UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jaša Knap

KRATKI ZAKONI V GRUPAH

Delo diplomskega seminarja

Mentor: doc. dr. Urban Jezernik

Ljubljana, 2024

Kazalo

Kratki zakoni v grupah

Povzetek

TODO

Short Group Laws

Abstract

TODO

Math. Subj. Class. (2020): 20, 05C81
Ključne besede: ..., ...
Keywords: ..., ...

1 Uvod

Abstraktni produkt elementov $a_1, \dots, a_k$ ter njihovih inverzov $a_1^{-1}, \dots, a_k^{-1}$, je *$k$-črkovni zakon v grupi G*, če ima lastnost, da za vsako zamenjavo $a_1, \dots, a_k$ s konkretnimi elementi $g_1, \dots, g_k \in G$ dobimo rezultat $1_G \in G$. Zakonu 1 pravimo *trivialni zakon*, ki v kontekstu raziskovanja zakonov ni posebej zanimiv.

Najosnovnejši primer netrivialnega dvočrkovnega zakona se pojavi pri Abelovih grupah. Grupa G je namreč Abelova natanko tedaj, ko za vsaka elementa $g, h \in G$ velja $gh = hg$, kar je ekvivalentno zahtevi

$$ghg^{-1}h^{-1} = [g, h] = 1_G.$$

Grupa G je torej Abelova natanko tedaj, ko je štiričrkovna beseda $aba^{-1}b^{-1}$ v njej zakon.

Nadvse pomembno je vprašanje, ali vsaka grupa premore netrivialni zakon. Odgovor nanj je v splošnem negativen, kar bomo videli v nadaljevanju kot posledico trditve 5.4. Očitna posledica Lagrangeevega izreka pa je, da vsaka končna grupa G premore netrivialni zakon $a^{|G|}$, saj za vsak element $g \in G$ velja

$$g^{|G|} = 1_G.$$

To dejstvo si natančneje oglejmo na primeru simetrične grupe S_n. Zanjo po Lagrangeevem izreku velja enočrkovni zakon $a^{n!}$, katerega dolžina znaša $n!$, kar je po Stirlingovi formuli približno

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Asimptotsko gledano je to zelo dolg zakon, veliko krajši je na primer že zakon oblike $a^{\exp(S_n)}$, kjer smo označili $\exp(S_n) = \operatorname{lcm}(1, \dots, n)$, za katerega s pomočjo osnovnega izreka o praštevilih 5.7 dobimo asimptotsko oceno

$$\operatorname{lcm}(1, \dots, n) \sim e^n.$$

Trenutno najboljša ocena za dolžine kratkih zakonov izhaja iz članka [8], ki bo predstavljena v razdelku 5.1.

Na tej točki se naravno pojavi nekaj vprašanj: kako dolgi so najkrajši netrivialni zakoni za določeno grupo oziroma družino grup? Ali lahko ocenimo asimtotsko rast dolžine najkrajših netrivialnih zakonov za družine grup, recimo za družino $\mathrm{Sym}(n)$? Kaj pa za vse grupe moči n ali manj? Katere družine grup se še posebej naravno pojavljajo pri takšnem raziskovanju? Prav ta vprašanja bodo bistvo diplomske naloge, v kateri bom predstavil dosedanje rezultate ter različne pristope, ki so jih ubrali raziskovalci. Na koncu bom predstavil, kako lahko z uporabo računalnika dobimo vpogled v delež zakonov med besedami.

Zgodovinsko gledano so zgornja vprašanja razmeroma sodobna. Obravnavanje lastnosti zakonov namreč v nekem smislu sega že do Abela in Galoisa, saj lahko tako Abelove kot rešljive grupe zelo naravno karakteriziramo s pomočjo zakonov. Zakoni so pomembni tudi za obravnavo klasičnih Bursidovih problemov, ki matematikom burijo domišljijo že od začetka 20. stoletja. Ti problemi sprašujejo po končnosti specifičnih kvocientov prostih grup, kar bo nekoliko podrobneje razloženo v razdelku 6.

2 Osnovni pojmi za obravnavo zakonov

Za natančno formulacijo in razumevanje zakonov moramo uvesti pojem proste grupe.

2.1 Proste grupe

Naslednjo definicijo proste grupe najdemo v članku [16].

Definicija 2.1. Grupa F je *prosta* nad neprazno množico S, če za vsako preslikavo $\iota : S \to F$ in vsako grupo G in vsako preslikavo $\iota : X \to G$ obstaja natanko en homomorfizem $\tilde{\varphi} \in \mathrm{Hom}(F, G)$, da velja $\tilde{\varphi} \circ \iota = \varphi$. Z drugimi besedami, spodnji diagram komutira. Tej lastnosti pravimo *univerzalna lastnost prostih grup*.

Trditev 2.2. *Naj bo S neprazna množica. Potem do izomorfizma natančno obstaja največ ena prosta grupa nad množico S.*

Dokaz. Dokaz trditve je vzet iz [16, str. 4]. Naj bosta F in F' prosti grupi nad množico S. Označimo z i in j inkluziji $i : S \to F$ in $j : F'$, ki jima po definiciji 2.1 pripadata. Po univerzalni lastnosti prostih grup lahko inkluziji razširimo do homomorfizmov $\varphi_i : F' \to F$ in $\varphi_j : F \to F'$. (TODO vstavi komutativni diagram) Kompozitum $\varphi_i \circ \varphi_j : F \to F$ je na množici S identiteta. Ker sta tako $\varphi_i \circ \varphi_j$ kot id_F razširitvi inkluzije i, mora po enoličnosti razširitev veljati $\varphi_i \circ \varphi_j = \mathrm{id}_F$. Simetrično pokažemo še $\varphi_j \circ \varphi_i = \mathrm{id}_{F'}$, torej sta grupi F in F' izomorfni. □

Zaradi te trditve je $F(S)$ upravičena oznaka za prosto grupo nad množico S. Še več, grupi $F(S)$ in $F(T)$ sta si izomorfni kot grupi natanko tedaj, ko sta si S in T izomorfni kot množici. Zato bomo v primeru, ko je S končna množica moči k, namesto $F(S)$ pisali F_k.

Naj bo sedaj S poljubna neprazna množica. Definiramo grupo okrajšanih besed nad množico S kot

$$S^* := \{s_1 s_2 \cdots s_n | n \in \mathbb{N}, \forall i = 1, \dots, n.\, s_i \in S \cup S^{-1}, \forall i = 1, \dots n-1.\, s_i \neq s_{i+1}^{-1}\}.$$

Operacija nad njej je stikanje besed, ki jim nato še okrajšamo sosednje inverze. Ta operacija je dobro definirana, grupa S^* pa prosta nad množico S. Ti dejstvi sta natančno dokazani v viru ([11, str. 4, tridtev 1.9]). Po trditvi 2.2 sledi $S^* \cong F(S)$, zato si lahko elemente prostih grup predstavljamo kot okrajšane besede. Z upoštevanjem tega dejstva lahko elementom proste grupe $F(S)$ definiramo dolžino.

Definicija 2.3. Naj bo beseda $w \in F(S)$ oblike $w = s_1 \cdots s_n$. Potem število $l(w) := n$ imenujemo *dolžina besede w*.

Opomba 2.4. Po definiciji množenja besed v prostih grupah je očitno, da za vsaki besedi w_1, w_2 velja trikotniška neenakost $l(w_1 w_2) \leq l(w_1) l(w_2)$.

Pri konstrukciji zakonov stalno uporabljamo naslednjo na videz očitno trditev, ki jo vendarle moramo dokazati.

Trditev 2.5. *Proste grupe so* torzijsko proste*. Z drugimi besedami, vsi elementi razen enote so neskončnega reda.*

Dokaz. Naj bo $F(S)$ prosta grupa nad neprazno množico S. Recimo, da obstaja beseda $w \in F(S)$ končnega reda oblike $w = a_1 a_2 \dots a_n$ za paroma neinverzne $a_1, \dots, a_n \in S$. Naj bo preslikava $j : S \to (\mathbb{Z}, +)$, ki vse elemente a_i slika v pozitivna števila. Po univerzalni lastnosti prostih grup jo lahko razširimo do homomorfizma $\varphi_j \in \mathrm{Hom}(F(S), \mathbb{Z})$. Ker je φ_j homomorfizem, bo $\varphi(w) = \sum_{i=1}^{n} \varphi(a_i) > 0$. To je prosislovno, saj bi moral red elementa $\varphi(w)$ deliti red besede w, grupa $(\mathbb{Z}, +)$ pa je torzijsko prosta, zato je element $\varphi_j(w)$ v njej neskončnega reda. $\square$

Brez dokaza bomo privzeli Nielsen–Schreierjev izrek, ki je klasični rezultat v teoriji prosti grup. Potrebovali ga bomo za dokaz komutatorske leme, še bolj izrazito pa pri obravnavi zakonov z računalnikom v razdelku 6.

Izrek 2.6 (Nielsen–Schreierjev izrek)**.** *Vsaka podgrupa proste grupe je prosta.*

Bralec lahko dokaz najde v [11, str. 5–8].

2.2 Definicija in osnovne lastnosti zakonov

Za začetek uvedimo blago zlorabo notacije. Naj bo podana prosta grupa $F_k = \langle a_1, \dots, a_k \rangle$ in naj bo w beseda v njej. Naj bo G grupa in naj bodo $g_1, \dots, g_k \in G$. Potem definiramo

$$w(g_1, \dots, g_k) := \varphi(w),$$

kjer je $\varphi \in \mathrm{Hom}(F_k, G)$ po univerzalni lastnosti induciran s slikami $a_i \mapsto g_i$ za $i = 1, \dots, k$. To je formalna definicija intuitivne ideje „vstavljanja konkretnih elementov grupe v abstraktne elemente“iz uvodnega poglavja. Z njeno pomočjo definiramo zakone.

Definicija 2.7. Beseda $w \in F_k$ je *k-črkovni zakon v grupi G*, če za vse k-terice elementov $g_1, \dots, g_k \in G$ velja $w(g_1, \dots, g_k) = 1_G$. Za vsako podgrupo $H \leq G$ pravimo tudi, da je $w \in F_k$ *k-črkovni zakon v podgrupi H*, če za vse k-terice elementov $h_1, \dots, h_k \in H$ velja $w(h_1, \dots, h_k) = 1_G$.

Ta definicija nam omogoča vpogled v strukturo zakonov. Naj $K(G, k) \subseteq F_k$ *označuje množico k-črkovnih zakonov v grupi G*. Potem v luči prejšnje definicije velja

$$K(G, k) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi).$$

Ta množica je končni presek edink v G in posledično tudi sama edinka. Še več, je karakteristična, saj za vsak avtomorfizem $\alpha \in \mathrm{Aut}(F_2)$ velja

$$K(G, k) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi \circ \alpha).$$

To je preprosta posledica dejstva, da φ preteče grupo $\mathrm{Hom}(F_k, G)$ natanko tedaj, ko jo preteče $\varphi \circ \alpha$.

Lema 2.8. *Naj bo G grupa ter $H_1, \dots, H_n$ njene podgrupe končnega indeksa, torej $[G : H_i] < \infty$ za $i = 1, \dots, n$. Potem je tudi $\bigcap_{i=1}^{n} H_i$ podgrupa končnega indeksa v G in velja*

$$\left[G : \bigcap_{i=1}^{n} H_i\right] \leq \prod_{i=1}^{n} [G : H_i].$$

Dokaz. Dovolj je dokazati trditev za $n = 2$, za višje vrednosti sledi z indukcijo. Naj bosta $H_1, H_2 \leq G$ podgrupi končnega indeksa, označimo $S := H_1 \cap H_2$, ki je podgrupa v G. Naj bosta A_1 in A_2 množici odsekov podgrup H_1 in H_2 v G ter naj bo A množica odsekov podgrupe S v G. Definiramo preslikavo $f : A \to A_1 \times A_2$ s predpisom $f(gS) = (gH_1, gH_2)$. Desna smer sklepa

$$gS = hS \iff gh^{-1} \in H_1,\, gh^{-1} \in H_2 \iff gH_1 = hH_1,\, gH_2 = hH_2$$

nam podaja dobro definiranost, leva pa injektivnost preslikave f, ki nam podaja oceno $|A| \leq |A_1||A_2|$. $\square$

Z uporabo te leme direktno sledi, da je v primeru končnosti grupe G grupa $K(G, k)$ podgrupa končnega indeksa največ $|G|^{|G|^k}$ v F_k. Za vsak homomorfizem $\varphi \in \mathrm{Hom}(F_k, G)$ namreč po prvem izreku o izomorfizmu velja

$$|F_k/\ker\varphi| = |\mathrm{im}\,\varphi| \leq |G|.$$

To dejstvo bo še posebej pobmembno pri iskanju zakonov z računalnikom.

