Többszörösen élesen tranzitív halmazok véges csoportokban

habilitációs tudományos előadás

Nagy Gábor Péter

Szegedi Tudományegyetem
Bolyai Intézet, Geometria Tanszék

2013. március 12.

Áttekintés

1. A probléma története
2. Eredmények majdnem egyszerű csoportokra
3. Eredmények affin típusú csoportokra
4. Permutation codes

Tartalomjegyzék

Élesen 2-tranzitív halmazok 2-tranzitív csoportokban

Program az 1970-es évektől (Lorimer, O'Nan, Grundhöfer, Müller)

Mutassuk meg a véges 2-tranzitív csoportok különböző osztályaira, hogy nem tartalmaznak élesen 2-tranzitív halmazokat.

A máig nyitott esetek:

1. Affin típus: $G = \mathbb{F}_p^{2n} \rtimes \mathsf{Sp}(2n, q)$, ahol q páratlan.
2. Sporadikus majdnem egyszerű típusú: 24-ed fokú M_{24} Mathieu-csoport.
3. A rossz fiú: $G = S_n$.
   A Bruck-Ryser tétel (1949) szerint ekkor **vagy** n két négyzet összege **vagy** $n \equiv 0, 3 \pmod 4$.
   Lam-Thiel-Swiercz komputereredménye (1989) szerint $n \neq 10$.
4. A kellemes meglepetés: $G = A_n$. Szükséges feltétel: $n \equiv 0, 1 \pmod 4$.

Módszerek

Korábban használt módszerek egyes 2-tranzitív permutációcsoport osztályok kizárására:

- Lorimer-féle leszámlálási módszerek (1973): $\mathsf{PU}(3, q^2)$ valamint a Ree- és a Suzuki-csoportok.
- O'Nan-féle „ellentmondó részcsoport" módszer (1985): $\mathsf{P\Gamma L}(m, q)$ és a Higman-Sims sporadikus egyszerű csoport.
- Theo Grundhöfer és Peter Müller karakterelméleti módszere (2008): $\mathsf{PSp}(2d, 2)$ 2-tranzitív hatása és a Co_3 Conway-csoport.
- Számítógépes módszerek P. Östergård CLIQUER és L. Soicher GRAPE programjai felhasználásával. (Klikk-keresés a permutáció-gráfban.)

A fő Lemmánk

Lemma

Legyen G az Ω véges halmazon ható permutációcsoport. Tegyük fel, hogy a B, C részhalmazokra és a p prímre teljesül $p \nmid |B||C|$ és $p \mid |B \cap g(C)|$ bármely $g \in G$ esetén. Ekkor G nem tartalmaz élesen tranzitív permutációhalmazt.

Bizonyítás. Tegyük fel, hogy $S \subseteq G$ élesen tranzitív halmaz. A

$$\{(b, c, s) \mid b \in B, c \in C, s \in S, s(c) = b\},$$

halmazt kétszeresen leszámlálva kapjuk, hogy

$$|B||C| = \sum_{s \in S} |B \cap s(C)| \equiv 0 \pmod{p}.$$

Ellentmondás. □

Tartalomjegyzék

1. alkalmazás: Élesen 2-tranzitív halmazok A_n-ben

Tétel (P. Müller, GN, 2010)

Ha $n \equiv 2, 3 \pmod 4$, akkor az A_n alternáló csoport nem tartalmaz élesen 2-tranzitív permutációhalmazt.

Bizonyítás.

- Legyen $B = \{(i,j) \mid i < j\}$, $C = \{(i,j) \mid i > j\}$.
- Az n-re tett feltétel szerint $|B| = |C| = n(n-1)/2$ **páratlan.**
- A $g \in S_n$ permutáció **paritásának** definíciója szerint

$$|\{(i,j) \mid i < j,\ i^g > j^g\}| \equiv \operatorname{sgn}(g) \pmod 2.$$

- Ebből következik $|B \cap C^g| \equiv 0 \pmod 2$ minden $g \in A_n$ esetén. □

Következmény

Az M_{23} Mathieu-csoport nem tartalmaz élesen 2-tranzitív halmazt.

