x,y) \in (\rho \circ \sigma) \cup (\rho \circ \tau). \end{aligned}$$

(Ekvivalencija formula u trećem i četvrtom redu dokaza sledi iz toga što se kvantifikator $\exists$ „slaže" sa disjunkcijom.)

(c)
$$\begin{aligned} &(x,y) \in \rho \circ (\sigma \cap \tau) \\ \sim\ &(\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma \cap \tau) \\ \sim\ &(\exists z)((x,z) \in \rho \wedge ((z,y) \in \sigma \wedge (z,y) \in \tau)) \\ \sim\ &(\exists z)(((x,z) \in \rho \wedge (z,y) \in \sigma) \wedge ((x,z) \in \rho \wedge (z,y) \in \tau)) \quad (6.15) \\ \models\ &(\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma) \wedge (\exists z)((x,z) \in \rho \wedge (z,y) \in \tau) \quad (6.16) \\ \sim\ &(x,y) \in \rho \circ \sigma \wedge (x,y) \in \rho \circ \tau \\ \sim\ &(x,y) \in (\rho \circ \sigma) \cap (\rho \circ \tau). \end{aligned}$$

Ovde smo u (6.15) koristili idempotentnost ($p \sim p \wedge p$) da bismo „duplirali" formulu $(x,z) \in \rho$. Kako se kvantifikator $\forall$ „ne slaže" sa disjunkcijom (videti opet spisak valjanih formula i komentare ispod), imamo samo da formula u četvrtom redu ima za posledicu onu u petom, ali nisu ekvivalentne.

(b) i (d) se dokazuju analogno.

Primer da pod (c) ne mora važiti jednakost konstruišemo posmatrajući jedini korak u gornjem dokazu u kojem je izvedena formula samo posledica prethodne, a ne ekvivalentna s njom. Preciznije, konstruisaćemo relacije tako da važi (6.16) ali ne i (6.15). Recimo, ako uzmemo $x = 1$ i $y = 4$, treba da postoji z (npr. $z = 2$) takav da $(1,2) \in \rho$ i $(2,4) \in \sigma$, kao i z (npr. $z = 3$) takav da $(1,3) \in \rho$ i $(3,4) \in \tau$, ali ne i z takvo da $(1,z) \in \rho$, $(z,4) \in \sigma$ i $(z,4) \in \tau$.

Neka je, dakle, $A = \{1,2,3,4\}$, $\rho = \{(1,2),(1,3)\}$, $\sigma = \{(2,4)\}$ i $\tau = \{(3,4)\}$. Tada je:

$$\begin{aligned} \sigma \cap \tau &= \emptyset \\ \rho \circ (\sigma \cap \tau) &= \emptyset \\ \rho \circ \sigma &= \{(1,4)\} \\ \rho \circ \tau &= \{(1,4)\} \\ \rho \circ \sigma \cap \rho \circ \tau &= \{(1,4)\}. \end{aligned}$$

Dakle, zaista ne mora biti $\rho \circ (\sigma \cap \tau) = \rho \circ \sigma \cap \rho \circ \tau$.

23. U prethodnom zadatku dokazano je

$$\begin{aligned} & (x,y) \in \rho \circ (\sigma \cap \tau) \\ \sim\ & (\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma \wedge (z,y) \in \tau). \end{aligned} \tag{6.17}$$

kao i, s druge strane,

$$\begin{aligned} & (x,y) \in (\rho \circ \sigma) \cap (\rho \circ \tau) \\ \sim\ & (\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma) \wedge (\exists t)((x,t) \in \rho \wedge (t,y) \in \tau) \end{aligned} \tag{6.18}$$

Uvek važi (6.17)$\models$(6.18). S druge strane, iz uslova datog u zadatku imamo $(x,z) \in \rho \wedge (x,t) \in \rho \Rightarrow z = t$, pa sledi

$$\begin{aligned} (6.18) \quad \sim\ & (\exists z)(\exists t)((x,z) \in \rho \wedge (z,y) \in \sigma \wedge (x,t) \in \rho \wedge (t,y) \in \tau) \\ \models\ & (\exists z)(\exists t)((x,z) \in \rho \wedge (z,y) \in \sigma \wedge (x,t) \in \rho \wedge (t,y) \in \tau \wedge z = t) \\ \models\ & (\exists z)(\exists t)((x,z) \in \rho \wedge (z,y) \in \sigma \wedge (z,y) \in \tau). \end{aligned}$$

24. Po teoremi 4.13(b) $\rho \subseteq \sigma \cap \tau$ znači $\rho \subseteq \sigma$ i $\rho \subseteq \tau$. Na osnovu teoreme 4.34 je $\rho \circ \tau \subseteq \sigma \circ \tau$ i $\sigma \circ \rho \subseteq \sigma \circ \tau$, pa je prema teoremi 4.13(a) i $(\rho \circ \tau) \cup (\sigma \circ \rho) \subseteq \sigma \circ \tau$.

25. (a)
$$\begin{aligned} x \in \theta[A \cap B] \quad \sim\ & (\exists y)(y \in A \cap B \wedge x\theta y) \\ \sim\ & (\exists y)(y \in A \wedge y \in B \wedge x\theta y) \\ \models\ & (\exists y)(y \in A \wedge x\theta y) \wedge (\exists y)(y \in B \wedge x\theta y) \\ \sim\ & x \in \theta[A] \wedge x \in \theta[B] \\ \sim\ & x \in \theta[A] \cap \theta[B] \end{aligned}$$

(b) Neka je $X = \{a,b\}, A = \{a\}, B = \{b\}$ i $\theta = X^2$. Tada je $A \cap B = \emptyset$, dakle $\theta[A \cap B] = \emptyset$, ali $\theta[A] = \theta[B] = \{a,b\}$, pa $\theta[A] \cap \theta[B] = \{a,b\}$.

Napomena. Definiciju skupa $\theta[Y]$ je uopštenje prve projekcije skupa ($\pi_1(\theta)$ je ustvari $\theta[X]$), kao i direktne slike skupa (definicija 5.21), u slučaju kada je θ funkcija.

26. $\rho \cup \sigma$: Neka je $x \in A$. Pošto je ρ neograničena, postoji $y \in A$ takvo da $(x, y) \in \rho$, pa samim tim i $(x, y) \in \rho \cup \sigma$.

$\rho \circ \sigma$: Neka je $x \in A$. Pošto je ρ neograničena, postoji $y \in A$ takvo da $(x, y) \in \rho$. Kako je i σ neograničena, postoji $z \in A$ takvo da $(y, z) \in \sigma$. Iz $(x, y) \in \rho$ i $(y, z) \in \sigma$ sledi $(x, z) \in \rho \circ \sigma$, pa je i $\rho \circ \sigma$ neograničena.

27. Koristeći definicije operacija nad relacijama dobijamo:

$$\begin{aligned}
(x,y) \in \rho^{-1} \circ \overline{(\rho \circ \sigma)} &\sim (\exists z)((x,z) \in \rho^{-1} \wedge (z,y) \in \overline{(\rho \circ \sigma)}) \\
&\sim (\exists z)((z,x) \in \rho \wedge \neg(z,y) \in \rho \circ \sigma) \\
&\sim (\exists z)((z,x) \in \rho \wedge \neg(\exists t)((z,t) \in \rho \wedge (t,y) \in \sigma)) \\
&\sim (\exists z)((z,x) \in \rho \wedge (\forall t)\neg((z,t) \in \rho \wedge (t,y) \in \sigma)) \\
&\sim (\exists z)((z,x) \in \rho \wedge (\forall t)((z,t) \in \rho \Rightarrow (t,y) \notin \sigma)) \\
&\models (\exists z)((z,x) \in \rho \wedge ((z,x) \in \rho \Rightarrow (x,y) \notin \sigma)) \\
&\models (\exists z)(x,y) \notin \sigma \\
&\sim (x,y) \in \overline{\sigma}.
\end{aligned}$$

Da je formula u šestom redu posledica one u petom sledi iz teoreme 3.27(a). U narednom koraku koristili smo pravilo $p, p \Rightarrow q \models q$, a u poslednjem smo izostavili kvantifikator jer on ne deluje ni na jednu pojavu promenljive.

Konstruišimo primer koji pokazuje da može biti $\rho^{-1} \circ \overline{(\rho \circ \sigma)} \subset \overline{\sigma}$. To možemo postići npr. tako što obezbedimo da u pretposlednjem redu ne važi ekvivalencija. Uzmimo, recimo, da je $x = 1$, $y = 2$ i $(x, y) \notin \sigma$, ali da ne postoji z takvo da $(z, x) \in \rho$. Dakle, neka su na skupu $A = \{1, 2\}$ relacije $\rho = \sigma = \emptyset$; tada je i $\rho^{-1} = \emptyset$ pa i $\rho^{-1} \circ \overline{(\rho \circ \sigma)} = \emptyset$. S druge strane, $\overline{\sigma} = A^2$ pa npr. $(1, 2) \in \overline{\sigma}$.

28.
$$\begin{aligned}
(x,y) \in (\rho \circ \sigma) \cap \tau &\sim (x,y) \in \rho \circ \sigma \wedge (x,y) \in \tau \\
&\sim (\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma) \wedge (x,y) \in \tau \\
&\sim (\exists z)((x,z) \in \rho \wedge (z,y) \in \sigma \wedge (x,y) \in \tau) \\
&\models (\exists z)((x,z) \in \rho \wedge (x,y) \in \tau). \qquad (6.19)
\end{aligned}$$

S druge strane imamo

$$\begin{aligned}
&(x,y) \in (\rho \circ \rho^{-1}) \circ \tau \\
\sim\ &(\exists t)((x,t) \in \rho \circ \rho^{-1} \wedge (t,y) \in \tau) \\
\sim\ &(\exists t)((\exists z)((x,z) \in \rho \wedge (z,t) \in \rho^{-1}) \wedge (t,y) \in \tau) \\
\sim\ &(\exists t)(\exists z)(((x,z) \in \rho \wedge (t,z) \in \rho) \wedge (t,y) \in \tau) \\
\sim\ &(\exists z)(\exists t)((x,z) \in \rho \wedge (t,z) \in \rho \wedge (t,y) \in \tau). \qquad (6.20)
\end{aligned}$$

Iz tvrđenja 3.27(b) sledi da iz $(x, z) \in \rho \wedge (x, y) \in \tau$ sledi $(\exists t)((t, z) \in \rho \wedge (t, y) \in \tau)$, pa (6.19) implicira (6.20).

Da bismo konstruisali primer kada je $(\rho \circ \sigma) \cap \tau \subset (\rho \circ \rho^{-1}) \circ \tau$, posmatrajmo jedini korak u gornjem izvođenju u kojem nije važila ekvivalencija. Uzmimo da je $x = 1$, $z = 2$, $y = 3$ i da važi $(x, z) \in \rho$ i $(x, y) \in \tau$ ali ne i $(z, y) \in \sigma$. Dakle, neka $\rho = \{(1, 2)\}$, $\sigma = \emptyset$ i $\tau = \{(1, 3)\}$. Tada je $\rho \circ \sigma = \emptyset$ pa je i $(\rho \circ \sigma) \cap \tau = \emptyset$. S druge strane, $\rho \circ \rho^{-1} = \{(1, 1)\}$ i $(\rho \circ \rho^{-1}) \circ \tau = \{(1, 3)\}$.

Napomena. U razvijanju izraza $(x, y) \in (\rho \circ \rho^{-1}) \circ \tau$ uveli smo prvo promenljivu t, pa onda z. To smo učinili stoga što tako dobijamo formulu koja više liči na (6.19), a naravno to ne utiče na značenje formule.

29.
$$\begin{aligned} & (x,y) \in \rho \cap (\tau \circ \sigma) \\ \sim\ & (x,y) \in \rho \wedge (x,y) \in \tau \circ \sigma \\ \sim\ & (x,y) \in \rho \wedge (\exists z)((x,z) \in \tau \wedge (z,y) \in \sigma) \\ \sim\ & (\exists z)((x,y) \in \rho \wedge (x,z) \in \tau \wedge (z,y) \in \sigma). \end{aligned} \tag{6.21}$$

S druge strane je

$$\begin{aligned} & (x,y) \in (\rho \cap \tau) \circ \sigma \\ \sim\ & (\exists z)((x,z) \in \rho \cap \tau \wedge (z,y) \in \sigma) \\ \sim\ & (\exists z)((x,z) \in \rho \wedge (x,z) \in \tau \wedge (z,y) \in \sigma). \end{aligned} \tag{6.22}$$

Ostaje da dokažemo da su formule (6.21) i (6.22) ekvivalentne uz date pretpostavke.

(6.21)⇒(6.22). $(z,y) \in \sigma$ nam daje $(y,z) \in \sigma^{-1}$. Iz toga i $(x,y) \in \rho$ dobijamo $(x,z) \in \rho \circ \sigma^{-1}$, pa kako je $\rho \circ \sigma^{-1} \subseteq \rho$, zaključujemo $(x,z) \in \rho$.

(6.22)⇒(6.21). Iz $(x,z) \in \rho$ i $(z,y) \in \sigma$ dobijamo $(x,y) \in \rho \circ \sigma$, što sa $\rho \circ \sigma \subseteq \rho$ implicira $(x,y) \in \rho$.

30.
$$\begin{aligned} & (x,y) \in (\rho \cup (\sigma \circ \tau))^* \\ \sim\ & (x+1,y+1) \in \rho \cup (\sigma \circ \tau) \\ \sim\ & (x+1,y+1) \in \rho \vee (x+1,y+1) \in (\sigma \circ \tau) \\ \sim\ & (x+1,y+1) \in \rho \vee (\exists z)((x+1,z) \in \sigma \wedge (z,y+1) \in \tau). \end{aligned} \tag{6.23}$$

S druge strane je

$$\begin{aligned} & (x,y) \in \rho^* \cup (\sigma^* \circ \tau^*) \\ \sim\ & (x,y) \in \rho^* \vee (x,y) \in (\sigma^* \circ \tau^*) \\ \sim\ & (x+1,y+1) \in \rho \vee (\exists t)((x,t) \in \sigma^* \wedge (t,y) \in \tau^*) \\ \sim\ & (x+1,y+1) \in \rho \vee \\ & (\exists t)((x+1,t+1) \in \sigma \wedge (t+1,y+1) \in \tau). \end{aligned} \tag{6.24}$$

Ako važi (6.23), onda važi i (6.24) za $t = z-1$. Obratno, ako važi (6.24), važi i (6.23) za $z = t+1$. Dakle,

$$(x,y) \in (\rho \cup (\sigma \circ \tau))^* \sim (x,y) \in \rho^* \cup (\sigma^* \circ \tau^*),$$

što znači da je $(\rho \cup (\sigma \circ \tau))^* = \rho^* \cup (\sigma^* \circ \tau^*)$.

