

NORMAGRÁFOK GALOIS-GYŰRŰK FELETT

Vincze Erika

Matematikus MSc. II. évf.

Témavezető: Dr. Rónyai Lajos
egyetemi tanár
Algebra Tanszék,
BME Matematika Intézet

**BME
2012**

A dolgozat bemutatását a TÁMOP - 4.2.2.B-10/1–2010-0009 "Új tehetséggondozó programok és kutatások a Műegyetem tudományos műhelyeiben" című program támogatta.

Budapest, 2012.12.26.

Tartalomjegyzék

1. Bevezetés	3
2. A Hensel-felemelés	4
2.1. A $\mathbb{Z}_{p^s}$ gyűrű	4
2.2. A $\mathbb{Z}_{p^s}[x]$ polinomgyűrű	4
2.3. Alapvetően irreducibilis polinomok	5
3. Galois-gyűrűk	7
3.1. A Galois-gyűrűk egységeinek csoportja	8
3.2. A p -adikus reprezentáció	8
3.3. Galois-gyűrűk automorfizmusai	8
3.4. Norma és nyom	9
3.5. Abel-csoportok karakterei	10
3.6. Gauss-összegek Galois-gyűrű felett	11
4. A projektív normagráf és spektruma	13
4.1. A normagráf véges test felett	13
4.2. A normagráf a $GR(p^s, p^{sm})$ Galois-gyűrű felett	14
4.2.1. A projektív normagráf és szomszédossági mátrixa	14
4.3. Az M sajátértékei a $GR(2^2, 2^{2m})$ Galois-gyűrű esetén	16
5. A $GR(4, 16)$ Galois-gyűrű	18
5.1. A projektív normagráf	18
5.2. Eredmények a $GR(4, 16)$ Galois-gyűrű esetére	20
5.2.1. Az M^2 sajátértékeinek kiszámítása a sajátvektorok segítségével	20
5.2.2. Az eredmények bemutatása és ellenőrzése további számításokkal	21
6. Összefoglalás	26

1. Bevezetés

A Galois-gyűrűk a véges testek érdekes általánosításai: a modulo m egészek $\mathbb{Z}_m$ gyűrűjéből kaphatók egyszerű algebrai bővítéssel, ahol $m > 1$ prímszám. Prím m esetében éppen a véges testek adódnak. Az általános Galois-gyűrűk szerkezete bonyolultabb a véges testekénél, például nem triviális nilpotens elemeik is vannak. Az utóbbi időben több érdekes, a véges testekre alapozott diszkrét matematikai konstrukciót sikerült Galois-gyűrűkre támaszkodva általánosítani. Egyebek között a hibajavító kódok területén több ilyen konstrukció látott napvilágot. A jelen munka célja is egy ilyen általánosítás megfogalmazása és vizsgálata.

Alon, Rónyai és Szabó véges testek felett definiálták a projektív normagráfokat, amelyek több gráfelméleti extrémális probléma kapcsán bizonyultak hasznosnak. Ezt a konstrukciót általánosítjuk oly módon, hogy az eredetiben szereplő véges testbővítés helyett egy Galois-gyűrű Galois-bővítését, és a megfelelő normaleképezést használjuk.

Szabó eredményét általánosítva megmutatjuk, hogy ezen gráfok M adjacenciamátrixának spektruma kifejezhető (általánosított) Gauss-összegek segítségével. Itt természetesen Galois-gyűrűk feletti Gauss-összegek lépnek fel. Ezekről a tudomány mai állása szerint jóval kevesebb ismert, mint a véges testek feletti klasszikus Gauss-összegekről. Ennek megfelelően részeredményeket tudunk bizonyítani M sajátértékeinek nagyságáról. Itt elsősorban a legkisebbnek tekinthető új esettel foglalkozunk, amikor az alapgyűrű $\mathbb{Z}_4$.

A dolgozatban áttekintjük a későbbiekben használandó fogalmakat, illetve bizonyítás nélkül közöljük a szükséges tételeket. Bemutatásra kerülnek a Galois-gyűrűk, felépítésük, jellemzőbb tulajdonságaik. Bevezetjük a norma fogalmát, és az annak felhasználásával létrehozott normagráfot. Fő célunk a normagráf spektrumának (az M szomszédossági mátrix sajátértékeinek) vizsgálata. Ehhez Gauss-összegeket használunk.

A szükséges fogalmak bemutatása után a dolgozat második részében a $GR(2^2, 2^{2m})$ Galois-gyűrűkkel foglalkozunk, ahol $m > 1$. Itt bizonyítjuk Szabó Tibor sajátértékek abszolútértékéről szóló állítását test helyett Galois-gyűrű felett. A Gauss-összegekről meglévő ismereteink függvényében kiszámítjuk a szomszédossági mátrix sajátértékeit. Eredményünk az M mátrix sajátértékeire vonatkozó tétel, amely a sajátértékek abszolútértékét adja meg.

A dolgozatban végül a legkisebb érdekes $GR(2^2, 2^{2m})$ alakú Galois-gyűrű, a $GR(4, 16)$ felett konkrét számításokat mutatunk a karakterekre, illetve a Gauss-összegekre, ezzel is alátámasztva az általános esetre kapott eredményeket. Ezen felül a $GR(4, 16)$ Galois-gyűrűre kapott eredményeink nem csupán az abszolútértékekre vonatkoznak, hanem a sajátértékek pontos értékeit is megkapjuk, azok multiplicitásával együtt.

A Galois-gyűrűkre kapott saját eredmények a 4.2. és a 4.3. alfejezetben, a számítások az 5. fejezetben találhatók.

2. A Hensel-felemelés

2.1. A $\mathbb{Z}_{p^s}$ gyűrű

Ebben a szakaszban a $\mathbb{Z}_{p^s}$ gyűrűkkel, illetve a $\mathbb{Z}_{p^s}[x]$ -beli polinomokkal kapcsolatos alapvető tényeket foglaljuk össze. Legyen p tetszőleges prím, az s egy pozitív egész szám, $\mathbb{Z}_{p^s}$ a modulo p^s egészek gyűrűje, melynek egy reprezentáns rendszere

$$\mathbb{Z}_{p^s} = \{0, 1, 2, \dots, p^s - 1\}.$$

A p -hez relatív prím $a \in \mathbb{Z}_{p^s}$ elemek a gyűrű egységei.

2.1. Tétel. $\mathbb{Z}_{p^s}$ minden ideálja főideál, vagyis $\mathbb{Z}_{p^s}$ ideáljai: $(1), (p), (p^2), \dots, (p^{s-1})$. Ekkor (p) a $\mathbb{Z}_{p^s}$ egyetlen maximális ideálja, és $\mathbb{Z}_{p^s}/(p) \cong \mathbb{F}_p$, ahol $\mathbb{F}_p$ a p elemszámú véges test.

A $\mathbb{Z}_{p^s}$ gyűrű elemei kifejezhetők a következő alakban:

$$c_0 + c_1p + \dots + c_{s-1}p^{s-1},$$

ahol $0 \leq c_i \leq p - 1$.

A

$$\mathbb{Z}_{p^s} \longrightarrow \mathbb{F}_p$$

$$c_0 + c_1p + \dots + c_{s-1}p^{s-1} \longrightarrow c_0$$

leképezés gyűrűhomomorfizmus, amelyet a következőképpen jelölünk.

$$\overline{c_0 + c_1p + \dots + c_{s-1}p^{s-1}} = c_0.$$

A homomorfizmus magja természetesen a (p) ideál.

2.2. A $\mathbb{Z}_{p^s}[x]$ polinomgyűrű

A fenti $\mathbb{Z}_{p^s} \longrightarrow \mathbb{F}_p$ homomorfizmus kiterjeszthető a $\mathbb{Z}_{p^s}$ feletti $\mathbb{Z}_{p^s}[x]$, illetve a $\mathbb{F}_p$ feletti $\mathbb{F}_p[x]$ polinomgyűrűkre:

$$\mathbb{Z}_{p^s}[x] \longrightarrow \mathbb{F}_p[x]$$

$$a_0 + a_1x + \dots + a_nx^n \longrightarrow \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n,$$

ahol x a $\mathbb{Z}_{p^s}$ és az $\mathbb{F}_p$ feletti változó, $a_i \in \mathbb{Z}_{p^s}$, $i = 0, 1, \dots, n$. Hasonlóan jelöljük az $f(x) \in \mathbb{Z}_{p^s}$ leképezéssel kapott képét: $\bar{f}(x)$. Könnyen látható, hogy a leképezés gyűrűhomomorfizmus $\mathbb{Z}_{p^s}[x]$ gyűrűről $\mathbb{F}_p[x]$ gyűrűre, melynek magja a (p) ideál. Jelen esetben

$$(p) = \mathbb{Z}_{p^s}[x]p = \{f(x)p : f(x) \in \mathbb{Z}_{p^s}[x]\}$$

a p által generált főideál. Még általánosabban, tetszőleges $f(x) \in \mathbb{Z}_{p^s}[x]$ -re az $f(x)$ által generált ideál:

$$(f(x)) = \mathbb{Z}_{p^s}[x]f(x) = \{f(x)g(x) : g(x) \in \mathbb{Z}_{p^s}[x]\}.$$

2.2. Tétel. A $(p) = \mathbb{Z}_{p^s}[x]p$ ideál prímeálja a $\mathbb{Z}_{p^s}[x]$ polinomgyűrűnek, $\mathbb{Z}_{p^s}[x]$ minden prímeálja tartalmazza (p) -t, és $\mathbb{Z}_{p^s}[x]$ minden (p) -t valódi részként tartalmazó prímeál maximális ideál.

