

BESEDNI PROBLEM V PROSTI INVERZNI POLGRUPI

TINA DRNOVŠEK

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku je obravnavan besedni problem v prosti inverzni polgrupi. Prvi del zajema splošno teorijo inverzne polgrupe. V nadaljevanju je na kratko nakazana konstrukcija proste inverzne polgrupe preko proste polgrupe z involucijo. Temu sledi reševanje besednega problema, tj. iskanje algoritma, ki določa, kdaj dve besedi predstavljata enak element v prosti inverzni polgrupi. Znanih je več možnih pristopov k reševanju, v članku je predstavljena rešitev s pomočjo Scheiblichovih normalnih form.

THE WORD PROBLEM FOR THE FREE INVERSE SEMIGROUP

The article discusses the word problem in the free inverse semigroup. The first part covers the general theory of inverse semigroups. This is followed by a brief outline of the construction of the free inverse semigroup through free semigroup with involution. The paper then addresses the solution to the word problem, i.e., we describe an algorithm that determines when two words represent the same element in a free inverse semigroup. While there are several possible approaches to the solution, we present the solution using Scheiblich normal forms.

1. Uvod

Teorija inverznih polgrup se je začela razvijati na začetku petdesetih let prejšnjega stoletja. Prva sta pojem inverzne polgrupe neodvisno vpeljala ruski matematik V.V. Wagner leta 1952 in angleški matematik G. Preston leta 1954. Pomembno vlogo pri tem je imelo raziskovanje polgrupe parcialnih permutacij, ki jo bomo predstavili v nadaljevanju. Wagner je prvi opazil, da je kompozitum parcialnih permutacij poseben primer kompozituma binarnih relacij. Množica vseh parcialnih permutacij, opremljena z operacijo kompozituma, tvori inverzno polgrupo. Pravimo ji tudi simetrična inverzna polgrupa. Eden od zgodnejših rezultatov proučevanja inverznih polgrup je Wagner-Prestonov izrek. Ta nam pove, da lahko vsako inverzno polgrupo vložimo v neko simetrično inverzno polgrupo.

Glavno teoretično podlago črpamo iz [3], medtem ko v drugem poglavju dodatno povzemamo tudi [1] in [2].

2. Na kratko o inverznih polgrupah

Uvedimo osnovni primer polgrupe, ki ga bomo uporabljali v nadaljevanju.

Zgled 1. Naj bo X neprazna množica. Označimo z X^+ množico vseh končnih zaporedij elementov v X brez praznega niza. Element v X^+ je torej oblike $(x_1, \dots, x_n)$, kjer je $x_i \in X$. Pravimo mu *niz* ali *beseda*. Na množici nizov definiramo binarno operacijo *konkatenacijo* oziroma *lepljenje*, ki niza $x = (x_1, \dots, x_m)$ in $y = (y_1, \dots, y_n)$ preslika v $xy = (x_1, \dots, x_m, y_1, \dots, y_n)$. Množica X^+ postane polgrupa za to operacijo.

Definicija 2. Naj bo S polgrupa. Element $x \in S$ je *regularen*, če obstaja tak element $a \in S$, da velja $axa = a$ in $xax = x$. V tem primeru elementu a pravimo *inverz* elementa x . Če je vsak element a v polgrupi S regularen, polgrupo S imenujemo *regularna polgrupa*.

Opazimo, da zgornja definicija inverza posplošuje definicijo inverza v grupah. Namreč, za element x iz grupe G in njegov inverz očitno veljata zgornji identiteti. Obratno, če za elementa a in x v grupi G enakost $axa = a$ množimo z leve strani z a^{-1} , dobimo, da je $xa = 1$, in če množimo z desne strani, $ax = 1$. Zaključimo, da je $a = x^{-1}$.

Definicija 3. Če ima vsak element a v polgrupi S natanko en inverz, polgrupo S imenujemo *inverzna polgrupa*, inverz elementa a pa označimo z a^{-1} .

Pomemben zgled je *simetrična inverzna polgrupa* $\mathcal{I}(X)$, množica vseh parcialnih permutacij množice X :

Zgled 4. *Parcialna permutacija* množice X je injektivna preslikava $p : X_1 \rightarrow X$, kjer X_1 označuje podmnožico množice X . Množici X_1 pravimo *domena*, $p(X_1)$ pa *slika*, označimo ju z $\text{dom}(p)$ in $\text{im}(p)$. Oglejmo si primer parcialne permutacije množice $X = \{1, 2, 3, 4\}$, za katero velja, da je $\text{dom}(p) = \{1, 3, 4\}$, $p(1) = 2$, $p(3) = 3$, $p(4) = 1$. Lahko jo predstavimo s tabelo:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & \emptyset & 3 & 1 \end{pmatrix}.$$

Za podmnožico $Y \subseteq X$ z 1_Y označimo preslikavo, za katero je $\text{dom}(1_Y) = Y$ in vsak element $y \in Y$ preslika samega vase. Z 0 označimo parcialno permutacijo, katere domena je $\emptyset$. Pravimo ji ničelna parcialna permutacija.

Definirajmo kompozitum dveh parcialnih permutacij p in q na naraven način: $pq(x) = p(q(x))$ za vsak $x \in \text{dom}(pq)$, pri čemer za domeno pq vzamemo: $\text{dom}(pq) = \{x \in \text{dom}(q) \mid q(x) \in \text{dom}(p)\}$. Če opremimo množico $\mathcal{I}(X)$ s komponiranjem, je enostavno preveriti, da dobimo polgrupo z enoto 1_X oziroma monoid.

Definiramo še inverz parcialne permutacije p : $\text{dom}(p^{-1}) = \text{im}(p)$ in za vsak $x \in \text{dom}(p^{-1})$ je $p^{-1}(x) = y$, če je $p(y) = x$. Enostavno se prepričamo, da veljata enakosti $pp^{-1}p = p$ in $p^{-1}pp^{-1} = p^{-1}$. Preverimo še, da je inverz p^{-1} enolično določen. Predpostavimo, da za parcialni permutaciji p in q velja $pqp = p$ in $qpq = q$. Za $x \in \text{dom}(p)$ velja $p(q(p(x))) = p(x)$. Ker je p injektivna preslikava, sledi $q(p(x)) = x$ in zato $\text{im}(p) \subseteq \text{dom}(q)$. Podobno iz druge enakosti sledi $\text{dom}(q) \subseteq \text{im}(p)$, torej je $\text{dom}(q) = \text{im}(p)$. Ker je parcialna permutacija p bijekcija med $\text{dom}(p)$ in $\text{im}(p)$, je p^{-1} enolično določen. Torej je $\mathcal{I}(X)$ primer inverznega monoida.