31. Odgovore na pitanja iz zadatka dajemo u sledećoj tablici:

	ρ	σ	τ	ω	θ_1	θ_2
refleksivnost	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
irefleksivnost	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$
simetričnost	$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$
antisimetričnost	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
tranzitivnost	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$

Većina polja popunjava se na očigledan način, samo neka zahtevaju dodatno objašnjenje. Npr. simetričnost poslednje dve relacije: ako je x brat osobe y, ne mora i y biti brat osobe x (jer y može biti ženskog pola), ali mora ako su u pitanju muškarci. Tranzitivnost relacije ω: ako su x i y dede istog unuka (dakle, imaju zajedničkog potomka) a y i z takođe, ne moraju i x i z imati zajedničkog potomka.

32. (a) Definišimo relaciju na skupu R: $x\rho y$ ako i samo ako $|x-y|<2$. Ona je očigledno refleksivna i simetrična ali nije tranzitivna: $0\rho 1$ i $1\rho 2$ ali ne i $0\rho 2$.

(b) Relacija $\leq$ (na bilo kom od skupova $N, Z, R, \ldots$) je refleksivna i tranzitivna, ali ne i simetrična.

(c) Prazna relacija $\emptyset$ je simetrična i tranzitivna, ali ne i refleksivna. (Mogli smo uzeti npr. i relaciju $\triangle_B$ na skupu A takvom da je $B \subset A$.)

(d) Definišimo relaciju na skupu R: $x\sigma y$ ako i samo ako $x-y<2$. Ona je očigledno refleksivna, ali nije simetrična: $1\sigma 4$ ali ne i $4\sigma 1$. Nije ni tranzitivna: $2\sigma 1$ i $1\sigma 0$ ali ne i $2\rho 0$.

(e) Relacija $\neq$ na bilo kom skupu (npr. na N) je simetrična ali nije refleksivna ni tranzitivna: $1\neq 2$ i $2\neq 1$ ali ne i $1\neq 1$. (Još jedan primer je relacija iz zadatka 24 prethodne glave.)

(f) Relacija $<$ (na bilo kom od skupova $N, Z, R, \ldots$) je tranzitivna, ali nije ni refleksivna ni simetrična.

33. Neka su ρ i σ refleksivne. Iz $\triangle_A \subseteq \rho$ sledi da je $\triangle_A \subseteq \rho\cup\sigma$, a iz $\triangle_A \subseteq \rho$ i $\triangle_A \subseteq \sigma$ da je $\triangle_A \subseteq \rho\cap\sigma$ (teorema 4.13).

Za svako $x\in A$ iz $(x,x)\in\rho$ sledi $(x,x)\in\rho^{-1}$, pa je i ρ^{-1} refleksivna.

Ako $\triangle_A \subseteq \rho$ i $\triangle_A \subseteq \sigma$, imamo $\triangle_A = \triangle_A\circ\triangle_A \subseteq \rho\circ\sigma$, te je i $\rho\circ\sigma$ refleksivna.

34. (a) Neka su ρ i σ irefleksivne. Za svako $x\in A$, pošto $(x,x)\notin\rho$ i $(x,x)\notin\sigma$, imamo $(x,x)\notin\rho\cup\sigma$ i $(x,x)\notin\rho\cap\sigma$, pa su i $\rho\cup\sigma$ i $\rho\cap\sigma$ irefleksivne.

Za svako $x\in A$ iz $(x,x)\notin\rho$ sledi $(x,x)\notin\rho^{-1}$, pa je i ρ^{-1} irefleksivna.

(b) Neka je $A=\{1,2\}$, $\rho=\{(1,2)\}$ i $\sigma=\{(2,1)\}$. Te dve relacije su očigledno irefleksivne, ali $\rho\circ\sigma=\{(1,1)\}$ nije.

35. (a) Neka su ρ i σ simetrične, tj. važi $\rho^{-1}=\rho$ i $\sigma^{-1}=\sigma$. Tada je $(\rho\cup\sigma)^{-1} = \rho^{-1}\cup\sigma^{-1} = \rho\cup\sigma$, pa je i $\rho\cup\sigma$ simetrična.

Analogno je $(\rho\cap\sigma)^{-1}=\rho^{-1}\cap\sigma^{-1}=\rho\cap\sigma$, pa je i $\rho\cap\sigma$ simetrična.

Takođe, $(\rho^{-1})^{-1}=\rho=\rho^{-1}$, te je i ρ^{-1} simetrična.

(b) Ako je $\rho\circ\sigma=\sigma\circ\rho$, onda imamo $(\rho\circ\sigma)^{-1}=\sigma^{-1}\circ\rho^{-1}=\sigma\circ\rho=\rho\circ\sigma$.

Obratno, ako je $\rho\circ\sigma$ simetrična, onda $\rho\circ\sigma=(\rho\circ\sigma)^{-1}=\sigma^{-1}\circ\rho^{-1}=\sigma\circ\rho$.

36. (a) Ako $(x,y)\in\rho^{-1}$ i $(y,x)\in\rho^{-1}$, imamo $(y,x)\in\rho$ i $(x,y)\in\rho$. Kako je ρ antisimetrična, sledi $x=y$.

Takođe, ako (x,y), $(y,x)\in\rho\cap\sigma$ to povlači $(x,y),(y,x)\in\rho$, pa opet $x=y$.

(b) Neka je prvo $\rho=\{(1,2)\}$ i $\sigma=\{(2,1)\}$. Ove relacije su antisimetrične ali $\rho\cup\sigma=\{(1,2),(2,1)\}$ očigledno nije antisimetrična.

Dalje, neka je $\rho=\{(1,2),(4,3)\}$ i $\sigma=\{(2,4),(3,1)\}$. I ove relacije su antisimetrične ali $\rho\circ\sigma=\{(1,4),(4,1)\}$ nije.

37. Neka su ρ i σ tranzitivne. Neka $(x,y),(y,z)\in\rho\cap\sigma$. Odatle dobijamo $(x,y),(y,z)\in\rho$, što povlači $(x,z)\in\rho$, kao i $(x,y),(y,z)\in\sigma$, odakle $(x,z)\in\sigma$. Dakle, $(x,z)\in\rho\cap\sigma$, pa je $\rho\cap\sigma$ tranzitivna.

Prema teoremi 4.32(c) je $\rho^{-1}\circ\rho^{-1}=(\rho\circ\rho)^{-1}=\rho^{-1}$, pa je i ρ^{-1} tranzitivna.

(b) Kontraprimer za $\rho\cup\sigma$: neka je $A=\{1,2,3\}$, $\rho=\{(1,2)\}$ i $\sigma=\{(2,3)\}$. Ove relacije su tranzitivne, ali $\rho\cup\sigma=\{(1,2),(2,3)\}$ nije.

Kontraprimer za $\rho\circ\sigma$: neka je $A=\{1,2,3,4,5\}$, $\rho=\{(1,2),(3,4)\}$ i $\sigma=\{(2,3),(4,5)\}$. Ove relacije su tranzitivne, ali $\rho\circ\sigma=\{(1,3),(3,5)\}$ nije.

38. Iz $\rho\subseteq\sigma$ i teoreme 4.34 imamo $\rho\circ\sigma\circ\rho\subseteq\rho\circ\sigma\circ\sigma$. Iz tranzitivnosti relacije σ sledi $\sigma\circ\sigma\subseteq\sigma$ pa je $\rho\circ\sigma\circ\sigma\subseteq\rho\circ\sigma$. Dalje, iz $\rho=\triangle_A\circ\rho$ i refleksivnosti relacije σ (tj. $\triangle_A\subseteq\sigma$) dobijamo $\rho\circ\sigma=\triangle_A\circ\rho\circ\sigma\subseteq\sigma\circ\rho\circ\sigma$.

39. S jedne strane, zbog $\rho\subseteq\sigma$ i tranzitivnosti σ imamo $\sigma\circ\rho\circ\sigma\subseteq\sigma\circ\sigma\circ\sigma\subseteq\sigma\circ\sigma\subseteq\sigma$. Obratno, zbog refleksivnosti ρ i uslova $\rho\subseteq\sigma$ imamo $\sigma=\sigma\circ\triangle_X\circ\triangle_X\subseteq\sigma\circ\rho\circ\rho\subseteq\sigma\circ\rho\circ\sigma$.

40. Pošto je dato $\rho\circ\sigma\subseteq\sigma\circ\rho$, treba još dokazati da je $\sigma\circ\rho\subseteq\rho\circ\sigma$. Ali zbog simetričnosti relacija ρ i σ imamo $\rho^{-1}=\rho$ i $\sigma^{-1}=\sigma$, pa primenjujući teoreme 4.32(c) i 4.34(a) dobijamo

$$\sigma\circ\rho=\sigma^{-1}\circ\rho^{-1}=(\rho\circ\sigma)^{-1}\subseteq(\sigma\circ\rho)^{-1}=\rho^{-1}\circ\sigma^{-1}=\rho\circ\sigma.$$

41. Iz tranzitivnosti ρ dobijamo $\rho\circ\rho\subseteq\rho$. Sledi

$$(\rho\circ\rho^{-1})\circ(\rho\circ\rho^{-1})=\rho\circ(\rho^{-1}\circ\rho)\circ\rho^{-1}\subseteq\rho\circ\rho\circ\rho^{-1}\subseteq\rho\circ\rho^{-1}$$

pa je i $\rho\circ\rho^{-1}$ tranzitivna.

42. Pretpostavimo da $(x,y),(y,z)\in\rho\circ\sigma$. To znači da postoje s i t takvi da $(x,s)\in\rho$, $(s,y)\in\sigma$, $(y,t)\in\rho$ i $(t,z)\in\sigma$. Iz $(s,y)\in\sigma$ i $(y,t)\in\rho$ sledi da $(s,t)\in\sigma\circ\rho\subseteq\triangle_A$, dakle $s=t$. Sada iz $(x,s)\in\rho$ i $(s,z)\in\sigma$ dobijamo $(x,z)\in\rho\circ\sigma$.

43. (a) Neka $(x,y),(y,z)\in\sigma_n$. Tada $x+n\le y$ i $y\le y+n\le z$, pa $x+n\le z$, tj. $(x,z)\in\sigma_n$.

(b) Neka je $m\le n$. Ako $(x,y)\in\sigma_n$, sledi $x+n\le y$ odakle $x+m\le y$, tj. $(x,y)\in\sigma_m$. Obrnuto, neka $\sigma_n\subseteq\sigma_m$. Pošto $(0,n)\in\sigma_n\subseteq\sigma_m$, imamo $0+m\le n$.

(c) Ako $(x,y)\in\sigma_m\circ\sigma_n$, to znači da za neko $z\in N$ važi $(x,z)\in\sigma_m$ i $(z,y)\in\sigma_n$. Tada $x+m+n\le z+n\le y$, tj. $(x,y)\in\sigma_{m+n}$.

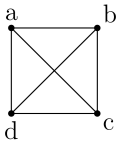
Napomena. Deo (a) sledi iz (c) i (b): $\sigma_n\circ\sigma_n\subseteq\sigma_{2n}\subseteq\sigma_n$.

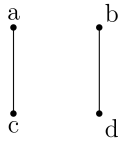
44. Odgovarajuće relacije ekvivalencije predstavićemo tablicama i grafovima:

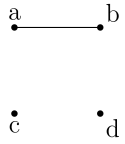
	a	b	c	d
a	$\top$	$\top$	$\top$	$\top$
b	$\top$	$\top$	$\top$	$\top$
c	$\top$	$\top$	$\top$	$\top$
d	$\top$	$\top$	$\top$	$\top$

	a	b	c	d
a	$\top$	$\bot$	$\top$	$\bot$
b	$\bot$	$\top$	$\bot$	$\top$
c	$\top$	$\bot$	$\top$	$\bot$
d	$\bot$	$\top$	$\bot$	$\top$

	a	b	c	d
a	$\top$	$\top$	$\bot$	$\bot$
b	$\top$	$\top$	$\bot$	$\bot$
c	$\bot$	$\bot$	$\top$	$\bot$
d	$\bot$	$\bot$	$\bot$	$\top$







45. (a) R: Svaka prava p paralelna je samoj sebi.

S: Ako je $p \parallel q$, onda je i $q \parallel p$.

T: Ako je $p \parallel q$ i $q \parallel r$, onda je i $p \parallel r$.

(b) R: Svaka duž a podudarna je samoj sebi.

S: Ako je $a \cong b$, onda je i $b \cong a$.

T: Ako je $a \cong b$ i $b \cong c$, onda je i $a \cong c$.

(Analogno su relacije ekvivalencije i podudarnost uglova, podudarnost trouglova itd.)

(c) R: Za svako $a \in N$ $a \equiv_m a$ znači da $m \mid a - a$, što je tačno jer je 0 deljiva svakim prirodnim brojem.

S: Neka je $a \equiv_m b$, tj. $m \mid a - b$. Ali $b - a = -(a - b)$, tj. ti brojevi se razlikuju samo po predznaku. Stoga $m \mid b - a$, dakle $b \equiv_m a$.

T: Neka je $a \equiv_m b$ i $b \equiv_m c$. To znači da $m \mid a - b$ i $m \mid b - c$. Kako je $a - c = (a - b) + (b - c)$, prema teoremi 1.7 je i $m \mid a - c$, tj. $a \equiv_m c$.

(d) R: Za svako $a \in R$ $a\rho a$ znači da $a - a \in Q$, što je tačno.

S: Neka je $a\rho b$, tj. $a - b \in Q$. Tada je i broj $b - a = -(a - b)$ racionalan, pa $b\rho a$.

T: Neka je $a\rho b$ i $b\rho c$; dakle $a-b, b-c \in Q$. Tada i $a-c = (a-b)+(b-c) \in Q$, pa $a\rho c$.

(e) R: Neka je $x \in Z$. Tada $x + x = 2x \in P$, pa $x \sim x$.

S: Neka važi $x \sim y$, odnosno $x + y \in P$. Tada i $y + x \in P$ pa $y \sim x$.

T: Neka $x \sim y$ i $y \sim z$. To znači da $x + y \in P$ i $y + z \in P$, pa i $x + z = (x + y) + (y + z) - 2y \in P$, što znači $x \sim z$.

