Univerzitet u Beogradu

Matematički fakultet

Eliminacija kvantifikatora i srednjoškolska nastava algebre

- Master rad -

Student: Miroslav M. Krčevinac
Mentor: dr Nebojša Ikodinović

Beograd, 2014.

Sadržaj

Predgovor

U ovom radu se govori o eliminaciji kvantifikatora, postupku koji ima velike primene u mnogim oblastima matematike kao što su: algebra, geometrija, matematička logika, teorijsko računarstvo itd. U ranoj teoriji modela, eliminacija kvantifikatora je korišćena da se pokaže da razne teorije poseduju određena model-teoretska svojstva, poput odlučivosti i kompletnosti. Uobičajeno je da se prvo pokaže da teorija dopušta eliminaciju kvantifikatora, a potom se dokaže odlučivost ili kompletnost razmatranjem formula bez kvantifikatora.

Rad se sastoji iz pet delova, a sedam poglavlja.

U prvom poglavlju dat je pregled osnovnih pojmova matematičke logike. Tu se prvenstveno misli na pojmove u vezi sa logikom prvog reda, kao što su valjane formule, modeli, kontramodeli, relacija zadovoljenja, Hilbertov sistem za dedukciju, preneks normalna forma.

U drugom poglavlju na raznim primerima su analizirani logički aspekti rešavanja raznih vrsta (ne)jednačina, koje se obrađuju tokom srednjoškolske nastave matematike. U ovim primerima akcenat je na primeni tautologija i valjanih formula. Takođe, primerima su motivisani i sadržaji koji se nalaze u nastavku rada.

U trećem poglavlju uveden je pojam odlučivosti, kao jedan od pojmova koji je u tesnoj vezi sa eliminacijom kvantifikatora. Dat je opis metode eliminacije kvantifikatora, kao i pregled nekih teorija koje je dopuštaju. Poslednji deo poglavlja predstavlja primer jednog kriterijuma za utvrđivanje da li neka teorija dopušta eliminaciju kvantifikatora.

Sledeća tri poglavlja u radu posvećena su trima odabranim teorijama koje dopuštaju eliminaciju kvantifikatora: teoriji gustih uređenih Abelovih grupa bez krajnjih tačaka (četvrto poglavlje), teoriji algebarski zatvorenih polja (peto poglavlje) i teoriji realno zatvorenih polja (šesto poglavlje). U četvrtom poglavlju nalazi se i deo koji se odnosi na Furije-Mockinovu metodu za rešavanje sistema linearnih nejednačina, kao primer primene eliminacije kvantifikatora u elementarnoj algebri. Peto poglavlje govori o pojmu rezolvente dva polinoma, koji se koristi u dokazu eliminacije kvantifikatora za teoriju algebarski zatvorenih polja. Šesto poglavlje, sadrži kratku priču o eliminaciji kvantifikatora u teoriji realno zatvorenih polja, kao i priču o metodi virtuelne supstitucije, jednoj od nekoliko metoda koje se koriste u tu svrhu.

Poslednje, sedmo poglavlje, čine srednjoškolski zadaci na kojima je ilustrovana eliminacija kvantifikatora. Tu je uglavnom reč o primeni eliminacije kvantifikatora na neke iracionalne (ne)jednačine.

Za kraj, želeo bih da izrazim posebnu zahvalnost *dr Nebojši Ikodinoviću*, koji mi je ukazao veliku čast prihvativši da bude moj mentor i pruživši mi neizmernu pomoć prilikom izrade ovog master rada. Njegova predavanja iz kursa *Metodika nastave matematike i računarstva* na IV godini osnovnih studija na Matematičkom fakultetu u Beogradu su bila moja najveća motivacija. Uživao sam pohađajući taj kurs.

1 Logika prvog reda

Logika prvog reda opisuje takozvane **operacijsko-relacijske strukture**. Jednu takvu strukturu shvatamo kao uređenu četvorku $\mathbf{M} = (M, \mathcal{R}, \mathcal{F}, C)$, gde je M neki neprazan skup, $\mathcal{R}$ skup nekih relacija skupa M, $\mathcal{F}$ skup nekih operacija skupa M i $C \subseteq M$. Skup M nazivamo *domenom* strukture $\mathbf{M}$, a elemente skupa C nazivamo *konstantama* strukture $\mathbf{M}$.

Svaka operacija i svaka relacija ima svoju dužinu[1]. Preciznije rečeno, n-arna operacija skupa M je funkcija $f : M^n \longrightarrow M$, a n-arna relacija je podskup $R \subseteq M^n$. Skup svih relacija nad skupom M je $\bigcup_{n\in\mathbb{N}} \mathcal{P}(M^n)$, dok je $\bigcup_{n\in\mathbb{N}}\{f \mid f : M^n \longrightarrow M\}$ skup svih operacija skupa M. Ako strukturu čini samo domen sa operacijama i konstantama, bez relacija, onda tu strukturu nazivamo *algebrom*.

Najjednostavnija klasifikacija pomenutih struktura vrši se prema jeziku strukture, odnosno prema broju i dužini relacija i operacija, kao i broju konstanti koje učestvuju u njihovoj definiciji. Drugim rečima, vrstu neke strukture određujemo izborom tri međusobno disjunktna skupa: $\mathrm{Rel}_{\mathcal{L}}$, $\mathrm{Fun}_{\mathcal{L}}$ i $\mathrm{Const}_{\mathcal{L}}$. Elementi skupa $\mathrm{Rel}_{\mathcal{L}}$ zovu se *relacijski znaci*, elementi skupa $\mathrm{Fun}_{\mathcal{L}}$ *funkcijski ili operacijski znaci*, a elementi skupa $\mathrm{Const}_{\mathcal{L}}$ *simboli konstanti.* Disjunktna unija tri pomenuta skupa predstavlja *jezik* date strukture. Ako taj jezik označimo sa $\mathcal{L}$, onda važi

$$\mathcal{L} = \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Fun}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}}.$$

Za svaki jezik $\mathcal{L}$, na skupu $\mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Fun}_{\mathcal{L}}$ definisana je funkcija $ar : \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Fun}_{\mathcal{L}} \longrightarrow \mathbb{N}$ koja svakom znaku $S \in \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Fun}_{\mathcal{L}}$ pridružuje neki prirodan broj $ar(S)$, takozvanu arnost znaka S.

Pokažimo kako se u logici prvog reda opisuju operacijsko - relacijske strukture. Za vrstu struktura koje želimo da opisujemo opredeljujemo se izborom odgovarajućeg jezika $\mathcal{L} = \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Fun}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}}$. Simbole jezika nazivamo i *nelogičkim simbolima.* Pored ovih simbola, u logici prvog reda koriste se i sledeći *logički simboli*:

- beskonačan skup promenljivih $Var = \{x, y, z, x_1, y_1, z_1, \ldots\}$;
- logički veznici: $\neg$, $\wedge$, $\vee$, $\Rightarrow$ i $\Leftrightarrow$;
- logičke konstante: $\top$, $\bot$;
- znak jednakosti: $=$;
- pomoćni znaci: ( ) ,
- kvantifikatori: $\forall$ (univerzalni) i $\exists$ (egzistencijalni).

Logički i nelogički simboli predstavljaju *alfabet* na kome sastavljamo opise izabrane vrste struktura. U ovim opisima glavnu ulogu imaju *izrazi*(*termi*) i *formule.*

Pod skupom svih izraza jezika $\mathcal{L}$, u oznaci $\mathrm{Term}_{\mathcal{L}}$, podrazumevamo najmanji skup konačnih nizova (logičkih i nelogičkih) simbola takav da:

[1] Koristi se i termin arnost.

- promenljive i simboli konstanti jezika $\mathcal{L}$ su izrazi, odnosno $\mathrm{Const}_{\mathcal{L}} \subseteq \mathrm{Term}_{\mathcal{L}}$ i $\mathrm{Var} \subseteq \mathrm{Term}_{\mathcal{L}}$;
- ako $F \in \mathrm{Fun}_{\mathcal{L}}$ i $t_1, \ldots, t_{ar(F)} \in \mathrm{Term}_{\mathcal{L}}$, onda $F(t_1, \ldots, t_{ar(F)}) \in \mathrm{Term}_{\mathcal{L}}$.

Pod skupom atomičnih (elementarnih) formula jezika $\mathcal{L}$, u oznaci $\mathrm{At}_{\mathcal{L}}$, podrazumevamo skup koji, pored $\top$ i $\bot$, sadrži još samo:

- jednakosti $u = v$, za sve $u, v \in \mathrm{Term}_{\mathcal{L}}$, i
- zapise oblika $R(t_1, \ldots, t_{ar(R)})$, za svaki relacijski simbol $R \in \mathrm{Rel}_{\mathcal{L}}$ i bilo koje terme $t_1, \ldots, t_{ar(R)} \in \mathrm{Term}_{\mathcal{L}}$.

Konačno, definišemo skup svih formula jezika $\mathcal{L}$, u oznaci $\mathrm{For}_{\mathcal{L}}$, kao najmanji skup konačnih nizova simbola takav da:

- sve atomične formule su formule, odnosno $\mathrm{At}_{\mathcal{L}} \subseteq \mathrm{For}_{\mathcal{L}}$;
- ako $\alpha \in \mathrm{For}_{\mathcal{L}}$, onda $\neg\alpha \in \mathrm{For}_{\mathcal{L}}$;
- ako $\alpha, \beta \in \mathrm{For}_{\mathcal{L}}$, onda $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \Rightarrow \beta), (\alpha \Leftrightarrow \beta) \in \mathrm{For}_{\mathcal{L}}$;
- ako $\alpha \in \mathrm{For}_{\mathcal{L}}$, $x \in Var$, onda $\forall x\alpha \in \mathrm{For}_{\mathcal{L}}$ i $\exists x\alpha \in \mathrm{For}_{\mathcal{L}}$.

Primetimo da su definicije izraza i formula induktivne, i da su skupovi izraza i formula različiti za različite izbore sadržaja jezika $\mathcal{L}$. Napomenimo i to da važe osnovne konvencije o pisanju formula, kao što su pravila o brisanju zagrada, dogovoreni prioriteti logičkih veznika itd.

Pojavljivanje promenljive u formuli može biti *slobodno* ili *vezano*. Svako pojavljivanje promenljive koja nije pod dejstvom kvantifikatora naziva se *slobodnim*, a ona pojavljivanja koja jesu pod dejstvom kvantifikatora nazivaju se *vezanim*.

Sve promenljive koje imaju slobodna pojavljivanja u nekoj formuli nazivaju se slobodne promenljive te formule. Skup svih slobodnih promenljivih formule α označavamo sa $\mathrm{Fr}(\alpha)$. Funkciju $\mathrm{Fr} : \mathrm{For}_{\mathcal{L}} \longrightarrow \mathcal{P}(\mathrm{Var})$ precizno definišemo indukcijom po složenosti formule:

- $\mathrm{Fr}(\top) = \mathrm{Fr}(\bot) = \emptyset$;
- $\mathrm{Fr}(u = v) = V(u) \cup V(v)$, $u, v \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(R(t_1, \ldots, t_{ar(R)})) = V(t_1) \cup \ldots \cup V(t_{ar(R)})$, $R \in \mathrm{Rel}_{\mathcal{L}}$, $t_1, \ldots, t_{ar(R)} \in \mathrm{Term}_{\mathcal{L}}$;
- $\mathrm{Fr}(\neg\alpha) = \mathrm{Fr}(\alpha)$;
- $\mathrm{Fr}(\alpha * \beta) = \mathrm{Fr}(\alpha) \cup \mathrm{Fr}(\beta)$, $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$;
- $\mathrm{Fr}(\forall x\alpha) = \mathrm{Fr}(\exists x\alpha) = \mathrm{Fr}(\alpha) \backslash \{x\}$, $x \in \mathrm{Var}$.

Za svaku formulu α, skup $\mathrm{Fr}(\alpha)$ je konačan. Ako je $\mathrm{Fr}(\alpha) \subseteq \{x_1, \ldots, x_n\}$, onda formulu α označavamo i sa $\alpha(x_1, \ldots, x_n)$ kada želimo da istaknemo činjenicu da su sve slobodne promenljive formule α neke od promenljivih $x_1, \ldots, x_n$. Za formulu σ kažemo da je **rečenica** jezika $\mathcal{L}$ ako nema slobodnih promenljivih, tj. ako je $\mathrm{Fr}(\alpha) = \emptyset$. Skup svih rečenica jezika $\mathcal{L}$ označavamo sa $\mathrm{Sent}_{\mathcal{L}}$.

1.1 Relacija zadovoljenja

Da bismo određivali vrednosti izraza, odnosno govorili o tačnosti formula, potrebno je da preciziramo kontekst u kome posmatramo izraze i formule. To činimo tako što izaberemo neki skup M (domen interpretacije), a zatim na tom skupu interpretiramo nelogičke simbole (poštujući njihovu vrstu i dužinu) i promenljivama dodelimo neke elemente skupa M.

Neka je $\mathcal{L}$ jezik i M neki neprazan skup. **Interpretacija** jezika $\mathcal{L}$ na skupu M jeste svaka funkcija $\mathcal{J}_M$ sa domenom $\mathcal{L}$ koja svakom $R \in \mathrm{Rel}_{\mathcal{L}}$ pridružuje jednu ar(R)-arnu relaciju skupa M ($\mathcal{J}_M(R) \subset M^{ar(R)}$), svakom $F \in \mathrm{Fun}_{\mathcal{L}}$ pridružuje jednu ar(F)-arnu operaciju skupa M ($\mathcal{J}_M(F) : M^{ar(F)} \longrightarrow M$) i svakom $c \in \mathrm{Const}_{\mathcal{L}}$ jedan element skupa M tj. $\mathcal{J}_M(c) \in M$. **Model** jezika $\mathcal{L}$ nad nepraznim skupom M je

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

gde je $\mathcal{J}_M$ neka interpretacija jezika $\mathcal{L}$ na skupu M. Dakle, svaki model nekog jezika jednoznačno je određen skupom M i interpretacijom $\mathcal{J}_M$ tog jezika u datom skupu. Ako je $\mathbf{M}$ model jezika $\mathcal{L}$ određen nekom interpretacijom $\mathcal{J}_M$, za svaki $S \in \mathcal{L}$ umesto $\mathcal{J}_M(S)$ kraće se pise $S^{\mathbf{M}}$.

Valuacija promenljivih u skupu M jeste svaka funkcija $\mu : Var \longrightarrow M$. Ako je zadat model $\mathbf{M}$ jezika $\mathcal{L}$ i valuacija $\mu : Var \longrightarrow M$, onda svakom izrazu $t \in \mathrm{Term}_{\mathcal{L}}$ pridružujemo jedinstvenu vrednost $t^{\mathbf{M}}[\mu] \in M$ koju nazivamo *vrednost izraza t u modelu* $\mathbf{M}$ *za valuaciju* μ. Funkciju $t \mapsto t^{\mathbf{M}}[\mu]$ definišemo indukcijom po složenosti izraza t:

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

Slično tome, svakoj formuli $\alpha \in \mathrm{For}_{\mathcal{L}}$ pridružujemo istinitosnu vrednost $\alpha^{\mathbf{M}}[\mu] \in \{0, 1\}$ koju nazivamo *istinitosna vrednost formule* α *u modelu* $\mathbf{M}$ *za valuaciju* μ. Funkciju $\alpha \mapsto \alpha^{\mathbf{M}}[\mu]$ definišemo indukcijom po složenosti formule α:

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

gde je $\mu(x/a)$ valuacija koja promenljivama dodeljuje iste vrednosti kao i valuacija μ, osim promenljivoj x kojoj dodeljuje vrednost a.

Na vrednost izraza u nekom modelu utiču samo vrednosti promenljivih koje se pojavljuju u tom izrazu. Slično tome, na istinitosnu vrednost formule u nekom modelu utiču samo vrednosti slobodnih promenljivih te formule.

Navedimo i sledeću lemu, čiji se dokaz, opet indukcijom po složenosti terma t, može pronaći u [6]:

Lema 1. *Neka je $\boldsymbol{M}$ proizvoljan model jezika $\mathcal{L}$ i $\mu_1, \mu_2 : Var \longrightarrow M$ dve valuacije. Tada važi sledeće:*

1. *za svaki izraz $t \in Term_{\mathcal{L}}$, ako je $\mu_1(v) = \mu_2(v)$, za sve $v \in V(t)$, onda je $t^{\boldsymbol{M}}[\mu_1] = t^{\boldsymbol{M}}[\mu_2]$;*
2. *za svaku formulu $\alpha \in For_{\mathcal{L}}$, ako je $\mu_1(v) = \mu_2(v)$, za sve $v \in Fr(\alpha)$, onda je $\alpha^{\boldsymbol{M}}[\mu_1] = \alpha^{\boldsymbol{M}}[\mu_2]$.*

Iz prethodne leme zaključujemo da je pri određivanju vrednosti izraza t u modelu $\mathbf{M}$ za valuaciju $\mu : Var \longrightarrow M$ značajna samo restrikcija $\mu\mid_{V(t)}$. Kako je $V(t)$ konačan skup, tj. $|V(t)| = n$, za neki prirodan broj n, onda odgovarajuće restrikcije svih valuacija možemo identifikovati sa skupom M^n, jer je pri nekom podrazumevanom uređenju promenljivih $V(t) = \{x_1, \ldots, x_n\}$ svakim $\vec{a} = (a_1, \ldots, a_n) \in M^n$ određena po jedna restrikcija $\nu = \begin{pmatrix} x_1 & \ldots & x_n \\ a_1 & \ldots & a_n \end{pmatrix}$. Navedeni razlozi opravdavaju upotrebu oznake $t^{\mathbf{M}}[\vec{a}]$ za vrednost izraza t u modelu $\mathbf{M}$ za neki $\vec{a} \in M^n$. Napomenimo da isto važi i za formule, pa sa $\alpha^{\mathbf{M}}[\vec{a}]$ označavamo istinitosnu vrednost formule α u modelu $\mathbf{M}$ za neki $\vec{a} \in M^n$.

Sada možemo definisati kada je neka formula tačna. Naime, formula α je tačna, tj. važi u modelu $\mathbf{M}$ za $\vec{a}$, u oznaci $\mathbf{M} \models \alpha[\vec{a}]$, ako je $\alpha^{\mathbf{M}}[\vec{a}] = 1$.

Ako je $V(t) = \emptyset$, tj. ako je t izraz bez promenljivih (zatvoreni izraz) pri određivanju njegove vrednosti u nekom modelu valuacije ne igraju nikakvu ulogu. Drugim rečima, vrednost zatvorenog izraza t potpuno je određena samo izabranim modelom $\mathbf{M}$ i tu vrednost označavamo sa $t^{\mathbf{M}}$. Analogno, ako je $\mathrm{Fr}(\alpha) = \emptyset$, tj. ako je α rečenica, njena istinitosna vrednost zavisi samo od izabranog modela $\mathbf{M}$, a valuacije nisu od značaja, pa ih izostavljamo iz razmatranja. Činjenicu da je rečenica α tačna u modelu $\mathbf{M}$ označavamo sa $\mathbf{M} \models \alpha$.

1.2 Modeli i kontramodeli

U matematičkoj logici veoma je važan sledeći problem: ako je data neka rečenica jezika $\mathcal{L}$, odrediti, ako uopšte postoji, strukturu jezika $\mathcal{L}$ u kojoj je ta rečeneica tačna, odnosno strukturu u kojoj nije tačna. **Model** rečenice $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ jeste svaka struktura jezika $\mathcal{L}$ u kojoj je ta rečenica tačna. Kažemo da je rečenica **zadovoljiva** ako ima bar jedan model. **Kontramodel** rečenice $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ jeste svaka struktura jezika $\mathcal{L}$ u kojoj ta rečenica nije tačna.

Problem zadovoljivosti, odnosno nezadovoljivosti neke rečenice, prirodno se proširuje na problem ispitivanja zadovoljivosti, odnosno nezadovoljivosti nekog skupa rečenica tj. neke *teorije*. Bilo koji skup rečenica $T \subseteq \mathrm{Sent}_{\mathcal{L}}$ naziva se *teorijom* jezika $\mathcal{L}$, a rečenice koje pripadaju T nazivaju se *aksiomama* te teorije.

Model teorije T jezika $\mathcal{L}$ jeste bilo koja struktura na jeziku $\mathcal{L}$ koja zadovoljava sve rečenice iz T. Kontramodel teorije T je bilo koja struktura koja ne zadovoljava bar jednu rečenicu iz T.