Definicija 2.9. Naj bo G grupa in $S \subseteq G$ njena *simetrična* podmnožica. To pomeni, da velja $S = S^{-1} := \{s^{-1} | s \in S\}$. Potem $\mathrm{Cay}(G, S)$ označuje graf z vozlišči $V = G$ in povezavami $E = \{(p, q) |\, p^{-1}q \in S\}$. Imenujemo ga *Cayleyjev graf grupe G, generiran z množico S.*

Opomba 2.10. Pogoj simetričnosti $S = S^{-1}$ nam pove, da je $\mathrm{Cay}(G, S)$ pravi graf in ne zgolj usmerjen. Imamo namreč

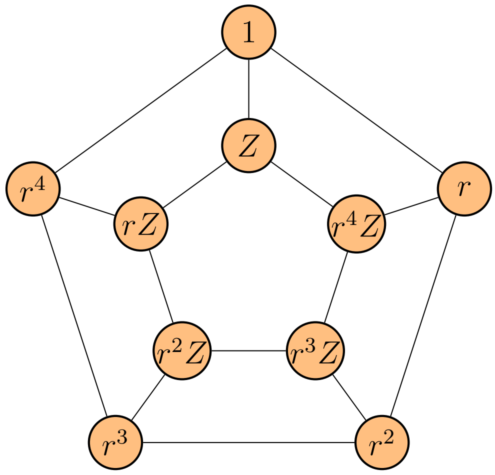
$$(p, q) \in E \iff p^{-1}q \in S \iff q^{-1}p \in S \iff (q, p) \in E.$$

Preden si ogledamo dva primera, dokažimo nasledjo preprosto, a pomembno trditev.

Trditev 2.11. *Naj bo S končna grupa moči k. Cayleyjev graf $Cay(G, S)$ je $|S|$-regularen, povezan graf.*

Dokaz. Naj bo $g \in G$ vozlišče Cayleyjevega grafa $\mathrm{Cay}(G, S)$. Potem je g povezano z enoto 1_G, saj je $\langle S \rangle = G$, torej lahko zapišemo $g = s_1 s_2 \cdots s_n$ za neke elemente $s_i \in S$. Ta produkt določa povezavo v Cayleyjevem grafu. Ker je vsako vozlišče povezano z enoto 1_G, je graf povezan. Iz $gs_i = gs_j$ sledi $s_i = s_j$, zato iz vsakega vozlišča vodi natanko $|S|$ različnih povezav. $\square$

Primer 2.12. Na spodnjih slikah imamo Cayleyjev graf grupe diedrske grupe $D_{10} = \langle r, Z \rangle$ za različni generatorski množici.



$\diamondsuit$

Definicija 2.13. Številu

$$\alpha_k(G) := \min \{l(w) | \, w \in F_k \setminus \{1\} \text{ je zakon v } G\} \cup \{\infty\}$$

rečemo *k-črkovna ožina grupe G.*

Opomba 2.14. Ime ožina grupe – ki je uporabljeno na primer v virih [14], [1] in [13] – je nekoliko zavajajoče. Izhaja iz Cayleyjevega grafa grupe, vsak njegov cikel $g_1, g_2, \ldots, g_n, g_1$ namreč podaja zvezo $s_1 s_2 \cdots s_n = 1_G$ za elemente $s_i \in S$, kjer za $i = 2, \ldots, n$ velja $s_i = g_{i-1}^{-1} g_i$ in $s_1 = g_n^{-1} g_1$. V kontekstu zakonov je to ime do neke mere neupravičeno, saj beseda $s_1 s_2 \cdots s_n$ ni nujno zakon v grupi. Če si pogledamo na primer grupo $C_3 \times C_5 = \langle (\xi, 1), (1, \eta) \rangle$, bo Cayleyjev graf $\mathrm{Cay}(C_3 \times C_5, \{(\xi, 1)^{\pm 1}, (1, \eta)^{\pm 1}\})$ vseboval 3-cikel, ki ga porodi generator $(\xi, 1)$. Po drugi strani pa beseda ξ^3 očitno ni zakon v grupi $C_3 \times C_5$, ki premore element reda 5. Ker je grupa $C_3 \times C_5$ Abelova, ni težko razmisliti, da velja $\alpha_k(C_3 \times C_5) = 4$ za $k \geq 2$ in $\alpha_1(C_3 \times C_5) = 15$.

Izkaže se, da so najbolj zanimivi in za obravnavo relevantni dvočrkovni zakoni. To nam sporočata naslednji dve trditvi.

Trditev 2.15. *Obstaja vložitev grupe $F_{2 \cdot 3^k} = \langle a_1, \ldots, a_{2 \cdot 3^k} \rangle$ v grupo $F_2 = \langle a, b \rangle$, da velja $l(a_i) = 2k + 1$, kjer $l(w)$ označuje dolžino besede $w \in F_2 = \langle a, b \rangle$.*

Dokaz. Dokaz trditve ni posebno zahteven, vendar je nekoliko preveč tehničen za naše potrebe, saj bi zahteval uvedbo in razumevanje pojmov Schreierjevega grafa in fundamentalne grupe grafa, ki ju sicer tekom naloge ne potrebujemo. Naveden je v [14, str. 5], glavna ideja je obravnavati Cayleyev graf proste grupe F_2 z dvema generatorjema. Drevo vseh besed dolžine k na ustrezen način dopolnimo (do Schreierjevega grafa) tako, da dodamo povezave listom. Pri tem dobimo cikle dolžine $2k + 1$ in (s pomočjo fundamentalne grupe grafa) utemeljimo, da lahko jih lahko obravnavamo kot elemente $F_{2 \cdot 3^k}$, vložene v F_2. $\square$

Posledica 2.16. *Naj bo G grupa in $k \geq 2$ naravno število. Potem velja*

$$\alpha_k(G) \leq \alpha_2(G)$$

in

$$\alpha_2(G) \leq \left(2 \left\lceil \log_3 \left(\frac{k}{2}\right) \right\rceil + 1\right) \alpha_k(G).$$

Dokaz. Prva neenakost je očitna, saj so vsi dvočrkovni zakoni tudi k-črkovni zakoni. Druga neenakost drži, saj lahko po prejšnji trditvi vložimo $F_{2\lceil \log_3(\frac{k}{2})\rceil}$ v F_2 tako, da noben generator ni daljši od $2\left\lceil \log_3(\frac{k}{2})\right\rceil + 1$. Hkrati velja $F_k \subseteq F_{2\lceil \log_3(\frac{k}{2})\rceil}$, kar nam da želeno neenakost. $\square$

2.3 Teorija naključnih sprehodov

Za obravnavo zakonov v simetričnih grupah bomo potrebovali naključne sprehode, natančneje lene naključne sprehode (TODO poglej, če se res tako imenuje). Naj bo G grupa, generirana s simetrično podmnožico $S \subseteq G$. Tekom tega razdelka naj bo $\Gamma = \mathrm{Cay}(G, S)$, ki je po prejšnjem premisleku

Definicija 2.17. Leni naključni sprehod je naključno zaporedje elementov $w_n \in S$ za $n \in \mathbb{N} \cup \{0\}$, porojeno s formulo

$$\mathbb{P}(w_{n+1} = g |\, w_n = h) = \begin{cases} \frac{1}{2}; & \text{če } g = h, \\ \frac{1}{2|S|}; & \text{če } g = sh \text{ za neki } s \in S. \end{cases}$$

Na vsakem koraku lenega naključnega sprehoda se torej z verjetnostjo 1/2 element ne spremeni, z verjetnostjo 1/2 pa se naključno spremeni v enega od svojih sosedov, ki jih je $|S|$. To lahko opišemo tudi z matrikami. Recimo, da je u_n vejretnostna porazdelitev $|G|$ razsežnega vektorja, ki predstavlja vozlišča grafa Γ, po n-tem koraku in recimo, da začetno porazdelitev u_0 poznamo. Dalje, definiramo matriko lenega naključnega sprehoda $M \in M_{|G|}(\mathbb{R})$, s predpisom

$$M = \frac{1}{2}\left(I + \frac{1}{|S|}A\right) = \frac{1}{2}(I + \tilde{A}),$$

kjer smo z A označili matriko sosesščine grafa Γ, z $\tilde{A}$ pa smo označili matriko $\frac{1}{|S|}A$, da . Ni težko premisliti, da po definiciji 2.17 sledi zveza

$$u_n = M^n u_0,$$

ki nam omogoča vpogled v lastnosti naključnih sprehodov.

Lema 2.18. *Matrika M je diagonalizabilna, sebiadjungirana in njene lastne vrednosti ležijo v intervalu* $[0, 1]$.

Dokaz. Ker je realna matrika M simetrična, je diagonalizabilna, sebiadjungirana in velja, da so vektorji, ki pripadajo paroma različnim lastnim vrednostim, med seboj ortogonalni. Enako velja za matriko A. Sebiadjungiranost nam implicira realnost lastnih vrednosti matrik M in A. Z oceno matričnih norm

$$\sqrt{\lambda_{\max}(\tilde{A}^2)} = \sqrt{\lambda_{\max}(\tilde{A}^T\tilde{A})} = ||\tilde{A}||_2 \leq \sqrt{||A||_1}||\tilde{A}||_\infty = 1$$

sledi, da ima matrika $\tilde{A}$ lastne vrednosti v intervalu $[-1, 1]$, kar pomeni, da lastne vrednosti matrike M ležijo v intevalu $[0, 1]$. $\square$

Ker vemo, da so vse lastne vrednosti realne, jih lahko po razvrstimo po velikosti:

$$1 \geq \lambda_1(G,S) \geq \lambda_2(G,S) \geq \ldots \geq \lambda_{|G|}(G,S).$$

Izkaže se, da je glede na izbiro grupe G in njene generirajoče množice S lastna vrednost $\lambda_1(G,S) = 1 > \lambda_2(G,S)$. (TODO, posledica tega, da je Γ povezan + konvergence zaporedja) Razliko $1 - \lambda_2(G,2)$ imenujemo *spektralna razlika* grafa Γ.

Definicija 2.19. Diameter Cayleyjevega grafa $\Gamma = \mathrm{Cay}(G,S)$ je število

$$\mathrm{diam}(G,S) := \min\left\{n \in \mathbb{N} | \forall g \in G. \exists s_1, \ldots, s_n \in S \cup \{1_G\}.g = s_1 \cdots s_n\right\}$$

Intuitivno nam diameter Cayleyjevega grafa poda najmanjše število korakov, po katerem lahko naključni sprehod po grafu Γ doseže poljubni element grupe G. Za vse končnogenerirane in posledično končne grupe je diameter dobro definiran. Za ocenjevanje dolžin zakonov v grafih je bistvena sledeča zveza med diametrom grafa in spektralno razliko lenega naključnega sprehoda.

Trditev 2.20. *Velja zveza*

$$1 - \lambda_1(G,S) \geq \frac{1}{2|S|\,\mathrm{diam}(G,S)^2}.$$

Dokaz. □

Od tod sledi pomembna posledica

Posledica 2.21. *Naj bo vektor $u = \frac{1}{|G|}I$ in naj bo e_1 bazni vektor enote 1_G (TODO tole bolje razloži). Potem velja ocena*

$$|M^n e_1 - u| \leq \lambda_1(G,S)^n \leq \left(1 - \frac{1}{2|S|\,\mathrm{diam}(G,S)^2}\right)^n.$$

Dokaz. Desna neenakost je direktna posledica trditve 2.20. (TODO zakaj leva stran enačbe ... to bi se moralo dati intuitivno dokazati) □

Za konec potrebujemo še zadnjo lemo.

Lema 2.22. *Naj bo E podmnožica grupe G in naj bo $\alpha := |E|/|G|$ in naj bo $(w_n)_{n\in\mathbb{N}}$ leni naključni sprehod. Če velja ocena*

$$n \geq 2|S|\,\mathrm{diam}(G,S)^2 \log(2|G|),$$

velja $\mathbb{P}(w_n \in E) \geq \alpha/2$.

Dokaz. TODO, to je Cauchy–Schwarz □

Glavni rezultat, ki bo zagotovil obstoj kratkih zakonov v simetričnih grupah, je Helfgott–Seressov izrek, ki omeji diameter Cayleyjevih grafov simetričnih grup, generiranih s parom elementov.

Izrek 2.23 (Helfgott–Seress)**.** *Naj par $(\sigma,\tau) \in S_n^2$ generira grupo S_n, torej $\langle\sigma,\tau\rangle = S_n$. Potem obstaja konstanta $C > 0$, da je diameter grafa $\Gamma = \mathrm{Cay}(S_n, \{\sigma^{\pm 1}, \tau^{\pm 1}\})$ največ*

$$\exp(C \log(n)^4 \log(\log(n))).$$

Dokaz tega izreka je zelo težek in se močno nanaša na klasifikacijo končnih enostavnih grup, zato ga opuščamo. Bralec ga lahko najde v članku [6].

3 Komutatorska in razširitvena lema

3.1 Komutatorska lema

Recimo, da poznamo zakone v nekaterih podmnožicah grupe G, zanima pa nas, kako bi iz njih zgradili zakone za večje podmnožice te grupe. Na to vprašanje odgovarjata komutatorska in razširitvena lema, ki sta ključni orodji pri obravnavanju zakonov. Začeli bomo z dokazom komutatorske leme, za katero bomo potrebujemo nekaj definicij.

Definicija 3.1. Naj bo G grupa in $w \in F_k$. Potem množico

$$Z(G, w) := \left\{(g_1, .., g_k) \in G^k \middle| w(g_1, \dots, g_k) = 1_G\right\}$$

imenujemo *izginajoča množica besede w v grupi G*. Tu $w(g_1, \dots, g_k)$ označuje sliko v skladu z notacijo na začetku razdelka 2.2.

Definicija 3.2. Naj bo G grupa. Element $g \in G$ je *periodičen*, če je oblike $g = h^n$ za neki element $h \in G$ in število $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Sicer rečemo, da je g *aperiodičen*.