46. Relacija normalnosti nije refleksivna (štaviše, nijedna prava nije normalna na sebe) pa nije relacija ekvivalencije.

47. (a) R: Svaki zaposleni radi u istoj prostoriji sa samim sobom.

S: Ako x radi u istoj prostoriji sa y, onda i y radi u istoj prostoriji kao x.

T: Ako x i y rade u istoj prostoriji i y i z rade u istoj prostoriji, onda i x i z rade u istoj prostoriji.

(b) Obeležimo radnike skraćeno prema početnim slovima imena (A=Arsenije itd.). Dati uslovi govore da: 1) $[A] = [C]$; 2) $[C]$, $[D]$ i $[F]$ su različite klase ekvivalencije i 3) $[F] = [B] = [E]$. Dakle, imamo 3 klase ekvivalencije: $\{A, C\}$, $\{B, E, F\}$ i $\{D\}$. Sledi da relaciju ρ možemo prikazati tablicom:

ρ	A	B	C	D	E	F
A	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
B	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$
C	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
D	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
E	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$
F	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$

48. R: Neka $(a,b) \in R^2$. Važi: $(a,b)\rho(a,b)$ akko je $a-b=a-b$, što je očigledno ispunjeno.

    S: Neka važi $(a,b)\rho(c,d)$. To znači da je $a-b=c-d$, pa je i $c-d=a-b$, što znači $(c,d)\rho(a,b)$.

    T: Neka je $(a,b)\rho(c,d)$ i $(c,d)\rho(e,f)$. Odatle dobijamo $a-b=c-d$ i $c-d=e-f$, pa je i $a-b=e-f$, tj. $(a,b)\rho(e,f)$.

49. R: Neka je $(x,y) \in R^2$. Imamo: $(x,y)\rho(x,y)$ akko je $x+y=x+y$ i $x^2+y^2=x^2+y^2$, što je očigledno tačno.

    S: Neka je $(x,y)\rho(z,t)$. To znači da je $x+y=z+t$ i $x^2+y^2=z^2+t^2$. Ali tada je i $z+t=x+y$ i $z^2+t^2=x^2+y^2$, što znači $(z,t)\rho(x,y)$.

    T: Neka je $(x,y)\rho(z,t)$ i $(z,t)\rho(u,v)$. To znači da je $x+y=z+t$ i $x^2+y^2=z^2+t^2$, kao i $z+t=u+v$ i $z^2+t^2=u^2+v^2$. Odatle dobijamo $x+y=u+v$ i $x^2+y^2=u^2+v^2$, što znači $(x,y)\rho(u,v)$.

    Napomena. Čitalac može pokušati da dokaže da je ρ ustvari relacija jednakosti: $\rho=\triangle_{R^2}$.

50. Iz teoreme 4.42 dobijamo $\rho\circ\rho=\rho$, pa imamo

$$\begin{aligned}
& (x,y)\in\rho\cap(\sigma\circ(\rho\cap\tau))\\
\sim\ & (x,y)\in\rho\wedge(x,y)\in\sigma\circ(\rho\cap\tau)\\
\sim\ & (x,y)\in\rho\wedge(\exists z)((x,z)\in\sigma\wedge(z,y)\in\rho\cap\tau)\\
\sim\ & (x,y)\in\rho\wedge(\exists z)((x,z)\in\sigma\wedge(z,y)\in\rho\wedge(z,y)\in\tau)\\
\sim\ & (\exists z)((x,y)\in\rho\wedge(x,z)\in\sigma\wedge(y,z)\in\rho\wedge(z,y)\in\tau)\\
\models\ & (\exists z)((x,z)\in\rho\circ\rho\wedge(x,z)\in\sigma\wedge(z,y)\in\tau)\\
\sim\ & (\exists z)((x,z)\in\rho\wedge(x,z)\in\sigma\wedge(z,y)\in\tau)\\
\sim\ & (\exists z)((x,z)\in\rho\cap\sigma\wedge(z,y)\in\tau)\\
\sim\ & (x,y)\in(\rho\cap\sigma)\circ\tau
\end{aligned}$$

51. R: Neka je $x\in A$. Kako su ρ i σ refleksivne, imamo da je $(x,x)\in\rho$ i $(x,x)\in\sigma$ pa i $(x,x)\in\rho\cap\sigma$.

    S: Neka $(x,y)\in\rho\cap\sigma$. To znači da $(x,y)\in\rho$, što sa simetričnošću relacije ρ daje $(y,x)\in\rho$. Slično dobijamo i $(y,x)\in\sigma$, pa $(y,x)\in\rho\cap\sigma$.

    T: Iz $\rho\circ\rho=\rho$ i $\sigma\circ\sigma=\sigma$ sledi $(\rho\cap\sigma)\circ(\rho\cap\sigma)\subseteq(\rho\circ\rho)\cap(\rho\circ\sigma)\cap(\sigma\circ\rho)\cap(\sigma\circ\sigma)\subseteq(\rho\circ\rho)\cap(\sigma\circ\sigma)\subseteq\rho\cap\sigma$.

    (Pretposlednja inkluzija važi zato što je $A\cap B\subseteq A$ za proizvoljne skupove A i B.)

    Mogli smo se i pozvati na zadatke 33, 35 i 37, gde je na drugi način dokazivano da se osobine refleksivnosti, simetričnosti i tranzitivnosti prenose na presek relacija.

52. R: ρ je refleksivna odakle $\triangle_A\subseteq\rho$ i $\triangle_A=\triangle_A^{-1}\subseteq\rho^{-1}$ (teorema 4.32) pa $\triangle_A\subseteq\rho\cap\rho^{-1}$. Sledi da je $\rho\cap\rho^{-1}$ refleksivna.

    S: $(\rho\cap\rho^{-1})^{-1}=\rho^{-1}\cap(\rho^{-1})^{-1}=\rho^{-1}\cap\rho=\rho\cap\rho^{-1}$.

    T: Iz tranzitivnosti relacije ρ imamo $\rho\circ\rho\subseteq\rho$ i $\rho^{-1}\circ\rho^{-1}=(\rho\circ\rho)^{-1}\subseteq\rho^{-1}$ (koristili smo teoremu 4.34) pa

$$\begin{aligned}
(\rho\cap\rho^{-1})\circ(\rho\cap\rho^{-1}) &\subseteq ((\rho\cap\rho^{-1})\circ\rho)\cap((\rho\cap\rho^{-1})\circ\rho^{-1})\\
&\subseteq (\rho\circ\rho)\cap(\rho^{-1}\circ\rho)\cap(\rho\circ\rho^{-1})\cap(\rho^{-1}\circ\rho^{-1})\\
&\subseteq \rho\cap(\rho^{-1}\circ\rho)\cap(\rho\circ\rho^{-1})\cap\rho^{-1}\subseteq\rho\cap\rho^{-1}.
\end{aligned}$$

53. ($\Leftarrow$) Pretpostavimo prvo da važi $\rho \circ \rho^{-1} = \rho$.

R: Neka je $x \in A$, prema uslovu zadatka postoji $y \in A$ takvo da $(x, y) \in \rho$. Odatle sledi da $(y, x) \in \rho^{-1}$. Iz uslova $(x, y) \in \rho$ i $(y, x) \in \rho^{-1}$ dobijamo $(x, x) \in \rho \circ \rho^{-1}$, odnosno $(x, x) \in \rho$.

S: $\rho^{-1} = (\rho \circ \rho^{-1})^{-1} = (\rho^{-1})^{-1} \circ \rho^{-1} = \rho \circ \rho^{-1} = \rho$.

T: Koristeći upravo dokazanu činjenicu da je $\rho^{-1} = \rho$, dobijamo $\rho \circ \rho = \rho \circ \rho^{-1} = \rho$.

($\Rightarrow$) Neka je sada ρ relacija ekvivalencije. Koristeći teoremu 4.45 dobijamo $\rho \circ \rho^{-1} = \rho \circ \rho = \rho$.

54. ($\Rightarrow$) Ako je ρ relacija ekvivalencije, prema teoremi 4.45 je $(\rho \circ \rho^{-1}) \cup \triangle_A = (\rho \circ \rho) \cup \triangle_A = \rho \cup \triangle_A = \rho$.

($\Leftarrow$) R: Iz datog uslova direktno sledi $\triangle_A \subseteq \rho$.

S: $\rho^{-1} = ((\rho \circ \rho^{-1}) \cup \triangle_A)^{-1} = (\rho \circ \rho^{-1})^{-1} \cup \triangle_A^{-1} = (\rho \circ \rho^{-1}) \cup \triangle_A = \rho$.

T: Iz date relacije i već dokazane simetričnosti dobijamo $\rho \circ \rho = \rho \circ \rho^{-1} \subseteq \rho$.

55. ($\Rightarrow$) Iz refleksivnosti relacije ρ i teoreme 4.32 imamo $\sigma = \triangle_A \circ \sigma \subseteq \rho \circ \sigma$ i slično $\sigma \subseteq \sigma \circ \rho$ pa, kako je $\rho = \rho \circ \rho$,

$$\sigma \circ \rho \circ \sigma \subseteq (\rho \circ \sigma) \circ (\rho \circ \rho) \circ (\sigma \circ \rho) = (\rho \circ \sigma \circ \rho) \circ (\rho \circ \sigma \circ \rho) \subseteq \rho \circ \sigma \circ \rho$$

(jer je $\rho \circ \sigma \circ \rho$ tranzitivna).

($\Leftarrow$) R: Iz refleksivnosti ρ i σ sledi $\triangle_A = \triangle_A \circ \triangle_A \circ \triangle_A \subseteq \rho \circ \sigma \circ \rho$.

S: Pošto su ρ i σ simetrične, imamo $(\rho \circ \sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1} \circ \rho^{-1} = \rho \circ \sigma \circ \rho$.

T: Kako je $\rho \circ \rho = \rho$, sledi $(\rho \circ \sigma \circ \rho) \circ (\rho \circ \sigma \circ \rho) = \rho \circ (\sigma \circ \rho \circ \sigma) \circ \rho \subseteq \rho \circ (\rho \circ \sigma \circ \rho) \circ \rho = \rho \circ \sigma \circ \rho$.

56. (a) ($\Leftarrow$) R: Iz $\triangle_A \subseteq \rho$ sledi $\triangle_A \subseteq \rho \cup \sigma$.

S: $(\rho \cup \sigma)^{-1} = \rho^{-1} \cup \sigma^{-1} = \rho \cup \sigma$ (jer su ρ i σ simetrične).

T: treba dokazati $(\rho \cup \sigma) \circ (\rho \cup \sigma) \subseteq \rho \cup \sigma$, tj. prema zadatku 22,

$$(\rho \circ \rho) \cup (\rho \circ \sigma) \cup (\sigma \circ \rho) \cup (\sigma \circ \sigma) \subseteq \rho \cup \sigma. \tag{6.25}$$

Međutim, iz tranzitivnosti ρ i σ sledi $\rho \circ \rho \subseteq \rho \subseteq \rho \cup \sigma$ i $\sigma \circ \sigma \subseteq \sigma \subseteq \rho \cup \sigma$, a iz datog uslova $\rho \circ \sigma \subseteq \rho \cup \sigma$. Odatle je i

$$\sigma \circ \rho = \sigma^{-1} \circ \rho^{-1} = (\rho \circ \sigma)^{-1} = (\rho \cup \sigma)^{-1} = \rho \cup \sigma.$$

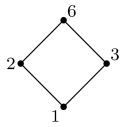
Sada (6.25) sledi iz teoreme 4.13(a).

($\Rightarrow$) Iz tranzitivnosti $\rho \cup \sigma$, odnosno uslova (6.25) i teoreme 4.13(a) sledi $\rho \circ \sigma \subseteq \rho \cup \sigma$. S druge strane, koristeći $\triangle_A \subseteq \sigma$ i $\triangle_A \subseteq \rho$, imamo $\rho = \rho \circ \triangle_A \subseteq \rho \circ \sigma$ i $\sigma = \triangle_A \circ \sigma \subseteq \rho \circ \sigma$ odakle, opet prema teoremi 4.13(a), sledi $\rho \cup \sigma \subseteq \rho \circ \sigma$.

(b) ($\Rightarrow$) Iz zadatka 35 sledi da, ako je $\rho \circ \sigma$ simetrična, mora važiti $\rho \circ \sigma = \sigma \circ \rho$.

($\Leftarrow$) Prema zadatku 33 $\rho \circ \sigma$ je refleksivna. Prema zadatku 35 i uslovu $\rho \circ \sigma = \sigma \circ \rho$ ona je i simetrična. Ostaje da dokažemo tranzitivnost:

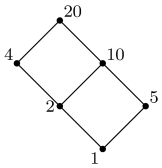
$$(\rho \circ \sigma) \circ (\rho \circ \sigma) = (\rho \circ \rho) \circ (\sigma \circ \sigma) \subseteq \rho \circ \sigma.$$



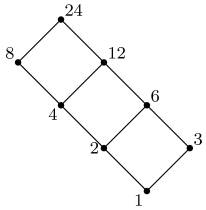
Slika 6.16: Dijagram za $(D_6, |)$

Slika 6.17: Dijagram za $(D_8, |)$

Slika 6.18: Dijagram za $(D_9, |)$



Slika 6.19: Dijagram za $(D_{20}, |)$



Slika 6.20: Dijagram za $(D_{24}, |)$

57. (a) Haseovi dijagrami zadatih parcijalnih uređenja prikazani su na slikama gore.

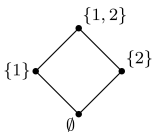
(b) Iz gornjih primera možemo zaključiti da je $(D_n, |)$ linearno uređenje ako i samo ako je n stepen prostog broja; dokažimo to.

($\Rightarrow$) Neka je $n = p^k$, gde je p prost i $k \in N$. Tada su delitelji broja n brojevi $1, p, p^2, \ldots, p^k$, i svaka dva od njih su uporedivi: $p^i \mid p^j$ za $i \leq j$.

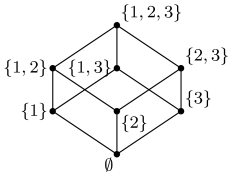
($\Leftarrow$) Ovaj deo dokaza sprovodimo kontrapozicijom: ako n nije stepen prostog broja dokazujemo da $(D_n, |)$ nije linearno uređenje. Zaista, n tada ima bar dva prosta faktora, recimo p i q. Ali p i q su neuporedivi u uređenju $(D_n, |)$ (niti je $p \mid q$ niti $q \mid p$) pa to uređenje nije linearno.