Primer 1. *Neka je* $\mathcal{L}_{OF} = \{\leq, +, -, \cdot, 0, 1\}$, *pri čemu je* $Rel_{\mathcal{L}} = \{\leq\}$, $Fun_{\mathcal{L}} = \{+, -, \cdot\}$, $Const_{\mathcal{L}} = \{0, 1\}$ *i* $ar(\leq) = ar(+) = ar(\cdot) = 2$, $ar(-) = 1$. *Označimo sa* T_{OF} *teoriju jezika* $\mathcal{L}_{OF}$, *čije su aksiome sledeće rečenice:*

(1) $\forall x \forall y (x + y = y + x)$

(2) $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$

(3) $\forall x (x + 0 = x)$

(4) $\forall x (x + (-x) = 0)$

(5) $\forall x \forall y (x \cdot y = y \cdot x)$

(6) $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$

(7) $\forall x (x \cdot 1 = x)$

(8) $\forall x (x \neq 0 \Rightarrow \exists y (x \cdot y = 1))$

(9) $\forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$

(10) $0 \neq 1$

(11) $\forall x (x \leq x)$

(12) $\forall x \forall y (x \leq y \wedge y \leq x \Rightarrow x = y)$

(13) $\forall x \forall y \forall z (x \leq y \wedge y \leq z \Rightarrow x \leq z)$

(14) $\forall x \forall y (x \leq y \vee y \leq x)$

(15) $\forall x \forall y \forall z (x \leq y \Rightarrow x + z \leq y + z)$

(16) $\forall x \forall y \forall z (x \leq y \wedge 0 \leq z \Rightarrow x \cdot z \leq y \cdot z)$

Svaki model u kome su tačne sve navedene rečenice nazivamo uređenim poljem. Strukture $\boldsymbol{R} = (\mathbb{R}, \leq, +, -, \cdot, 0, 1)$ *i* $\boldsymbol{Q} = (\mathbb{Q}, \leq, +, -, \cdot, 0, 1)$, *sa standardnim interpretacijama nelogičkih simbola, jesu uređena polja.*

$\triangle$

1.3 Valjane formule

Formula $\alpha \in \mathrm{For}_{\mathcal{L}}$ je **valjana**, u oznaci $\models \alpha$, ako za svaki model $\mathbf{M}$ i svaku valuaciju $\mu : Var \longrightarrow M$ važi $\mathbf{M} \models \alpha[\mu]$. Specijalno, rečenica $\sigma \in \mathrm{Sent}_{\mathcal{L}}$ je valjana ako je tačna u svakom modelu jezika $\mathcal{L}$.

Ne moramo razmatrati valjane formule, već pažnju možemo usmeriti samo na valjane rečenice. Razlog tome je sledeći: ako je $\alpha(x_1, \ldots, x_n)$ valjana formula, onda je to i njeno univerzalno zatvorenje tj. rečenica $\forall x_1 \ldots \forall x_n \alpha(x_1, \ldots, x_n)$. Da bismo se u to uverili, pretpostavimo da je formula α valjana i dokažimo da je tada valjana i formula $\forall x \alpha$, gde je x proizvoljna promenljiva.

Neka je $\mathbf{M}$ proizvoljan model odgovarajućeg jezika i $\mu : Var \longrightarrow M$ proizvoljna valuacija. Pošto je α valjana formula imamo da za svako $a \in M$ važi $\mathbf{M} \models \alpha[\mu(x/a)]$, jer $\mathbf{M} \models \alpha[\nu]$, za svaku valuaciju ν, pa specijalno i za valuacije $\mu(x/a)$, $a \in M$. Prema definiciji relacije zadovoljenja, iz $\mathbf{M} \models \alpha[\mu(x/a)]$, za sve $a \in M$, sledi da $\mathbf{M} \models \alpha[\mu]$. Važi i obrnuto, ako je $\forall x \alpha$ valjana formula, onda je valjana i formula α. Ako proizvoljno izaberemo model $\mathbf{M}$ i valuaciju $\mu : Var \longrightarrow M$, tada će iz $\mathbf{M} \models \forall x \alpha[\mu]$ slediti da $\mathbf{M} \models \alpha[\mu(x/a)]$, za bilo koje $a \in M$, pa specijalno i za $a = \mu(x)$, što znači da će biti i $\mathbf{M} \models \alpha[\mu]$.

Za razliku od iskaznih formula, ne postoji univerzalni postupak pomoću kojeg bismo mogli da ispitamo valjanost bilo koje formule logike prvog reda. Ipak mogu se izvesti neki opšti zaključci.

Sve formule logike prvog reda koje su *instance iskaznih tautologija* sigurno su valjane. Pod instancom tautologije podrazumevamo formulu koja se dobija zamenom svih iskaznih slova nekim formulama prvog reda, pri čemu ista slova menjamo istim formulama. Napomenimo da svaka tautologija ima neograničeno mnogo instanci.

Pokažimo da su instance tautologija zaista valjane. Neka je $\tau(p_1, \ldots, p_n)$ tautologija i $\underline{\tau}$ formula dobijena tako što su slova $p_1, \ldots, p_n$ redom zamenjena formulama $\alpha_1, \ldots, \alpha_n \in \mathrm{For}_{\mathcal{L}}$. Tada će za proizvoljan model $\mathbf{M}$ i bilo koju valuaciju μ važiti $\underline{\tau}^{\mathbf{M}}[\mu] = \hat{v}(\tau)$, gde je $\hat{v}$ valuacija iskaznih slova takva da je $v(p_i) = \alpha_i^{\mathbf{M}}[\mu]$, $i = 1, \ldots, n$, odakle sledi tvrđenje.

U narednoj tabeli su prikazane neke tautologije sa svojim nazivima[2]. Napomenimo da se generalno tautologije *ne dele* na „tablične” i na one koje to nisu. Izdvajanje ovih tautologija olakšava rešavanje pojedinih zadataka koji se pojavljuju u narednom poglavlju.

$p \Rightarrow p$	zakon refleksivnosti za implikaciju
$p \vee \neg p$	zakon isključenja trećeg
$\neg(p \wedge \neg p)$	zakon neprotivrečnosti
$\neg\neg p \Leftrightarrow p$	zakon dvojne negacije
$((p \Rightarrow q) \Rightarrow p) \Rightarrow p$	Pirsov zakon
$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	zakon tranzitivnosti za implikaciju
$((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Rightarrow (p \Leftrightarrow r)$	zakon tranzitivnosti za ekvivalenciju
$\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$	zakon negiranja implikacije

[2] Tautologije iz tabele su preuzete iz [1].

$(p \Rightarrow q) \Leftrightarrow \neg p \vee q$	zakon uklanjanja implikacije
$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$	zakon uklanjanja ekvivalencije
$(\neg p \Rightarrow (q \wedge \neg p)) \Rightarrow p$	zakon svođenja na apsurd
$(p \Rightarrow q) \Leftrightarrow (p \Leftrightarrow (p \wedge q))$	zakon o pravoj posledici
$p \vee p \Leftrightarrow p\,,\ p \wedge p \Leftrightarrow p$	zakon idempotencije za $\vee$ i $\wedge$
$p \wedge q \Leftrightarrow q \wedge p\,,\ p \vee q \Leftrightarrow q \vee p$	zakon komutacije za $\wedge$ i $\vee$
$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$	zakon asocijacije za $\vee$
$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	zakon asocijacije za $\wedge$
$p \vee (p \wedge q) \Leftrightarrow p\,,\ p \wedge (p \vee q) \Leftrightarrow p$	zakoni apsorpcije
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	zakon distribucije $\vee$ prema $\wedge$
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	zakon distribucije $\wedge$ prema $\vee$
$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	De Morganov zakon
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	De Morganov zakon
$(p \wedge (p \Rightarrow q)) \Rightarrow q$	modus ponens
$((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p$	modus tolens
$(p \Rightarrow r) \wedge (q \Rightarrow r) \Leftrightarrow ((p \vee q) \Rightarrow r)$	dokaz nabrajanjem
$p \vee \bot \Leftrightarrow p$	pravilo sabiranja sa $\bot$
$p \wedge \top \Leftrightarrow p$	pravilo množenja sa $\top$

Postoji dosta valjanih formula koje nisu instance iskaznih tautologija. Navedimo neke od najjednostavnijih[3]:

- univerzalni kvantifikator se „lepo slaže” sa konjukcijom
$$\forall x(\alpha \wedge \beta) \Leftrightarrow \forall x\alpha \wedge \forall x\beta$$
- egzistencijalni kvantifikator se „lepo slaže” sa disjunkcijom
$$\exists x(\alpha \vee \beta) \Leftrightarrow \exists x\alpha \vee \exists x\beta$$
- univerzalni kvantifikator se samo „delimično slaže” sa disjunkcijom
$$\forall x(\alpha \vee \beta) \Leftarrow \forall x\alpha \vee \forall x\beta$$
- egzistencijalni kvantifikator se samo „delimično slaže” sa konjukcijom
$$\exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$$
- ukoliko x **nije** slobodna promenljiva formule α onda su valjane i formule
$$\forall x(\alpha \vee \beta) \Leftrightarrow \alpha \vee \forall x\beta$$
$$\exists x(\alpha \wedge \beta) \Leftrightarrow \alpha \wedge \exists x\beta$$

[3] Dokazi valjanosti ovih formula mogu se pronaći u [6].

- dva kvantifikatora iste vrste mogu zameniti mesta

$$\forall x \forall y \alpha \Leftrightarrow \forall y \forall x \alpha$$

$$\exists x \exists y \alpha \Leftrightarrow \exists y \exists x \alpha$$

- De Morganovi zakoni za kvantifikatore

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

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

- zamena promenljive termom - ako je t zatvoren izraz nekog jezika i α formula istog jezika, onda je formula

$$\forall x \alpha \Rightarrow \alpha(x/t)$$

  valjana, pri čemu je $\alpha(x/t)$ formula dobijena iz α tako što su sva slobodna pojavljivanja promenljive x zamenjena izrazom t

1.4 Sistemi za dedukciju logike prvog reda

Pojam valjanosti je semantičke prirode, a koncept dokazivanja i sistema za dedukciju vodi do pojma teoreme koji je sintaksno - deduktivne prirode. Kao što je teorija modela vezana za semantiku, tako su deduktivni sistemi i teorija dokaza vezani za sintaksu. Pojam *teoreme* je deduktivni pandan pojma valjane formule, koji je semantičke prirode. Između ova dva pojma postoji veza: ako je neka formula valjana, onda ona može biti dokazana u okviru nekog deduktivnog sistema, a ako za neku formulu postoji dokaz u okviru deduktivnog sistema onda je ona sigurno valjana. Sistemi za dedukciju za logiku prvog reda su čisto sintaksne prirode - primenjuju se kroz kombinovanje simbola, ne ulazeći u semantiku formula.

Zadržaćemo se na primeru Hilbertovog sistema za dedukciju.

Za formulu φ kažemo da je dokaziva iz skupa pretpostavki Γ, u oznaci $\Gamma \vdash \varphi$, akko postoji konačan niz formula $\varphi_1, \varphi_2, \ldots, \varphi_n$ sa sledećim svojstvima:

1. φ_n je formula φ;
2. svaka formula φ_k, $k = 1, \ldots, n$, zadovoljava jedan od sledećih uslova:
   - $\varphi_i \in \mathcal{A}$, ili
   - $\varphi_i \in \Gamma$, ili
   - φ_i je neposredna posledica nekog od pravila iz $\mathcal{R}$ čije premise pripadaju skupu $\{\varphi_1, \ldots, \varphi_{i-1}\}$

pri čemu je $\mathcal{A}$ beskonačan skup formula određenih shemama

(H1) $\alpha \Rightarrow (\beta \Rightarrow \alpha)$

(H2) $(\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$

(H3) $\alpha \wedge \beta \Rightarrow \alpha$

(H4) $\alpha \wedge \beta \Rightarrow \beta$

(H5) $\alpha \Rightarrow (\beta \Rightarrow \alpha \wedge \beta)$

(H6) $\alpha \Rightarrow \alpha \vee \beta$

(H7) $\beta \Rightarrow \alpha \vee \beta$

(H8) $(\alpha \Rightarrow \gamma) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow (\alpha \vee \beta \Rightarrow \gamma))$

(H9) $\neg\alpha \Rightarrow (\alpha \Rightarrow \perp)$

(H10) $(\alpha \Rightarrow \perp) \Rightarrow \neg\alpha$

(H11) $\perp \Rightarrow \alpha$

(H12) $\alpha \vee \neg\alpha$

(H13) $\alpha(x := t) \Rightarrow \exists x\alpha$

(H14) $\forall x\alpha \Rightarrow \alpha(x := t)$

dok $\mathcal{R}$ čine pravila:

- β je neposredna posledica formula α i $\alpha \Rightarrow \beta$, za proizvoljne formule α i β
- $\gamma \Rightarrow \forall x\alpha$ je neposredna posledica formule $\gamma \Rightarrow \alpha$, za proizvoljnu formulu α, bilo koju promenljivu x i svaku formulu γ u kojoj x nije slobiodna promenljiva
- $\exists x\alpha \Rightarrow \gamma$ je neposredna posledica formule $\alpha \Rightarrow \gamma$, za proizvoljnu formulu α, bilo koju promenljivu x i svaku formulu γ u kojoj x nije slobiodna promenljiva

Svaki niz formula $\varphi_1, \varphi_2, \ldots, \varphi_n$ koji zadovoljava uslove **1.** i **2.** nazivamo Γ-dokazom, odnosno dokazom formule φ_n iz skupa pretpostavki Γ.

1.5 Preneks normalna forma

Jedna tehnika koju možemo koristiti prilikom rešavanja različitih problema u logici prvog reda jeste konstrukcija *preneks normalne forme*. Ovaj pojam je neophodan za sprovođenje *Furije*[4]-*Mockinove*[5] *procedure*, o kojoj će biti reči u jednom od narednih poglavlja.

Formule α i β nekog jezika $\mathcal{L}$ jesu *semantički ekvivalentne*, u oznaci $\alpha \equiv \beta$, ako je $\models \alpha \Leftrightarrow \beta$. Neke od valjanih formula govore upravo o semantičkoj ekvivalentnosti određenih formula, kao na primer

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

$$\exists x(\alpha \vee \beta) \equiv \exists x\alpha \vee \exists x\beta.$$

[4]Joseph Fourier (1768 - 1830) - francuski matematičar i fizičar
[5]Theodore Samuel Motzkin (1908 - 1970) - izraelsko-američki matematičar

Ove ekvivalencije zajedno sa nekim koje se koriste u iskaznoj logici, omogućavaju nam da sve kvantifikatore neke formule „izvučemo napred” tj. da formulu transformišemo u preneks normalnu formu.

Formula α je u **preneks normalnoj formi** ukoliko je oblika

$$Q_1x_1 \ldots Q_nx_n\theta$$

gde je svaki Q_i neki kvantifikator, a θ je formula bez kvantifikatora. Deo $Q_1x_1 \ldots Q_nx_n$ se naziva *prefiks* formule α. Prefiks može biti prazan, pa se i svaka formula bez kvantifikatora smatra formulom u preneks normalnoj formi.

Navedimo da važi i sledeća lema, čiji dokaz se može pronaći u [6]:

Lema 2. *Svaka formula je ekvivalentna formuli koja je u preneks normalnoj formi.*

U praksi algoritam koji se koristi za nalaženje preneks normalne forme date formule ima sledeće korake:

- oslobađanje logičkih veznika $\Rightarrow$ i $\Leftrightarrow$ izražavanjem preko $\wedge$, $\vee$ i $\neg$; tu koristimo sledeće logičke ekvivalencije
$$\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$$
$$\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$$
- upotreba De Morganovih zakona za „uvlačenje negacije unutra”
$$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$$
$$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$$
- oslobađanje duplih negacija
$$\neg\neg\alpha \equiv \alpha$$
- preimenovanje nekih vezanih promenljivih (ukoliko je to neophodno)
- „pomeranje” kvantifikatora ispred formule.

Za kraj uvedimo još neke pojmove. Za neku formulu jezika $\mathcal{L}$ kažemo da je *egzistencijalna formula* ako je u preneks formi koja sadrži jedino egzistencijalne kvantifikatore u svom prefiksu. Za egzistencijalnu formulu kažemo da je *primitivna* ako je oblika $\exists x_1 \ldots \exists x_n \alpha(x_1, \ldots, x_n)$, pri čemu je α konjukcija atomičnih i negacija atomičnih formula.

2 Neke primene tautologija i valjanih formula

Nakon što smo uveli pojam valjanih formula, red je i da vidimo koja je njihova uloga tj. kako ih možemo primeniti. Akcenat će biti na primeni tautologija i valjanih formula za rešavanje jednačina i nejednačina. Preciznije rečeno, na primerima ćemo analizirati logičke aspekte rešavanja raznih vrsta jednačina i nejednačina. Primeri, koji su najveći deo ovog poglavlja, poslužiće kao motivacija za ono što će biti izloženo u nastavku rada.

Za naredne primere (samo u okviru ovog poglavlja) koristićemo termin zadaci. Simbol ♦ označava kraj zadatka.

Zadatak 1. *Rešiti po* $x \in \mathbb{R}$ *nejednačinu* $(x-1)(x-2) > 0$.

Rešenje. Kako nam je cilj da rešimo zadatak sa logičkog aspekta, razmotrimo sledeći ekvivalencijski lanac:

$$\begin{aligned}(x-1)(x-2) > 0 \quad &\Leftrightarrow \quad (x-1>0 \land x-2>0) \lor (x-1<0 \land x-2<0)\\ &\Leftrightarrow \quad (x>1 \land x>2) \lor (x<1 \land x<2)\\ &\Leftrightarrow \quad x>2 \lor x<1\end{aligned}$$

Dakle, vidimo da su rešenja svi realni brojevi manji od 1 i uz njih svi realni brojevi veći od 2. Drugim rečima, skup svih rešenja je interval oblika $(-\infty, 1) \cup (2, +\infty)$. ♦

Zadržimo se malo na ovom zadatku i analizirajmo šta smo sve iskoristili prilikom formiranja ekvivalencijskog lanca. U prvom redu primetimo da je iskorišćena ekvivalencija o pozitivnosti proizvoda dva realna broja

$$a \cdot b > 0 \Leftrightarrow (a > 0 \land b > 0) \lor (a < 0 \land b < 0)\,.$$

Takođe, u ovom zadatku iskorišćena je i tautologija

$$(p \Rightarrow q) \Leftrightarrow (p \Leftrightarrow (p \land q))$$

koja se pojavljuje u pomenutoj tablici na početku poglavlja i nosi naziv *zakon o pravoj posledici*. Ovu tautologiju smo iskoristili pri prelasku iz drugog u treći red, gde prema njoj važi da je $x < 1$ i $x < 2$ ekvivalentno sa $x < 1$, jer $x < 1$ povlači $x < 2$.

Prilikom rešavanja jednačina koje su „sastavljene” od racionalnih algebarskih izraza koristi se ekvivalencija

$$\frac{A(x)}{B(x)} = 0 \Leftrightarrow A(x) = 0 \land B(x) \neq 0. \tag{1}$$

Zadatak 2. *Rešiti jednačinu* $1 - \dfrac{1}{x} = \dfrac{2}{x^2 - x} - \dfrac{2}{x-1}$.

Rešenje. Formirajmo ponovo ekvivalencijski lanac:

$$
\begin{aligned}
1-\frac{1}{x}=\frac{2}{x^2-x}-\frac{2}{x-1} \quad &\Leftrightarrow \quad \frac{x-1}{x}-\frac{2}{x(x-1)}+\frac{2}{x-1}=0\\
&\Leftrightarrow \quad \frac{(x-1)^2-2+2x}{x(x-1)}=0\\
&\Leftrightarrow \quad \frac{x^2-2x+1-2+2x}{x(x-1)}=0\\
&\Leftrightarrow \quad \frac{x^2-1}{x(x-1)}=0
\end{aligned}
$$

Sada primenjujemo formulu (1):

$$
\begin{aligned}
1-\frac{1}{x}=\frac{2}{x^2-x}-\frac{2}{x-1} \quad &\Leftrightarrow \quad x^2-1=0 \land x(x-1)\neq 0\\
&\Leftrightarrow \quad (x-1)(x+1)=0 \land x\neq 0 \land x\neq 1\\
&\Leftrightarrow \quad (x-1=0 \lor x+1=0) \land x\neq 0 \land x\neq 1\\
&\Leftrightarrow \quad (x=1 \lor x=-1) \land x\neq 0 \land x\neq 1 \qquad (\star)\\
&\Leftrightarrow \quad (x=1 \land x\neq 0 \land x\neq 1) \lor (x=-1 \land x\neq 0 \land x\neq 1)\\
&\Leftrightarrow \quad \perp \lor (x=-1 \land x\neq 0 \land x\neq 1)\\
&\Leftrightarrow \quad x=-1
\end{aligned}
$$

Dakle, zaključujemo da je $x=-1$ jedino rešenje date jednačine. ♦

Napomenimo da smo u ovom zadatku iskoristili važno svojstvo distributivnosti $\land$ prema $\lor$ $(\star)$, kao i pravilo logičkog sabiranja sa $\perp$ na samom kraju ekvivalencijskog lanca.

