

# Csoportok növekedése

Szakdolgozat

**Szerző: Györgypál Tamás**

Témavezető: Somlai Gábor

Matematika BSc, matematikus szakirány



Eötvös Loránd Tudományegyetem  
Természettudományi Kar  
Budapest, 2025

# Köszönetnyilvánítás

Mindenekelőtt szeretném őszinte hálámat kifejezni témavezetőmnek, Somlai Gábornak, aki nemcsak vállalta szakdolgozatom szakmai irányítását, hanem mindig készséggel állt rendelkezésemre a munka minden szakaszában. Értékes tanácsaival, türelmével és támogatásával nagyban hozzájárult ahhoz, hogy a dolgozat elkészülhessen. Köszönöm, hogy szakértelmével segítette munkámat.

# Tartalomjegyzék

|                                                                                         |           |
|-----------------------------------------------------------------------------------------|-----------|
| <b>1. Fourier-analízis véges csoportokon</b>                                            | <b>5</b>  |
| 1.1. Definíciók és alapismeretek . . . . .                                              | 5         |
| 1.2. Fourier-analízis a $\mathbb{Z}_p$ csoporton . . . . .                              | 6         |
| <b>2. Cayley-gráfok és csoportok átmérői</b>                                            | <b>9</b>  |
| 2.1. Definíciók . . . . .                                                               | 9         |
| 2.2. A Babai-sejtés . . . . .                                                           | 10        |
| <b>3. A Babai-sejtés igazolása a <math>\text{PSL}_2(\mathbb{F}_p)</math> csoportra</b>  | <b>12</b> |
| 3.1. Nagy halmaz generálása logaritmikus lépésben . . . . .                             | 12        |
| 3.2. Az egész csoport elérése egy nagy halmazból . . . . .                              | 24        |
| <b>4. Expanderek</b>                                                                    | <b>26</b> |
| 4.1. Kombinatorikus megközelítés . . . . .                                              | 26        |
| 4.2. Algebrai megközelítés . . . . .                                                    | 29        |
| 4.3. Cayley-gráfok és expanderek kapcsolata . . . . .                                   | 35        |
| <b>5. Az <math>\text{SL}_2(\mathbb{F}_p)</math> csoport és az expanderek kapcsolata</b> | <b>37</b> |
| 5.1. Definíciók és alapismeretek . . . . .                                              | 37        |
| 5.2. Valószínűségi mértékek az $\text{SL}_2(\mathbb{F}_p)$ csoporton . . . . .          | 40        |
| 5.3. A fő tétel bizonyítása . . . . .                                                   | 42        |

## Bevezetés

A csoportelméletben természetes az éppen szóban forgó csoport Cayley-gráfját vizsgálni valamely generátorhalmaza mellett. Ezen dolgozat a véges, nem kommutatív, egyszerű csoportok Cayley-gráfjainak az átmérőivel foglalkozik. 1992-ben Babai László megfogalmazta azt a sejtést, miszerint bármely  $G$  véges, nem kommutatív, egyszerű csoport tetszőleges generátorrendszere mellett a Cayley-gráfjának átmérője legfeljebb  $(\log |G|)^C$ , ahol  $C$  egy univerzális konstans. A dolgozatom központjában a sejtés bizonyítása áll a  $\mathrm{PSL}_2(\mathbb{F}_p)$  csoportokra.

Először ismertetünk néhány Fourier-analízisbeli alapfogalmat a  $\mathbb{Z}_p$  csoport felett. Fourier-analízisbeli eszközök segítségével bizonyítunk egy kombinatorikai állítást, amire a későbbiekben szükségünk lesz.

Ezután bevezetjük a Cayley-gráfok fogalmát, és megmutatjuk azoknak néhány alaptulajdonságát. Ismertetjük a már fent említett Babai-sejtést, és megmutatjuk, hogy a nem kommutativitás megkövetelése szükséges úgy, hogy adunk egy kommutatív csoportsorozatot, amelyre nem létezhet jó univerzális konstans.

Majd rátérünk a sejtés bizonyítására a  $\mathrm{PSL}_2(\mathbb{F}_p)$  csoportok körében. Azt mutatjuk meg, hogy az ilyen csoportok körében egy, a csoport méretéhez képest kicsi halmazt összeszorozva magával háromszor, a halmaz nagy mértékben nő. Ennek belátásához sok segédlemmán és állításon keresztül vezet az út. Majd végül belátjuk, hogy a csoport méretéhez képest nagy halmazból konstans lépésben elérjük az egész csoportot. Szeretnék megemlíteni néhány, a szakdolgozatomon túlmutató eredményt. Pyber László és Szabó Endre bebizonyították a sejtést minden véges, egyszerű, korlátos rangú Lie-típusú csoportra [16]. A bizonyításuk középpontjában egy, a 3.1.1. állításhoz nagyon hasonló áll. Majd később Martino Garonzi, Halasi Zoltán és Somlai Gábor bebizonyították a sejtést a  $\mathrm{PSL}_n(\mathbb{F}_q)$ ,  $\mathrm{PSp}_n(\mathbb{F}_q)$  és a  $\mathrm{PSU}_n(\mathbb{F}_q)$  csoportokra, ha  $q \notin \{9, 81\}$ ,  $q$  páratlan, és a generátorhalmazok tartalmaznak legalább egy transzvekciót [8].

Bevezetjük az expander fogalmát. Az expanderek új fogalomnak számítanak a matematikában, viszont sok felhasználási területük van, például hálózateleméletben, számítástechnikában, komplexitáselméletben, kódelméletben, stb. Kétféle megközelítést adunk az expanderek definíciójára, először egy gráfelméleten alapulót, ami a gráfbeli csúcshalmazok határának nagyságát veszi alapul. Majd adunk egy lineáris algebrán alapuló definíciót is, pontosabban a gráf spektrális résének nagyságára fogalmazzuk át az expanderek definícióját. A két definíció ekvivalenciáját a Cheeger-egyenlőtlenség fogja realizálni. Továbbá rámutatunk arra, hogy milyen kapcsolat van egy gráf expander mivolta és az átmérője között, és ebből vonunk le csoportelméleti következtetéseket. Ahogy az a dolgozatban is említésre kerül, Grigory Margulis volt az első, aki egzakt

konstrukciót adott egy expander családra, méghozzá a  $\mathbb{Z}_n \times \mathbb{Z}_n$  csúcshalmazokon ügyes élválasztásokkal. Bár a dolgozatban erről nem esik szó, viszont szeretném ismertetni Mark Pinsker korai eredményét az expanderekkel kapcsolatban. Ő bebizonyította, hogy rögzített  $d \geq 3$  természetes szám mellett, létezik egy  $\varepsilon(d) > 0$  konstans, amire egyenletesen választva egy  $n$  csúcsú  $d$ -reguláris  $G_{n,d}$  gráfot, akkor a  $h(G_{n,d}) > \varepsilon(d)$  esemény valószínűsége 1-hez tart ahogy  $n \rightarrow \infty$  [15]. Továbbá megemlítsük érdemesek a Ramanujan-gráfok, hiszen a definiálásához szükséges spektrál gráfelméleti alapok ismertetését megteesszük a dolgozat során. A Ramanujan-gráfok olyan  $d$ -reguláris  $G$  gráfok, melyek spektrális rése a lehető legnagyobb, vagyis  $\lambda(G) = \max_{|\lambda_i| < d} |\lambda_i| \leq 2\sqrt{d-1}$ . A dolgozat során oly sokat foglalkozott  $\text{PSL}_2(\mathbb{F}_p)$  csoportok Cayley-gráfjai segítségével explicit megadható Ramanujan-gráfok jól választott generátorhalmazok esetén.

Végül visszatérünk az  $\text{PSL}_2(\mathbb{F}_p)$  csoporthoz és azt mutatjuk meg, hogy bizonyos feltételek mellett ezen csoportok Cayley-gráfjai expandert alkotnak. Ez fontos eredmény, hiszen ismertetni fogjuk, hogy attól, mert ezen csoportok átmérői a csoportok méretéhez képest logaritmikusak, nem következik, hogy expandert alkotnak.

# 1. Fourier-analízis véges csoportokon

A dolgozatban feldolgozott cikkek megértéséhez szükségünk van néhány alapvető Fourier-analízisbeli eszköz és módszer ismertetésére. Ennek a fejezetnek a megírásában nagyban hagyatkoztam a [1] cikkekre.

## 1.1. Definíciók és alapismeretek

Legyen  $G$  egy tetszőleges véges csoport és  $f : G \rightarrow \mathbb{C}$  egy  $G$ -n értelmezett komplex értékű függvény.

**1.1.1. Definíció.** Az  $f$  függvény egyes, kettes és végtelen normáján a következőket értjük

$$\begin{aligned}\|f\|_1 &= \sum_{g \in G} |f(g)|, \\ \|f\|_2 &= \sqrt{\sum_{g \in G} |f(g)|^2}, \\ \|f\|_\infty &= \max_{g \in G} |f(g)|.\end{aligned}$$

**1.1.2. Definíció (Függvények konvolúciója).** Egy véges  $G$  csoport felett értelmezett  $f$  és  $h$  függvények konvolúciója

$$f * h(x) = \sum_{g \in G} f(xg^{-1})h(g).$$

Az  $n$ -szeres konvolúciót, vagyis amikor egy függvényt összekonvoluálunk saját magával  $n$ -szer, a következőképp jelöljük

$$f^{*n} = \underbrace{f * f * \cdots * f}_{n\text{-szer}}.$$

**1.1.3. Megjegyzés.** Abel-csoport esetén a jelölés természetesen

$$f * h(x) = \sum_{g \in G} f(x - g)h(g).$$

**1.1.4. Tétel (Young-egyenlőtlenség).** Legyen  $p, q, r \in \mathbb{N}^* \cup \{\infty\}$  úgy, hogy  $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$ , továbbá  $f, h : G \rightarrow \mathbb{C}$ . Ekkor

$$\|f * g\|_r \leq \|f\|_p \|g\|_q.$$

**1.1.5. Állítás.** Legyen  $G$  véges csoport és  $A, B \subset G$ . Ekkor  $\|\chi_A * \chi_B\|_1 = |A||B|$

**Bizonyítás:**  $\|\chi_A * \chi_B\|_1 = \left\| \sum_{g \in G} \chi_A(xg^{-1})\chi_B(g) \right\|_1 = \sum_{x \in G} \sum_{g \in G} \chi_A(xg^{-1})\chi_B(g) =$   
 $\sum_{b \in B} \sum_{x \in G} \chi_A(xb^{-1}) = \sum_{b \in B} \sum_{\substack{x \in G \\ xb^{-1} \in A}} 1 = |A||B|. \quad \square$

## 1.2. Fourier-analízis a $\mathbb{Z}_p$ csoporton

A következő definíció és két állítás egy függvény Fourier-transzformáltjáról és annak tulajdonságairól szól. Érdekes megjegyezni, hogy ezek ugyanúgy realizálhatók bármely Abel-csoport esetén a csoport irreducibilis karaktereit használva.

**1.2.1. Definíció (Fourier-transzformált).** Az  $f : \mathbb{Z}_p \rightarrow \mathbb{C}$  függvény diszkrét Fourier-transzformáltját  $\widehat{f}$ -al jelöljük, és

$$\widehat{f}(x) = \sum_{g \in \mathbb{Z}_p} f(g) e^{\frac{-2\pi i g x}{p}},$$

ahol a szorzást modulo  $p$  értjük.

**1.2.2. Állítás.** Legyenek  $f, h : \mathbb{Z}_p \rightarrow \mathbb{C}$  függvények. Ekkor  $\widehat{f * h}(x) = \widehat{f}(x)\widehat{h}(x) \quad \forall x \in \mathbb{Z}_p$ .

**Bizonyítás:**  $\widehat{f * h}(x) = \sum_{g \in \mathbb{Z}_p} f * h(g) e^{\frac{-2\pi i g x}{p}} = \sum_{g \in \mathbb{Z}_p} \left( \sum_{s \in \mathbb{Z}_p} f(g-s)h(s) \right) e^{\frac{-2\pi i g x}{p}} =$

$$\sum_{g \in \mathbb{Z}_p} \sum_{s \in \mathbb{Z}_p} f(g-s) e^{\frac{-2\pi i (g-s)x}{p}} h(s) e^{\frac{-2\pi i s x}{p}} = \sum_{s \in \mathbb{Z}_p} h(s) e^{\frac{-2\pi i s x}{p}} \sum_{g \in \mathbb{Z}_p} f(g-s) e^{\frac{-2\pi i (g-s)x}{p}} = (*)$$

Rögzített  $s$ -re  $\sum_{g \in \mathbb{Z}_p} f(g-s) e^{\frac{-2\pi i (g-s)x}{p}} = \sum_{g \in \mathbb{Z}_p} f(g) e^{\frac{-2\pi i g x}{p}}$ , tehát

$$(*) = \sum_{s \in \mathbb{Z}_p} h(s) e^{\frac{-2\pi i s x}{p}} \widehat{f}(x) = \widehat{f}(x) \sum_{s \in \mathbb{Z}_p} h(s) e^{\frac{-2\pi i s x}{p}} = \widehat{f}(x)\widehat{h}(x). \quad \square$$

**1.2.3. Állítás (Parseval-tétel).** Legyen  $f : \mathbb{Z}_p \rightarrow \mathbb{C}$ . Ekkor a Fourier-transzformáció konstans szorzó erejéig egy izometria

$$\|\widehat{f}\|_2^2 = p\|f\|_2^2.$$

**Bizonyítás:**  $\|\widehat{f}\|_2^2 = \sum_{g \in \mathbb{Z}_p} |\widehat{f}(g)|^2 = \sum_{g \in \mathbb{Z}_p} \widehat{f}(g) \overline{\widehat{f}(g)} = \sum_{g, s, t \in \mathbb{Z}_p} f(s) \overline{f(t)} e^{\frac{-2\pi i s g}{p}} e^{\frac{2\pi i t g}{p}} =$

$$\sum_{s, t \in \mathbb{Z}_p} f(s) \overline{f(t)} \sum_{g \in \mathbb{Z}_p} e^{\frac{-2\pi i (s-t)g}{p}} = (*)$$

Ha  $s \neq t$ , akkor  $\sum_{g=0}^{p-1} e^{\frac{-2\pi i (s-t)g}{p}} = \frac{e^{-2\pi i (s-t)} - 1}{e^{\frac{-2\pi i (s-t)}{p}} - 1} = 0$ . Ha pedig  $s = t$ , akkor  $\sum_{g=0}^{p-1} e^{\frac{-2\pi i (s-t)g}{p}} =$

$$\sum_{g=0}^{p-1} 1 = p. \text{ Mindezek alapján}$$

$$(*) = p \sum_{s \in \mathbb{Z}_p} f(s) \overline{f(s)} = p \sum_{s \in \mathbb{Z}_p} |f(s)|^2 = p \|f\|_2^2. \quad \square$$

A következő kombinatorikai állítás az előzőekkel ellentétben már specifikusan az egyik későbbiekben feldolgozandó cikkben [9] szerepel és véges testekbeli halmazok méretének becslésére szolgál.

**1.2.4. Állítás.** Legyen  $p$  prímszám,  $A \subset \mathbb{F}_p$  és  $S \subset \mathbb{F}_p^*$ . Ekkor bármely  $c \in (0, 1]$ -hez létezik legalább  $(1 - c)|S|$  olyan  $s \in S$ , hogy

$$|A + sA| \geq \frac{c}{\frac{1}{p} + \frac{p}{|S||A|^2}} \geq \frac{c}{2} \min \left\{ p, \frac{|S||A|^2}{p} \right\}$$

**Bizonyítás:** A második egyenlőtlenség triviális, mert ha  $\frac{1}{p} \geq \frac{p}{|S||A|^2}$ , akkor  $\frac{c}{\frac{1}{p} + \frac{p}{|S||A|^2}} \geq \frac{cp}{2}$ . Hasonlóan, ha  $\frac{p}{|S||A|^2} \geq \frac{1}{p}$ , akkor  $\frac{c}{\frac{1}{p} + \frac{p}{|S||A|^2}} \geq \frac{c|S||A|^2}{2p}$ .

$$\begin{aligned} p \sum_{s \in S} \|\chi_A * s\chi_A\|_2^2 &\stackrel{\text{Parseval}}{=} \sum_{s \in S} \|\widehat{\chi_A * s\chi_A}\|_2^2 = \sum_{s \in S} \|\widehat{\chi_A} \cdot s\widehat{\chi_A}\|_2^2 = \sum_{s \in S} \sum_{g \in \mathbb{F}_p} |\widehat{\chi_A}(g) \cdot \widehat{\chi_A}(sg)|^2 \leq \\ &|S| |\widehat{\chi_A}(0)|^4 + \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} |\widehat{\chi_A}(x) \cdot \widehat{\chi_A}(y)|^2 = |S| |A|^4 + \left( \sum_{x \in \mathbb{F}_p^*} |\widehat{\chi_A}(x)|^2 \right)^2 = |S| |A|^4 + p^2 \|\chi_A\|_2^4 = \\ &|S| |A|^4 + p^2 |A|^2. \end{aligned}$$

Eszerint létezik egy olyan  $s_0 \in S$ , hogy

$$\|\chi_A * s_0 \chi_A\|_2^2 \leq \frac{|A|^4}{p} + \frac{p|A|^2}{|S|}.$$

Másrésről bármely  $c \in (0, 1]$ -hez létezik legalább  $(1 - c)|S|$  olyan  $s \in S$  elem, amire

$$\|\chi_A * s\chi_A\|_2^2 \leq \frac{1}{c} \left( \frac{|A|^4}{p} + \frac{p|A|^2}{|s|} \right).$$

A Cauchy–Bunyakovszkij–Schwarz-egyenlőtlenség miatt

$$\|\chi_A * s\chi_A\|_1^2 \leq |A + sA| \cdot \|\chi_A * s\chi_A\|_2^2,$$

mert

$$\|\chi_A * s\chi_A\|_1^2 = \left( \sum_{g \in G} 1 \cdot |\chi_A * s\chi_A(g)| \right)^2 \stackrel{\text{C.B.S.}}{\leq} |A + sA| \sum_{g \in G} |\chi_A * s\chi_A(g)|^2 = |A + sA| \cdot \|\chi_A * s\chi_A\|_2^2.$$

Az 1.1.5. állítás miatt  $\|\chi_A * g\chi_A\|_1 = |A|^2$  bármely  $g \in \mathbb{F}_p^*$ -re, tehát

$$|A + s_0 A| \geq \frac{\|\chi_A * s_0 \chi_A\|_1^2}{\|\chi_A * s_0 \chi_A\|_2^2} \geq \frac{|A|^4}{\frac{|A|^4}{p} + \frac{p|A|^2}{|S|}} = \frac{1}{\frac{1}{p} + \frac{p}{|S||A|^2}}.$$

Másrészt legalább  $(1 - c)|S|$  darab  $s \in S$  elemre igaz, hogy

$$|A + sA| \geq \frac{\|\chi_A * s\chi_A\|_1^2}{\|\chi_A * s\chi_A\|_2^2} \geq \frac{|A|^4}{\frac{c|A|^4}{p} + \frac{p|A|^2}{|S|}} = \frac{c}{\frac{1}{p} + \frac{p}{|S||A|^2}}.$$

□

## 2. Cayley-gráfok és csoportok átmérői

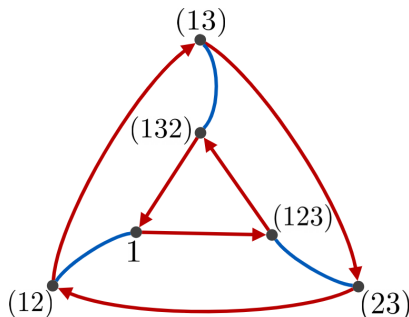
### 2.1. Definíciók

**2.1.1. Definíció (Cayley-gráf).** Egy  $G$  csoport és annak egy  $S \subseteq G$  részhalma által implikált  $Cay(G, S)$  Cayley-gráfján azt a  $(V, E)$  irányított gráfot értjük, ahol  $V = G$  és  $E = \{(g, gs) \mid g \in G, s \in S\}$ .