58. (a) Traženi dijagrami su:

Slika 6.21: Dijagram za $(P(\{1\}), \subseteq)$



Slika 6.22: Dijagram za $(P(\{1, 2\}), \subseteq)$



Slika 6.23: Dijagram za $(P(\{1, 2, 3\}), \subseteq)$

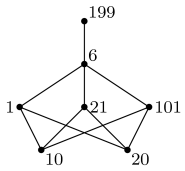
(b) Dokažimo da je $(P(A), \subseteq)$ linearno uređenje samo ako A ima samo 1 element. Zaista, ako $A = \{a\}$, jedini elementi skupa $P(A)$ su $\emptyset$ i $\{1\}$ i oni su uporedivi ($\emptyset \subseteq \{1\}$). S druge strane, ako A ima bar 2 elementa, npr. $a, b \in A$, tada su $\{a\}$ i $\{b\}$ neuporedivi elementi, pa $(P(A), \subseteq)$ nije linearno.

59. (a) Dovoljno je dokazati irefleksivnost i tranzitivnost, jer iz njih sledi i antisimetričnost relacije ρ.

IR: $n \rho n$ bi značilo da je cifra jedinica broja n manja od cifre jedinica istog tog broja, što ne važi ni za jedno $n \in N$.

T: Pretpostavimo da je $m\rho n$ i $n\rho k$. To znači da je cifra jedinica broja m manja od cifre jedinica broja n, a cifra jedinica broja n manja od cifre jedinica broja k. Sledi da je cifra jedinica broja m manja od cifre jedinica broja k, odnosno $m\rho k$.

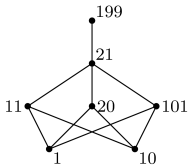
(b) Haseov dijagram ove relacije na skupu $\{1, 6, 10, 20, 21, 101, 199\}$ izgleda ovako:



60. (a) IR: $n\rho n$ bi značilo da je zbir cifara broja n manji od zbira cifara istog tog broja, što ne važi ni za jedno $n \in N$.

T: Pretpostavimo da je $m\rho n$ i $n\rho k$. To znači da je zbir cifara broja m manji od zbira cifara broja n, a zbir cifara broja n manji od zbira cifara broja k. Sledi da je zbir cifara broja m manji od zbir cifara broja k, odnosno $m\rho k$.

(b) Haseov dijagram ove relacije na skupu $\{1, 10, 11, 20, 21, 101, 199\}$ izgleda ovako:

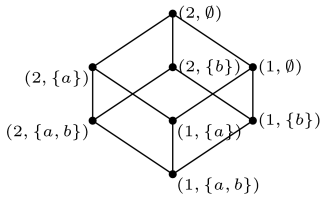


61. (a) R: Za svaki $(m, X) \in \{1, 2\} \times P(\{a, b\})$ je $m \leq m$ i $X \supseteq X$, pa je $(m, X)\rho(m, X)$.

AS: Neka je $(m, X)\rho(n, Y)$ i $(n, Y)\rho(m, X)$. To znači da je $m \leq n$ i $n \leq m$ (odakle $m = n$), kao i $X \supseteq Y$ i $Y \supseteq X$ (odakle $X = Y$). Dakle, $(m, X) = (n, Y)$.

T: Neka je $(m, X)\rho(n, Y)$ i $(n, Y)\rho(k, Z)$. To znači da je $m \leq n$ i $n \leq k$ (odakle $m \leq k$), kao i $X \supseteq Y$ i $Y \supseteq Z$ (odakle $X \supseteq Z$). Dakle, $(m, X)\rho(k, Z)$.

(b) Haseov dijagram date relacije izgleda ovako:



62. R: Za svako $A \in P(N)$ je $\min(A) = \min(A)$, pa je $A\rho A$.

AS: Neka je $A\rho B$ i $B\rho A$, odnosno $\min(A) \leq \min(B)$ i $\min(B) \leq \min(A)$. Odatle je $\min(A) = \min(B)$, ali to ne znači da je $A = B$; npr. ako $A = \{1\}$ i $B = \{1, 2\}$, tada $A\rho B$ i $B\rho A$ ali $A \neq B$.

Kako $(P(N), \rho)$ nije parcijalno uređenje, ne može biti ni linearno uređenje.

63. Neka je $\rho \subseteq N^2$ relacija ekvivalencije i relacija poretka, tada na osnovu teorema 4.45 i 4.58 važi: $\triangle_N \subseteq \rho$, $\rho = \rho^{-1}$, $\rho \cap \rho^{-1} = \triangle_N$ i $\rho \circ \rho = \rho$. Koristeći $\rho = \rho^{-1}$ i $\rho \cap \rho^{-1} = \triangle_N$ dobijamo $\rho = \rho \cap \rho = \triangle_N$. Dakle dijagonala $\triangle_N = \{(x, x) : x \in N\}$ je jedina relacija sa tim svojstvom.

64. (a) R: Pošto $x\rho x$ i $y\sigma y$ za sve $x \in A, y \in B$ (refleksivnost ρ i σ) imamo $(x, y)\tau(x, y)$.

    S: Ako $(x, y)\tau(u, v)$, to znači $x\rho u$ i $y\sigma v$, pa zbog simetričnosti ρ i σ: $u\rho x$ i $v\sigma y$, odakle $(u, v)\tau(x, y)$.

    T: Ako $(x, y)\tau(u, v)$ i $(u, v)\tau(p, q)$, to znači $x\rho u, y\sigma v, u\rho p$ i $v\sigma q$. Iz tranzitivnosti ρ i σ: $x\rho p, y\sigma q$, odakle $(x, y)\tau(p, q)$.

    (b) Refleksivnost i tranzitivnost dokazuju se kao pod (a).

    AS: Neka $(x, y)\tau(u, v)$ i $(u, v)\tau(x, y)$. Tada važi $x\rho u, y\sigma v, u\rho x$ i $v\sigma y$, pa iz antisimetričnosti ρ i σ sledi $x = u$ i $y = v$, tj. $(x, y)\tau(u, v)$.

    (c) Tranzitivnost se dokazuje kao pod (a).

    IR: Iz $(x, x) \notin \rho$ i $(y, y) \notin \sigma$ za sve $x \in A, y \in B$ (irefleksivnost ρ i σ) dobijamo da ne važi ni $(x, y)\tau(x, y)$.

65. R: Neka $a \in A$. Pošto je ρ refleksivna, $(a, a) \in \rho$. Pošto je σ refleksivna, $(a, a) \in \sigma$, dakle i $(a, a) \in \sigma^{-1}$. Odavde sledi $(a, a) \in \rho \cap \sigma^{-1}$.

    AS: Neka $(a, b) \in \rho \cap \sigma^{-1}$ i $(b, a) \in \rho \cap \sigma^{-1}$. To znači da $(a, b), (b, a) \in \rho$ i $(a, b), (b, a) \in \sigma^{-1}$. Iz antisimetričnosti relacije ρ dobijamo $a = b$ (antisimetričnost σ čak nije ni neophodna).

    T: Neka $(a, b) \in \rho \cap \sigma^{-1}$ i $(b, c) \in \rho \cap \sigma^{-1}$. Ovo znači da $(a, b), (b, c) \in \rho$ i $(a, b), (b, c) \in \sigma^{-1}$. Pošto je ρ tranzitivna, dobijamo $(a, c) \in \rho$. $(a, b), (b, c) \in \sigma^{-1}$ znači $(b, a), (c, b) \in \sigma$, pa iz tranzitivnosti σ dobijamo $(c, a) \in \sigma$, odnosno $(a, c) \in \sigma^{-1}$. Dakle, $(a, c) \in \rho \cap \sigma^{-1}$.

66. ($\Rightarrow$) Iz $\rho \subseteq \rho \cup \sigma$ i $\sigma \subseteq \rho \cup \sigma$ sledi $(\rho \circ \sigma) \cup (\sigma \circ \rho) \subseteq ((\rho \cup \sigma) \circ \sigma) \cup ((\rho \cup \sigma) \circ \rho) = (\rho \cup \sigma) \circ (\rho \cup \sigma) \subseteq \rho \cup \sigma$, prema zadatku 22.

    ($\Leftarrow$) IR: Za svako $a \in A$ iz $(a, a) \in \rho \cup \sigma$ sledilo bi $(a, a) \in \rho$ ili $(a, a) \in \sigma$, što je nemoguće jer su ρ i σ irefleksivne.

    T: Iz $\rho \circ \rho \subseteq \rho$, $\sigma \circ \sigma \subseteq \sigma$, uslova (4.4) i zadatka 22 sledi $(\rho \cup \sigma) \circ (\rho \cup \sigma) = (\rho \circ \rho) \cup ((\rho \circ \sigma) \cup (\sigma \circ \rho)) \cup (\sigma \circ \sigma) \subseteq \rho \cup (\rho \cup \sigma) \cup \sigma = \rho \cup \sigma$.

67. ($\Rightarrow$) Ako $(x, y) \in A^2$, tada $x, y \in A$, pa zbog linearne uređenosti $x\rho y$ ili $y\rho x$. To znači: $x\rho y$ ili $x\rho^{-1}y$, tj. $(x, y) \in \rho \cup \rho^{-1}$. Dakle $A^2 \subseteq \rho \cup \rho^{-1}$. Obrnuta inkluzija je trivijalna.

    ($\Leftarrow$) Iz $\rho \cup \rho^{-1} = A^2$ sledi da za sve $x, y \in A$ $x(\rho \cup \rho^{-1})y$, odnosno $x\rho y$ ili $y\rho x$.

68. ($\Leftarrow$) Ako je $\rho = \sigma$, iz tranzitivnosti odmah sledi $\rho \circ \sigma = \rho \circ \rho = \rho$, pa je to linearno uređenje.

    ($\Rightarrow$) Obratno, pretpostavimo suprotno, da je $\rho \neq \sigma$. Tada npr. postoji $(x, y) \in \rho \setminus \sigma$ i, naravno $x \neq y$ (u suprotnom bi bilo $(x, y) \in \sigma$ zbog refleksivnosti). Iz $(x, y) \in \rho, (y, y) \in \sigma$ imamo $(x, y) \in \rho \circ \sigma$. Iz $(y, y) \in \rho, (y, x) \in \sigma$ (zbog $(x, y) \notin \sigma$ i linearnosti relacije σ) imamo $(y, x) \in \rho \circ \sigma$. Ako bi $\rho \circ \sigma$ bila relacija poretka, iz antisimetričnosti bi sledilo $x = y$, kontradikcija.

69.
$$\begin{aligned} x(>_N \circ <_N)y &\sim (\exists z)(x > z \wedge z < y) \\ &\sim (\exists z)(z < x \wedge z < y) \\ &\sim (\exists z) z < \min(x, y). \end{aligned}$$

Analogno se pokazuje $x(<_N \circ >_N)y \Leftrightarrow (\exists z) z > \max(x, y)$. Kako je $<_N \circ >_N = N^2$, sigurno važi $(>_N \circ <_N) \subseteq (<_N \circ >_N)$. S druge strane, primetimo da $(1, 2) \notin (>_N \circ <_N)$ jer ne postoji $z \in N$ takvo da $z < \min(1, 2) = 1$, ali da $(1, 2) \in (<_N \circ >_N)$ jer postoji $z > \max(1, 2) = 2$ npr. $z = 3$. Odavde zaključujemo da ne je $(>_N \circ <_N) \subset (<_N \circ >_N)$.

70. Najpre napomenimo da je definicija relacije $\leq$ dobra: da li će važiti $[A] \leq [B]$ ne zavisi od izbora predstavnika klasa $[A]$ i $[B]$. Zaista, ako i $A_1 \in [A]$ i $B_1 \in [B]$, to znači da $\models A_1 \Leftrightarrow A$ i $\models B_1 \Leftrightarrow B$, pa $\models A \Rightarrow B$ važi ako i samo ako je $\models A_1 \Rightarrow B_1$.

R: $[A] \leq [A]$ jer $\models A \Rightarrow A$ za svaku formulu A.

AS: Ako $[A] \leq [B]$ i $[B] \leq [A]$, to znači da $\models A \Rightarrow B$ i $\models B \Rightarrow A$, pa i $A \sim B$, dakle $[A] = [B]$ (teorema 2.23).

T: Ako $[A] \leq [B]$ i $[B] \leq [C]$, to znači da $\models A \Rightarrow B$ i $\models B \Rightarrow C$, dakle i $\models A \Rightarrow C$, tj. $[A] \leq [C]$.

71. (a) $\rho_R = \rho \cup \{(1, 1), (2, 2), (3, 3), (4, 4)\}$.

$\rho_S = \rho_S \cup \{(3, 2), (4, 3)\}$.

Obeležimo prvo $\rho_1 = \rho$ i $\rho_2 = \rho \cup \rho \circ \rho = \rho \cup \{(1, 3), (1, 1), (2, 2), (2, 4)\}$. Dalje, $\rho_3 = \rho_2 \cup (\rho_2 \circ \rho) = \rho_2 \cup \{(1, 4)\}$. Konačno, $\rho_4 = \rho_3 \cup (\rho_3 \circ \rho) = \rho_3$ pa je tranzitivno zatvorenje $\rho_T = \rho_3$.

(b) $\triangle_N$ je refleksivna, simetrična i tranzitivna pa je $(\triangle_N)_R = \triangle_N$, $(\triangle_N)_S = \triangle_N$ i $(\triangle_N)_T = \triangle_N$.

(c) $\leq_N$ je refleksivna i tranzitivna pa je $(\leq_N)_R = \leq_N$ i $(\leq_N)_T = \leq_N$.
$(\leq_N)_S = \leq_N \cup (\leq_N)^{-1} = N^2$.

(d) $(<_N)_R = <_N \cup \triangle_N = \leq_N$.
$(<_N)_S = <_N \cup (<_N)^{-1} = (\neq_N)$ (relacija $\neq$ na skupu N).
$<_N$ je tranzitivna pa je $(<_N)_T = <_N$.

72. (a) Refleksivno zatvorenje relacije ρ je $\rho' = \rho \cup \triangle_A = \{(a, a), (a, b), (b, b), (b, d), (c, d), (c, c), (d, d)\}$.

(b) Relacija ρ' nije tranzitivna, jer $(a, b) \in \rho'$ i $(b, d) \in \rho'$ ali $(a, d) \notin \rho'$. Dakle, ona nije relacija poretka.

