Hemisystems and Strongly Regular Graphs

Valentino Smaldore

Università degli Studi di Padova

Combinatorial Designs and Codes

joint works with V. Pallozzi Lavorante and F. Romaniello

July 9, 2024

Hemisystems on $H(3, q^2)$

m-regular systems

$\mathcal{P}_{d,e}$:=polar space of rank (vector dimension of a maximal subspace) d, and e as follows:

$\mathcal{P}_{d,e}$	$Q^+(2d-1,q)$	$H(2d-1,q)$	$W(2d-1,q)$	$Q(2d,q)$	$H(2d,q)$	$Q^-(2d+1,q)$
e	0	1/2	1	1	3/2	2

$\mathcal{M}_{\mathcal{P}_{d,e}}$ will denote the set of generators of the polar space $\mathcal{P}_{d,e}$, while $|\mathcal{M}_{\mathcal{P}_{d-1,e}}|$ will denote the number of generators passing through a point.

Definition

A (non-trivial) m-regular system on a polar space $\mathcal{P}_{d,e}$ is a set $\mathcal{R}$ of generators such that every point of $\mathcal{P}_{d,e}$ lies on exactly m generators in $\mathcal{R}$, $0 < m < |\mathcal{M}_{\mathcal{P}_{d-1,e}}|$.

Hemisystems on $H(3, q^2)$

Segre's Theorem

m-regular systems were introduced on Hermitian varieties by Beniamino Segre in *Forme e geometrie hermitiane, con particolare riguardo al caso finito*. In that article Segre proved the following theorem on Hermitian surfaces $H(3, q^2)$, whose generators are lines, and each point lies on $n = q + 1$ of them.

Theorem (Segre's Theorem, 1965)

Let $\mathcal{H} = H(3, q^2)$ be an Hermitian surface. m-regular systems do not exist for q even. If q is odd, all the m-regular systems on $\mathcal{H}$ are hemistystems, i.e. $m = \frac{n}{2} = \frac{q+1}{2}$.

Hemisystems on $H(3, q^2)$

Segre's hemisystem on $H(3,9)$

$q = 3$
$|H(3,9)| = 280$
$|\mathcal{M}_{H(3,9)}| = 112.$

Proposition (B. Segre, 1965)

There exists a hemisystem, unique up to isomorphism, of 56 generator lines on the Hermitian surface $H(3,9)$.

Hemisystems on $H(3, q^2)$
Thas' conjecture

Hemisystems on $H(3, q^2)$

Results for $q > 3$

1. *Hemisystems on the Hermitian surface*, A. Cossidente, T. Penttila, Journal of the London Mathematical Society, 72(2), pp. 731-741, 2005.
2. *Every flock generalized quadrangle has a hemisystem*, J. Bamberg, M. Giudici, G.F. Royle, Bulletin of the London Mathematical Society, 42 pp. 795–810, 2010.
3. *Hemisystems of small flock generalized quadrangles*, J. Bamberg, M. Giudici, G.F. Royle, Designs Codes and Cryptography, 67, pp. 137–157, 2013.
4. *A new infinite family of hemisystems of the Hermitian surface*, J. Bamberg, M. Lee, K. Momihara, Q. Xiang, Combinatorica, 38, pp. 43–66, 2018.

New hemisystem of the Hermitian surface

Korchmáros-Nagy-Speziali construction

Theorem (G. Korchmáros, G. Nagy, P. Speziali, 2019)

Let p be a prime number where $p = 1 + 16a^2$, with an integer a. Then there exist an hemisystem in the Hermitian surface $H(3, p^2)$ of $PG(3, p^2)$.

Theorem (V. Pallozzi Lavorante, V.S., 2023)

The previous theorem holds also when $p = 1 + 4a^2$.

The new hemisystem
Maximal curves

$\mathcal{X}$:=projective algebraic curve of $PG(3, q^2)$.

Theorem (Hasse-Weil bound)

$|N_{q^2}(\mathcal{X}) - q^2 - 1| \leq 2\mathfrak{g}q$, *where* $\mathfrak{g}$ *is the genus of* $\mathcal{X}$.

Definition

A curve $\mathcal{X}$ *is maximal if its number of points* $N_{q^2}(\mathcal{X})$ *attains the Hasse-Weil upper bound.*

The new hemisystem
Sufficient conditions

$\mathcal{X}$ maximal curve naturally embedded in $H(3,q^2)$.
$\forall P \in H(3,q^2) \setminus \mathcal{X}$, let n_P be the number of generators on P meeting $\mathcal{X}$.

