

EÖTVÖS LORÁND TUDOMÁNYEGYETEM

TERMÉSZETTUDOMÁNYI KAR

Ciklikus Hadamard - mátrixok

Bsc Szakdolgozat

Szerecz Vilmos

Matematika BSc

Matematikai elemző szakirány

Témavezető: Somlai Gábor



Budapest

2024

Köszönetnyilvánítás

Szeretném megköszönni a témavezetőmnek, Somlai Gábornak a lehetőséget és a témát a szakdolgozatomhoz. Szeretném megköszönni továbbá családomnak és barátaimnak a rengeteg támogatást, amit tanulmányaim alatt nyújtottak. Támogatás nélkül feladtam volna.

Tartalomjegyzék

1. Absztrakt	4
2. Bevezető	4
3. Definíciók	5
4. Hadamard-mátrixok	8
5. Ciklikus mátrixok	11
6. Cayley-gráfok	13
7. Diszkrét Pompeiu-probléma	13
7.1. Matolcsi Máté súlyfüggvénye	16
7.1.1. Konkrét súlyok	17
7.2. A súlyfüggvény megvalósítása számítógép segítségével.	22

1. Absztrakt

Ebben a dolgozatban bemutatom a kapcsolatot a Sylvester [18] által definiált Hadamard-mátrixok, és az eredetileg Pompeiu [16] által kért probléma diszkretizálása [11] között. Ennek segítségével használok Babai [1] és Lovász [13] eredményeit a Cayley-gráfok sajátértékeiről. Belátjuk, hogy a két probléma ekvivalens azzal, hogy egy $\mathbb{Z}_2^n$ -beli vektorra merőleges hipersík felezi-e Matolcsi [14] súlyfüggvényét. Explicit módon kimondom Matolcsi [14] súlyfüggvényének részleteit. Ezek után adok egy alsó korlátot a $\mathbb{Z}_2^n$ -beli vektor egyeseinek számára.

2. Bevezető

Egy Hadamard-mátrix egy olyan négyzetes ± 1 mátrix, amelynek sorai és oszlopai páronként ortogonálisak:

$$HH^T = n \cdot Id.$$

Ezeket először Sylvester [18] írta le 1867-ben, és belátta, hogy 2^j méretű valós Hadamard-mátrixok léteznek, megmutatva egy generáló algoritmust, amellyel végtelen sok Hadamard-mátrix előállítható. Majd Hadamard [5] 1893-ban vizsgálta tovább a kérdést, megmutatva alapeseteket $n = 12, 20$ -ra, belátva, hogy nem csak 2 hatvány méretűek léteznek, sőt belátta, hogy valós esetben csak $n = 1, 2, 4k$ méretűek lehetnek. Hadamard [5] eredetileg azt kérdezte, hogy mi a maximális determinánsa egy mátrixnak, ha elemei az egységkörről származnak. Erre a kérdésre volt a válasz a később róla elnevezett Hadamard-mátrix. Ennek a mátrixosztálynak, ha komplex egyhosszú elemekkel vizsgáljuk, akkor minden n -re létezik eleme, erre példa a Fourier-mátrixok. Valós esetben csak egy sejtésünk van, ami az egyik legrégibben fennálló kombinatorikai sejtés: az Hadamard-sejtés, miszerint minden $4n$ méretre létezik valós Hadamard-mátrix. Cati és Pasechnik [3] egy nagy adatbázist állítottak össze az eddig ismert Hadamard-mátrixokról, egészen $n = 3000$ -ig.

Egy ciklikus mátrix olyan négyzetes mátrix, amely egy vektor ciklikus permutációival van generálva. Ryser [17] azt sejtette meg 1963-ban, hogy $n = 4$ -nél nagyobb méretű ciklikus Hadamard-mátrixok nem léteznek. Egyszerűen látható, hogy a $v = (-1, 1, 1, 1)$ által generált mátrix Hadamard. Erre a sejtésre Turyn [19] 1965-ben adott egy szűkítést, bizonyítva, hogy $n > 4$ -re csak akkor létezhet valós ciklikus Hadamard-mátrix, ha $n = 4u^2$, ahol u páratlan, és nem prímszám. Leung és Schmidt [12] szűkítették a nyitott u^2 esetek listáját, a részletekért lásd [12] [15]. Míg Hadamard-mátrixból sok van, ciklikus Hadamard-mátrixból igen kevés, és a lehetséges mátrixok száma folyamatosan csökken.

A sík egy pozitív Lebesgue-mértékkel rendelkező kompakt részhalmaza Pompeiu-

tulajdonsággal rendelkezik, ha igaz rá a következő: ha $f : \mathbb{R}^2 \rightarrow \mathbb{C}$ folytonos, és

$$\int_{\sigma(K)} f d\lambda_2 = 0$$

minden $\sigma(K)$ távolságtartó transzformációra, akkor ebből következik, hogy $f \equiv 0$. Tudjuk, hogy minden sokszög Pompeiu. Tudjuk, hogy a kör nem Pompeiu. Pompeiu kérdése [16] az, hogy ha egy sima határú, kompakt részhalmaz nem Pompeiu, akkor az a kör-e [10]. A Lebesgue-mértéket lecserélve a számláló mértékre, a távolságtartó transzformációkat eltolásokra, ezt diszkretizálni lehet, lásd [11]:

$$\sum_{s \in S} f(x + s) = 0$$

Ezt a diszkrét problémát lehet összekapcsolni Matolcsi [14] súlyfüggvényével, ahol ennek egy súlyozott változatát vizsgáljuk.

Ebben a dolgozatban belátom, hogy a diszkrét Pompeiu-probléma ekvivalens azzal, hogy a Matolcsi [14] súlyfüggvényével súlyozott $\mathbb{Z}_2^n$ -t felezi-e egy $v \in \mathbb{Z}_2^n$ vektorra merőleges hipersík. Adok egy alsó határt a v -ben szereplő 1-esek számára: $k > \frac{n}{65}$.

3. Definíciók

Ebben a szekcióban definíciók sorozata található, amelyeket később használni fogok.

3.1. Definíció. [9] *Csoport.* Egy G nemüres halmaz csoport, ha értelmezünk elemein egy $*$ kétváltozós műveletet, melyre igazak a következők:

- $*$ asszociatív, vagyis bármely $a, b, c \in G$ -re $(a * b) * c = a * (b * c)$;
- létezik $e \in G$ kétoldali neutrális elem, melyre $e * g = g * e$ minden $g \in G$ -re;
- minden $g \in G$ -nek létezik g^{-1} kétoldali inverze, melyre $g^{-1} * g = g * g^{-1} = e$.

Jelölés: $(G, *)$.

3.2. Definíció. [9] *Abel-csoport.* Abel-csoport egy olyan csoport, amely kommutatív, vagyis a fenti jelölésekkel: $a, b \in G$ esetén $a * b = b * a$.

3.3. Definíció. [9] *Gyűrű.* Az R gyűrű, ha az R halmazon értelmezett egy összeadásnak nevezett $+$ jelű művelet is, és egy szorzásnak nevezett, általában egymás mellé írással jelölt művelet is, a következő tulajdonságokkal:

- R az összeadásra nézve Abel-csoport. (Ez tehát azt jelenti, hogy $+$ egy asszociatív és kommutatív művelet, amelyre nézve van nullelem, és minden elemnek van ellentettje.)
- R a szorzásra nézve asszociatív.
- Érvényes a disztributivitás: tetszőleges $x, y, z \in R$ esetén $(x + y)z = xz + yz$ és $z(x + y) = zx + zy$.

3.4. Definíció. [9] *Test.* Az olyan kommutatív, egységelemes gyűrűket, amelyekben minden nem nulla elemmel lehet osztani, testnek nevezzük. Ha egy gyűrű nem nulla elemei csoportot alkotnak a szorzásra, akkor a gyűrűt ferdetestnek hívjuk. A testek a kommutatív ferdetestek.

