EÖTVÖS LORÁND TUDOMÁNYEGYETEM

TERMÉSZETTUDOMÁNYI KAR

Gráfok, izomorfizmus-probléma, algebrai eszközök

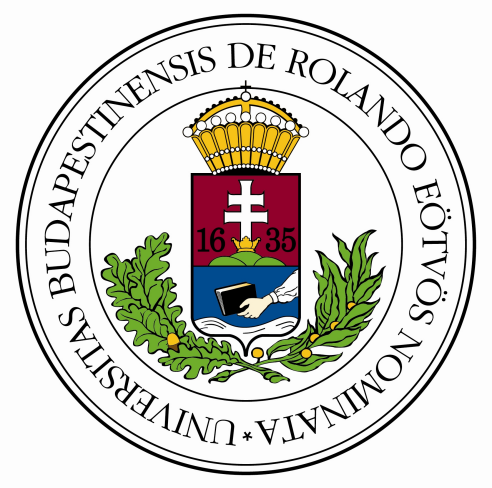
Bsc Szakdolgozat

Prágai Bálint János

Matematika BSc

Matematikai elemző szakirány

Témavezető: Somlai Gábor



Budapest

2023

Köszönetnyílvánítás

Szeretném megköszönni a témavezetőmnek, Somlai Gábornak a lehetőséget, hogy nála írhattam a szakdolgozatomat ebből a számomra nagyon izgalmas és érdekes témából, illetve a rendszeres konzultációkat, melyek során sokkal mélyebben megérthettem ezt az igen mély és bonyolult témakört. Szeretném megköszönni továbbá családomnak és barátaimnak a rengeteg támogatást amit tanulmányaim alatt nyújtottak, nékülük nem jutottam volna idáig.

Tartalomjegyzék

1. Bevezetés, probléma leírása

Arthur Cayley a gráfok egy új osztályát vezette be egy 1878-as cikkében. A definíció a csoport generátorainak egy meghatározott részhalmazát használja, és így szimmetrikus és jól struktúrált gráfokat kapunk, amik többek között az expander gráfok keresésére is alkalmas eszközzé teszi őket. Ezek a gráfok azóta Cayley gráfokként váltak ismertté és azóta is széles körben kutatják őket.
Egy 1970-es cikkében D. Ž. Djoković eredményt ért el a ciklikus gráfok izomorfizmusával kapcsolatban és ez az eredmény könnyen kapcsolható a Cayley gráfokhoz. Nem olyan rég pedig Stefaan De Winter, Ellen Kamischke, és Zeying Wang egy 2016-ban megjelent tanulmányban a parciális differenciahalmazok és erősen reguláris gráfok kapcsolatát vizsgálva bukkantak egy kapcsolatra a Cayley gráfokkal. Ezeket összekapcsolja, hogy mindkét cikk az adjacencia mátrix sajátértékeinek felhasználásval oldják meg a problémát. Ebben a dolgozatban részben ezt a két eredményt dolgozom fel, valamint egy megoldási utat fedezek fel az egyik, De Winterék cikkében meg nem válaszolt problémára.
Ehhez viszont szükség lesz a témakör lineáris algebrai alapjaira, amit a második fejezetben taglalok, továbbá szükségünk van némi csoportelméleti alapra, illetve néhány bonyolultabb fogalomra, hogy jobban átlátható legyen a témakör, ezt a 3. fejezetben fejtem ki. A 4. fejezetben az erősen reguláris gráfok tulajdonságait vizsgálom, így minden elő lesz készítve, hogy rendesen beszélhessek a Cayley gráfok és az erősen reguláris gráfok kapcsolatáról az 5. fejezetben. Az 5. fejezet továbbá tartalmaz értekezéseket parciális differencia halmazok és Cayley gráfok kapcsolatáról, valamint a cospektrális Cayley gráfok izomorfizmusának vizsgálatáról és esetleges eldöntésésről. Ezek után a dolgozat befejező 6. fejezetében a fentebb már említett problémát fogom próbálni megoldani, ami nem más, mint $(216, 40, 4, 8)$ paraméterű, erősen reguláris Cayley gráfot keressek (izomorfia erejéig).

2. Lineáris algebrai alapok

2.1. Gráfok és mátrixok kapcsolata

2.1. Definíció. [8] Egy n-csúcsú, irányított Γ gráf $A(\Gamma)$ adjacencia mátrixának nevezünk egy $\mathbb{Z}^{n\times n}$ mátrixot, ha $A(\Gamma)_{uv}$ a gráf u csúcsából v csúcsába futó éleinek száma. (Ez általában 0 vagy 1.)

Ha a Γ irányítatlan, akkor minden élt két ellentétes irányú irányított élnek veszünk, ekkor $A(\Gamma)$ egy szimmetrikus $(0, 1)$-mátrix. Ha a gráfban nincsenek hurokélek, akkor az $A(\Gamma)$ diagonálisa csupa 0. Megjegyzendő, hogy azonos csúcsokon

értelmezett, különböző irányított gráfok adjacencia mátrixa eltérő, még akkor is, ha ezek a gráfok izomorfak. Az alábbi lemma megmutatja, hogy ez nem lesz probléma.

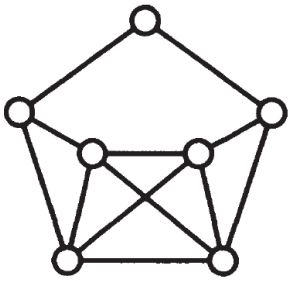
2.2. Lemma. *[8] Legyen X és Y két különböző irányított gráf ugyanazon a csúcshalmazon. X és Y izomorf akkor és csak akkor, ha létezik egy P permutáció mátrix, hogy $P^T A(X)P = A(Y)$.*

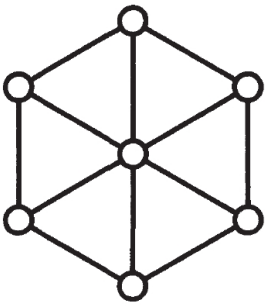
Bizonyítás. X és Y ha izomorfak, akkor létezik X csúcsainak egy permutációja, amelyik Y csúcsaiba viszi őket.
Ha ezt tekintjük a gráfok $A(X)$ és $A(Y)$ adjacencia mátrixain, akkor $A(X)$ oszlopai a csúcsok felsorolása valamilyen sorrendben, a sorai a csúcsok ugyanebben a sorrendben. A csúcsok permutálása igazából azt jelenti, hogy a megfelelő csúcshoz tartozó oszlopot átcseréljük a megfelelő helyre. Viszont ez pontosan akkor történik meg, ha $A(X)$-et megszorozzuk jobbról egy P permutáció mátrixszal. A sorok hasonlóan, itt a szorzás viszont a P mátrix transzponáltjával történik.
Így megkapjuk, hogy $P^T A(X)P = A(Y)$. □

2.3. Definíció. [8] Egy mátrix karakterisztikus polinomja $\phi(A, x) = det(xI - A)$. Ha Γ egy gráf, akkor az $A(\Gamma)$ adjacencia mátrix karakterisztikus polinomját jelöljük $\phi(\Gamma, x)$-szel.

2.4. Definíció. [8] Egy mátrix spektruma a mátrix sajátértékeinek listája, az ő multiplicitásaikkal. Hasonlóan fogalmazhatjuk meg Γ gráf spektrumát, ami legyen $A(\Gamma)$ spektruma.

Fontos megfigyelni, hogy a gráf spektruma nem határozza meg a gráf izomorfizmus osztályát:





2.5. Példa. Ez a két gráf láthatóan nem izomorf, viszont mindkét gráf karakterisztikus polinomja

$$(x+2)(x+1)^2(x-1)^2(x^2-2x-6),$$

így a sajátértékeik:

$$\{-2, -1^{(2)}, 1^{(2)}, 1 \pm \sqrt{7}\}.$$

(Itt a kitevők a sajátértékek multiplicitását hivatottak jelölni.)

2.6. Definíció. [8] Két gráfot, akik spektruma megegyezik, kospektrális gráfoknak nevezzük.

Viszont némi információ így is kinyerhető a gráf spektrumából:

2.7. Lemma. *[8] Legyen Γ egy irányított gráf, $A(\Gamma)$ adjacencia mátrixxal. Az u és v csúcsok közötti r-hosszú séták száma $(A(\Gamma)^r)_{uv}$.*

Bizonyítás. Jelöljük $A(\Gamma)$-t A-val.
Tekintsük $r = 1$-et. Ekkor $A^r = A$ és ekkor az 1 hosszú séta u és v közötti élt jelenti, ami azt jelenti, hogy $A_{uv} = 1$, ami valóban 1, mert uv is szomszédosak. Tegyük fel, hogy $r = n$-re teljesül, ekkor tekintsük $A^{n+1} = A^n A$-t. Az indukciós feltétel miatt A^n_{uv} az u és v csúcsok közötti $r = n$ hosszú séták számát adja.
Ekkor az u és v közötti $n+1$ hosszú séták száma megegyezik az két csúcs közötti n hosszú séták száma u-ból w csúcsokba, amik szomszédosak v-vel. De ez a (u, v) eleme az $A^n A = A^{n+1}$ mátrixnak, ahol A v-hez tartozó oszlopának nem nulla elemei pontosan v szomszédai. Tehát az állítás következik az indukcióból. □

2.8. Definíció. [8] Egy A mátrix nyoma a mátrix diagonális elemeinek összege. Jele: $\mathrm{tr}(A)$.

A lemma eredménye megmutatja, hogy a Γ-beli r-hosszú séták száma $\mathrm{tr}(A(\Gamma)^r)$, így megkapjuk a következőt:
- $\mathrm{tr}(A(\Gamma)) = 0$
- $\mathrm{tr}(A(\Gamma)^2) = 2e$
- $\mathrm{tr}(A(\Gamma)^3) = 6t$,

ahol e a Γ gráf éleinek száma, t pedig a háromszögek száma.

Bár ezek is fontos eredmények, egy gráf adjacencia mátrixából még egy kicsit több információ szerezhető: A mátrix négyzetes, így a mátrixa nyoma megegyezik a mátrix sajátértékeinek összegével is, valamint $A(\Gamma)^r$ sajátértékei a mátrix sajátértékeinek

az r-edik hatványai, tehát $\mathrm{tr}(A(\Gamma)^r)$-t meghatározza az adjacencia mátrix spektruma.