73. Iz definicije imamo da je $\rho = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3), (6, 5), (7, 5), (7, 6), (8, 5), (8, 6), (8, 7), (10, 9), (11, 9), (11, 10), (12, 9), (12, 10), (12, 11)\}$.

(a) Relacija ρ je tranzitivna: ako je x desno od y i y desno od z, onda je i x desno od z (ovo se može proveriti i pomoću nabrojanih uređenih parova). Sledi da je $\rho_T = \rho$.

(b) ρ_T nije simetrična, npr. zato što $(2, 1) \in \rho_T$ ali $(1, 2) \notin \rho_T$. Njeno simetrično zatvorenje je $\rho_S = \rho \cup \{(1, 2), (1, 3), (2, 3), (1, 4), (2, 4), (3, 4),$

$(5,6),(5,7),(6,7),(5,8),(6,8),(7,8),(9,10),(9,11),(10,11),(9,12),(10,12),(11,12)\}$.

(c) ρ_S nije refleksivna jer $(1,1) \notin \rho_S$. Njeno refleksivno zatvorenje je $\rho_R = \rho_S \cup \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7),(8,8),(9,9),(10,10),(11,11),(12,12)\}$.

(d) Dobili smo relaciju za koju je $x\rho_R y$ akko su x i y u istom redu. Lako proveravamo da je ona relacija ekvivalencije (npr. ako je x u istom redu kao y a y u istom redu kao z, onda je i x u istom redu kao z).

74. (a) $x\rho_T y$ znači da skakač može u nekoliko skokova stići od polja x do polja y. Ona je, naravno, tranzitivna.

R: Za svako polje x skakač može u dva poteza stići od x do nekog drugog polja a zatim nazad na x.

S: Ako skakač može stići od x do y, obrnutim redosledom poteza može stići i od y do x.

Nije teško pokazati da skakač može stići od svakog polja šahovske table do svakog drugog, pa imamo samo jednu klasu ekvivalencije: skup svih polja šahovske table.

(b) $x\sigma_T y$ znači da lovac može u nekoliko poteza stići od polja x do polja y. I ona je tranzitivna.

Na isti način kao pod (a) dokazuje se da je i σ_T refleksivna i simetrična.

Nije teško pokazati da lovac može stići od nekog polja šahovske table do nekog drugog ako i samo ako su ona iste boje. Dakle, imamo dve klase ekvivalencije: skup belih i skup crnih polja.

6.5 Funkcije i kardinalnost skupova

1. (a) f nije 1-1 jer je $f(2) = f(4)$. Ona jeste ,,na" jer se u svaki od elemenata kodomena B preslikava neki element domena A.

(b) g jeste 1-1: ne postoje dva elementa domena A sa istom slikom. Ona nije ,,na" jer se u element 2 kodomena C ne preslikava nijedan element iz A.

(c) h jeste i 1-1 i ,,na".

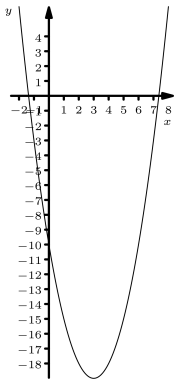
2. (a) 1-1: Iz $f(x) = f(y)$ sledi $2x-1 = 2y-1$, a odatle lako dobijamo $x = y$.

,,na": Za svaki $b \in R$ tražimo $a \in R$ takav da $f(a) = 2a - 1 = b$. Lako dobijamo da je $a = \frac{b+1}{2}$, pa je f i ,,na".

Na sličan način za svaku linearnu funkciju $f : R \to R$ (tj. funkciju zadatu sa $f(x) = ax + b$ za $a, b \in R$) dokazujemo da je bijekcija.

(b) Kao pod (a) dobijamo da je f_1 1-1. Međutim, ona nije ,,na", jer za $b = 0$ ne postoji ceo broj a takav da $f(a) = 0$. (Sve slike celih brojeva su neparni brojevi.)

(c) Sa grafika date funkcije možemo zaključiti da niti on seče svaku horizontalnu pravu, niti svaku od njih seče najviše jednom:



Slika 6.24: Grafik funkcije $g(x) = x^2 - 6x - 10$

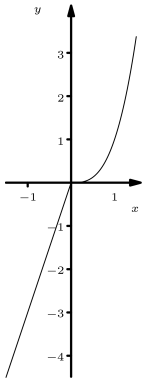
Dakle, dokazujemo da g nije ni 1-1 ni ,,na".

1-1: Zapišimo $g(x) = (x^2 - 6x + 9) - 19 = (x-3)^2 - 19$. Iz tog oblika lako vidimo da je $g(2) = g(4) = 1 - 19 = -18$ pa g nije 1-1.

,,na": Kako je $g(x) = (x-3)^2 - 19 \geq -19$, za bilo koje $b < -19$ ne postoji $a \in R$ za koje je $g(a) = b$.

Na sličan način za svaku kvadratnu funkciju $f : R \to R$ dokazujemo da nije bijekcija.

(d) Skicirajmo ponovo prvo grafik date funkcije:



Slika 6.25: Grafik funkcije $h(x)$

Pomoću njega zaključujemo da je h bijekcija. Dokažimo to:

1-1: Pretpostavimo da je $h(x) = h(y)$. Posmatramo tri slučaja.

1° $x < 0$ i $y < 0$. Tada je $3x = 3y$, odakle $x = y$.

2° $x \geq 0$ i $y \geq 0$. Tada imamo $x^3 = y^3$, pa opet dobijamo $x = y$.

3° Inače, neka je recimo $x < 0$ i $y \geq 0$. Tada je $h(x) = 3x < 0$ i $h(y) = y^3 \geq 0$ pa ni ne može biti $h(x) = h(y)$.

Kako smo proverili sve slučajeve, sledi da je h 1-1.

,,na": Neka je dato $b \in R$. Posmatramo dva slučaja.

1° $b < 0$. Ako pogledamo grafik vidimo da treba da tražimo $a < 0$ koje će se slikati u b. Za $a < 0$ iz $h(a) = 3a = b$ sledi da je $a = \frac{b}{3}$.

2° $b \geq 0$. Sada tražimo takvo $a \geq 0$: $h(a) = a^3 = b$, pa sledi $a = \sqrt[3]{b}$.

Zaključujemo da h jeste ,,na".

Napomena. Da je h bijekcija sledi i iz opštijeg tvrđenja koje će biti dokazano u zadatku 14.

(e) 1-1: Kako je $k(2,0) = k(1,1) = 2$, k nije 1-1.

,,na" Za svako $b \in Z$ je $k(b,0) = b$ pa je k ,,na".

(f) 1-1: Pošto je $k_1(2,1) = k_1(1,2) = 3$, ni k_1 nije 1-1.

,,na": Kako je $k_1(x,y) \geq 1 + 1 = 2$, nijedan par $(x,y) \in N^2$ se ne slika u 1, pa k_1 nije ,,na".

(g) 1-1: Funkcija NZD nije 1-1 jer je $NZD(2,4) = NZD(6,8) = 2$.

,,na": Funkcija jeste ,,na": za svako $b \in N$ je $NZD(b,b) = b$.

(h) 1-1: Ni funkcija NZS nije 1-1: $NZS(2,3) = NZS(6,1) = 6$.

,,na": NZS jeste ,,na": za svako $b \in N$ je $NZS(b,b) = b$.

(i) 1-1: Funkcija m nije 1-1 jer je $m(\{1,2\}) = m(\{1\}) = 1$.

,,na": m jeste ,,na" jer za svako $b \in N$ imamo $m(\{b\}) = b$.

3. Prema teoremi 5.18 inverzna funkcija postoji ako i samo ako je data funkcija bijekcija. Dakle, inverzne funkcije možemo tražiti za sledeće funkcije.

   Zadatak 1(c): njena inverzna funkcija je $h^{-1} : A \to A$ data sa $h^{-1} : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

   Zadatak 2(a): $f^{-1}(b) = \frac{b+1}{2}$ (iskoristili smo račun izveden prilikom provere uslova ,,na").

   Zadatak 2(d): Prateći slučajeve iz provere ,,na" uslova, dobijamo da je $h^{-1} : R \to R$ definisana sa $h^{-1}(b) = \begin{cases} \frac{b}{3} & b < 0 \\ \sqrt[3]{b} & b \geq 0 \end{cases}$

4. I rešenje. Svaka od funkcija f, g, h je bijekcija, a iz teoreme 5.14 sledi da je kompozicija bijekcija takođe bijekcija.

   II rešenje. Možemo i direktno naći inverznu funkciju za svaku od datih funkcija: $f^{-1}(x) = \sqrt[3]{x}$, $g^{-1}(x) = -\ln x$ i $h^{-1}(x) = \frac{1}{x}$ (h je sama sebi inverzna). Prema teoremi 5.20 je $(h \circ g \circ f)^{-1}(x) = (f^{-1} \circ g^{-1} \circ h^{-1})(x) = \sqrt[3]{-\ln \frac{1}{x}}$.

5. I rešenje. 1-1: Pretpostavimo da je $g(x) = g(y)$. To znači $2f(x) + 3 = 2f(y) + 3$, odakle $2f(x) = 2f(y)$, dakle i $f(x) = f(y)$. Kako je f 1-1 funkcija, zaključujemo da je $x = y$.

   ,,na": Neka je $x \in R$. Dokazujemo da postoji $y \in R$ takvo da $g(y) = x$. To bi značilo $2f(y) + 3 = x$, odnosno $f(y) = \frac{x-3}{2}$. Kako je f ,,na" funkcija, sledi da postoji $y \in R$ za koje to važi.

   II rešenje. Kako su i f i funkcija $h : R \to R$ data sa $h(x) = 2x+3$ bijekcije, prema teoremi 5.14 sledi da je i $g = h \circ f$ bijekcija.

6. (a) $g \circ f(999) = g(f(999)) = g(27) = 28$.

   $f \circ g(999) = f(g(999)) = f(1000) = 1$.

   (b) Iz teoreme 5.14 sledi da, ako bi $g \circ f$ bila 1-1, onda bi i f bila 1-1. Međutim, to nije tačno: $f(1) = f(10) = 1$. Dakle, $g \circ f$ nije 1-1.

7. (a) Funkcija f nije 1-1 jer $f(avlija) = f(cuprija)$. Dakle, ne postoji f^{-1}.

   g jeste 1-1 (ne postoje dve knjige skupa B sa istim brojem stranica) i ,,na" (za svaki broj iz skupa C postoji knjiga s tim brojem stranica). Dakle, ona je bijekcija pa ima inverznu funkciju

$$g^{-1} : \begin{pmatrix} 200 & 500 & 450 & 250 & 270 & 300 \\ avlija & besnilo & cuprija & ocevi & ubistvo & zid \end{pmatrix}.$$

   (b) $f^{-1} \circ g$ nema smisla jer ni ne postoji f^{-1}. Funkcija $f \circ g$ ne može se konstruisati jer kodomen C funkcije g nije sadržan u domenu funkcije f. Slično je i sa $g \circ f$. Jedina od navedenih kompozicija koja postoji je

$$f \circ g^{-1} : \begin{pmatrix} 200 & 500 & 450 & 250 & 270 & 300 \\ andric & pekic & andric & selenic & selenic & pavlovic \end{pmatrix}.$$

8. (a) f je uvek ,,na" jer za svako slovo $a \in A$ postoji bar jedna reč koja počinje na a.

   (b) Ako je $n = 1$, f je bijekcija jer tada ona preslikava slova (reči dužine 1) u sebe, tj. ona je tada identičko preslikavanje.

   Takođe, ako je $m = 1$, f je opet bijekcija jer za svako slovo $a \in A$ imamo tačno po jednu reč koja se u njega preslikava a to je $\underbrace{aa \ldots a}_{n}$.

   U svim ostalim slučajevima f nije 1-1. Zaista, ako je $n \geq 2$ i skup A ima bar 2 slova (recimo a i b) tada postoje bar 2 reči koje počinju slovom a: jedna počinje sa $ab\ldots$ a druga sa $aa\ldots$

9. (1) (a) Da, to je npr. funkcija $f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

   (b) Ne, recimo funkcija $g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 3 \end{pmatrix}$ nije 1-1.

   (c) Ne. Ako bi neka funkcija $h : A \to B$ bila ,,na", u skupu A bi postojalo bar 7 različitih elemenata (koji bi se redom slikali u 1,2,3,4,5,6,7).

   (d) Ne (sledi iz (c)).

   (2)(a) Ne. Ako bi $g : A \to B$ bila 1-1, $g(1), g(2), g(3), g(4), g(5)$ i $g(6)$ bi bili različiti elementi skupa B, a on ima samo 5 elemenata.

   (c) Ne (sledi iz (a)).

   (d) Da, to je npr. funkcija $f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 5 \end{pmatrix}$.

   (e) Ne, recimo funkcija $h : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 4 & 4 \end{pmatrix}$ nije "na".

   Napomena. Prema definiciji 5.27 i teoremi 5.28 1-1 funkcija $f : A \to B$ postoji akko je A ima manji ili jednak broj elemenata nego B, a ,,na" funkcija $f : A \to B$ postoji akko A ima veći ili jednak broj elemenata nego B.

10. 1-1: Neka je $f^{-1}(x) = f^{-1}(y)$. Tada i $f(f^{-1}(x)) = f(f^{-1}(y))$, odnosno $x = y$.

    „na": Za svako $b \in X$ postoji element iz Y koji se slika u b funkcijom f^{-1}: $f^{-1}(f(b)) = b$.

11. 1-1: Neka je $g \circ f(x) = g \circ f(y)$. Kako je g 1-1, iz $g(f(x)) = g(f(y))$ sledi $f(x) = f(y)$, a kako je i f 1-1, odatle je $x = y$.

    „na": Neka je $c \in C$. Pošto je g „na", postoji $b \in B$ takav da $g(b) = c$. Ali i f je „na" pa postoji $a \in A$ takav da $f(a) = b$. Sve to znači da je $g \circ f(a) = g(f(a)) = g(b) = c$.

12. 1-1: Pretpostavimo da je $h(a_1, c_1) = h(a_2, c_2)$. To znači da je $g(f(a_1), c_1) = g(f(a_2), c_2)$. Kako je g 1-1, zaključujemo da je $(f(a_1), c_1) = (f(a_2), c_2)$. Odatle dobijamo da je $c_1 = c_2$, ali i $f(a_1) = f(a_2)$. Pošto je i f 1-1, sledi $a_1 = a_2$. Dakle, $(a_1, c_1) = (a_2, c_2)$.