3.5. Definíció. [9] *Ciklikus csoport.* Egy G csoportot ciklikusnak nevezünk, ha egy alkalmas g elemének az egész kitevőjű hatványaiból áll. Az ilyen g elemeket a G generátorelemeinek nevezzük. Vagyis a g elem generálja a G csoportot.

3.6. Definíció. [9] *Homomorfizmus.* Legyenek $(A, *)$, $(B, \otimes)$ csoportok. Egy $f : A \rightarrow B$ homomorfizmus, ha $f(a * b) = f(a) \otimes f(b)$ minden $a, b \in A$ -ra.

3.7. Definíció. [9] *Izomorfia.* Legyenek $(A, *)$, $(B, \otimes)$ csoportok. Legyen f egy bijektív homomorfizmus. Ekkor f izomorfia A és B között. Két struktúra izomorf, ha létezik izomorfia közöttük.

3.8. Definíció. [9] *Elemi Abel p -csoport.* Az olyan G csoportokat, amelyek izomorfak a $(\mathbb{Z}_p^+)^n$ -re, elemi Abel p -csoportnak hívunk, ahol p prím, n pedig egész.

3.9. Definíció. [6] *Karakterisztikus függvény.* Legyen X halmaz, $A \subseteq X$, legyen T test. Az $1_A : X \rightarrow T$ függvényt az A csoport karakterisztikus függvényének nevezzük, ha

$$1_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

minden $x \in X$ -re.

3.10. Definíció. [6] *Skaláris szorzás.* Legyen V egy vektortér a $\mathbb{K}$ test felett. Definálunk egy bilineáris függvényt a következő módon: $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}$, valamint $\langle a, b \rangle = \sum a_i b_i$, ahol $a, b \in V$. Ezt a V vektortéren értelmezett skalárszorzásnak hívjuk.

3.11. Definíció. [4] *Abel-csoport karaktere.* $\chi_v : A \rightarrow \mathbb{C}^*$ homomorfizmus, ahol $v \in A$, $\mathbb{C}^* = (\mathbb{C} \setminus \{0\}, \cdot)$, vagyis a komplex számokból képzett multiplikatív csoport a klasszikus szorzásművelettel.

Karakter példák:

- C_n ciklikus csoport karaktere:

$$\chi_k(x) = \exp\left(\frac{2\pi i}{n} xk\right),$$

ahol C_n az n elemű ciklikus csoport, és xk modulo n van értelmezve. Mivel $\exp(\frac{2\pi i}{n})$ egy n -edik egységgyök, tehát n -edik hatványa 1, így ha x -et megváltoztatjuk n valami egész többszörösével, akkor az exponenciális függvény értéke nem változik.

- elemi Abel p -csoport karaktere:

$$\chi_u(v) = \exp\left(\frac{2\pi i}{p} \langle u, v \rangle\right),$$

ahol $\langle u, v \rangle$ a 3.10 definícióban van definiálva.

Az előző példákban láthattuk, hogy $x \mapsto \exp\left(\frac{2\pi i}{n} x\right)$ homomorfizmus.

3.12. Definíció. [9] *Mátrixok tenzorszorzata.* Ha A egy $n \times m$ -es, B egy $p \times q$ -s mátrix, akkor a két mátrix tenzorszorzata egy $pm \times qn$ -es mátrix: $(A \otimes B)_{pr+vs, qs+w} = a_{rs} b_{vw}$

$$A \otimes B = \begin{pmatrix} a_{11} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} & a_{12} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} & \dots \\ a_{21} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} & a_{22} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Ezt szokás tenzorszorzat helyett Kronecker-szorzatnak nevezni.

3.13. Definíció. *Ciklikus mátrix.* Egy A $n \times n$ -es mátrix ciklikus, ha $A_{ij} = u_{j-i}$, ahol $u \in \mathbb{T}^n$ vektor, és a $j - i$ index modulo n van számolva.

Ez a definíció pont azt jelenti, hogy egy vektor generálja a mátrixot: az első sor maga a vektor, a második sor a vektor elemei eltolva egyvel jobbra (az utolsó elem az első lesz), és így tovább.

3.14. Definíció. *Írányítatlan gráf.* Egy gráf irányítatlan, ha minden él fordítottja is él a gráfban.

3.15. Definíció. [1] *Színezett gráf.* Legyen V csúcshalmaz, és legyen $c_x : V \times V \rightarrow \mathbb{C}$ függvény minden élhez színt (súlyt) rendel. Lehet úgy tekinteni a nem élekre, mint amik 0 színt (súlyt) kaptak.

3.16. Definíció. [1] *Cayley-gráf.* Legyen G egy csoport $*$ csoportművelettel, és S egy generátorhalmaz. $\text{Cay}(G, S)$ gráfban a csúcsok legyenek megfeleltethetőek a G elemeivel, és akkor legyen közöttük él, ha $g_1^{-1} * g_2 \in S$.

3.17. Definíció. [8] *Adjacencia-mátrix.*

A $G = (V, E)$ gráf, szomszédsági mátrixa a következő $n \times n$ -es mátrix:

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

Írányított és irányítatlan gráfok esetében is használható. Irányítatlan gráf esetén ez a mátrix szimmetrikus. A G gráf adjacencia mátrixát $\text{Adj}(G)$ -vel jelöljük.

3.18. Állítás. *Amennyiben G egy ciklikus csoport, akkor $\text{Adj}(\text{Cay}(G, S))$ is ciklikus lesz.*

Ezt a fenti állítást triviális belátni.

3.19. Definíció. [1] *Színezett Cayley-gráf.* Legyen G csoport és $\alpha : G \rightarrow \mathbb{C}$. Ekkor $\text{Cay}(G, \alpha)$ színezett Cayley-gráf definiálható G -n: $c_x(g, h) = \alpha(g^{-1}h)$

Ha α egy S halmaz karakterisztikus függvénye, akkor a $\text{Cay}(G, S)$ Cayley-gráfot kapjuk, így ez egy tényleges általánosítása a Cayley-gráf fogalmának.

4. Hadamard-mátrixok

4.1. Definíció. [2] *Hadamard-mátrixok.* Egy $n \times n$ -s H mátrix Hadamard, ha minden eleme 1 vagy -1 , illetve HH^T diagonális, vagyis minden sor merőleges a többi sorra.

A HH^T -t ebben az esetben pontosan ismerjük: $HH^T = nId$. Ugyanis itt a főátló elemeiben négyzetösszegek szerepelnek 1 abszolút értékű számokból, vagyis n van mindenhol a főátlóban.

Az előző definíció általánosítható.

4.2. Definíció. [2] *Komplex Hadamard-mátrixok.* Minden eleme $z \in \mathbb{C}$, $|z| = 1$. Itt HH^* mátrixtól várjuk el, hogy diagonális legyen, ahol H^* a transzponált konjugáltját jelöli.

4.3. Állítás. Az Hadamard-tulajdonság zárt sorok és oszlopok cseréjére, illetve sorok és oszlopok $1, -1$ -gyel való szorzásra, valamint a transzponálásra.

Bizonyítás. A sorok és oszlopok cseréje után az adott sor/oszlop továbbra is csak önmagára lesz nem merőleges. Nemnulla skalárral való szorzás nem változtat azon a tulajdonságon, hogy két vektor merőleges-e.

$$0 = \langle a, b \rangle \Rightarrow \langle \lambda a, b \rangle = \lambda \langle a, b \rangle = 0.$$

Tehát ha egy a vektor merőleges egy másik b vektorra, akkor a merőleges $-b$ -re is. $\square$

Sorok és oszlopok cseréjével, ± 1 -gyel való szorzással lehet úgy átalakítani egy Hadamard-mátrixot, hogy az első sorban és oszlopban csupa 1-esek szerepeljenek. Ez a művelet egy ekvivalenciarelációt definiál a Hadamard-mátrixokon. Az átalakítást követően ugyanolyan alakú Hadamard-mátrixokat egy hasonlósági osztályba soroljuk. $n = 1, 2, 4, 8, 12$ -re egy hasonlósági osztály létezik, vagyis hasonlóság erejéig a mátrix egyértelmű.