2.9. Definíció. [16] Egy gráf két pontjának távolsága a köztük lévő legrövidebb út hossza.

2.10. Definíció. [16] Egy gráf átmérője a két legtávolabbi csúcsának távolsága.

2.11. Lemma. *[16] Ha Γ gráf átmérője d, akkor $A(\Gamma)$ mátrixnak legalább $d+1$ különböző sajátértéke van.*

Bizonyítás. Az $(A+I)^r$ mátrix ij elem csakis akkor nemnulla, ha i és j csúcsok egy legfeljebb r hosszú úttal vannak összekötve. Következésképpen az $(A+I)^r$, $r = 0, \dots d$ mátrixok egy lineárisan független halmazt alkotnak az A-n értelmes polinomok terében. Ez azt jelenti, hogy $A, A^2, \dots$ hatványok d fokig lineárisan függetlenek lesznek.
Az A mátrix valós szimmetrikus, így diagonalizálható, viszont a minimálpolinom nem változik a diagonalizálással. A minimálpolinom ($\prod(x-\lambda_i)$, λ_i a sajátértékek) lesz a legkisebb fokú olyan polinom, amibe A-t helyettesítve 0-át kapunk, tehát itt már összefüggőnek kell lennie az A hatványoknak. A minimál polinomban szereplő λ sajátértékek végig különbözőek, a minimál polinom foka így a különböző sajátértékek száma. A^d fokig függetlenek az A mátrix hatványai, így minimálpolinom fokának magasabbnak kell lennie, ami $d+1$, ami azt jelenti, hogy $d+1$ különböző sajátértéke van az A mátrixunknak.

□

2.2. Szimmetrikus mátrixok

Mint az előző alfejezetben kiderült, a gráf adjacencia mátrixa egy szimmetrikus mátrix. Ezen mátrixoknak sok nagyon hasznos tulajdonságuk van, amit a későbbiekben kihasználunk majd. Kezdjük az egyik talán legfontosabb eredménnyel:

2.12. Lemma. *[8] Legyen A egy valós szimmetrikus mátrix. Ha u és v a mátrix különböző sajátértékeihez tartozó sajátvektorai, akkor u és v ortogonálisak egymásra.*

Bizonyítás. Tegyük fel, hogy $Au = \lambda u$ és $Av = \tau v$. Mivel A szimmetrikus, $u^T A v = (v^T A u)^T$. A bal oldal megfelel $\tau u^T v$-nek, míg a jobb oldal $\lambda u^T v$-nek. Mivel feltételünk az, hogy $\lambda \neq \tau$, így az egyenlőség csak akkor teljesülhet, ha $u^T v = 0$. □

2.13. Lemma. *[8] Egy valós szimmetrikus A mátrix sajátértékei is valósak.*

Bizonyítás. Legyen u az A mátrix λ saját értékéhez tartozó saját vektora. Tekintsük az $Au = \lambda u$ egyenletet. Ha vesszük az egyenlet komplex konjugáltját, akkor $A\overline{u} = \overline{\lambda}\overline{u}$ egyenlethez jutunk. Ebből következik, hogy $\overline{u}$ is az A mátrix sajátvektora. $\overline{u} \neq 0$ definíció szerint, így $u^T\overline{u} > 0$. Az előző lemmából látszik, hogy nem lehet a két sajátvektornak különböző sajátértéke, mert ha azok különbözőek lennének, akkor a vektorok ortogonálisak lennének egymásra. így $\lambda = \overline{\lambda}$ és ezzel bizonyítottuk az állítást. □

Szükségünk lesz még a szimmetrikus mátrixok diagonalizálhatóságára is, de ehhez először be kell vezetnünk az invariancia fogalmát.

2.14. Definíció. [7] Az U alteret A-invariánsnak nevezzük, ha $Au \in U$ minden $u \in U$ esetén.

2.15. Lemma. *[8] Legyen $A \in \mathbb{R}^{n\times n}$ egy szimmetrikus mátrix. Ha U egy $\mathbb{R}^n$-beli A-invariáns altér, akkor $U^\perp$ is A-invariáns.*

Bizonyítás. Bármely két u, v vektorra nekünk teljesül a

$$v^T(Au) = (Av)^T u$$

egyenlőség. Ha $u \in U$, akkor $Au \in U$, így ha $v \in U^\perp$, akkor $v^T(Au) = 0$. Ebből következik, hogy $(Av)^T u = 0$, amikor $u \in U$ és $v \in U^\perp$. Ebből pedig $Av \in U^\perp$ következik, ha $v \in U^\perp$, emiatt pedig $U^\perp$ A-invariáns. □

Láttuk, hogy minden négyzetes mátrixnak van legalább egy sajátértéke, mert a $\det(xI - A) = 0$ egyenletnek van legalább egy valós megoldása, mert az A mátrix szimmetrikus. (A $\det(xI - A) = 0$ egyenletnek mindig van komplex gyöke, de esetünkben ez a megoldás valós és ez az igazi eredmény.) Egy valós szimmetrikus mátrixnak így kell lennie legalább egy valós sajátértékének, amit jelöljön θ, és emiatt kell lennie legalább egy valós sajátvektorának is. Ezt fogja erősíteni az alábbi lemma is:

2.16. Lemma. *[8] Legyen $A \in \mathbb{R}^{n\times n}$ szimmetrikus mátrix. Ha U egy nemnulla A-invariáns altér $\mathbb{R}^n$-ben, akkor U tartalmazza A egy sajátvektorát.*

Bizonyítás. Legyen R egy egy olyan mátrix, aminek az oszlopai ortonormált bázist alkotnak U-ban, tehát U-t pontosan az Rx alakú vektorok alkotják. Ekkor U A-invarianciája miatt $AR = RB$ valamilyen B négyzetes mátrixra.
Mivel $R^T R = I$

$$R^T AR = R^T RB = B,$$

ami implikálja, hogy B valós szimmetrikus. Mivel minden szimmetrikus mátrixnak van legalább egy sajátértéke, így választhatunk egy u valós vektort, hogy B λ sajátértékéhez tartozó sajátvektora legyen. Ekkor $ARu = RBu = \lambda Ru$, és mivel $u \neq 0$ és R oszlopai lineárisan függetlenek, $Ru \neq 0$. Tehát Ru egy U-beli sajátvektora A-nak. □

2.17. Tétel. *[8] Legyen $A \in \mathbb{R}^{n\times n}$ mátrix. Ekkor $\mathbb{R}^n$-ben van egy A sajátvektoraiból álló ortonormált bázis.*

Bizonyítás. Indukciót használunk. Vegyünk egy A ortonormált sajátvektoraiból álló $\{u_1, \ldots, u_m\}$ halmaz, valamilyen $m < n$-re és legyen M az általuk kifeszített altér. Mivel A-nak van legalább egy sajátértéke, $m \geq 1$.
Ekkor az M-altér A-invariáns, így $M^\perp$ is A-invariáns, így $M^\perp$ tartalmaz egy u_{m+1} (normalizált) sajátvektort. Ekkor $\{u_1, \ldots, u_m, u_{m+1}\}$ A sajátvektorainak egy $m+1$ méretű, ortonormált halmaza. Innen indukcióval látszik, hogy ez a halmaz kiterjeszthető úgy, hogy $\mathbb{R}^n$-beli bázist kapjunk, ami tisztán A sajátvektoraiból áll. □

3. Csoportelméleti alapok

A dolgozat által feldolgozott téma nem igényli semelyik csoportelméleti téma komoly bevezetését, viszont nagyon is érdemes alapvető fogalmak bevezetése, hogy a későbbi eredményeket megfelelő kontextusba helyezhessük. Felelevenítjük a csoport fogalmát, utána csoportok néhány fajtáját vizsgáljuk meg.

3.1. Definíció. [7] A G nem üres halmaz csoport, ha értelmezett rajta egy kétváltozós $*$ művelet úgy, hogy

1. a $*$ művelet *asszociatív*, azaz minden $g, h, k \in G$ esetén $(g * h) * k = g * (h * k)$;
2. létezik $e \in G$ kétoldali *neutrális elem*, melyre $e * g = g * e$ teljesül minden $g \in G$-re;
3. minden $g \in G$-nek van kétoldali g^{-1} *inverze*, melyre $g * g^{-1} = g^{-1} * g = e$;

3.2. Definíció. [7] Kommutatív csoport vagy *Abel-csoport*: a $*$ kommutatív, azaz minden $g, h \in G$ esetén $g * h = h * g$.

3.3. Definíció. [7] A G csoport *ciklikus*, ha egy eleme hatványaiból áll.
Az ilyen elem neve G egy *generátora*.

3.4. Definíció. [7] Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre. A $\phi : G \to H$ leképzés homomorfizmus, ha művelettartó: $\phi(a * b) = \phi(a) \bullet \phi(b)$ minden $a, b \in G$-re. Ha ϕ kölcsönösen egyértelmű is a G és H csoportok között, akkor ϕ izomorfizmus. A G és H izomorf csoportok, ha van közöttük izomorfizmus, jele: $G \cong H$.

3.5. Tétel. *[7] G ciklikus $\iff G \cong \mathbb{Z}^+$ vagy $G \cong \mathbb{Z}_n^+$, ahol n egy pozitív egész.*

3.6. Definíció. [8] Egy Γ gráf önmagával vett izomorfizmusát automorfizmusnak hívjuk. Az automorfizmus tehát a gráf csúcsainak olyan permutációja, ami a csúcsokat csúcsokba, az éleket pedig élekbe viszi.

3.7. Definíció. [8] Vegyük egy Γ gráf minden automorfizmusát. Ez nem egy üres halmaz, mivel az identitás egy gráf automorfizmus, ezt jelölje e. Ha g a Γ gráf egy automorfizmusa, akkor g^{-1} is egy automorfizmus, és ha veszünk egy második h automorfizmust, akkor gh kompozíció is Γ egy automorfizmusa lesz. Tehát Γ automorfizmusai csoportot alkotnak, ezt Γ automorfizmus csoportjának nevezzük, jele: $\mathrm{Aut}(\Gamma)$.

3.8. Definíció. [8] A $\mathrm{Sym}(V)$ *szimmetrikus csoport* egy olyan csoport, ami egy V halmaz elemeinek minden permutációját tartalmazza, így $\mathrm{Aut}(\Gamma)$ egy részhalmaza, sőt részcsoportja $\mathrm{Sym}(V(\Gamma))$-nek. A permutációk egymás utáni végzése a permutációk szorzata.

3.9. Példa. A K_n (n csúcsú teljes gráf) csúcsain minden permutáció automorfizmus, tehát $\mathrm{Aut}(K_n) \cong \mathrm{Sym}(n)$.

A Cayley gráfokat ebben a szekcióban vezetjük be, mivel a definíció szorosan kapcsolódik a csoportelmélethez.

3.10. Definíció. [6] [*Cayley-gráf*] Legyen G egy véges csoport, és legyen S a $\{G \backslash e\}$ elemeinek egy részhalmaza, amire igaz, hogy zárt inverzképzésre, azaz $s \in S \Rightarrow s^{-1} \in S$. A $\Gamma(G, E)$ gráfban $u, v \in G$ csúcsok szomszédosak, ha $\exists s \in S$, hogy

$$u \circ s = v$$

ahol $\circ$ a csoportművelet.