Naredni zadaci ilustruju logičke aspekte rešavanja iracionalnih (ne)jednačina.

Zadatak 3. *Rešiti jednačinu* $\sqrt{x+2}-\sqrt{x-6}=2$.

Rešenje. Prvo moramo odrediti uslove pod kojima je data jednačina definisana tj. odrediti sve vrednosti x za koje data jednačina „ima smisla”. Stoga mora da važi $x+2\geq 0$ i $x-6\geq 0$, odakle lako zaključujemo da je jednačina definisana za $x\geq 6$. Dalje rešavanje jednačine sprovodimo kvadriranjem. To bismo mogli opet predstaviti odgovarajućim ekvivalencijskim lancem:

$$
\begin{aligned}
\sqrt{x+2}-\sqrt{x-6}=2 \land x\geq 6 \quad &\Leftrightarrow \quad \sqrt{x+2}=2+\sqrt{x-6} \land x\geq 6\\
&\Leftrightarrow \quad x+2=4+4\sqrt{x-6}+x-6 \land x\geq 6\\
&\Leftrightarrow \quad 4\sqrt{x-6}=4 \land x\geq 6\\
&\Leftrightarrow \quad \sqrt{x-6}=1 \land x\geq 6\\
&\Leftrightarrow \quad x-6=1 \land x\geq 6\\
&\Leftrightarrow \quad x=7 \land x\geq 6\\
&\Leftrightarrow \quad x=7
\end{aligned}
$$

Stoga zaključujemo da je broj 7 jedino rešenje date jednačine. ♦

Zadatak 4. *Rešiti nejednačinu* $\sqrt{x-2}>x-4$.

Rešenje. Ovu nejednačinu ćemo rešiti korišćenjem sledeće ekvivalencije

$$\sqrt{A(x)} > B(x) \Leftrightarrow (A(x) \geq 0 \wedge B(x) < 0) \vee (A(x) \geq 0 \wedge B(x) \geq 0 \wedge A(x) > B^2(x)) \qquad (2)$$

čije izvođenje će biti prikazano na kraju ovog zadatka. Primenom (2) dobija se

$$\begin{aligned}
\sqrt{x-2} > x-4 \quad &\Leftrightarrow \quad (x-2 \geq 0 \wedge x-4 < 0) \vee (x-2 \geq 0 \wedge x-4 \geq 0 \wedge x-2 > (x-4)^2)\\
&\Leftrightarrow \quad (x \geq 2 \wedge x < 4) \vee (x \geq 2 \wedge x \geq 4 \wedge x-2 > x^2-8x+16)\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee (x \geq 4 \wedge x^2-9x+18 < 0)\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee (x \geq 4 \wedge (x-3)(x-6) < 0)\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee (x \geq 4 \wedge ((x-3 > 0 \wedge x-6 < 0) \vee (x-3 < 0 \wedge x-6 > 0))\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee ((x \geq 4 \wedge x-3 > 0 \wedge x-6 < 0) \vee (x \geq 4 \wedge x-3 < 0 \wedge x-6 > 0))\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee ((x \geq 4 \wedge x > 3 \wedge x < 6) \vee (x \geq 4 \wedge x < 3 \wedge x > 6))\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee (4 \leq x < 6) \vee \perp
\end{aligned}$$

Primetimo da je treća „ili-grana” $x \geq 4 \wedge x < 3 \wedge x > 6$ nemoguća. Sada imamo

$$\begin{aligned}
\sqrt{x-2} > x-4 \quad &\Leftrightarrow \quad (2 \leq x < 4) \vee (4 \leq x < 6) \vee \perp\\
&\Leftrightarrow \quad (2 \leq x < 4) \vee (4 \leq x < 6)\\
&\Leftrightarrow \quad 2 \leq x < 6
\end{aligned}$$

Skup svih rešenja je interval $[2, 6)$.

Vratimo se ekvivalenciji (2). Osetljivo mesto u toj ekvivalenciji je kako se iz nejednakosti $\sqrt{A(x)} > B(x)$ može strogo zaključiti da mora da važi $A(x) \geq 0$. Iako to deluje jasno, evo logičkog objašnjenja, koje koristi kvantifikator $\exists$:

$$\sqrt{A(x)} > B(x) \Rightarrow (\exists M) M = \sqrt{A(x)}.$$

Ideja je bila u tome da $\sqrt{A(x)}$ nekako uključimo u izvesnu jednakost i da potom upotrebimo jedan smer iz ekvivalencije

$$y = \sqrt{x} \Leftrightarrow (y^2 = x \wedge x \geq 0 \wedge y \geq 0).$$

Prema tome, imamo

$$\begin{aligned}
\sqrt{A(x)} > B(x) \quad &\Rightarrow \quad (\exists M) M = \sqrt{A(x)}\\
&\Rightarrow \quad (\exists M)(M = \sqrt{A(x)} \wedge A(x) \geq 0)\\
&\Rightarrow \quad A(x) \geq 0.
\end{aligned}$$

Zahvaljujući dobijenoj posledici imamo izvođenje ekvivalencije (2):

$$\begin{aligned}
\sqrt{A(x)} > B(x) \quad &\Leftrightarrow \quad (\sqrt{A(x)} > B(x) \wedge A(x) \geq 0 \wedge (B(x) < 0 \vee B(x) \geq 0))\\
&\Leftrightarrow \quad (\sqrt{A(x)} > B(x) \wedge A(x) \geq 0 \wedge B(x) < 0) \vee\\
&\qquad\;\; (\sqrt{A(x)} > B(x) \wedge A(x) \geq 0 \wedge B(x) \geq 0)\\
&\Leftrightarrow \quad (A(x) \geq 0 \wedge B(x) < 0) \vee (A(x) > B^2(x) \wedge A(x) \geq 0 \wedge B(x) \geq 0).
\end{aligned}$$

Poslednji red u lancu važi jer nejednakosti $A(x) \geq 0$ i $B(x) < 0$ povlače $\sqrt{A(x)} > B(x)$ i jer važi $p > q \Leftrightarrow p^n > q^n$, ako su $p, q \geq 0$ i $n = 1, 2, 3, \ldots$, što je primenjeno u desnoj „ili-grani”.

♦

Pređimo sada na nekoliko zadataka sa jednačinama u kojima učestvuju parametri.

Zadatak 5. *U zavisnosti od realnog parametra a rešiti jednačinu* $\dfrac{x+a}{x+2}-\dfrac{x-a}{x^2-4}=\dfrac{x}{x-2}$.

Rešenje. Prikažimo postupak rešavanja jednačine pomoću ekvivalencijskog lanca

$$\begin{aligned}
\frac{x+a}{x+2}-\frac{x-a}{x^2-4}=\frac{x}{x-2} \quad &\Leftrightarrow \quad \frac{(x+a)(x-2)-x+a-x(x+2)}{x^2-4}=0\\
&\Leftrightarrow \quad \frac{x^2-2x+ax-2a-x+a-x^2-2x}{x^2-4}=0\\
&\Leftrightarrow \quad \frac{(a-5)x-a}{x^2-4}=0\\
&\Leftrightarrow \quad (a-5)x-a=0 \wedge x^2-4\neq 0\\
&\Leftrightarrow \quad (a-5)x=a \wedge x\neq 2 \wedge x\neq -2
\end{aligned}$$

U ovom delu zadatka dolazi do diskusije rešenja jednačine po realnom parametru a. Ako se osvrnemo na jednačinu $(a-5)x=a$, videćemo da je u pitanju linearna jednačina sa jednom nepoznatom. U zavisnosti od toga da li je $a-5\neq 0$ ili $a-5=0$ tj. $a\neq 5$ ili $a=5$ ova jednačina, redom, ima jedinstveno rešenje $x=\dfrac{a}{a-5}$ ili nema rešenja. Vratimo se ekvivalencijskom lancu.

$$\begin{aligned}
\frac{x+a}{x+2}-\frac{x-a}{x^2-4}=\frac{x}{x-2} \quad &\Leftrightarrow \quad (a-5)x=a \wedge (a\neq 5 \vee a=5) \wedge x\neq 2 \wedge x\neq -2\\
&\Leftrightarrow \quad ((a-5)x=a \wedge a\neq 5 \wedge x\neq 2 \wedge x\neq -2) \vee\\
&\qquad\quad ((a-5)x=a \wedge a=5 \wedge x\neq 2 \wedge x\neq -2)\\
&\Leftrightarrow \quad (x=\frac{a}{a-5} \wedge a\neq 5 \wedge x\neq 2 \wedge x\neq -2) \vee (0\cdot x=5 \wedge x\neq 2 \wedge x\neq -2)\\
&\Leftrightarrow \quad (x=\frac{a}{a-5} \wedge a\neq 5 \wedge x\neq 2 \wedge x\neq -2) \vee (\perp \wedge x\neq 2 \wedge x\neq -2)\\
&\Leftrightarrow \quad (x=\frac{a}{a-5} \wedge a\neq 5 \wedge x\neq 2 \wedge x\neq -2) \vee \perp\\
&\Leftrightarrow \quad x=\frac{a}{a-5} \wedge a\neq 5 \wedge x\neq 2 \wedge x\neq -2\\
&\Leftrightarrow \quad x=\frac{a}{a-5} \wedge a\neq 5 \wedge \frac{a}{a-5}\neq 2 \wedge \frac{a}{a-5}\neq -2\\
&\Leftrightarrow \quad x=\frac{a}{a-5} \wedge a\neq 5 \wedge a\neq 10 \wedge a\neq \frac{10}{3}
\end{aligned}$$

Sada možemo dati potpuno rešenje polazne jednačine:

1. Ako je $a\neq 5 \wedge a\neq 10 \wedge a\neq \dfrac{10}{3}$, onda jednačina ima jedinstveno rešenje $x=\dfrac{a}{a-5}$.

2. Ako je $a=5 \vee a=10 \vee a=\dfrac{10}{3}$, onda jednačina nema rešenja.

♦

Zadatak 6. *Rešiti jednačinu* $\dfrac{a}{x-b}+\dfrac{a}{x+b}=\dfrac{2b}{x^2-b^2}$, *gde su* a,b *realni parametri.*

Rešenje. Za razliku od prethodnog zadatka ova jednačina ima 2 parametra, pa će diskusija biti malo složenija.

$$\begin{aligned}
\frac{a}{x-b}+\frac{a}{x+b}=\frac{2b}{x^2-b^2} \quad &\Leftrightarrow \quad \frac{a(x+b)+a(x-b)-2b}{x^2-b^2}=0\\
&\Leftrightarrow \quad \frac{ax+ab+ax-ab-2b}{x^2-b^2}=0\\
&\Leftrightarrow \quad \frac{2ax-2b}{x^2-b^2}=0\\
&\Leftrightarrow \quad \frac{ax-b}{x^2-b^2}=0\\
&\Leftrightarrow \quad ax-b=0 \wedge x^2-b^2\neq 0\\
&\Leftrightarrow \quad ax=b \wedge x\neq b \wedge x\neq -b
\end{aligned}$$

Jednačina $ax=b$ ima jedinstveno rešenje $x=\dfrac{b}{a}$ za $a\neq 0$. Ako je $a=0$, onda se dodatno razmatraju dva slučaja za parametar b. Ako je $a=0$ i $b=0$, svaki realan broj je rešenje jednačine. Ako je $a=0$ i $b\neq 0$, jednačina nema rešenja.
U slučajevima kada jednačina $ax=b$ ima rešenja ispitajmo da li su tada zadovoljeni uslovi $x\neq b$ i $x\neq -b$.
Ako je $a\neq 0$, onda mora da važi $\dfrac{b}{a}\neq b$ i $\dfrac{b}{a}\neq -b$. U tom slučaju dobija se $b\neq ab$ i $b\neq -ab$ tj. $ab-b\neq 0$ i $ab+b\neq 0$. Pomenuta dva uslova su ekvivalentna sa $b(a-1)\neq 0$ i $b(a+1)\neq 0$, odnosno sa konjukcijom $a\neq 1\wedge a\neq -1\wedge b\neq 0$. Dakle, ako je $a\neq 0$ i $a\neq 1$ i $a\neq -1$ i $b\neq 0$, onda jednačina ima jedinstveno rešenje $\dfrac{b}{a}$.
Za $a=1$ data jednačina se svodi na $\dfrac{2x}{x^2-b^2}=\dfrac{2b}{x^2-b^2}$, odakle zaključujemo da jednačina nema rešenja ni za jedno realno b. Slično, za $a=-1$ dobija se $\dfrac{-2x}{x^2-b^2}=\dfrac{2b}{x^2-b^2}$, odakle takođe zaključujemo da ni za jedno realno b jednačina nema rešenja.
Na kraju ako je $b=0$, onda se dobija $\dfrac{2a}{x}=\dfrac{0}{x^2}$, pa vidimo da za $a=0$ svaki realan broj različit od 0 je rešenje, a za $a\neq 0$ jednačina nema rešenja. ♦

Zadatak 7. *Rešiti jednačinu* $\dfrac{1}{x}+\dfrac{p^2}{x-1}=1$, $p\in\mathbb{R}$.

Rešenje. Formirajmo opet odgovarajući lanac ekvivalencija

$$\begin{aligned}
\frac{1}{x}+\frac{p^2}{x-1}=1 \quad &\Leftrightarrow \quad \frac{x-1+p^2x-x^2+x}{x(x-1)}=0\\
&\Leftrightarrow \quad \frac{-(x^2-(p^2+2)x+1)}{x(x-1)}=0\\
&\Leftrightarrow \quad x^2-(p^2+2)x+1=0\wedge x\neq 0\wedge x\neq 1
\end{aligned}$$

Zadržimo se na rešavanju kvadratne jednačine $x^2-(p^2+2)x+1=0$. Njena diskriminanta je

$$D=(p^2+2)^2-4=(p^2+2+2)(p^2+2-2)=p^2(p^2+4)$$

pa vidimo da je $D \geq 0$, odakle zaključujemo da jednačina za svaku vrednost parametra p ima realna rešenja. Odredimo ih:

$$x_{1,2} = \frac{p^2+2 \pm \sqrt{(p^2+2)^2-4}}{2} = \frac{p^2+2 \pm \sqrt{p^2(p^2+4)}}{2} = \frac{p^2+2 \pm p\sqrt{p^2+4}}{2}$$

tačnije

$$x_1 = \frac{p^2+2+p\sqrt{p^2+4}}{2} \quad , \quad x_2 = \frac{p^2+2-p\sqrt{p^2+4}}{2}$$

Primetimo da će rešenja za $p \neq 0$ biti realna i različita, a za $p = 0$ dobijamo $x = 1$, što zbog uslova $x \neq 1$ ne može biti rešenje polazne jednačine.
Ostalo je da proverimo da li su za dobijene x_1 i x_2 zadovoljeni uslovi. Najpre posmatrajmo x_1. Za njega važi

$$x_1 = \frac{p^2+2+p\sqrt{p^2+4}}{2} > \frac{p^2+2+p\sqrt{4}}{2} = \frac{p^2+2+2p}{2} = \frac{(p+1)^2+1}{2} > 0$$

gde je prva nejednakost posledica nejednakosti $p^2+4 > 4$. Odavde dobijamo da je $x_1 \neq 0$.
Dalje, posmatrajmo x_2. Kako važi da iz $p^2+4 > p^2$ sledi $\sqrt{p^2+4} > \sqrt{p^2} = |p| \geq -p$, tada je ispunjeno i

$$x_2 = \frac{p^2+2-p\sqrt{p^2+4}}{2} > \frac{p^2+2+p^2}{2} = \frac{2p^2+2}{2} = p^2+1 > 1$$

na osnovu čega se može zaključiti da je $x_2 \neq 1$. Na analogan način se pokazuje da važi i $x_1 \neq 1$, odnosno $x_2 \neq 0$. ♦

Kao poslednji od zadataka u kojima učestvuju realni parametri navodimo i rešavamo jedan sistem od dve linearne jednačine sa dve nepoznate i parametrima. Tom prilikom na logičkom aspektu predstavićemo Kramerovu teoremu.

Neka je dat sistem

$$\begin{cases} a_1x & + & b_1y & = & c_1 \\ a_2x & + & b_2y & = & c_2 \end{cases}$$

i neka je

$$D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1 \quad \text{determinanta sistema}$$

$$D_x = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix} = c_1b_2 - c_2b_1 \quad \text{determinanta nepoznate } x$$

$$D_y = \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} = a_1c_2 - a_2c_1 \quad \text{determinanta nepoznate } y$$

Prema tome, kod datog sistema imamo sledeće mogućnosti:

1. $D \neq 0$ - sistem je tada određen tj. ima tačno jedno rešenje $(x, y) = \left(\dfrac{D_x}{D}, \dfrac{D_y}{D}\right)$

2. $D = 0 \land (D_x \neq 0 \lor D_y \neq 0)$ - sistem je tada protivrečan tj. nema rešenja

3. $D = 0 \wedge (D_x = 0 \wedge D_y = 0) \wedge (a_1 \neq 0 \vee a_2 \neq 0 \vee b_1 \neq 0 \vee b_2 \neq 0)$ - sistem je tada neodređen, sa jednom slobodnom nepoznatom

4. $(a_1 = 0 \wedge a_2 = 0 \wedge b_1 = 0 \wedge b_2 = 0) \wedge (c_1 \neq 0 \vee c_2 \neq 0)$, što povlači $D = 0 \wedge (D_x = 0 \wedge D_y = 0)$; tada je sistem protivrečan

5. $(a_1 = 0 \wedge a_2 = 0 \wedge b_1 = 0 \wedge b_2 = 0) \wedge (c_1 = 0 \wedge c_2 = 0)$; tada je sistem potpuno neodređen, što znači da je svaki uređen par realnih brojeva (x_0, y_0) rešenje sistema

Zadatak 8. *Diskutovati rešenja sistema jednačina*

$$\begin{cases} ax & + & y & = & 1 \\ x & + & ay & = & b \end{cases}$$

za razne vrednosti realnih parametara a i b.

Rešenje. Izdvojimo koeficijente sistema, kao i odgovarajuće determinante

$$a_1 = a, \quad b_1 = 1, \quad c_1 = 1, \quad a_2 = 1, \quad b_2 = a, \quad c_2 = b$$

$$D = \begin{vmatrix} a & 1 \\ 1 & a \end{vmatrix} = a^2 - 1 = (a-1)(a+1)$$

$$D_x = \begin{vmatrix} 1 & 1 \\ b & a \end{vmatrix} = a - b$$

$$D_y = \begin{vmatrix} a & 1 \\ 1 & b \end{vmatrix} = ab - 1$$

Prema prethodno prikazanoj diskusiji imamo:

1. za $D \neq 0$ tj. $a \neq 1 \wedge a \neq -1$, sistem ima jedinstveno rešenje $(x, y) = \left(\dfrac{a-b}{a^2-1}, \dfrac{ab-1}{a^2-1} \right)$

2. ako je $(a^2 - 1 = 0 \wedge (a - b \neq 0 \vee ab - 1 \neq 0)) \vee ((a = 0 \wedge 1 = 0 \wedge 1 = 0 \wedge a = 0) \wedge$ $(1 \neq 0 \vee b \neq 0))$, tačnije, kada iskoristimo da je iskaz $1 = 0$ netačan i svojstva konjukcije i disjunkcije, $a^2 - 1 = 0 \wedge (a - b \neq 0 \vee ab - 1 \neq 0)$ sistem nema rešenja.