Alább példák olvashatóak Hadamard-mátrixokra az osztály Reprezentánsával.

- $n=1$:

$$\mathbf{H}_1 = \begin{pmatrix} 1 \end{pmatrix}$$

- $n=2$:

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Ez a mátrix szimmetrikus, vagyis $\mathbf{H}\mathbf{H}^T = \mathbf{H}^2$.

- $n = 4$:

$$\mathbf{H}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

Észrevehetjük, hogy

$$\mathbf{H}_4 = \begin{pmatrix} \mathbf{H}_2 & \mathbf{H}_2 \\ \mathbf{H}_2 & -\mathbf{H}_2 \end{pmatrix}$$

Ez általánosságban is igaz: ha vesszük a tenzor szorzatát két Hadamard-mátrixnak, akkor az eredmény is Hadamard lesz.

Az előbbi példa pont a $H_2 \otimes H_2$.

4.4. Állítás. [18] Egy $H \otimes H_2$ mártix Hadamard, ha H $n \times n$ -es tetszőleges Hadamard, H_2 pedig a 2×2 -es Hadamard-mátrix.

Bizonyítás.

$$\mathbf{H}_{uj} = \begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$$

Ha veszünk két tetszőleges oszlopvektort innen, akkor az első n koordinátában 0 a skalár szorzatuk, és a második n -ben is, függetlenül attól, hogy szoroztuk-e -1 -gyel. Ha veszünk két különböző vektort az első H oszlopaiból, azok továbbra is merőlegesek lesznek egymásra. Ha vesszük bárhol ugyanazt a két oszlopot, akkor azok skaláris szorzata $2n$ lesz. Ha veszünk egy vektort az első H oszlopaiból és egy másikat a második H oszlopaiból, akkor az továbbra is merőleges lesz, mert H merőleges $-H$ -ra. Ha vesszük ugyanazt a vektort az első H oszlopaiból és a második H oszlopaiból, akkor azok merőlegesek lesznek, hiszen $n + (-n) = 0$. $\square$

Ezek alapján végtelen sok Hadamard-mátrix létezik, de nem csak ezzel a módszerrel lehet Hadamard-mátrixokat generálni.

Lényegi részét képi a valós Hadamard mátrixoknak a méret kérdése. Korábban már említettem, hogy minden valós Hadamard-mátrix ekvivalens egy olyan mátrixszal, amelynek az első sora csupa 1-es. Az, hogy merőleges rá a második sor, azt jelenti, hogy $\frac{n}{2}$ darab 1-es, és $\frac{n}{2}$ darab -1 -es van a második sorban, vagyis n páros. Az viszont, hogy a harmadik sor merőleges a második sorra, azt jelenti, hogy az $\frac{n}{2}$ darab egyes alatt van $\frac{n}{4}$ 1-es és $\frac{n}{4}$ -1 -es, ugyanígy az $\frac{n}{2} - 1$ -essel. Innen következik a következő állítás:

4.5. Állítás. [5] $n = 1, 2$ kivételével minden valós Hadamard-mátrix mérete osztható négygyel.

4.6. Sejtés. [5] Hadamard-sejtés. Minden $n \in 4\mathbb{N}$ számra létezik-e valós $n \times n$ -es Hadamard-mátrix. Ez az úgynevezett Hadamard-sejtés (Hadamard Conjecture - HC).

A HC komplex esetben egy megoldott probléma, ekkor ugyanis minden $n \in \mathbb{N}$ -re létezik komplex Hadamard-mátrix [2]. Egy példa ezekre az úgynevezett Fourier-mátrixok: $F_N = (\omega^{ij})_{ij}$, ahol $\omega = e^{\frac{2i\pi}{n}}$.

A következő állítás a szimmetrikus Hadamard-mátrixok sajátértékeiről szól: szimmetrikus esetben igen egyszerű ezt meghatározni.

4.7. Állítás. [18] Ha H szimmetrikus, akkor H sajátértékei $\pm\sqrt{n}$.

Bizonyítás. Mivel H szimmetrikus, ezért

$$HH^T = H^2 = n \cdot Id.$$

Tegyük fel, hogy H -nak sajátértéke λ , v sajátvektorral. Ekkor

$$H^2v = H(Hv) = H(\lambda v) = \lambda(Hv) = \lambda(\lambda v) = \lambda^2v.$$

Mivel $n \cdot Id$ -nek csak az n a sajátértéke, ezért H -nak a $\pm\sqrt{n}$ lehet. $\square$

Míg az előző állítások csak az Hadamard-mátrixok méretéről szóltak, a következő a ciklikus Hadamard-mátrixok méretéről szól.

4.8. Állítás. [19] Csak $n = 4u^2$ méretű valós ciklikus Hadamard-mátrix létezik, ahol u páratlan, és nem egy prímszám.

5. Ciklikus mátrixok

A ciklikus mátrixokat a 3.13-as definícióban definiáltuk. Szórol szóra ugyanaz a definíció:

5.1. Definíció. *Ciklikus mátrix.* Egy A $n \times n$ -es mátrix ciklikus, ha $A_{ij} = u_{j-i}$, ahol $u \in \mathbb{T}^n$ vektor, és a $j - i$ index modulo n van számolva.

Példa ciklikus mátrixra egy Cayley-gráf adjacencia mátrixa. Legyen most a $G = \mathbb{Z}^5$ és $S = \{2; -2\}$. Ebből a következő adjacencia mátrix generálódik:

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Ezen látszódik, hogy ciklikus. Amennyiben $S = \{1; -1\}$, akkor a Cayley-gráfunk egy kör, ami ha $G = \mathbb{Z}^n$ -ben n páratlan, akkor izomorf a fenti $S = \{2; -2\}$ esettel.

Egy ciklikus mátrix sajátértékei és sajátvektorai meghatározhatóak a generátorvektorából. Ha csak annyit tudunk a mátrixról, hogy ciklikus, a sajátvektorok akkor is ismertek:

5.2. Állítás. [20] Egy ciklikus mátrix sajátvektorai a $v_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})$ vektorok $j = 0, 1, \dots, n-1$ -re, ahol $\omega = e^{2i\pi/n}$, vagyis az n -edik primitív egységgyökök.

Bizonyítás. Ha $u = (u_0, u_1, \dots, u_{n-1})$ egy vektor, és egy C ciklikus mátrix, akkor $Cu = y$. Ha kibonjuk az y -t: $y_0 = u_0c_0 + u_1c_1 + \dots$; $y_1 = u_0c_{n-1} + u_1c_0 + \dots$ $y_k = u_0c_{0-k} + u_1c_{1-k}$, ahol $i - j$ index modulo n van számolva. Vagyis $y_k = \sum u_i c_{i-k}$, ahol az indexek továbbra is modulo n .

Legyen u_j egy sajátvektor, vagyis $u_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})$. Ekkor y_k a következőképp áll elő:

$$y_k = \sum_{i=0}^{n-1} c_{i-k} \omega_n^{ij}.$$

Ebből a szummából kiemelve ω_n^{kj} -t a következő kifejezést kapjuk:

$$y_k = \omega_n^{kj} \sum_{i=0}^{n-1} c_{i-k} \omega_n^{(i-k)j}.$$

Ez a szumma már független a k -tól, ugyanis ez csak egy ciklikus eltolása az összeadásnak, vagyis csak a tagok sorrendjét változtattuk meg. A szummán kívül pedig pont az a vektorelem áll, amit most vizsgálunk, vagyis ez tényleg egy sajátvektor. $\square$

Az előző bizonyításban sokkal több minden jött ki, mint amit eredetileg szeretnünk volna, ugyanis a bizonyítás alapján tudjuk a sajátértékeket is:

$$\sum_{i=0}^{n-1} c_i \omega_n^{ij}.$$

Tehát a generáló vektorból direkt számolhatóak a sajátértékek.