3.11. Megjegyzés. Abel csoportok felett ezt gyakran $u + s = v$-ként írnánk fel. Azért volt fontos kikötni, hogy S inverzre zárt legyen, mert így a gráf irányítatlan lesz:

$$u + s = v \iff v + (-s) = u.$$

3.12. Definíció. [8] Egy gráfot csúcstranzitívnak nevezünk, ha automorfizmus csoportja tranzitívan hat a csúcsain. Tehát bármely $u; v$ csúcspárra létezik automorfizmus, ami egyiket a másikba viszi.

3.13. Tétel. *[8] A $\Gamma(G, C)$ Cayley gráf csúcstranzitív.*

Bizonyítás. Minden $g \in G$-re a

$$\rho_g : x \mapsto xg$$

leképzés G eleminek egy permutációja. Ez $\Gamma(G, C)$ automorfizmusa, mivel

$$(yg)(xg)^{-1} = ygg^{-1}x^{-1} = yx^{-1},$$

így $xg \sim yg \iff x \sim y$, ahol $x \sim y$ azt jelenti, hogy van a két csúcs között él. A ρ_g permutációk egy G-vel izomorf részcsoportját alkotják a $\Gamma(G, C)$ automorfizmus csoportjának. Ez a részcsoport tranzitívan hat $\Gamma(G, C)$ csúcsain, mert bármely $g, h \in V(\Gamma)$ párra a $\rho_{g^{-1}h}$ permutáció g-t a h-ba viszi. Ezzel beláttuk, hogy $\Gamma(G, C)$ csúcstranzitív. □

3.14. Definíció. $\Gamma(G, C)$ csúcstranzitív $\iff$ $\Gamma(G, C)$ szimmetrikus gráf.

4. Erősen reguláris gráfok

A dolgozat az additív Abel-csoportokon értelmezett, erősen reguláris Cayley gráfokat vizsgálja, ehhez viszont a csoportelmélet mellett le kell fektetni elég erős gráfelméleti alapokat, mivel az erősen reguláris gráfok témaköre eléggé összetett. Megjegyzendő, hogy egyátalán nem triviális eldönteni, hogy két gráf izomorf-e, vagy hogy egy gráfnak létezik-e nem-identitás automorfizmusa. Viszont vannak esetek, amikor ezek egészen egyértelműen látszanak:

4.1. Definíció. [8] Legyen Γ egy nem üres és nem teljes gráf. Γ-t *erősen reguláris gráf*nak hívjuk $\mathrm{erg}(n, k, \lambda, \mu)$ paraméterekkel, ha k-reguláris, minden **szomszédos** csúcsnak λ közös szomszédja van és minden **nem szomszédos** csúcsnak pontosan μ közös szomszédja van.

4.2. Példa. Egy egyszerű példa az 5-hosszú kör (C_5). A gráf 2-reguláris, úgy hogy a szomszédos csúcsoknak nincs közös szomszédja, valamint a nem szomszédos csúcsoknak pontosan 1 szomszédja van. Így megkapjuk, hogy a C_5 erősen reguláris gráf $(5, 2, 0, 1)$ paraméterekkel.

Könnyen belátható, hogy ha Γ erősen reguláris gráf (n, k, λ, μ) paraméterekkel, akkor a komplementere is erősen reguláris $(n, \overline{k}, \overline{\lambda}, \overline{\mu})$ paraméterekkel, ahol

$$\begin{aligned} \overline{k} &= n - k - 1, \\ \overline{\lambda} &= n - 2 - 2k + \mu, \\ \overline{\mu} &= n - 2k + \lambda. \end{aligned}$$

Egy erősen reguláris gráf primitív, ha mind önmaga, mind a komplementere összefüggő, különben imprimitívnek hívjuk.

4.3. Lemma. *[8] Legyen Γ egy erősen reguláris gráf (n, k, λ, μ) paraméterekkel. Ekkor az alábbiak ekvivalensek:*

1. *Γ nem összefüggő*
2. *$\mu = 0$,*
3. *$\lambda = k - 1$,*
4. *Γ izomorf mK_{k+1}, valamilyen $m > 1$-re. (Itt mK_{k+1} m darab diszjunkt $k+1$ méretű teljes gráf uniója)*

Bizonyítás. A bizonyításunk egy körbe bizonyítás lesz. Tegyük fel, hogy Γ nem összefüggő és legyen Γ_1 a Γ egy komponense. Egy Γ_1-beli csúcsnak nincs közös szomszédja $\Gamma \backslash \Gamma_1$-beli csúcsokkal, így $\mu = 0$. Ha veszünk egy u csúcsot, és az ő szomszédait (legyen V a szomszédok halmaza), akkor V-ben bármely két csúcs össze van kötve. Ez a $\mu = 0$-ból következik, mert két V-beli különböző pont közös szomszédainak száma nem 0. Most tekintsük az u-tól 2 távolságra lévő pontokat. (Ezek olyan pontok akik nincsenek összekötve u-val.) Viszont ezekhez a pontokhoz vezet u-ból 2-hosszú út, ami ellentmondás. Pontosabban kifejtve ez a $\mu = 0$ feltétel azt mondja, hogy ha két pont között van 2-hosszú út, akkor van 1-hosszú is, azaz szomszédosak. Ha $\mu = 0$, akkor $\forall u \in V(\Gamma)$ csúcsnak szomszédosnak kell lennie, ebből következik, hogy $\lambda = k - 1$.

Végül, ha $\lambda = k - 1$, akkor a csúcsunkat tartalmazó komponensnek muszály a K_{k+1} teljes gráfnak lennie, így Γ ilyen teljes gráfok diszjunkt uniója. □

Az erősen reguláris gráfok paraméterei nem függetlenek, már csak egyszerű számolásokból is következik, hogy ha egy csúcsnak k szomszédos csúcsa van, akkor $n-k-1$ nem szomszédos csúcsának kell lennie. Egy kicsit tovább gondolva: Ha egy u csúcsnak k szomszédja van, akkor ők szomszédosak u-val, valamint szomszédosak

u további λ szomszédjával. Ezek a csúcsok így $k-\lambda-1$ csúccsal szomszédosak, amik u-val nem, így $k(k-\lambda-1)$ élt számolhatunk meg az u-val szomszédos csúcsok között. Ha tekintjük az $n-k-1$ nem-szomszédot, amikkel u-nak van μ közös szomszédja, ami összesen $\mu(n-k-1)$ élt alkot. A fentiekből a

$$k(k-\lambda-1)=\mu(n-k-1)$$

egészségi feltétel következik. (Nyílván itt minden számnak egésznek kell lennie, mert egy gráfban se a csúcsok száma, se a regularitás nem lehet nem-egész, és nyílvánvalóan a szomszédok és nem szomszédok száma se.) Sokszor úgy keresnek erősen reguláris gráfokat, hogy ehhez hasonló egészségi feltételek mellett megalkotnak lehetséges paraméterlistákat és ilyen paraméterekkel rendelkező gráfokat próbálnak találni. A dolgozatban később mi is hasonló módszert fogunk alkalmazni egy erősen reguláris Cayley gráf keresésére.
Legyen A mátrix egy erősen reguláris $\Gamma(n,k,\lambda,\mu)$ gráf adjacencia mátrixa. Az alábbi sorokban megvizsgáljuk, hogy hogyan számolhatóak a gráf paramétereiből sajátértékek és azokból megállapítunk további egészségi feltételeket.

[8] Az A^2 mátrix ij eleme megmutatja az i és j csúcsok közötti 2-hosszú séták számát. Egy erősen reguláris gráfban ez a szám csak attól függ, hogy a két csúcs megegyezik-e vagy különbözőek és szomszédosak vagy nem szomszédosak. Ebből felírhatjuk, hogy

$$A^2=kI+\lambda A+\mu(J-I-A)\iff A^2-(\lambda-\mu)A-(k-\mu)I=\mu J$$

alakba is átírható.
Ebből az egyenletből felírhatóak A sajátértékei. Mivel Γ k-reguláris volt, így k biztosan A sajátértéke lesz, az $\mathbf{1}$ sajátvektorral. A 2.12 lemma alapján A minden más sajátvektora merőleges kell, hogy legyen $\mathbf{1}$-re. Tehát ha vesszük az A $\theta\neq k$ sajátértékét és a hozzá tartozó $\mathbf{v}$ sajátvektort, akkor

$$A^2v-(\lambda-\mu)Av-(k-\mu)Iv=\mu Jv=0,$$

így

$$\theta^2-(\lambda-\mu)\theta-(k-\mu)=0.$$

Tehát A k-tól különböző sajátértékei az $x^2-(\lambda-\mu)x-(k-\mu)$ másodfokú polinom gyökei kell, hogy legyenek.

Legyen $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. Ekkor a polinom két gyöke:

$$\begin{aligned} \theta_1 &= \frac{(\lambda - \mu) + \sqrt{\Delta}}{2}, \\ \theta_2 &= \frac{(\lambda - \mu) - \sqrt{\Delta}}{2}. \end{aligned} \tag{1}$$

$\theta_1\theta_2 = (\mu - k)$, így feltéve, hogy $\mu < k$, következik, hogy a sajátértékek különböző előjelű, nem nulla számok. Feltehetjük, hogy $\theta_1 > 0$
Láttuk, hogy az erősen reguláris gráf sajátértékei függenek a paraméterektől, akkor mit tudunk elmondani a multiplicitásukról? Legyenek a sajátértékek multiplicitásai m_{θ_1} és m_{θ_2}. Mivel a k multiplicitása 1 és a sajátértékek összege az A nyoma, ami 0, így megkapjuk, hogy:

$$m_{\theta_1} + m_{\theta_2} = n - 1, m_{\theta_1}\theta_1 + m_{\theta_2}\theta_2 = -k, \tag{2}$$

Átalakítva megkapjuk, hogy

$$m_{\theta_1} = -\frac{(n-1)\theta_2 + k}{\theta_1 - \theta_2}, m_{\theta_2} = \frac{(n-1)\theta_1 + k}{\theta_1 - \theta_2} \tag{3}$$

Most tekintsük az alábbit:

$$(\theta_1 - \theta_2)^2 = (\theta_1 + \theta_2)^2 - 4\theta_1\theta_2 = (\lambda - \mu)^2 + 4(k - \mu) = \Delta$$

Behelyettesítve ezt és a sajátértékek képletét a multiplicitások képletébe kapunk két erős egészségi feltételt:

$$m_{\theta_1} = \frac{1}{2}\left((n-1) - \frac{2k + (n-1)(\lambda - \mu)}{\sqrt{\Delta}}\right)$$

és

$$m_{\theta_2} = \frac{1}{2}\left((n-1) + \frac{2k + (n-1)(\lambda - \mu)}{\sqrt{\Delta}}\right).$$

Ezek a képletek nagyon erős feltételek, mivel adott paraméterekre ki tudjuk direkt számolni a multiplicitásokat, amik, ha nem egész számok, akkor nem létezik ilyen paraméterezésű erősen reguláris gráf.