Lema 3.3. *Naj bosta $w_1, w_2 \in F_2 = \langle a, b\rangle$ besedi. Potem velja natanko ena izmed naslednjih trditev.*

1. *Besedi w_1 in w_2 komutirata in sta periodični z isto osnovo: Obstaja element $c \in F_2$ ter števili $k_1, k_2 \in \mathbb{Z}$, da velja $w_1 = c^{k_1}$ in $w_2 = c^{k_2}$.*
2. *Podgrupa $\langle w_1, w_2\rangle \subseteq F_2 = \langle a, b\rangle$ je izomorfna prosti grupi F_2.*

Dokaz. TODO $\square$

Osnovna ideja komutatorske leme je pravzaprav preprosta. Recimo, da imamo besedi $w_1, w_2 \in F_2 \setminus \{1_{F_2}\} = \langle a, b\rangle$, ki jima pripadata izginjajoči množici $Z(G, w_1)$ ter $Z(G, w_2)$. oglejmo si komutator $w = [w_1, w_2]$. Če vzamemo par $(g, h) \in Z(G, w_1)$, bo veljalo

$$w(g, h) = [w_1(g, h), w_2(g, h)] = [1_{F_2}, w_2(g, h)] = 1_{F_2}.$$

Seveda velja simetrično tudi za pare druge izginjajoče množice. Od tod sledi sklep

$$Z(G, [w_1, w_2]) \supseteq Z(G, w_1) \cup Z(G, w_2).$$

Glavni problem, na katerega lahko naletimo pri takšnem združevanju besed, je potencialna trivialnost komutatorja $[w_1, w_2]$, ki bi ustrezala trivialnemu zakonu. Po lemi 3.3 je komutator $[w_1, w_2]$ trivialen natanko tedaj, ko sta besedi w_1 in w_2 periodični z isto osnovo. Komutatorska lema podaja konstrukcijo, ki preprečuje pojav takšnih zapletov. V sledeči obliki se pojavi v članku [8] in magistrskem delu [14], po katerem so povzeti dokazi.

Lema 3.4. *Naj bo $k \geq 2$, $e \in \mathbb{N}$ in naj bodo besede $w_1, \dots, w_m \in F_k$ netrivialne, pri čemer je $m = 2^e$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 2m \left(m + \sum_{i=1}^{m} l(w_i)\right),$$

da za vsako grupo G velja

$$Z(G, w) \supseteq Z(G, w_1) \cup \ldots \cup Z(G, w_m).$$

Dokaz. Dokaz poteka z indukcijo po $e \in \mathbb{N}$. Naj bo $F_k = \langle a_1, \ldots, a_k \rangle = \langle S \rangle$. Za $e = 0$ (oziroma $m = 1$) vzamemo $w = [s, w_1]$, kjer je $s \in S$ takšna črka, da beseda w_1 ni periodična z osnovo s. To lahko zaradi pogoja $k \geq 2$ vedno storimo. Zaradi ustrezne izbire je komutator $[s, w_1]$ po lemi 3.3 aperiodičen z dolžino največ $2(l(w_1) + 1)$. Kot smo videli v predhodnem razmisleku, za poljubno grupo G velja $\mathrm{Z}(G, w) \supseteq \mathrm{Z}(G, s) \cup \mathrm{Z}(G, w_1)$.

Zdaj se lotimo indukcijskega koraka v primeru $e \geq 1$ oziroma $m \geq 2$. Naj bodo podane besede $w_1, \ldots, w_{m/2}, w_{m/2+1}, \ldots, w_{2m}$. Po indukcijski predpostavki obstajata aperiodični besedi $v_1, v_2 \in F_k$, da velja

$$l(v_1) \leq m\left(\frac{m}{2} + \sum_{i=1}^{m/2} l(w_i)\right), \quad l(v_2) \leq m\left(\frac{m}{2} + \sum_{i=m/2+1}^{m} l(w_i)\right)$$

in

$$\mathrm{Z}(G, v_1) \supseteq \mathrm{Z}(G, w_1) \cup \ldots \cup \mathrm{Z}(G, w_{m/2}),$$
$$\mathrm{Z}(G, v_2) \supseteq \mathrm{Z}(G, w_{m/2+1}) \cup \ldots \cup \mathrm{Z}(G, w_m)$$

za vsako grupo G.

Zdaj moramo le še ugotoviti, kako lahko besedi v_1 ter v_2 ustrezno združimo. Po lemi 3.3 vemo, da bo komutator $[v_1, v_2]$ trivialen natanko v primeru $v_1 = v_2^{\pm 1}$, ker sta v_1 in v_2 po predpostavki aperiodični. V primeru, da sta periodični, imamo

$$\mathrm{Z}(G, w_1) = \mathrm{Z}(G, w_2)$$

in lahko nastavimo $w := v_1$ ali $w := v_2$, pri čemer je pogoj na dolžino besede w očitno izpolnjen. Če imamo $v_1 \neq v_2^{\pm 1}$, nastavimo $w := [v_1, v_2]$. V tem primeru je beseda w aperiodična, kot je razloženo v viru [15]. Tega rezultata ne bomo podrobneje predstavili, saj bi lahko aperiodičnost zagotovili na enak način kot v indukcijskem koraku z minimalno slabšim rezultatom. Indukcijska predpostavka nam zagotavlja

$$l(w) \leq 2m\left(\frac{m}{2} + \sum_{i=1}^{m/2} l(w_i)\right) + 2m\left(\frac{m}{2} + \sum_{i=m/2+1}^{m} l(w_i)\right) = 2m\left(m + \sum_{i=1}^{m} l(w_i)\right).$$

□

Lemo brez težav posplošimo tudi na število besed, ki ni dvojiška potenca.

Lema 3.5. *Naj bo $k \geq 2$ in naj bodo podane netrivialne besede $w_1, \ldots, w_m \in F_m$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 8m\left(m + \sum_{i=1}^{m} l(w_i)\right),$$

da za vsako grupo G velja

$$\mathrm{Z}(G, w) \supseteq \mathrm{Z}(G, w_1) \cup \ldots \cup \mathrm{Z}(G, w_m).$$

Dokaz. Naj bo e takšno naravno število, da velja $m \leq 2^e < 2m$. Nastavimo

$$w_1' := w_1, \ldots, w_m' := w_m, w_{m+1}' := w_1, \ldots, w_{2^e}' := w_{2^e - m}.$$

Ker velja $m < 2m$ in $\sum_{i=1}^{2^e} w_i' \leq 2\sum_{i=1}^{m} l(w_i)$, želena ocena sledi z uporabo leme 3.4. □

Ta rezultat lahko nekoliko omilimo, da dobimo bolj praktično oceno.

Posledica 3.6. *Naj bo $k \geq 2$ in naj bodo podane netrivialne besede $w_1, \ldots, w_m \in F_k$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 8m^2 \left(1 + \max_{i=1,\ldots,m} l(w_i)\right)$$

Dokaz. To je direktna posledica leme 3.5 skupaj z dejstvom, da je

$$\sum_{i=1}^{m} l(w_i) \leq m \max_{i=1,\ldots,m} l(w_i).$$

□

Primer 3.7. Najelegantnejša uporaba komutatorske leme se pojavi pri obravnavi grupe kot direktnega produkta. Naj bo recimo $G = C_5 \times D_{10}$. V podgrupi C_5 imamo zakon $x^5 \in F_2$ dolžine 5, razširitvena lema 3.10 pa nam bo povedala, da obstaja zakon dolžine 8 v D_{10}. Po lemi 3.4 torej obstaja netrivialna beseda $w \in F_2$ dolžine največ $2 \cdot (5 + 8) = 26$, ki je zakon v grupi G. ♢

Primer 3.8. Naj bo G grupa. Recimo, da red vsakega njenega elementa deli vsaj eno izmed naravnih števil $n_1 \ldots, n_m$. Če za vsak $i = 1, \ldots, m$ uvedemo množico $H_{n_i} := \{g \in G | g^{n_i} = 1_G\}$, očitno velja, da je $\bigcup_{i=1}^m H_{n_i} = G$. Ker za vsak i velja $Z(G, a^{n_i}) = H_{n_i} \times G$, lahko s pomočjo komutatorske leme 3.6 združimo besede a^{n_i} v besedo w dolžine

$$l(w) \leq 8m^2 \left(1 + \max_{i=1,\ldots,m} n_i\right),$$

ki je zakon v grupi G, saj velja

$$Z(G, w) \supseteq \bigcup_{i=1}^{m} Z(G, a^{n_i}) = \bigcup_{i=1}^{m} H_{n_i} \times G = G \times G.$$

♢

Čeprav sta ta primera razmeroma enostavna, sta ključna pri praktično vseh konstrukcijah zakonov, kar bomo videli recimo na koncu razdelka 5.2 pri obravnavi družine grup $\mathrm{PSL}_2(q)$.

3.2 Razširitvena lema

Nekoliko bolj povezana s strukturo grup je razširitvena lema. Za njeno formulacijo najprej definirajmo kratka eksaktna zaporedja.

Definicija 3.9. Naj bodo A, B, C grupe in naj $\mathbf{1}$ označuje trivialno grupo. Kratko eksaktno zaporedje je zaporedje homomorfizmov

$$\mathbf{1} \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to \mathbf{1},$$

kjer je $\ker \psi = \operatorname{im} \varphi$, φ je injektivni in ψ surjektivni homomorfizem.

Lema 3.10. *Naj bo N edinka v grupi G in naj bosta $i : N \to G$ inkluzija ter $\pi : G \to G/N$ kanonična projekcija. To lahko zapišemo z naslednjim kratkim eksaktnim zaporedjem.*

$$\mathbf{1} \to N \xrightarrow{i} G \xrightarrow{\pi} G/N \to \mathbf{1}$$

Naj bo $F_k = \langle a_1, \ldots, a_k \rangle = \langle S \rangle$. Naj bo $w_N \in F_k$ netrivialni zakon v grupi N in $w_{G/N} \in F_k$ netrivialni zakon v kvocientu G/N. Potem obstaja netrivialni k-črkovni zakon v grupi G dolžine kvečjem $l(w_N)l(w_{G/N})$.

Dokaz. Dokaz je prirejen po [14, str. 10] in obravnava dva možna primera oblike zakona $w_{G/N}$. V prvem primeru je $w_{G/N}$ enočrkovni zakon, torej je oblike $w_{G/N} = s^n$ za neko črko $s \in S$ in neničelno celo število n. V tem primeru je za vsak $i = 1, \ldots, k$ beseda a_i^n zakon v kvocientu G/N. Definirajmo besedo

$$w := w_N(a_1^n, \ldots, a_k^n).$$

Ker je za vsak $i = 1, \ldots, k$ beseda a_i^n zakon v kvocientu, preslikava $g \mapsto g^n$ vse elemente iz G slika v elemente edinke N. Ker je w_N netrivialni zakon v grupi N in med paroma različnimi besedami a_i^n ne more priti do krajšanja, je beseda w netrivialni zakon v grupi G.

Če $w_{G/N}$ ni enočrkovni zakon, lahko brez škode za splošnost predpostavimo, da je oblike $w_{G/N} = a_1 w'_{G/N} a_2$, kjer se $w'_{G/N}$ niti ne začne z a_1^{-1} niti ne konča z a_2^{-1}. To storimo z zaporednim izvajanjem enega izmed treh korakov:

- Če je zakon $w_{G/N}$ oblike $a_1 w'_{G/N} a_1$, ga konjugiramo s črko a_1 tolikokrat, da se zadnja črka razlikuje od a_1.
- Če je zakon oblike $w_{G/N}$ oblike $a_1 w'_{G/N} a_1^- 1$, ga konjugiramo s črko a_1^{-1}, s čimer zmanjšamo problem.
- Če zakon ni ene izmed zgornjih dveh oblik, izvedemo takšno bijektivno transformacijo črk, da se beseda začne z a_1 in, če je le mogoče, konča z a_2. To transformacijo nam inducira univerzalna lastnost prostih grup.

Pri tem se zavedajmo, da zakoni v grupi tvorijo karakteristično edinko proste grupe F_k (glej razmislek pod definicijo 2.7), zato je uporaba zgoraj naštetih transformacij legitimna. Nato definiramo besede

$$w_i := w_{G/N}(a_i, \ldots, a_k, a_1, \ldots, a_{i-1}).$$

Ni težko preveriti, da so netrivialne kombinacije besed w_i, torej $w_i w_j$, $w_i^{-1} w_j$, $w_i^{-1} w_j^{-1}$, $w_i w_j^{-1}$, $w_i w_i$, $w_i^{-1} w_i^{-1}$ za vse paroma različne $i, j \in \{1, \ldots, k\}$, okrajšane. Zato je

$$w := w_N(w_1, \ldots, w_k)$$

netrivialni zakon za grupo G. Vse besede w_i namreč inducirajo preslikave, ki G slikajo v N, w_N pa je netrivialni zakon za N. □

Primer 3.11. S pomočjo razširitvene leme lahko dokažemo, da za vsak $n \in \mathbb{N}$ obstaja zakon $w \in F_2$ v diedrski grupi D_{2n} dolžine 8. Ker ima podgrupa $\langle r \rangle \subseteq D_{2n}$ indeks 2, je edinka, zato lahko tvorimo kratko eksaktno zaporedje

$$\mathbf{1} \to \langle r \rangle \xrightarrow{i} D_{2n} \xrightarrow{\pi} D_{2n}/\langle r \rangle \to \mathbf{1}.$$

Ker je podgrupa $\langle r \rangle$ Abelova, je v njej zakon beseda $[a,b] = aba^{-1}b^{-1}$, grupa $D_{2n}/\langle r \rangle$ pa je moči 2 in je zato v njej zakon beseda a^2. Po lemi 3.10 torej obstaja beseda $w \in F_2$ dolžine $l(w) \leq 8$, ki je zakov v D_{2n}. Če sledimo konstrukciji izreka, vidimo, da je to natanko beseda $w = [a^2, b^2] = a^2b^2a^{-2}b^{-2}$. $\diamondsuit$

Iz primera je razvidno, da je moč razširitvene leme je še posebej izrazita, kadar ima grupa kakšno edinko z lepimi lastnosti, kot so na primer rešljivost, nilpotentnost ali celo Abelovost. Od tod sledi tudi, da so s stališča preučevanja zakonov *virtualno nilpotentne* oziroma *rešljive grupe* – torej grupe, ki imajo nilpotentno oziroma rešljivo edinko končnega indeksa – praktično enake nilpotentnim oziroma rešljivim. Naravna posledica razširitvene leme je tudi dejstvo, da bistveno vlogo pri iskanju kratkih zakonov igrajo enostavne grupe, saj lahko problem iskanja zakonov v neenostavnih grupah vedno prevedemo na dva manjša; na problema edinke in njenega kvocienta.

