Matematička teorija računarstva

M. Klaričić Bakula

Split, 2009/10.

Sadržaj

Uvod

DODATI UVOD!

.....

Poglavlje 1.

Osnove matematičke logike

1.1. Logika sudova

1.1.1. Uvod

Jedan od osnovnih problema u matematičkoj logici je ispitati istinitost neke rečenice (logičke forme) i to promatrajući samo njen oblik, a ne i sadržaj. Logika sudova, ili propozicijska logika, je jedna od najjednostavnijih formalnih teorija. U njoj rečenice promatramo kao forme sastavljene od "atomarnih" djelova koji su povezani veznicima: *ne*, *i*, *ili*, *ako...onda* i *ako i samo ako* (pišemo *akko*).

Podsjetimo se: sud je svaka suvisla izjavna rečenica koja je istinita ili lažna, ali ne oboje. Ovo svakako ne može biti definicija suda, jer se može postaviti pitanje što je rečenica, ili pak što je istinita rečenica. Pogledajmo nekoliko primjera.

1. Rečenica "Dva plus dva je jednako četiri." jest sud, i to istinit.
2. Rečenica "Dva plus dva je jednako pet." jest sud, i to lažan.
3. Rečenica "x plus dva je jednako osam." nije sud, jer za nju ne možemo reći je li istinita ili lažna dok ne znamo koliko je x.
4. Rečenica "Koliko je sati?" nije sud, jer nije izjavna rečenica.

Sudovi (1) i (2) su jednostavnog oblika, tj. atomarni su. Pomoću veznika *ne*, *i*, *ili*, *ako...onda* i *ako i samo ako* iz jednostavnih sudova možemo graditi složenije sudove. Na primjer rečenica "Ako pada kiša, onda nosim kišobran." je primjer složenog suda.

U logici sudova proučavamo i logička zaključivanja, te određujemo koja su korektna, a koja nisu. Promotrimo neke primjere. Zaključivanje:

$$\frac{\begin{array}{c}\text{Ako pada kiša, onda nosim kišobran.}\\ \text{Pada kiša.}\end{array}}{\text{Nosim kišobran.}}$$

je primjer korektnog zaključivanja. Formalno zapisano, ono je oblika

$$\frac{\begin{array}{c}A \longrightarrow B\\ A\end{array}}{B}_1 \quad ,$$

a nazivamo ga *modus ponens*.

No zaključivanje:

$$\frac{\begin{array}{c}\text{U nedjelju ću ići u kino.}\\ \text{Danas nije nedjelja.}\end{array}}{\text{Danas ne idem u kino.}}$$

nije korektno. Formalno ga zapisujemo kao

$$\frac{\begin{array}{c}A \longrightarrow B\\ -A\end{array}}{-B} \quad .$$

Dakle, važno je razlučiti koje je zaključivanje korektno, odnosno što je logička posljedica.

Formalno matematičko zaključivanje čini se sitničavim ako ga usporedimo s dokazivanjem u svakodnevnoj praksi u kojoj je intuitivna matematička mjera strogosti najčešće dovoljna. Međutim u slučajevima sumnje ili spora valja pribjeći većoj strogosti.

Ovo je poglavlje, uz manje izmjene, preuzeto iz [3].

1.1.2. Jezik logike sudova

Sada ćemo definirati koji su osnovni znakovi logike sudova i kako gradimo formule: kada je to zadano smatramo da je zadan jezik teorije. No prije definicije formula uvest ćemo još neke pojmove.

Skup je osnovni pojam u matematici koga je nemoguće definirati uz pomoć jednostavnijih pojmova, no intuitivno je jasno što podrazumijevamo pod pojmom "skup". Možemo reći da je to "množina", "mnoštvo", "kolekcija", "familija" ili slično. Skupovima ćemo se više baviti u sljedećem poglavlju.

Abeceda ili *alfabet* je proizvoljan neprazan skup. Svaki element abecede je *simbol* ili *znak*. *Riječ* u nekoj abecedi je bilo koji konačan niz znakova iz dane abecede. Ako je A neka abeceda, onda s A^* označavamo skup svih riječi u abecedi A. Po dogovoru smatramo da skup svih riječi proizvoljne abecede sadrži praznu riječ ε. Najvažnija operacija na skupu riječi je *konkatenacija*: ako su a i b oznake za riječi, onda kažemo da je riječ ab nastala konkatenacijom riječi a i b.

Primjer 1. *Neka je* $A = \{\alpha, \beta\}$. *Tada riječi* $\alpha\alpha\beta\alpha$ *i* $\beta\alpha\beta\beta\alpha$ *pripadaju skupu* A^*. *Njihovom konkatenacijom možemo dobiti riječ* $\alpha\alpha\beta\alpha\beta\alpha\beta\beta\alpha$ *koja je također u skupu* A^*.

Abeceda $\mathcal{A}$ logike prvog reda je unija skupova A_1, A_2, A_3, gdje je:

1. $A_1 = \{P_0, P_1, P_2, \ldots\}$ skup čije elemente nazivamo propozicijskim varijablama
2. $A_2 = \{-, \wedge, \vee, \longrightarrow, \longleftrightarrow\}$ skup čije elemente nazivamo logičkim veznicima
3. $A_3 = \{(\ ,\ )\}$ skup čije elemente nazivamo pomočnim simbolima.

Logičke veznike nazivamo redom: *negacija* $(-)$, *konjukcija* $(\wedge)$, *disjunkcija* $(\vee)$, *kondicional* $(\longrightarrow)$ i *bikondicional* $(\longleftrightarrow)$.

Sada ćemo definirati najvažnije riječi abecede logike sudova, a to su formule.

Definicija 1.1.1. *Atomarna formula je svaka propozicijska varijabla. Formula je definirana sljedećim:*

a) svaka atomarna formula je formula

b) ako su A i B formule, onda su i riječi $(-A)$, $(A \wedge B)$, $(A \vee B)$, $(A \longrightarrow B)$ i $(A \longleftrightarrow B)$ formule

c) riječ abecede logike sudova je formula ako i samo ako je nastala primjenom konačno mnogo koraka pravila a) i b).

Primjedba 1.1.1. *Općenito ćemo formule označavati velikim latiničnim slovima s početka abecede (A, B, C, F, G,...), dok ćemo za propozicijske varijable koristiti velika latinična slova s kraja abecede (P, Q, R, S, V,...).*

Da bismo izbjegli pisanje velikog broja zagrada uvest ćemo prioritet logičkih veznika: najveći prioritet ima negacija, zatim konjukcija i disjunkcija, a najmanji prioritet imaju kondicional i bikondicional. Na primjer, formulu $(((-P) \wedge Q) \longrightarrow R)$ pišemo kao $(-P \wedge Q) \longrightarrow R$.

1.1.3. Semantika

Svako preslikavanje sa skupa propozicijskih varijabli u skup $\{0, 1\}$ nazivamo interpretacijom. Po složenosti formule definiramo interpretacije na proizvoljnim formulama u skladu s danom semantičkom tablicom:

P	Q	$-P$	$P \wedge Q$	$P \vee Q$	$P \longrightarrow Q$	$P \longleftrightarrow Q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Ako je vrijednost interpretacije I na formuli F jednaka 1, tj. $I(F) = 1$, onda kažemo da je formula F istinita za interpretaciju I. Ako je vrijednost interpretacije I na formuli F jednaka 0, tj. $I(F) = 0$, onda kažemo da je formula F neistinita za interpretaciju I.

Primjer 2. *Neka je $I(P) = I(Q) = 0$ i $I(R) = 1$. Odredimo $I(F)$, gdje je $F \equiv (-P \vee Q) \longrightarrow -R$.*

P	Q	R	$-P$	$-P \vee Q$	$-R$	$(-P \vee Q) \longrightarrow -R$
0	0	1	1	1	0	0

Dakle, $I(F) = 0$. Očito $I(F)$ ovisi o $I(P)$, $I(Q)$ i $I(R)$, pa bi za neke druge vrijednosti $I(P)$, $I(Q)$ i $I(R)$ imali različitu vrijednost $I(F)$. Pogledajmo sve moguće

interpretacije:

P	Q	R	$-P$	$-P \vee Q$	$-R$	$(-P \vee Q) \longrightarrow -R$
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	1	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	1
1	0	1	0	0	0	1
1	1	0	0	1	1	1
1	1	1	0	1	0	0

Primijetimo da smo ovakvom tablicom formuli F pridružili funkciju sa skupa $\{0,1\}^3$ *na skup* $\{0,1\}$. *Takvu funkciju nazivamo* istinosnom funkcijom.

Definicija 1.1.2. *Za formulu F kažemo da je ispunjiva, odnosno oboriva, ako postoji interpretacija I za koju je $I(F) = 1$, odnosno $I(F) = 0$.*
Za formulu F kažemo da je valjana (tautologija) ako je istinita za svaku interpretaciju.
Za formulu F kažemo da je antitautologija ako je neistinita za svaku interpretaciju.

Uočimo da su valjane formule upravo one formule koje su istinite bez obzira na istinitost svojih atomarnih djelova. Sada ćemo navesti neke važne formule koje su valjane.

1. $--P \longleftrightarrow P$, princip dvojne negacije
2. $P \vee -P$, princip isključenja trećeg
3. $-(P \wedge -P)$, princip neproturječnosti
4. $(P \longrightarrow Q) \longleftrightarrow (-Q \longrightarrow -P)$, princip kontrapozicije
5. $-P \longrightarrow (P \longrightarrow Q)$, princip negacije premise
6. $-(P \vee Q) \longleftrightarrow -P \wedge -Q$, De Morganov princip
7. $-(P \wedge Q) \longleftrightarrow -P \vee -Q$, De Morganov princip.

1.1.4. Logička implikacija

Definicija 1.1.3. *Kažemo da formula B logički slijedi iz formule A (ili da A logički implicira B), i pišemo $A \Rightarrow B$, ako za svaku interpretaciju I za koju je $I(A) = 1$ vrijedi $I(B) = 1$.*

Definicija 1.1.4. *Kažemo da su formule A i B logički ekvivalentne, i pišemo $A \Leftrightarrow B$, ako za svaku interpretaciju I vrijedi $I(A) = I(B)$.*

Nije teško vidjeti da za proizvoljne formule A i B vrijedi

$$A \Rightarrow B \text{ ako i samo ako je } A \longrightarrow B \text{ valjana formula.}$$

Drugim riječima, implikacija se može svesti na valjanost kondicionala. Analogno,

$$A \Leftrightarrow B \text{ ako i samo ako je } A \longleftrightarrow B \text{ valjana formula,}$$

tj. ekvivalencija se može svesti na valjanost bikondicionala.

Lako je provjeriti da vrijedi:

1. Svaka formula implicira samu sebe.
2. Ako $A \Rightarrow B$ i $B \Rightarrow C$, onda $A \Rightarrow C$. (*hipotetički silogizam*)
3. Antitautologija implicira svaku formulu, a logički slijedi samo iz antitautologije.
4. Valjana formula logički slijedi iz svake formule, a implicira samo valjane formule.
5. Logička ekvivalencija je uzajamna implikacija ($A \Leftrightarrow B$ akko $A \Rightarrow B$ i $B \Rightarrow A$).
6. Svaka formula je logički ekvivalentna samoj sebi.
7. Ako je $A \Leftrightarrow B$, onda je $B \Leftrightarrow A$.
8. Ako je $A \Leftrightarrow B$ i $B \Leftrightarrow C$, onda je $A \Leftrightarrow C$.
9. Valjane formule su sve međusobno logički ekvivalentne.
10. Antitautologije su sve međusobno logički ekvivalentne.

Kao što smo vidjeli, logička implikacija je usko vezana uz kondicional. To je dovelo do tendencije da se "implicira" koristi za čitanje znaka " $\longrightarrow$ " za kondicional, što nikako nije ispravno! Naime, kada kažemo da jedna formula implicira drugu izričemo određenu tvrdnju o tim formulama, a kada među njima stavimo znak " $\longrightarrow$ " gradimo složeniju formulu. Slično vrijedi i za logičku ekvivalenciju i znak " $\longleftrightarrow$ ".

Pogledajmo sada u kakvoj su vezi logička implikacija i dokaz nekog matematičkog teorema s pretpostavkom P i tvrdnjom Q. U logičkoj notaciji to možemo pisati kao $P \Rightarrow Q$. Uz ovo su vezana sljedeća tri suda:

1. $Q \Rightarrow P$ (obrat suda)
2. $-Q \Rightarrow -P$ (obrat suda po kontrapoziciji)
3. $-P \Rightarrow -Q$ (suprotni sud).

Zanima nas kakva je veza među njima? Podsjetimo se da $P \Rightarrow Q$ ako i samo ako je $P \longrightarrow Q$ valjana formula, pa možemo ispitati njihovu vezu pomoću semantičke tablice.

P	Q	$P \longrightarrow Q$	$-P \longrightarrow -Q$	$Q \longrightarrow P$	$-Q \longrightarrow -P$
0	0	1	1	1	1
0	1	1	0	0	1
1	0	0	1	1	0
1	1	1	1	1	1

Zaključujemo:

1. P logički implicira Q ako i samo ako $-Q$ logički implicira $-P$.
2. Ako P logički implicira Q, onda ne mora Q logički implicirati P.
3. Ako P logički implicira Q, onda ne mora $-P$ logički implicirati $-Q$.

Upravo zbog 1) možemo provoditi dokaz obratom po kontrapoziciji.

1.2. Logika prvog reda

1.2.1. Uvod

U prethodnom poglavlju proučavali smo klasičnu logiku sudova, no u njoj ne možemo izraziti mnoga logička zaključivanja koja koristimo u svakodnevnom životu. Pogledajmo jedan primjer.

$$\frac{\begin{array}{c}\text{Svi ljudi su smrtni.}\\ \text{Grci su ljudi.}\end{array}}{\text{Grci su smrtni.}}$$

Lako je vidjeti da ovo jednostavno zaključivanje ne možemo opisati formulama logike sudova, već moramo u obzir uzeti i sadržaj rečenica (što ne želimo!).

Označimo redom predikate:

$$\begin{aligned} &C(x) \ldots \text{"}x \text{ je čovjek"},\\ &S(x) \ldots \text{"}x \text{ je smrtan"},\\ &G(x) \ldots \text{"}x \text{ je Grk"}. \end{aligned}$$

U tom slučaju gornji primjer možemo zapisati u obliku:

$$\frac{\begin{array}{c}\forall x\,(C(x) \longrightarrow S(x))\\ \forall x\,(G(x) \longrightarrow C(x))\end{array}}{\forall x\,(G(x) \longrightarrow S(x))}$$

sljedeći primjer bio je nerješiv za srednjovjekovne logičare. Pomoću Aristotelovih silogizama nisu uspjevali zapisati ovo očito valjano zaključivanje.

$$\frac{\text{Sve elipse su krivulje.}}{\text{Svatko tko crta elipsu crta krivulju.}}$$

Uvedemo li opet oznake

$$\begin{aligned} &E(x) \ldots \text{"}x \text{ je elipsa"},\\ &K(x) \ldots \text{"}x \text{ je krivulja"},\\ &C(x,y) \ldots \text{"}y \text{ crta } x\text{"}, \end{aligned}$$

onda gornji primjer možemo pisati kao

$$\frac{\forall x\,(E\,(x) \longrightarrow K\,(x))}{\forall y\,(C\,(x,y) \wedge E\,(x) \longrightarrow C\,(x,y) \wedge K\,(x))}$$

Logika sudova ne može formalno zapisati ni neke jednostavne matematičke pojmove. Jedan takav primjer je pojam neprekidnosti u točki. Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ neprekidna u točki x_0. Tada je istinita formula

$$\forall\varepsilon\exists\delta\forall x\,(|x - x_0| < \delta \longrightarrow |f\,(x) - f\,(x_0)| < \varepsilon)\,.$$

Negacija gornje formule, tj. formula

$$-\forall\varepsilon\exists\delta\forall x\,(|x - x_0| < \delta \longrightarrow |f\,(x) - f\,(x_0)| < \varepsilon)$$

je formalni zapis činjenice da funkcija f ima prekid u točki x_0. Primjenom pravila prijelaza za kvantifikatore dobivamo

$$\exists\varepsilon\forall\delta\exists x\,(|x - x_0| < \delta \wedge |f\,(x) - f\,(x_0)| \geq \varepsilon)\,.$$

Važno je uočiti da u prethodnim primjerima istinitost zaključaka ne ovisi o istinitosti dijelova koji su dobiveni samo rastavljanjem s obzirom na logičke veznike. To znači da za opis ovakvih zaključivanja moramo prije svega usvojiti širi jezik.

Ovako dobivena logika, koju nazivamo *logikom prvog reda* ili *predikatnom logikom*, ima veću izražajnu moć, no gubi neka dobra svojstva logike sudova, a tu prije svega mislimo na odlučivost. Za svaku formulu logike sudova možemo u konačno mnogo koraka provjeriti je li valjana, no to nije moguće za formule logike prvog reda.

1.2.2. Jezik logike prvog reda

Abeceda $\mathcal{A}$ logike prvog reda je unija skupova $A_1,\ldots,A_6$, gdje je:

1. $A_1 = \{v_0, v_1, v_2, \ldots\}$ prebrojiv skup čije elemente nazivamo individualnim varijablama
2. $A_2 = \{-, \wedge, \vee, \longrightarrow, \longleftrightarrow, \forall, \exists\}$ skup logičkih veznika
3. $A_3 = \{R_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo relacijskim simbolima (predikatima)
4. $A_4 = \{f_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo funkcijskim simbolima
5. $A_5 = \{c_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo konstantskim simbolima
6. $A_6 = \{(\ ,\ )\}$ skup čije elemente nazivamo pomoćnim simbolima.

Veznik $\forall$ nazivamo *univerzalnim kvantifikatorom* i čitamo ga "za svaki", dok veznik $\exists$ nazivamo *egzistencijalnim kvantifikatorom* i čitamo ga "postoji (neki)". Smatramo da je za svaki od relacijskih i funkcijskih simbola poznato kolika im je mjesnost. Na primjer, dvomjesni funkcijski simbol se interpretira kao funkcija dvije varijable.

Definicija 1.2.1. *Term je riječ dane abecede $\mathcal{A}$ za koju vrijedi:*

a) svaka individualna varijabla i svaki konstantski simbol iz $\mathcal{A}$ je term

b) ako je f n-mjesni funkcijski simbol iz $\mathcal{A}$ i $t_1, \ldots, t_n$ termi, onda je i $f(t_1, \ldots, t_n)$ term

c) riječ abecede $\mathcal{A}$ je term ako i samo ako je nastala primjenom konačno mnogo koraka pravila a) i b).

Na primjer, uzmimo $\{\ln, \sin, \exp\} \subset A_4$, $\{v_1, x\} \subset A_1$ i $c_3 \in A_5$. Sljedeće su riječi termi: c_3, x, $\ln x$, $\exp(\sin v_1)$, $\ln(\exp(\sin c_3))$.

Definicija 1.2.2. *Ako je R n-mjesni relacijski simbol iz $\mathcal{A}$ i $t_1, \ldots, t_n$ termi, onda je $R(t_1, \ldots, t_n)$ atomarna formula abecede $\mathcal{A}$. Formula u abecedi $\mathcal{A}$ je definirana sljedećim:*

a) svaka atomarna formula je formula

b) ako su A i B formule, onda su i riječi $(-A)$, $(A \wedge B)$, $(A \vee B)$, $(A \longrightarrow B)$ i $(A \longleftrightarrow B)$ formule

c) ako je A formula i x varijabla, onda su riječi $(\forall x A)$ i $(\exists x A)$ formule

d) riječ abecede $\mathcal{A}$ je formula ako i samo ako je nastala primjenom konačno mnogo koraka pravila a), b) i c).

Primjedba 1.2.1. *Uobičajeno je umjesto $\exists x (x \in S \wedge P(x))$ pisati $(\exists x \in S) P(x)$, a umjesto $\forall x (x \in S \longrightarrow P(x))$ analogno pišemo $(\forall x \in S) P(x)$. Također, umjesto $\exists x (P(x) \wedge \forall y (P(y) \longrightarrow y = x))$ pišemo $\exists! x P(x)$. Dakle, treba uvijek voditi računa o tomu da se radi samo o uvriježenim zapisima.*

Pogledajmo jedan primjer: neka je R dvomjesni relacijski simbol koji interpretiramo kao "*biti jednak*" na skupu realnih brojeva $\mathbb{R}$. Na primjer, $R(x, y)$ bismo čitali "x *je jednak* y",a $R(x, 2)$ bismo čitali "x *je jednak* 2". Također, $R(1, 3)$ bismo čitali "1 *je jednako* 3", i to bi (za razliku od prethodna dva primjera) bio sud, i to lažan. "x *je jednak* 2" nije sud jer ne možemo utvrditi da li je ova izjavna rečenica istinita ili lažna, a isto vrijedi i za izjavnu rečenicu "x *je jednak* y". No uvođenjem odgovarajučeg broja kvantifikatora u gradnju formule kojoj je podformula $R(t_1, t_2)$, dobit ćemo sudove. Na primjer, formula

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) R(x, y)$$

je neistina, dok su formule

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R}) R(x, y),$$

$$(\exists x \in \mathbb{R}) R(x, 2)$$

istine. Ovo su bili primjeri *zatvorenih* formula, tj. formula kod kojih su sve varijable vezane kvantifikatorima, no definicija formule dozvoljava i *otvorene* formule, tj. formule kod kojih nisu sve varijable vezane kvantifikatorima. Jedna takva bi bila

$$(\forall x \in \mathbb{R}) R(x, y).$$

Slično kao prije poštivat ćemo prioritet logičkih veznika, s tim što sada veznici $\forall$ i $\exists$ imaju najveći i međusobno jednak prioritet.

Pogledajmo još neke primjere korektnih formula:

1. $(\forall x \in \mathbb{R})\, x \geq 0$ (ovaj sud je lažan)
2. $(\exists x \in \mathbb{N})\, x$ je paran (ovaj sud je istinit)
3. $(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\, y \geq x$ (ovaj sud je istinit).

Posebnu pažnju treba posvetiti negaciji kvantifikatora. Lako se vidi da vrijedi:

1. $-\forall x A \Leftrightarrow \exists x\,(-A)$
2. $-\exists x A \Leftrightarrow \forall x\,(-A)\,.$

Pogledajmo u nekoliko primjera kako se provodi negacija formula koje sadrže kvantifikatore:

1. $-\forall x \forall y\,(P\,(x,y) \longrightarrow R\,(x,y)) \Leftrightarrow \exists x \exists y\,(P\,(x,y) \wedge -R\,(x,y))$
2. $-\,(\forall x \in A)\,(\forall y \in A)\,(x \neq y \longrightarrow f\,(x) \neq f\,(y))$
   $\Leftrightarrow (\exists x \in A)\,(\exists y \in A)\,(x \neq y \wedge f\,(x) = f\,(y))$
3. $-\,(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\;\; x^2 + y^2 \geq 0 \Leftrightarrow (\exists x \in \mathbb{R})\,(\exists y \in \mathbb{R})\;\; x^2 + y^2 < 0.$

Ovo je poglavlje, uz manje izmjene, preuzeto iz [3].

Poglavlje 2.

Skupovi

2.1. Osnovni pojmovi

Skup je osnovni matematički pojam koga je nemoguće definirati pomoću jednostavnijih pojmova, no intuitivno je jasno što podrazumijevamo pod pojmom "skup". Možemo reći da je to "množina", "mnoštvo", "kolekcija", "familija" ili slično, no time nismo rekli ništa novo, već smo samo koristili sinonime. Matematička disciplina koja se bavi skupovima zove se *teorija skupova*. Njen osnivač *Georg Cantor* o skupu je rekao sljedeće:

"Skup je mnoštvo koje shvaćamo kao jedno."

Dakle, skup možemo smatrati cjelinom sastavljenom od za tu cjelinu osnovnih dijelova koje nazivamo *elementima* tog skupa. Intuitivno pretpostavljamo da postoji određeni odnos između skupa i njegovih elemenata. I ne samo to, za svaki objekt možemo reći pripada li nekom skupu ili ne. Skupove ćemo u matematici najčešće označavati velikim latiničnim slovima $A, B, C, X, Y, \ldots$, a njihove elemente malim latiničnim slovima $a,\ b,\ c,\ x,\ y,\ \ldots$

Pojam "*biti element skupa*" je također osnovni matematički pojam. Činjenicu da je x element skupa S zapisujemo kao $x \in S$ i čitamo "x *je element skupa* S" ili "x *pripada skupu* S". Slično, činjenicu da y nije element skupa S zapisujemo kao $y \notin S$ i čitamo "y *nije element skupa* S" ili "y *ne pripada skupu* S". Na primjer, označimo li sa S skup svih riba u Jadranskom moru, onda vrijedi: tunj $\in S$, pirana $\notin S$, srdela $\in S$.

Definirajmo sada neke jednostavne pojmove vezane uz skupove.

Definicija 2.1.1. *Neka su A i B skupovi. Ako je svaki element skupa A ujedno i element skupa B, onda kažemo da je skup A podskup skupa B (ili da je skup A sadržan u skupu B) i pišemo $A \subseteq B$. Kažemo još i da je skup B nadskup skupa A (ili da skup B sadrži skup A), a to pišemo kao $B \supseteq A$. Oznaku $\subseteq$ čitamo kao "inkluzija".*

Definicija 2.1.2. *Ako je $A \subseteq B$ i ako postoji neki $b \in B$ takav da $b \notin A$, onda kažemo da je skup A pravi podskup skupa B i pišemo $A \subset B$ ili $A \subsetneq B$.*

Definicija 2.1.3. *Kažemo da je skup A jednak skupu B i pišemo $A = B$ ako je svaki element skupa A ujedno i element skupa B, te ako je svaki element skupa B ujedno i element skupa A.*

Očito je

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A),$$

pa prema tomu provjeriti jesu li dva skupa A i B jednaka znači provjeriti je li $A \subseteq B$ i $B \subseteq A$.

Ukoliko dva skupa A i B nisu jednaka pišemo $A \neq B$. Očito je da vrijedi

$$A \neq B \Leftrightarrow (A \nsubseteq B \vee B \nsubseteq A),$$

pri čemu je

$$A \nsubseteq B \Leftrightarrow \exists a\,(a \in A \wedge a \notin B).$$

Propozicija 2.1.1. *Neka su A, B i C bilo koji skupovi. Vrijedi:*

1. $A \subseteq A$
2. $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$
3. $(A = B \wedge B = C) \Rightarrow A = C$.

Dokaz. Direktno iz definicija. ■

U mnogim situacijama je potrebno promatrati samo podskupove nekog skupa U, koji tada poprima značenje *univerzalnog skupa* (univerzuma). Naravno, univerzalnost skupa U je relativna i varira od problema do problema. Drugi važni istaknuti skup je *prazni skup*, tj. skup bez ijednog elementa. Označavamo ga s $\emptyset$.

Skupove i njihove međusobne odnose ponekad zorno prikazujemo tzv. *Vennovim dijagramima*. Ipak, važno je istaknuti da takvi crteži ne predstavljaju dokaz.

2.2. Zadavanje skupova

Skup smatramo *zadanim* ako je nedvosmislemo rečeno, objašnjeno ili specificirano što su elementi toga skupa. Prema tomu, zadati neki skup znači dati zakon, ograničenje, propis, specifikaciju ili svojstvo kojim se točno određuju članovi toga skupa.

Skupove možemo zadati na više načina:

1. Navođenjem potpune liste elemenata toga skupa unutar para vitičastih zagrada. Na primjer, skup samoglasnika u hrvatskom jeziku je skup $S = \{a, e, i, o, u\}$. Pritom poredak nije važan i ponovljene elemente ne uzimamo u obzir. Vitičaste zagrade igraju dvostruku ulogu: one su simbol ujedinjavanja dijelova u cjelinu i klasifikator objekata na one koji koji pripadaju skupu i na one koji mu ne pripadaju.

2. Isticanjem nekog karakterističnog svojstva koje imaju samo elementi toga skupa, tj. nekim propisom.
, skup svih pozitivnih cijelih brojeva zadajemo s $\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\}$, a centralnu, jediničnu kružnicu sa $S_1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

2.3. Booleove operacije na skupovima

Definicija 2.3.1. *Neka je U proizvoljan skup. Partitivni skup skupa U, u oznaci $\mathcal{P}(U)$, je skup svih podskupova skupa U. Često pišemo i 2^U.*

Na primjer,

1. $\mathcal{P}(\emptyset) = \{\emptyset\}$
2. $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$
3. $\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

Uvedimo sada neke operacije sa skupovima.