2.1. Definíció. Legyen f_1 és f_2 két $\mathbb{Z}_{p^s}[x]$ -beli polinom. Az f_1 és f_2 polinomokat $\mathbb{Z}_{p^s}[x]$ gyűrűben relatív prímnek nevezzük, ha léteznek olyan λ_1 és λ_2 $\mathbb{Z}_{p^s}[x]$ -beli polinomok, amelyekkel

$$\lambda_1 f_1 + \lambda_2 f_2 = 1.$$

Ezzel ekvivalens a következő állítás:

$$\mathbb{Z}_{p^s}[x]f_1 + \mathbb{Z}_{p^s}[x]f_2 = \mathbb{Z}_{p^s}[x].$$

Az $\mathbb{F}_p$ -beli relatív prímiség hasonlóan definiálható. Ismert továbbá, hogy két $\mathbb{F}_p$ -beli polinom akkor és csak akkor relatív prím $\mathbb{F}_p$ felett, ha nincs 1-nél nagyobb fokú közös osztójuk.

2.1. Lemma. Legyen f_1 és f_2 két $\mathbb{Z}_{p^s}[x]$ -beli polinom. f_1 és f_2 akkor és csak akkor relatív prímek $\mathbb{Z}_{p^s}[x]$ -ben, ha $\bar{f}_1$ és $\bar{f}_2$ relatív prímek $\mathbb{F}_p[x]$ -ben.

A polinomok $\mathbb{Z}_{p^s}$, illetve $\mathbb{F}_p$ feletti felbontása között teremt fontos és algoritmikus kapcsolatot a következő állítás:

2.2. Lemma. (Hensel-lemma)

Legyen $f(x)$ egy főegyütthatós $\mathbb{Z}_{p^s}$ feletti polinom, és tegyük fel, hogy

$$\bar{f}(x) = g_1(x)g_2(x) \dots g_r(x),$$

ahol

$$g_1(x), g_2(x), \dots, g_r(x)$$

páronként relatív prím $\mathbb{F}_p[x]$ -beli polinomok. Ekkor léteznek páronként relatív prím

$$f_1(x), f_2(x), \dots, f_r(x)$$

$\mathbb{Z}_{p^s}[x]$ -beli polinomok, melyekre

$$f(x) = f_1(x)f_2(x) \dots f_r(x)$$

és $\bar{f}_i(x) = g_i(x)$, $i = 1, 2, \dots, r$.

2.3. Alapvetően irreducibilis polinomok

Legyen f egy főegyütthatós m -edfokú polinom $\mathbb{Z}_{p^s}$ fölött, ahol $m \geq 1$ egész szám. Ha $\bar{f}$ irreducibilis (vagy primitív) $\mathbb{F}_p[x]$ -ben, akkor f -et $\mathbb{Z}_{p^s}$ feletti alapvetően irreducibilis (vagy primitív, megfelelően) polinomnak nevezzük. Természetesen a $\mathbb{Z}_{p^s}$ feletti alapvetően primitív polinomok alapvetően irreducibilisek is.

2.3. Tétel. Tetszőleges $m \geq 1$ egész számra létezik m -edfokú egy főegyütthatós, alapvetően irreducibilis polinom $\mathbb{Z}_{p^s}$ felett, amely osztja $x^{p^m-1} - 1$ -et $\mathbb{Z}_{p^s}[x]$ -ben.

2.2. Definíció. Legyen $g(x)$ egy főegyütthatós $\mathbb{F}_p$ feletti polinom. A $\mathbb{Z}_{p^s}$ feletti $f(x)$ polinomot a $g(x)$ polinom $\mathbb{Z}_{p^s}[x]$ -beli Hensel-felemeltjének hívjuk, ha $\bar{f}(x) = g(x)$ és létezik olyan n pozitív egész szám, amely nem osztható p -vel úgy, hogy

$$f(x) \mid (x^n - 1)$$

$\mathbb{Z}_{p^s}[x]$ -ben.

2.4. Tétel. Legyen $s \geq 1$ egész szám, g egy főegyütthatós $\mathbb{F}_p$ feletti polinom, melynek nincsenek többszörös gyökei, és x nem osztja g -t $\mathbb{F}_p[x]$ -ben. Ekkor g -nek létezik pontosan egy Hensel-felemeltje $\mathbb{Z}_{p^s}[x]$ -ben.

3. Galois-gyűrűk

Ebben a szakaszban – szintén a bizonyítások mellőzésével – Zhe-Xian Wan [2] könyve alapján a számunkra most legfontosabb algebrai struktúrákat, a Galois-gyűrűket tárgyaljuk.

3.1. Definíció. A Galois-gyűrű olyan egységelemes véges gyűrű, amelyben a nullosztók a nullával együtt egy $(p \cdot 1)$ főideált alkotnak valamely p prím számra. A definícióban szereplő $p \cdot 1$ -re:

$$p \cdot 1 = \underbrace{1 + 1 + \dots + 1}_p.$$

3.2. Definíció. A gyűrű karakterisztikáján a legkisebb olyan n természetes számot értjük, amelyre a gyűrű bármely r elemére teljesül az $n \cdot r = \underbrace{r + r + \dots + r}_{n \text{ darab}} = 0$ egyenlőség.

Amennyiben ilyen n szám nem létezik, akkor azt mondjuk, hogy a gyűrű karakterisztikája 0.

3.1. Példa. Tekintsük a $\mathbb{Z}_{p^s}$ gyűrűt, ahol p prím, s tetszőleges egész szám. A előbbihez hasonlóan definiáljuk $n \cdot 1$ -et, minden $n \in \mathbb{Z}_{p^s}$ elemre. Látható, hogy az 1 egységeleme a $\mathbb{Z}_{p^s}$ gyűrűnek, és a nullosztói a nullával a (p) főideált alkotják. Így $\mathbb{Z}_{p^s}$ egy p^s elemű Galois-gyűrű. A 2.1 tétel szerint (p) az egyetlen maximális ideálja a $\mathbb{Z}_{p^s}$ gyűrűnek.

Ha $s = 1$, akkor $\mathbb{Z}_{p^s} = \mathbb{F}_p$ a p elemű test, és $(p) = (0)$ a nullideál.

3.2. Példa. Legyen $h(x)$ egy főegyütthatós alapvetően irreducibilis m -edfokú polinom $\mathbb{Z}_{p^s}[x]$ -ben. Ekkor a $\mathbb{Z}_{p^s}[x]/(h(x))$ gyűrű Galois-gyűrű.

Az így kapott $\mathbb{Z}_{p^s}[x]/(h(x))$ gyűrű karakterisztikája p^s , elemszáma pedig p^{sm} . Az ilyen tulajdonsággal rendelkező Galois-gyűrűt $GR(p^s, p^{sm})$ -mel jelöljük, vagyis $\mathbb{Z}_{p^s} = GR(p^s, p^s)$.

3.1. Lemma. Legyen S Galois-gyűrű, melynek karakterisztikája p^s , elemszáma p^{sm} , ahol p prím, s és m pozitív egész szám. Legyen $f(x)$ egy $\mathbb{Z}_{p^s}$ feletti polinom, és tegyük fel, hogy $\bar{f}(x)$ -nek létezik $\bar{\beta}$ gyöke $\mathbb{F}_{p^m}$ -ben, és $\bar{f}'(\bar{\beta}) \neq 0$. Ekkor $f(x)$ -nek létezik pontosan egy $\alpha \in S$ gyöke úgy, hogy $\bar{\alpha} = \bar{\beta}$.

3.1. Tétel. Legyen S egy p^s karakterisztikájú, p^{sm} elemű Galois-gyűrű, ahol p prím, s és m pozitív egész szám. Az S gyűrű izomorf a $\mathbb{Z}_{p^s}[x]/(h(x))$ gyűrűvel, ahol $h(x)$ $\mathbb{Z}_p$ feletti egy főegyütthatós alapvetően irreducibilis m -edfokú polinom.

Ebből következik, hogy bármely két azonos karakterisztikájú és elemszámú Galois-gyűrű izomorf egymással. Tehát egységesen használhatjuk minden p^s karakterisztikájú, p^{sm} elemszámú gyűrűre a $GR(p^s, p^{sm})$ jelölést.

3.1. A Galois-gyűrűk egységeinek csoportja

3.2. Tétel. Legyen $S = GR(p^s, p^{sm})$ és jelölje S^* az S egységeinek csoportját. Ekkor

$$S^* = G_1 \times G_2,$$

ahol G_1 egy $p^m - 1$ -edrendű ciklikus csoport, $G_2 = \{1 + \pi : \pi \in (p)\}$ pedig egy $p^{(s-1)m}$ -edrendű csoport a következők szerint:

1. Ha p páratlan, vagy $p = 2$ és $s \leq 2$, akkor G_2 m darab p^{s-1} -edrendű ciklikus csoport direkt szorzata.
2. Ha $p = 2$ és $s \geq 3$, akkor G_2 egy másodrendű, egy 2^{s-2} -edrendű és $m - 1$ darab 2^{s-1} -edrendű ciklikus csoport direkt szorzata.