4 Nilpotentne in rešljive grupe

4.1 Definicija in osnovne lasntosti

Intuitivno gledano so nilpotntne in rešljive grupe tiste, ki so po svoji strukturi še najbolj podobne Abelovim. Da jih lahko vpeljemo, moramo najprej uvesti nekaj pojmov.

Definicija 4.1. Naj bo G grupa in $H, K \leq G$ njeni podgrupi. Potem definiramo *komutator podgrup H in K* kot podgrupo

$$[H, K] = \langle [h, k] | h \in H, k \in K \rangle.$$

Definicija 4.2. Naj bo G grupa in $(H_k)_{k \geq 1}$ padajoče zaporedje njenih podgrup, torej $H_{i+1} \subseteq H_i$ za vsak $i \geq 1$. Rečemo, da se *zaporedje $(H_k)_{k \geq 1}$ izteče z grupo K*, če obstaja naravno število n, da velja $H_k = K$ za vsako naravno število $k \geq n$.

Definicija 4.3. Grupa G je *nilpotentna*, če se *spodnja centralna vrsta* $(\gamma_k(G))_{k \geq 1}$, podana rekurzivno z

$$\gamma_1(G) := G \text{ in } \gamma_{k+1}(G) := [\gamma_k(G), G],$$

izteče s trivialno grupo. Najmanjšemu številu d, za katero je $\gamma_{d+1} = \{1_G\}$, rečemo *razred nilpotentnosti grupe G*.

Na kratko razmislimo, da je vsak člen spodnje centralne vrste $\gamma_k(G)$ edinka v grupi G. Osnovna ideja je, da lahko konjugiranje prenesemo v notranjost komutatorja: Za poljubne elemente $g, h, k \in G$ velja zveza

$$[g, h]^k = kghg^{-1}h^{-1}k^{-1} = kgk^{-1}khk^{-1}kg^{-1}k^{-1}kh^{-1}k^{-1} = [kgk^{-1}, khk^{-1}] = [g^k, h^k].$$

Elementi grupe $\gamma_1(G) = [G, G]$ so po definiciji oblike $\prod_{i=1}^n [g_i, h_i]$ za neke elemente $g_i, h_i \in G$, zato za vsak element $k \in G$ velja

$$\left(\prod_{i=1}^n [g_i, h_i] \right)^k = \prod_{i=1}^n [g_i^k, h_i^k].$$

S tem smo dokazali, da je $\gamma_1(G)$ edinka v G, z indukcijo pokažemo enako za vse nadaljnje člene. S tem smo hkrati utemeljili tudi, da za vsako število $k \geq 0$ velja $\gamma_{k+1}(G) \triangleleft \gamma_k(G)$.

Celo družino primerov nilpotentnih grup nam podaja naslednja ugotovitev.

Trditev 4.4. *Vse p-grupe so nilpotentne. Natančneje, če je $|G| = p^d$ za neko naravno število $d \geq 1$, potem je G nilpotentna razreda največ d.*

Dokaz. Naj bo $|G| = p^k$. Dokaz poteka z indukcijo po k. Za $k = 1$ je grupa Abelova in zato očitno nilpotentna. Za $k \geq 2$ uporabimo posledico razredne formule, da imajo p-grupe netrivialni center. Če je $Z(G) = G$ je grupa Abelova. Sicer sta po indukcijski predpostavki grupi $Z(G)$ in $G/Z(G)$ nilpotentni. Nilpotentnost kvocienta implicira obstoj najmanjšega števila m, za katero velja $\gamma_m(G) \subseteq Z(G)$. Od tod direktno sledi, da je $\gamma_{m+1}(G) = \{1_G\}$. □

Primer 4.5. Trditev 4.4 nam sporoča, da so vse diedrske grupe oblike $D_{2\cdot 2^k}$ nilpotentne. Izkaže se, da so to tudi vse. $\diamondsuit$

V resnici lahko o strukturi končnih nilpotentnih grup povemo nekoliko več.

Trditev 4.6. *Končne nilpotentne grupe so direktni produkt svojih p-podgrup Sylowa.*

Dokaz. TODO, treba je dokazati, da je vsaka p-podgrupa Sylowa edinka, dokaz iz wikipedije: $\square$

Posledica 4.7. *Nilpotentna grupa G moči n ali manj je razreda nilpotentnosti največ $\lfloor \log_2(n) \rfloor - 1$.*

Dokaz. Naj bo G nilpotentna grupa moči n ali manj. Po trditvi 4.6 je v skrajnem primeru enaka svoji 2-podgrupi Sylowa, katere moč je največ $2^{\log_2(n)}$ oziroma $2^{\lfloor \log_2(n) \rfloor}$, ker mora biti moč celo število. To nam v luči dokaza trditve 4.4 sporoča, da je razred nilpotentnosti grupe G največ $\lfloor \log_2(G) \rfloor - 1$ (tu člen -1 prihaja iz definicije razreda nilpotentnosti, glej 4.3). $\square$

Definicija 4.8. Grupa G je *rešljiva*, če se *izpeljana vrsta* $(G^{(k)})_{k\geq 0}$, podana rekurzivno z

$$G^{(0)} := G \text{ in } G^{(k+1)} := [G^{(k)}, G^{(k)}],$$

izteče s trivialno grupo. Najmanjšemu številu d, za katero je $G^{(d)} = \{1_G\}$, rečemo *razred rešljivosti grupe G*.

Analogno kot pri nilpotentnih grupah sklepamo, da izpeljana vrsta $(G^{(k)})_{k\geq 0}$ tvori verigo edink, ki so vse hkrati tudi edinke v G.

Primer 4.9. Diedrske grupe $D_{2n} = \langle r, Z \rangle$ so rešljive razreda največ 2. Z računom je enostavno pokazati, da je $(D_{2n})^{(1)}$ podmnožica Abelove podgrupe $\langle r \rangle$, zato bo grupa $(D_{2n})^{(2)} = ((D_{2n})^{(1)})^{(1)}$ trivialna. Ta sklep namiguje na nekatere lastnosti rešljivih grup, ki jih bomo obravnavali v trditvi 4.11. $\diamondsuit$

Primer 4.10. Vse nilpotentne grupe so rešljive, saj za vsako število $k \geq 0$, saj velja $G^{(0)} = \gamma_0(G) = G$, z indukcijo sledi

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \subseteq [\gamma_{k-1}(G), G] = \gamma_k(G).$$

Niso pa vse nilpotentne grupe rešljive, primer so recimo diedrske grupe D_{2n}, kjer $2n$ ni dvojiška potenca. $\diamondsuit$

Trditev 4.11. *Za rešljive grupe veljajo naslednje osnovne lasnosti.*

1. *Vsaka podgrupa rešljive grupe je rešljiva.*
2. *Vsak kvocient rešljive grupe je rešljiv.*
3. *Naj bo $N \triangleleft G$ in naj bosta N in G/N rešljivi grupi razreda d_N oziroma $d_{G/N}$. Potem je G rešljiva grupa razreda največ $d_N + d_{G/N}$.*
4. *Naj bosta $M, N \triangleleft G$ rešljivi razreda d_M oziroma d_N. Potem je edinka MN rešljiva razreda največ $d_M + d_N$.*

Dokaz. 1. To je očitna posledica dejstva, da za $H \leq G$ velja $H^{(k)} \subseteq G^{(k)}$ za vsak $k \in \mathbb{N} \cup \{0\}$.

2. Naj bo G rešljiva in naj bo $N \triangleleft G$. Zaradi rešljivosti grupe G obstaja naravno število d, da je $G^k \subseteq N$ za vse $k \geq d$, kar implicira $(G/N)^{(k)} = \left\{1_{G/N}\right\}$ za vse $k \geq d$.

3. Ker je G/N rešljiva grupa razreda $n_{G/N}$, bo $G^{(k)} \subseteq N$ za vse $k \geq d_{G/N}$. Ker je N rešljiva razreda d_N, bo nadalje veljalo $G^{(k)} = \{1_G\}$ za vse $k \geq d_M + d_N$.

4. Dokaz je prirejen po opombi 4 iz [14, str.4]. Po drugem izreku o izomorfizmu lahko zapišemo kratko eksaktno zaporedje

$$\mathbf{1} \to M \to MN \to MN/M \cong N/(N \cap M) \to \mathbf{1}.$$

Ker je N rešljiva, je po drugi točki trditve njen kvocient $N/(N \cap M)$ rešljiv razreda največ d_N in posledično tudi kvocient MN/M. Ker je M rešljiva razreda d_M, po tretji točki trditve sledi $(MN)^{(k)} = \{1_G\}$ za vse $k \geq d_N + d_M$.

□

Razširitvena lema 3.10 nam ponuja naslednjo skromno oceno dolžine kratkih netrivialnih zakonov v rešljivih oziroma nilpotentnih grupah.

Trditev 4.12. *Obstaja beseda $w \in F_2 = \langle a, b\rangle$ dolžine $l(w) \leq 4^d$, ki je zakon v vseh grupah razreda rešljivosti (ali nilpotentnosti) d ali manj.*

Dokaz. Trditev je posledica razširitvene leme 3.10, dokaz poteka z indukcijo po razredu rešljivosti grupe G, ki ga označimo z d. Za $d = 1$ je grupa G Abelova, zato je ustrezni zakon beseda $w = [a, b]$, ki je dolžine 4. Za $d > 1$ opazimo, da je kvocient $G/G^{(1)}$ Abelova grupa, $G^{(1)}$ pa rešljiva grupa razreda največ $d - 1$. Zato z uporabo razširitvene leme in indukcijske predpostavke najdemo besedo $w \in F_2$ dolžine

$$l(w) \leq 4 \cdot 4^{d-1} = 4^d,$$

ki je zakon v grupi G. Za nilpotentne grupe upoštevamo dejstvo $G^{(1)} \subseteq \gamma_1(G)$, kar implicira komutativnost grupe $G/\gamma_1(G)$ ($G^{(1)}$ je po definiciji najmanjša edinka, za katero je kvocient $G/G^{(1)}$ Abelova grupa). □

Opomba 4.13. V članku [8, str. 8] je podana nekoliko šibkejša meja $l(w) \leq 4 \cdot 6^{d-1}$, ker je avtor uporabil šibkejšo obliko razširitvene leme.

4.2 Konstrukcija kratkih zakonov v nilpotentnih in rešljivih grupah

Konstrukcija kratkih zakonov v nilpotentnih grupah je opisana v članku [4] in z razlagami dopolnjena v magistrskem delu [14]. Glavna ideja je poiskati kratke netrivialne predstavnike izpeljane vrste proste grupe $F_2 = \langle a, b\rangle$. Najprej definiramo zaporedji $(a_n)_n$ in $(b_n)_n$ v F_2 s predpisoma

$$a_0 := a,\ a_{n+1} := [b_n^{-1}, a_n] \text{ in } b_0 := b,\ b_{n+1} := [a_n, b_n].$$

Besede, ki jih bomo konstruirali s tema zaporedjema, morajo biti netrivialne, zato potrebujemo naslednjo lemo (lema 3.1 v viru [8] oziroma lema 8 v [14]).

Lema 4.14. *Za vsako nenegativno celo število n so besede $a_n a_n$, $a_n^{-1} a_n^{-1}$, $b_n b_n$, $b_n^{-1} b_n^{-1}$, $a_n^{-1} b_n$, $b_n^{-1} a_n$, $a_n b_n^{-1}$, $b_n a_n^{-1}$, $a_n^{-1} b_n^{-1}$ in $b_n a_n$ okrajšane.*

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ je trditev očitna, ker sta a in b različna generatorja grupe F_2. Za $n > 0$ najprej razpišimo produkt $a_n a_n$.

$$a_n a_n = [b_{n-1}^{-1}, a_{n-1}]^2 = b_{n-1}^{-1} a_{n-1} b_{n-1} \underbrace{a_{n-1}^{-1} b_{n-1}^{-1}}_{\text{ni krajšanja}} a_{n-1} b_{n-1} a_{n-1}^{-1}$$

Ker po indukcijski predpostavki vemo, da ne more priti do krajšanja v produktu $a_{n-1}^{-1} b_{n-1}^{-1}$, ne more priti do krajšanja v produktu $a_n a_n$ ali njegovem inverzu $a_n^{-1} a_n^{-1}$. Enako sklepamo za preostale produkte.

- Produkt $b_n b_n$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1}^{-1} a_{n-1}$.
- Produkt $a_n^{-1} b_n$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1} a_{n-1}$.
- Produkt $b_n b_n^{-1}$ in njegov inverz sta okrajšana, ker je okrajšan $a_{n-1}^{-1} b_{n-1}$.
- Produkt $a_n^{-1} b_n^{-1}$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1} b_{n-1}$.