Definicija 2.3.2. *Neka je U dani skup i A, B njegovi podskupovi.*

a) Unija skupova A i B, u oznaci $A \cup B$, je skup

$$A \cup B = \{x \in U : x \in A \vee x \in B\}.$$

b) Presjek skupova A i B, u oznaci $A \cap B$, je skup

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}.$$

c) Razlika skupova A i B, u oznaci $A \setminus B$, je skup

$$A \setminus B = \{x \in U : x \in A \wedge x \notin B\}.$$

Ove osnovne operacije sa skupovima nazivamo Booleovim operacijama. Uočimo odmah da je

$$(\forall A, B \in \mathcal{P}(U))\,(A \cup B, A \cap B, A \setminus B \in \mathcal{P}(U)).$$

Također

$$(\forall A, B \subseteq U)\,(A \cap B \subseteq A, B \subseteq A \cup B).$$

Definicija 2.3.3. *Neka je U dani skup i $A, B \subseteq U$. Kažemo da su skupovi A i B disjunktni ako je $A \cap B = \emptyset$.*

Propozicija 2.3.1. *Neka je U proizvoljan skup i $A, B \subseteq U$. Vrijedi*

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

Dokaz. Dokaz provodimo indirektno, reductio ad absurdum.

Pretpostavimo suprotno, tj. da je $(A \setminus B) \cap (B \setminus A) \neq \emptyset$. Tada postoji neki $x \in (A \setminus B) \cap (B \setminus A)$, pa za njega vrijedi $x \in (A \setminus B)$ i $x \in (B \setminus A)$. Odatle je $x \in A, x \notin B$ i $x \in B, x \notin A$, što je nemoguće. Budući da smo došli do kontradikcije, zaključujemo da je pretpostavka bila pogrešna. Zato mora vrijediti $(A \setminus B) \cap (B \setminus A) = \emptyset$. ■

Sada ćemo uvesti i jednu unarnu operaciju sa skupovima.

Definicija 2.3.4. *Neka je U dani skup i $A \subseteq U$. Komplement skupa A u odnosu na skup U, u oznaci A^c, je skup*

$$A^c = U \setminus A = \{x \in U : x \notin A\}.$$

Uočimo da je za svaki $A \subseteq U$ ispunjeno $A^c \subseteq U$.

Pogledajmo jedan primjer: ako je $U = \{1, 2, 3, 4, 5, 6, 7\}$ i $A = \{2, 5, 6\}$, onda je $A^c = \{1, 3, 4, 7\}$.

Primjedba 2.3.1. *Neka je U dani skup i $A, B \subseteq U$. Uočimo da vrijedi sljedeće:*

1. $U^c = \emptyset$, $\emptyset^c = U$
2. $A \setminus B = A \cap B^c$
3. $A = B \Leftrightarrow A^c = B^c$.

Pogledajmo sada koja svojstva imaju Booleove operacije.

Teorem 2.3.1. *Neka je U dani skup i $A \subseteq U$. Vrijedi:*

1. $A \cup A = A$, $A \cap A = A$ *(idempotentnost)*
2. $A \cup U = U$, $A \cap \emptyset = \emptyset$
3. $A \cup \emptyset = A$, $A \cap U = A$
4. $A \cup A^c = U$, $A \cap A^c = \emptyset$
5. $(A^c)^c = A$ *(involutornost).*

Dokaz. Dokaz ćemo provesti direktno. S obzirom da u svim slučajevima dokazujemo jednakost skupova, svaki put treba dokazati dvije inkluzije. Tvrdnje $(1) - (4)$ su očigledne, pa ćemo dokazati samo tvrdnju (5).

Neka je $A \subseteq U$. Treba dokazati da je $(A^c)^c \subseteq A$ i $A \subseteq (A^c)^c$.

Dokažimo najprije $A \subseteq (A^c)^c$. Ako je $A = \emptyset$, onda je očito ispunjeno $A = \emptyset \subseteq (A^c)^c$. Pretpostavimo sada da je $A \neq \emptyset$. Za bilo koji $x \in A$ vrijedi

$$x \in A \Rightarrow (x \in U \wedge x \in A) \Rightarrow (x \in U \wedge x \notin A^c) \Rightarrow x \in (A^c)^c,$$

pa je $A \subseteq (A^c)^c$.

Dokažimo da vrijedi i obratna inkluzija. Ako je $(A^c)^c = \emptyset$, onda je ispunjeno $(A^c)^c = \emptyset \subseteq A$. Pretpostavimo sada da je $(A^c)^c \neq \emptyset$. Za bilo koji $x \in (A^c)^c$ vrijedi

$$x \in (A^c)^c \Rightarrow (x \in U \wedge x \notin A^c) \Rightarrow x \in A.$$

Prema tomu vrijedi $(A^c)^c \subseteq A$, čime je dokazano i $(A^c)^c = A$. ■

Teorem 2.3.2. *Neka je U dani skup i $A, B \subseteq U$. Vrijedi:*

1. $A \cup B = B \cup A$, $A \cap B = B \cap A$ *(komutativnost)*
2. $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$ *(de Morganove formule).*

Dokaz. Svojstvo (1) je direktna posljedica komutativnosti disjunkcije i konjukcije.

Dokažimo svojstva (2) . Prvo ćemo dokazati da je $(A \cup B)^c = A^c \cap B^c$, tj. da vrijede dvije odgovarajuće inkluzije. Slučajeve kada je $(A \cup B)^c$ ili $A^c \cap B^c$ prazan skup preskačemo jer tada tvrdnja trivijalno vrijedi.

Dokažimo najprije da je $(A \cup B)^c \subseteq A^c \cap B^c$. Za bilo koji $x \in (A \cup B)^c$ vrijedi

$$\begin{aligned} x \quad &\in \quad (A \cup B)^c \Rightarrow (x \in U \wedge x \notin A \cup B) \Rightarrow (x \in U \wedge x \notin A \wedge x \notin B) \\ &\Rightarrow \quad (x \in U \wedge x \notin A) \wedge (x \in U \wedge x \notin B) \Rightarrow (x \in A^c \wedge x \in B^c) \\ &\Rightarrow \quad x \in A^c \cap B^c. \end{aligned}$$

Dakle, dokazali smo da je $(A \cup B)^c \subseteq A^c \cap B^c$.

Dokažimo da vrijedi i obratna inkluzija. Za bilo koji $x \in A^c \cap B^c$ vrijedi

$$\begin{aligned} x \quad &\in \quad A^c \cap B^c \Rightarrow (x \in A^c \wedge x \in B^c) \Rightarrow (x \in U \wedge x \notin A \wedge x \notin B) \\ &\Rightarrow \quad (x \in U \wedge x \notin A \cup B) \Rightarrow x \in (A \cup B)^c . \end{aligned}$$

Dakle, $(A \cup B)^c \subseteq A^c \cap B^c$, pa smo tako dokazali i jednakost tih skupova.

Drugu formulu u (2) dokazat ćemo koristeći već dokazana svojstva Booleovih operacija. Prema prvoj formuli u (2) imamo

$$(A^c)^c \cap (B^c)^c = (A^c \cup B^c)^c ,$$

odakle je po svojstvu involutornosti

$$A \cap B = (A^c \cup B^c)^c .$$

No, prema Napomeni 2.3.1. znamo da je

$$(A \cap B)^c = [(A^c \cup B^c)^c]^c ,$$

iz čega slijedi

$$(A \cap B)^c = A^c \cup B^c,$$

što je i trebalo dokazati. ■

Analogno se mogu dokazati i sljedeća svojstva Booleovih operacija:

Teorem 2.3.3. *Neka je U dani skup i $A, B, C \subseteq U$. Vrijedi:*

1. $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ *(asocijativnost)*
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributivnost).*

Dokaz. Sami za vježbu. ■

Zadatak 1. *Neka je U dani skup i $A, B, C \subseteq U$. Dokažite da vrijedi:*

1. $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$
2. $A \cap B^c$ *i* B *su disjunktni*
3. $A \cup B = (A \cap B^c) \cup B$ *(unija prikazana kao unija dvaju disjunktnih skupova)*

4. $A \cap B$ *i* $A \cap B^c$ *su disjunktni skupovi*

5. $(A \cap B) \cup (A \cap B^c) = A$ *(skup prikazan kao unija dvaju disjunktnih skupova)*

6. $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Partitivni skup $\mathcal{P}(U)$ zajedno s operacijama $\cup, \cap$ i $\setminus$ zove se *Booleova algebra skupova* na U.

Primjedba 2.3.2. *Pojam unije i presjeka dvaju skupova može se poopćiti na više skupova.*
Neka je $\mathcal{F}$ *neka familija skupova.*

a) *Unija skupova familije* $\mathcal{F}$*, u oznaci* $B = \bigcup_{A \in \mathcal{F}} A$*, je skup definiran s*

$$x \in B \Leftrightarrow (\exists A \in \mathcal{F})\, x \in A.$$

b) *Presjek skupova familije* $\mathcal{F}$*, u oznaci* $D = \bigcap_{A \in \mathcal{F}} A$*, je skup definiran s*

$$x \in D \Leftrightarrow (\forall A \in \mathcal{F})\, x \in A.$$

I u ovom slučaju vrijede de Morganove formule

$$\begin{aligned} \left(\bigcup_{A \in \mathcal{F}} A\right)^c &= \bigcap_{A \in \mathcal{F}} A^c, \\ \left(\bigcap_{A \in \mathcal{F}} A\right)^c &= \bigcup_{A \in \mathcal{F}} A^c. \end{aligned}$$

U Zadatku 1. prikazali smo skupove $A \cup B$ i A kao unije disjunktnih skupova. Ovakav rastav je često od velike pomoći, pa ćemo ga poopćiti u sljedećoj definiciji.

Definicija 2.3.5. *Neka je* $A \neq \emptyset$ *proizvoljan skup. Particija skupa* A *je bilo koja familija* $\mathcal{F} \subseteq \mathcal{P}(A)$ *koja ima svojstva:*

a) $(\forall X \in \mathcal{F})\ X \neq \emptyset$

b) $(\forall X, Y \in \mathcal{F})\ (X \cap Y = \emptyset \vee X = Y)$

c) $\bigcup_{X \in \mathcal{F}} X = A$.

Dakle, $\mathcal{F}$ je particija skupa A ako i samo ako za svaki $x \in A$ postoji jedinstveni skup $X \in \mathcal{F}$ takav da je $x \in X$.

Na primjer, $\mathcal{F}_1 = \{\{1\}, \{2,3\}, \{4\}\}$ i $\mathcal{F}_2 = \{\{1,2\}, \{3,4\}\}$ su dvije particije skupa $A = \{1,2,3,4\}$.

Osim Booleovih operacija, na skupu $\mathcal{P}(A)$ možemo definirati i neke druge operacije, a jedna od njih je *simetručna razlika skupova.*

Definicija 2.3.6. *Neka je* U *dani skup i* $A, B \subseteq U$*. Simetrična razlika skupova* A *i* B*, u oznaci* $A \triangle B$*, je skup definiran s*

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Očito je $A \triangle B \subseteq U$ za svaki izbor $A, B \subseteq U$.

Zadatak 2. *Neka je U dani skup i $A, B \subseteq U$. Dokažite da vrijedi:*

1. $A \triangle B = (A \cup B) \setminus (A \cap B)$
2. $A \triangle B = B \triangle A$
3. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
4. $A \triangle \emptyset = \emptyset \triangle A = A$
5. $A \triangle A = \emptyset$.

2.4. Kartezijev umnožak skupova

U ovom ćemo se odjeljku upoznati s još jednim važnim načinom izgradnje novih skupova.

Neka su $A, B \neq \emptyset$ proizvoljni neprazni skupovi, te $a \in A$ i $b \in B$. Objekt (a, b) nazivamo *uređenim parom*, pri čemu je a prvi član (prva koordinata) uređenog para, a b drugi član (druga koordinata) uređenog para (a, b). Uočimo da je važan poredak članova uređenog para.

Stroga matematička definicija uređenog para glasi ovako:

Definicija 2.4.1. *Neka su A i B neprazni skupovi, te $a \in A$, $b \in B$. Uređeni par elemenata a i b, u oznaci (a, b), je skup*

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Važno je znati kada su dva uređena para jednaka. To nam govori sljedeći teorem.

Teorem 2.4.1. *Dva uređena para (a, b) i (a', b') su jednaka ako i samo ako je $a = a'$ i $b = b'$.*

Dokaz. Dokaz provodimo direktno, i to na način da ćemo dokazati istinitost dviju odgovarajućih implikacija.
Dokažimo najprije da $(a, b) = (a', b') \Rightarrow (a = a' \wedge b = b')$. Pretpostavimo da je $(a, b) = (a', b')$. Po definiciji znamo da je tada

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}. \tag{2.1}$$

Razlikujemo dva slučaja:
a) $a = b$
U ovom slučaju je $\{a, b\} = \{a, a\} = \{a\}$, pa iz (2.1) slijedi

$$\{\{a'\}, \{a', b'\}\} = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}.$$

Iz definicije jednakosti skupova zaključujemo da je $\{a\} = \{a'\} = \{a', b'\}$, a konačno (opet po definiciji jednakosti skupova) $a' = b' = a = b$.
Dakle, $a = a'$ i $b = b'$, što je i trebalo dokazati.

b) $a \neq b$

Ako je $a \neq b$, onda je zasigurno $\{a, b\} \neq \{a'\}$ (dvočlan skup ne može biti jednak jednočlanomu). Zbog (2.1) zaključujemo da je $\{a, b\} = \{a', b'\}$, pa je stoga i $\{a\} = \{a'\}$. Odavde je $a = a'$, a onda je i $b = b'$.

Dokažimo još da $(a = a' \wedge b = b') \Rightarrow (a, b) = (a', b')$.

Ako je $a = a'$ i $b = b'$, onda je $\{a\} = \{a'\}$ i $\{a, b\} = \{a', b'\}$. Odatle odmah slijedi

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} = (a', b'),$$

čime je dokaz završen. ■

Primjedba 2.4.1. *Uočimo da je općenito* $(a, b) \neq (b, a)$. *Štoviše, iz* $(a, b) = (b, a)$ *slijedi* $a = b$. *Za razliku od toga,* $\{a, b\} = \{b, a\}$.

Definicija 2.4.2. *Neka su* A *i* B *neprazni skupovi. Kartezijev (ili direktni) umnožak skupova* A *i* B, *u oznaci* $A \times B$, *je skup definiran s*

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Skupove A *i* B *nazivamo faktorima Kartezijeva umnoška. Ako je barem jedan od skupova* A *i* B *prazan, dogovorno uzimamo* $A \times B = \emptyset$.

Primjer 3. *Neka je* $A = \{\alpha, \beta\}$ *i* $B = \{1, 2, 3\}$.

$$\begin{aligned} A \times B &= \{(\alpha, 1), (\alpha, 2), (\alpha, 3), (\beta, 1), (\beta, 2), (\beta, 3)\}, \\ B \times A &= \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}. \end{aligned}$$

Iz gornjeg primjera je jasno da Kartezijevo množenje nije komutativna operacija.

Posebno je zanimljivo Kartezijevo množenje skupa sa samim sobom.

Definicija 2.4.3. *Neka je* A *neprazan skup. Kartezijev kvadrat skupa* A, *u oznaci* A^2, *je skup definiran s*

$$A^2 = A \times A = \{(a, b) : a, b \in A\},$$

a njegova dijagonala je skup

$$I_A = \{(a, a) : a \in A\}.$$

Očito je $I_A \subseteq A^2$ i $I_A \neq A^2$ čim A ima više od jednog elementa.

Primjer 4. *Dva poznata primjera su:*

1. $A = B = \mathbb{R}$ *(koordinatna ravnina)*

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$$

2. $A = B = [0, 1]$ *(jedinični kvadrat u koordinatnoj ravnini)*

$$[0, 1]^2 = \{(x, y) : x, y \in [0, 1]\}.$$

Operacija Kartezijeva množenja ima neka svojstva vezana uz Booleove oparacije.

Teorem 2.4.2. *Neka su A, B, C proizvoljni skupovi. Vrijedi:*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
3. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

Dokaz. Sami za vježbu. ■

Pojam Kartezijeva umnoška možemo poopćiti i na više od dva faktora.
Ako je $n \in \mathbb{N}$ i $A_1, A_2, \ldots, A_n$ neprazni skupovi, definiramo

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i,\ i = 1, 2, \ldots n\},$$

pri čemu $(a_1, a_2, \ldots, a_n)$ zovemo *uređena n-torka.* Ako je bilo koji od skupova $A_i,\ i = 1, 2, \ldots n$, prazan, definiramo $A_1 \times A_2 \times \cdots \times A_n = \emptyset$.
Naravno, možemo Kartezijev umnožak n skupova definirati i induktivno kao

$$\begin{aligned} A_1 \times A_2 \times A_3 &= (A_1 \times A_2) \times A_3, \\ &\vdots \\ A_1 \times A_2 \times \cdots \times A_{n-1} \times A_n &= (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n. \end{aligned}$$

Odatle posebno slijedi

$$(a_1, a_2, \ldots, a_n) = (a_1', a_2', \ldots, a_n') \Leftrightarrow a_1 = a_1' \wedge \cdots \wedge a_n = a_n'.$$

Zadatak 1. *Uvjerite se da Kartezijev umnožak nije asocijativan, tj. da postoje skupovi X, Y, Z takvi da je $(X \times Y) \times Z \neq X \times (Y \times Z)$. Dakle, ne valja definirati uređenu trojku (x, y, z) kao skup $\{\{x\}, \{x, y\}, \{x, y, z\}\}$.*

Primjer 5. *Dva poznata primjera su:*

1. $A = B = C = \mathbb{R}$ *(koordinatni prostor)*

$$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$$

2. $A = B = C = [0, 1]$ *(jedinična kocka u koordinatnom prostoru)*

$$[0, 1]^3 = \{(x, y, z) : x, y, z \in [0, 1]\}.$$

Poglavlje 3.

Relacije

3.1. Osnovni pojmovi

Pojam *relacije* je jedan od najvažnijih matematičkih pojmova uopće, a kao poseban slučaj sadrži pojam funkcije.

Primjeri iz svakidašnjeg života pokazuju da je često potrebno između dvaju skupova uspostaviti nekakav odnos.

Neka je na primjer A skup svih dnevnih listova koji izlaze u Splitu, a neka je B skup svih stanovnika grada Splita. Između skupova A i B postoji izvjestan odnos koji se sastoji u tomu da neki stanovnici Splita čitaju neke dnevne listove: pri tome neki čitaju samo jedan, neki više njih, a postoje također i oni stanovnici Splita koji ne čitaju nijedan dnevni list. Ako nam $a \in A$ označava *Slobodnu Dalmaciju*, onda je a u vezi s određenim brojem elemenata skupa B, tj. s određenim brojem stanovnika Splita. To su upravo oni $b \in B$ koji čitaju *Slobodnu Dalmaciju*.

Pogledajmo još jedan primjer: neka je sada $A = \{a, b, c, d\}$ društvo od četiri osobe, a $B = \{e, f, g\}$ neko drugo društvo od tri osobe. Između ta dva društva možemo uspostaviti odnos "poznavanja". Pretpostavimo da osoba a poznaje osobe e i g, osoba b poznaje osobu f, osoba c poznaje osobe e, f i g, a osoba d ne poznaje nikoga od njih. Na ovaj je način putem "poznavanja" ustanovljen (uočen) odnos između skupova A i B. Stoga je prirodno promatrati umnožak $A \times B$ budući se u njemu javljaju sve mogućnosti poznavanja. Imamo:

$$\begin{aligned} A \times B &= \{(a,e),(a,f),(a,g),(b,e),(b,f),(b,g), \\ &\quad (c,e),(c,f),(c,g),(d,e),(d,f),(d,g)\}. \end{aligned}$$

Odredimo li da su u parovima samo osobe koje se "poznaju", dobivamo skup

$$R = \{(a,e),(a,g),(b,f),(c,e),(c,f),(c,g)\} \subseteq A \times B.$$

Ovi primjeri ukazuju na potrebu proučavanja proizvoljnih podskupova Kartezijeva umnoška $A \times B$.

Definicija 3.1.1. *Neka su A i B skupovi. Svaki podskup R Kartezijeva umnoška $A \times B$ zove se (binarna) relacija. Skup A označavamo s $D_1(R)$, a skup B s $D_2(R)$. Za element $a \in A$ kažemo da je u relaciji R s $b \in B$ ako je $(a,b) \in R$. Domena relacije R je skup*

$$D(R) = \{a \in A : (\exists b \in B)\,(a,b) \in R\},$$

a slika relacije R skup

$$K(R) = \{b \in B : (\exists a \in A)\,(a,b) \in R\}.$$

Činjenicu da je $(a,b) \in R$ često pišemo u obliku aRb i kažemo da a ima svojstvo da je u relaciji R s b.

Ako je $A \neq B$ kažemo da je $R \subseteq A \times B$ *heterogena* relacija, a ako je $A = B$ kažemo da je $R \subseteq A \times A$ *homogena* relacija na skupu A.

Posebno izdvajamo homogenu relaciju I_A (ili u oznaci Δ_A), koja je za bilo koji neprazan skup A definirana s

$$I_A = \{(a,a) : a \in A\},$$

a koju zovemo *dijagonala* ili *identična relacija* na skupu A.

Definiciju binarne relacije može se proširiti na podskupove Kartezijeva produkta $A_1 \times \cdots A_n, n \in \mathbb{N}$, i tada govorimo o *$n$-arnim relacijama*. Nama će ipak biti najvažnije binarne relacije koje ćemo u nastavku jednostavno zvati relacije.

Uvedimo sada još nekoliko pojmova vezanih uz relacije.

Definicija 3.1.2. *Neka je $R \subseteq A \times B$ neprazna relacija. Suprotna (inverzna) relacija relaciji R je relacija $R^{-1} \subseteq B \times A$ definirana s*

$$R^{-1} = \{(b,a) : (a,b) \in R\}.$$

Definicija 3.1.3. *Neka je $R \subseteq A \times B$. Komplement relacije R je relacija $R^c \subseteq A \times B$ definirana s*

$$R^c = \{(a,b) \in A \times B : (a,b) \notin R\}.$$

Definicija 3.1.4. *Neka su A, B, C neprazni skupovi, te $R \subseteq A \times B$ i $S \subseteq B \times C$. Kompozicija relacija R i S je relacija $S \circ R \subseteq A \times C$ definirana s*

$$S \circ R = \{(a,c) : (\exists b \in B)\,((a,b) \in R \wedge (b,c) \in S)\}.$$

Primjer 6. *Neka je $A = \{1,2,3\}$, $B = \{a,b\}$ i $C = \{x,y\}$. Definirajmo relacije $R \subseteq A \times B$ i $S \subseteq B \times C$ s*

$$\begin{aligned} R &= \{(1,a),(2,b),(3,a),(3,b)\}, \\ S &= \{(a,y),(b,x)\}. \end{aligned}$$

Lako se vidi da je na primjer

$$\begin{aligned} R^{-1} &= \{(a,1),(b,2),(a,3),(b,3)\}, \\ S^c &= \{(a,x),(b,y)\}, \\ S \circ R &= \{(1,y),(2,x),(3,x),(3,y)\}. \end{aligned}$$

Primjer 7. *Neka je $A = \{1,2,3\}$. Definirajmo homogene relacije R i S na skupu A s*

$$\begin{aligned} R &= \{(1,1),(2,2),(3,1),(3,2)\}, \\ S &= \{(1,2),(2,3)\}. \end{aligned}$$

Tada je

$$\begin{aligned} S \circ R &= \{(1,2),(2,3),(3,2),(3,3)\}, \\ R \circ S &= \{(1,2),(2,1),(2,2)\}, \end{aligned}$$

pa je očito da kompozicija relacija općenito nije komutativna.

Teorem 3.1.1. *Neka su A, B, C, D neprazni skupovi, te $R \subseteq A \times B$, $S \subseteq B \times C$ i $Z \subseteq C \times D$. Vrijedi*

$$Z \circ (S \circ R) = (Z \circ S) \circ R.$$

Dokaz. Dokažimo da je $Z \circ (S \circ R) \subseteq (Z \circ S) \circ R$.

Ako je $Z \circ (S \circ R) = \emptyset$ onda tvrdnja trivijalno vrijedi, stoga pretpostavimo da je relacija $Z \circ (S \circ R)$ neprazna. Kako je $Z \circ (S \circ R) \subseteq A \times D$, uzmimo proizvoljan par $(a, d) \in Z \circ (S \circ R)$, gdje je $a \in A$ i $d \in D$. Po definiciji kompozicije relacija znamo da postoji neki $c \in C$ takav da je $(a, c) \in S \circ R$ i $(c, d) \in Z$. Nadalje, jer je $(a, c) \in S \circ R$ to postoji neki $b \in B$ takav da je $(a, b) \in R$ i $(b, c) \in S$. Po definiciji kompozicije iz $(b, c) \in S$ i $(c, d) \in Z$ slijedi $(b, d) \in Z \circ S$ i analogno iz $(a, b) \in R$ i $(b, d) \in Z \circ S$ slijedi $(a, d) \in (Z \circ S) \circ R$, što je i trebalo dokazati.

Suprotnu inkluziju dokažemo analogno. ■

Prethodni teorem nam u stvari kaže da je kompozicija relacija asocijativna. Stoga za homogenu relaciju R na skupu A ima smisla definirati potencije relacije R na sljedeći način:

$$\begin{aligned} R^0 &= I_A, \\ R^1 &= R, \\ R^2 &= R \circ R, \\ &\vdots \\ R^{n+1} &= R^n \circ R, \ n > 1. \end{aligned}$$

Propozicija 3.1.1. *Neka je $R \subseteq A \times B$. Vrijedi:*

$$R \circ I_A = R, \quad I_B \circ R = R.$$

Dokaz. Dokazat ćemo samo prvi identitet jer se drugi dokazuje analogno.

Znamo da je $R \circ I_A \subseteq A \times B$. Uzmimo proizvoljan $(a, b) \in R \circ I_A$. Po definiciji kompozicije to znači da postoji neki $a' \in A$ takav da je $(a, a') \in I_A$ i $(a', b) \in R$. No iz $(a, a') \in I_A$ slijedi $a = a'$, pa je $(a, b) \in R$. Dakle, $R \circ I_A \subseteq R$.

Obratno, uzmimo proizvoljan $(a, b) \in R$. Kako za svaki $a \in A$ vrijedi $(a, a) \in I_A$, to po definiciji kompozicije slijedi $(a, b) \in R \circ I_A$, pa je $R \subseteq R \circ I_A$. ■

Primjedba 3.1.1. *Posebno, ako je $R \subseteq A \times A$, iz prethodne propozicije slijedi*

$$R \circ I_A = I_A \circ R = R. \tag{3.1}$$

Štoviše, I_A je jedina relacija na A sa svojstvom da je za svaku relaciju $R \subseteq A \times A$ ispunjeno (3.1). *Naime, ako bi za neku relaciju Q na A za sve R vrijedilo $R \circ Q = Q \circ R = R$, onda bismo za $R = I_A$ imali*

$$I_A \circ Q = Q \circ I_A = I_A. \tag{3.2}$$

No iz (3.1) *za $R = Q$ dobijemo $Q \circ I_A = I_A \circ Q = Q$ pa iz tog i* (3.2) *slijedi*

$$I_A = Q.$$

Lema 3.1.1. *Neka su A i B neprazni skupovi, te $R, S \subseteq A \times B$. Vrijedi:*

1. $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$
2. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
4. $(R^{-1})^{-1} = R$.

Dokaz. Sami za vježbu. ■

Homogene relacije mogu imati neka posebna svojstva koja su dana u sljedećoj definiciji.

Definicija 3.1.5. *Neka je R homogena relacija na skupu A. Kažemo da je relacija R :*

a) refleksivna ako vrijedi

$$(\forall x \in A)\,(x, x) \in R$$

b) irefleksivna ako vrijedi

$$(\forall x \in A)\,(x, x) \notin R$$

c) simetrična ako vrijedi

$$(\forall x \in A)\,(\forall y \in A)\,((x, y) \in R \longrightarrow (y, x) \in R)$$

d) antisimetrična ako vrijedi

$$(\forall x \in A)\,(\forall y \in A)\,((x, y) \in R \wedge (y, x) \in R \longrightarrow x = y)$$

e) tranzitivna ako vrijedi

$$(\forall x \in A)\,(\forall y \in A)\,(\forall z \in A)\,((x, y) \in R \wedge (y, z) \in R \longrightarrow (x, z) \in R)\,.$$

Geometrijski gledano, refleksivna relacija sadrži dijagonalu I_A skupa A, irefleksivna relacija ne siječe dijagonalu I_A, a simetrična relacija je simetrična s obzirom na dijagonalu I_A.