Očitno je vsaka inverzna polgrupa tudi regularna. Obrat pa velja ob posebnih pogojih. Pomembno povezavo med inverznimi in regularnimi polgrupami nam predstavljajo idempotenti, ki v inverznih polgrupah komutirajo. Spomnimo najprej, da je element e idempotent, če zanj velja $e^2 = e$.

Izrek 5. Naj bo S regularna polgrupa. Idempotenti v S komutirajo natanko tedaj, ko je polgrupa S inverzna.

Dokaz. Lotimo se najprej lažje implikacije v desno. Naj bosta a, b inverza elementa x . Tedaj so elementi ax, bx, xa, xb idempotenti, saj je $(ax)^2 = (axa)x = ax$, podoben račun pa naredimo še za preostale elemente. Ker idempotenti komutirajo, dobimo

$$\begin{aligned} a &= axa = a(xbx)a = (ax)(bx)a = (bx)(ax)a \\ &= bx(axa) = bxa = (bxb)xa = b(xb)(xa) \\ &= b(xa)(xb) = b(xax)b = bxb \\ &= b. \end{aligned}$$

S tem smo dokazali, da je polgrupa S inverzna.

Sedaj privzemimo, da je S inverzna polgrupa. Naj bosta e in f idempotenta v S . Z x označimo inverz elementa ef . Pokažimo, da sta si ef in fxe inverzna:

$$\begin{aligned}(ef)(fxe)(ef) &= e(ff)x(ee)f = e(fxe)f = ef, \\ (fxe)(ef)(fxe) &= fx(ee)(ff)xe = f(xefx)e = fxe.\end{aligned}$$

Opazimo, da velja

$$(fxe)(fxe) = f(xefx)e = fxe,$$

iz česar sledi, da je fxe idempotentni inverz elementa ef . Ker ima v S vsak element enoličen inverz, sledi $fxe = x$ in je x idempotent. Ker je vsak idempotent sam sebi inverz, zaključimo, da je $ef = x$ in je ef idempotent. Iz simetrije sledi, da je tudi fe idempotent, zato je

$$\begin{aligned}ef(fe)ef &= e(ff)(ee)f = efef = ef, \\ fe(ef)fe &= fefe = fe,\end{aligned}$$

torej sta ef in fe inverza ef . Zaključimo, da je $ef = fe$, kar smo želeli dokazati. ■

Med drugim smo v dokazu pokazali, da je množica idempotentov $E(S)$ inverzne polgrupe S zaprta za množenje.

Idempotenti igrajo v inverznih polgrupah zelo pomembno vlogo, saj sta za vsak element s iz inverzne polgrupe elementa ss^{-1} in $s^{-1}s$ idempotenta.

Odgovor na vprašanje, kateri elementi so idempotenti v $\mathcal{I}(X)$, nam pove naslednja trditev.

Trditev 6. Idempotenti v $\mathcal{I}(X)$ so ravno identične preslikave na podmnožicah množice X .

Dokaz. Identične preslikave na podmnožicah množice X so očitno idempotenti. Dokazati moramo, da drugih ni. Vzemimo poljuben idempotent f . Ker je $f^{-1} = f$, velja $f = ff = f^{-1}f$, element $f^{-1}f$ pa je identična preslikava na svoji domeni. ■

2.1 Naravna delna urejenost

Na inverzni polgrupi S definiramo relacijo $\leq$, ki jo imenujemo *naravna delna urejenost* na naslednji način: za elementa $s, t \in S$ velja $s \leq t$ natanko tedaj, ko je $s = te$ za neki idempotent e .

Za začetek preverimo, ali zgornja relacija res delno ureja polgrupo S . Relacija $\leq$ je refleksivna, saj je $s = s(s^{-1}s)$. Pokažimo sedaj, da je antisimetrična. Predpostavimo, da drži $s \leq t$ in $t \leq s$. Tedaj je $s = te$ in $t = sf$ za idempotenta e in f . Če upoštevamo, da idempotenti komutirajo, dobimo $s = te = (sf)e = sef$. Pomnožimo enačbo s f z desne in dobimo želeni rezultat: $t = sf = (sef)f = sef = s$. Preostane nam še tranzitivnost. Recimo, da za elemente $s, t, u \in S$ velja $s \leq t$ in $t \leq u$, kjer sta e in f idempotenta. Sledi $s = u(fe)$, kjer je fe idempotent, torej $s \leq u$.

Zgled 7. Kakšna je naravna delna urejenost v simetrični inverzni polgrupi $\mathcal{I}(X)$? Po definiciji naravne delne urejenosti za $f, g \in \mathcal{I}(X)$ velja $f \leq g$, če in samo če obstaja taka množica $Y \subseteq X$, da je $f = g1_Y$. To pa je ekvivalentno temu, da je $\text{dom}(f) \subseteq \text{dom}(g)$ in da za vsak $x \in \text{dom}(f)$ velja $f(x) = g(x)$, torej je f zožitev preslikave g .

Definicija 8. Naj bo $(P, \leq)$ delno urejena množica. Podmnožici $Q \subseteq P$ pravimo *urejenostni ideal*, če iz $y \in Q$ in $x \leq y$ sledi $x \in Q$. Za poljubno podmnožico $A \subseteq P$ definiramo *urejenostni ideal, generiran z množico A* , na naslednji način:

$$[A]^\downarrow = \{y \mid y \leq a \text{ za neki element } a \in A\}.$$

Če je $A = \{a\}$, ideal označimo z $a^\downarrow$ in ga imenujemo *glavni urejenostni ideal* elementa a .

Opazimo, da je primer urejenostnega ideala množica $E(S)$. Če za elementa $x \in S$ in $y \in E(S)$ drži neenakost $x \leq y$, lahko zapišemo $x = ye$ za neki idempotent e . Ker je $E(S)$ zaprta za množenje, je tudi x idempotent.

Definicija 9. Naj bo $(P, \leq)$ delno urejena množica. Element z je *spodnja meja* x in y , če je $z \leq x$ in $z \leq y$. Če obstaja največji element v množici spodnjih mej x in y , ga imenujemo *natančna spodnja meja* x in y , ki jo označimo z $x \wedge y$. Delno urejeno množico, v kateri ima vsak par elementov natančno spodnjo mejo, imenujemo *polemreža*.

Naravno delno urejenost med idempotenti v inverzni polgrupi lahko zapišemo tudi bolj preprosto, kar nam pove naslednja trditev.

