Algebrai módszerek néhány véges geometriai és gráfelméleti probléma kapcsán

című Ph. D. disszertáció tézisei

Készítette: Kovács István

Témavezető: Dr. Szőnyi Tamás
Eötvös Loránd Tudományegyetem
Számítógéptudományi Tanszék

Szegedi Tudományegyetem, Bolyai Intézet
Szeged, 2002

1 Belső magpontok véges projektív terekben

Jelölje $\mathrm{PG}(n, q)$ a q elemű véges testre épített, n dimenziós projektív teret, lsd. [**6**]. Legyen $\mathcal{B}$ a tér néhány pontjából álló halmaz. A $P \in \mathcal{B}$ pontot a $\mathcal{B}$ *belső magpontjának* nevezzük, ha a P-t tartalmazó bármely hipersík a $\mathcal{B}$-t legfeljebb $n-1$ további pontban metszi. Egyszerűbben fogalmazva síkbeli ponthalmazokra, P belső magpontja $\mathcal{B}$-nek, ha bármely a P-n átmenő egyenes a $\mathcal{B}$-t legfeljebb egy további pontban metszi. A $\mathcal{B}$ belső magpontjainak halmazát a továbbiakban $IN(\mathcal{B})$-vel jelöljük.

Az egyszerűség kedvéért rögzítsük a következő jelöléseket: $k := |\mathcal{B}|$ és $i := |IN(\mathcal{B})|$. Legyen $\mathcal{B}$ síkbeli ponthalmaz. A $k = q+2$ és q páros esetet A. Bichara és Korchmáros G. tanulmányozták, lsd. [**1**]. Az $i \geq 3$ és q páratlan esetben a $k \leq q+1$ korlát teljesül. Wettl F. megmutatta, hogyha q páratlan és $k = q+1$, akkor $IN(\mathcal{B})$ egy kúpszeletbe írható; sőt $IN(\mathcal{B}) \neq \mathcal{B}$ esetén:

$$i \leq \frac{q+1}{2},$$

lsd. [**18**]. Azon $\mathcal{B}$ ponthalmazok leírását, melyekre $k = q+1$ és $i = \frac{q+1}{2}$ ($q > 121$ továbbra is páratlan) Szőnyi T. végezte el, lsd. [**17**].

Az 1. Fejezet célja a fenti eredmények általánosítása magasabb dimenziós terekre. Ehhez a kúpszelet egy lehetséges $\mathrm{PG}(n, q)$-beli megfelelőjét adjuk meg: a $\mathrm{PG}(n, q)$ $(2 \leq n \leq q-2)$ egy ponthalmazát n-ed rendű *normál racionális görbének* nevezzük, ha az projektíven ekvivalens a következő ponthalmazzal:

$$\mathcal{N}_n := \Big\{P(t) = \mathbf{P}(t^n, t^{n-1}, \ldots, t, 1) \,|\, t \in \mathbb{F}_q \cup \{\infty\}\Big\},$$

ahol $t = \infty$ a $\mathbf{P}(1, 0, \ldots, 0)$ pontot definiálja. Fő eredményünk a következő:

1.1. Tétel. [**10**]
(i) Legyen $\mathcal{B} \subset \mathrm{PG}(n, q)$, q páratlan, $k = q+1$, $n \geq 3$ és $i \leq \frac{q+1}{2}$. Ha

$$i \geq (4n+6)^2 + (n-2),$$

akkor $IN(\mathcal{B})$ egy normál racionális görbébe írható.

(ii) Legyen $\mathcal{B} \subset \mathrm{PG}(n, q)$, $n \geq 3$, $k = q+1$, q páratlan, $i = \frac{q+1}{2}$, és $q > q_0$. (q_0 jelölje azt a minimális q értéket, amelyre $(1+\sqrt{3})r_3(m) < 0,01m$, $m \geq q-1$, ahol $r_3(m)$ a maximális elemszáma az olyan $A \subset \{1, \ldots, m\}$ halmazoknak, melyekből nem választható ki három-elemű számtani sorozat.) Ha

$$q + 1 \geq 32n^2 + 98n + 68,$$

akkor $IN(\mathcal{B})$ projektíven ekvivalens a

$$\{P(t) \mid t = (1 + la^2)/(2a),\, a \in \mathbb{F}_q \cup \{\infty\}\} \subset \mathcal{N}_n$$

ponthalmazzal, ahol $l \in \mathbb{F}_q$ egy nem-négyzet elem. Továbbá a $\mathcal{B} \setminus IN(\mathcal{B})$-beli pontok az $\mathcal{N}_n$ egy képzetes húrjára esnek.