    „na": Neka je $d \in D$. Pošto je g „na", postoji $(b, c) \in B \times C$ takvo da $g(b, c) = d$. Pošto je i f „na", postoji $a \in A$ takvo da $f(a) = b$. Dakle $h(a, c) = g(f(a), c) = g(b, c) = d$.

13. 1-1: Pretpostavimo da važi $h(x_1, y_1) = h(x_2, y_2)$. To znači da je $(f^{-1}(x_1), g(y_1)) = (f^{-1}(x_2), g(y_2))$. Odatle dobijamo $f^{-1}(x_1) = f^{-1}(x_2)$ i $g(y_1) = g(y_2)$. Pošto je f bijekcija, i f^{-1} je bijekcija (prema teoremi 5.19), dakle i 1-1, pa iz $f^{-1}(x_1) = f^{-1}(x_2)$ sledi $x_1 = x_2$. Pošto je i g 1-1, iz $g(y_1) = g(y_2)$ dobijamo $y_1 = y_2$. Iz ovog sledi da je $(x_1, y_1) = (x_2, y_2)$.

    „na": Neka je $(a, d) \in A \times D$. Treba da nađemo element skupa $C \times B$ koji se u njega preslikava. Pošto je $f^{-1} : C \to A$ „na", postoji $c \in C$ takvo da $f^{-1}(c) = a$. Pošto je i g „na", postoji $b \in B$ takvo da $g(b) = d$. To znači da je $h(c, b) = (f^{-1}(c), g(b)) = (a, d)$.

14. 1-1: Neka je $h(x) = h(y)$ za neke $x, y \in A \cup B$. Imamo tri mogućnosti:

    1° $x, y \in A$. Tada je $h(x) = f(x)$ i $h(y) = f(y)$, pa pošto je f 1-1 iz $f(x) = f(y)$ dobijamo $x = y$.

    2° $x, y \in B$. Sada imamo $h(x) = g(x)$ i $h(y) = g(y)$, pa analogno slučaju 1° dobijamo $x = y$.

    3° $x \in A$, $y \in B$. Tada $h(x) \in A$ i $h(y) \in B$, pa kako su A i B disjunktni, nemoguće je da bude $h(x) = h(y)$.

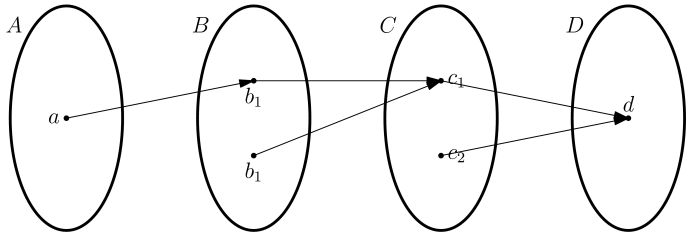
    „na": Neka je $x \in A \cup B$. Ako je $x \in A$, onda i $f^{-1}(x) \in A$ pa $h(f^{-1}(x)) = f(f^{-1}(x)) = x$. Analogno razmatramo i slučaj $x \in B$.

15. ($\Rightarrow$) Neka je $g \circ f$ 1-1. Prema teoremi 5.14(c) sledi da je i f 1-1. Dokažimo (5.4). Neka su $y_1, y_2 \in f[X]$; to znači da postoje $x_1, x_2 \in X$ takvi da $f(x_1) = y_1$ i $f(x_2) = y_2$. Pretpostavimo da je $g(y_1) = g(y_2)$, tj. $g(f(x_1)) = g(f(x_2))$. Pošto je $g \circ f$ 1-1, iz $g \circ f(x_1) = g \circ f(x_2)$ sledi $x_1 = x_2$, a odatle $y_1 = f(x_1) = f(x_2) = y_2$.

    ($\Leftarrow$) Neka je f 1-1 i važi (5.4). Pretpostavimo da je $g \circ f(x_1) = g \circ f(x_2)$ za neke $x_1, x_2 \in X$. Kako važi $f(x_1), f(x_2) \in f[X]$, iz $g(f(x_1)) = g(f(x_2))$ zbog (5.4) sledi $f(x_1) = f(x_2)$, a pošto je f 1-1, imamo $x_1 = x_2$.

16. Na osnovu teoreme 5.14 dobijamo da, ako je $h \circ g \circ f$ bijekcija, f mora biti 1-1, a h mora biti „na". Evo primera koji pokazuje da ništa više od toga ne mora da važi: neka je $A = \{a\}, B = \{b_1, b_2\}, C = \{c_1, c_2\}, D = \{d\}$, a

funkcije date sa: $f : \begin{pmatrix} a \\ b_1 \end{pmatrix}, g : \begin{pmatrix} b_1 & b_2 \\ c_1 & c_1 \end{pmatrix}$ i $h : \begin{pmatrix} c_1 & c_2 \\ d & d \end{pmatrix}$. Ovde f nije ,,na", g nije ni 1-1 ni ,,na", a h nije 1-1.



17. Pošto je $g \circ f$ 1-1, iz teoreme 5.14 direktno sledi da je f 1-1. Dokažimo da je i ,,na". Neka je $y \in Y$ proizvoljno; obeležimo $z = g(y)$. Kako je $g \circ f$,,na", postoji $x \in X$ takvo da $(g \circ f)(x) = z$. Sada imamo $g(f(x)) = g(y)$, pa pošto je g 1-1 zaključujemo da je $f(x) = y$.

18. 1-1: Neka je $g(b_1) = g(b_2)$. Pošto je f ,,na", postoje $a_1, a_2 \in A$ takvi da je $f(a_1) = b_1$ i $f(a_2) = b_2$. Pošto je $h \circ g \circ f(a_1) = h(g(b_1)) = h(g(b_2)) = h \circ g \circ f(a_2)$, a $h \circ g \circ f$ je 1-1, sledi da je $a_1 = a_2$, pa mora biti i $f(a_1) = f(a_2)$, odnosno $b_1 = b_2$.

    ,,na": Neka je $c \in C$, i $d = h(c)$. Pošto je $h \circ g \circ f$,,na", postoji $a \in A$ takvo da $h \circ g \circ f(a) = d$. Međutim, to znači da je $h(g(f(a))) = h(c)$, pa pošto je h 1-1, dobijamo $g(f(a)) = c$, tj. $f(a)$ je element koji se slika u c funkcijom g.

19. Pre svega, iz definicije sledi da svaka ,,2-1" funkcija, pa i $f \circ f$, mora biti ,,na". Odatle, primenom teoreme 5.14, dobijamo da je i f ,,na". Međutim, ni za jedno $x \in X$ ne mogu postojati tri različita elementa $a_1, a_2, a_3 \in X$ takva da $f(a_1) = f(a_2) = f(a_3) = x$: u suprotnom, ako su $b_1, b_2, b_3 \in X$ takvi da $f(b_1) = a_1$, $f(b_2) = a_2$ i $f(b_3) = a_3$, tada se funkcijom $f \circ f$ bar tri elementa b_1, b_2, b_3 slikaju u x, što je kontradikcija sa uslovom da je $f \circ f$,,2-1". Dakle, i f je ,,2-1".

20. Neka $f : X \to Y$ i $g : Y \to Z$. Pretpostavimo suprotno, da postoji element $z \in Z$ takav da $(g \circ f)(a) = z$ za sve $a \in X$. Kako je g netrivijalna, postoji još neki element $z_1 \in Z \setminus \{z\}$ takav da $g(y) = z_1$ za neko $y \in Y$. Pošto je f ,,na", postoji $x \in X$ takvo da $f(x) = y$. Tada je $(g \circ f)(x) = g(f(x)) = g(y) = z_1$, kontradikcija.

21. 1-1: Ako je $f(a_1) = f(a_2)$, to znači $(a_1, a_1) = (a_2, a_2)$ odakle sledi $a_1 = a_2$. Dakle, f je 1-1 za svaki skup A.

    ,,na": Ako su $a, b \in A$ dva različita elementa, očigledno ne postoji $x \in A$ takav da je $f(x) = (a, b)$. Zato mora biti $|A| = 1$ da bi f bila ,,na".

    (Ako je A konačan skup, npr. $|A| = n$, možemo i ovako rezonovati: da bi $f : A \to B$ bila ,,na", mora biti $|A| \geq |B|$, pa kako je $|A^2| = n^2$, $|A| \geq |A^2|$ može važiti samo za $|A| = 1$.)

22. 1-1: Neka je $a \in A$ proizvoljno. Tada je $f(\{a\}, \{a\}) = f(\emptyset, \{a\}) = (\{a\}, \emptyset)$, što znači da f nije 1-1.

    ,,na": Za par $(\emptyset, \{a\})$ ne postoje skupovi X i Y takvi da $X \cup Y = \emptyset$ i $X \setminus Y = \{a\}$ (uvek mora biti $X \setminus Y \subseteq X \cup Y$), pa se u taj par ne slika nijedan element. Dakle f nije ni ,,na".

23. 1-1: $f(\emptyset,\emptyset) = f(\{a\},\{b\}) = 0$, pa f nije 1-1.

,,na": Kako skup $A \cap B = \{b, c\}$ ima samo 2 elementa, i svi ostali skupovi $X \cap Y$ za $X \subseteq A$, $Y \subseteq B$ mogu imati najviše po dva elementa. Dakle, ne postoje $X \in P(A)$ i $Y \in P(B)$ takvi da $f(X, Y) = 3$, pa f nije ,,na".

Kako f nije 1-1 ni ,,na", ona nije bijekcija.

24. (a) R: Za svako $x \in A$ je $f(x) = f(x)$ pa $x \sim x$.

S: Ako $x \sim y$, to znači da je $f(x) = f(y)$. Odatle je $f(y) = f(x)$, dakle i $y \sim x$.

T: Ako $x \sim y$ i $y \sim z$, onda je $f(x) = f(y) = f(z)$, pa je i $x \sim z$.

(b) Za svaku klasu ekvivalencije $[x]_\sim$ je $g(x) = [x]_\sim$, dakle g je ,,na".

25. (a) R: Neka $b \in B$. Zbog refleksivnosti ρ imamo $f(b)\rho f(b)$, pa sledi $b\sigma b$.

AS: Ako važi $b_1\sigma b_2$ i $b_2\sigma b_1$, tada $f(b_1)\rho f(b_2)$ i $f(b_2)\rho f(b_1)$. Iz antisimetričnosti ρ sledi $f(b_1) = f(b_2)$, pa pošto je f 1-1, sledi $b_1 = b_2$.

T: Ako važi $b_1\sigma b_2$ i $b_2\sigma b_3$, to znači $f(b_1)\rho f(b_2)$ i $f(b_2)\rho f(b_3)$, pa iz tranzitivnosti ρ dobijamo $f(b_1)\rho f(b_3)$, dakle i $b_1\sigma b_3$.

(b) Odgovor je: da. Neka $b_1, b_2 \in B$. Pošto je (A, ρ) linearno uređenje, elementi $f(b_1)$ i $f(b_2)$ su uporedivi, tj. važi $f(b_1)\rho f(b_2)$ ili $f(b_2)\rho f(b_1)$. U prvom slučaju je $b_1\sigma b_2$, a u drugom $b_2\sigma b_1$. U oba slučaja b_1 i b_2 su uporedivi.

(c) Ovde je odgovor: ne. Npr. ako $B = \{b\}, A = \{a_1, a_2\}, f(b) = a_1$ i $\rho = \triangle_A$, biće $\sigma = \triangle_B$. σ jeste linearno, ali ρ nije. Razlog je, naravno, to što f ne mora biti ,,na".

26. (a) Treba da ispitamo da li je σ relacija poretka i, ako jeste, da li su svaka dva elementa njome uporediva. Međutim, σ nije antisimetrična: ako važi $b_1\sigma b_2$ i $b_2\sigma b_1$, to znači da postoje $a_1, a_2 \in A$ takvi da $f(a_1) = b_1$, $f(a_2) = b_2$ i $a_1\rho a_2$, i da postoje $a_2', a_1' \in A$ takvi da $f(a_2') = b_2$, $f(a_1') = b_1$ i $a_2'\rho a_1'$. (Ne znamo da mora biti $a_1 = a_1'$ niti $a_2 = a_2'$.) Odavde ne možemo zaključiti $b_1 = b_2$. Evo primera za to: neka $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2\}$, $f : \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_2 & b_1 \end{pmatrix}$ i $\rho = \{(a_1, a_2), (a_2, a_3), (a_3, a_4)\}$. Tada važi i $b_1\sigma b_2$ i $b_2\sigma b_1$, ali nije $b_1 = b_2$.

(b) R: Neka je $b \in B$. Kako je f ,,na", postoji $a \in A$ takvo da je $f(a) = b$. ρ je refleksivna, pa je $a\rho a$; dakle

$$f(a) = b \wedge f(a) = b \wedge a\rho a,$$

što znači $b\sigma b$.

S: Neka važi $b_1\sigma b_2$. To znači da postoje $a_1, a_2 \in A$ takvi da $f(a_1) = b_1$, $f(a_2) = b_2$ i $a_1\rho a_2$. Kako je ρ simetrična, sledi i $a_2\rho a_1$, pa i $b_2\sigma b_1$.

T: Neka je $b_1\sigma b_2$ i $b_2\sigma b_3$. Prva relacija znači da postoje $a_1, a_2 \in A$ takvi da $f(a_1) = b_1$, $f(a_2) = b_2$ i $a_1\rho a_2$, a druga da postoje $a_2', a_3 \in A$ takvi da $f(a_2') = b_2$, $f(a_3) = b_3$ i $a_2'\rho a_3$. (Obratiti pažnju: ne možemo zaključiti da je $a_2 = a_2'$!) Iz $f(a_2) = b_2 = f(a_2')$ i (5.6), međutim, sledi da $a_2\rho a_2'$. Sada pomoću tranzitivnosti ρ iz $a_1\rho a_2$ i $a_2\rho a_2'$ dobijamo $a_1\rho a_2'$, a iz toga i $a_2'\rho a_3$ dalje i $a_1\rho a_3$. Kako je $f(a_1) = b_1$ i $f(a_3) = b_3$, zaključujemo $b_1\sigma b_3$.

27. Neka $x \leq_B y$. Ako $x = y$, onda je $f^{-1}(x) = f^{-1}(y)$, pa samim tim, zbog refleksivnosti, i $f^{-1}(x) \leq_A f^{-1}(y)$. Ako $x \neq y$ tada, pošto je $(A, \leq_A)$ linearno, $f^{-1}(x) \leq_A f^{-1}(y)$ ili $f^{-1}(y) \leq_A f^{-1}(x)$. Pretpostavimo da važi ovo drugo. Pošto f čuva poredak, imamo da važi $f(f^{-1}(y)) \leq_B f(f^{-1}(x))$, tj. $y \leq_B x$. Iz antisimetričnosti zaključujemo $x = y$; kontradikcija.

