

Osnutek diplomske naloge

Jaša Knap

Mentor: Urban Jezernik

25. februar 2024

1 Motivacija

Zakon v grupi G je abstrakten produkt elementov x, y ter njunih inverzov x^{-1}, y^{-1} , ki ima lastnost, da za vsako zamenjavo x in y s konkretnima elementoma $g, h \in G$ dobimo rezultat 1 v G . Zakonu 1 pravimo trivialen zakon, v kontekstu naloge nas ne bo zanimal. Najosnovnejši primer 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 zakone. Odgovor nanj je v splošnem negativen, recimo grupa $\text{Sym}(\mathbb{N})$ nima nobenega (netrivialnega) zakona. Očitna posledica Lagrangeevega elementa pa je, da vsaka končna grupa premore zakon, saj veja

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

Če za G vzamemo na primer grupo $\text{Sym}(n)$, bo torej $x^{n!}$ zakon, ki pa je razmeroma dolg. Precej krajši je recimo zakon $x^{\text{lcm}(1, \dots, n)}$, ki je prav tako posledica Lagrangeevega izreka. Na tej točki se naravno pojavi nekaj vprašanj: kako dolgi so najkrajši zakoni za določeno grupo oziroma družino grup? Ali lahko ocenimo asimptotsko rast dolžine najkrajših zakonov za družine grup, recimo za družino $\text{Sym}(n)$? Prav ti vprašanja bosta bistvo diplomske naloge, v kateri bom predstavil dosedanje rezultate ter različne pristope, ki so jih uporabili raziskovalci.

2 Osnove

Najprej bom definiriral 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:

Lema 2.1 (Komutatorska lema). *Naj bodo $\omega_1, \omega_2, \dots, \omega_m$ dvočrkovne besede ter $Z(G, \omega_1), \dots, Z(G, \omega_m)$. Potem obstaja beseda ω dolžine*

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

za katero velja

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

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. Trivialna posledica je recimo dejstvo, da iz $G = A \cup B$ in imamo besedi ω_1, ω_2 , za kateri velja $A \subseteq Z(G, \omega_1)$, $B \subseteq Z(G, \omega_2)$, potem obstaja beseda ω , katere dolžina je

$$l(\omega) \leq 16(l(\omega_1) + l(\omega_2) + 2),$$

ki je zakon v grupi G . Nekoliko bolj povezana s strukturo grup pa je razširitvena lema.

Lema 2.2 (Razširitvena lema). *Naj bo G grupa in $N \triangleleft G$ njena edinka. Naj bo ω_N zakon za N in $\omega_{G/N}$ zakon za kvocientno grupo G/N . Potem obstaja zakon ω za grupo G , katerega dolžina je*

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

Njena moč 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 z netrivialnim centrom, saj v primeru netrivialnosti centra lahko uporabimo zgornjo oceno. 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 družino mnoge posebne lastnosti.

3.1 Nilpotentne grupe

3.2 Rešljive grupe

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

3.4 Simetrične grupe $\mathrm{Sym}(n)$

4 Neskončne grupe in skoraj zakoni

Na koncu bom predstavil še ključne ugotovitve v neskončnih grupah. Tam je smiselno uvesti tudi pojem skoraj zakonov, torej besed, ki uničijo skoraj vse pare elementov v grupi, vendar pa niso nujno zakoni.

5 Viri in literatura