Trditev 10. Naj bo S inverzna polgrupa. Za idempotenta $e, f \in E(S)$ drži $e \leq f$ natanko tedaj, ko je $e = ef = fe$.

Dokaz. Predpostavimo, da velja $e \leq f$ za neka idempotenta e in f . Tedaj obstaja idempotent i , da je $e = fi$. Potem je $fe = f(fi) = fi = e$. Torej je $e = fe = ef$. Implikacija v levo je očitna. ■

Zaradi naslednje trditve množici idempotentov v inverzni polgrupi pogosto rečemo kar polemreža idempotentov.

Trditev 11. Naj bo S inverzna polgrupa. Definiramo relacijo na množici $E(S)$:

$$e \leq f \iff e = ef = fe.$$

Tedaj je $(E(S), \leq)$ polemreža.

Dokaz. Najprej dokažimo, da $\leq$ delno ureja $E(S)$. Refleksivnost je očitna. Iz $e \leq f$ in $f \leq e$ sledi $e = ef = fe = f$, kar nam da antisimetričnost. Sedaj predpostavimo, da je $e \leq f$ in $f \leq i$. Velja $e = ef = e(fi) = (ef)i = ei$. Podobno je tudi $e = ie$ in tako $e \leq i$.

Vzemimo $e, f \in E(S)$. Pokazali bomo, da je ef natančna spodnja meja elementov e in f . Velja $ef \leq e$, ker je $(ef)e = (fe)e = fe = ef$ in idempotenti komutirajo. Podobno je $ef \leq f$. Predpostavimo, da je $i \leq e$ in $i \leq f$. Tedaj $i(ef) = (ie)f = if = i$ in $i(ef) = (ef)i$, zato je $i \leq ef$. Torej je $e \wedge f = ef$, s čimer je dokaz končan. ■

Če povežimo trditvi 10 in 11, zaključimo, da je delna urejenost iz trditve 11 zožitev na množico idempotentov $E(S)$ naravne delne urejenosti na inverzni polgrupi S .

2.2 Homomorfizmi in kongruence

Definicija 12. *Homomorfizem* med polgrupama S in T je taka preslikava $\theta : S \rightarrow T$, da za vsaka elementa $s, t \in S$ drži $\theta(st) = \theta(s)\theta(t)$.

V naslednjem poglavju bomo potrebovali tudi pojem polgrupe z involucijo.

Definicija 13. *Polgrupa z involucijo* S je polgrupa s preslikavo $i : S \rightarrow S$, ki zadošča naslednjima pogojem:

1. $i(i(s)) = s$ za vse $s \in S$,
2. $i(st) = i(t)i(s)$ za vse $s, t \in S$.

Preslikavi i pravimo *involucija*.

Hitro vidimo, da je vsaka inverzna polgrupa polgrupa S z involucijo, kjer je $i(s) = s^{-1}$ za vsak $s \in S$.

Definicija 14. Homomorfizem $\theta : S \rightarrow T$ med polgrupama z involucijo S in T je *involucijski homomorfizem*, če velja $\theta(i_S(s)) = i_T(\theta(s))$ za vsak $s \in S$.

Opazimo, da je vsak homomorfizem med inverznimi polgrupami involucijski homomorfizem. Namreč,

$$\begin{aligned}\theta(s)\theta(s^{-1})\theta(s) &= \theta(s), \\ \theta(s^{-1})\theta(s)\theta(s^{-1}) &= \theta(s^{-1}).\end{aligned}$$

Iz enoličnosti inverzov dobimo enakost $\theta(s^{-1}) = \theta(s)^{-1}$.

Definicija 15. Naj bosta $(P, \leq)$ in $(Q, \leq)$ delno urejeni množici. Funkcija $\theta : P \rightarrow Q$ ohranja urejenost, če iz $x \leq y$ sledi $\theta(x) \leq \theta(y)$. Urejenostni izomorfizem je bijektivna funkcija θ , ki ohranja urejenost, njen inverz pa prav tako ohranja urejenost. V tem primeru pravimo, da sta delno urejeni množici P in Q izomorfni.

Definicija 16. Kongruenca na polgrupi S je ekvivalenčna relacija ρ na S , za katero velja naslednji sklep: če $a \rho b$, $c \rho d$, potem $ac \rho bd$ za vse elemente a, b, c in d .

Naj bo $\theta : S \rightarrow T$ homomorfizem med polgrupama S in T . Tedaj je *jedro homomorfizma* $\ker \theta$ relacija na S , definirana kot

$$\ker \theta = \{(a, b) \in S \times S \mid \theta(a) = \theta(b)\}.$$

Očitno je $\ker \theta$ kongruenca na S .

Enostavno je preveriti, da velja naslednja trditev.

Trditev 17. Naj bo S polgrupa in ρ kongruenca na S . Množica S/ρ je polgrupa za operacijo $*$, definirano z

$$[a]_\rho * [b]_\rho = [ab]_\rho$$

za vsaka elementa $a, b \in S$. Preslikava $\rho^\sharp : S \rightarrow S/\rho$ s predpisom

$$\rho^\sharp(a) = [a]_\rho$$

je surjektivni homomorfizem.

Množico S/ρ v trditvi imenujemo *kvocientna polgrupa*, preslikavo $\rho^\sharp$ pa *kanonični epimorfizem*. Simbolu $\wr$ pravimo *razvezaj*.

Naj bo ρ poljubna relacija na polgrupi S . Presek vseh kongruenc, ki jo vsebujejo, je kongruenca, ki jo označimo s $\rho^\#$. Pravimo, da je to *kongruenca, generirana z ρ* . Presek ni prazen, saj obstaja vsaj ena kongruenca, ki vsebuje ρ , namreč univerzalna kongruenca. To je največja kongruenca, ki je definirana s predpisom $x \rho y$ za vsaka x, y iz polgrupe S .

Definicija 18. Naj bo S inverzna polgrupa. Definiramo relacijo σ na S : za elementa $s, t \in S$ velja $s \sigma t$, če in samo če obstaja element u , da je $u \leq s, t$.

Trditev 19. Naj bo S inverzna polgrupa. Velja:

1. relacija σ je kongruenca,
2. S/σ je grupa,
3. Če je ρ taka kongruenca na S , da je S/ρ grupa, potem je $\sigma \subseteq \rho$.

Dokaz trditve lahko bralec najde v [3]. Kongruenci σ v trditvi 19 pravimo *najmanjša grupna kongruenca*.

3. Prosta inverzna polgrupa

Pričnimo z definicijo proste inverzne polgrupe.

