Krohn-Rhodesova teorija

Miošić, Ivan

Krohn-Rhodesova teorija

Miošić, Ivan

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Ivan Miošić

KROHN-RHODESOVA TEORIJA

Diplomski rad

Voditelji rada:
doc. dr. sc. Marko Horvat
doc. dr. sc. Vedran Čačić

Zagreb, 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Gospodinu, roditeljima i sestrama

Sadržaj

Uvod

Krohn-Rhodesova teorija začeta je 1965. godine značajnim rezultatom u teoriji konačnih polugrupa. Za svoj rad [11], autori Kenneth Krohn i John Rhodes zaslužili su doktorsku titulu redom sa sveučilišta MIT i Harvard. Štoviše, cijela matematička teorija, koju izlažemo u ovom radu, dobila je naziv po ovom dvojcu.

Krohn-Rhodesov teorem za konačne polugrupe analogon je Jordan-Hölderovog teorema za konačne grupe. Ugrubo govoreći, ovaj teorem dokazuje postojanje prostih faktora u teoriji konačnih polugrupa. Preciznije, ustanovljeno je postojanje kolekcije jednostavnih konačnih polugrupa čijim kombiniranjem je moguće dobiti sve konačne polugrupe. Iznenađujuća je činjenica da se dokaz i interpretacija ovog čisto algebarskog rezultata oslanjaju na teoriju konačnih automata. U ovom radu razmatramo prvenstveno ovu neočekivanu povezanost algebre i računarstva te opisujemo sve pojmove potrebne za shvaćanje Krohn-Rhodesova teorema.

Cijeli ovaj rad prožima središnja ideja o povezanosti između konačnih automata i konačnih polugrupa. Konačni automat najjednostavniji je matematički model izračunavanja. Zami-šljamo ga kao apstraktni stroj koji se može nalaziti u konačno mnogo stanja. Ovaj stroj može primati kao ulaz konačno mnogo različitih znakova. Nakon čitanja jednog znaka, stroj mijenja svoje stanje ovisno o trenutnom stanju i pročitanom znaku te prelazi na čitanje novog znaka. Izračunavanje konačnog automata stoga ovisi o konačnom nizu ulaznih znakova i shvaćamo ga kao slijed stanja u kojima se stroj nalazi tijekom čitanja znakova. Polugrupa je temeljna algebarska struktura. To je naprosto skup čije elemente možemo kombinirati tako da kao rezultat dobijemo elemente iz istog skupa. Istaknuto svojstvo ove operacije je *asocijativnost*, čime je omogućeno njeno ulančavanje.

Kako bismo detaljnije razmotrili gore navedenu povezanost, proučavat ćemo dualnu teoriju, čiji je jedan dio smješten u teorijskom računarstvu, a drugi u apstraktnoj algebri. U fokusu nam je računarski aspekt teorije, dok algebarski koristimo uglavnom kao sredstvo za analizu konačnih automata.

Nakon uvođenja osnovnih pojmova (odjeljci 1.1, 1.2 i 1.3), konačnom automatu pridružujemo konačnu polugrupu na prirodan način (odjeljak 1.4). Prvo poglavlje zatvaramo uvođenjem *transformacijske polugrupe*, algebarske strukture kojoj je u

osnovi konačna polugrupa i njeno *djelovanje* na skup (odjeljak 1.5). Pokazano je da ova struktura potpuno algebarski opisuje konačni automat. Argumentirana je i obratna tvrdnja, dakle da je konačni automat računarski pandan transformacijske polugrupe.

Dva početna odjeljka drugog poglavlja bave se međusobnim odnosom dvaju konačnih automata te transformacijskih polugrupa. Kao i u ostalim algebarskim teorijama, zanimaju nas preslikavanja koja čuvaju strukturu ovih objekata i koja posljedično omogućuju da poistovjetimo objekte s istim karakteristikama (odjeljak 2.1). Potom se okrećemo specifičnijem obliku odnosa, karakterističnim za logičko-računarske teorije — pojam *simulacije* jednog objekta drugim (odjeljak 2.2). U literaturi o konačnim automatima za ovaj pojam uobičajen je naziv *prekrivanje*, što poštujemo i ovdje.

U preostala dva odjeljka drugog poglavlja uvodimo važne metode kombiniranja konačnih automata, odnosno transformacijskih polugrupa. Motivaciju za ove postupke pronalazimo razmatrajući konačne automate s izlazom (odjeljak 2.3). Njihovi serijski i paralelni spojevi usmjeravaju nas u definiciji raznovrsnih *produkata* konačnih automata, odnosno transformacijskih polugrupa (odjeljak 2.4).

Time završavamo pregled temeljnih pojmova u dualnoj teoriji. Zadnje poglavlje postupno nas vodi do glavnog rezultata teorije, proslavljenog i već spomenutog Krohn-Rhodesovog teorema. On govori o *dekompozicijama* složenijih automata u jednostavnije. Tehnika kojom se koristimo kako bismo proizveli tražene dekompozicije slična je kao u teoriji grupa, gdje do dekompozicijskih rezultata dolazimo promatranjem kvocijentnih struktura (odjeljci 3.1 i 3.2).

U procesu rastava proizvoljnog konačnog automata susrećemo se sa dvije ključne vrste jednostavnijih konačnih automata (odjeljci 3.3 i 3.4). U konačnim automatima prve vrste svaki ulaz jednoznačno određuje sljedeće stanje automata, neovisno o trenutnom stanju, pa ih nazivamo *reset* automati. Kod druge vrste konačnih automata svaki ulaz permutira cijeli skup stanja automata, stoga ih nazivamo *permutacijski*.

Rad kulminira iskazom Krohn-Rhodesovog teorema (odjeljak 3.5). Iznosimo djelomični dokaz, a čitatelja upućujemo na relevantnu literaturu za detalje. Zaključno raspravljamo o važnosti i utjecaju ovog rezultata, te spominjemo novija istraživanja u Krohn-Rhodesovoj teoriji, koja pokazuju postojanje aktivnog interesa za ovo područje.

Poglavlje 1

Osnovni pojmovi

Iako su neki od njih općepoznati, izlažemo osnovne pojmove radi potpunosti, utvrđivanja notacije i isticanja rezultata potrebnih u nastavku. Iskusniji čitatelji mogu preskočiti prva tri odjeljka i koristiti ih samo kao referencu. Sadržajno slijedimo glavni izvor [8], uz određene stilske i notacijske promjene.

Pretpostavljamo osnovno poznavanje naivne teorije skupova (za podsjetnik vidi [19, Uvod]). Prema udžbeniku [24], skup prirodnih brojeva bez nule označavamo s $\mathbb{N}_+ = \{\,1, 2, 3, \dots\,\}$, a skup $\{\,0\,\} \cup \mathbb{N}_+$ s $\mathbb{N}$. Također, identitetu na proizvoljnom skupu X označavamo s I_X.

1.1 Relacije

Definicija 1.1. Neka su X i Y skupovi. *Relacija* između skupova X i Y je podskup Kartezijevog produkta $X \times Y$.

Neka je R relacija između skupova X i Y. Za par $(x, y) \in X \times Y$ takav da vrijedi $(x, y) \in R$ obično pišemo $x\ R\ y$. Ako vrijedi $X = Y$, tada kažemo da je R relacija *na* skupu X.

Definicija 1.2. Neka je X skup i R relacija na X. Za relaciju R kažemo da je *refleksivna* ako za sve $x \in X$ vrijedi $x\ R\ x$. Relacija R je *simetrična* ako za sve $x, y \in X$ takve da $x\ R\ y$ vrijedi i $y\ R\ x$. Konačno, relacija R je *tranzitivna* ako za sve $x, y, z \in X$ vrijedi:

$$(x\ R\ y) \wedge (y\ R\ z) \implies x\ R\ z.$$

Relacija ekvivalencije na skupu X je refleksivna, simetrična i tranzitivna relacija.

Definicija 1.3. Neka je X neprazan skup. Skup π podskupova od X je *particija* skupa X ako vrijedi:

(i) svaki skup $A \in \pi$ je neprazan;

(ii) $\bigcup \pi := \bigcup_{A \in \pi} A = X$;

(iii) za sve $A, B \in \pi$, $A \neq B$, vrijedi $A \cap B = \emptyset$.

Skup δ podskupova od X je *dekompozicija* skupa X ako za njega vrijede uvjeti (i) i (ii). Elemente particije (dekompozicije) nazivamo *blokovi*. Particije $\{ X \}$ i $\{ \{ x \} : x \in X \}$ nazivamo *trivijalne*.

Kao što je poznato, relacije ekvivalencije i particije skupa usko su povezane. Neka je X neprazan skup i R relacija ekvivalencije na X. Za svaki $x \in X$ definiramo skup $[x]_R = \{ y \in X : x \, R \, y \} \subseteq X$ koji zovemo *klasa ekvivalencije* od x s obzirom na relaciju R (ukoliko je relacija ekvivalencije R jasna iz konteksta, pišemo samo $[x]$). Sada definiramo skup $X/R = \{ [x]_R : x \in X \}$. Lako se uvjeriti da ovaj skup čini particiju skupa X. Zovemo ga *kvocijentni skup* od X s obzirom na relaciju R.

Obratno, neka je zadana particija π skupa X. Neka je relacija R na X definirana tako da za sve $x, y \in X$ vrijedi $x \; R \; y$ ako i samo ako x i y pripadaju istom bloku particije π. Pokazuje se da je R relacija ekvivalencije na skupu X. Zovemo je *relacija ekvivalencije pridružena particiji* π.

U oba slučaja, dobro su definirane surjekcije $\varphi_R : X \to X/R$ i $\varphi_\pi : X \to \pi$ takve da za sve $x \in X$ vrijedi:

$$\varphi_R(x) = [x]_R \text{ i}$$
$$\varphi_\pi(x) = A, \text{ gdje je } A \text{ jedinstveni blok particije } \pi \text{ koji sadrži } x.$$

Zovemo ih *kanonska surjekcija na kvocijentni skup*, odnosno *particiju*.

Vraćamo se u kontekst općenitih relacija. Neka je W neprazan skup i R relacija na W. Uređeni par $\mathcal{F} = (W, R)$ nazivamo *relacijska struktura* ili *okvir* (eng. *frame*). Definiramo pojam **bisimulacije**, koji predstavlja moćan alat u modalnoj logici (vidi [3]). Kako i samo ime govori, bisimulacija je formalizacija koncepta međusobne simulabilnosti između sustava. Sa sličnim konceptom ćemo se susresti u nastavku (vidi odjeljak 2.2).

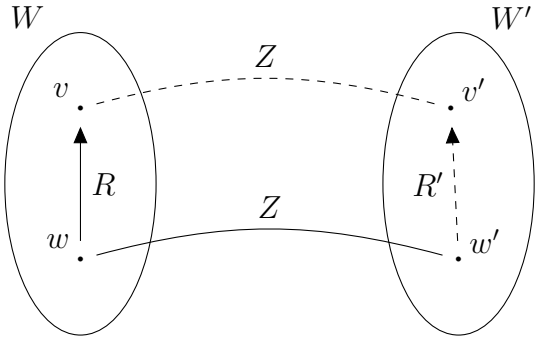
Definicija 1.4 (Bisimulacija)**.** Neka su $\mathcal{F} = (W, R)$ i $\mathcal{F}' = (W', R')$ okviri. Neka je Z relacija između skupova W i W'. Kažemo da je relacija Z *bisimulacija okvira* $\mathcal{F}$ i $\mathcal{F}'$ ako vrijede uvjeti:

(i) $(\forall\, (w, w') \in Z)\, (\forall v \in W)\; (w \; R \; v \implies (\exists v' \in W')\; (v, v') \in Z \wedge w' \; R' \; v')$;

(ii) $(\forall\, (w, w') \in Z)\, (\forall v' \in W')\; (w' \; R' \; v' \implies (\exists v \in W)\; (v, v') \in Z \wedge w \; R \; v)$.

Ako postoji bisimulacija između okvira $\mathcal{F}$ i $\mathcal{F}'$, kažemo da su oni *bisimulirani*.

Dijagram koji ilustrira uvjet (i) je dan na slici 1.1. Ako zrcalimo sliku u odnosu na vertikalnu os, dobijemo ilustraciju uvjeta (ii). Kako bismo intuitivno opisali pojam bisimulacije iz definicije 1.4, nazovimo elemente skupova W i W' *svjetovi*, a relacije R i R' shvatimo kao relacije *dostižívosti* između svjetova. Dakle, ako za $w, v \in W$ vrijedi $w\ R\ v$, kažemo da je svijet v *dostižív* iz svijeta w. Uvjet (i) iz definicije bisimulacije sada interpretiramo na sljedeći način. Za bilo koji uređeni par svjetova $(w, w') \in Z$ i bilo koji svijet $v \in W$ dostižív iz w, postoji svijet $v' \in W'$ koji je dostižív iz w', takav da vrijedi $(v, v') \in Z$.



Slika 1.1: Bisimulacija između okvira ([3, slika 2.3])

Mi ćemo zahtijevati da bisimulacija povezuje svaki svijet prvog okvira s barem jednim svijetom drugog okvira, i obratno. Slijedi formalizacija ovog koncepta.

Definicija 1.5. Neka su X i Y skupovi. Kažemo da je relacija $R \subseteq X \times Y$ *bisurjektivna* ako vrijedi:

(i) $(\forall x \in X)\,(\exists y \in Y)\ x\ R\ y$;

(ii) $(\forall y \in Y)\,(\exists x \in X)\ x\ R\ y$.

Primjer 1.6. Neka je sada $\mathcal{R}$ skup relacija na nepraznom skupu W. Uređeni par $\mathcal{F} = (W, \mathcal{R})$ nazivamo *generalizirani okvir*. Računarski primjer generaliziranog okvira je *označeni tranzicijski sustav* (kratica LTS, od eng. *Labelled Transition System*). Slijedi definicija i opis.

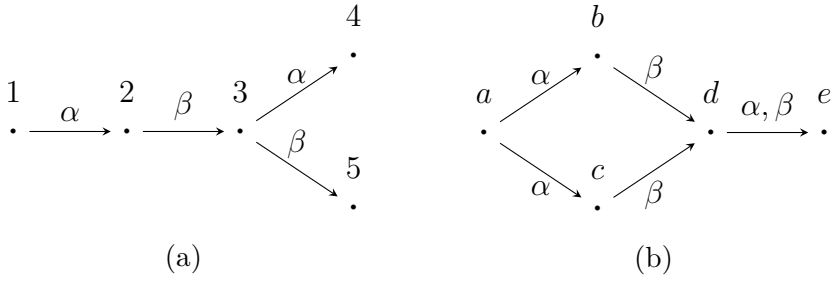
Neka je S neprazan skup i $\{\, R_\ell \colon \ell \in L \,\}$ skup relacija na S indeksiran skupom L. LTS je uređeni par $(S, \{\, R_\ell \colon \ell \in L \,\})$. Skup S zovemo *skup stanja* (eng. *states*), a skup L *skup oznaka* (eng. *labels*). Na slici 1.2 prikazani su LTS-ovi $\mathcal{F} = (S, \{\, R_\ell \colon \ell \in L \,\})$ i $\mathcal{F}' = (S', \{R'_\ell \colon \ell \in L\})$, gdje je $S = \{\, 1, 2, 3, 4, 5 \,\}$, $S' = \{\, a, b, c, d, e \,\}$ i $L = \{\, \alpha, \beta \,\}$.

Definiramo relaciju $Z \subset S \times S'$ tako da vrijedi:

$$Z = \{\, (1,a)\,, (2,b)\,, (2,c)\,, (3,d)\,, (4,e)\,, (5,e)\,\}\,.$$

Može provjeriti da je Z bisurjektivna bisimulacija okvira $\mathcal{F}$ i $\mathcal{F}'$ (uz zanemarivanje oznaka).

Vidimo da LTS-ovi mogu poslužiti kao apstraktni model izračunavanja ([3, primjer 1.3]). U toj interpretaciji, stanja predstavljaju stanja računala, a oznake programe. Tada $r\ R_\ell\ v$ znači da postoji izvršavanje programa ℓ koje počinje u stanju u i završava u stanju v.



Slika 1.2: Primjer LTS-ova ([3, slika 2.4])

Za opis automata kojima ćemo se baviti, trebamo koncept **parcijalne funkcije**. Intuitivno, parcijalna funkcija je preslikavanje među skupovima koje može biti nedefinirano u nekim točkama domene.

Definicija 1.7. Neka su X i Y skupovi te $\varnothing \notin X \cup Y$. *Parcijalna funkcija* iz skupa X u skup Y je svaka funkcija $F\colon X \cup \{\,\varnothing\,\} \to Y \cup \{\,\varnothing\,\}$ takva da vrijedi $F\,(\varnothing) = \varnothing$. Pišemo $F\colon X \rightharpoonup Y$.

Skup $\mathcal{D}_F = \{\, x \in X\colon F(x) \neq \varnothing\,\} \subseteq X$ zovemo *domena specifikacije* parcijalne funkcije F. Ako je $\mathcal{D}_F = X$, parcijalnu funkciju F smatramo pravom funkcijom s domenom X (kažemo i *totalnom na* X). Ako pak vrijedi $\mathcal{D}_F = \emptyset$, parcijalna funkcija F zove se *prazna funkcija* i označava s $\mathcal{E}$ (ponekad i $\mathcal{E}_X$).

Skup svih parcijalnih funkcija iz skupa X u skup Y označavamo s $\mathbf{PF}\,(X,Y)$. Posebno, ako je $X = Y$, umjesto $\mathbf{PF}\,(X,X)$ pišemo samo $\mathbf{PF}\,(X)$.

1.2 Konačni automati

Kao što smo opisali u uvodu, konačni automat zamišljamo kao apstraktni stroj koji se u svakom trenutku nalazi u točno jednom od konačno mnogo stanja. Trenutno stanje automata mijenja se ovisno o ulaznim podacima. Slijedi formalni opis.

Definicija 1.8 (Konačni automat)**.** *Konačni automat* je uređena trojka $\mathcal{M} = (Q, \Sigma, F)$, gdje je:

- Q konačan skup koji zovemo *skup stanja*;
- Σ konačan skup koji zovemo *ulazna abeceda* ili *alfabet*;
- $F\colon Q \times \Sigma \rightharpoonup Q$ parcijalna funkcija koju zovemo *funkcija prijelaza*.

Ako je funkcija prijelaza F totalna, kažemo da je automat $\mathcal{M}$ *potpun*.

Neka je alfabet Σ iz prethodne definicije. Njegove elemente nazivat ćemo *znakovi*, a neprazne konačne nizove znakova iz Σ *riječi*. Riječ $w = (\sigma_1, \sigma_2, \ldots, \sigma_k)$ pišemo kraće $w = \sigma_1\sigma_2\cdots\sigma_k$. Broj $k \in \mathbb{N}_+$ zovemo *duljina riječi* i pišemo $|w| = k$. Skup svih riječi nad alfabetom Σ označavamo sa Σ^+.

Opišimo sada formalno rad automata. Pristup je sličan onome iz [17], vrlo popularne knjige iz teorije izračunljivosti.

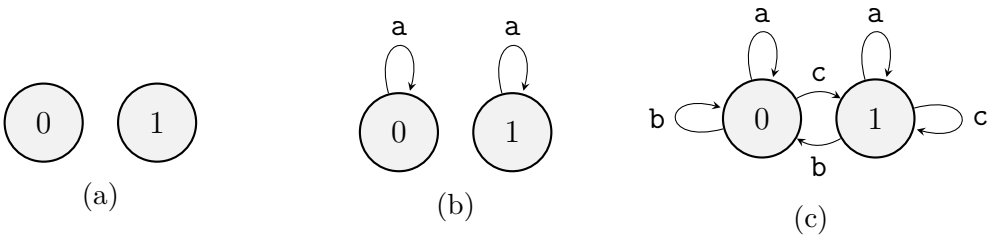
Definicija 1.9. Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat i $q_0 \in Q$ proizvoljno stanje. Neka je $w = \sigma_1\sigma_2\cdots\sigma_k \in \Sigma^+$ riječ. Konačni niz stanja $q_0, q_1, \ldots, q_k \in Q$ takvih da vrijedi $q_i = F(q_{i-1}, \sigma_i)$ za svaki $i = 1, 2, \ldots, k$ nazivamo *izračunavanje* automata $\mathcal{M}$ s riječi w iz stanja q_0. Stanje q_0 naziva se *početno*, stanje q_k *završno*, dok se riječ w naziva *ulazna riječ* ili samo *ulaz*. Ako vrijedi $F(q_{j-1}, \sigma_j) = \varnothing$ za neki $j \leq k$, neka je $\ell \leq k$ najmanji takav. Kažemo da je izračunavanje automata $\mathcal{M}$ *prekinuto znakom* σ_ℓ.

Primjer 1.10. Konačne automate obično prikazujemo dijagramima, preciznije označenim usmjerenim grafovima.

(*i*) Najmanji automati imaju jedno stanje i jednočlani alfabet. Neka je dakle $Q = \{0\}$ i $\Sigma = \{\mathtt{a}\}$. Postoje dva konačna automata sa skupom stanja Q i ulaznom abecedom Σ, prikazana na slici 1.3. U prvom automatu funkcija prijelaza je prazna, dok se u drugom ponaša kao identiteta na skupu Q.

(*ii*) Situacija je zanimljivija ako imamo više stanja i/ili elemenata alfabeta. Neka je $Q = \{0, 1\}$ i $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. Na slici 1.4 prikazana su tri moguća konačna automata sa skupom stanja Q i alfabetom Σ.

Slika 1.3: Svi konačni automati s jednim stanjem i jednočlanim alfabetom



Slika 1.4: Konačni automati s dva stanja i tročlanom abecedom

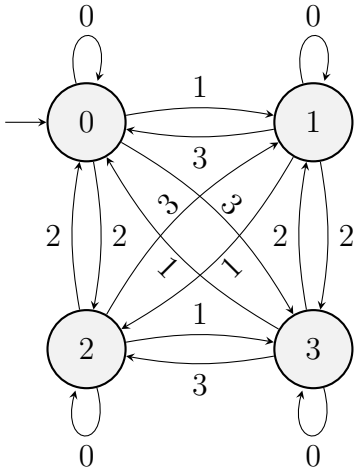
(*iii*) Neka je $N \in \mathbb{N}$ i $Q = \Sigma = \{\, 0, 1, \ldots, N-1 \,\}$. Konstruirajmo konačni automat za zbrajanje modulo N. Za svaki $(q, \sigma) \in Q \times \Sigma$ definirajmo

$$F(q, \sigma) = (q + \sigma) \bmod N.$$

Dijagram za $N = 4$ je prikazan na slici 1.5. Ukoliko računanje automata pokrenemo iz stanja 0 (označenog strelicom ni od kuda) s početnom riječi $w \in \Sigma^+$, završit ćemo u stanju koje odgovara zbroju svih članova konačnog niza w modulo N.

(*iv*) Konačni automati neraskidivo su povezani s *regularnim izrazima*. Kao što smo istaknuli, tematika formalnih jezika nam nije u fokusu, no svakako je vrijedna spomena (istaknimo da postoje algebarske teorije koje se primarno bave odnosom konačnih automata i regularnih izraza, vidi [10], [22], [5, Volume A]). Ograničavamo se na iznošenje samo najosnovnijih pojmova (opširnije se može pročitati u već spomenutom udžbeniku [17]).

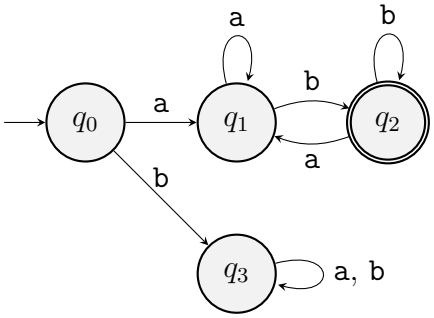
Jezik nad alfabetom Σ je podskup od Σ^* (vidi primjer 1.17). *Regularni izraz* je jezik dobiven od praznih i jednočlanih jezika konačnom primjenom regularnih operacija: unije, konkatenacije i Kleenejeve zvijezde. *Deterministički automat* je petorka $(Q, \Sigma, \delta, q_0, F)$, gdje je (Q, Σ, δ) potpuni konačni automat, $q_0 \in Q$ istaknuto stanje koje nazivamo *početno* te $F \subseteq Q$ skup stanja koja nazivamo *stanja prihvaćanja*. Kažemo da deterministički automat *prihvaća* riječ $w \in \Sigma^*$ ako završno stanje njegovog izračunavanja s ulazom w iz stanja q_0 pripada



Slika 1.5: Konačni automat za zbrajanje modulo $N = 4$

skupu F. Jezik koji *prepoznaje* deterministički automat je skup svih riječi koje taj automat prihvaća. Poznato je da deterministički automati prepoznaju točno regularne izraze ([17, teorem 1.54]).

Deterministčke automate prikazujemo vrlo slično konačnim automatima. Početno stanje označeno je strelicom ni od kuda, dok su završna stanja obrubljena dvjema kružnicama. Automat na slici 1.6 prepoznaje regularni izraz $\mathtt{a}\,(\mathtt{a} \cup \mathtt{b})^*\,\mathtt{b}$. To je jezik koji se sastoji od svih riječi nad alfabetom $\Sigma = \{\,\mathtt{a}, \mathtt{b}\,\}$ koje počinju znakom `a` i završavaju znakom `b`.



Slika 1.6: Deterministički automat koji prepoznaje regularni izraz $\mathtt{a}\,(\mathtt{a} \cup \mathtt{b})^*\,\mathtt{b}$

Vidljiva je sličnost između konačnih automata i LTS-ova iz primjera 1.6. Doista, svaki konačni automat možemo interpretirati kao LTS. U nastavku opisujemo pretvorbu konačnog automata u LTS. Tijekom ovog procesa ćemo se susresti s važnim konceptima za daljnje proučavanje konačnih automata.

Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Najprije fiksirajmo proizvoljni znak σ iz alfabeta Σ. Promotrimo automat $\mathcal{M}$ „restringiran" na znak σ, dakle razmotrimo samo prijelaze u kojima sudjeluje znak σ. Ovo nas navodi da definiramo parcijalnu funkciju $F_\sigma \colon Q \rightharpoonup Q$ tako da za sve $q \in Q$ vrijedi

$$F_\sigma(q) = F(q, \sigma). \tag{1}$$

LTS $\mathcal{F} = (Q, \{\, F_\sigma \colon \sigma \in \Sigma \,\})$ nazivamo *LTS pridružen konačnom automatu* $\mathcal{M}$. Vidimo da je, u smislu izračunavanja, LTS $\mathcal{F}$ istovjetan konačnom automatu $\mathcal{M}$.

Napomena. Glavna razlika između konačnih automata i LTS-ova (izuzev moguće beskonačnosti skupa relacija) jest funkcijsko svojstvo relacije prijelaza kod konačnih automata. Ovime je osigurana jednoznačnost izračunavanja konačnih automata. LTS-ovi su primjer nedeterminističkog modela izračunavanja.

Osvrnimo se i na parcijalnost funkcije prijelaza kod konačnih automata. Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Element $\varnothing \notin Q$ možemo shvatiti kao bespovratno stanje potpunog automata $\mathcal{M}' = (Q \cup \{\, \varnothing \,\}, \Sigma, F)$. Kao takvo, ovo stanje implementira poznati programerski koncept *iznimke* (eng. *exception*) u izračunavanju.

Primjer 1.11. Razmatramo konačne automate iz primjera 1.10. U dijelu (i), kod prvog automata je parcijalna funkcija $F_{\mathtt{a}}$ prazna. Kod drugog automata je $F_{\mathtt{a}} = I_Q$.

U dijelu (ii), kod automata sa slike 1.4a su sve parcijalne funkcije $F_{\mathtt{a}}$, $F_{\mathtt{b}}$ i $F_{\mathtt{c}}$ prazne. Za automat sa slike 1.4b vrijedi $F_{\mathtt{a}} = I_Q$ te su funkcije $F_{\mathtt{b}}$ i $F_{\mathtt{c}}$ ponovno prazne. Kod automata sa slike 1.4c imamo ponovno $F_{\mathtt{a}} = I_Q$, dok su funkcije $F_{\mathtt{b}}$ i $F_{\mathtt{c}}$ redom konstante s vrijednostima 0 i 1 na Q.

U dijelu (iii), za sve $\sigma \in \Sigma$, parcijalna funkcija F_σ zadana je tako da za sve $q \in Q$ vrijedi $F_\sigma(q) = (q + \sigma) \bmod N$.

Uvedimo još jedan koristan pojam vezan uz konačni automat $\mathcal{M} = (Q, \Sigma, F)$. Ako postoji $\sigma \in \Sigma$ takav da vrijedi $F_\sigma = I_Q$, tada kažemo da je automat $\mathcal{M}$ *monoidan*. U suprotnom, možemo ga dopuniti do monoidnog automata.

Definicija 1.12. Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat koji nije monoidan. Neka je $\Lambda \notin \Sigma$. Definiramo skup $\Sigma^\bullet = \Sigma \cup \{\, \Lambda \,\}$ i funkciju $F^\bullet \colon Q \times \Sigma^\bullet \rightharpoonup Q$ tako da $F^\bullet|_{Q \times \Sigma} = F$ te dodatno $F^\bullet_\Lambda = I_Q$. Konačni automat $\mathcal{M}^\bullet = (Q, \Sigma^\bullet, F^\bullet)$ nazivamo *monoidni automat pridružen automatu* $\mathcal{M}$.

Primjer 1.13. Primjetimo da je automat sa slike 1.3b monoidni automat pridružen konačnom automatu sa slike 1.3a. Isto vrijedi i za monoidni automat sa slike 1.4b u odnosu na konačni automat sa slike 1.4a.

1.3 Polugrupe

Osnovna algebarska struktura koju ćemo izučavati u ovom radu jest polugrupa. Pretpostavljamo da je čitatelj upoznat s osnovnim algebarskim pojmovima, kao što su binarna operacija na skupu i asocijativnost (vidi [25]).

Definicija 1.14 (Polugrupa)**.** Neka je S neprazan skup i neka je $\cdot\colon S \times S \to S$ asocijativna binarna operacija na S. Uređeni par $(S, \cdot)$ naziva se *polugrupa*. Operaciju $\cdot$ zovemo još i *množenje*. Govorimo i samo o polugrupi S, podrazumijevajući pritom množenje. Za $s, s' \in S$, kraće pišemo ss' umjesto $s \cdot s'$. Ponekad ćemo pak pisati $s \cdot_S s'$, kako bismo naglasili polugrupu.

Zbog asocijativnosti množenja, umnožak $n \in \mathbb{N}_+$ elemenata $s_1, s_2, \ldots, s_n$ polugrupe S neovisan je o položaju zagrada. Pišemo $\prod_{i=1}^{n} s_i := s_1 s_2 \cdots s_n$. U slučaju da vrijedi $s_1 = s_2 = \cdots = s_n = s$, koristimo oznaku $s^n := \prod_{i=1}^{n} s_i$.

Primjer 1.15. Neka je X proizvoljan skup. Na skupu $\mathbf{PF}(X)$ svih parcijalnih funkcija iz X u X (vidi definiciju 1.7) definiramo množenje kao kompoziciju funkcija. Neka je za sve $f, g \in \mathbf{PF}(X)$ umnožak fg jednak kompoziciji $g \circ f$ (za motivaciju ovog poretka vidi odjeljak 1.4). Skup $\mathbf{PF}(X)$ s ovim množenjem čini polugrupu. Primijetimo još da je $\mathbf{PF}(X)$ konačna polugrupa ako i samo ako je skup X konačan.

Definicija 1.16. Neka je T polugrupa. Element $e \in T$ takav da za sve $t \in T$ vrijedi $et = te = t$ nazivamo *neutralni element*. Polugrupa koja sadrži neutralni element zove se *monoid*.

Trivijalno je provjeriti da je neutralni element u monoidu jedinstven. Neka je T monoid s neutralnim elementom e i neka je $t \in T$. *Red elementa* t je najmanji prirodni broj k za koji vrijedi $t^k = e$, ako takav postoji. Inače kažemo da je element t *beskonačnog reda*.

Sljedeća konstrukcija pokazuje da svaku polugrupu S trivijalno možemo proširiti do monoida (usporedi definiciju 1.12). Ako je S monoid, tada stavljamo $S^\bullet := S$. Inače uzmemo $e \notin S$ i definiramo $S^\bullet := S \cup \{ e \}$. Na ovom skupu definiramo operaciju $*$, koja proširuje množenje iz S, tako da za sve $s, s' \in S^\bullet$ vrijedi:

$$s * s' = \begin{cases} ss' & \text{ako } s, s' \in S; \\ s' & \text{ako } s = e; \\ s & \text{ako } s' = e. \end{cases}$$

Primjer 1.17. Opišimo polugrupu s kojom ćemo najčešće baratati u nastavku. Prisjetimo se skupa Σ^+ svih riječi nad konačnom abecedom Σ. Neka su $u = \sigma_1 \sigma_2 \cdots \sigma_k$

i $v = \tau_1\tau_2\cdots\tau_\ell$ dvije riječi. Definiramo operaciju *konkatenacije* riječi na skupu Σ^+, u oznaci $\circ$, pravilom $u \circ v = \sigma_1\sigma_2\cdots\sigma_k\tau_1\tau_2\cdots\tau_\ell$.

Vidimo da je $(\Sigma^+, \circ)$ polugrupa. Dodamo li skupu Σ^+ *praznu riječ* ε, koja je neutralni element u odnosu na konkatenaciju riječi, dobijemo monoid $\Sigma^* := \Sigma^+ \cup \{\,\varepsilon\,\}$. Skup Σ smatramo podskupom od Σ^+, dakle i od Σ^*, kao skup svih riječi duljine 1.

Istražujemo dalje svojstva polugrupa. Važni algebarski koncepti su produktna struktura te podstruktura zatvorena s obzirom na operaciju.

Definicija 1.18. Neka su S i T polugrupe. Skup $S \times T$ čini polugrupu uz množenje definirano tako da za sve $(s_1, t_1), (s_2, t_2)$ vrijedi $(s_1, t_1)(s_2, t_2) = (s_1s_2, t_1t_2)$. Ovu polugrupu nazivamo *direktni produkt polugrupa S i T*.

Definicija 1.19. Neka je S polugrupa i T monoid s neutralnim elementom e. Za podskup $U \subseteq S$ kažemo da je *potpolugrupa* od S ako je U zatvoren s obzirom na množenje iz polugrupe S. Slično, za podskup $V \subseteq T$ kažemo da je *podmonoid* od T ako je V potpolugrupa od T s istim neutralnim elementom e.

Lako je pokazati da je presjek proizvoljno mnogo potpolugrupa također potpolugrupa. Neka je S polugrupa i Z proizvoljan podskup od S. Definiramo *potpolugrupu generiranu skupom Z*, u oznaci $\langle Z\rangle$, kao presjek svih potpolugrupa od S koje sadrže skup Z. Ovako definirana potpolugrupa je očito najmanja potpolugrupa od S koja sadrži Z. Analogno se definira i *podmonoid generiran skupom*.

Lema 1.20. *Neka je S polugrupa i Z podskup od S. Tada vrijedi:*

$$\langle Z\rangle = \left\{ \prod_{i=1}^{n} z_i \colon n \in \mathbb{N}_+,\ z_i \in Z \right\}.$$

Dokaz. $\boxed{\subseteq}$ Skup na desnoj strani očito sadrži Z. Također je i zatvoren na množenje, pa je potpolugrupa od S.

$\boxed{\supseteq}$ Svaka potpolugrupa od S koja sadrži Z zbog zatvorenosti mora sadržavati i umnožak od proizvoljno (konačno) mnogo njegovih članova. □

Preslikavanja među algebarskim strukturama koja se dobro ponašaju u odnosu na operaciju su temelj za mnoge važne algebarske tehnike.

Definicija 1.21. Neka su S i T polugrupe. Kažemo da je funkcija $\varphi\colon S \to T$ *homomorfizam* polugrupa S i T ako za sve $x, y \in S$ vrijedi $\varphi(xy) = \varphi(x)\varphi(y)$. Injektivni homomorfizam nazivamo *monomorfizam*, surjektivni *epimorfizam*, a injektivni i surjektivni *izomorfizam*. Homomorfizam $f : S \to S$ naziva se *endomorfizam* polugrupe S.

Primjer 1.22. Susretat ćemo se s dvije vrste polugrupa čiji elementi su preslikavanja na nekoj polaznoj polugrupi. Neka je S polugrupa i X skup.

- Skup S^X svih funkcija sa skupa X u polugrupu S je polugrupa zajedno sa standardnim točkovnim množenjem funkcija.
- Skup $\mathrm{End}(S)$ svih endomorfizama od S zajedno s kompozicijom funkcija je monoid, s identitetom kao neutralnim elementom.

Polugrupa Σ^+ iz primjera 1.17 se često u teoriji kategorija naziva *slobodna polugrupa nad skupom* Σ. Iako se nećemo baviti ovim područjem, posudit ćemo nazivlje te ćemo koristiti važni rezultat sljedeće propozicije (algebarski uvod u teoriju kategorija može se pronaći u udžbeniku [9]). Sa $\imath\colon \Sigma \to \Sigma^+$ smo označili ulaganje skupa Σ u nadskup Σ^+.

Propozicija 1.23. *Neka je Σ konačan skup. Neka je T polugrupa i $f\colon \Sigma \to T$ preslikavanje. Tada postoji jedinstveni homomorfizam polugrupa $f^+\colon \Sigma^+ \to T$ takav da vrijedi $f^+\imath = f$, tj. za koji sljedeći dijagram komutira:*

$$\begin{array}{ccc} \Sigma & \xrightarrow{\ f\ } & T \\ & {\scriptstyle\imath}\searrow \quad \nearrow{\scriptstyle f^+} & \\ & \Sigma^+ & \end{array} \quad .$$

Dokaz. Definiramo preslikavanje $f^+\colon \Sigma^+ \to T$ tako da za sve $w = \sigma_1\sigma_2\ldots\sigma_k \in \Sigma^+$ vrijedi:

$$f^+(w) = f(\sigma_1) \cdot_T f(\sigma_2) \cdot_T \cdots \cdot_T f(\sigma_k).$$

Očito vrijedi tražena jednakost $f^+\imath = f$. Trivijalno se provjeri da je f^+ homomorfizam polugrupa.

Pretpostavimo da je $g\colon \Sigma^+ \to T$ homomorfizam takav da vrijedi $g\imath = f$. Neka je $w = \sigma_1\sigma_2\ldots\sigma_k \in \Sigma^+$ proizvoljna riječ. Kako je g homomorfizam, mora vrijediti:

$$g(w) = g(\sigma_1) \cdot_T g(\sigma_2) \cdot_T \cdots \cdot_T g(\sigma_k).$$

No, kako su svi $\sigma_i \in \Sigma$, vrijedi $g(\sigma_i) = g\imath(\sigma_i)$, što je po pretpostavci jednako $f(\sigma_i)$. Konačno dobijemo:

$$g(w) = g(\sigma_1) \cdot_T g(\sigma_2) \cdot_T \cdots \cdot_T g(\sigma_k) = f(\sigma_1) \cdot_T f(\sigma_2) \cdot_T \cdots \cdot_T f(\sigma_k) = f^+(w).$$

Jer je $w \in \Sigma^+$ proizvoljno odabran, zaključujemo $g = f^+$. □

U odjeljku 1.1 ustvrdili smo da relacije uvode odnose među elementima jednog ili više skupova. Posebno smo istaknuli relacije ekvivalencije, jer one vežu elemente istog skupa koji dijele određeno zajedničko svojstvo. Kod polugrupa postoji i jači oblik povezanosti elemenata.

Definicija 1.24. Neka je S polugrupa. Relacija ekvivalencije $\sim$ na S naziva se *kongruencijom* ako za sve $x, y \in S$ vrijedi:

$$x \sim y \implies (\forall s \in S)\ xs \sim ys \wedge sx \sim sy. \tag{2}$$

Primjer 1.25. Vezano za prethodnu definiciju, postavljaju se dva pitanja: povlači li desna strana implikacije (2) lijevu te postoji li uopće relacija ekvivalencije na polugrupi koja nije kongruencija. U slučaju da je polugrupa zapravo monoid, odgovor na prvo pitanje je trivijalno potvrdan.

Neka je alfabet $\Sigma = \{\, \mathtt{0} \,\}$. Neka je R relacija na polugrupi Σ^+ takva da za sve $u, v \in \Sigma^+$ vrijedi:

$$u\ R\ v \iff (|u| \leq 2 \text{ i } |v| \leq 2) \text{ ili } (|u| > 2 \text{ i } |v| > 2).$$

Relacija R je relacija ekvivalencije, ali nije kongruencija, jer vrijedi $\mathtt{0}\ R\ \mathtt{00}$, no $\mathtt{00} \not R\, \mathtt{000}$. Također, desna strana implikacije ne povlači lijevu, kako se vidi na primjeru riječi $\mathtt{00}$ i $\mathtt{000}$, koje same nisu u relaciji, no pomnožene s bilo kojim elementom iz Σ^+ jesu.

Neka je $\sim$ kongruencija na polugrupi S. Kvocijentni skup $S/\!\sim$ (vidi raspravu nakon definicije 1.3) također čini polugrupu, uz množenje naslijeđeno iz S:

$$[s] \cdot [t] = [st] \text{ za sve } s, t \in S.$$

Provjerimo da je ova operacija dobro definirana. Za s', $t' \in S$ takve da $[s] = [s']$ i $[t] = [t']$ imamo $s \sim s'$ i $t \sim t'$. No kako je $\sim$ kongruencija, slijedi $st \sim s't$ i $s't \sim s't'$. Budući da je $\sim$ relacija ekvivalencije, posebno je tranzitivna. Zajedno s prethodnim izrazima ovo daje $st \sim s't'$, tj. $[st] = [s't']$. Ovo upravo znači $[s] \cdot [t] = [s'] \cdot [t']$.

Polugrupu $S/\!\sim$ nazivamo *kvocijentna polugrupa*. Kanonska surjekcija $\varphi_\sim \colon S \to S/\!\sim$ je u ovom kontekstu epimorfizam polugrupa koji nazivamo *kanonski epimorfizam*. Sljedeća propozicija otkriva usku povezanost između homomorfizama i kongruencija polugrupa.

Propozicija 1.26. *Neka je S polugrupa i $\sim$ relacija na S. Relacija $\sim$ je kongruencija na S ako i samo ako postoji polugrupa T i homomorfizam polugrupa $f \colon S \to T$ takav da za sve $x, y \in S$ vrijedi*

$$x \sim y \iff f(x) = f(y). \tag{3}$$

Dokaz. $\boxed{\Rightarrow}$ Neka je $\sim$ kongruencija na S i neka je $\varphi_\sim$ kanonski epimorfizam. Provjerimo da $\varphi_\sim$ zadovoljava uvjet (3). Neka su x, $y \in S$ takvi da $x \sim y$. To je ekvivalentno s $[x]_\sim = [y]_\sim$, što upravo znači $\varphi_\sim(x) = \varphi_\sim(y)$.

$\boxed{\Leftarrow}$ Neka su T polugrupa i $f\colon S \to T$ homomorfizam takvi da je ispunjen uvjet (3). Trivijalno se vidi da je $\sim$ relacija ekvivalencije. Neka su $x, y \in S$ takvi da $x \sim y$. Za proizvoljni $s \in S$, koristeći činjenicu da je f homomorfizam, dobivamo:

$$\begin{aligned} x \sim y &\implies f(x) = f(y) \implies f(s)f(x) = f(s)f(y) \\ &\implies f(sx) = f(sy) \implies sx \sim sy. \end{aligned}$$

Analogno $x \sim y$ povlači $xs \sim ys$. Zaključujemo da je $\sim$ kongruencija na S. □

Definicija 1.27. Kongruencija $\sim$ iz propozicije 1.26 jednoznačno je definirana homomorfizmom f. Nazivamo je *kongruencija pridružena homomorfizmu* f.

Nastavimo raspravu o homomorfizmima i kongruencijama. U teoriji grupa važno mjesto zauzima prvi teorem o izomorfizmu. Kod polugrupa ulogu kvocijentnih grupa preuzimaju kvocijentne polugrupe.

Teorem 1.28 (Prvi teorem o izomorfizmu za polugrupe)**.** *Neka su S i T polugrupe, $f\colon S \to T$ epimorfizam polugrupa te neka je $\sim$ kongruencija na S pridružena homomorfizmu f. Tada su polugrupe $S/\!\sim$ i T izomorfne.*

Dokaz. Pokažimo da je preslikavanje $f^\sim\colon S/\!\sim \to T$ takvo da za svaki $s \in S$ vrijedi $f^\sim([s]) = f(s)$ izomorfizam polugrupa. Ova funkcija je dobro definirana, jer je kongruencija $\sim$ pridružena homomorfizmu f.

Kako je f surjekcija, za svaki $t \in T$ postoji $s \in S$ takav da je $f(s) = t$. No tada je i $f^\sim([s]) = t$, pa zaključujemo da je $f^\sim$ također surjekcija.

Za injektivnost, uzmimo $[s]$, $[s'] \in S/\!\sim$ takve da $f^\sim([s]) = f^\sim([s'])$. Iz toga imamo $f(s) = f(s')$, što po definiciji kongruencije $\sim$ znači $s \sim s'$, dakle upravo $[s] = [s']$.

Ostaje pokazati da je $f^\sim$ homomorfizam. Budući da je f homomorfizam, za proizvoljne $[x], [y] \in S/\!\sim$ dobijemo:

$$f^\sim([x] \cdot [y]) = f^\sim([xy]) = f(xy) = f(x)f(y) = f^\sim([x])f^\sim([y]).$$ □

Na kraju odjeljka, istaknimo neke koncepte iz teorije grupa s kojima ćemo se susretati. Pretpostavljamo da je čitatelj već upoznat s njenim osnovama, koje se mogu primjerice pronaći u [25] ili podrobnije u [9]. Za grupu G kažemo da je *prosta* grupa ako je $|G| > 1$ i jedine normalne podgrupe od G su $\{\, e \,\}$ i G.

Neka je G_0, G_1, …, G_n, za $n \in \mathbb{N}_+$, niz podgrupa od G takav da vrijedi

$$G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{\, e \,\}. \tag{4}$$

Ovaj niz naziva se *kompozicijski slijed* od G ako za svaki $i = 0, 1, \ldots, n-1$ vrijedi:

(*i*) G_i je normalna podgrupa od G_{i+1},

(*ii*) G_{i+1}/G_i je prosta grupa.

Za konačnu grupu lagano je ustanoviti da kompozicijski slijed uvijek postoji. Sljedeći poznati teorem pokazuje da je taj slijed zapravo jedinstven. Interesantni i kratki dokaz iz [2] izlazi izvan okvira ovoga rada.

Teorem 1.29 (Jordan-Hölderov teorem)**.** *Neka je G konačna grupa. Neka su*

$$G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{ e \},$$
$$G = K_m \supset K_{m-1} \supset \cdots \supset K_1 \supset K_0 = \{ e \}$$

dva kompozicijska slijeda od G. Tada vrijedi $m = n$ i za svaki $j \in \{ 0, 1, \ldots, m-1 \}$ postoji jedinstveni $i \in \{ 0, 1, \ldots, n-1 \}$ tako da vrijedi $K_{j+1}/K_j \approx G_{i+1}/G_i$, i obratno.

1.4 Polugrupa konačnog automata

Prethodni odjeljci uvodnog su karaktera i opisuju matematičke strukture našeg izučavanja. Na prvi je pogled teško uvidjeti povezanost između konačnih automata i polugrupa. Sličnost uočavamo pri usporedbi procesa izračunavanja automata, odnosno uzastopnog množenja elemenata polugrupe. U oba slučaja, uzastopni rezultati (stanja automata, odnosno elementi polugrupe) uvijek pripadaju početnom skupu. Štoviše, oba procesa imaju deterministično Markovljevo svojstvo neovisnosti o prošlosti, tj. ovise samo o trenutnom rezultatu i sljedećem ulazu, odnosno faktoru. Opišimo detaljnije ovu korespondenciju.

Pri kraju odjeljka 1.2, opisali smo transformaciju konačnog automata $\mathcal{M} = (Q, \Sigma, F)$ u pridruženi LTS $(Q, \{ F_\sigma \colon \sigma \in \Sigma \})$. Za svaki $\sigma \in \Sigma$, parcijalna funkcija F_σ opisuje promjenu stanja automata $\mathcal{M}$ prilikom čitanja znaka σ. Nakon što doista pročita znak σ, automat $\mathcal{M}$ nalazi se u novom stanju i spreman je za čitanje sljedećeg znaka. Proces se dakle ponavlja. Stoga prethodnu konstrukciju proširujemo i na svaku riječ nad alfabetom Σ (jer su to upravo konačni nizovi znakova). To postižemo koristeći kompoziciju spomenutih parcijalnih funkcija, slično kao u dokazu propozicije 1.23.

Neka je $w = \sigma_1 \sigma_2 \cdots \sigma_k \in \Sigma^+$ proizvoljna riječ. Definiramo parcijalnu funkciju $F_w \colon Q \rightharpoonup Q$ tako da za sve $q \in Q$ vrijedi:

$$F_w(q) = F_{\sigma_k}(F_{\sigma_{k-1}}(\cdots(F_{\sigma_1}(q))\cdots)). \tag{5}$$

U nastavku koristimo notaciju $qF_\sigma := F_\sigma(q)$. Nadalje, pišemo $qF_w := qF_{\sigma_1}F_{\sigma_2}\cdots F_{\sigma_k}$ (što otkriva motivaciju za ovu vrstu zapisa).

Skup parcijalnih funkcija $\{ F_w \in \mathbf{PF}(Q) : w \in \Sigma^+ \}$ potpuno opisuje konačni automat $\mathcal{M}$. Ova preslikavanja stoga prirodno definiraju relaciju ekvivalencije $\equiv$ na skupu Σ^+, kako slijedi. Neka za $u, v \in \Sigma^+$ vrijedi:

$$u \equiv v \iff F_u = F_v. \tag{6}$$

Pokažimo da je $\equiv$ kongruencija na polugrupi Σ^+. Neka su u, $v \in \Sigma^+$ takvi da vrijedi $u \equiv v$. To znači da vrijedi $F_u = F_v$, pa za proizvoljni $q \in Q$ i sve $w \in \Sigma^+$ dobijemo:

$$qF_{wu} = qF_wF_u = qF_wF_v = qF_{wv}.$$

Ovo povlači $F_{wu} = F_{wv}$, dakle vrijedi $wu \equiv wv$. Analogno se pokaže i $uw \equiv vw$.

Definicija 1.30 (Polugrupa konačnog automata)**.** Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Neka je $\equiv$ kongruencija na skupu Σ^+ definirana izrazom (6). Ovu kongruenciju nazivamo *kongruencija automata* $\mathcal{M}$ te je označavamo i s $\equiv_{\mathcal{M}}$, ako želimo naglasiti automat. Kvocijentnu polugrupu $\Sigma^+/\equiv_{\mathcal{M}}$ označavamo sa $\mathbf{S}(\mathcal{M})$ i zovemo je *polugrupa konačnog automata* $\mathcal{M}$.

Primjer 1.31. Ponovno razmaramo primjer 1.10.

(*i*) Polugrupa konačnog automata sa slike 1.3b je $\{[\mathtt{a}]\}$.

(*ii*) Polugrupa konačnog automata sa slike 1.4b je $\{ [\mathtt{a}] \}$. Automatu sa slike 1.4c pridružena je polugrupa $\{ [\mathtt{a}], [\mathtt{b}], [\mathtt{c}] \}$, čije množenje je zadano tablicom 1.1a.

(*iii*) Za proizvoljni $n \in \mathbb{N}$, skup $\{ 0, 1, \ldots, n-1 \}$ čini grupu uz operaciju zbrajanja modulo n i u ovom kontekstu je uobičajeno koristiti oznaku $\mathbb{Z}_n$. Polugrupa pridružena konačnom automatu za zbrajanje modulo N iz dijela (*iii*) primjera 1.10 je izomorfna upravo polugrupi $\mathbb{Z}_N$.