Gornja svojstva homogenih relacija se skupovno mogu opisati na sljedeći način.

Lema 3.1.2. *Neka je R relacija na skupu A. Vrijedi:*

1. *R je refleksivna ako i samo ako je $I_A \subseteq R$*
2. *R je irefleksivna ako i samo ako je $R \cap I_A = \emptyset$*
3. *R je simetrična ako i samo ako je $R \subseteq R^{-1}$*
4. *R je antisimetrična ako i samo ako je $R \cap R^{-1} \subseteq I_A$*
5. *R je tranzitivna ako i samo ako je $R \circ R \subseteq R$.*

Dokaz. Tvrdnje 1., 2. i 4. očigledno vrijede, pa ćemo dokazati samo preostale tvrdnje.

Dokažimo najprije tvrdnju 3. Pretpostavimo da je relacija R simetrična. Ako je $R = \emptyset$, onda je $R = \emptyset \subseteq R^{-1}$, pa je tvrdnja trivijalno ispunjena. Pretpostavimo stoga da je R neprazna, te uzmimo proizvoljan $(x, y) \in R$. Relacija R je simetrična, pa je $(y, x) \in R$, a iz ovoga po definiciji inverzne relacije slijedi $(x, y) \in R^{-1}$. Dakle, dokazali smo da je $R \subseteq R^{-1}$. Obratno, neka je $R \subseteq R^{-1}$. Ako je $R = \emptyset$ tvrdnja trivijalno vrijedi (prazna relacija je simetrična). Pretpostavimo stoga da je $R \neq \emptyset$ i uzmimo proizvoljan par $(x, y) \in R$. Jer je $R \subseteq R^{-1}$ slijedi $(x, y) \in R^{-1}$, a po definiciji inverzne relacije odmah možemo zaključiti da je $(y, x) \in R$. Time smo dokazali da je R simetrična.

Dokažimo još i tvrdnju 5. Pretpostavimo da je R tranzitivna. Ako je $R \circ R = \emptyset$ tvrdnja trivijalno vrijedi, pa pretpostavimo stoga da je $R \circ R$ neprazna, te uzmimo proizvoljan par $(x, z) \in R \circ R$. Po definiciji kompozicije relacija znamo da postoji neki $y \in A$ takav da je $(x, y) \in R$ i $(y, z) \in R$. Jer je R tranzitivna slijedi i da je $(x, z) \in R$, pa zaključujemo da vrijedi $R \circ R \subseteq R$. Obratno, neka je $R \circ R \subseteq R$. Ako je $R = \emptyset$ tada je i $R \circ R = \emptyset$, pa tvrdnja trivijalno vrijedi (prazna relacija je tranzitivna). Pretpostavimo stoga da je R neprazna, te da je $(x, y) \in R$ i $(y, z) \in R$. Tada je $(x, z) \in R \circ R \subseteq R$, pa je $(x, z) \in R$. Dakle, R je tranzitivna, što je i trebalo dokazati. ■

Primjedba 3.1.2. *Uočimo da iz $R \subseteq R^{-1}$ po Lemi 3.1.1. slijedi $R^{-1} \subseteq (R^{-1})^{-1} = R$, pa iz te dvije inkluzije zaključujemo da je $R = R^{-1}$. Dakle, može se reći da je relacija R simetrična ako i samo ako je $R = R^{-1}$.*

Sada ćemo navesti neka svojstva koja mogu imati heterogene relacije (naravno, mogu ih imati i homogene relacije kao poseban slučaj heterogenih relacija).

Definicija 3.1.6. *Neka su A i B skupovi, te $R \subseteq A \times B$. Kažemo da je relacija R :*

a) injektivna ako vrijedi

$$(\forall x \in A)\,(\forall x' \in A)\,(\forall y \in B)\,((x, y) \in R \wedge (x', y) \in R \longrightarrow x = x')$$

b) funkcionalna ako vrijedi

$$(\forall x \in A)\,(\forall y \in B)\,(\forall y' \in B)\,((x, y) \in R \wedge (x, y') \in R \longrightarrow y = y')$$

c) surjektivna ako vrijedi

$$(\forall y \in B)\,(\exists x \in A)\,(x, y) \in R$$

d) totalna ako vrijedi

$$(\forall x \in A)\,(\exists y \in B)\,(x, y) \in R.$$

Lema 3.1.3. *Neka su A i B skupovi, te $R \subseteq A \times B$. Vrijedi:*

1. R je injektivna ako i samo ako je $R^{-1} \circ R \subseteq I_A$

2. R je funkcionalna ako i samo ako je $R \circ R^{-1} \subseteq I_B$

3. R je surjektivna ako i samo ako je $R \circ R^{-1} \supseteq I_B$

4. R je totalna ako i samo ako je $R^{-1} \circ R \supseteq I_A$.

Dokaz. Za ilustraciju ćemo dokazati samo prvu tvrdnju, a oba smjera dokaza ćemo provesti obratom po kontrapoziciji.

Pretpostavimo da $R^{-1} \circ R \nsubseteq I_A$. To svakako znači da je $R^{-1} \circ R \neq \emptyset$, te da

$$(\exists x \in A)\,(\exists x' \in A)\,\left(x \neq x' \wedge (x, x') \in R^{-1} \circ R\right).$$

Po definiciji kompozicije relacija iz gornjega slijedi

$$(\exists x \in A)\,(\exists x' \in A)\,(\exists y \in B)\,\left(x \neq x' \wedge (x, y) \in R \wedge (y, x') \in R^{-1}\right),$$

a po definiciji inverzne relacije slijedi

$$(\exists x \in A)\,(\exists x' \in A)\,(\exists y \in B)\,(x \neq x' \wedge (x, y) \in R \wedge (x', y) \in R),$$

iz čega zaključujemo da relacija R nije injektivna.

Obratno, pretpostavimo da R nije injektivna. To znači da

$$(\exists x \in A)\,(\exists x' \in A)\,(\exists y \in B)\,(x \neq x' \wedge (x, y) \in R \wedge (x', y) \in R).$$

Iz ovoga po definiciji inverzne relacije slijedi

$$(\exists x \in A)\,(\exists x' \in A)\,(\exists y \in B)\,\left(x \neq x' \wedge (x, y) \in R \wedge (y, x') \in R^{-1}\right),$$

to jest

$$(\exists x \in A)\,(\exists x' \in A)\,\left(x \neq x' \wedge (x, x') \in R^{-1} \circ R\right),$$

pa $R^{-1} \circ R \nsubseteq I_A$. ■

Definicija 3.1.7. *Funkcionalne relacije nazivamo parcijalnim funkcijama. Totalne funkcionalne relacije nazivamo funkcijama.*

Ako je relacija $f \subseteq A \times B$ parcijalna funkcija, a želimo to naglasiti, onda pišemo $f : A \rightharpoonup B$. Ako je f definirana u točki $x \in A$ pišemo $f(x) \downarrow$, a ako nije pišemo $f(x) \uparrow$.

3.2. Relacije ekvivalencije

Definicija 3.2.1. *Homogenu binarnu relaciju koja je refleksivna, simetrična i tranzitivna nazivamo relacijom ekvivalencije.*

Ovakve relacije igraju vrlo važnu ulogu u matematici i imaju mnoga lijepa svojstva. Relaciju ekvivalencije često označavamo simbolom $\sim$ ili $\cong$. Ako je $x \sim y$, onda kažemo da je x ekvivalentan s y. Važan primjer relacije ekvivalencije je relacija $=$ ("biti jednak").

Neka je $A \neq \emptyset$ proizvoljan skup i $\sim$ relacija ekvivalencije na njemu. Svakom elementu a skupa A možemo pridružiti skup

$$[a] = \{x \in A : x \sim a\},$$

tj. skup svih onih elemenata skupa A koji su u relaciji $\sim$ s a. Skup $[a]$ nazivamo *klasom ekvivalencije* određenom elementom a, a sam element *a reprezentantom klase* $[a]$. Budući je $(\forall a \in A)\, a \sim a$, to je $(\forall a \in A)\, [a] \neq \emptyset$.

Pogledajmo još neka važna svojstva klasa ekvivalencije.

Teorem 3.2.1. *Neka je $A \neq \emptyset$ proizvoljan skup, $\sim$ relacija ekvivalencije na A, te $x, y \in A$.*

1. *Ako $x \nsim y$, onda je $[x] \cap [y] = \emptyset$*
2. *Ako je $x \sim y$, onda je $[x] = [y]$.*

Dokaz. Dokažimo najprije prvu tvrdnju.

Neka su $x, y \in A$ takvi da $x \nsim y$. Dokažimo da je $[x] \cap [y] = \emptyset$. Pretpostavimo suprotno, tj. da je $[x] \cap [y] \neq \emptyset$. To znači da postoji neki $a \in [x] \cap [y]$. Iz $a \in [x]$ slijedi $a \sim x$, a iz $a \in [y]$ slijedi $a \sim y$. Kako je $\sim$ relacija ekvivalencije na A to je ona simetrična i tranzitivna, pa iz $a \sim x$ slijedi $x \sim a$, a iz $x \sim a$ i $a \sim y$ slijedi $x \sim y$. Obratom po kontrapoziciji dobijemo da iz $x \nsim y$ slijedi $[x] \cap [y] = \emptyset$.

Dokažimo još i drugu tvrdnju.

Pretpostavimo da je $x \sim y$. Treba dokazati $[x] \subseteq [y]$ i $[y] \subseteq [x]$. Dokažimo najprije $[x] \subseteq [y]$. Znamo da je $[x] \neq \emptyset$, pa uzmimo bilo koji element a iz $[x]$. To znači da je $a \sim x$. Zbog tranzitivnosti relacije $\sim$, iz $a \sim x$ i $x \sim y$ slijedi $a \sim y$, pa je $a \in [y]$. Dakle, $[x] \subseteq [y]$. Kako je relacija $\sim$ simetrična, to iz $x \sim y$ slijedi $y \sim x$, pa je po prethodnom $[y] \subseteq [x]$. ■

Prema prethodnom teoremu možemo zaključiti da za proizvoljne $x, y \in A$ vrijedi $[x] \cap [y] = \emptyset$ ili $[x] = [y]$. Odavde slijedi da za svaki $x \in A$ postoji jedinstvena klasa $[a]$ čiji je on član.

Stavimo li u jedan skup sve te različite klase koje definira relacija $\sim$ na skupu A, dobit ćemo skup čiji su elementi neprazni, po parovima disjunktni podskupovi skupa A, a čija je unija jednaka čitavom skupu A. Prema tomu, dobit ćemo jednu *particiju* skupa A. Tu particiju nazivamo *kvocijentnim skupom* skupa A po relaciji $\sim$ i označavamo je s $A/\sim$.

Dakle, svaka relacija ekvivalencije na skupu A definira jednu particiju skupa A na klase ekvivalencije. No kao što ćemo vidjeti, vrijedi i obrat. No prije nego to dokažemo uvest ćemo funkciju koja elementima skupa pridružuje njima pripadne klase po nekoj relaciji ekvivalencije.

Propozicija 3.2.1. *Neka je $\sim$ relacija ekvivalencije na skupu A i relacija τ na $A \times (A/\sim)$ definirana s*

$$(a, [x]) \in \tau \quad \textit{ako i samo ako} \quad a \in [x].$$

Relacija τ je funkcionalna, totalna i surjektivna.

Dokaz. Kako je za svaki $a \in A$ ispunjeno $a \in [a]$, to je relacija τ očigledno totalna i surjektivna. Pokažimo još da je funkcionalna. Neka je $a \in A$, te $[x]$ i $[y]$ dvije klase iz $A/\sim$ takve da je $(a,[x]) \in \tau$ i $(a,[y]) \in \tau$. Iz ovoga slijedi $a \in [x]$ i $a \in [y]$, tj. $a \in [x] \cap [y]$. Po svojstvima klasa relacije ekvivalencije τ zaključujemo da je $[x] = [y]$, pa je relacija τ funkcionalna. ■

Definicija 3.2.2. *Neka je $\sim$ relacija ekvivalencije na skupu A. Funkcija $\tau : A \to A/\sim$ definirana izrazom*

$$\tau(a) = [a]$$

zove se projekcija skupa A na kvocijentni skup $A/\sim$.

Teorem 3.2.2. *Svaka relacija ekvivalencije na skupu A definira jednu particiju skupa A. U istom elementu particije nalaze se oni i samo oni elementi skupa A koji su međusobno ekvivalentni.*

Dokaz. Neka je $\sim$ neka relacija ekvivalencije na skupu A. Dokazat ćemo da $A/\sim$ određuje jednu particiju skupa A.

Kako je relacija $\sim$ refleksivna, to je za svaki $x \in A$ ispunjeno $x \in [x]$. Iz ovoga slijedi $A = \cup_{x\in A}[x]$ i $[x] \neq \emptyset$ za sve $x \in A$. Nadalje, znamo da je za sve $x, y \in A$ ispunjeno $[x] \cap [y] = \emptyset$ ili $[x] = [y]$, pa $A/\sim$ zaista određuje jednu particiju skupa A. ■

Zanimljivo je da vrijedi i obrat prethodnog teorema: svaka particija skupa A definira jednu relaciju ekvivalencije na A. O tome nam govori naredni teorem.

Teorem 3.2.3. *Neka je $\mathcal{F}$ jedna particija skupa A. Tada je relacija $R_{\mathcal{F}}$ na skupu A definirana s*

$$(x,y) \in R_{\mathcal{F}} \text{ ako i samo ako } (\exists S \in \mathcal{F})\,(x \in S \wedge y \in S)$$

relacija ekvivalencije na A.

Dokaz. Neka su $x, y \in A$ u istom elementu particije $\mathcal{F}$. Po definiciji relacije $R_{\mathcal{F}}$ tada je $(x,y) \in R_{\mathcal{F}}$ i $(y,x) \in R_{\mathcal{F}}$, pa je relacija $R_{\mathcal{F}}$ simetrična. Posebno, ako je $x = y$ slijedi $(x,x) \in R_{\mathcal{F}}$, pa je $R_{\mathcal{F}}$ refleksivna. Dokažimo još i da je $R_{\mathcal{F}}$ tranzitivna. Pretpostavimo da je $(x,y) \in R_{\mathcal{F}}$ i $(y,z) \in R_{\mathcal{F}}$. Tada postoje elementi S_1 i S_2 particije $\mathcal{F}$ takvi da je $x, y \in S_1$ i $y, z \in S_2$. No to znači da je $y \in S_1 \cap S_2$, pa mora vrijediti $S_1 = S_2$ iz čega slijedi da su i x i z u istom elementu particije $\mathcal{F}$, pa je $(x,z) \in R_{\mathcal{F}}$. Dakle, $R_{\mathcal{F}}$ je i tranzitivna, pa je $R_{\mathcal{F}}$ relacija ekvivalencije na skupu A. ■

Primjer 8. *Neka je $\mathcal{P}$ skup svih pravaca neke ravnine. Na skupu $\mathcal{P}$ definiramo relaciju $\parallel$* ("biti paralelan"). *Podsjetimo se da su dva pravca u ravnini paralelna ako nemaju nijednu zajedničku točku ili ako se podudaraju.*
Očito je $\parallel$ relacija ekvivalencije na $\mathcal{P}$ (provjerite sami!). Klase ekvivalencije nazivamo smjerovima u ravnini.
Da li je relacija $\perp$ ("biti okomit") *relacija ekvivalencije na $\mathcal{P}$? (Nije!)*

Primjer 9. *Neka je $\mathcal{T}$ skup svih trokuta u nekoj ravnini. Relacije $\sim$* ("biti sličan"), *$\cong$* ("biti sukladan") *i ρ* ("imati istu površinu") *su relacije ekvivalencije na $\mathcal{T}$.*

Primjer 10. *Neka je E^3 prostor točaka.* Orijentirana dužina *u E^3 je svaki uređeni par točaka $(A, B) \in E^3 \times E^3$. Oznaka za orjentiranu dužinu je $(A, B) = \overrightarrow{AB}$. Označimo sa $\mathcal{O}$ skup svih orjentiranih dužina u E^3, tj.*

$$\mathcal{O} = \left\{ \overrightarrow{AB} : A, B \in E^3 \right\} = E^3 \times E^3.$$

Na skupu $\mathcal{O}$ definiramo relaciju $\equiv$ (biti ekvivalentan) na sljedeći način: reći ćemo da je orijentirana dužina $\overrightarrow{AB}$ ekvivalentna orijentiranoj dužini $\overrightarrow{CD}$, i pist ćemo $\overrightarrow{AB} \equiv \overrightarrow{CD}$ ako i samo ako dužine $\overline{AD}$ i $\overline{BC}$ imaju zajedničko polovište-
Provjerite sami da je relacija $\equiv$ relacija ekvivalencije na $\mathcal{O}$. Kvocijentni skup $\mathcal{O}/\equiv$ označavamo kao V^3, a njegove elemente (klase ekvivalencije) nazivamo vektorima.

3.3. Zatvorenja relacija

Često nam je potrebno neku homogenu relaciju bez poželjnih osobina (refleksivnosti, simetričnosti, tranzitivnosti) proširiti na način da poprimi neka od tih svojstava. Tada govorimo o zatvorenjima te relacije s obzirom na željena svojstva. Zatvorenje je, dakle, najmanja relacija koja sadrži polaznu relaciju a koja ujedno ima i željeno svojstvo.

Definicija 3.3.1. *Neka je R relacija na skupu A.*

1. *Refleksivno zatvorenje relacije R je najmanja relacija $R^r \subseteq A^2$ takva da je R^r refleksivna i $R \subseteq R^r$.*
2. *Simetrično zatvorenje relacije R je najmanja relacija $R^s \subseteq A^2$ takva da je R^s simetrična i $R \subseteq R^s$.*
3. *Tranzitivno zatvorenje relacije R je najmanja relacija $R^t \subseteq A^2$ takva da je R^t tranzitivna i $R \subseteq R^t$.*

U teoriji računarstva nam je vrlo često potrebno pronaći *refleksivno i tranzitivno zatvorenje* relacije R koje označavamo s R^*.

Teorem 3.3.1. *Neka je R relacija na skupu A. Tada je:*

1. $R^r = R \cup I$
2. $R^s = R \cup R^{-1}$
3. $R^t = \bigcup_{n=1}^{\infty} R^n$
4. $R^* = R^t \cup I = \bigcup_{n=0}^{\infty} R^n$
5. *najmanja relacija ekvivalencije koja sadrži R je relacija $R^e = \left(R \cup R^{-1}\right)^*$.*

Dokaz. Sami za vježbu. ■

Lema 3.3.1. *Neka su R i S relacije na skupu A. Vrijedi*

$$(R \cup S)^* = \left(R^* S^*\right)^*.$$

Dokaz. Sami za vježbu. ■

3.4. Relacije uređaja

Osim relacija ekvivalencije s kojima smo se upoznali u prethodnoj točki, važan je još jedan tip binarnih homogenih relacija.

Definicija 3.4.1. *Homogenu binarnu relaciju koja je refleksivna, antisimetrična i tranzitivna nazivamo relacijom djelomičnog (parcijalnog) uređaja.*

Definicija 3.4.2. *Uređeni par (A, ρ) sastavljen od skupa A i relacije djelomičnog uređaja ρ na skupu A zove se djelomično (parcijalno) uređen skup.*

Kao i u prethodnom, za relacije djelomičnog uređaja često se umjesto $(x, y) \in \rho$ piše $x \rho y$.

Primjer 11. *Definirajmo relaciju ρ na skupu $\mathbb{N}$ s*

$$(x, y) \in \rho \text{ ako i samo ako } x \text{ dijeli } y.$$

Očito je ova relacija refleksivna, antisimetrična i tranzitivna, pa je $(\mathbb{N}, \rho)$ djelomično uređen skup. Ipak, nisu svi elementi skupa $\mathbb{N}$ "usporedivi". Na primjer, $(2, 5) \notin \rho$ i također $(5, 2) \notin \rho$.

Gornji primjer nas motivira za sljedeću definiciju.

Definicija 3.4.3. *Neka je ρ realcija djelomičnog uređaja na skupu A. Ako vrijedi*

$$(\forall x \in A)\,(\forall y \in A)\,((x, y) \in \rho \vee (y, x) \in \rho)\,,$$

onda kažemo da je ρ relacija linearnog (totalnog) uređaja na skupu A.
Uređeni par (A, ρ) u tom slučaju nazivamo linearno (totalno) uređenim skupom ili jednostavno uređenim skupom.

Poznati primjer uređenog skupa je $(\mathbb{R}, \leq)$, dok je poznati primjer djelomično uređenog skupa $(\mathcal{P}(S), \subseteq)$, gdje je S neki neprazan skup. Relaciju $\subseteq$ nazivamo *relacijom sadržavanja*.

Djelomično uređene skupove se često prikazuje shematski.

Radi jasnoće ćemo nadalje za relaciju djelomičnog uređaja koristiti oznaku $\preceq$ da je ne bismo miješali s oznakom $\leq$ koju koristimo za relaciju uređaja "manje ili jednako" na skupovima brojeva.

Definicija 3.4.4. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$. Kažemo da je $m \in X$ najmanji element u skupu X ako vrijedi*

$$(\forall x \in X)\, m \preceq x.$$

Kažemo da je $m \in X$ minimalni element u skupu X ako vrijedi

$$(\forall x \in X)\,(x \preceq m \longrightarrow x = m)\,.$$

Kažemo da je $n \in X$ najveći element u skupu X ako vrijedi

$$(\forall x \in X)\, x \preceq n.$$

Kažemo da je $n \in X$ maksimalni element u skupu X ako vrijedi

$$(\forall x \in X)\, (n \preceq x \longrightarrow x = n)\,.$$

Očigledno je da je najmanji element ujedno i minimalan, a najveći element ujedno i maksimalan. Obrat, međutim, ne mora vrijediti. Također, djelomično uređen skup može imati više minimalnih i maksimalnih elemenata, a ne mora imati ni najveći ni najmanji element.

Primjer 12. *Neka je $A = \{a, b, c, d, e, f\}$, te neka je relacija $\preceq$ na skupu A dana kao*

$$\begin{aligned}\preceq \; &= \{(a,a)\,,(b,b)\,,(c,c)\,,(d,d)\,,(e,e)\,,(f,f)\,,(a,c)\,,\\ &\quad (c,b)\,,(c,d)\,,(a,b)\,,(a,d)\,,(e,f)\}\,.\end{aligned}$$

Elementi a i e su minimalni, a elementi b, d i f su maksimalni po $\preceq$. No u A nema po $\preceq$ ni najmanjeg ni najvećeg elementa.

Primjer 13. *Neka je $A = \{a, b, c, d, e\}$, te neka je relacija $\preceq$ na skupu A dana kao*

$$\begin{aligned}\preceq \; &= \{(a,a)\,,(b,b)\,,(c,c)\,,(d,d)\,,(e,e)\,,(a,c)\,,\\ &\quad (c,b)\,,(c,d)\,,(a,b)\,,(a,d)\,,(b,e)\,,(d,e)\,,(a,e)\,,(c,e)\}\,.\end{aligned}$$

Element a je minimalan i najmanji, a element e maksimalan i najveći po $\preceq$.

Definicija 3.4.5. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$.*
Element d skupa A je donja međa skupa X u A ako za svaki $x \in X$ vrijedi $d \preceq x$.
Najveća donja međa, ako postoji, zove se infimum skupa X i označava sa $\inf X$.
Element g skupa A je gornja međa skupa X u A ako za svaki $x \in X$ vrijedi $x \preceq g$.
Najmanja gornja međa, ako postoji, zove se supremum skupa X i označava sa $\sup X$.

Na primjer, u uređaju $(\mathbb{N}, \leq)$ je $\inf \mathbb{N} = 1$, a $\sup \mathbb{N}$ ne postoji. U djelomičnom uređaju $(\mathcal{P}(S), \subseteq)$ je $\inf \mathcal{P}(S) = \emptyset$, a $\sup \mathcal{P}(S) = S$.

Podsjetimo se da smo kod uspoređivanja brojeva često koristili relaciju $<$. Općenito su takve relacije definirane na sljedeći način.

Definicija 3.4.6. *Homogenu binarnu relaciju koja je irefleksivna i tranzitivna nazivamo relacijom strogog djelomičnog (parcijalnog) uređaja.*

Definicija 3.4.7. *Neka je $\prec$ relacija strogog djelomičnog uređaja na skupu A. Ako vrijedi*

$$(\forall x \in A)\, (\forall y \in A)\, [x \neq y \longrightarrow ((x,y) \in \rho \vee (y,x) \in \rho)]$$

onda kažemo da je $\prec$ relacija strogog uređaja na skupu A.
Uređeni par $(A, \prec)$ u tom slučaju nazivamo strogo uređenim skupom.

3.5. Dobro utemeljene relacije

Definicija 3.5.1. *Neka je R relacija djelomičnog uređaja na skupu A. R-lanac je bilo koji s obzirom na relaciju R linearno uređen podskup skupa A. Ako je R-lanac prebrojivo beskonačan nazivamo ga (rastućim) ω-R-lancem.*

Dakle, ako je, na primjer, $\{a_1, a_2, \ldots, a_8\} \subseteq A$ i ako vrijedi

$$a_1 R a_2 R a_3 \cdots a_7 R a_8,$$

onda je $\{a_1, a_2, \ldots, a_8\}$ R-lanac u skupu A. Ako je $\{a_1, a_2, \ldots, a_n, \ldots\} \subseteq A$ i ako vrijedi

$$(\forall n \in \mathbb{N}) \quad a_n R a_{n+1},$$

onda je $\{a_1, a_2, \ldots, a_n, \ldots\}$ ω-R-lanac u A. No ako je $\{a_1, a_2, \ldots, a_n, \ldots\}$ ω-R^{-1}-lanac u A, tj. ako vrijedi

$$(\forall n \in \mathbb{N}) \quad a_n R^{-1} a_{n+1},$$

odnosno

$$(\forall n \in \mathbb{N}) \quad a_{n+1} R a_n,$$

onda kažemo da je $\{a_1, a_2, \ldots, a_n, \ldots\}$ *padajući* ω-R-lanac u A.

Definicija 3.5.2. *Kažemo da je relacija djelomičnog uređaja $R \subseteq A^2$ dobro utemeljena na skupu A ako u A nema padajućih ω-R-lanaca (tj. ako u A nema beskonačnih padajućih R-lanaca).*

Primjer 14. *Relacija $\leq$ nije dobro utemeljena ni na skupu $\mathbb{R}$ ni na intervalu $(0, 1)$, no jest dobro utemeljena na skupu $\mathbb{N}$. Relacija $\subseteq$ je dobro utemeljena na bilo kojem skupu konačnih skupova.*

Teorem 3.5.1. *Relacija R je dobro utemeljena ako i samo ako je relacija R^t dobro utemeljena.*

Dokaz. Sami. ■

Teorem 3.5.2. *Relacija djelomičnog uređaja $R \subseteq A^2$ je dobro utemeljena ako i samo ako svaki neprazan podskup slupa A ima R-minimalni element.*

Dokaz. Dokažimo najprije smjer dovoljnosti. a dokaz ćemo provesti kontradikcijom. Pretpostavimo stoga da svaki neprazan podskup skupa A ima R-minimalni element i da u skupu A postoji beskonačni padajući R-lanac. Članovi tog lanca tvore jedan neprazan podskup skupa A, pa on po pretpostavci ima R-minimalni element. No to, pak, znači da takav lanac ne može beskonačno padati, što je u kontradikciji s našom pretpostavkom.

Dokažimo sada smjer nužnosti obratom po kontrapoziciji. Neka u A postoji neprazan podskup, neki B, koji nema R-minimalni element. Kako je $B \neq \emptyset$ to postoji neki $a_0 \in B$ koji sigurno nije R-minimalan. Štoviše, mora postojati i neki $a_1 \in B$ koji ni sam nije R-minimalan i za kojeg vrijedi $a_0 R a_1$. Očito se ovaj postupak može nastaviti tako da dobijemo beskonačni padajući R-lanac elemenata iz $B \subseteq A$ što znači da R dobro utemeljena na skupu A. ■

3.6. Funkcije

Već smo rekli da su *funkcije* posebne relacije, tj. binarne relacije koje su **funkcionalne** i **totalne**. No kako su funkcije same po sebi važan matematički pojam posvetit ćemo im posebnu točku. Pogledajmo najprije jedan primjer.