Definicija 20. Naj bo X neprazna množica. Inverzna polgrupa $FIS(X)$ s funkcijo $\iota : X \rightarrow FIS(X)$ je *prosta inverzna polgrupa na X* , če za vsako inverzno polgrupo S in funkcijo $\kappa : X \rightarrow S$ obstaja enoličen homomorfizem $\theta : FIS(X) \rightarrow S$, za katerega je $\theta\iota = \kappa$. Z drugimi besedami, spodnji diagram komutira.

$$\begin{array}{ccc} X & \xrightarrow{\kappa} & S \\ \downarrow \iota & \searrow \theta & \\ FIS(X) & & \end{array}$$

Podobno definiramo prosti objekt v kateri koli konkretni kategoriji.

Zgled 21. Naj bo X neprazna množica. Kot v zgledu 1 tvorimo množico besed X^+ . Z ι označimo vložitev množice X v X^+ . Tedaj je (X^+, ι) prosta polgrupa na X . Premislamo: če je S poljubna polgrupa in $\kappa : X \rightarrow S$ poljubna funkcija, potem je ustrezna $\theta(x_1, \dots, x_n) = \kappa(x_1) \cdots \kappa(x_n)$.

Če sedaj poljubno polgrupo S obravnavamo kot množico $X = S$, lahko konstruiramo prosto polgrupo X^+ . Definiramo homomorfizem $\phi : X^+ \rightarrow S$ na naraven način $\phi(s_1, \dots, s_n) = s_1 \cdots s_n$. Ker je ϕ surjektiv, velja $X^+ / \ker \phi \cong S$, zato je vsaka polgrupa kvocient proste polgrupe.

Da pokažemo obstoj prostih inverznih polgrup, bomo najprej konstruirali proste polgrupe z involucijo. Prosto polgrupo z involucijo definiramo kot prosti objekt v kategoriji polgrup z involucijo, v kateri so morfizmi involucijski homomorfizmi.

Prosto polgrupo z involucijo konstruiramo na naslednji način. Naj bo X množica. Z X^{-1} označimo množico, ki je disjunktna in ekvipolentna množici X . Naj bo $\pi : X \rightarrow X^{-1}$ bijektivna korespondenca. Označimo $x^{-1} = \pi(x)$. Množica nizov $(X \cup X^{-1})^+$, ki jo označimo s $FSI(X)$, postane prosta polgrupa, kot smo spoznali v zgledu 21.

Definiramo involucijo v $FSI(X)$: za vsak $y \in X \cup X^{-1}$ velja

$$y^{-1} = \begin{cases} x^{-1}; & \text{če } y = x \in X, \\ x; & \text{če } y = x^{-1} \in X^{-1}, \end{cases}$$

za $y_1 \dots y_n \in (X \cup X^{-1})^+$ pa definiramo $(y_1 \dots y_n)^{-1} = y_n^{-1} \dots y_1^{-1}$. Tako postane $FSI(X)$ polgrupa z involucijo. Bodi $\iota' : X \rightarrow FSI(X)$ vložitev.

Izrek 22. Polgrupa $(FSI(X), \iota')$ je prosta polgrupa z involucijo na X .

Dokaz. Naj bo T polgrupa z involucijo in $\kappa : X \rightarrow T$ poljubna funkcija. Definiramo $\theta : X \cup X^{-1} \rightarrow T$ s predpisom $\theta(x) = \kappa(x)$ in $\theta(x^{-1}) = \kappa(x)^{-1}$. Vemo, da je $FSI(X)$ prosta polgrupa. Zato lahko funkcijo θ razširimo do homomorfizma $\theta : FSI(X) \rightarrow T$. Funkcija θ je involucijski homomorfizem, saj $\theta(x^{-1}) = \kappa(x)^{-1} = \theta(x)^{-1}$. Očitno velja tudi $\theta\iota' = \kappa$. ■

Opomba 23. Če prosti polgrupi z involucijo $FSI(X)$ dodamo prazen niz, dobimo *prosti monoid z involucijo*, ki ga označimo s $FMI(X)$.

Definiramo binarno relacijo ρ na $FSI(X)$ s predpisom:

$$\rho = \{(uu^{-1}u, u) \mid u \in FSI(X)\} \cup \{(uu^{-1}vv^{-1}, vv^{-1}uu^{-1}) \mid u, v \in FSI(X)\},$$

ki generira kongruenco $\rho^\#$ na $FSI(X)$. Kongruenco imenujemo *Wagnerjeva kongruenca*. Naj bo $FIS(X) = FSI(X)/\rho^\#$ in funkcija $\iota : X \rightarrow FIS(X)$ podana z $\iota = (\rho^\#)^\natural \iota'$.

Izrek 24. Polgrupa $(FIS(X), \iota)$ je prosta inverzna polgrupa na X .

Dokaz lahko bralec najde v [3].

4. Besedni problem

Sedaj se lahko lotimo reševanja besednega problema v prosti inverzni polgrupi. Želeli bi ugotoviti, kdaj dva niza iz polgrupe z involucijo $FSI(X)$ predstavljata isti element v prosti inverzni polgrupi $FIS(X)$. Z drugimi besedami, zanima nas, ali niza pripadata istemu kongruenčnemu razredu $\rho^\#$.

Če za dva niza $u, v \in FSI(X)$ drži, da pripadata istemu kongruenčnemu razredu, pravimo, da sta *ekvivalentna*. Ekvivalentnost nizov u in v označimo z $u \equiv v$.

Za motivacijo si oglejmo primer dveh nizov iz polgrupe z involucijo $FSI(X)$. Z nekaj dela lahko pokažemo, da sta si ekvivalentna v prosti inverzni polgrupi $FIS(X)$. Na koncu tega poglavja bo določanje, ali sta si niza ekvivalentna, enostavnejše.