3.2. A p -adikus reprezentáció

A 2.3 tétel szerint létezik olyan alapvetően primitív $h(x)$ m -edfokú $\mathbb{Z}_{p^s}$ feletti polinom, amely osztja az $x^{p^m-1} - 1$ polinomot $\mathbb{Z}_{p^s}[x]$ -ben. Ekkor $\bar{h}(x)$ m -edfokú primitív polinom $\mathbb{F}_p$ felett. Legyen α_p a $\bar{h}(x)$ polinom gyöke $\mathbb{F}_{p^m}$ felett. Az α_p primitív eleme $\mathbb{F}_{p^m}$ -nek. A 3.1 lemma szerint $h(x)$ polinomnak létezik pontosan egy olyan α gyöke $GR(p^s, p^{sm})$ Galois-gyűrűben, amelyre $\bar{\alpha} = \alpha_p$. Az α elem rendje $p^m - 1$, gyöke egy $\mathbb{Z}_{p^s}$ feletti $h(x)$ alapvetően primitív, egy főegyütthatós, m -edfokú polinomnak, amely osztja az $x^{p^m-1} - 1$ polinomot $\mathbb{Z}_{p^s}[x]$ -ben. Ekkor

$$GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\alpha] = \{a_0 + a_1\alpha + \dots + a_{m-1}\alpha^{m-1}\}.$$

Az $a_i \in \mathbb{Z}_{p^s}$, $i = 0, 1, \dots, m-1$ elemek egyértelműek. Továbbá $h(x)$ az egyetlen $\leq m$ -edfokú egy főegyütthatós polinom $\mathbb{Z}_{p^s}$ fölött, amelynek α a gyöke. Az α elemről feltehetjük, hogy $\mathbb{Z}_{p^s}[x]/(p) \cong \mathbb{F}_{p^m}$ -beli rendje is $p^m - 1$.

Legyen $\tau = \{0, 1, \alpha, \dots, \alpha^{p^m-2}\}$. A $GR(p^s, p^{sm})$ Galois-gyűrű minden c eleme egyértelműen írható a következő alakban:

$$c = a_0 + a_1p + \dots + a_{s-1}p^{s-1},$$

ahol $a_0, a_1, \dots, a_{s-1} \in \tau$.

A c akkor és csak akkor egység, ha $a_0 \neq 0$, és c akkor és csak akkor nullosztó vagy 0, ha $a_0 = 0$.

3.3. Galois-gyűrűk automorfizmusai

Legyen $S = GR(p^s, p^{sm})$ Galois-gyűrű, melynek részgyűrűje $R = \mathbb{Z}_{p^s} = GR(p^s, p^s)$, $S = R[\alpha]$, ahol α az S egy $p^m - 1$ multiplikatív rendű eleme, továbbá gyöke egy R fölötti m -edfokú $h(x)$ alapvetően irreducibilis polinomnak, amely osztja $x^{p^m-1} - 1$ -et $R[x]$ -ben.

S azon automorfizmusait, amelyek R -et elemenként fixen hagyják, az S gyűrű R fölötti automorfizmusainak nevezzük. Az S gyűrű R fölötti automorfizmusai csoportot alkotnak a kompozícióra nézve, melyet az S gyűrű R feletti Galois-csoportjának nevezünk. Az S gyűrű R feletti Galois-csoportját $Gal(S/R)$ -lel jelöljük.

Ha $\tau \in \text{Gal}(S/R)$, akkor τ megőrzi pS -t is. A homomorfizmus tétel szerint $S/pS \cong \mathbb{F}_{p^m}$, ezért τ az $\mathbb{F}_{p^m}$ -nek egy automorfizmusát indukálja, jelölje ezt az automorfizmust $\bar{\tau}$. Ezt használva megmutatható, hogy $\text{Gal}(S, R)$ izomorf az $\mathbb{F}_{p^m} / \mathbb{F}_p$ feletti Galois-csoportjával.

3.3. Tétel. A

$$\text{Gal}(GR(p^s, p^{sm})/\mathbb{Z}_{p^s}) \rightarrow \text{Gal}(\mathbb{F}_{p^{sm}}, \mathbb{F}_{p^s})$$

$$\tau \rightarrow \bar{\tau}$$

leképezés csoportizomorfizmus. Tehát van olyan Φ R feletti automorfizmusa S -nek, hogy $\text{Gal}(S, R) = \langle \Phi \rangle$ és $\Phi^m = \text{id}$, ahol id az identikus leképezés S -en.

Azaz $\text{Gal}(GR(p^s, p^{sm})/\mathbb{Z}_{p^s})$ izomorf az m -edrendű ciklikus csoporttal.

3.4. Norma és nyom

Legyen $S = GR(p^s, p^{sm})$, melynek részgyűrűje $R = \mathbb{Z}_{p^s}$, Φ pedig az S gyűrű R feletti olyan automorfizmusa, amely generálja a Galois-csoportot. Tetszőleges $C \in S$ elemnek definiálhatjuk a nyomát:

$$\text{Tr}_{S/R}(C) = C + \Phi(C) + \dots + \Phi^{m-1}(C).$$

Az $C \in S$ elem R -re vonatkozó normája pedig

$$N_{S/R}(C) = C\Phi(C) \dots \Phi^{m-1}(C).$$

Nyilvánvaló, hogy $\text{Tr}_{S/R}$ és $N_{S/R}$ is független a Φ választásától. Ha S és R gyűrű egyértelmű, $\text{Tr}_{S/R}$ helyett T , $N_{S/R}$ helyett N jelölést használunk. A továbbiakban a nyom és a norma alapvető tulajdonságait soroljuk fel.

Az $C, D \in S$ és $a \in R$ elemekre teljesülnek a következők:

1. $\text{Tr}(C) \in R$,
2. $\text{Tr}(C + D) = \text{Tr}(C) + \text{Tr}(D)$,
3. $\text{Tr}(aC) = a\text{Tr}(C)$ és $\text{Tr}(a) = m \cdot a$,
4. $\text{Tr}(\Phi(C)) = \text{Tr}(C)$.

A normát illetően pedig:

1. $N(C) \in R$,
2. $N(CD) = N(C)N(D)$,
3. $N(aC) = a^m N(C)$ és $N(a) = a^m$,
4. $N(\Phi(C)) = N(C)$.
5. Ha $C \in S^*$, akkor $N(C) \in R^*$.

3.5. Abel-csoportok karakterei

Legyen G Abel-csoport (multiplikatív írásmóddal), melynek rendje $|G|$, egységeleme 1_G . A G csoportnak egy χ karaktere egy $G \rightarrow U$ homomorfizmus, ahol U az 1 abszolútértékű komplex számok multiplikatív csoportja. Vagyis χ egy leképezés G -ről U -ra, amelyre $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ minden $g_1, g_2 \in G$ elem esetén. Nyilván $\chi(1_G) = 1$ teljesül. Továbbá

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$$

minden $g \in G$ elemre, tehát a χ értékei $|G|$ -edik egységgyökök. Tudjuk továbbá, hogy $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$ és így $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ minden $g \in G$ elemre, ahol a felülvonás a komplex konjugálást jelöli.

A karakterek közül megemlíjtük a χ_0 triviális karaktert, amelyre $\chi_0(g) = 1$ minden $g \in G$ elemre. A G véges sok $\chi_1 \dots \chi_n$ karakteréből képezhetünk szorzatkaraktert $\chi_1 \dots \chi_n$, amelyre $\chi_1 \dots \chi_n(g) = \chi_1(g) \dots \chi_n(g)$. Ha $\chi_1 = \dots = \chi_n = \chi$, akkor $\chi_1 \dots \chi_n$ -et χ^n -nel jelöljük. A G karaktereiből álló $\hat{G}$ halmaz Abel-csoportot alkot a karakterek szorzására nézve. Mivel G karakterei csak $|G|$ -edik egységgyökök értékeit vehetik fel, így $\hat{G}$ véges.

3.1. Megjegyzés. Bármely különböző $g_1, g_2 \in G$ elemre létezik olyan χ karaktere G -nek, amelyre $\chi(g_1) \neq \chi(g_2)$.

3.4. Tétel. Ha a G véges Abel-csoportnak χ nem a triviális karaktere, akkor

$$\sum_{g \in G} \chi(g) = 0.$$

Ha $g \in G$ és $g \neq 1_G$, akkor

$$\sum_{\chi \in \hat{G}} \chi(g) = 0.$$

3.5. Tétel. Egy G véges Abel-csoport karaktereinek száma $|G|$.

3.3. Definíció. Azon karakterek halmazát, melyek a G egy H részcsoportján azonosan 1-et vesznek fel, a H $\hat{G}$ -beli annihilátorának nevezzük.

3.6. Tétel. Legyen H a G véges Abel-csoport egy részcsoportja. Ekkor a H annihilátora $\hat{G}$ -ben egy $|G|/|H|$ -rendű részcsoportja $\hat{G}$ -nek.

A következő, testek karaktereire vonatkozó tételekre a dolgozatban nem lesz szükség, csupán a testekre vonatkozó további tételek értelmezéséhez hasznosak. Megfigyelhető a gyűrűk karaktereihez való viszonyuk, különböző értelmezésük.

Az $\mathbb{F}_q$ ($q = p^s$, ahol p prím és $s > 1$ egész szám) véges test esetén két fontos Abel-csoportról beszélhetünk, a test additív és a multiplikatív csoportjáról. Fontos különbséget tennünk a két struktúrához tartozó karakterek között.

Tekintsük először $\mathbb{F}_q$ additív csoportját. Legyen p a test karakterisztikája, így az $\mathbb{F}_q$ tartalmazza $\mathbb{F}_p$ prímtestet, amelyet $\mathbb{Z}/(p)$ -vel azonosítunk. Jelölje Tr az $\mathbb{F}_q \rightarrow \mathbb{F}_p$ nyomleképezést. A Tr segítségével definiáljuk a $\chi_1 : \mathbb{F}_q \rightarrow \mathbb{C}$ leképezést.

$$\chi_1(c) = e^{2\pi i Tr(c)/p}$$

minden $c \in \mathbb{F}_q$ elemre. Ez az $\mathbb{F}_q$ additív csoportjának egy karaktere, mivel ha $c_1, c_2 \in \mathbb{F}_q$, akkor $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$, és így $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$. Az additív csoport karakterére az additív karakter elnevezést használjuk. A χ_1 karaktert az $\mathbb{F}_q$ kanonikus karakterének nevezzük. $\mathbb{F}_q$ minden karaktere kifejezhető a kanonikus karakterrel.