Minden  $Cay(G, S)$ -beli él megfeleltethető  $S$  egy elemének. Legtöbbször ha Cayley-gráfokról van szó, akkor fel van téve, hogy  $S$  egy generátorhalmaz (vagyis  $Cay(G, S)$  összefüggő) és az is, hogy az egységelem nincs benne  $S$ -ben, mert az csak hurokéleket rak minden csúcsra.

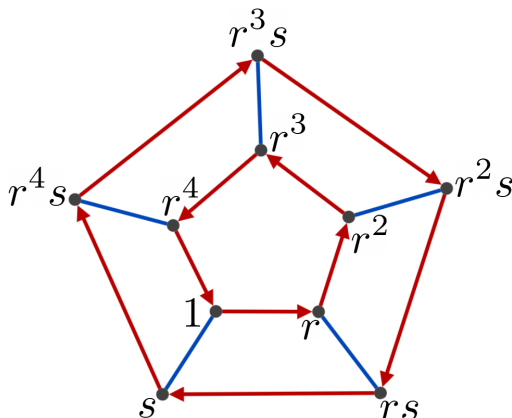
Ha  $s, s^{-1} \in S$ , akkor az  $s$ -hez tartozó éleket tekinthetjük irányítatlannak, mert  $(g, gs) \in E$  és  $(gs, gss^{-1}) = (gs, g) \in E$ . Ha pedig  $S = S^{-1}$ , akkor  $Cay(G, S)$  egy irányítatlan gráf.

**2.1.2. Példa.** Legyen  $G = S_3$  és  $S$  az  $\{(12), (123)\}$  generátorhalmaz.



Az  $(123)$  permutációhoz a piros, az  $(12)$  permutációhoz pedig a kék élek tartoznak, amik irányítatlanok, hiszen  $(12)^{-1} = (12)$ .

**2.1.3. Példa.** Legyen  $G = D_5 = \langle r, s \mid r^5 = 1, s^2 = 1, srs = r^{-1} \rangle$  és  $S$  az  $\{r, s\}$  generátorhalmaz.



A Cayley-gráf definíciójából látszik, hogy bármely csoport Cayley-gráfja egy  $d$ -reguláris gráf, ahol  $d$   $|S|$ -től függ.

**2.1.4. Definíció (Csúcstranzitivitás).** Egy  $(V, E)$  gráfot csúcstranzitívnak nevezzük, ha bármely  $u, v \in V$  csúcsokhoz létezik egy  $\varphi : V \rightarrow V$  gráfautomorfizmus úgy, hogy  $\varphi(u) = v$ .

**2.1.5. Állítás.** Bármely  $\text{Cay}(G, S)$  gráf csúcstranzitív.

**Bizonyítás:** Legyen  $g_1, g_2 \in G$  ( $g \neq h$ ) két tetszőleges csoportbeli elem.

Legyen  $\varphi : G \rightarrow G$ ,  $\varphi(g) = g_2 g_1^{-1} g$ . Ekkor  $\varphi(g_1) = g_2$  és  $\varphi$  egy gráfautomorfizmus, mert ha veszünk két csúcsot, akik össze vannak kötve  $(g, gs)$ , akkor azok képei is össze lesznek kötve:  $(g_2 g_1^{-1} g, g_2 g_1^{-1} gs)$ .  $\square$

## 2.2. A Babai-sejtés

**2.2.1. Definíció (Gráf átmérője).** Egy  $(V, E)$  véges gráf átmérőjén a két, egymástól legmesszebb lévő csúcs közti távolságot értjük, vagyis  $\text{diam}(V, E) = \max_{u, v \in V} d(u, v)$ , ahol  $d(u, v)$  az  $u$  és  $v$  csúcsok közti legrövidebb út hosszát jelöli.

Babai László és Seress Ákos a következő sejtést fogalmazták meg az 1992-ben megjelent cikkükben [3].

**2.2.2. Sejtés (Babai-sejtés).** Létezik egy abszolút  $C$  konstans úgy, hogy bármely  $G$  nem kommutatív, egyszerű csoport és annak bármely  $S$  generátorhalmazára

$$\text{diam}(\text{Cay}(G, S)) \leq (\log |G|)^C.$$

**2.2.3. Megjegyzés.** Kommutatív, egyszerű csoportokra valóban nem feltétlenül igaz a sejtés. Például legyen  $G_p = \mathbb{Z}_p = \langle g \mid g^p = 1 \rangle$ , ahol  $p$  egy prímszám és  $S = \{g\}$ , ekkor  $\log |G_p| = \log(p)$  és  $\text{diam}(\text{Cay}(G, S)) = \frac{p-1}{2}$  ( $p \neq 2$ ), amiből következik, hogy ha  $p \rightarrow \infty$ , akkor  $C \rightarrow \infty$ , vagyis nem létezik jó abszolút konstans.

Most lássunk egy állítást, ami kommutatív csoportok átmérőjére ad egy alsó becslést, amely megtalálható a már fent is említett [3] cikkben.

**2.2.4. Állítás.** Legyen  $G$  egy tetszőleges véges Abel-csoport és  $S$  neki egy generátorhalmaza. Ekkor

$$\text{diam}(\text{Cay}(G, S)) > |S| \left( \frac{|G|^{\frac{1}{|S|}}}{2e} - 1 \right).$$

**Bizonyítás:** Legyen  $d = \text{diam}(\text{Cay}(G, S))$  és  $S = \{s_1, s_2, \dots, s_{|S|}\}$ . Ekkor  $G$  bármely eleme felírható az  $s_1^{k_1} s_2^{k_2} \dots s_{|S|}^{k_{|S|}}$  alakban, ahol  $\sum_{i=1}^{|S|} |k_i| \leq d$ . Mivel  $G$  kommutatív, ezért a szorzás sorrendje nem számít, tehát

$$|G| \leq 2^{|S|} \binom{d + |S| - 1}{|S| - 1} < \left( \frac{2e(d + |S|)}{|S|} \right)^{|S|},$$

és ezzel beláttuk az állítást. □

### 3. A Babai-sejtés igazolása a $\mathrm{PSL}_2(\mathbb{F}_p)$ csoportra

$$\mathrm{SL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_p, ad - bc = 1 \right\}$$

$$\mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p) / \{\pm I\}$$

A következőkben a Babai-sejtést fogjuk bizonyítani a  $\mathrm{PSL}_2(\mathbb{F}_p)$  csoportra. Vagyis azt, hogy ha a nem kommutatív, egyszerű csoportok közül csak a  $\mathrm{PSL}_2(\mathbb{F}_p)$  csoportokat vesszük figyelembe (ahol  $p > 3$  egy prímszám), akkor létezik jó abszolút konstans.

A dolgozat során végig az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoporttal fogunk dolgozni, hiszen a  $\mathrm{PSL}_2(\mathbb{F}_p)$  csoport faktora neki, és  $|\mathrm{SL}_2(\mathbb{F}_p)| = 2|\mathrm{PSL}_2(\mathbb{F}_p)|$  bármely  $p$  prímre. Tehát ha igazoljuk a sejtést az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoportra és vesszük a  $\mathrm{PSL}_2(\mathbb{F}_p)$  egy generátor rendszerét, akkor annak a felemeltjéről már tudni fogjuk, hogy igaz rá a sejtés. A fő célunk az lesz, hogy bebizonyítsuk az alábbi állítást, és ebben a fejezetben nagyban hagyatkozunk Harald Helfgott munkájára [9].

#### 3.1. Nagy halmaz generálása logaritmikus lépésben

**3.1.1. Állítás.** Legyen  $p$  prímszám és  $A$  az  $\mathrm{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza. Ekkor az alábbiak igazak:

- (a) Ha  $|A| < p^{3-\delta}$  valamely rögzített  $\delta > 0$  számra, akkor

$$|A \cdot A \cdot A| > c|A|^{1+\varepsilon}$$

ahol  $c > 0$  és  $\varepsilon > 0$  csakis  $\delta$ -tól függnék.

- (b) Ha  $|A| > p^\delta$  valamely rögzített  $\delta$ -ra, akkor létezik egy csakis  $\delta$ -tól függő  $n \in \mathbb{N}$  szám úgy, hogy  $\mathrm{SL}_2(\mathbb{F}_p)$  bármely eleme kifejezhető legfeljebb  $n$  az  $A \cup A^{-1}$  halmazbeli elem szorzataként.

Itt fontos megjegyezni, hogy mind az (a), mind a (b) pontban szereplő  $c$ ,  $\varepsilon$  és  $n$  együtthatók nem függnék  $p$ -től. Az állítás (a) részének segítségével logaritmikus időben fel tudjuk fűjni a generátor halmazunkat "nagyra", ezt úgy értve, hogy már közel  $p^3$  méretű legyen a generált halmazunk. A  $p^3$ -re azért hivatkozunk nagyként, mert  $|\mathrm{SL}_2(\mathbb{F}_p)| = p^3 - p$ . A (b) rész segítségével pedig konstans lépésben elérjük a csoport összes elemét.

A tétel (a) részének bizonyításához vezető úton nagy segítségünkre lesz az alábbi távolságfogalom, amely Ruzsa Imre, magyar matematikus nevéhez fűződik.

**3.1.2. Definíció (Ruzsa-távolság [17]).** Egy  $G$  csoportban legyen  $A$  és  $B$  két tetszőleges részhalmaz. Az ő Ruzsa-távolságuk alatt a következőt értjük

$$d(A, B) = \log \frac{|AB^{-1}|}{\sqrt{|A||B|}}$$

Bár az így definiált  $d$  függvény elsőre egy metrikának tűnhet a  $\mathcal{P}(G)$  halmazon, valójában nem az. Legyen például  $A = B = gH$ , ahol  $H$  a  $G$  csoport egy tetszőleges nem triviális részcsoporthja,  $g$  pedig egy tetszőleges nem  $H$ -beli elem, ekkor

$$d(gH, gH) = \log \frac{|gHg^{-1}H^{-1}|}{\sqrt{|gH||gH|}} = \log \frac{|gHg^{-1}H|}{\sqrt{|H||H|}} = \log \frac{|(gHg^{-1})H|}{|H|},$$

ami nem feltétlenül 0, hiszen ha  $H$  nem normálosztó, akkor  $(gHg^{-1})H$  számossága sokkal nagyobb lehet mint  $|H|$ . Viszont ennek ellenére a háromszög-egyenlőtlenség igaz rá.

**3.1.3. Lemma (Háromszög-egyenlőtlenség [17]).** Egy  $G$  csoportban legyenek  $A$ ,  $B$  és  $C$  tetszőleges részhalmazok. Ekkor

$$d(A, C) \leq d(A, B) + d(B, C).$$

**Bizonyítás:** Azt szeretnénk belátni, hogy

$$\begin{aligned} d(A, C) \leq d(A, B) + d(B, C) &\iff \\ \log \frac{|AC^{-1}|}{\sqrt{|A||C|}} &\leq \log \frac{|AB^{-1}|}{\sqrt{|A||B|}} + \log \frac{|BC^{-1}|}{\sqrt{|B||C|}} \iff \\ \frac{|AC^{-1}|}{\sqrt{|A||C|}} &\leq \frac{|AB^{-1}|}{\sqrt{|A||B|}} \cdot \frac{|BC^{-1}|}{\sqrt{|B||C|}} \iff \\ |AC^{-1}||B| &\leq |AB^{-1}||BC^{-1}|. \end{aligned}$$

Ezt úgy szeretnénk belátni, hogy konstruálunk egy  $f : AC^{-1} \times B \hookrightarrow AB^{-1} \times BC^{-1}$  injekciót. Az összes  $d \in AC^{-1}$  elemhez rögzítsünk egy  $(a_d, c_d) \in A \times C$  párost úgy, hogy  $a_dc_d^{-1} = d$ . Ezt felhasználva legyen

$$f(d, b) = (a_db^{-1}, bc_d^{-1}).$$

Az  $f$  képhalmazából választott tetszőleges  $(a_db^{-1}, bc_d^{-1})$  párosból egyértelműen visszafejthető a  $d$  értéke, hiszen  $a_db^{-1}bc_d^{-1} = d$ . Viszont  $d$ -hez egyértelműen választottuk az  $a_d$  és a  $b_d$  elemeket, amikből már  $b$ -t is tudjuk. Vagyis  $f$  valóban egy injektív leképezés.  $\square$

Mostantól a háromszög-egyenlőtlenség használatát úgy jelöljük, hogy az egyenlőtlenség fölé írunk egy háromszöget:  $\triangle \geq$  vagy  $\triangle \leq$ .

Egy  $n > 0$  természetes szám mellett a továbbiakban jelölje  $A_n$  az  $A \cup A^{-1}$ -beli elemek legfeljebb  $n$  elemű szorzatainak a halmazát, vagyis

$$A_n = \left\{ a_1 a_2 \dots a_n \mid a_1, a_2, \dots, a_n \in A \cup A^{-1} \cup \{1\} \right\}.$$

**3.1.4. Lemma.** Legyen  $n > 2$  egy természetes szám és  $A$  egy részhalmaza a  $G$  csoportnak úgy, hogy

$$|A_n| > c|A|^{1+\varepsilon},$$

valamely  $c > 0$  és  $\varepsilon > 0$  számokra. Ekkor

$$|A \cdot A \cdot A| > c'|A|^{1+\varepsilon'},$$

ahol  $c' > 0$  és  $\varepsilon' > 0$  csakis  $c$ -től,  $\varepsilon$ -től és  $n$ -től függenek.

**Bizonyítás:** A fent bizonyított háromszög-egyenlőtlenséget fogjuk használni.

$$\frac{|A_n|}{|A|} = \frac{|A_{n-2} \cdot A_2|}{|A|} \triangleq \frac{|A_{n-2} \cdot A^{-1}| |A \cdot A_2|}{|A|} \leq \frac{|A_{n-1}|}{|A|} \frac{|A_3|}{|A|}$$

Ezt rekurzívan ismételve kapjuk, hogy

$$\frac{|A_n|}{|A|} \leq \left( \frac{|A_3|}{|A|} \right)^{n-2}.$$

Felhasználva a lemma feltételeit kapjuk, hogy

$$c|A|^\varepsilon < \frac{|A_n|}{|A|} \leq \left( \frac{|A_3|}{|A|} \right)^{n-2}.$$

Már csak annyit szeretnénk megtenni, hogy  $\frac{|A_3|}{|A|}$ -t felülről becsüljük  $\frac{|A \cdot A \cdot A|}{|A|}$  egy hatványával. Ezt úgy fogjuk megtenni, hogy az  $A_3$ -ban előforduló összes típusú szorzatot külön-külön becsülünk a háromszög-egyenlőtlenség segítségével.

$$\begin{aligned} \frac{|A \cdot A \cdot A^{-1}|}{|A|} &= \frac{|A \cdot A \cdot A^{-1}| |A^{-1}|}{|A|^2} \triangleq \frac{|A \cdot A \cdot A| |A^{-1} \cdot A^{-1}|}{|A|^2} \leq \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^2, \\ \frac{|A \cdot A^{-1} \cdot A|}{|A|} &= \frac{|A \cdot A^{-1} \cdot A| |A|}{|A|^2} \triangleq \frac{|A \cdot A^{-1} \cdot A^{-1}| |A \cdot A|}{|A|^2} = \frac{|A \cdot A \cdot A^{-1}| |A \cdot A|}{|A|^2} \leq \\ &\leq \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^2 \frac{|A \cdot A \cdot A|}{|A|} \leq \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^3, \\ \frac{|A^{-1} \cdot A \cdot A|}{|A|} &= \frac{|A^{-1} \cdot A \cdot A| |A^{-1}|}{|A|^2} \triangleq \frac{|A^{-1} \cdot A \cdot A^{-1}| |A^{-1} \cdot A^{-1}|}{|A|^2} = \frac{|A \cdot A^{-1} \cdot A| |A \cdot A|}{|A|^2} \leq \end{aligned}$$

$$\leq \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^3 \frac{|A \cdot A \cdot A|}{|A|} = \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^4.$$

Mindezek alapján

$$\begin{aligned} \frac{|A_3|}{|A|} &\leq \frac{1}{|A|} \left( |A \cdot A \cdot A| + |A^{-1} \cdot A^{-1} \cdot A^{-1}| + |A \cdot A \cdot A^{-1}| + |A \cdot A^{-1} \cdot A^{-1}| + |A \cdot A^{-1} \cdot A| + |A^{-1} \cdot A \cdot A^{-1}| + \right. \\ &\quad \left. + |A^{-1} \cdot A \cdot A| + |A^{-1} \cdot A^{-1} \cdot A| \right) = \frac{2}{|A|} \left( |A \cdot A \cdot A| + |A \cdot A \cdot A^{-1}| + |A \cdot A^{-1} \cdot A| + |A^{-1} \cdot A \cdot A| \right) \leq \\ &\leq 2 \left( \frac{|A \cdot A \cdot A|}{|A|} + \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^2 + \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^3 + \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^4 \right) < 8 \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^4. \end{aligned}$$

Ezt felhasználva

$$\begin{aligned} c|A|^\varepsilon &< \left( \frac{|A_3|}{|A|} \right)^{n-2} < 8^{n-2} \left( \frac{|A \cdot A \cdot A|}{|A|} \right)^{4(n-2)} \implies \\ |A \cdot A \cdot A| &> \frac{c^{\frac{1}{4(n-2)}}}{\sqrt[4]{8}} |A|^{1+\frac{\varepsilon}{4(n-2)}}. \end{aligned}$$

Tehát a  $c' = \frac{c^{\frac{1}{4(n-2)}}}{\sqrt[4]{8}}$  és az  $\varepsilon' = \frac{\varepsilon}{4(n-2)}$  választások kielégítik az állítást.  $\square$

Ez a lemma kulcsfontosságú lesz a továbbiakban, hiszen ha találunk valamilyen univerzális  $k$  konstanst, amire  $|A_k| > c|A|^{1+\varepsilon}$ , akkor be is láttuk a 3.1.1. állítás (a) részét. És pontosan ez lesz innentől a célunk. Először azért fogunk dolgozni, hogy találjunk egy  $\text{Tr}(A)$ -tól függő elemszámú, egyidejűleg diagonalizálható mátrixok egy halmazát  $A_4$ -ben, ahol  $A_4 = \left\{ a_1 a_2 a_3 a_4 \mid a_1, a_2, a_3, a_4 \in A \cup A^{-1} \cup \{1\} \right\}$ , ahogy azt már ezelőtt is definiáltuk.

**3.1.5. Állítás.** Legyen  $A$  a  $G$  csoport egy tetszőleges nem üres részhalmaza és jelölje  $\Omega_A$  az olyan konjugáltosztályok halmazát, amelyeknek van közös eleme az  $A$ -val. Ekkor létezik egy olyan  $a \in A$ , hogy

$$|C_G(a) \cap (A^{-1}A)| \geq \frac{|\Omega_A||A|}{|A \cdot A \cdot A^{-1}|}.$$

**Bizonyítás:** Vegyük az  $a, h_1, h_2$  elemeket az  $A$  halmazból, amikre igaz, hogy  $h_1 a h_1^{-1} = h_2 a h_2^{-1}$ . Ekkor  $h_2^{-1} h_1 \in A^{-1}A \cap C_G(a)$ . Tehát egy durva alsó becslést alkalmazva kapjuk, hogy bármely  $A$ -beli  $a$  elemre

$$|\{h a h^{-1} \mid h \in A\}| \geq \frac{|A|}{|C_G(a) \cap A^{-1}A|}.$$

Tartalmazom  $\Gamma \subset A$  az  $\Omega_A$ -beli konjugáltosztályokból egy-egy reprezentáns elemet. Tegyük fel, hogy bármely  $g \in \Gamma$ -re igaz, hogy  $|C_G(g) \cap A^{-1}A| < \frac{|\Omega_A||A|}{|A \cdot A \cdot A^{-1}|}$ . Ekkor

$$|A \cdot A \cdot A^{-1}| \geq |\{h g h^{-1} \mid h \in A, g \in \Gamma\}| \geq$$

$$\geq \sum_{g \in \Gamma} \frac{|A|}{|C_G(g) \cap A^{-1}A|} > \sum_{g \in \Gamma} \frac{|A \cdot A \cdot A^{-1}|}{|\Omega_A|} = |A \cdot A \cdot A^{-1}|,$$

tehát ellentmondásra jutottunk.  $\square$

**3.1.6. Lemma.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$  csoport egy tetszőleges részhalmaza. Ekkor  $A_2$  tartalmaz legalább  $\frac{1}{4}|A| - 1$  olyan mátrixot, amelyek nyoma nem  $\pm 2$ .