Zadržimo se na iskaznoj formuli $a^2 - 1 = 0 \wedge (a - b \neq 0 \vee ab - 1 \neq 0)$. Naime, važi sledeći lanac ekvivalencija

$$\begin{array}{rcl} (a^2 - 1 = 0 \wedge (a - b \neq 0 \vee ab - 1 \neq 0)) & \Leftrightarrow & ((a = -1 \vee a = 1) \wedge (a \neq b \vee ab \neq 1)) \\ & \Leftrightarrow & ((a = -1 \wedge a \neq b) \vee (a = -1 \wedge ab \neq 1) \vee \\ & & (a = 1 \wedge a \neq b) \vee (a = 1 \wedge ab \neq 1)) \\ & \Leftrightarrow & ((a = -1 \wedge b \neq -1) \vee (a = -1 \wedge b \neq -1) \vee \\ & & (a = 1 \wedge b \neq 1) \vee (a = 1 \wedge b \neq 1)) \\ & \Leftrightarrow & (a = -1 \wedge b \neq -1) \vee (a = 1 \wedge b \neq 1) \end{array}$$

Dakle, ako je $(a = -1 \wedge b \neq -1) \vee (a = 1 \wedge b \neq 1)$ sistem nema rešenja.

3. ako je $a^2 - 1 = 0 \wedge (a - b = 0 \wedge ab - 1 = 0) \wedge (a \neq 0 \vee 1 \neq 0 \vee 1 \neq 0 \vee a \neq 0)$, onda je sistem neodređen, sa jednom slobodnom nepoznatom

Slično prethodnom slučaju, dobija se ekvivalencijski lanac

$$\begin{gathered} a^2-1=0 \wedge (a-b=0 \wedge ab-1=0) \wedge (a \neq 0 \vee 1 \neq 0 \vee 1 \neq 0 \vee a \neq 0) \\ \Leftrightarrow \\ a^2-1=0 \wedge (a-b=0 \wedge ab-1=0) \wedge a \neq 0 \\ \Leftrightarrow \\ (a=-1 \vee a=1) \wedge (a=b \wedge ab=1) \wedge a \neq 0 \\ \Leftrightarrow \\ (a=-1 \wedge a=b \wedge ab=1 \wedge a \neq 0) \vee (a=1 \wedge a=b \wedge ab=1 \wedge a \neq 0) \\ \Leftrightarrow \\ (a=-1 \wedge b=-1) \vee (a=1 \wedge b=1) \end{gathered}$$

Dakle, ako je $(a=-1 \wedge b=-1) \vee (a=1 \wedge b=1)$ sistem je neodređen, sa jednom slobodnom nepoznatom.

4. ako je $(a=0 \wedge 1=0 \wedge 1=0 \wedge a=0) \wedge (1=0 \wedge b=0)$ sistem bi trebalo da je potpuno neodređen; međutim, ovde to *nije ispunjeno*, jer je pomenuta formula (zbog netačnosti iskaza $1=0$ i istinitosti konjukcije) ekvivalentna sa $\perp$, pa pod datim pretpostavkama ovog slučaja sistem takođe nema rešenja

♦

Koristi od primene matematičke logike pri rešavanju problema imaju i druge oblasti matematike, kao na primer geometrija. Naredni zadatak predstavlja primer jednog geometrijskog problema koji se može rešiti primenom matematičke logike.

Zadatak 9. *Pokazati da je relacija paralelnosti pravih u ravni jedna tranzitivna relacija.*

Rešenje. Neka su date prave p, q i r, takve da je prava p paralelna pravoj q i prava q paralelna pravoj r. Ako koristimo standardnu oznaku za paralelnost dve prave u ravni, ovaj zadatak se svodi na dokazivanje sledeće implikacije

$$p \parallel q \wedge q \parallel r \Rightarrow p \parallel r.$$

Definicija paralelnosti pravih u ravni data je ekvivalencijom

$$p \parallel q \Leftrightarrow (p \equiv q \vee p \cap q = \emptyset).$$

Primenom date definicije dobija se

$$\begin{aligned} p \parallel q \wedge q \parallel r \quad &\Leftrightarrow \quad (p \equiv q \vee p \cap q = \emptyset) \wedge (q \equiv r \vee q \cap r = \emptyset) \\ &\Leftrightarrow \quad (p \equiv q \wedge q \equiv r) \vee (p \equiv q \wedge q \cap r = \emptyset) \vee (p \cap q = \emptyset \wedge q \equiv r) \vee (p \cap q = \emptyset \wedge q \cap r = \emptyset) \end{aligned}$$

Dodajmo da važi:

$$\begin{gathered} (p \equiv q \wedge q \equiv r) \Rightarrow p \equiv r \\ (p \equiv q \wedge q \cap r = \emptyset) \Rightarrow p \cap r = \emptyset \\ (p \cap q = \emptyset \wedge q \equiv r) \Rightarrow p \cap r = \emptyset \end{gathered}$$

pa odatle imamo

$$p \parallel q \wedge q \parallel r \quad \Rightarrow \quad p \equiv r \vee p \cap r = \emptyset \vee (p \cap q = \emptyset \wedge q \cap r = \emptyset)$$

Dalje imamo

$$\begin{aligned} p \cap q = \emptyset \wedge q \cap r = \emptyset \quad & \Leftrightarrow \quad (p \cap q = \emptyset \wedge q \cap r = \emptyset) \wedge \top \\ & \Leftrightarrow \quad (p \cap q = \emptyset \wedge q \cap r = \emptyset) \wedge (p \equiv r \vee p \cap r = \emptyset \vee p \cap r = \{S\}) \\ & \Leftrightarrow \quad (p \cap q = \emptyset \wedge q \cap r = \emptyset \wedge p \equiv r) \vee (p \cap q = \emptyset \wedge q \cap r = \emptyset \wedge p \cap r = \emptyset) \vee \\ & \qquad\; (p \cap q = \emptyset \wedge q \cap r = \emptyset \wedge p \cap r = \{S\}) \end{aligned}$$

Na osnovu V Euklidovog postulata dobijamo da je iskaz $p \cap q = \emptyset \wedge q \cap r = \emptyset \wedge p \cap r = \{S\}$ netačan, jer su prave p i r paralelne pravoj q i prolaze kroz tačku S van prave q.
Stoga

$$p \cap q = \emptyset \wedge q \cap r = \emptyset \quad \Rightarrow \quad p \equiv r \vee p \cap r = \emptyset \vee \bot$$

Konačno

$$\begin{aligned} p \parallel q \wedge q \parallel r \quad & \Rightarrow \quad p \equiv r \vee p \cap r = \emptyset \vee p \equiv r \vee p \cap r = \emptyset \vee \bot \\ & \Leftrightarrow \quad p \equiv r \vee p \cap r = \emptyset \\ & \Leftrightarrow \quad p \parallel r \end{aligned}$$

Time je dokazana tranzitivnost relacije paralelnosti pravih u ravni. ♦

3 Metoda eliminacije kvantifikatora

3.1 Odlučivost

Jedan od centralnih pojmova logike prvog reda je pojam *odlučivosti*. Metod eliminacije kvantifikatora je jedan od metoda koji imaju ulogu u ispitivanju odlučivosti neke teorije. Logika prvog reda nije odlučiva i ne postoji opšti postupak za određivanje da li je neka formula valjana ili nije. Iako logika prvog reda nije odlučiva, postoje neke teorije prvog reda koje su odlučive. Neke od odlučivih teorija su[6]: Prezburgerova aritmetika, teorija Bulovih algebri, teorija algebarski zatvorenih polja date karakteristike, teorija realno zatvorenih uređenih polja, teorija euklidske geometrije, teorija hiperboličke geometrije. Primeri neodlučivih teorija su: teorija semigrupa, teorija grupa, teorija polja, Peanova aritmetika.

Pre nego što se razvila teorija odlučivosti opšte uverenje je bilo da su svi matematički problemi odlučivi, s tim što nije uvek lako konstruisati postupak odlučivanja. Danas se zna da su mnogi matematički problemi neodlučivi i za većinu netrivijalnih matematičkih teorija se zna ili očekuje da su neodlučive. Jedna od najvažnijih ideja u navedenim razmatranjima jeste ideja kodiranja. Gedel[7] je prvi koristio kodiranje za analizu logičkih pojmova kao što su izraz, formula, dokaz, teorema.

U nastavku podrazumevaćemo da je jezik $\mathcal{L}$ najviše prebrojiv. Samim tim, skupovi izraza, formula i konačnih nizova formula su efektivno dati tj. postoji postupak kojim se u konačno mnogo koraka utvrđuje da li je nešto izraz, formula ili konačan niz formula jezika $\mathcal{L}$, sve pomenute objekte možemo kodirati. Dakle, kodiranje nam omogućava da svakom izrazu, svakoj formuli i svakom nizu formula pridružimo po jedan prirodan broj. Međutim, pitanje koje se u ovakvoj situaciji postavlja je: *Postoji li postupak (algoritam) kojim možemo u konačno mnogo koraka da utvrdimo da li je neki prirodan broj kôd nekog od objekata koje smo kodirali i ako jeste, možemo li eksplicitno i da odredimo taj objekat (izraz, formulu, niz formula)*? Odgovor je potvrdan.

Pomenuti algoritam se sastoji od dve osnovne procedure: jedna utvrđuje da li je neki niz logičkih simbola i simbola jezika $\mathcal{L}$ izraz tog jezika, a druga utvrđuje da li je neki niz logičkih simbola i simbola jezika $\mathcal{L}$ formula tog jezika.

Sada možemo zaključiti da su funkcije $f_{izraz} : \mathbb{N} \longrightarrow \mathbb{N}$ i $f_{formula} : \mathbb{N} \longrightarrow \mathbb{N}$ definisane sa

$$f_{izraz}(n) = \begin{cases} 1, & \text{ako je } n \text{ kôd nekog izraza jezika } \mathcal{L} \\ 0, & \text{inače} \end{cases}$$

i

$$f_{formula}(n) = \begin{cases} 1, & \text{ako je } n \text{ kôd neke formule jezika } \mathcal{L} \\ 0, & \text{inače} \end{cases}$$

rekurzivne.

[6] Spisak teorija je preuzet iz [9].
[7] Kurt Gödel (1906 - 1978) - austrijski matematičar

Na sličan način se može uočiti da postoji algoritam koji utvrđuje da li je neki konačan niz formula $\varphi_1, \dots \varphi_n$ dokaz neke date formule φ. Neophodno je proveriti da li je formula nekog od oblika koje nam daje konačan broj shema aksioma, ili je neposredna posledica nekih od konačno mnogo formula primenom nekog od pravila izvođenja (kojih takođe ima konačno mnogo).

Na isti način se mogu proučavati i drugih skupova formula, pre svega onih koji su *efektivno zadati* tj. *rekurzivni*. Skup formula T je rekurzivan ukoliko postoji algoritam koji daje odgovor „**da**" ili „**ne**" na pitanje: *Da li formula* φ *pripada* T? Drugim rečima, skup formula je rekurzivan ako znamo koje formule mu pripadaju, a koje ne.

Pored rekurzivnosti, sa praktičnog stanovišta je veoma značajna i odlučivost nekog skupa formula. Skup formula T je odlučiv ako postoji algoritam koji daje odgovor „**da**" ili „**ne**" na pitanje: *Da li je formula* φ *posledica skupa* T? Drugim rečima, skup formula je odlučiv ako znamo koje su formule dokazive, a koje nisu. Formula φ je odlučiva u T ako je $T \vdash \varphi$ ili $T \vdash \neg\varphi$. Time smo pomoću pojma rekurzivnih funkcija na formalan način uveli pojam odlučivosti.

3.2 Opis metoda eliminacije kvantifikatora

Pod pojmom eliminacije kvantifikatora neke formule φ jezika $\mathcal{L}$ podrazumeva se određivanje formule ψ, koja je ekvivalentna formuli φ i u sebi ne sadrži kvantifikatore. Formula ψ se još naziva i *eliminanta* za formulu φ. Metod eliminacije kvantifikatora je najstariji i u kontekstu automatskog dokazivanja teorema najznačajniji metod. Naziv metoda potiče od Tarskog[8], koji je dao nekoliko njegovih najznačajnijih primena dokazavši odlučivost nekoliko teorija kao što su: teorija algebarski zatvorenih polja, teorija realno zatvorenih polja, teorija dobrog uređenja, teorija Bulovih algebri. Suštinski isti metod bio je primenjivan i pre toga za predikatski račun sa jednakošću, gusto linearno uređenje bez krajnjih tačaka, Prezburgerovu aritmetiku, a kasnije i za dokaz odlučivosti teorije Abelovih grupa.

Metod eliminacije kvantifikatora zasniva se na tome da se data formula φ transformiše u formulu ψ tako da važi $\models \varphi \Leftrightarrow \psi$, pri čemu je formula ψ „jednostavnija" od formule φ (obično se misli na to da formula ψ ima manje promenljivih od formule φ).

Metod eliminacije kvantifikatora za dokazivanje odlučivosti neke teorije je značajan i po tome što ima i neke „nuspojave":

- kada je teorija data aksiomatski, ovaj metod može da indukuje i dokaz kompletnosti teorije,
- metod indukuje proceduru odlučivanja koja je efektivno opisiva i moguće ju je automatizovati.

Neformalno govoreći, smisao metoda eliminacije kvanifikatora je u tome da se odredi skup „jednostavnih" formula jezika takav da je svaka formula tog jezika ekvivalentna nekoj jednostavnoj formuli. Termin „jednostavna" formula je vrlo ironičan s obzirom na to da su formule dobijene primenom ovog metoda vrlo složene. Stoga se ovaj termin često odnosi na formule bez kvantifikatora.

[8]Alfred Tarski (1901 - 1983) - poljski matematičar, logičar i filozof

Neka je $\mathcal{K}$ efektivno izabran skup formula jezika $\mathcal{L}$. Kažemo da teorija T *dopušta eliminaciju kvantifikatora* do na klasu $\mathcal{K}$ akko za svaku formulu φ jezika $\mathcal{L}$ postoji formula ψ iz skupa $\mathcal{K}$ takva da važi $T \models \varphi \Leftrightarrow \psi$. Ukoliko je za sve formule klase $\mathcal{K}$ moguće efektivno odrediti da li su posledice teorije T, onda je teorija koja dopušta eliminaciju kvantifikatora *odlučiva*. U većini primena klasa $\mathcal{K}$ je skup formula bez kvantifikatora.

Generalno, metod dokazivanja odlučivosti teorije T jezika $\mathcal{L}$ je sastavljen iz sledeća tri koraka:

1. bira se pogodan skup osnovnih formula jezika $\mathcal{L}$ i on se proglašava za klasu $\mathcal{K}$;

2. pokaže se da za svaku formulu φ jezika $\mathcal{L}$ postoji formula ψ iz klase $\mathcal{K}$ takva da je $T \models \varphi \Leftrightarrow \psi$;

3. pokaže se da je za svaku formulu ψ iz $\mathcal{K}$ moguće efektivno ispitati da li važi $T \models \psi$.

3.3 Primer kriterijuma za teorije koje dopuštaju eliminaciju kvantifikatora

U ovom odeljku navodimo jedan od kriterijuma kojim se dokazuje da teorija dopušta eliminaciju kvantifikatora. O drugim kriterijumima, koji su većinom povezani sa pojmom kompletnosti teorija može se pročitati u [7].

Da ponovimo: za teoriju T kažemo da dopušta eliminaciju kvantifikatora ako za svaku formulu $\varphi(x_1, \ldots, x_n)$, $n \geq 1$, postoji formula $\psi(x_1, \ldots, x_n)$ bez kvantifikatora, tzv. otvorena formula, takva da

$$T \models \forall x_1 \ldots \forall x_n(\varphi(x_1, \ldots, x_n) \Leftrightarrow \psi(x_1, \ldots, x_n)).$$

Pri dokazivanju predstojećeg kriterijuma biće nam potrebna i jedna lema. Navedimo je.

Lema 3. *Svaka egzistencijalna formula je logički ekvivalentna disjunkciji primitivnih egzistencijalnih formula.*

Dokaz ove leme se može pronaći u [7].

Naredna teorema daje jedan od kriterijuma za teorije koje dopuštaju eliminaciju kvantifikatora.

Teorema 1. *Teorija T dopušta eliminaciju kvantifikatora akko je svaka primitivna egzistencijalna formula sa samo jednim egzistencijalnim kvantifikatorom ekvivalentna u teoriji T nekoj formuli bez kvantifikatora.*

Dokaz. Pretpostavimo da teorija T dopušta eliminaciju kvantifikatora. To po definiciji znači da za svaku formulu $\varphi(x_1, \ldots, x_n)$ postoji neka formula $\psi(x_1, \ldots, x_n)$ bez kvantifikatora takva da važi $T \models \forall x_1 \ldots \forall x_n(\varphi(x_1, \ldots, x_n) \Leftrightarrow \psi(x_1, \ldots, x_n))$. Posebno, prethodno tvrđenje važi za svaku primitivnu egzistencijalnu formulu koja ima samo jedan egzistencijalni kvantifikator.
Dokažimo obrnuto. Pretpostavimo da je svaka primitivna egzistencijalna formula sa samo jednim egzistencijalnim kvantifikatorom ekvivalentna u teoriji T nekoj formuli bez kvantifikatora. Na osnovu teoreme 4. imamo da za svaku formulu teorije T postoji formula u preneks normalnoj formi koja joj je ekvivalentna. Odavde sledi da je dovoljno dokazati da je svaka formula teorije T, koja

je u preneks normalnoj formi, ekvivalentna nekoj formuli bez kvantifikatora. To dokazujemo indukcijom po broju kvantifikatora formule u preneks normalnoj formi. Neka je φ formula u preneks normalnoj formi koja sadrži tačno jedan kvantifikator.

1.slučaj: formula φ je oblika $\exists x\psi$, gde je ψ otvorena formula
Tada iz prethodne leme sledi da postoje neke primitivne egzistencijalne formule $\psi_1, \dots, \psi_m$ takve da $T \models \exists x\psi \Leftrightarrow (\psi_1 \vee \dots \vee \psi_m)$. Po pretpostavci važi da za svaku formulu ψ_i postoji otvorena formula φ_i takva da je $T \models \psi_i \Leftrightarrow \varphi_i$, za svaki $i = \overline{1, m}$. Odavde pak sledi $T \models (\psi_1 \vee \dots \vee \psi_m) \Leftrightarrow (\varphi_1 \vee \dots \vee \varphi_m)$, odnosno $T \models \varphi \Leftrightarrow (\varphi_1 \vee \dots \vee \varphi_m)$. Formula $\varphi_1 \vee \dots \vee \varphi_m$ je otvorena, pa je ovaj slučaj dokazan.
2.slučaj: formula φ je oblika $\forall x\psi$, gde je ψ otvorena formula
Prema De Morganovim zakonima važi $\models \forall x\psi \Leftrightarrow \neg\exists x\neg\psi$. Prema 1. slučaju postoji otvorena formula φ takva da važi $T \models \exists x\neg\psi \Leftrightarrow \varphi$. Odatle i $T \models \neg\exists x\neg\psi \Leftrightarrow \neg\varphi$, odnosno $T \models \forall x\psi \Leftrightarrow \neg\varphi$. Formula $\neg\varphi$ je otvorena, pa je time i ovaj slučaj dokazan.

Pretpostavimo da teorema važi za svaku formulu ψ u preneks normalnoj formi koja ima n kvantifikatora. Neka je φ formula u preneks normalnoj formi čiji prefiks sadrži tačno $n+1$ kvantifikator. Posmatrajmo opet dva slučaja (u odnosu na prvi levi kvantifikator).

1.slučaj: neka je formula φ oblika $\exists x\varphi'$, gde je φ' formula u preneks obliku čiji prefiks sadrži tačno n kvantifikatora. Prema induktivnoj pretpostavci postoji otvorena formula ψ' takva da je $T \models \varphi' \Leftrightarrow \psi'$. Tada važi i $T \models \exists x\varphi' \Leftrightarrow \exists x\psi'$. Na isti način kao i u bazi indukcije pokaže se da postoji otvorena formula ψ takva da je $T \models \psi \Leftrightarrow \exists x\psi'$, odnosno $T \models \varphi \Leftrightarrow \psi$.
2. slučaj: neka je formula φ oblika $\forall x\varphi'$, gde je φ' formula u preneks obliku čiji prefiks sadrži tačno n kvantifikatora. Prema induktivnoj pretpostavci postoji otvorena formula ψ' takva da je $T \models \varphi' \Leftrightarrow \psi'$. Tada važi i $T \models \forall x\varphi' \Leftrightarrow \forall x\psi'$. Slično kao u bazi indukcije pokaže se da postoji neka otvorena formula ψ takva da važi $T \models \psi \Leftrightarrow \forall x\psi'$. $\square$

Primeri nekih teorija koje dopuštaju eliminaciju kvantifikatora[9] su:

- teorija algebarski zatvorenih polja;
- teorija gustih uređenih Abelovih grupa bez krajnjih tačaka;
- teorija gustih linearnih uređenja bez krajnjih tačaka;
- teorija realno zatvorenih uređenih polja;
- teorija Bulovih algebri;
- Prezburgerova aritmetika.