3.7. Tétel. *Bármely $b \in \mathbb{F}_q$ elemre a χ_b függvény, melyre $\chi_b(c) = \chi_1(bc)$ tetszőleges $c \in \mathbb{F}_q$ elem esetén additív karaktere $\mathbb{F}_q$ -nak, és $\mathbb{F}_q$ összes karaktere kifejezhető ebben az alakban.*

A $b = 0$ eset éppen a triviális additív karaktert adja, azaz $\chi_0(c) = 1$ minden $c \in \mathbb{F}_q$ elem esetén.

Az $\mathbb{F}_q$ multiplikatív csoportjának, $\mathbb{F}_q^*$ -nak a karakterei a multiplikatív karakterek. Mivel $\mathbb{F}_q^*$ egy $q - 1$ -edrendű ciklikus csoport, karakterei egyszerűen kifejezhetők.

3.8. Tétel. *Legyen $g \in \mathbb{F}_q$ rögzített primitív elem (azaz generátora $\mathbb{F}_q^*$ -nak). Minden $j = 0, 1, \dots, q - 2$ esetén a következő ϕ_j függvény*

$$\phi_j(g^k) = e^{2\pi i j k / (q-1)}, k = 0, 1, \dots, q - 2$$

definiálja egy multiplikatív karakterét $\mathbb{F}_q$ -nak, valamint $\mathbb{F}_q$ összes multiplikatív karaktere kifejezhető ilyen alakban.

3.6. Gauss-összegek Galois-gyűrű felett

Legyen először χ egy additív, ϕ egy multiplikatív karaktere $\mathbb{F}_q$ -nak. Akkor a $g(\chi, \phi)$ Gauss-összeget a

$$g(\chi, \phi) = \sum_{c \in \mathbb{F}_q^*} \chi(c) \phi(c)$$

formulával definiáljuk.

A továbbiakban Galois-gyűrűk feletti Gauss-összegekre lesz szükségünk. Legyen S egy Galois-gyűrű, χ az S additív csoportjának, ϕ pedig az S^* multiplikatív csoportjának a karaktere. Ekkor legyen

$$g(\chi, \phi) = \sum_{T \in S^*} \chi(T) \phi(T).$$

A Gauss-összegek ismerete a projektív normagráf sajátértékeinek kiszámításához szükséges. Így tehát a további vizsgálatok előtt ezek leírása következik.

A számunkra esetre való szűkítés miatt a 4-karakterisztikájú Galois-gyűrűk esetében vizsgáljuk a Gauss-összegeket. A korábbi jelölésekkel $p = 2, s = 2$. A megfelelő $h(x)$ polinom, mellyel az S bővítést kaptuk R -nek m -edfokú, ennek gyöke α . A 4-karakterisztikájú Galois-gyűrűnk tehát $S = GR(2^2, 2^{2m}) = \mathbb{Z}_4[\alpha]$. Az S gyűrű véges lokális kommutatív gyűrű, egyértelmű $2S$ maximális ideállal, és $K = R/2S \cong \mathbb{F}_{2^m}$ maradéktesttel.

A 3.2 tétel alapján az egységscsoport a következőképpen írható le:

3.9. Tétel. *S^* és K^* jelölje S illetve K egységeinek csoportját.*

$$S^* = K^* \times (1 + 2S),$$

ahol K^* $2^m - 1$ -edrendű ciklikus csoport, $1 + 2S$ pedig m darab másodrendű ciklikus csoport direkt szorzata, így egy 2^m -edrendű csoport. Vagyis S^* rendje $(2^m - 1)2^m$.

A Gauss-összegek tulajdonságait és a kapcsolódó tételeket Yunchang Oh és Heung-Joon Oh [3], illetve Philippe Langevin és Patrick Solé [4] cikke szerint mutatjuk be. Az S gyűrű χ_T ($T \in S$) additív karakterei definiálhatók a következőképpen:

$$\chi_T(U) = i^{Tr(TU)},$$

ahol $U \in S$ és i a komplex képzetes egység és $Tr : S \rightarrow R$ a nyom. Látható, hogy χ_0 az S triviális karaktere, $\chi_T(U) = \chi_1(TU)$ és $\bar{\chi}_T(U) = \chi_T(-U)$. Továbbá ha $T_1 \neq T_2$, $(T_1, T_2 \in S)$, akkor $\chi_{T_1} \neq \chi_{T_2}$.

Legyen ϕ egy multiplikatív karaktere S^* -nak. A

$$g(\chi_T, \phi) = \sum_{C \in S} \chi_T(C) \phi(C)$$

kifejezések az S -n értelmezett Gauss-összegek. Könnyen adódik, hogy

$$g(\chi_T, \phi) = \begin{cases} 4^m - 2^m, & \text{ha } \chi_T \text{ és } \phi \text{ triviálisak} \\ 0, & \text{ha } \chi_T \text{ triviális és } \phi \text{ nemtriviális.} \end{cases}$$

Yunchang Oh és Heung-Joon Oh [3] 3.1. tétele teljesül az S^* karaktereire:

3.10. Tétel. *Legyen ϕ az S^* nemtriviális karaktere. Ekkor a következők teljesülnek:*

1. *ha $T \in S^*$, akkor $g(\chi_T, \phi) = \phi(T^{-1})g(\chi_1, \phi)$, vagyis $\overline{g(\chi_1, \phi)} = \phi(-1)g(\bar{\chi}_1, \phi)$.*
2. *Ha $T \in 2S$ és ϕ nemtriviális $1 + 2S$ -en, akkor $g(\phi, \chi_T) = 0$.*

A későbbiekben használjuk Yunchang Oh és Heung-Joon Oh [3] 3.3. tételét:

3.11. Tétel. *Legyen ϕ az S^* nemtriviális karaktere. Ha ϕ nemtriviális $1 + 2S$ -en, akkor*

$$g(\chi_1, \phi)g(\bar{\chi}_1, \phi) = 4^m \phi(-1)$$

és

$$|g(\chi_T, \phi)| = \begin{cases} 2^m, & \text{ha } T \in S^* \\ 0, & \text{ha } T \in 2S \end{cases}.$$

4. A projektív normagráf és spektruma

A következőkben Galois-tesztetek esetében megismert eredmények megfelelőit szeretnénk megfogalmazni, illetve ellenőrizni a Galois-gyűrűk esetére. Pontosabban a $\mathbb{Z}_{p^s}$ Galois-gyűrű m -edfokú bővítéséről lesz szó, ahol $p = 2$, $s = 2$.

A normagráf vizsgálata a álvéletlen gráfok konstrukciójában segít. A álvéletlen gráfokat a sajátértékeik segítségével érthetjük meg: Adott egy G gráf, a szomszédossági mátrixának sajátértékei $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. G második sajátértéke $\lambda = \lambda(G) = \max\{\lambda_2, |\lambda_n|\}$. Könnyen belátható, hogy d -reguláris gráfokra $\lambda_1 = d$. Az olyan gráfok, amelyeknek a második sajátértéke kisebb nagyságrendű a legnagyobbánál, a véletlen gráfok bizonyos tulajdonságaival rendelkeznek. Minél nagyobb ez a spektrális rés, annál nagyobb a gráf véletlenszerűsége. Azzal az esettel foglalkozunk, amikor egy legfeljebb $n/2$ -fokú gráf második sajátértéke konstans szorzó erejéig legalább a négyzetgyöke a fokszámnak, vagyis olyan G gráfokkal, melyekre $\lambda(G) = \Theta(\sqrt{\lambda_1})$.

Az alábbiakban bemutatásra kerülő véges test feletti projektív normagráfok megfelelnek ennek a tulajdonságnak. Belátható, hogy a projektív normagráfok szomszédossági mátrixainak sajátértékei Gauss-összegek, így pontos értékeik előjeltől eltekintve kiszámíthatóak. A második sajátértékükre teljesül, hogy aszimptotikusan a fokszám gyökei, így tehát ezek álvéletlen gráfoknak tekinthetők.

4.1. A normagráf véges test felett

Alon-Rónyai-Szabó [5] cikke nyomán definiáljuk a $G_{q,t}$ projektív normagráfot. Legyen q prímszám, $t > 1$ egész, és jelölje $\mathbb{F}_q$ a q elemű véges testet. A $G = G_{q,t}$ normagráf $V(G)$ csúcsainak halmaza a $\mathbb{F}_{q^{t-1}} \times \mathbb{F}_q^*$ direkt szorzat, ahol $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ a $\mathbb{F}_q$ multiplikatív csoportja.

A $\mathbb{F}_q$ feletti $\mathbb{F}_{q^{t-1}}$ testbővítésen definiálhatunk normát a következőképpen:

$$N : \mathbb{F}_{q^{t-1}} \longrightarrow \mathbb{F}_q$$

$$X \longrightarrow N(X) := X^{(q^{t-1}-1)/(q-1)}.$$

Az így kapott normaleképezés egy multiplikatív függvény: ha $X, Y \in \mathbb{F}_{q^{t-1}}$, akkor

$$N(X \cdot Y) = N(X) \cdot N(Y).$$

A normagráfban az (A, a) és a (B, b) csúcsok között akkor és csak akkor megy él, ha $N(A + B) = a \cdot b$. A $G_{q,t}$ gráf csúcsainak száma $n = q^{t-1}(q-1)$. Adott $(A, a) \in V(G_{q,t})$ és tetszőleges $B \in \mathbb{F}_{q^{t-1}}$ esetén, ahol $B \neq -A$, létezik pontosan egy $b \in \mathbb{F}_q^*$ úgy, hogy (A, a) és (B, b) szomszédosak (megy közöttük él) $G_{q,t}$ normagráfban. Ezért a $G_{q,t}$ gráf $q^{t-1} - 1 = n^{1-1/t}$ -reguláris. Belátható, hogy a $G_{q,t}$ gráf $K_{t,(t-1)!+1}$ -mentes.