A fent említett Hadamard-mátrixokkal való kapcsolata a ciklikus mátrixoknak a következő sejtés:

5.3. Sejtés. [17] *CHC (Circulant Hadamard Conjecture)*. $n = 4$ -nél nagyobb n -ekre nem létezik valós ciklikus Hadamard-mátrix.

$n = 4$ -re létezik:

$$H_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

Ennél nagyobb ciklikus Hadamard mátrix nem létezik, és ekvivalencia erejéig ez az egyetlen 4×4 -es, mivel 4×4 -es H mátrixok egyértelműek. Ennél kisebb már csak a triviális 1×1 -es illetve 2×2 -es H mátrixok ciklikusak.

A fent említett H_4 ciklikus és szimmetrikus Hadamard, vagyis a sajátértékeinek egyszerre kell megfelelnie a ciklikus mátrixok és a szimmetrikus Hadamard-mátrixoknál kiszámolt értékeknek. A szimmetrikus Hadamard számolása annyit mond meg, hogy a sajátértékek 2 és -2 valamilyen multiplicitással. A ciklikusságból

az következik, hogy: jelen esetben legyen $\omega = i$, mivel i egy 4-edik primitív egységgyök. Ekkor a négy sajátvektor a következő: $v_1 = (1, 1, 1, 1)$; $v_2 = (1, i, -1, -i)$; $v_3 = (1, -1, 1, -1)$; $v_4 = (1, -i, -1, i)$. A hozzájuk tartozó sajátértékek pedig $2, -2, -2, -2$ ugyanebben a sorrendben. Tehát ez a mátrix tényleg teljesíti mindkét mátrixosztály által meghatározott feltételeket.

6. Cayley-gráfok

Amennyiben az A csoport ciklikus, úgy a belőle generált Cayley-gráfok is ciklikusak. Ha egy Cayley-gráf ciklikus, akkor a (súlyozott) adjacencia-mátrixa is ciklikus. A korábban definiált fogalmak és kimondott állítások alapján ismerjük a sajátértékeit a ciklikus mátrixoknak. Ezeken kívül még Babai [1] és Lovász [13] a következőt mondták ki Cayley-gráfok sajátértékeiről:

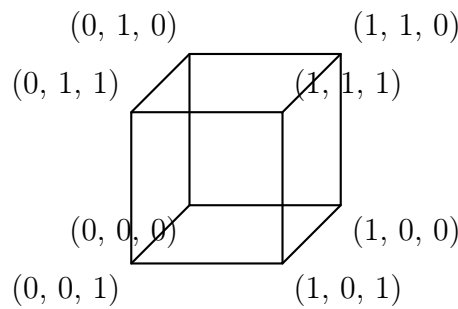
6.1. Tétel. [1] Egy A Abel-csoport színezett Cayley-gráfjának, $Cay(A, \alpha)$ -nak a spektruma:

$$\lambda_i = \sum_{g \in A} \alpha(g) \chi_i(g)$$

minden $i = 0 \dots n$ -re.

6.2. Állítás. [7] Amennyiben egy $Cay(G, S)$ Cayley-gráf S generátorhalmaza zárt az inverzképzésre, vagyis $\forall s \in S \Rightarrow s^{-1} \in S$, akkor az a Cayley-gráf irányítatlan.

6.3. Példa. Legyen $G = \mathbb{Z}_2^k$, $S = (e_1, e_2, \dots, e_k)$, ahol e_i a csupa 0 vektor, kivéve az i -edik helyen, ahol 1-es. Ez a halmaz a k dimenziós egységkockát generálja Cayley-gráfként. Itt minden elem önmagának az inverze, ugyanis koordinátáinként $0 + 0 = 0, 1 + 1 = 0$ modulo 2. Ezt így tudjuk ábrázolni $k = 3$ esetben:



7. Diszkrét Pompeiu-probléma

Ebben a szekcióban egy merően más témáról fogok írni, amelyről később kiderül, hogy nagyon szorosan kapcsolódik a fent leírtakhoz.

Pompeiu [16] eredetileg a következő kérdést tette fel:

7.1. Kérdés. [16] Legyen K kompakt, pozitív Lebesgue-mérhető halmaz. Igaz-e, hogy ha egy $f : \mathbb{R}^2 \rightarrow \mathbb{C}$ folytonos függvényre igaz, hogy

$$\int_{\sigma(K)} f(x, y) d\lambda_x d\lambda_y = 0,$$

ahol $\sigma(K)$ K egy távolságtartó transzformációja, és ez igaz $\forall \sigma(K)$ -ra, akkor ebből következik, hogy $f \equiv 0$, vagyis f a konstans 0 függvény?

Ezt a fenti kérdést lehet diszkretizálni a következő módon:

7.2. Definíció. [11] Legyen $S \subseteq A$, $S \neq \emptyset$, ahol A egy Abel-csoport, és S véges. Azt mondjuk, hogy S -nek van diszkrét Pompeiu-tulajdonsága, ha egy $f : A \rightarrow \mathbb{C}$ függvényre igaz, hogy

$$\sum_{s \in S} f(x + s) = 0$$

minden $x \in A$ -ra, akkor f azonosan 0.

Azt mondjuk, hogy S nem Pompeiu-halmaz f -re nézve, ha létezik $f \neq 0$, ami kielégíti a fenti egyenletet.

7.3. Definíció. [11] *Súlyfüggvény.* Legyen A egy Abel-csoport. Ekkor súlyfüggvénynek hívunk egy $w : A \rightarrow \mathbb{Z}_0^+$ függvényt.

Megjegyzés: ez a függvény képezhet $\mathbb{Q}$ -ba vagy $\mathbb{Z}$ -be is.

A következő definíció összekapcsolja az előbb bevezetett fogalmakat:

7.4. Definíció. [11] *Pompeiu súlyfüggvény.* Legyen $w : A \rightarrow \mathbb{Q}$ súlyfüggvény. Azt mondjuk, hogy w Pompeiu súlyfüggvény, ha bármely $f : A \rightarrow \mathbb{C}$ függvényre igaz, hogy

$$\sum_{s \in S} w(s) f(x + s) = 0$$

minden $x \in A$ -ra, akkor abból f azonosan 0 következik. Azt mondjuk, hogy w nem Pompeiu-súlyfüggvény f -re nézve, ha létezik $f \neq 0$, ami kielégíti a fenti egyenletet.

Végig lehet gondolni, hogy az előző definícióban a w a $\mathbb{Q}$ -ba képez. Észrevehetjük, hogy ha w -t megszorozzuk egy racionális számmal, attól még a Pompeiu tulajdonsága nem fog változni. Vagyis felszorozhatjuk úgy, hogy w csak egész értékeket vegyen fel.

A legegyszerűbb súlyfüggvény, amit vizsgálhatunk, az 1_S karakterisztikus függvény. Vegyünk egy speciális esetet:

Legyen A Abel-csoport, legyen $S \subseteq A$. Legyen most $\Gamma = \text{Cay}(A, S)$. Ebből meghatározható $\text{Adj}(\Gamma)$, ami Γ adjacencia-mátrixa. $\text{Adj}(\Gamma)$ csúcshalmaza Γ csoport elemei. Ekkor

$$Adj(a, s) = \begin{cases} 1 & \text{ha } a \in A \text{ és } as \in S, s \in S, \\ 0 & \text{különben.} \end{cases}$$

7.5. Tétel. [11] Legyen A egy n elemű Abel-csoport, legyen $S \subseteq A$, legyen $f : A \rightarrow \mathbb{C}$ függvény, $w : A \rightarrow \mathbb{Q}$ súlyfüggvény, $t \in A$ tetszőleges. Ekkor

$$\sum_{a \in A} f(a)w(a+t) = 0 \iff Adj(\Gamma)g = 0$$

ahol $Adj(\Gamma)$ a $Cay(A, S)$ adjacencia-mátrixa, $g = (f(a_1), f(a_2), f(a_3) \dots f(a_n))$, ahol $a_i \in A$.