2. alkalmazás: Élesen 1-tranzitív halmazok M_{22}-ben

Tétel (P. Müller, GN, 2010)

A 22-edfokó természetes permutációelőállításában az M_{22} Mathieu-csoport nem tartalmaz élesen tranzitív halmazt.

Bizonyítás.

- Definiáljuk a $\mathcal{W}_{23}$ Witt-dizájnt az $\Omega' = \{1, \ldots, 23\}$ ponthalmazon.
- Reprezentáljuk M_{23}-at mint $\mathcal{W}_{23}$ automorfizmuscsoportját.
- Legyen $\Omega = \{1, \ldots, 22\}$ és $G = M_{22}$ a $23 \in \Omega'$ elem stabilizátora.
- Legyen $B \subset \Omega$ a $\mathcal{W}_{23}$ egy blokkja és $C = \Omega \setminus B$.
- Ekkor $|B| = 7, |C| = 15$ és minden $g \in G$ esetén $|B \cap C^g| = 0, 4$ vagy 6.
- $p = 2$ választással a tétel következik a Lemmából. □

Következmény

Az M_{23} Mathieu-csoport nem tartalmaz élesen 2-tranzitív halmazt.

3. alkalmazás: Szimmetrikus dizájn automorfizmuscsoportja

Tétel (Lorimer, 1973)

Ha $k \geq 2$ és $q \geq 5$, akkor $G = \mathsf{P\Gamma L}(k, q)$ nem tartalmaz élesen 2-tranzitív permutációhalmazt.

Bizonyítás. Leszámlálás.

Tétel (O'Nan, 1985)

$G = \mathsf{P\Gamma L}(k, q)$ nem tartalmaz élesen 2-tranzitív permutációhalmazt, kivéve ha $k = 2$ és $q = 2, 3, 4$.

Bizonyítás. Karakterelméletet használ. □ Éles.

Tétel (P. Müller, GN, 2010)

Legyen D nemtriviális szimmetrikus dizájn és $G = \mathrm{Aut}(D)$. Ekkor G nem tartalmaz élesen 2-tranzitív permutációhalmazt.

Bizonyítás. Kombinatorikus. □ Esetünkben $D = \mathsf{PG}(k-1, q)$, $k \geq 3$.

O'Nan tételének kombinatorikus bizonyítása

Bemutatjuk a szimmetrikus dizájn módszert a projektív tér példáján.

Tétel (O'Nan, 1985)

Legyen $G = \mathrm{P\Gamma L}(k, q)$ a $\mathsf{PG}(k-1, q)$ projektív téren vett természetes hatásában, $k \geq 3$. Ekkor G nem tartalmaz élesen 2-tranzitív halmazt.

Bizonyítás.

- Legyen $B = C$ hipersík, $P \notin B$, és S élesen 2-tranzitív halmaz G-ben.
- Jelölje a, b azon $s \in S_P$ permutációk számát, melyekre $s(B) = B$, illetve $s(B) \neq B$. Ekkor $|B|^2 = \sum_{s \in S_P} |B \cap s(B)|$ miatt

$$\begin{aligned} a + b &= |\mathsf{PG}(k-1, q)| - 1 \\ a\,|\mathsf{PG}(k-2, q)| + b\,|\mathsf{PG}(k-3, q)| &= |\mathsf{PG}(k-2, q)|^2 \end{aligned}$$

- Ebből $a = \dfrac{q^{k-1} - 1}{q^{k-2}(q-1)}$, ellentmondás. □

Tartalomjegyzék

4^{th} application: Sharply 1-transitive sets in $\mathsf{Sp}(2n, 2^m)$

Proposition (P. Müller, GN, 2010)

Let n, m be positive integers, $n \geq 2$, $q = 2^m$. Let $G = \mathsf{Sp}(2n, q)$ be the permutation group in its natural permutation actions on $\Omega = \mathbb{F}_q^{2n} \setminus \{0\}$. Then, G does not contain a sharply transitive set of permutations.

Bizonyítás.