□

Opomba 4.15. Produkti oblike $a_n b_n$ oziroma njihovi inverzi $b_n^{-1} a_n^{-1}$ niso nujno okrajšane besede, na primer že za $n = 1$ dobimo $a_1 b_1 = b^{-1} a b a a^{-1} b a^{-1} b^{-1}$. To dejstvo bomo izkoristili v nadaljevanju pri dokazu ocene iz trditve 4.18.

Najprej se prepričajmo, da so besede a_n oziroma b_n elementi izpeljane grupe $F_2^{(n)}$. Najdemo jo kot razmislek na koncu dokaza leme 9 v [14, str. 14].

Lema 4.16. *Za vsako nenegativno celo število n so besede a_n oziroma b_n elementi izpeljane grupe $F_2^{(n)} \subseteq F_2 = \langle a, b \rangle$.*

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ je $a_0 = a \in F_2 = F_2^{(0)}$ in $b_0 = b \in F_2 = F_2^{(0)}$. Za $n > 0$ velja $a_{n+1} = [b_n^{-1}, a_n] \in \left[F_2^{(n)}, F_2^{(n)}\right] = F_2^{(n+1)}$ in $b_{n+1} = [a_n, b_n] \in \left[F_2^{(n)}, F_2^{(n)}\right] = F_2^{(n+1)}$. □

Nato ocenimo dolžino členov zaporedij $(a_n)_n$ in $(b_n)_n$. Pri tem je za razliko od praktično vseh prejšnjih ocen pomembnejša spodnja meja, ki nam sporoča, da so elemeti a_n in b_n netrivialni predstavniki izpeljane podgrupe $F_2^{(n)}$. Posledično so te besede zakoni za vse rešljive grupe razreda rešljivosti n ali manj.

Lema 4.17. *Za vsak $n \in \mathbb{N} \cup \{0\}$ velja $4^n \geq l(a_n) = l(b_n) \geq 2^n$.*

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ očitno velja $l(a_0) = l(a) = l(b) = l(b_0) = 1$. Za $n \geq 1$ z upoštevanjem definicij zaporedij razpišemo

$$\begin{aligned} l(b_{n+1}) &= l(a_n b_n a_n^{-1} b_n^{-1}) \\ &= l(a_n b_n) + l(a_n) + l(b_n) \\ &= l(b_n^{-1} a_n b_n a_n^{-1}) \\ &= l(a_{n+1}) \end{aligned}$$

Za sklep v drugi in tretji vrstici je bila potrebna lema 4.14 ter preprost sklep, da za besedi $w_1, w_2 \in F_2$, katerih produkt w_1w_2 je okrajšana beseda, velja $l(w_1w_2) = l(w_1) + l(w_2)$.

Iz druge vrstice sledi

$$l(b_{n+1}) = l(a_nb_n) + l(a_n) + l(b_n) \geq l(a_n) + l(b_n) = 2l(b_n).$$

od koder z indukcijo dobimo $l(a_n) = l(b_n) \geq 2^n$. Iz tretje vrstice direktno sledi $l(b_{n+1}) \leq 4l(b_n)$ od koder z indukcijo dobimo $l(b_n) \leq 4^n$. Mimogrede – s tem razmislekom smo na novi način dokazali oceno 4.12. $\square$

Zaradi leme 4.17 lahko dobro definiramo zaporedje naravnih števil $c_n := l(a_n) = l(b_n)$, ki nam podaja dolžine netrivialnih besed v grupi $F_2^{(n)}$. Pred izračunom splošnega člena uvedimo naslednjo notacijo. Funkcija $f : \mathbb{N} \cup \{0\} \to \mathbb{R}$ je *razreda* $o(1)$, če je $\lim_{n\to\infty} f/n = 0$. To so torej funkcije, ki asimptotsko gledano zelo malo vplivajo na oceno.

Lema 4.18. *Zaporedje c_n za vsako število $n \geq 0$ ustreza rekurzivni zvezi $c_{n+2} = 3c_{n+1}+2c_n$ z začetnima členoma $c_0 = 1$ in $c_1 = 4$. Od tod lahko natančno izračunamo splošni člen tega zaporedja in ocenimo zgornjo mejo z zvezama*

$$c_n = \left(\frac{1}{2} + \frac{5}{2\sqrt{17}}\right)\left(\frac{3+\sqrt{17}}{2}\right)^n + \left(\frac{1}{2} - \frac{5}{2\sqrt{17}}\right)\left(\frac{3-\sqrt{17}}{2}\right)^n \leq C_1\iota^n + o(1),$$

kjer je $\iota := (3+\sqrt{17})/2 = 3{,}5615528\ldots$ in $C_1 = 1/2 + 5/(2\sqrt{17}) = 1{,}1063391\ldots$.

Dokaz. Dokaz je v podobni obliki podan v [14, str. 15] in se stalno sklicuje lemo 4.14, ki preprečuje nezaželena krajšanja med stičišči besed. Po definiciji zaporedij a_n in b_n hitro vidimo, da je $c_0 = l(a) = 1$ ter $c_1 = l([b^{-1}, a]) = 4$. Nato izrazimo

$$\begin{aligned}
c_{n+2} &= l(b_{n+2}) \\
&= l([a_{n+1}, b_{n+1}]) \\
&= l([[b_n^{-1}, a_n], [a_n, b_n]]) \\
&= l(b_n^{-1}a_nb_n \underbrace{a_n^{-1}a_n}_{\text{se pokrajša}} b_na_n^{-1}b_n^{-1}) + l([a_n, b_n^{-1}]) + l([b_n, a_n]) \\
&= \underbrace{l(b_n^{-1}a_nb_n)}_{l(a_{n+1})-l(a_n^{-1})=c_{n+1}-c_n} + \underbrace{l(b_n) + l(a_n^{-1}) + l(b_n^{-1})}_{3c_n} + \underbrace{l([a_n, b_n^{-1}])}_{l(a_{n+1})=c_{n+1}} + \underbrace{l([b_n, a_n])}_{l(b_{n+1})=c_{n+1}}.
\end{aligned}$$

To nam za $n \geq 0 \cup \{0\}$ podaja želeno zvezo $c_{n+2} = 3c_{n+1} + 2c_n$ skupaj z začetnima vrednostima $c_0 = 1$ in $c_1 = 4$. Temu rekurzivno podanemu zaporedju pripada matrična enačba, ki jo poenostavimo z diagonalizacijo kvadratne matrike, spodaj označene z A

$$\begin{bmatrix} c_{n+1} \\ c_n \end{bmatrix} = \underbrace{\begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix}}_{A}^n \begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{3-\sqrt{17}}{2} & \frac{3+\sqrt{17}}{2} \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \frac{3-\sqrt{17}}{2} & 0 \\ 0 & \frac{3+\sqrt{17}}{2} \end{bmatrix}^n \begin{bmatrix} -\frac{1}{\sqrt{17}} & \frac{1}{2} + \frac{3}{2\sqrt{17}} \\ \frac{1}{\sqrt{17}} & \frac{1}{2} - \frac{3}{2\sqrt{17}} \end{bmatrix} \begin{bmatrix} 4 \\ 1 \end{bmatrix}.$$

Druga vrstica te matrične enačbe nam podaja želeni izraz splošnega člena c_n. Neenakost $c_n \leq C_1\iota^n + o(1)$ je posledica dejstva, da je po absolutni vrednosti največja lastna vrednost matrike A enaka $\iota = (3+\sqrt{17})/2 = 3{,}5615528\ldots$. Člen, ki pripada manjši lastni vrednosti konvergira proti 0, zato je razreda $o(1)$. $\square$

Direktna posledica te leme je naslednja ugotovitev za rešljive grupe.

Trditev 4.19. *Obstaja netrivialna beseda $w \in F_2$, ki je zakon v vseh grupah razreda rešljivosti n ali manj, dolžine*

$$l(w) \leq C_1 \iota^n + o(1),$$

kjer sta konstanti C_1 in ι enaki kot v lemi 4.18.

Dokaz. Naj bo G rešljiva grupa razreda d. Po prejšnji lemi obstaja netrivialna beseda $w \in F_2^{(n)}$ dolžine $C_1\iota^n + o(1)$. Ker je grupa G rešljiva razreda $d \leq n$, je $G^{(n)} = G^{(d)} = \{1_G\}$. To pomeni, da za vsak par elementov $g, h \in G$ velja $w(g,h) = 1_G$, torej je w zakon v grupi G. □

Ta ugotovitev je asimptotsko gledano veliko boljši rezultat od trditve 4.12. Zdaj moramo pridobljeno znanje le še prevesti na nilpotentne grupe. Brez dokaza (najdemo ga v [14, str. 17–18]) bomo privzeli naslednje razmeroma znano dejstvo o členih spodnje centralne vrste.

Lema 4.20. *Za vsako število $n \geq 0$ velja inkluzija*

$$G^{(n)} \subseteq \gamma_{2^n}(G).$$

Naslednja trditev je kombinacija posledice 4 in leme 11 iz naloge [14, str. 16–17].

Trditev 4.21. *Obstaja netrivialna beseda $w \in F_2$, ki je zakon v vseh nilpotentnih grupah G moči največ n, dolžine*

$$l(w) \leq C_3 \log(n)^\kappa + o(1),$$

kjer sta $C_3 = 7{,}712869694\ldots$ in $\kappa = \log_2(\iota) = 1{,}832506\ldots$ konstanti.

Dokaz. Za vsako število $k \geq 1$ je število $e = \lceil \log_2(k) \rceil$ najmanjše naravno število, da velja $k \leq 2^e < 2k$. Od tod po lemi 4.20 sledi

$$F_2^{(e)} \subseteq \gamma_{2^e}(F_2) \subseteq \gamma_k(F_2).$$

Po trditvi 4.19 obstaja netrivialna beseda $w \in F_2^{(e)}$ dolžine največ $C_1\iota^e + o(1)$. Zaradi izbira števila e lahko zapišemo

$$l(w) \leq C_1\iota^e = C_1 2^{\log_2(\iota)e} < C_1(2k)^{\log_2(\iota)} = C_1 \iota k^{\log_2(\iota)} = C_2 k^\kappa.$$

Naj bo grupa G nilpotentna razreda d, moči n ali manj. Zaradi nilpotentnosti G za vsako celo število $i \geq 0$ iz netrivialnosti grupe $\gamma_i(G)$ sledi netrivialnost kvocienta $\gamma_i(G)/\gamma_{i+1}(G)$, saj je centralna vrsta nilpotentnih grup pred iztekom strogo padajoča. Za razred nilpotentnosti d velja po posledici 4.7 ocena $d \leq \lfloor \log_2(G) \rfloor \leq \log_2(n)$. Zato po prvem sklepu dokaza obstaja netrivialna beseda $w \in \gamma_d(G)$ dolžine

$$l(w) \leq C_2 d^\kappa \leq C_2 \log_2(n)^\kappa = \frac{C_2}{\log_2(n)^\kappa} \log(n)^\kappa = C_3 \log(n)^\kappa,$$

saj velja $w \in \gamma_{\lfloor \log_2(n) \rfloor}(F_2) \subseteq \gamma_d(F_2)$. Od tod z analognim razmislekom kot v trditvi 4.19 sledi, da je w netrivialni zakon v vseh nilpotentnih grupah razreda d ali manj. □

V nadaljevanju članka [4, str. 5–9] avtorja eksponent κ iz prejšnje trditve izboljšata na $\lambda := 1{,}44115577\ldots$, pri čemer je treba namesto konstante C_3 vzeti faktor oblike $(8{,}395184144\ldots + o(1))$. To storita s preučevanjem funkcije

$$\gamma(w) := \max\left\{n \in \mathbb{N} |\, w \in \gamma_n(F_2)\right\} \cup \{\infty\}\,.$$

Če namreč definiramo $\gamma_n := \gamma(a_n) = \gamma(b_n)$, lahko za vsako celo število $n \geq 0$ dokažemo zvezo $\gamma_{n+2} - 2\gamma_{n+1} - \gamma_n \geq 0$, s čimer po enakem postopku kot v dokazu 4.18 ocenimo spodnjo mejo $\gamma_n \geq C_4(1+\sqrt{2})^n - o(1)$. Avtorja razmislek zaključita z ugotovitvijo, da je namesto eksponenta $\kappa = \log_2(\iota)$ ustrezen $\lambda := \log_{1+\sqrt{2}}(\iota)$.

Da dobimo primerljiv rezultat za rešljive grupe, se moramo precej bolj potruditi. Postopek je opisan v [17, str. 3–4] oziroma podrobneje v [14, str. 19–25]. Sklicuje se na lastnosti grup avtomorfizmov nilpotentnih grup, ki jih vložimo v primerne splošne linearne grupe. Slednjim znamo natančno omejiti razrede rešljivosti, saj so predmet klasične obravnave v teoriji grup. Ker je jedro te vložitve nilpotentno, se lahko zaradi razširitvene leme 3.10 skličemo na rezultat o dolžinah zakonov v nilpotentnih grupah [**?**], kar nam zagotovi naslednji izrek (formulacija iz [14, str. 25]).