Az **??** Tétel-ben az (i) bizonyításához egy síkbeli állítást igazolunk először. Megmutatjuk, hogy amennyiben a síkbeli $\mathcal{B}$ halmazra teljesül, hogy

$$\sqrt{i} \geq 4(q + 2 - k) + 10, \tag{1}$$

akkor $IN(\mathcal{B})$ kúpszeletbe írható. Legyen $\mathcal{B}$ az **??** Tétel (i)-ben szereplő ponthalmaza. A bizonyítás egyik kulcsmozzanata a következő: a $\mathcal{B}$ vetítések egymás utáni alkalmazásával leképezhető egy síkbeli ponthalmazra, amelyre teljesül az (**??**)-beli feltétel, így az kúpszeletbe írható. A fenti síkbeli állítás igazolásához fő eszközünk a következő eredmény:

1.2. Tétel. [**18**]
Legyen $\mathcal{B} \subset \mathrm{PG}(2, q)$, $|\mathcal{B}| = k$, q páratlan. Megadható egy Γ_{2n} $2n$-edrendű, duális algebrai görbe ($n = q + 2 - k$), amely tartalmazza a $\mathcal{B}$ magpontjaiban húzható érintőit. Továbbá:

(i) Γ_{2n} *nem tartalmaz* $IN(\mathcal{B})$*-beli szelőt;*

(ii) $I(P, \Lambda_P \cap \Gamma_{2n}) = 2$ *bármely* $P \in IN(\mathcal{B})$ *pontra;*

(iii) Γ_{2n} *nem csak dupla komponensekből áll.*

Az **??** Tétel (ii) pontjára kapjuk (i)-ből, hogy $IN(\mathcal{B})$ egy normál racionális görbe részhalmaza. Ezt felhasználva az $IN(\mathcal{B})$ jellemzésére vonatkozó állítás következik [**16**]-ból.

2 Cayley-gráfok véges Ábel-csoportokon

Legyen $(H, +)$ egy véges Ábel-csoport, egységelemét jelöljük 0-val. A $T \subseteq H \setminus \{0\}$ részhalmaz esetén definiáljunk egy irányított Γ gráfot a következőképpen:

$$V(\Gamma) := H, \quad E(\Gamma) := \{\, (h, h + k) \in H \times H \mid h \in H,\, k \in T \,\}.$$

Γ-t a H feletti T által definiált *Cayley-gráfnak* nevezzük. A továbbiakban ezt $\mathsf{Cay}(H, T)$-vel jelöljük, lsd. [**5**]. Ha $T = -T := \{-h \mid h \in T\}$, akkor a $\mathsf{Cay}(H, T)$-n irányítatlan gráfot értünk. A $\mathsf{Cay}(H, T)$ teljes automorfizmus csoportját $\mathsf{Aut}(H, T)$-vel fogjuk jelölni. A definícióból azonnal látható, hogy $\mathsf{Aut}(H, T)$ tartalmazza a H reguláris reprerezentációját, mint egy reguláris részcsoportot. Alábbi vizsgálataink kiindulópontja a következő probléma:

(P) jellemezzük az $\mathsf{Aut}(H, T)$ csoportokat.