Ez a tétel itt van először ebben a formában kimondva, de Kiss-Malikiosis-Somlai-Vizer [11] cikk több helyen implicit módon használja.

7.6. Megjegyzés. Vegyük észre, hogy a 7.5 tétel azt mondja ki, hogy ha van egy w nem-Pompeiu súlyfüggvényünk, amit f tanúsít, akkor az ekvivalens azzal, hogy $Cay(A, S)$ adjacencia mátrixának g egy nemnulla sajátvektora 0 sajátértéssel. Ugyanakkor, ha megvizsgáljuk az ekvivalencia (7.5) bal oldalát is, a következőt vesszük észre: $\langle f, w_t \rangle = 0$. Vegyük észre, hogy itt az $w = 1_S$, vagyis ez egy egyszínű Cayley-gráf.

Ha a Cayley-gráfunk súlyozott (színezett), akkor a súlyok kerülnek az adjacencia mátrixba, és az alábbi tétel áll fenn:

7.7. Tétel. [11] Legyen A Abel-csoport, legyen $S \subseteq A$, legyen $f : A \rightarrow \mathbb{C}$ függvény, $w : A \rightarrow \mathbb{Q}$ súlyfüggvény, $t \in A$ tetszőleges. Ekkor

$$\sum_{a \in A} f(a)w(a+t) = 0 \iff Adj_w(\Gamma)g = 0,$$

ahol $Adj_w(\Gamma)$ a $Cay(A, S)$ adjacencia-mátrixa w súlyokkal, és g következőképp néz ki:

$$g = (f(a_1), f(a_2), f(a_3) \dots f(a_n)),$$

ahol $a_i \in A$.

Legyen χ_v egy karakter. Babai [1] és Lovász [13] eredménye alapján ismerjük a sajátértékeket a ciklikus Cayley-gráfoknak. Babaival [1] ellentétben itt nem $\alpha(a)$ -val jelöljük a színezőfüggvényt, hanem $w(a)$ -val. Ekkor a ciklikus Cayley-gráf sajátértékei minden χ_v -re:

$$\sum_{a \in A} \chi_v(a)w(a).$$

Mi innentől az $A = \mathbb{Z}_2^n$ elemi Abel-csoportot fogjuk vizsgálni. Legyen $\chi_v : A \rightarrow C^*$ karakter. Ekkor minden $v \in A$ -ra:

$$\chi_v(a) = \exp\left(\frac{2\pi i}{2}\langle a, v \rangle\right) = (-1)^{\langle a, v \rangle}.$$

Vagyis minden $v \in \mathbb{Z}_2^n$ -re megkapjuk a Cayley-gráf egy sajátértékét:

$$\sum_{a \in \mathbb{Z}_2^n} (-1)^{\langle a, v \rangle} w(a).$$

Pompeiu [16] - vagyis pontosabban Kiss-Malikiosis-Somlai-Vizer [11] kérdése pont az volt, hogy ez az összeg lehet-e 0 valamilyen v -re.

Észrevehetjük, hogy az $(-1)^{\langle a, v \rangle}$ két értéket vehet fel: ± 1 . Vagyis az érték 1, ha u és v merőleges egymásra $\mathbb{Z}_2^n$ vektortérben; -1 , ha nem merőlegesek. Tehát:

$$\sum_{a \in \mathbb{Z}_2^n} (-1)^{\langle a, v \rangle} w(a) = \sum_{\substack{a \in \mathbb{Z}_2^n \\ a \perp v}} w(a) - \sum_{\substack{a \in \mathbb{Z}_2^n \\ a \not\perp v}} w(a).$$

Ha $v \neq 0$, hiszen a 0-vektorra minden vektor merőleges, akkor a következő formula:

$$\sum_{\substack{a \in \mathbb{Z}_2^n \\ a \perp v}} w(a) = \sum_{\substack{a \in \mathbb{Z}_2^n \\ a \not\perp v}} w(a).$$

Tehát jelen esetben Pompeiu kérdése a következő: Létezik-e olyan $v \in \mathbb{Z}_2^n$, hogy a v -re merőleges hipersík pont felezi a súlyfüggvényt?

7.1. Matolcsi Máté súlyfüggvénye

Mi a számunkra fontos súlyfüggvényt Matolcsi Máté [14] cikkéből nyerjük ki. Matolcsi csupán egy egyenletrendszerrel írt fel, aminek a kapcsolatát a Pompeiu-problémával évekkel később ismerték fel a Kiss-Malikiosis-Somlai-Vizer [11] cikke alapján. Matolcsi [14] arra használta, hogy új bizonyítást 4.8-re.

A súlyfüggvény definíciója az alábbi formulából nyerhető ki:

$$\sum_{d=1}^{n-1} \left(\sum_{j=0}^{n-1} u_j u_{j+d} \right)^2,$$

ahol $j + d \bmod n$ -ben van számolva. A súlyfüggvény $w : \mathbb{Z}_2^n \rightarrow \mathbb{N}$, és minden $v \in \mathbb{Z}_2^n$ -re az értéke az, hogy a felső összegből a koordinátákban szereplő 1-esek hányféleképpen jöhetnek ki. Az u_i változókat elképzelhetjük, mint a $\mathbb{Z}_2^n$ vektortér generátorai, azaz ezek másodrendű elemek. A négyzetük így a multiplikatív csoport

egységeleme, vagyis 1. Mivel később ezt egy Abel-csoportként kezeljük, ahol affin hipersíkokat vizsgálunk majd, az egységelemre nullaként és a $\mathbb{Z}_2^n$ elemeire vektorokként hivatkozunk, amik között az összeadás lesz a művelet. Amíg az u_i betűket használjuk, a műveletet szorzásként írjuk.

A formulából $u_i u_j u_k u_l$ négyes szorzatok jönnek ki. Itt ha két u -nak az értéke megegyezik, akkor fent említett négyzetemelés miatt kiesnek, vagyis a négyesből kettes, kettesből nullás lesz. Ezt úgy is lehet megfogalmazni, hogy mivel a rendje 2, ezért a négyzete 1. Ez azt jelenti, hogy minden pontnak, amelynek 1, 3 vagy 5-nél több 1-e van a koordinátaiban, azoknak a súlya 0, vagyis csak a 0, 2, 4 darab egyes-sel rendelkező vektoroknak lehet súlya. Matolcsi [14] cikke alapján Kiss, Matolcsi és Somlai belátta a következőt ¹.

7.8. Állítás. *A Matolcsi-féle súlyfüggvényre a Pompeiu-probléma és a ciklikus Hadamard sejtés (CHC) ekvivalens.*

Mivel a CHC és a Pompeiu-probléma ennél a súlyfüggvénynél ekvivalens, ezért feltehetjük, hogy n osztja 4-et.

Megkérdezhetjük, hogy mik a konkrét súlyok.

7.1.1. Konkrét súlyok

Amennyiben formális összegeket képezünk az u_j változók szorzataiból, vagyis kiszámoljuk, hogy melyik vektor milyen súllyal szerepel $\mathbb{Z}_2^n$ -ben, akkor ezek az együtthatók nem negatív egész számok, és akkor a rendszer súlya az egy ilyen formális összeg súlya, vagyis az együtthatók összege.