4.4. Lemma. *[8] Egy összefüggő reguláris gráf, aminek pontosan 3 külöböző sajátértéke van erősen reguláris.*

Bizonyítás. Tegyük fel, hogy Γ egy összefüggő reguláris gráf, k, θ, τ sajátértékekkel,

ahol k a fokszám. Ha $A = A(\Gamma)$, akkor a

$$M := \frac{1}{(k-\theta)(k-\tau)}(A-\theta I)(A-\tau I)$$

mátrix polinom minden sajáértéke 0 vagy 1. A bármely θ-hoz vagy τ-hoz tartozó sajátvektora benne van M magterében, így megkapjuk, hogy M rangja megegyezik k, mint sajátérték multiplicitásával. Mivel Γ összefüggő volt, így ez a multiplicitás 1, azaz $M\mathbf{1} = \mathbf{1}$, amiből következik, hogy $M = \frac{1}{n}J$.
Itt láthatjuk, hogy J A-ban egy másodfokú polinom, azaz A^2 az I, J és A mátrixok lineáris kombinációja. Ennek megfelelően Γ erősen reguláris. □

A Krein korlátok az erősen reguláris gráfok kutatásának talán legfontosabb feltételei, de a bevezetésükhüz még néhány karakterizációt be kell, hogy vezessünk.

4.5. Lemma. *[8] Legyen Γ egy erősen reguláris gráf (n, k, λ, μ) paraméterekkel és k, θ és τ különböző sajátértékekkel. Ekkor*

$$m_\theta m_\tau = \frac{nk\overline{k}}{(\theta-\tau)^2}$$

Bizonyítás. Induljunk ki a multiplicitások (3) egyenletbeli alakjaiból, valamint a sajátértékek (1) egyenletbeli alakjaiból. Ekkor átalakítások sorozatából megkapjuk a végeredményt. □

4.6. Lemma. *[8] Legyen Γ egy erősen reguláris gráf (n, k, λ, μ) paraméterekkel és k, θ és τ különböző sajátértékekkel. Ha $m_\theta = m_\tau$, akkor $k = (n-1)/2, \lambda = (n-5)/4$ és $\mu = (n-1)/4$.*

Bizonyítás. Ha $m_\theta = m_\tau$, akkor mindkét multiplicitás $(n-1)/2$, ezt jelöljük m-mel. Ez alapján m relatív prím n-nel, így az előző lemmából 4.5 következik, hogy $m^2 | k\overline{k}$. Mivel $k+\overline{k} = n-1$, így az egyetlen lehetséges eset, hogy $k\overline{k} \leq (n-1)^2/4 = m^2$, ahol egyenlőség csakis $k = \overline{k}$ estén áll fennt. Az előző két feltétel szerint egyenlőségnek kell lennie, így $k = \overline{k} = m$. Mint korábban (2) beláttuk, $m(\theta+\tau) = -k$, ebből következik, hogy $\theta + \tau = \lambda - \mu = -1$, tehát $\lambda = \mu - 1$. Végül $k(k-\lambda-1) = \overline{k}\mu$ miatt $\mu = k - \lambda - 1$, amiből $\mu = k/2$. Ezekből következik, hogy Γ a lemmában megállapított paraméterekkel rendelkezik. □

4.7. Tétel. *[8](A tétel is a bizonyításbeli lemmák is ebből a forrásból származnak) [Krein korlátok] Legyen Γ egy primitív, erősen reguláris gráf (n, k, λ, μ) paraméterekkel és k, θ és τ különböző sajátértékekkel. Jelölje m_θ és m_τ a θ és τ sajátértékek*

multiplicitásait. Ekkor

$$\theta\tau^2 - 2\theta^2\tau - \theta^2 - k\theta + k\tau^2 + k\tau \geq 0,$$
$$\theta^2\tau - 2\theta\tau^2 - \tau^2 - k\tau + k\theta^2 + k\theta \geq 0$$

Ha az első egyenlőtlenség éles, akkor $k \geq m_\theta$, ha a második, akkor $k \geq m_\tau$. Ha mindkét egyenlőtlenség éles, akkor az alábbiak egyike teljesül:

1. Γ *az 5-hosszú kör C_5,*
2. Γ*-nak vagy a komplementerének első komponense üres, a második pedig erősen reguláris,*
3. Γ *minden részkomponense erősen reguláris.*

Bizonyítás. A bizonyítás hosszú és rész-lemmákra lesz bontva. A könnyebb olvashatóság miatt bevezetek pár jelölést:
Γ egy primitív, erősen reguláris gráf (n, k, λ, μ) paraméterekkel és k, θ és τ különböző sajátértékekkel, ahol nem teszünk fel semmit θ és τ előjeléről (avagy bármelyik lehet a pozitív sajátérték). Legyen u a gráf egy tetszőleges csúcsa és legyen X_1 és X_2 az u-hoz viszonyított elő és második komponensen a gráfnak. A gráfkomponensek adjacencia mátrixai legyenek A_1 és A_2. A lemmák bizonyításaiban m-et fogok használni m_θ helyett.

4.8. Lemma. *Ha $k \geq m_\theta$, akkor τ az első komponens egy sajátértéke, legalább $k - m_\theta$ multiplicitással.*

Bizonyítás. Legyen U egy $V(\Gamma)$-án értelmezett tér, ami magába foglalja azokat a függvényeket, amik összege 0 Γ u-tól függő komponensein. Ez a tér $n-3$ dimenziós. Legyen T az a tér, amit Γ τ-hoz tartozó olyan sajátvektorai feszítenek ki, amik összege 0 $V(X_1)$-en. T egy $n - m - 2$ dimenziós tér, aminek az egésze benne van U-ban. Jelölje N azt a teret, ami tartalmazza a $V(\Gamma)$-án 0 értékű függvényeket, amik tartója $V(X_1)$-ben van; Az N dimenziója $k - 1$ és őt is tartalmazza U.
Amennyiben $k > m$, akkor teljesül, hogy $dim(N)+dim(T) > dim(U)$, tehát $\dim(N \cap T) \geq k-m$. Minden $N \cap T$-beli vektor egy τ-hoz tartozó sajátvektora Γ-nak, amiket megszorítva $V(X_1)$-re X_1 sajátvektora ugyanahhoz a sajátértékhez. □

4.9. Lemma. *Ha $k \geq m_\theta$, akkor*

$$(m_\theta - 1)(k\lambda - \lambda^2 - (k - m_\theta)\tau^2) - (\lambda + (k - m_\theta)\tau)^2 \geq 0.$$

Bizonyítás. Tudjuk, hogy λ A_1 egy sajátértéke, aminek a multiplicitása legalább 1, valamint hogy τ is sajátérték, legalább $k - m$ multiplicitással. Így marad $m - 1$

sajátértékünk kezeletlenül, jelölje őket $\sigma_1 \dots \sigma_{m-1}$.
Ekkor

$$0 = tr(A_1) = \lambda + (k-m)\tau + \sum_i \sigma_i$$

és

$$k\lambda = tr(A_1^2) = \lambda^2 + (k-m)\tau^2 + \sum_i \sigma_i^2.$$

A Cauchy-Schwarz egyenlőtlenségből következik, hogy

$$(m-1)\sum_i \sigma_i^2 \geq \left(\sum_i \sigma_i\right)^2,$$

Ahol egyenlőség akkor és csak akkor áll fenn, ha mind az $(m-1)$ σ_i sajátérték megegyezik. A fenti két egyenletből következik a lemma állításában szereplő egyenlőtlenség. □

4.10. Lemma. *Ha $k < m_\theta$, akkor*

$$(m_\theta - 1)(k\lambda - \lambda^2 - (k-m_\theta)\tau^2) - (\lambda + (k-m_\theta)\tau)^2 > 0.$$

Bizonyítás. Definiáljuk a $p(x)$ polinomot a következőképp:

$$p(x) := (m-1)(k\lambda - \lambda^2 - (k-m)x^2) - (\lambda + (k-m)x)^2.$$

Ekkor a polinomot átrendezhetjük, hogy

$$p(x) = (m-1)k\lambda - m\lambda^2 + 2\lambda(m-k)x + (k-1)(m-k)x^2,$$

Amiből kiszámolva a diszkriminánst, a következőt kapjuk:

$$-4\lambda(m-k)(m-1)k(k-1-\lambda).$$

Mivel $k < m$ és $1 < m$, látszik, hogy a kifejezés értéke negatív, hacsak $\lambda = 0$ nem teljesül. $\lambda = 0$ esetén

$$p(x) = (k-1)(m-k)x^2,$$

Nyílván $p(\tau) \neq 0$, hacsak τ nem 0. Ha $\lambda = 0$ és $\tau = 0$, akkor Γ egy teljes páros gráf $K_{k,k}$, ami sajátértékei $k, 0, -k$. Viszont, ha $\tau = 0$, akkor $\theta = -k$ és $m = 1$, ami ellentmond a $k < m$ feltevésünknek. □

Érdemes megjegyezni, hogy a 4.9 lemma alapján, ha $k < m_\theta$, akkor $p(x) \geq 0$ minden x választás mellett. A 4.8 lemma alapján pedig ha $k \geq m_\theta$, akkor a τ

sajátértéknek teljesítenie kell a $p(\tau) \geq 0$ egyenlőtlenséget.
Most megmutattuk, hogy akár teljesül, hogy $k \geq m_\theta$, akár nem,

$$(m_\theta - 1)(k\lambda - \lambda^2 - (k - m_\theta)\tau^2) - (\lambda + (k - m_\theta)\tau)^2 \geq 0.$$

Az egyenlet átírható k, θ és τ függvényére:

$$-\frac{k\tau(\tau+1)(\theta+1)}{(k+\theta\tau)(\theta-\tau)}(2\theta^2\tau + \theta^2 - \theta\tau^2 + k\theta - k\tau^2 - 2k\tau) \geq 0. \tag{4}$$

Hasonlóan kifejezhető az X_2-ben lévő csúcsok száma az

$$l := -\frac{k(\tau+1)(\theta+1)}{k+\theta\tau},$$

és Γ primitivitása miatt ez szigorúan pozitív szám. Ebből következik, hogy

$$-\frac{k\tau(\tau+1)(\theta+1)}{(k+\theta\tau)(\theta-\tau)} = \frac{l\tau}{\theta-\tau}.$$

Γ primitivitásából következik, hogy $\tau \neq 0$, tehát $\tau(\theta-\tau)^{-1} < 0$, a (4) egyenletből következik, hogy

$$(2\theta^2\tau + \theta^2 - \theta\tau^2 + k\theta - k\tau^2 - 2k\tau) \leq 0.$$

Ezzel befejeztük a tételünk első állításának bizonyítását, és mivel nem tettünk fel semmit a sajátértékeink előjeléről, így megkapjuk a másik egyenlőtlenség bizonyítását θ és τ felcserélésével.
Következő lépésben azt az esetet vizsgáljuk, ahol az egyik egyenlőtlenség éles.