Jelenleg távolinak tűnik egy az összes lehetséges H-t magában foglaló leírás **(P)**-re. Disszertációnkban azt a speciális esetet tekintjük, amikor H egy prím-hatvány rendű ciklikus csoport. Jelölje Z_n az n-ed rendű ciklikus csoportot. A $\mathsf{Cay}(Z_n, T)$ Cayley-gráfokat n-ed rendű *ciklikus gráfoknak* is nevezzük. Az alábbiakban néhány később előforduló gráfokkal és permutációcsoportokkal kapcsolatos fogalmat tekintünk át:

Jelölje $(\mathbb{Z}_n, \oplus, \odot)$ a moduló n maradékosztályok gyűrűjét, melynek elemeit azonosítjuk a $\{0, 1, \ldots, n-1\}$ halmazzal. A továbbiakban szintén $\mathbb{Z}_n$-nel fogjuk jelölni a $(\mathbb{Z}_n, +)$ csoportot, és $\mathbb{Z}_n^*$-nel a $\mathbb{Z}_n$ egységeinek multiplikatív csoportját. Az alábbiak során p-n mindig egy prím számot értünk. Definiáljuk a következő permutációcsoportot:

$$\mathrm{Aff}(n, K) := \{x \mapsto a \odot x \oplus b \mid a \in K,\, b \in \mathbb{Z}_n\} \leq \mathrm{Sym}(\mathbb{Z}_n),$$

ahol $K \leq \mathbb{Z}_n^*$. Néhány számunkra fontos $\mathbb{Z}_{p^m}^*$-beli részcsoportot gyűjtünk össze $\mathcal{K}$-ban:

$$\mathcal{K} := \begin{cases} \{K \leq \mathbb{Z}_{p^m}^* \mid |K| \mid (p-1)\}, & \text{ha } p > 2; \\ \{\{1\}, \langle 2^m - 1\rangle, \langle 2^{m-1} - 1\rangle\}, & \text{ha } p = 2, m > 1. \end{cases}$$

Legyenek G_1 ill. G_2 az M_1 ill. M_2 halmazon ható permutációcsoportok. $(G_1 \wr G_2)$-vel fogjuk jelölni a G_1 és G_2 koszorú szorzatát, tehát $G_1 \wr G_2 \leq \mathrm{Sym}(M_1 \times M_2)$, melynek rendje $|G_1||G_2|^{|M_1|}$.

Legyenek Γ és Σ tetszőleges (irányított) gráfok. A Γ és Σ *lexikografikus szorzatán* a Γ^* (irányított) gráfot értjük:
$V(\Gamma^*) := V(\Gamma) \times V(\Sigma)$,
$E(\Gamma^*) := \{\, \big((x, y), (x', y')\big) \mid (x, x') \in E(\Gamma) \,\vee\, (x = x' \wedge (y, y') \in E(\Sigma))\,\}$.
Γ^*-ra a szokásos $\Gamma[\Sigma]$ jelölést fogjuk használni.

Legyen G az M halmazon ható tranzitív permutációcsoport, azaz $G \leq \mathrm{Sym}(M)$. Adott $B \subseteq M$ esetén legyen $B^g := \{x^g : x \in B\}$. A $B \subseteq M$ részhalmazt a G *blokkjának* hívjuk, ha $B^g = B$ vagy $B^g \cap B = \emptyset$ minden g-re, $g \in G$. Ha B egy blokk, akkor ez elmondható a B^g-ről is. Az összes B^g, $g \in G$, blokk a G egy particióját adja, amelyet a G *blokk-rendszerének* nevezünk, lsd. **[19]**. Nyilvánvalóan az M egyetlen elemét tartalmazó halmaz ill. a teljes M a G-nek blokkjai. Az általuk indukált blokk-rendszereket *triviálisnak* nevezzük. Azt mondjuk, hogy a G *primitív*, ha az csak triviális blokk-rendszerekkel rendelkezik.

Legyen $\mu := \{B_1, \ldots, B_k\}$ a G egy blokk-rendszere. A $g \in G$ esetén jelölje $\overline{g}$ a g által indukált permutációt μ-n. Ekkor a $g \mapsto \overline{g}$ leképezés homomorfizmus $\mathrm{Sym}(\mu)$-be, továbbá a G homomorf képe tranzitíven hat μ-n, lsd. **[19]**. Ezt a G *indukált hatásának* nevezzük, jelölése: G^μ.