Primjer 15. *Neka je H skup svih državljana Republike Hrvatske, $Z = \{0, 1, \ldots, 9\}$ skup znamenki dekadskog sustava i $J = \{(a_1, \ldots, a_{13}) : a_1, \ldots, a_{13} \in Z\}$ skup svih trinaesteroznamenkastih brojeva sa znamenkama iz Z. Elemente skupa J možemo interpretirati kao JMBG-ove državljana RH.*
Definiramo relaciju $f \subseteq H \times J$ ovako

$$(x, a) \in f \text{ ako i samo ako je } a \text{ JMBG osobe } x.$$

Znamo da svakom državljaninu RH pripada jedinstveni JMBG, pa je ova relacija funkcionalna i totalna. Točnije, f je funkcija.

Napomenimo da se često funkcije definira kao uređene trojke (A, B, f), gdje su A i B neprazni skupovi, a f pravilo pridruživanja po kojemu se svakom elementu skupa A pridružuje jedan i samo jedan element skupa B. Mi nećemo koristiti takvu definiciju da bismo izbjegli uvođenje pojma "pravila pridruživanja" koji intuitivno nije jasan.

No koristit ćemo uobičajene oznake: za funkciju f umjesto $f \subseteq A \times B$ pisat ćemo $f : A \to B$, a umjesto $(x, y) \in f$ pisat ćemo $y = f(x)$. Element x nazivamo *argumentom* (neovisnom varijablom), a element y *slikom* ili vrijednošću funkcije (ovisnom varijablom).

Funkcije se često prikazuju *dijagramima*.

Već smo se upoznali s inverznom relacijom i slikom relacije, no kada je relacija funkcija uvode se neke posebne oznake i pojmovi.

Definicija 3.6.1. *Neka je $f : A \to B$ funkcija i $C \subseteq A$, $D \subseteq B$.*

a) Slika skupa C u odnosu na funkciju f je skup

$$f(C) = \{f(x) : x \in C\} \subseteq B$$

b) Praslika skupa D u odnosu na funkciju f je skup

$$f^{-1}(D) = \{x \in A : f(x) \in D\} \subseteq A.$$

Očito je

$$\begin{aligned} f(A) &\subseteq B, \quad f^{-1}(B) = A, \\ f(\emptyset) &= \emptyset, \quad f^{-1}(\emptyset) = \emptyset. \end{aligned}$$

Napomenimo da kada se radi o jednočlanim podskupovima ne pišemo vitičaste zagrade, već jednostavno stavljamo

$$f^{-1}(y) = \{x \in A : f(x) = y\}.$$

Primjer 16. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana s* $f(x) = 7$ *za sve* $x \in \mathbb{R}$. *Vrijedi:*

$$K(f) = \{7\}, \ f([1,2]) = \{7\}, \quad f^{-1}(\mathbb{R}) = f^{-1}(7) = \mathbb{R},$$
$$f^{-1}([1,4]) = \emptyset, \quad f^{-1}([3,8]) = \mathbb{R}, \quad f^{-1}(\{6,7\}) = \mathbb{R}.$$

Primjer 17. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana s* $f(x) = x^2$ *za sve* $x \in \mathbb{R}$. *Vrijedi:*

$$K(f) = [0,\infty), \ f([1,2]) = [1,4], \quad f^{-1}(\mathbb{R}) = f^{-1}([0,\infty)) = \mathbb{R},$$
$$f^{-1}(4) = \{-2,2\}, \quad f^{-1}([2,4]) = \left[-2,\sqrt{2}\right] \cup \left[\sqrt{2},2\right], \quad f^{-1}(-1) = \emptyset.$$

Propozicija 3.6.1. *Neka je* $f : A \to B$ *dana funkcija, te* $X, Y \subseteq A$. *Vrijedi:*

1. $f(X \cup Y) = f(X) \cup f(Y)$
2. $f(X \cap Y) \subseteq f(X) \cap f(Y)$.

Dokaz. Dokažimo najprije $f(X \cup Y) = f(X) \cup f(Y)$.

Neka je $y \in f(X \cup Y)$ proizvoljan. To znači da postoji neki $x \in X \cup Y$ takav da je $y = f(x)$. Jer je $x \in X \cup Y$, to je $x \in X$ ili $x \in Y$. Iz ovoga slijedi $y = f(x) \in f(X)$ ili $y = f(x) \in f(Y)$, pa je $y \in f(X) \cup f(Y)$. Dakle, dokazali smo da je $f(X \cup Y) \subseteq f(X) \cup f(Y)$.

Obratno, neka je $y \in f(X) \cup f(Y)$. To znači da je $y \in f(X)$ ili $y \in f(Y)$. Ako je $y \in f(X)$ onda postoji neki $x \in X$ takav da je $y = f(x)$, a ako je $y \in f(Y)$ onda postoji neki $x \in Y$ takav da je $y = f(x)$. U svakom slučaju, postoji neki $x \in X \cup Y$ takav da je $y = f(x)$, pa je $y \in f(X \cup Y)$. Dakle, dokazali smo i da je $f(X) \cup f(Y) \subseteq f(X \cup Y)$, čime je dokaz prve tvrdnje završen.

Dokažimo sada drugu tvrdnju.

Uzmimo proizvoljan $y \in f(X \cap Y)$. To znači da postoji neki $x \in X \cap Y$ takav da je $y = f(x)$. Za x vrijedi $x \in X$ i $x \in Y$, pa je $y \in f(X)$ i $y \in f(Y)$. Dakle, vrijedi $y \in f(X) \cap f(Y)$, pa je tvrdnja dokazana. ■

Dokazat ćemo protuprimjerom da ne vrijedi $f(X \cap Y) \supseteq f(X) \cap f(Y)$.

Neka je $A = \{a,b\}$, $a \neq b$, i $B = \{b\}$. Definirat ćemo funkciju $f : A \to B$ sa $f(a) = f(b) = b$. Neka je $X = \{a\}$ i $Y = \{b\}$. Vrijedi $X \cap Y = \emptyset$, pa je $f(X \cap Y) = \emptyset$. No s druge strane je $f(X) = f(Y) = \{b\}$, pa je $f(X) \cap f(Y) = \{b\} \neq \emptyset$. Dakle, $f(X) \cap f(Y) \not\subseteq f(X \cap Y)$.

Propozicija 3.6.2. *Neka je* $f : A \to B$ *dana funkcija, te* $X, Y \subseteq B$. *Vrijedi:*

1. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$
2. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$
3. $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$.

Dokaz. Dokazat ćemo samo prvu tvrdnju. Preostale tvrdnje dokažite sami.

Uzmimo proizvoljan $x \in f^{-1}(X \cup Y)$. Iz ovoga odmah slijedi $f(x) \in X \cup Y$. To dalje znači da je $f(x) \in X$ ili $f(x) \in Y$, pa je $x \in f^{-1}(X)$ ili $x \in f^{-1}(Y)$, odnosno $x \in f^{-1}(X) \cup f^{-1}(Y)$. Dakle, dokazali smo da je $f^{-1}(X \cup Y) \subseteq f^{-1}(X) \cup f^{-1}(Y)$.

Obratno, neka je $x \in f^{-1}(X) \cup f^{-1}(Y)$. Iz ovoga slijedi $f(x) \in X$ ili $f(x) \in Y$. Dakle, $f(x) \in X \cup Y$, pa je $x \in f^{-1}(X \cup Y)$, čime smo dokazali da je $f^{-1}(X) \cup f^{-1}(Y) \subseteq f^{-1}(X \cup Y)$. Zajedno s prethodnim to daje $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. ■

Iz prethodne dvije propozicije vidimo da se praslike ponašaju bolje nego slike.

Krene li se od definicije funkcije kao uređene trojke, graf funkcije $f : A \to B$ se definira kao skup

$$\Gamma_f = \{(x, f(x)) : x \in A\} \subseteq A \times B.$$

No vidimo da se u okviru naše definicije funkcije kao posebne relacije graf funkcije f i sama funkcija f poklapaju, pa nećemo posebno definirati graf funkcije. Točnije, kao što bilo koju relaciju možemo prikazati grafički, tako to možemo napraviti i kada je riječ o funkciji.

Primjer 18. *Nacrtajte funkcije $f, g : \mathbb{R} \to \mathbb{R}$ definirane formulama $f(x) = 2x$ odnosno $g(x) = x^2$ za sve $x \in \mathbb{R}$.*

Definicija 3.6.2. *Neka su A, B proizvoljni skupovi i $C \subseteq A$. Kažemo da je funkcija $g : C \to B$ restrikcija ili ograničenje funkcije $f : A \to B$ (odnosno da je funkcija f ekstenzija ili proširenje funkcije g) ako je $g \subset f$. Pišemo $g = f|_C$.*

Primjedba 3.6.1. *Može se dokazati da je $g \subset f$ ako i samo ako je $D(g) \subset D(f)$ i $(\forall x \in D(g))\, g(x) = f(x)$.*

Primjer 19. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = |x|$ za sve $x \in \mathbb{R}$,a funkcija $g : \mathbb{R}_0^+ \to \mathbb{R}$ izrazom $g(x) = x$ za sve $x \in \mathbb{R}_0^+$. Tada je $g = f|_{\mathbb{R}_0^+}$.*

Primjer 20. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = \sqrt{x^2}$ za sve $x \in \mathbb{R}$,a funkcija $g : \mathbb{R}_0^+ \to \mathbb{R}$ izrazom $g(x) = x$ za sve $x \in \mathbb{R}_0^+$. Tada je $g = f|_{\mathbb{R}_0^+}$.*

Primjer 21. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = \sqrt{1 - \sin^2 x} = |\cos x|$ za sve $x \in \mathbb{R}$, a funkcija $g : \left[\frac{\pi}{2}, \frac{3\pi}{2}\right] \to \mathbb{R}$ izrazom $g(x) = -\cos x$ za sve $x \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]$. Tada je $g = f|_{\left[\frac{\pi}{2}, \frac{3\pi}{2}\right]}$.*

Uočimo da je restrikcija neke funkcije na zadani skup jedinstveno određena, dok to nije slučaj s proširenjem. Pogledajmo jedan primjer.

Primjer 22. *Neka je funkcija $f : [0,1] \to \mathbb{R}$ definirana izrazom $f(x) = \sqrt{1 - x^2}$ za sve $x \in [0,1]$, a funkcija $g : [-1,1] \to \mathbb{R}$ izrazom*

$$g(x) = \begin{cases} x + 1, & x \in [-1, 0) \\ \sqrt{1 - x^2}, & x \in [0, 1] \end{cases}$$

za sve $x \in [-1,1]$. Tada je $f = g|_{[0,1]}$. No funkcija $h : [-1,1] \to \mathbb{R}$ definirana izrazom

$$h(x) = \begin{cases} 1, & x \in [-1, 0) \\ \sqrt{1 - x^2}, & x \in [0, 1] \end{cases}$$

za sve $x \in [-1,1]$ je također proširenje funkcije f, tj. $f = h|_{[0,1]}$.

Već smo definirali kompoziciju relacija i dokazali da je ona asocijativna. Sada ćemo dokazati da je kompozicija dviju funkcija funkcija.

Teorem 3.6.1. *Neka su dane funkcije $f : A \to B$ i $g : B \to C$. Tada je i $g \circ f$ funkcija, te $g \circ f : A \to C$.*

Dokaz. Po definiciji kompozicije relacija znamo da je $g \circ f \subseteq A \times C$. Dokažimo najprije da je $D(g \circ f) = A$. Kako je $D(f) = A$ i $D(g) = B$, to je $(\forall x \in A)(\exists y \in B) f(x) = y$ i $(\forall y \in B)(\exists z \in C) g(y) = z$. Dakle, $(\forall x \in A)(\exists z \in C)(g \circ f)(x) = z$, pa je relacija $g \circ f$ totalna, tj. $D(g \circ f) = A$. Dokažimo još da je $g \circ f$ funkcionalna. Neka je $x \in A$ i $z, z' \in C$ takvi da je $(g \circ f)(x) = z$ i $(g \circ f)(x) = z'$. Jer je $(g \circ f)(x) = z$ to postoji neki $y \in B$ takav da je $f(x) = y$ i $g(y) = z$. Jer je $(g \circ f)(x) = z'$ to postoji neki $y' \in B$ takav da je $f(x) = y'$ i $g(y') = z'$. Jer je f funkcionalana slijedi $y = y'$, a jer je i g funkcionalna slijedi $z = z'$. Dakle, $g \circ f$ je funkcionalna. ■

Primjedba 3.6.2. *Iz dokaza prethodnog teorema se vidi da se analogna tvrdnja može izreći i za parcijalne funkcije.*

Primjedba 3.6.3. *Posljedica prethodnog teorema jest da je za sve $x \in D(f)$ ispunjeno*

$$(g \circ f)(x) = g(f(x)).$$

Među funkcijama važnu ulogu igraju one koje su injektivne i surjektivne, tj. injekcije i surjekcije. Podsjetimo se da je funkcija $f : A \to B$ injektivna ako vrijedi

$$(\forall x \in A)(\forall x' \in A)(\forall y \in B)(f(x) = y \wedge f(x') = y \longrightarrow x = x'),$$

te da je surjektivna ako vrijedi

$$(\forall y \in B)(\exists x \in A) f(x) = y.$$

Mogli bismo to izreći i ovako: funkcija $f : A \to B$ je injektivna ako vrijedi

$$(\forall y \in K(f))(\exists x \in A) f^{-1}(y) = \{x\},$$

a surjektivna ako vrijedi

$$K(f) = B.$$

Primjer 23. *Funkcija $f : \mathbb{R} \to \mathbb{R}_0^+$ definirana izrazom $f(x) = |x|$ za sve $x \in \mathbb{R}$ je surjektivna, ali nije injektivna (na primjer $f(-1) = f(1)$). Funkcija $g : \mathbb{R} \to \mathbb{R}$ definirana izrazom $g(x) = 2x + 2$ za sve $x \in \mathbb{R}$ je injektivna i surjektivna.*

Definicija 3.6.3. *Funkcija je bijekcija ako je injekcija i surjekcija.*

Posebno, homogenu bijekciju $f : A \to A$ nazivamo *permutacijom* skupa A.

Primjer 24. *Funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = x^3$ za sve $x \in \mathbb{R}$ je bijekcija. Funkcija $g : [0,1] \to [0,1]$ definirana izrazom $g(x) = \sqrt{1 - x^2}$ za sve $x \in \mathbb{R}$ je također bijekcija.*

Primjedba 3.6.4. *Posebno važna bijekcija koju ćemo često spominjati je tzv. identiteta na skupu A, tj. funkcija $i_A : A \to A$ definirana izrazom $i_A(x) = x$ za sve $x \in A$. Svojstva ove funkcije ispitana su još kada je bila općenito riječ o relacijama, pa znamo da je za svaku funkciju $f : A \to B$ ispunjeno*

$$f \circ id_A = id_B \circ f = f.$$

Zadatak 1. *Dokažite da je:*

1. *kompozicija dviju injekcija injekcija*
2. *kompozicija dviju surjekcija surjekcija*
3. *kompozicija dviju bijekcija bijekcija.*

Sljedeći teorem će nam omogućiti da uvedemo pojam inverzne funkcije.

Teorem 3.6.2. *Neka je dana funkcija $f : A \to B$. Relacija f^{-1} je funkcija ako i samo ako je f bijekcija. Štoviše, f^{-1} je i sama bijekcija.*

Dokaz. Pretpostavimo najprije da je f bijekcija i pokažimo da je u tom slučaju f^{-1} funkcija, i to bijekcija.

Kako je f surjekcija, to za svaki $y \in B$ postoji neki $x \in A$ takav da je $f(x) = y$. Dakle, za svaki $y \in B$ postoji neki $x \in A$ takav da je $f^{-1}(y) = x$, iz čega odmah slijedi da je f^{-1} totalna relacija. Dokažimo još da je f^{-1} funkcionalna. Uzmimo stoga proizvoljan $y \in B$ i neke $x, x' \in A$ takve da je $f^{-1}(y) = x$ i $f^{-1}(y) = x'$. Iz ovoga slijedi $f(x) = y$ i $f(x') = y$. Jer je f injektivna slijedi $x = x'$, pa je f^{-1} funkcionalna relacija. Dakle, f^{-1} je funkcija.

Dokažimo da je f^{-1} surjekcija. Kako je f totalna, to za svaki $x \in A$ postoji neki $y \in B$ takav da je $f(x) = y$. Dakle, za svaki $x \in A$ postoji neki $y \in B$ takav da je $f^{-1}(y) = x$, pa je f surjekcija. Dokažimo još i da je f^{-1} injekcija. Uzmimo proizvoljne $y, y' \in B$ i neki $x \in A$ takve da je $f^{-1}(y) = f^{-1}(y') = x$. Slijedi $f(x) = y$ i $f(x) = y'$. Jer je f funkcionalna mora vrijediti $y = y'$, pa je f^{-1} injekcija. Dakle, f^{-1} je bijekcija.

Treba još dokazati da kad god je f^{-1} funkcija da je onda f bijekcija. No ovo slijedi iz drugog dijela već provedenog dokaza: zamjenimo li f sa f^{-1} i iskoristimo li činjenicu da je $(f^{-1})^{-1} = f$ možemo uočiti da se funkcionalnost i totalnost relacije f^{-1} na f prenose kao injektivnost i surjektivnost, pa je u tom slučaju f bijekcija. ■

Primjedba 3.6.5. *Iz dokaza prethodnog teorema se vidi da je f^{-1} parcijalna funkcija ako i samo ako je f injekcija.*

Teorem 3.6.3. *Neka je $f : A \to B$ bijekcija. Vrijedi*

$$f^{-1} \circ f = id_A, \qquad f \circ f^{-1} = id_B \quad ,$$

i f^{-1} je jedina funkcija s ovim svojstvima.

Dokaz. Po Teoremu 3.6.2. znamo da je f^{-1} bijekcija, a po teoremu 3.6.1. znamo da su $f^{-1} \circ f : A \to A$ i $f \circ f^{-1} : B \to B$ funkcije, i to bijekcije. Dokazat ćemo da je riječ upravo o identitetama na A odnosno B.

Uzmimo proizvoljne $x \in A,\ y \in B$. Jer su f i f^{-1} bijekcije vrijedi

$$\begin{aligned} \left(f^{-1} \circ f\right)(x) &= f^{-1}(f(x)) = x = id_A(x), \\ \left(f \circ f^{-1}\right)(y) &= f\left(f^{-1}(y)\right) = y = id_B(y), \end{aligned}$$

pa zaključujemo da je $f^{-1} \circ f = id_A$ i $f \circ f^{-1} = id_B$.

Dokažimo da je f^{-1} jedina funkcija s ovakvim svojstvom. Pretpostavimo suprotno, tj. da postoji neka funkcija $g : B \to A$ takva da je $g \circ f = id_A$ i $f \circ g = id_B$, a da je pri tomu $g \neq f^{-1}$. Tada vrijedi

$$\begin{aligned} (g \circ f) \circ f^{-1} &= id_A \circ f^{-1} = f^{-1}, \\ g \circ \left(f \circ f^{-1}\right) &= g \circ id_B = g, \end{aligned}$$

pa zbog asocijativnosti kompozicije slijedi $g = f^{-1}$. No ovo je u kontradikciji s pretpostavkom da je $g \neq f^{-1}$, pa je f^{-1} jedinstvena funkcija s ovim svojstvima. ■

Primjedba 3.6.6. *Posljedica prethodnog teorema jest da je za sve $x \in D(f)$ i sve $y \in K(f)$ ispunjeno*

$$\left(f^{-1} \circ f\right)(x) = x, \qquad \left(f \circ f^{-1}\right)(y) = y.$$

Ovo poglavlje je dijelom preuzeto iz [2].

3.7. Relacije potpunog djelomičnog uređaja

U matematičkoj teoriji računarstva *potpuni djelomični uređaji* imaju poseban značaj. Dokazuje se, naime, da neprekidne funkcije definirane na skupovima s takvim uređajem imaju mnoga poželjna svojstva među kojima je i ono da uvijek imaju najmanju čvrstu točku. Polazimo od činjenice da se na skupu raznih podataka koji se javljaju na ulazu i izlazu računala može na prirodan način uvesti uređaj *"po aproksimaciji"* ($x \leq y$ ako i samo ako je x aproksimacija od y). Kako su i same funkcije posebne relacije, tj. skupovi uređenih parova podataka, to se i one mogu promatrati kao podaci. Jasno je i da se svaka parcijalna funkcija može pretvoriti u totalnu uvođenjem novog elementa $\perp$ ("dno") u njenu kodomenu K i stavljanjem

$$f(x) = \perp$$

kad god je f nedefinirana u x. Element $\perp$ tumačimo kao "praznu" informaciju pa je on manji od svakog drugog elementa, odnosno on je najmanji element kodomene. Uređaj među tako proširenim funkcijama se sada definira adekvatno uređaju među podacima: ako su f i g funkcije sa D u $K_\perp$ definiramo:

$$f \leq g \ \text{ ako i samo ako } \ (\forall x \in D) \quad f(x) \leq g(x),$$

(dakle, za svaki $x \in D$ element $f(x)$ je aproksimacija elementa $g(x)$).

No nas posebno zanimaju *izračunljive* funkcije, tj. funkcije za koje znamo da pojava informacije (njihove vrijednosti) na izlazu ovisi samo o tome da li je konačno mnogo informacija (argumenata) potrebno na ulazu. Pokazat će se da su takve upravo neprekidne funkcije definirane na potpuno djelomično uređenim skupovima.

Definicija 3.7.1. *Neka je $(X, \leq)$ djelomični uređaj. Kažemo da je skup $A \subseteq X$ usmjeren u $(X, \leq)$ ako*

$$(\forall a, b \in A)\,(\exists c \in A)\,(a \leq c \wedge b \leq c)\,.$$

Definicija 3.7.2. *Kažemo da je djelomični uređaj potpun ako svaki u njemu usmjeren skup ima supremum.*

Postoji i alternativna ekvivalentna definicija koja koristi pojam ω-lanaca. Navodimo i nju jer ćemo u radu koristiti obje definicije.

Definicija 3.7.3. *Kažemo da je djelomični uređaj potpun ako u njemu svaki ω-lanac ima supremum.*

Djelomične uređaje kraće označavamo **CPO** (*Complete Partial Order*). Iako je, ako želimo biti potpuno korektni, potrebno pisati $(X, \leq)$ često ćemo radi jednostavnosti pisati samo X, pogotovo ako se podrazumijeva o kakvoj relaciji potpunog djelomičnog uređaja $\leq$ se radi ili ako to u danom trenutku nije važno.

Ako radimo u teoriji koja dopušta prazne lance, tj. koja dopušta da je i prazan skup usmjeren, onda vrijedi sljedeći teorem.

Teorem 3.7.1. *Svaki potpun djelomično uređen skup ima najmanji element.*

Dokaz. Neka je $(X, \leq)$ neki CPO. Vrijedi

$$(\forall x \in X)\,(\forall y \in \emptyset)\,y \leq x,$$

ili drugim riječima, svaki element skupa X je gornja međa praznog skupa. Označimo li

$$\sup \emptyset = \bot$$

dobijemo

$$(\forall x \in X)\,\bot \leq x,$$

pa je $\bot$ traženi najmanji element. ■

Uočimo da smo u dokazu koristili pretpostavku da je $\emptyset$ usmjeren skup i da po definiciji CPO-a ima supremum. Ako ne dopuštamo usmjerenost praznog skupa, onda se tvrdnja ovog teorema dodaje u definiciju CPO-a kao još jedan uvjet. Dakle, u tom slučaju bi djelomični uređaj bio potpun ako ima najmanji element i ako u njemu svaki usmjeren skup ima supremum.

Primjer 25. *Pogledajmo nekoliko poznatih djelomičnih uređaja.*

1. $(\mathbb{N} \cup \{\infty\}, \leq)$ *je CPO*
2. $(\mathbb{N}, \leq)$ *nije CPO*
3. $([0, \infty], \leq)$ *je CPO*
4. $\left(2^X, \subseteq\right)$ *je CPO.*

Funkcije definirane na CPO-ima imaju i neka lijepa svojstva. Sljedeća dva su važna za definiranje neprekidnih funkcija na takvim skupovima.

Teorem 3.7.2. *Neka su X i Y CPO-i. Ako je funkcija $f : X \to Y$ monotono rastuća i $A \subseteq X$ usmjeren u X onda je i $f(A) \subseteq Y$ usmjeren u Y.*

Dokaz. Uzmimo bilo koje $c, d \in f(A)$. To znači da postoje neki $a, b \in A$ takvi da je $f(a) = c$ i $f(b) = d$. Jer je A usmjeren u X to postoji neki $m \in A$ takav da je $a \leq m$ i $b \leq m$. Jer je f monotono rastuća to je $f(a) = c \leq f(m)$ i $f(b) = d \leq f(m)$. Dakle, $f(A)$ je usmjeren u Y. ■

Teorem 3.7.3. *Neka su X i Y CPO-i. Ako je funkcija $f : X \to Y$ monotono rastuća i skup $A \subseteq X$ usmjeren, onda je*

$$\sup f(A) \leq f(\sup A).$$

Dokaz. Po prethodnom teoremu znamo da je skup $f(A)$ usmjeren u Y, pa sigurno ima supremum. Uzmimo bilo koji $x \in A$. Vrijedi $x \leq \sup A$, a jer je f monotono rastuća slijedi $f(x) \leq f(\sup A)$. Iz ovoga uzimanjem supremuma po A, koji također postoji jer je A usmjeren u X, dobijemo

$$\sup_{x \in A} f(x) = \sup f(A) \leq \sup_{x \in A} f(\sup A) = f(\sup A).$$

■

Sada možemo dati definiciju neprekidnih funkcija na CPO-ima.

Definicija 3.7.4. *Neka su X i Y CPO-i. Kažemo da je monotono rastuća funkcija $f : X \to Y$ neprekidna ako za svaki usmjereni skup $A \subseteq X$ vrijedi*

$$f(\sup A) = \sup f(A).$$

Ekvivalentna definicija koja koristi ω-lance bila bi ova.

Definicija 3.7.5. *Neka su X i Y CPO-i. Kažemo da je monotono rastuća funkcija $f : X \to Y$ neprekidna ako za svaki ω-lanac $\{x_n\}_{n \in \mathbb{N}_0}$ u X vrijedi*

$$f\left(\sup_n x_n\right) = \sup_n f(x_n).$$

Vratimo se sada na teoriju računarstva. Ako elemente skupa X shvatimo kao konačne aproksimacije egzaktnog elementa $\sup X$, onda jednakost

$$f(\sup X) = \sup f(X)$$

znači da je vrijednost funkcije f na beskonačnom objektu $\sup X$ potpuno određena njenim vrijednostima na konačnim (početnim) aproksimacijama $x \in X$. To je smisao u kojem treba promatrati neprekidnost funkcija na CPO-ima.

Zanimljivo je da postoje monotone funkcije koje nisu neprekidne. Promotrimo skup $\{0,1\}^\infty$ svih nizova nula i jedinica, te na njemu definirajmo uređaj "prefiks". Na primjer, vrijedi $001 \leq 00100$, no nizovi 011 i 010 nisu međusobno usporedivi.

Lako se provjeri da je $(\{0,1\}^\infty, \leq)$ parcijalno uređen skup, i to potpun. I skup $\{\bot, \top\}$ uz uređaj $\bot \leq \top$ je CPO.

Definirajmo funkciju $f : \{0,1\}^\infty \to \{\bot, \top\}$ s

$$f(x) = \begin{cases} \top, & x \text{ ima beskonačan broj jedinica} \\ \bot, & \text{inače} \end{cases}.$$

Lako se vidi da je f dobro definirana monotono rastuća funkcija, no nije neprekidna! naime, vrijedi:

$$1 \leq 11 \leq 111 \leq \cdots \leq 1^n \leq \cdots,$$

i

$$f(1) = f(11) = f(111) = \cdots = f(1^n) = \bot, \qquad f(1^\infty) = \top.$$

Iz toga slijedi

$$\sup_n \{f(1^n)\} = \sup\{\bot\} = \bot \neq f\left(\sup_n 1^n\right) = f(1^\infty) = \top,$$

pa f nije neprekidna.