**Bizonyítás:** Legyen  $g \in A$  egy olyan mátrix, ami nem a  $\pm I$  és  $\text{Tr}(g) = 2$  vagy  $-2$ . Ha nem tudunk ilyen  $g$ -t választani, akkor készen vagyunk. Tudunk úgy bázist választani, hogy  $g = \begin{pmatrix} \lambda & t \\ 0 & \lambda^{-1} \end{pmatrix}$ . Mivel  $\text{Tr}(g) = \pm 2$ , ezért  $\lambda = \pm 1$ , hiszen

$$\text{Tr}(g) = \pm 2 \iff \lambda + \lambda^{-1} = \pm 2 \iff \lambda^2 \pm 2\lambda + 1 = 0 \iff (\lambda \pm 1)^2 = 0 \iff \lambda = \pm 1.$$

Tehát  $g = \begin{pmatrix} \pm 1 & t \\ 0 & \pm 1 \end{pmatrix}$  alakba írható, ahol  $t \neq 0$ , hiszen  $g \neq \pm I$ . Legyen

$$B = \left\{ h \in A \mid \text{Tr}(h) = \pm 2 \text{ és legalább egy közös sajátvektora van } g\text{-val} \right\}.$$

Először tegyük fel, hogy  $|B| \leq \frac{1}{4}|A| + 3$ . Legyen  $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A \setminus B$  egy tetszőleges mátrix. Nyilván  $c \neq 0$ , mert  $h \notin B$ . Ha bármely ilyen  $h$  mátrixnak a nyoma nem  $\pm 2$ , akkor készen vagyunk. Ha  $\text{Tr}(h) = \pm 2$ , akkor vizsgáljuk a  $gh$  és  $g^{-1}h$  mátrixok nyomát:

$$\begin{aligned} gh &= \begin{pmatrix} \pm 1 & t \\ 0 & \pm 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \pm a + tc & \dots \\ \dots & \pm d \end{pmatrix} \\ g^{-1}h &= \begin{pmatrix} \mp 1 & -t \\ 0 & \mp 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \mp a - tc & \dots \\ \dots & \mp d \end{pmatrix} \end{aligned}$$

Vagyis  $\text{Tr}(gh) = \pm(a + d) + tc = \pm 2 + tc$  és  $\text{Tr}(g^{-1}h) = \mp(a + d) - tc = \pm 2 - tc$ . Mivel sem  $t$ , sem  $c$  nem 0, ezért vagy  $gh$ -nak vagy  $g^{-1}h$ -nak a nyoma különbözik  $\pm 2$ -től. Ezek alapján  $A \cup A \cdot A \cup A^{-1} \cdot A$ -nak legalább  $\frac{1}{3}|A \setminus B| \geq \frac{1}{4}|A| - 1$  eleme van aminek a nyoma nem  $\pm 2$ .

Most tegyük fel, hogy  $|B| > \frac{1}{4}|A| + 3$ . Legyen  $h \in A$  olyan mátrix, aminek nincs közös sajátvektora  $g$ -vel. Ekkor legfeljebb kettő  $g' \in B$  elem létezik, amire  $\text{Tr}(g'h) = \pm 2$ , hiszen ahogy azt már korábban levezettük  $\text{Tr}(g'h) = \pm 2 + t'c$ , ami egy elsőfokú egyenlet  $t'$ -ben. Következtetésként,  $A \cdot A$  legalább  $\frac{1}{4}|A| + 3 - 2 = \frac{1}{4}|A| - 1$  mátrixot tartalmaz, amelyek nyoma különböző  $\pm 2$ -től.  $\square$

**3.1.7. Definíció.** Két azonos dimenziójú  $A$  és  $B$  négyzetes mátrixot ( $A, B \in \mathcal{M}_n$ ) egyidejűleg diagonizálhatónak nevezünk, ha létezik egy közös bázis, amiben mindketten egyszerre diagonálisak. Vagyis  $\exists S \in \mathcal{M}_n$  úgy, hogy  $S^{-1}AS$  és  $S^{-1}BS$  is diagonális.

**3.1.8. Következmény.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza. Feltéve, hogy  $|A| \geq 4$  és  $\text{Tr}(A) \geq 2$ , létezik legalább  $\frac{(|\text{Tr}(A)|-2)(\frac{1}{4}|A|-1)}{|A_6|}$  egyidejűleg diagonalizálható mátrix  $A_4$ -ben.

**Bizonyítás:** Legyen  $B = \{g \in A_2 \mid \text{Tr}(g) \neq \pm 2\}$ . Az előző lemma értelmében  $|B| \geq \frac{1}{4}|A| - 1$ . Alkalmazva a 3.1.5. állítást, kapunk egy olyan  $b \in B$  elemet, amire igaz, hogy

$$|C_G(b) \cap B^{-1}B| \geq \frac{|\Omega_B||B|}{|B \cdot B \cdot B^{-1}|} \geq \frac{|\text{Tr}(B)||B|}{|B \cdot B \cdot B^{-1}|} \geq \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|}.$$

Azt szeretnénk belátni, hogy a  $C_G(b) \cap B^{-1}B$  halmaz minden eleme diagonális abban a bázisban, amiben  $b$  az. Tegyük fel, hogy  $b$  diagonális valamilyen általunk választott bázisban, tehát  $b = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ . Mivel  $\text{Tr}(b) \neq \pm 2$ , ezért  $b \neq \pm I$  (és ezáltal  $\lambda \neq \lambda^{-1}$ ), hiszen

$$\text{Tr}(b) \neq \pm 2 \iff \lambda + \lambda^{-1} \neq \pm 2 \iff \lambda^2 \pm 2\lambda + 1 \neq 0 \iff (\lambda \pm 1)^2 \neq 0 \iff \lambda \neq \pm 1.$$

Vegyünk egy tetszőleges  $\begin{pmatrix} m & n \\ k & l \end{pmatrix}$  mátrixot a  $C_G(b) \cap B^{-1}B$  halmazból, ami nyilván kommutál  $b$ -vel

$$\begin{aligned} \begin{pmatrix} m & n \\ k & l \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} &= \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} m & n \\ k & l \end{pmatrix} \iff \\ \begin{pmatrix} \lambda m & \lambda^{-1} n \\ \lambda k & \lambda^{-1} l \end{pmatrix} &= \begin{pmatrix} \lambda m & \lambda n \\ \lambda^{-1} k & \lambda^{-1} l \end{pmatrix} \iff \\ \begin{cases} \lambda n = \lambda^{-1} n \\ \lambda k = \lambda^{-1} k \end{cases} &\stackrel{\lambda \neq \lambda^{-1}}{\iff} n = k = 0. \end{aligned}$$

Tehát valóban, ha  $b$  diagonális, akkor a  $C_G(b) \cap B^{-1}B$  minden eleme is az. Másrésről  $A_4 \supseteq B^{-1}B$  és ezzel beláttuk, amit szerettünk volna.  $\square$

A következő lemma alapvető fontosságú lesz abban, hogy találjunk egy olyan univerzális  $k$  konstanst, amire  $A_k$  méretét alulról tudjuk becsülni  $A$  és  $\text{Tr}(A)$  méretének segítségével.

**3.1.9. Lemma.** Legyen  $G \leq \text{GL}(V)$ , ahol  $V$  egy  $K$  test feletti vektortér. Továbbá legyen  $W = W_1 \cup W_2 \cup \dots \cup W_n$ , ahol  $W_1, W_2, \dots, W_n < V$  valódi alterek. Legyen  $A$  egy tetszőleges részhalmaza a  $G$  csoportnak és  $\mathcal{O}$  valamely  $V$ -beli elem  $\langle A \rangle$ -orbitja úgy, hogy  $\mathcal{O} \not\subseteq W$ . Ekkor léteznek  $\alpha > 0$  és  $m \in \mathbb{N}$  számok, amik csak  $n$ -től és  $\dim(V)$ -től függenek úgy, hogy bármely  $x \in \mathcal{O}$ -hoz létezik legalább  $\max\{1, \alpha|A|\}$  olyan  $g \in A_m$  elem úgy, hogy  $gx \notin W$ .

**Bizonyítás:** Először azt szeretnénk belátni, hogy létezik  $g_1, g_2, \dots, g_l \in A_r$  úgy, hogy bármely  $x \in \mathcal{O}$ -ra létezik legalább egy  $1 \leq i \leq l$  index, hogy  $g_i x \notin W$  ( $l$  és  $r$  itt is csak  $\dim(V)$ -től és  $n$ -től függnék). Ezt teljes indukcióval fogjuk belátni a  $(d_W, s_W)$  számkettőre nézve, ahol

$$d_W = \max_{1 \leq i \leq n} \dim W_i \text{ és } s_W = |\{W_i \mid \dim W_i = d_W\}|.$$

Másszóval, az aktuális  $W$ -ben szereplő alterek maximális dimenziójára és az ilyen dimenziójú alterek számára indukciózunk. Az lesz a célunk, hogy az indukciós lépés során  $W$ -ről egy olyan  $W'$ -re lépjünk, ahol  $d_W > d_{W'}$  vagy  $d_W = d_{W'}$  viszont  $s_W > s_{W'}$ .

Legyen  $D = \bigcup_{\dim W_i = d_W} W_i$ .

Ha  $D \cap \mathcal{O} = \emptyset$ , akkor legyen  $W' = W \setminus D$ . Alkalmazva az indukciós feltevést  $W'$ -re kapunk  $g_1, g_2, \dots, g_{l_{W'}} \in A_{r_{W'}}$  elemeket, hogy bármely  $x \in \mathcal{O}$ -re létezik legalább egy  $1 \leq i \leq l_{W'}$ , hogy  $g_i x \notin W'$ . Mivel  $D \cap \mathcal{O} = \emptyset$ , ezért az is igaz, hogy  $g_i x \notin W$ .

Ha  $D \cap \mathcal{O} \neq \emptyset$ , akkor létezik egy olyan  $x' \in \mathcal{O} \cap D$ , amihez létezik egy  $g \in A \cup A^{-1}$  úgy, hogy  $gx' \notin D$ . Ekkor legyen  $W' = W \cap gW = (W_1 \cap gW) \cup (W_2 \cap gW) \cup \dots \cup (W_n \cap gW)$ . Mivel  $x'$  valamely maximális dimenziójú  $W_i$  altérben benne van, viszont a  $g$  szerinti képe nincs, ezért  $W'$  kevesebb  $d_W$  dimenziójú alteret tartalmaz ( $s_W > s_{W'}$ ) vagy  $d_W > d_{W'}$ . Akárhogy is, alkalmazhatjuk az indukciós feltevést  $W'$ -re.

Az indukciós feltevés szerint létezik  $g'_1, g'_2, \dots, g'_{l'} \in A_{r'}$  úgy, hogy bármely  $x \in \mathcal{O}$ -hoz legalább az egyik  $g'_i x \notin W' = W \cap gW$ , vagyis  $g'_i x \notin W$  vagy  $g'_i x \notin gW$ . Ha  $g'_i x \notin gW$ , akkor  $g^{-1}g'_i x \notin W$ .

Mindezek alapján legyen

$$g_1 = g'_1, g_2 = g'_2, \dots, g_{l'} = g'_{l'}$$

$$g_{l'+1} = g^{-1}g'_1, g_{l'+2} = g^{-1}g'_2, \dots, g_{2l'} = g^{-1}g'_{l'} \quad (l = 2l' \text{ és } r = r' + 1).$$

Végül, bármely  $x \in \mathcal{O}$  és bármely  $g \in A$ -ra legalább egy  $g_i gx$  nem lesz benne  $W$ -ben, ahol  $1 \leq i \leq l$  és  $g_i \in A_r$ . Minden lehetséges  $g_i g$  legfeljebb  $l$  különböző  $g \in A$  elemhez tartozhat. Tehát, legalább  $\min\{1, \frac{|A|}{l}\}$   $h = g_i g$  elemre igaz, hogy  $hx \notin W$ .  $\square$

**3.1.10. Következmény.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza ( $p > 3$ ). Létezik egy olyan  $k$  abszolút konstans, hogy  $\overline{\mathbb{F}_p}^2$  bármely  $v_1, v_2$  bázisához tartozik egy  $g \in A_k$  elem úgy, hogy  $gv_i \neq \lambda v_j \quad \forall \lambda \in \overline{\mathbb{F}_p}, i, j \in \{1, 2\}$ .

**Bizonyítás:** Az előző 3.1.9. lemmát szeretnénk használni. Legyen  $V = \mathcal{M}_2(\mathbb{F}_p)$ , vagyis a  $2 \times 2$ ,  $\mathbb{F}_p$  feletti invertálható mátrixok vektortere. Továbbá legyen

$$W = \{h \in V \mid hv_i = \lambda v_j \text{ ahol } \lambda \in \overline{\mathbb{F}_p} \text{ és } i, j \in \{1, 2\}\} = M_{1,1} \cup M_{1,2} \cup M_{2,1} \cup M_{2,2},$$

ahol  $M_{i,j} = \{h \in V \mid hv_i = \lambda v_j \text{ ahol } \lambda \in \mathbb{F}_p\} < V$  és  $x = I$ . Mivel  $\langle A \rangle = \text{SL}_2(\mathbb{F}_p)$ , ezért  $\mathcal{O} = \text{SL}_2(\mathbb{F}_p)$ , tehát a lemma értelmében létezik egy  $k$  konstans és  $g \in A_k$  úgy, hogy  $gx = g \notin W$  és ezt szeretnénk volna belátni. Viszont ahhoz, hogy használni tudjuk az előző lemmát, először ellenőriznünk kell, hogy  $\mathcal{O} = \text{SL}_2(\mathbb{F}_p) \not\subseteq W$ .

Azt fogjuk megmutatni, hogy  $|\text{SL}_2(\mathbb{F}_p)| < |W \cap \mathcal{O}|$ . Ismert, hogy  $|\text{SL}_2(\mathbb{F}_p)| = p(p^2 - 1)$ . Tudjuk, hogy

$$W \cap \mathcal{O} = G_{1,1} \cup G_{1,2} \cup G_{2,1} \cup G_{2,2},$$

ahol  $G_{i,j} = \{h \in \text{SL}_2(\mathbb{F}_p) \mid hv_i = \lambda v_j \text{ ahol } \lambda \in \mathbb{F}_p\}$ . Vegyünk egy tetszőleges  $G_{i,j}$ -beli  $g$  elemet és egy  $v \in \mathbb{F}_p^2$  vektort, ami nem skalárszorosa  $v_i$ -nek. Mivel  $\det(g) = 1$  és  $gv_i = \lambda v_j$ , ezért  $gv$  értéke egyértelmű kell legyen adott  $\lambda$  mellett. Tehát  $|G_{i,j}| \leq p^2 - 1$ , vagyis  $|W \cap \mathcal{O}| \leq 4(p^2 - 1)$ . Mivel feltettük, hogy  $p > 3$  prím, ezért  $|W \cap \mathcal{O}| \leq 4(p^2 - 1) < p(p^2 - 1) = |\text{SL}_2(\mathbb{F}_p)|$ .  $\square$

**3.1.11. Következmény.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza. Ekkor léteznek olyan abszolút  $c > 0$  és  $k \in \mathbb{N}$  konstansok úgy, hogy bármely két rögzített  $v_1, v_2 \in \overline{\mathbb{F}_p}^2$  vektor mellett

$$|A_k \setminus (H_{v_1} \cup H_{v_2})| > c|A|,$$

ahol  $H_v = \{h \in \text{SL}_2(\mathbb{F}_p) \mid h\text{-nak } v \text{ egy sajátvektora}\}$ .

**Bizonyítás:** Az előző bizonyításhoz hasonlóan, szintén a 3.1.9. lemmát szeretnénk használni. Most is legyen  $V = \mathcal{M}_2(\mathbb{F}_p)$ ,  $x = I$  és  $W = H'_{v_1} \cup H'_{v_2}$ , ahol

$$H'_{v_i} = \{h \in \mathcal{M}_2(\mathbb{F}_p) \mid h\text{-nak } v_i \text{ egy sajátvektora}\}.$$

Mivel  $x = I$ , ezért  $\mathcal{O} = \langle A \rangle = \text{SL}_2(\mathbb{F}_p)$ . Ahhoz, hogy használni tudjuk a lemmát, be kell látnunk, hogy  $\text{SL}_2(\mathbb{F}_p) \not\subseteq W$ . Vegyük az alábbi három  $\text{SL}_2(\mathbb{F}_p)$ -beli mátrixot:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Ezen mátrixoknak nincsen közös sajátvektora, tehát nem léteznek olyan  $v_1, v_2$  vektorok, amire bármely  $\text{SL}_2(\mathbb{F}_p)$ -beli mátrixnak ők a sajátvektorai lennének.

Tehát a 3.1.9. lemma alapján létezik egy abszolút  $k \in \mathbb{N}$  és egy  $c > 0$  úgy, hogy legalább  $c|A|$  darab  $g \in A_k$ -re igaz, hogy  $gx = g \notin W$ . Vagyis  $|A_k \setminus (H_{v_1} \cup H_{v_2})| > c|A|$ , és ezt szeretnénk volna belátni.  $\square$

A következő lemma segítségével megmutatjuk, hogy hogyan gyárthatunk "nagy" halmazt egyidejűleg diagonalizálható mátrixok és egy olyan elem segítségével, aki nem diagonális az ő közös sajátbázisukban.

**3.1.12. Lemma.** Legyen  $V \subset \text{SL}_2(\mathbb{F}_p)$  egyidejűleg diagonalizálható mátrixok egy halmaza (a közös sajátvektoraik legyenek  $v_1$  és  $v_2$ ). Legyen továbbá  $g \in \text{SL}_2(\mathbb{F}_p)$  olyan, hogy  $gv_i \neq \lambda v_j \ \forall \lambda \in \overline{\mathbb{F}_p}, i, j \in \{1, 2\}$ . Ekkor

$$|VgVg^{-1}V| \geq \frac{1}{2} \left( \frac{1}{4}|V| - 6 \right) |V|^2.$$

**Bizonyítás:** Bár feltettük, hogy létezik a fenti feltételekkel rendelkező  $g$  mátrix, valóban a 3.1.10. következmény biztosítja számunkra egy ilyen elem létezését. A továbbiakban írjunk minden mátrixot a  $v_1, v_2$  bázisban. A fentiek értelmében  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , ahol  $a, b, c, d \neq 0$  és bármely  $V$ -beli  $v$  mátrixra igaz, hogy  $v = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$ . Tekintsük a

$$g \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} g^{-1} = \begin{pmatrix} rad - r^{-1}bc & ab(r^{-1} - r) \\ cd(r - r^{-1}) & r^{-1}ad - rbc \end{pmatrix}$$

mátrixot. A mellékátló elemeinek a szorzata  $-abcd(r - r^{-1})^2$ . Vegyük az  $r \mapsto -abcd(r - r^{-1})^2$  leképzést, ez nem küldhet négynél több különböző elemet egy tetszőlegesen választott  $\mathbb{F}_p^*$ -beli elembe, hiszen a  $-abcd(r - r^{-1})^2 = \lambda$  egy negyedfokú egyenlet. Vagyis

$$|\{h_{12}h_{21} \mid h \in gVg^{-1}\}| \geq \frac{|V|}{4}.$$

A főátlón lévő elemek akkor és csakis akkor lehetnek egyszerre nullák, ha  $r^2 - r^{-2} = 0$ , ami az  $r$  legfeljebb négy különböző értékére történhet meg. Legyen  $U = \{h \in gVg^{-1} \mid h_{11}h_{12}h_{21} \neq 0 \text{ és } h_{22}h_{12}h_{21} \neq 0\}$ , ekkor  $|\{h_{12}h_{21} \mid h \in U\}| \geq \frac{|V|}{4} - 6$ , mert a mellékátlón lévő elemek akkor és csakis akkor lehetnek nullák, ha  $r = \pm 1$  (ekkor a főátlón lévő elemek nem nullák, hiszen  $ad - bc = 1$ ), ha  $r \neq \pm 1$ , akkor a főátló mindkét eleme nullának kell lennie, amiről megmutattuk, hogy legfeljebb négy értékre lehet igaz.