28. R: Ako $f \in F_N$, za svako $n \in N$ važi $f(n) \leq f(n)$ pa je $f \rho f$.

    AS: Neka važi $f \rho g$ i $g \rho f$. To znači da je za sve $n \in N$ $f(n) \leq g(n)$ i $g(n) \leq f(n)$, dakle $f(n) = g(n)$. Sledi da je $f = g$.

    T: Neka važi $f \rho g$ i $g \rho h$. To znači da je za sve $n \in N$ $f(n) \leq g(n)$ i $g(n) \leq h(n)$, dakle i $f(n) \leq h(n)$. Sledi da je $f \rho h$.

    L: Ako definišemo funkcije $f, g \in F_N$ ovako:

$$f(n) = \begin{cases} 1, & \text{ako je } n \text{ parno} \\ 0, & \text{ako je } n \text{ neparno} \end{cases} \quad \text{i} \quad g(n) = \begin{cases} 0, & \text{ako je } n \text{ parno} \\ 1, & \text{ako je } n \text{ neparno} \end{cases}$$

    onda ne važi ni $f \rho g$ ni $g \rho f$. Dakle, (F_N, ρ) nije linearno uređenje.

29. $f[A] = \{2, 3\}$, $f[B] = \{1, 2\}$, $f^{-1}[A] = \{1, 2, 3, 4\}$ i $f^{-1}[B] = \{2\}$.

30. $g[R] = R^+ \cup \{0\}$ (rang funkcije g), $g[(1, 2)] = (1, 4)$, $g^{-1}[[0, 1]] = [-1, 1]$ i $g^{-1}[(1, 2)] = (-\sqrt{2}, -1) \cup (1, \sqrt{2})$.

31. Kao i obično, neke dokaze sprovodimo tranformacijama predikatskih formula, a neke baratanjem elementima skupova. Najpre, tvrđenje (a) je očigledno.

    (b) Pretpostavimo da je $A \subseteq B$. Tada

$$\begin{aligned} y \in f[A] &\sim (\exists a \in A) f(a) = y \\ &\sim (\exists a)(a \in A \wedge f(a) = y) \\ &\models (\exists a)(a \in B \wedge f(a) = y) \\ &\sim (\exists a \in B) f(a) = y \\ &\sim y \in f[B]. \end{aligned}$$

    (c) Ako je $C \subseteq D$, imamo

$$\begin{aligned} x \in f^{-1}[C] &\sim f(x) \in C \\ &\models f(x) \in D \\ &\sim x \in f^{-1}[D]. \end{aligned}$$

(d)
$$\begin{aligned} y \in f[A \cup B] &\sim (\exists a \in A \cup B) f(a) = y \\ &\sim (\exists a)(a \in A \cup B \wedge f(a) = y) \\ &\sim (\exists a)((a \in A \vee a \in B) \wedge f(a) = y) \\ &\sim (\exists a)((a \in A \wedge f(a) = y) \vee (a \in B \wedge f(a) = y)) \\ &\sim (\exists a)(a \in A \wedge f(a) = y) \vee (\exists a)(a \in B \wedge f(a) = y) \\ &\sim (\exists a \in A) f(a) = y \vee (\exists a \in B) f(a) = y \\ &\sim y \in f[A] \vee y \in f[B] \\ &\sim y \in f[A] \cup f[B]. \end{aligned}$$

(e)

$$\begin{aligned} x \in f^{-1}[C \cup D] &\sim f(x) \in C \cup D \\ &\sim f(x) \in C \vee f(x) \in D \\ &\sim x \in f^{-1}[C] \vee x \in f^{-1}[D] \\ &\sim x \in f^{-1}[C] \cup f^{-1}[D]. \end{aligned}$$

(f) Neka $y \in f[A \cap B]$. To znači da postoji $a \in A \cap B$ takvo da $f(a) = y$. Pošto $a \in A$ i $f(a) = y$, dobijamo $y \in f[A]$. Analogno, pošto $a \in B$ i $f(a) = y$, dobijamo $y \in f[B]$. Dakle, $y \in f[A] \cap f[B]$.

(g) Analogno dokazu pod (e).

(h) Dokažimo $g \circ f[A] \subseteq g[f[A]]$ i $g[f[A]] \subseteq g \circ f[A]$. Pretpostavimo prvo da $z \in g \circ f[A]$. To znači da postoji $a \in A$ takvo da $g \circ f(a) = z$, tj. $g(f(a)) = z$. Ali tada $f(a) \in f[A]$ pa $z \in g[f[A]]$.

Obratno, neka $z \in g[f[A]]$. To znači da postoji $y \in f[A]$ takav da $g(y) = z$. To što $y \in f[A]$ dalje znači da postoji $a \in A$ takav da $f(a) = y$. Ali tada je $g \circ f(a) = z$, pa $z \in g \circ f[A]$.

(i)
$$\begin{aligned} x \in (g \circ f)^{-1}[E] &\sim g \circ f(x) \in E \\ &\sim g(f(x)) \in E \\ &\sim f(x) \in g^{-1}[E] \\ &\sim x \in f^{-1}[g^{-1}[E]]. \end{aligned}$$

32. (a) Neka prvo $y \in f[A] \setminus f[B]$. Tada postoji $a \in A$ takav da $f(a) = y$. Kako $y \notin f[B]$, sledi $a \notin B$. Dakle, $a \in A \setminus B$, pa $y \in f[A \setminus B]$.

(b)
$$\begin{aligned} x \in f^{-1}[C \setminus D] &\sim f(x) \in C \setminus D \\ &\sim f(x) \in C \wedge f(x) \notin D \\ &\sim x \in f^{-1}[C] \wedge x \notin f^{-1}[D] \\ &\sim x \in f^{-1}[C] \setminus f^{-1}[D] \end{aligned}$$

(c) Pod (a) je već dokazano da je $f[A] \setminus f[B] \subseteq f[A \setminus B]$. Neka je sada f 1-1 funkcija i $y \in f[A \setminus B]$. Tada postoji $a \in A \setminus B$ takav da $f(a) = y$. Odatle sledi $y \in f[A]$. Međutim, ako bi postojalo $b \in B$ takvo da $f(b) = y$, iz uslova 1-1 bi sledilo $a = b$, tj. $a \in B$, što nije tačno. Dakle $y \notin f[B]$, pa imamo i $f[A \setminus B] \subseteq f[A] \setminus f[B]$.

(d) Primer kada važi striktna inkluzija: $X = \{x_1, x_2\}$, $Y = \{y\}$, $A = \{x_1, x_2\}$, $B = \{x_1\}$ i $f : \begin{pmatrix} x_1 & x_2 \\ y & y \end{pmatrix}$. Tada je $f[A] = f[B] = \{y\}$ pa je $f[A] \setminus f[B] = \emptyset$. S druge strane $A \setminus B = \{x_2\}$, pa $f[A \setminus B] = \{y\}$.

33. Pretpostavimo suprotno, da postoji $y \in f[A] \cap f[B]$. Pošto $y \in f[A]$, postoji $a \in A$ takav da je $f(a) = y$. Pošto $y \in f[B]$, postoji i $b \in B$ takav da je $f(b) = y$. Međutim, f je 1-1, pa iz $f(a) = f(b)$ dobijamo $a = b$. Dakle, $a \in A \cap B$, kontradikcija.

34. Prema definiciji simetrične razlike imamo:

$$\begin{aligned} & x \in f^{-1}[A \triangle B] \\ \sim\ & f(x) \in A \triangle B \\ \sim\ & (f(x) \in A \wedge f(x) \notin B) \vee (f(x) \notin A \wedge f(x) \in B) \\ \sim\ & (x \in f^{-1}[A] \wedge x \notin f^{-1}[B]) \vee (x \notin f^{-1}[A] \wedge x \in f^{-1}[B]) \\ \sim\ & x \in f^{-1}[A] \triangle f^{-1}[B] \end{aligned}$$

35. (a) Neka je $a \in A$. Tada direktno imamo $f(a) \in f[A]$, pa $a \in f^{-1}[f[A]]$.

(b) Neka je f 1-1 i $x \in f^{-1}[f[A]]$. To znači da je $f(x) \in f[A]$, tj. da postoji $a \in A$ takvo da $f(a) = f(x)$. Kako je f 1-1, sledi $a = x$, odnosno $x \in A$. Dakle, $f^{-1}[f[A]] \subseteq A$.

(c) Primer kada jednakost ne važi: uzmimo $X = \{x_1, x_2\}$, $Y = \{y\}$, $A = \{x_1\}$ i $f : \begin{pmatrix} x_1 & x_2 \\ y & y \end{pmatrix}$. Tada je $f[A] = \{y\}$ pa je $f^{-1}[f[A]] = \{x_1, x_2\} \neq A$.

36. (a) Neka prvo $y \in f[f^{-1}[A]]$. To znači da postoji $x \in f^{-1}[A]$ takvo da je $f(x) = y$. Međutim, $x \in f^{-1}[A]$ znači da je $f(x) \in A$, dakle $y \in A$.

(b) Obratno, neka je f „na". Tada, ako $y \in A$, onda postoji $x \in X$ takvo da $f(x) = y$. Kako $y \in A$, imamo da je $x \in f^{-1}[A]$, a odatle sledi $y \in f[f^{-1}[A]]$. Dakle, u ovom slučaju je i $A \subseteq f[f^{-1}[A]]$.

(c) Primer kada jednakost ne važi: uzmimo $X = \{x\}$, $Y = \{y_1, y_2\}$, $A = \{y_1\}$ i $f : \begin{pmatrix} x \\ y_2 \end{pmatrix}$. Tada je $f^{-1}[A] = \emptyset$ pa je i $f[f^{-1}[A]] = \emptyset \neq A$.

37. I rešenje. Neka su $A_1, A_2 \in P(X)$ i neka je $A_1 \neq A_2$. To znači da postoji $a \in A_1 \setminus A_2$ ili $a \in A_2 \setminus A_1$, recimo ovo prvo. Pošto je $a_1 \in A_1$, direktno dobijamo $f(a) \in f[A_1]$. Ali važi i $f(a) \notin f[A_2]$: zaista, ako bi postojalo $x \in A_2$ takvo da $f(x) = f(a)$, pošto je f 1-1 imali bismo $a = x \in A_2$, kontradikcija. Dakle, $f[A_1] \neq f[A_2]$, tj. $g(A_1) \neq g(A_2)$.

II rešenje. Iz zadatka 32(a) i iz $A_1 \setminus A_2 \neq \emptyset$ sledi $f[A_1] \setminus f[A_2] \neq \emptyset$.

38. (a) π_1 nije 1-1 jer npr. $\pi_1(1,1) = 1 = \pi_1(1,2)$.

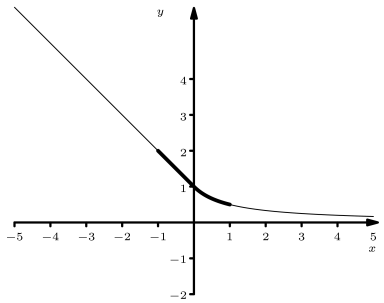
(b) π_1 je „na": za svako $x \in R$ imamo element koji se slika u x, recimo $\pi_1(x,1) = x$.

(c) Dokažimo da je $\pi_1[A] = \{x \in R : 0 \leq x \leq 1\}$ (to je interval $[0,1]$).

Prvo dokazujemo $\pi_1[A] \subseteq [0,1]$: za svako $(x,y) \in A$ je $0 \leq x \leq 1$, drugim rečima $\pi_1(x,y) \in [0,1]$.

S druge strane $[0,1] \subseteq \pi_1[A]$ jer za svaki element $x \in [0,1]$ imamo $\pi_1(x,2) = x$ i $(x,2) \in A$, pa $x \in \pi_1[A]$.

39. (1) (a) Skicirajmo grafik funcije i zaključimo da je ona 1-1 ali nije „na":



1-1: Dokažimo da je f 1-1. Neka je $f(x) = f(y)$; treba pokazati da sledi $x = y$. Posmatramo tri slučaja:

1° $x < 0$ i $y < 0$. Tada je $-x + 1 = -y + 1$, odakle $x = y$.

2° $x \geq 0$ i $y \geq 0$. Tada je $\frac{1}{x+1} = \frac{1}{y+1}$, odakle opet lako sledi $x = y$.

3° $x < 0$ i $y \geq 0$ (ili obrnuto). Ali tada je $f(x) = -x + 1 > 1$ i $f(y) = \frac{1}{y+1} \leq 1$ pa ni ne može biti $f(x) = f(y)$.

„na": f nije „na", jer se nijedan $x \in R$ ne slika u neki negativan broj: za $x < 0$ je $f(x) = -x + 1 > 1$, a za $x \geq 0$ je $f(x) = \frac{1}{x+1} > 0$.

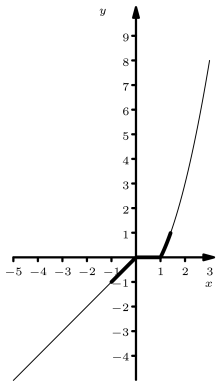
(b) Kako f nije bijekcija, ona nema inverznu funkciju.

(c) $f[(-1,1)] = \{f(x) : -1 < x < 1\} = (\frac{1}{2}, 2)$, jer je $f[(-1,0)] = (1,2)$ i $f[[0,1)] = (\frac{1}{2}, 1]$. (Videti podebljani deo grafika.)
$f^{-1}[(-1,1)] = \{x \in R : f(x) \in (-1,1)\} = (0,\infty)$. Naime, možemo posmatrati slučajeve:

1° $x < 0$. Tada je $f(x) = -x + 1 \notin (-1,1)$.

2° $x \geq 0$. Tada je $f(x) = \frac{1}{x+1}$, a $-1 < \frac{1}{x+1} < 1$ za sve $x > 0$.

(2) (a) Skicirajmo grafik funcije i zaključimo da ona nije 1-1 ali jeste „na":



1-1: Funkcija nije 1-1, jer se svi elementi intervala $[0,1]$ slikaju u nulu, npr. $f(0) = f(1) = 0$.