Sada ćemo dati ključni teorem ovog poglavlja koji ćemo nadalje često koristiti. No najprije definirajmo što je to čvrsta točka funkcije.

Definicija 3.7.6. *Neka je X skup i $f : X \to X$ funkcija. Kažemo da je $x \in X$ čvrsta (fiksna) točka funkcije f ako vrijedi $f(x) = x$.*

Teorem 3.7.4. *(Knaster-Tarski-Klenee) Ako je X CPO i $f : X \to X$ neprekidna funkcija onda f ima najmanju čvrstu točku.*

Dokaz. Kako je X CPO znamo da ima najmanji element, označimo ga s $\bot$. Promotrimo niz $\{f^n(\bot)\}_{n\in\mathbb{N}_0}$. Lako se pokaže da je taj niz lanac u X. Naime, kako je $\bot$ najmanji element u X vrijedi

$$\bot \leq f(\bot).$$

Jer je f neprekidna ona je i monotono rastuća, pa slijedi

$$f(\bot) \leq f^2(\bot).$$

Analogno dobijemo

$$f^2(\bot) \leq f^3(\bot),$$

a induktivno slijedi i

$$f^n(\bot) \leq f^{n+1}(\bot).$$

Dakle, $\{f^n(\bot)\}_{n\in\mathbb{N}_0}$ je lanac u X pa ima supremum. kako je f neprekidna vrijedi

$$f\left(\sup_n f^n(\bot)\right) = \sup_n f(f^n(\bot)) = \sup_n f^{n+1}(\bot) = \sup_n f^n(\bot),$$

pa je upravo $\sup_n f^n(\bot)$ čvrsta točka funkcije f.

Pokažimo još da je i najmanja. Pretpostavimo da je i neki $x \in X$ čvrsta točka funkcije f. Svakako je

$$\perp \leq x,$$

pa je i

$$f(\perp) \leq f(x) = x.$$

Slično kao i prije dobijemo

$$f^n(\perp) \leq x$$

iz čega slijedi

$$\sup f^n(\perp) \leq \sup_n x = x.$$

Dakle, $\sup f^n(\perp)$ je najmanja čvrsta točka funkcije f. ■

Na CPO-ima se mogu uvoditi i razni konstrukti: suma, direktna suma, Kartezijev umnožak, itd. Uz odgovarajuće uređaje oni i sami mogu biti CPO-i. Najzanimljiviji je Kartezijev umnožak CPO-a u kojem se uvodi uređaj "po koordinatama". On ima lijepo svojstvo da su funkcije definirane na njemu neprekidne ako i samo ako su neprekidne po koordinatama.

Poglavlje 4.

Principi indukcije

Dokazi raznih svojstava znatno ovise o izboru metode dokazivanja, a često je to neka iz familije metoda indukcije. Najčešće su to matematička indukcija i strukturalna indukcija, no one su obje posebni slučajevi jedne snažne metode dokazivanja koju zovemo dobro utemeljena indukcija.

4.1. Matematička indukcija

Skup prirodnih brojeva gradimo počevši od jedinice (u nekim slučajevima se počinje od nule), te dodajući redom sljedbenike. U tom skupu nema drugih brojeva osim onih dobivenih na ovaj način. Ovoj činjenici odgovara princip dokazivanja kojeg nazivamo *matematička indukcija*.

Neka je $P(n)$ neko svojstvo prirodnih brojeva. Princip matematičke indukcije kaže sljedeće: želimo li dokazati da svojstvo $P(n)$ imaju svi prirodni brojevi n dovoljno je dokazati da

1. vrijedi $P(1)$
2. za bilo koji prirodni broj m iz pretpostavke da vrijedi $P(m)$ mora slijediti i da vrijedi $P(m+1)$.

U logičkoj notaciji to bismo zapisali ovako:

$$(\forall n \in \mathbb{N})\, P(n) \leftrightarrow (P(1) \wedge (\forall m \in \mathbb{N})\, (P(m) \longrightarrow P(m+1))).$$

Princip matematičke indukcije je intuitivno vrlo jasan, a po svom obliku je sličan ostalim principima indukcije. Uočimo da kad god neko svojstvo $P(n)$ ne vrijedi za sve prirodne brojeve n, onda postoji neki najmanji prirodni broj m za kojeg ono ne vrijedi.

4.2. Strukturalna indukcija

Ovaj princip upotrebljavamo kada želimo dokazati da neko svojstvo $P(x)$ imaju svi elementi skupa S "izgrađenog po pravilu". Takvi su oni skupovi čiji su elementi izgrađeni počevši od atoma a nekim danim pravilom R. Ovo je, naravno, najjednostavniji slučaj jer općenito može postojati bilo koji broj atoma i pravila. Princip

strukturalne indukcije kaže sljedeće: želimo li dokazati da svojstvo $P(x)$ imaju svi elementi x skupa S dovoljno je dokazati da

1. vrijedi $P(a)$
2. za bilo koji $x \in S$ iz pretpostavke da vrijedi $P(x)$ mora slijediti i da vrijedi $P(R(x))$.

Pogledajmo konkretno kako bi to izgledalo kada bi S bio skup svih aritmetičkih izraza nastalih gradnjom pomoću operacija iz skupa $\{+, -, \times\}$, a počevši od atoma koji su cijeli brojevi ili lokacije (varijable). U ovom slučaju princip strukturalne indukcije kaže: da bismo dokazali da neko svojstvo $P(a)$ vrijedi za sve aritmetičke izraze $a \in$Aexp dovoljno je dokazati da

1. $P(m)$ vrijedi za sve $m \in \mathbb{Z}$
2. $P(x)$ vrijedi za sve $x \in$Loc
3. ako za proizvoljne $a_1, a_2 \in$Aexp vrijedi $P(a_1)$ i $P(a_2)$ onda vrijedi i $P(a_1 \circ a_2)$, gdje je $\circ$ bilo koja operacija iz $\{+, -, \times\}$.

U logičkoj notaciji to bismo zapisali ovako:

$$\begin{aligned} & (\forall a \in \text{Aexp})\, P(a) \\ \longleftrightarrow\ & ((\forall m \in \mathbb{Z})\, P(m) \wedge (\forall x \in \text{Loc})\, P(x) \\ & \wedge (\forall a_1, a_2 \in \text{Aexp})\, (\forall \circ \in \{+, -, \times\})\, (P(a_1) \wedge P(a_2) \longrightarrow P(a_1 \circ a_2))) . \end{aligned}$$

Slično kao kod matematičke indukcije, kad god neko svojstvo $P(a)$ ne vrijedi za neki izraz a, onda postoji neki njegov najmanji podizraz e za kojeg ne vrijedi $P(e)$. Ovo funkcionira s toga što se nijedan aritmetički izraz ne može usitnjavati do u beskonačnost: kada tad dođemo do atoma koji su nedjeljivi. Ovo možemo tumačiti i ovako: ako je uređaj među izrazima definiran kao "biti podizraz", onda u skupu Aexp nema beskonačnih padajućih lanaca. Drugim riječima, uz ovakav uređaj Aexp dobro utemeljen skup. Ovo nas vodi do općeg principa indukcije koji ujedinjuje ova dva prethodna.

4.3. Dobro utemeljena (transfinitna) indukcija

Teorem 4.3.1. *Neka je $\prec$ dobro utemeljena relacija na skupu X i $P(x)$ neko svojstvo elemenata skupa X. Vrijedi*

$$(\forall x \in X)\, P(x) \longleftrightarrow (\forall x \in X)\, ((\forall y \precapprox x)\, P(y) \longrightarrow P(x)) .$$

Drugim riječima: ako želimo dokazati da svojstvo $P(x)$ vrijedi za sve elemente x skupa X dovoljno je dokazati da za proizvoljni $x \in X$ iz pretpostavke da $P(y)$ vrijedi za sve (prave) prethodnike y elementa x slijedi da vrijedi i $P(x)$.

Dokaz. Smjer nužnosti je očigledan, pa dokažimo samo smjer dovoljnosti. Dokaz provodimo kontradikcijom. Pretpostavimo da vrijedi

$$(\forall x \in X)\, ((\forall y \precapprox x)\, P(y) \longrightarrow P(x))$$

i da postoji neki $a \in X$ takav da vrijedi $\neg P(a)$. U tom slučaju je skup

$$S = \{x \in X : \neg P(x)\}$$

neprazan, pa ima minimalni element po $\prec$, neki $m \in S$. I za njega vrijedi $\neg P(m)$. No s druge strane, svi elementi skupa X koji su ispred m nisu u skupu S, pa za njih mora vrijediti svojstvo P. No po pretpostavci bi tada moralo vrijediti i $P(m)$, pa smo došli do kontradikcije. Dakle, skup S mora biti prazan, odnosno $(\forall x \in X)\, P(x)$. ■

Transfinitna indukcija je, dakle, vrlo važan alat u dokazivanju tvrdnji na skupovima koji su dobro utemeljeni, no postavlja se pitanje koliko ima takvih skupova? Sljedeći teorem nam govori da su takvi u stvari svi neprazni skupovi, što nam još više ističe značaj ovog principa indukcije.

Teorem 4.3.2. *Neka je S proizvoljni neprazni skup. Tada postoji binarna relacija kojom je skup S dobro utemeljen.*

Dokaz. Dokaz ovog teorema bazira se na Aksiomu izbora. ■

Poglavlje 5.

Grafovi i stabla

U poglavljima koja slijede često ćemo razne aptraktne objekte (na primjer automate) ili postupke (na primjer izvode riječi) prikazivati pomoću grafova ili stabala. Stoga ćemo ukratko dati neke osnovne definicije donekle prilagođene našim potrebama.

Definicija 5.0.1. *Graf G je uređeni par $G = (V, E)$, pri čemu je V konačan skup čije elemente nazivamo čvorovima, a E skup (neuređenih) parova čvorova koje nazivamo bridovima.*

Definicija 5.0.2. *Put u grafu je niz čvorova među kojima postoje bridovi, drugim riječima to je niz $\{v_i\}_{i\in I} \subseteq V$, $I = \{1, 2, \ldots, k\}$, $k \in \mathbb{N}$, takav da vrijedi*

$$(\forall i \in I \setminus \{k\})\ (v_i, v_{i+1}) \in E.$$

Duljina ovakvog puta je $k - 1$.

Definicija 5.0.3. *Usmjereni graf je uređeni par $G = (V, E)$, pri čemu je V konačan skup čije elemente nazivamo čvorovima, a E skup uređenih parova čvorova koje nazivamo strelicama. Ako je $(v_i, v_k) \in E$ pišemo $v_i \to v_k$. Kažemo da je v_i prethodnik od v_k, a v_k sljedbenik od v_i.*

Definicija 5.0.4. *Put u usmjerenom grafu je niz čvorova među kojima postoje strelice, drugim riječima to je niz $\{v_i\}_{i\in I} \subseteq V$, $I = \{1, 2, \ldots, k\}$, $k \in \mathbb{N}$, takav da vrijedi*

$$(\forall i \in I \setminus \{k\})\ v_i \to v_{i+1}.$$

Kažemo da je to put od v_1 k v_k. Duljina ovakvog puta je $k - 1$.

Definicija 5.0.5. *Stablo je usmjereni graf za kojeg vrijedi:*

1. *postoji točno jedan čvor zvan korijen koji nema prethodnika i od kojeg vodi put do svakog čvora*
2. *svaki čvor, osim korijena, ima točno jednog prethodnika*
3. *sljedbenici svakog čvora uređeni s s lijeva.*

Za stabla se koristi posebna terminologija različita od one za grafove. Sljedbenik nekog čvora je njegov **sin**, a prethodnik mu je **otac**. Ako postoji put od v_i do v_k onda kažemo da je v_k **potomak** čvora v_i, odnosno da je v_i **predak** čvora v_k. Svaki čvor je sam sebi i potomak i predak. Čvor bez potomaka je **list**, dok su svi čvorovi koji nisu listovi **unutrašnji čvorovi**.

Poglavlje 6.

Konačni automati

6.1. Sustavi s konačnim brojem stanja

Konačni automat je matematički model sustava kojeg karakteriziraju diskretni ulaz te konačni broj mogućih stanja od kojih svako sadrži samo one informacije o prošlosti koje su potrebne za određenje budućeg ponašanja sustava. Na primjer, takav je sustav kontrolni mehanizam dizala.

U računalnoj znanosti nalazimo mnoštvo primjera takvih sustava, a teorija konačnih automata je vrlo korisna za njihovo dizajniranje. Neki od svakodnevno korištenih programa kao što su tekst-editori i leksički analizatori dizajniraju se pomoću sustava s konačnim brojem stanja.

Prije formalne definicije promotrimo jedan jednostavan primjer. Zamislimo da neki čovjek stoji na lijevoj obali rijeke te da čamcem u koji jedva stanu on i još "nešto" mora preći na desnu obalu te rijeke. Čovjek mora prevesti vuka, kozu i zelje, a jasno je da ne smije same na lijevoj obali ostavljati vuka i kozu ili kozu i zelje. Može li čovjek uspješno sve prevesti na desnu obalu i ako može na koji način to treba učiniti? Matematički model ovog problema opisuje svako stanje skupovima "stanovnika" lijeve i desne obale rijeke. Očito postoji $16 = 2^4$ mogućih particija skupa $\{č, v, k, z\}$ na dva dijela. Početno stanje bi bilo $\{č, v, k, z\} - \emptyset$, a završno $\emptyset - \{č, v, k, z\}$. Neka stanja kao na primjer $\{k, z\} - \{č, v\}$ su fatalna, pa ne mogu biti dozvoljena u našem sustavu. Ulazi bi opisivali akcije koje poduzima čovjek: kako on mora uvijek biti u brodu prilikom prelaska, to je dovoljno navesti njegovog suputnika ako nije sam. Na primjer, ulaz k bi značio da čovjek prevozi kozu, a ulaz $č$ samog sebe. Ovisno o ulazu mijenjalo bi se stanje sustava. Na primjer, ako smo bili u stanju $\{v, z\} - \{č, k\}$ i na ulazu bi imali $č$, novo stanje bi bilo $\{v, z, č\} - \{k\}$. Dijagram prelaza bi bio:

slika KA1

Uočimo da automat ima jedno početno stanje, jedno završno stanje (u ovom slučaju), te da u svakom stanju pamti samo najnužnije za prelaz u sljedeće stanje.

6.2. Osnovni pojmovi

Simbol ili **slovo** je apstrakti pojam koji se ne definira baš kao ni točka u geometriji. **Abeceda** je bilo koji skup slova, a za naše potrebe dostajat će konačne abecede.

Abecede ćemo najčešće označavati velikim grčkim slovom Σ. **Riječ** u abecedi Σ je konačan niz slova abecede Σ, a riječi najčešće označavamo latiničnim slovima $w, u, v, z, \ldots$ Skup svih riječi u abecedi Σ označavamo s Σ^*. **Duljina riječi** w, u oznaci $|w|$, je broj slova u njoj. Jedina riječ duljine nula je **prazna riječ**, a označavamo je s ε. **Prefiks** neke riječi je njen početni komad bilo koje duljine, dok je **sufiks** neke riječi njen završni komad bilo koje duljine. Ako se prefiks odnosno sufiks razlikuju od same riječi onda kažemo da su pravi prefiks odnosno pravi sufiks. **Podriječ** neke riječi je bilo koja riječ sadržana u njoj. **Palindrom** je riječ koja se čita jednako sprijeda i straga.

Osnovna operacija među riječima je **konkatenacija** ili "ljepljenje" riječi. Ako su w_1 i w_2 riječi, onda je

$$w_1 w_2$$

(čitamo w_1 konkatenacija w_2) također riječ. Neutralni element za konkatenaciju je prazna riječ jer vrijedi

$$(\forall w)\ \ \varepsilon w = w\varepsilon = w.$$

Jezik u abecedi Σ je bilo koji skup riječi abecede Σ, a najčešće ga označavamo velikim latiničnim slovom L. Očito je $L \subseteq \Sigma^*$, odnosno $L \in 2^{\Sigma^*}$. Po definiciji su i $\emptyset$ i $\{\varepsilon\}$ jezici, i to različiti.

6.3. Deterministički konačni automat (DKA)

Definicija 6.3.1. *Deterministički konačni automat (ili kraće konačni automat) je uređena petorka $(Q, \Sigma, \delta, q_0, F)$ pri čemu je:*

1. *Q konačan skup čije elemente nazivamo stanjima*
2. *Σ abeceda koju nazivamo abecedom ulaza*
3. *$q_0 \in Q$ istaknuto stanje koje nazivamo početnim stanjem*
4. *$F \subseteq Q$ skup istaknutih stanja koja nazivamo završnim stanjima*
5. *$\delta : Q \times \Sigma \to Q$ parcijalna funkcija koju nazivamo funkcijom prelaza.*

Kako interpretiramo funkciju prelaza? Prelaz $\delta(p, a) = q$, gdje su $p, q \in Q$ i $a \in \Sigma$, znači sljedeće: ako je automat u stanju p i na ulazu mu se pojavi slovo a onda se vrši prelazak u stanje q.

Funkciju δ vrlo jednostavno možemo proširiti tako da postane totalna funkcija. Točnije, dodamo li skupu stanja Q još jedno novo stanje $q_{trash} \notin Q$ možemo na jedinstven način definirati totalnu funkciju $\delta' : Q \times \Sigma \to Q \cup \{q_{trash}\}$ za koju vrijedi

$$\delta'(p, a) = \begin{cases} \delta(p, a), & \delta(p, a) \downarrow \\ q_{trash}, & \delta(p, a) \uparrow \end{cases}, \ p \in Q, a \in \Sigma.$$

Kako je δ' jedinstveno proširenje koje postoji za svaku funkciju prelaza δ (u najboljem slučaju je $\delta' = \delta$) to ćemo ubuduće δ tretirati kao totalnu funkciju. Ipak, treba pamtiti da je ona u stvarnosti najčešće parcijalna funkcija jer ne moraju postojati

prelazi iz svih stanja za sve moguće ulaze (štoviše, iz nekih stanja ne mora ni biti izlaza).

Svakom konačnom automatu se na jedinstven način pridružuje usmjereni graf zvan **dijagram prelaza** i to na sljedeći način: čvorovima grafa odgovaraju stanja, a strelicama grafa prelazi. Strelice su labelirane odgovarajućim slovima na ulazu. Ako pri ulazu a postoji prelaz iz stanja p u stanje q, onda u dijagramu prelaza postoji strelica između stanja p i q označena slovom a ($p \xrightarrow{a} q$). Čvorovi koji odgovaraju završnim stanjima su istaknuti podebljanim rubom, dok u čvor koji predstavlja početno stanje vodi strelica s labelom START.

Pogledajmo jedan primjer. Neka je automat M definiran s

1. $Q = \{q_0, q_1, q_2, q_3\}$
2. $\Sigma = \{0, 1\}$
3. q_0 je početno stanje
4. $F = \{q_0\}$
5. δ je definirana tablicom:

u-s	q_0	q_1	q_2	q_3
0	q_2	q_3	q_0	q_1
1	q_1	q_0	q_3	q_2

.

Ovakvom konačnom automatu odgovarao bi dijagram prelaza kao na slici.

slika KA2

Da bismo mogli "čitati" riječi (a ne samo pojedinačna slova) moramo proširiti funkciju δ na skup $Q \times \Sigma^*$, a novodobivenu funkciju označit ćemo s δ^*. Funkcija $\delta^* : Q \times \Sigma^* \to Q$ definirana je s

1. $(\forall p \in Q)\ \ \delta^*(p, \varepsilon) = p$
2. $(\forall p \in Q)\,(\forall w \in \Sigma^*)\,(\forall a \in \Sigma)\ \ \delta^*(p, wa) = \delta(\delta^*(p, w), a)$.

Ovo znači da bez čitanja slova na ulazu ne možemo promijeniti stanje, te ako je ulaz neprazan i na njemu je riječ wa najprije pređemo u stanje $\delta^*(p, w) = q$, a zatim u stanje $\delta^*(q, a) = \delta(q, a)$. Vidimo da je $\delta^*(p, w)$ jedinstveno stanje takvo da u dijagramu prelaza do njega postoji put iz stanja p označen labelama koje čitane redom s lijeva na desno tvore riječ w. Kako je funkcija δ^* jedinstveno određena funkcijom prelaza δ to se u praksi najčešće potpuno zanemaruje formalna razlika među njima pa se i označavju istim slovom δ. Uočimo da kvantifikaciju u točki 2. treba shvatiti u smislu prethodne napomene o proširivanju funkcije δ na totalnu funkciju. Strogo gledano kvantifikacija bi se smjela provoditi samo na onim stanjima i slovima na kojima je δ definirana, no radi jednostavnosti ćemo to zadržati na intuitivnoj razini. Kada god ustrebamo strogo razmatranje možemo koristiti proširenu funkciju δ' kod koje se ne javljaju takvi problemi.

Konačni automat "prihvaća" riječ w ako niz prelaza koji po ulaznim slovima odgovaraju riječi w vodi od početnog stanja u neko od završnih. Drugim riječima, konačni automat $M = (Q, \Sigma, \delta, q_0, F)$ prihvaća riječ w ako vrijedi

$$\delta(q_0, w) = p, \quad p \in F.$$

Definicija 6.3.2. *Jezik $L(M)$ kojeg prihvaća konačni automat $M = (Q, \Sigma, \delta, q_0, F)$ je skup riječi u abecedi Σ definiran s*

$$L(M) = \{w \in \Sigma^* : \delta(q_0, w) \in F\}.$$

Klasu svih jezika koje prihvaćaju konačni automati označavat ćemo s KAJ, odnosno

$$KAJ = \{L : (\exists \text{ konačni automat } M)\ L(M) = L\}.$$

6.4. Nedeterministički konačni automat (NKA)

Pojam **nedeterminizma** igra vrlo važnu ulogu u teoriji računarstva, pa se je s njime dobro upoznati već na ovom jednostavnom nivou u kome (kako će se kasnije pokazati) nije nužan.

Zašto smo konačne automate iz prethodne cjeline zvali *deterministički konačni automati*? To je očigledno već iz prirode same funkcije prelaza δ : slike pridružene parovima (p, a) su stanja. Drugim riječima, jednom kada smo došli u stanje p a na ulazu se pojavilo slovo a nemamo izbora - neminovno ćemo preći u stanje $\delta(p, a)$ (pod uvjetom da je δ definirana u (p, a)). Naš cilj je ovakav model apstraktnog stroja proširiti na način da dozvolimo prelaze u nula, jedno ili više mogućih stanja pri istom slovu na ulazu. Dakle, razlika bi bila u definiciji funkcije prelaza δ : ona bi sada za slike uzimala elemente partitivnog skupa 2^Q. Takav novi automat zovemo **nedeterministički konačni automat**.

Pogledajmo jedan primjer.

$$slikaKA3$$

Lako se vidi da automat sa slike prihvaća sve riječi u abecedi $\{0, 1\}$ koje sadrže dvije sljedne nule ili dvije sljedne jedinice. Nedeterminizam se očituje u prelascima iz početnog stanja q_0 : pri pojavi slova 0 na ulazu možemo preći u stanja q_0 ili q_3, a pri pojavi slova 1 u stanja q_0 ili q_1. Sam odabir se vrši na nedeterministički način, a mogućnost takvog odabira nam osigurava **Aksiom izbora**.

Definicija 6.4.1. *Nedeterministički konačni automat je uređena petorka $(Q, \Sigma, \delta, q_0, F)$ pri čemu je:*

1. *Q konačan skup čije elemente nazivamo stanjima*
2. *Σ abeceda koju nazivamo abecedom ulaza*
3. *$q_0 \in Q$ istaknuto stanje koje nazivamo početnim stanjem*
4. *$F \subseteq Q$ skup istaknutih stanja koja nazivamo završnim stanjima*
5. *$\delta : Q \times \Sigma \to 2^Q$ parcijalna funkcija koju nazivamo funkcijom prelaza.*

Kako sada interpretiramo funkciju prelaza? Prelaz $\delta(p,a) = \{q_1, \ldots, q_n\}$, gdje su $p, q_1, \ldots, q_n \in Q$ i $a \in \Sigma$, znači sljedeće: ako je automat u stanju p i na ulazu mu se pojavi slovo a onda se na nedeterministički način odabire neki $i \in \{1, \ldots, n\}$ i automat prelazi u stanje q_i. Nadalje, nećemo to u definiciji δ posebno naglašavati, no jasno je da preslikavanje tipa $\delta(p,a) = \emptyset$ nema smisla, pa takvu mogućnost **isključujemo**.

Slično kao i prije, da bismo čitali riječi moramo proširiti funkciju δ na skup $Q \times \Sigma^*$. Funkcija $\delta^* : Q \times \Sigma^* \to 2^Q$ definirana je s

1. $(\forall p \in Q)\ \ \delta^*(p, \varepsilon) = \{p\}$
2. $(\forall p \in Q)\,(\forall w \in \Sigma^*)\,(\forall a \in \Sigma)$

$$\delta^*(p, wa) = \{q \in Q : (\exists r \in \delta^*(p,w))\, q \in \delta(r,a)\}.$$

Korisno je proširiti i samu δ^* na način da možemo čitati riječi na skupovima stanja. Dakle, trebamo proširenje $\delta^{**} : 2^Q \times \Sigma^* \to 2^Q$ definirano s

3. $\left(\forall P \in 2^Q\right)(\forall w \in \Sigma^*)\ \ \delta^{**}(P, w) = \bigcup_{p \in P} \delta^*(p, w)$.

I opet ćemo zanemariti formalnu razliku među funkcijama δ, δ^* i δ^{**} jer su za danu funkciju prelaza δ proširenja δ^* i δ^{**} definirana na jedinstven način. Kao i uslučaju DKA funkciju δ možemo na jedinstven način proširiti do totalne funkcije δ' dodavanjem još jednog stanja q_{trash} skupu Q pa ćemo kada nam god ustreba funkciju δ tretirati kao da je totalna funkcija.

Sada možemo definirati jezik kojeg prihvaća neki nedeterministički automat.

Definicija 6.4.2. *Jezik $L(M)$ kojeg prihvaća nedeterministički konačni automat $M = (Q, \Sigma, \delta, q_0, F)$ je skup riječi u abecedi Σ definiran s*

$$L(M) = \{w \in \Sigma^* : \delta(q_0, w) \cap F \neq \emptyset\}.$$

Klasu svih jezika koje prihvaćaju nedeterministički konačni automati označavat ćemo s $NKAJ$, odnosno

$$NKAJ = \{L : (\exists \text{ nedet. kon. automat } M)\ \ L(M) = L\}.$$

6.5. Ekvivalencija klasa KAJ i $NKAJ$

Očigledno je da svaki deterministički konačni automat možemo smatrati posebnim slučajem nedeterminističkog konačnog automata u kome su sve slike funkcije δ jednočlani skupovi. Iz te činjenice odmah slijedi da je klasa jezika koje prihvaćaju deterministički konačni automati sadržana u klasi jezika koje prihvaćaju nedeterministički konačni automati, odnosno da vrijedi inkluzija $DKAJ \subseteq NKAJ$. No zanimljivo je da iako model NKA naizgled predstavlja pravo proširenje modela DKA on to nije. Dokazat ćemo, naime, da vrijedi i obratna inkluzija.

Teorem 6.5.1. *($NKAJ \subseteq DKAJ$) Neka je L jezik kojeg prihvaća neki NKA. Tada postoji i neki DKA koji prihvaća L.*

Dokaz. Neka je L jezik kojeg prihvaća nedeterministički konačni automat $M = (Q, \Sigma, \delta, q_0, F)$. Definirat ćemo deterministički konačni automat $M' = (Q', \Sigma, \delta', q_0', F')$ na sljedeći način:

(i) Uvest ćemo oznaku $\{q_1, \ldots, q_n\} = [q_1, \ldots, q_n]$, za svaki $\{q_1, \ldots, q_n\} \subseteq Q$

(ii) $Q' = 2^Q$

(iii) $q_0' = \{q_0\} = [q_0]$

(iv) $F' = \{q' \in Q' : q' \cap F \neq \emptyset\}$

(v) funkciju prelaza δ' definiramo uvjetom da za sve $a \in \Sigma, p_1, \ldots, p_i, q_1, \ldots, q_j \in Q$ vrijedi

$$\delta'([p_1, \ldots, p_i], a) = [q_1, \ldots, q_j] \longleftrightarrow \delta(\{p_1, \ldots, p_i\}, a) = \{q_1, \ldots, q_j\}.$$

Dokaz provodimo tako da najprije indukcijom po duljini ulazne riječi x dokažemo pomoćnu tvrdnju

$$T: \ \delta'(q_0', x) = [q_1, \ldots, q_j] \longleftrightarrow \delta(q_0, x) = \{q_1, \ldots, q_j\}.$$

Ako je duljina ulazne riječi x jednaka 0, onda je $x = \varepsilon$, pa je

$$\delta'(q_0', \varepsilon) = q_0' = [q_0] \longleftrightarrow \delta(q_0, \varepsilon) = \{q_0\}.$$

Pretpostavimo da tvrdnja T vrijedi za ulazne riječi x duljine manje od $n \in \mathbb{N}$.