Definition

The set of generators $\mathcal{M}$ is an half-hemisystem on $\mathcal{X}$ if:

(A) *On each $Q \in \mathcal{X}$ there are exactly $\frac{q+1}{2}$ generators from $\mathcal{M}$.*

(B) *For any point $P \in H(3,q^2) \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{n_P}{2}$ generators on P meeting $\mathcal{X}$.*

$\mathcal{H}$ set of all imaginary chords of $\mathcal{X}$.

Theorem

$\mathcal{M} \cup \mathcal{H}$ is an hemisystem of $H(3,q^2)$.

The new hemisystem
Fuhrmann-Torres curve

$$\mathcal{X}^+ := Y^q - YZ^{q-1} = X^{\frac{q+1}{2}} Z^{\frac{q-1}{2}}.$$
$$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{\frac{q+1}{2}} = v^q - v, u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1)\}.$$

Proposition

- *$\mathcal{X}^+$ has genus $\mathfrak{g}(\mathcal{X}^+) = \frac{1}{4}(q-1)^2$;*
- *$N_{q^2}(\mathcal{X}^+) = \frac{1}{2}(q^3 + q) + 1$;*
- *$Aut(\mathcal{X}^+)$ has an index 2 subgroup isomorphic to $PSL(2, q) \times C_{\frac{q+1}{2}}$.*

The new hemisystem

- $\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
- $Z(\mathfrak{G}) = C_{\frac{q+1}{2}}$;
- $\mathfrak{G}/C_{\frac{q+1}{2}} \cong PGL(2, q)$;
- $\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{\frac{q+1}{2}}$;

$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$.

- Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1; then the orbit $\mathcal{M}_1$ of ℓ_1 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)(q^3 - q)$;
- Take a point $P_2 \in \Omega$, together with a generator ℓ_2 on P_2; then the orbit $\mathcal{M}_2$ of ℓ_2 has size $\frac{1}{2}(q+1)^2$.

$$\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$$

While $\mathcal{X}$ is the normal rational curve we get the Cossidente-Penttila hemisystem, $\mathfrak{G} := PGL(2, q^2)$, $\mathfrak{H} := PSL(2, q^2)$.

Strongly regular graphs
Definitions

Definition

A graph G is a pair $(V(G), E(G))$ where

- *$V = V(G)$ is a non-empty set of element called vertices*
- *$E = E(G)$ is the set of edges, together with an incidence function $\phi : E \to V \times V$: if $\phi(e) = \{u, v\}$ we say that e joins u and v, and those are called adjacent vertices or neighbours.*

Definition

A strongly regular graph with parameters (v, k, λ, μ) is a graph with v vertices, each vertex lies on k edges, any two adjacent vertices have λ common neighbours and any two non-adjacent vertices have μ common neighbours.

Strongly regular graphs

Strongly regular graph on the lines of $\mathcal{E}$

$V(\Gamma) := \mathcal{E}$.
$E(\Gamma) := \{(\ell, r) | \ell \cap r \neq \emptyset\}$.

Proposition

Γ *is an srg* $\left(\frac{(q^3+1)(q+1)}{2}, \frac{(q^2+1)(q-1)}{2}, \frac{q-3}{2}, \frac{(q-1)^2}{2}\right)$.

While $q = 5$ **we get the Cossidente-Penttila strongly regular graph,** $G = srg(378, 52, 1, 8)$.

Strongly regular graphs

Strongly regular graph on the lines of $\mathcal{E}$

Lemma

Let $\mathcal{E}$ be an hemisystem of the Hermitian surface $H(3, q^2)$, $q > 3$. Then the automorphism group of the graph $\Gamma_{\mathcal{E}}$ is isomorphic to the automorphism group of $\mathcal{E}$.

Proof.

Trivially $Aut(\mathcal{E}) \leq Aut(\Gamma_{\mathcal{E}})$. Since $H(3, q^2)$ does not contain triangles, thus maximal cliques of the graphs are made of the $\frac{q+1}{2}$ lines through a point, permuted by the graph automorphisms. □

Theorem

The isomorphism classes of hemisystems of $H(3, q^2)$ are in 1-to-1 correspondence with the isomorphism classes of related srg's.