Rögzítsünk egy  $h \in U$  mátrixot. Továbbá legyen

$$f_h(s, t) = \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix} \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} = \begin{pmatrix} sth_{11} & st^{-1}h_{12} \\ s^{-1}th_{21} & s^{-1}t^{-1}h_{22} \end{pmatrix}.$$

Világos, hogy  $f_h(s, t) \in VgVg^{-1}V$ . A mellékátló szorzata  $h_{12}h_{21}$ , vagyis a  $h \in U$  ismeretében visszafejthető  $s^2, t^2$  és  $st$  az  $f_h(s, t)$ -ből. Tehát, rögzített  $h$  mellett legfeljebb kettő  $(s, t)$  párra lesz az  $f_h(s, t)$  mátrix megegyező. Ezek szerint, választva egy konkrét  $h$ -t minden  $\{h_{12}h_{21} \mid h \in U\}$ -beli elemhez, kapjuk, hogy

$$|VgVg^{-1}V| \geq \frac{1}{2} |\{h_{12}h_{21} \mid h \in U\}| |V|^2 \geq \frac{1}{2} \left( \frac{1}{4}|V| - 6 \right) |V|^2.$$

□

**3.1.13. Állítás.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza. Feltéve, hogy  $|\text{Tr}(A)| \geq 2$ ,  $|A| \geq 4$  és  $p > 3$ , akkor létezik egy abszolút  $k \in \mathbb{N}$  konstans úgy, hogy

$$|A_k| \geq \frac{1}{2} \left( \frac{1}{4} \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|} - 6 \right) \left( \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|} \right)^2.$$

**Bizonyítás:** A 3.1.8. következmény szerint létezik  $V \subset A_4$  egyidejűleg diagonalizálható mátrixok halmaza úgy, hogy  $|V| \geq \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|}$ . A  $V$ -ben lévő mátrixok közös sajátvektorai legyenek  $v_1$  és  $v_2$ , a 3.1.10. következmény szerint létezik egy  $g \in A_l$  úgy, hogy  $gv_i \neq \lambda v_j$  bármely  $\lambda \in \overline{\mathbb{F}_p}$ ,  $i, j \in \{1, 2\}$ . Végül, az előző lemma szerint

$$\begin{aligned} |A_{2l+12}| &\geq |VgVg^{-1}V| \geq \frac{1}{2} \left( \frac{1}{4}|V| - 6 \right) |V|^2 \geq \\ &\geq \frac{1}{2} \left( \frac{1}{4} \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|} - 6 \right) \left( \frac{(|\text{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|} \right)^2. \end{aligned}$$

□

Az előző állítás segítségével megmutattuk, hogy  $|A_k|$  mérete alulról becsülhető nagyjából  $\frac{|\text{Tr}(A)|^3|A|^3}{8|A_6|^3}$ -nal. Természetes ötlet, hogy megpróbáljunk egy  $k$ -tól független  $k'$  másik univerzális konstans találni úgy, hogy  $|\text{Tr}(A_{k'})| \geq |A|^{\frac{1}{3}}$ . Pontosan ezt fogjuk tenni. Persze, még utána marad a feladat, hogy ezt a két eredményt megpróbáljuk valahogy összehangolni egy új univerzális konstansban.

**3.1.14. Lemma.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges részhalmaza. Rögzítsünk az  $\overline{\mathbb{F}_p}^2$  egy  $v_1, v_2$  bázisát és írjunk minden  $\text{SL}_2(\mathbb{F}_p)$ -beli mátrixot ebben a bázisban. Feltéve, hogy bármely  $g \in A$  mátrixra igaz, hogy  $g_{12}, g_{21} \neq 0$  (vagyis a  $v_1, v_2$  nem sajátbázisa egyetlen  $A$ -beli elemnek sem), akkor

$$|\text{Tr}(AA^{-1})| \geq \frac{|A|}{2|\{(g_{11}, g_{22}) \mid g \in A\}|}.$$

**Bizonyítás:** Válasszuk olyan  $g, h \in A$  mátrixokat, amikre igaz, hogy a főátlóik megegyeznek, vagyis  $g_{11} = h_{11}, g_{22} = h_{22}$ . Felhasználva, hogy  $h_{11}h_{22} - h_{12}h_{21} = 1$ , kapjuk, hogy

$$\text{Tr}(gh^{-1}) = g_{11}h_{22} + g_{22}h_{11} - g_{12}h_{21} - g_{21}h_{12} = 2g_{11}g_{22} - g_{12}h_{21} - g_{21} \frac{g_{11}g_{22} - 1}{h_{21}}.$$

Vagyis, egy rögzített  $g \in A$  mátrixhoz legfeljebb kettő  $h \in A$  tartozhat úgy, hogy  $h_{11}h_{22} - h_{12}h_{21} = 1$  és  $\text{Tr}(gh^{-1}) = k$  valamely szintén rögzített  $k \in \mathbb{F}_p$  értékhez, hiszen a  $\text{Tr}(gh^{-1}) = k$  egy  $h_{21}$ -ben másodfokú egyenletre redukálódik. És ebből adódik a lemma állítása. □

**3.1.15. Állítás.** Legyen  $A$  az  $\text{SL}_2(\mathbb{F}_p)$ -nek egy tetszőleges generátorhalmaza. Ekkor léteznek olyan abszolút  $k \in \mathbb{N}$  és  $c > 0$  konstansok, hogy

$$\text{Tr}(A_k) > c|A|^{\frac{1}{3}}.$$

**Bizonyítás:** Válasszunk egy  $h \in A$  mátrixot úgy, hogy  $\text{Tr}(h) \neq \pm 2$ . Amennyiben nem tudunk ilyen elemet választani, akkor a 3.1.6. lemma alapján  $A_2$ -ből már biztosan tudunk. Minden  $\text{SL}_2(\mathbb{F}_p)$ -beli mátrixot írjunk a  $h$  sajátvektoraiból álló  $v_1, v_2$  bázisban.

A 3.1.11. következmény értelmében léteznek  $k_0 \in \mathbb{N}$  és  $c_0 > 0$  abszolút konstansok, hogy  $|X| > c_0|A|$ , ahol  $X = A_{k_0} \setminus (H_{v_1} \cup H_{v_2})$ . A 3.1.14. lemma értelmében

$$|\text{Tr}(A_{2k_0})| \geq |\text{Tr}(XX^{-1})| \geq \frac{|X|}{2|\{(g_{11}, g_{22}) \mid g \in X\}|}.$$

Legyen  $t \in \mathbb{F}_p$ , ekkor definiáljuk  $D_t$ -t a következőképp  $\{(g_{11}, g_{22}) \mid g_{11} + g_{22} = t \text{ és } g \in X\}$ . Válasszuk meg  $t_0$ -t úgy, hogy  $|D_{t_0}|$  maximális legyen. Tudjuk, hogy  $h = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$ . Vizsgáljuk a  $hg$  mátrix nyomát, ahol  $g \in X$  és  $(g_{11}, g_{22}) \in D_{t_0}$ .

$$\text{Tr}(hg) = rg_{11} + r^{-1}g_{22} = (r - r^{-1})g_{11} + r^{-1}t_0 = rt_0 + (r^{-1} - r)g_{22}$$

Vagyis különböző  $g, g'$  mátrixokra, amik főátlói benne vannak  $D_{t_0}$ -ban, a  $hg$  és a  $hg'$  mátrixok nyomai is különbözőek kell, hogy legyenek. Tehát

$$|\text{Tr}(A_{k_0+2})| \geq |\text{Tr}(hX)| \geq |D_{t_0}| \geq \frac{|\{(g_{11}, g_{22}) \mid g \in X\}|}{|\text{Tr}(X)|}.$$

Az eddig felírt két egyenlőtlenség megfelelő tagjait összeszorozva kapjuk, hogy

$$|\text{Tr}(A_{2k_0})||\text{Tr}(A_{k_0+2})| \geq \frac{|X|}{2|\text{Tr}(X)|}.$$

Mindkét oldalt végigszorozva  $|\text{Tr}(X)|$ -el, majd egy egyszerű felsőkorlátot véve adódik, hogy

$$|\text{Tr}(A_{2k_0})|^3 \geq |\text{Tr}(A_{2k_0})||\text{Tr}(A_{k_0+2})||\text{Tr}(X)| \geq \frac{1}{2}|X|.$$

Mindezek alapján

$$|\text{Tr}(A_{2k_0})| \geq \frac{c_0^{\frac{1}{3}}}{2^{\frac{1}{3}}}|A|^{\frac{1}{3}}.$$

□

A következő állítást bizonyítás nélkül mondjuk ki.

**3.1.16. Állítás.** Legyen  $\delta > 0$  és  $a, b \in \mathbb{F}_{p^n}^*$ , ahol  $n \in \mathbb{N}$  tetszőleges. Ekkor bármely  $V \subset \mathbb{F}_{p^n}^*$ -ra, amire  $C < |V| < p^{1-\delta}$  igaz, hogy

$$|\{a(xy + x^{-1}y^{-1}) + b(x^{-1}y + xy^{-1}) \mid x, y \in V_{20}\}| > |V|^{1+\varepsilon},$$

ahol  $C > 0$  és  $\varepsilon > 0$  csakis a  $\delta$ -tól függnnek.

Be szeretnénk látni a 3.1.1. állítás (a) pontját, ami a következőképpen szól:

Ha  $|A| < p^{3-\delta}$  valamely rögzített  $\delta > 0$  számra, akkor

$$|A \cdot A \cdot A| > c|A|^{1+\varepsilon}$$

ahol  $c > 0$  és  $\varepsilon > 0$  csakis  $\delta$ -tól függnék.

Ehhez a 3.1.4. lemmát szeretnénk használni, vagyis az lesz a célunk, hogy találjunk egy olyan  $k \in \mathbb{N}$  számot, amire igaz, hogy  $|A_k| \geq c|A|^{1+\varepsilon}$ .

Feltehetjük, hogy  $p$  nagyobb valamilyen abszolút konstansnál, hiszen ha nem lenne az, akkor az (a) pontban szereplő  $c$  konstans elég kicsire megválasztva az állítást beláttuk. Ugyanezen ok miatt feltehető, hogy  $|A|$  is nagyobb valamilyen abszolút konstansnál.

A 3.1.15. állítás értelmében léteznek olyan  $k_0 \in \mathbb{N}$  és  $c_0 > 0$  abszolút konstansok, hogy  $|\text{Tr}(A_{k_0})| \geq c_0|A|^{\frac{1}{3}}$ . Az előbb elmondottak alapján feltehető, hogy  $|A| \geq \max\{\frac{4^3}{c_0^3}, 2^3\}$ , vagyis  $|\text{Tr}(A_{k_0})| \geq 4$  és  $|A| \geq 2$ . Ezek alapján az  $A$ -ra alkalmazható a 3.1.8. következmény, ami azt állítja, hogy létezik legalább

$$\frac{(|\text{Tr}(A_{k_0})| - 2)(\frac{1}{4}|A_{k_0}| - 1)}{|A_{6k_0}|} \geq \frac{c_0|A|^{\frac{1}{3}}|A_{k_0}|}{16|A_{6k_0}|}$$

egyidejűleg diagonalizálható mátrix  $A_{4k_0}$ -ban. Legyen  $V$  ezen mátrixok sajátértékeinek halmaza, ami bijekcióban áll magukkal a mátrixokkal, hiszen minden ilyen mátrix  $\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$  alakú. Nyilván feltehetjük, hogy  $c_0 < 1$  és azt is, hogy  $|A_{6k_0}| < |A|^{1+\frac{1}{6}}$ , különben a 3.1.4. lemma alapján már kész volnánk. Továbbá a feltevéseink között volt, hogy  $|A| < p^{3-\delta}$ . Ezek alapján

$$C < \frac{c_0}{16}|A|^{\frac{1}{6}} < |V| < |A|^{\frac{1}{3}} < p^{1-\frac{\delta}{3}},$$

ahol választhatunk ilyen megfelelő  $C$  konstans, hiszen feltettük, hogy  $|A|$  alulról korlátos.

A 3.1.10. következmény értelmében létezik egy olyan  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A_{k_1}$  mátrix, hogy  $a, b, c, d \neq 0$ , ahol  $k_1$  egy abszolút konstans.

$$\begin{aligned} \text{Tr}\left(\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\right) &= ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1}) \\ \implies \text{Tr}(A_{160k_0+2k_1}) &= \text{Tr}(A_{20 \cdot 4k_0+k_1+20 \cdot 4k_0+k_1}) \supset \\ &\supset \{ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1}) \mid x, y \in V_{20}\} \end{aligned}$$

Alkalmazva a 3.1.16. állítást, kapjuk, hogy

$$|\text{Tr}(A_{160k_0+2k_1})| > |V|^{1+\varepsilon},$$

ahol  $\varepsilon$  csakis  $\delta$ -tól függ. Az előzőekben használt okok miatt szintén feltehetjük, hogy

$$\frac{|\mathrm{Tr}(A_{160k_0+2k_1})||A_{160k_0+2k_1}|}{|A_{6(160k_0+2k_1)}|} \geq 40,$$

különben készen volnánk. A 3.1.13. állítás alapján létezik egy olyan abszolút  $k_2$  konstans, hogy

$$\begin{aligned} |A_{k_2(160k_0+2k_1)}| &\geq \frac{1}{2^{16}} \frac{|\mathrm{Tr}(A_{160k_0+2k_1})|^3 |A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3} \geq \frac{1}{2^{16}} \frac{|\mathrm{Tr}(A_{160k_0+2k_1})|^3}{|A_{6(160k_0+2k_1)}|^3} |V|^{3(1+\varepsilon)} \geq \\ &\geq \frac{1}{2^{16}} \frac{|\mathrm{Tr}(A_{160k_0+2k_1})|^3}{|A_{6(160k_0+2k_1)}|^3} \frac{c_0^3 |A_{k_0}|^3}{2^{12} |A_{6k_0}|^3} |A|^{1+\varepsilon} \geq \frac{c_0^3}{2^{28}} \frac{|A|^6}{|A_{6(160k_0+2k_1)}|} |A|^{1+\varepsilon}. \end{aligned}$$

Vagyis,  $|A_{6(160k_0+2k_1)}| \geq \frac{c_0^{\frac{3}{7}}}{16} |A|^{1+\frac{\varepsilon}{7}}$  vagy  $|A_{k_2(160k_0+2k_1)}| \geq \frac{c_0^{\frac{3}{7}}}{16} |A|^{1+\frac{\varepsilon}{7}}$ . Felhasználva a 3.1.4. lemmát, beláttuk a fő tételünk (a) pontját.

Ennek segítségével tudunk konstruálni egy  $p^{3-\delta}$  méretű halmazt úgy, hogy az  $A$  generátorhalmazunkat önmagával összeszorozzuk  $(\log \frac{p}{|A|})^c$ -szer.

## 3.2. Az egész csoport elérése egy nagy halmazból

Most már csak azt kell megmutatnunk, hogy létezik egy  $p$ -től független szám úgy, hogy egy majdnem akkora halmazból, mint maga az  $\mathrm{SL}_2(\mathbb{F}_p)$  hogyan kapjuk meg az egész csoportot ennyi lépésben.

**3.2.1. Lemma.**  $\mathrm{SL}_2(\mathbb{F}_p)$  bármely eleme a következő alakba írható

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix},$$

ahol  $x, y, z, s, t \in \mathbb{F}_p$ .

**Bizonyítás:** Legyen  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$  egy tetszőleges mátrix. Tegyük fel, hogy  $a \neq 0$ . Ekkor számolással igazolható, hogy

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1+ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-a^2 & 1 \end{pmatrix}.$$

Ha  $a = 0$ , akkor  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & d \end{pmatrix}$ . Ha  $d = 0$ , akkor a Gauss-elimináció segítségével olyan alakba tudjuk hozni ahol a bal felső elem nem nulla.  $\square$

**3.2.2. Lemma.** Legyen  $p$  prím. Legyen  $H$  az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoport felső vagy alsó háromszög-mátrix részcsoportha. Legyen továbbá  $A \subset H$  olyan, hogy  $|A| > 2p^{\frac{5}{3}} + 1$ . Ekkor  $A_8$  tartalmazza a  $H$  összes 2 nyomú elemét.

**Bizonyítás:** Feltehetjük, hogy  $H$  a felső háromszög-mátrixok csoportja. Legyen

$$P_r(A) = \left\{ x \in \mathbb{F}_p \left| \begin{pmatrix} r & x \\ 0 & r^{-1} \end{pmatrix} \in A \right. \right\}.$$

Mivel  $|A| > 2p^{\frac{5}{3}} + 1$ , ezért a skatulya-elv alapján létezik egy  $r \in \mathbb{F}_p^*$  úgy, hogy  $|P_r(A)| > 2p^{\frac{2}{3}}$ . Legyen  $t \neq r$  és  $\begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \in A$ . Ekkor

$$\begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} r & x \\ 0 & r^{-1} \end{pmatrix} \begin{pmatrix} t^{-1} & -u \\ 0 & t \end{pmatrix} \begin{pmatrix} r^{-1} & x' \\ 0 & r \end{pmatrix} = \begin{pmatrix} 1 & r(-x' + t^2x) + (1 - r^2)ut \\ 0 & 1 \end{pmatrix}.$$

Tehát  $P_1(AAA^{-1}A^{-1}) \supset r(-P_r(A) + t^2P_r(A)) + (1 - r^2)ut$ . Legyen

$$S = \left\{ t \in \mathbb{F}_p^* \left| t \neq r \text{ és } \exists u \in \mathbb{F}_p : \begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \in A \right. \right\}.$$

Mivel  $|A| > 2p^{\frac{5}{3}} + 1$ , ezért  $|S| > \frac{2p^{\frac{5}{3}} - p}{p} > p^{\frac{2}{3}}$ . Az 1.2.4. állítás következtében létezik egy olyan  $t \in S$ , hogy

$$|r(-P_r(A) + t^2P_r(A)) + (1 - r^2)ut| = |P_r(A) - t^2P_r(A)| \geq \frac{1}{\frac{1}{p} + \frac{1}{2|S||P_r(A)|^2}} \geq \frac{1}{\frac{1}{p} + \frac{1}{2p}} = \frac{2}{3}p$$

Vagyis

$$\left( r(-P_r(A) + t^2P_r(A)) + (1 - r^2)ut \right) + \left( r(-P_r(A) + t^2P_r(A)) + (1 - r^2)ut \right) = \mathbb{F}_p$$

Tehát  $AAA^{-1}A^{-1}AAA^{-1}A^{-1}$  tartalmazza az összes  $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$  alakú mátrixot, és ezt szerettük volna belátni.  $\square$

Már csak a 3.1.1. állítás (b) pontja maradt hátra. Az (a) pont miatt feltehetjük, hogy  $|A| > 6p^{3-\frac{1}{3}} = 6p^{\frac{8}{3}} > (2p^{\frac{5}{3}} + 1)(p + 1)$ . A skatulya-elv szerint létezik legalább  $2p^{\frac{5}{3}} + 1$  mátrix, amelyek felső sora pozitív szorzó erejéig megegyezik, és hasonló okok miatt ugyanez elmondható az alsó sorokról is. Vagyis az  $AA^{-1}$  tartalmaz legalább  $2p^{\frac{5}{3}} + 1$  felső, illetve alsó háromszög-mátrixot, hiszen

$$\begin{pmatrix} m & n \\ a & b \end{pmatrix} \begin{pmatrix} s & t \\ \lambda a & \lambda b \end{pmatrix}^{-1} = \begin{pmatrix} m & n \\ a & b \end{pmatrix} \begin{pmatrix} \lambda b & -t \\ -\lambda a & s \end{pmatrix} = \begin{pmatrix} \lambda(mb - na) & ns - mt \\ 0 & bs - at \end{pmatrix}.$$

Az előző lemma alapján  $(AA^{-1})_8$  tartalmazza az összes  $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$  és  $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$  alakú mátrixot. Másrészt viszont megmutattuk, hogy  $\text{SL}_2(\mathbb{F}_p)$  minden eleme

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

alakba írható. Tehát  $\text{SL}_2(\mathbb{F}_p) = (AA^{-1})_8(AA^{-1})_8(AA^{-1})_8(AA^{-1})_8(AA^{-1})_8$ , ami azt jelenti, hogy  $A_{80}$  tartalmazza az összes  $\text{SL}_2(\mathbb{F}_p)$ -beli mátrixot.