Neka je x neka ulazna riječ duljine n. Tada je $x = ya$, gdje je y ulazna riječ duljine manje od n i $a \in \Sigma$. Na riječ y možemo primijeniti pretpostavku indukcije tvrdnje T, pa dobijemo

$$\delta'(q_0', y) = [p_1, \ldots, p_i] \longleftrightarrow \delta(q_0, y) = \{p_1, \ldots, p_i\}.$$

S druge strane, po definiciji funkcije prelaza δ' znamo da vrijedi

$$\delta'([p_1, \ldots, p_i], a) = [q_1, \ldots, q_j] \longleftrightarrow \delta(\{p_1, \ldots, p_i\}, a) = \{q_1, \ldots, q_j\}.$$

Koristeći tranzitivnost ekvivalencije dobijemo

$$\delta'(q_0', ya) = [q_1, \ldots, q_j] \longleftrightarrow \delta(q_0, ya) = \{q_1, \ldots, q_j\}.$$

Ovim je dokazan korak indukcije, a time i tvrdnja T.

Ako sada primijetimo da $\delta'(q_0', x)$ leži u F' ako i samo ako $\delta(q_0, x)$ sadrži neko završno stanje iz tvrdnje T odmah dobijemo da vrijedi

$$\delta'(q_0', x) \in F' \longleftrightarrow \delta(q_0, x) \cap F \neq \emptyset,$$

pa je

$$L(M') = L(M).$$

■

6.6. NKA s praznim prelazima (NKA_ε)

Model NKA s kojim smo se upoznali može se proširiti na način da dozvolimo prelaze u nova stanja čak i ako se nije pojavilo ništa na ulazu. Takve prazne prelaze nazivamo ε-prelazima, a kako to može izgledati vidi se na sljedećem dijagramu prelaza.

$$slikaKA4$$

Tako dobiveni prošireni model nedetrminističkog automata zovemo **nedetrministički automat s ε-prelazima**, a kraće ga označavmo s NKA_ε. Definicija samog automata ostaje ista osim što podrazumijevamo da su mogući prelazi ako je na ulazu ε, tj. u dijagramu prelaza takvog automata dio puta koji prelazimo čitajući ulaznu riječ mogu tvoriti i bridovi označeni s ε koji se ne javljaju eksplicitno u ulaznoj riječi.

Koliko god izgledalo da smo s ovim napravili pravo proširenje modela NKA slično kao i prije pokazat će se da klasa jezika koju prihvaćaju NKA_ε ostaje ista kao klasa jezika koju prihvaćaju NKA. Inkluzija $NKAJ \subseteq NKA_\varepsilon J$ je očigledna: svaki NKA može se promatrati kao poseban slučaj NKA_ε u kome nema ε-prelaza. Sljedeći teorem nam daje i obratnu inkluziju.

Teorem 6.6.1. *($NKA_\varepsilon J \subseteq NKAJ$) Neka je L jezik kojeg prihvaća neki NKA_ε. Tada postoji i neki NKA koji prihvaća L.*

Dokaz. Prije nego definiramo NKA koji prihvaća jezik L uvest ćemo neke oznake. Neka je L jezik kojeg prihvaća neki NKA_ε u oznaci $M = (Q, \Sigma, \delta, q_0, F)$.

Za $p \in Q$ s $Cl_\varepsilon(p)$ označit ćemo skup svih stanja $q \in Q$ takvih da u dijagramu prelaza automata M postoji put od p do q označen samim ε-ima. Prirodno to proširujemo i na skupove stanja na sljedeći način:

$$Cl_\varepsilon(\{p_1, \ldots, p_n\}) = \bigcup_{i=1}^{n} Cl_\varepsilon(p_i).$$

Krenimo sada na sam dokaz. Definiramo novi automat $M' = (Q, \Sigma, \delta', q_0, F')$ na sljedeći način:

(i) Skup završnih stanja F' definiramo kao

$$F' = \begin{cases} F \cup \{q_0\}, & Cl_\varepsilon(q_0) \cap F \neq \emptyset \\ F, & \text{inače} \end{cases}.$$

(ii) Funkciju prelaza δ' definiramo posredno uvodeći najprije proširenu funkciju prelaza $\delta^* : Q \times \Sigma^* \to 2^Q$ za $p \in Q$, $P, R \subseteq Q$, $a \in \Sigma$ i $w \in \Sigma^*$ definiranu s

$$\begin{aligned} \delta^*(p, \varepsilon) &= Cl_\varepsilon(p), \\ \delta^*(p, wa) &= Cl_\varepsilon(R), \quad R = \{r \in Q : r \in \delta(q, a),\ q \in \delta^*(p, w)\}, \\ \delta^*(P, w) &= \bigcup_{p \in P} \delta^*(p, w). \end{aligned}$$

Ovakav postupak je nužan jer δ dozvoljava "čitanje" ε-na dok nova funkcija prelaza δ' to neće smjeti. Sada jednostavno za proizvoljne $p \in Q$ i $a \in \Sigma$ stavljamo

$$\delta'(p, a) = \delta^*(p, a).$$

Uočimo da automat M' nema ε-prelaza, a prihvaćanje prazne riječi smo osigurali definicijom skupa F'. Sada se indukcijom poduljini ulazne riječi x (počevši od baze $|x| = 1$) lako dokaže da za bilo koju ulaznu riječ $x \in \Sigma^* \setminus \{\varepsilon\}$ vrijedi

$$\delta'(q_0, x) = \delta(q_0, x),$$

te da je $\delta'(q_0, x) \cap F' \neq \emptyset$ ako i samo ako je $\delta(q_0, x) \cap F \neq \emptyset$. Iz ovoga slijedi $L(M') = L(M)$. ■

Poglavlje 7.

Regularni jezici

7.1. Osnovni pojmovi

U ovom odjeljku ćemo se upoznati s jednostavnim izrazima koji opisuju klasu **re -gularnih jezika**. Važnost ovih izraza je u tome što se ta klasa poklapa s klasom jezika koje prihvaćaju konačni automati, pa ćemo dobiti jednostavan način za opisivanje jezika koje prihvaćaju konačni automati. Kasnije ćemo vidjeti da takav zapis omogućava jednostavno povezivanje znanja o neprekidnim funkcijama definiranim na CPO-ima i znanja o regularnim jezicima, odnosno KA jezicima.

Definicija 7.1.1. *Neka je Σ abeceda i L, L_1 i L_2 skupovi iz 2^{Σ^*}.*

1. *Konkatenacija skupova L_1 i L_2, u oznaci L_1L_2, je skup*

$$L_1L_2 = \{xy : x \in L_1 \wedge y \in L_2\}$$

2. *Kleenejevo zatvorenje skupa L, u oznaci L^*, je skup*

$$L^* = \bigcup_{i=0}^{\infty} L^i$$

gdje je

$$\begin{aligned} L^0 &= \{\varepsilon\} \\ (\forall n \in \mathbb{N})\, L^n &= LL^{n-1}. \end{aligned}$$

Uočimo da se u skladu s prethodnim prirodno definira skup

$$L^+ = \bigcup_{i=1}^{\infty} L^i = LL^*,$$

te da vrijedi

$$\varepsilon \in L^+ \text{ akko } \varepsilon \in L.$$

Sada kada smo definirali ove osnovne operacije na skupovima možemo dati definiciju regularnih izraza i skupova (jezika) koje oni opisuju.

Definicija 7.1.2. *Neka je Σ abeceda. Regularni izrazi i skupovi koje oni opisuju definirani su induktivno na sljedeći način:*

1. *$\emptyset$ je regularni izraz koji opisuje prazan skup*
2. *ε je regularni izraz koji opisuje skup $\{\varepsilon\}$*
3. *$a \in \Sigma$ je regularni izraz koji opisuje skup $\{a\}$*
4. *ako su r i s regularni izrazi koji redom opisuju skupove R i S, onda su $(r+s)$, (rs) i (r^*) regularni izrazi koji redom opisuju skupove $R \cup S$, RS i R^*.*

Uvođenjem prednosti među operacijama možemo izbjeći pisanje suvišnih zagrada. Smatramo da najjače veže *, zatim konkatenacija i na kraju +. Tako, na primjer, izraz

$$((0\,(1^*)) + 0)$$

možemo uz uvažavanje prednosti pisati kao

$$01^* + 0.$$

Također, uvodimo izraz r^+ kao kraći zapis za rr^*.

Definicija 7.1.3. *Neka je r regularni izraz. Odgovarajući skup kojeg r opisuje označavamo s $L(r)$ i nazivamo jezikom opisanim izrazom r. Klasu jezika opisanih regularnim izrazima nazivamo klasom regularnih jezika i označavamo s RJ.*

Primjedba 7.1.1. *Iako strogo matematički gledano treba razlikovati regularne izraze i skupove koje oni opisuju mi ćemo ih zbog jednostavnosti ponekad u zapisima poistovjećivati (osobitu prilikom korištenja tzv. aritmetike regularnih izraza). Stoga npr. zapis $w \in r$ tumačimo kao "riječ w pripada skupu opisanom regularnim izrazom r" iako bi to trebalo zapisati kao $w \in L(r)$.*

7.2. Ekvivalencija klasa KAJ i RJ

U ovom odjeljku ćemo dokazati da su klase KAJ i RJ u stvari jedna te ista klasa jezika. Kroz dva teorema dokazat ćemo da vrijedi $RJ \subseteq NKA_\varepsilon J$ i $KAJ \subseteq RJ$, no koristeći saznanja iz prethodnog poglavlja moći ćemo zaključiti da je $KAJ = RJ$.

Teorem 7.2.1. *($RJ \subseteq NKA_\varepsilon J$) Neka je r neki regularni izraz. Tada postoji neki NKA_ε koji prihvaća $L(r)$.*

Dokaz. Mi ćemo dokazati čak i jaču tvrdnju nego je tvrdnja teorema.

(T): za svaki regularni izraz r postoji neki NKA_ε M sa samo jednim završnim stanjem iz kojeg nema prelaza, a koji prihvaća $L(r)$.

Dokaz provodimo strukturalnom indukcijom.

Baza indukcije.

Ako je r atom imamo tri moguća slučaja, a za svaki od njih dat ćemo dijagram prelaza odgovarajućeg automata M.

(i) $r = \varepsilon$

$slikaRJ1$

(ii) $r = \emptyset$

$slikaRJ2$

(iii) $r = a \in \Sigma$

$slikaRJ3$

Dokažimo sada da ovakvo svojstvo regularnih izraza ne gubi primjenom pravila gradnje regularnih izraza.

Neka su r_1 i r_2 regularni izrazi za koje vrijedi tvrdnja T. Tada postoje odgovarajući automati $M_1 = (Q_1, \Sigma_1, \delta_1, q_1, \{f_1\})$ i $M_2 = (Q_2, \Sigma_2, \delta_2, q_2, \{f_2\})$ takvi da redom prihvaćaju jezike $L(r_1)$ i $L(r_2)$. Bez smanjenja općenitosti možemo pretpostaviti da vrijedi $Q_1 \cap Q_2 = \emptyset$, jer uvjek možemo preimenovati stanja automata M_1 ili M_2 tako da to bude ispunjeno. S obzirom na pravila gradnje regularnih izraza imamo tri moguća slučaja:

(i) $r = r_1 + r_2$

Definirat ćemo novi NKA_ε $M = (Q, \Sigma, \delta, q_0, \{f_0\})$ sa samo jednim završnim stanjem iz kojeg nema prelaza na sljedeći način

$$\begin{aligned} Q &= Q_1 \cup Q_2 \cup \{q_0, f_0\}, \quad q_0, f_0 \notin Q_1 \cup Q_2, \\ \Sigma &= \Sigma_1 \cup \Sigma_2, \end{aligned}$$

dok je nova funkcija prelaza $\delta : Q \times \Sigma \to 2^Q$ definirana s

$$\begin{aligned} \delta(q_0, \varepsilon) &= \{q_1, q_2\}, \\ \delta(p, a) &= \delta_1(p, a), \quad p \in Q_1 \setminus \{f_1\}, \quad a \in \Sigma_1 \cup \{\varepsilon\}, \\ \delta(p, a) &= \delta_2(p, a), \quad p \in Q_2 \setminus \{f_2\}, \quad a \in \Sigma_2 \cup \{\varepsilon\}, \\ \delta(f_1, \varepsilon) &= \delta(f_2, \varepsilon) = \{f_0\}. \end{aligned}$$

Što se točno događa u novom automatu M najbolje se vidi na dijagramu prelaza.

$slikaRJ4$

Iz gornjeg dijagrama lako se vidi da vrijedi

$$L(M) = L(M_1) \cup L(M_2) \overset{pp}{=} L(r_1) \cup L(r_2) \overset{def}{=} L(r_1 + r_2) = L(r).$$

(ii) $r = r_1 r_2$

Definirat ćemo novi NKA_ε $M = (Q, \Sigma, \delta, q_1, \{f_2\})$ sa samo jednim završnim stanjem iz kojeg nema prelaza na sljedeći način

$$\begin{aligned} Q &= Q_1 \cup Q_2, \\ \Sigma &= \Sigma_1 \cup \Sigma_2, \end{aligned}$$

dok je funkcija prelaza $\delta : Q \times \Sigma \to 2^Q$ definirana s

$$\begin{aligned} \delta(p, a) &= \delta_1(p, a), \quad p \in Q_1 \setminus \{f_1\}, \quad a \in \Sigma_1 \cup \{\varepsilon\}, \\ \delta(f_1, \varepsilon) &= \{q_2\}, \\ \delta(p, a) &= \delta_2(p, a), \quad p \in Q_2, \quad a \in \Sigma_2 \cup \{\varepsilon\} \end{aligned}$$

$slikaRJ5$

Iz dijagrama prelaza automata M lako se vidi da vrijedi

$$L(M) = L(M_1)\,L(M_2) \overset{pp}{=} L(r_1)\,L(r_2) \overset{def}{=} L(r_1 r_2) = L(r).$$

(iii) $r = r_1^*$

Definirat ćemo novi NKA_ε $M = (Q, \Sigma_1, \delta, q_0, \{f_0\})$ sa samo jednim završnim stanjem iz kojeg nema prelaza kao

$$Q = Q_1 \cup \{q_0, f_0\}, \qquad q_0, f_0 \notin Q_1,$$

a funkcija prelaza $\delta : Q \times \Sigma \to 2^Q$ definirana je s

$$\begin{aligned} \delta(q_0, \varepsilon) &= \delta(f_1, \varepsilon) = \{q_1, f_0\}, \\ \delta(p, a) &= \delta_1(p, a), \quad p \in Q_1 \setminus \{f_1\}, \quad a \in \Sigma_1 \cup \{\varepsilon\}, \end{aligned}$$

$slikaRJ6$

Iz dijagrama prelaza automata M lako se vidi da vrijedi

$$L(M) = L(M_1)^* \overset{pp}{=} L(r_1)^* \overset{def}{=} L(r_1^*) = L(r).$$

Ovim je dokazan korak indukcije, pa i sama tvrdnja T. ■

Primjer 26. *Konstruirajte NKA_ε koji prihvaća jezik opisan regularnim izrazom*

$$r = 01^* + 1.$$

$slikaRJ7$

Teorem 7.2.2. *$(DKAJ \subseteq RJ)$ Neka je L jezik kojeg prihvaća neki DKA. Tada postoji regularni izraz koji opisuje L.*

Dokaz. Neka jezik L prihvaća automat $M = (\{q_1, q_2, \ldots, q_n\}, \Sigma, \delta, q_1, F)$. Za $i, j \in \{1, \ldots, n\}, k \in \{0, 1, \ldots, n\}$ s R_{ij}^k označimo skup svih riječi $x \in \Sigma^*$ takvih da vrijedi

$$\delta(q_i, x) = q_j,$$

uz uvjet da za svaki pravi prefiks y riječi x iz

$$\delta(q_i, y) = q_l$$

mora slijediti $l \leq k$. Drugim riječima, R_{ij}^k je skup svih riječi iz Σ^* koje prevode automat M iz stanja q_i u stanje q_j ne prolazeći pritom kroz nijedno stanje s indeksom većim od k. Naravno, to ne znači da sami i, j ne mogu biti veći od k. Kako nema stanja s indeksom većim od n to R_{ij}^n označava skup svih riječi iz Σ^* koje prevode automat M iz stanja q_i u stanje q_j. Nadalje, očito je da vrijedi

$$L(M) = \bigcup_{q_j \in F} R_{1j}^n.$$

Uspijemo li pronaći regularne izraze koji opisuju svakog od R_{1j}^n iz definicije regularnih izraza i skupova koje opisuju odmah će slijediti

$$L = L(M) = L(r), \quad r = \sum_{q_j \in F} r_{1j}^n.$$

Uočimo najprije da za skupove R_{ij}^k općenito vrijedi sljedeća rekurzivna relacija (po $k \in \mathbb{N}_0$):

$$R_{ij}^0 = \begin{cases} \{a \in \Sigma : \delta(q_i, a) = q_j\}, & i \neq j \\ \{a \in \Sigma : \delta(q_i, a) = q_j\} \cup \{\varepsilon\}, & i = j \end{cases},$$

$$R_{ij}^k = R_{ik}^{k-1} \left(R_{kk}^{k-1}\right)^* R_{kj}^{k-1} \cup R_{ij}^{k-1}, \qquad k \in \mathbb{N}.$$

Koristeći ovu relaciju indukcijom po $k \in \mathbb{N}_0$ ćemo dokazati da za svaki R_{ij}^k postoji odgovarajući regularni izraz r_{ij}^k koji ga opisuje.

Baza indukcije ($k = 0$).

Kako nijedno stanje iz Q nema indeks 0, to je R_{ij}^0 konačan skup riječi duljine 1 ili 0, odnosno selementi R_{ij}^0 su slova iz Σ i (ili) prazna riječ ε. Dakle, r_{ij}^0 možemo pisati kao

$$r_{ij}^0 = \begin{cases} a_1 + \cdots + a_l, & i \neq j \\ a_1 + \cdots + a_l + \varepsilon, & i = j \end{cases},$$

gdje je $l \in \mathbb{N}$, $a_1, \ldots, a_l \in \Sigma$.

Pretpostavimo da za skup R_{ij}^{k-1} postoji regularni izraz r_{ij}^{k-1} koji ga opisuje. Promotrimo li rekurzivnu relaciju za R_{ij}^k vidimo da se u njoj javljaju samo operacije dozvoljene u gradnji regularnih jezika, odnosno R_{ij}^k je opisan regularnim izrazom

$$r_{ij}^k = r_{ik}^{k-1} \left(r_{kk}^{k-1}\right)^* r_{kj}^{k-1} + r_{ij}^{k-1}$$

čime je dokazan korak indukcije.

Dakle,

$$L = L\left(\sum_{q_j \in F} r_{1j}^n\right).$$

■

Primjer 27. *Pronađite regularni izraz za jezik kojeg prihvaća automat čiji je dijagram prelaza kao na slici*

slikaRJ8

Odmah vidimo da vrijedi

$$\begin{aligned} r &= r_{12}^3 + r_{13}^3 \\ &= \left(r_{13}^2 \left(r_{33}^2\right)^* r_{32}^2 + r_{12}^2\right) + \left(r_{13}^2 \left(r_{33}^2\right)^* r_{33}^2 + r_{13}^2\right) \\ &= \left(r_{13}^2 \left(r_{33}^2\right)^* r_{32}^2 + r_{12}^2\right) + \left(r_{13}^2 \left(r_{33}^2\right)^+ + r_{13}^2\right) \\ &= \left(r_{13}^2 \left(r_{33}^2\right)^* r_{32}^2 + r_{12}^2\right) + r_{13}^2 \left(\left(r_{33}^2\right)^+ + \varepsilon\right) \\ &= \left(r_{13}^2 \left(r_{33}^2\right)^* r_{32}^2 + r_{12}^2\right) + r_{13}^2 \left(r_{33}^2\right)^* \\ &= r_{13}^2 \left(r_{33}^2\right)^* \left(r_{32}^2 + \varepsilon\right) + r_{12}^2. \end{aligned}$$

Sada redom pronađemo manje složene izraze.

$$\begin{aligned} r_{13}^2 &= r_{12}^1 \left(r_{22}^1\right)^* r_{23}^1 + r_{13}^1 \\ &= 0\left(\varepsilon + 00\right)^* (1 + 01) + 1 \\ &= 0\left(00\right)^* (1 + 01) + 1 \\ &= 0\left(00\right)^* (\varepsilon + 0)\, 1 + 1 \\ &= 0^+ 1 + 1 = \left(0^+ + \varepsilon\right) 1 = 0^* 1, \end{aligned}$$

i slično

$$\begin{aligned} r_{12}^2 &= 0\left(00\right)^*, \\ r_{32}^2 &= (0 + 1)\left(00\right)^*, \\ r_{33}^2 &= (0 + 1)\, 0^* 1. \end{aligned}$$

Dakle,

$$\begin{aligned} r &= r_{13}^2 \left(r_{33}^2\right)^* \left(r_{32}^2 + \varepsilon\right) + r_{12}^2 \\ &= 0^* 1 \left((0 + 1)\, 0^* 1\right)^* \left((0 + 1)\left(00\right)^* + \varepsilon\right) + 0\left(00\right)^*. \end{aligned}$$

7.3. Lema o pumpanju za regularne jezike

Lema o pumpanju za regularne jezike (a time i za jezike koje prihvaćaju konačni automati) je vrlo jako oruđe za dokazivanje neregularnosti jezika. Korisna je i za razvijanje algoritama pomoću kojih se ispituje da li je neki regularni jezik konačan ili beskonačan. Osnova dokaza ove leme leži u činjenici da čitanjem riječi koje imaju više slova nego je stanja u automatu u dijagramu prelaza moramo proći više puta kroz isto stanje, tj. moramo napraviti "petlju".

Lema 7.3.1. *Neka je L regularni jezik. Tada postoji konstanta $n \in \mathbb{N}$ koja nije veća od broja stanja minimalnog konačnog automata koji prihvaća L i koja je takva da za bilo koju riječ $z \in L$ duljine barem n vrijedi:*

1. $z = uvw$
2. $|uv| \leq n$
3. $|v| \geq 1$
4. $(\forall i \in \mathbb{N}_0) \quad uv^i w \in L.$

Dokaz. Neka je L regularni jezik. Tada postoji neki (po broju stanja) minimalni konačni automat $M = (Q, \Sigma, \delta, q_1, F)$ takav da vrijedi $L = L(M)$, pri čemu je $Q = \{q_1, \ldots, q_n\}$. Neka je $z = a_1 \cdots a_m \in L$ ulazna riječ za koju vrijedi $|z| = m \geq n$. Za sve $j \in \{1, \ldots, m\}$ definiramo

$$\begin{aligned} \delta(q_1, \varepsilon) &= q_1 = q_{i_0} \\ \delta(q_1, a_1 \cdots a_j) &= q_{i_j} \in Q. \end{aligned}$$

Skup $\{q_{i_0}, q_{i_1}, \ldots, q_{i_m}\} \subseteq Q$ ima $m+1$ stanja, a znamo da Q ima n stanja, pa su neka od tih stanja nužno jednaka. To znači da postoje neki indeksi $k, j \in \{0, 1, \ldots, m\}$, pri čemu je $k < j$, takvi da je $q_{i_k} = q_{i_j}$. Kako je $z \in L$ to je $q_{i_m} \in F$, a zbog $q_{i_k} = q_{i_j}$ vrijedi

$$\begin{aligned} & \delta(q_0, a_1 \cdots a_k a_{k+1} \cdots a_m) \\ = \; & \delta(q_{i_k}, a_{k+1} \cdots a_m) = \delta\left(q_{i_j}, a_{k+1} \cdots a_m\right) = \delta(q_{i_k}, a_{j+1} \cdots a_m) \\ = \; & \delta\left(q_{i_j}, a_{j+1} \cdots a_m\right) = q_{i_m}, \end{aligned}$$

pa je i riječ $a_1 \cdots a_k a_{j+1} \cdots a_m = a_1 \cdots a_k (a_{k+1} \cdots a_j)^0 a_{j+1} \cdots a_m \in L$. Lako se vidi da bi isto vrijedilo za riječ $a_1 \cdots a_k (a_{k+1} \cdots a_j)^i a_{j+1} \cdots a_m,\ i \in \mathbb{N}$. Posljedica je to činjenice da "petlju" koju radimo prilikom proslaska kroz stanje $q_{i_k} = q_{i_j}$ možemo proći $0, 1, \ldots, i$ puta, gdje je i bilo koji prirodni broj. Najbolje se to vidi iz slike:

$$slikaRJ9$$

Označimo li sada

$$z = a_1 \cdots a_k a_{k+1} \cdots a_j a_{j+1} \cdots a_m = uvw,$$

pri čemu je

$$\begin{aligned} u &= a_1 \cdots a_k, \\ v &= a_{k+1} \cdots a_j, \\ w &= a_{j+1} \cdots a_m, \end{aligned}$$

lako vidimo da vrijede tvrdnje $1 - 4$. ■

Kako primjenjujemo ovu lemu? Slutimo li da neki jezik L nije regularan pretpostavimo najprije da jest. Za konstantu $n \in \mathbb{N}$ kao iz leme (ne moramo znati koji je to konkretno broj) izaberemo riječ z duljine barem n. Ako za svaki rastav riječi z oblika $z = uvw$ za koju vrijedi $|uv| \leq n$ i $|v| \geq 1$ pronađemo neki $i \in \mathbb{N}_0$ takav da $uv^i w \notin L$ došli smo do kontradikcije, pa možemo zaključiti da je početna pretpostavka o regularnosti jezika L bila netočna.

Primjer 28. *Dokažite da jezik* $L = \left\{0^{i^2} : i \in \mathbb{N}\right\}$ *nije regularan.*

Pretpostavimo da je jezik L regularan i neka je n konstanta iz Leme o pumpanju za regularne jezike. Promotrimo riječ $z = 0^{n^2} \in L$. Po Lemi o pumpanju tada postoji rastav $z = uvw$ takav da vrijedi $|uv| \leq n$ i $|v| \geq 1$ (uočimo da ne znamo kakav je točno taj rastav). Po Lemi bi, između ostalog, moralo vrijediti $uv^2w \in L$. No vrijedi

$$n^2 = |uvw| < \left|uv^2w\right| = |uvw| + |v| \leq |uvw| + |uv| \leq n^2 + n < (n+1)^2.$$

Dakle,

$$n^2 < \left|uv^2w\right| < (n+1)^2,$$

pa riječ uv^2w ne može pripadati jeziku L. Ovo je, pak, u kontradikciji s tvrdnjom Leme o pumpanju, pa zaključujemo da L ne može biti regularan jezik.

7.4. Svojstva zatvorenosti klase RJ

Podsjetimo se da iako ćemo sve teoreme iskazivati za regularne jezike rezultati ovog odjeljka vrijede istodobno i za jezike koje prihvaćaju konačni automati.