Strongly regular graphs
Case $q = 3$

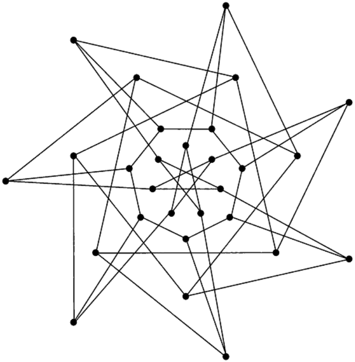
While $q = 3$ the Cossidente-Penttila strongly regular graph has parameters $(56, 10, 0, 2)$. The $srg(56, 10, 0, 2)$ is usually called *Gewirtz graph*.

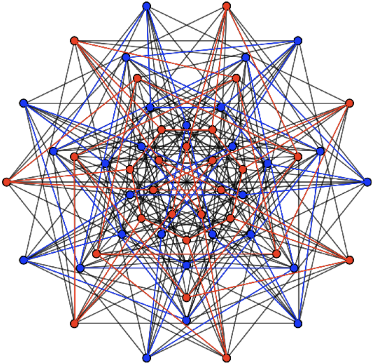
Proposition (A. E. Brouwer, W. Haemers, 1993)

The Gewirtz graph is defined by its spectrum.

Strongly regular graphs

Case $q = 3$

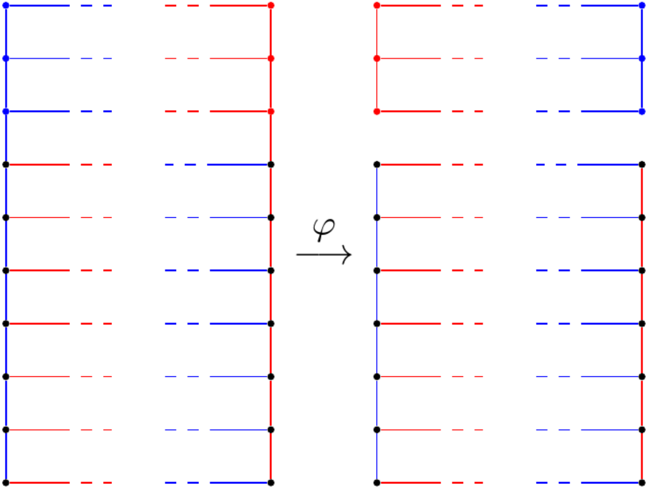




The Gewirtz graph splits into two copies of the *Coxeter graph* G, a cubic graph with 28 vertices, 42 edges, and $Aut(G) \cong PGL(2, 7)$.

Strongly regular graphs

Case $q = 3$



Strongly regular graphs
Case $q = 3$

Proposition

Both Segre's hemisystem and Gewirtz graph are unique up to isomorphisms.

Theorem (V. Pallozzi Lavorante, F. Romaniello, V. S.)

$$Aut(\Gamma_{\mathcal{E}}) \cong Aut(\mathcal{E}) \rtimes \langle \varphi \rangle \cong PSL(3,4).V$$

Strongly regular graphs

Plücker coordinates and Klein Quadric

Definition

Take $u = (u_0, u_1, u_2, u_3), v = (v_0, v_1, v_2, v_3) \in PG(3, q)$*. The line* $\langle u, v\rangle$ *has Plücker coordinates* $(p_{01}, p_{02}, p_{03}, p_{12}, p_{13}, p_{23})$ *where*

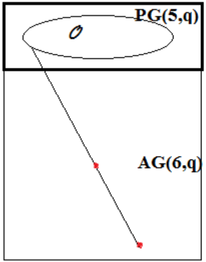
$$p_{ij} = \begin{vmatrix} u_i & u_j \\ v_i & v_j \end{vmatrix} = u_i v_j - u_j v_i .$$

The *Klein correspondence* $\mathcal{K}$ maps lines of $PG(3, q)$ in points of the *Klein Quadric* $Q^+(5, q) := p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0$.