Zgled 25. Naj bo $X = \{a, b\}$. Dana imamo dva niza iz proste polgrupe z involucijo $FSI(X)$:

$$u = aa^{-1}baaa^{-1}a^{-1}bb^{-1}a,$$

$$v = bb^{-1}aa^{-1}bbb^{-1}aaa^{-1}.$$

Trdimo, da sta si u in v ekvivalentna. Velja:

$$u = aa^{-1}baaa^{-1}a^{-1}bb^{-1}a \equiv aa^{-1}bbb^{-1}aaa^{-1}a^{-1}a,$$

saj je $aaa^{-1}a^{-1}bb^{-1} \equiv ((aa)(aa)^{-1})(bb^{-1}) \equiv bb^{-1}aaa^{-1}a^{-1}$. Sedaj upoštevamo, da je $aa^{-1}a^{-1}a \equiv a^{-1}aaa^{-1}$ in $aa^{-1}a \equiv a$, ter dobimo:

$$u \equiv aa^{-1}bbb^{-1}aa^{-1}aaa^{-1} \equiv aa^{-1}bbb^{-1}aaa^{-1}.$$

Ker je $b \equiv bb^{-1}b$ in $aa^{-1}bb^{-1} \equiv bb^{-1}aa^{-1}$, lahko niz preoblikujemo v:

$$u \equiv aa^{-1}bb^{-1}bbb^{-1}aaa^{-1} \equiv bb^{-1}aa^{-1}bbb^{-1}aaa^{-1} = v.$$

Pri reševanju besednega problema v prostih inverznih polgrupah se bomo opirali na že znano rešitev besednega problema v prostih grupah. Prosto grupo lahko enostavno opišemo s pomočjo $FMI(X)$. Nizom, ki ne vključujejo nobenega podniza oblike xx^{-1} in $x^{-1}x$ v $FMI(X)$, pravimo *reducirani nizi*. Vsak niz lahko enostavno preoblikujemo v reduciran niz, s tem da izbrišemo vse faktorje xx^{-1} in $x^{-1}x$. Tak niz je enolično določen, označimo ga z $\text{red}(u)$. Množico reduciranih nizov opremimo z binarno operacijo $u \cdot v = \text{red}(uv)$ in dobimo prosto grupo $FG(X)$. Prazen niz je po definiciji reduciran niz in je enota v prosti grupi $FG(X)$. Tako konstruirana grupa res zadostuje univerzalni lastnosti, o čemer se lahko bralec prepriča v [4].

Lema 26. Kvocientna grupa $FIS(X)/\sigma$ je prosta grupa na X in za vsaka $u, v \in FIS(X)$ velja, da je $u\sigma v$ natanko tedaj, ko je $\text{red}(u) = \text{red}(v)$.

Dokaz. Definiramo homomorfizem $\theta : FIS(X) \rightarrow FG(X)$ s predpisom $\theta(w) = \text{red}(w)$. Preverimo dobro definiranoost. Za vsaka elementa u in v iz proste polgrupe z involucijo $FSI(X)$, za katera velja $u \rho v$, očitno velja tudi $\text{red}(u) = \text{red}(v)$. Posledično sklep drži za poljubna elementa v istem kongruenčnem razredu $\rho^\#$. Iz rešitve besednega problema v prosti grupi vemo, da velja $\text{red}(\text{red}(u)\text{red}(v)) = \text{red}(uv)$, zato je θ res homomorfizem. Ker je $FIS(X)/\ker \theta = FG(X)$ grupa, lahko uporabimo trditev 19. Velja $\sigma \subseteq \ker \theta$. Dokazati moramo še obratno inkluzijo $\ker \theta \subseteq \sigma$. Vzemimo niza $u, v \in FIS(X)$, za katera velja $\text{red}(u) = \text{red}(v)$. Brez škode za splošnost predpostavimo, da je $u = st$ in $v = sxx^{-1}t$. Velja $sxx^{-1} \leq s$. Ker je naravna delna urejenost usklajena z množenjem, velja $sxx^{-1}t \leq st$. Pokazali smo, da je $v \leq u, v$, torej je $u \sigma v$. ■

4.1 Scheiblichova normalna forma

Reševanja besednega problema se bomo lotili v dveh korakih. Najprej bomo poljuben niz v prosti inverzni polgrupi zapisali v posebni obliki, Scheiblichovi normalni formi (SNF). V drugem koraku pa bomo pokazali, kdaj sta dva niza v Scheiblichovi normalni formi ekvivalentna.

Prvi korak je enostavnejši. Zapis temelji na tem, da idempotenti komutirajo, zaradi česar lahko prevedemo poljuben niz v ekvivalenten niz, zapisan kot produkt idempotentov, ki mu na koncu sledi element, ki v splošnem ni idempotent.

Če neki niz v zapišemo kot v_1v_2 , rečemo, da je v_1 *predpona* niza v in v_2 *pripona*.

Trditev 27. Naj bo w_0 niz v prosti inverzni polgrupi $FIS(X)$. Potem je

$$w_0 \equiv (a_1a_1^{-1}) \dots (a_na_n^{-1})a,$$

kjer so nizi a_i in a reducirani in $a = a_i$ za neki i .

Dokaz. Če je w_0 reduciran niz, zapišemo $w_0 \equiv (w_0w_0^{-1})w_0$ in smo končali. Sicer z u označimo najdaljšo predpono w_0 , ki je reduciran niz. Tedaj zapišemo $w_0 = uv$, kjer u in v nista prazna niza. Naj bo z najdaljša pripona u , da je z^{-1} predpona v . Zaradi izbire u pripona z ni prazen niz. Velja $u = u_1z$ in $v = z^{-1}v_1$, kjer sta u_1 in v_1 lahko prazna niza. Sedaj poračunamo:

$$w_0 = uv = (u_1z)(z^{-1}v_1) \equiv (u_1u_1^{-1}u_1z)(z^{-1}v_1) \equiv (u_1zz^{-1}u_1^{-1})(u_1v_1) = (uu^{-1})(u_1v_1).$$

Niz $w_1 = u_1v_1$ je očitno krajši od niza w_0 . Postopek ponovimo na nizu w_1 . Algoritem se v končnem številu korakov konča, saj smo zmanjšali dolžino nereduciranega niza. ■

Sedaj to obliko še olepšamo in prispemo do zelenega zapisa. Opazimo namreč, da velja naslednje:

Lema 28. Naj bo reduciran niz b predpona niza a . Tedaj velja $aa^{-1} \equiv aa^{-1}bb^{-1}$ v $FIS(X)$.

Dokaz. Če zapišemo $a = bu$, velja $aa^{-1}bb^{-1} = (bu)(bu)^{-1}bb^{-1} \equiv (bb^{-1}b)u(bu)^{-1} \equiv (bu)(bu)^{-1} = aa^{-1}$. ■

Po zgornji lemi lahko torej iz niza $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})a$ odstranimo odvečne nize a_i : iz množice $\{a_1, \dots, a_n\}$ pobrišemo tiste nize, ki so prave predpone nekega drugega niza a_i . Na ta način dobimo množico $\{b_1, \dots, b_m\}$ in tako $u \equiv (b_1b_1^{-1}) \dots (b_mb_m^{-1})a$. Element a v trditvi 27 je enak nekemu nizu a_i in je zato predpona nekega niza b_i .

Definicija 29. Beseda $w = (a_1a_1^{-1}) \dots (a_na_n^{-1})a$ je zapisana v *Scheiblichovi normalni formi* (SNF), če velja naslednje.