Izrek 4.22. *Za vsako število $n \in \mathbb{N} \cup \{0\}$ obstaja netrivialna beseda $w \in F_2$ dolžine*

$$l(w) \leq (C_{10} + o(1)) \log(n)^{\lambda},$$

ki je zakon za v vseh rešljivih grupah moči n ali manj, kjer sta konstanti enaki $C_{10} := 86.321{,}05422\ldots$ in $\lambda := 4{,}331612776\ldots$

5 Enostavne, polenostavne in simetrične grupe

Začnimo z razmislekom o pomembnosti enostavnih grup pri iskanju kratkih zakonov v splošnih grupah. Glavno idejo smo pravzaprav že videli v opombi pod razširitveno lemo 3.10, kjer smo ugotovili, da lahko problem iskanja kratkih zakonov v neki konkretni grupi prevedemo na problem o njeni edinki in kvocientu po tej edinki. Ta razčlenjevanje se ustavi pri enostavnih grupah, ki nimajo pravih, netrivialnih edink.

Ker je klasifikacija končnih enostavnih grup zaključena, lahko marsikaj povemo o njihovi strukturi. Po tej klasifikaciji denimo obstaja 18 družin enostavnih grup ter 26 sporadičnih grup, ki ne spadajo v nobeno izmed prej omenjenih družin. Za asimptotsko analizo dolžin zakonov nas sporadične grupe prav nič ne motijo. Ker so končne vse od njih premorejo netrivialne zakone, ki jih povežemo s komutatorsko lemo 3.5 v besedo w_{spor}, ki je zakon v vseh sporadičnih grupah. Recimo, da nam s funkcijo $f(n)$ uspe omejiti dolžino besede $w_{\text{druž}}(n)$, ki je zakon v vseh grupah moči n ali manj, ki pripadajo eni izmed 18-ih družin končnih enostavih grup. Potem s pomočjo komutatorske leme 3.4 dobimo besedo w, ki je zakon v vseh enostavnih grupah velikosti n ali manj, katere dolžina je

$$l(w) \leq 2 \cdot 2(2 + l(w_{\text{spor}}) + l(w_{\text{druž}})) \leq 4f(n) + o(1).$$

Vidimo torej, da nas pri asimptotski obravnavi zakonov sporadične grupe prav nič ne ovirajo. Omenimo še to, da iskanja kratkih zakonov v družinah končnih enostavnih grup lotimo z metodo maksimalnega reda elementa, ki je razložena v 3.8. Pri tem je najbolj problematična družina grup $\mathrm{PSL}_2(q)$, katere članice imajo razmeroma visoke rede elementov glede na njihove velikosti. Ta družina grup si zaradi svojih posebnih lasnosti zasluži svoj razdelek v tem poglavju.

Morda presenetljivo pa se izkaže, da so simetrične grupe pomembne za obravnavo enostavnih. Ta zveza bo podrobneje razložena na koncu poglavja.

5.1 Simetrične grupe

Obravnava simetričnih grup je najnatančneje opisana v članku [8], kjer avtorja dokažeta obstoj kratkih zakonov v simetričnih grupah s pomočjo naključnih sprehodov. Ker je celoten dokaz glavnega rezultata preveč specifičen za okvir te diplomske naloge, bom predstavil le del, ki je bralcu te naloge vsebinsko nov, tematsko drugačen od dosedanjih konstrukcij s komutatorsko in razširitveno lemo.

Osnovna ocena članka [8] izhaja iz dolžin kratkih zakonov v simetričnih grupah izhaja iz zgornje meje maksimalnega reda elementov v simetrični grupi, ki jo je dokazal Edmund Landau leta 1903 v knjigi [9].

Trditev 5.1 (Landau). *Z $g(n)$ označimo maksimalni red elementa v simetrični grupi S_n. Obstaja konstanta $C > 0$, da za vsa naravna števila n velja*

$$g(n) \leq \exp(C(n \log n)^{1/2}).$$

Landau je izrek dokazal z uporabo osnovnega izreka o praštevilih. Eno izmed njegovih oblik bomo spoznali v obliki izreka 5.7 v naslednjem razdelku. Od tod po enakem postopku kot v primeru 3.8 z uporabo komutatorske leme na besedah

$a, a^2, \ldots, a^{g(n)}$ na elementih proste grupe $F_2 = \langle a, b\rangle$ dobimo asimptotsko gledano enako oceno

$$\alpha(n) \leq \exp(C(n \log n)^{1/2}),$$

kjer smo z $\alpha(n)$ označili dolžino najkrajšega netrivialnega zakona v grupi S_n.

Avtorja članka [8] sta rezultat močno izboljšala.

Izrek 5.2 (Kozma–Thom)**.**

$$\alpha(n) \leq \exp(C \log(n)^4 \log(\log n)) \tag{5.1}$$

To sta storila z uporabo zahtevnih izrekov, ki močno temeljita na klasifikaciji končnih enostavnih grup, zato ju v nalogi ne bomo dokazovali. To sta:

- Liebeckove izrek ([10]) o strukturi podgrup grupe S_n, ki opredeli vrste podrgup v odvisnosti od načina delovanja na S_n. Najpomembnejši rezultat izreka je ugotovitev, da je vsaka podgrupa $\Gamma \subseteq S_n$, ki ne sodi med prve štiri vrste, omejena z $|\Gamma| \leq \exp((1 + o(1)) \log(n)^2)$.
- Helfgott–Seressov izrek ([6]), ki poda asimptotsko oceno na diametre Cayleyjevih grafov grupe S_n. V nalogi smo ga formulirali v razdelku o naključnih sprehodih kot izrek 2.23.

Dokaz ocene 5.1 v grobem poteka v dveh delih. Za potrebe naše naloge se čimbolj osredotočimo na prvega; ta nam namreč ponuja nov vpogled v razumevanje zakonov, saj izkoristi moč naključnih sprehodov. Čeprav je tudi drugi del izreka zelo pomemben, je konceptualno dosti bolj podoben konstrukcijam, ki smo jih že spoznali, njegovo bistvo je spretna uporaba komutatorske leme. Začnimo tako, da za vsako naravno število $k \leq n$ razdelimo pare $(\sigma, \tau) \in S_k^2$ na tiste, ki generirajo grupo S_k ali A_k (to je prva vrsta podgrup po Liebeckovem izreku), in tiste, ki generirajo preostale vrste podgrup.

1. Najprej za vsako naravno število $k \leq n$ z zapisom $P(k)$ označimo množico k-ciklov grupe S_k. Helfgott-Seressov izrek nam zagotovi obstoj množice $W \subseteq F_2$, velikosti $|W| \leq 8n^2 \log n$, da za vsak $w \in W$ velja

   $$l(w) \leq \exp(C \log(n)^4 \log(\log(n))). \tag{5.2}$$

   Še več, za vse $k \leq n$ in vse pare $(\sigma, \tau) \in S_k^2$, ki generirajo S_k, obstaja beseda $w \in W$, tako da je $w(\sigma, \tau) \in P(k)$. Ker beseda 1_{F_2} ni k-cikel (za $k \geq 2$, primer $k = 1$ pripada trivialni podgrupi in nas ne zanima), je beseda w netrivialna. Nato definiramo množico

   $$W' := \left\{ w^k \middle| w \in W,\, 1 \leq k \leq n \right\},$$

   ki ne vsebuje enote 1_{F_2}, ker je grupa F_2 torzijsko prosta (glej posledico 2.5). S pomočjo ocene moči W sklepamo $|W'| \leq 8n^3 \log n$. Ker za vsak $k \leq n$ in za vsak $(\sigma, \tau) \in S_k^2$ obstaja beseda $w \in W'$, da je $w(\sigma, \tau) = 1_{F_2}$, po komutatorski lemi 3.6 in oceni 5.2 obstaja netrivialna beseda $v \in F_2$, dolžine

   $$l(v) \leq \exp(C \log(n)^4 \log(\log(n))).$$

2. V drugem primeru z obravnavanjem podgrup po Liebeckovem izreku konstruiramo netrvialno besedo $\tilde{v} \in F_2$, ki trivializira vse pare $(\sigma, \tau) \in S_k^2$, ki ne generirajo grupe S_k (veljati mora $\tilde{v}(\sigma, \tau) = 1_{F_2}$ za vse pare s to lastnostjo). Na primer, v prvo vrsto spadajo podgrupe oblike S_k ali A_k, ki spadajo pod prejšnjo točko dokaza, mejo za meto vrsto pa nam direktno podaja Liebeckov izrek. Vrste dva do štiri je treba obravnavati vsako posebej. Na koncu zakone v posameznih vrstah grup povežemo s komutatorsko lemo.

5.2 Grupe $PSL_2(q)$

Tekom tega poglavja bo p vedno označevalo praštevilo, q pa praštevilsko potenco oblike $q = p^k$ za neko naravno število $k \geq 1$. Začnimo z definicijo družine grup $\mathrm{PSL}_n(q)$.

Definicija 5.3. Naj bo $n \in \mathbb{N}$ in $q \in \mathbb{N}$ praštevilska potenca, torej $q = p^k$. Potem definiramo grupo

$$\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q)).$$

V primeru $n = 2$ so elementi podgrupe $Z(\mathrm{SL}_n(q))$ skalarne 2×2 matrike z lastnostjo $\det \lambda I = 1_{\mathbb{F}_q}$. To enačbo prevedemo na enačbo oblike $(\lambda - 1)(\lambda + 1) = 0$. Če ima polje $\mathbb{F}_q$ karakteristiko 2 – kar se zgodi natanko v primeru $q = 2^k$ – sta $\lambda_{1,2} = \pm 1$ isti element, sicer pa dva različna. Tako dobimo

$$\mathrm{PSL}_2(q) = \begin{cases} \mathrm{SL}_2(q); & p = 2, \\ \mathrm{SL}_2(q)/\{I, -I\}; & p \neq 2. \end{cases}$$

Družina $\mathrm{PSL}_2(q)$ ima – poleg svoje problematičnosti pri iskanju kratkih zakonov – zelo posebne lastnosti. Ena izmed glavnih je sledeča.

Trditev 5.4. *Naj bo p praštevilo. Potem ima vsak netrivialni zakon v grupi* $\mathrm{PSL}_2(p)$ *dolžino vsaj p. Posledično enako velja za grupi* $\mathrm{GL}_2(p)$ *in* $\mathrm{SL}_2(p)$*, saj se zakoni prenašajo na podgrupe in kvociente.*

Dokaz. Ker je trditev prikazana kot zanimivost, bomo dokaz izpustili. Bralec ga lahko najde v [14]. Glavna ideja je pokazati, da lahko z matrikami, ki predsatvljajo strižne transformacije, v primeru prekratkih besed vedno dobimo matriko, ki ni identiteta. □

Direktna posledica te leme je recimo dejstvo, da grupa $\mathrm{Sym}(\mathbb{N})$ nima netrivialnih zakonov, saj vsebuje vse $\mathrm{PSL}_2(p)$ kot podgrupe. Še bolj očiten primer grupe, ki nima dvočrkovnih zakonov, je sicer kar prosta grupa $F_2 = \langle x, y \rangle$. Če bi bila netrivialna beseda $w \in F_2 = \langle a, b \rangle$ zakon v njej, bi prišli do protislovja s preslikavo, ki jo inducirajo slike $x \mapsto a$, $y \mapsto b$.

5.2.1 Konstrukcija zakonov v grupah $PSL_2(q)$

Osnovna konstrukcija zakonov v grupah $\mathrm{PSL}_2(q)$ poteka prek obravnave redov elementov in uporabe komutatorske leme v slogu primera 3.8. Dokaz je prirejen po [14, str. 36–37] in

Lema 5.5. *Red poljubnega element $A \in \mathrm{PSL}_2(q)$ deli vsaj eno izmed števil p, $q-1$ ali $q+1$.*

Dokaz. Naj bo matrika $A \in \mathrm{PSL}_2(q)$. Obravnavajmo primere glede na njeno Jordanovo formo J_A. Naj bo $\chi_A(X) \in \mathbb{F}_q[X]$ karakteristični polinom matrike A.

1. Če je A diagonalizabilna, je njena Jordanova forma oblike

$$J_A = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix},$$

kjer sta $\alpha, \beta \in \mathbb{F}_q^*$ (0 ne moreta biti, ker je matrika A obrnljiva). Ker je $(\mathbb{F}_q^*, \cdot)$ grupa moči $q-1$, velja $\alpha^{q-1} = \beta^{q-1} = 1$ in od tod $J_A^{q-1} = I$ oziroma $A^{q-1} = I$.

2. Če je $\chi_A(X)$ razcepen v $\mathbb{F}_q[X]$, vendar matrika A ni diagonalizabilna, mora biti njena Jordanova forma oblike

$$J_A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} = I + N.$$

Diagonalna elementa morata namreč oba biti enaka 1 po razmisleku v definiciji 5.3. Ker velja $J_A^p = (I+N)^p = I^p + N^p = I$, red matrike A deli p.

3. Če $\chi_A(X)$ ni razcepen v $\mathbb{F}_q[X]$, je razpecen v $\mathbb{F}_{q^2}[X] = \mathbb{F}_q[X]/(\chi_A(X))$. Naj bo $\alpha \in \mathbb{F}_{q^2}$ neka ničla $\chi_A(X)$. Pokazati moramo, da je potem tudi α^q njegova ničla. Naj bo $\chi_A(X) = X^2 + bX + c$ za neka $b, c \in \mathbb{F}_q^*$. Potem iz enačbe $\alpha^2 + b\alpha + c = 0$ sledi

$$0 = (\alpha^q + b\alpha + c)^q = \alpha^{2q} + b^q\alpha^q + c^q =_{\text{točka 1}} \alpha^{2q} + b\alpha^q + c.$$

Tako lahko matriko A diagonaliziramo v kolobarju $M_2(\mathbb{F}_{q^2})$ v obliki

$$J_A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^q \end{bmatrix}.$$

Ker velja $\det A = \det J_A = \alpha\alpha^q = 1$, red A deli število $q-1$.