4.11. Lemma. *Ha*

$$(m_\theta - 1)(k\lambda - \lambda^2 - (k - m_\theta)\tau^2) - (\lambda + (k - m_\theta)\tau)^2 = 0,$$

akkor $k \geq m_\theta$. *Továbbá vagy* Γ *első komponense erősen reguláris, vagy* $k = m_\theta$ *és* $\lambda = 0$.

Bizonyítás. A 4.9 lemma alapján egyenlőség nem teljesülhet $k < m_\theta$ esetén, így $k \geq m_\theta$. Ha 4.9 lemmában lévő Cauchy-Schwarz egyenlőtlenség egyenlőséggel teljesül, akkor minden σ_i sajátértéknek egyenlőnek kell lennie; ezt az értéket jelöljük σ-val. Ezek alapján X_1-nek legfeljebb 3 sajátértéke lehet, amik λ, σ és τ.
Ha $k = m$, akkor

$$0 = (k-1)(k\lambda - \lambda^2) - \lambda^2 = k^2\lambda - k\lambda^2 - k\lambda = k\lambda(k - \lambda - 1).$$

Mivel Γ se üres, se teljes gráf, így $k \neq 0$ és $k \neq \lambda+1$, amiből következik, hogy $\lambda = 0$. Most feltehetjük, hogy $k > m$ és szétválaszthatjuk az eseteket, ahol X_1-nek 1,2 vagy 3 sajátértéke van. Ha csak 1 van neki, akkor üres, tehát $\lambda = \sigma = \tau = 0$. Mivel $\theta\tau = \mu - k$, így $\mu = k$ teljesülne, avagy Γ egy teljes páros gráf lenne, ami viszont nem primitív.
Ha X_1-nek 2 sajátértéke van, akkor a [2.11] alapján X_1 minden komponensének az átmérője legfeljebb 1 lehet, így X_1 klikkek uniója.
Mivel Γ nem teljes, így legalább 2 klikk van, amiből következik, hogy X_1 erősen reguláris.
Ha 3 sajátértékkel rendelkezik X_1, akkor ő egy reguláris gráf, aminek a legnagyobb sajátértéke egyszerű. A Perron-Frobenius tétel miatt a legnagyobb sajátérték multiplicitása megegyezik a reguláris gráf komponenseinek számával, amiből következik, hogy X_1 összefüggő. A 4.4 lemma alapján X_1 erősen reguláris.
A befejezéshez szükségünk van Γ komplementerére, ami erősen reguláris lesz

$$(n, n-1-k, n-2-2k+\mu, n-2k+\lambda)$$

paraméterekkel, és sajátértékei $(n-k-1), (-1-\tau), (-1-\theta)$, megfelelően $1, m_\tau$ és m_θ multiplicitásokkal. Ha egyenlővé tesszük l-t $(n-1-k)$-val és b-t $(n-2-2k+\mu)$-vel, akkor az

$$(m_\theta - 1)(lb - b^2 - (l - m_\theta)(\tau+1)^2) - (b + (l - m_\theta)(-\tau-1))^2 \geq 0$$

egyenletet kapjuk. Ha ismét alkalmazzuk a k, θ és τ függvényébe átírást:

$$-\frac{k\tau(\tau+1)(\theta+1)}{(k+\theta\tau)(\theta-\tau)}(2\theta^2\tau + \theta^2 - \theta\tau^2 + k\theta - k\tau^2 - 2k\tau)$$

Meglepő módon újra ezt az eredményt kapjuk. Így kijelenthetjük, hogy ha egyenlőséggel teljesül a korlát Γ-ra akkor egyenlőséggel teljesül $\overline{\Gamma}$-ra is, amiből következik, hogy vagy $l = m_\theta$ vagy $\overline{\Gamma}$ első komponense is erősen reguláris. Ebből adódóan Γ második komponense vagy teljes gráf vagy erősen reguláris.
Összefoglalva, ha egyenlőség teljesül, akkor X_1 üres vagy erősen reguláris, X_2 teljes gráf vagy erősen reguláris. Ebből egyenesen következik, hogy C_5 az egyetlen erősen reguláris gráf, amire X_1 üres és X_2 teljes gráf, a Clebsch-gráf egy példa arra, amikor X_1 üres és X_2 erősen reguláris és mutatunk majd példát arra, hogy mindkét rész erősen reguláris.

□

□

5. Cayley gráfok, erősen reguláris gráfok és parciális differencia halmazok kapcsolata

5.1. Parciális differencia halmazok

A Cayley gráfok jobb megértéséhez először érdemes bevezetni a parciális differencia halmazok fogalmát, valamint megismerni néhány tulajdonságukat.

5.1. Definíció. [15] Legyen G egy (additív) Abel-csoport. A $D \subset G$ részhalmazt (n, k, λ) differenciahalmaznak nevezzük, ha $|G| = n, |D| = k$, és minden $0 \neq g \in G$-re pontosan λ db olyan $d, d' \in D$ pár van, melyre $d - d' = g$.

5.2. Példa. A mod 7 additív csoportban differenciahalmaz $D = \{0, 1, 3\}$; $D(7, 3, 1)$ paraméterekkel.
A mod 11 additív csoportban differneciahalmaz a $D = \{1, 3, 4, 5, 9\}$; $D(11, 5, 1)$ paraméterekkel.

5.3. Definíció. [4] Legyen G egy n elemű véges csoport, e egységelemmel.
Az $\mathcal{D}(n, k, \lambda, \mu)$ parciális differencia halmaz (PDS, az angol *partial difference set*-ből) G egy k-elemű részhalmaza, amire teljesül, hogy a $gh^{-1}; g, h \in \mathcal{D}$ kifejezés:

1. minden $\mathcal{D}$-beli nem egység elemet pontosan λ-szor vesz fel,
2. minden $G \backslash \mathcal{D}$-beli nem egység elemet pontosan μ akalommal vesz fel.

Ha $\mathcal{D}^{-1} = \mathcal{D}$ és $e \notin \mathcal{D}$, akkor $\mathcal{D}$-t regulárisnak nevezzük, valamint ha $\lambda \neq \mu$, akkor a $\mathcal{D}^{-1} = \mathcal{D}$ automatikusan teljesül.

5.4. Példa. Legyen q egy páratlan prímhatvány, amire teljesül, hogy $q \equiv 1 (\text{mod } 4)$. Ekkor $GF(q)$ nemnulla négyzetei egy parciális differencia halmazt alkotnak $GF(q)$ additív csoportjában $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ paraméterekkel. Ezeket a PDS-eket Paley-típusú parciális differencia halmazoknak nevezzük. [4]

5.2. Cayley gráfok

Korábban, a 3.10 definícióban láttuk, hogy ez eléggé megengedő, így a Cayley gráfok a gráfok egy elég népes és kutatott osztálya, mivel sok jó tulajdonsággal rendelkeznek, mint pl. szimmetria. Ez a dolgozat viszont nem vizsgálja a teljes osztályt, csak egy szabályosabb részét, nevezetesen az erősen reguláris Cayley gráfokat. A következő definíció meg is fogja mutatni, hogy miért volt fontos a PDS-ek

bevezetése, utána pedig az erősen reguláris Cayley gráfok paramétereit vizsgáljuk majd.

5.5. Példa. Az 5 elemű kör erősen reguláris Cayley erg(5,2,0,1) paraméterekkel, ahol a csoport az 5 elemű additív Abel-csoport, és $\mathcal{D} = \{1, 4\}$.
A 9 csúcsú általánosított négyszög (generalized quadrangle) erősen reguláris Cayley erg(9,4,1,2) paraméterekkel, $\mathbb{Z}_3 \times \mathbb{Z}_3$ additív Abel csoport felett és
$\mathcal{D} = \{(1, 0), (2, 0), (0, 1), (0, 2)\}$

5.6. Definíció. [3] Legyen G egy csoport. A δ leképzést komplex számok multiplikatív csoportjába a csoport egy karakterének nevezzük, ha $\delta(x + y) = \delta(x)\delta(y)$ teljesül, $x, y \in G$. δ így a csoport egy homomorfizmusa is.

5.7. Állítás. *[3] Legyen $\Gamma(G, S)$ egy Cayley gráf és δ egy karaktere G-nek. Ekkor G egy karakteréből számolt*

$$[\delta(g_0), \delta(g_1), \ldots \delta(g_n)]$$

vektor Γ sajátvektora, ahol $\delta(g_0) = \delta(1) = 1$.

5.8. Állítás. *Az előző állításban szereplő sajátvektorhoz tartozó sajátérték: $\sum_{s\in S} \delta(s)$.*

Bizonyítás. Jelöljük $y \sim x$-szel azon y csúcsokat, akik x szomszédai. Mivel $\Gamma(G, S)$ egy Cayley-gráf, így $\sum_{y\sim x} \delta(y) = \sum_{s\in S} \delta(x + s)$. Ez Cayley gráfokban homomorfizmus, így $\sum_{s\in S} \delta(x + s) = \sum_{s\in S} \delta(x) \cdot \delta(s) = \delta(x)(\sum_{s\in S} \delta(s))$. Ha megszorozzuk a $A(\Gamma)$ gráfot egy karakteréből számolt vektorral, akkor szintén $\delta(x)(\sum_{s\in S} \delta(s))$ eredményt kapjuk, így $\sum_{s\in S} \delta(s)$ valóban sajátérték. □

5.9. Állítás. *[9] [Első Ortogonalitási Reláció] Ezek a vektorok páronként lineárisan függetlenek, hisz az alábbi formula szerint páronként ortogonálisak.*

$$\sum_{g\in G} \overline{\delta_1(g)}\delta_2(g) = 0$$

Ahol a $\delta_1 \neq \delta_2$, különben az egyenlet jobb oldalán akkor $|G|$ állna.

5.10. Állítás. *[3] A G Abel csoport különböző karaktereinek száma $|G|$.*

5.11. Állítás. *A triviális karakter $\delta = 1$; $\delta(g) = 1(g) = 1$. $A(\Gamma)\mathbf{1} = k \cdot \mathbf{1}$, ahol a Γ gráf k reguláris.*

5.12. Lemma. *[3] Legyen δ egy karaktere G-nek, ami egy olyan $\delta : G \to \mathbb{C}^*$ leképzés, hogy $\delta(x + y) = \delta(x)\delta(y)$ teljesül. Ekkor $\sum_{y\sim x} \delta(y) = (\sum_{s\in S} \delta(s))\delta(x)$, úgy, hogy a $(\delta(x))_{x\in G}$ vektor egy jobb-sajátvektora az $A(\Gamma)$ mátrixnak a $\delta(S) := \sum_{s\in S} \delta(s)$ sajátértékkel. Az $n = |G|$ különböző karakter független sajátvektorokat ad, így megkapjuk a gráf spektrumát.*

5.13. Példa. Tekintsük a $\mathcal{C}_5$ 5-hosszú kört, mint Cayley-gráfot $\mathbb{Z}_5$ felett.
Itt $S = \{-1.1\}$. A gráf spektruma $\{\zeta+\zeta^{-1}|\zeta^5 = 1\}$, ami 2 és $\frac{1}{2}(-1\pm\sqrt{5})$. (Mindkettő multiplicitása 2.)