## 4. Expanderek

Ebben a fejezetben expander gráfcsoportokat fogunk vizsgálni. Az expanderek reguláris, erősen összefüggő gráfok, és egy viszonylag új fogalom a matematikában. Viszont sok felhasználási területük van, például hálózatelméletben, számítástechnikában, komplexitáselméletben, kódelméletben, stb. Az erősen összefüggőség szoros kapcsolatban van a gráf átmérőjével, és expanderek segítségével szeretnénk csoportelméleti következtetéseket levonni. A továbbiakban feltesszük a szóbanforgó gráfokról, hogy összefüggőek, nem irányítottak és hurokmentesek. Ebben a fejezetben nagyban hagyatkozunk a [12] és a [13] forrásokra.

### 4.1. Kombinatorikus megközelítés

**4.1.1. Definíció.** Legyen  $G = (V, E)$  egy tetszőleges gráf és  $M, N \subset V$  tetszőleges diszjunkt részhalmazai a gráf csúcsainak. Ekkor az  $M$  különböző határait és az  $M$  és  $N$  között futó éleket a következőképpen értelmezzük

$$\partial_{\text{in}} M = \{m \in M \mid \exists v \in V \setminus M \text{ úgy, hogy } (m, v) \in E\}$$

$$\partial_{\text{out}} M = \{v \in V \setminus M \mid \exists m \in M \text{ úgy, hogy } (m, v) \in E\}$$

$$\partial_{\text{edge}} M = \{(m, v) \in E \mid v \in V \setminus M, m \in M\}$$

$$E(M, N) = \{(m, n) \in E \mid m \in M, n \in N\}$$

**4.1.2. Definíció.** Egy  $G = (V, E)$  véges gráf Cheeger konstansát a következőképpen definiáljuk

$$h(G) = \min \left\{ \frac{|\partial_{\text{edge}}(X)|}{|X|} \mid \emptyset \neq X \subset V \text{ és } |X| \leq \frac{|V|}{2} \right\}.$$

A Cheeger konstans egy mérőszáma annak, hogy a gráf mennyire összefüggő, vagyis minél nagyobb a Cheeger konstans, annál nehezebb leválasztani a  $V$  egy részhalmazát a gráf többi részétől élek elhagyásával. Az is világos, hogy egy nagy Cheeger konstanssal rendelkező gráf gyorsan nő, olyan értelemben, hogy ha a csúcsainak egy részhalmazához ismételve hozzávesszük a határát, akkor "gyorsan" bekebelezzük a gráfot. Érződik, hogy egy gráf ilyenfajta összefüggősege és az átmérője között van kapcsolat, és ezt nemsokára meg is mutatjuk.

Könnyen látható, hogy egy gráf Cheeger konstansa pontosan akkor 0, ha a gráf nem összefüggő.

**4.1.3. Példa.** Vegyük az  $n$  hosszú kört:  $C_n$  ( $n \geq 2$ ). Világos, hogy bárhogyan is veszünk ki egy legfeljebb  $\lfloor \frac{n}{2} \rfloor$  elemű  $X$  részhalmazát  $C_n$ -nek, akkor  $|\partial_{\text{edge}}(X)| \geq 2$ .

Tehát legyen  $X$  minél több egymás mellett lévő csúcs összesége, így  $|\partial_{\text{edge}}(X)| = 2$ . A legnagyobb ilyen  $X$  csúcshalmaz mérete a Cheeger konstans definíciója miatt  $\lfloor \frac{n}{2} \rfloor$  lehet. Ezek alapján

$$h(C_n) = \frac{2}{\lfloor \frac{n}{2} \rfloor}.$$

**4.1.4. Lemma.** Legyen  $G = (V, E)$  egy véges, összefüggő gráf. Ekkor

$$\frac{2}{|V|} \leq h(G) \leq \min_{v \in V} \{\deg(v)\}.$$

**Bizonyítás:** Vegyünk a  $V$  csúcshalmaz egy tetszőleges  $X$  nemüres részhalmazát úgy, hogy  $|X| \leq \frac{|V|}{2}$ . Mivel  $G$  összefüggő, ezért  $|\partial_{\text{edge}}(X)| \geq 1$ . Tehát

$$\frac{|\partial_{\text{edge}}(X)|}{|X|} \geq \frac{1}{|X|} \geq \frac{2}{|V|}.$$

A felsőbecslést illetően pedig legyen  $X = \{v\}$  valamely  $v$  csúcsra. Ekkor  $|\partial_{\text{edge}}(X)| = \deg(v)$ , tehát

$$\frac{|\partial_{\text{edge}}(X)|}{|X|} = \frac{\deg(v)}{|\{v\}|} = \deg(v),$$

vagyis  $h(G) \leq \min_{v \in V} \{\deg(v)\}$ . □

**4.1.5. Definíció.** Egy  $G = (V, E)$  gráf tetszőleges  $v \in V$  csúcsától legfeljebb  $n$  távolságra lévő csúcsok halmazát a következőképpen jelöljük

$$B_n(v) = \{w \in V \mid d(v, w) \leq n\}$$

Mint ahogy az már ezelőtt is említésre került, a Cheeger konstans és a gráfbeli növekedés összefügg. Ezt a következő lemma részletezi.

**4.1.6. Lemma.** Legyen  $G = (V, E)$  egy véges, összefüggő gráf és  $v \in V$  egy tetszőleges csúcs. Ekkor

$$|B_n(v)| \geq \min \left\{ \frac{|V|}{2}, \left( 1 + \frac{h(G)}{M} \right)^n \right\},$$

ahol  $M = \max_{v \in V} \{\deg(v)\}$ .

**Bizonyítás:** Azt szeretnénk megmutatni, hogy ha  $|B_n(v)| \leq \frac{|V|}{2}$ , akkor

$$|B_{n+1}(v)| \geq \left( 1 + \frac{h(G)}{M} \right) |B_n(v)|.$$

Vizsgáljuk azokat a csúcsokat, akik  $B_{n+1}(v)$ -ben benne vannak, viszont  $B_n(v)$ -ben nem, vagyis a  $\partial_{\text{out}}(B_n(v))$  halmazt. Az összes ilyen csúcsba legfeljebb  $M$   $\partial_{\text{edge}}(B_n(v))$ -beli él futhat be. Tehát

$$|\partial_{\text{out}}(B_n(v))| = |B_{n+1}(v) \setminus B_n(v)| \geq \frac{\partial_{\text{edge}}(B_n(v))}{M} \geq \frac{h(G)}{M} |B_n(v)|.$$

Ezek alapján

$$|B_{n+1}(v)| = |B_n(v)| + |B_{n+1}(v) \setminus B_n(v)| \geq \left(1 + \frac{h(G)}{M}\right) |B_n(v)|.$$

□

**4.1.7. Állítás.** Legyen  $G = (V, E)$  egy véges, összefüggő gráf. Ekkor

$$\text{diam}(G) \leq 2 \frac{\log \frac{|V|}{2}}{\log \left(1 + \frac{h(G)}{M}\right)} + 3,$$

ahol  $M = \max_{v \in V} \{\deg(v)\}$ .

**Bizonyítás:** Válasszunk két tetszőleges  $v, w \in V$  csúcsot. Azt szeretnénk megmutatni, hogy

$$d(v, w) \leq 2 \frac{\log \frac{|V|}{2}}{\log \left(1 + \frac{h(G)}{M}\right)} + 3.$$

Legyen  $n$  az a legkisebb természetes szám, amire  $\left(1 + \frac{h(G)}{M}\right)^n \geq \frac{|V|}{2}$ . Ekkor az előző lemma miatt

$$|B_{n+1}(v)| > \frac{|V|}{2} \text{ és } |B_n(w)| \geq \frac{|V|}{2}.$$

Ez azt jelenti, hogy  $B_{n+1}(v) \cap B_n(w) \neq \emptyset$ , tehát  $d(v, w) \leq 2n + 1$ . Mivel  $v$  és  $w$  tetszőleges csúcsok voltak, ezért  $\text{diam}(G) \leq 2n + 1$ . Másrésztől

$$n = \left\lfloor \frac{\log \frac{|V|}{2}}{\log \left(1 + \frac{h(G)}{M}\right)} \right\rfloor \leq \frac{\log \frac{|V|}{2}}{\log \left(1 + \frac{h(G)}{M}\right)} + 1,$$

tehát

$$\text{diam}(G) \leq 2 \frac{\log \frac{|V|}{2}}{\log \left(1 + \frac{h(G)}{M}\right)} + 3.$$

□

**4.1.8. Definíció (Expander).** Egy  $d$ -reguláris, növekvő csúcsszámú, összefüggő  $(G_i)_{i \in \mathbb{N}}$  gráfokból álló sorozatot  $\varepsilon$ -expandernek nevezünk, ha bármely  $i$ -re  $h(G_i) \geq \varepsilon$ , ahol  $\varepsilon > 0$ .

Sokáig nem volt explicit konstrukció expanderekre. Először Grigory Margulis adott egy konstrukciót [18], amiről be tudta látni, hogy egy expander:

Legyen  $G_n = (\mathbb{Z}_n \times \mathbb{Z}_n, E)$ , ahol egy  $(x, y)$  csúcs össze van kötve az  $(x + y, y)$ ,  $(x - y, y)$ ,  $(x, y + x)$ ,  $(x, y - x)$ ,  $(x + y + 1, y)$ ,  $(x - y + 1, y)$ ,  $(x, y + x + 1)$  és az  $(x, y - x + 1)$  csúcsokkal (minden művelet modulo  $n$  értendő). Látható, hogy  $G_n$  egy 8-reguláris gráf bármely  $n$ -re. A bizonyítását annak, hogy ez valóban expander, nem részletezzük.

**4.1.9. Példa.** A  $G_n = C_n$  gráfok nem alkotnak expandert. Az igaz, hogy  $C_n$  bármely  $n$ -re egy 2-reguláris gráf, viszont

$$h(C_n) = \frac{2}{\lfloor \frac{n}{2} \rfloor} \rightarrow 0 \text{ ahogy } n \rightarrow \infty.$$

Általában eldönteni egy  $d$ -reguláris gráfsorozatról, hogy valóban expander-e, nagyon nehéz.

Fel szeretnénk használni a nemrég bizonyított gráfok átmérőjéről szóló állításunkat. Legyen  $(G_i)_{i \in \mathbb{N}}$  egy  $\varepsilon$ -expander, ekkor bármely a sorozatbeli gráfra igaz, hogy

$$M_{G_i} = \max_{v \in V_i} \{\deg(v)\} = d \text{ és } h(G_i) \geq \varepsilon,$$

tehát

$$\text{diam}(G_i) \leq 2 \frac{\log \frac{|V_i|}{2}}{\log(1 + \frac{h(G_i)}{M_{G_i}})} + 3 \leq 2 \frac{\log \frac{|V_i|}{2}}{\log(1 + \frac{\varepsilon}{d})} + 3 \leq C \log |V_i|,$$

ahol  $C$  egy megfelelően nagy univerzális konstans.

Ez azért fontos, mert ha veszünk véges csoportok egy sorozatát valamilyen generátorrendszerekkel (például  $(\text{SL}_2(\mathbb{F}_p))_p$ , ahol  $p$  befutja a prímszámokat) és megmutatjuk, hogy az ő Cayley-gráfjaik expandert alkotnak, akkor tudni fogjuk, hogy ilyen generátorrendszerek mellett az ő átmérőik nagyságrendileg az elemszámaiknak a logaritmusával egyenlő.

## 4.2. Algebrai megközelítés

A meglévő expander definíciónk gráfelméleti alapokon nyugszik, pontosabban azon, hogy az adott gráfok bármely csúcshalmazainak határa "nagy". Most azonban szeretnénk egy lineáris algebrai megközelítést adni az expanderekre, ami gráfok spektrális résén fog alapulni.

**4.2.1. Definíció (Szomszédsági mátrix).** Egy  $G = (V, E)$  véges gráf  $A$  adjacencia, vagy szomszédsági mátrixán azt a  $|V| \times |V|$ -es mátrixot értjük, amire

$$a_{i,j} = \begin{cases} 1 & \text{ha } (i, j) \in E \\ 0 & \text{különben} \end{cases}.$$

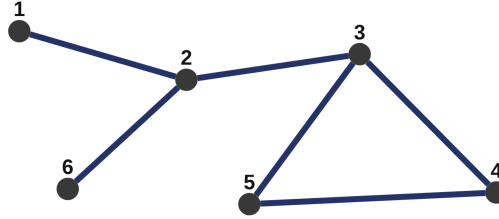
**4.2.2. Definíció (Fokszám mátrix).** Egy  $G = (V, E)$  véges gráf  $D$  fokszám mátrixán azt a  $|V| \times |V|$ -es diagonális mátrixot értjük, aminek a főátlójának  $i$ . eleme  $\deg(v_i)$ .

**4.2.3. Definíció (Laplace mátrix).** Egy  $G = (V, E)$  véges, hurokél mentes gráf  $L$  Laplace mátrixán a  $D - A$  mátrixot értjük, ahol  $A$  a gráf szomszédsági mátrixa,  $D$

pedig a gráf foksám mátrixa. Világos, hogy

$$l_{ij} = \begin{cases} -1 & \text{ha } i \neq j \text{ és } (i, j) \in E \\ \deg(v_i) & \text{ha } i = j \\ 0 & \text{különben} \end{cases}.$$

**4.2.4. Példa.** Tekintsük az alábbi egyszerű gráfot.



Ekkor a gráf szomszédsági, foksám és Laplace mátrixa a következő:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ és}$$

$$L = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 3 & -1 & 0 & 0 & -1 \\ 0 & -1 & 3 & -1 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & -1 & 2 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ahogy az a definíciókból is látszik, a szomszédsági, illetve Laplace mátrixok valós értékűek és szimmetrikusak. A következő, lineáris algebrából jól ismert tételt bizonyítás nélkül elfogadjuk.

**4.2.5. Tétel.** Legyen  $M$  egy valós értékű, szimmetrikus négyzetes mátrix. Ekkor  $M$  összes sajátértéke valós:

$$\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n.$$

Tehát bármely véges gráf szomszédsági és Laplace mátrixának a sajátértékei valósak. Egy  $d$ -reguláris gráf esetén a szomszédsági mátrix minden sorában és oszlopában pontosan  $d$  darab egyes található. Ekkor a Laplace mátrix a következő alakba írható

$$dI - A.$$

Vagyis, ha az  $A$  szomszédsági mátrix sajátértékei a  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  számok, akkor a Laplace mátrix sajátértékei a következők:  $d - \lambda_n \geq d - \lambda_{n-1} \geq \dots \geq d - \lambda_1$ .

Az expanderek vizsgálata szempontjából minket a reguláris gráfok fognak érdekelni. A következő lemma egy  $d$ -reguláris gráf szomszédsági mátrixának a sajátértékeinek közelebbi megértéséről szól.

**4.2.6. Lemma.** Legyen  $G = (V, E)$  egy  $d$ -reguláris véges gráf, a szomszédsági mátrixa  $A$  és ezen mátrix sajátértékei  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Ekkor

- (a)  $\lambda_1 = d$ .
- (b)  $\lambda_2 = \lambda_3 = \dots = \lambda_k = d$  akkor és csakis akkor ha  $G$ -nek legalább  $k$  darab összefüggőségi komponense van.

**Bizonyítás:** (a): Egyrészt,  $A$ -nak minden sorának és oszlopának összege  $d$ , ezért

$$A\mathbf{1} = \begin{pmatrix} \sum_{i=1}^n a_{1i} \\ \sum_{i=1}^n a_{2i} \\ \vdots \\ \sum_{i=1}^n a_{1n} \end{pmatrix} = \begin{pmatrix} d \\ d \\ \vdots \\ d \end{pmatrix} = d\mathbf{1},$$

tehát a  $d$  valóban sajátértéke az  $A$ -nak.

Másrészt, meg kell mutatnunk, hogy nincs nagyobb sajátérték. Legyen  $\lambda$  egy tetszőleges sajátértéke  $A$ -nak és  $v = (v_1 \ \dots \ v_n)^T$  a  $\lambda$  egy olyan sajátvektora, amire igaz, hogy  $|v_j| \leq 1$  bármely  $j$ -re és létezik egy olyan  $v_i$  koordinátája, amire  $|v_i| = 1$ . Ekkor

$$|\lambda| = |\lambda v_i| = \left| \sum_{j=1}^n a_{ij} v_j \right| \stackrel{\Delta}{\leq} \sum_{j=1}^n |a_{ij}| |v_j| \leq \sum_{j=1}^n |a_{ij}| = d.$$

(b): Tegyük fel, hogy  $G$ -nek legalább  $k$  darab összefüggőségi komponense van és legyenek  $C_1, C_2, \dots, C_r$  a gráf összes összefüggőségi komponense ( $r \geq k$ ). Legyen  $\mathbf{1}_{C_i}$  az a vektor, amely a  $C_i$  komponens csúcsainál 1, minden más csúcsnál pedig 0 értékű. Világos, hogy  $\langle \mathbf{1}_{C_i}, \mathbf{1}_{C_j} \rangle = 0$  ha  $i \neq j$ , másszóval páronként merőlegesek és  $A\mathbf{1}_{C_i} = d\mathbf{1}_{C_i}$  bármely  $i$ -re. Tehát  $\lambda_2 = \lambda_3 = \dots = \lambda_r = d$ .

Most tegyük fel, hogy létezik egy olyan  $x \notin \text{span}\{\mathbf{1}_{C_1}, \mathbf{1}_{C_2}, \dots, \mathbf{1}_{C_r}\}$  vektor amire  $Ax = dx$ , ekkor választhatunk egy  $C_i$  komponenst amin  $x$  nem konstans. Ezt  $x$  választása miatt meg tudjuk tenni. Legyen  $v \in C_i$  olyan csúcs, amire  $x_v$  maximális. Mivel  $d$  az  $x$ -hez tartozó sajátérték, ezért

$$\sum_{w \in \partial_{\text{out}}(v)} x_w = dx_v.$$

$x_v$  maximálitása miatt  $x_w = x_v$  bármely  $w \in \partial_{\text{out}}(v)$  esetén. Ezt ismételve kapjuk, hogy bármely  $w \in C_i$  csúcsra  $x_w = x_v$ , vagyis  $x$  konstans  $C_i$ -n, ami ellentmondás.  $\square$

Következtetésként levonhatjuk, hogy egy  $d$ -reguláris gráf akkor és csakis összefüggő, ha  $\lambda_2 < d = \lambda_1$ . Az fog kiderülni, hogy a  $\lambda_2$  eltérése  $d$ -től összefügg azzal, hogy a gráf mennyire erősen összefüggő.