$\square$

Za konkretno grupo $G = \mathrm{PSL}_2(q)$ definirajmo podmnožice

$$H_m := \{A \in \mathrm{PSL}_2(q) |\, A^m = I\}$$

za števila $m \in \{p, q-1, q+1\}$. Po razmisleku iz prejšnje leme te podmnožice tvorijo pokritje G. Z uporabo komutatorske leme **??**, je zakon v grupi G beseda oblike

$$\begin{aligned} w &= [[ba^pb^{-1}, a^{q-1}], a^{q+1}] \\ &= ba^pb^{-1}a^{q-1}ba^{-p}b^{-1}\cancel{a^{1-q}}a^{q+1}\cancel{a^{q-1}}ba^pb^{-1}a^{1-q}ba^{-p}b^{-1}a^{-q-1} \\ &= ba^pb^{-1}a^{q-1}ba^{-p}b^{-1}a^{q+1}ba^pb^{-1}a^{1-q}ba^{-p}b^{-1}a^{-q-1} \end{aligned}$$

dolžine

$$l(w) = 4(2+p+q) \leq 8(q+1).$$

Pred uporabo komutatorske leme moramo navesti še dva rezultata.

Lema 5.6.

$$|\mathrm{PSL}_2(q)| = \begin{cases} (q^2-1)q; & p=2, \\ \frac{1}{2}(q^2-1)q; & p \neq 2. \end{cases}$$

Dokaz. Grupa $\mathrm{GL}_2(q)$ ima $(q^2-1)(q^2-q)$ elementov. Če hočemo, da je matrika $A \in M_2(\mathbb{F}_q)$ obrnljiva, imamo namreč za prvi stolpec q^2-1 izbir, za drugega pa q^2-q. Od tod sledi, da ima $\mathrm{SL}_2(q)$ $(q^2-1)q$ elementov, saj je $|\mathbb{F}_q^*| = q-1$. V primeru $p \neq 2$, nam kvocient po centru odbije še polovico elementov. □

Lema 5.7. *Naj bo preslikava* $\tau : \mathbb{R} \to \mathbb{N} \cup \{0\}$, *ki prešteje število praštevilskih potenc, podana s predpisom*

$$\tau(x) = \sum_{p^k \leq x,\, k \in \mathbb{N}} 1.$$

Potem velja $\tau(x) = (1+o(1))\frac{n}{\log(n)}$.

Ta lema je ena izmed oblik osnovnega izreka o praštevilih. Leta 1851 je Čebišev dokazal ([5, str. 4–5]), da limita $\frac{\tau(x)}{x/\log(x)}$ – če le obstaja – mora biti 1, kar bi potrdilo Gaussovo domnevo. Obstoja limite mu ni uspelo dokazati, je pa to uspelo Riemannu v svojem znamenitem članku [12] leta 1859, v katerem je povezal porazdeltev praštevil s funkcijo zeta in formuliral Riemannovo hipotezo. Ker je dokaz netrivialen, ga bomo opustili, Riemann ga je v prej omenjenem članku dokazal z uporabo kompleksne analize. Nekoliko več o tej lemi piše v članku [8].

Zdaj se lahko lotimo konstrukcije netrivialnega zakona za vse grupe oblike $\mathrm{PSL}_2(q)$, moči manjše ali enake številu $n \in \mathbb{N}$. Z uporabo lem 5.6 in 5.7 vemo, da moramo moramo konstruirati zakone za vse grupe $\mathrm{PSL}_2(q)$, za katere je $q \leq \sqrt[3]{(1+o(1))2n}$. Od tod dobimo besedo $w \in F_2$ dolžine

$$l(w) \leq 8\left(\frac{3\sqrt[3]{(1+o(1))2n}}{\log((1+o(1))2n))}\right)^2 \cdot 8\sqrt[3]{(1+o(1))2n} \leq 1152(1+o(1))\frac{n}{\log(n)^2},$$

ki je zakon za vse grupe $\mathrm{PSL}_2(q)$, moči n ali manj. Ta rezultat ni najboljši in je predstavljal oviro, kot je bilo omenjeno v tretjem odstavku članka [1, str. 6]. Izognemo se ji lahko z uporabo naključnih sprehodov, ki prinaša naslednji rezultat.

Izrek 5.8 (Bradford–Thom)**.** *Za vsako naravno število* $n \in \mathbb{N}$ *obstaja beseda* $w \in F_2$ *dolžine*

$$O(n^{2/3}\log(n)^3),$$

ki je zakon v vsaki grupi $\mathrm{PSL}_2(q)$, *moči* n *ali manj.*

Dokaz tega izreka je glavni rezultat članka [1]. Ker je nekoliko preveč specifičen za okvir te naloge, ga opuščamo. Poteka podobno kot dokaz enačbe 5.1, le da moramo uporabiti ustrezen ekvivalent Helfgott-Seressovega in Liebeckovega izreka.

5.3 Povezava s problemom v splošni grupi

Za reševanje problema kratkih zakonov v splošni grupi bomo uporabili naše znanje o rešljivih grupah z uvedbo rešljivega radikala.

Definicija 5.9. Naj bo G končna grupa. Največjo rešljivo edinko G imenujemo *rešljivi radikal grupe* G in ga označimo z $S(G)$. Če je $S(G)$ trivialna grupa, rečemo, da je G *polenostavna grupa.*

Lema 5.10. *Rešljivi radikal je dobro definiran v končnih grupah.*

Dokaz. Naj bosta M in N rešljivi edinki končne grupe G. Po četrti točke trditve 4.11 je tudi MN rešljiva edinka (produkt edink je vedno edinka, manj očitna je rešljivost). Ker je grupa G končna, ima kočno mnogo edink, s primerjanjem vseh parov v končnem številu korakov najdemo največjo. □

Lema 5.11. *Naj bo G končna grupa. Potem je kvocient $G/S(G)$ polenostavna grupa.*

Dokaz. Dokaz poteka s protislovjem. Recimo, da $G/S(G)$ ni polenostavna grupa in ima netrivialno rešljivo edinko N. Po korespondenčnem izreku je $N = N'/S(G)$ za neko edinko $N' \triangleleft G$. Ker sta tako $N'/S(G)$ kot $S(G)$ rešljivi grupi, po tretji točki trditve 4.11 sledi, da je N' rešljiva in hkrati strogo večja od $S(G)$, kar je protislovno z definicijo rešljivega radikala. □

Naj bo G poljubna končna grupa. S tvorjenjem kratkega eksaktnega zaporedja

$$\mathbf{1} \to S(G) \to G \to G/S(G) \to \mathbf{1}$$

in uporabo razširitvene leme 3.10 vidimo, da za netrivialna zakona $w_{S(G)}$ in $w_{G/S(G)}$ v grupah $S(G)$ oziroma $G/S(G)$ obstaja netrivialni zakon w_G v grupi G, dolžine

$$l(w_G) \leq l(w_{S(G)})l(w_{G/S(G)}).$$

V lemi 5.11 smo dokazali, da je grupa $G/S(G)$ polenostavna. Bistvo polenostavnih objektov je, da jih lahko zapišemo kot produkte enostavnih. To dejstvo bi seveda morali natančno formulirati in dokazati, vendar bi korektna obravnava zavzela prevelik delež naloge, zato jo izpustimo. Če povzamemo bistvo, problem o polenostavnih grupah s pomočjo razširitvene leme 3.10 razčlenimo na problem o simetričnih grupah in grupah avtomorfizmov enostavnih grup. Slednjih se lahko presenetljivo elegantno lotimo s pomočjo Schreierjeve domneve, ki jo bomo formulirali. Podrobnešja razprava se nahaja v [14, 28–31].

Definicija 5.12. Naj bo G grupa in $\operatorname{Aut}(G)$ njena grupa avtomorfizmov. Ker je grupa notranjih avtomorfizmov $\operatorname{Inn}(G) = \{x \mapsto gxg^{-1} |\, g \in G\}$ njena edinka, lahko definiramo kvocient $\operatorname{Out}(G) := \operatorname{Aut}(G)/\operatorname{Inn}(G)$, ki mu rečemo *grupa zunanjih avtomorfizmov grupe* G.

Izrek 5.13 (Schreierjeva domneva)**.** *Naj bo G končna enostavna grupa, ki ni Abelova. Potem je grupa* $\operatorname{Out}(G)$ *rešljiva razreda največ* 3.

Schreierjevo domnevo so potrdili z uporabo klasifikacije končnih enostavnih grup. Vprašanje, ali obstaja bolj elementaren dokaz, ostaja odprto [3, str. 133]. Glede na to, da se iskanje zakonov v enostavnih grupah močno naslanja na to klasifikacijo, bomo domnevo brez zadržkov uporabili. Naj bo H poljubna nekomutativna enostavna grupa. S tvorjenjem kratkega eksaktnega zaporedja

$$\mathbf{1} \to \operatorname{Inn}(H) \to \operatorname{Aut}(H) \to \operatorname{Out}(H) \to \mathbf{1}$$

in uporabo razširitvene leme 3.10 vidimo, da za netrivialna zakona $w_{\mathrm{Inn}(H)}$ in $w_{\mathrm{Out}(H)}$ v grupah $\mathrm{Inn}(H)$ oziroma $\mathrm{Out}(H)$ obstaja netrivialni zakon $w_{\mathrm{Aut}(H)}$ v grupi $\mathrm{Aut}(H)$, dolžine

$$l(w_{\mathrm{Aut}(H)}) \leq l(w_{\mathrm{Inn}(H)}) l(w_{\mathrm{Out}(H)}).$$

Ker je H enostavna, velja $H \cong \mathrm{Inn}(H)$. Za splošno grupo G namreč velja $G/Z(G) \cong \mathrm{Inn}(G)$, v primeru enostavnosti (nekomutativne) grupe pa je center seveda trivialen. Dalje, po Schreierjevi domnevi 5.13 in lemi 4.18 obstaja zakon dolžine $c_3 = 50$, ki je zakon za vse rešljive grupe razreda 3 ali manj. Tako zgornjo enačbo prevedemo na

$$l(w_{\mathrm{Aut}(H)}) \leq 50 l(w_H).$$

Ko vse to združimo, dobimo (TODO napiši po komponentah kaj dobiš. V resnici čisto preoblikuj in ustrezno utemelji, zakaj ne moreš lepo povedati).

6 Iskanje zakonov z računalnikom

Na roke dokazati, da je beseda zakon, je – z izjemo posebnih primerov – zoprno. Zato je zelo naravno pomisliti na uporabo računalnika. V tem poglavju sta opisana dva različna pristopa za iskanje oziroma razumevanje zakonov v končnih grupah. Programa se nahajata v repozitoriju diplomske naloge `https://github.com/MightyOwler/Diplomska-naloga/` v mapi `Program_za_racunsko_iskanje_zakonov`.

6.1 Iskanje zakonov v grupah $\mathrm{PSL}_2(p)$

Najprimitivnejši način iskanja zakonov v dani grupi G je kar po definiciji: Poiščemo vse besede grupe $F_2 = \langle a, b \rangle$ določene dolžine, nato pa jih izvrednotimo na vseh možnih parih. Za začetek me je zanimalo, koliko zakonov dolžine 17 ali manj premorejo grupe $\mathrm{PSL}_2(p)$. Za višje dolžine je bilo potrebno generirati nepraktično veliko besed. Pri tem se zavedamo, da grupe $\mathrm{PSL}_2(p)$ ne morejo imeti zakonov krajših od p-črk po trditvi 5.4. Program sem spisal v jeziku C++, ki je v splošnem veliko hitrejši od GAP-a, opisuje ga spodnja psevdokoda.

```
# generiranje besed in parov elementov

za k = 1, ... , 17:
    - generiaj vse okrajšane besede dolžine k
    - shrani jih v datoteko

za p = 2, 3, 5, 7, 11, 13, 17:
    - predstavi elemente grupe PSL_2(p) kot 2x2 matrike
    - generiraj vse pare elementov
    - pare shrani v datoteko

# preverjanje zakonov

za p = 2, 3, 5, 7, 11, 13, 17:
    za k = p, ... , 17:
        - preberi pare grupe PSL_2(p) in besede dolžine k
        iz generiranih datotek
        - na vsaki besedi evalviraj vse pare
        - če je rezultat vseh evalvacij besede identična matrika,
        je ta beseda zakon
```

Hitro se je izkazalo, da je tak pristop zelo neučinkovit. Problem je namreč v tem, da število besed dolžine k narašča eksponentno. Če brez škode za splošnost fiksiramo prvo črko, je to število enako 3^{k-1}, saj lahko v vsakem koraku dodamo natanko 3 črke, da ne pride do krajšanja. Tudi če bi obravnavali tako imenovane *komutatorske besede*, ki vsebujejo enako število črk kot njihovih inverzov (število črk a je enako številu črk a^{-1}, podobno za b), število dvočrkovnih besed, ki bi jih morali pregledati, mnogo prehitro narašča, da bi lahko pokazali karkoli smiselnega.