$\cdot$	[a]	[b]	[c]
[a]	[a]	[b]	[c]
[b]	[b]	[b]	[c]
[c]	[c]	[b]	[c]

(a)

$\cdot$	[a]	[b]	[ab]	[ba]
[a]	[a]	[ab]	[ab]	[a]
[b]	[ba]	[b]	[b]	[ba]
[ab]	[a]	[ab]	[ab]	[a]
[ba]	[ba]	[b]	[b]	[ba]

(b)

Tablica 1.1: Tablice množenja za polugrupe automata sa slika 1.4c i 1.6

(*iv*) Promatrajmo konačni automat u osnovi determinističkog automata sa slike 1.6. Direktnim računom dobijemo da je njegova polugrupa $\{\,[\mathtt{a}], [\mathtt{b}], [\mathtt{ab}], [\mathtt{ba}]\,\}$ zadana tablicom množenja 1.1b.

Naglašavamo da se polugrupa $\mathbf{S}(\mathcal{M})$ automata $\mathcal{M} = (Q, \Sigma, F)$ sastoji od klasa ekvivalencije $s = [w] \in \Sigma^+/\equiv$, gdje podrazumijevamo $w \in \Sigma^+$. Možda nije odmah jasno da je ova polugrupa uvijek konačna, no to će slijediti iz nadolazeće rasprave. Naime, do iste polugrupe možemo doći i drugim putem. Definiramo preslikavanje $\mathbf{F}\colon \Sigma \to \mathbf{PF}(Q)$ pravilom $\mathbf{F}(\sigma) = F_\sigma$. Označimo njegovu sliku s

$$\mathbf{F}(\mathcal{M}) := \mathbf{F}(\Sigma) = \{\, F_\sigma \in \mathbf{PF}(Q) : \sigma \in \Sigma \,\} \subseteq \mathbf{PF}(Q)\,.$$

Propozicija 1.32. *Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Tada su $\mathbf{S}(\mathcal{M})$ i $\langle \mathbf{F}(\mathcal{M}) \rangle$ izomorfne polugrupe.*

Dokaz. Primjenimo propoziciju 1.23 na funkciju $\mathbf{F}$. Time dobijemo homomorfizam polugrupa $\mathbf{F}^+\colon \Sigma^+ \to \mathbf{PF}(Q)$ takav da za sve $\sigma \in \Sigma$ vrijedi $\mathbf{F}^+(\sigma) = \mathbf{F}(\sigma) = F_\sigma$. Zbog jednakosti (5), za sve $w \in \Sigma^+$ vrijedi $\mathbf{F}^+(w) = F_w$. Sada iz uvjeta (6) slijedi da je kongruencija pridružena homomorfizmu $\mathbf{F}^+$ upravo kongruencija automata $\mathcal{M}$.

Iz leme 1.20 i jednakosti (5) dobijemo da je $\langle \mathbf{F}(\mathcal{M}) \rangle = \{\, F_w \in \mathbf{PF}(Q) : w \in \Sigma^+ \,\}$. No, ovo je upravo slika homomorfizma $\mathbf{F}^+$. Tvrdnja sada slijedi iz teorema 1.28. □

Primjer 1.33. U primjeru 1.31 ustanovili smo da je polugrupa $\{\,[\mathtt{a}], [\mathtt{b}], [\mathtt{c}]\,\}$ automata sa slike 1.4c zadana tablicom množenja 1.1a. Odgovarajući skup parcijalnih funkcija $\{\, F_\mathtt{a}, F_\mathtt{b}, F_\mathtt{c} \,\}$ zajedno s operacijom kompozicije funkcija čini polugrupu zadanu identičnom tablicom množenja. Slično, polugrupa $\{\,[\mathtt{a}], [\mathtt{b}], [\mathtt{ab}], [\mathtt{ba}]\,\}$ automata sa slike 1.6 izomorfna je polugrupi $\{\, F_\mathtt{a}, F_\mathtt{b}, F_\mathtt{ab}, F_\mathtt{ba} \,\} \subseteq \mathbf{PF}(Q)$.

Prethodna propozicija direktno pokazuje da je polugrupa $\mathbf{S}(\mathcal{M})$ uvijek konačna, jer je $\langle \mathbf{F}(\mathcal{M}) \rangle$ potpolugrupa konačne polugrupe $\mathbf{PF}(Q)$. Također, elemente polugrupe $\mathbf{S}(\mathcal{M})$ sada možemo smatrati preslikavanjima koja „djeluju" na skup Q. U idućem odjeljku formaliziramo koncept djelovanja polugrupe na skup.

1.5 Transformacijske polugrupe

Definicija 1.34. Neka je X konačan skup i neka je S konačna polugrupa. Neka je $\cdot\colon X \times S \rightharpoonup X$ parcijalna funkcija na X takva da za sve $s, t \in S$ vrijede svojstva:

(*i*) *Kvaziasocijativnost*: $(\forall x \in X)\ (x \cdot s) \cdot t = x \cdot (st)$;

(*ii*) *Dosljednost*: $((\forall x \in X)\ x \cdot s = x \cdot t) \implies s = t$.

Parcijalnu funkciju $\cdot$ nazivamo *djelovanje* polugrupe S na skup X, a trojku $\mathcal{S} = (X, S, \cdot)$ *transformacijska polugrupa*. Ukoliko je djelovanje jasno iz konteksta, onda za $x \in X$ i $s \in S$ pišemo xs umjesto $x \cdot s$ te (X, S) umjesto $(X, S, \cdot)$. Ako pak želimo naglasiti transformacijsku polugrupu iz koje dolazi djelovanje, pišemo $\cdot_S$. U slučaju da je S monoid s neutralnim elementom e, govorimo o *transformacijskom monoidu*, uz uvjet $x \cdot e = x$, za sve $x \in X$. Analogno definiramo i *transformacijsku grupu*.

Napomena. Transformacijske polugrupe mogu se definirati za proizvoljni skup i polugrupu, bez uvjeta konačnosti. No, u Krohn-Rhodesovoj teoriji razmatraju se isključivo konačne transformacijske polugrupe (usporedi konačnost polugrupe konačnog automata i definiciju 1.36). Stoga smo se odlučili za ovakvu definiciju.

Neka je $\mathcal{S} = (X, S)$ transformacijska polugrupa. Elemente konačne polugrupe S možemo ekvivalentno promatrati kao parcijalne funkcije na skupu X. Doista, za $s \in S$ definiramo funkciju $\mathbf{s} \in \mathbf{PF}(X)$ tako da za sve $x \in X$ vrijedi $\mathbf{s}(x) = x \cdot s$. Interpretirajmo zahtjeve dosljednosti i kvaziasocijativnosti djelovanja iz ove perspektive.

Neka su $s, t \in S$ prozivoljni. Promotrimo kompoziciju funkcija $\mathbf{s}$ i $\mathbf{t}$ (vidi primjer 1.15). Neka je $x \in X$ proizvoljan. Tada vrijedi:

$$(x \cdot s) \cdot t = (\mathbf{s}(x)) \cdot t = \mathbf{t}(\mathbf{s}(x)) = (\mathbf{t} \circ \mathbf{s})(x) = (\mathbf{st})(x).$$

Dakle, kvaziasocijativnost odgovara funkcijskoj kompoziciji.

Neka sada za sve $x \in X$ vrijedi $s \cdot s = x \cdot t$. To znači da za sve $x \in X$ imamo $\mathbf{s}(x) = \mathbf{t}(x)$. No, to povlači $\mathbf{s} = \mathbf{t}$. Vidimo dakle da zahtjev dosljednosti odgovara uvjetu jednakosti funkcija.

Zbog ove interpretacije ćemo u daljnjem, počevši već s idućom definicijom, kod transformacijske polugrupe $\mathcal{S} = (X, S)$ poistovjetiti polugrupu S sa potpolugrupom od $\mathbf{PF}(X)$ [1].

[1] Ne direknto povezano, ali zanimljivo za istaknuti, jest činjenica da je svaka polugrupa S izomorfna nekoj potpolugrupi od $\mathbf{PF}(S^\bullet)$ (vidi [6]). Ovo pokazuje da je teorija konačnih polugrupa tek dio teorije transformacijskih polugrupa.

Definicija 1.35. Neka je $\mathcal{S} = (X, S)$ transformacijska polugrupa. Za $x \in X$, neka je $\overline{x}\colon X \to X$ konstantna funkcija na skupu X s vrijednošću x. Skup $\overline{X} = \{\, \overline{x}\colon x \in X \,\}$ je očigledno potpolugrupa od $\mathbf{PF}(X)$. Trasformacijsku polugrupu $\overline{\mathcal{S}} = (X, \langle S \cup \overline{X} \rangle)$ nazivamo *zatvorenje* transformacijske polugrupe $\mathcal{S}$. Nadalje, s $\mathcal{S}^\bullet$ označavamo transformacijski monoid $(X, S^\bullet)$ ili ekvivalentno $(X, S \cup \{\, I_X \,\})$ (usporedi definiciju 1.12).

Vraćamo se u računarski kontekst, kako bismo povezali konačne automate i upravo definirane transformacijske polugrupe. To će nam biti i glavni izvor primjera transformacijskih polugrupa.

Definicija 1.36 (Transformacijska polugrupa konačnog automata)**.** Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Djelovanje $\cdot_{\mathcal{M}}\colon Q \times \mathbf{S}(\mathcal{M}) \rightharpoonup Q$ njegove polugrupe $\mathbf{S}(\mathcal{M})$ na skup stanja Q definiramo tako da za sve $q \in Q$ i $s = [w] \in \mathbf{S}(\mathcal{M})$ vrijedi

$$q \cdot_{\mathcal{M}} s = qF_w. \tag{7}$$

Transformacijsku polugrupu $(Q, \mathbf{S}(\mathcal{M}), \cdot_{\mathcal{M}})$ zovemo *transformacijska polugrupa konačnog automata* $\mathcal{M}$ i označavamo sa $\mathbf{TS}(\mathcal{M})$.

Uvjerimo se da je prethodna definicija dobra, tj. da su ispunjena svojstva kvaziasocijativnosti i dosljednosti djelovanja. Neka su $s = [u], t = [v] \in \mathbf{S}(\mathcal{M})$ proizvoljni. Tada je $s \cdot t = [uv]$, pa za bilo koji $q \in Q$ vrijedi:

$$(q \cdot_{\mathcal{M}} s) \cdot_{\mathcal{M}} t = (qF_u) \cdot_{\mathcal{M}} t = qF_uF_v = qF_{uv} = q \cdot_{\mathcal{M}} (s \cdot t).$$

Pretpostavimo sada da za sve $q \in Q$ vrijedi $q \cdot_{\mathcal{M}} s = q \cdot_{\mathcal{M}} t$. Ovo znači $qF_u = qF_v$ za sve $q \in Q$, pa zaključujemo $F_u = F_v$. Slijedi $u \equiv v$, što konačno povlači $s = t$.

Primjer 1.37. Neka je $n \in \mathbb{N}_+$. Definiramo trivijalnu transformacijsku polugrupu $\mathbf{n} = (\mathbb{Z}_n, \emptyset)$. Nadalje, transformacijsku grupu $(\mathbb{Z}_n, \mathbb{Z}_n)$, u kojoj je djelovanje zadano prirodno kao modularno zbrajanje, ćemo također označavati sa $\mathbb{Z}_n$. Odredimo transformacijske polugrupe konačnih automata iz primjera 1.10.

(i) Automotu sa slike 1.3a pridružena je transformacijska polugrupa $(\{\, 0 \,\}, \emptyset)$, dakle upravo $\mathbf{1}$. Automatu sa slike 1.3b pridružena je transformacijska grupa $\mathbf{1}^\bullet = (\{\, 0 \,\}, \{\, [a] \,\})$ (kasnije ćemo pokazati da je ona ekvivalentna s $\mathbb{Z}_1$).

(ii) Transformacijska polugrupa pridružena konačnom automatu

- sa slike 1.4a je $\mathbf{2}$;
- sa slike 1.4b je $\mathbf{2}^\bullet$;
- sa slike 1.4c je $\overline{\mathbf{2}}^\bullet$.

(*iii*) Automatu za zbrajanje modulo N iz dijela (*iii*) primjera 1.10 pridružena je transformacijska grupa $\mathbb{Z}_N$.

(*iv*) Konačnom automatu sa slike 1.6 pridružena je transformacijska polugrupa $(\{\, q_0, q_1, q_2, q_3 \,\}, \{\, [\mathtt{a}], [\mathtt{b}], [\mathtt{ab}], [\mathtt{ba}] \,\})$. Identifikacijom elemenata polugrupe s parcijalnim funkcijama, ova transformacijska polugrupa ekvivalentna je transformacijskoj polugrupi $(\{\, q_0, q_1, q_2, q_3 \,\}, \{\, F_{\mathtt{a}}, F_{\mathtt{b}}, F_{\mathtt{ab}}, F_{\mathtt{ba}} \,\})$.

Obratno, svakoj transformacijskoj polugrupi možemo pridružiti konačni automat. Kasnije ćemo precizirati u kojem su odnosu ovi pridruženi objekti.

Definicija 1.38. Neka je $\mathcal{S} = (X, S, \cdot)$ transformacijska polugrupa. Definiramo parcijalnu funkciju prijelaza $F\colon X \times S \rightharpoonup X$ pomoću djelovanja $\cdot$ tako da za sve $x \in X$ i $s \in S$ vrijedi:

$$F(x, s) = x \cdot s.$$

Konačni automat (X, S, F) zovemo *konačni automat transformacijske polugrupe* $\mathcal{S}$ i označavamo sa $\mathbf{SM}(\mathcal{S})$ (od engleskog naziva *state machine*).

Primjer 1.39. Konačni automat $\mathcal{M}$ sa slike 1.4c pridružen je transformacijskoj polugrupi $\overline{\mathbf{2}}^{\bullet}$, tj. vrijedi $\mathcal{M} = \mathbf{SM}(\overline{\mathbf{2}}^{\bullet})$. Također, transformacijskoj grupi $\mathbb{Z}_N$, za $N \in \mathbb{N}_+$, pridružen je upravo konačni automat za zbrajanje modulo N iz dijela (*iii*) primjera 1.10.

Kod konačnog automata $\mathbf{SM}(\mathcal{S}) = (X, S, F)$ transformacijske polugrupe $\mathcal{S}$, elemente konačne polugrupe S smatramo znakovima alfabeta. Očekujemo da je operacija konkatenacije na skupu S^+ povezana s množenjem iz polugrupe S. Zaista, iz perspektive automata $\mathbf{SM}(\mathcal{S})$ postoji bliska veza među ovim operacijama. Čitanjem riječi $w = s_1 s_2 \cdots s_k \in S^+$, iz stanja $x \in X$ ovaj automat prelazi u stanje

$$xF_{s_1 s_2 \cdots s_k} = xF_{s_1} F_{s_2} \cdots F_{s_k} = (((x \cdot s_1) \cdot_S s_2) \cdots) \cdot_S s_k.$$

No, zbog kvaziasocijativnosti djelovanja transformacijske polugrupe $\mathcal{S}$, ovo je upravo stanje $x \cdot_S (s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k) = xF_{s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k}$. Dakle, točno ono u koje automat prelazi čitanjem znaka $s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k \in S$. Uvodimo oznaku $\langle w \rangle = s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k$. Primjetimo da smo upravo dokazali jednakost $xF_w = x \cdot_S \langle w \rangle$.

Poglavlje 2

Dualna teorija

Glavni predmet izučavanja ovog rada su dvije matematičke strukture definirane u prethodnom poglavlju: konačni automati i transformacijske polugrupe. Iako pripadaju različitim granama matematike (teorijskom računarstvu, odnosno algebri), u odjeljku 1.5 uvjerili smo se u njihovu dualnost. U ovom poglavlju prikazujemo paralelni razvoj tehnika kojima analiziramo ove strukture i njihov međusobni odnos. Nastavljamo pratiti izvor [8].

2.1 Homomorfizmi

U odjeljku 1.3 istraživali smo preslikavanja između polugrupa koja čuvaju algebarsku strukturu. Uvjerili smo se da ova preslikavanja mogu služiti za usporedbu i čak identifikaciju raznih polugrupa. Vođeni ovim primjerom, proučavat ćemo preslikavanja između konačnih automata, odnosno transformacijskih polugrupa, koja poštuju njihove strukture.

Definicija 2.1 (Homomorfizam konačnih automata)**.** Neka su $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$ konačni automati. Neka su $\alpha\colon Q \to Q'$ i $\beta\colon \Sigma \to \Sigma'$ funkcije takve da za sve $q \in Q$ i $\sigma \in \Sigma$ koji zadovoljavaju uvjet $qF_\sigma \neq \varnothing$ vrijedi:

$$\alpha(qF_\sigma) = (\alpha(q))F'_{\beta(\sigma)}. \tag{1}$$

Uređeni par (α, β) nazivamo *homomorfizam konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ te pišemo $(\alpha, \beta) : \mathcal{M} \to \mathcal{M}'$.

Ako su α i β injekcije (surjekcije), kažemo da je (α, β) *monomorfizam (epimorfizam) konačnih automata. Izomorfizam konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ je homomorfizam transformacijskih polugrupa koji je monomorfizam i epimorfizam. U posljednjem slučaju kažemo da su konačni automati $\mathcal{M}$ i $\mathcal{M}'$ *izomorfni* i pišemo $\mathcal{M} \cong \mathcal{M}'$.

Drugim riječima, ako je (α, β) homomorfizam konačnih automata $\mathcal{M}$ i $\mathcal{M}'$, tada sljedeći dijagram komutira:

$$\begin{array}{ccc} Q \times \Sigma & \xrightarrow{(\alpha,\beta)} & Q' \times \Sigma' \\ \Big\downarrow{\scriptstyle F} & & \Big\downarrow{\scriptstyle F'} \\ Q & \xrightarrow{\quad\alpha\quad} & Q' \end{array} .$$

Primjetimo da lijeva strana dijagrama predstavlja automat $\mathcal{M}$, a desna automat $\mathcal{M}'$.

Preslikavanje $\beta\colon \Sigma \to \Sigma'$ možemo shvatiti kao preslikavanje s kodomenom Σ'^{+}. Proširimo ga do homomorfizma polugrupa $\beta^{+}\colon \Sigma^{+} \to \Sigma'^{+}$, pomoću propozicije 1.23. Pokažimo da jednakost analogna (1) vrijedi i za svaku riječ nad Σ, uz korištenje funkcije β^{+} umjesto β. Za $q \in Q$ i $w = \sigma_1\sigma_2\cdots\sigma_k \in \Sigma^{+}$ takve da je $qF_w \neq \varnothing$ imamo:

$$\begin{aligned} \alpha\left(qF_w\right) &= \alpha\left(qF_{\sigma_1}F_{\sigma_2}\cdots F_{\sigma_k}\right) = \left(\alpha(qF_{\sigma_1}F_{\sigma_2}\cdots F_{\sigma_{k-1}})\right) F'_{\beta(\sigma_k)} \\ &= \cdots = \left(\alpha(q)\right) F'_{\beta(\sigma_1)}\cdots F'_{\beta(\sigma_k)} = \left(\alpha(q)\right) F'_{\beta(\sigma_1)\cdots\beta(\sigma_k)} = \left(\alpha(q)\right) F'_{\beta^{+}(w)}. \end{aligned}$$

Definicija 2.2 (Homomorfizam transformacijskih polugrupa)**.** Neka su $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ i $\mathcal{S}' = (X', S', \cdot_{\mathcal{S}'})$ transformacijske polugrupe. Neka su $\alpha\colon X \to X'$ funkcija i $\beta\colon S \to S'$ homomorfizam polugrupa takvi da za sve $x \in X$ i $s \in S$ za koje je $x \cdot_{\mathcal{S}} s \neq \varnothing$ vrijedi:

$$\alpha\left(x \cdot_{\mathcal{S}} s\right) = \alpha(x) \cdot_{\mathcal{S}'} \beta(s). \tag{2}$$

Uređeni par (α, β) nazivamo *homomorfizam transformacijskih polugrupa* $\mathcal{S}$ i $\mathcal{S}'$ te pišemo $(\alpha, \beta) : \mathcal{S} \to \mathcal{S}'$.

Ako su α i β injekcije (surjekcije), kažemo da je (α, β) *monomorfizam (epimorfizam) transformacijskih polugrupa. Izomorfizam transformacijskih polugrupa* $\mathcal{S}$ i $\mathcal{S}'$ je homomorfizam transformacijskih polugrupa koji je monomorfizam i epimorfizam. U posljednjem slučaju kažemo da su transformacijske polugrupe $\mathcal{S}$ i $\mathcal{S}'$ *izomorfne* te pišemo $\mathcal{S} \cong \mathcal{S}'$.

Homomorfizmi konačnih automata i transformacijskih polugrupa definirani su potpuno analogno. Stoga se lako pokaže da su transformacijske polugrupe pridružene izomorfnim konačnim automatima također izomorfne. Dakle, vrijedi sljedeći rezultat.

Propozicija 2.3. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ izomorfni konačni automati. Tada su i njima pridružene transformacijske polugrupe $\mathbf{TS}\left(\mathcal{M}\right)$ i $\mathbf{TS}\left(\mathcal{M}'\right)$ izomorfne. Dualno, neka su $\mathcal{S}$ i $\mathcal{S}'$ izomorfne transformacijske polugrupe. Tada su i njima pridruženi konačni automati $\mathbf{SM}\left(\mathcal{S}\right)$ i $\mathbf{SM}\left(\mathcal{S}'\right)$ izomorfni.*

Primjer 2.4.

(*i*) Konstruirajmo homomorfizam konačnih automata iz dijela (*ii*) primjera 1.10. Označimo automate sa slika 1.4b i 1.4c redom sa $\mathcal{M} = (\mathbb{Z}_2, \{\mathtt{a}\}, F)$ i $\mathcal{M}' = (\mathbb{Z}_2, \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}, G)$. Neka je $\alpha = I_{\mathbb{Z}_2}$ te β ulaganje skupa $\{\mathtt{a}\}$ u nadskup $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. Lako je provjeriti da je (α, β) monomorfizam konačnih automata $\mathcal{M}$ i $\mathcal{M}'$. Također, monomorfizam pridruženih transformacijskih polugrupa $\mathbf{TS}(\mathcal{M})$ i $\mathbf{TS}(\mathcal{M}')$ je upravo par (α, β^+).

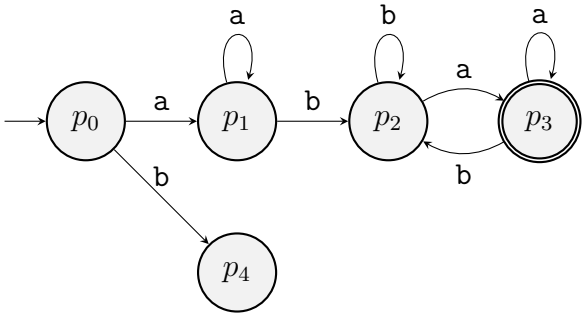
(*ii*) Deterministički automat prikazan na slici 2.1 prepoznaje jezik zadan regularnim izrazom $\mathtt{a}(\mathtt{a} \cup \mathtt{b})^* \mathtt{b}(\mathtt{a} \cup \mathtt{b})^* \mathtt{a}$ (sve riječi nad alfabetom $\{\mathtt{a}, \mathtt{b}\}$ koje započinju i završavaju znakom $\mathtt{a}$ te sadrže barem jedan znak $\mathtt{b}$). Označimo njegov konačni automat s $\mathcal{M}' = (\{p_0, p_1, p_2, p_3, p_4\}, \{\mathtt{a}, \mathtt{b}\}, G)$. Nadalje, označimo s $\mathcal{M} = (\{q_0, q_1, q_2, q_3\}, \{\mathtt{a}, \mathtt{b}\}, F)$ konačni automat sa slike 1.6. Definirajmo preslikavanje $\alpha\colon \{p_0, p_1, p_2, p_3, p_4\} \to \{q_0, q_1, q_2, q_3\}$ tako da vrijedi:

$$\alpha(p_0) = q_0,\ \alpha(p_1) = \alpha(p_3) = q_1,\ \alpha(p_2) = q_2,\ \alpha(p_4) = q_3.$$

Preslikavanje β neka bude identiteta na alfabetu $\{\mathtt{a}, \mathtt{b}\}$. Provjerimo da je (α, β) epimorfizam konačnih automata $\mathcal{M}'$ i $\mathcal{M}$. Primjerice, za stanje p_2 imamo:

$$\alpha(p_2 G_{\mathtt{a}}) = \alpha(p_3) = q_1 = q_2 F_{\mathtt{a}} = \alpha(p_2) F_{\mathtt{a}} \text{ te}$$
$$\alpha(p_2 G_{\mathtt{b}}) = \alpha(p_2) = q_2 = q_2 F_{\mathtt{b}} = \alpha(p_2) F_{\mathtt{b}}.$$

Ostali parovi se provjere analogno.



Slika 2.1: Deterministički automat koji prepoznaje reg. izraz $\mathtt{a}(\mathtt{a} \cup \mathtt{b})^* \mathtt{b}(\mathtt{a} \cup \mathtt{b})^* \mathtt{a}$

Najavili smo da ćemo detaljnije istražiti odnos između operacija **TS** i **SM**.

Propozicija 2.5. *Neka je $\mathcal{S}$ transformacijska polugrupa. Tada vrijedi*

$$\mathbf{TS}(\mathbf{SM}(\mathcal{S})) \cong \mathcal{S}.$$

Dokaz. Neka je $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$. Nazovimo s $\mathcal{M}$ njoj pridruženi automat $\mathbf{SM}(\mathcal{S}) = (X, S, F)$. Sada je $\mathbf{TS}(\mathbf{SM}(\mathcal{S})) = \mathbf{TS}(\mathcal{M}) = (X, \mathbf{S}(\mathcal{M}), \cdot_{\mathcal{M}})$.