**4.2.7. Definíció.** Egy  $d$ -reguláris gráf spektrális résén a  $d - \lambda_2$  értéket értjük, ahol  $\lambda_2$  a gráf szomszédsági mátrixának a második legnagyobb sajátértéke.

Az expanderek definíciójának átfogalmazásához szükségünk lesz egy összefüggő  $d$ -reguláris gráf Cheeger konstansa és a spektrális rése közötti kapcsolatra. Ebben a Cheeger-egyenlőtlenség lesz a segítségünkre. Mielőtt erre rátérnénk, először bizonyítás nélkül kimondunk egy tételt és egy lemmát, amire szükségünk lesz.

**4.2.8. Tétel (Courant–Fischer-tétel [2]).** Legyen  $M$  egy valós értékű, szimmetrikus négyzetes mátrix és  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  a sajátértékei. Továbbá legyen  $v_i$  egy valós, a  $\lambda_i$  sajátértékhez tartozó sajátvektor. Ekkor

$$\begin{aligned}\lambda_1 &= \max_{x \neq 0} \frac{x^T M x}{x^T x} = \min_{\substack{x \in \text{span}\{v_2, \dots, v_n\}^\perp \\ x \neq 0}} \frac{x^T M x}{x^T x}, \\ \lambda_2 &= \max_{\substack{x \in \text{span}\{v_1\}^\perp \\ x \neq 0}} \frac{x^T M x}{x^T x} = \min_{\substack{x \in \text{span}\{v_3, \dots, v_n\}^\perp \\ x \neq 0}} \frac{x^T M x}{x^T x}, \\ &\dots \\ \lambda_n &= \max_{\substack{x \in \text{span}\{v_1, \dots, v_{n-1}\}^\perp \\ x \neq 0}} \frac{x^T M x}{x^T x} = \min_{x \neq 0} \frac{x^T M x}{x^T x}.\end{aligned}$$

Legyen egy egyszerű,  $d$ -reguláris véges gráf adjecencia mátrixának második legnagyobb sajátértéke  $\lambda_2$ . Világos, hogy ekkor a gráf Laplace mátrixának a második legkisebb sajátértéke  $d - \lambda_2$ . A Courant-Fischer-tétel értelmében:

$$d - \lambda_2 = \min_{\substack{x \perp \mathbf{1} \\ x \neq 0}} \frac{x^T L x}{x^T x}$$

**4.2.9. Lemma ([19]).** Legyen  $G = (V, E)$  egy összefüggő, egyszerű,  $d$ -reguláris véges gráf szomszédsági mátrixának második legnagyobb sajátértéke  $\lambda_2$ . Ekkor

$$d - \lambda_2 = \min_{\substack{x \perp \mathbf{1} \\ x \neq 0}} \frac{x^T L x}{x^T x} = \min_{\substack{x \perp \mathbf{1} \\ x \neq 0}} \frac{\sum_{(u,v) \in E} (x_u - x_v)^2}{2 \sum_{v \in V} x_v^2}.$$

**4.2.10. Tétel (Cheeger-egyenlőtlenség).** Legyen  $G = (V, E)$  egy véges, egyszerű,  $d$ -reguláris gráf, aminek az adjecencia mátrixának a sajátértékei  $d = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Ekkor

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}.$$

**Bizonyítás:** Először lássuk az első egyenlőtlenséget. Létezik egy olyan  $X \subset V$ ,  $|X| \leq \frac{|V|}{2}$  csúcshalmaz, amire a Cheeger konstans realizálódik, vagyis  $h(G) = \frac{|\partial_{\text{edge}}(X)|}{|X|}$  ( $Y := V \setminus X$ ). Legyen az  $y$  vektor a következőképpen definiálva:

$$y_v = \begin{cases} \frac{1}{d|X|} & \text{ha } v \in X \\ -\frac{1}{d|Y|} & \text{ha } v \in Y \end{cases}$$

Vegyük észre, hogy  $y \perp \mathbf{1}$ , hiszen  $\langle y, \mathbf{1} \rangle = \sum_{v \in X} \frac{1}{d|X|} + \sum_{v \in Y} \left(-\frac{1}{d|Y|}\right) = \frac{1}{d} - \frac{1}{d} = 0$ .

$$\begin{aligned} \frac{\sum_{(u,v) \in E} (y_u - y_v)^2}{2 \sum_{v \in V} y_v^2} &= \frac{\sum_{(u,v) \in E(X,Y)} \left(\frac{1}{d|X|} + \frac{1}{d|Y|}\right)^2}{\sum_{v \in X} \frac{1}{d^2|X|^2} + \sum_{v \in Y} \frac{1}{d^2|Y|^2}} = \frac{\left(\frac{1}{d|X|} + \frac{1}{d|Y|}\right)^2 \sum_{(u,v) \in E(X,Y)} 1}{\frac{1}{d^2|X|^2} \sum_{v \in X} 1 + \frac{1}{d^2|Y|^2} \sum_{v \in Y} 1} = \\ &= \frac{\left(\frac{1}{|X|} + \frac{1}{|Y|}\right)^2 E(X,Y)}{\frac{1}{|X|} + \frac{1}{|Y|}} = \left(\frac{1}{|X|} + \frac{1}{|Y|}\right) |\partial_{\text{edge}}(X)| \leq 2 \frac{|\partial_{\text{edge}}(X)|}{|X|} = 2h(G) \end{aligned}$$

Az előző lemma alapján  $d - \lambda_2 \leq 2h(G)$ , vagyis  $\frac{d - \lambda_2}{2} \leq h(G)$ .

Most lássuk az másik egyenlőtlenséget. Legyen  $x$  egy olyan vektor, amire realizálódik a  $d - \lambda_2 = \frac{\sum_{(u,v) \in E} (x_u - x_v)^2}{2 \sum_{v \in V} x_v^2}$  egyenlőség. Feltéhetjük, hogy az  $x$  vektor legfeljebb  $\lfloor \frac{n}{2} \rfloor$  koordinátája pozitív, mert ha ez nem lenne igaz, akkor dolgozhatunk a  $-x$  vektorral. Legyen

$$y_u = \begin{cases} x_u & \text{ha } x_u > 0 \\ 0 & \text{különben} \end{cases} \quad \text{és} \quad z_u = \begin{cases} -x_u & \text{ha } x_u < 0 \\ 0 & \text{különben} \end{cases}.$$

Világos, hogy  $y \geq 0$  és  $z \leq 0$ . Az  $y$  és  $z$  vektorok definíciójából következik, hogy

$$\begin{aligned} ((y_u - y_v) - (z_u - z_v))^2 &\geq (y_u - y_v)^2 + (z_u - z_v)^2 \text{ és} \\ (y_u - z_u)^2 &\leq y_u^2 + z_u^2. \end{aligned}$$

Ezeket felhasználva kapjuk, hogy

$$\frac{\sum_{(u,v) \in E} (x_u - x_v)^2}{2 \sum_{v \in V} x_v^2} = \frac{\sum_{(u,v) \in E} ((y_u - y_v) - (z_u - z_v))^2}{2 \sum_{v \in V} (y_v - z_v)^2} \geq \frac{\sum_{(u,v) \in E} (y_u - y_v)^2 + \sum_{(u,v) \in E} (z_u - z_v)^2}{2 \sum_{v \in V} y_v^2 + 2 \sum_{v \in V} z_v^2}.$$

Mivel pozitív  $a, b, c, d$  számokra teljesül, hogy  $\frac{a+b}{c+d} \geq \min \left\{ \frac{a}{c}, \frac{b}{d} \right\}$ , ezért elég belátnunk, hogy

$$\frac{\sum_{(u,v) \in E} (y_u - y_v)^2}{2 \sum_{v \in V} y_v^2} \geq \frac{h^2(G)}{2d}.$$

Nyilván ugyanezt a  $z$  vektorra is be kellene látnunk, de arra a bizonyítás hasonló. A Cauchy–Bunyakovszkij–Schwarz, illetve a nem negatív számokra fennálló  $(a+b)^2 \leq 2(a^2+b^2)$  egyenlőtlenségeket felhasználva kapjuk, hogy

$$\begin{aligned} \frac{\sum_{(u,v) \in E} (y_u - y_v)^2}{2 \sum_{v \in V} y_v^2} &= \frac{\sum_{(u,v) \in E} |y_u - y_v|^2}{2 \sum_{v \in V} y_v^2} \cdot \frac{\sum_{(u,v) \in E} |y_u + y_v|^2}{\sum_{(u,v) \in E} (y_u + y_v)^2} \stackrel{\text{C.B.S.}}{\geq} \frac{1}{(a+b)^2 \leq 2(a^2+b^2)} \\ &\geq \frac{\left( \sum_{(u,v) \in E} |y_u - y_v| |y_u + y_v| \right)^2}{4 \left( \sum_{v \in V} y_v^2 \right) \left( \sum_{(u,v) \in E} (y_u^2 + y_v^2) \right)} = \frac{\left( \sum_{(u,v) \in E} |y_u^2 - y_v^2| \right)^2}{8d \left( \sum_{v \in V} y_v^2 \right)^2}. \end{aligned}$$

Számozzuk meg a csúcsokat 1-től  $n$ -ig (vagyis  $V = \{1, 2, \dots, n\}$ ) úgy, hogy  $y_1 \geq y_2 \geq \dots \geq y_n$ . Továbbá, legyen  $S_k = \{1, 2, \dots, k\}$ . Mivel feltettük, hogy  $x$ -nek legfeljebb  $\lfloor \frac{n}{2} \rfloor$  koordinátája pozitív, ezért bármely  $i > \lfloor \frac{n}{2} \rfloor$  indexre  $y_i = 0$ . Fel fogjuk használni, hogy  $y_i^2 - y_j^2 = (y_i^2 - y_{i+1}^2) + (y_{i+1}^2 - y_{i+2}^2) + \dots + (y_{j-1}^2 - y_j^2)$ . Foglalkozzunk a számlálóban lévő kifejezéssel:

$$\begin{aligned} \sum_{(u,v) \in E} |y_u^2 - y_v^2| &= 2 \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{j=i+1}^n a_{ij} (y_i^2 - y_j^2) = 2 \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{i \leq k} \sum_{j > k} a_{ij} (y_k^2 - y_{k+1}^2) = \\ &= 2 \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (y_k^2 - y_{k+1}^2) |E(S_k, V \setminus S_k)| \geq 2 \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (y_k^2 - y_{k+1}^2) |S_k| h(G) = \\ &= 2h(G) \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} k (y_k^2 - y_{k+1}^2) = 2h(G) \sum_{v \in V} y_v^2. \end{aligned}$$

Mindezt felhasználva

$$d - \lambda_2 \geq \frac{\left( \sum_{(u,v) \in E} |y_u^2 - y_v^2| \right)^2}{8d \left( \sum_{v \in V} y_v^2 \right)^2} \geq \frac{\left( 2h(G) \sum_{v \in V} y_v^2 \right)^2}{8d \left( \sum_{v \in V} y_v^2 \right)^2} = \frac{h^2(G)}{2d},$$

amiből következik, hogy

$$h(G) \leq \sqrt{2d(d - \lambda_2)}.$$

□

A Cheeger-egyenlőtlenség segítségével átfogalmazhatjuk az expanderek definícióját, hiszen ha  $(G_i)_{i \in \mathbb{N}}$  egy  $\varepsilon$ -expander, vagyis  $h(G_i) \geq \varepsilon$  bármely  $i$ -re, akkor

$$\sqrt{2d(d - \lambda_2(G_i))} \geq h(G_i) \implies d - \lambda_2(G_i) \geq \frac{\varepsilon^2}{2d}.$$

És fordítva, ha  $d - \lambda_2(G_i) \geq \varepsilon$  valamely  $\varepsilon > 0$  konstansra, akkor

$$h(G_i) \geq \frac{d - \lambda_2}{2} \geq \frac{\varepsilon}{2}.$$

**4.2.11. Következmény (Expander átfogalmazás).** Egy  $d$ -reguláris, növekvő csúcsszámú, összefüggő  $(G_i)_{i \in \mathbb{N}}$  gráfokból álló sorozat egy  $C$ -expander valamilyen  $C > 0$  konstansra akkor és csakis akkor, ha

$$\limsup_{i \rightarrow \infty} \lambda_2(G_i) < d.$$

### 4.3. Cayley-gráfok és expanderek kapcsolata

Bizonyítás nélkül kimondunk egy mély, a csoportelméletet és spektrálméletet összekötő tételt [11], amely bizonyítása megtalálható a [6] számú hivatkozásban.

**4.3.1. Tétel (Diaconis-Shahshahani-tétel).** Legyen  $G$  egy véges csoport és  $S \subset G$  egy tetszőleges generátorrendszere úgy, hogy  $1 \notin S$  és  $S$  zárt a konjugálásra nézve. Ekkor a  $\text{Cay}(G, S)$  sajátértékei a

$$\lambda_\chi = \frac{1}{\chi(1)} \sum_{s \in S} \chi(s)$$

számok  $\chi(1)^2$  multiplicitással, ahol  $\chi$  befutja a csoport irreducibilis karaktereit.

A véges Abel-csoportokat jól értjük, és természetes ötlet lenne az Abel-csoportok Cayley-gráfjainak körében expandereket keresni. Azonban a következő tétel kimondja, hogy ez reménytelen.

**4.3.2. Tétel.** Legyen  $(G_i)_{i \in \mathbb{N}}$  egy növekvő elemszámú, kommutatív csoportok egy rendszere tetszőleges, rögzített elemszámú  $S_i$  generátorrendszerek mellett ( $|S_i| = d$  bármely  $i$ -re). Ekkor  $(\text{Cay}(G_i, S_i))_{i \in \mathbb{N}}$  nem egy expander gráfcsalád.

**Bizonyítás:** Az általánosság megsértése nélkül feltehető, hogy  $-S_i = S_i$ , mert azt fogjuk megmutatni, hogy bármelyik  $G_i$  csoport túl lassan nő és ha ezt nagyobb generátorrendszer mellett is meg tudjuk mutatni, akkor készen vagyunk. Kommutatív csoportok lévén, additív jelölést fogunk használni. A már megszokott módon legyen az egységelem  $n$  sugarú környezete

$$B_n(0) = \left\{ \alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_d s_d \mid \alpha_i \geq 0 \text{ és } \sum_{i=1}^d \alpha_i \leq n \right\}.$$

Mivel  $G_i$  kommutatív, ezért az összeadás sorrendjét figyelmen kívül hagyhatjuk ha meg szeretnénk becsülni  $B_n(0)$  nagyságát. Pontosabban azzal becsülhetjük felülről, hogy  $n$ -ig a természetes számokat hányféleképpen lehet felírni  $d$  darab nem negatív természetes szám összegeként. Feltehető, hogy  $n$  nagyobb mint  $d$ .

$$\begin{aligned} |B_n(0)| &\leq \sum_{l=0}^n \binom{l+d-1}{d-1} \leq \sum_{l=0}^{d-1} \binom{l+d-1}{d-1} + \sum_{l=d}^n \frac{(l+d-1)^{d-1}}{(d-1)!} \leq \\ &\leq \sum_{l=0}^{d-1} \binom{l+d-1}{d-1} + \sum_{l=d}^n \frac{2^d}{(d-1)!} l^{d-1} \leq \frac{2^d}{(d-1)!} n^d + C, \end{aligned}$$

ahol  $C = \sum_{l=0}^{d-1} \binom{l+d-1}{d-1}$  univerzális konstans olyan szempontból, hogy csakis  $d$ -től függ, ami rögzített. Vagyis  $|B_n(0)| = O(n^d)$ , viszont megmutattuk, hogy az expanderek exponenciális növekedésűek, lévén a Cheeger konstansuk alulról korlátos. Tehát  $(Cay(G_i, S_i))_{i \in \mathbb{N}}$  valóban nem alkothat expandert.  $\square$

A következő tételt bizonyítás nélkül mondjuk ki.

**4.3.3. Tétel.** Legyen  $(G_i)_{i \in \mathbb{N}}$  egy növekvő elemszámú, véges, feloldható csoportok egy rendszere tetszőleges, rögzített elemszámú  $S_i$  generátorrendszerek mellett ( $|S_i| = d$  bármely  $i$ -re) úgy, hogy bármely csoport kommutátorlánc legfeljebb  $n$  hosszú, ahol  $n$  egy rögzített természetes szám. Ekkor  $(Cay(G_i, S_i))_{i \in \mathbb{N}}$  nem expander.

## 5. Az $\text{SL}_2(\mathbb{F}_p)$ csoport és az expanderek kapcsolata

Ebben a fejezetben az lesz a célunk, hogy megmutassuk azt, hogy megfelelő feltételek mellett a  $(\text{Cay}(\text{SL}_2(\mathbb{F}_p), S_p))_p$  gráfcsalád expandert alkot és a [8] cikk alapján fogjuk ezt megtenni. Bár már megmutattuk, hogy a  $\text{Cay}(\text{SL}_2(\mathbb{F}_p), S)$  gráfnak logaritmikus átmérője van és azt is tudjuk, hogy egy expanderben szereplő gráfok átmérője logaritmikus, ettől még nem biztos, hogy egy logaritmikus átmérővel rendelkező  $d$ -reguláris gráfcsalád expandert alkot. Minket szimmetrikus  $S_p$  generátorhalmazok fognak érdekelni, ami azt jelenti, hogy  $S_p^{-1} = S_p$ , ahol  $|S_p| = 2d$  ( $d$  rögzített természetes szám). Természetesen feltehetjük, hogy  $I \notin S_p$  bármely  $p$ -re.

### 5.1. Definíciók és alapismeretek

Ismertetünk néhány jelölést és a továbbiakban fontos szerepet játszó állítást és tételt. A következő lemma egy klasszikus gráfelméleti összefüggés [12].

**5.1.1. Lemma.** Legyen  $G$  egy véges gráf és  $A$  a szomszédsági mátrixa. Ekkor  $A_{ij}^k$  egyenlő a  $k$  hosszú sétáknak a számával az  $i$  csúcsból a  $j$  csúcsba. A főátlón lévő számok tehát a  $k$  hosszú körök száma  $G$ -ben.

Az előző lemmát átfogalmazzuk csoportok Cayley-gráfjára és azok sajátértékeire.

**5.1.2. Következmény.** Legyen  $G$  egy véges csoport az  $S$  generátorrendszerrel, továbbá legyenek  $|S| = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{|G|}$  a  $\text{Cay}(G, S)$  sajátértékei és  $A$  a szomszédsági mátrixa. Jelölje  $W_{2m}$  a  $2m$  hosszú séták számát az egységelemből önmagába. Ekkor

$$\text{Tr}(A^{2m}) = \sum_{i=1}^{|G|} \lambda_i^{2m} = |G|W_{2m}.$$

Ferdinand Georg Frobenius az  $\text{SL}_2(\mathbb{F}_p)$  csoporttal kapcsolatos eredményei [10] alapján a következő lemmát fogalmazhatjuk meg.

**5.1.3. Lemma.** Az  $\text{SL}_2(\mathbb{F}_p)$  csoport bármely nemtriviális  $\mathbb{C}$  feletti irreducibilis reprezentációjának a dimenziója nagyobb vagy egyenlő, mint  $\frac{p-1}{2}$ .

**5.1.4. Definíció (Multiplikatív energia).** Legyen  $A$  és  $B$  két tetszőleges részhalmaza a  $G$  csoportnak. Az multiplikatív energiájukon a következő halmaz számosságát értjük

$$E(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 \mid a_1 b_1 = a_2 b_2\}|$$

A multiplikatív energiára vonatkozó képlet átírható a következő lemma segítségével.