Legyen Γ tetszőleges (irányított) gráf, és legyen $\mu := \{X_1, \ldots, X_k\}$ a $V(\Gamma)$ egy particiója. A Γ *μ-szerinti hányadosán* a Σ (irányított) gráfot értjük:

$$V(\Sigma) := \mu, \quad E(\Sigma) := \{(X_i, X_j) \mid i \neq j,\, \exists_{x \in X_i} \exists_{y \in X_j} : (x, y) \in E(\Gamma)\}.$$

Jelölés: $\Gamma/\mu := \Sigma$. Könnyen belátható, hogyha Γ egy csúcs-tranzitív (irányított) gráf, és μ az $\mathsf{Aut}(\Gamma)$ blokk-rendszere, akkor a természetes leképezés

$$\tau : \mathsf{Aut}(\Gamma) \to \mathrm{Sym}(\mu)$$

egy homomorfizmus $\mathsf{Aut}(\Gamma/\mu)$-be, így $\mathsf{Aut}(\Gamma)^\mu \leq \mathsf{Aut}(\Gamma/\mu)$. Ha $K = \ker(\tau)$ és G az $\mathsf{Aut}(\Gamma)$ τ-melletti képe, akkor csoportelméleti terminológiával: $\mathsf{Aut}(\Gamma)$ a K egy G-vel történő *bővítése.* Ezt a következőkben $K \bullet G$-vel jelöljük. Ez a konstrukció a **(P)** explicit megoldásánál kap majd fontos szerepet a $\Gamma = \mathsf{Cay}(Z_{p^m}, T)$, $m \leq 4$ esetben (lsd. **??** Tétel (c) pontja).

Azt mondjuk, hogy $\Gamma = \mathsf{Cay}(\mathbb{Z}_{p^m}, T)$ *felbontható*, ha az előáll kisebb rendű ciklikus gráfok lexikografikus szorzataként (természetesen az egyes komponensek rendje szintén a p hatványa). Jelölje H_i a $\mathbb{Z}_{p^m}$-nek a p^i-edrendű részcsoportját. η_i-val jelöljük a $\mathbb{Z}_{p^m}$-nek a H_i mellékosztályaiból álló partícióját. Jelölje $\Gamma^{(s)}$ a Γ-nak a H_s-beli csúcsok által feszített részgráfját.

2.1. Lemma. **[12]**
Ha a $\Gamma = \mathsf{Cay}(\mathbb{Z}_{p^m}, T)$ *nem teljes és nem üres ciklikus gráf felbontható, akkor létezik olyan* $1 \leq s \leq m-1$ *egész, hogy* $\Gamma = \Gamma/\eta_s[\Gamma^{(s)}]$ *és*

$$\mathsf{Aut}(\Gamma) = \mathsf{Aut}(\Gamma/\eta_s) \wr \mathsf{Aut}(\Gamma^{(s)}).$$

Módszerünkben fontos szerepet kapnak a $\mathsf{Cay}(H, T)$ sajátértékei. Jelölje H^* a H irreducibilis karaktereinek halmazát. Jelölje $\mathcal{V}$ a $f : H \to \mathbb{C}$ függvények terét. A H elemeinek egy rögzített $h_1, \ldots, h_n$ sorrendje mellett azonosítsuk f-et az $(f(h_1), \ldots, f(h_n))^\top$ vektorral; nyilván $H^* \subset \mathcal{V}$. Jól ismert, hogy $\chi \in H^*$ sajátvektora $\mathsf{Cay}(H, T)$-nek, továbbá a $T \neq \emptyset$ halmaz esetén a megfelelő sajátértéke: $\sum_{h \in T} \chi(h)$, lsd. **[5]**. Rögzítsük e sajátértékre a $\chi(T)$ jelölést.

A H-n értelmezhető *Fourier-transzformáció* segítségével kapcsolatot létesítünk a sajátértékek és az automorfizmusok között. Az $f \in \mathcal{V}$ esetén, definiáljuk az f *Fourier-transzformáltját* mint azt az $\hat{f} : H^* \to \mathbb{C}$ függvényt, amelyre:

$$\hat{f}(\chi) := \sum_{h \in H} f(h)\chi(-h).$$

2.2. Állítás. **[12]**

(i) Legyen $\chi \in H^*$, $F \in \mathsf{Aut}(H, T)$. *Definiáljuk az* f*-et,* $f \in \mathcal{V}$ *mint* $f(h) := \chi(F(h))$, $h \in H$. *Ekkor*

$$\forall_{\chi' \in H^*} : \hat{f}(\chi')\big(\chi'(T) - \chi(T)\big) = 0.$$

(ii) Ha a $\chi \in H^*$ *esetén:* $\ker(\chi) = \{0\}$ *és* $\chi(T)$ *multiplicitása* 1*, akkor* $\mathsf{Aut}(H, T) \cong H$. *(E feltételek mellett* $H = Z_n$*, továbbá* $\langle \chi \rangle = H^*$.*)*