Definiramo funkciju $\beta\colon \mathbf{S}(\mathcal{M}) \to S$ tako da za sve $w = s_1 s_2 \cdots s_k \in S^+$ vrijedi:

$$\beta([w]) = s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k.$$

Najprije se uvjerimo da je funkcija β dobro definirana. Neka su $u = s_1 s_2 \cdots s_k, v = t_1 t_2 \cdots t_\ell \in S^+$ takvi da je $[u] = [v]$. Ovo povlači $F_u = F_v$, što znači da za sve $x \in X$ vrijedi $xF_u = xF_v$. Mi trebamo pokazati da vrijedi $s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k = t_1 \cdot_S t_2 \cdot_S \cdots \cdot_S t_k$, to jest, uz oznaku s kraja odjeljka 1.5, $\langle u \rangle = \langle v \rangle$. Koristeći jednakost koja je tamo pokazana, sada dobijemo $x \cdot_S \langle u \rangle = x \cdot_S \langle v \rangle$, za sve $x \in X$. Zbog dosljednosti djelovanja transformacijske polugrupe $\mathcal{S}$, konačno slijedi $\langle u \rangle = \langle v \rangle$.

β je homomorfizam polugrupa, jer za sve $u = s_1 s_2 \cdots s_k, v = t_1 t_2 \cdots t_\ell \in S^+$ imamo:

$$\beta([u][v]) = \beta([uv]) = (s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k) \cdot_S (t_1 \cdot_S t_2 \cdot_S \cdots \cdot_S t_k) = \beta([u]) \cdot_S \beta([v]).$$

Nadalje, β je surjekcija, jer za sve $s \in S$ vrijedi $\beta([s]) = s$. Pokažimo da je i injekcija. Neka su $u = s_1 s_2 \cdots s_k, v = t_1 t_2 \cdots t_\ell \in S^+$ takvi da vrijedi $\beta([u]) = \beta([v])$. Trebamo pokazati da je $[u] = [v]$, odnosno $F_u = F_v$. Neka je $x \in X$ proizvoljan. Računamo:

$$\begin{aligned} xF_u &= xF_{s_1}F_{s_2}\cdots F_{s_k} = (x \cdot_{\mathcal{S}} s_1)F_{s_2}\cdots F_{s_k} = \cdots = (((x \cdot_S s_1) \cdot_S s_2) \cdots) \cdot_S s_k \\ &= x \cdot_{\mathcal{S}} (s_1 \cdot_S s_2 \cdot_S \cdots \cdot_S s_k) = x \cdot_{\mathcal{S}} \beta([u]) = x \cdot_{\mathcal{S}} \beta([v]) = \cdots = xF_v. \end{aligned}$$

Zaključujemo da je β traženi izomorfizam.

Provjerimo još da za par (I_X, β) vrijedi jednakost (2). Neka su $x \in X$ i $w = s_1 s_2 \cdots s_k \in S^+$ takvi da je $x \cdot_{\mathcal{M}} [w] \neq \varnothing$. Računom analognim kao gore dobijemo:

$$I_X(x \cdot_{\mathcal{M}} [w]) = xF_w = I_X(x) \cdot_{\mathcal{S}} \beta([w]). \qquad \square$$

Iz prethodne propozicije slijedi da je **TS** surjektivna operacija, tj. za svaku transformacijsku polugrupu $\mathcal{S}$ postoji konačni automat $\mathcal{M}$ za koji vrijedi $\mathcal{S} \cong \mathbf{TS}(\mathcal{M})$ (uzmimo $\mathcal{M} = \mathbf{SM}(\mathcal{S})$). Analogoni za operaciju **SM** nažalost ne vrijede, dakle niti tvrdnja propozicije niti posljednja opaska o surjektivnosti operacije. Intuitivno objašnjenje je da operacija **S**, figurativno rečeno, „napuše" ulaznu abecedu konačnog automata do pridružene polugrupe (vidi primjerice dio (iv) primjera 1.31). Stoga očekujemo da će svaki konačni automat biti „manji" od onoga pridruženog transformacijskoj polugrupi polaznog automata (vidi lemu 2.16).

2.2 Prekrivači

Kada govorimo o automatima, prvenstveno nas zanima što oni računaju. Proučavanje njihove unutarnje građe korisno je samo u aspektu koji se odražava na njihovu funkcionalnost. Stoga, za razliku od algebarskih teorija u kojima je centralan koncept izomorfizma ili jednake građe, ovdje ćemo raspravljati o jednakosti automata na osnovi onoga što mogu izračunati.

Formalizacija ovog koncepta idejno je slična bisimulacijama okvira (definicija 1.4). U ovom odjeljku proučavamo **simulacije**, važne relacije između konačnih automata. Slijedi intuitivni opis ovog pojma.

Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat te neka je $\mathcal{M}' = (Q', \Sigma', F')$ konačni automat koji može simulirati rad automata $\mathcal{M}$. To znači da izračunavanje automata $\mathcal{M}$ s nekom riječi (vidi definiciju 1.9) možemo odrediti iz izračunavanja automata $\mathcal{M}'$ s odgovarajućom ulaznom riječi. Očito tada prvo moramo znati kako pretvoriti ulaz za automat $\mathcal{M}$ u ulaz za automat $\mathcal{M}'$. Neka je ta pretvorba zadana preslikavanjem $\nu\colon \Sigma \to \Sigma'$.

Nadalje, svakom stanju u $\mathcal{M}$ mora biti pridruženo barem jedno stanje u $\mathcal{M}'$. To ćemo postići pomoću surjektivne parcijalne funkcije $\mu\colon Q' \rightharpoonup Q$. Naime, iz stanja $q' \in Q'$ moramo biti u stanju jednoznačno odrediti odgovarajuće stanje $\mu(q') \in Q$. Također, neka stanja automata $\mathcal{M}'$ mogu biti irelevantna za simulaciju automata $\mathcal{M}$, stoga dopuštamo parcijalnost funkcije μ.

Konačno, treba vrijediti sljedeće. Pokrenimo automat $\mathcal{M}$ s ulazom $w \in \Sigma^+$ iz stanja $q \in Q$. Paralelno pokrenimo automat $\mathcal{M}'$ s ulazom $\nu^+(w)$ iz bilo kojeg stanja $q' \in Q'$ za koje vrijedi $\mu(q') = q$. Rezultirajuće izračunavanje automata $\mathcal{M}$ možemo jednoznačno odrediti pomoću parcijalne funkcije μ iz izračunavanja automata $\mathcal{M}'$. Prelazimo na formalnu definiciju.

Definicija 2.6 (Prekrivač konačnog automata)**.** Neka su $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$ konačni automati. Neka je $\mu\colon Q' \rightharpoonup Q$ surjektivna parcijalna funkcija i $\nu\colon \Sigma \to \Sigma'$ funkcija. Neka za svaki $q' \in Q'$ i svaki $\sigma \in \Sigma$, takve da je $\mu(q')F_\sigma \neq \varnothing$, vrijedi:

$$\mu\left(q'\, F'_{\nu(\sigma)}\right) = \mu(q')F_\sigma. \tag{3}$$

Uređeni par (μ, ν) naziva se *prekrivač automata* $\mathcal{M}$ *automatom* $\mathcal{M}'$. Govorimo i da automat $\mathcal{M}'$ *prekriva* automat $\mathcal{M}$ te pišemo $\mathcal{M} \leq \mathcal{M}'$, ili $\mathcal{M} \leq_{(\mu,\nu)} \mathcal{M}'$ ako želimo naglasiti prekrivač.

Sada možemo i formalno opisati simulaciju izračunavanja automata $\mathcal{M}$ pomoću automata $\mathcal{M}'$. Neka je $w \in \Sigma^+$ ulazna riječ za automat $\mathcal{M}$ koji se nalazi u početnom stanju $q_0 \in Q$. Uzmemo proizvoljni $q'_0 \in Q'$ takav da vrijedi $\mu(q'_0) = q_0$ i odredimo $w' = \nu^+(w)$. Pokrenemo automat $\mathcal{M}'$ iz početnog stanja q'_0 s ulaznom riječi w'.

Neka je niz $q'_0, q'_1, \ldots, q'_k$ dobiveno izračunavanje automata $\mathcal{M}'$. Tada znamo da je rezultirajuće izračunavanje automata $\mathcal{M}$ niz $\mu(q'_0) = q_0, \mu(q'_1), \ldots, \mu(q'_k)$.

Napomena. Prokomentirajmo uvjet $\mu(q')F_\sigma \neq \varnothing$ iz prethodne definicije. Vrijednost $\mu(q')F_\sigma$ može biti nedefinirana u dva slučaja: ako je $\mu(q') = \varnothing$ ili ako je $qF_\sigma = \varnothing$, gdje je $Q \ni q = \mu(q') \neq \varnothing$. U prvom slučaju je stanje $q' \in Q'$ irelevantno za simulaciju, dok je u drugom izračunavanje automata $\mathcal{M}$ prekinuto ulazom σ. Vidimo da se oba slučaja mogu zanemariti pri razmatranju simulacije jednog automata drugim.

Kao u raspravi nakon definicije 2.1, pokaže se da iz jednakosti (3) slijedi da za sve $q' \in Q'$ i $w \in \Sigma^+$ takve da je $\mu(q')F_w \neq \varnothing$ vrijedi analogna jednakost:

$$\mu\left(q' F'_{\nu^+(w)}\right) = \mu(q')F_w. \tag{4}$$

Primjer 2.7. Prisjetimo se automata za modularno zbrajanje iz dijela (*iii*) primjera 1.10. Neka su M i N prirodni brojevi takvi da M dijeli N. Pokažimo da automat $\mathcal{N} = (\mathbb{Z}_N, \mathbb{Z}_N, G)$ za zbrajanje modulo N prekriva automat $\mathcal{M} = (\mathbb{Z}_M, \mathbb{Z}_M, F)$ za zbrajanje modulo M. Za $M = N$ je tvrdnja trivijalno ispunjena, stoga pretpostavimo $N \geq 2M$. Neka je parcijalna funkcija $\mu\colon \mathbb{Z}_N \to \mathbb{Z}_M$ zadana s $\mu(k) = k \bmod M$, za sve $k \in \mathbb{Z}_N$. Neka je funkcija ν ulaganje skupa $\mathbb{Z}_M$ u nadskup $\mathbb{Z}_N$.

Važno je primijetiti da za sve $n \in \mathbb{N}_+$ vrijedi jednakost $n \bmod N \bmod M = n \bmod M$. Doista, neka je $n = n_0 + a \cdot N$, gdje je $n_0 \in \mathbb{Z}_N$ i $a \in \mathbb{N}_+$. Tada je $n \bmod N \bmod M = n_0 \bmod M$. Zbog $N = k \cdot M$, za neki $k \in \mathbb{N}_+$, slijedi i $n \bmod M = n_0 \bmod M$.

Za proizvoljno stanje $k \in \mathbb{Z}_N$ i ulaz $\ell \in \mathbb{Z}_M$ sada imamo:

$$\begin{aligned}
\mu(k\, G_{\nu(\ell)}) &= \mu\left((k + \nu(\ell)) \bmod N\right) = \mu\left((k + \ell) \bmod N\right) \\
&= (k + \ell) \bmod N \bmod M = (k + \ell) \bmod M \\
&= (k \bmod M + \underbrace{\ell}_{<M} \bmod M) \bmod M \\
&= (k \bmod M + \ell) \bmod M = \mu(k)F_\ell.
\end{aligned}$$

Uočavamo da relacija prekrivanja s pravom nosi oznaku $\leq$, jer ima neka svojstva refleksivnog parcijalnog uređaja (vidi [19, definicija 1.61]). Njena refleksivnost je očita. Također se lako može pokazati da iz $\mathcal{M} \leq_{(\mu,\nu)} \mathcal{M}'$ i $\mathcal{M}' \leq_{(\mu',\nu')} \mathcal{M}''$ slijedi $\mathcal{M} \leq_{(\mu\circ\mu',\nu'\circ\nu)} \mathcal{M}''$.

Potaknuti ovim razmatranjima, definiramo pojam **ekvivalentnosti** konačnih automata koji se zasniva na postojanju prekrivača između dva konačna automata. Koncept je analogan već spomenutim relacijama bisimulacije.

Definicija 2.8 (Ekvivalentnost konačnih automata)**.** Neka su $\mathcal{M}$ i $\mathcal{M}$ konačni automati. Kažemo da su $\mathcal{M}$ i $\mathcal{M}'$ *ekvivalentni* ako vrijedi $\mathcal{M} \leq \mathcal{M}'$ i $\mathcal{M}' \leq \mathcal{M}$. U ovom slučaju pišemo $\mathcal{M} \equiv \mathcal{M}'$.

Kao i kod homomorfizama, definicija prekrivača transformacijskih polugrupa je potpuno analogna onoj za konačne automate.

Definicija 2.9 (Prekrivač transformacijske polugrupe)**.** Neka su $\mathcal{S} = (X, S, \cdot_S)$ i $\mathcal{S}' = (X', S', \cdot_{S'})$ transformacijske polugrupe. Neka je $\mu\colon X' \rightharpoonup X$ surjektivna parcijalna funkcija i $\nu\colon S \to S'$ funkcija. Neka za sve $q' \in Q'$ i $s \in S$, takve da je $\mu(q') \cdot_S s \neq \varnothing$, vrijedi

$$\mu(q') \cdot_S s = \mu\left(q' \cdot_{S'} \nu(s)\right). \tag{5}$$

Uređeni par (μ, ν) nazivamo *prekrivač transformacijske polugrupe* $\mathcal{S}$ *transformacijskom polugrupom* $\mathcal{S}'$. Govorimo i da $\mathcal{S}'$ *prekriva* $\mathcal{S}$ te pišemo $\mathcal{S} \leq \mathcal{S}'$.

Istaknimo da u prethodnoj definiciji ne zahtijevamo da preslikavanje ν bude homomorfizam polugrupa S i S' (usporedi definiciju 2.2). Ekvivalentnost transformacijskih polugrupa definira se analogno kao i za konačne automate.

Primjer 2.10. Slično kao u primjeru 2.7, pokažimo da za prirodne brojeve M i N takve da M dijeli N vrijedi da transformacijska grupa $\mathbb{Z}_N$ prekriva transformacijsku polugrupu $\mathbb{Z}_M$. Parcijalna funkcija μ ponovno je zadana s $\mu(k) = k \bmod M$, za sve $k \in \mathbb{Z}_N$, a funkcija ν ostaje isto ulaganje. Potpuno analognim raspisom kao u navedenom primjeru vidimo da vrijedi uvjet (5).

U prethodnom primjeru prekrivač konačnih automata generirao je odgovarajući prekrivač pridruženih transformacijskih polugrupa. Sljedeći općeniti rezultat pokazuje da ovo nije slučajnost.

Propozicija 2.11. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ konačni automati takvi da je $\mathcal{M} \leq \mathcal{M}'$. Tada vrijedi:*

$$\mathbf{TS}\left(\mathcal{M}\right) \leq \mathbf{TS}\left(\mathcal{M}'\right).$$

Dokaz. Neka su $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$. Neka je (μ, ν) prekrivač od $\mathcal{M}$ s $\mathcal{M}'$. Neka je funkcija $f\colon \mathbf{S}\left(\mathcal{M}\right) \to \mathbf{S}\left(\mathcal{M}'\right)$ zadana na sljedeći način. Neka je $s \in \mathbf{S}\left(\mathcal{M}\right)$ proizvoljan. Neka je $w \in \Sigma^+$ neka riječ za koju vrijedi $s = [w]$. Tada definiramo $f(s) = [\nu^+(w)]$. Ovim postupkom možemo dobiti više od jedne funkcije. Fiksirajmo jednu od njih i nazovimo je $\bar{\nu}$.

Neka su sada $q' \in Q'$ i $s \in \mathbf{S}\left(\mathcal{M}\right)$ takvi da je $\mu(q') \cdot_S s \neq \varnothing$. Neka je $w \in \Sigma^+$ takav da vrijedi $s = [w]$ i koji je odabran u konstrukciji funkcije $\bar{\nu}$. Tada vrijedi:

$$\mu\left(q' \cdot_{\mathcal{M}'} \bar{\nu}(s)\right) = \mu(q'\, F'_{\nu^+(w)}) = \mu(q') F_w = \mu(q') \cdot_{\mathcal{M}} s.$$

Zaključujemo da je $(\mu, \bar{\nu})$ prekrivač od $\mathbf{TS}\left(\mathcal{M}\right)$ s $\mathbf{TS}\left(\mathcal{M}'\right)$. □

Analogno se dokaže da je i sljedeća dualna tvrdnja istinita.

Propozicija 2.12. *Neka su $\mathcal{S}$ i $\mathcal{S}'$ transformacijske polugrupe takve da je $\mathcal{S} \leq \mathcal{S}'$. Tada vrijedi:*

$$\mathbf{SM}(\mathcal{S}) \leq \mathbf{SM}(\mathcal{S}').$$

Za kraj odjeljka, odgovaramo na pitanje koje se nameće samo od sebe: koji je odnos između homomorfizama i prekrivanja? Sljedeća lema potvrđuje da je postojanje monomorfizma ili epimorfizma jače svojstvo od postojanja prekrivača. Zaključujemo da su prekrivanja fleksibilniji oblik povezanosti među konačnim automatima (transformacijskim polugrupama), što se pokazuje neophodnim za daljnji razvoj teorije.

Lema 2.13. *Neka su $\mathcal{M}_1 = (Q_1, \Sigma_1, F_1)$, $\mathcal{M}_2 = (Q_2, \Sigma_2, F_2)$ i $\mathcal{M}' = (Q', \Sigma', F')$ konačni automati. Neka su $(\alpha_1, \beta_1) : \mathcal{M}' \to \mathcal{M}_1$ i $(\alpha_2, \beta_2) : \mathcal{M}' \to \mathcal{M}_2$ redom epimorfizam i monomorfizam automata. Tada vrijedi $\mathcal{M}_1 \leq \mathcal{M}_2$.*

Dokaz. Neka je $\alpha_2^{-1} \colon Q_2 \rightharpoonup Q'$ parcijalna funkcija takva da je $\mathcal{D}_{\alpha_2^{-1}} = \alpha_2(Q') \subseteq Q_2$ i koja je inverzna funkciji α_2 na ovoj domeni. Neka je $\beta_1^{-1} \colon \Sigma_1 \to \Sigma'$ bilo koja funkcija takva da za sve $\sigma_1 \in \Sigma_1$ vrijedi:

$$\beta_1^{-1}(\sigma_1) = \theta, \text{ gdje je } \theta \in \Sigma' \text{ neki element za koji vrijedi } \beta_1(\theta) = \sigma_1.$$

Provjerimo da je $(\alpha_1 \circ \alpha_2^{-1}, \beta_2 \circ \beta_1^{-1})$ traženi prekrivač.

Očito je $\alpha_1 \circ \alpha_2^{-1}$ surjekcija. Neka su $q_2 \in Q_2$ i $\sigma_1 \in \Sigma_1$ takvi da $F_1((\alpha_1 \circ \alpha_2^{-1})(q_2), \sigma_1) \neq \varnothing$. Prvo se uvjerimo da vrijedi

$$\alpha_2^{-1}(F_2(q_2, (\beta_2 \circ \beta_1^{-1})(\sigma_1))) = F'(\alpha_2^{-1}(q_2), \beta_1^{-1}(\sigma_1)).$$

Doista, jer je (α_2, β_2) homomorfizam, imamo:

$$\begin{aligned} \alpha_2(F'(\alpha_2^{-1}(q_2), \beta_1^{-1}(\sigma_1))) &= F_2((\alpha_2 \circ \alpha_2^{-1})(q_2), (\beta_2 \circ \beta_1^{-1})(\sigma_1)) \\ &= F_2(q_2, (\beta_2 \circ \beta_1^{-1})(\sigma_1)). \end{aligned}$$

Dalje je lako. Dobijemo:

$$\begin{aligned} (\alpha_1 \circ \alpha_2^{-1})(F_2(q_2, (\beta_2 \circ \beta_1^{-1})(\sigma_1))) &= \alpha_1(F'(\alpha_2^{-1}(q_2), \beta_1^{-1}(\sigma_1))) \\ &= F_1((\alpha_1 \circ \alpha_2^{-1})(q_2), \sigma_1). \end{aligned}$$

□

Primjer 2.14. Supstitucijama $\mathcal{M}' = \mathcal{M}_1$ ili $\mathcal{M}' = \mathcal{M}_2$ iz prethodne leme direktno slijedi da epimorfizmi ili monomorfizmi između dva automata generiraju prekrivače tih automata. Na primjer, u dijelu (*ii*) primjera 2.4 konstruirali smo epimorfizam konačnih automata sa slika 2.1 i 1.6. Sada možemo zaključiti da je konačni automat sa slike 1.6 prekriven onim sa slike 2.1.

Kao direktnu posljedicu leme 2.13, dobijemo i sljedeći rezultat o odnosu homomorfizama i prekrivača.

Korolar 2.15. *Neka su $\mathcal{M}$ i $\mathcal{M}$ izomorfni automati. Tada su $\mathcal{M}$ i $\mathcal{M}'$ ekvivalentni.*

Iz prethodnog korolara te propozicije 2.5 slijedi da su transformacijske polugrupe $\mathcal{S}$ i $\mathbf{TS}(\mathbf{SM}(\mathcal{S}))$ ekvivalentne. Najavili smo da ćemo predstaviti i dualni rezultat o odnosu operacija **TS** i **SM**.

Lema 2.16. *Neka je $\mathcal{M}$ konačni automat. Tada vrijedi:*

$$\mathcal{M} \leq \mathbf{SM}(\mathbf{TS}(\mathcal{M})).$$

Dokaz. Neka je $\mathcal{M} = (Q, \Sigma, F)$. Tada vrijedi $\mathbf{TS}(\mathcal{M}) = (Q, \mathbf{S}(\mathcal{M}), \cdot_{\mathcal{M}})$ i nadalje $\mathbf{SM}(\mathbf{TS}(\mathcal{M})) = (Q, \mathbf{S}(\mathcal{M}), F')$. Pokazujemo da je (I_Q, ν) traženi prekrivač, gdje je funkcija $\nu\colon \Sigma \to \mathbf{S}(\mathcal{M})$ zadana tako da za sve $\sigma \in \Sigma$ vrijedi $\nu(\sigma) = [\sigma]$. Za sve $q \in Q$ i $\sigma \in \Sigma$ takve da je $qF_\sigma \neq \varnothing$ po definicijama 1.36 i 1.38 vrijedi:

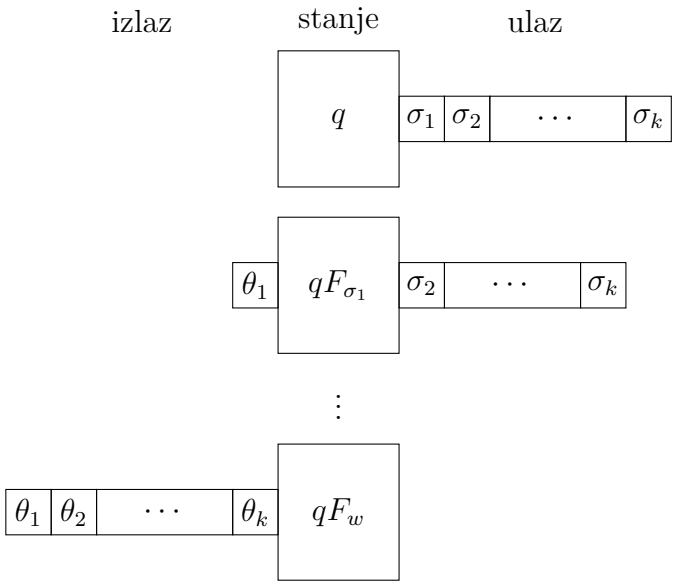
$$\mu(qF'_{\nu(\sigma)}) = qF'_{[\sigma]} = \mu(q) \cdot_{\mathcal{M}} [\sigma] = \mu(q)F_\sigma. \qquad \square$$

2.3 Mealyjevi automati

Do sada razmatrani automati tijekom svog rada nisu proizvodili izvana uočljive efekte. U ovom odjeljku, definiramo automate koji imaju mogućnost ispisa vrijednosti. Postoje dvije važne vrste konačnih automata s izlazom: Mooreovi ([14]) i Mealyjevi ([12]). Pokazuje se da su ove dvije vrste automata međusobno ekvivalentne u smislu računarskih sposobnosti. U ovom odjeljku bavimo se isključivo Mealyjevim automatima.

Definicija 2.17. Neka je Q konačan skup stanja, Σ ulazni alfabet i Θ izlazni alfabet. Neka je $F\colon Q \times \Sigma \to Q$ parcijalna funkcija prijelaza te $G\colon Q \times \Sigma \to \Theta$ funkcija izlaza. Petorka $\hat{\mathcal{M}} = (Q, \Sigma, \Theta, F, G)$ naziva se *Mealyjev automat*.

U osnovi svakog Mealyjevog automata jest konačni automat, stoga koristimo oznaku $\hat{\mathcal{M}}$. Za razliku od običnog automata, Mealyjev automat prilikom prijelaza između stanja ispisuje simbol iz alfabeta Θ, određen funkcijom G. Zamišljamo ga kao „crnu kutiju" zajedno s trakom podijeljenom na ćelije u kojima su zapisani ulazni znakovi. Svojim radom ovaj automat ulaznu riječ sa trake $w \in \Sigma^+$ pretvara znak po znak do izlaza $u \in \Theta^+$ (slika 2.2). Važna svojstva ovog procesa jesu „in-place" zamjena ulaznog znaka izlaznim, tj. u istoj ćeliji trake, te da izračunavanje završava čim je cijela traka pročitana.



Slika 2.2: Rad Mealyjevog automata ([8, slika, 2.1])

Kao zanimljivu digresiju, a u svrhu daljnje motivacije za proučavanje konačnih automata, kratko raspravljamo o karakteristikama izračunavanja Mealyjevih automata. Svaki Mealyjev automat „računa" jedinstvenu funkciju koja prevodi riječi iz ulazne abecede u riječi iz izlazne abecede. Osnovna karakteristika ove funkcije jest da je sljedeći znak izlaza neposredno određen trenutnim znakom na ulazu (i stanjem u kojem se stroj trenutno nalazi). Formalizirajmo ovaj koncept.