Szabó a [1] cikkében megmutatta, hogy a $G_{q,t}$ gráf szomszédossági mátrixának sajátértékei a következő alakban írhatók:

$$\pm \left| \sum_{\substack{C \in \mathbb{F}_{q^{t-1}} \\ C \neq 0}} \chi(C) \phi(N(C)) \right|.$$

Ha $\chi = \chi_0$, de $\phi = \phi_0$ a triviális karakterek, akkor a megfelelő sajátérték $q^{t-1} - 1$, amely éppen a G gráf foka.

Ha $\chi = \chi_0$ és $\phi \neq \phi_0$, akkor a megfelelő sajátértékek

$$\pm \left| \sum_{\substack{C \in \mathbb{F}_{q^{t-1}} \\ C \neq 0}} \phi(N(C)) \right| = \pm \left| \frac{q^{t-1} - 1}{q - 1} \sum_{c \in \mathbb{F}_{q^*}} \phi(c) \right| = 0.$$

Ha $\chi \neq \chi_0$, de $\phi = \phi_0$, akkor a megfelelő sajátértékek

$$\pm \left| \sum_{\substack{C \in \mathbb{F}_{q^{t-1}} \\ C \neq 0}} \chi(C) \right| = \pm 1.$$

Ha χ és ϕ sem a triviális karakterek, akkor

$$\pm \left| \sum_{\substack{C \in \mathbb{F}_{q^{t-1}} \\ C \neq 0}} \chi(C) \phi(N(C)) \right| = q^{(t-1)/2}.$$

Célunk, hogy véges testek helyett Galois-gyűrűkre és megfelelő Galois-bővítésekre definiáljuk a normagráfot, majd az így kapott gráf szomszédossági mátrixának sajátértékeit vizsgáljuk.

4.2. A normagráf a $GR(p^s, p^{sm})$ Galois-gyűrű felett

4.2.1. A projektív normagráf és szomszédossági mátrixa

Legyenek R és S véges Galois-gyűrűk, $R \leq S$ és jelölje $N : S \rightarrow R$ az $N_{S/R}$ normaleképezést.

A $G = G_{R,S}$ gráf csúcshalmaza $V = S \times R^*$. Az $(A, a) \in V$ és $(B, b) \in V$ csúcsok között akkor megy él, ha $N(A + B) = a \cdot b$. A projektív normagráf szomszédossági mátrixát jelöljük M -mel. Az M sorait és oszlopait (A, a) párokkal indexeljük, ahol $A \in S$, $a \in R^*$. Az M gráf k -reguláris, ahol $k = |S^*| = |S| - |pS|$. Itt p az $|S|$ egyetlen prímosztója. Ugyanis az $(A, a) \in V$ csúcshoz pontosan k számú $B \in S$ választható úgy, hogy $A + B \in S^*$ teljesüljön. Ekkor nyilván $N(A + B) \in R^*$, és pontosan egy $b \in R^*$ létezik, melyre $N(A + B) = a \cdot b$.

Jelölje M a gráf szomszédossági mátrixát, M sorait és oszlopait is V elemeivel indexeljük, és

$$M_{(A,a)(B,b)} = \begin{cases} 1, & \text{ha } N(A + B) = a \cdot b \\ 0, & \text{különben.} \end{cases}$$

Célunk, hogy formulát adjunk az M mátrix sajátértékeire. Legyen χ az S tetszőleg additív karaktere, ϕ az R^* egy multiplikatív karaktere. Jelölje $V_{\chi,\phi}$ azt a $|V|$ hosszú oszlopvektort, melyet $V(G)$ elemeivel koordinátázunk, és az (A, a) koordinátához tartozó elem a $\chi(A)\phi(a)$, vagyis

$$V_{\chi,\phi} = (\dots, \chi(A)\phi(a), \dots)^T.$$

Megjegyezzük, hogy az $S \times R^*$ csoport (az S additív és az R^* multiplikatív csoportok direkt szorzata) karakterei éppen az

$$(A, a) \longrightarrow \chi(A)\phi(a)$$

leképezések, ahol χ az S , ϕ pedig az R^* karakterein fut végig. Egy H Abel-csoport nem-triviális ψ karaktere esetén

$$\sum_{h \in H} \psi(h) = 0$$

Ezt alkalmazva adódik, hogy a $V_{\chi, \phi}$ vektorok páronként merőlegesek egymásra, tehát a $\mathbb{C}^{|V|}$ tér egy ortogonális bázisát alkotják. A következő eredmény közvetlen, egyszerű általánosítása Szabó [1] testekre vonatkozó eredményének.

4.1. Tétel. Az M^2 mátrix sajátértékei éppen a

$$\left| \sum_{C \in S^*} \chi(C)\phi(N(C)) \right|^2$$

számok, hol χ az S és ϕ az R^* karakterein fut végig.

Bizonyítás: $MV_{\chi, \phi}$ -nek az (A, a) -hoz tartozó komponense:

$$\begin{aligned} \sum_{\substack{(B, b) \in V, \\ N(A+B)=ab}} \chi(B)\phi(b) &= \sum_{\substack{B \in S, \\ (A+B) \in S^*}} \chi(B)\phi\left(\frac{N(A+B)}{a}\right) \\ &= \sum_{C \in S^*} \chi(C-A)\phi\left(\frac{N(C)}{a}\right) = \sum_{C \in S^*} \chi(C)\phi(N(C))\overline{\chi(A)\phi(a)}, \end{aligned}$$

azaz

$$MV_{\chi, \phi} = \sum_{C \in S^*} \chi(C)\phi(N(C))V_{\bar{\chi}, \bar{\phi}}.$$

Az M -et ismételten alkalmazva

$$M^2V_{\chi, \phi} = \left| \sum_{C \in S^*} \chi(C)\phi(N(C)) \right|^2 V_{\chi, \phi}.$$

□

A $V_{\chi, \phi}$ vektorok tehát az M^2 egy teljes sajátvektorrendszerét alkotják, ebben a bázisban M^2 diagonális és éppen a 4.1 tételben kapott értékek a sajátértékei. Tudjuk továbbá, hogy az M valós szimmetrikus mátrix, tehát diagonalizálható. Az M^2 sajátértékei megegyeznek az M sajátértékeinek négyzetével.

4.2. Tétel. Az M mátrix sajátértékei

$$\pm \left| \sum_{C \in S^*} \chi(C)\phi(N(C)) \right|$$

alakúak, ahol χ az S és ϕ az R^* karakterein fut végig.

Vegyük észre, hogy itt az S^* -on értelmezett $g(\chi, \phi \circ N)$ Gauss-összeg abszolút értékéről van szó.

Abban az esetben, amikor R és S is véges testek, Szabó megadta a lehetséges sajátértékek abszolútértékeit. Célunk ennek a részleges kiterjesztése lesz. A fő nehézséget az jelenti, hogy az általános Galois-gyűrűk felett sokkal kevesebbet tudunk a Gauss-összegekről, mint testek felett.

4.3. Az M sajátértékei a $GR(2^2, 2^{2m})$ Galois-gyűrű esetén

A következőkben feltesszük, hogy $R = \mathbb{Z}_4$ és $S = GR(2^2, 2^{2m})$.

Tudjuk továbbá, hogy S véges, lokális kommutatív gyűrű, melynek maximális ideálja $2S$, és az $S/2S$ maradékosztálygyűrű a 2^m -elemű $\mathbb{F}_{2^m}$ test, melyet jelöljünk K -val. A 3.9 tétel szerint

$$S^* = K^* \times (1 + 2S),$$

ahol K^* $2^m - 1$ -edrendű ciklikus csoport, $1 + 2S$ pedig m darab másodrendű ciklikus csoport direkt szorzata.

Esetünkben $R = \mathbb{Z}_4$, tehát $R^* = \{1, -1\}$. Az R^* csoportok két karaktere van, a triviális ϕ_0 és a $\phi : R^* \rightarrow \mathbb{C}^*$ leképezés, melyre $\phi(1) = 1$ és $\phi(-1) = -1$.

Megmutatjuk, hogy erre az utóbbi ϕ karakterre $\phi \circ N$ nem a triviális leképezés az $1 + 2S$ halmazon. A $\phi \circ N$ nem triviális voltának igazolásához elég azt belátni, hogy $1 + 2S$ -ben van -1 normájú elem, azaz olyan elem, aminek a normája nem 1 (az egységeket a normaleképezés 1,-1-re képezi).

Legyen α az S olyan eleme, amelynek a képe a $\text{mod } 2$ redukciónál olyan elem lesz, amelynek a nyoma nem 0. Ilyen van, mert véges testek bővítésénél a nyom nem az azonosan 0 függvény a [6] 2.35 tétele, a normálbázistétel miatt. Más szóval $\text{Tr}(\alpha) = 1 + 2\beta$ alkalmas $\beta \in S$ elemmel.

Ekkor

$$N(1 + 2\alpha) = 1 + 2\text{Tr}(\alpha) = 1 + 2(1 + 2\beta) = 3 = -1.$$

Ezzel beláttuk, hogy $\phi \circ N$ nem triviális $2S$ -en. Így a 3.11 tétel szerint:

4.3. Tétel. Ha $\phi \neq \phi_0$, akkor

$$|g(\chi_T, \phi \circ N)| = \begin{cases} 2^m, & \text{ha } T \in S^* \\ 0 & \text{különben.} \end{cases}$$

Bizonyítás: A fentiek során beláttuk, hogy amennyiben ϕ nem a triviális karaktere S -nek, akkor $\phi \circ N$ nem a triviális leképezés az $1 + 2S$ halmazon. Ekkor χ -re és $\phi \circ N$ -re alkalmazható a 3.11 tétel Gauss-összegek abszolútértékeire vonatkozó eredménye, vagyis

$$|g(\chi_T, \phi \circ N)| = \begin{cases} 2^m, & \text{ha } T \in S^* \\ 0, & \text{ha } T \in 2S \end{cases}.$$

Ez éppen a bizonyítandó állítás.