Lines	**Points**
$PG(3, q)$	Klein Quadric $Q^+(5, q) \subseteq PG(5, q)$
$H(3, q^2)$	$Q^-(5, q)$ in a Baer subgeometry $PG(5, q) \subseteq PG(5, q^2)$
Hemisystem	$(\frac{q+1}{2})$-ovoid of $Q^-(5, q)$

Strongly regular graphs

Linear Representation



$X_\infty := PG(5,q)$

$V(\Gamma) := PG(6,q) \setminus X_\infty \cong AG(6,q).$
$E(\Gamma) := \{(x,y) | \{\langle x,y\rangle \cap X_\infty\} \in \mathcal{O}\}.$

Proposition

Γ *is an* $srg(q^6, \frac{1}{2}(q^3+1)(q^2-1), \frac{1}{4}(q^4-5), \frac{1}{4}(q^4-1)).$

Two-weight codes

$[n, k]_q$-linear codes

Definition

An $[n, k]_q$-linear code $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ of dimension k.
The elements of $\mathcal{C}$ are said codewords.

Definition

- *The Hamming distance between two codewords $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ is the number of entries in which x and y differ:* $d(x, y) = |\{i | x_i \neq y_i\}|$.
- *The minimum distance of a code $\mathcal{C}$ is* $d = d(\mathcal{C}) = min\{d(x, y) | x, y \in \mathcal{C}, x \neq y\}$.

In this case we say $\mathcal{C}$ is a $[n, k, d]_q$-linear code.

Theorem

Let $\mathcal{C}$ be a $[n, k, d]_q$-linear code. Then, $\mathcal{C}$ can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.
If is used for detection, $\mathcal{C}$ can detect $d - 1$ errors.

Two-weight codes

Hamming weight

Definition

Let $\mathcal{C}$ be a $[n, k, d]_q$-linear code.

- *The Hamming weight of a codeword c is the number of non-zero entries of c, i.e. $w(c) = d(c, 0)$.*
- *The minimum weight of a code $\mathcal{C}$ is $w(\mathcal{C}) = min\{w(c) | c \in \mathcal{C}, c \neq 0\}$.*

Proposition

Let $\mathcal{C}$ be a $[n, k]_q$-linear code, then $d(\mathcal{C}) = w(\mathcal{C})$.

The minimum distance can be found studying weights!!

Two-weight codes

$\Omega \subseteq \mathbb{F}_q^k$, with $\Omega = -\Omega$ and $0 \notin \Omega$, define the graph $G(\Omega)$:
$V(G(\Omega)) := \mathbb{F}_q^k$.
$E(G(\Omega)) := \{(x, y) | x - y \in \Omega\}$.
$PG(k-1, q) \supseteq \Sigma := \{\langle \mathbf{v} \rangle \ : \ \mathbf{v} \in \Omega\}$.

Theorem (R. Calderbank, W. M. Kantor, 1986)

If $\Sigma = \{\langle \mathbf{v_i} \rangle \ : \ i = 1, \ldots, n\}$ is a proper subset of $PG(k-1, q)$ that spans $PG(k-1, q)$, then the following are equivalent:

(i) *$G(\Omega)$ is a strongly regular graph;*

(ii) *Σ is a projective $(n, k, n - w_1, n - w_2)$-set for some w_1 and w_2;*

(iii) *the linear code $C = \{(\mathbf{x} \cdot \mathbf{v_1}, \mathbf{x} \cdot \mathbf{v_2}, \ldots, \mathbf{x} \cdot \mathbf{v_n}) \ : \ \mathbf{x} \in \mathbb{F}_q^k\}$ (here $\mathbf{x} \cdot \mathbf{v}$ is the classical scalar product) is an $[n, k]_q$-linear two-weight code with weights w_1 and w_2.*

Two-weight codes

New results

Proposition

The $(\frac{q+1}{2})$-ovoid $\mathcal{O}$ is a projective $(\frac{1}{2}(q^3+1)(q+1), 6, \frac{1}{2}(q^2+1)(q+1), \frac{1}{2}(q^3-q^2+q+1))$-set, which gives the $[\frac{1}{2}(q^3+1)(q+1), 6, \frac{1}{2}q^2(q^2-1)]_q$-linear two-weight code with weights $w_1 = \frac{1}{2}q^2(q^2-1)$ and $w_2 = \frac{1}{2}q^2(q^2+1)$.

Corollary

There exists a $[375, 6, 300]_5$-linear two-weight code with weights $w_1 = 300$ and $w_2 = 325$.

Problem

Find if the two-weight codes arising from non-isomorphic hemisystems are equivalent or not.


GAME
OVER