1. Besede a_i in a so reducirane.
2. Nobena beseda a_i iz množice $\{a_1, \dots, a_n\}$ ni prava predpona katere koli druge besede iz množice $\{a_1, \dots, a_n\}$.
3. Beseda a je predpona enega od a_i .

Besedam $\{a_1, \dots, a_n\}$ pravimo *komponente* w , a pa imenujemo *koren*.

Dokazali smo torej naslednji izrek.

Izrek 30. Vsak niz v prosti inverzni polgrupi je ekvivalenten nizu v Scheiblichovi normalni formi.

Zgled 31. Oglejmo si, kako algoritem deluje na konkretnem nizu.

Vzemimo niza $u = aa^{-1}baaa^{-1}a^{-1}bb^{-1}a$ in $v = bb^{-1}aa^{-1}bbb^{-1}aaa^{-1}$ iz zgleda 25. Kot nam narekuje algoritem iz dokaza trditve 27, na vsakem koraku zapišemo najdaljšo predpono od niza w_i , ki je reducirana beseda. Označimo jo z a_i . Dobimo:

1. $a_1 = a, w_1 = baaa^{-1}a^{-1}bb^{-1}a$,
2. $a_2 = baa, w_2 = bbb^{-1}a$,
3. $a_3 = bb, w_3 = ba$.

Torej je $u \equiv (aa^{-1})(baaa^{-1}a^{-1}b^{-1})(bbb^{-1}b^{-1})ba$. Preverimo, da noben niz a_i ni predpona nobenega drugega niza iz množice komponent. Podobno izračunamo niz v Scheiblichovi normalni formi, ki je ekvivalenten nizu v .

1. $b_1 = b, w_1 = aa^{-1}bbb^{-1}aaa^{-1}$,
2. $b_2 = a, w_2 = bbb^{-1}aaa^{-1}$,
3. $b_3 = bb, w_3 = baaa^{-1}$,
4. $b_4 = baa, w_4 = ba$.

Ker je b_1 prava predpona niza b_3 , ga odstranimo iz množice komponent.

Zapišimo $v \equiv (aa^{-1})(bbb^{-1}b^{-1})(baaa^{-1}a^{-1}b^{-1})ba$. Iz zapisa v Scheiblichovih normalnih formah lahko zaključimo, da sta u in v ekvivalentna.

Zapišimo dve pomembni opaznanji o elementih v Scheiblichovi normalni formi.

Lema 32. Naj bosta $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})a$ in $v = (b_1b_1^{-1}) \dots (b_mb_m^{-1})b$ niza, zapisana v Scheiblichovi normalni formi. Če sta u in v ekvivalentna, potem sta korena a in b enaka.

Dokaz. Če sta niza u in v ekvivalentna, velja $u \sigma v$ v grupi $FIS(X)/\sigma$. Zato velja $\text{red}(u) = \text{red}(v)$ po lemi 26. Dobimo $a = \text{red}(u) = \text{red}(v) = b$. ■

Lema 33. Naj bo $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})a$ niz, zapisan v Scheiblichovi normalni formi. Niz u je idempotent natanko tedaj, ko je a prazen niz.

Dokaz. Naj bo u idempotent. Potem je $[u]_\sigma$ idempotent, torej enota v prosti grupi $FIS(X)/\sigma$. Očitno element $[uu^{-1}]_\sigma$ tudi predstavlja enoto. Iz leme 26 sledi, da je $\text{red}(u) = \text{red}(uu^{-1}) = 1$. Torej je a prazen niz. Obratno, če je a prazen niz, je u produkt idempotentov, ki komutirajo, in zato sam idempotent. ■

4.2 Delna urejenost na reduciranih nizih

Za reševanje drugega dela besednega problema moramo vpeljati več novih pojmov. Uvedimo delno urejenost na reduciranih nizih: $b \leq_p a$, če je b predpona a . To je ekvivalentno temu, da lahko zapišemo $a = bu$, kjer je bu reduciran niz. Paru elementov a in b rečemo, da sta *neprimerljiva*, če ni niti $b \leq_p a$ niti $a \leq_p b$. Za množico A rečemo, da je *neprimerljiva*, če je vsak par elementov v množici A neprimerljiv.

Spomnimo se, da za element x rečemo, da je *maksimalen*, če za vsak element a v neki delno urejeni množici A , za katerega je $x \leq a$, velja $x = a$. Za podmnožico $A \subseteq FG(X)$ definiramo $\max(A)$ kot množico maksimalnih elementov množice A glede na zgornjo delno urejenost.

Sedaj z I označimo množico vseh končnih nepraznih neprimerljivih podmnožic $FG(X) \setminus \{1\}$, z Y pa množico vseh končnih nepraznih urejenostnih idealov $FG(X)$, ki poleg enote vsebujejo še

vsaj en element. Urejenostni ideal, generiran z neprazno podmnožico $A \subseteq FG(X)$, označimo z $[A]^\downarrow$. Urejenost na Y je definirana na naslednji način: $A \leq B$, če in samo če $B \subseteq A$. Tedaj je $(Y, \cup)$ polmreža za operacijo unija množic.

Trditev 34. Obstaja bijektivna preslikava iz množice Y v množico I .

Dokaz. Definiramo preslikavi $f : Y \rightarrow I$ in $g : I \rightarrow Y$ s predpisoma:

$$f : A \mapsto \max(A),$$

$$g : B \mapsto [B]^\downarrow.$$

Dobra definiranost preslikave f je očitna. Če je množica B v I , je $[B]^\downarrow$ urejenostni ideal. Ta vsebuje množico B , torej vsebuje element, ki ni enota.

Sedaj bomo dokazali, da sta si funkciji f in g inverzni. Najprej predpostavimo, da je $A \in Y$. Velja $[\max(A)]^\downarrow \subseteq A$, kajti za $x \in [\max(A)]^\downarrow$ je $x \leq_p a$ za neki $a \in \max(A) \subseteq A$. Od tod sledi, da je $x \in A$, saj je A urejenostni ideal. Pokažimo še inkluzijo v drugo smer. Naj bo $a \in A$. Potem je $a \leq_p a'$ za neki maksimalni element a' . Torej je $a \in [\max(A)]^\downarrow$ in zaključimo, da je $A = [\max(A)]^\downarrow$.