U ovom radu zadržaćemo se na primerima teorija gustih uređenih Abelovih grupa bez krajnjih tačaka, algebarski zatvorenih polja i realno zatvorenih polja.

[9] Spisak teorija je preuzet sa [10].

4 Eliminacija kvantifikatora za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka

U vezi sa eliminacijom kvantifikatora u ovom poglavlju razmotrićemo teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka. Ova teorija je primer jedne od onih koje dopuštaju eliminaciju kvantifikatora. Za početak navedimo definiciju teorije gustih uređenih Abelovih grupa bez krajnjih tačaka.

Jezik ove teorije, koju ćemo dalje označavati sa T_{Ab}, čini skup $\mathcal{L}_{Ab} = \{+, -, 0, <, =\}$, koji je sastavljen od binarnog operacijskog simbola $+$, unarnog operacijskog simbola $-$, simbola konstante 0 i binarnih relacijskih simbola $<$ i $=$. Aksiome teorije T_{Ab}, pored aksioma jednakosti, su:

- $\forall x \forall y \forall z((x + y) + z = x + (y + z))$
- $\forall x(x + 0 = x \wedge 0 + x = x)$
- $\forall x(x + (-x) = 0 \wedge -x + x = 0)$
- $\forall x \forall y(x + y = y + x)$
- $\forall x \forall y(x < y \vee y < x \vee y = x)$
- $\forall x(\neg(x < x))$
- $\forall x \forall y \forall z(x < y \wedge y < z \Rightarrow x < z)$
- $\forall x \forall y(x < y \Rightarrow (\exists z)(x < z \wedge z < y))$
- $\forall x \forall y \forall z(x < y \Rightarrow x + z < y + z)$
- $\forall x \exists y(y < x)$
- $\forall x \exists y(x < y)$

Preostale binarne relacijske simbole $>$, $\leq$, $\geq$ možemo uvesti, ukoliko za njima bude potrebe, na sledeći način:

$$x > y \Leftrightarrow y < x, \quad x \leq y \Leftrightarrow (x < y \vee x = y), \quad x \geq y \Leftrightarrow y \leq x$$

Kako je u teoriji T_{Ab} funkcijski simbol $+$ asocijativan, u izrazu $x + x + \ldots + x$ zagrade nisu bitne, pa ih možemo obrisati. Takođe, izraz $\underbrace{x + x + \ldots + x}_{n}$ kraće ćemo zapisivati nx, a vrednost n zvati koeficijent uz x.

Formulišimo i dokažimo teoremu koja tvrdi da pomenuta teorija T_{Ab} dopušta eliminaciju kvantifikatora.

Teorema 2. *Teorija gustih uređenih Abelovih grupa bez krajnjih tačaka dopušta eliminaciju kvantifikatora.*

Dokaz. Razmotrimo formulu oblika $\exists x(\alpha_0, \ldots, \alpha_k)$, gde su α_i atomične formule. Primetimo da atomične formule u ovoj strukturi imaju dva oblika: $u = v$ i $u < v$. Prvo, možemo eliminisati negacije atomičnih formula. Formule oblika $\neg(u < v)$ zamenjujemo formulom $v = u \vee v < u$, a formule oblika $\neg(u = v)$ formulom $u < v \vee v < u$. Prevodeći izraz u disjunktivnu normalnu formu i koristeći svojstvo da se egzistencijalni kvantifikator ,,lepo slaže" sa konjukcijom tj. da je formula $\exists x(F(x) \wedge G(x)) \Leftrightarrow \exists x F(x) \wedge \exists x G(x)$ valjana, dobijamo disjunkciju formula oblika $\exists x(\beta_0, \ldots, \beta_l)$, gde su β_i atomične formule. Ako β_i ne sadrži x možemo je pomeriti izvan dejstva kvantifikatora pomenute formule. Ukoliko su neki od β_i oblika $x = x$, jednostavno ih zanemarimo. Ako je u pitanju izraz $x = v$ ili $v = x$ (gde je v različito od x) onda možemo zameniti x sa v u svakom delu formule koji je pod uticajem datog kvantifikatora, a potom eliminisati i β_i i kvantifikator. Ovo je opravdano sledećom logičkom ekvivalencijom

$$\exists x(x = v \wedge \varphi(x, v)) \Leftrightarrow \varphi(v, v).$$

Preostale formule moraju biti oblika $x < x$, $u < x$ i $x < v$, gde su u i v različiti od x. Ako se u formuli pojavi $x < x$ jednostavno ga možemo zameniti sa $\perp$, prema jednoj od aksioma teorije T_{Ab} koja glasi $\forall x(\neg(x < x))$. Inače, formulu možemo napisati u obliku

$$\exists x(\bigwedge_i (u_i < x) \wedge \bigwedge_j (x < v_j)).$$

Za ovu poslednju formulu važi sledeći niz ekvivalencija

$$\exists x(\bigwedge_i (u_i < x) \wedge \bigwedge_j (x < v_j))$$
$$\Leftrightarrow$$
$$\exists x \bigwedge_{i,j} (u_i < x \wedge x < v_j)$$
$$\Leftrightarrow$$
$$\exists x \bigwedge_{i,j} (u_i < x < v_j)$$
$$\Leftrightarrow$$
$$\bigwedge_{i,j} (u_i < v_j)$$

čime smo pokazali kako se eliminiše egzistencijalni kvantifikator. Ukoliko se u formuli pojavi univerzalni kvantifikator, tu formulu prevodimo u drugi oblik pomoću formule $\forall x A(x) \Leftrightarrow \neg\exists x \neg A(x)$, pa se sve opet svodi na prethodno opisani postupak. $\square$

Primer 2. *Struktura* $(\mathbb{Q}, +, -, 0, <, =)$*, sa skupom racionalnih brojeva, je jedan primer modela teorije gustih uređenih Abelovih grupa bez krajnjih tačaka. Struktura* $(\mathbb{R}, +, -, 0, <, =)$*, sa skupom realnih brojeva, bi bila drugi primer.*

$\triangle$

4.1 Furije-Mockinova procedura

U prethodnom delu smo dokazali da teorija gustih uređenih Abelovih grupa bez krajnjih tačaka dopušta eliminaciju kvantifikatora. Jedan od metoda kojima je moguće ilustrovati eliminaciju kvantifikatora u pomenutoj teoriji je *Furije-Mockinova procedura*. Ova procedura predstavlja proceduru odlučivanja za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka. Zasnovana je na Furijeovom metodu za rešavanje linearnih nejednakosti nad poljem racionalnih brojeva. Takođe, ovom procedurom možemo „proveriti” da li je neka formula teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka.

Furije - Mockinova procedura se može predstaviti kroz određeni niz koraka:

1. U prvom koraku se podrazumeva da se formula za koju treba ispitati da li je teorema prebaci u preneks normalnu formu, što se postiže na način koji je već opisan u prvom poglavlju.

2. Negacije eliminišemo pomoću sledećih veza

$$\neg(x = y) \Leftrightarrow (x < y) \vee (y < x)$$

$$\neg(x < y) \Leftrightarrow (x = y) \vee (y < x)$$

   Primetimo da novodobijena formula sadrži samo logičke veznike $\wedge$ i $\vee$.

3. Svaku od atomskih formula pojednostavljujemo tako da sadrži najviše jedno pojavljivanje izraza oblika ny. To se postiže pomoću sledećih veza:

$$(x_1 = (x_2 + ny) + x_3) \Leftrightarrow (x_1 = (x_2 + x_3) + ny)$$

$$(x_1 = (x_2 + ny) + my) \Leftrightarrow (x_1 = x_2 + (m + n)y)$$

$$(x_1 + ny = x_2 + my) \Leftrightarrow (x_1 = x_2) \text{ , pri čemu je } m = n$$

$$(x_1 + ny = x_2 + my) \Leftrightarrow (x_1 = x_2 + (m - n)y) \text{ , pri čemu je } m > n$$

$$(x_1 + ny = x_2 + my) \Leftrightarrow (x_1 + (n - m)y = x_2) \text{ , pri čemu je } n > m$$

$$(x_1 < (x_2 + ny) + x_3) \Leftrightarrow (x_1 < (x_2 + x_3) + ny)$$

$$(x_1 < (x_2 + ny) + my) \Leftrightarrow (x_1 < x_2 + (m + n)y)$$

$$(x_1 + ny < x_2 + my) \Leftrightarrow (x_1 < x_2) \text{ , pri čemu je } m = n$$

$$(x_1 + ny < x_2 + my) \Leftrightarrow (x_1 < x_2 + (m - n)y) \text{ , pri čemu je } m > n$$

$$(x_1 + ny < x_2 + my) \Leftrightarrow (x_1 + (n - m)yx_2) \text{ , pri čemu je } n > m$$

4. Koristimo

$$F \wedge (G \vee H) \Leftrightarrow (F \wedge G) \vee (F \wedge H)$$

$$(F \vee G) \wedge H \Leftrightarrow (F \wedge H) \vee (F \wedge G)$$

   za transformisanje tekuće formule, tačnije njenog dela bez kvantifikatora, u disjunktivnu normalnu formu

5. Egzistencijalni kvantifikator može da „prođe” kroz disjunkciju, preciznije rečeno važi

$$(\exists x)(F_1 \vee F_2 \vee \ldots \vee F_n) \Leftrightarrow (\exists x)F_1 \vee (\exists x)F_2 \vee \ldots \vee (\exists x)F_n$$

Ako u F_i nema atomskih formula koje zavise od x onda je $(\exists x)F_i \Leftrightarrow F_i$ i time je eliminisan egzistencijalni kvantifikator. U suprotnom, formula F_i može biti napisana u obliku $G_i \wedge H_i$, gde je G_i konjukcija svih atomskih formula iz F_i koje ne sadrže x. kako G_i ne sadrži x onda važi

$$(\exists x)(G_i \wedge H_i) \Leftrightarrow G_i \wedge (\exists x)H_i.$$

6. Potrebno je eliminisati kvantifikatore $\exists x$ iz svih formula $(\exists x)H_i$. Svaka od ovih formula je oblika

$$(\exists x)(t_1 = s_1 \wedge \ldots \wedge t_j = s_j \wedge q_1 < r_1 \wedge \ldots \wedge q_k < r_k)$$

pri čemu važi $j + k > 0$, za svako i, $1 \leq i \leq j$, y se pojavljuje u t_i ili s_i i za svako i, $1 \leq i \leq k$, y se pojavljuje u q_i ili u r_i.
Prvo razmotrimo slučaj da postoji bar jedna jednakost ($j > 0$). Ako je $j = 1$ i $k = 0$, onda $(\exists y)(t_1 = s_1)$ može da se zameni sa $\top$. Inače, obrišemo jednu jednakost ($t_m = s_m$) i iskoristimo je za eliminisanje promenljive y iz preostalih $j + k - 1$ atomskih formula. Pretpostavimo da se promenljiva y pojavljuje u izrazu t_m i to sa koeficijentom c_m. Ako je atomska formula oblika $q_p < r_p$ i y se u izrazu q_p pojavljuje sa koeficijentom c_p, onda je u nejednakosti

$$c_m q_p + c_p s_m < c_m r_p + c_p t_m$$

koeficijent uz y sa obe strane jednak $c_p c_m$, pa promenljiva y može biti eliminisana. Ako je atomska formula oblika $q_p < r_p$ i y se u izrazu r_p pojavljuje sa koeficijentom c_p, onda je u nejednakosti

$$c_m q_p + c_p t_m < c_m r_p + c_p s_m$$

koeficijent uz y sa obe strane jednak $c_p c_m$, pa promenljiva y može biti eliminisana. Analogno se y može eliminisati iz jednakosti oblika $s_p = t_p$. U dobijenoj konjukciji nema više pojavljivanja promenljive y, pa kvantifikator $(\exists y)$ iz $(\exists y)H_i$ može biti eliminisan.
Razmotrimo slučaj $j = 0$. Tada je formula $(\exists y)H_i$ oblika

$$(\exists y)(q_1 < r_1 \wedge \ldots \wedge q_k < r_k).$$

Ako se y u svakoj nejednakosti nalazi sa desne strane tada zamenjujemo $(\exists y)H_i$ sa $\top$. Slično, ako se y u svakoj nejednakosti nalazi sa leve strane tada zamenjujemo $(\exists y)H_i$ sa $\top$. Inače, za svaki par m, p takav da se y nalazi sa raznih strana u nejednakostima $q_m < r_m$ i $q_p < r_p$, odgovarajući par nejednakosti zamenjujemo nejednakošću

$$c_p q_m + c_m q_p < c_p r_m + c_m r_p$$

pri čemu je c_m koeficijent uz y u m-toj nejednakosti, a c_p koeficijent uz y u p-toj nejednakosti, pa je koeficijent uz y sa obe strane nejednakosti $c_p c_m$. Ako u polaznoj formuli H_i ima j nejednakosti sa promenljivom y na levoj i k nejednakosti sa promenljivom y na desnoj strani, onda novodobijena formula ima ukupno $j \cdot k$ nejednakosti iz kojih se promenljiva y može trivijalno eliminisati. Nakon toga nema više pojavljivanja promenljive y pa kvantifikator $(\exists y)$ iz $(\exists y)H_i$ može biti eliminisan.

Ilustrujmo Furije-Mockinovu proceduru na jednom primeru.

Primer 3. *Pokažimo da je formula $\forall x \forall y(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y)$ teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka primenom Furije-Mockinove procedure.*

$\forall x \forall y(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y)$
$\Leftrightarrow$
$\forall x \neg \exists y(\neg(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y))$
$\Leftrightarrow$
$\forall x \neg \exists y(2x < 3y \wedge 3x < 2y \wedge \neg(7x < 7y))$
$\Leftrightarrow$
$\forall x \neg \exists y(2x < 3y \wedge 3x < 2y \wedge (7x = 7y \vee 7y < 7x))$
$\Leftrightarrow$
$\forall x \neg \exists y((2x < 3y \wedge 3x < 2y \wedge 7x = 7y) \vee (2x < 3y \wedge 3x < 2y \wedge 7y < 7x))$
$\Leftrightarrow$
$\forall x \neg (\exists y(2x < 3y \wedge 3x < 2y \wedge 7x = 7y) \vee \exists y(2x < 3y \wedge 3x < 2y \wedge 7y < 7x))$
$\Leftrightarrow$
$\forall x \neg((14x < 21x \wedge 21x < 14x) \vee (14x < 21x \wedge 21x < 14x))$
$\Leftrightarrow$
$\neg \exists x((14x < 21x \wedge 21x < 14x) \vee (14x < 21x \wedge 21x < 14x))$
$\Leftrightarrow$
$\neg \exists x((0 < 7x \wedge 7x < 0) \vee (0 < 7x \wedge 7x < 0))$
$\Leftrightarrow$
$\neg(\exists x(0 < 7x \wedge 7x < 0)) \vee (\exists x(0 < 7x \wedge 7x < 0))$
$\Leftrightarrow$
$\neg(0 < 0 \vee 0 < 0)$
$\Leftrightarrow$
$\neg(\perp \vee \perp)$
$\Leftrightarrow$
$\top$

$\triangle$

4.2 Primena Furije-Mockinove procedure u rešavanju sistema linearnih nejednačina

Furije-Mockinova metoda se može iskoristiti za rešavanje sistema linearnih nejednačina sa znakom $<$ (kao i onih sa znakom $\leq$), kojima su nepoznate $x_1, x_2, \ldots, x_n \in \mathbb{R}$, $n = 1, 2, 3, \ldots$ Napomenimo da je pojam *sistem nejednačina* zapravo isto što i *konjukcija nejednačina*.

Najpre se bira neki redosled traženja nepoznatih. Uzmimo, na primer, da je x_1 prvi član u tom redosledu. Tada, pomoću ekvivalencija

$$x < a \wedge x < b \Leftrightarrow x < min(a, b)$$

$$x > a \wedge x > b \Leftrightarrow x > max(a, b)$$

$$a < x \wedge x < b \Leftrightarrow a < x < b$$

i raznih drugih činjenica o rešavanju neke linearne nejednačine po određenoj nepoznatoj, za nepoznatu x_1 određujemo obrazac oblika

$$\mathcal{A}(x_2, \ldots, x_n) < x_1 < \mathcal{B}(x_2, \ldots, x_n) \tag{3}$$

gde izrazi $\mathcal{A}$ i $\mathcal{B}$ ne sadrže x_1. Preciznije govoreći, polazni sistem je ekvivalentan sa novim sistemom sastavljenim od (3) i podsistema koji ne sadrži x_1. Dalje se sa novim sistemom slično nastavlja i tako sve do kraja tj. dok se odredi i poslednja nepoznata.

Potrebno je napomenuti da postoji mogućnost i da polazni sistem bude nemoguć. U opisanom postupku (algoritmu) to bi se prikazalo tako što bismo došli do neke „konstantske" nejednačine koja je nemoguća.

Treba naglasiti da se, ukoliko imamo nejednačine oblika (3), tada dodaje nejednačina

$$\mathcal{A}(x_2, \ldots, x_n) < \mathcal{B}(x_2, \ldots, x_n). \tag{4}$$

Drugim rečima, nema nejednačine koja se može „rešiti" po x_1. To znači da x_1 ostaje slobodno.

U slučaju da se u sistemu nejednačina pojave oba znaka nejednakosti, i $<$ i $\leq$, neophodno je iskoristiti opštu ekvivalenciju

$$a \leq b \Leftrightarrow a < b \vee a = b \tag{5}$$

i nakon toga obaviti takozvano logičko množenje, čime se prelazi na disjunkciju sistema, od kojih je svaki rešiv upotrebom ideja Furije-Mockinovog metoda i Gausovog metoda.

Primer 4. *Rešiti sistem linearnih nejednačina*

$$x + y < 3 \;\wedge\; 2x - y > 1 \;\wedge\; x - y < 4 \;\wedge\; x - 3y > 2$$

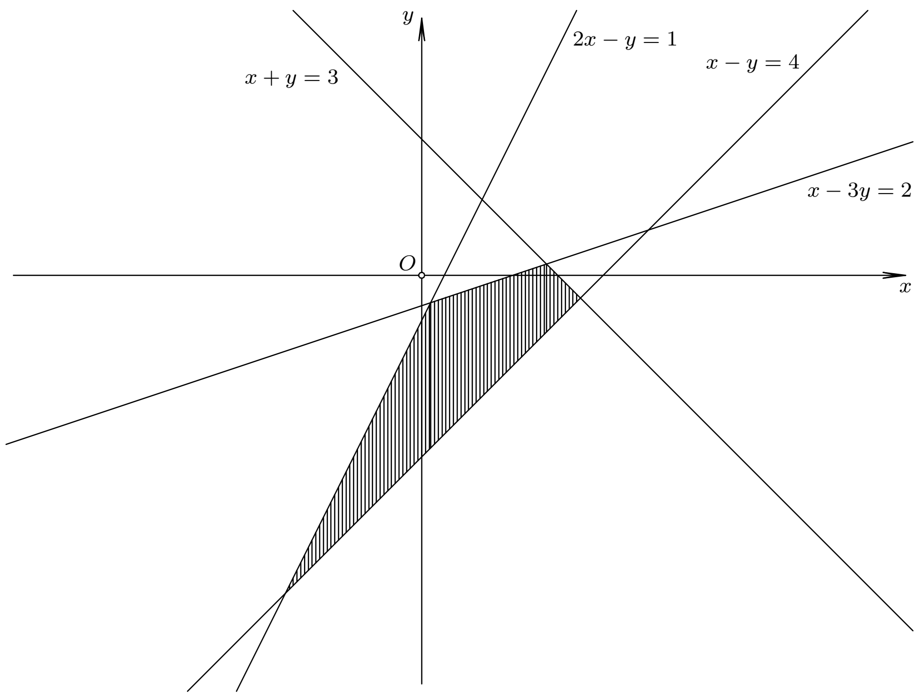
Sve nejednačine u ovom sistemu resićemo po x, tj. ideja nam je da x odredimo pomoću y.