5.3. Caley gráfok izomorfizmus problémája

1967-ben A. Ádám [1] felvetette a következő problémát:

5.14. Probléma. *Vegyük a $0 < k_1 < k_2 < \ldots < k_m < n$ adott egész számokat és legyen $G_n(k_1, \ldots, k_m)$ egy irányított gráf $P_1, \ldots, P_n$ pontokkal. P_i és P_J között fut él akkor és csak akkor, ha valamilyen t-re $k_t \equiv j - i \pmod n$. Két ilyen $G_n(k_1, \ldots, k_m)$ és $G'_n(k'_1, \ldots, k'_m)$ gráf izomorfizmusának elégséges feltétele volt akkoriban, hogy létezik egy $0 < r < n$ szám, ami relatív prím n-hez és egy α permutációja $\{1, \ldots, n\}$ elemeknek, hogy $k'_t \equiv rk_{\alpha(t)} \pmod n$ minden $1 \leq t \leq n$-re.*

Djokovic bebizonyította [5], hogy ez a feltétel nem csak elégséges, de szükséges ha n egy prímszám. A probléma felvetésében megnevezett gráfok a 3.10 definícióban már ismertetett Cayley-gráfok, amik kutatásának története igazán itt kezdődött el: Li survey cikkében [11] látható rengeteg eredmény amit a Djokovic tanulmány továbbfejlesztései ([2], [13], [14]) inspiráltak.
A cikk n = p prímre vonatkozó része könnyen értelmezhető, aminek jó értelmezéséhez érdemes bevezetnünk egy pár jelölést:
Legyen $N = \{1, 2, \ldots, n-1\} \subset \mathbb{Z}_n$. A $\mathbb{Z}_n$ elemein M multiplikatív csoport N részhalmazain hat. Egy $a \in M$ elem hatása egy $K \subset N$ halmazon

$$K \to a \circ K = \{a \circ k \mid k \in K\},$$

ahol $(n, a) = 1$. Speciálisan $|K| = |a \circ K|$. $K \sim K'$-vel jelöljük, ha létezik olyan $a \in M$, amire teljesül, hogy $K' = a \circ K$. Jelen esetben vegyük mind K-t, mind K'-t egy m elemű halmaznak, amikre a fenti előállítás úgy is igaz, hogy ha $G_n(K) \cong G_n(K')$, akkor $K \sim K'$, aminek nyílván a megfordítása is igaz, avagy ha $K \sim K'$, akkor $G_n(K) \sim G_n(K')$.

5.15. Lemma. *[5] Ha $G_n(K) \cong G_n(K')$, $n = p^a$, akkor léteznek $K_1 \sim K$, $K'_1 \sim K'$ és N egy τ permutációja, amikre $\tau(k) = k$ és $k \in N^0$ illetve $K_1(\varepsilon^k) = K'_1\ (\varepsilon^{\tau(k)}); k \in N$. ($N^0$ az az $n = p^a$-hoz relatív prím számok halmaza és ε a primitív n-edik egységgyökök.)*

Bizonyítás. Mivel $p^{a-1} - 1$ szám osztható p-vel N-ben,

$$p^a - 1 > p(p^{a-1} - 1),$$

tehát kell, hogy létezzen legalább egy $k_0 \in N^0$, hogy $\pi(k_0) \in N^0$. Beillesztve $K_1 = k_0 \circ K$ és $K_1' = \pi(k_0) \circ K'$ képleteket kapjuk, ammiből $G_n(K) \cong G_n(K_1)$ és $G_n(K') \cong G_n(K_1')$ következik. $G_n(K) \cong G_n(K_1)$ miatt létezik egy σ permutációja N-nek, hogy

$$K_1(\varepsilon^k) = K_1'(\varepsilon^{\sigma(k)}), k \in N.$$

Mivel $n = p$, ezért a 0 kivételével minden szám relatív prím p-hez, így N^0 lecserélhető N-re. K_1 és K_1' definíciójából következik, hogy

$$K_1(x) = K(x^{k_0})*, K_1' = K'(x^{\pi(k_0)})*$$

ahol a csillag azt jelenti, hogy a kitevőket mod n kell venni. Ebből látszik, hogy

$$K_1(\varepsilon) = K_1'(\varepsilon)$$

valamint

$$K_1(\varepsilon^k) = K_1'(\varepsilon^k), k \in N^0.$$

Amiből σ kicserélhető τ-ra ami kielégíti a $\tau(k) = k$-t a fenti feltételekre. □

5.16. Tétel. *[5] Ha $n = p$ prím, akkor a 5.14 problémában definiált $G_n(k_1, \ldots, k_m)$ és $G_n'(k_1', \ldots, k_m')$ gráfok izomorfak $\iff$ létezik egy $0 < r < n$ szám, ami relatív prím n-hez és egy α permutációja $\{1, \ldots, n\}$ elemeknek, hogy $k_t' \equiv rk_{\alpha(t)} \pmod n$ minden $1 \leq t \leq n$-re.*

Bizonyítás. Legyen $G_n(K) \cong G_n(K')$. Az előző lemmából

$$K_1(\varepsilon^k) = K_1'(\varepsilon^k), k \in N,$$

ahol $K_1 \sim K$, $K_1' \sim K'$. Ha $K_1(x) - K_1'(x) \neq 0$, akkor ez egy legfeljebb $p - 1$ fokú egész együtthatós polinom konstans tag nélkül. Ez a polinom nem osztható az ε minimálpolinomjával, ami

$$1 + x + \ldots + x^{p-1}.$$

Ebből következik, hogy csakis $K_1(x) = K_1'(x)$ állhat fenn, avagy $K_1 = K_1'$, amiből $K \sim K'$. Ezzel beláttuk a nehezebb irányát az állításnak, a másik irány triviális. □

5.17. Állítás. *$n = p$ prím és relatív prímmel szorzás esetén a kospektralitás ekvivalens az izomorfiával, viszont ez az ekvivalencia prím hatványok esetén már nem áll fenn.*

Bár ez az állítás igaz, a szerző által hozott példa nem helyes: $n = 5^2$ és $K = \{1, 2, 4, 5, 7, 12, 17, 22\}$, $K' = \{1, 3, 4, 5, 8, 13, 18, 23\}$ esetén, ha K-ba és K'-be behe-

lyettesítjük as 25. egységgyököket, akkor nem azonos sajátértékeket kapunk, avagy a két gráf a példában nem is kospektrális, így egyátalán nem releváns a példa.

6. Erősen reguláris Cayley gráf keresése

S. L. Ma egy 1994-es cikkében [12] létrehozott egy listát, ami tartalmazta minden lehetséges parciális differencia halmaz paramétereit $k \leq 100$ esetén. 32 kivételével mind a 187 eset létezése ismert volt. '97-ben még megoldott 13 esetet, melyekről így már tudjuk, hogy nem léteznek, ez hagyott 19 paraméterhalmazt nyitott kérdésnek. Fiedler és Klin bebizonyítottak még egy esetet 1998-ban amit 2007-ben Kohnert is megtalált. S. de Winter 2 kivételével kizárta a maradék létezését. Ez a kettő pedig a $(216, 40, 4, 8)$ és $(216, 43, 10, 8)$. Én az előbbivel fogok foglalkozni.
Mielőtt viszont belefogunk a keresésbe, fontos lesz pár eszközünk működését lefektetni:

6.1. Definíció. [9]
Legyen G egy véges csoport, $|G| = n$ és legyen v egy csoportelem. Definiáljuk $\chi_v(x)$ reprezentációt, amire teljesül, hogy $\chi_v(x) = exp(\frac{2\pi i}{n} \cdot \langle v, x \rangle)$,ahol $\langle v, x \rangle$ a mod n vett skaláris szorzata a 2 elemnek.

A fenti definícióból nyilván következik, hogy

$$\chi_v(x+y) = exp\left(\frac{2\pi i}{n} \cdot \langle v, x+y \rangle\right) = exp\left(\frac{2\pi i}{n} \cdot \langle v, x \rangle\right) \cdot exp\left(\frac{2\pi i}{n} \cdot \langle v, y \rangle\right)$$

6.2. Állítás. *[9] Legyen G egy véges Abel csoport, $|G| = n$ és legyen g egy csoportelem. Ezen felül legyen $\chi_g(x)$ a fentiekben definiált reprezentáció. Ekkor $\sum_{s \in S} \chi_g(s) \in Spec(G, S)$ minden g eleme G-re, a 5.8 állítás alapján.*

Specifikusan mi ezt a 216 elemű $\mathbb{Z}_2^3 \times \mathbb{Z}_3^3$ csoportra, fogjuk nézni, mivel a de Winter tanulmányból kiindulva ezen érdemes a $(216, 40, 4, 8)$-at keresni, ha létezik. A tanulmányból látszik, hogy minden kisebb csoportra a PDS létezése már eldöntött, valamint a dolgozatban feljebb említett egészségi feltételek teljesülnek a paraméterszettre:

$$(k = 40; m_k = 1)$$
$$\theta_1 = \frac{4 - 8 * \sqrt{(-4)^2 + 4(40-8)}}{2} = 4,$$
$$m_{\theta_1} = -\frac{215 \cdot (-8) + 40}{4+8} = 140,$$
$$\theta_2 = \frac{4 - 8 * \sqrt{(-4)^2 - 4(40-8)}}{2} = -8,$$
$$m_{\theta_2} = \frac{215 \cdot 4 + 40}{4+8} = 75.$$

Továbbá a Krein-korlátok is rendben vannak,

$$4 * (-8)^2 - 2 * 16 * (-8) - 16 - 40 * 4 + 40 * (-8)^2 + 40 * (-8) = 2576 \geq 0,$$
$$4^2 * (-8) - 2 * 4 * (-8)^2 - (-8)^2 - 40 * (-8) + 40 * 16 + 40 * 4 = 416 \geq 0.$$

$$\varphi_{(u,v)}(x,y) = exp\left(\frac{2\pi i}{2} \cdot \langle x, u\rangle_2\right) \cdot exp\left(\frac{2\pi i}{3} \cdot \langle y, v\rangle_3\right),$$

ahol $u \in \mathbb{Z}_2^3$, $v \in \mathbb{Z}_3^3$ és $\langle ., . \rangle_n$ a mod n skalár szorzást jelenti.
Mivel az exponenciális függvény számítása numerikusan nem annyira pontos és nagyon költséges, ezért mi az egységgyökök egy más alakját használjuk majd az algoritmusunkhoz:

$$\varphi'_{(u,v)}(x,y) = (-1)^{\langle x,u\rangle_2} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right)^{\langle y,v\rangle_3}.$$

6.1. Az algoritmus általánosan

Egy mohó algoritmust fogunk használni a keresésre, ezt először általánosan fogalmazzuk meg, aztán teszteljük kisebb csoportokra és végül megnézzük, hogy hogyan teljesít a $\mathbb{Z}_2^3 \times \mathbb{Z}_3^3$ csoporton.
Legyen $\mathbf{u} \in G \backslash \{0\}$, ahol G egy n elemű additív Abel-csoport.
Legyen C halmaz G minden k elemű részhalmaza által alkotott halmaz és ezeket a részhalmazokat jelölje $S_i, i = 1 \ldots k$. A lehetséges PDS-eket jelölje PDS_{pot}, a megtaláltakat jelölje PDS_{fin}.