□

A sajátértékek nagyságának a multiplicitása kiszámolható: a 2^m abban az esetben szerepel, amennyiben $T \in S^*$, vagyis $|S^*| = |S| - |2S| = 4^m - 2^m$ -szer. A megfelelő sajátérték pedig 0 minden más esetben, azaz 2^m -szer.

Azon lehetőségek maradtak, amikor ϕ és így $\phi \circ N$ is a triviális karakter, amelynek az értéke 1 minden $T \in S^*$ elemen.

Ebben az esetben a $g(\chi, \phi \circ N)$ Gauss-összeg $\sum \chi(T)$ lesz, ahol az összegezés az $T \in S^*$ egységekre terjed ki.

Ez viszont előáll két teljes összeg különbségeként: egyrészt vesszük az összeget a teljes S -re, majd ebből kivonjuk a $2S$ -re vett összeget. Mindkét esetben (additív) csoportra összegezzünk. Az összeg vagy a csoport rendje lesz, vagy pedig 0, aszerint, hogy a karakter triviális-e a csoporton, vagy sem.

A következő esetek lehetségesek:

- $\chi = \chi_0$. Ekkor

$$\sum_{A \in S^*} \chi(A) = |S^*| = |S| - |2S| = 4^m - 2^m.$$

Ez egyetlen esetben fordul elő.

- $\chi \neq \chi_0$, de χ triviális $2S$ -en. Ekkor

$$\sum_{A \in S^*} \chi(A) = \sum_{A \in S} \chi(A) - \sum_{A \in 2S} \chi(A) = 0 - |2S| = -2^m.$$

A 3.5 tétel alapján tudjuk, hogy a karakterek száma a csoport elemszámával egyezik meg, tehát $|\hat{R}^*| = 2$ és $|\hat{S}| = 4^m$. A $2S$ annihilátorának a számosságának a kiszámítására alkalmazható a 3.6 tétel, vagyis ennek elemszáma $|2S|/|S| = 2^m$. A triviális karaktert az előző lehetőségnél számoltuk, így a -2^m multiplicitása $2^m - 1$.

- χ nem triviális $2S$ -en sem. Ekkor

$$\sum_{A \in S^*} \chi(A) = 0.$$

Ez minden korábbtól különböző esetben teljesül, vagyis $4^m - 1 - (2^m - 1) = 4^m - 2^m$ -szer.

A kapott eredményeinket foglalja össze a következő tétel:

4.4. Tétel. Az $R = \mathbb{Z}_4$ és az $S = GR(2^2, 2^m)$ Galois-bővítésére értelmezett normagráf sajátértékei a következők:

- Ha $\phi \neq \phi_0$, akkor

$$|g(\chi_T, \phi \circ N)| = \begin{cases} 2^m, & \text{ha } T \in S^* \\ 0 & \text{különben.} \end{cases}$$

A 2^m multiplicitása $4^m - 2^m$, a 0 sajátértéké pedig 2^m .

- Ha $\phi = \phi_0$ és

- Ha $\chi = \chi_0$, akkor $|g(\chi_T, \phi \circ N)| = 4^m - 2^m$ a megfelelő sajátérték 1 multiplicitással.
- Ha $\chi \neq \chi_0$, de triviális $2S$ -en, akkor $g(\chi_T, \phi \circ N) = -2^m$, amely $2^m - 1$ -szeres sajátérték.
- $\chi \neq \chi_0$, és nem triviális $2S$ -en sem, akkor $|g(\chi_T, \phi \circ N)| = 0$, amely $4^m - 2^m$ -szeres sajátérték.

Az M mátrix sajátértékeinek abszolútértéke tehát: 0, 4^m multiplicitással; 2^m , $4^m - 1$ multiplicitással, illetve 1-szeres sajátérték a $4^m - 2^m$.

5. A $GR(4, 16)$ Galois-gyűrű

A normagráf szomszédossági mátrixának sajátértékeit a $GR(2^2, 2^{2m})/\mathbb{Z}_4$ gyűrűbővítés esetére még jobban megvizsgáljuk. A Galois-gyűrű és a normagráf szerkezetének részletesebb megismeréséhez a legkisebb ilyen gyűrűt, vagyis az $m = 2$ eset leírását használjuk. Továbbiakban $GR(2^2, 2^{2 \cdot 2}) = GR(4, 16) = S$ jelölést használjuk. Az R gyűrű pedig a $\mathbb{Z}_4$ modulo 4 egész számok gyűrűje, amelyet reprezentálhatjuk a következőképpen:

$$R = \mathbb{Z}_4 = \{0, 1, 2, 3\}.$$

A könnyebb számítások érdekében a 3 helyett a modulo 4 vele megegyező -1 reprezentánst használjuk. Ekkor $|R| = 4$, $|S| = 16$ teljesül. Továbbá

$$\mathbb{Z}_4/(2) \cong \mathbb{F}_2.$$

Az S véges lokális gyűrű maximális ideálja: $2S$, $K = R/2S \cong \mathbb{F}_4$.

Legyen $h(x) = x^2 + x + 1$. A $h(x)$ polinom irreducibilis modulo 2, vagyis alapvetően irreducibilis és egy főgyütthetős polinom. Továbbá $h(x)$ alapvetően primitív polinom, és osztja az $x^3 - 1$ polinomot $\mathbb{Z}$ felett, tehát $\mathbb{Z}_4$ felett is, ezért a gyökeire alkalmazható a p -adikus előállításról szóló tétel.

Az $R[x]/(h(x))$ az R másodfokú Galois-bővítését adja, vagyis az S gyűrűt. Ha α az S gyűrű egy olyan eleme, amelyre $f(\alpha) = 0$, akkor $S = R[\alpha]$.

A gyűrű elemei $a + b\alpha$ alakban írhatók, ahol $a, b \in \mathbb{Z}_4$. Az α elemre a következők teljesülnek:

$$\alpha^2 = -\alpha - 1,$$

ahonnan

$$\alpha^3 = \alpha(-\alpha - 1) = -\alpha^2 - \alpha = -(-\alpha - 1) - \alpha = 1.$$

Az α multiplikatív rendje tehát 3.

R multiplikatív csoportját jelölje R^* , amelyről tudjuk, hogy $R^* = \{1; -1\}$, így $|R^*| = 2$.

5.1. A projektív normagráf

A normagráfot továbbra is jelölje $G_{p^s, t}$, amely esetünkben $G_{4, 2}$. A normagráf pontjainak halmaza: $V = S \times R^*$, vagyis $|V| = 16 \cdot 2 = 32$. $(A, a) \in V$ és $(B, b) \in V$ esetén $((A, a), (B, b))$ éle a projektív normagráfnak, ha $N(A + B) = ab$. A gráf k -reguláris, ahol k az S egységeinek száma, esetünkben

$$k = |S| - |2S| = 16 - 4 = 12.$$

Az S multiplikatív csoportja tehát 12 elemű. A korábbiak szerint írható $S = K^* \times (1 + 2S)$ alakban.

A 3-Sylow $\{1; \alpha; -\alpha - 1\}$. A 2-Sylow pedig $1 + 2S$ lesz, amely nyilvánvalóan csupa egységekből áll, zárt a szorzásra, az elemeinek száma pedig 4.

Jelölje továbbá Φ az S egyetlen nem triviális automorfizmusát. A 3.5 tétel szerint a Galois-csoport kételemű. A nemtriviális automorfizmus R -et elemenként fixen hagyja, az α elemet peddig csak a multiplikatív inverzébe viheti, ami $-\alpha - 1$, mert nincs más

harmadrendű elem S -ben.

Ezzel tehát Φ a következőképpen hat S -en:

$$\Phi : a + b\alpha \longrightarrow a + b(-\alpha - 1) = a - b - b\alpha,$$

ahol $a, b \in R$. A norma leképezi a 12 elemű multiplikatív csoportot a kételemű $R^* = \{1; -1\}$ multiplikatív csoportra. A harmadrendű elemek a magjában vannak, és a $-1 = 3$ is. Ezzel a 6 magbeli elem: a 3-Sylow elemei, és ezek ellentettjei:

$$1, \alpha, -\alpha - 1, -1, -\alpha, \alpha + 1.$$

A többi egység normája -1 lesz.

Legyen χ az S tetszőleg additív karaktere, ϕ az R^* multiplikatív karaktere.

S -nek 16 additív karaktere van. Az S additív csoportja (jelölje $\langle S, + \rangle$) izomorf $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ -gyel. Így minden $A \in S$ -re $4A = 0$.

Tehát az additív karakterekre $\chi(A) \in \{1; -1; i; -i\}$ teljesül.

$$\begin{aligned} \chi^* : \langle \mathbb{Z}_4, + \rangle &\longrightarrow \mathbb{C}^* \\ a &\longrightarrow i^a \\ a + b &\longrightarrow i^{a+b} \end{aligned}$$

.

$$\begin{aligned} \chi^\# : \{\alpha; 2\alpha; 3\alpha; 0\} &\longrightarrow \mathbb{C}^* \\ a\alpha &\longrightarrow i^a. \end{aligned}$$

Ezekkel a jelölésekkel az S összes karaktere

$$a + b\alpha \longrightarrow \chi^{*r}(a)\chi^{\#s}(b\alpha)$$

alakú, ahol $0 \leq r < 4, 0 \leq s < 4$.

R^* karakterei:

- triviális
 $\phi(a) = 1 \quad \forall a \in R^*$
- $\phi(-1) = -1, \phi(1) = 1$.