Naj bo $B \in I$. Opazili smo že, da je $B \subseteq [B]^\downarrow$. Dokažimo najprej, da je vsak element v B maksimalen v množici $[B]^\downarrow$. Recimo, da $b \in B$ ni maksimalen. Tedaj obstaja $b' \in [B]^\downarrow$, za katerega je $b <_p b'$. Istočasno pa po definiciji glavnega urejenostnega ideala obstaja element $b'' \in B$, za katerega velja $b <_p b' \leq_p b''$. To pomeni, da sta elementa b in b'' iz množice B primerljiva, kar ni mogoče. Preostane nam še pokazati, da je $\max([B]^\downarrow) \subseteq B$. Vzemimo poljuben element $a \in \max([B]^\downarrow)$. Spet obstaja neki element $b \in B$, da je $a \leq_p b$. Ker pa je a maksimalen, velja kar $a \in B$. ■

Idempotent v Scheiblichovi normalni formi je oblike $u = (a_1 a_1^{-1}) \dots (a_n a_n^{-1})$. Ker noben niz a_i ni prava predpona niza a_j za različna indeksa i in j , je $\{a_1, \dots, a_n\}$ množica neprimerljivih elementov v $FG(X) \setminus \{1\}$. Po ugotovitvah v dokazu zadnje trditve je množica komponent idempotenta u enaka $\max([a_1, \dots, a_n]^\downarrow)$. Zdi se, da so idempotenti v Scheiblichovi normalni formi v korespondenci s končnimi nepraznimi urejenostnimi ideali $FG(X)$, ki vključujejo vsaj en element, ki ni enota. Dokazali bomo še več, namreč, da je polmreža idempotentov v prosti inverzni polgrupi izomorfná polmreži $(Y, \cup)$.

V nadaljevanju bomo razlikovali med urejenostnimi ideali v delno urejeni množici $(FG(X), \leq_p)$ od urejenostnih idealov v $(Y, \cup)$ na naslednji način: če je množica $A \subseteq FG(X)$, označimo urejenostni ideal, generiran z A , z $[A]^\downarrow$. Če pa je $I \in Y$, označimo glavni urejenostni ideal, ki ga I generira, z $[I]$. Tako je množica $[a_1, \dots, a_n]^\downarrow$ enaka $\{y \in FG(X) \mid y \leq_p a_i \text{ za neki } i \in \{1, \dots, n\}\}$. Naj bo $y \in X \cup X^{-1}$. Vemo že, da je množica $\{1, y\}$ urejenostni ideal v delno urejeni množici $(FG(X), \leq_p)$. Ta pa generira v polmreži $(Y, \cup)$ glavni urejenostni ideal $[\{1, y\}]$, ki ga lahko preprosto opišemo. Velja $[\{1, y\}] = \{I \in Y \mid y \in I\}$.

Za $I \subseteq FG(X)$ in $a \in FG(X)$ definiramo $a \cdot I = \{\text{red}(aw); w \in I\}$.

Lema 35. Naj bo $I \in Y$ in $a \in FG(X)$. Potem je $a \cdot I \in Y$, če in samo če $a^{-1} \in I$.

Dokaz. Najprej se lotimo implikacije v desno smer. Ker je $a \cdot I \in Y$ in je 1 element vsakega urejenostnega ideala v $FG(X)$, vemo, da je $1 \in a \cdot I$. Od tod pa sledi, da je $1 = \text{red}(aw)$ za neki $w \in I$. Ker je w reduciran niz, sledi $w = a^{-1} \in I$. Sedaj predpostavimo, da je a^{-1} element urejenostnega ideala I . Dokazati moramo, da je $a \cdot I \in Y$, torej, da je $a \cdot I$ neprazen končen urejenostni ideal v $FG(X)$, ki poleg enote vsebuje še vsaj en element. Ker je $I \in Y$, je $a \cdot I$ končna množica. Zapišemo lahko $a = \text{red}(a1)$ in $1 = \text{red}(aa^{-1})$, zato sta $1, a \in a \cdot I$. Pokažimo še, da je $a \cdot I$ urejenostni ideal. Vzemimo element $b \in a \cdot I$ in naj bo $c \leq_p b$. Dokazujemo, da je $c \in a \cdot I$. Velja $b = \text{red}(au)$ za neki $u \in I$. Naj bo v najdaljša pripona a , da je v^{-1} predpona u . Natančneje,

$a = a'v$ in $u = v^{-1}u'$. Torej je $b = \text{red}(au) = a'u'$. Po definiciji $\leq_p$ je c predpona b . Ločimo dva primera glede na to, ali je c predpona a' ali je predpona $a'p$, kjer je p predpona u' .

1. Niz c je predpona a' . Potem je $a' = cp$ za nek niz p in $a = a'v = cpv$. Tedaj je $v^{-1}p^{-1}$ predpona $a^{-1} \in I$, od koder sledi, da je $v^{-1}p^{-1} \in I$. Tako dobimo $\text{red}(a(v^{-1}p^{-1})) = \text{red}(cpv(v^{-1}p^{-1})) = c$.
2. Preostane nam primer, ko je $c = a'p$, kjer je p predpona u' . Postopamo podobno kot v prvi točki. Velja, da je $v^{-1}p$ predpona u . Ker je $u \in I$, je tudi $v^{-1}p \in I$. Tedaj je $\text{red}(a(v^{-1}p)) = \text{red}(a'v(v^{-1}p)) = a'p = c$.

Obakrat lahko zaključimo, da je $c \in a \cdot I$. ■

Definicija 36. Naj bo $(E, \wedge)$ polmreža. Množico urejenostnih izomorfizmov med glavnimi urejenostnimi ideali v E z operacijo komponiranja parcialnih permutacij imenujemo *Munnova polgrupa*. Označimo jo s T_E .

Definiramo preslikavo $\phi_x : [\{1, x^{-1}\}] \rightarrow [\{1, x\}]$ s predpisom:

$$\phi_x(I) = x \cdot I.$$

Trditev 37. Obstaja homomorfizem

$$\phi : FIS(X) \rightarrow T_Y,$$

za katerega velja $\phi(x) = \phi_x$ za vse $x \in X$. Za vsak idempotent $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})$ je domena $\phi(u)$ enaka $[[a_1, \dots, a_n]^\downarrow]$.