$x + y < 3 \;\wedge\; 2x - y > 1 \;\wedge\; x - y < 4 \;\wedge\; x - 3y > 2$
$\Leftrightarrow$
$x < 3 - y \;\wedge\; x > \frac{1}{2}(y + 1) \;\wedge\; x < y + 4 \;\wedge\; x > 3y + 2$
$\Leftrightarrow$
$x < min(3 - y, y + 4) \;\wedge\; x > max(\frac{1}{2}(y + 1), 3y + 2)$
$\Leftrightarrow$
$max(\frac{1}{2}(y + 1), 3y + 2) < min(3 - y, y + 4) \;\wedge\; max(\frac{1}{2}(y + 1), 3y + 2) < x < min(3 - y, y + 4)$
$\Leftrightarrow$
$\frac{1}{2}(y + 1) < 3 - y \;\wedge\; \frac{1}{2}(y + 1) < y + 4 \;\wedge\; 3y + 2 < 3 - y \;\wedge\; 3y + 2 < y + 4 \;\wedge$
$\wedge\; max(\frac{1}{2}(y + 1), 3y + 2) < x < min(3 - y, y + 4)$
$\Leftrightarrow$
$y < \frac{5}{3} \;\wedge\; y > -7 \;\wedge\; y < \frac{1}{4} \;\wedge\; y < 1 \;\wedge\; max(\frac{1}{2}(y + 1), 3y + 2) < x < min(3 - y, y + 4)$

$\Leftrightarrow$
$-7 < y \ \wedge \ y < min(\frac{5}{3}, \frac{1}{4}, 1) \ \wedge \ max(\frac{1}{2}(y+1), 3y+2) < x < min(3-y, y+4)$
$\Leftrightarrow$
$-7 < y \ \wedge \ y < \frac{1}{4} \ \wedge \ max(\frac{1}{2}(y+1), 3y+2) < x < min(3-y, y+4)$
$\Leftrightarrow$
$-7 < y < \frac{1}{4} \ \wedge \ max(\frac{1}{2}(y+1), 3y+2) < x < min(3-y, y+4)$

Stigli smo do rešenja: y sme da bude broj između -7 i $\frac{1}{4}$, dok je odgovarajući x bilo koji broj u navedenim granicama $max(\frac{1}{2}(y+1), 3y+2)$, $min(3-y, y+4)$.

$\triangle$



Slika 1: Grafički prikaz sistema linearnih nejednačina iz primera 4.

Prethodni sistem jednačina sa dve nepoznate x, y može biti i grafički predstavljen u $\mathbb{R}^2$ (Slika 1.). Naime, svaka od nejednačina predstavlja skup tačaka u ravni sa jedne strane odgovarajuće prave. Uzmimo, na primer, nejednačinu $x + y < 3$. Da bismo grafički predstavili skup svih tačaka $(x_0, y_0) \in \mathbb{R}$ koji zadovoljavaju datu nejednačinu potrebno je prvo nacrtati grafik funkcije $x+y = 3$, što je jedna prava. Ta prava deli $\mathbb{R}^2$ na dve poluravni, od kojih jedna predstavlja rešenje nejednačine. U tom slučaju dovoljno je uzeti proizvoljnu tačku iz jedne od poluravni i proveriti da li zadovoljava nejednačinu. Ukoliko zadovoljava, rešenje je poluravan kojoj ta tačka pripada, a ako ne onda je rešenje suprotna poluravan.

Primer 5. *Rešiti sistem linearnih nejednačina*

$$x + y + z > 1 \ \wedge \ x - y - z < 1 \ \wedge \ x + y - z > 0$$

Odaberimo najpre redosled po kome ćemo tražiti nepoznate. Neka to bude redosled $x - y - z$.

$x + y + z > 1 \ \wedge \ x - y - z < 1 \ \wedge \ x + y - z > 0$
$\Leftrightarrow$
$x > -y - z + 1 \ \wedge \ x < y + z + 1 \ \wedge \ x > -y + z$
$\Leftrightarrow$
$x > max(-y - z + 1, -y + z) \ \wedge \ x < y + z + 1$
$\Leftrightarrow$
$max(-y - z + 1, -y + z) < y + z + 1 \ \wedge \ max(-y - z + 1, -y + z) < x < y + z + 1$
$\Leftrightarrow$
$-y - z + 1 < y + z + 1 \ \wedge \ -y + z < y + z + 1 \ \wedge \ max(-y - z + 1, -y + z) < x < y + z + 1$
$\Leftrightarrow$
$-2y < 2z \ \wedge \ -2y < 1 \ \wedge \ max(-y - z + 1, -y + z) < x < y + z + 1$
$\Leftrightarrow$
$y > -z \ \wedge \ y < -\frac{1}{2} \ \wedge \ max(-y - z + 1, -y + z) < x < y + z + 1$
$\Leftrightarrow$
$-z < y < -\frac{1}{2} \ \wedge \ max(-y - z + 1, -y + z) < x < y + z + 1$

Stigli smo do rešenja: y *može biti bilo koji broj manji od* $-\frac{1}{2}$, z *bilo koji broj manji od* y, *a samim tim i od* $-\frac{1}{2}$, *a* x *je bilo koji broj u granicama* $max(-y - z + 1, -y + z)$, $y + z + 1$.

$\triangle$

Primer 6. *Rešiti „mešoviti" sistem linearnih nejednačina*

$$x > 0 \ \wedge \ y > 0 \ \wedge \ x + y \leq 1$$

S obzirom na (5) sistem je ekvivalentan sa

$x > 0 \ \wedge \ y > 0 \ \wedge \ (x + y < 1 \ \vee \ x + y = 1)$
$\Leftrightarrow$
$(x > 0 \ \wedge \ y > 0 \ x + y < 1) \ \vee \ (x > 0 \ \wedge \ y > 0 \ \wedge \ x + y = 1)$

Sada smo dobili dve grane. Prvu čini sistem linearnih nejednačina, a drugu sistem od dve nejednačine i jedne jednačine. U prvoj grani primenićemo Furije-Mockinovu metodu, a u drugoj metodu zamene. Nastavljamo ekvivalencijski lanac

$\Leftrightarrow$
$(x > 0 \ \wedge \ x < 1 - y \ \wedge \ y > 0) \ \vee \ (x > 0 \ \wedge \ y > 0 \ \wedge \ x = 1 - y)$
$\Leftrightarrow$
$(0 < x < 1 - y \ \wedge \ y > 0) \ \vee \ (1 - y > 0 \ \wedge \ y > 0 \ \wedge \ x = 1 - y)$
$\Leftrightarrow$
$(0 < 1 - y \ \wedge \ y > 0 \ \wedge \ 0 < x < 1 - y) \ \vee \ (y < 1 \ \wedge \ y < 0 \ \wedge \ x = 1 - y)$
$\Leftrightarrow$
$(0 < y < 1 \ \wedge \ 0 < x < 1 - y) \ \vee \ (0 < y < 1 \ \wedge \ x = 1 - y)$

Kao što vidimo, skup rešenja je unija dva skupa. Kako je ovde moguće da „spojimo” dve grane dobijamo da se ekvivalencijski lanac završava sa

$\Leftrightarrow$
$0 < y < 1 \ \wedge \ 0 < x \leq 1 - y$

Dakle, dobili smo nešto prostiji opis skupa svih rešenja.

$\triangle$

5 Eliminacija kvantifikatora za teoriju algebarski zatvorenih polja

Pod *algebarski zatvorenim poljem* podrazumeva se algebarska struktura $(K, +, \cdot, 0, 1)$ u kojoj važe sledeće aksiome:

- za svako $a, b \in K$, $a + b, a \cdot b \in K$ (zatvorenost skupa K u odnosu na binarne operacije $+$ i $\cdot$)
- za svako $a, b, c \in K$, $(a+b)+c = a+(b+c)$ i $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asocijativnost operacija $+$ i $\cdot$)
- postoji element $0 \in K$ takav da za svako $a \in K$, $a + 0 = 0 + a = a$ (postojanje aditivnog neutrala)
- postoji element $1 \in K$ takav da za svako $a \in K$, $a \cdot 1 = 1 \cdot a = a$ (postojanje multiplikativnog neutrala)
- za svako $a \in K$ postoji $-a \in K$ takav da $-a+a = a+(-a) = 0$ (postojanje aditivnih inverza)
- za svako $a \in K, a \neq 0$ postoji $a^{-1} \in K$ takav da $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (postojanje multiplikativnih inverza)
- za svako $a, b \in K$, $a + b = b + a$ i $a \cdot b = b \cdot a$ (komutativnost operacija $+$ i $\cdot$)
- za svako $a, b, c \in K$, $a \cdot (b+c) = a \cdot b + a \cdot c$ i $(b+c) \cdot a = b \cdot a + c \cdot a$ (distributivnost $\cdot$ prema $+$)
- $\exists x(y_0 + y_1 x + \ldots + y_n x^n = 0) \vee y_n = 0$, $n = 1, 2, 3, \ldots$

Prema ovim aksiomama svako polje K je algebarski zatvoreno ako svaki polinom stepena ≥ 1 nad tim poljem ima koren. Polje $\mathbb{C}$ kompleksnih brojeva je primer modela za teoriju algebarski zatvorenih polja.

Primeri eliminacije kvantifikatora za teoriju algebarski zatvorenih polja odavno su poznati u klasičnoj algebri. Jedan od najpoznatijih je *teorema o rezolventi*.

Najpre uvedimo pojam rezolvente. Neka su $a(x) = \sum_{i=0}^{m} a_i x^i$ i $b(x) = \sum_{j=0}^{n} b_j x^j$ kompleksni polinomi. *Rezolventa polinoma* $a(x)$ i $b(x)$ je determinanta

$$Res(a,b) = \begin{vmatrix} a_0 & a_1 & \ldots & a_m & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_m & \ldots & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & \ldots & a_0 & a_1 & \ldots & a_m \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_n & \ldots & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & \ldots & b_0 & b_1 & \ldots & b_n \end{vmatrix}$$

Dakle, $Res(a,b)$ je determinanta reda $m+n$, gde su m i n stepeni polinoma $a(x)$, odnosno $b(x)$.

Primer 7. *Odredimo rezolventu polinoma* $3x+2$ *i* x^3+x^2+x-1.

$$Res(3x+2,\, x^3+x^2+x-1) = \begin{vmatrix} 3 & 2 & 0 & 0 \\ 0 & 3 & 2 & 0 \\ 0 & 0 & 3 & 2 \\ 1 & 1 & 1 & -1 \end{vmatrix} = -41$$

△

Glavno svojstvo rezolvente daje sledeća

Teorema 3. *Kompleksni polinomi* $a(x)$ *i* $b(x)$ *imaju zajednički koren u polju kompleksnih brojeva akko je* $Res(a,b)=0$.

Ovu teoremu možemo drugačije zapisati i u obliku

$$\exists x(a(x)=0 \wedge b(x)=0) \Leftrightarrow Res(a,b)=0.$$

Neka su dati polinomi $a(x)=y_m+y_{m-1}x+\ldots+y_0x^m$, $b(x)=z_n+z_{n-1}x+\ldots+z_0x^n$. Uvedimo polinome:

$$a_0(x)=a(x),\ a_1(x)=y_m+y_{m-1}x+\ldots+y_1x^{m-1},\ldots,\ a_m(x)=y_m$$

$$b_0(x)=b(x),\ b_1(x)=z_n+z_{n-1}x+\ldots+z_1x^{n-1},\ldots,\ b_m(x)=z_n$$

Tada prema prethodnoj teoremi imamo

$$\exists x(a(x)=0 \wedge b(x)=0)$$

$$\Leftrightarrow$$

$$\bigvee_{\substack{i<m \\ j<n}} (d^\circ a_i = m-i \wedge d^\circ b_j = n-j \wedge Res(a_i,b_j)=0) \vee \bigwedge_{i,j}(y_i=0 \wedge z_j=0)$$

$$\Leftrightarrow$$

$$\bigvee_{\substack{i<m \\ j<n}} (y_0=0 \wedge \ldots \wedge y_{i-1}=0 \wedge y_i \neq 0 \wedge z_0=0 \wedge \ldots \wedge z_{j-1}=0 \wedge z_j \neq 0 \ \wedge\ Res(p_i,q_j)=0) \vee$$

$$\bigwedge_{i,j}(y_i=0 \wedge z_j=0) \tag{6}$$

Time smo razmotrili jedan slučaj eliminacije kvantifikatora. Razmotrimo još dva slučaja.

S obzirom da je svako algebarski zatvoreno polje beskonačno (koreni polinoma $(x-x_0)(x-x_1)\ldots(x-x_n)+1$ su različiti od $x_0,\ldots,x_n$), za polinom $a(x)=\sum_{i=1}^{n} y_i x^i$ imamo

$$\exists x(a(x)\neq 0) \Leftrightarrow (y_0 \neq 0 \vee \ldots \vee y_n \neq 0). \tag{7}$$

Sada ćemo pokazati da se eliminacija kvantifikatora u formuli

$$\exists x(a(x) = 0 \land b(x) \neq 0)$$

svodi na prethodni slučaj. Prvo, primetimo da je

$$b(x) \neq 0 \Leftrightarrow (\exists y)(yb(x) - 1 = 0)$$

i da se y javlja kao faktor u svakom članu polinoma, osim u slobodnom članu. Ako promenljivu y izaberemo tako da se ne javlja u formuli $a(x) = 0 \land b(x) = 0$, onda je

$$\exists x(a(x) = 0 \land b(x) \neq 0) \Leftrightarrow \exists x \exists y(a(x) = 0 \land yb(x) - 1 = 0)$$

Prema prvom slučaju formula $\exists x(a(x) = 0 \land b(x) \neq 0)$ ekvivalentna je disjunkciji $\varphi_1 \lor \ldots \lor \varphi_k$ koja ne sadrži kvantifikatore i svaka formula φ_j za $j < k$ je (za odgovarajući polinom b'_j) oblika

$$y_0 = 0 \land \ldots \land y_{i-1} = 0 \land y_i \neq 0 \land z_0 y = 0 \land \ldots \land z_{j-1} y = 0 \land z_j y \neq 0 \land Res(a_i, b'_j) = 0.$$

Kako je $\exists\, x \bigvee_i \varphi_i \Leftrightarrow \bigvee_i \exists\, x \varphi_i$ valjana formula, dovoljno je izvesti eliminaciju kvantifikatora u formuli $\exists\, y \varphi_i$. Da bismo to uradili dovoljno je eliminisati egzistencijalni kvantifikator u formuli

$$\exists y(y \neq 0 \land Res(a_i, b'_j) = 0)$$

odnosno u formuli oblika

$$\exists y(y \neq 0 \land m(y) = 0)$$

gde je $m(y)$ polinom. Ako polinom $m(y)$ napišemo u obliku

$$m(y) = m_0 + m_1 y + \ldots + m_k y^k$$

dobijamo da je

$$\exists y(y \neq 0 \land m(y) = 0) \Leftrightarrow \bigvee_{i<j} (m_i \neq 0 \land m_j \neq 0).$$

Sada prelazimo na opšti slučaj eliminacije kvantifikatora u teoriji algebarski zatvorenih polja. Neka je φ bilo koja formula teorije polja. Prema Lemi 2. formula φ je ekvivalentna formuli u preneks normalnoj formi

$$Q_1 x_1, \ldots, Q_n x_n \psi$$

gde je ψ formula bez kvantifikatora. Koristeći valjanu formulu

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

kao i to da nas eliminacija kvantifikatora u formuli $\neg\varphi$ do istog rezultata za formulu φ, možemo pretpostaviti da je Q_n egzistencijalni kvantifikator.

Dalje, prema teoremi o disjunktivnoj normalnoj formi, postoje formule $\psi_1, \ldots, \psi_k$ takve da je

$$\psi \Leftrightarrow \psi_1 \lor \ldots \lor \psi_n$$

i svaka formula ψ_i je konjukcija formula oblika $u = 0$, $v \neq 0$. Pri tome je korišćena činjenica da je svaki term jezika teorije polja jednak nekom polinomu. Kako je $v_1 \neq 0 \wedge \ldots \wedge v_n \neq 0 \Leftrightarrow v_1 \ldots v_n \neq 0$, to se može uzeti da je svaki disjunkt ψ_i oblika

$$a_1 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0.$$

S obzirom na valjanu formulu

$$\exists x \bigvee_i \psi_i \Leftrightarrow \bigvee_i \exists x \psi_i$$

dovoljno je da se navede postupak eliminacije kvantifikatora za formule oblika

$$\exists x(a_1 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0). \tag{8}$$

Neka je $\lambda_i x^{n_i}$ član najvišeg stepena polinoma $a_i(x)$, $i = 1, \ldots, m$, i neka je $n_\theta = m + \sum_i n_i$. Odredićemo formule θ_1 i θ_2 oblika (8) tako da je $\theta \Leftrightarrow \theta_1 \vee \theta_2$ i $n_{\theta_1}, n_{\theta_2} < n_\theta$ ukoliko je $n_\theta > 1$ i $m \geq 2$.

Najpre pretpostavimo da je $n_1 = 0$. Onda je

$$\theta \Leftrightarrow a_1 = 0 \wedge \exists x(a_2 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0)$$

pa zato pretpostavimo da je $n_1 \neq 0$ i $n > 1$. Možemo takođe uzeti da je $n_2 \leq n_1$. Neka je $a_1' = \lambda_2 a_1 \lambda_1 x^{n_1 - n_2} a_2$, $a_2' = a_2 - \lambda_2 x^{n_2}$. Tada je

$$\theta \Leftrightarrow (\lambda_2 = 0 \wedge \exists x(a_1 = 0 \wedge a_2' = 0 \ldots \wedge a_m = 0 \wedge b \neq 0) \vee$$

$$\lambda_2 \neq 0 \wedge \exists x(a_1' = 0 \wedge a_2 = 0 \ldots \wedge a_m = 0 \wedge b \neq 0).$$

Sada je očigledno da za formulu θ_1 možemo izabrati prvi disjunkt, a za formulu θ_2 drugi disjunkt desne strane ove ekvivalencije. Na ovaj način je definisana rekurzivna procedura za eliminisanje kvantifikatora kojom se dolazi do slučajeva (6) i (7), a kako se oni rešavaju već je opisano.

5.1 Šturmov algoritam

Eliminacija kvantifikatora u teoriji algebarski zatvorenih polja se može izvršiti i na drugačiji način, upotrebom najvećeg zajedničkog delioca za dva polinoma. Neka je F algebarski zatvoreno polje i neka su $f, g \in K[x]$. Tada, u slučaju da f i g imaju zajednički koren a, najveći zajednički delilac polinoma f i g je stepena ≥ 1, jer $x - a$ deli oba polinoma. Drugim rečima

$$\exists x(f(x) = 0 \wedge g(x) = 0) \Leftrightarrow d^\circ NZD(f, g) \geq 1$$

Za nalaženje $NZD(f, g)$ može se koristiti Euklidov algoritam, koji se završava u konačno mnogo koraka, jer sam postupak zavisi od stepena f i g. Zbog toga se može videti da se ovaj algoritam opisuje jednom formulom bez kvantifikatora tj. ako je:

$f = q_1 g + m_2$
$g = q_2 m_2 + m_3$
$m_2 = q_3 m_3 + m_4$
$\vdots$
$m_{i-2} = q_{i-1} m_{i-1} + q_i$
$m_{i-1} = q_i m_i$, $d^\circ f > d^\circ g > d^\circ m_2 > \ldots > d^\circ m_i$

onda je

$$\exists x(f(x) = 0 \land g(x) = 0) \Leftrightarrow f = q_1 g + m_2 \land \ldots \land m_{i-1} = q_i m_i \land z \neq 0$$

gde je z koeficijent uz najviši stepen promenljive x u m_i. Primetimo i da desna strana prethodne ekvivalencije ne sadrži kvantifikatore. Navedimo za kraj *Šturmovu*[10] *teoremu*:

Teorema 4. *Neka je $p(x)$ realan polinom i neka je $p_0, p_1, \ldots, p_r$ niz realnih polinoma definisanih na sledeći način:*

- $p_0 = p$
- $p_1 = p'$ *(prvi izvod od p)*
- *za sve $0 < i < r$ postoji polinom q_i takav da je*
  $p_{i-1} = p_i q_i - p_{i+1}$, *gde je* $p_{i+1} \neq 0$ *i* $d^\circ p_{i+1} < d^\circ p_i$
- $p_{r-1} = p_r q_r$

Neka je $d(a)$ promena znakova u nizu $p_0(a), \ldots, p_r(a)$, nule se pritom zanemaruju. Neka su a i b realni brojevi koji nisu koreni polinoma p, i neka je $a < b$. Tada je broj korena polinoma p, ne računajući višestrukost korena u intervalu $[a, b]$ jednak $d(a) - d(b)$.