**5.1.5. Lemma.** Legyen  $A$  és  $B$  két tetszőleges részhalmaza a  $G$  csoportnak. Ekkor

$$E(A, B) = \|\chi_A * \chi_B\|_2^2.$$

**Bizonyítás:** Legyen  $h \in G$  tetszőleges.  $\chi_A * \chi_B(h) = \sum_{g \in G} \chi_A(hg^{-1})\chi_B(g)$  = hányféleképpen lehet felírni  $h$ -t egy  $A$  és egy  $B$ -beli elem szorzataként. Ez alapján

$$\begin{aligned} \|\chi_A * \chi_B\|_2^2 &= \sum_{g \in G} (\chi_A * \chi_B(g))^2 = \sum_{g \in G} (\chi_A * \chi_B(g))(\chi_A * \chi_B(g)) = \\ &= \sum_{g \in G} |\{(a_1, b_1) \mid a_1 \in A, b_1 \in B, a_1 b_1 = g\}| \cdot |\{(a_2, b_2) \mid a_2 \in A, b_2 \in B, a_2 b_2 = g\}| = \\ &= \sum_{g \in G} |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 \mid a_1 b_1 = a_2 b_2 = g\}| = E(A, B). \end{aligned}$$

□

A következő tétel a Balog-Szemerédi-Gowers-tételkörnek egy nemkommutatív verziója, amelyet bizonyítás nélkül mondunk ki.

**5.1.6. Tétel.** Legyen  $A$  és  $B$  két tetszőleges részhalmaza a  $G$  csoportnak úgy, hogy  $E(A, B) \geq \frac{1}{K}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$ , ahol  $K > 1$  rögzített konstans. Ekkor létezik egy  $A' \subset A$  halmaz úgy, hogy  $|A'| = \Omega\left(\frac{1}{K^{O(1)}}|A|\right)$  és  $|A'(A')^{-1}| = O(K^{O(1)}|A|)$  valamely abszolút  $C$  konstansra.

A továbbiakban jelölje  $\mu_S$  az éppen szóban forgó  $G$  csoporton értelmezett,  $S$  tartójú valószínűségi mértéket, ahol  $S$  a csoport egy generátor rendszere:

$$\mu_S(g) = \frac{1}{|S|} \sum_{s \in S} \delta_s(g),$$

ahol  $\delta_s$  az  $s$  elemhez tartozó Dirac delta függvény:

$$\delta_s(g) = \begin{cases} 1 & \text{ha } g = s \\ 0 & \text{ha } g \neq s \end{cases}$$

Feltéve, hogy  $S$  egy szimmetrikus  $2d$  elemszámú generátorrendszer, akkor a konvolúció segítségével a következő formulát írhatjuk fel:

$$\mu_s^{*2m}(1) = \frac{W_{2m}}{(2d)^{2m}}$$

$\text{girth}(G)$  a  $G$  gráf legrövidebb körének méretére használt jelölés. Az lesz a célunk, hogy belássuk a következő tételt.

**5.1.7. Tétel.** Legyen  $d \geq 2$  egy rögzített természetes szám, és legyenek  $2d$  elemszámú, szimmetrikus generátorrendszerei az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoportoknak az  $S_p$  halmazok úgy, hogy

$$\mathrm{girth}\left(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)\right) \geq \tau \log_{2d} p,$$

ahol  $\tau > 0$  egy  $p$ -től független rögzített konstans. Ekkor  $(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p))_p$  egy expander.

Ez a tétel a következménye a következő állításnak.

**5.1.8. Állítás.** Tegyük fel, hogy a  $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$  gráfokra  $(|S_p| = 2d)$  teljesül, hogy

$$\mathrm{girth}\left(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)\right) \geq \tau \log_{2d} p.$$

Ekkor bármely pozitív  $\varepsilon$ -ra létezik egy  $C(\varepsilon, \tau) > 0$  valós szám úgy, hogy ha  $n > C(\varepsilon, \tau) \log_{2d} p$ , akkor

$$\|\mu_{S_p}^{*n}\|_2 < p^{-\frac{3}{2}+\varepsilon}.$$

Lássuk, hogy miért következik a most vázolt állításból a fenti fő tétel. Mivel  $S_p$  egy szimmetrikus generátor halmaz, ezért

$$\mu_{S_p}^{*2n}(1) = \sum_{g \in G} \mu_{S_p}^{*n}(g) \mu_{S_p}^{*n}(g^{-1}) = \sum_{g \in G} \left(\mu_{S_p}^{*n}(g)\right)^2 = \|\mu_{S_p}^{*n}\|_2^2.$$

Ez alapján bármely  $n > C(\varepsilon, \tau) \log_{2d} p$  természetes számra  $W_{2n} < \frac{(2d)^{2n}}{p^{3-2\varepsilon}}$ . Legyen  $\lambda_{2,p}$  a  $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$  szomszédsági mátrixának második legnagyobb sajátértéke és ennek multiplicitása  $m_p(\lambda_{2,p})$ . Tudjuk, hogy

$$|\mathrm{SL}_2(\mathbb{F}_p)| W_{2n} = \sum_{i=1}^{|\mathrm{SL}_2(\mathbb{F}_p)|} \lambda_{i,p}^{2n} > m_p(\lambda_{2,p}) \lambda_{2,p}^{2n}.$$

A 5.1.3. lemma alapján állíthatjuk, hogy  $m_p(\lambda_{2,p}) \geq \frac{p-1}{2} \geq \frac{p}{3}$ , de a konstans szorzó elhanyagolható. Ahogy azt már korábban is ismertettük,  $|\mathrm{SL}_2(\mathbb{F}_p)| = p^3 - p < p^3$ . Mindezek alapján

$$p^3 \frac{(2d)^{2n}}{p^{3-2\varepsilon}} > p \lambda_{2,p}^{2n} \implies \frac{(2d)^{2n}}{p^{1-2\varepsilon}} > \lambda_{2,p}^{2n} \implies \frac{2d}{p^{\frac{1-2\varepsilon}{2n}}} > \lambda_{2,p}.$$

Legyen  $n = C(\varepsilon, \tau) \log_{2d} p$ , ekkor

$$\lambda_{2,p} < \frac{2d}{p^{\frac{1-2\varepsilon}{2n}}} = (2d)^{1-\frac{1-2\varepsilon}{C(\varepsilon, \tau)}} < 2d,$$

és ezzel beláttuk a kívánt tételt, hiszen  $\limsup_{p \rightarrow \infty} \lambda_{2,p} < 2d$ . Természetesen még hátravan ennek az állításnak a bizonyítása.

## 5.2. Valószínűségi mértékek az $\mathrm{SL}_2(\mathbb{F}_p)$ csoporton

**5.2.1. Definíció (K-approximációs részcsoporth).** Legyen  $G$  egy tetszőleges csoport és  $1 \in H$  egy olyan szimmetrikus részhalmaza ( $H^{-1} = H$ ), amelyre létezik egy olyan  $X \subset G$  úgy, hogy  $|X| \leq K$ , ahol  $K \geq 1$  konstans,  $H \cdot H \subseteq X \cdot H$  és  $H \cdot H \subseteq H \cdot X$ . Ekkor  $H$ -t  $K$ -approximációs részcsoporthnak nevezzük.

Ezt a fogalmat Terence Tao vezette be először [5] és arra hivatott, hogy megállapítsa, hogy egy csoport részhalmaza mennyire van közel ahhoz, hogy részcsoporth legyen. Itt a  $K$  konstans egy mérőszámként is felfogható. Szintén Tao nevéhez fűződik a következő tétel, amire nemsokára szükségünk lesz.

**5.2.2. Tétel.** Legyen  $A$  és  $B$  két multiplikatív részhalmaza a  $G$  csoportnak és  $K \geq 1$  rögzített konstans. Ekkor a következő két állítás ekvivalens valamilyen konstans erejéig, úgy érteve, hogy ha az  $i$ . állítás igaz valamely  $C_i$  abszolút konstansra, akkor a  $j$ . állítás is fennáll valamely  $C_j$  abszolút konstansra.

$$(1) \quad d(A, B) = \log \frac{|AB^{-1}|}{\sqrt{|A||B|}} \leq C_1 \log K.$$

$$(2) \quad \text{Létezik egy } C_2 K^{C_2}\text{-approximációs } H \text{ részcsoporth úgy, hogy } H \leq C_2 K^{C_2} |A|, \\ A \subset X \cdot H \text{ és } B \subset Y \cdot H \text{ valamely } X, Y \text{ multiplikatív részhalmazokra amikre} \\ |X|, |Y| \leq C_2 K^{C_2}.$$

Ebben az alfejezetben az lesz a célunk, hogy bebizonyítsuk a következő állítást.

**5.2.3. Állítás.** Legyen  $\nu$  egy szimmetrikus valószínűségi mérték az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoporton, vagyis  $\nu(g) = \nu(g^{-1})$ . Ha valamely rögzített  $0 < \gamma < \frac{3}{4}$  konstansra fennáll, hogy

$$(a) \quad \|\nu\|_\infty < \frac{1}{p^\gamma},$$

$$(b) \quad \|\nu\|_2 > p^{-\frac{3}{2} + \gamma},$$

$$(c) \quad \nu^{*2}(H) < \frac{1}{p^\gamma} \text{ bármely } H \text{ valódi részcsoporthra,}$$

Ekkor létezik egy  $\gamma$ -tól függő  $\varepsilon > 0$  konstans úgy, hogy ha  $p$  elég nagy, akkor

$$\|\nu * \nu\|_2 < \frac{1}{p^\varepsilon} \|\nu\|_2.$$

**Bizonyítás:** Tegyük fel, hogy nem igaz az állítás, vagyis bárhogyan választunk egy  $\varepsilon > 0$  konstanst

$$\|\nu * \nu\|_2 > \frac{1}{p^\varepsilon} \|\nu\|_2.$$

Azt fogjuk megmutatni, hogy ha  $\varepsilon$ -t eléggé kicsire választjuk, akkor a (b) feltétel sérülni fog. Legyen  $J = 10 \log p$ . Az egészrész függvénnyel analóg függvényt fogunk legyártani a  $\nu$  mértékből.

$$\tilde{\nu} = \sum_{j=1}^J \frac{1}{2^j} \chi_{A_j},$$

ahol  $A_j = \left\{ g \mid \frac{1}{2^j} < \nu(g) \leq \frac{1}{2^{j+1}} \right\}$  és  $A_{J+1} = \left\{ g \mid 0 < \nu(g) \leq \frac{1}{2^J} \right\}$ . Megjegyzendő, hogy bármely  $1 \leq j \leq J$  indexre  $|A_j| \leq 2^j$ , hiszen ha lenne  $2^j + 1$  olyan elem, akinek a mértéke nagyobb mint  $\frac{1}{2^j}$ , akkor  $\sum_{k=1}^{2^j+1} \nu(g_k) > \sum_{k=1}^{2^j+1} \frac{1}{2^k} = 1 + \frac{1}{2^j} > 1$ . Ekkor bármely  $g \in \text{SL}_2(\mathbb{F}_p)$  elemre igaz, hogy

$$\tilde{\nu}(g) \leq \nu(g) \leq 2\tilde{\nu}(g) + \frac{1}{2^J} \chi_{A_{J+1}}(g).$$

E miatt és az kezdeti feltevésünk miatt  $\tilde{\nu}$ -ra is igaz, hogy  $\|\tilde{\nu} * \tilde{\nu}\|_2 > \frac{1}{p^\varepsilon} \|\tilde{\nu}\|_2$ . Most szeretnénk egy felső, illetve alsó becslést adni  $\|\tilde{\nu} * \tilde{\nu}\|_2$ -ra és  $\|\tilde{\nu}\|_2$ -ra. Először nézzük a felső becslést, ahol a háromszög-egyenlőtlenséget fogjuk használni.

$$\|\tilde{\nu} * \tilde{\nu}\|_2 = \left\| \sum_{1 \leq i, j \leq J} \frac{1}{2^{i+j}} \chi_{A_i} * \chi_{A_j} \right\|_2 \triangleq \sum_{1 \leq i, j \leq J} \frac{1}{2^{i+j}} \|\chi_{A_i} * \chi_{A_j}\|_2.$$

A skatulya-elv alapján létezik olyan  $i$  és  $j$  indexek, amikre

$$\|\tilde{\nu} * \tilde{\nu}\|_2 \leq \frac{J^2}{2^{i+j}} \|\chi_{A_i} * \chi_{A_j}\|_2.$$

Most lássuk az alsó becslést

$$\|\tilde{\nu}\|_2 = \sqrt{\sum_{l=1}^J \frac{|A_l|}{2^{2l}}} \geq \sqrt{\frac{|A_i|}{2^{2i}} + \frac{|A_j|}{2^{2j}}} \stackrel{\text{AM-GM}}{\geq} \frac{1}{2^{\frac{i}{2}} 2^{\frac{j}{2}}} |A_i|^{\frac{1}{4}} |A_j|^{\frac{1}{4}}.$$

Felhasználva mindkét becslést, azt kapjuk, hogy

$$\frac{J^2}{2^{i+j}} \|\chi_{A_i} * \chi_{A_j}\|_2 \geq \|\tilde{\nu} * \tilde{\nu}\|_2 > \frac{1}{p^\varepsilon} \|\tilde{\nu}\|_2 \geq \frac{1}{p^\varepsilon 2^{\frac{i}{2}} 2^{\frac{j}{2}}} |A_i|^{\frac{1}{4}} |A_j|^{\frac{1}{4}} \implies$$

$$\implies E(A_i, A_j) = \|\chi_{A_i} * \chi_{A_j}\|_2 > \frac{2^{\frac{i}{2}} 2^{\frac{j}{2}}}{J^2 p^\varepsilon |A_i|^{\frac{1}{4}} |A_j|^{\frac{1}{4}}} \geq \frac{|A_i|^{\frac{1}{2}} |A_j|^{\frac{1}{2}}}{J^2 p^\varepsilon |A_i|^{\frac{1}{4}} |A_j|^{\frac{1}{4}}} \geq \frac{1}{p^{2\varepsilon}} |A_i|^{\frac{3}{4}} |A_j|^{\frac{3}{4}}.$$

Az  $A = A_i$  és  $B = A_j$  jelölésekkel alkalmazva az 5.1.6. tételt, kapunk egy  $A_1 \subset A$  halmazt, amire  $|A_1| > \frac{1}{p^{\varepsilon_1}} |A|$ , ahol  $\varepsilon_1 = 4C_1\varepsilon$  és  $C_1$  egy abszolút konstans úgy, hogy

$$|A_1 A_1^{-1}| < p^{\varepsilon_1} |A_1|.$$

Vegyük észre, hogy ekkor

$$d(A_1, A_1) \leq \varepsilon_1 \log p,$$

hiszen

$$d(A_1, A_1) = \log \frac{|A_1 A_1^{-1}|}{\sqrt{|A_1| |A_1|}} < \log \frac{p^{\varepsilon_1} |A_1|}{|A_1|} = \varepsilon_1 \log p.$$

Emiatt alkalmazhatjuk az 5.2.2. tételt, vagyis létezik egy  $H$   $p^{\varepsilon_2}$ -approximációs részcsoporthoz, amire

$$|H| < p^{\varepsilon_2} |A_1|, A_1 \subset XH, A_1 \subset HY \text{ és } |X|, |Y| < p^{\varepsilon_2},$$

ahol  $\varepsilon_2 = C_2 \varepsilon_1$  és  $C_2$  egy abszolút konstans. Mivel  $A_1 \subset \bigcup_{x \in X} xH$  és  $|X| < p^{\varepsilon_2}$ , ezért a skatulya-elv alapján létezik egy  $x_0 \in X$  úgy, hogy

$$|A_1 \cap x_0 H| > \frac{1}{p^{\varepsilon_2}} |A_1|.$$

Másrészről  $A_1 \subset A = A_i$  és  $\min \left\{ \frac{|A_i|}{2^i}, \frac{|A_j|}{2^j} \right\} \geq \frac{1}{j^{2p^\varepsilon}}$ , ezért

$$\nu(x_0 H) > \nu(A_1 \cap x_0 H) > \frac{1}{2^i} |A_1 \cap x_0 H| > \frac{1}{2^i p^{\varepsilon_2}} |A_1| > \frac{1}{2^i p^{\varepsilon_2} p^{\varepsilon_1}} |A_i| > \frac{1}{p^{\varepsilon_1 + \varepsilon_2 + 2\varepsilon}} = \frac{1}{p^{\varepsilon_3}}.$$

Felhasználva az (a) feltevésünket, adódik, hogy  $|H| > p^{\gamma - \varepsilon_3}$ . Mivel  $A_1 \subset A_i$ ,  $|H| < p^{\varepsilon_2} |A_1|$ , ezért  $|H| < 2^i p^{\varepsilon_2}$ .

A Young-egyenlőtlenség  $\|f * g\|_2 \leq \|f\|_2 \|g\|_1$  alakját használva

$$\|\chi_{A_i} * \chi_{A_j}\| \leq |A_i|^{\frac{1}{2}} |A_j| \leq 2^{\frac{i}{2}} 2^j.$$

Ezt felhasználva és a kezdeti (b)  $\|\nu\|_2 > p^{-\frac{3}{2} + \gamma}$  feltevést, kapjuk, hogy

$$p^{-\frac{3}{2} + \gamma} \leq \frac{1}{p^{2\varepsilon}} \|\nu\|_2 \leq \frac{1}{2^{i+j}} \|\chi_{A_i} * \chi_{A_j}\|_2 \leq \frac{1}{2^{\frac{i}{2}}} \implies 2^i \leq p^{3-2\gamma}.$$

Visszatérve  $H$  méretének becsléséhez adódik, hogy  $|H| \leq p^{3-2\gamma+\varepsilon_2}$ . Mivel  $H$  egy  $p^{\varepsilon_2}$ -approximációs részcsoporthoz, ezért

$$\begin{aligned} |H^3| &= |H \cdot H^2| \leq |H^2 \cdot X| < |H \cdot X^2| < p^{2\varepsilon_2} |H| \implies \\ &\implies |H \cdot H \cdot H| < |H|^{1 + \frac{2\varepsilon_2}{\gamma - \varepsilon_3}}. \end{aligned}$$

A 3.1.1. állítás (a) pontját használva állíthatjuk, hogy  $H$  nem generátorhalmaza az  $\text{SL}_2(\mathbb{F}_p)$  csoportnak, vagyis őt tartalmazza valamely  $G_0$  valódi részcsoporthoz. Az előzőek fényében és  $\varepsilon$ -t elég kicsinek megválasztva (úgy, hogy legyen  $\varepsilon_3 < \frac{\gamma}{2}$ ) adódik, hogy  $\nu(x_0 G_0) > \frac{1}{p^{\frac{\gamma}{2}}} \implies \nu^{*2}(G_0) > \frac{1}{p^\gamma}$ , ami ellentmondás.  $\square$

### 5.3. A fő tétel bizonyítása

**5.3.1. Tétel (Dickson).** Legyen  $p \geq 5$  prím. Ekkor az  $\text{SL}_2(\mathbb{F}_p)$  csoport bármely részcsoporthoz izomorf a következő csoportok valamelyikével:

(a)  $2\left(\frac{p\pm 1}{2}\right)$  rendű diédercsoport és azok részcsoporthai.

(b)  $\frac{p(p-1)}{2}$  rendű Borel részcsoporthai és részcsoporthai.

(c)  $A_4, S_4$  vagy  $A_5$ .

**5.3.2. Állítás.** Legyen  $H$  az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoport egy 60-nál nagyobb elemszámú valódi részcsoporthja. Ekkor a  $H$ -nak a második kommutátora triviális, vagyis bármely  $g_1, g_2, g_3, g_4 \in H$  elemekre

$$\left[[g_1, g_2], [g_3, g_4]\right] = 1.$$

**Bizonyítás:**  $H > 60$ , tehát  $H \not\cong A_4, S_4, A_5$  az előző tétel alapján. Ha  $H$  izomorf egy diéder csoporttal, akkor ismert, hogy  $H' = \langle r^2 \rangle$ . Ekkor  $[y^{2^n}, y^{2^m}] = 1$ . Ha  $H$  egy Borel részcsoporthal izomorf, akkor feltehetjük, hogy izomorf a felső háromszög-mátrix csoporttal. Vizsgáljuk az első kommutátor részcsoporthot:

$$\begin{pmatrix} a & x \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} b & y \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} a^{-1} & -x \\ 0 & a \end{pmatrix} \begin{pmatrix} b^{-1} & -y \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},$$

ahol  $\alpha \in \mathbb{F}_p$ . Világos, hogy az ilyen alakú mátrixok kommutálnak egymással.  $\square$

**5.3.3. Tétel.** Legyen  $d \geq 2$  egy rögzített természetes szám, és legyenek  $d$  elemszámú részhalmazai az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoportoknak az  $S_p$  halmazok úgy, hogy

$$\mathrm{girth}\left(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)\right) \geq \tau \log_{2d} p,$$

ahol  $\tau > 0$  egy  $p$ -től független rögzített konstans. Ekkor, ha  $p > (2d)^{\frac{17}{\tau}}$ , akkor  $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$  összefüggő.