1. Algorithm Általános algoritmus

$PDS_{pot} \leftarrow \varnothing$ ▷ Az első nagy ciklusban megkeressük a lehetséges PDS-eket.
$a \leftarrow exp(\frac{2\pi i}{n})$
$h \leftarrow 0$
for $i = 1...|C|$ **do**
  Sum $\leftarrow 0$
  for $j = 1 \dots k$ **do**
    $h \leftarrow a^{<\mathbf{u},\mathbf{s}_{i,j}>_n}$ ▷ $\mathbf{s}_{i,j} \in S_i$
    Sum $\leftarrow$ Sum$+h$
  end for
  if Sum $\in Spec(G, S)$ **then**
    $PDS_{pot} \leftarrow PDS_{pot} \cup \{S_i\}$
  else
    $i \leftarrow i + 1$
  end if
end for

$PDS_{fin} \leftarrow \varnothing$ ▷ A második nagy ciklusban a PDS jelöltjeinkből kiválasztjuk azokat, akik tényleg teljesítik a feltételeinket.
for $i = 1 \dots |PDS_{pot}|$ **do**
  SumErr $\leftarrow 0$ ▷ Az összeghibák száma egy jelöltnél, ha ez 0, akkor őt PDS-nek jelöljük.
  for $j = 1 \dots (n - 1)$ **do** ▷ A $G\backslash\{0\}$ elemein megyünk végig
    Sum $\leftarrow 0$
    for $l = 1 \dots k$ **do** ▷ $|S_i| = k$
      $h \leftarrow a^{<\mathbf{g}_j,\mathbf{s}_{i,l}>_n}$ ▷ $\mathbf{g} \in G\backslash\{0\}$
      Sum $\leftarrow$ Sum$+h$
    end for
    if Sum $\notin Spec(G, S)$ **then**
      SumErr $\leftarrow$ SumErr$+1$
    else
      $j \leftarrow j + 1$
    end if
  end for
  if SumErr $= 0$ **then**
    $PDS_{fin} \leftarrow PDS_{fin} \cup S_i$
  else
    $i \leftarrow i + 1$
  end if
end for

Bár kicsi csoportokra kézzel még számolható lenne az algoritmusunk, megéri már ezekre is számítógéppel számolni, mivel így ellenőrizhető a módszerünk helyessége. Sagemathben implementáltam a algoritmust, mivel ebben a programozási nyelvben már megvalósították a csoportokat és az egységgyököket. (Nem tökéletes a megvalósítás, de erre majd a nagy csoportunk vizsgálatánál visszatérünk.) A Sagemath egy szimbolikus nyelv, így egészen tisztán fordíthatóak át a matematikai koncepciók kódba, viszont ez néhány, időnként zavaró kompromisszumot hordoz magában. A legfontosabb talán az objektumok típusának konfliktusai. A csoportok elemei moduló léteznek és a velük végzett műveletek is autómatikusan moduló számoldónak, ami nem teszi őket kompatibilissé csoportjukon kívüli objektumokkal (pl. sima egész számok (int)). Ezt helyenként elég csúnyán lehet megoldani, ez majd tükröződni fog a kódban.
A rövid környezeti bevezető után tekintsük az algoritmus teljesítményét két kisebb példán, amit akár kézzel is lehet ellenőrizni: $\mathbb{Z}_5$ és a $\mathbb{Z}_3 \times \mathbb{Z}_3$ erre megfelelőek lesznek. A két csoport sajátértékei a (1) egyenletek alapján:
$\mathbb{Z}_5$: $k = 2$, $\theta_1 = \frac{-1+\sqrt{5}}{2}$, $\theta_2 = \frac{-1-\sqrt{5}}{2}$
$\mathbb{Z}_3 \times \mathbb{Z}_3$: $k = 4$, $\theta_1 = \frac{-1+\sqrt{9}}{2} = 1$, $\theta_2 = \frac{-1-\sqrt{9}}{2} = -2$
A kód a következőképp nézz ki:

```
##########################################
######### Built on Sage ver 10.0 ############
##########################################
import itertools
import random as rand
import numpy as np

#### Group generation ####
#GR_s = AdditiveAbelianGroup([5]);
#GR_s = AdditiveAbelianGroup([9]);
GR_s = AdditiveAbelianGroup([3,3]);
#GR_s.gens();

UCF = UniversalCyclotomicField();

#### Eigen values ####
#eig_1 = ZZ(2);
#eig_2 = (-1+sqrt(5))/2;
#eig_3 = (-1-sqrt(5))/2;
eig_1 = 4;
eig_2 = 1;
eig_3 = -2;
```

Az első kódrészben meghívunk minden szükséges könyvtárat és csoportokat létrehozzuk beépített függvények segítségével, valamint rögzítjük a sajátértékeket.

```
#### Potential PDS ####
temp_PDS = [];
temp_Gr = list(GR_s);
temp_Gr.pop(0);
#for comb in itertools.combinations(temp_Gr, 2):
for comb in itertools.combinations(temp_Gr, 4):
    temp_PDS.append(comb);

~~~~~~
#len(temp_PDS);
#temp_PDS;
```

Ezután jön a lehetséges PDS-ek létrehozása. Fogjuk a csoport nem 0 elemeit és létrehozzuk minden k elemű részcsoportjukat. (Ez a $\mathbb{Z}_5$-nél 2 elemű csoportokat jelent, a $\mathbb{Z}_3 \times \mathbb{Z}_3$-nál pedig 4 eleműeket.)

```
#### Finding PDS ####
PDS = [];
#u = 8;
u = vector(rand.choice(temp_PDS[1]));
#a = UCF.gen(5);
#a = UCF.gen(9);
a = UCF.gen(3);

for i in range(len(temp_PDS)):
    Sum = 0;
    for j in range(len(temp_PDS[i])):
        #kitev = int(np.array(list((u*vector(temp_PDS[i][j])) % 5)));
        #kitev = int(np.array(list((u*vector(temp_PDS[i][j])) % 9)));
        kitev =u*vector(temp_PDS[i][j]);
        kitev = kitev % 3;
        h = a^(kitev);
        Sum += h;
    if Sum in [eig_1,eig_2,eig_3]:
        PDS.append(temp_PDS[i])
    else:
        i += 1;
PDS;
```

Az első nagy ciklus jön az algoritmus szerint. Látható, hogy a típusok néhány esetben kényelmetlenek, de a számítások jók, a korábban definiált reprezentációnk szerint jónak ítélt PDS_{pot}-jainkat kigyűjtjük egy listába, amivel majd tovább fogunk számolni. Megjegyzendő, hogy a tesztelés a lehetséges PDS-ekre egy (véletlenszerűen) választott csoportelemmel történik.

```
62  61  trPDS = []
63  62  for i in range(len(PDS)):
64  63      SumErr = 0;
65  64      for k in range(len(temp_Gr)):
66  65          Sum = 0;
67  66          for j in range(len(PDS[i])):
68  67              b1 = vector(PDS[i][j])
69  68              u = vector(temp_Gr[k])
70  69              #kitev = int(np.array(list((u*vector(PDS[i][j])) % 5)));
71  70              kitev_1 = u*b1;
72  71              kitev_1 = int(kitev_1) % 3;
73  72              h = a^(kitev_1);
74  73              Sum += h;
75  74          #Sum;
76  75          if Sum not in [eig_1,eig_2,eig_3]:
77  76              SumErr += 1;
78  77      #SumErr;
79  78      if SumErr == 0:
80  79          trPDS.append(PDS[i]);
81  80      else:
82  81          i+=1;
83  82  len(trPDS);
84  83  trPDS;
```

A kód utolsó részében, az algoritmusunk szerinti második nagy ciklusban a PDS-jelöltjeinkből válogatjuk ki azokat, akik tényleg jók. A megfelelő PDS-ek minden nem 0 csoportelemmel szorozva sajátértéket kell, hogy adjanak, ha bármely csoportelemre ez nem teljesül, akkor őket kidobjuk. Az algoritmus és a kód is **for** ciklust használ itt, viszont ez javítható lenne, egy **while** ciklussal, SumErr > 0 leállási feltétel mellett.

Outputok:

Csak a $\mathbb{Z}_3 \times \mathbb{Z}_3$-re számolt outputot fogjuk elemezni, mivel az sokkal tanulságosabb a 216 elemű csoportunk vizsgálatára nézve.

Az első for ciklusból kapott PDS_{pot}:

```
[((0, 1), (0, 2), (1, 0), (2, 0)), ((0, 1), (0, 2), (1, 0), (2, 1)), ((0, 1), (0, 2), (1, 0), (2, 2)), ((0, 1),
(0, 2), (1, 1), (2, 0)), ((0, 1), (0, 2), (1, 1), (2, 1)), ((0, 1), (0, 2), (1, 1), (2, 2)), ((0, 1), (0, 2),
(1, 2), (2, 0)), ((0, 1), (0, 2), (1, 2), (2, 1)), ((0, 1), (0, 2), (1, 2), (2, 2)), ((1, 0), (1, 1), (2, 0),
(2, 1)), ((1, 0), (1, 1), (2, 0), (2, 2)), ((1, 0), (1, 1), (2, 1), (2, 2)), ((1, 0), (1, 2), (2, 0), (2, 1)),
((1, 0), (1, 2), (2, 0), (2, 2)), ((1, 0), (1, 2), (2, 1), (2, 2)), ((1, 1), (1, 2), (2, 0), (2, 1)), ((1, 1),
(1, 2), (2, 0), (2, 2)), ((1, 1), (1, 2), (2, 1), (2, 2))]
```

Kicsit nehezen olvasható, de a csoportok 4 darab 2 dimenziós vektorokból állnak. Emlékeztetőképp ezek voltak azok a részhalmazai a csoportnak, amik **egy** csoportelemmel szorozva teljesítették a feltételt. Most őket vizsgáljuk tovább **minden** csoportelemmel:

```
[((0, 1), (0, 2), (1, 0), (2, 0)), ((0, 1), (0, 2), (1, 1), (2, 2)), ((0, 1), (0, 2), (1, 2), (2, 1)), ((1, 0),
(1, 1), (2, 0), (2, 2)), ((1, 0), (1, 2), (2, 0), (2, 1)), ((1, 1), (1, 2), (2, 1), (2, 2))]
```

A második szűrést már csak 6 darab 4 elemű részhalmaz élte túl. Ezek között

fellelhető a 5.5 példában már említett PDS is, de jelen vannak mások is. Ezek izomorf gráfokat eredményeznek. Ebből látszik, hogy az algoritmusunk jól működik, így kipróbálhatjuk a nagy csoportra is.

6.2. A 216 elemű Abel csoport vizsgálata

Az előző alfejezetben láthattuk, hogy az algortimusunk helyesen működött vektorok használata mellett is, így egészen jó esélyünk lehet találni vele valamit a (216,40,4,8)-ra is. Ekkor érdemes belegondolni, hogy hány 40 elemű részhalmazt tudunk kiválasztani a $\mathbb{Z}_2^3 \times \mathbb{Z}_3^3 \backslash \{0\}$-ból. Ez egy 10^{43} nagyságrendű szám, tehát nem sok reményünk van kiszámolni minden részhalmazára felfogható időn belül. Ezért kénytelenek vagyunk bevezetni valamiféle randomizálást a kódba és reménykedni, hogy szerencsések leszünk a választással.