[10] Jacques Charles Francois Sturm (1803 - 1855) - francuski matematičar

6 Eliminacija kvantifikatora za teoriju realno zatvorenih polja

Za kraj razmotrimo metod eliminacije kvantifikatora za teoriju realno zatvorenih polja. Realno zatvorena polja su specijalna vrsta uređenih polja. Podsetimo se da su uređena polja sve strukture definisane na jeziku $\mathcal{L}_{OR} = \{+, \cdot, -, 0, 1, \leq\}$, gde su $+$ i $\cdot$ binarni operacijski simboli, $-$ unarni operacijski simbol, 0 i 1 simboli konstanti, a $\leq$ binarni relacijski simbol, a koje zadovoljavaju sledeće aksiome:

(P1) $\forall x \forall y \forall z ((x+y)+z = x+(y+z))$

(P2) $\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$

(P3) $\forall x (x + 0 = 0 + x = x)$

(P4) $\forall x (x \cdot 1 = 1 \cdot x = x)$

(P5) $\forall x \exists (-x)(x + (-x) = -x + x = 0)$

(P6) $\forall x \neq 0 (x \cdot x^{-1} = x^{-1} \cdot x = 1)$

(P7) $\forall x \forall y (x + y = y + x)$

(P8) $\forall x \forall y (x \cdot y = y \cdot x)$

(P9) $\forall x \forall y \forall z (x \cdot (y + z) = x \cdot y + x \cdot z)$

(U1) $\forall x \forall y (x \leq y \vee y \leq x)$

(U2) $\forall x \forall y ((x \leq y \wedge y \leq x) \Rightarrow x = y)$

(U3) $\forall x \forall y \forall z ((x \leq y \wedge y \leq z) \Rightarrow x \leq z)$

(M1) $\forall x \forall y \forall z (x \leq y \Rightarrow x + z \leq y + z)$

(M2) $\forall x \forall y \forall z ((x \leq y \wedge 0 \leq z) \Rightarrow x \cdot z \leq y \cdot z)$

Aksiome (P1)-(P9) su aksiome polja, aksiome (U1)-(U3) zovemo aksiome uređenja, dok su aksiome (M1) i (M2) poznate kao aksiome monotonosti.

Realno zatvorena polja su strukture koje zadovoljavaju gore pomenute aksiome uređenih polja i još tri sheme aksioma:

(**1**) za sve $n \geq 0$: $\forall x_0, \ldots, x_{2n} \exists y (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$

(**2**) za sve $n \geq 1$: $\forall x_1, \ldots, x_n (x_1^2 + \ldots + x_n^2 + 1 \neq 0)$

(**3**) $\forall x \exists y (y^2 = x \vee y^2 + x = 0)$

Standardni model za teoriju realno zatvorenih polja je polje realnih brojeva $\mathbb{R}$. Glavni rezultat u vezi sa teorijom realno zatvorenih polja (RCF), koji je prvi dokazao Tarski, jeste taj da ova teorija dopušta eliminaciju kvantifikatora. Dokaz ovog rezultata se može izvesti na dva različita načina. Jedan je da se upotrebom model-teoretske „mašinerije” okarakterišu klase teorija koje dopuštaju eliminaciju kvantifikatora, pa da se potom pokaže da teorija RCF pripada toj klasi. Ovaj pristup nam ipak ne daje metod kojim se eksplicitno prikazuje kako da se „nosimo” sa eliminacijom kvantifikatora. Drugi način je da se konstruiše algoritam za eliminaciju kvantifikatora, pa da se potom dokaže ispravnost algoritma. Sâm Tarski je pomoću ovog pristupa dokazao da teorija RCF dopušta eliminaciju kvantifikatora.

Već duže vreme primena eliminacije kvantifikatora u problemima van same matematike je prilično ograničena zbog praktične složenosti implementiranih metoda. Do pre nekoliko godina, neke od tih metoda su bile u mogućnosti da reše neke interesantne probleme u nauci, inženjerstvu, a takođe i u ekonomiji. Mada povećan rast kompjuterske moći igra određenu ulogu, uglavnom je teorijski rad taj koji je doprineo tom razvoju.

Neke od pomenutih metoda koje implementiraju eliminaciju kvantifikatora su cilindrična algebarska dekompozicija (CAD), kao i virtuelna zamena. U nastavku ćemo se zadržati na metodi virtuelne supstitucije, a o drugoj metodi, kao i o još nekim metodama, se više može pronaći, između ostalog, u [11].

6.1 Metoda virtuelne supstitucije

Velika složenost postupka za eliminaciju kvantifikatora naterala je istraživače da proučavaju neke potprobleme opšteg problema i razvijaju efikasnije procedure za neke formule specijalnog oblika. Jedna od takvih metoda jeste *metoda virtuelne supstitucije*. Ona je posebno efikasna za formule u kojima su kvantifikovane promenljive najviše kvadratnog stepena, pa ćemo je zato i opisati za formule oblika

$$\exists y_1 \cdots \exists y_n \exists x \varphi(y_1, \ldots, y_n, x)$$

gde je φ Bulovska kombinacija formula oblika $f \sim 0$, $\sim \in \{=, <, >, \leq, \geq, \neq\}$, f je polinom po x najviše stepena 2 čiji su koeficijenti polinomi ostalih promenljivih, tj. pripadaju $\mathbb{Q}(y_1, \ldots, y_n)$. Formule oblika $f \sim 0$ nazivaćemo elementarnim formulama. Metoda koju opisujemo podrazumeva najpre eliminaciju krajnjeg unutrašnjeg kvantifikatora koji vezuje x.

Zamislimo da su $y_1, \ldots, y_n$ realni parametri. Svaka elementarna formula razbija domen promenljive x na skup vrednosti koje zadovoljavaju tu formulu i skup vrednosti koje je ne zadovoljavaju. Skup vrednosti koje zadovoljavaju formulu $f \sim 0$ jeste unija konačno mnogo intervala čije su krajnje tačke $-\infty$, $+\infty$ ili nule polinoma f. Na primer, ako je $f = ax^2 + bx + c$, nule su:

$$\begin{array}{ll} x_0 = -\frac{c}{b} & \text{ako je } a = 0 \wedge b \neq 0 \\ x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a} & \text{ako je } a \neq 0 \wedge b^2 - 4ac \geq 0 \\ x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a} & \text{ako je } a \neq 0 \wedge b^2 - 4ac \geq 0. \end{array}$$

Naravno, skup elementarnih formula ima zajedničko rešenje akko je neprazan presek skupova rešenja svake elementarne formule posebno. Ovaj presek takođe je unija konačno mnogo intervala koji mogu biti ograničeni ili neograničeni, otvoreni, zatvoreni ili poluzatvoreni/poluotvoreni. Svaka krajnja tačka pomenutih intervala je $-\infty$, $+\infty$ ili je oblika $\frac{a+b\sqrt{c}}{d}$, $a, b, c, d \in \mathbb{Q}(y_1, \ldots, y_n)$. Od ovih tačaka obrazujemo tzv. *skup kandidata*, uključujući u nekim slučajevima novu (infinitezimalnu) promenljivu ε:

1. $\frac{a+b\sqrt{c}}{d}$ je kandidat ako je ova tačka leva, odnosno desna krajnja tačka levo-, odnosno desno-zatvorenog intervala sadržanog u preseku,
2. $e + \varepsilon$ je kandidat ako je e leva krajnja tačka levo-otvorenog intervala sadržanog u preseku,
3. $e - \varepsilon$ je kandidat ako je e desna krajnja tačka desno-otvorenog intervala sadržanog u preseku,
4. $-\infty$ je kandidat ako presek sadrži sleva neograničen interval,
5. $+\infty$ je kandidat ako presek sadrži zdesna neograničen interval.

Svakog kandidata K zamenjujemo u φ umesto x i ispitujemo da li je formula $\varphi[x/K]$ tačna. Naravno, supstitucije $\left[x/\frac{a+b\sqrt{c}}{d}\right]$, $[x/e+\varepsilon]$, $[x/e-\varepsilon]$, $[x/-\infty]$, $[x/+\infty]$ nisu standardne i metoda virtuelne supstitucije ih eliminiše (pa zato navedene supstitucije nazivamo virtuelnim) posebnim pravilima, tako da se u rezultujućoj formuli ne pojavljuju. Postoji 30 pravila koja se odnose na supstituciju, jer postoji 6 vrsta elementarnih formula ($\sim \in \{=, <, >, \leq, \geq, \neq\}$) i 5 vrsta kandidata. Ukratko ćemo opisati ova pravila za neke elementarne formule $f \sim 0$.

1. Supstitucija $\left[x/\frac{a+b\sqrt{c}}{d}\right]$

Zbir i proizvod izraza $\frac{a+b\sqrt{c}}{d}$ i $\frac{a'+b'\sqrt{c}}{d'}$, $d, d' \neq 0$, $a, b, c, d, a', b', d' \in \mathbb{Q}(y_1, \ldots, y_n)$ jeste izraz istog oblika:

$$\frac{a+b\sqrt{c}}{d} + \frac{a'+b'\sqrt{c}}{d'} = \frac{(d'a+da')+(d'b+db')\sqrt{c}}{dd'}$$

i

$$\frac{a+b\sqrt{c}}{d} \cdot \frac{a'+b'\sqrt{c}}{d'} = \frac{(aa'+bb'c)+(ab'+a'b)\sqrt{c}}{dd'}.$$

Dakle, izraz $f\left[x/\frac{a+b\sqrt{c}}{d}\right]$ je oblika $\frac{a^*+b^*\sqrt{c}}{d^*}$. Primetimo da je $d^* = d^k$, gde je k stepen polinoma f po x. Neka je $\delta = 1$, ako je $k = 1$, i $\delta = 0$ ako je $k = 0, 2$. U slučaju da je $b = 0$, tj. da je $f\left[x/\frac{a+b\sqrt{c}}{d}\right] = \frac{a^*}{d^*}$, onda definišemo:

$$f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] = 0 \overset{\text{def}}{\iff} a^* = 0,$$
$$f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] \leq 0 \overset{\text{def}}{\iff} a^*d^\delta \leq 0,$$
$$f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] < 0 \overset{\text{def}}{\iff} a^*d^\delta < 0.$$

Uopšte, za proizvoljno b stavljamo:

$$\begin{aligned}
f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] &= 0 \stackrel{\text{def}}{\Longleftrightarrow} a^*b^* \leq 0 \wedge a^{*2} - b^{*2}c = 0,\\
f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] &\leq 0 \stackrel{\text{def}}{\Longleftrightarrow} \left(a^*d^\delta \leq 0 \wedge 0 \leq a^{*2} - b^{*2}c\right) \vee \left(b^*d^\delta \leq 0 \wedge a^{*2} - b^{*2}c \leq 0\right),\\
f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] &< 0 \stackrel{\text{def}}{\Longleftrightarrow} \left(a^*d^\delta \leq 0 \wedge 0 < a^{*2} - b^{*2}c\right) \vee\\
&\qquad\qquad \left(b^*d^\delta \leq 0 \wedge (a^*d^\delta < 0 \vee a^{*2} - b^{*2}c < 0)\right),\\
f\left[x/\tfrac{a+b\sqrt{c}}{d}\right] &\neq 0 \stackrel{\text{def}}{\Longleftrightarrow} a^*b^* > 0 \vee a^{*2} - b^{*2}c \neq 0.
\end{aligned}$$

Navedene definicije su semantički korektne, tj. leve strane su ekvivalentne desnim uz uslove $c \geq 0$ i $d \neq 0$.

2. Supstitucija $[x/e+\varepsilon]$

Neka je $e = \frac{a+b\sqrt{c}}{d}$ i ε novi simbol za pozitivnu infinitezimalu koji može biti interpretiran u nekoj ekstenziji polja $\mathbb{R}$. Koriste se sledeća svojstva koja proizlaze iz Tejlorove formule za f u tački α.

Neka je $0 \neq f(x) \in \mathbb{R}[x]$ i $\alpha \in \mathbb{R}$. Tada je:

1. $f(\alpha+\varepsilon) \neq 0$;
2. $f(\alpha) \neq 0 \Rightarrow f(\alpha) \cdot f(\alpha+\varepsilon) > 0$ (tj. f ne menja znak u infinitezimalnoj okolini od α);
3. $0 = f(\alpha) = \ldots = f^{(k-1)}(\alpha) \neq f^{(k)}(\alpha) \Rightarrow f^{(k)}(\alpha) \cdot f(\alpha+\varepsilon) > 0$ (tj. najviši izvod po x od f koji nije jednak nuli za α određuje znak polinoma f u desnoj infinitezimalnoj okolini od α).

Navedena svojstva opravdavaju semantičku korektnost narednih definicija.

Za $f = \sum_{i=0}^{n} a_i x^i$, gde su a_i polinomi koji ne sadrže x, definišemo formulu $\nu(f)$ rekurzivno na sledeći način:

- ako je $n = 0$, onda je $\nu(f) \stackrel{\text{def}}{\Longleftrightarrow} f < 0$;
- ako je $n > 0$, onda je $\nu(f) \stackrel{\text{def}}{\Longleftrightarrow} f < 0 \vee (f = 0 \wedge \nu(f'))$.

Najzad, uvodimo sledeće definicije:

$$\begin{aligned}
(f = 0)[x/e+\varepsilon] &\stackrel{\text{def}}{\Longleftrightarrow} \bigwedge_{i=0}^{n} a_i = 0,\\
(f < 0)[x/e+\varepsilon] &\stackrel{\text{def}}{\Longleftrightarrow} \nu(f)[x/e+\varepsilon],\\
(f \leq 0)[x/e+\varepsilon] &\stackrel{\text{def}}{\Longleftrightarrow} (f = 0)[x/e+\varepsilon] \vee (f < 0)[x/e+\varepsilon],\\
(f \neq 0)[x/e+\varepsilon] &\stackrel{\text{def}}{\Longleftrightarrow} \bigvee_{i=0}^{n} a_i \neq 0.
\end{aligned}$$

3. Supstitucija $[x/e - \varepsilon]$

Ove supstitucije se uvode analogno kao prethodne i nećemo ih navoditi.

4. Supstitucija $[x/-\infty]$

Za $f = \sum_{i=0}^{n} a_i x^i$, gde su a_i polinomi koji ne sadrže x, definišemo formulu $\mu(f)$ rekurzivno na sledeći način:

- ako je $n = 0$, onda je $\mu(f) \overset{\text{def}}{\Longleftrightarrow} a_0 < 0$;
- ako je $n > 0$, onda je $\mu(f) \overset{\text{def}}{\Longleftrightarrow} (-1)^n a_n < 0 \vee (a_n = 0 \vee \mu(\sum_{i=0}^{n-1} a_i x))$.

Sada, uvodimo odgovarajuće definicije:

$$\begin{aligned}
(f = 0)[x/-\infty] &\overset{\text{def}}{\Longleftrightarrow} \bigwedge_{i=0}^{n} a_i = 0,\\
(f < 0)[x/-\infty] &\overset{\text{def}}{\Longleftrightarrow} \mu(f),\\
(f \leq 0)[x/-\infty] &\overset{\text{def}}{\Longleftrightarrow} (f = 0)[x/-\infty] \vee (f < 0)[x/-\infty],\\
(f \neq 0)[x/-\infty] &\overset{\text{def}}{\Longleftrightarrow} \bigvee_{i=0}^{n} a_i \neq 0.
\end{aligned}$$

5. Supstitucija $[x/+\infty]$

Ove supstitucije se uvode analogno kao prethodne i nećemo ih navoditi.

Detaljna razmatranja, uključujući i dokaz korektnosti metode, data su u [12].

Primer 8. *Posmatrajmo formulu oblika*

$$\varphi(u) \equiv \exists x \psi(u, x)$$

gde je $\psi(u, x) \equiv (x^2 + ux + 1 = 0 \wedge x > 0)$. *Eliminacija dela „*$\exists x$*" iz* φ *je tipičan primer proširenja Gausovog postupka eliminacije. Bilo koje* x *koje zadovoljava* ψ *mora zadovoljavati i jednačinu* $x^2 + ux + 1 = 0$. *Stoga*

$$\{\frac{-u + \sqrt{u^2 - 4}}{2}, \frac{-u - \sqrt{u^2 - 4}}{2}\}$$

je dovoljan skup kandidata. Virtuelna zamena x *u izrazima mora da uključi uslov* $u^2 - 4 \geq 0$ *i da reši kvadratne korenove i imenioce. Za prvi izraz dobijamo*

$$u^2 - 4 \geq 0 \wedge 0 = 0 \wedge -u + \sqrt{u^2 - 4} > 0 \equiv$$

$$u^2 - 4 \geq 0 \wedge (-u > 0 \vee (-u)^2 < u^2 - 4) \equiv$$

$$u^2 - 4 \geq 0 \wedge u < 0$$

Slično, za drugi izraz dobijamo

$$u^2 - 4 \geq 0 \wedge 0 = 0 \wedge -u - \sqrt{u^2 - 4} > 0 \equiv$$
$$u^2 - 4 \geq 0 \wedge -u > 0 \wedge (-u)^2 > u^2 - 4) \equiv$$
$$u^2 - 4 \geq 0 \wedge u < 0$$

Poslednji rezultat eliminacije je disjunkcija rezultata obe zamene

$$(u^2 - 4 \geq 0 \wedge u < 0) \vee (u^2 - 4 \geq 0 \wedge u < 0)$$

Lako se vidi da je ova formula ekvivalentna sa $u \leq -2$*.*

$\triangle$

7 Razni zadaci

Poslednje poglavlje ovog rada sadrži neke od srednjoškolskih zadataka rešenih pomoću metode eliminacije kvantifikatora. Naravno, u pitanju su zadaci iz oblasti elementarne algebre i geometrije. Kao i u drugom poglavlju, koristićemo termin zadaci, dok će simbol ⧫ označavati kraj zadatka.