„na": Dokažimo da je f „na". Neka je $b \in R$ proizvoljan. Tražimo $a \in R$ takvo da je $f(a) = b$. Posmatramo tri slučaja:

1° $b < 0$. Tada je $f(b) = b$.

2° $b = 0$. Tada je npr. $f(1) = 0$.

3° $b > 0$. Treba da nađemo $a \in R$ takvo da je $f(a) = a^2 - 1 = b$, pa dobijamo $a = \sqrt{b+1}$. Kako je $b > 0$, sledi $a > 1$ pa je zaista $f(a) = a^2 - 1 = b$.

(b) Kako f nije bijekcija, ona nema inverznu funkciju.

(c) $f[(-1,1)] = \{f(x) : -1 < x < 1\} = (-1,0]$, jer je $f[(-1,0)] = (-1,0)$ i $f[[0,1)] = \{0\}$.
Dokažimo da je $f^{-1}[(-1,1)] = \{x \in R : f(x) \in (-1,1)\} = (-1,\sqrt{2})$ (videti podebljani deo grafika). Naime, možemo posmatrati slučajeve:

1° $x < 0$. Tada treba da bude $-1 < f(x) = x < 1$, pa $-1 < x < 0$.

2° $0 \le x \le 1$. Tada je uvek $f(x) = 0 \in (-1, 1)$.

3° $x > 1$. Treba da bude $-1 < x^2 - 1 < 1$, što važi za $1 < x < \sqrt{2}$.

40. Dokažimo indukcijom po n da je $f(n) = 2^{n-1} + 1$ za sve $n \in N$.

B.I. $n = 1$. Po definiciji je $f(1) = 2 = 2^0 + 1$.

I.H. Pretpostavimo da je $f(n) = 2^{n-1} + 1$ za neko n.

I.K. Tada je $f(n+1) = 2f(n) - 1 = 2(2^{n-1} + 1) - 1 = 2^n + 1$.

41. (a) Ispišimo prvih nekoliko vrednosti funkcije f: $f(0) = 3$, $f(1) = f(0) + 2 = 5$, $f(2) = f(1) + 2 = 7$ itd. Možemo zaključiti da je $f(n) = 2n + 3$ za sve $n \in N$; dokažimo to indukcijom.

B.I. Za $n = 0$ je zaista $f(0) = 2 \cdot 0 + 3$.

I.H. Pretpostavimo da je $f(n) = 2n + 3$ za neko n.

I.K. Sada je $f(n+1) = f(n) + 2 = (2n + 3) + 2 = 2(n + 1) + 3$.

(b) Ponovo ćemo ispisati prvih nekoliko vrednosti funkcije g: $g(1) = 2$, $g(2) = 3g(1) + 2 = 8$, $g(3) = 3g(2) + 2 = 26$, $g(4) = 3g(3) + 2 = 80$ itd. Dokažimo indukcijom da je $g(n) = 3^n - 1$ za sve n.

B.I. Za $n = 1$ imamo $g(1) = 2 = 3^1 - 1$.

I.H. Pretpostavimo da je $g(n) = 3^n - 1$ za neko n.

I.K. Koristeći indukcijsku hipotezu dobijamo $g(n + 1) = 3g(n) + 2 = 3(3^n - 1) + 2 = 3^{n+1} - 1$.

42. (a) Dokaz sprovodimo indukcijom. Kako prema rekurentnoj vezi svaki sledeći član niza zavisi od dva prethodna, prirodno je da koristimo indukciju „dubine" 2 (dakle, u indukcijskoj hipotezi pretpostavljamo da tvrđenje važi za neka dva broja).

B.I. Za $n = 0$ je $a_0 = 2 = 2^0 + 1$, a za $n = 1$: $a_1 = 3 = 2^1 + 1$.

I.H. Neka je $a_{n-1} = 2^{n-1} + 1$ i $a_n = 2^n + 1$ za neko n.

I.K. Prema indukcijskoj hipotezi je $a_{n+1} = 3a_n - 2a_{n-1} = 3(2^n + 1) - 2(2^{n-1} + 1) = 3 \cdot 2^n + 3 - 2^n - 2 = 2 \cdot 2^n + 1 = 2^{n+1} + 1$.

(b) Zadatak ponovo dokazujemo indukcijom.

B.I. Za $n = 0$ je $a_0 = 0 = 0 \cdot 2^0$, a za $n = 1$: $a_1 = 2 = 1 \cdot 2^1$.

I.H. Neka je $a_{n-1} = (n-1)2^{n-1}$ i $a_n = n \cdot 2^n$ za neko n.

I.K. Prema indukcijskoj hipotezi je $a_{n+1} = 4(a_n - a_{n-1}) = 4(n2^n - (n-1)2^{n-1}) = 4 \cdot (2n - (n-1))2^{n-1} = (n+1)2^{n+1}$.

43. (a) Treba da nađemo vezu između $f(n) = 1 \cdot 2 \cdot \ldots \cdot n$ i $f(n-1) = 1 \cdot 2 \cdot \ldots \cdot (n-1)$. U prvom proizvodu se nalazi jedan faktor više (to je n) pa je $f(n) = nf(n-1)$. Naravno, početna vrednost je $f(1) = 1$.

Rekurzivna funkcija u Javi izgleda ovako:

```
int Faktorijel(int n)
  {
  if(n==1)
    return 1;
  else
    return n*Faktorijel(n-1);
  }
```

(b) Sada tražimo vezu između $f(n) = n^2$ i $f(n-1) = (n-1)^2 = n^2-2n+1$. Vidimo da je $f(n) = f(n-1) + 2n - 1$. Početna vrednost je $f(1) = 1$.

Rekurzivna funkcija u Javi izgleda ovako:

```
int Kvadrat(int n)
  {
  if(n==1)
    return 1;
  else
    return Kvadrat(n-1)+2*n-1;
  }
```

44. (a) Neka je $X = \{x_1, x_2, \ldots, x_n\}$ i $Y = \{y_1, y_2, \ldots, y_n\}$.

(⇒) Ako je f 1-1, to znači da su elementi $f(x_1), f(x_2), \ldots, f(x_n)$ svi različiti. Ali Y ima tačno n elemenata, pa osim nabrojanih ne može postojati nijedan koji nije slika nekog elementa iz X.

(⇐) Neka je f „na". Ako f ne bi bila 1-1, postojala bi bar dva elementa iz X, npr. x_1 i x_2, koji se preslikavaju u isti element skupa Y. To znači da su svi elementi skupa Y: $f(x_1) = f(x_2), f(x_3), \ldots, f(x_n)$, dakle ima ih najviše $n-1$, što je nemoguće. (Kako je f „na", Y ne može imati drugih elemenata osim slika elemenata iz X.)

(b) Prvo, ako je $f_1 : N \to Z$ data sa $f_1(x) = x$, ona je 1-1 ali nije „na" (nijedan $x \in N$ se ne slika u -1). S druge strane, ako je $f_2 : Z \to N \cup \{0\}$ data sa $f_2(x) = |x|$, ona je „na" ali nije 1-1 (jer je $f_2(-1) = f_2(1)$).

45. $f^{-1} = f$ znači: ako $f(a) = b$, onda i $f(b) = a$. To znači da možemo „upariti" elemente skupa A: u isti par stavljamo elemente koji se slikaju jedan u drugi. Pošto f nema fiksnih tačaka, nijedan element nije uparen sam sa sobom. Dakle, A ima paran broj elemenata.

46. (a) Definišemo funkciju $f : A \times B \to B \times A$ ovako: $f(a, b) = (b, a)$. Dokažimo da je ona bijekcija.

1-1: Ako je $f(a_1, b_1) = f(a_2, b_2)$, to znači da je $(b_1, a_1) = (b_2, a_2)$. Odatle je $b_1 = b_2$ i $a_1 = a_2$, pa je $(a_1, b_1) = (a_2, b_2)$.

„na": Za svako $(b, a) \in B \times A$ je $f(a, b) = (b, a)$, pa je f „na".

(b) Sada definišemo funkciju $g : A \times (B \times C) \to (A \times B) \times C$: $g(a, (b, c)) = ((a, b), c)$. Dokažimo da je i ona bijekcija.

1-1: Iz $g(a_1, (b_1, c_1)) = g(a_2, (b_2, c_2))$ je $((a_1, b_1), c_1) = ((a_2, b_2), c_2)$. Sledi da je $(a_1, b_1) = (a_2, b_2)$ (odakle $a_1 = a_2$ i $b_1 = b_2$) i $c_1 = c_2$. Stoga je $(b_1, c_1) = (b_2, c_2)$ i konačno $(a_1, (b_1, c_1)) = (a_2, (b_2, c_2))$.

„na": Neka je dat element $((a, b), c) \in (A \times B) \times C$. Tada očigledno $g(a, (b, c)) = ((a, b), c)$.

47. Iz $|A| = |C|$ i $|B| = |D|$ sledi da postoje bijekcije $f : A \to C$ i $g : B \to D$. Definišimo $h : A \times B \longrightarrow C \times D$ na sledeći način: $h(a, b) = (f(a), g(b))$. Dokažimo da je h bijekcija.

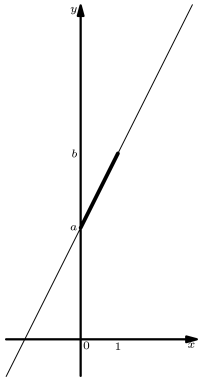
1-1: Pretpostavimo da važi $h(a, b) = h(c, d)$, što znači $(f(a), g(b)) = (f(c), g(d))$. Kako su dva uređena para jednaka akko su im obe koordinate jednake, sledi $f(a) = f(c)$ pa, pošto je f 1-1, dobijamo $a = c$. Analogno imamo i $g(b) = g(d)$ pa $b = d$ jer je i g 1-1. Dakle, $(a, b) = (c, d)$.

„na": Neka $(c,d) \in C \times D$. Tada, pošto su f i g „na" funkcije, postoji $a \in A$ takvo da $f(a) = c$ i postoji $b \in B$ takvo da $g(b) = d$. Odatle $h(a,b) = (f(a), g(b)) = (c,d)$.

48. (a) Funkcija $f : (\frac{\pi}{2}, -\frac{\pi}{2}) \to R$ data sa $f(x) = \operatorname{tg} x$ je bijekcija, pa $|(\frac{\pi}{2}, -\frac{\pi}{2})| = |R|$.

(b) Definišimo prvo linearnu funkciju $g : R \to R$ tako da $g(0) = a$ i $g(1) = b$. Jednačina prave kroz tačke $(0,a)$ i $(1,b)$ je $\frac{y-a}{x-0} = \frac{b-a}{1-0}$, tj. $y = a + (b-a)x$. Dakle, $g(x) = (b-a)x + a$.

Sada uzmimo restrikciju te funkcije na interval $(0,1)$, dakle funkciju $g_1 : (0,1) \to (a,b)$ datu sa $g_1(x) = (b-a)x + a$:



Ona će biti bijekcija pa je $|(0,1)| = |(a,b)|$.

(c) Kako se skupovi $(0,1)$ i $[0,1]$ razlikuju samo u dva elementa (0 i 1) definisaćemo našu funkciju tako što ćemo sve brojeve u nizu $0, 1, \frac{1}{2}, \frac{1}{2^2}, \ldots$ „pomeriti" za dva mesta a sve ostale elemente preslikati u sebe. Dakle, bijekciju $h : [0,1] \to (0,1)$ definišemo sa

$$h(x) = \begin{cases} \frac{1}{2}, & \text{ako je } x = 0 \\ \frac{1}{2^{n+2}}, & \text{ako je } x = \frac{1}{2^n} \text{ za neko } n \in N \cup \{0\} \\ x, & \text{inače.} \end{cases}$$

Literatura

[1] I. Dolinka, *Kratak uvod u analizu algoritama*, Univerzitet u Novom Sadu, Novi Sad, 2008.

[2] R. Doroslovački, *Algebra*, Stylos, Novi Sad, 1995.

[3] P. A. Fejer, D. A. Simovici, *Mathematical Foundations of Computer Science*, Springer, New York, 1991.

[4] G. Haggard, J. Schlipf, S. Whitesides, *Discrete Mathematics for Computer Science*, Thomson Brooks/Cole, Belmont, 2006.

[5] J. L. Hein, *Discrete Structures, Logic and Computability* (3rd ed.), Jones and Bartlett, Sudbury, 2010.

[6] A. Jovanović, A. Perović, B. Veličković, *Teorija skupova*, Matematički fakultet, Beograd, 2007.

[7] D. Mašulović, *Odabrane teme diskretne matematike*, Prirodno-matematički fakultet, Novi Sad, 2007.

[8] D. Mašulović, *Diskretna matematika za informatičare 1*, Prirodno-matematički fakultet, Novi Sad, 2014.

[9] V. Mićić, Z. Kadelburg, D. Đukić, *Uvod u teoriju brojeva* (5. dopunjeno izdanje), Društvo matematičara Srbije, Beograd, 2013.

[10] S. Milić, *Elementi matematičke logike i teorije skupova*, Institut za matematiku, Novi Sad, 1981.

[11] N. Mudrinski, *Predavanja iz algebre za informatičare*, Prirodno-matematički fakultet, Novi Sad, 2017.

[12] Đ. Paunić, *Strukture podataka i algoritmi*, Univerzitet u Novom Sadu, Novi Sad, 1997.

[13] V. Petrović, *Teorija grafova*, Univerzitet u Novom Sadu, Novi Sad, 1998.

[14] M. Racković, S. Škrbić, J. Vidaković, *Uvod u baze podataka*, Univerzitet u Novom Sadu, Novi Sad, 2007.

[15] G. S. Rao, *Mathematical Foundations of Computer Science*, I.K. International, New Delhi, 2006.

[16] Y. N. Singh, *Mathematical Foundations of Computer Science*, New Age International, New Delhi, 2005.

[17] B. Šešelja, A. Tepavčević, *Algebra 1, teorija i zadaci*, Univerzitet u Novom Sadu i Simbol, Novi Sad, 2010.

[18] G. Vojvodić, *Predavanja iz matematičke logike*, Univerzitet u Novom Sadu, Novi Sad, 2007.

[19] G. Vojvodić, *Predavanja iz algebre*, Univerzitet u Novom Sadu, Novi Sad, 2007.

[20] G. Vojvodić, B. Šobot, *Zbirka zadataka iz matematičke logike i algebre*, Zavod za udžbenike, Beograd, 2011.

[21] G. Zigler, *Smem li da brojim?*, Matematički institut SANU, Centar za promociju nauke i Zavod za udžbenike, Beograd, 2012.

Indeks