- Let $\mathcal{E}$ be an elliptic quadric of $\mathsf{PG}(2n-1, q)$ whose quadratic equation polarizes to the invariant symplectic form $\langle ., . \rangle$ of G.
- Let ℓ be a line of $\mathsf{PG}(2n-1, q)$ which is nonsingular with respect to $\langle ., . \rangle$.
- Then for any $g \in G$, ℓ^g is nonsingular and $|\mathcal{E} \cap \ell^g| = 0$ or 2.
- Furthermore, both $|\mathcal{E}|$ and $|\ell|$ are odd for $n \geq 2$. We apply the Main Lemma with $B = \mathcal{E}$, $C = \ell$ and $p = 2$. □

Theorem (GN, 2012)

Let $G \leq \mathsf{GL}(d,p)$ be a transitive linear group acting on $\mathbb{F}_p^d \setminus \{0\}$. Assume that G contains a sharply transitive set. Then, one of the following holds:

1. $G \leq \Gamma\mathsf{L}(1,p^d)$ and the corresponding translation plane is a generalized André plane.
2. $G \triangleright \mathsf{SL}(d/e,p^e)$ for some divisor $e < d$ of d with $e \neq d$.
3. p is odd and $G \triangleright \mathsf{Sp}(d/e,p^e)$ for some divisor e of d.
4. $p^d \in \{5^2, 7^2, 11^2, 17^2, 23^2, 29^2, 59^2\}$ and G is one of the seven finite sharply transitive linear groups of Zassenhaus. The corresponding translation planes are called Zassenhaus nearfield planes.
5. $p^d \in \{5^2, 7^2, 11^2\}$, and G is a solvable exceptional transitive linear group.
6. $p^d = 3^4, 19^2$ or 29^2, and the number of translation planes is 21, 3 or 8, respectively.
7. $p^d = 16$ and $G = A_7$. The corresponding translation planes are the Lorimer-Rahilly and Johnson-Walker planes.

Tartalomjegyzék

Error correction block codes

- We call the finite set Ω an alphabet.
- An element $\boldsymbol{x} \in \Omega^n$ is a word of length n.
- The Hamming distance of the words $\boldsymbol{x}, \boldsymbol{y} \in \Omega^n$ is

$$d(\boldsymbol{x}, \boldsymbol{y}) = |\{i \mid x_i \neq y_i\}|.$$

- A subset $C \subseteq \Omega^n$ is a block code of length n. The elements of C are called codewords.
- The minimum distance of C is

$$d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

- Important parameters: length n, minimum distance d and the rate

$$R = \frac{\log_{|\Omega|} |C|}{n}.$$

- Aim: Codes with given parameters. Good params: R, d/n large.

Permutation codes and sharply t-transitive sets

Definition

$C \subseteq \Omega^n$ is a permutation code of length n provided $|\Omega| = n$ and each symbol $\omega \in \Omega$ occurs precisely once in each codeword $\boldsymbol{x} \in C$.

Proposition

The following are the same:

- Sharply t-transitive sets of permutations of degree n.
- Permutation codes of minimum distance $n - t + 1$ and maximum size $n(n-1)\cdots(n-t+1)$.

Permutation codes and powerline communication (PLC)

- Powerline Ethernet Networking (PLN)
- Bandwidth 200-500 Mbps
- Broadband over powerline (BPL)
- **Bad:** Powering up/down
- Smart Grid

- Symbols are small orthogonal frequency modulations
- **Power output must remain constant:**
  $\longrightarrow$ Symbol ω_i must occur r_i times in each block of length n; $r_1 + \cdots + r_{|\Omega|} = n$
- **Gaussian white noise:**
  $\longrightarrow$ usual error correction methods
- **Narrow band noise:** masks small number of frenquencies over a long period of time
  $\longrightarrow$ $|\Omega|$ large and r_i small for all i
- **Impulse noise:** masks all frequencies for a small number of time slots
  $\longrightarrow$ keep the length n „short”

THANK YOU FOR YOUR ATTENTION!!!

KÖSZÖNÖM A FIGYELMET!!!