Kratki zakoni v grupah

Osnutek diplomske naloge

Jaša Knap
Mentor: dr. Urban Jezernik

29. februar 2024

1 Motivacija

Dvočrkovni zakon v grupi G je abstrakten produkt elementov x, y ter njunih inverzov x^{-1} in y^{-1}, ki ima lastnost, da za vsako zamenjavo x in y s konkretnima elementoma $g, h \in G$ dobimo rezultat $1 \in G$.

Opomba 1.1. *Definicijo n-črkovnih zakonov dobimo tako, da v zgornji definiciji elementa x, y (in njuna inverza) nadomestimo z elementi $x_1, x_2, \ldots, x_n$ (in njihovimi inverzi), ki jih zamenjujemo s konkretnimi elementi $g_1, g_2, \ldots, g_n \in G$.*

Zakonu 1 pravimo trivialen zakon, v kontekstu raziskovanja zakonov ni posebej zanimiv. Najosnovnejši primer netrivialnega zakona se pojavi pri Abelovih grupah, kjer za poljubna elementa $x, y \in G$ velja $xy = yx$, kar je ekvivalentno zahtevi

$$xyx^{-1}y^{-1} = [x, y] = 1.$$

Grupa G je torej Abelova natanko tedaj, ko je štiričrkovna beseda $xyx^{-1}y^{-1}$ v njej zakon.
Nadvse pomembno je vprašanje, ali vsaka grupa premore netrivialen zakon. Odgovor nanj je v splošnem negativen, protiprimer je recimo grupa $\mathrm{Sym}(\mathbb{N})$. Očitna posledica Lagrangeevega izreka pa je, da vsaka končna grupa premore netrivialen zakon, saj veja

$$x^{|G|} = 1.$$

Če za G vzamemo grupo $\mathrm{Sym}(n)$, bo $x^{n!}$ zakon, ki pa je razmeroma dolg. Precej krajši zakon za isto grupo je $x^{\mathrm{lcm}(1,\ldots,n)}$, ki je prav tako posledica Lagrangeevega izreka.

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? Prav ta vprašanja bodo bistvo diplomske naloge, v kateri bom predstavil dosedanje rezultate ter različne pristope, ki so jih ubrali raziskovalci.

2 Osnove

Najprej bom definiral osnovne pojme, kot so beseda, dolžina besede, izginjajoča množica itd. Poleg tega bom predstavil in dokazal dve osnovni lemi, brez katerih zakonov praktično ne moremo razumeti. Prva izmed njih je komutatorska lema.

Definicija 2.1. *Naj bo G grupa in ω dvočrkovna beseda v črkah x in y. Za vsaka $g, h \in G$ označimo z $\omega(g, h)$ produkt elementov, ki jih določa ω, če x zamenjamo z g in y s h. Izginjajočo množico besede ω definiramo kot*

$$Z(G, \omega) = \{(g, h) \in G \times G |\, \omega(g, h) = 1\}.$$

Očitno je beseda ω zakon za G natanko tedaj, ko velja $Z(G, \omega) = G$.

Lema 2.2 (Komutatorska lema)**.** *Naj bodo $\omega_1, \omega_2, \ldots, \omega_m$ netrivialne dvočrkovne besede ter $Z(G, \omega_1), \ldots, Z(G, \omega_m)$ njihove izginjajoče množice. Potem obstaja netrivialna beseda ω dolžine*

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

za katero velja

$$Z(G, \omega) \supseteq Z(G, \omega_1) \cup Z(G, \omega_2) \cup \ldots \cup Z(G, \omega_m).$$

Ta lema je izredno pomembna, saj nam omogoča, da iz že znanih besed ustvarimo novo besedo, katere izginjajoča množica je večja od vsake posamezne izginjajoče množice. Nekoliko bolj povezana s strukturo grup pa je razširitvena lema.