(iii) Legyen $\chi \in H^*$ *és* $K = \ker(\chi)$. *Ha*

$$\forall_{\chi' \in H^*} : \chi'(T) = \chi(T) \Rightarrow K \leq \ker(\chi'),$$

akkor K *mellékosztályai az* $\mathsf{Aut}(H, T)$ *egy blokk-rendszerét adják.*

A következő lépés során a T struktúrájára következtetünk a $\chi(T)$ sajátértékek bizonyos tuljadonságaiból a $H = \mathbb{Z}_{p^m}$ esetben. Legyen ε egy primitív complex p^m-edik egységgyök. A $\mathbb{Z}_{p^m}$ karakterei a következő alakban írhatóak:

$$\chi_i : j \mapsto \varepsilon^{ij},\ i,j \in \mathbb{Z}_{p^m}.$$

Az alábbiakban rögzítsük a nem-üres $T \subseteq \mathbb{Z}_{p^m} \setminus \{0\}$ halmazt. Továbbá legyen $\Gamma := \mathsf{Cay}(\mathbb{Z}_{p^m}, T)$, és $\lambda_i := \chi_i(T)$, $i \in \mathbb{Z}_{p^m}$. Fő eredményeinket az alábbi állítás tartalmazza. Ehhez további fogalmakat vezetünk be: legyen $G(T) := \{t \in \mathbb{Z}_{p^m}^* \mid \lambda_t = \lambda_1\}$. Könnyen látható, hogy $G(T)$ részcsoportja $\mathbb{Z}_{p^m}^*$-nek. Azt mondjuk, hogy T H_i-triviális, ha $T \setminus H_i$ előáll a H_i néhány mellékosztályának uniójaként, és $T \cap H_i = \emptyset \vee H_i \setminus \{0\}$.

2.3. Állítás. [12]

(i) T két részre bontható: $T = T_1 \cup T_2$, hogy T_1 a H_1 néhány mellékosztályának uniójából áll, és $T_2 = T_2 \odot t$ bármely t-re, $t \in G(T)$.

(ii) Ha $\lambda_1 = \lambda_t$ és $p \mid t$, akkor T H_1-triviális.

(iii) Ha $\lambda_1 = \lambda_p = \ldots = \lambda_{p^k}$ valamely $1 \leq k \leq m-1$ $(1 < m)$ egészre, akkor T H_{k+1}-triviális.

(iv) Ha $k < m-1$ (iii)-ban és $\lambda_1 \neq \lambda_{p^{k+1}}$, akkor η_{k+1} egy blokk-rendszere $\mathsf{Aut}(\mathbb{Z}_{p^m}, T)$-nek.

E fejezetet a fenti állítások néhány alkalmazásával zárjuk. A **??** Állítás implikálja a következő spektrál kritériumot:

2.4. Tétel. [11]
Legyen H egy n-ed rendű $(n > 2)$ Ábel-csoport, és jelölje n' az n legnagyobb valódi osztóját. Ha $\mathsf{Aut}(H,T) \ncong H$, akkor $\mathsf{Cay}(H,T)$-nek legfeljebb n' egyszeres sajátértéke van.

Legyen G egy tranzitív permutációcsoport, mely tartalmaz egy reguláris Ábel-csoportot, jelöljük ezt H-val. Ekkor megmutatható, hogy a G izomorf egy $\mathsf{Aut}(H,T)$-beli részcsoporttal, lsd. [**11**]. Ez alapján fenti eredményeinkkel a következő klasszikusnak számító tételekhez juthatunk el. Mindkét tétel W. Burnside-tól származik:

2.5. Tétel. [3]
Bármely p-ed fokú tranzitív permutációcsoport vagy duplán tranzitív, vagy izomorf az $\mathrm{Aff}(p,K)$ csoporttal valamely $K < \mathbb{Z}_p^*$ mellett.