```
26  25  #### Potential PDS ####
27  26  temp_PDS = [];
28  27  temp_Gr = GR_s;
29  28  temp_Gr.pop(0);
30  29  for i in range(1000000):
31  30      temp_PDS.append(rand.sample(temp_Gr,40));
```

Ekkor szembesülünk a következő technikai problémával: Előzőleg említettem, hogy a Sagemath csoport implementálása nem tökéletes, és ez itt bukott ki, ugyanis a vegyes modulójú csoportok elemeit nem tudja jól kezelni. A csoport létrehozása még probléma nélkül megvalósul, de bármely művelet a csoport elemein a vektor első elemének modulusával fog történni, ami nekünk nem elfogadható, így egy kicsit szokatlan, de funkcionális megoldást kellett alkalmazni a csoport generálásánál:

```
6   5   #### Group generation ####
7   6   gr1 = list(AdditiveAbelianGroup([2,2,2]));
8   7   gr2 = list(AdditiveAbelianGroup([3,3,3]));
9   8
10  9   def brkdwn(rec, cuz):
11  10      out = [];
12  11      for i in rec:
13  12          for j in cuz:
14  13              out.append((i,j))
15  14      return out
```

Ez a függvény legenerálja az összes párt a két csoport 3 dimenziós vektoraiból, valamint így elég ugyanúgy a csupa 0 elemet eltávolítanunk, ami szintén a legelső lesz. Nyílván az elemek új felépítése némi változtatást kíván meg a konkrét számításokban.

```
#### Finding PDS ####
PDS = [];
paramOor = 0;
eigOor = 0;
u = vector(temp_PDS[0][0][0]);
u;
v = vector(temp_PDS[0][0][1]);
v;
#u*a;
a1 = UCF.gen(2);
a2 = UCF.gen(3);
rossz = [37,38,39,40];

for i in range(len(temp_PDS)):
    Sum = 0;
    paramErr = 0;
    params = matrix(2,3);
    for j in range(len(temp_PDS[i])):
        b1 = vector(temp_PDS[i][j][0])
        b2 = vector(temp_PDS[i][j][1])
        kitev_1 = u*b1;
        kitev_1 = int(kitev_1) % 2;
        kitev_2 = v*b2;
        kitev_2 = int(kitev_2) % 3;
        h = a1^(kitev_1) * a2^(kitev_2);
        Sum += h;
```

```
trPDS = []
for i in range(len(PDS)):
    SumErr = 0;
    for k in range(len(temp_Gr)):
        Sum = 0;
        for j in range(len(PDS[i])):
            b1 = vector(PDS[i][j][0])
            b2 = vector(PDS[i][j][1])
            u = vector(temp_Gr[k][0])
            v = vector(temp_Gr[k][1])
            kitev_1 = u*b1;
            kitev_2 = v*b2;
            kitev_1 = int(kitev_1) % 2;
            kitev_2 = int(kitev_2) % 3;
            h = a1^(kitev_1) * a2^(kitev_2);
            Sum += h;
        #Sum;
        if Sum not in [eig_1,eig_2,eig_3]:
            SumErr += 1;
    #SumErr;
    if SumErr == 0:
        trPDS.append(PDS[i]);
    else:
        i+=1;
len(trPDS);
trPDS;
```

Paraméterezés:

Hatodik egységgyököket szorzunk össze (második és harmadik egységgyökök szorzata hatodik), ami azt jelenti, hogy ezeknek csak bizonyos kombinációi adhatnak ki sajátértékeket. A 4 példáján keresztül mutatom be a kód működését:

4	0	0
0	0	0

A táblázat oszlopai a 3. egységgyökök balról jobbra, a sorai a 2. egységgyökök fentről le. Ha a 4-et akarjuk megkapni sajátértéknek, akkor az (1,1) cellában kell 4-nek szerepelnie. Nyílván itt csak 4 elemet néztünk meg, így ehhez hozzá kell még adnunk "0"-kat. Ezt a úgy tehetjük meg, hogy az alábbi két típusú formáció egyikével növeljük a táblázatot:

1	1	1
0	0	0

vagy

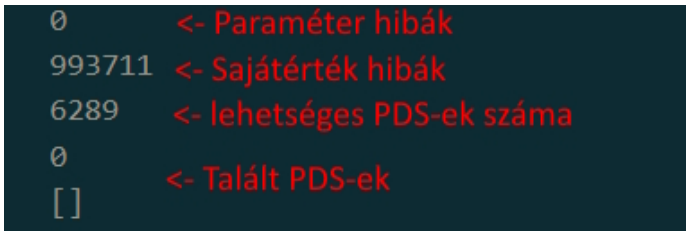
1	0	0
1	0	0

Nyílván ezt lehet növelni más oszlopokban vagy sorokban is hozzáadni a táblázathoz. Ezek harmadik vagy második egységgyökök összege lesz, ami 0, így a célunknak megfelel. A módszer pontos részletei olvashatóak a [10] cikkben. A kódban kicsit egyszerűbben gondolkozunk: nem engedünk meg egy cellában se 36-nál nagyobb számot.

```
59  58          params[kitev_1,kitev_2] += 1;
60  59      #Sum;
61  60      for k in rossz:
62  61          for l in range(params.nrows()):
63  62              if k in params[l]:
64  63                  paramErr += 1;
65  64      if paramErr > 0:
66  65          paramOor += 1;
67  66          i += 1;
68  67      elif Sum in [eig_1,eig_2,eig_3]:
```

Ezen megközelítéssel van némi probléma: nem pontosan ellenőrzi, hogy a "0"-ák jól jönnek-e ki vagy, hogy a 40 sajátérték nem csak a triviális paraméterezésből jön ki, viszont kellett valamilyen kompromisszumot kötni, hogy az így is lassan futó program értelmes időn belül adjon eredményt. Így itt is van egy fejlesztési lehetőség.

Output:



1 millió futtatásra is kb. 4 óra volt a futási ideje a programnak, ami jól mutatja, hogy az algoritmus nem tökéletes. A legenerált részcsoportok közül kb. 7000 volt PDS_{pot}, ami nem sok arányaiban, de körülbelül erre számítottunk. Ezután még őket teszteltük minden csoportelemmel, és az eredményünk az lett, hogy nem találtunk ténylegesen PDS tulajdonságú halmazt. Ez egyfelől várakozásainknak megfelel, másfelől önmagában nem túl sokatmondó, mivel az 1 milliós minta még mindig nagyságrendekkel kisebb, mint a részhalmazok lehetséges száma.
Összefoglalva, az eredményünk nagyon is limitálva van a számítási kapacitásaink, illetve az algoritmus tökéletlensége által. Egy jobb algoritmus biztosan jobb eredményeket érne el, valószínüleg nagyobb méretű halmazt is tudna egyszerre feldolgozni. Ami viszont lényegesen javítana az eredményeken az a keresési spektrum valamilyen előleges szűkítése a lehetséges PDS-ek keresési halmazán, hiszen ott történik a legnagyobb szűrés, ott iterálunk végig a legnagyobb halmazon.

Hivatkozások

[1] A., Ádám: Research Problem 2-10, J. Combin. Theory **2** (1967): 393.

[2] Bafai, L. "Isomorphism problem for a class of point-symmetric structures." Acta Mathematica Hungarica 29.3-4 (1977): 329-336.

[3] Brouwer, Andries E., and Willem H. Haemers. Spectra of graphs. Springer Science & Business Media, 2011

[4] De Winter, Stefaan, Ellen Kamischke, and Zeying Wang. "Automorphisms of strongly regular graphs with applications to partial difference sets." Designs, Codes and Cryptography 79 (2016): 471-485.

[5] Djoković, D. Ź. "Isomorphism problem for a special class of graphs." Acta Mathematica Hungarica 21.3-4 (1970): 267-270.

[6] Cayley, Professor. "Desiderata and suggestions: No. 2. The Theory of groups: graphical representation." American journal of mathematics 1.2 (1878): 174-176.

[7] Emil, Kiss. Bevezetés az algebrába. Typotex Kft, 2007.

[8] Godsil, Chris, and Gordon F. Royle. Algebraic graph theory. Vol. 207. Springer Science & Business Media, 2001.

[9] Isaacs, I. Martin. Character theory of finite groups. Vol. 359. American Mathematical Soc., 2006.

[10] Kiss, Gergely, et al. "On the discrete Fuglede and Pompeiu problems." Analysis & PDE 13.3 (2020): 765-788.

[11] Li, Cai Heng. "On isomorphisms of finite Cayley graphs—a survey." Discrete mathematics 256.1-2 (2002): 301-334.

[12] Ma, Siu Lun. "A survey of partial difference sets." Designs, Codes and Cryptography 4.4 (1994): 221-261.

[13] Muzychuk, Mikhail. "Ádám's conjecture is true in the square-free case." Journal of Combinatorial Theory, Series A 72.1 (1995): 118-134.

[14] Palfy, Peter P. "Isomorphism problem for relational structures with a cyclic automorphism." European Journal of Combinatorics 8.1 (1987): 35-43.

[15] Szőnyi, Tamás. "Szimmetrikus struktúrák." (2013).

[16] West, Douglas Brent. Introduction to graph theory. Vol. 2. Upper Saddle River: Prentice hall, 2001.