Lema 2.3 (Razširitvena lema)**.** *Naj bo G grupa in $N \triangleleft G$ njena edinka. Naj bo ω_N netrvialen zakon za N in $\omega_{G/N}$ netrvialen zakon za kvocientno grupo G/N. Potem obstaja netrvialen zakon ω za grupo G, katerega dolžina je*

$$l(\omega) \leq l(\omega_N) l(\omega_{G/N}).$$

Moč te leme je še posebej izrazita, kadar ima edinka N lepe lastnosti. Če je N na primer Abelova, v njej gotovo obstaja zakon dolžine 4, torej se zgornja neenakost prevede na $l(\omega) \leq 4l(\omega_{G/N})$. Direktna posledica je dejstvo, da nas zares zanimajo le grupe s trivialnim centrom, saj v primeru netrivialnosti centra lahko uporabimo zgornjo oceno. Še več, ker je v splošnem $\mathrm{Inn}(G) \cong G \big/ Z(G)$, se lahko sklicujemo na lastnosti notranjih avtomorfizmov grup. Hkrati postaja razvidno, da bodo pomembno vlogo pri problemu igrale nilpotentne in rešljive grupe.

3 Končne grupe

Preučevanje zakonov v končnih grupah je lažje kot v neskončnih, v katerih na primer že sam obstoj zakonov ni zagotovljen. Predstavil bom dosedanje rezultate o zgornjih mejah asimptotske rasti nilpotentnih, rešljivih in enostavnih grupah. Poleg tega bosta pomembni tudi poglavji o projektivnih posebnih linearnih grupah $\mathrm{PSL}_2(q)$ in o simetričnih grupah $\mathrm{Sym}(n)$, saj imata ti družini mnoge posebne lastnosti.

3.1 Nilpotentne in rešljive grupe grupe

Nilpotentnost in rešljivost grup sta močni lastnosti, ki nam omogočata razmeroma tesno oceno za asimptotsko rast dolžine kratkih zakonov. V magistrskem delu [2] je predstavljen in dokazan naslednji izrek.

Izrek 3.1. *Obstaja dvočrkovna beseda ω, ki je zakon za vse nilpotentne grupe moči manjše ali enake n, za katero velja ocena*

$$l(\omega) \leq (C + o(1)) \log(n)^{\nu}.$$

Pri tem je $C \approx 8,395$, $\nu \approx 1,441$, $o(1)$ pa funkcija odvisna od n, za katero velja $\lim_{n\to\infty} o(1) = 0$.

Prvi korak pri dokazu tega izreka je konstrukcija zaporedja besed $\{c_i\}_{i=1}^{\infty}$, za katerega je člen c_k zakon za vse grupe z redom nilpotentnosti k ali manj. Dolžino besede $l(c_k)$ določimo prek rekurzivne zveze. Osnovno oceno dobimo tako, da red nilpotentnosti ocenimo z močjo grupe, nato pa to oceno izboljšamo z upoštevanjem lastnosti spodnje centralne vrste proste grupe $\mathbb{F}_2$. V delu [2] je predstavljen tudi rezultat za rešljive grupe, katerega dokaz je precej zahtevnejši od dokaza za nilpotentne grupe.

Izrek 3.2. *Obstaja dvočrkovna beseda ω, ki je netrivialen zakon za vse rešljive grupe moči manjše ali enake n, za katero velja ocena*

$$l(\omega) \leq (D + o(1)) \log(n)^{\lambda}.$$

Pri tem je $D \approx 86320$, $\lambda \approx 4,332$, $o(1)$ pa funkcija odvisna od n, za katero velja $\lim_{n\to\infty} o(1) = 0$.