7.9. Állítás. *Az egész rendszer súlya $n^2(n-1)$.*

Bizonyítás. Direkt leszámolással a Cauchy-szorzatból (7.1). Minden 4-es egy súlyt ad valamelyik vektorhoz, és a belső szumma n^2 súlyt ad, a külső ezt megismétli $n-1$ -szer. A belső szumma $u_i u_j u_k u_l$ alakú, ez pont az i, j, k, l indexekkel szereplő vektorhoz ad súlyt, természetesen a négyzetre emelések után. Vagyis az összsúly $n^2(n-1)$. $\square$

7.10. Állítás. ² *A 0-vektor súlya n^2 .*

Bizonyítás. Vizsgáljuk meg, hogy a 0-vektor hányféleképp jöhet ki. 0-vektor akkor jön létre, ha minden u_i kiesik. Lefixált d -vel minden u_j -hez pont a másik u_j tartozik: $u_j u_{j+d} u_j u_{j+d}$. Van ebből n darab minden d -re, vagyis ez fed $n(n-1)$ súlyt. Viszont van egy különleges eset, a $d = \frac{n}{2}$. Ekkor minden j -re a fentiek mellett a következő

¹Somlai Gábor, mint témavezetőm informált róla, hogy ez az eredmény nem jelent meg sehol.

²Saját eredmény.

lesz igaz: $u_j u_{j+d} u_{j+d} u_j$ is 0-t ad, mivel $u_j = u_{j+2d} = u_{j+n}$. Ebből n darab van, és csak a $d = \frac{n}{2}$ esetben, vagyis a 0 vektor súlya $n(n-1) + n = n^2$. $\square$

7.11. Állítás. ³ Minden olyan vektornak, amiben 2 egyes van, egymástól páros távolságra a súlya 8, különben 0.

Bizonyítás. Legyen d rögzített: d lefixálásával az összegben szereplő távolságot rögzítjük. Ekkor két egyes csak akkor jöhet ki, ha $u_j u_{j+d} u_{j+d} u_{j+2d}$ alakban megadható a 4-es, ahol mindent mod n -ben számolunk. Ebből a $u_j u_{j+2d}$ kettes jön, amiből nyilvánvaló, hogy a távolságuk csak páros lehet.

Legyen most az index rögzítve: j, i , távolságuk $2l$. Hogy az indexek ne bonyolódjanak túl, a köztes, kieső pontot u_k -val jelölöm. Amennyiben találunk megfelelő i, j, k indexeket, akkor azok mindenképp 2 súlyt kapnak, mivel u_i, u_k, u_k, u_j -ből jön egy, és u_k, u_j, u_i, u_k -ból jön a másik, mivel szimmetrikus. Számoljuk le, hogy mik lehetnek a köztes pontok! Feltehetjük, hogy $i < j$, ekkor a köztes pont lehet i és j között, vagyis $i < k_{bel} < j$, vagy lehet "kívül" vagyis vagy $j < k_{kul}$ vagy $k_{kul} < i$. Az egyértelmű indexek (olvashatóság miatt a k lemarad, csak a "kul / bel" maradt): $u_j u_{bel} u_{bel} u_i$. A második esetben $u_i u_{kul} u_{kul} u_j$. Ezeket meg lehet ismételni úgy, hogy kul-t kicseréljük bel-re és fordítva. Vagyis minden ilyen vektornak $4 \cdot 2 = 8$ súlya van. $\square$

Feltehetjük a kérdést, hogy hány darab ilyen vektorunk van. Ha rögzítünk egy indexet, akkor hozzá $\frac{n}{2} - 1$ másik index jó. Indexből n darab van, de mindent kétszer számoltunk, vagyis $\frac{n}{2} (\frac{n}{2} - 1)$ darab két egyessel rendelkező vektorunk van, aminek van súlya is. Ezek összesen $8 \cdot \frac{n}{2} (\frac{n}{2} - 1) = 2n^2 - 4n$ súlyt fednek le. Láthatjuk, ezek alapján, hogy a súlyok igen nagy része a 4 egyessel rendelkező vektorokba esik.

7.12. Állítás. ⁴ Legyenek az indexekre igazak a következők:

- $0 \leq i < j < k < l < n$;
- $k - i = l - j$;
- $k - i = l - j = \frac{n}{2}$

Ekkor az ezeken az indexeken 1-et, mindenhol máshol 0-t felvevő vektor súlya 16.

Amennyiben az utolsó feltétel nem igaz rá, a súlya csak 8.

Bizonyítás. Egyszerűbb a 8 súlyú bizonyítással kezdeni. Rögzíthetjük az első indexet 0-ba, hiszen az egész forgatásinvariáns. Most nem próbáljuk leszámolni őket, csak

³Saját eredmény.

⁴Saját eredmény.

megvizsgálni. Ebben az esetben első index b , második $b + c$, a harmadik index $b + c + b$, ahol $c + 2b < n$. Amennyiben $c + 2b$ túlcsordul, azt máshol fogjuk vizsgálni. Ezt a négyest tudja produkálni a $d \in \{b, b + c, n - b, n - (b + c)\}$. Ezek mindegyike 2 súlyt ad, hasonló módon mint a két egyessel rendelkező vektorok. Szépen kiírva az indexnégyesek a $0, i, j, k$ jelölést használva $0 < i < j < k < n$:

- $0, i, j, k$
- $0, j, i, k$
- $i, 0, k, j$
- $j, 0, k, i$

Akkor, ha tudjuk, hogy $j = \frac{n}{2}$ következik, hogy $k - i = \frac{n}{2}$. Az előző 4-esek továbbra is igazak, ezen felül jönnek még be a következő négyesek:

- $0, k, j, i$
- $k, 0, i, j$
- $0, j, k, i$
- $j, 0, i, k$

A négy indexet $4!$ módon rendezhetjük sorba, de mivel az első kettő a második kettővel felcserélhető (ugyanazt az esetet adják), ezért csak 12 különböző eset van. Tehát a fenti eseteken kívül még leszámoljuk, hogy a maradék négy index-sorozat sehogyan sem jöhet ki.

- $0, i, k, j$: $k - j$ távolsága ebben az irányban szigorúan nagyobb mint $0 - i$ távolsága, mivel k -től el kell jutni 0 -ba, majd 0 -ból i -be majd i -ből j -be, ami szigorúan nagyobb, mint 0 -ból i -be.
- $i, 0, j, k$: Ugyanaz, mint az előbb
- $0, k, i, j$: Ugyanaz, mint az előbb
- $k, 0, j, i$: Ugyanaz, mint az előbb

Ez az összes súly. □

A 16 súlyúakat le tudjuk számolni direkt módon. Mivel egy feltétele annak, hogy 16 legyen a súlya, hogy a szemközti elemek $\frac{n}{2}$ távolságra legyenek, ezért minden ilyen le tudunk generálni azzal, hogy a $[0, \frac{n-2}{2})$ intervallumból választunk két elemet, amit megtehetünk $\binom{\frac{n-2}{2}}{2}$ módon, vagyis az összsúlyuk $16 \binom{\frac{n-2}{2}}{2}$.

Tehát eddig láttunk $n^2 + 2n^2 - 4n + 16\binom{\frac{n-2}{2}}{2}$ súlyt az $n^3 - n^2$ súlyból. A maradék súly az „általános” helyzetű négyesekből adódik. Vagyis

$$n^2 + 2n^2 - 4n + 16\binom{\frac{n-2}{2}}{2} + MAR = n^3 - n^2.$$

Ez átrendezve:

$$n^3 - 6n^2 - 16n - 16 = MAR.$$

Ezen a összegben meg kell vizsgálnunk, hogy osztható-e 8-cal. Ez az összeg valóban osztható 8-cal, mivel a tagok egyenként is oszthatóak 8-cal (n páros).

A következő állítás saját eredmény, saját ötletből született, és a bizonyítás is saját. Azt vizsgáljuk meg, hogy abban a vektorban, amelyre merőleges hipersíkot szeretnénk állítani, hány egyes szerepelhet.

7.13. Állítás. ⁵ Amennyiben a vektorban legfeljebb $\frac{n}{65}$ darab 1-es van, akkor arra merőleges hipersík sosem felezi a súlyfüggvényt.