**Bizonyítás:** Legyen  $G_p$  az  $S_p$  által generált részcsoporthja az  $\mathrm{SL}_2(\mathbb{F}_p)$  csoportnak. Azt szeretnénk megmutatni, hogy elég nagy  $p$ -re  $G_p = \mathrm{SL}_2(\mathbb{F}_p)$ . Az világos, hogy  $G_p \not\cong A_4, S_4, A_5$ , hiszen az azt jelentené, hogy  $S_p$  tartalmaz egy kis rendű elemet, ami megsértene a feltételt miszerint a legkisebb kör a gráfban nagyobb mint  $\tau \log_{2d} p$ .

Az előző állítás alapján bármely  $s_1, s_2, s_3, s_4 \in S_p$  generátorelemekre

$$\left[[s_1, s_2], [s_3, s_4]\right] = 1,$$

ami implikál egy 16 hosszú kört  $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ -ben, ezzel megsértve a legkisebb körre vonatkozó feltételt ha  $\tau \log_{2d} p \geq 17 \iff p \geq (2d)^{\frac{17}{\tau}}$   $\square$

Kimondunk egy segédlemmát.

**5.3.4. Lemma.** Jelölje  $W_k(L)$  az  $L$  hosszú szavak halmazát az  $F_k$  szabadcsoportban. Legyen  $\Sigma(k, l)$  egy részhalmaza a  $W_k(2l)$  halmaznak úgy, hogy  $|\Sigma(k, l)| > l^6$  és legyen  $T = \{[g_1, g_2] \mid g_1, g_2 \in \Sigma(k, l)\}$ . Ekkor  $|T| > l^3$ .

**Bizonyítás:** Tegyük fel, hogy  $|T| \leq l^3$ . Ekkor létezik egy  $a \in T$  úgy, hogy

$$|\{(g_1, g_2) \in \Sigma(k, l) \times \Sigma(k, l) \mid [g_1, g_2] = a\}| > \frac{|\Sigma|^2}{l^3}.$$

Hasonló okok miatt létezik egy  $b \in \Sigma(k, l)$ ,  $b \neq 1$  úgy, hogy

$$|\{g \in \Sigma(k, l) \mid [b, g] = a\}| > \frac{|\Sigma(k, l)|}{l^3} > l^3.$$

Legyen  $\Sigma_1 = \{g \in \Sigma(k, l) \mid [b, g] = a\}$ . Legyen  $g, h \in \Sigma_1$ , ekkor

$$\begin{cases} gb^{-1}g^{-1} = b^{-1}a \\ hb^{-1}h^{-1} = b^{-1}a \end{cases} \implies gb^{-1}g^{-1}hbh^{-1} = 1 \iff b(h^{-1}g) = (h^{-1}g)b.$$

Vagyis  $b$  és  $h^{-1}g$  kommutálnak. Mivel egy szabadcsoportban dolgozunk, ezért létezik egy  $x \in F_k$  úgy, hogy  $x^n = h^{-1}g$  és  $b = x^m$ . Tehát  $b^n = (h^{-1}g)^m$ , ami egyértelműen meghatározza  $h^{-1}g$ -t a  $b$  függvényében. Mivel  $x^n, x^m \in W_k(2l)$ , ezért  $n, m < 2l$ , vagyis legfeljebb  $4l^2$  lehetséges értéke lehet az  $(n, m)$  kettősnek. Ezek alapján

$$|\Sigma_1|^2 < 4l^2|\Sigma_1| \implies |\Sigma_1| < 4l^2,$$

ami ellentmondás, hiszen megmutattuk, hogy  $|\Sigma_1| > l^3$ . □

**5.3.5. Következmény.** Az előző jelöléseket használva, legyen  $\Sigma(k, l)$  egy részhalmaza a  $W_k(2l)$  halmaznak úgy, hogy  $\forall g_1, g_2, g_3, g_4 \in \Sigma(k, l)$  elemekre  $\left[[s_1, s_2], [s_3, s_4]\right] = 1$ . Ekkor  $|\Sigma(k, l)| < l^6$ .

**Bizonyítás:** Az előző lemma jelöléseit használva, állíthatjuk, hogy bármely  $x_1, x_2 \in T$  elemekre  $[x_1, x_2] = 1$ . Viszont tudjuk, hogy egy szabadcsoportban két elem akkor és csakis akkor kommutálnak, ha valamely csoportbeli elem hatványai. Ez alapján,  $T$ -t tartalmazza a szabadcsoport egy ciklikus részcsoporthja. Másrésztől  $T \subseteq W_k(8l)$ , tehát  $|T| = O(l)$ . Az előző lemma tagadását használva kapjuk, hogy  $|\Sigma(k, l)| < l^6$ . □

A következő tétel biztosítja számunkra a legkisebb körre vonatkozó alsó becslést.

**5.3.6. Tétel.** Rögzített  $d$  mellett, az  $\text{SL}_2(\mathbb{F}_p)$  csoport egy random Cayley-gráfjának legrövidebb köre legalább  $(\frac{1}{3} - o(1)) \log_{d-1} |\text{SL}_2(\mathbb{F}_p)|$  ahogy  $p \rightarrow \infty$ .

Legyen  $F_n$  a  $n$  elem által generált szabadcsoport, és a generátorai legyenek  $a_1, a_2, \dots, a_n$ . Jelölje  $\mu$  az  $F_n$ -en értelmezett,  $\{a_1, a_2, \dots, a_n\}$  tartójú valószínűségi mértéket

$$\mu = \frac{1}{2n} \sum_{i=1}^n (\delta_{a_i} + \delta_{a_i^{-1}}).$$

Továbbá legyen  $\mathcal{P}^{(l)}(x, y)$  annak a valószínűsége, hogy az  $x$  csúsból indulva  $l$  lépés után  $y$ -ba jutunk, ha a bolyongást a  $\mu$  szerint végezzük.

**5.3.7. Állítás (Kesten).** Legyen  $F_n$  a  $n$  elem által generált szabadcsoport, és a generátorai legyenek  $a_1, a_2, \dots, a_n$ . Jelölje  $\mu$  az  $F_n$ -en értelmezett,  $\{a_1, a_2, \dots, a_n\}$  tartójú valószínűségi mértéket

$$\mu = \frac{1}{2n} \sum_{i=1}^n (\delta_{a_i} + \delta_{a_i^{-1}}).$$

Továbbá legyen  $\mathcal{P}^{(l)}(x, y)$  annak a valószínűsége, hogy az  $x$  csúcsból indulva  $l$  lépés után  $y$ -ba jutunk, ha a bolyongást a  $\mu$  szerint végezzük. Ekkor

$$\limsup_{l \rightarrow \infty} \sqrt[l]{\mathcal{P}^{(l)}(x, x)} = \frac{\sqrt{2n-1}}{n}.$$

A fenti tétel következményeként állítható, hogy ha  $l$  páros, akkor  $\mathcal{P}^{(l)}(x, y) \leq \mathcal{P}^{(l)}(x, x) \leq \left(\frac{\sqrt{2n-1}}{n}\right)^l$ .

Még hátravan az 5.1.8. állítás bizonyítása. Az állítást úgy fogjuk belátni, hogy az 5.2.3. állítást alkalmazzuk az  $\mu_{S_p}^{*l}$  mértékekre, ahol  $l \sim \log p$ . Befogjuk bizonyítani, hogy erre a mértékekre fennállnak az (a) és (c) tulajdonságok. Világos, hogy azt szeretnénk megmutatni, hogy a (b) tulajdonság nem teljesül.

Szeretném megjegyezni, hogy a cikk feldolgozása során egy jelentős hibára bukkantam ebben a bizonyításban, mégpedig arra, hogy a cikk szerzői felhasználták azt, hogy

$$\|\mu_{S_p}^{*l}\|_{\infty} |\text{supp}(\mu_{S_p}^{*l})| \leq 1,$$

ami nyilvánvalóan nem igaz, hiszen az egyenlőtlenségnek fordítva kellene állnia. A bizonyításban továbbá egy másik rossz irányú becslés is használatra került, mégpedig

$$\left\lfloor \frac{\tau}{2} \log_{2d} p \right\rfloor - 1 \geq \frac{\tau}{2} \log_{2d} p,$$

ami szintén világos, hogy nem igaz. Ezért adtam egy másik bizonyítását az állításnak.

Legyen  $l_0 = \left\lfloor \frac{\tau}{2} \log_{2d} p \right\rfloor - 1$ . A feltevésünkéből, miszerint  $\text{girth}\left(\text{Cay}(\text{SL}_2(\mathbb{F}_p), S_p)\right) \geq \tau \log_{2d} p$ , következik, hogy egy legfeljebb  $l_0$  hosszú véletlen séta a gráfon olyan, mintha a séta egy  $2d$ -reguláris fán történne, vagy úgy is mondhatnánk, hogy az  $F_{2d}$  Cayley-gráfján. Ezt tudván, felhasználva az előző tételt, kapjuk, hogy

$$\begin{aligned} \|\mu_{S_p}^{*l_0}\|_{\infty} &= \max_{\substack{g \in \text{SL}_2(\mathbb{F}_p) \\ d(1, g) \leq l_0}} \mu_{S_p}^{*l_0}(g) \leq \max_{\substack{g \in \text{SL}_2(\mathbb{F}_p) \\ d(1, g) \leq l_0}} \mathcal{P}^{(l_0)}(1, g) \leq \left(\frac{\sqrt{4d-1}}{2d}\right)^{l_0} = \\ &= \left(\frac{\sqrt{4d-1}}{2d}\right)^{\left\lfloor \frac{\tau}{2} \log_{2d} p \right\rfloor - 1} < \left(\frac{\sqrt{4d-1}}{2d}\right)^{\frac{\tau}{2} \log_{2d} p} = p^{-\frac{\tau}{2} \log_{2d} \frac{2d}{\sqrt{4d-1}}}. \end{aligned}$$

Ha feltesszük, hogy  $\tau < 3$ , akkor

$$\frac{\tau}{2} \log_{2d} \frac{2d}{\sqrt{4d-1}} = \frac{\tau}{2} \left(1 - \frac{1}{2} \log_{2d}(4d-1)\right) < \frac{\tau}{2} \left(1 - \frac{1}{2} \log_{2d}(2d)\right) = \frac{\tau}{4} < \frac{3}{4},$$

vagyis a  $\gamma = \frac{\tau}{2} \log_{2d} \frac{2d}{\sqrt{4d-1}}$  választással teljesül az 5.2.3. állítás (a) feltétele a  $\mu_{S_p}^{*l_0}$  mértékre. A Young-egyenlőtlenség  $\|f * g\|_\infty \leq \|f\|_\infty \|g\|_1$  alakját használva

$$\|\mu_{S_p}^{*(l_0+1)}\|_\infty = \|\mu_{S_p}^{*l_0} * \mu_{S_p}\|_\infty \leq \|\mu_{S_p}^{*l_0}\|_\infty \|\mu_{S_p}\|_1 = \|\mu_{S_p}^{*l_0}\|_\infty \cdot 1 \leq p^{-\frac{\tau}{2} \log_{2d} \frac{2d}{\sqrt{4d-1}}},$$

vagyis azt kaptuk, hogy bármely  $l \geq l_0$  számra teljesül az imént említett feltétel.

Most megmutatjuk, hogy ha  $l \geq l_0$ , akkor a  $\mu_{S_p}^{*2l}$  mértékre teljesül a 5.2.3. (c) feltétele, ha  $\gamma < \frac{3\tau}{16}$ . Tegyük fel, hogy létezik egy  $a \in \text{SL}_2(\mathbb{F}_p)$  úgy, hogy  $\mu_{S_p}^{*l}(aG_0) > \frac{1}{p^{\frac{\gamma}{2}}}$  valamely  $G_0$  valódi részcsoportha (amiből következik, hogy  $\mu_{S_p}^{*2l}(G_0) > \frac{1}{p^\gamma}$ ). Ekkor

$$\begin{aligned} \frac{1}{p^{\frac{\gamma}{2}}} &< \mu_{S_p}^{*l}(aG_0) = \sum_{y \in \text{SL}_2(\mathbb{F}_p)} \mu_{S_p}^{*(l-l_0)}(y) \mu_{S_p}^{*l_0}(yaG_0) \leq \\ &\leq \sum_{y \in \text{SL}_2(\mathbb{F}_p)} \mu_{S_p}^{*(l-l_0)}(y) \max_{b \in \text{SL}_2(\mathbb{F}_p)} \mu_{S_p}^{*l_0}(bG_0) = \max_{b \in \text{SL}_2(\mathbb{F}_p)} \mu_{S_p}^{*l_0}(bG_0). \end{aligned}$$

Jelölje  $W_S(L)$  az  $L$  hosszú szavakat az  $S$  generátorrendszerre nézve. Továbbá, legyen

$$\Sigma(S, l_0) = \{g \in G_0 \cap W_S(2l_0)\}.$$

Felhasználva az 5.3.2. állítást, az 5.3.7. állítást és az 5.3.5. következményt, állíthatjuk, hogy

$$l_0^6 > |\Sigma(S, l_0)| \geq \frac{\mu_{S_p}^{*2l_0}(G_0)}{\|\mu_{S_p}^{*2l_0}\|_\infty} > \frac{1}{p^\gamma \|\mu_{S_p}^{*2l_0}\|_\infty} > \frac{1}{p^\gamma} \left( \sqrt{\frac{d^2}{2d-1}} \right)^{2l_0} \stackrel{\gamma < \frac{3\tau}{16}}{>} \left( \frac{d^2}{2d-1} \right)^{\frac{l_0}{4}},$$

ami ellentmondás, hiszen az egyenlőtlenség-lánc két végét vizsgálva azt kapjuk, hogy

$$\begin{aligned} \left( \frac{\tau}{2} \log_{2d} p \right)^6 &> l_0^6 > \left( \frac{d^2}{2d-1} \right)^{\frac{l_0}{4}} > \left( \frac{d^2}{2d} \right)^{\frac{\frac{\tau}{2} \log_{2d}(p) - 2}{4}} = \frac{d^{\frac{\tau}{4} \log_{2d}(p) - 1}}{(2d)^{\frac{\tau}{8} \log_{2d}(p) - \frac{1}{2}}} = \\ &= \frac{\sqrt{2d}}{d} \cdot \frac{p^{\frac{\tau}{4} \log_{2d}(d)}}{p^{\frac{\tau}{8} \log_{2d}(2d)}} > \frac{\sqrt{2d}}{d} \cdot \frac{p^{\frac{\tau}{4} \cdot \frac{3}{5}}}{p^{\frac{\tau}{8}}} = \frac{\sqrt{2d}}{d} p^{\frac{7\tau}{40}}, \end{aligned}$$

ami nem igaz elég nagy  $p$ -re.

Tegyük fel, hogy az 5.2.3. állítás (b) feltétele is fennáll a  $\mu_{S_p}^{*l}$  mértékre, ahol  $l \geq l_0$ , vagyis  $\|\mu_{S_p}^{*l}\|_2 > p^{-\frac{3}{2} + \gamma}$ . Ekkor használhatjuk az 5.2.3. állítást az összes  $\mu_{S_p}^{*l}$ ,  $l \geq l_0$  mértékre. Tehát

$$\|\mu_{S_p}^{*l}\|_2 > p^\varepsilon \|\mu_{S_p}^{*2l}\|,$$

valamely  $\varepsilon$ -ra, ami csakis  $\gamma$ -tól függ. Viszont ekkor

$$\|\mu_{S_p}^{*l}\|_2 > p^\varepsilon \|\mu_{S_p}^{*2l}\|_2 > p^{2\varepsilon} \|\mu_{S_p}^{*4l}\|_2 > \cdots > p^{n\varepsilon} \|\mu_{S_p}^{*2nl}\|_2 \stackrel{(b)}{>} p^{n\varepsilon} p^{-\frac{3}{2} + \gamma} = p^{-\frac{3}{2} + n\varepsilon + \gamma}.$$

$n$ -t elég nagyra választva azt kapjuk, hogy  $\|\mu_{S_p}^{*l}\|_2 > 1$ , ami ellentmondás. És ezzel beláttuk az 5.1.8. állítást.

## Hivatkozások

- [1] Åberg, Philip. "Fourier analysis on finite groups." (2024).
- [2] Avron, H., 2008. A generalized Courant-Fischer minimax theorem.
- [3] Babai, L. and Seress, Á., 1992. On the diameter of permutation groups. European journal of combinatorics, 13(4), pp.231-243.
- [4] Bourgain, J. and Gamburd, A., 2008. Uniform expansion bounds for Cayley graphs of. Annals of Mathematics, pp.625-642.
- [5] Breuillard, E., Green, B. and Tao, T., 2012. The structure of approximate groups. Publications mathématiques de l'IHÉS, 116, pp.115-221.
- [6] Diaconis, P. and Shahshahani, M., 1981. Generating a random permutation with random transpositions. Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete, 57(2), pp.159-179.
- [7] Eberhard, S., 2024. Diameter of classical groups generated by transvections. Journal of Algebra, 653, pp.220-256.
- [8] Garonzi, M., Halasi, Z. and Somlai, G., 2024. On the diameter of Cayley graphs of classical groups with generating sets containing a transvection. Israel Journal of Mathematics, 261(2), pp.899-950.
- [9] Helfgott, H.A., 2008. Growth and generation in. Annals of Mathematics, pp.601-623.
- [10] Humphreys, J.E., 1975. Representations of  $SL(2, p)$ . The American Mathematical Monthly, 82(1), pp.21-39.
- [11] Liu, X. and Zhou, S., 2018. Eigenvalues of Cayley graphs. arXiv preprint arXiv:1809.09829.
- [12] Lountzi, A., 2015. Expander graphs and explicit constructions.
- [13] L. Lovász: Eigenvalues of graphs, 2007
- [14] Pálfi Péter Pál, Csoportok és reprezentációik, 2020
- [15] Pinsker, M.S., 1973, June. On the complexity of a concentrator. In 7th International Teletraffic Conference (Vol. 4, pp. 1-318).
- [16] Pyber, L. and Szabó, E., 2010. Growth in finite simple groups of Lie type of bounded rank. arXiv preprint arXiv:1005.1858.

- [17] Ruzsa, I.Z., 1996. Sums of finite sets, Number theory (New York, 1991–1995), 281–293.
- [18] Shlomo Hoory, Nathan Linial, and Avi Wigderson: Expander graphs and their application, Bulletin of the American Mathematical Society, 43, 2006
- [19] Thomas Sauerwald and He Sun, Spectral Graph Theory and Applications, 2011

## Mesterséges intelligencia alapú eszközök használatáról szóló nyilatkozat

Alulírott Györgypál Tamás nyilatkozom, hogy szakdolgozatom elkészítése során az alább felsorolt feladatok elvégzésére a megadott MI alapú eszközöket alkalmaztam:

| Feladat                    | Felhasznált eszköz               | Felhasználás helye | Megjegyzés |
|----------------------------|----------------------------------|--------------------|------------|
| Nyelvhelyesség ellenőrzése | Writefull                        | Teljes dolgozat    | —          |
| Dolgozat formázása         | Gemini 2.5 Flash<br>GPT-4.5 (o4) | Teljes dolgozat    | —          |

A felsoroltakon túl más mesterséges intelligencia alapú eszközt nem használtam.