Definicija 2.18. Neka su Σ i Θ konačni alfabeti. Proizvoljna funkcija $f\colon \Sigma^+ \to \Theta$ naziva se *sekvencijalni stroj*. Za $k \in \mathbb{N}_+$ i $\sigma_1, \sigma_2, \ldots, \sigma_k \in \Sigma$, označimo $f(\sigma_1\sigma_2\cdots\sigma_k) = \theta_k \in \Theta$. Tada možemo rekurznivno definirati funkciju $\bar{f}\colon \Sigma^+ \to \Theta^+$ pravilom

$$\bar{f}(\sigma_1\sigma_2\cdots\sigma_k) = \theta_1\theta_2\cdots\theta_k, \text{ za sve } k \geq 1. \tag{6}$$

Definicija 2.19. Neka je $\hat{\mathcal{M}} = (Q, \Sigma, \Theta, F, G)$ Mealyjev automat. Za svaki $q \in Q$ rekurzivno definiramo funkciju $\mathfrak{M}_q\colon \Sigma^+ \to \Theta$ tako da za sve $k \in \mathbb{N}$, $k \geq 2$ i $\sigma_1, \sigma_2, \ldots, \sigma_k \in \Sigma$ vrijedi:

$$\mathfrak{M}_q(\sigma_1) = q\,G_{\sigma_1} \text{ i}$$
$$\mathfrak{M}_q(\sigma_1\sigma_2\cdots\sigma_k) = (qF_{\sigma_1\cdots\sigma_{k-1}})G_{\sigma_k}.$$

Kažemo da Mealyjev automat $\hat{\mathcal{M}}$ *implementira* sekvencijalni stroj $f\colon \Sigma^+ \to \Theta$ ako postoji $q_0 \in Q$ takav da vrijedi $\mathfrak{M}_{q_0} = f$.

Primjerice, naš konačni automat iz primjera 1.10 za modularno zbrajanje modulo N može se shvatiti kao Mealyjev automat koji implementira sekvencijalni stroj $f\colon \mathbb{N}_N \to \mathbb{N}_N$ zadan s $f(\sigma_1\sigma_2\cdots\sigma_n) = \sigma_1 + \sigma_2 + \cdots \sigma_n \pmod N$.

Za sada znamo da svaki Mealyjev automat implementira sekvencijalnu funkciju. Dokazat ćemo da *donekle* vrijedi i obrat ove tvrdnje, dakle da je svaka sekvencijalna funkcija implementirana Mealyjevim automatom. Kažemo donekle, jer ćemo morati dopustiti (prebrojivo) beskonačan skup stanja Mealyjevog automata. Ovakve automate nazivat ćemo *generalizirani Mealyjevi automati*.

Prije iskaza teorema, uvodimo *lijeve translacije* na skupu Σ^*. Neka je $u \in \Sigma^*$ proizvoljan. Definiramo funkciju $L_u\colon \Sigma^+ \to \Sigma^+$ tako da za sve $w \in \Sigma^+$ stavimo $L_u(w) = uw$. Primjetimo da za $u_1,\, u_2 \in \Sigma^*$ vrijedi $L_{u_1} \circ L_{u_2} = L_{u_1u_2}$.

Propozicija 2.20. *Neka su Σ i Θ konačni skupovi i $f\colon \Sigma^+ \to \Theta$ proizvoljni sekvencijalni stroj. Neka je $Q = \{\, fL_u\colon u \in \Sigma^* \,\}$. Definiramo funkcije $F\colon Q \times \Sigma \to Q$ i $G\colon Q \times \Sigma \to \Theta$ tako da za sve $fL_u \in Q$ i $\sigma \in \Sigma$ vrijedi:*

$$\begin{aligned}(fL_u)\, F_\sigma &= fL_uL_\sigma = fL_{u\sigma} \quad i\\ (fL_u)\, G_\sigma &= (fL_u)\,(\sigma) = f(u\sigma).\end{aligned}$$

Tada generalizirani Mealyjev automat $\hat{\mathcal{M}}_f = (Q, \Sigma, \Theta, F, G)$ implementira sekvencijalni stroj f.

Dokaz. Za početno stanje uzmimo $q_0 = fL_\varepsilon$. Neka je $w = \sigma_1\sigma_2\cdots\sigma_k \in \Sigma^+$ proizvoljna riječ. Lagano je pokazati da za sve $u \in \Sigma^*$ vrijedi $(fL_u)\, F_w = fL_{uw}$. Dobijemo:

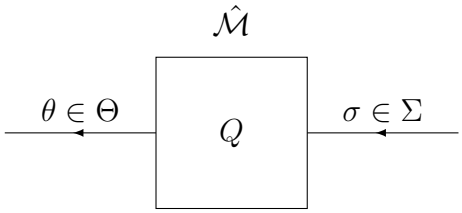
$$\mathfrak{M}_{q_0}(w) = ((fL_\varepsilon)\, F_{\sigma_1\cdots\sigma_{k-1}})G_{\sigma_k} = (fL_{\varepsilon\sigma_1\cdots\sigma_{k-1}})G_{\sigma_k} = f(w). \qquad \square$$

Ako je skup stanja automata $\hat{\mathcal{M}}_f$ konačan, možemo reći da je sekvencijalni stroj f *Mealy-izračunljiv*. Pokazuje se da je (generalizirani) Mealyjev automat $\hat{\mathcal{M}}_f$ „najmanji" automat koji implementira stroj f. Upravo zbog ove jedinstvenosti, teorija konačnih automata jest algebarska, za razliku od kombinatorne teorije izračunljivosti i složenosti kod Turingovih strojeva. Opširnija rasprava o ovoj temi može se pronaći u [15, poglavlje 5].

Vraćamo se na osnovni tijek izlaganja. Svrha promatranja automata s izlazom u ovom radu je sljedeća. Želimo istražiti načine na koji možemo kombinirati dva konačna automata kako bismo dobili novi konačni automat. Funkcionalnost dobivenog automata ovisit će o funkcionalnosti polaznih automata te o samoj metodi kombiniranja.

Kod automata s izlazom, pruža nam se nekoliko načina spajanja dva automata u jedan. Osnovni način je shvaćanje dva odvojena automata kao jedan veliki automat

sastavljen od dva pod-automata koji rade neovisno jedan o drugome. Ovo odgovara onome što nazivamo **paralelni spoj** automata. Osim ovoga, možemo povezati automate na međusobno ovisan način, i to tako da izlaz jednog automata prosljedimo kao ulaz drugom automatu. Time dobijemo **serijski spoj** automata. U svrhu vizualizacije ovih spojeva, pojedine Mealyjeve automate prikazujemo pojednostavljeno kao na slici 2.3.



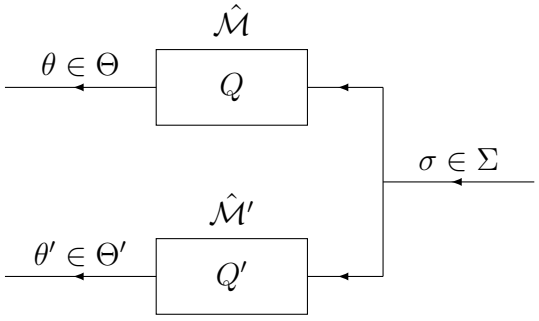
Slika 2.3: Pojednostavljeni prikaz Mealyjevog automata $\hat{\mathcal{M}} = (Q, \Sigma, \Theta, F, G)$

Neka su $\hat{\mathcal{M}} = (Q, \Sigma, \Theta, F, G)$ i $\hat{\mathcal{M}}' = (Q', \Sigma', \Theta', F', G')$ Mealyjevi automati. Pretpostavimo najprije da vrijedi $\Sigma = \Sigma'$, dakle da automati $\hat{\mathcal{M}}$ i $\hat{\mathcal{M}}'$ imaju istu ulaznu abecedu Σ. Njihov paralelni spoj, ilustriran slikom 2.4, jest novi Mealyjev automat

$$\hat{\mathcal{M}} \wedge \hat{\mathcal{M}}' = (Q \times Q', \Sigma, \Theta \times \Theta', F \wedge F', G \wedge G')\,,$$

gdje za sve $(q, q') \in Q \times Q'$ i $\sigma \in \Sigma$ vrijedi

$$(F \wedge F')((q, q')\,, \sigma) = (F(q, \sigma), F'(q', \sigma)) \text{ i}$$
$$(G \wedge G')((q, q')\,, \sigma) = (G(q, \sigma), G'(q', \sigma))\,.$$



Slika 2.4: Paralelni spoj dva Mealyjeva automata s istom ulaznom abecedom ([8, slika 2.2])

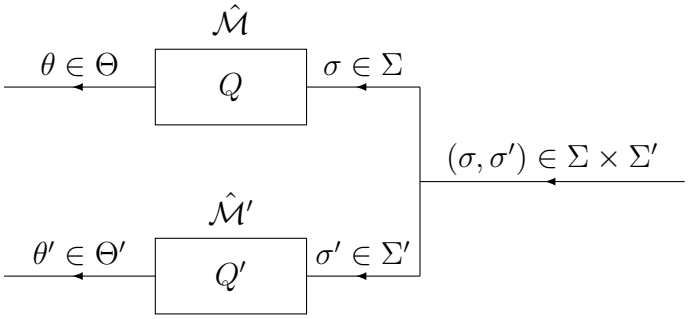
Čak i u slučaju da ne vrijedi $\Sigma = \Sigma'$, možemo konstruirati paralelni spoj Mealyjevih automata $\hat{\mathcal{M}}$ i $\hat{\mathcal{M}}'$, koji će imati dva toka ulaznih podataka (slika 2.5).

Definiramo novi Mealyjev automat

$$\hat{\mathcal{M}} \times \hat{\mathcal{M}}' = (Q \times Q', \Sigma \times \Sigma', \Theta \times \Theta', F \times F', G \times G')\,,$$

gdje za sve $(\sigma, \sigma') \in \Sigma \times \Sigma'$ i $(q, q') \in Q \times Q'$ vrijedi

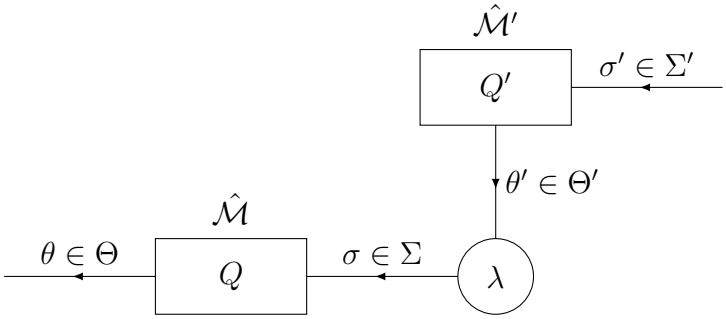
$$(F \times F')((q, q')\,, (\sigma, \sigma')) = (F(q, \sigma), F'(q', \sigma')) \text{ i}$$
$$(G \times G')((q, q')\,, (\sigma, \sigma')) = (G(q, \sigma), G'(q', \sigma'))\,.$$



Slika 2.5: Paralelni spoj dva Mealyjeva automata s različitom ulaznom abecedom ([8, slika 2.3])

Prelazimo na serijski spoj, ilustriran slikom 2.6. Kako bismo izlaz automata $\hat{\mathcal{M}}'$ proslijedili kao ulaz automatu $\hat{\mathcal{M}}$, pretvorimo znakove iz Θ' u znakove iz Σ funkcijom $\lambda\colon \Theta' \to \Sigma$. Pomoću ove funkcije, definiramo preslikavanje $\omega\colon Q' \times \Sigma' \to \Sigma$ kao kompoziciju $\omega = \lambda \circ G'$. Sada za svaki ulaz $\sigma' \in \Sigma'$ definiramo indeksirano preslikavanje $\omega_{\sigma'}\colon Q' \to \Sigma$ takvo da za sva stanja $q' \in Q'$ vrijedi $\omega_{\sigma'}(q') = \omega(q', \sigma')$. Rezultirajući Mealyjev automat označavamo s

$$\hat{\mathcal{M}}\,\omega\,\hat{\mathcal{M}}' = (Q \times Q', \Sigma', \Theta, F\,\omega\,F', G\,\omega\,G')\,,$$



Slika 2.6: Serijski spoj dva Mealyjeva automata

gdje za sve $\sigma' \in \Sigma'$ i $(q, q') \in Q \times Q'$ vrijedi

$$(F \,\omega\, F')((q, q'), \sigma') = (F(q, \omega_{\sigma'}(q')), F'(q', \sigma')) \text{ i}$$
$$(G \,\omega\, G')((q, q'), \sigma') = G(q, \omega_{\sigma'}(q')).$$

Mealyjev automat $\hat{\mathcal{M}} \,\omega\, \hat{\mathcal{M}}'$ nazivamo *kaskadni produkt* Mealyjevih automata $\hat{\mathcal{M}}$ i $\hat{\mathcal{M}}'$ *induciran s* ω.

2.4 Produkti

U prethodnom odjeljku prikazali smo nekoliko načina spajanja Mealyjevih automata. Oni će nam poslužiti kao motivacija za definicije raznih produkata konačnih automata. Jednostavno ćemo ukloniti izlazni alfabet i funkciju izlaza. U cijelom ovom odjeljku, $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$ su konačni automati.

Definicija 2.21. Pretpostavimo da vrijedi $\Sigma = \Sigma'$. *Ograničeni direktni produkt konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ je konačni automat

$$\mathcal{M} \wedge \mathcal{M}' = (Q \times Q', \Sigma, F \wedge F'),$$

gdje za sve $\sigma \in \Sigma$ i $(q, q') \in Q \times Q'$ vrijedi

$$(F \wedge F')((q, q'), \sigma) = (F(q, \sigma), F'(q', \sigma)).$$

Definicija 2.22. *(Pravi) direktni produkt konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ je konačni automat

$$\mathcal{M} \times \mathcal{M}' = (Q \times Q', \Sigma \times \Sigma', F \times F'),$$

gdje za sve $(\sigma, \sigma') \in \Sigma \times \Sigma'$ i $(q, q') \in Q \times Q'$ vrijedi

$$(F \times F')((q, q'), (\sigma, \sigma')) = (F(q, \sigma), F'(q', \sigma')).$$

Definicija 2.23. Neka je $\omega \colon Q' \times \Sigma' \to \Sigma$ zadana funkcija. *Kaskadni produkt konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ *induciran s* ω je konačni automat

$$\mathcal{M} \,\omega\, \mathcal{M}' = (Q \times Q', \Sigma', F \,\omega\, F'),$$

gdje za sve $\sigma' \in \Sigma'$ i $(q, q') \in Q \times Q'$ vrijedi

$$(F \,\omega\, F')((q, q'), \sigma') = (F(q, \omega(q', \sigma')), F'(q', \sigma')).$$

Funkciju ω nazivamo i *kaskadno preslikavanje*.

Razmotrimo detaljnije kaskadni produkt automata $\mathcal{M}$ i $\mathcal{M}'$. Dobiveni automat $\mathcal{M}\,\omega\,\mathcal{M}'$ ima mogućnost pratiti u kojem se stanju nalazi svaki njegov sastavni automat. Ulazi za produktni automat su ulazi automata $\mathcal{M}'$, dakle prvog u serijskom nizu. Taj automat prilikom čitanja ulaznog znaka mijenja stanje kao i inače, tj. u skladu s njegovom funkcijom prijelaza F'. Drugi automat kao ulaz posredno dobije znak, koji ovisi o trenutnom stanju prvog automata te njegovom ulaznom znaku. Na taj način se promjene stanja u prvom automatu kaskadno utječu na rad drugog automata.

Domena kaskadnog preslikavanja ω neće biti uvijek eksplicitno navedena, već određena iz konteksta. U slučaju da vrijedi $Q' \times \Sigma' = \Sigma$, podrazumijevani izbor za ω je I_Σ. Spomenimo još usputno da se kaskadni produkt može definirati i za potisne automate, s neočekivanim svojstvima (vidi [1]).

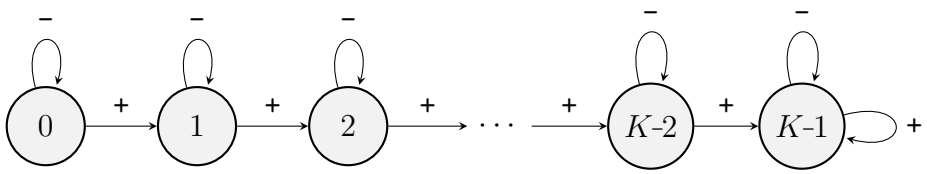
Primjer 2.24.

(*i*) Neka su M i N prirodni brojevi. Pravi paralelni produkt automata za zbrajanje modulo M s automatom za zbrajanje modulo N je automat koji paralelno računa odgovarajuće ostatke.

(*ii*) Neka su $N, K \in \mathbb{N}_+$. Neka je $\mathcal{N} = \mathbf{SM}(\mathbb{Z}_N) = \{\, \mathbb{Z}_N, \mathbb{Z}_N, F' \,\}$ konačni automat za zbrajanje modulo N iz dijela (*iii*) primjera 1.10. Neka je $\mathcal{M} = (\mathbb{N}_K, \{\, \texttt{-}, \texttt{+} \,\}, F)$ konačni automat, čija funkcija prijelaza F je takva da za sve $k \in \mathbb{N}_K$ i $\sigma \in \{\, \texttt{-}, \texttt{+} \,\}$ vrijedi:

$$k\,F_\sigma = \begin{cases} k, \text{ ako } \sigma = \texttt{-}; \\ k+1, \text{ ako } \sigma = \texttt{+} \text{ i } k < K-1; \\ K-1, \text{ ako } \sigma = \texttt{+} \text{ i } k = K-1 \end{cases} .$$

Konačni automat $\mathcal{M}$ prikazan je na slici 2.7. Završno stanje izračunavanja ovog automata iz početnog stanja 0 s ulaznom riječi $w \in \{\, \texttt{-}, \texttt{+} \,\}^+$, koja sadrži najviše $(K-1)$ znakova +, odgovara točnom broju znakova + u riječi w. Ovaj konačni automat se stoga naziva *ograničeni brojač veličine* K.



Slika 2.7: Brojač veličine K

Neka je preslikavanje $\omega\colon \mathbb{Z}_N \times \mathbb{Z}_N \to \{\,\mathsf{-},\mathsf{+}\,\}$ zadano tako da za sve $q, \sigma' \in \mathbb{Z}_N$ vrijedi sljedeće:

$$\omega\,(q,\sigma) = \begin{cases} \mathsf{-} \text{ ako } q+\sigma < N; \\ \mathsf{+}, \text{ inače} \end{cases}.$$

Promotrimo kaskadni produkt $\mathcal{M}\,\omega\,\mathcal{N} = (\mathbb{N}_K \times \mathbb{Z}_N, \mathbb{Z}_N, F\,\omega\,F')$. Neka je $u \in (\mathbb{Z}_N)^+$ konačan niz brojeva čiji je zbroj, kojeg označavamo sa $\mathrm{sum}(u)$, manji od $K \cdot N$. Tada izračunavanje automata $\mathcal{M}\,\omega\,\mathcal{N}$ iz početnog stanja $(0,0)$ s ulaznom riječi u završava u stanju (k,n) za koje vrijedi $\mathrm{sum}(u) = k \cdot N + n$. Drugim riječima, automat $\mathcal{M}\,\omega\,\mathcal{N}$ izračunava kvocijent i ostatak pri dijeljenju s N broja dobivenog kao zbroj svih članova ulaznog niza, pod uvjetom da ovaj zbroj nije „prevelik" (točnije, manji od $K \cdot N$).

(*iii*) Direktni produkt dva deterministička automata koristan je za dokaz zatvorenosti regularnih jezika na operacije unije i presjeka (vidi [17, teorem 1.25]).

U ovom trenutku čini se da su produkti konačnih automata motivirani paralelnim i serijskim spojem Mealyjevih automata međusobno neusporedivi u smislu mogućnosti simulacije jednog produkta drugim. Da tome ipak nije tako, potvrđuje sljedeći rezultat. Njime je dokazano da se direktni produkt može simulirati kaskadnim produktom. Zbog toga ćemo se u nastavku pretežito koristiti upravo kaskadnim produktom.

Lema 2.25. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ konačni automati. Tada postoji konačni automat $\mathcal{M}''$ ekvivalentan automatu $\mathcal{M}'$ i preslikavanje ω za koje vrijedi:*

$$\mathcal{M} \times \mathcal{M}' \leq \mathcal{M}\,\omega\,\mathcal{M}''.$$

Dokaz. Označimo $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$. Ideja je pronaći automat s jednakom funkcionalnošću kao automat $\mathcal{M}'$, no koji kao ulaz prima i znakove iz Σ, samo kako bi ih prosljedio automatu $\mathcal{M}$. To postižemo duplikacijom stanja putem Kartezijevog produkta.

Definiramo konačni automat $\mathcal{M}'' = (Q', \Sigma' \times \Sigma, F'')$, čija funkcija prijelaza je zadana tako da za sve $q' \in Q'$ i $(\sigma', \sigma) \in \Sigma' \times \Sigma$ vrijedi $F''\,(q', (\sigma', \sigma)) = F'\,(q', \sigma')$. Preslikavanje $\omega\colon Q' \times (\Sigma' \times \Sigma)$ definiramo tako da za sve $q' \in Q'$ i $(\sigma', \sigma) \in \Sigma' \times \Sigma$ vrijedi $\omega\,(q', (\sigma', \sigma)) = \sigma$. Lako se vidi da uz ovaj izbor dobijemo traženi prekrivač.

Ostaje pokazati ekvivalentnost konačnog automata $\mathcal{M}''$ s početnim automatom $\mathcal{M}'$. Prekrivanje $\mathcal{M}' \leq \mathcal{M}''$ je očigledno iz definicije automata $\mathcal{M}''$. Obratno prekrivanje $\mathcal{M}'' \leq \mathcal{M}'$ dobijemo za prekrivač (I_Q, ν), gdje je funkcija $\nu\colon \Sigma' \times \Sigma \to \Sigma$ takva da za sve $(\sigma', \sigma) \in \Sigma' \times \Sigma$ vrijedi $\nu\,(\sigma', \sigma) = \sigma$. □

Uvodimo još jedan produkt automata, koji je generalizacija kaskadnog produkta. Naime, kod kaskadnog produkta je za svaki $\sigma' \in \Sigma'$ preslikavanje $\omega_{\sigma'}$ unaprijed zadano. Sada ćemo dopustiti da ga automat prima kao dodatni ulazni podatak.

Definicija 2.26. *Vjenačni produkt konačnih automata* $\mathcal{M}$ i $\mathcal{M}'$ je konačni automat

$$\mathcal{M} \circ \mathcal{M}' = \left(Q \times Q', \Sigma^{Q'} \times \Sigma', F \circ F'\right),$$

gdje za sve $(q, q') \in Q \times Q'$, $f \in \Sigma^{Q'}$ i $\sigma' \in \Sigma'$ vrijedi

$$(F \circ F')((q, q'), (f, \sigma')) = (F(q, f(q')), F'(q', \sigma')).$$

Definirajmo produkte transformacijskih polugrupa koji odgovaraju produktima konačnih automata. Nakon toga ćemo uspostaviti odnos između najvažnijih dualno definiranih produkata. U nastavku su sa $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ i $\mathcal{S}' = (X', S', \cdot_{\mathcal{S}'})$ označene transformacijske polugrupe.

Definicija ograničenog direktnog produkta kod transformacijskih polugrupa je nezgrapna i tehnički kompliciranа. Kako nam ovaj produkt neće biti pretjerano koristan, izostavljamo ga iz rasprave, a zainteresiranog čitatelja upućujemo na [8, odjeljak 2.6]. Definicija pravog direktnog produkta transformacijskih polugrupa je jednostavnija.

Definicija 2.27. *(Pravi) direktni produkt transformacijskih polugrupa* $\mathcal{S}$ i $\mathcal{S}'$ je transformacijska polugrupa

$$\mathcal{S} \times \mathcal{S}' = (X \times X', S \times S', \cdot)$$

gdje je za sve $(x, y) \in X \times X'$ i $(s, t) \in S \times S'$ djelovanje $\cdot$ transformacijske polugrupe $\mathcal{S} \times \mathcal{S}'$ dano s

$$(x, y) \cdot (s, t) = (x \cdot_{\mathcal{S}} s, y \cdot_{\mathcal{S}'} t).$$

Kod transformacijskih polugrupa ne postoji direktni analogon kaskadnog produkta. Stoga definiramo odmah vjenačni produkt. Pokažimo prije svega da je skup $S^{X'} \times S'$ polugrupa. Prvo za proizvoljni $s' \in S'$ definiramo operaciju $*_{s'}$ na skupu $S^{X'}$. Neka su f i g proizvoljne funkcije iz skupa $S^{X'}$. Neka za svaki $x' \in X'$ vrijedi:

$$(f *_{s'} g)(x') = f(x') \cdot_S g(x' \cdot_{\mathcal{S}'} s').$$

Sada možemo definirati množenje $*$ na skupu $S^{X'} \times S'$. Za sve $(f, s'), (g, t') \in S^{X'} \times S'$ stavimo

$$(f, s') * (g, t') = (f *_{s'} g, s' \cdot_{S'} t').$$

Definicija 2.28. *Vjenačni produkt transformacijskih polugrupa* $\mathcal{S}$ i $\mathcal{S}'$ je transformacijska polugrupa

$$\mathcal{S} \circ \mathcal{S}' = \left(X \times X', S^{X'} \times S', \circ\right),$$

gdje je za sve $(x, x') \in X \times X'$ i $(f, s') \in S^{X'} \times S'$ djelovanje $\circ$ dano s

$$(x, x') \circ (f, s') = (x \cdot_{\mathcal{S}} f(x'), x' \cdot_{\mathcal{S}'} s').$$

Uvjerimo se u valjanost prethodne definicije. Kvaziasocijativnost vrijedi, jer za sve $(x,x') \in X \times X'$ i $(f,s'),(g,t') \in S^{X'} \times S'$ imamo

$$\begin{aligned}
&((x,x') \circ (f,s')) \circ (g,t') = (x \cdot_S (f(x')), x' \cdot_{S'} s') \circ (g,t') \\
&= ((x \cdot_S (f(x'))) \cdot_S g(x' \cdot_{S'} s'), (x' \cdot_{S'} s') \cdot_{S'} t') = (x \cdot_S (f(x') \cdot_S g(x' \cdot_{S'} s')), x' \cdot_{S'} (s' \cdot_{S'} t')) \\
&= (x \cdot_S (f *_{s'} g)(x'), x' \cdot_{S'} (s' \cdot_{S'} t')) = (x,x') \circ (f *_{s'} g, s' \cdot_{S'} t') = (x,x') \circ ((f,s') * (g,t')).
\end{aligned}$$

Lako se pokaže da dosljednost djelovanja $\circ$ slijedi iz dosljednosti djelovanja $\cdot_S$ i $\cdot_{S'}$.