Dokaz. Najprej dokažimo, da je ϕ_x izomorfizem polmrež. Dobro definiranost nam zagotavlja lema 35. Namreč, $I \in [\{1, x^{-1}\}]$ se preslika v $x \cdot I$, ki je element Y , saj je $x^{-1} \in I$. Od tod sledi, da je $\phi_x(I) \in [\{1, x\}]$. Očitno velja $\phi_x(I \cup J) = \phi_x(I) \cup \phi_x(J)$, torej je ϕ_x homomorfizem polmrež. Dokažimo, da je surjektiven: vzemimo $J \in [\{1, x\}]$, tedaj je $x^{-1} \cdot J \in Y$ po lemi 35. Torej $x^{-1} \cdot J \in [\{1, x^{-1}\}]$ in velja $\phi_x(x^{-1} \cdot J) = J$. Pokažimo, da je injektiven. Predpostavimo, da za neka $I, J \in [\{1, x^{-1}\}]$ velja $\phi_x(I) = \phi_x(J)$. To pomeni, da za vsak element $a \in I$ obstaja element $b \in J$, da velja $\text{red}(xa) = \text{red}(xb)$. Tedaj je $\text{red}(x^{-1}\text{red}(xa)) = \text{red}(x^{-1}xa) = \text{red}(a)$, kar je po drugi strani enako $\text{red}(x^{-1}\text{red}(xb)) = \text{red}(b)$. Od tod pa že sledi injektivnost, ker sta a in b reducirana.

Po definiciji proste inverzne polgrupe $FIS(X)$ na množici X preslikavo $\phi_X : X \rightarrow T_Y$, podano s predpisom $\phi_X(x) = \phi_x$, razširimo do homomorfizma $\phi : FIS(X) \rightarrow T_Y$, za katerega velja $\phi|_X = \phi_X$.

Preostane nam pokazati še zadnji del trditve. Najprej dokažimo, da je za reduciran niz a domena $\phi(aa^{-1})$ enaka $[[a]^\downarrow]$. To enostavno preverimo za $a \in X \cup X^{-1}$. Ker je $\phi(aa^{-1}) = \phi(a)\phi(a)^{-1} = \phi_a\phi_a^{-1}$, je $\text{dom}(\phi(aa^{-1})) = \text{dom}(\phi_a) = [\{1, a\}] = [[a]^\downarrow]$. Sedaj nadaljujemo induktivno. Naj bo a reduciran niz dolžine $n + 1$. Tedaj lahko pišemo $a = by$, kjer je $y \in X \cup X^{-1}$ in b reduciran niz dolžine n . Velja $\text{dom}(\phi(aa^{-1})) = \phi(b)([\{1, y\}])$. Namreč: $\text{dom}(\phi(aa^{-1})) = \text{dom}(\phi(a)^{-1}) = \text{im}(\phi(a)) = \text{im}(\phi(b)\phi(y)) = \phi(b)\phi(y)([\{1, y^{-1}\}]) = \phi(b)([\{1, y\}])$.

Sedaj trdimo, da je $\phi(b)([\{1, y\}]) = [[a]^\downarrow]$. Vzemimo $J \in \phi(b)([\{1, y\}])$. Tedaj je $J = b \cdot I$, kjer je $I \in [\{1, y\}]$. Torej je $a \in J$, saj je $a = by$ in $y \in I$. Posledično je $J \in [[a]^\downarrow]$. Sedaj dokažimo še v drugo smer, naj bo $J \in [[a]^\downarrow]$. Potem je $a \in J$ in ker je $b \leq_p a$, je tudi $b \in J$. Po lemi 35 je ideal $I = b^{-1} \cdot J$ element množice Y . Ker je $a = by$, sledi $y \in I$. Torej je $I \in [\{1, y\}]$. Ker je $\phi(b)(I) = b \cdot I = J$, vemo, da je $J \in \phi(b)([\{1, y\}])$.

Torej za reducirane nize a velja, da je $\text{dom}(\phi(aa^{-1})) = [[a]^\downarrow]$. Sedaj zapišimo idempotent $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})$ v Scheiblichovi normalni formi. Potem je $\phi(u) = \phi(a_1a_1^{-1}) \dots \phi(a_na_n^{-1})$. Domena $\phi(u)$ je unija domen $\phi(a_ia_i^{-1})$, saj je produkt elementov v Y unija elementov. Zato je domena $\phi(u)$ enaka $[[a_1, \dots, a_n]^\downarrow]$. ■

Izrek 38 (Ekvivalentnost dveh SNF). Naj bosta $u = (a_1a_1^{-1}) \dots (a_na_n^{-1})a$ in $v = (b_1b_1^{-1}) \dots (b_mb_m^{-1})b$ niza v Scheiblichovi normalni formi. Potem je $u \equiv v$ natanko tedaj, ko $\{a_1, \dots, a_n\} = \{b_1, \dots, b_m\}$ in $a = b$.

Dokaz. Implikacija v levo je po definiciji kongruence očitna. Lotimo se dokaza implikacije v desno smer. Po lemi 32 vemo že, da sta korena a in b enaka. Zato zapišemo:

$$(a_1a_1^{-1}) \dots (a_na_n^{-1})a \equiv (b_1b_1^{-1}) \dots (b_mb_m^{-1})a,$$

od tod pa velja

$$(a_1a_1^{-1}) \dots (a_na_n^{-1})aa^{-1} \equiv (b_1b_1^{-1}) \dots (b_mb_m^{-1})aa^{-1}.$$

Iz konstrukcije Scheiblichovih normalnih form velja, da je a predpona enega od nizov a_i in enega od nizov b_i . Uporabimo lemo 28 in dobimo:

$$u' = (a_1a_1^{-1}) \dots (a_na_n^{-1}) \equiv (b_1b_1^{-1}) \dots (b_mb_m^{-1}) = v'.$$

Torej je $\phi(u') = \phi(v')$. Po trditvi 37 vemo, da sta domeni $\phi(u') = [[a_1, \dots, a_n]^\downarrow]$ in $\phi(v') = [[b_1, \dots, b_m]^\downarrow]$ enaki. Ker imata enaka urejenostna ideala enaki množici maksimalnih elementov, sledi $\{a_1, \dots, a_n\} = \{b_1, \dots, b_m\}$. ■

Zgornji izrek 38, združen z 30, nam reši besedni problem.

Zgled 39. Kot smo pokazali že v zgledu 31, je množica komponent niza u oziroma v enaka $\{a, baa, bb\}$, koren pa je ba . Zaključimo, da sta niza u in v ekvivalentna.

LITERATURA

- [1] P. M. Higgins. *Techniques of Semigroup Theory*. Oxford University Press, New York, 1992.
- [2] G. Kudryavtseva. Povabilo v inverzne polgrupe. *Obzornik mat. fiz.*, 67(4):121–135, 2020.
- [3] M. V. Lawson. *Inverse Semigroups*. World Scientific, River Edge, 1998.
- [4] A. Myasnikov. Free groups. [Ogled: 4. 5. 2023], Spletna stran: <https://www.math.unl.edu/~mbrittenham2/classwk/990s08/public/myasnikov.1.free.groups.pdf>.