Bizonyítás. Adok egy nagyon durva felső becslést a megőleges altér eltoltjának a súlyára, és belátom, hogy ez is kisebb, mint a súlyfüggvény fele.

Legyen v vektor, amiben tetszőleges helyen legyen k darab 1-es. Ahhoz, hogy egy vektor súlya az eltolt altér súlyához számítson, az kell, hogy páratlan sok helyen legyen ugyanott 1-es. Mivel tudjuk, hogy csak olyan vektoroknak van súlya, amelyekben 2 vagy 4 darab 1-es szerepel, ezért tudjuk, hogy elég a páratlansokaságból az 1-et és a 3-at vizsgálni. Először vizsgáljuk meg azt, amikor egy egyes egyezik v -vel. Becsüljük felül a 2 egyessel rendelkező vektork súlyát az eltolt altérben: $8k(n-k)$. A k egyesből k -féleképp választhatunk, hozzá $n-k$ -féleképp jöhet a másik egyes, hogy legyen 8 súly, szóval ezeket sikeresen felülbecsültük.

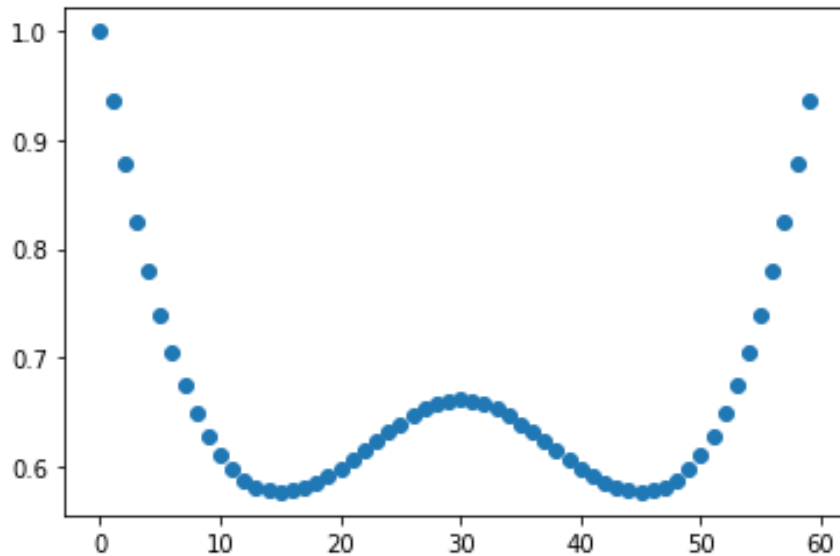
Becsüljük most felül a 4 egyessel rendelkező vektorokat: $16 \cdot 4 \cdot k\binom{n-k}{2}$. A k darab egyesből k -féleképp választhatunk ki egyet, a maradékból először $\binom{n-k}{2}$ -féleképp kiválasztunk két egyest, majd ehhez a háromhoz legfeljebb négy helyen lehet a negyedik egyes, hogy lehessen súlya, és akkor becsüljük a legszebben felül, ha 16 súlyt adunk mindennek. Azért lehet csak négy helyen, mert három pont elhelyezkedése már meghatározza a lehetséges d értékeket. A másik eset, hogy 3 egyest választunk a k -ból. Ekkor is nagyon hasonló módon tudunk becsülni: $16 \cdot 4\binom{k}{3}$.

Legyen $k = \frac{n}{c}$ valamilyen c konstanssal! Ekkor a fenti kifejezések kibonthatóak és még tovább felülbecsülhetőek: $8\frac{n^2}{c} + 32\frac{n^3}{c} + 32\frac{n^3}{c^3}$. A kérdés, hogy ez mikor kisebb $\frac{1}{2}(n^3 - n^2)$ -nél. Ez algebrai átalakítások után 64-nél nagyobb c -k esetén igaz. Vagyis $c = 65$ jó választás, vagyis $\frac{n}{65}$ darab 1 esetén nem lehet felező. $\square$

⁵Saját eredmény.

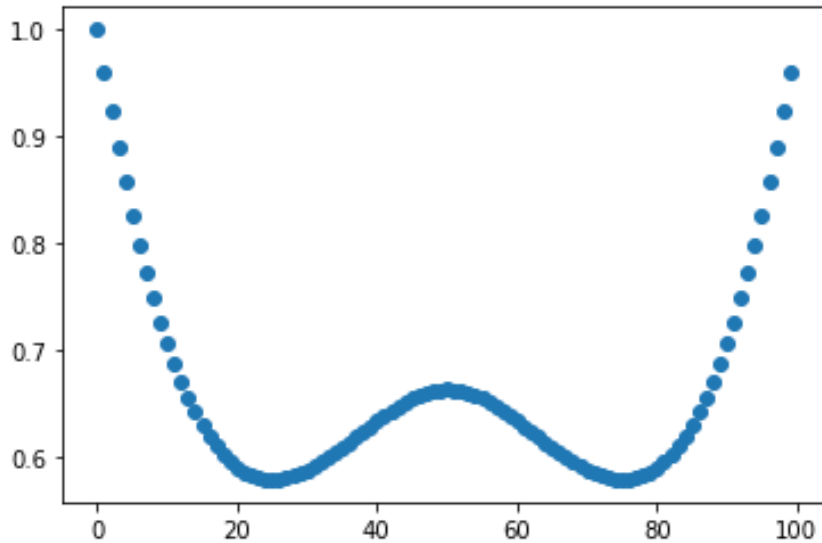
Felhívnom a figyelmet, hogy ez az állítás és ez a bizonyítás nagyon durva felső becslést alkalmazott. A sejtés az, hogy $\frac{n}{2}$ környékén létezhetnek a ténylegesen felező vektorok.

El lehet gondolkodni, hogy hogyan viselkedik a függvény a bővítésre ⁶: ha van egy v vektorunk, amelyre a merőleges alteret állítanánk, akkor hogyan viselkedik a súlyfüggvény, ha hozzáadunk/elveszünk egy egyest valahonnan. A későbbiekben bemutatott programkód alapján feltételezzük, hogy ez nem monoton. A legegyszerűbb bővítés a következő: mindig a soron következő egyest vegyük be a 0-vektorból indulva. Ekkor a merőleges altér súlya $\frac{n}{4}$ -ig csökken, majd $\frac{n}{2}$ -ig nő, utána megint csökken $\frac{3n}{4}$ -ig, majd megint nő n -ig. Vagyis az $f(k) :=$ 'az első k darab 1-es, a többi 0' függvény nem globálisan monoton, vannak lokális maximumjai, minimumjai. A következő ábrák a merőleges altér súlyának arányát mutatják $n = 60$ illetve $n = 100$ esetben.



1. ábra. $n = 60$ eset

⁶Ez az állítás a következő szekcióban leírt program eredményei, tehát saját eredmény.



2. ábra. $n = 100$ eset

Az ábrák nagyon hasonlítanak egymásra, amiből arra lehet következtetni, hogy állandó az arány. Szépen látszanak a lokális minimum és a lokális maximum helyek.

7.2. A súlyfüggvény megvalósítása számítógép segítségével.

A következőkben egy olyan programot fogok bemutatni, amit én írtam a súlyfüggvényre, illetve a hozzá tartozó számításokra.. A program maga kis n -ekre ($n = 200$ -ig) kiszámolja a teljes súlyfüggvényt, illetve ha adunk neki egy n hosszú v vektort, kiszámolja a v -re merőleges altér súlyát. Hogy összehasonlítható legyen a felezéssel, ezért ha a súlyt leosztjuk az összsúllyal, akkor pont a százalékos súlyarányt kapjuk. Ezt az arányt láthattuk az előző szekcióban. A program Python nyelven volt írva, Python 3.7.10 verzión. A programhoz a következő csomagok kellenek:

- `from collections import Counter`
- `import random`, ha véletlen vektorokat szeretnénk tesztelni.