Definicija 7.4.1. *Kažemo da je neka klasa jezika $\mathcal{K}$ zatvorena s obzirom na operaciju $\circ$ ako iz pretpostavke $L_1, L_2 \in \mathcal{K}$ slijedi $L_1 \circ L_2 \in \mathcal{K}$.*

Teorem 7.4.1. *Klasa regularnih jezika zatvorena je s obzirom na uniju, konkatenaciju i Kleenejevo zatvorenje.*

Dokaz. Tvrdnja ovog teorema je direktna posljedica definicije regularnih jezika. ■

Teorem 7.4.2. *Klasa regularnih jezika zatvorena je s obzirom na komplement. Drugim riječima, ako je L regularni jezik u abecedi Σ onda je i $\Sigma^* \setminus L$ regularni jezik.*

Dokaz. Neka je L regularni jezik u abecedi Σ. Tada postoji minimalni konačni automat $M = (Q, \Sigma, \delta, q_0, F)$ takav da vrijedi $L = L(M)$. Da bismo dobili pravi komplement u odnosu na Σ^* potrebno je da funkcija prelaza δ bude totalna kako je napomenuto u uvodnom dijelu. Dakle, želimo li napraviti pravi komplement u odnosu na cijelu abecedu Σ moramo minimalni automat M proširiti novim stanjem q_{trash} (ono ima ulogu "koša za otpatke") za koje vrijedi

$$(\forall a \in \Sigma)(\forall q \in Q)(\delta(q,a) \uparrow \longrightarrow \delta(q,a) = q_{trash}),$$

Daljnji postupak je jednostavan: definiramo li automat $M' = (Q, \Sigma, \delta, q_0, Q \setminus F)$ lako vidimo da M' prihvaća riječ w ako i samo ako je $\delta(q_0, w) \in Q \setminus F$, to jest ako i samo ako je $w \in \Sigma^* \setminus L$. Drugim riječima, $L(M') = \Sigma^* \setminus L = L^c$. ■

Korolar 7.4.1. *Klasa regularnih jezika zatvorena je s obzirom na presjek.*

Dokaz. Tvrdnja slijedi iz zatvorenosti klase RJ na uniju i komplement jer je $L_1 \cap L_2 = (L_1^c \cup L_2^c)^c$. ■

Za nastavak moramo najprije definirati pojam **supstitucije** u regularnim jezicima.

Definicija 7.4.2. *Neka su Σ i Δ abecede. Supstitucija slova iz abecede Σ jezicima u abecedi Δ je bilo koja funkcija $f : \Sigma \to 2^{\Delta^*}$.*

Supstitucija $f : \Sigma \to 2^{\Delta^*}$ se na jedinstven način proširuje na riječi i jezike s:

1. $f(\varepsilon) = \varepsilon$
2. $f(xa) = f(x) f(a)$
3. $f(L) = \bigcup_{x \in L} f(x)$.

Primjer 29. *Neka je $\Sigma = \{0,1\}$ i $\Delta = \{a,b\}$. Definirajmo supstituciju $f : \Sigma \to 2^{\Delta^*}$ s*

x	0	1
$f(x)$	$\{a\}$	$\{b\}^*$

.

Tada je npr. $f(010) = f(0) f(1) f(0) = \{a\}\{b\}^*\{a\} = L(ab^*a)$.

Teorem 7.4.3. *Klasa regularnih jezika zatvorena je s obzirom na supstituciju regularnim jezicima.*

Dokaz. Neka je R regularni jezik u abecedi Σ i $f : \Sigma \to 2^{\Delta^*}$ neka supstitucija definirana s

$$(\forall a \in \Sigma)\ \ f(a) = R_a \in 2^{\Delta^*},$$

pri čemu su svi jezici R_a regularni. Znamo da u tom slučaju postoje regularni izrazi r i r_a za sve $a \in \Sigma$ koji redom opisuju jezike R i R_a za sve $a \in \Sigma$. Lako se vidi da zamjenom svih pojava slova $a \in \Sigma$ u regularnom izrazu r odgovarajućim regularnim izrazom r_a opet dobivamo regularni izraz. Kako se postupak provodi za sva slova iz Σ koja se javljaju u r čuvajući operacije lako se vidi da je konačni rezultat opet regularan izraz. Stoga je i jezik $f(R)$ kojeg opisuje regularan.

Striktan dokaz bismo proveli indukcijom po gradnji izraza r. ■

Primjer 30. *Neka je* $\Sigma = \{a, b\}$ *i* $\Delta = \{0, 1\}$. *Definirajmo supstituciju* $f : \Sigma \to 2^{\Delta^*}$ *s* $f(a) = 0^*$ *i* $f(b) = 101^+$. *Izvršimo li zamjene* $r_a = 0^* \longrightarrow a$ *i* $r_b = 101^+ \longrightarrow b$ *u izrazu* r *dobit ćemo novi regularni izraz*

$$f(r) = (0^*)^* 101^+ + 101^+ (0^*)^+ = 0^*101^+ + 101^+0^*.$$

Iznimno važna vrsta supstitucija su **homomorfizmi**: homomorfizam je supstitucija koja svakom slovu abecede Σ pridružuje jedinstvenu riječ iz Δ^*. Uočimo da riječ u ovom slučaju ne promatramo kao jednočlan jezik već baš kao riječ. Može se definirati i inverzni homomorfizam: ako je $h : \Sigma \to \Delta^*$ homomorfizam, onda je

$$h^{-1}(L) = \{x \in \Sigma^* : h(x) \in L\},$$

odnosno

$$h^{-1}(w) = \{x \in \Sigma^* : h(x) = w\}.$$

Naravno, tu smo u obzir uzeli prirodno proširenje homomorfizma h na riječi i jezike.

Teorem 7.4.4. *Klasa regularnih jezika zatvorena je s obzirom na homomorfizam i inverzni homomorfizam.*

Dokaz. Kako pojedine riječi možemo promatrati kao jednočlane jezike prva tvrdnja slijedi iz prethodnog teorema.

Dokažimo drugu tvrdnju.

Neka je L regularni jezik u abecedi Σ i $h : \Delta \to \Sigma^*$ homomorfizam. Znamo da postoji konačni automat $M = (Q, \Sigma, \delta, q_0, F)$ koji prihvaća L. Konstruirajmo konačni automat M' koji prihvaća $h^{-1}(L)$ čitanjem slova $a \in \Delta$ i simuliranjem rada automata M na riječi $h(a)$. Stavljamo $M' = (Q, \Delta, \delta', q_0, F)$, pri čemu je δ' definirana s

$$(\forall q \in Q)\,(\forall a \in \Delta)\,\delta'(q, a) = \delta(q, h(a)).$$

Indukcijom po duljini ulazne riječi x lako dokažemo da vrijedi

$$\delta'(q_0, x) = \delta(q_0, h(x)).$$

Dakle, automat M' prihvaća riječ x ako i samo ako automat M prihvaća riječ $h(x)$. Iz ovoga odmah slijedi

$$L(M') = h^{-1}(L(M)) = h^{-1}(L),$$

pa je $h^{-1}(L)$ regularni jezik. ■

7.5. Algoritmi odlučivosti za regularne jezike

Vrlo je važno imati podesne algoritme za ispitivanje raznih svojstava regularnih jezika. Pitanja koja postavljamo mogu biti:

- Da li je regularni jezik kojeg promatramo konačan, beskonačan ili čak prazan (ovo posljednje pitanje se možda čini trivijalnim, no nije tako!)?
- Da li je jedan regularni jezik (konačni automat) ekvivalentan drugom regularnom jeziku (konačnom automatu)?
- Da li je neki regularni izraz (konačni automat) minimalan, tj. postoji li ekvivalentan regularni izraz (konačni automat) s manjim brojem stanja?

Uočimo da se ista pitanja mogu postavljati i za regularne jezike i za jezike koje prihvaćaju konačni automati. Kako imamo na raspolaganju mehanički postupak za "prevođenje" jezika iz jednog oblika u drugi dovoljno je dati odgovore na po jedno pitanje, a mi ćemo pretpostaviti da su regularni jezici prikazani kao jezici koje prihvaćaju konačni automati.

Sljedeći teorem nam daje odgovor na pitanje o kardinalnom broju nekog KA jezika.

Teorem 7.5.1. *Jezik $L(M)$ kojeg prihvaća konačni automat M s $n \in \mathbb{N}$ stanja je:*

1. *neprazan ako i samo ako M prihvaća neku riječ duljine manje od n*
2. *beskonačan ako i samo ako M prihvaća neku riječ duljine l takve da je $n \leq l < 2n$.*

Dokaz. 1. Smjer dovoljnosti je očigledan.
Dokažimo smjer nužnosti. Pretpostavimo da M prihvaća neki neprazan jezik $L(M)$. Neka je riječ w duljine ne veće od duljine najkraće riječi koju prihvaća M. Po Lemi o pumpanju možemo zaključiti da je nužno $|w| < n$ jer bi u suprotnom vrijedilo $w = uvy,\ uv^0y \in L$ i $|uv^0y| < |w|$ što po pretpostavci o izboru riječi w nije moguće. Dakle, u $L(M)$ jer riječ duljine manje od n pa M prihvaća takvu riječ.

2. Dokažimo smjer dovoljnosti. Ako u $L(M)$ postoji riječ w takva da je $n \leq |w| < 2n$ (pri čemu je u ovom smjeru desna nejednakost nebitna) onda po Lemi o pumpanju odmah slijedi da je jezik $L(M)$ beskonačan.
Dokažimo smjer nužnosti. Pretpostavimo da je $L(M)$ beskonačan. Tada sigurno postoji riječ w takva da je $|w| \geq n$ (jer bi u suprotnom zbog činjenice da su abaecede automata konačne jezik $L(M)$ bio konačan). Ako je još i $|w| < 2n$ dokaz je gotov jer je w tražena riječ. Ako u $L(M)$ nema niti jedne druge riječi duljine l takve da je $n \leq l < 2n$ onda to znači da se duljine riječi iz skupa $L(M)$ nalaze u skupu $\{0, 1, 2, \ldots, n-1\} \cup \{2n, , 2n+1, \ldots, m\}$. Uzmimo neku riječ w u $L(M)$ čija je duljina u skupu $\{2n, , 2n+1, \ldots, m\}$ ali ne dulju od najkraće takve riječi (radi se o podskupu skupa $\mathbb{N}$ pa znamo da to možemo napraviti). Za w vrijedi $|w| \geq 2n$ pa po Lemi o pumpanju slijedi da postoje riječi w_1, w_2, w_3 takve da vrijedi:
a) $w = w_1w_2w_3$
b) $|w_1w_2| \leq n,\ 1 \leq |w_2| \leq n$

c) $w_1w_3 \in L(M)$.

Zbog ograničenja na duljine riječi iz $L(M)$ imamo dvije mogućnosti: $|w_1w_3| < n$ i $|w_1w_3| \geq 2n$.

Ako je $|w_1w_3| < n$ zbog $|w_2| \leq n$ dobijemo $|w_1w_2w_3| = |w| < 2n$ što nije moguće. Ako je pak $|w_1w_3| \geq 2n$ onda u $L(M)$ imamo riječ duljine manje od duljine riječi w a iz skupa $\{2n, , 2n+1, \ldots, m\}$ što zbog načina izbora riječi w nije moguće. Dakle u $L(M)$ mora biti riječi duljina iz skupa $\{n, , n+1, \ldots, 2n-1\}$. ■

Uočimo da su algoritmi predloženi u prethodnom teoremu prilično neefikasni. Ipak, lako je provjeriti da li je jezik kojeg prihvaća neki KA prazan ili beskonačan na sljedeći način. Najprije iz njegovog dijagrama prelaza izbacimo sva nedohvatna stanja: ako je nakon toga ostalo barem jedno završno stanje jezik nije prazan. Nakon toga, pazeći da ne promijenimo jezik kojeg prihvaća automat, odbacimo sva stanja koja nisu završna, a iz kojih se ne može stići u neko završno stanje. Automat prihvaća beskonačan jezik ako i samo ako je nakon toga u dijagramu prelaza ostao barem jedan ciklus.

Lako se vidi da postoji algoritam kojim je moguće odrediti jesu li konačni automati M_1 i M_2 međusobno ekvivalentni. Naime, označimo li redom $L_1 = L(M_1)$ i $L_2 = L(M_2)$ po prethodnim teoremima znamo da za jezik

$$L_3 = (L_1 \cap L_2^c) \cup (L_1^c \cap L_2)$$

postoji automat M_3 takav da je $L_3 = L(M_3)$. Uočimo da M_3 prihvaća barem jednu riječ ako i samo ako je $L_1 \neq L_2$. Stoga je po prethodnom teoremu moguće naći algoritam kojim se ispituje vrijedi li $L_1 = L_2$: to će vrijediti ako i samo ako je L_3 prazan jezik.

7.6. Minimizacija konačnih automata

Nekom jeziku L na prirodan načino možemo pridružiti relaciju ekvivalencije R_L definiranu na sljedeći način: za riječi $x, y \in \Sigma^*$ vrijedit će xR_Ly ako i samo ako za svaku riječ $z \in \Sigma^*$ vrijedi da su ili obje riječi xz i yz u L ili nijedna od njih. Čitatelju ostavljamo da provjeri kako je R_L zaista relacija ekvivalencije na Σ^*, a samim time ona definira kvocijentni skup L/R_L čiji su elementi klase ekvivalencije. U najgorem će slučaju svaka riječ biti jedini element svoje klase ekvivalencije, no moguć je i manji broj klasa. Broj tih klasa naziva se **indeksom** jezika L i može se dokazati da je on uvijek konačan broj ako je L regularni jezik.

Kako je i za očekivati, postoji na prirodan način definirana relacija ekvivalencije R_M na skupu Σ^* svih riječi u abecedi konačnog automata $M = (Q, \Sigma, \delta, q_0, F)$. Definirana na sljedeći način: za riječi $x, y \in \Sigma^*$ vrijedit će xR_My ako i samo ako je $\delta(q_0, x) = \delta(q_0, y)$. Lako se vidi da je R_M relacija ekvivalencije (jer je takva i relacija "biti jednak"), pa R_M dijeli skup Σ^* na klase ekvivalencije, i to na po jednu za svako stanje iz Q dohvatno iz q_0. Nadalje, ako je xR_My, onda je i xzR_Myz za sve $z \in \Sigma^*$ jer je

$$\delta(q_0, xz) = \delta(\delta(q_0, x), z) = \delta(\delta(q_0, y), z) = \delta(q_0, yz).$$

Općenito za relaciju ekvivalencije R na skupu L kažemo da je **invarijantna s desna** ako za svaki $z \in L$ iz xRy slijedi $xzRyz$, pa dakle svaki konačni automat M

inducira jednu s desna invarijantnu relaciju ekvivalencije definiranu kao R_M. Ova činjenica je formalizirana u narednom teoremu.

Teorem 7.6.1. *(Teorem Myhilla i Nerodea) Sljedeće su tri tvrdnje međusobno ekvivalentne:*

1. *Skup $L \subseteq \Sigma^*$ prihvaća neki konačni automat M*
2. *L je unija nekih klasa ekvivalencije neke desno invarijantne relacije ekvivalencije konačnog indeksa*
3. *Neka je relacija R_L definirana s xR_Ly ako i samo ako za svaku riječ $z \in \Sigma^*$ vrijedi $xz \in L$ točno onda kada je $yz \in L$. Tada je R_L relacija ekvivalencije konačnog indeksa.*

Dokaz. (1) $\Rightarrow$ (2)

Pretpostavimo da skup (jezik) L prihvaća konačni automat $M = (Q, \Sigma, \delta, q_0, F)$. Definirajmo relaciju R_M na Σ^* s

$$xR_My \text{ ako i samo ako je } \delta(q_0, x) = \delta(q_0, y).$$

Očito je R_M relacija ekvivalencije na Σ^* a lako se vidi i da je desno invarijantna. Indeks relacije R_M je konačan jer je u najgorem slučaju jednak broju stanja automata M. nadalje, L je unija onih klasa ekvivalencije relacije R_M koje sadrže neku riječ x takvu da je $\delta(q_0, x) \in F$, točnije onih klasa koje odgovaraju završnim stanjima automata M.

(2) $\Rightarrow$ (3)

Dokazat ćemo da je bilo koja relacija ekvivalencije S koja zadovoljava (2) profinjenje relacije R_L iz (3), to jest da joj je svaka klasa ekvivalencije unutar neke klase ekvivalencije relacije R_L. To bi značilo da indeks relacije R_L ne može biti veći od indeksa relacije S pa je nužno konačan.

Pretpostavimo da je xSy za neke $x, y \in L$. Jer je S desno invarjantna to za sve $z \in \Sigma^*$ vrijedi $xzSyz$ pa je $yz \in L$ ako i samo ako je $xz \in L$. Iz ovoga slijedi xR_Ly, to jest $[x]_S \subseteq [x]_{R_L}$. Jer su x i y bili proizvoljni zaključujemo da to vrijedi za sve klase relacije S odnosno da je S profinjenje relacije R_L.

(3) $\Rightarrow$ (1)

Relacija R_L definirana kao u (3) je desno invarijantna. Naime, iz definicije relacije R_L znamo da za svaku riječ $z \in \Sigma^*$ vrijedi $xz \in L$ točno onda kada je $yz \in L$. Uzmimo proizvoljnu riječ $w \in \Sigma^*$. Želimo dokazati da iz xR_Ly slijedi xwR_Lyw. To znači da za svaku riječ $v \in \Sigma^*$ mora vrijediti $xwv \in L$ točno onda kada vrijedi $ywv \in L$. No iz xR_Ly za $z = wv$ dobijemo upravo to pa vrijedi xwR_Lyw.

Neka je Q' (konačan) skup klasa ekvivalencije relacije R_L i $[x] \in Q'$ klasa koja sadrži x. Definiramo:

$$\delta'([x], a) = [xa].$$

Ovakva definicija funkcije δ' je dobra jer ne ovisi o izboru predstavnika klasa a što je posljedica desne invarijantnosti relcije R_L. Naime, uzmemo li bilo koji $y \in [x]$ iz xR_Ly slijedi $xz \in L$ točno onda kada je $yz \in L$. Posebno, za $z = az'$, $xaz' \in L$ točno onda kada je $yaz' \in L$, dakle je xaR_Lya i $[xa] = [ya]$.

Sada definiramo

$$\begin{aligned} q_0' &= [\varepsilon], \\ F' &= \{[x] : x \in L\}, \\ M' &= (Q', \Sigma, \delta', q_0', F'). \end{aligned}$$

Očito M' prihvaća L jer je $\delta'(q_0', x) = \delta'([\varepsilon], x) = [x]$ i $x \in L(M')$ ako i samo ako je $[x] \in F'$ ako i samo ako je $x \in L$. ■

Primjer 31. *Neka je jezik L opisan regularnim izrazom $r = 0^*10^*$. Dijagram prelaza odgovarajućeg automata M za kojeg vrijedi $L = L(M) = L(r)$ je dan na slici.*

$slikaRJ9$

Sva su mu stanja dostižna iz početnog, pa relacija R_M ima šest klasa ekvivalencije i one su redom

$$\begin{aligned} C_a &= (00)^*, \quad C_d = (00)^* 01, \\ C_b &= (00)^* 0, \quad C_e = 0^*100^*, \\ C_c &= (00)^* 1, \quad C_f = 0^*10^*1(0+1)^*. \end{aligned}$$

Jezik L je unija triju od ovih klasa: C_c, C_d i C_e.Relacija R_L jezika L iz gornjeg primjera definirana je na sljedeći način: za $x, y \in \{0,1\}^*$ vrijedi xR_Ly ako i samo ako je ispunjeno jedno od troje:
1) ni x ni y nemaju jedinica
2) i x i y imaju po jednu jedinicu
3) i x i y imaju više od jedne jedinice.
Na primjer, ako je $x = 010$ i $y = 1000$ onda je $xz \in L$ ako i samo ako je $z \in 0^*$. No vrijedit će $yz \in L$ ako i samo ako je $z \in 0^*$, to jest pod u potpunosti istim uvjetima. No s druge strane, ako je $x = 01$ i $y = 00$ onda se lako vidi da za $z = 0$ neće vrijediti $yz = 000 \in L$ iako je $xz = 010 \in L$, to jest nije ispunjeno xR_Ly.
Odgovarajući kvocijentni skup relacije R_L sastoji se od tri klase: $C_1 = 0^*$, $C_2 = 0^*10^*$ i $C_1 = 0^*10^*1(0+1)^*$. Jezik L je samo jedna od tih klasa: C_2. Uočimo i da postoji veza između klasa $C_a, \ldots, C_f$ i $C_1, C_2, C_3 : C_1 = C_a \cup C_b$, $C_2 = C_c \cup C_d \cup C_e$ i $C_3 = C_f$.

Jednom kada smo pronašli klase ekvivalencije relacije R_L odgovarajući *minimalni konačni automat* M' ekvivalentan automatu M konstruiramo na sljedeći način: izaberemo reprezentante klasa C_1, C_2, C_3, recimo redom $\varepsilon, 1$ i 11. Svakoj klasi odgovara jedno stanje, početno odgovara klasi C_1, a završno klasi C_2. Funkcija prelaza se vidi iz dijagrama prelaza automata M'.

$slikaRJ10$

Korolar 7.6.1. *Minimalni konačni automat koji prihvaća jezik L je jedinstven do na izomorfizam (tj. imena stanja) a konstrukcija mu je dana u dokazu prethodnog teorema.*

Poglavlje 8.

Kontekstno slobodni jezici

8.1. Osnovni pojmovi

U ovom poglavlju upoznat ćemo se s **kontekstno slobodnim gramatikama** i jezicima koje one opisuju- **konteksto slobodnim jezicima**. Oni su od velike važnosti u definiranju programskih jezika, formaliziranju parsinga te raznim obradama nizova.

Konteksto slobodna gramatika je, slobodno rečeno, skup varijabli koje nazovamo **sintaktičkim kategorijama** ili **neterminalima**, a od kojih svaka predstavlja neki jezik. Sami jezici su opisani rekurzivno jedni preko drugih pomoću jednostavnih simbola koje nazivamo **terminalima**. Pravila koja opisuju odnose među varijablama nazivamo **produkcijama**.

Definicija 8.1.1. *Konteksto slobodna gramatika (KSG) je uređena četvorka* $G = (V, T, P, S)$ *gdje je:*

1. V *konačan skup čije elemente nazivamo varijablama*
2. T *konačan skup za kojeg vrijedi* $V \cap T = \emptyset$, *a čije elemente nazivamo terminalima*
3. P *konačan skup pravila oblika*

$$A \to \alpha, \quad A \in V,\ \alpha \in (V \cup T)^*$$

koja nazivamo produkcijama

4. $S \in V$ *istaknuta varijabla koju nazivamo početnom varijablom.*

Primjer 32. *Jedna kontekstno slobodna gramatika je* $G = (\{E\}, \{+, *, (,), \mathrm{id}\}, P, E)$, *gdje je*

$$P = \{E \to E + E,\ E \to E * E,\ E \to (E),\ E \to \mathrm{id}\},$$

što se kraće piše

$$E \to E + E \mid E * E \mid (E) \mid \mathrm{id}\ .$$

Da bismo u zapisu bez posebnog navođenja znali o kakvim se objektima radi dogovorno se uzima da se slova X, Y, Z koriste kao metavarijable za objekte koji mogu biti bilo varijable bilo terminali, ostala velika latinična slova za varijable, slova x, y, u, v, w za nizove terminala, ostala mala latinična slova za terminale i mala grčka slova za nizove čiji su elementi bilo varijable bilo terminali.

8.2. Izvodi

Da bismo definirali jezike koje izvode kontekstno slobodne gramatike najprije moramo definirati **relaciju izvoda** među nizovima iz $(V \cup T)^*$.

Definicija 8.2.1. *Neka je $G = (V, T, P, S)$ kontekstno slobodna gramatika, $A \in V$ te $\alpha, \beta, \gamma \in (V \cup T)^*$. Relacija $\Rightarrow_G$ "izvoda" u G definirana je na skupu $(V \cup T)^*$ na sljedeći način: $\alpha A \gamma \Rightarrow_G \alpha\beta\gamma$ ako i samo ako u P postoji produkcija $A \to \beta$. U tom slučaju kažemo da niz $\alpha A \gamma$ u gramatici G direktno izvodi niz $\alpha\beta\gamma$.*

S $\overset{*}{\Rightarrow}_G$ označit ćemo refleksivno i tranzitivno zatvorenje relacije $\Rightarrow_G$. Drugim riječima, za bilo koji niz $\alpha \in (V \cup T)^*$ vrijedit će $\alpha \overset{*}{\Rightarrow}_G \alpha$, a za nizove $\alpha_1, \alpha_2, \ldots, \alpha_n \in (V \cup T)^*$ takve da je

$$\alpha_1 \Rightarrow_G \alpha_2,\ \alpha_2 \Rightarrow_G \alpha_3,\ \cdots,\alpha_{n-1} \Rightarrow_G \alpha_n$$

vrijedit će $\alpha_1 \overset{*}{\Rightarrow}_G \alpha_n$. Ako posebno želimo istaknuti broj koraka izvoda pisat ćemo $\alpha \overset{k}{\Rightarrow}_G \beta$. Ako je jasno o kojoj se gramatici radi u izvodu možemo izostaviti pisanje indeksa G.

Definicija 8.2.2. *Neka je $G = (V, T, P, S)$ kontekstno slobodna gramatika. Kažemo da je niz $\alpha \in (V \cup T)^*$ sentencijalna forma ako vrijedi $S \overset{*}{\Rightarrow}_G \alpha$.*

Sada možemo definirati jezike koje izvode kontekstno slobodne gramatike.

Definicija 8.2.3. *Jezik $L(G)$ izveden gramatikom G je skup*

$$L(G) = \left\{ w \in T^* : S \overset{*}{\Rightarrow}_G w \right\}.$$

Drugim riječima, ako je G gramatika jezik $L(G)$ je skup svih njenih sentencijalnih formi koje se sastoje samo od terminala.

Definicija 8.2.4. *Kažemo da je jezik L kontekstno slobodan ako postoji kontekstno slobodna gramatika G takva da vrijedi $L = L(G)$.*

Primjer 33. *Neka je dana kontekstno slobodna gramatika*

$$G = (\{S, A, B\}, \{a, b\}, P, S),$$

pri čemu je P skup od šest od produkcija

$$\begin{aligned} S &\to aB \mid bA \\ A &\to aS \mid bAA \mid a \\ B &\to bS \mid aBB \mid b. \end{aligned}$$

Može se provjeriti da vrijedi

$$L(G) = \left\{ w \in \{a, b\}^+ : |w|_a = |w|_b \right\}.$$

8.3. Stabla izvoda

Ponekad je korisno izvode riječi u kontekstno slobodnoj gramatici prikazivati pomoću **stabala izvoda**. Formalno, stablo izvoda za gramatiku $G = (V, T, P, S)$ je stablo za koje vrijedi sljedeće:

1. Svaki čvor ima labelu koja je simbol iz $V \cup T \cup \{\varepsilon\}$.
2. Labela korijena je S.
3. Ako je čvor unutrašnji onda mu je labela element skupa V.
4. Ako čvor ima labelu ε onda je list i jedini sin svoga oca.
5. Ako čvor v ima labelu $A \in V$, a čvorovi $v_1, \ldots, v_n$ labelirani s $X_1, \ldots, X_n$, su mu redom sinovi, onda u P postoji produkcija $A \to X_1 \cdots X_n$.

Stabla na prirodan način opisuju izvođenje sentencijalnih formi u gramatici G. Ako pročitamo labele listova stabla s lijeva na desno dobit ćemo sentencijalnu formu čije je to stablo izvoda.

$$slikaKSJ1$$

Podstablo stabla izvoda je neki unutrašnji čvor zajedno sa svim svojim potomcima. Očigledno je ono i samo stablo izvoda, samo što u korijenu nema labelu S već neku drugu varijablu iz V. Ako je to npr. varijabla A, onda kažemo da je takvo podstablo A-stablo.

Sljedeći teorem dovodi u vezu relaciju izvoda i stabla izvoda.

Teorem 8.3.1. *Neka je $G = (V, T, P, S)$ kontekstno slobodna gramatika i $\alpha \in (V \cup T)^*$. Vrijedi: $S \overset{*}{\Rightarrow}_G \alpha$ ako i samo ako postoji neko stablo izvoda gramatike G koje izvodi α.*

Dokaz. Pokazuje se da je lakše dokazati jaču tvrdnju čija je jednostavna posljedica tvrdnja teorema.
(T) Neka je $A \in V$ i $\alpha \in (V \cup T)^*$. Vrijedi: $A \overset{*}{\Rightarrow}_G \alpha$ ako i samo ako postoji neko A-stablo izvoda gramatike G koje izvodi α.

Dokažimo najprije smjer dovoljnosti.