Zadatak 1. *Rešiti po $x \in \mathbb{R}$ jednačinu $\sqrt[3]{2-x} = 1 - \sqrt{x-1}$.*

Rešenje. Ovu jednačinu nećemo rešiti idejom kvadriranja, kubiranja i sl. već ćemo izložiti jedan opšti postupak. Naime, u prvom koraku za svaki od korenova uvedimo po jednu novu, pomoćnu promenljivu, a potom koristimo definiciju korena

$$\begin{aligned}
\sqrt[3]{2-x} = 1 - \sqrt{x-1} \quad &\Leftrightarrow \quad (\exists y \in \mathbb{R})(\exists z \in \mathbb{R})(y = \sqrt[3]{2-x} \wedge z = \sqrt{x-1} \wedge y = 1 - z) \\
&\Leftrightarrow \quad (\exists y \in \mathbb{R})(\exists z \in \mathbb{R})(y^3 = 2 - x \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge \\
&\qquad \wedge z \geq 0 \wedge y = 1 - z) \\
&\Leftrightarrow \quad (\exists y \in \mathbb{R})(\exists z \in \mathbb{R})((1-z)^3 = 2 - x \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge \\
&\qquad \wedge z \geq 0 \wedge y = 1 - z)
\end{aligned}$$

Koristeći jednakost $y = 1 - z$ izbacili smo y iz ostalih formula, odnosno iz prve jednačine. Tu se koristi zakon zamene za jednakost

$$x = A \wedge \psi(x) \Leftrightarrow x = A \wedge \psi(A)$$

gde je A neki izraz, a $\psi(x)$ neka formula[11]. Na taj način y je ostalo samo u jednačini $y = 1 - z$. U skladu s tim, pitanje njegovog postojanja je svedeno na pitanje postojanja z. Prema tome, u prethodnoj formuli izostavljamo tu jednačinu, kao i deo $(\exists y \in \mathbb{R})$ na početku formule. Tako imamo

$$\begin{aligned}
&\Leftrightarrow \quad (\exists z \in \mathbb{R})((1-z)^3 = 2 - x \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0) \\
&\Leftrightarrow \quad (\exists z \in \mathbb{R})(z^3 - 3z^2 + 3z - x + 1 = 0 \wedge z^2 - x + 1 = 0 \wedge x - 1 \geq 0 \wedge z \geq 0) \\
&\Leftrightarrow \quad (\exists z \in \mathbb{R})(-3z^2 + z(x+2) - x + 1 = 0 \wedge z^2 - x + 1 = 0 \wedge x - 1 \geq 0 \wedge z \geq 0)
\end{aligned}$$

Pomnožili smo drugu jednačinu sa $-z$ i dodali prvoj, a sada ćemo drugu pomnožiti sa 3 i dodati prvoj

$$\Leftrightarrow \quad (\exists z \in \mathbb{R})(z(x+2) - 4(x-1) = 0 \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0)$$

U nameri da izbacimo z u prvoj jednačini ćemo razlikovati slučajeve $x + 2 = 0$, $x + 2 \neq 0$. U tu svrhu pridružujemo disjunkciju $x + 2 = 0 \vee x + 2 \neq 0$, „logički množimo” i koristimo svojstvo da se egzistencijalni kvantifikator „lepo slaže” sa disjunkcijom.

$$\begin{aligned}
&\Leftrightarrow \quad (\exists z \in \mathbb{R})(z(x+2) - 4(x-1) = 0 \wedge (x + 2 = 0 \vee x + 2 \neq 0) \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge \\
&\qquad \wedge z \geq 0) \\
&\Leftrightarrow \quad (\exists z \in \mathbb{R})((z(x+2) - 4(x-1) = 0 \wedge x + 2 = 0 \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0) \vee \\
&\qquad \vee (z(x+2) - 4(x-1) = 0 \wedge x + 2 \neq 0 \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0)) \\
&\Leftrightarrow \quad (\exists z \in \mathbb{R})(z(x+2) - 4(x-1) = 0 \wedge x + 2 = 0 \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0) \vee \\
&\qquad \vee (\exists z \in \mathbb{R})(z(x+2) - 4(x-1) = 0 \wedge x + 2 \neq 0 \wedge z^2 = x - 1 \wedge x - 1 \geq 0 \wedge z \geq 0)
\end{aligned}$$

[11]Detaljnije o zakonu zamene za jednakost se može čitati u [2].

Prva grana je nemoguća jer pored $x+2=0$ se pojavljuje i jednačina $x-1=0$. Dalje nastavljamo sa drugom granom. Naći ćemo z iz prve jednačine i onda iz ostalih izbaciti z.

$$\begin{aligned}
&\Leftrightarrow \quad (\exists z\in\mathbb{R})(z(x+2)-4(x-1)=0\wedge x+2\neq 0\wedge z^2=x-1\wedge x-1\geq 0\wedge z\geq 0)\\
&\Leftrightarrow \quad (\exists z\in\mathbb{R})(z=\frac{4(x-1)}{x+2}\wedge x+2\neq 0\wedge \frac{16(x-1)^2}{(x+2)^2}=x-1\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0)
\end{aligned}$$

Zahvaljujući nejednakosti $x+2\neq 0$ i jednakosti koja sadrži z pitanje postojanja z svedeno je na pitanje postojanja x. Zato izbacujemo z-jednakost i ne pišemo kvantifikator $(\exists z\in\mathbb{R})$. Eliminacijom pomoćnih promenljivih i odgovarajućih kvantifikatora dobili smo da je polazna iracionalna jednačina ekvivalentna dobijenoj formuli koja sadrži samo x.

$$\begin{aligned}
&\Leftrightarrow \quad 16(x-1)^2=(x+2)^2(x-1)\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0\\
&\Leftrightarrow \quad (x-1)(16(x-1)-(x+2)^2))=0\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0\\
&\Leftrightarrow \quad (x-1)(x-2)(x-10)=0\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0\\
&\Leftrightarrow \quad (x=1\vee x=2\vee x=10)\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0\\
&\Leftrightarrow \quad (x=1\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0)\vee\\
&\qquad\ \vee(x=2\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0)\vee\\
&\qquad\ \vee(x=10\wedge x+2\neq 0\wedge x-1\geq 0\wedge \frac{4(x-1)}{x+2}\geq 0)
\end{aligned}$$

Imamo tri grane. U svakoj na početku stoji po jedna jednakost koja određuje x. Te jednakosti prepisujemo i za svaku granu posebno koristimo zakon zamene za jednakost.

$$\begin{aligned}
&\Leftrightarrow \quad (x=1\wedge 1+2\neq 0\wedge 1-1\geq 0\wedge \frac{4(1-1)}{1+2}\geq 0)\vee\\
&\qquad\ \vee(x=2\wedge 2+2\neq 0\wedge 2-1\geq 0\wedge \frac{4(2-1)}{2+2}\geq 0)\vee\\
&\qquad\ \vee(x=10\wedge 10+2\neq 0\wedge 10-1\geq 0\wedge \frac{4(10-1)}{10+2}\geq 0)\\
&\Leftrightarrow \quad x=1\vee x=2\vee x=10
\end{aligned}$$

Rešenja su upravo brojevi 1, 2 i 10. ♦

Zadatak 2. *Rešiti po $x\in\mathbb{R}$ jednačinu $\sqrt{x+1}+\sqrt{2x+3}=1$.*

Rešenje. I ovaj zadatak rešićemo sličnom idejom, uvešćemo nove promenljive.

$$\begin{aligned}
\sqrt{x+1}+\sqrt{2x+3}=1 \quad &\Leftrightarrow \quad (\exists s\geq 0)(\exists t\geq 0)(x+1=s^2\wedge x+1\geq 0\wedge\\
&\qquad\ \wedge 2x+3=t^2\wedge 2x+3\geq 0\wedge s+t=1)\\
&\Leftrightarrow \quad (\exists s\geq 0)(\exists t\geq 0)(x+1=s^2\wedge x+1\geq 0\wedge 2x+3=t^2\wedge\\
&\qquad\ \wedge 2x+3\geq 0\wedge s=1-t)
\end{aligned}$$

Iskoristićemo jednakost $s = 1 - t$ u cilju izbacivanja s iz ostalih formula. Napomenimo da se mora dodati uslov $s \geq 0$ tj. uslov $1 - t \geq 0$. Nakon toga, slično prethodnom zadatku, formiraćemo ekvivalencijski lanac, gde ćemo se usput rešiti i kvantifikatora $(\exists t \geq 0)$ i na određenim mestima primeniti zakon zamene za jednakost:

$$
\begin{array}{ll}
\Leftrightarrow & (\exists t \geq 0)(x + 1 = (1 - t)^2 \wedge x + 1 \geq 0 \wedge 2x + 3 = t^2 \wedge 2x + 3 \geq 0 \wedge 1 - t \geq 0) \\
\Leftrightarrow & (\exists t \geq 0)(x + 1 = 1 - 2t + t^2 \wedge x + 1 \geq 0 \wedge 2x + 3 = t^2 \wedge 2x + 3 \geq 0 \wedge t \leq 1) \\
\Leftrightarrow & (\exists t \geq 0)(x + 1 = 1 - 2t + 2x + 3 \wedge x + 1 \geq 0 \wedge 2x + 3 = t^2 \wedge 2x + 3 \geq 0 \wedge t \leq 1) \\
\Leftrightarrow & (\exists t \geq 0)(2t = x + 3 \wedge x + 1 \geq 0 \wedge 2x + 3 = t^2 \wedge 2x + 3 \geq 0 \wedge t \leq 1) \\
\Leftrightarrow & (\exists t \geq 0)(t = \dfrac{x+3}{2} \wedge x + 1 \geq 0 \wedge 2x + 3 = t^2 \wedge 2x + 3 \geq 0 \wedge t \leq 1) \\
\Leftrightarrow & (\exists t \geq 0)(t = \dfrac{x+3}{2} \wedge x + 1 \geq 0 \wedge 2x + 3 = \dfrac{(x+3)^2}{4} \wedge 2x + 3 \geq 0 \wedge t \leq 1) \\
\Leftrightarrow & (x + 3)^2 = 4(2x + 3) \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & x^2 + 6x + 9 = 8x + 12 \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & x^2 - 2x - 3 = 0 \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & (x + 1)(x - 3) = 0 \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & (x + 1 = 0 \vee x - 3 = 0) \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & (x = -1 \vee x = 3) \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & (x = -1 \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \vee \\
 & \vee (x = 3 \wedge x + 1 \geq 0 \wedge 2x + 3 \geq 0 \wedge \dfrac{x+3}{2} \leq 1) \\
\Leftrightarrow & (x = -1 \wedge -1 + 1 \geq 0 \wedge 2 \cdot (-1) + 3 \geq 0 \wedge \dfrac{-1+3}{2} \leq 1) \vee \\
 & \vee (x = 3 \wedge 3 + 1 \geq 0 \wedge 2 \cdot 3 + 3 \geq 0 \wedge \dfrac{3+3}{2} \leq 1)
\end{array}
$$

Kako nejednakost $\dfrac{3+3}{2} \leq 1$ nije tačna, dobijamo da je cela druga grana nemoguća.

$$
\begin{array}{ll}
\Leftrightarrow & x = -1 \vee \perp \\
\Leftrightarrow & x = -1
\end{array}
$$

Dakle, jedino rešenje polazne jednačine je broj -1. ♦

Zadatak 3. *Dokazati ekvivalenciju*

$$(\exists x \geq 0) x^2 + 2px + q = 0 \Leftrightarrow q \leq 0 \vee (q > 0 \wedge p < 0 \wedge p^2 - q \geq 0)$$

gde su p, q realni parametri.

Rešenje. Pravimo ekvivalencijski lanac

$$
\begin{aligned}
(\exists x \geq 0) x^2 + 2px + q = 0 \quad &\Leftrightarrow \quad (\exists x \geq 0)(x+p)^2 = p^2 - q \\
&\Leftrightarrow \quad (\exists x \geq 0)(x+p)^2 = p^2 - q \wedge p^2 - q \geq 0 \\
&\Leftrightarrow \quad (\exists x \geq 0)((x = -p + \sqrt{p^2 - q} \vee x = -p - \sqrt{p^2 - q}) \wedge p^2 - q \geq 0) \\
&\Leftrightarrow \quad ((-p + \sqrt{p^2 - q} \geq 0 \vee -p - \sqrt{p^2 - q} \geq 0) \wedge p^2 - q \geq 0) \\
&\Leftrightarrow \quad \sqrt{p^2 - q} \geq p \wedge p^2 - q \geq 0
\end{aligned}
$$

Napomenimo da je poslednja ekvivalencija posledica nejednakosti $-p + \sqrt{p^2 - q} \geq -p - \sqrt{p^2 - q}$. Sada nam je namera da se oslobodimo korena tj. da kvadriramo obe strane. Da bismo to učinili nepokvarivši ekvivalencijski lanac, moramo pridružiti disjunkciju $p \geq 0 \vee p < 0$.

$$
\begin{aligned}
&\Leftrightarrow \quad \sqrt{p^2 - q} \geq p \wedge (p \geq 0 \vee p < 0) \wedge p^2 - q \geq 0 \\
&\Leftrightarrow \quad (\sqrt{p^2 - q} \geq p \wedge p \geq 0 \wedge p^2 - q \geq 0) \vee (\sqrt{p^2 - q} \geq p \wedge p < 0 \wedge p^2 - q \geq 0)
\end{aligned}
$$

U prvoj grani ćemo se osloboditi korena, a drugu svesti na $p < 0 \wedge p^2 - q \geq 0$ jer taj deo povlači nejednakost $\sqrt{p^2 - q} \geq p$.

$$
\begin{aligned}
&\Leftrightarrow \quad (p^2 - q \geq p^2 \wedge p \geq 0 \wedge p^2 - q \geq 0) \vee (p < 0 \wedge p^2 - q \geq 0) \\
&\Leftrightarrow \quad (q \leq 0 \wedge p \geq 0 \wedge p^2 - q \geq 0) \vee (p < 0 \wedge p^2 - q \geq 0) \\
&\Leftrightarrow \quad (q \leq 0 \wedge p \geq 0) \vee (p < 0 \wedge p^2 - q \geq 0)
\end{aligned}
$$

Lako se proverava, razlikovanjem dva slučaja $q \leq 0$ i $q > 0$, da je desna strana ekvivalentna sa

$$
\Leftrightarrow \quad q \leq 0 \vee (q > 0 \wedge p < 0 \wedge p^2 - q \geq 0)
$$

pa taj deo ovde nećemo ispisivati. ♦

Za kraj rešićemo jedan od zadataka iz analitičke geometrije primenom eliminacije kvantifikatora. U pitanju je zadatak sa određivanjem geometrijskog mesta tačaka.

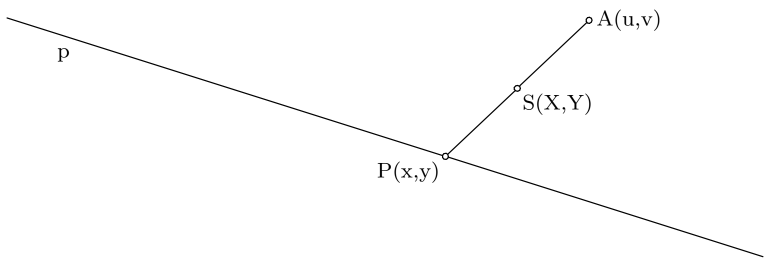
Zadatak 4. *Date su prava p i tačka A. Odrediti geometrijsko mesto tačaka S koje nastaju kao središta duži AP, kad tačka P „ide" po pravoj p.*

Rešenje. Neka prava p ima jednačinu $ax + by + c = 0$, gde su a, b, c zadani realni brojevi, ne svi jednaki 0 tj. $a^2 + b^2 + c^2 \neq 0$. Tačka $A(u, v)$ ne pripada toj pravoj, pa važi $au + bv + c \neq 0$. Označimo sa $S(X, Y)$ središte duži SP, kad „tačka P ide po pravoj p". Stavili smo te reči pod navodnike jer ne odgovaraju uobičajenom strogom izražavanju.
Označimo sa S_k skup svih tako nastalih tačaka S. Tada jedno određenje skupa S_k u duhu rečenog glasi:

$(X, Y) \in S_k$ akko (X, Y) je središte duži AP, pri čemu tačka P „ide" po pravoj p.

Upotrebom egzistencijalnog kvantifikatora taj zapis se može ovako prevesti

$$
(X, Y) \in S_k \Leftrightarrow \exists x \exists y (ax + by + c = 0 \wedge X = \frac{x + u}{2} \wedge Y = \frac{y + v}{2}).
$$



Sada nas čeka zadatak izbacivanja kvantifikatora iz desne „polovine” ekvivalencije. Iz poslednje dve jednačine naći ćemo x i y i zameniti u prvu jednačinu:

$$\begin{array}{ll}\Leftrightarrow & \exists x \exists y (ax + by + c = 0 \wedge x = 2X - u \wedge y = 2Y - v) \\ \Leftrightarrow & \exists x \exists y (x = 2X - u \wedge y = 2Y - v \wedge a(2X - u) + b(2Y - v) + c = 0) \\ \Leftrightarrow & \exists x \exists y (x = 2X - u \wedge y = 2Y - v) \wedge a(2X - u) + b(2Y - v) + c = 0\end{array}$$

Kako je deo $\exists x \exists y (x = 2X - u \wedge y = 2Y - v)$ tačan onda se ekvivalencijski lanac nastavlja sa

$$\begin{array}{ll}\Leftrightarrow & a(2X - u) + b(2Y - v) + c = 0 \\ \Leftrightarrow & 2aX + 2bY + (-au - bv + c) = 0\end{array}$$

Stigli smo do eliminante, koja predstavlja traženo geometrijsko mesto tačaka. Lako zaključujemo da je traženo geometrijsko mesto tačaka - prava. ⧫

8 Zaključak

U ovom radu je prikazan metod eliminacije kvantifikatora sa posebnim osvrtom na tri teorije: teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka, teoriju algebarski zatvorenih polja i teoriju realno zatvorenih polja. Ovaj metod igra veoma važnu ulogu u matematičkoj logici, posebno pri dokazivanju nekih model-teoretskih svojstava, kao što su odlučivost i kompletnost. Takođe, veliku ulogu ima i u teorijskom računarstvu, gde se najviše primenjuje u vezi sa raznim procedurama odlučivanja, koje se kasnije povezuju sa pojmom izračunljivosti.

U ovom radu, eliminacija kvantifikatora nije razmatrana u vezi sa svojstvom kompletnosti neke teorije. Akcenat je bio samo na vezi sa odlučivošću teorije. Razlog tome je što ovaj metod osim odgovora na pitanje da li je neka teorija odlučiva ili ne tj. odgovora na pitanje da li za svaku formulu možemo utvrditi jeste li ili nije teorema date teorije, daje i samu proceduru odlučivanja, što se smatra vrlo korisnom posledicom.

Kako postoji dosta razvijena matematička teorija koja se bavi baš eliminacijom kvantifikatora, u trećem poglavlju naveden je i dokazan primer jednog od mnogih kriterijuma za utvrđivanje da li data teorija dopušta eliminaciju kvantifikatora.

U odeljku Furije-Mockinova procedura dat je glavni primer primene metoda eliminacije kvantifikatora u teoriji gustih uređenih Abelovih grupa bez krajnjih tačaka, pri čemu se u zadacima kao primer modela pojavljuje struktura $(\mathbb{R}, +, -, 0, <)$. U vezi sa teorijom algebarski zatvorenih polja pomenuta su dva načina pomoću kojih se može izvršiti eliminacija kvantifikatora. Jedan od njih koristi pojam rezlovente dva polinoma, a drugi NZD za dva polinoma. Takođe, u delu rada koji se odnosi na teoriju realno zatvorenih polja, videli smo kao primer upotrebu diskriminante pri eliminaciji egzistencijalnog kvantifikatora iz kvadratne jednačine.

Najbolji pokazatelj primene metode eliminacije kvantifikatora, ali i primene tautologija, valjanih formula i Furije-Mockinove procedure, jesu mnogobrojni zadaci i primeri prikazani u ovom radu. Neki od njih su posebno razmatrani, sa logičkog aspekta, čemu su bila posvećena dva poglavlja, drugo i sedmo. Takvo sagledavanje i način rešavanja su, vrlo korisni i precizni, ali, nažalost, u maloj meri zastupljeni u srednjoškolskoj nastavi.

Literatura

[1] Milan Božić, Slobodan Vujić, Matematička logika sa elementima opšte logike za III razred srednjeg usmerenog obrazovanja, Naučna knjiga, Beograd, 1979.

[2] Slaviša B. Prešić, Raznice I, Prosvetni pregled, Beograd, 1997.

[3] Milivoje Lazić, Logika u nastavi matematike, Akademska misao, 2003.

[4] Žarko Mijajlović, Zoran Marković, Kosta Došen, Hilbertovi problemi i logika, Zavod za udžbenike i nastavna sredstva, Beograd, 1986.

[5] Predrag Janičić, Matematička logika u računarstvu, četvrto elektronsko izdanje, Beograd, 2008. (preuzeto sa sajta http://www.matf.bg.ac.rs/∼janicic)

[6] Nebojša Ikodinović, Uvod u matematičku logiku, Beograd, 2014. (preuzeto sa sajta http://www.matf.bg.ac.rs/p/nebojsa-ikodinovic/cas/1191/uml—skripta/)

[7] http://web.math.pmf.unizg.hr/∼vukovic/Skripte/APPLOG-skripta-2011.pdf, pristupljeno 01.08.2014.

[8] Miodrag Rašković, Nebojša Ikodinović, Priče o malim i velikim brojevima, Zavod za udžbenike, Beograd, 2010.

[9] http://en.wikipedia.org/wiki/Decidability_(logic), pristupljeno 10.08.2014.

[10] http://en.wikipedia.org/wiki/Quantifier_elimination, pristupljeno 10.08.2014.

[11] In B. H. Matzat,G.-M. Greuel and G. Hiss, editors, Algorithmic Algebra and Number Theory, Springer, Berlin, 1998.

[12] Volker Weispfenning, Quantifier elimination for real algebra - the quadratic case and beyond, Appl. Algebra Eng. Commun. Comput, 8(2):85101, 1997.