Istaknimo da su svi uvedeni produkti asocijativni na klasi svih konačnih automata, odnosno transformacijskih polugrupa. Smatramo da je ovo svojstvo intuitivno opravdano (za formalni raspis, vidi [8, str. 60]). Asocijativnost je preduvjet za tehnike iz idućeg poglavlja, kojima nalazimo prekrivače jednog automata ili transformacijske polugrupe produktom od njih konačno mnogo.

U sljedećih par rezultata opisane su korisne veze između raznih produkata. Većina se odnosi na postojanje prekrivača međusobno pridruženih struktura. Kod direktnih produkata situacija je jasna.

Propozicija 2.29. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ konačni automati. Tada vrijedi:*

$$\mathbf{TS}(\mathcal{M} \times \mathcal{M}') \leq \mathbf{TS}(\mathcal{M}) \times \mathbf{TS}(\mathcal{M}').$$

Dokaz. Neka vrijedi $\mathcal{M} = (Q, \Sigma, F)$ i $\mathcal{M}' = (Q', \Sigma', F')$. Tada je njihov direktni produkt $\mathcal{M} \times \mathcal{M}' = (Q \times Q', \Sigma \times \Sigma', F \times F')$. Funkcija $\nu\colon \mathbf{S}(\mathcal{M} \times \mathcal{M}') \to \mathbf{S}(\mathcal{M}) \times \mathbf{S}(\mathcal{M}')$ neka je zadana tako da za sve $[(u,v)] \in \mathbf{S}(\mathcal{M} \times \mathcal{M}')$, gdje je $u \in \Sigma^+$ i $v \in \Sigma'^+$, vrijedi $\nu([(u,v)]) = ([u],[v])$. Provjerimo da je ν dobro definirana.

Neka su $u, u' \in \Sigma^+$ i $v, v' \in \Sigma'^+$ takvi da je $[(u,v)] = [(u',v')]$. Ovo je ekvivalentno s $(F \times F')_{(u,v)} = (F \times F')_{(u',v')}$. Zbog definicije direktnog produkta, ovo vrijedi ako i samo ako je $F_u = F_{u'}$ i $G_v = G_{v'}$. No iz toga upravo slijedi $[u] = [u']$ i $[v] = [v']$, pa dakle i $([u],[v]) = ([u'],[v'])$.

Dokažimo da je $(I_{Q \times Q'}, \nu)$ traženi prekrivač transformacijskih polugrupa. Označimo sa $*$ djelovanje transformacijske polugrupe $\mathbf{TS}(\mathcal{M}) \times \mathbf{TS}(\mathcal{M}')$. Neka su $(q,q') \in Q \times Q'$ i $[(u,v)] \in \mathbf{S}(\mathcal{M} \times \mathcal{M}')$ takvi da je $(q,q') * ([u],[v]) \neq \varnothing$. Konačno dobijemo:

$$\begin{aligned}
(q,q') * ([u],[v]) &= (q \cdot_{\mathcal{M}} [u], q' \cdot_{\mathcal{M}} [v]) = (qF_u, q'G_v) \\
&= (q,q')(F \times F')_{(u,v)} = (q,q') \cdot_{\mathcal{M} \times \mathcal{M}'} [(u,v)].
\end{aligned}$$

□

Zbog propozicije 2.5, za transformacijske polugrupe vrijedi i jača tvrdnja.

Propozicija 2.30. *Neka su $\mathcal{S}$ i $\mathcal{S}'$ transformacijske polugrupe. Tada vrijedi:*

$$\mathbf{SM}(\mathcal{S} \times \mathcal{S}') \cong \mathbf{SM}(\mathcal{S}) \times \mathbf{SM}(\mathcal{S}').$$

Najčešće ćemo koristiti kaskadni produkt automata i vjenačni produkt transformacijskih polugrupa. Stoga je sljedeći rezultat od iznimne važnosti (za dokaz vidi [8, teorem 2.6.4]).

Propozicija 2.31. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ konačni automati. Neka je ω proizvoljno kaskadno preslikavanje između automata $\mathcal{M}'$ i $\mathcal{M}$. Tada vrijedi:*

$$\mathbf{TS}\left(\mathcal{M}\,\omega\,\mathcal{M}'\right) \leq \mathbf{TS}\left(\mathcal{M}\right) \circ \mathbf{TS}\left(\mathcal{M}'\right).$$

Završni rezultat će nam biti koristan u sljedećem poglavlju. Dokaz je jednostavan.

Lema 2.32. *Neka su $\mathcal{M}$ i $\mathcal{M}'$ konačni automati takvi da je $\mathcal{M} \leq \mathcal{M}'$. Neka je $\mathcal{U}$ proizvoljni konačni automat. Tada za svako kaskadno preslikavanje ω vrijedi:*

$$\mathcal{M}\,\omega\,\mathcal{U} \leq \mathcal{M}'\,\omega\,\mathcal{U} \quad i \quad \mathcal{U}\,\omega\,\mathcal{M} \leq \mathcal{U}\,\omega\,\mathcal{M}'.$$

Dualno, neka su $\mathcal{S}$ i $\mathcal{S}'$ transformacijske polugrupe takve da je $\mathcal{S} \leq \mathcal{S}'$. Neka je $\mathcal{V}$ proizvoljna transformacijska polugrupa. Tada vrijedi:

$$\mathcal{S} \circ \mathcal{V} \leq \mathcal{S}' \circ \mathcal{V} \quad i \quad \mathcal{V} \circ \mathcal{S} \leq \mathcal{V} \circ \mathcal{S}'.$$

Neke primjene do sada razvijene teorije izložene su u [8, odjeljak 2.8]. Primjeri obuhvaćaju raznovrsna područja, uključujući elektrotehniku, biologiju stanice i kemijske procese u organizmu.

Poglavlje 3

Dekompozicije

Produktne konstrukcije iz prethodnog odlomka omogućuju nam da od manjih konačnih automata izgradimo veće i složenije automate. U ovom poglavlju cilj nam je istražiti obratni proces, dakle rastav složenih automata na jednostavnije sastavne dijelove. Krajnji cilj nam je odrediti „najmanju" kolekciju konačnih automata takvu da je produktima njenih elemenata moguće simulirati proizvoljni konačni automat. Sve navedeno odnosi se i na transformacijske polugrupe, no kao što je već naglašeno u uvodu, u središtu našeg interesa je računarski aspekt teorije.

Definicija 3.1. Neka je $\mathcal{M}$ konačni automat. *Kaskadna dekompozicija konačnog automata* $\mathcal{M}$ je svaki konačni niz automata $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ $(k \in \mathbb{N}_+)$ takav da za neka kaskadna preslikavanja $\omega_1, \omega_2, \ldots, \omega_{k-1}$ vrijedi:

$$\mathcal{M} \leq \mathcal{M}_1 \, \omega_1 \, \mathcal{M}_2 \, \omega_2 \cdots \omega_{k-1} \, \mathcal{M}_k.$$

Analogno se definira *vjenačna dekompozicija konačnog automata.*

Definicija 3.2. Neka je $\mathcal{S}$ transformacijska polugrupa. *Vjenačna dekompozicija transformacijske polugrupe* $\mathcal{S}$ je svaki konačni niz transformacijskih polugrupa $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ $(k \in \mathbb{N}_+)$ takav da vrijedi:

$$\mathcal{S} \leq \mathcal{S}_1 \circ \mathcal{S}_2 \circ \cdots \circ \mathcal{S}_k.$$

Još kažemo da dekompozicija čini *konačni prekrivač* konačnog automata, odnosno transformacijske polugrupe. Zbog propozicija 2.11 i 2.31, svaka kaskadna dekompozicija konačnog automata generira vjenačnu dekompoziciju njegove transformacijske polugrupe.

Vrijedi čak i više: ako znamo kako konstruirati dekompoziciju proizvoljnog konačnog automata, tada će rezultati iz prethodnog poglavlja direktno proizvesti dekompoziciju proizvoljne transformacijske polugrupe. Argumentirajmo ovu tvrdnju. Neka

je $\mathcal{S}$ proizvoljna transformacijska polugrupa. Pretpostavimo da je $\mathcal{M}_1$, $\mathcal{M}_2$, ..., $\mathcal{M}_k$ kaskadna dekompozicija konačnog automata $\mathbf{SM}(\mathcal{S})$, tj. neka postoje kaskadna preslikavanja ω_1, ω_2, ..., ω_{k-1} za koja vrijedi:

$$\mathbf{SM}(\mathcal{S}) \leq \mathcal{M}_1 \, \omega_1 \, \mathcal{M}_2 \, \omega_2 \cdots \omega_{k-1} \, \mathcal{M}_k.$$

Sada redom iz propozicija 2.5, 2.11 i 2.31 doista dobijemo

$$\begin{aligned} \mathcal{S} \cong \mathbf{TS}(\mathbf{SM}(\mathcal{S})) &\leq \mathbf{TS}(\mathcal{M}_1 \, \omega_1 \, \mathcal{M}_2 \, \omega_2 \cdots \omega_{k-1} \, \mathcal{M}_k) \\ &\leq \mathbf{TS}(\mathcal{M}_1) \circ \mathbf{TS}(\mathcal{M}_2) \circ \cdots \circ \mathbf{TS}(\mathcal{M}_k). \end{aligned}$$

U nastavku ćemo pokazati da za svaki konačni automat uistinu postoji kanonska kaskadna dekompozicija koja se sastoji od „jednostavnih" automata. Precizirajmo koje automate smatramo jednostavnima. Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Za proizvoljni $\sigma \in \Sigma$, razmotrimo učinak parcijalne funkcije $F_\sigma \colon Q \rightharpoonup Q$. Dva su moguća ekstremna slučaja s obzirom na veličinu slike ove funkcije:

- slika je jednočlani skup $\{ q \}$, za neki $q \in Q$ — funkciju F_σ tada nazivamo *reset automata* $\mathcal{M}$, ili
- slika je cijeli skup Q — funkcija F_σ je u ovom slučaju bijekcija, odnosno permutacija skupa Q i nazivamo je *permutacija automata* $\mathcal{M}$.

Ovi nazivi opisuju ponašanje automata $\mathcal{M}$ prilikom čitanja ulaza σ. Ako su sve funkcije F_σ reseti, konačni automat $\mathcal{M}$ nazivamo *reset automat*. U slučaju da su sve funkcije F_σ permutacije, konačni automat $\mathcal{M}$ nazivamo *permutacijski automat*. Kasnije ćemo obrazložiti zašto upravo ove dvije vrste automata smatramo jednostavnima. Do njih ćemo doći preko hibridnih automata, u kojima su sve funkcije F_σ ili permutacije ili reseti. Takav automat $\mathcal{M}$ nazivamo *reset-permutacijski* automat.

3.1 Dopustive relacije i particije

Prisjetimo se dekompozicijskih rezultata iz teorije grupa. Uobičajeni put kojim smo do njih dolazili vodi preko normalnih podgrupa. One definiraju particije grupe koje i same možemo organizirati u strukturu grupe. Time dobijemo drugi faktor dekompozicije (prvi je polazna podgrupa). U ovom odjeljku oponašamo ovaj postupak za konačne automate, odnosno transformacijske polugrupe.

Definicija 3.3 (Dopustiva relacija automata)**.** Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Relacija ekvivalencije R na skupu Q naziva se *dopustiva relacija konačnog automata* $\mathcal{M}$ ako za sve $q, q' \in Q$ i $\sigma \in \Sigma$ vrijedi:

$$q \; R \; q' \wedge (qF_\sigma, q'F_\sigma \neq \varnothing) \implies (qF_\sigma) \; R \; (q'F_\sigma). \tag{1}$$

Primijetimo uzgred da je relacija R dopustiva za konačni automat $\mathcal{M}$ ako i samo ako je za svaki $\sigma \in \Sigma$ relacija R bisimulacija okvira (Q, F_σ) sa samim sobom (vidi definiciju 1.4).

Ponovno kao u raspravi nakon definicije 2.1, za dopustive relacije vrijedi implikacija analogna (1) ako umjesto znaka $\sigma \in \Sigma$ stavimo bilo koju riječ $w \in \Sigma^+$. Doista, za $w = \sigma_1\sigma_2 \cdots \sigma_k \in \Sigma^+$ imamo:

$$\begin{aligned} q\ R\ q' &\implies (qF_{\sigma_1})\ R\ (q'F_{\sigma_1}) \implies (qF_{\sigma_1}F_{\sigma_2})\ R\ (q'F_{\sigma_1}F_{\sigma_2}) \\ &\implies \cdots \implies (qF_{\sigma_1}F_{\sigma_2}\cdots F_{\sigma_k})\ R\ (q'F_{\sigma_1}F_{\sigma_2}\cdots F_{\sigma_k}) \iff (qF_w)\ R\ (q'F_w). \end{aligned}$$

Definicija 3.4. Neka je $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ transformacijska polugrupa. Relacija ekvivalencije R na skupu X naziva se *dopustiva relacija transformacijske polugrupe* $\mathcal{S}$ ako za sve $x, x' \in X$ i $s \in S$ vrijedi:

$$x\ R\ x' \wedge (x \cdot_{\mathcal{S}} s, x' \cdot_{\mathcal{S}} s \neq \varnothing) \implies (x \cdot_{\mathcal{S}} s)\ R\ (x' \cdot_{\mathcal{S}} s). \tag{2}$$

Prisjetimo se relacija kongruencije na polugrupama iz odjeljka 1.3. Vidimo da su dopustive relacije analogoni ovih relacija na konačnim automatima i transformacijskim polugrupama.

Većina koncepata koje uvedemo dualno za konačne automate i transformacijske polugrupe bit će invarijantni na prijelaz s jedne strukture na drugu. Primjer takve invarijantnosti je sljedeća lema. Primjetimo da su njom iskazane dvije tvrdnje, što opravdava „recikliranje" simbola.

Lema 3.5. *Neka je $\mathcal{M}$ konačni automat i R njegova dopustiva relacija. Tada je R dopustiva relacija i njegove transformacijske polugrupe* $\mathbf{TS}(\mathcal{M})$.

Dualno, neka je $\mathcal{S}$ transformacijska polugrupa i R njena dopustiva relacija. Tada je R dopustiva relacija i njenog konačnog automata $\mathbf{SM}(\mathcal{S})$.

Dokaz. Neka je $\mathcal{M} = (Q, \Sigma, F)$. Vrijedi $\mathbf{TS}(M) = (Q, \mathbf{S}(\mathcal{M}), \cdot_{\mathcal{M}})$. Uzmimo $q, q' \in Q$ takve da vrijedi $q\ R\ q'$. Neka je $s = [w] \in \mathbf{S}(\mathcal{M})$ takav da vrijedi $q \cdot_{\mathcal{M}} s, q' \cdot_{\mathcal{M}} s \neq \varnothing$. Iz ovoga slijedi i $qF_w, q'F_w \neq \varnothing$. Već smo istaknuli da je implikacija analogna (1) istinita za riječ $w \in \Sigma^+$. Stoga imamo $(qF_w)\ R\ (q'F_w)$. Ovo je pak ekvivalentno s $(q \cdot s)\ R\ (q' \cdot s)$. Analogno se dokaže i druga tvrdnja. □

Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Za proizvoljne $\sigma \in \Sigma$ i $A \subseteq Q$ definiramo skup

$$A\,F_\sigma := F_\sigma(A) = \{\, qF_\sigma \colon q \in A \text{ i } qF_\sigma \neq \varnothing \,\} \subseteq Q.$$

Ovu definiciju možemo proširiti i na sve $w \in \Sigma^+$, tako da vrijedi:

$$A\,F_w := \{\, qF_w \colon q \in A \text{ i } qF_w \neq \varnothing \,\} \subseteq Q.$$

Definicija 3.6 (Dopustiva particija automata)**.** Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Particija π skupa Q naziva se *dopustiva particija konačnog automata* $\mathcal{M}$ ako za sve $A \in \pi$ i $\sigma \in \Sigma$ postoji blok $B \in \pi$ takav da vrijedi $A\,F_\sigma \subseteq B$.

Napomena. Analogno kao gore, u prethodnoj definiciji umjesto znaka σ može stajati bilo koja riječ $w \in \Sigma^+$.

Neka je $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ transformacijska polugrupa. Analogno kao kod automata, za proizvoljne $s \in S$ i $A \subseteq X$ definiramo $A\,s := \{\, x \cdot_{\mathcal{S}} s \colon x \in A \text{ i } x \cdot_{\mathcal{S}} s \neq \varnothing \,\} \subseteq X$.

Definicija 3.7. Neka je $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ transformacijska polugrupa. Particija π skupa X naziva se *dopustiva particija transformacijske polugrupe* $\mathcal{S}$ ako za sve $A \in \pi$ i $s \in S$ postoji blok $B \in \pi$ takav da vrijedi $A\,s \subseteq B$.

Kao što je očekivano, dopustive relacije generiraju dopustive particije, i obratno.

Lema 3.8. *Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Relacija ekvivalencije R na skupu Q je dopustiva relacija automata $\mathcal{M}$ ako i samo ako je particija $\pi = Q/R$ dopustiva particija automata $\mathcal{M}$.*

Dualno, neka je $\mathcal{S} = (X, S, \cdot_{\mathcal{S}})$ transformacijska polugrupa. Relacija ekvivalencije R na skupu X je dopustiva relacija transformacijske polugrupe $\mathcal{S}$ ako i samo ako je particija $\pi = X/R$ dopustiva particija transformacijske polugrupe $\mathcal{S}$.

Dokaz. Dokazujemo samo tvrdnju za automate, jer je dokaz druge tvrdnje analogan.

$\boxed{\Rightarrow}$ Neka je R dopustiva relacija automata $\mathcal{M}$. Uzmimo proizvoljne $\sigma \in \Sigma$ i $A \in \pi$. Trebamo pokazati da postoji $B \in \pi$ takav da $A\,F_\sigma \subseteq B$. U slučaju da vrijedi $A\,F_\sigma = \emptyset$, možemo proizvoljno odabrati $B \in \pi$. U suprotnom, uzmimo $q \in A$ takav da je $qF_\sigma \neq \varnothing$. Neka je $B \in \pi$ blok particije kojem pripada element qF_σ. Pokažimo da za ovaj izbor vrijedi tražena inkluzija.

Neka je $q' \in A$ takav da $q'F_\sigma \neq \varnothing$ proizvoljan. Elementi q i q' pripadaju istoj klasi ekvivalencije relacije R, dakle $q\ R\ q'$. Relacija R je dopustiva i po izboru znamo da vrijedi $qF_\sigma \neq \varnothing$ i $q'F_\sigma \neq \varnothing$. Dakle, slijedi $(qF_\sigma)\ R\ (q'F_\sigma)$. Ovo upravo znači da elementi qF_σ i $q'F_\sigma$ pripadaju istoj klasi ekvivalencije, odnosno istom bloku B particije π.

$\boxed{\Leftarrow}$ Direktno iz definicije relacije ekvivalencije pridružene particiji. □

Sada kao jednostavnu posljedicu lema 3.5 i 3.8 dobijemo i sljedeći rezultat.

Korolar 3.9. *Neka je $\mathcal{M}$ konačni automat i π njegova dopustiva particija. Tada je π dopustiva particija i njegove transformacijske polugrupe $\mathbf{TS}(\mathcal{M})$.*

Dualno, neka je $\mathcal{S}$ transformacijska polugrupa i π njena dopustiva particija. Tada je π dopustiva particija i njenog konačnog automata $\mathbf{SM}(\mathcal{S})$.

3.2 Kvocijentne strukture

Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat i π njegova dopustiva particija. Zbog moguće nepotpunosti automata $\mathcal{M}$, za neke $A \in \pi$ i $\sigma \in \Sigma$ skup $A\,F_\sigma$ može biti prazan. Tada blok $B \in \pi$ takav da vrijedi $A\,F_\sigma \subseteq B$ očito postoji, ali nije jedinstven. Ako pak skup $A\,F_\sigma$ nije prazan, ovaj izbor je nužno jedinstven, zbog disjunktnosti blokova particije.

Definicija 3.10 (Kvocijentni konačni automat)**.** Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat i π njegova dopustiva particija. Definiramo parcijalnu funkciju $F^\pi \colon \pi \times \Sigma \rightharpoonup \pi$ tako da za sve $A \in \pi$ i $\sigma \in \Sigma$ vrijedi:

$$A\,F^\pi_\sigma := F^\pi(A, \sigma) = \begin{cases} B, \text{ ako je } A\,F_\sigma \neq \emptyset \text{ i } B \in \pi \text{ takav da } A\,F_\sigma \subseteq B; \\ \varnothing, \text{ inače} \end{cases}.$$

Konačni automat $\mathcal{M}/\pi = (\pi, \Sigma, F^\pi)$ nazivamo *kvocijentni konačni automat od* $\mathcal{M}$ *s obzirom na particiju* π ili π*-faktor automata* $\mathcal{M}$.

Dualna definicija kvocijentne strukture za transformacijske polugrupe malo je kompliciranija, jer moramo osigurati da vrijedi svojstvo dosljednosti djelovanja. U tu svrhu, uvodimo kongruenciju na polugrupi i promatramo njenu kvocijentnu polgrupu. Konačno dobijemo sljedeću definiciju.

Definicija 3.11. Neka je $\mathcal{S} = (X, S, \cdot_S)$ transformacijska polugrupa i π njena dopustiva particija. Definiramo najprije parcijalnu funkciju $\cdot_\pi \colon \pi \times S \rightharpoonup \pi$ tako da za sve $A \in \pi$ i $s \in S$ vrijedi:

$$A \cdot_\pi s = \begin{cases} B, \text{ ako je } A\,s \neq \emptyset \text{ i } B \in \pi \text{ takav da } A\,s \subseteq B; \\ \varnothing, \text{ inače} \end{cases}.$$

Sada definiramo kongruenciju $\approx$ na polugrupi S tako da za sve $s, s' \in S$ vrijedi

$$s \approx s' \iff (\forall A \in \pi)\ A \cdot_\pi s = A \cdot_\pi s'.$$

Djelovanje polugrupe $S/\!\approx$ na skup π označavamo s $\cdot_{\langle\pi\rangle}$ i definiramo tako da za sve $[s] \in S/\!\approx$ i $A \in \pi$ vrijedi $A \cdot_{\langle\pi\rangle} [s] := A \cdot_\pi s$. Transformacijsku polugrupu $\mathcal{S}/\langle\pi\rangle = (\pi, S/\!\approx, \cdot_{\langle\pi\rangle})$ nazivamo *kvocijentna transformacijska polugrupa* od $\mathcal{S}$ s obzirom na particiju π.

Kvocijentni konačni automati i transformacijske polugrupe definirani su analogno kao i kvocijentne polugrupe iz odjeljka 1.3. Stoga će vrijediti i analogni rezultati, uz analogan dokaz. Primjerice, sljedeća lema iskazuje rezultat analogan postojanju kanonskog epimorfizma između polugrupe i njene kvocijentne polugrupe.

Lema 3.12. *Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat i π njegova dopustiva particija. Prisjetimo se kanonske surjekcije $\varphi_\pi \colon Q \to \pi$ na particiju (vidi odjeljak 1.1). Par (φ_π, I_Σ) je epimorfizam konačnih automata $\mathcal{M}$ i $\mathcal{M}/\pi$, koji nazivamo* kanonski epimorfizam na $\mathcal{M}/\pi$.

Već smo istaknuli analogiju između dopustivih relacija konačnih automata (transformacijskih polugrupa) i relacija kongruencije na polugrupama. Nakon uvođenja kvocijentnih struktura, u stanju smo izreći rezultat o povezanosti homomorfizama i dopustivih relacija, u duhu propozicije 1.26.

Propozicija 3.13. *Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat i R relacija na skupu Q. Relacija R je dopustiva za automat $\mathcal{M}$ ako i samo ako postoji konačni automat $\mathcal{N}$ i homomorfizam automata $(\alpha, \beta) : \mathcal{M} \to \mathcal{N}$ takav da za sve $q, q' \in Q$ vrijedi:*

$$q \; R \; q' \iff \alpha(q) = \alpha(q'). \tag{3}$$

Zanimljivo je istaknuti i sljedeći rezultat o odnosu kvocijentnih struktura i operacije **TS**.

Lema 3.14. *Neka je $\mathcal{M}$ konačni automat i π njegova dopustiva particija. Tada vrijedi:*

$$\mathbf{TS}\,(\mathcal{M}/\pi) \cong \mathbf{TS}\,(\mathcal{M})/\langle\pi\rangle.$$

Dokaz. Neka je $\mathcal{M} = (Q, \Sigma, F)$. Tada vrijedi $\mathbf{TS}\,(\mathcal{M}/\pi) = (\pi, \mathbf{S}\,(\mathcal{M}/\pi), \cdot_{\mathcal{M}/\pi})$ i $\mathbf{TS}\,(\mathcal{M})/\langle\pi\rangle = (\pi, \mathbf{S}\,(\mathcal{M})/\!\approx, \cdot_{\langle\pi\rangle})$. Neka je $\beta \colon \mathbf{S}\,(\mathcal{M}/\pi) \to \mathbf{S}\,(\mathcal{M})/\!\approx$ funkcija takva da za sve $[w]_{\equiv_{\mathcal{M}/\pi}} \in \mathbf{S}\,(\mathcal{M}/\pi)$ vrijedi $\beta([w]_{\equiv_{\mathcal{M}/\pi}}) = [[w]_{\equiv_{\mathcal{M}}}]_{\approx}$. Pokaže se da je β dobro definirani izomorfizam polugrupa. Konačno je (I_π, β) traženi izomorfizam transformacijskih polugrupa. □

Dekompozicije automata na početku poglavlja definirali smo isključivo za produkte koji odgovaraju serijskom spoju Mealyjevih automata. Dakako, moguće je promatrati i dekompozicije bazirane na paralelnom spoju, ali ttakva bi teorija bila ponešto uža (usporedi lemu 2.25). Predstavit ćemo jedan rezultat koji ilustrira ovakav način rastava automata. On će se pokazati korisnim za rastav vrlo jednostavnih automata (vidi teorem 3.22).