Pretpostavimo da A-stablo izvodi α u gramatici G. Dokaz ćemo provesti indukcijom po broju k unutrašnjih čvorova stabla izvoda. Očigledno stablo izvoda mora imati barem jedan unutrašnji čvor (korijen), pa nam je baza indukcije dana za $k = 1$. U tom slučaju A-stablo ima samo korijen s labelom A i njegove sinove (koji su listovi) s labelama $X_1, \ldots, X_n$, a koje zajedno daju α. Po definiciji stabla izvoda to znači da u P postoji produkcija $A \to X_1 \cdots X_n = \alpha$, pa $A \Rightarrow_G \alpha$.
Pretpostavimo da tvrdnja vrijedi za stabla s manje od k unutrašnjih čvorova.
Neka A-stablo s točno $k > 1$ unutrašnjih čvorova izvodi α u gramatici G. Promotrimo redom sinove korijena: neka su to $v_1, \ldots, v_n$, a njihove labele neka su $X_1, \ldots, X_n$. Pročitamo li redom izvedene forme iz $v_1, \ldots, v_n$ dobit ćemo $\alpha_1 \cdots \alpha_n = \alpha$. Po definiciji stabla izvoda u P mora postojati produkcija oblika $A \to X_1 \cdots X_n$. Kako je dubina promatranog A- stabla barem 2 ne mogu svi $v_1, \ldots, v_n$ biti listovi, pa su

neke od labela $X_1, \ldots, X_n$ varijable. Ako je neki X_i terminal, onda je v_i list, a je X_i varijabla, onda je podstablo s korijenom v_i X_i-stablo. Takvo stablo ima manje od k unutrašnjih čvorova, pa se na njega može primijeniti pretpostavka indukcije iz čega slijedi $X_i \overset{*}{\Rightarrow}_G \alpha_i$. Uzevši sve zajedno dobijemo

$$A \Rightarrow_G X_1 \cdots X_n \overset{*}{\Rightarrow}_G \alpha_1 \cdots \alpha_n = \alpha,$$

čime je dokazan korak indukcije.

Dokažimo sada smjer nužnosti.

Neka $A \overset{*}{\Rightarrow}_G \alpha$. Dokaz provodimo indukcijom po broju koraka izvoda. Izvoda mora imati barem jedan korak (nećemo uzeti u obzir trivijalni slučaj $A = \alpha$), pa nam je baza indukcije dana za $k = 1$. U tom slučaju u P postoji produkcija $A \to \alpha$, pa je po definiciji stabla izvoda pripadno A-stablo izvoda dubine 1 kojem korijen ima labelu A, a sinovi su listovi kojima labele pročitane redom daju α. Pretpostavimo da tvrdnja vrijedi za izvode s manje od k koraka.

Neka $A \overset{k}{\Rightarrow}_G \alpha,\ k > 1$. Prvi korak izvoda je neka produkcija oblika $A \to X_1 \cdots X_n$, pri čemu svaki simbol forme α mora biti ili neki X_i ili izveden iz nekog X_i. Također, za $i < j$ dio α izveden iz X_i leži lijevo od dijela izvedenog iz X_j. Dakle, za $\alpha = \alpha_1 \cdots \alpha_n$ i za svaki $i \in \{1, \ldots, n\}$ vrijedi:

$$(i) \quad \alpha_i = X_i, \quad X_i \in T,$$

$$(ii) \quad X_i \overset{*}{\Rightarrow}_G \alpha_i, \quad X_i \in V,$$

a pritom nisu svi X_i iz skupa T jer je to slučaj iz baze indukcije. U slučaju (ii) izvod ima manje od k koraka, pa se može primijeniti pretpostavka indukcije, odnosno postoji X_i-stablo koje izvodi α_i. Sada A-stablo koje izvodi α dobijemo tako da mu u korijen stavljamo A, sinovi korijena su redom čvorovi označeni labelama $X_1, \ldots, X_n$. Svi čvorovi s labelama X_i iz slučaja (i) su listovi, a svi čvorovi X_i iz slučaja (ii) su korijeni X_i-stabala. Čitajući redom labele listova takvog stabla dobit ćemo upravo α. Ovim je dokazan korak indukcije.

Sada iz tvrdnje T lako dobijemo tvrdnju teorema ako uzmemo posebno $A = S$.

■

8.4. Desno linearni jezici

U ovom odjeljku ćemo vidjeti kakva je veza između kontekstno slobodnih jezika i jezika koje prihvaćaju konačni automati (odnosno regularnih jezika). Pokazat će se da je skup jezika koje prihvaćaju konačni automati pravi podskup skupa kontekstno slobodnih jezika.

Definicija 8.4.1. *Za kontekstno slobodnu gramatiku G kažemo da je desno linearna ako su joj sve produkcije oblika*

$$\begin{aligned} A &\to aB, \qquad A, B \in V,\ a \in T \cup \{\varepsilon\}, \\ A &\to a, \qquad A \in V,\ a \in T \cup \{\varepsilon\}. \end{aligned}$$

Definicija 8.4.2. *Za jezik L kažemo da je desno linearan ako je $L = L(G)$ za neku desno linearnu gramatiku G. Klasu svih desno linearnih jezika označavamo s DLJ.*

Teorem 8.4.1. *Klasa DLJ zatvorena je s obzirom na uniju, konkatenaciju i Kleenejevo zatvorenje.*

Dokaz. Neka su L_1 i L_2 desno linearni jezici. Tada postoje desno linearne gramatike G_1 i G_2 takve da vrijedi

$$L_i = L(G_i), \quad i = 1, 2.$$

Neka je

$$G_i = (V_i, T_i, P_i, S_i), \quad i = 1, 2,$$

a bez smanjenja općenitosti možemo pretpostaviti da je $V_1 \cap V_2 = \emptyset$. Sada ćemo za svaku od triju operacija definirati desno linearnu gramatiku G koja izvodi odgovarajući jezik.

1) $L = L_1 \cup L_2$

U ovom slučaju stavljamo

$$G = (V_1 \cup V_2 \cup \{S\}, T_1 \cup T_2, P, S)$$

pri čemu zahtijevamo da $S \notin V_1 \cup V_2$, a skup produkcija je definiran s

$$P = P_1 \cup P_2 \cup \{S \to S_1 \mid S_2\}.$$

Lako se vidi da je

$$L(G) = L(G_1) \cup L(G_2) = L_1 \cup L_2 = L.$$

2) $L = L_1 L_2$

U ovom slućaju je G kao u prethodnom osim što je skup produkcija P definiran s

$$\begin{aligned} P &= \{S \to S_1\} \cup \{B \to bD : B \to bD \in P_1\} \cup \\ &\quad \cup \{B \to bS_2 : B \to b \in P_1\} \cup P_2. \end{aligned}$$

Lako se vidi da je

$$L(G) = L(G_1) L(G_2) = L_1 L_2 = L.$$

3) $L = L_1^*$

Najprije ćemo konstruirati odgovarajuću desno linearnu gramatiku za jezik L^+. Definiramo

$$G = (V_1 \cup \{S\}, T_1, P, S), \quad S \notin V_1,$$

a skup produkcija P je zadan s

$$P = \{S \to S_1\} \cup \{B \to bS_1 : B \to b \in P_1\} \cup P_1.$$

Sada imamo

$$L(G) = L(G_1)^+ = L_1^+.$$

Kako je $L = L_1^* = L_1^+ \cup \{\varepsilon\}$, a jezik $\{\varepsilon\}$ je desno linearan, po a) zaključujemo da je i jezik L desno linearan (ovo, naravno, nije nužno raditi ako L_1 sadrži praznu riječ). ■

Teorem 8.4.2. *(RJ ⊆ DLJ) Svi regularni jezici su desno linearni.*

Dokaz. Kako su atomarni regularni jezici $\emptyset, \{\varepsilon\}$ i $\{a\}$ desno linearni (odgovarajuće DL gramatike su dane produkcijama $S \to A,\ S \to \varepsilon,\ S \to a$), a klasa DLJ je zatvorena na sve operacije kojima se grade regularni jezici, to je svaki regularni jezik desno linearan. ■

Korolar 8.4.1. *($KAJ \subseteq DLJ$) Svi jezici koje prihvaćaju konačni automati su desno linearni.*

Teorem 8.4.3. *($DLJ \subseteq KAJ$) Svi desno linearni jezici su KA jezici.*

Dokaz. Dovoljno je za proizvoljni desno linearni jezik naći neki NKA koji ga prihvaća.

Neka je L neki desno linearni jezik. Tada postoji desno linearna gramatika $G = (V, T, P, S)$ takva da vrijedi $L = L(G)$. Definiramo:

$$\begin{aligned} Q &= V \cup \{q\},\ \ q \notin V, \\ q_0 &= S, \quad \Sigma = T, \\ F &= \begin{cases} \{q\}, & \varepsilon \notin L \\ \{q, S\}, & \varepsilon \in L \end{cases}. \end{aligned}$$

Funkcija prelaza δ definirana je s

$$\delta(A, x) = \begin{cases} \{B \in V : A \to xB \in P\}, & A \to x \notin P \\ \{B \in V : A \to xB \in P\} \cup \{q\}, & A \to x \in P \end{cases},$$

za $A \in V$ i $x \in \Sigma^*$. Uočimo da iz završnog stanja q nema prelaza. Sada definiramo traženi automat M kao $M = (Q, \Sigma, \delta, S, F)$ i lako se vidi da vrijedi

$$L(M) = L(G) = L,$$

pa je L KA jezik. ■

Primjer 34. *Pronađite konačni automat koji prihvaća jezik $L(G)$ ako je gramatika G dana produkcijama*

$$P = \{S \to aA \mid aB,\ A \to aC \mid a,\ B \to bC \mid b,\ C \to cS\}.$$

Sljedimo konstrukciju automat M kao u prethodnom teoremu. Stavljamo

$$\begin{aligned} Q &= \{S, A, B, C, q\}, \\ q_0 &= S, \quad T = \{a, b, c\}, \end{aligned}$$

a kako je definirina funkcija prelaza δ vidi se iz dijagrama prelaza automata M.

$$slikaDL1$$

Do sada smo dokazali da vrijedi

$$\begin{aligned} DLJ &= KAJ, \\ RJ &\subseteq DLJ, \end{aligned}$$

no koristeći činjenicu da vrijedi

$$KAJ = RJ$$

lako možemo zaključiti da je ispunjeno i

$$RJ = KAJ = DLJ. \tag{8.1}$$

No mi ćemo kasnije dokazati da se i bez korištenja konačnih automata može dokazati inkluzija $DLJ \subseteq RJ$. Ipak, relacija (8.1) nam omogućava da bez dokaza damo sljedeći teorem.

Teorem 8.4.4. *Klasa DLJ zatvorena je s obzirom na presjek, komplement, supstituciju, homomorfizam i inverzni homomorfizam.*

8.5. Uklanjanje suvišnih produkcija

Kod desno linearnih gramatika ne smatra se poželjnim imati produkcije oblika $A \to B$ i $A \to \varepsilon$ (osim $S \to \varepsilon$) jer one ne doprinose izražajnosti jezika. Stoga ih je potrebno ukloniti ali tako da se ne promijeni jezik, to jest da novodobivena gramatika G' bude ekvivalentna polaznoj gramatici G.

Lema 8.5.1. *(Lema o praznoj riječi) Za svaku desno linearnu gramatiku G u kojoj postoje produkcije oblika $A \to B$ i $A \to \varepsilon$ možemo formirati desno linearnu gramatiku G' ekvivalentnu gramatici G, a za koju vrijedi:*

1. *ako $L(G)$ ne sadrži praznu riječ, onda se ε ne javlja u G*
2. *ako $L(G)$ sadrži praznu riječ, onda u G' postoji jedinstvena produkcija $S' \to \varepsilon$, gdje je S' početna varijabla gramatike G', u kojoj se ε javlja s desne strane.*

Dokaz. Dokaz dajemo u obliku algoritma kojim se uklanjaju sve suvišne produkcije.

1) $\varepsilon \notin L(G)$

Ovo znači da u P sigurno ne postoji produkcija oblika $S \to \varepsilon$, pa se provodi sljedeći postupak:

za svaku produkciju $A \to \varepsilon$
.....za svaku produkciju $B \to aA$
.....dodaj $B \to aA$
izbaci $A \to \varepsilon$
za svaku produkciju $A \to B$
.....za svaku produkciju $C \to aA$
.....dodaj $C \to aB$
izbaci $A \to B$

2) $\varepsilon \in L(G)$

Ovo znači da $S \overset{*}{\Rightarrow}_G \varepsilon$, pa je potrebno uvesti novu početnu varijablu $S' \notin V$ i P uvesti jednu dodatnu produkciju $S' \to S \mid \varepsilon$. To osigurva da se u starom skupu produkcija sigurno ne javlja produkcija $S' \to \varepsilon$, pa se nakon toga provede isti postupak kao u prvom slučaju pri čemu S tretiramo kao i svaku drugu varijablu. Ovakav postupak će izbaciti sve produkcije koje su dovele do izvoda $S \overset{*}{\Rightarrow}_G \varepsilon$, a prihvaćanje prazne riječi smo osigurali s $S' \to \varepsilon$.

U oba slučaja novodobivena gramatika G' je tražena gramatika. ■

Primjer 35. *Izbacite suvišne produkcije iz gramatike G ako je*

$$\begin{aligned} P.....S &\to 1A \mid 0 \\ A &\to 0A \mid 1A \mid B \mid \varepsilon \\ B &\to 0B \mid 1B \mid \varepsilon. \end{aligned}$$

Vidimo da $\varepsilon \notin L(G)$, pa nije potrebno uvoditi novu početnu varijablu. Postupak provodimo u tri koraka.

1. Izbacimo $B \to \varepsilon$

$$\begin{aligned} S &\to 1A \mid 0 \\ A &\to 0A \mid 1A \mid B \mid \varepsilon \mid \varepsilon \\ B &\to 0B \mid 1B \mid 0 \mid 1. \end{aligned}$$

2. Izbacimo $A \to \varepsilon$

$$\begin{aligned} S &\to 1A \mid 0 \mid 1 \\ A &\to 0A \mid 1A \mid B \mid 0 \mid 1 \\ B &\to 0B \mid 1B \mid 0 \mid 1. \end{aligned}$$

3. Izbacimo $A \to B$

$$\begin{aligned} S &\to 1A \mid 1B \mid 0 \mid 1 \\ A &\to 0A \mid 1A \mid 0B \mid 1B \mid 0 \mid 1 \\ B &\to 0B \mid 1B \mid 0 \mid 1. \end{aligned}$$

Vidimo da su produkcije simetrične po A i B, pa je očigledno jedna od tih varijabli suvišna. Jezik će ostati isti i ako imamo skup produkcija

$$\begin{aligned} S &\to 1A \mid 0 \mid 1 \\ A &\to 0A \mid 1A \mid 0 \mid 1. \end{aligned}$$

Iz slike se još bolje vidi ravnopravnost A i B.

$$slikaDLJ2$$

8.6. Lema o pumpanju za kontekstno slobodne jezike

.....

8.7. Svojstva zatvorenosti klase KSJ

.....

8.8. Aritmetika regularnih izraza

Označimo s $\mathcal{U}$ skup svih jezika u abecedi Σ, to jest uzmimo da je $\mathcal{U} = 2^{\Sigma^*}$. Znamo da će uz relaciju inkluzije $\subseteq$ skup $(\mathcal{U}, \subseteq)$ biti CPO. Najmanji element mu je prazan skup, dok se supremum nekog lanca nalazi kao unija elemenata tog lanca. Definirajmo funkciju $f : \mathcal{U} \to \mathcal{U}$ s

$$f(x) = ax + b,$$

gdje su a i b regularni izrazi koji opisuju neke zadane elemente skupa $\mathcal{U}$ (ako pritom izraz $ax + b$ promatramo kao zapis jezika onda se očigledno radi o zapisu desno linearnog jezika). Funkcija f je u stvari linearna funkcija, pa se lako dokaže da je f neprekidna, a time i monotono rastuća na skupu $\mathcal{U}$. *Zanemarimo na tren razliku između regularnih izraza i skupova koje opisuju.* Lako se provjeri da vrijedi

$$\begin{aligned} \emptyset &\subseteq b = f(\emptyset) \subseteq (a+\varepsilon)\, b = f^2(\emptyset) \subseteq \left(a^2 + a + \varepsilon\right) b = f^3(\emptyset) \subseteq \cdots \\ \cdots &\subseteq \left(a^n + \cdots + a + \varepsilon\right) b = f^{n+1}(\emptyset) \subseteq \cdots . \end{aligned}$$

Iz ovoga slijedi

$$f^\infty(\emptyset) = \left(\sum_{n=0}^{\infty} a^n\right) b = a^* b.$$

Po teoremu o čvrstoj točki znamo da funkcija f ima najmanju čvrstu točku $\mathrm{fix}(f)$ i da je

$$\mathrm{fix}(f) = \sup_n f^n(\perp) = \bigcup_n f^n(\emptyset) = f^\infty(\emptyset) = a^* b.$$

No čvrsta točka funkcije f je u stvari rješenje jednadžbe

$$x = ax + b,$$

pa to rješenje sada znamo i *"algebarski"* izračunati: vrijedi, dakle,

$$x = a^* b.$$

Primjer 36. *Sada npr. znamo riješiti i sustav*

$$\begin{aligned} x &= 0x + 1y + \varepsilon \\ y &= 0y + 1x. \end{aligned}$$

Iz druge jednadžbe po prethodnom dobijemo $y = 0^*1x$, *pa uvrštavanjem u prvu jednadžbu slijedi* $x = 0x + 10^*1x + \varepsilon = (0 + 10^*1)\, x + \varepsilon$, *odakle lako dobijemo* $x = (0 + 10^*1)^* \varepsilon = (0 + 10^*1)^*$ *i zatim* $y = 0^*1\,(0 + 10^*1)^*$.
No ovo nam omogućuje da na gotovo algebarski način nađemo regularni izraz koji opisuje jezik izveden nekom desno linearnom gramatikom. Naime, gramatika G *koja odgovara sustavu iz ovog primjera bila bi zadana produkcijama*

$$\begin{aligned} S &\to 0S \mid 1A \mid \varepsilon \\ A &\to 0A \mid 1S \end{aligned}$$

a vrijedi $L(G) = L(r)$ *gdje je* $r = (0 + 10^*1)^*$ *(jer* S *odgovara izrazu* x*).*

Ostaje odgovoriti da na pitanje kada je ovo rješenje jedinstveno, a na to nam odgovor daje sljedeći teorem. Uočimo da koristimo notaciju regularnih izraza iako radimo s općenitim jezicima.

Teorem 8.8.1. *Neka je za neke $a, b \in \mathcal{U}$ funkcija $f : \mathcal{U} \to \mathcal{U}$ definirana s*

$$f(x) = ax + b.$$

Tada je najmanja čvrsta točka funkcije f jezik a^*b, a ova čvrsta točka je ujedno i jedinstvena ako jezik a ne sadrži praznu riječ.

Dokaz. Da je $\text{fix}(f) = a^*b$ smo dokazali u prethodnom, pa dokažimo još i drugi dio tvrdnje teorema.

Pretpostavimo da $\varepsilon \notin a$, te neka je $x \in \mathcal{U}$ neka druga čvrsta točka funkcije f. Znamo da je funkciji f jezik a^*b najmanja čvrsta točka, pa nužno slijedi $a^*b \subseteq x$. Dokazat ćemo da vrijedi i obratna inkluzija iz čega će odmah slijediti $a^*b = x$.

Uzmimo bilo koju riječ $w \in x$. Kako je $x = ax + b$ slijedi $w \in ax$ ili $w \in b$. Ako je $w \in b$ dokaz je gotov jer iz toga odmah slijedi $w \in a^*b$. Promotrimo drugu mogućnost: ako je $w \in ax$ onda je $w = \alpha_1 w_1$, pri čemu je $\alpha_1 \in a$ i $w_1 \in x$. Kako jezik a ne sadrži praznu riječ mora vrijediti $|\alpha_1| \geq 1$, pa je riječ w_1 kraća od riječi w. Ponovimo prethodni postupak za riječ w_1 : opet je $w_1 \in ax$ ili $w_1 \in b$. Ako je $w_1 \in b$ dokaz je gotov, a ako nije opet zaključimo da je $w_1 = \alpha_2 w_2$, pri čemu je $\alpha_2 \in a$ i $w_2 \in x$. Postupak možemo nastaviti do u najviše $|x|$ koraka, tj. u nekom trenutku moramo dobiti $w_k \in b$. Iz toga slijedi

$$w = \alpha_1 \cdots \alpha_i \cdots \alpha_k w_k,$$

pri čemu su $\alpha_1, \ldots, \alpha_i, \ldots, \alpha_k \in a$ i $w_k \in b$, pa je $w \in a^*b$. Dakle, $x \subseteq a^*b$. ■

Ovaj nam teorem daje uvjet pod kojim će jezik a^*b sigurno biti jedinstveno rješenje jednadžbe $x = ax + b$, no odmah se može postaviti pitanje vrijedi li možda i neki slabiji uvjet, odnosno može li jezik a^*b biti jedinstveno rješenje jednadžbe $x = ax + b$ i ako jezik a sadrži praznu riječ? Odgovor je niječan: može se dokazati da je pod takvom pretpostavkom i jezik $(a^*b)^*$ čvrsta točka funkcije f.

U prethodnom smo se bavili rješenjima jednadžbi oblika $x = ax + b$ koje odgovaraju desno linearnim produkcijama, to jest produkcijama oblika $A \to aA \mid b$, no mi znamo da produkcije kontekstno slobodnih gramatika mogu imati općenitiji oblik

$$A_i \to u_1 A_{i_1} u_2 A_{i_2} u_3 \cdots u_k A_{i_k} u_{k+1} \mid \cdots, \quad i = 1, \ldots, n,$$

pri čemu je n broj varijabli promatrane gramatike. Uvedemo li kao i prije varijable $x_1, \ldots, x_n$ dobit ćemo jednadžbe oblika

$$x_i = u_1 x_{i_1} u_2 x_{i_2} u_3 \cdots u_k x_{i_k} u_{k+1} + \cdots, \quad i = 1, \ldots, n.$$

Sada definiramo funkcije $f_i : \mathcal{U}^n \to \mathcal{U}$ izrazima

$$f_i(x_1, \ldots, x_n) = x_i, \quad i = 1, \ldots, n.$$

Da bismo izbjegli rad s n funkcija izvršit ćemo spajanje svih f_i u jednu vektorsku funkciju $h_G : \mathcal{U}^n \to \mathcal{U}^n$ definiranu s

$$h_G(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)).$$

Iz činjenice da su sve f_i neprekidne odmah slijedi i da je h_G neprekidna (naime, i $\mathcal{U}^n$ je CPO uz koordinatno prenošenje uređaja iz $\mathcal{U}$, pa je neprekidnost po koordinatama dovoljna za globalnu neprekidnost). Po teoremu o čvrstoj točki zaključujemo da i funkcija h_G ima najmanju čvrstu točku

$$\operatorname{fix}(h_G) = (\operatorname{fix}(h_G)_1, \ldots, \operatorname{fix}(h_G)_n) = \sup_m h_G^m(\bot^n) = \bigcup_m h_G^m(\emptyset, \ldots, \emptyset).$$

No da bismo zaista odredili o kojim se jezicima tu radi potrebna nam je sljedeća lema.

Lema 8.8.1. *Riječ $w \in L(G)$ pripada jeziku $h_G^m(\emptyset, \ldots, \emptyset)_i$ ako i samo ako u gramatici G ima stablo izvoda visine ne veće od m u čijem korijenu je labela A_i.*

Dokaz. Dokaz provodimo indukcijom po $m \in \mathbb{N}_0$.

Ako je $m = 0$, onda je

$$h_G^m(\emptyset, \ldots, \emptyset)_i = h_G^0(\emptyset, \ldots, \emptyset)_i = (\emptyset, \ldots, \emptyset)_i = \emptyset.$$

Visina stabla izvoda ne može biti nula, pa nijedna riječ w nema takvo stablo, dakle $w \in \emptyset = h_G^0(\emptyset, \ldots, \emptyset)_i$, čime je dokazana baza indukcije u oba smijera.

Pretpostavimo da tvrdnja vrijedi u oba smijera za $m \in \mathbb{N}_0$.

Uzmimo sada neku riječ

$$w \in h_G^{m+1}(\emptyset, \ldots, \emptyset)_i = h_G(h_G^m(\emptyset, \ldots, \emptyset))_i.$$

To znači da je w nastala primjenom produkcije

$$A_i \to u_1 A_{i_1} u_2 A_{i_2} u_3 \cdots u_k A_{i_k} u_{k+1},$$

i oblika je

$$w = u_1 w_{i_1} u_2 w_{i_2} u_3 \cdots u_k w_{i_k} u_{k+1},$$

gdje su podriječi $w_{i_j} \in h_G^m(\emptyset, \ldots, \emptyset)_{i_j}$ za sve $j \in \{1, \ldots, k\}$. Po pretpostavci indukcije znamo da za svaku podriječ w_{i_j} postoji odgovarajuće stablo izvoda visine ne veće od m, a s labelom A_{i_j} u korijenu. Polazna riječ w ima, dakle, stablo izvoda kao na slici:

$$slikaDL2$$

Obratno, ako w ima ovakvo stablo izvoda, onda je

$$w = u_1 w_{i_1} u_2 w_{i_2} u_3 \cdots u_k w_{i_k} u_{k+1},$$

pri čemu po definiciji stabla izvoda u G mora postojati produkcija oblika

$$A_i \to u_1 A_{i_1} u_2 A_{i_2} u_3 \cdots u_k A_{i_k} u_{k+1}$$

a sve podriječi w_{i_j} imaju stabla izvoda koja su prava podstabla polaznog stabla (dakle, visina im nije veća od m) i u korijenu svakog od njih je odgovarajući A_{i_j}. Po pretpostavci indukcije slijedi $w_{i_j} \in h_G^m(\emptyset, \ldots, \emptyset)_{i_j}$ za sve $j \in \{1, \ldots, k\}$, pa je

$$w \in h_G(h_G^m(\emptyset, \ldots, \emptyset))_i, \ tj.\ w \in h_G^{m+1}(\emptyset, \ldots, \emptyset)_i.$$

Ovim je dokaz leme završen u oba smijera. ■

Teorem 8.8.2. *Riječ $w \in L(G)$ je iz $\operatorname{fix}(h_G)_i$ ako i samo ako $A_i \overset{*}{\Rightarrow}_G w$.*

Dokaz. Direktno iz prethodne leme uzmemo li u obzir da je

$$\operatorname{fix}(h_G)_i = \left(\bigcup\nolimits_m h_G^m(\emptyset, \ldots, \emptyset)\right)_i = \bigcup\nolimits_m h_G^m(\emptyset, \ldots, \emptyset)_i .$$

Naime vrijedi

$$\begin{aligned} w \quad &\in \quad \operatorname{fix}(h_G)_i \leftrightarrow w \in \left(\bigcup\nolimits_m h_G^m(\emptyset, \ldots, \emptyset)\right)_i \\ &\leftrightarrow \quad w \in \bigcup\nolimits_m h_G^m(\emptyset, \ldots, \emptyset)_i \leftrightarrow (\exists m \in \mathbb{N}_0)\, w \in h_G^m(\emptyset, \ldots, \emptyset)_i \\ &\leftrightarrow \quad (\exists m \in \mathbb{N}_0)\, A_i \overset{m}{\Rightarrow}_G w \leftrightarrow A_i \overset{*}{\Rightarrow}_G w. \end{aligned}$$

■

Korolar 8.8.1. *(DLJ $\subseteq$ RJ) Svi desno linearni jezici su regularni.*

Dokaz. Neka je L proizvoljan desno linearan jezik. Tada postoji desno linearna gramatika G takva da vrijedi $L = L(G)$. Sve jednadžbe dobivene iz produkcija gramatike G su oblika $x = ax + b$, pri čemu su a i b regularni izrazi. Rješenje ovakve jednadžbe je $x = a^*b$, što je regularan izraz. Shodno tome i konačno rješenje odgovarajuće jednadžbe za varijablu S biti će opisano regularnim izrazom, pa je i sam jezik $L(G) = L$ regularan. ■

Poglavlje 9.

Potisni automati

.....

Poglavlje 10.

Semantike programskih jezika

.....

Poglavlje 11.

Apstraktni strojevi sa stanjima

.....

Poglavlje 12.

Zadaci za vježbu

.....

Bibliografija

[1] J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages and Computation*, Addison Wesley Publishing Company, Reading, 1979.

[2] K. Kuratowski, A. Mostowski, *Set Theory*, North-Holand Publishing Company Amsterdam, 1968.

[3] M. Vuković, *Matematička logika I*, skripta Matematičkog odjela PMF-a, 2004.