2.6. Tétel. [3]
Ha $m > 1$, akkor $\mathbb{Z}_{p^m}$ B-csoport, azaz bármely primitív permutációcsoport, amely tartalmaz egy tranzitív, p^m-edrendű részcsoportot, duplán tranzitív.

3 Prímhatvány rendű ciklikus gráfok automorfizmusai

3.1 Él-tranzitív ciklikus gráfok

Él-tranzitív Cayley-gráfok $\mathsf{Cay}(\mathbb{Z}_n, T)$ ($T = \ominus T$) osztályozását találjuk [**14**]-ben arra az esetre, ha n négyzetmentes. Módszerünkkel a következő osztályozás adható:

3.1. Tétel. [**13**]
Ha $\mathsf{Cay}(\mathbb{Z}_{p^m}, T)$ *él-tranzitív, akkor az a következő (irányított) gráfok egyikével azonos:*

(a) K_{p^m} *(K_n jelöli az n pontú teljes gráfot);*

(b) $\mathsf{Cay}(\mathbb{Z}_{p^m}, K)$*, ahol* $K \in \mathcal{K}$*;*

(c) $\Gamma'[\overline{K_{p^i}}]$*, ahol* $1 \leq i < m$ *és* Γ' *egy az (a)-ban vagy (b)-ben leírt* p^{m-i}*-edrendű ciklikus gráf.*

3.2 Egy implicit osztályozás

Az alábbiakban rögzítsük a $\Gamma = \mathsf{Cay}(\mathbb{Z}_{p^m}, T)$ ciklikus gráfot. Azt mondjuk, hogy Γ *s-dimenziós*, ha s az a maximális egész, hogy $T \cap \mathbb{Z}^*_{p^m}$ előáll a H_s néhány mellékosztályának uniójaként. Első lépésben $\mathsf{Aut}(\Gamma)$-nak csupán egy alkalmas blokk-rendszere által indukált hatását adjuk meg:

3.2. Tétel. (Redukciós Tétel [**12**])
Tegyük fel, hogy a Γ és komplementere $\overline{\Gamma}$ is összefüggőek. Ha Γ s-dimenziós, akkor η_s blokk-rendszere $\mathsf{Aut}(\Gamma)$*-nak; továbbá:*

$$\mathsf{Aut}(\Gamma)^{\eta_s} \cong \mathrm{Aff}(\mathbb{Z}_{p^{m-s}}, K),$$

ahol $K \in \mathcal{K}$.

A tételt s-szerinti indukcióval igazoljuk a **??**- és a **??** Állítás segítségével. Az $s = 0$ esetben a **??** Tétel a következő egyszerűbb alakot ölti: $\mathsf{Aut}(\Gamma) = \mathrm{Aff}(\mathbb{Z}_{p^m}, K)$, $K \in \mathcal{K}$.

Ha a Γ és $\overline{\Gamma}$ közül legalább egyik nem összefüggő, akkor $\mathsf{Aut}(\Gamma)$ nyilvánvaló módon határozható meg az összefüggő komponensekből. Egyébként a **??** Tétel alkalmazható, és így adódik a következő rekurzív formula $\mathsf{Aut}(\Gamma)$-ra:

3.3. Tétel. [**12**]
$\mathsf{Aut}(\Gamma)$ *egyenlő a következők valamelyikével:*

(a) $\mathrm{Sym}(\mathbb{Z}_{p^m})$*;*

(b) $\mathrm{Sym}(\mathbb{Z}_{p^{m-s}}) \wr \mathsf{Aut}(\Gamma')$*, ahol* $1 \leq s \leq m-1$ *és* $\Gamma' = \Gamma^{(s)} \vee \overline{\Gamma}^{(s)}$*;*

(c) $\mathrm{Aff}(p^m, K)$*, ahol* $K \in \mathcal{K}$*;*

(d) $\mathrm{Aff}(p^{m-s}, K) \wr \mathrm{Sym}(\mathbb{Z}_{p^s})$*, ahol* $1 \le s \le m-1$ *és* $K \in \mathcal{K}$*;*