Definicija 3.15. Neka je X proizvoljan skup. Neka su π i ρ particije od X takve da za sve $A \in \pi$ i $B \in \rho$ vrijedi $|A \cap B| \leq 1$. Kažemo da su particije π i ρ *ortogonalne*.

Propozicija 3.16. *Neka je $\mathcal{M}$ konačni automat. Neka su π i ρ ortogonalne dopustive particije od $\mathcal{M}$. Tada vrijedi:*

$$\mathcal{M} \leq \mathcal{M}/\pi \times \mathcal{M}/\rho.$$

Dokaz. Označimo $\mathcal{M} = (Q, \Sigma, F)$ te $\mathcal{M}/\pi = (\pi, \Sigma, F^\pi)$ i $\mathcal{M}/\rho = (\rho, \Sigma, F^\rho)$. Neka je funkcija $\nu\colon \Sigma \to \Sigma \times \Sigma$ takva da za sve $\sigma \in \Sigma$ vrijedi $\nu(\sigma) = (\sigma, \sigma)$. Neka je parcijalna funkcija $\mu\colon \pi \times \rho \rightharpoonup Q$ zadana za sve $(A, B) \in \pi \times \rho$ sa

$$\mu(A, B) = \begin{cases} q, \text{ ako } A \cap B = \{\, q \,\}; \\ \varnothing, \text{ ako } A \cap B = \emptyset \end{cases} .$$

Kako su particije π i ρ ortogonalne, μ je dobro definirana. Provjerimo da je (μ, ν) traženi prekrivač. Za $(A, B) \in \pi \times \rho$ takve da $A \cap B = \{\, q \,\}$ i proizvoljni $\sigma \in \Sigma$ vrijedi:

$$\begin{aligned} \mu((A, B)\,(F^\pi \times F^\rho)_{\nu(\sigma)}) &= \mu(A\,F^\pi_{\nu(\sigma)}, BF^\rho_{\nu(\sigma)}) = \mu(\varphi_\pi(q)F^\pi_\sigma, \varphi_\rho(q)F^\rho_\sigma) \\ &= \mu(\varphi_\pi(qF_\sigma), \varphi_\rho(qF_\sigma)) = qF_\sigma = \mu(A, B)F_\sigma. \end{aligned}$$ □

Uvjerili smo se da pomoću particije konačnog automata možemo definirati kvocijentni objekt, također sa strukturom konačnog automata. Situacija je dakle analogna već spomenutom slučaju normalnih podgrupa iz teorije grupa. Ovo je znak da smo spremni dokazati prvi kaskadni dekompozicijski rezultat u teoriji konačnih automata. Kao izvor koristimo [8, teorem 3.3.1].

Za particiju π proizvoljnog skupa X označimo s $\max(\pi)$ maksimalni broj elemenata u svim blokovima particije π, tj. $\max(\pi) = \max\{\, |A| \colon A \in \pi \,\}$. Očito vrijedi $1 \leq \max(\pi) \leq |X|$, dok se jednakosti postižu samo za trivijalne particije. *Veličinu automata* $\mathcal{M} = (Q, \Sigma, F)$, u oznaci $|\mathcal{M}|$, definiramo kao broj njegovih stanja.

Teorem 3.17. *Neka je $\mathcal{M}$ konačni automat i π njegova dopustiva particija. Tada postoji konačni automat $\mathcal{M}'$ takav da vrijedi $|\mathcal{M}'| = \max(\pi)$ i*

$$\mathcal{M} \leq \mathcal{M}'\,\omega\,(\mathcal{M}/\pi)\,.$$

Dokaz. Neka je $\mathcal{M} = (Q, \Sigma, F)$. Uvijek možemo pronaći particiju ρ skupa Q, ne nužno i dopustivu za automat $\mathcal{M}$, takvu da $|\rho| = \max(\pi)$ i koja je ortogonalna particiji π. Doista, neka je skup $\{\, q_1, q_2, \ldots, q_M \,\} \subseteq Q$ element particije π s maksimalnim brojem elemenata, gdje smo označili $M = \max(\pi)$. Tada particiju $\rho = \{\, B_1, B_2, \ldots, B_M \,\}$ konstruiramo na sljedeći način. Redom za $j = 1, 2, \ldots, M$ stavimo q_j u skup B_j, zajedno s po jednim elementom iz svih ostalih članova particije π koje već nismo ispraznili.

Neka je $F'\colon \rho \times (\pi \times \Sigma) \rightharpoonup \rho$ parcijalna funkcija takva da za sve $B \in \rho$ i $(A, \sigma) \in \pi \times \Sigma$ vrijedi:

$$BF'_{(A,\sigma)} := F'(B, (A, \sigma)) = \begin{cases} \varphi_\rho(qF_\sigma), \text{ ako } A \cap B = \{\, q \,\}, \\ \varnothing, \text{ inače.} \end{cases}$$

Tvrdimo da je $\mathcal{M}' = (\rho, \pi \times \Sigma, F')$ traženi konačni automat. Po definiciji kaskadnog produkta vrijedi $\mathcal{M}' \,\omega\, (\mathcal{M}/\pi) = (\rho \times \pi, \Sigma, F' \,\omega\, F^{\pi})$, gdje za sve $(B, A) \in \rho \times \pi$ i $\sigma \in \Sigma$ imamo:

$$(B, A)\,(F' \,\omega\, F^{\pi})_{\sigma} = (G\,(B, (A, \sigma))\,, F^{\pi}(A, \sigma))\,.$$

Definiramo parcijalnu funkciju $\mu\colon \rho \times \pi \rightharpoonup Q$ tako da za svaki $(B, A) \in \rho \times \pi$ vrijedi:

$$\mu(B, A) = \begin{cases} q, \text{ ako } B \cap A = \{\, q \,\}\,; \\ \varnothing, \text{ ako } B \cap A = \emptyset \end{cases} .$$

Za sve $(B, A) \in \rho \times \pi$ takve da $B \cap A = \{\, q \,\}$ i sve $\sigma \in \Sigma$ vrijedi:

$$\begin{aligned} \mu((B, A)\,(F' \,\omega\, F^{\pi})_{\sigma}) &= \mu((F'(B, (A, \sigma)), F^{\pi}(A, \sigma))) \\ &= \mu((\varphi_{\rho}(qF_{\sigma}), \varphi_{\pi}(qF_{\sigma}))) = qF_{\sigma} = \mu(B, A)F_{\sigma}. \end{aligned}$$

Zaključujemo da je (μ, I_{Σ}) traženi prekrivač. □

3.3 Reset-permutacijski prekrivači

Na početku poglavlja definirali smo *reset-permutacijske automate* kao hibride između jednostavnih reset i permutacijskih automata. U ovom odjeljku istražujemo kako se ovi automati prirodno pojavljuju kao elementi dekompozicije proizvoljnog konačnog automata. Najprije trebamo proširiti raspravu o dopustivim particijama iz odjeljka 3.1 na dekompozicije skupa (vidi definiciju 1.3).

Definicija 3.18. Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat. Dekompozicija δ skupa stanja Q naziva se *dopustivom za automat* $\mathcal{M}$ ako za sve $A \in \delta$ i $\sigma \in \Sigma$ postoji $B \in \delta$ takav da vrijedi $A\,F_{\sigma} \subseteq B$.

Primjetimo da u prethodnoj definiciji izbor od $B \in \delta$ ne mora biti jedinstven, čak niti u slučaju da je $A\,F_{\sigma} \neq \emptyset$ (usporedi raspravu s početka odjeljka 3.2). Općenito će stoga postojati više od jedne parcijalne funkcije $F^{\delta}\colon \delta \times \Sigma \rightharpoonup \delta$ takve da za sve $A \in \delta$ i $\sigma \in \Sigma$ vrijedi $A\,F^{\delta}_{\sigma} := F^{\delta}(A, \sigma) = B$, gdje je B neki takav da $A\,F_{\sigma} \subseteq B$. Konačni automat $\mathcal{M}/\delta = (\delta, \Sigma, F^{\delta})$ nazivamo *kvocijentni automat od* $\mathcal{M}$ *s obzirom na dekompoziciju* δ ili δ*-faktor automata* $\mathcal{M}$[1].

Ova rasprava ukazuje da je jednostavnije baratati s particijama nego s dekompozicijama. Zato ćemo sada opisati postupak kojim za dane konačni automat i dopustivu

[1]Ovdje nailazimo na nejednoznačnost sličnu kao kod indeksa parcijalno-rekurzivne funkcije. Koristimo analogni dogovor onome iz [24, napomena 3.56]. Dakle kada kažemo kvocijentni automat s obzirom na dekompoziciju, mislimo na proizvoljno odabran, fiksirani automat s ovim svojstvom.

dekompoziciju konstruiramo novi konačni automat s dopustivom particijom. Postupak je baziran na standardnom zahvatu *disjunktifikacije* iz teorije skupova (usporedi [19, definicija 1.44.]).

Neka je $\mathcal{M} = (Q, \Sigma, F)$ konačni automat, δ njegova dopustiva dekompozicija i $\mathcal{M}/\delta = (\delta, \Sigma, F^\delta)$ kvocijentni automat od $\mathcal{M}$ s obzirom na dekompoziciju δ. Definiramo skup

$$Q^* = \{\, (q, A) \in Q \times \delta \colon A \in \delta \text{ i } q \in A \,\}.$$

Uočimo da smo ovim „dupli\-cirali" stanja iz Q. Neka je preslikavanje $F^* \colon Q^* \times \Sigma \to Q^*$ zadano tako da za sve $(q, A) \in Q^*$ i $\sigma \in \Sigma$ vrijedi $(q, A)\, F^*_\sigma = (qF_\sigma, A\, F^\delta_\sigma)$. Definicija je dobra, tj. doista vrijedi $(q, A)\, F^*_\sigma \in Q^*$, jer je $qF_\sigma \in A\, F^\delta_\sigma$ po definiciji funkcije F^δ. Definiramo automat $\mathcal{M}^* = (Q^*, \Sigma, F^*)$. Istaknimo par njegovih značajnih svojstava.

(*i*) Definiramo $\delta^* = \{\, \{\, (q, A) : q \in A \,\} : A \in \delta \,\}$, tj. skup podskupova od Q^* koji se sastoje od parova s istom drugom koordinatom. Primijetimo da je δ^* particija skupa Q^*. Štoviše, lagano se vidi da je ovo dopustiva particija. Nadalje, vrijedi $\max(\delta^*) = \max(\delta)$. Konačno, kvocijenti automat $\mathcal{M}^*/\delta^*$ izomorfan je s odabranim kvocijentnim automatom $\mathcal{M}/\delta$. Naime, skup δ^* je kanonski bijektivan skupu δ, dok je funkcija F^* direktno izvedena iz funkcije F^δ.

(*ii*) Pokažimo da automat $\mathcal{M}^*$ doista prekriva automat $\mathcal{M}$. Neka je $\mu \colon Q^* \to Q$ zadana tako da za sve $(q, H_i) \in Q^*$ vrijedi $\mu(q, H_i) = q$. Funkcija μ je očito surjektivna te za sve $(q, A) \in Q^*$ i $\sigma \in \Sigma$ vrijedi:

$$\mu((q, H_i)\, F^*_\sigma) = \mu(qF_\sigma, H_i F^\delta_\sigma) = qF_\sigma = \mu(q, A)F_\sigma.$$

Sada iz teorema 3.17 dobijemo sljedeći rezultat.

Korolar 3.19. *Neka je $\mathcal{M}$ konačni automat, δ njegova dopustiva dekompozicija i $\mathcal{M}/\delta$ kvocijentni automat od $\mathcal{M}$ s obzirom na δ. Tada postoji konačni automat $\mathcal{M}'$ takav da vrijedi $|\mathcal{M}'| = \max(\delta)$ i*

$$\mathcal{M} \leq \mathcal{M}'\, \omega\, (\mathcal{M}/\delta)\,.$$

Prelazimo na konstrukciju reset-permutacijskog prekrivača. Neka je $\mathcal{M} = (Q, \Sigma, F)$ proizvoljan konačni automat i označimo $n = |\mathcal{M}| = |Q|$. Uzmimo dekompoziciju δ skupa Q koja se sastoji od svih podskupova od Q koji imaju točno $(n-1)$ elemenata. Budući da za sve $A \in \pi$ i $\sigma \in \Sigma$ vrijedi $|A\, F_\sigma| \leq |A|$, slijedi da je ova dekompozicija dopustiva za automat $\mathcal{M}$. Dakle, po korolaru 3.19 možemo pronaći konačni automat $\mathcal{M}'$ takav da vrijedi $\mathcal{M} \leq \mathcal{M}'\, \omega\, (\mathcal{M}/\delta)$. Primjetimo da vrijedi

$$|\mathcal{M}'| = \max(\delta) = n - 1 < |\mathcal{M}|.$$

Analizirajmo detaljnije konačni sautomat $\mathcal{M}/\delta = (\delta, \Sigma, F^\delta)$. Uzmimo proizvoljni $\sigma \in \Sigma$ i promotrimo skup $QF_\sigma = F_\sigma(Q)$, dakle skup stanja u koja možemo doći u originalnom automatu $\mathcal{M}$ prilikom čitanja znaka σ. Razlikujemo sljedeća dva slučaja.

(i) Ako vrijedi $|QF_\sigma| < n$, tada postoji $B \in \delta$ takav da $QF_\sigma \subseteq B$. Tada za sve $A \in \delta$ vrijedi $A\,F_\sigma \subseteq QF_\sigma \subseteq BF_\sigma$. Ovo dalje povlači $A\,F_\sigma^\delta = B$, za sve $A \in \delta$. Dakle, znak σ je **reset** automata $\mathcal{M}/\delta$.

(ii) U suprotnom je $QF_\sigma = Q$, dakle znak σ je permutacija početnog automata $\mathcal{M}$. Tada za sve $A \in \delta$ postoji $B \in \delta$ takav da $A\,F_\sigma = B$ (jednakost umjesto inkluzije, zbog kardinalnosti skupova). Štoviše, za $A, A' \in \delta$ takve da je $A \neq A'$ vrijedi $A\,F_\sigma \neq A'\,F_\sigma$, jer se A i A' razlikuju barem u po jednom elementu, koji imaju drukčiju sliku pod permutacijom F_σ. Zaključujemo da je znak σ **permutacija** i automata $\mathcal{M}/\delta$.

Zaključujemo da je konačni automat $\mathcal{M}/\delta$ **reset-permutacijski** automat.

Sada možemo isti postupak primjeniti na automat $\mathcal{M}'$, počevši s odgovarajućom dekompozicijom δ'. Zaključujemo da postoji automat $\mathcal{M}''$ takav da $|\mathcal{M}''| < |\mathcal{M}'|$ za koji vrijedi $\mathcal{M}' \leq \mathcal{M}'' \,\omega\, (\mathcal{M}'/\delta')$. Iz toga, po lemi 2.32 i tranzitivnosti relacije prekrivanja, slijedi $\mathcal{M} \leq \mathcal{M}'' \,\omega\, (\mathcal{M}'/\delta') \,\omega\, (\mathcal{M}/\delta)$, gdje su oba kvocijentna automata $\mathcal{M}/\delta$ i $\mathcal{M}'/\delta'$ reset-permutacijski automati. Nastavljajući ovu proceduru, dobijemo sljedeći značajni rezultat.

Teorem 3.20 (Reset-permutacijski prekrivač)**.** *Neka je $\mathcal{M}$ konačni automat i označimo $n = |\mathcal{M}|$. Tada se $\mathcal{M}$ može prekriti kaskadnim produktom od najviše $(n-1)$ reset-permutacijskih automata.*

Dokaz. Sve važno je već dokazano u prethodnoj raspravi. Ostaje istaknuti da je automat s dva stanja trivijalno reset-permutacijski, zbog čega je potrebno najviše $(n-1)$ automata ove vrste. Naravno, može se dogoditi da je već neki od ranijih automata u procesu reset-permutacijski, pa imamo manje od $(n-1)$ automata. □

3.4 Rastavi reset i permutacijskih automata

Kako i samo ime govori, reset-permutacijski automat prirodno se sastoji od dva pod-automata: jednog reset i jednog permutacijskog. Sljedeći teorem precizira sastav i prirodu ovih pod-automata.

Teorem 3.21 (Rastav reset-permutacijskog automata)**.** *Neka je $\mathcal{M}$ reset-permutacijski automat. Postoje reset automat $\mathcal{R}$ i permutacijski automat $\mathcal{P}$ takvi da vrijedi*

$$\mathcal{M} \leq \mathcal{R}^\cdot \,\omega\, \mathcal{P}.$$

Dokaz. Neka je $\mathcal{M} = (Q, \Sigma, F)$. Definiramo skupove $\Sigma^R = \{\, \sigma \in \Sigma \colon |QF_\sigma| = 1 \,\}$ i $\Sigma^P = \{\, \sigma \in \Sigma \colon QF_\sigma = Q \,\}$, dakle redom skup svih reset i permutacijskih ulaza za automat $\mathcal{M}$. Jasno, skupovi Σ^R i Σ^P su disjunktni te kako je $\mathcal{M}$ reset-permutacijski automat, vrijedi $\Sigma = \Sigma^R \cup \Sigma^P$.

Neka su $\equiv$ i $\mathbf{S}(\mathcal{M})$ redom kongruencija i polugrupa pridružena automatu $\mathcal{M}$. Označimo $\left[\Sigma^P\right] = \left\{\, [\sigma^P]_\equiv \colon \sigma^P \in \Sigma^P \,\right\} \subseteq \mathbf{S}(\mathcal{M})$. Neka je G potpolugrupa od $\mathbf{S}(\mathcal{M})$ generirana skupom $\left[\Sigma^P\right]$ (vidi raspravu nakon definicije 1.19). Dokažimo da je G grupa.

Uzmimo proizvoljni $g \in G$. Po lemi 1.20, vrijedi $g = \prod_{i=1}^{n} [\sigma_i^P]$, gdje je $n \in \mathbb{N}_+$ i za sve $i = 1, 2, \ldots, n$ je $\sigma_i^P \in \Sigma^P$. Tada je $g = [w^P]$, gdje je $w = \sigma_1^P \sigma_2^P \cdots \sigma_n^P$. Za pridruženu funkciju vrijedi $F_{w^P} = F_{\sigma_1^P} F_{\sigma_2^P} \cdots F_{\sigma_n^P}$, dakle je F_{w^P} kompozicija permutacija skupa Q, pa je i sama permutacija. Stoga je red elementa F_w u monoidu $\mathbf{PF}(Q)$ konačan (vidi raspravu nakon definicije 1.16). Zaključujemo da je i red od g konačan u polugrupi $\mathbf{S}(\mathcal{M})$. Zbog definicije potpolugrupe generirane skupom, vrijedi da je i inverz od g također u G.

Definiramo funkciju $F^P \colon G \times \Sigma \to G$ tako da za sve $g = [w^P] \in G$, gdje je $w^P \in (\Sigma^P)^*$, i $\sigma \in \Sigma$ vrijedi:

$$gF_\sigma^P = \begin{cases} [w^P \sigma], \text{ ako } \sigma \in \Sigma^P; \\ g \qquad\quad , \text{ ako } \sigma \in \Sigma^R \end{cases}.$$

Definiramo automat $\mathcal{P} = (G, \Sigma, F^P)$. Za svaki znak $\sigma^R \in \Sigma^R$, funkcija $F_{\sigma^R}^P$ je očito identiteta skupa G, pa posebno i permutacija ovog skupa.

Pokažimo da je za svaki znak $\sigma^P \in \Sigma^P$ pripadajuća funkcija $F_{\sigma^P}^P$ također permutacija skupa Q. Dovoljno je pokazati da je injekcija, zbog konačnosti skupa G. Stoga uzmimo proizvoljne $u^P, v^P \in (\Sigma^P)^*$ i pretpostavimo da vrijedi $[u^P]F_{\sigma^P}^P = [v^P]F_{\sigma^P}^P$. Ovo znači $[u^P \sigma^P] = [v^P \sigma^P]$, što po definiciji množenja u $\mathbf{S}(\mathcal{M})$ povlači $[u^P][\sigma^P] = [v^P][\sigma^P]$. No, $[\sigma^P]$ je element grupe G, što znači da postoji njegov inverzni element. Nakon množenja zadnje jednakosti zdesna s $[\sigma^P]^{-1}$, proizlazi $[u^P] = [v^P]$. Konačno, zaključujemo da je $\mathcal{P}$ permutacijski automat.

Okrećemo se konstrukciji reset automata. Definiramo funkciju prijelaza $F^R \colon Q \times (G \times \Sigma^R) \to Q$ tako da za sve $q \in Q$, $g = [w^P] \in G$ i $\sigma^R \in \Sigma^R$ vrijedi:

$$qF_{(g,\sigma^R)}^R = qF_{w^P} F_{\sigma^R} (F_{w^P})^{-1}.$$

(Kako je ulaz σ^R reset automata $\mathcal{M}$, vrijednost funkcije ostala bi ista bez prve primjene funkcije F_{w^P}. No, ovakva definicija će se kasnije pokazati korisna.) Funkcija F_{w^P} je permutacija skupa Q, pa je $F_{w^P}^{-1}$ dobro definirana. Nadalje, za sve $\sigma^R \in \Sigma^R$ vrijedi $|QF_{\sigma^R}| = 1$, pa onda i za sve $g = [w^P] \in G$ imamo $|QF_{(g,\sigma^R)}^R| = |QF_{\sigma^R} F_{w^P}^{-1}| = 1$. Zaključujemo da je $\mathcal{R} = (Q, G \times \Sigma^R, F^R)$ reset automat.

Neka je $\Lambda \notin G \times \Sigma$ i neka je $\mathcal{R}^\bullet = (Q, (G \times \Sigma^R)^\bullet, F^{R^\bullet})$ monoidni automat iz definicije 1.12 pridružen automatu $\mathcal{R}$, gdje je $(G\times\Sigma^R)^\bullet = (G\times\Sigma^R)\cup\{\,\Lambda\,\}$. Definiramo kaskadno preslikavanje $\omega\colon G \times \Sigma \to (G \times \Sigma^R)^\bullet$ tako da za sve $g \in G$ i $\sigma \in \Sigma$ vrijedi:

$$\omega(g,\sigma) = \begin{cases} \Lambda & \text{, ako } \sigma \in \Sigma^P; \\ (g,\sigma) & \text{, ako } \sigma \in \Sigma^R \end{cases}.$$

Promotrimo kaskadni produkt $\mathcal{R}^\bullet \omega\, \mathcal{P} = (Q \times G, \Sigma, F^\omega)$. Prisjetimo se da je funkcija $F^\omega\colon (Q \times G) \times \Sigma \to Q \times G$ zadana tako da za sve $(q, g) \in Q \times G$ i $\sigma \in \Sigma$ vrijedi:

$$F^\omega_\sigma(q,g) = (qF^{R^\bullet}_{\omega(g,\sigma)}, gF^P_\sigma).$$

Neka je funkcija $\mu\colon Q \times G \to Q$ takva da za sve $(q, g) \in Q \times G$, gdje je $g = [w^P]$ za $w^P \in (\Sigma^P)^*$, vrijedi $\mu(q, g) = qF_{w^P}$. Pokažimo da je (μ, I_Σ) prekrivač početnog automata $\mathcal{M}$ automatom $\mathcal{R}^\bullet \omega\, \mathcal{P}$. Prvo, μ je surjekcija jer je za svaki $w^P \in (\Sigma^P)^*$ funkcija F_{w^P} permutacija skupa Q. Neka su sada $q \in Q$ i $g = [w^P] \in G$ proizvoljni. Za $\sigma^P \in \Sigma^P$ vrijedi:

$$\begin{aligned}\mu((q,g)\,F^\omega_{\sigma^P}) &= \mu(F^{R^\bullet}_{\omega(g,\sigma^P)}(q), F^P_{\sigma^P}(g)) = \mu(F^{R^\bullet}(q,\Lambda), [w^P\sigma^P]) \\ &= \mu(q, [w^P\sigma^P]) = qF_{w^P\sigma^P} = qF_{w^P}F_{\sigma^P} = \mu(q,g)F_{\sigma^P}.\end{aligned}$$

Nadalje, za $\sigma^R \in \Sigma^R$ vrijedi:

$$\begin{aligned}\mu((q,g)\,F^\omega_{\sigma^R}) &= \mu(F^{R^\bullet}_{\omega(g,\sigma^R)}(q), F^P_{\sigma^R}(g)) = \mu(F^{R^\bullet}_{(g,\sigma^R)}(q), g) = \mu(qF_{w^P}F_{\sigma^R}(F_{w^P})^{-1}, g) \\ &= (qF_{w^P}F_{\sigma^R}(F_{w^P})^{-1})F_{w^P} = qF_{w^P}F_{\sigma^R} = \mu(q,g)F_{\sigma^R}.\end{aligned}$$ □

Neka je $\mathcal{R} = (Q, \Sigma, F)$ reset automat i $\mathcal{R}^\bullet = (Q, \Sigma^\bullet, F^\bullet)$ njemu pridruženi monoidni automat. Za sve $\sigma \in \Sigma^\bullet$ je funkcija $F^\bullet_\sigma\colon Q \rightharpoonup Q$ ili reset automata ili identiteta skupa Q. Ovakve automate nazivat ćemo *reset-monoidni*.

Teorem 3.22 (Rastav reset-monoidnog automata)**.** *Neka je $\mathcal{R}$ reset automat. Tada postoji $k \in \mathbb{N}_+$ takav da vrijedi:*

$$\mathcal{R}^\bullet \leq \underbrace{\mathbf{SM}(\,\overline{\mathbf{2}}^\bullet) \times \mathbf{SM}(\,\overline{\mathbf{2}}^\bullet) \times \cdots \times \mathbf{SM}(\,\overline{\mathbf{2}}^\bullet)}_{k\ puta}.$$

Dokaz. Neka je $\mathcal{R} = (Q, \Sigma, F)$. Ključno je uočiti da je svaka particija skupa stanja dopustiva za reset-monoidni automat $\mathcal{R}^\bullet$. Doista, neka je τ proizvoljna particija od Q i $\sigma \in \Sigma^\bullet$. Ako je σ reset automata $\mathcal{R}$, tada za svaki blok $A \in \tau$ vrijedi $|AF^\bullet_\sigma| = 1$,

pa je $A\,F_\sigma$ podskup onog bloka particije τ kojem pripada njegov jedini element. U suprotnom je σ identiteta skupa Q, pa za svaki $A \in \tau$ vrijedi $A\,F_\sigma = A \subseteq A$.