3.2 Grupe $\mathrm{PSL}_2(q)$ in $\mathrm{PSL}_n(q)$

Glavno vprašanje pri raziskovanju zakonov se glasi: Kako lahko ocenimo asimptotsko rast dolžine kratkih netrivialnih zakonov za družino vseh grup moči n ali manj? Eden izmed glavnih pristopov je, da problem s pomočjo razširitvene leme prevedemo na problema rešljivih in polenostavnih grup, problem polenostavnih pa na probleme enostavnih grup. Prek klasifikacije končnih enostavnih grup vemo, da obstaja 18 družin ter 26 sporadičnih končnih enostavnih grup. Pri asimptotski rasti dolžin kratkih netrivialnih zakonov so slednje zaradi komutatorske leme praktično zanemarljive. Po drugi strani se izkaže, da lahko najdemo dobre ocene za 17 izmed 18-ih družin. Edina izjema je družina $\mathrm{PSL}_2(q)$, ki zahteva posebno obravnavo.
Nekatere novejše ugotovitve na tem področju se nahajajo v člankih [3] in [4].

Definicija 3.3. *Naj bo $n \in \mathbb{N}$ in $q \in \mathbb{N}$ praštevilska potenca, torej $q = p^k$. Potem definiramo*

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

V primeru $n = 2$ dobimo

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

Družina $\mathrm{PSL}_2(q)$ ima zelo posebne lastnosti. Ena izmed glavnih je sledeča.

Lema 3.4. *Naj bo p praštevilo. Potem ima vsak netrivialen zakon za grupo $\mathrm{PSL}_2(p)$ dolžino vsaj p.*

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.
V tem poglavju bom predstavil nekaj možnih izboljšav dela [2], ki sem jih našel med branjem.

3.3 Simetrične grupe

Za razumevanje zakonov v grupah je ključno razumevanje zakonov v simetričnih grupah, med drugim zato, ker lahko vsako grupo obravnavamo kot podgrupo simetrične grupe. Pri tem se izkaže, da je iskanje zakonov tesno povezano z naključnimi sprehodi po ustreznih Cayleyjevih grafih grup. Ta pristop je podrobno opisan v člankih [5] in [1], njegova posebnost pa je nekonstruktivnost. Z drugimi besedami, mogoče je pokazati obstoj kratkih netrivialnih zakonov v grupah brez njihove konkretne konstrukcije. Tak pristop trenutno ne ponuja zgolj najboljših rezultatov za simetrične grupe, temveč tudi za enostavne, kar direktno vpliva na ocene dolžine netrivialnih zakonov v splošnih grupah. Zgled uspešnosti se odraža v osrednjem izreku članka [1].

Izrek 3.5. *Naj $\alpha(n)$ označuje dolžino najkrajšega netrivialnega zakona za grupo* $\mathrm{Sym}(n)$*. Obstaja konstanta $C > 0$, da velja*

$$\alpha(n) \leq \exp\left(C \log(n)^4 \log(\log(n))\right).$$

4 Neskončne grupe in skoraj zakoni

V diplomski nalogi bom večino pozornosti namenil končnim grupam, hkrati pa bom predstavil tudi nekaj osnovnih pristopov pri obravnavi zakonov za neskončne grupe, ki se pojavijo denimo v članku [5]. Tam je smiselno uvesti pojem skoraj zakonov, torej besed, ki uničijo skoraj vse pare elementov v grupi, niso pa nujno zakoni. Prav tako kot pri simetričnih grupah, tudi tu ključno vlogo igrajo naključni sprehodi.

Literatura

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

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

[3] H. Bradford in A. Thom, *Short laws for finite groups of Lie type*, verzija 5. 10. 2022 [ogled 29. 2. 2024], dostopno na `https://arxiv.org/abs/1811.05401`.

[4] H. Brandford, J. Schneider in A. Thom, *Non-singular word maps for linear groups*, verzija 7. 11. 2023 [ogled 29. 2. 2024], dostopno na `https://arxiv.org/abs/2311.03981`.

[5] G. Amir, G. Blachar, M. Gerasimova in G. Kozma, *Probabilistic laws on infinite groups*, verzija 18. 4. 2023 [ogled 29. 2. 2024], dostopno na `https://arxiv.org/abs/2304.09144`.