5.2. Eredmények a $GR(4, 16)$ Galois-gyűrű esetére

5.2.1. Az M^2 sajátértékeinek kiszámítása a sajátvektorok segítségével

A sajátvektorok és sajátértékek kiszámításához MATLAB 7.10.0 (R2010a) programot használtam.

Az M^2 lehetséges sajátvektorai a korábbiak szerint:

$$V_{\chi, \phi} = (\dots, \chi(A)\phi(a), \dots)^T$$

alakúak, ahol az S összes karaktere

$$a + b\alpha \longrightarrow \chi^{*r}(a)\chi^{\#s}(b\alpha)$$

alakú, ahol $0 \leq r < 4, 0 \leq s < 4$.

R^* -nak pedig kétféle karaktere van, a triviális, illetve a nemtriviális, amelyre $\phi(1) = 1$, $\phi(-1) = -1$.

A vektorokat

$$\begin{aligned} &(1, 1), (\alpha, 1), (-1 - \alpha, 1), (-1, 1), (-\alpha, 1), (1 + \alpha, 1) \\ &(1, -1), (\alpha, -1), (-1 - \alpha, -1), (-1, -1), (-\alpha, -1), (1 + \alpha, -1) \\ &(-1 + \alpha, 1), (1 - \alpha, 1), (2 + \alpha, 1), (2 - \alpha, 1), (1 + 2\alpha, 1), (-1 + 2\alpha, 1) \\ &(-1 + \alpha, -1), (1 - \alpha, -1), (2 + \alpha, -1), (2 - \alpha, -1), (1 + 2\alpha, -1), (-1 + 2\alpha, -1) \\ &(2, 1), (2\alpha, 1), (2 + 2\alpha, 1), (0, 1) \\ &(2, -1), (2\alpha, -1), (2 + 2\alpha, -1), (0, -1) \end{aligned}$$

$S \times R^*$ -beli elemekkel koordinátázzuk. A lehetséges értékeket kiszámolva tehát a sajátvektorokat abban az esetben, amikor ϕ nem a triviális karakter, az 1. táblázat oszlopai tartalmazzák. Amennyiben pedig ϕ triviális R^* -on, a sajátvektorok a 2. táblázat oszlopai. Az M mátrix elemeit a 3. táblázat tartalmazza, ahol az M mátrixot szintén a fenti $(A, a) \in S \times R^*$ elemekkel koordinátázzuk. A további számítások ezen elemek felhasználásával történtek.

Az M^2 sajátértékei a sajátvektorok táblázatbeli sorrendjével megegyező sorrendben pedig:

$$16, 16, 16, 16, 16, 0, 16, 0, 16, 16, 16, 16, 16, 0, 16, 0,$$

ha $\phi \neq \phi_0$,

$$0, 0, 0, 0, 0, 16, 0, 16, 0, 0, 0, 0, 0, 16, 0, 144$$

a $\phi = \phi_0$ esetben számolt sajátvektorokra.

Ez egybeesik az M mátrixnak a MATLAB 'eig' parancsával számolt sajátértékeivel.

Ekkor tehát az előforduló sajátértékek a 0, a 16 és a 144. Ezek multiplicitása:

$$0 : 16,$$

$$16 : 15,$$

$$144 : 1.$$

A MATLAB 'eig' parancsával kiszámolhatóak az M sajátértékei is, amelyek a 0, -4 , 4 , 12 értékeket veszik fel a következő multiplicitással:

$$0 : 16,$$

$$4 : 6,$$

$$-4 : 9,$$

$$12 : 1.$$

A $GR(2^2, 2^{2m})$ általános esetre kapott 4.4 összefoglaló tétel szerint a megfelelő sajátértékek abszolútértéke és multiplicitásuk: 0 , 4^m multiplicitással; 2^m , $4^m - 1$ multiplicitással, illetve 1-szeres sajátérték a $4^m - 2^m$, ami $m = 2$ esetén tehát: 0 , multiplicitása 16 , 4 , multiplicitása 15 , és a 12 egyszeres sajátérték.

Látható, hogy eredményeink egybeesnek az általánosan kimondott tételekkel, illetve a szűkített változat pontosítását is adja, hiszen a sajátértékek előjeles értékét is megkaptuk.

5.2.2. Az eredmények bemutatása és ellenőrzése további számításokkal

Ebben a fejezetben a kapott formulák helyességét ellenőrizzük, illetve bemutatjuk, hogyan használhatjuk ezeket a megfelelő adatok kiszámolására.

Elsőként a sajátértékeket számoljuk, a sajátvektorok bevezetése nélkül, a 4.2 tételben kimondott formulából, vagyis a

$$\sum_{C \in S^*} \chi(C) \phi(N(C))$$

értékét keressük. Látható, hogy ez a művelet több lépésből áll, ezért csak egy eset lépéseit követjük végig a 4. és az 5. táblázatokban, melyek utolsó sorának utolsó elemei adják a kívánt sajátértékeket.

Új eredményeket ezzel nem kapunk, hiszen a korábbiakban már előállítottuk az összes lehetséges sajátérték abszolútértékét, de ellenőrizhető, hogy azokat a formulából direkt számítással is előállíthatjuk.

A korábban bevezetett

$$a + b\alpha \longrightarrow \chi^{*r}(a)\chi^{\#s}(b\alpha)$$

karakterekkel számolunk, ahol $0 \leq r, s < 4$ lehetőségek közül az $r = s = 1$ esetet választjuk.

1. táblázat. Az M^2 sajátvektorai $\phi \neq \phi_0$ esetén

i	i	i	i	-1	-1	-1	-1	-i	-i	-i	-i	1	1	1	1
i	-1	-i	1	i	-1	-i	1	i	-1	-i	1	i	-1	-i	1
-1	i	1	-i	i	1	-i	-1	1	-i	-1	i	-i	-1	i	1
-i	-i	-i	-i	-1	-1	-1	-1	i	i	i	i	1	1	1	1
-i	-1	i	1	-i	-1	i	1	-i	-1	i	1	-i	-1	i	1
-1	-i	1	i	-i	1	i	-1	1	i	-1	-i	i	-1	-i	1
-i	-i	-i	-i	1	1	1	1	i	i	i	i	-1	-1	-1	-1
-i	1	i	-1	-i	1	i	-1	-i	1	i	-1	-i	1	i	-1
1	-i	-1	i	-i	-1	i	1	-1	i	1	-i	i	1	-i	-1
i	i	i	i	1	1	1	1	-i	-i	-i	-i	-1	-1	-1	-1
i	1	-i	-1	i	1	-i	-1	i	1	-i	-1	i	1	-i	-1
1	i	-1	-i	i	-1	-i	1	-1	-i	1	i	-i	1	i	-1
1	i	-1	-i	-i	1	i	-1	-1	-i	1	i	i	-1	-i	1
1	-i	-1	i	i	1	-i	-1	-1	i	1	-i	-i	-1	i	1
-i	1	i	-1	i	-1	-i	1	-i	1	i	-1	i	-1	-i	1
i	1	-i	-1	-i	-1	i	1	i	1	-i	-1	-i	-1	i	1
-i	i	-i	i	1	-1	1	-1	i	-i	i	-i	-1	1	-1	1
i	-i	i	-i	1	-1	1	-1	-i	i	-i	i	-1	1	-1	1
-1	-i	1	i	i	-1	-i	1	1	i	-1	-i	-i	1	i	-1
-1	i	1	-i	-i	-1	i	1	1	-i	-1	i	i	1	-i	-1
i	-1	-i	1	-i	1	i	-1	i	-1	-i	1	-i	1	i	-1
-i	-1	i	1	i	1	-i	-1	-i	-1	i	1	i	1	-i	-1
i	-i	i	-i	-1	1	-1	1	-i	i	-i	i	1	-1	1	-1
-i	i	-i	i	-1	1	-1	1	i	-i	i	-i	1	-1	1	-1
-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1	1	1
-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1
1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	1	-1	1	-1
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

2. táblázat. Az M^2 sajátvektorai $\phi = \phi_0$ esetén

i	i	i	i	-1	-1	-1	-1	-i	-i	-i	-i	1	1	1	1
i	-1	-i	1	i	-1	-i	1	i	-1	-i	1	i	-1	-i	1
-1	i	1	-i	i	1	-i	-1	1	-i	-1	i	-i	-1	i	1
-i	-i	-i	-i	-1	-1	-1	-1	i	i	i	i	1	1	1	1
-i	-1	i	1	-i	-1	i	1	-i	-1	i	1	-i	-1	i	1
-1	-i	1	i	-i	1	i	-1	1	i	-1	-i	i	-1	-i	1
i	i	i	i	-1	-1	-1	-1	-i	-i	-i	-i	1	1	1	1
i	-1	-i	1	i	-1	-i	1	i	-1	-i	1	i	-1	-i	1
-1	i	1	-i	i	1	-i	-1	1	-i	-1	i	-i	-1	i	1
-i	-i	-i	-i	-1	-1	-1	-1	i	i	i	i	1	1	1	1
-i	-1	i	1	-i	-1	i	1	-i	-1	i	1	-i	-1	i	1
-1	-i	1	i	-i	1	i	-1	1	i	-1	-i	i	-1	-i	1
1	i	-1	-i	-i	1	i	-1	-1	-i	1	i	i	-1	-i	1
1	-i	-1	i	i	1	-i	-1	-1	i	1	-i	-i	-1	i	1
-i	1	i	-1	i	-1	-i	1	-i	1	i	-1	i	-1	-i	1
i	1	-i	-1	-i	-1	i	1	i	1	-i	-1	-i	-1	i	1
-i	i	-i	i	1	-1	1	-1	i	-i	i	-i	-1	1	-1	1
i	-i	i	-i	1	-1	1	-1	-i	i	-i	i	-1	1	-1	1
1	i	-1	-i	-i	1	i	-1	-1	-i	1	i	i	-1	-i	1
1	-i	-1	i	i	1	-i	-1	-1	i	1	-i	-i	-1	i	1
-i	1	i	-1	i	-1	-i	1	-i	1	i	-1	i	-1	-i	1
i	1	-i	-1	-i	-1	i	1	i	1	-i	-1	-i	-1	i	1
-i	i	-i	i	1	-1	1	-1	i	-i	i	-i	-1	1	-1	1
i	-i	i	-i	1	-1	1	-1	-i	i	-i	i	-1	1	-1	1
-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1	1	1
-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1	1	1
-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