Neka je sada π particija skupa Q koja se sastoji od dva bloka. Kvocijentni automat $\mathcal{R}^\bullet/\pi$ tada ima dva stanja i također je reset-monoidni automat. „Najveći" automat s ovim svojstvom je $\mathbf{SM}(\,\overline{\mathbf{2}}^\bullet\,)$, pa naslućujemo da vrijedi $\mathcal{R}^\bullet/\pi \leq \mathbf{SM}(\,\overline{\mathbf{2}}^\bullet\,)$. Provjerimo formalno ovu slutnju.

Neka je $\pi = \{\, A_0, A_1 \,\}$. Tada je $\mathcal{R}^\bullet/\pi = (\,\pi, \Sigma^\bullet, (F^\bullet)^\pi\,)$. Definiramo funkciju $\nu\colon \Sigma^\bullet \to \mathbb{N}_2$ tako da za sve $\sigma \in \Sigma$ vrijedi:

$$\nu(\sigma) = \begin{cases} \overline{0}, \text{ ako je } \sigma \text{ reset s vrijednošću } A_0; \\ \overline{1}, \text{ ako je } \sigma \text{ reset s vrijednošću } A_1; \\ I_{\mathbf{2}}, \text{ ako je } \sigma \text{ identiteta.} \end{cases}$$

Surjekcija $\mu\colon \mathbb{N}_2 \to \pi$ dana je s $\mu(n) = A_n$. Očito je par (μ, ν) prekrivač automata $\mathcal{R}^\bullet$ automatom $\mathbf{SM}(\,\overline{\mathbf{2}}^\bullet\,)$.

Pokažimo sada da možemo pronaći particiju ρ skupa Q ortogonalnu s $\pi = \{\, A_0, A_1 \,\}$ (vidi definiciju 3.15). Blokove particije ρ konstruiramo sljedećom procedurom. U prvi bloku stavimo po jedan element iz skupova A_0 i A_1. U drugi blok stavimo ponovno po jedan element iz skupova A_0 i A_1 koje nismo do sada iskoristili, ako takvih ima. U suprotnom, preostale elemente stavimo u jednočlane blokove. Rezultirajuća particija ρ je po konstrukciji netrivijalna i ortogonalna s π.

Po prijašnjem zapažanju, particija ρ je također dopustiva za automat $\mathcal{R}^\bullet$. Stoga možemo primijeniti propoziciju 3.16 kako bi zaključili da vrijedi $\mathcal{R}^\bullet \leq (\mathcal{R}^\bullet/\pi) \times (\mathcal{R}^\bullet/\rho)$. Zbog $\mathcal{R}^\bullet/\pi \leq \mathbf{SM}(\,\overline{\mathbf{2}}^\bullet\,)$ i rezultata analognog lemi 2.32, zaključujemo da vrijedi $\mathcal{R}^\bullet \leq \mathbf{SM}(\,\overline{\mathbf{2}}^\bullet\,) \times (\mathcal{R}^\bullet/\rho)$.

Kvocijentni konačni automat $\mathcal{R}^\bullet/\rho$ također jest reset-monoidni, pa ovaj postupak možemo dalje primjeniti na njemu. Nastavljajući na isti način dobijemo željeni rastav reset-monoidnog automata. □

Neka je $\mathcal{P} = (Q, \Sigma, F)$ permutacijski automat. Tada je za sve $\sigma \in \Sigma$ preslikavanje $F_\sigma\colon Q \to Q$ permutacija skupa Q. Kao u dokazu teorema 3.21, vidi se da je polugrupa $\mathbf{S}\,(\mathcal{P}) \cong \mathbf{F}(\mathcal{P})$ ustvari **grupa**.

Grupa $\mathbf{F}(\mathcal{P})$ jest podgrupa grupe svih permutacija konačnog skupa Q, koju označavamo s G. Definirajmo transformacijsku grupu $\mathcal{G} = (G, G, \cdot_{\mathcal{G}})$. Djelovanje $\cdot_{\mathcal{G}}$ je množenje zdesna u grupi G i kao takvo je dosljedno (zbog postojanja inerza). Pridruženi konačni automat $\mathbf{SM}\,(\mathcal{G}) = (G, G, F^{\mathcal{G}})$ zvat ćemo *grupoidni automat*.

Lema 3.23. *Neka je $\mathcal{P}$ permutacijski automat. Neka je $\mathcal{G}$ kao gore. Tada vrijedi:*

$$\mathcal{P} \leq \mathbf{SM}\,(\mathcal{G})\,.$$

Dokaz. Označimo $\mathcal{P} = (Q, \Sigma, F)$ i $\mathbf{SM}(\mathcal{G}) = (G, G, F^{\mathcal{G}})$. Fiksirajmo proizvoljni $q_0 \in Q$. Definirajmo funkciju $\mu\colon G \to Q$ tako da za sve permutacije $g \in G$ vrijedi $\mu(g) = g(q_0)$. Funkcija μ je očito surjektivna. Neka je $\nu\colon \Sigma \to G$ funkcija takva da za sve $\sigma \in \Sigma$ vrijedi $\nu(\sigma) = F_\sigma$.

Pokažimo da je (μ, ν) traženi prekrivač. Neka su $g \in G$ i $\sigma \in \Sigma$ proizvoljni. Vrijedi:

$$\begin{aligned}\mu\left(gF^{\mathcal{G}}_{\nu(\sigma)}\right) &= \mu\left(gF^{\mathcal{G}}_{F_\sigma}\right) = \mu\left(g \cdot_{\mathcal{G}} F_\sigma\right) = \mu\left(g \cdot_G F_\sigma\right) \\ &= \mu\left(F_\sigma \circ g\right) = \left(F_\sigma \circ g\right)(q_0) = F_\sigma\left(g(q_0)\right) = \mu(g)F_\sigma. \qquad \square\end{aligned}$$

Istražimo sada rastav grupoidnog automata $\mathbf{SM}(\mathcal{G}) = (G, G, F^{\mathcal{G}})$. Neka je H normalna podgrupa od G. Označimo s $\mathcal{H}$ transformacijsku grupu $(H, H, \cdot_{\mathcal{H}})$. Neka je particija π skupa G zadana kao skup desnih klasa podgrupe H, dakle $\pi = G/H$. Znamo da skup G/H čini grupu uz množenje izvedeno iz G.

Koristeći svojstva normalne podgrupe, lako se dokaže da za kvocijentnu transformacijsku grupu vrijedi $\mathcal{G}/\langle\pi\rangle = (G/H, G/H, \cdot_\pi)$. Ovu transformacijsku grupu označavamo s $\mathcal{G}/\mathcal{H}$. Koristimo je u sljedećem teoremu, koji je direktna generalizacija spomenutih dekompozicijskih rezultata iz teorije grupa. Dokaz teorema je inspiriran raspravom iz [7, Section 6.5].

Propozicija 3.24. *Neka je G konačna grupa i neka je H njena normalna podgrupa. Tada, uz oznake kao gore, vrijedi:*

$$\mathbf{SM}(\mathcal{G}) \leq \mathbf{SM}(\mathcal{H})\, \omega\, \mathbf{SM}(\mathcal{G}/\mathcal{H}).$$

Dokaz. Particija $\pi = G/H$ skupa G sastavljena od desnih klasa podgrupe H u G je očito dopustiva za automat $\mathbf{SM}(\mathcal{G})$. Neka je $H = \{ h_1, h_2, \ldots, h_M \}$, gdje je $M \in \mathbb{N}_+$. Neka je $K = \{ k_1, k_2, \ldots, k_N \}$ jedan skup predstavnika desnih klasa od H u G, gdje je $N \in \mathbb{N}_+$. Pokažimo da je skup $\rho = \{ h_1K, h_2K, \ldots, h_MK \}$ također particija skupa G, i to ortogonalna s π.

Prvo dokazujemo da je ρ particija. Pretpostavimo da je $h_iK \cap h_jK \neq \emptyset$, za neke $i, j \leq M$, $i \neq j$. To bi značilo da postoje različiti $\ell, r \leq N$ takvi da $h_ik_\ell = h_jk_r$. No, tada bi vrijedilo $k_\ell = h_i^{-1}h_jk_r$, što bi značilo $Hk_\ell = Hh_i^{-1}h_jk_r = Hk_r$, kontradikcija. Brojanjem elemenata se sada jednostavno vidi da vrijedi i $\bigcup\rho = G$.

Neka je sada $Hk_i \in \pi$ proizvoljna desna klasa od H i $h_j \in H$ proizvoljan. Analogno kao prije, pokaže se $Hk_i \cap h_jK = \{ h_jk_i \}$. Stoga je ispunjen uvjet ortogonalnosti za particije π i ρ. Još primjetimo da vrijedi $|\rho| = M = |H| = \max(\pi)$.

Prisjetimo se dokaza teorema 3.17. Tamo smo također u početku konstruirali particiju ρ ortogonalnu početnoj particiji π za koju je vrijedilo $|\rho| = \max(\pi)$. Pomoću nje smo dobili drugi faktor dekompozicije polaznog automata, pored kvocijentnog

automata. Istim postupkom sada zaključujemo da postoji automat $\mathcal{N} = (\rho, G/H \times G, F^{\mathcal{N}})$ za koji vrijedi $\mathbf{SM}(\mathcal{G}) \leq \mathcal{N} \,\omega\, (\mathbf{SM}(\mathcal{G})/\pi)$.

Ostaje pokazati da vrijedi $\mathcal{N} \equiv \mathbf{SM}(\mathcal{H})$ i $\mathbf{SM}(\mathcal{G})/\pi \equiv \mathbf{SM}(\mathcal{G}/\mathcal{H})$. Dokazujemo $\mathcal{N} \leq \mathbf{SM}(\mathcal{H})$ i $\mathbf{SM}(\mathcal{G})/\pi \leq \mathbf{SM}(\mathcal{G}/\mathcal{H})$, a kako obratna prekrivanja trivijalno vrijede, ekvivalentnost konačnih automata slijedi po definiciji 2.8.

Promotrimo detaljnije rad automata $\mathcal{N}$. Njegova funkcija prijelaza $F^{\mathcal{N}}$ definirana je tako da za sve $h_iK \in \rho$ i $(Hk_j, g) \in G/H \times G$ vrijedi:

$$F^{\mathcal{N}}(h_iK, (Hk_j, g)) = \varphi_\rho((h_ik_j)F_g^{\mathcal{G}}) = \varphi_\rho(h_ik_jg).$$

Neka je $\mu\colon H \to \rho$ bijekcija takva da za sve $h_i \in H$ vrijedi $\mu(h_i) = h_iK$.

Ostaje još definirati funkciju $\nu\colon G/H \times G \to H$ takvu da par (μ, ν) čini prekrivač automata $\mathcal{N}$ automatom $\mathbf{SM}(\mathcal{H})$. Neka su dani $k_j \in K$ i $g \in G$. Umnožak k_jg pripada točno jednoj desnoj klasi od H u G, recimo Hk_ℓ. Tada postoji jedinstveni $\bar{h} \in H$ takav da vrijedi $k_jg = \bar{h}k_\ell$. Stoga definiramo $\nu(Hk_j, g) = \bar{h}$.

Pokažimo da je par (μ, ν) doista traženi prekrivač. Neka su $h_i \in H$ i $(Hk_j, g) \in G/H \times G$ proizvoljni. Označimo opet $\bar{h} = \nu(Hk_j, g)$, odnosno neka vrijedi $k_jg = \bar{h}k_\ell$, za neki $\ell \leq N$. Prvo primjetimo da vrijedi:

$$F^{\mathcal{N}}(h_iK, (Hk_j, g)) = \varphi_\rho(h_i \underbrace{k_jg}_{=\bar{h}k_\ell}) = \varphi_\rho(h_i\bar{h}k_\ell) = (h_i\bar{h})K.$$

Naposljetku vrijedi:

$$\begin{aligned}\mu(h_iF^{\mathcal{H}}_{\nu(Hk_i,g)}) &= \mu(h_iF^{\mathcal{H}}_{\bar{h}}) = \mu(h_i \cdot_G \bar{h}) = (h\bar{h})K \\ &= F^{\mathcal{N}}(h_iK, (Hk_j, g)) = F^{\mathcal{N}}(\mu(h_i), (Hk_j, g)).\end{aligned}$$

Drugo prekrivanje je jednostavno. □

Teorem 1.29 sada zajedno s propozicijom 3.24, lemom 2.32 i tranzitivnošću relacije prekrivanja daje sljedeći dekompozicijski rezultat za grupoidne automate (a zbog leme 3.23 posredno i za permutacijske).

Teorem 3.25 (Rastav grupoidnog automata)**.** *Neka je G konačna grupa i G_0, G_1, …, G_n njezin jedinstveni kompozicijski slijed. Neka je $\mathcal{G} = (G, G, \cdot_{\mathcal{G}})$ transformacijska grupa pridružena grupi G. Također, neka je $\mathcal{G}_i = (G_{i+1}/G_i, G_{i+1}/G_i, F^{\mathcal{G}_i})$ transformacijska grupa pridružena prostoj grupi G_{i+1}/G_i, za $i = 0, 1, \ldots, n-1$. Tada vrijedi:*

$$\mathbf{SM}(\mathcal{G}) \leq \mathbf{SM}(\mathcal{G}_{n-1}) \,\omega\, \mathbf{SM}(\mathcal{G}_{n-2}) \,\omega \cdots \omega\, \mathbf{SM}(\mathcal{G}_0).$$

3.5 Krohn-Rhodesov teorem

U prethodnim odjeljcima prikazali smo postupak dekompozicije konačnog automata na jednostavnije automate. Prvi i najvažniji teorem koji govori o dekompozicijama konačnih automata i transformacijskih polugrupa predstavili su Kenneth Krohn i John Rhodes 1965. godine u [11]. U ovom odjeljku donosimo iskaz teorema i skicu dokaza te raspravljamo o njegovu značenju i posljedicama.

U svojoj cijelosti, iskaz Krohn-Rhodesovog teorema, a pogotovo dokaz, tehnički je zahtjevan. Najveća poteškoća krije se iza sljedeće definicije, koju su uveli sami Krohn i Rhodes.

Definicija 3.26. Neka su S i T polugrupe. Kažemo da polugrupa S *dijeli* polugrupu T ako postoji potpolugrupa T' od T takva da je polugrupa S homomorfna slika polugrupe T'. U ovom slučaju pišemo $S \mid T$.

Sam iskaz Krohn-Rhodesova teorema sada postaje dohvatljiv i razumljiv. Donosimo najprije verziju koja govori o dekompoziciji transformacijskih polugrupa.

Teorem 3.27 (Krohn-Rhodesov teorem za transformacijske polugrupe)**.** *Neka je $\mathcal{S} = (X, S)$ proizvoljna transformacijska polugrupa. Tada postoji vjenačna dekompozicija od $\mathcal{S}$ koja se sastoji od sljedeće dvije skupine transformacijskih polugrupa:*

- $\overline{\mathbf{2}}^{\bullet}$*;*
- $\mathcal{G} = (G, G)$*, gdje je G konačna prosta grupa takva da $G \mid S$.*

Prethodni rezultat povijesno i konceptualno je dokazan prvi, upravo zbog definicije djeljivosti polugrupa i njihovog povijesnog matematičkog značaja (barem u usporedbi s konačnim automatima). S prolaskom vremena i sve većim rastom teorije računarstva, analogni teorem o dekompoziciji konačnih automata dobiva sve više značaja.

Teorem 3.28 (Krohn-Rhodesov teorem za konačne automate)**.** *Neka je $\mathcal{M}$ proizvoljni konačni automat. Tada postoji konačni prekrivač od $\mathcal{M}$ koji se sastoji od direktnog i kaskadnog produkta sljedeće dvije skupine konačnih automata:*

- $\mathbf{SM}(\overline{\mathbf{2}}^{\bullet})$*;*
- $\mathbf{SM}(\mathcal{G}) = \left(G, G, F^{\mathcal{G}}\right)$*, gdje je G konačna prosta grupa takva da $G \mid \mathbf{S}(\mathcal{M})$.*

U nastavku opisujemo što smo napravili u smjeru dokaza Krohn-Rhodesovog teorema te ističemo koji dio dokaza izlazi izvan okvira ovog rada. Najprije opet primijetimo, kao u raspravi s početka poglavlja, da verzija Krohn-Rhodesovog teorema

za konačne automate implicira verziju za transformacijske polugrupe. Zato se fokusiramo na verziju o konačnim automatima.

Skica dokaza Krohn-Rhodesovog teorema. Neka je $\mathcal{M} = (Q, \Sigma, F)$ proizvoljni konačni automat. Najprije možemo iskoristiti teorem 3.20 kako bismo dobili dekompoziciju $\mathcal{M} \leq \mathcal{M}_1 \,\omega\, \mathcal{M}_2 \,\omega \cdots \omega\, \mathcal{M}_{n-1}$, gdje je $n = |\mathcal{M}|$ i za svaki $i = 1, 2, \ldots, n$ je konačni automat $\mathcal{M}_i$ reset-permutacijski. Koristeći teorem 3.20, dobijemo da za sve $i = 1, 2, \ldots, n$ postoje reset automat $\mathcal{R}_i$ i permutacijski automat $\mathcal{P}_i$ takvi da vrijedi $\mathcal{M}_i \leq \mathcal{R}^{\bullet}_i \,\omega\, \mathcal{P}_i$.

Reset-monoidne automate $\mathcal{R}^{\bullet}_i$ po teoremu 3.22 prekrijemo direktnim produktom od konačno mnogo kopija konačnog automata $\mathbf{SM}(\overline{\mathbf{2}}^{\bullet})$. Permutacijski automat $\mathcal{P}_i$ najprije prekrijemo grupoidnim automatom $\mathbf{SM}(\mathcal{G})$, kao u lemi 3.23, a posljednji automat rastavimo do grupoidnih automata s prostim grupama, po teoremu 3.25.

Konačno, po lemi 2.32 i tranzitivnosti relacije prekrivanja konačnih automata, dobijemo željenu kaskadno-direktnu dekompoziciju polaznog konačnog automata $\mathcal{M}$.

Ono što preostaje za dokazati jest uvjet djeljivosti polugrupe konačnog automata $\mathbf{S}(\mathcal{M})$ dobivenim prostim grupama. Ovaj dio se pokazuje tehnički vrlo zahtjevnim, a ne suviše konceptualno informativnim. Zainteresiranog čitatelja upućujemo na neki od sljedećih izvora: [11], [21], [7, poglavlje 7], [23], [18, dodatak A], [13]. □

Teorem 3.28 pokazuje da sve konačne automate možemo simulirati konačnim produktima najjednostavnijih reset-monoidnih automata te prostih grupoidnih automata. Pokazuje se da su ovi automati doista *ireducibilni*, tj. da se ne mogu rastaviti na jednostavnije konačne automate (vidi [11]).

Primijetimo da je Krohn-Rhodesov teorem konstruktivan jer daje algoritam za rastav proizvoljnog konačnog automata. Doduše, ovaj algoritam je vrlo neefikasan, prvenstveno jer u prvom koraku (teorem 3.20) biramo „rastrošne" dekompozicije skupa. Potreba za razvojem efikasnijih algoritama dovela je do razvoja homološke teorije transformacijskih polugrupa u [5, Vol. B], programski implementirane u [4].

Iako je konstruktivan, Krohn-Rhodesov teorem ne garantira jednoznačnost dekompozicije konačnog automata i transformacijskih polugrupa. Stoga se razvila *algebarska teorija složenosti*, kojoj je cilj odrediti najmanje prekrivače proizvoljne transformacijske polugrupe. Ova teorija i dalje se aktivno proučava ([16]). Neke njene primjene su u određivanju evolucijske složenosti bioloških sustava, složenosti igara, umjetnoj inteligenciji, fizici, čak i psihologiji (vidi [15]). Za kraj spomenimo i proširenje Krohn-Rhodesovog teorema na teoriju kategorija u [20].

Bibliografija

[1] Tadashi Ae, *Direct or cascade product of pushdown automata*, Journal of Computer and System Sciences **14** (1977), br. 2, 257–263, http://www.sciencedirect.com/science/article/pii/S0022000077800160.

[2] Benjamin Baumslag, *A Simple Way of Proving the Jordan-Hölder-Schreier Theorem*, The American Mathematical Monthly **113** (2006), br. 10, 933–935, http://www.jstor.org/stable/27642092.

[3] Patrick Blackburn, Maarten de Rijke i Yde Venema, *Modal Logic*, Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 2001.

[4] Attila Egri-Nagy i Chrystopher Nehaniv, *Algebraic Hierarchical Decomposition of Finite State Automata: Comparison of Implementations for Krohn-Rhodes Theory*, sv. 3317, srpanj 2004, str. 315–316.

[5] Samuel Eilenberg, *Automata, Languages and Machines*, Academic Press, 1974.

[6] Jens Fehlau, *The Cayley type theorem for semigroups*, (2018).

[7] Abraham Ginzburg, *Algebraic theory of automata*, Academic Press, 2014.

[8] M. Holcombe, *Algebraic Automata Theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1982.

[9] Thomas Hungerford, *Algebra*, Springer, 2003.

[10] Masami Ito, *Algebraic Theory of Automata and Languages*, World Scientific Press, 2004.

[11] Kenneth Krohn i John Rhodes, *Algebraic Theory of Machines. I. Prime Decomposition Theorem for Finite Semigroups and Machines*, Transactions of the American Mathematical Society **116** (1965), 450–464, ISSN 00029947, http://www.jstor.org/stable/1994127.

[12] G. H. Mealy, *A method for synthesizing sequential circuits*, The Bell System Technical Journal **34** (1955), br. 5, 1045–1079.

[13] A.R. Meyer i C. Thompson, *Remarks on algebraic decomposition of automata*, Mathematical systems theory **3** (1969), 110–118, https://doi.org/10.1007/BF01746516.

[14] Edward F. Moore, *Gedanken-Experiments on Sequential Machines*, Automata Studies (Claude Shannon i John McCarthy, ur.), Princeton University Press, Princeton, NJ, 1956, str. 129–153.

[15] John Rhodes, *Applications of Automata Theory and Algebra*, World Scientific, 2010.

[16] John Rhodes i Benjamin Steinberg, *The Q-Theory of Finite Semigroups*, Springer Publishing Company, Incorporated, 2008, ISBN 0387097805.

[17] Michael Sipser, *Introduction to the Theory of Computation*, Course Technology, Boston, MA, 2013, ISBN 113318779X.

[18] Howard Straubing, *Finite Automata, Formal Logic, and Circuit Complexity*, Birkhauser Verlag, CHE, 1994, ISBN 3764337192.

[19] Mladen Vuković, *Teorija skupova*, Predavanja, 2015.

[20] Charles Wells, *A Krohn-Rhodes Theorem for categories*, Journal of Algebra **64** (1980), br. 1, 37–45, ISSN 0021-8693, http://www.sciencedirect.com/science/article/pii/0021869380901301.

[21] P. Zeiger, *Yet another proof of the cascade decomposition theorem for finite automata*, Mathematical systems theory **1** (1967), 225–228.

[22] Jean Éric Pin, *Mathematical Foundations of Automata Theory*, published online, 2012.

[23] Z. Ésik, *A proof of the Krohn–Rhodes Decomposition Theorem*, Theoretical Computer Science **234** (2000), br. 1, 287 – 300, ISSN 0304-3975, http://www.sciencedirect.com/science/article/pii/S0304397599003151.

[24] Vedran Čačić, *Komputonomikon*, Predavanja iz kolegija izračunljivost, 2020.

[25] Boris Širola, *Algebarske strukture*, Predavanja.

Sažetak

Krohn-Rhodesova teorija spaja računarsku teoriju konačnih automata i algebarsku teoriju konačnih polugrupa. U ovom radu dajemo pregled temeljnih ideja i koncepata ove dualne teorije. Pokazujemo kako je svakom konačnom automatu prirodno pridružena konačna polugrupa. Izučavamo pojmove homomorfizma i simulacije između konačnih automata, odnosno transformacijskih polugrupa. Predstavljamo metode za dobivanje novih automata ili polugrupa kombinacijom polaznih. Na koncu iskazujemo i djelomično dokazujemo temeljni Krohn-Rhodesov dekompozicijski teorem. Njime je utvrđeno postojanje rastava proizvoljnog konačnog automata, odnosno transformacijske polugrupe, u jednostavnije sastavne dijelove.

Summary

Krohn-Rhodes theory combines the computational theory of finite automata with the algebraic theory of finite semigroups. Here, an overview of the basic ideas and concepts from this dual theory is provided. It is shown that for each finite automaton there is a naturally associated finite semigroup. The concepts of homomorphism and simulation between finite automata and transformation semigroups, respectively, are studied. Several methods for obtaining new automata or semigroups by a combination of starting ones are presented. Finally, the fundamental Krohn-Rhodes decomposition theorem is stated, and proved to an extent. This theorem establishes the existence of a decomposition of an arbitrary finite automaton (and of any transformation semigroup as well) into simpler components.

Životopis

Ivan Miošić rođen je u ljetu 1996. godine u Makarskoj. Djetinjstvo provodi u prekrasnom Bristu, inače rodnom gradu velikog hrvatskog pjesnika i prezimenjaka, fra Andrije Kačića Miošića. Pohađa opću gimnaziju u Pločama. Tijekom ovog razdoblja sudjeluje u državnim natjecanjima iz matematike i fizike, a uz to trenira nogomet.

2015. godine započinje školovanje na matematičkom odsjeku PMF-a u Zagrebu. Studiranje upotpunjuje volontiranjem u udruzi, veslanjem i radom. Za diplomski studij, nakon konzultacija s budućim mentorom, odabire smjer računarstvo. U isto vrijeme postaje stipendist tvrtke Atos. Tijekom ljeta 2019. godine obavlja stručnu praksu u Leuvenu na institutu za umjetnu inteligenciju. Uživa u čitanju, druženju s obitelji i dobrim prijateljima te životu u rodnom mjestu.