Programleírás:

```

def uni_e(x):
    return tuple(sorted(tuple([key for key, val in Counter(x).items() if val == 1])))

def súlyfgv(n):
    vegsuly = []
    for d in range(1, n):
        súlyok = []
        for i in range(n):
            súlyok.append([i, (i+d)%n])
        súly1 = súlyok
        súly2 = súlyok
        for e in súly1:
            for f in súly2:
                vegsuly.append(uni_e(e+f))
    return dict(Counter(vegsuly))

```

Ez a kód felel a súlyfüggvény generálásához. Minden n -re visszaad egy szótárat, amelynek a kulcsai a vektorokban szereplő egyesek indexei, a hozzájuk tartozó értékek pedig a vektor súlya. A súlyfüggvény szótár következő módon néz ki $n = 60$ esetben:

```

{(): 3600,
 (0, 2): 8,
 (0, 1, 2, 3): 8,
 (0, 1, 3, 4): 8,
 (0, 1, 4, 5): 8,
 (0, 1, 5, 6): 8,
 (0, 1, 6, 7): 8,
 (0, 1, 7, 8): 8,
 (0, 1, 8, 9): 8,
 (0, 1, 9, 10): 8,
 (0, 1, 10, 11): 8,
 (0, 1, 11, 12): 8,
 (0, 1, 12, 13): 8,
 (0, 1, 13, 14): 8,
 (0, 1, 14, 15): 8,
 (0, 1, 15, 16): 8,
 (0, 1, 16, 17): 8,
 (0, 1, 17, 18): 8,
 (0, 1, 18, 19): 8,

```

Ez csak a kezdeti pár sora a szótárnak. Látható, hogy $()$, vagyis a 0 darab 1-es,

vagyis a 0-vektor súlya pont $60^2 = 3600$. A program később ezt a szótárat fogja megkapni egy bemeneti paraméterként.

7.14. Definíció. [8] *Ordo.* Legyenek f és $g : \mathbb{N} \rightarrow \mathbb{R}_0^+$ függvények. Azt mondjuk, hogy $f = \mathcal{O}(g)$, ha léteznek $n_0, c \in \mathbb{N}$ konstansok, hogy minden $n \geq n_0$ egészre $f(n) \leq c \cdot g(n)$.

Mivel ebben a szótárban a vektorok száma $\mathcal{O}(n^3)$, és ezeken az én algoritmusom végigiterál, ezért az az algoritmus, amely a súlyok eloszlását számolja ebben a megvalósításban nem lehet $\mathcal{O}(n^3)$ -nél gyorsabb. Kifejezetten hangsúlyozom, hogy ez erre a konkrét megvalósításra igaz csak, az én megoldásom igen nagy valószínűséggel szuboptimális.

A következő kódrészlet felel a merőleges altér kiszámítására:

```
def hadamard_vekt(n, vektor, a = a, b = b):
    m_alt_suly = 0
    for pont in b:
        if(len(pont)==0):
            m_alt_suly += a[()]
        else:
            skal = 0
            for k in range (len(pont)):
                if pont[k] in vektor:
                    skal = (skal + 1)%2
            if skal == 0:
                m_alt_suly += a[pont]
    return m_alt_suly
```

Ahol 'vektor' egy lista, amelyben különböző egész számok vannak, ezek a vektor indexei; 'a' a súlyfüggvényünk; 'b' a súlyfüggvény kulcsai, vagyis azok az indexek, amelyeknek súlya van. Ebben a programban vétett hiba miatt fedeztem fel a következő észrevételt:

7.15. Megfigyelés. Amennyiben a merőleges altérből az eltoltjába átrakjuk a 0-vektor súlyát, akkor találunk felező vektort. Amennyiben az egész súlyfüggvényből kivesszük a 0 súlyát, úgy találunk felező vektort.

Ezt az észrevételt véletlenvektor-generálással lehet megfigyelni: generálunk véletlen vektorokat, és kiíratjuk azokat, amelyek felezik. Egy példa $n = 60$ -ra, ahol a 0 súlya az eltoltban van, a lista feletti szám az arány, a lista alatti szám a 1-esek száma:

```
0.5
[3, 5, 7, 12, 16, 17, 19, 21, 23, 27, 30, 32, 33, 35, 37, 39, 40, 42, 44, 45, 51, 55, 56, 58, 59]
25
```


Egy példa $n = 60$ -ra, ahol a 0 súlya nincs a rendszerben:

[0, 3, 6, 8, 9, 11, 13, 14, 21, 22, 26, 28, 29, 32, 34, 35, 38, 39, 40, 42, 45, 51, 54, 55, 56, 57]
26

Matematikai értelme a hibás kód miatti felezésnek jelenleg nincsen, de érdekes jelenség. Ez alapján erősödik az a sejtésünk, hogy a 0-vektor súlya (n^2) miatt nincs egyenlőség.

Az eredeti verzió véletlenszerű vektoros tesztelésekor a tapasztalt minimális arány $n = 100$ -nál: 0.502602, a maximuma 0.509680, az átlag pedig 0.504969.

Hivatkozások

- [1] Babai, László. „Spectra of Cayley graphs.” *Journal of Combinatorial Theory, Series B* 27(2), (October 1979): 180–189
- [2] Banica, Teo. *Invitation to Hadamard matrices*. University of Cergy-Pontoise, 2010
- [3] Cati, Matteo; Pasechnik, Dmitrii. *A database of constructions of Hadamard matrices*. 2024
- [4] Conrad, Keith. *Characters of finite Abelian groups*, 2010
- [5] Hadamard, Jacques. *Résolution d’une question relative aux déterminants*, *Bull. Sci. Math.* 2 (1893): 240–246.
- [6] Izsák, Ferenc; Tarcsay, Zsigmond; Tüzes, Dániel: *Analízis jegyzetek I-III*. (2018)
- [7] Kelarev, Andrei. „On undirected Cayley graphs.” *Australasian Journal of Combinatorics*, 25, (2002): 73–78
- [8] Király, Zoltán. *Algoritmuselmélet*. Typotex Kft., 2014
- [9] Kiss, Emil. *Bevezetés az algebrába*. Typotex Kft., 2007
- [10] Kiss, Gergely; Laczkovich, Miklós. *Solutions to the discrete Pompeiu problem and to the finite Steinhaus tiling problem*. 2024
- [11] Kiss, Gergely; Malikiosis, Romanos Diogenes; Somlai, Gábor; Vizer, Máté. „On the discrete Fuglede and Pompeiu problems.” *Analysis and PDE*, 2019
- [12] Leung, Ka Hin, Schmidt, B.: „New restrictions on possible orders of circulant Hadamard matrices.” *Des. Codes Cryptogr.*, 64, 143–151 (2012)
- [13] Lovász, László. „Spectra of graphs with transitive groups.” *Period Math Hung* 6, (1975): 191–195.
- [14] Matolcsi, Máté. „A Walsh-Fourier approach to the circulant Hadamard conjecture.” *Algebraic Design Theory and Hadamard Matrices*; C. J. Colbourn (ed), *Springer Proceedings in Mathematics and Statistics*, 133, (2015): 201–208.
- [15] Mossinghoff, Michael. „Wieferich pairs and Barker sequences”. *Des. Codes Cryptogr.*, 53, (2009) 149–163.

- [16] Pompeiu, Dimitrie. „Sur une propriété intégrale des fonctions de deux variables réelles.” Bull. Sci. Acad. Roy. Belgique, 5(15), (1929): 265–269.
- [17] Ryser, Herbert John. Combinatorial Mathematics. Wiley, New York, 1963
- [18] Sylvester, James Joseph. „Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton’s rule, ornamental tile-work, and the theory of numbers.” The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 34(232), (1867): 461–475.
- [19] Turyn, Richard Joseph. „Character sums and difference sets.” Pacific J. Math. 15, 1965, 319–346 (1965)
- [20] Varga, Richard Steven. „Eigenvalues of circulant matrices.” Pacific Journal of Mathematics, 4(1), (March 1954)