3. táblázat. Az M mátrix

$N(A)=1, a=1$	$N(A)=1, a=-1$	$N(A)=-1, a=1$	$N(A)=-1, a=-1$	$N(A)=0, a=1$	$N(A)=0, a=-1$
0 1 1 0 0 0	0 0 0 0 1 1	1 0 0 1 0 0	0 1 1 0 0 0	1 0 0 1	0 1 1 0
1 0 1 0 0 0	0 0 0 1 0 1	0 1 0 0 0 1	1 0 0 0 1 0	0 1 0 1	1 0 1 0
1 1 0 0 0 0	0 0 0 1 1 0	0 0 1 0 1 0	0 0 0 1 0 1	0 0 1 1	1 1 0 0
0 0 0 0 1 1	0 1 1 0 0 0	0 1 1 0 0 0	1 0 0 1 0 0	1 0 0 1	0 1 1 0
0 0 0 1 0 1	1 0 1 0 0 0	1 0 0 0 1 0	0 1 0 0 0 1	0 1 0 1	1 0 1 0
0 0 0 1 1 0	1 1 0 0 0 0	0 0 0 1 0 1	0 0 1 0 1 0	0 0 1 1	1 1 0 0
0 0 0 0 1 1	0 1 1 0 0 0	0 1 1 0 0 0	1 0 0 1 0 0	0 1 1 0	1 0 0 1
0 0 0 1 0 1	1 0 1 0 0 0	1 0 0 0 1 0	0 1 0 0 0 1	1 0 1 0	0 1 0 1
0 0 0 1 1 0	1 1 0 0 0 0	0 0 0 1 0 1	0 0 1 0 1 0	1 1 0 0	0 0 1 1
0 1 1 0 0 0	0 0 0 0 1 1	1 0 0 1 0 0	0 1 1 0 0 0	0 1 1 0	1 0 0 1
1 0 1 0 0 0	0 0 0 1 0 1	0 1 0 0 0 1	1 0 0 0 1 0	1 0 1 0	0 1 0 1
1 1 0 0 0 0	0 0 0 1 1 0	0 0 1 0 1 0	0 0 0 1 0 1	1 1 0 0	0 0 1 1
1 0 0 0 1 0	0 1 0 1 0 0	0 0 0 1 1 0	0 0 1 0 0 1	1 1 0 0	0 0 1 1
0 1 0 1 0 0	1 0 0 0 1 0	0 0 1 0 0 1	0 0 0 1 1 0	1 1 0 0	0 0 1 1
0 0 1 1 0 0	1 0 0 0 0 1	0 1 0 0 1 0	1 0 0 0 0 1	1 0 1 0	0 1 0 1
1 0 0 0 0 1	0 0 1 1 0 0	1 0 0 0 0 1	0 1 0 0 1 0	1 0 1 0	0 1 0 1
0 0 1 0 1 0	0 1 0 0 0 1	1 0 1 0 0 0	0 1 0 1 0 0	0 1 1 0	1 0 0 1
0 1 0 0 0 1	0 0 1 0 1 0	0 1 0 1 0 0	1 0 1 0 0 0	0 1 1 0	1 0 0 1
0 1 0 1 0 0	1 0 0 0 1 0	0 0 1 0 0 1	0 0 0 1 1 0	0 0 1 1	1 1 0 0
1 0 0 0 1 0	0 1 0 1 0 0	0 0 0 1 1 0	0 0 1 0 0 1	0 0 1 1	1 1 0 0
1 0 0 0 0 1	0 0 1 1 0 0	1 0 0 0 0 1	0 1 0 0 1 0	0 1 0 1	1 0 1 0
0 0 1 1 0 0	1 0 0 0 0 1	0 1 0 0 1 0	1 0 0 0 0 1	0 1 0 1	1 0 1 0
0 1 0 0 0 1	0 0 1 0 1 0	0 1 0 1 0 0	1 0 1 0 0 0	1 0 0 1	0 1 1 0
0 0 1 0 1 0	0 1 0 0 0 1	1 0 1 0 0 0	0 1 0 1 0 0	1 0 0 1	0 1 1 0
1 0 0 1 0 0	0 1 1 0 1 1	1 1 1 1 0 0	0 0 0 0 1 1	0 0 0 0	0 0 0 0
0 1 0 0 1 0	1 0 1 1 0 1	1 1 0 0 1 1	0 0 1 1 0 0	0 0 0 0	0 0 0 0
0 0 1 0 0 1	1 1 0 1 1 0	0 0 1 1 1 1	1 1 0 0 0 0	0 0 0 0	0 0 0 0
1 1 1 1 1 1	0 0 0 0 0 0	0 0 0 0 0 0	1 1 1 1 1 1	0 0 0 0	0 0 0 0
0 1 1 0 1 1	1 0 0 1 0 0	0 0 0 0 1 1	1 1 1 1 0 0	0 0 0 0	0 0 0 0
1 0 1 1 0 1	0 1 0 0 1 0	0 0 1 1 0 0	1 1 0 0 1 1	0 0 0 0	0 0 0 0
1 1 0 1 1 0	0 0 1 0 0 1	1 1 0 0 0 0	0 0 1 1 1 1	0 0 0 0	0 0 0 0
0 0 0 0 0 0	1 1 1 1 1 1	1 1 1 1 1 1	0 0 0 0 0 0	0 0 0 0	0 0 0 0

4. táblázat. A sajátértékek 4.2 formulával való kiszámítása $\phi \neq \phi_0$ esetén

C	Tr(C)	$\chi(C)$	$N(C) = \phi(N(C))$	$\chi(C)\phi(N(C))$
1	2	i	1	i
α	-1	i	1	i
$-1 - \alpha$	-1	-1	1	-1
-1	2	-i	1	-i
$-\alpha$	1	-i	1	-i
$1 + \alpha$	1	-1	1	-1
$-1 + \alpha$	1	1	-1	-1
$1 - \alpha$	-1	1	-1	-1
$2 + \alpha$	-1	-i	-1	i
$2 - \alpha$	1	i	-1	-i
$1 + 2\alpha$	0	-i	-1	i
$-1 + 2\alpha$	0	i	-1	-i
$\sum$	0	0	0	-4

5. táblázat. A sajátértékek 4.2 formulával való kiszámítása $\phi = \phi_0$ esetén

C	Tr(C)	$\chi(C)$	$\phi_0(N(C))$	$\chi(C)\phi_0(N(C))$
1	2	i	1	i
α	-1	i	1	i
$-1 - \alpha$	-1	-1	1	-1
-1	2	-i	1	-i
$-\alpha$	1	-i	1	-i
$1 + \alpha$	1	-1	1	-1
$-1 + \alpha$	1	1	1	1
$1 - \alpha$	-1	1	1	1
$2 + \alpha$	-1	-i	1	-i
$2 - \alpha$	1	i	1	i
$1 + 2\alpha$	0	-i	1	-i
$-1 + 2\alpha$	0	i	1	i
$\sum$	0	0	12	0

6. Összefoglalás

A dolgozatban a Galois-gyűrűkkel foglalkoztunk. A vizsgálatok megkezdése előtt rendszereztük a témakörhöz kapcsolódó definíciókat és a korábban bizonyított tételeket. A célunk pedig a projektív normagráf sajátértékeinek kiszámítása volt, amelyekre a $GR(2^2, 2^{2m})$ Galois-gyűrűk esetében előjeltől eltekintve pontos értéket kaptunk. Megadtuk továbbá ezek multiplicitását is. Eredményeinket a 4.4 tételben foglaltuk össze.

A nehézséget a normagráf megfelelő definiálása, illetve a Galois-gyűrűkön értelmezett Gauss-összegek kiszámítása jelentette. A témával kapcsolatos tételek összegyűjtése után azokat a Galois-gyűrűkről meglévő ismereteink figyelembevételével alkalmazhattuk.

A legkisebb alkalmas Galois-gyűrű, a $GR(4, 16)$ esetére kiszámoltuk az M szomszédsági mátrixot, az M^2 sajátvektorait és a sajátértékeit, továbbá az M sajátértékeinek előjeles értékét, ezzel alátámasztva és pontosítva az általános esetre kapott eredményeket.

Hivatkozások

- [1] Szabó Tibor, On the spectrum of projective norm-graphs, *Information Processing Letters*, 86 no. 2. (2003) 71-74.
- [2] Zhe-Xian Wan, Lectures on Finite Fields and Galois Rings, *World Scientific Publishing Co. Pte. Ltd.*, (2003).
- [3] 3. Yunchang Oh and Heung-Joon Oh, Gauss Sums over Galois Rings of Characteristic 4, *Kangweon-Kyungki Math. Jour.* 9 (2001), No. 1, pp. 17.
- [4] Philippe Langevin and Patrick Solé, Gauss Sums over Quasi-Frobenius Rings in: Finite fields and Applications, *Springer Verlag*, (2001), pp 329–341.
- [5] N. Alon, L. Rónyai, Szabó T., Norm-graphs: Variations and Applications, *Journal of Combinatorial Theory, (Series B)*, 76 (1999), 280-290.
- [6] Rudolf Lidl and Harald Niederreiter, Introduction to finite fields and their applications, *Cambridge University Press*, (1988)