(e) $\big(\mathrm{Aff}(p^{m-s}, K) \wr \mathrm{Sym}(\mathbb{Z}_{p^s})\big) \cap \big(\mathrm{Sym}(\mathbb{Z}_{p^{m-r}}) \wr \mathsf{Aut}(\Gamma^{(r)})\big)$,
ahol $1 \le s, r \le m-1$*, és* $K \in \mathcal{K}$*.*

3.3 Explicit osztályozás

Az $\mathsf{Aut}(\mathbb{Z}_{p^m}, T)$ explicit osztályozása a következő esetekben ismert: $m = 2$ ([**7**]), $m = 3$ ([**8**]) és $m > 3, p > 2$ ([**9**]). A fenti cikkek mindegyike a $\mathbb{Z}_{p^m}$-n értelmezett Schur-gyűrűk használatára épült.

Módszerünkkel megadjuk az explicit karakterizációt az $1 \le m \le 4$ esetekben. Például, az $m = 2$ esetben könnyen látható, hogy bármely p^2-edrendű ciklikus gráf vagy 0-dimenziós vagy felbontható. Ezért a karakterizáció azonnal következik a **??** Lemma-ból és a **??** Tétel-ből.

E helyen csak az $m = 4$ és $p > 2$ esetre vonatkozó eredményt közöljük:

3.4. Tétel. [12]
Legyen Γ *egy* p^4*-edrendű ciklikus gráf,* $p > 2$*. Ekkor az* $\mathsf{Aut}(\Gamma)$ *a következő típusok valamelyikéhez tartozik:*

(a) $\mathrm{Sym}(\mathbb{Z}_{p^4})$*;*

(b) $\mathsf{Aut}(\Gamma_1) \wr \mathsf{Aut}(\Gamma_2)$*, ahol* Γ_1 *ill.* Γ_2 *valamely* p^s*-edrendű ill.* p^{4-s}*-edrendű ciklikus gráfok (*$1 \le s \le 3$*);*

(c) $\mathrm{Aff}(p^4, K)$*,* $\mathbb{Z}_p^p \bullet \mathrm{Aff}(p^3, K)$*,* $\mathbb{Z}_p^{p^2} \bullet \mathrm{Aff}(p^3, K)$*,* $\mathbb{Z}_{p^2}^p \bullet \mathrm{Aff}(p^2, K)$*,* $\mathbb{Z}_p^{p^2} \bullet \big(\mathbb{Z}_p^p \bullet \mathrm{Aff}(p^2, K)\big)$*, ahol* $K \in \mathcal{K}$*.*

4 A. E. Brouwer egy sejtésének megoldása

Jelölje $\Gamma^{(q)}$ a q-ad rendű Paley-gráf ($q := p^e$) egy csúcs szomszédjai által feszített részgráfját, azaz:

$$V(\Gamma^{(q)}) := (\mathbb{F}_q^*)^2, \quad E(\Gamma^{(q)}) := \{(x, y) \in (\mathbb{F}_q^*)^2 \times (\mathbb{F}_q^*)^2 \mid x - y \in (\mathbb{F}_q^*)^2\}.$$

Legyen $\mathbb{A} := (\mathbb{F}_q^*)^2$. Brouwer-től származik a következő sejtés, lsd. [**2**]:

4.1. Sejtés.

$$\mathsf{Aut}(\Gamma^{(q)}) = H := \{x \mapsto ax^{\pm p^i} \mid a \in \mathbb{A},\ 0 \le i \le e-1\} \le \mathrm{Sym}(\mathbb{A}).$$

Jelölje H_0 az $1 \in \mathbb{F}_q$ elem H-beli stabilizátorát. E fejezetben a problémát a Schur-gyűrűk nyelvére fogalmazzuk át, lsd [**4**]. Jelölje $\langle\langle\Gamma^{(q)}\rangle\rangle$ az $(\mathbb{F}_q^*)^2$-n értelmezett a $\Gamma^{(q)}$ által generált Schur-gyűrűt. Mivel $\mathsf{Aut}(\Gamma^{(q)}) = \mathsf{Aut}(\langle\langle\Gamma^{(q)}\rangle\rangle)$, Brouwer sejtése a következő állításokkal nyer igazolást:

4.2. Tétel. [15]
Legyen $\mathcal{R}$ *az* $(\mathbb{F}_q^*)^2$*-n értelmezett, és a* H_0*-hoz tartozó tranzitivitás-modulus. Ekkor*

$$\langle\!\langle \Gamma^{(q)} \rangle\!\rangle = \mathcal{R}.$$

4.3. Tétel. [15]
A fenti $\mathcal{R}$ *esetén,*

$$\mathsf{Aut}(\mathcal{R}) = H.$$

A **??** Tétel bizonyítása során spektrál technikákat kombinálunk Schur-gyűrű elméleti eredményekkel.

Irodalomjegyzék

[1] A. Bichara, G. Korchmáros, *Note on* $(q+2)$*-sets in a Galois plane of order* q*,* Annals of Discrete Math. **14** (1982), 117–122.

[2] A. E. Brouwer, *Locally Paley graphs,* Designs, Codes and Cryptography **21** (2000), 69–76.

[3] W. Burnside, *Theory of Groups of Finite Order,* 2nd ed., Cambridge University Press, Cambridge, UK, 1911.

[4] I. A. Faradžev, M. H. Klin, M. E. Muzychuk, *Cellular rings and groups of automorphisms of graphs,* In: Investigations on Algebraic Theory of Combinatorial Objects. Mathematics and Its Applications (Soviet Series, eds. I. A. Faradžev et al.), Kluwer Acad. Publ. **84** (1994), 1–152.

[5] C. Godsil, *Algebraic Combinatorics,* Chapman & Hall, New York 1993.

[6] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Mathematical Monographs, Clarendon Press 1998.

[7] M. H. Klin, *Automorphism Groups of Circulant Graphs,* Tagungsbericht of the conference Applicable Algebra, Oberwolfach, 14–20 Februar 1993, pp. 12.

[8] M. H. Klin and R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings,* Algebraic methods in graph theory, Vol. I,II (Szeged 1978), Colloq. Math. Soc. János Bolyai **25** (1981), 405–434.

[9] M. H. Klin and R. Pöschel, *Circulant graphs via Schur ring theory, II. Automorphism groups of circulant graphs on* p^n *vertices,* p *an odd prime,* Manuscript.

[10] I. Kovács, *On the Internal Nuclei of Sets in* $PG(n,q)$*,* q *is Odd,* Designs, Codes and Cryptography Vol.**24** (2001), 37–42.

[11] I. Kovács, *On automorphisms of Cayley-digraphs of abelian groups,* to appear in Discrete Math.

[12] I. Kovács, *On the automorphisms of circulants on* p^m *vertices,* p *an odd prime,* to appear in Linear Algebra and its Applications.

[13] I. Kovács, *Classifying arc-transitive circulants of prime-power order,* presented at the conference Combinatorics 2002, Maratea (Italy), July 2–10 2002.

[14] C. Li, D. Marušič, J. Morris, *Classifying Arc-Transitive Circulants of Square-Free Order,* J. of Algebraic Combinatorics **14** (2001), 145–151.

[15] M. Muzychuk, I. Kovács, *A solution of a problem of A.E. Brouwer,* submitted to the proceedings of the conference Geometric and Algebraic Combinatorics, Oisterwijk (The Netherlands), August 10–17, 2002.

[16] L. Storme, T. Szőnyi, *Intersection of arcs and normal rational curves in spaces of odd characteristic,* Finite Geometry and Combinatorics (ed. F. De Clerck at al.), Cambridge University Press 1993, 359–378.

[17] T. Szőnyi, *k-Sets in $PG(2, q)$ having a large set of internal nuclei,* in: Combinatorics '88, Volume 2 (eds. A. Barlotti et al.) Mediterranean Press, Rende (1991), 449–458.

[18] F. Wettl, *On the nuclei of a pointset of a finite projective plane,* Journal of Geometry **30** (1987), 157–163.

[19] H. Wielandt, *Finite Permutation Groups,* Academic Press, Berlin, 1964.