V splošnem se sicer da oceniti, z najmanj kolikšno verjetnostjo je naključna beseda $w \in F_2$ zakon v grupi G. Oceniti moramo indeks grupe zakonov $K(G, 2)$ v grupi F_2. S pomočjo razmisleka pod dokazom leme 2.8 v primeru $k = 2$ dobimo oceno

$$[F_2 : K(G, 2)] \leq |G|^{|G|^2},$$

kar vsekakor ni ravno spodbudno. Pa vendar se v praksi izkaže, da ti indeksi dejansko so razmeroma visoki. Članek [2] nam ponuja konkretne vrednosti naslednjih indeksov.

$$\begin{aligned} [F_2 : K(D_{10}, 2)] &= 2^2 \cdot 5^5 = 12500, \\ [F_2 : K(S_3, 2)] &= 2^2 \cdot 3^5 = 972, \\ [F_2 : K(A_4, 2)] &= 2^{10} \cdot 3^2 = 9216, \\ [F_2 : K(A_5, 2)] &= 2^{48} \cdot 3^{24} \cdot 5^{24} \approx 4.73 \cdot 10^{42}. \end{aligned}$$

V splošnem ni veliko grup, za katere bi poznali točne vrednosti teh kvocientov [2, str. 1]. Rezultatov za grupe $\mathrm{PSL}_2(q)$ nisem našel.

6.2 Iskanje generatorjev zakonov za nilpotentne grupe

Kot smo videli v prejšnjem poglavju, moramo do problema pristopiti bolj zvito. Delež zakonov med vsemi dvočrkovnimi besedami nam določa kvocient

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2, G)}.$$

Ni težko videti, da je grupa $F_2^{\exp(G)} = \left\{ w^{\exp(G)} \middle| w \in F_2 \right\}$ edinka v F_2. Za poljubni besedi $w \in F_2, u \in F_2$ in celo število n namreč velja $(w^n)^u = (w^u)^n$. Po tretjem izreku o izomorfizmu bi bilo zelo mamljivo zapisati

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2, G)} \cong \frac{F_2 \Big/ F_2^{\exp(G)}}{\left(\bigcap\limits_{\varphi \in \mathrm{Hom}(F_2 / F_2^{\exp(G)}, G)} \ker \varphi \right) \Big/ F_2^{\exp(G)}}.$$

Tu se pojavi nezanemarljiv problem: V splošnem nam nič ne zagotavlja končnosti kvocienta $B(2, \exp(G)) := F_2 / F_2^{\exp(G)}$. Pravzaprav smo prišli do klasičnega Burnsidovega problema, ki sprašuje po končnosti kvocientov oblike $B(m, n) := F_m / F_m^n$. Po rezultatu Lysenoka leta 1996 recimo velja, da je grupa $B(2, n)$ neskončna za $n \geq 8000$ ([18, str. 2]). Da lahko vseeno nadaljujemo s podobnim razmislekom, predpostavimo, da je grupa G nilpotentna razreda d.

Ker je poljubni člen spodnje centralne vrste edinka v F_2, je tudi grupa $\gamma_{d+1}(F_2)$. Produkt edink je edinka, zato je tudi $F_2^{\exp(G)} \gamma_{d+1}(F_2)$ edinka v F_2, in lahko tvorimo kvocient

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2, G)} \cong \frac{F_2 \Big/ F_2^{\exp(G)} \gamma_{d+1}(F_2)}{\left(\bigcap\limits_{\varphi \in \mathrm{Hom}(F_2 / F_2^{\exp(G)} \gamma_{d+1}(F_2), G)} \ker \varphi \right) \Big/ F_2^{\exp(G)} \gamma_{d+1}(F_2)}.$$

S tem smo problem v primeru nilpotentnih grup poenostavili, saj nam za izračun zakonov ni več treba računati jeder vseh homomorfizmov $F_2 \to G$, temveč le še $F_2 / F_2^{\exp(G)} \to G$. Hkrati pa računalniška konstrukcija tega kvocienta ni zahtevna, saj vsebuje GAP paket za delo z nilpotentnimi grupami `nq` ([7]), s pomočjo katerega lahko zgornji kvocient izračunamo in obravnavamo kot grupo. Tako sem izračunal indekse za vse nilpotentne grupe do vključno moči 64, za višje vrednosti je bila časovna zahtevnost prevelika. Program je dostopen na repozitoriju `https://github.com/MightyOwler/Diplomska-naloga`, opisuje ga naslednja psevdokoda.

```
vse nilpotentne grupe želenih moči shranimo v seznam
za vsako grupo G iz seznama:
    izračunamo vrednosti exp(G) in d
    kvocient := (zgornji izraz z ustreznimi vrednostmi)
    zakoni := presek homomorfizmov kvocient -> G
    poračunamo strukturo in velikost kvocienta kvocient/zakoni
izračunane rezultate shranimo v datoteko
```

Ta pristop do problema je mnogo boljši od pristopa v razdelku 5.2, saj je ne le bolj povezan s strukturo grup, temveč tudi omogoča boljši vpogled v splošno razumevanje zakonov. Z njegovo pomočjo je namreč lažje opaziti in posledično dokazati naslednje lastnosti zakonov. Začnimo s preprostimi.

Trditev 6.1. *Za vsako ciklično grupo C_n je*

$$F_2/K(C_n, 2) \cong C_n \times C_n$$

in posledično sledi

$$[F_2 : K(C_n, 2)] = n^2.$$

Z drugimi besedami, delež zakonov v cikličnih grupah med vsemi besedami je $1/n^2$.

Dokaz. Naj bo $F_2 = \langle a, b\rangle$. Najti moramo epimorfizem $F_2 \to C_n \times C_n$ z jedrom $K(C_n, 2)$. Na tej točki se spomnimo preprostega sklepa, da velja $K(C_n, 2) = K(C_n \times C_n, 2)$. Naj bo $\xi \in C_n$ generator ciklične grupe. Definirajmo preslikavo $\varphi : F_2 \to C_n \times C_n$, inducirano s slikama elementov $a \mapsto (\xi, 1_{C_n})$ in $b \mapsto (1_{C_n}, \xi)$. Ta preslikava je očitno surjektivna, preveriti moramo še, da je $\ker\varphi = K(C_n, 2)$. Najprej preverimo inkluzijo $\ker\varphi \subseteq K(C_n, 2)$. Naj bo $w \in \ker\varphi \subseteq F_2$ okrajšana beseda oblike $w = a^{r_1}b^{s_1} \dots a^{r_k}b^{s_k}$ za neka cela števila $r_1, s_1, \dots, r_k, s_k$. To pomeni, da je

$$\varphi(w) = \varphi(a^{r_1})\varphi(b^{s_1}) \dots \varphi(a^{r_k})\varphi(b^{s_k}) = \left(\xi^{r_1+\dots+r_k}, \xi^{s_1+\dots+s_k}\right) = (1_{C_n}, 1_{C_n})\,.$$

Z drugimi besedami, vsoti $r_1 + \dots + r_k$ in $s_1 + \dots + s_k$ morata biti deljivi z n. Zato imamo za poljubna elementa $g, h \in C_n$

$$w(g, h) = g^{r_1+\dots+r_k}h^{s_1+\dots+s_k}) = 1_{C_n},$$

torej je w zakon v C_n. Dokažimo še $\ker\varphi \supseteq K(C_n, 2)$. Naj bo $w \in K(C_n, 2)$ okrajšana beseda oblike $w = a^{r_1}b^{s_1} \dots a^{r_k}b^{s_k}$ za neka cela števila $r_1, s_1, \dots, r_k, s_k$. Potem velja

$$\varphi(w) = \varphi(a)^{r_1}\varphi(b)^{s_1} \dots \varphi(a)^{r_k}\varphi(b)^{s_k} = w(\varphi(a), \varphi(b)) = (1_{C_n}, 1_{C_n}).$$

Zadnja enakost sledi iz dejstva, da je w zakon v grupi C_n in posledično v $C_n \times C_n$. $\square$

Posledica 6.2. *Naj bo grupa G elementarno Abelova, torej $G = \prod_{i=1}^n C_{p^{k_i}}$. Potem velja $F_2/K(G,2) \cong C_{p^k} \times C_{p^k}$, kjer je $k = \max_{i=1,\dots,n} k_i$.*

Dokaz. Beseda $w \in F_2$ je zakon v C_{p^k} natanko tedaj, ko je zakon v vsakem faktorju produkta $\prod_{i=1}^n C_{p^{k_i}}$. Implikacija v levo je zato očitna, implikacija v desno pa tudi, saj za vsak $i = 1, \dots, n$ velja $C_{p^{k_i}} \leq C_{p^k}$, zakoni pa se prenašajo na podgrupe. □

Posledica 6.3. *Naj bo končna grupa G Abelova. Natančneje, naj bo v skladu s klasifikacijo končnih Abelovih grup oblike $G = \prod_{i=1}^n \prod_{j=1}^{n_i} C_{p_i^{k_{i,j}}}^{m_j}$, kjer so za vsak $i = 1, \dots, n$ p_i paroma različna praštevila, števila $n_i, m_i \geq 1$, in vsak $j = 1, \dots, n_i$ števila $k_{i,j} \geq 1$ paroma različna. Naj bodo $k_i = \max_{j=1,\dots,n_i}$. Potem velja $F_2/K(G,2) \cong C_e \times C_e$, kjer je $e = p_1^{k_1} \cdots p_n^{k_n} = \exp(G)$.*

Dokaz. V luči prejšnje posledice je beseda $w \in F_2$ zakon v grupi C_e natanko tedaj, ko je zakon v grupi $\prod_{i=1}^n C_{p^{k_i}}$, ki je po klasifikaciji končnih Abelovih grup izomorfna C_e. □

Od tod sledi, da delež zakonov v Abelovih grupah znaša natanko $1/\exp(G)^2$. Intuitivno je to še lažje videti z naslednjim neformalnim razmislekom. Naj bo podana beseda $w \in F_2 = \langle a, b \rangle$. Če hočemo preveriti, ali je zakon v Abelovi grupi G, se lahko pretvarjamo, da črke med seboj komutirajo. Tako w prevedemo na besedo oblike $w' = a^r b^s$, kjer r in s predstavljata vsoto eksponentov črk a oziroma b v besedi w. Beseda a^r je zakon v grupi G natanko tedaj, ko je $\exp(G)$ delitelj števila r. Torej je verjetnost, da bo w zakon po črki a enaka $1/\exp(G)$. Ker enako velja za b in sta evalvaciji a in b medsebojno neodvisni, je skupna verjetnost enaka $1/\exp(G)^2$.

TODO NAPIŠI POVEZAVO Z AMIT'S CONJECTURE

7 Zaključek

Slovar strokovnih izrazov

Literatura

[1] H. Bradford in A. Thom, *Short laws for finite groups and residual finiteness growth*, 2017, dostopno na `https://arxiv.org/abs/1701.08121`, verzija 1. 7. 2022 [ogled 29. 2. 2024].

[2] W. Cocke in D. Skabelund, *The free spectrum of a5*, International Journal of Algebra and Computation **30**(04) (2020) 685–691, dostopno na `https://doi.org/10.1142/S0218196720500162`.

[3] J. D. Dixon in B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, 1996.

[4] A. Elkasapy in A. Thom, *On the length of the shortest non-trivial element in the derived and the lower central series*, 2013, dostopno na `https://arxiv.org/abs/1311.0138`, verzija 1. 10. 2013 [ogled 29. 2. 2024].

[5] A. Granville, *Herald cramer and the distribution of prime numbers*, 1993, dostopno na `https://web.archive.org/web/20150923212842/http://www.dartmouth.edu/~chance/chance_news/for_chance_news/Riemann/cramer.pdf`.

[6] H. A. Helfgott in A. Seress, *On the diameter of permutation groups*, 2013, dostopno na `https://arxiv.org/abs/1109.3550`, verzija 31. 12. 2013 [ogled 8. 8. 2024].

[7] M. Horn in W. Nickel, *nq, nilpotent quotients of finitely presented groups, Version 2.5.11*, https://gap-packages.github.io/nq/, 2024, refereed GAP package.

[8] G. Kozma in A. Thom, *Divisibility and laws in finite simple groups*, Mathematische Annalen **364**(1-2) (2016) 79–95.

[9] E. Landau, *Uber die maximalordnung der permutationen gegebenen grades*, 1903, dostopno na `https://archive.org/details/archivdermathem48grungoog/page/n1/mode/2up`.

[10] M. W. Liebeck, *On minimal degrees and base sizes of primitive permutation groups*, Archiv der Mathematik **43**(01) (1984) 11–15, dostopno na `https://link.springer.com/article/10.1007/BF01193603`.

[11] R. Lyndon in P. Schupp, *Combinatorial group theory*, Springer Science and Business Media, 2015.

[12] B. Riemann, *Ueber die anzahl der primzahlen unter einer gegebenen grösse*, Monatsberichte der Berliner Akademie (1859), dostopno na `https://www.claymath.org/wp-content/uploads/2023/04/Wilkins-transcription.pdf`.

[13] S. Schleimer, *On the girth of groups* (2001).

[14] J. Schneider, *On the length of group laws*, magistrsko delo, Technische Universität Dresden, Department of mathematics, 2016.

[15] M.-P. Schützenberger, *Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre*, Comptes rendus de l'Académie des Sciences Paris, Série I Mathématique **248** (1959) 2435–2436, dostopno na `https://www-igm.univ-mlv.fr/~berstel/Mps/Travaux/A/1959EquationGroupeLibreCRAS.pdf`.

[16] J. P. Souvent, *Proste grupe in drevesa*, Matrika **11**(1) (2024), dostopno na `https://matrika.fmf.uni-lj.si/letnik-11/stevilka-1/pogacnik.pdf`.

[17] A. Thom, *About the length of laws for finite groups*, 2015, dostopno na `https://arxiv.org/abs/1508.07730`, verzija 5. 9. 2015 [ogled 29. 2. 2024].

[18] M. Vaughan-Lee in E. I. Zel'manov, *Bounds in the restricted burnside problem*, Journal of the Australian Mathematical Society **67**(2) (1999) 261–271, doi: 10.1017/S144678870000121X.