Contemporary algebraic and geometric techniques in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

Two-weight codes and hemisystems

Valentino Smaldore

Affiliation: Università degli Studi della Basilicata
Italy

Abstract

An $[n,k]$-linear code C over the finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. Vectors in C are called *codewords*, and the weight $w(v)$ of $v \in C$ is the number of non-zero entries in v. A *two-weight code* is an $[n,k]$-linear code C such that $|\{w : \exists v \in C \setminus \{\underline{0}\} \; w(v) = w\}| = 2$. R. Calderbank and W. M. Kantor in their seminal paper [2], described a connection between two-weight codes, strongly regular graphs and combinatorial structures as regular systems, ovoids and projective (n,k,h_1,h_2)-sets, i.e. proper, non-empty sets Σ of n points of the projective space $\mathrm{PG}(k-1,q)$ such that every hyperplane meets Σ in either h_1 or h_2 points.

For a subset Ω of $\mathbb{F}_q^k$, with $\Omega = -\Omega$ and $0 \notin \Omega$, define $G(\Omega)$ to be the graph whose vertices are the vectors of $\mathbb{F}_q^k$, and two vertices are adjacent if and only if their difference is in Ω. Moreover, let Σ denote the set of points in $\mathrm{PG}(k-1,q)$ that correspond to the vectors in Ω, i.e. $\Sigma = \{\langle \mathbf{v} \rangle : \mathbf{v} \in \Omega\}$.

Theorem 0.1 ([2, Theorems 3.1 and 3.2]) *Let Ω and Σ be defined as above. If $\Sigma = \{\langle \mathbf{v_i} \rangle : i = 1,\dots,n\}$ is a proper subset of $\mathrm{PG}(k-1,q)$ 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 $C = \{(\mathbf{x}\cdot\mathbf{v_1}, \mathbf{x}\cdot\mathbf{v_2},\dots,\mathbf{x}\cdot\mathbf{v_n}) : \mathbf{x} \in \mathbb{F}_q^k\}$ (here $\mathbf{x}\cdot\mathbf{v}$ is the classical scalar product) is an $[n,k]$-linear two-weight code with weights w_1 and w_2.*

In this talk we give a construction of projective sets from hemisystems on the Hermitian surface.
The Hermitian surface $\mathscr{U}_3$ of $PG(3,q^2)$ is the set of all self-dual points of a non-degenerate unitary polarity of $PG(3,q^2)$. A generator of $\mathscr{U}_3$ is a line of $PG(3,q^2)$ entirely contained in $\mathscr{U}_3$. The generators of the hermitian surface are the totally isotropic lines, the total number of lines of $\mathscr{U}_3$ is $(q^3+1)(q+1)$ and through any point $P \in \mathscr{U}_3$ there pass exactly $q+1$ lines.

Definition 0.2 *An m-*regular system *on $\mathscr{U}_3$ is a set $\mathscr{R}$ of isotropic lines such that every point of $\mathscr{U}_3$ lies on exactly m lines in $\mathscr{R}$,* $0 \leq m \leq q+1$.

When $m = \frac{q+1}{2}$, the $\left(\frac{q+1}{2}\right)$-regular system is also called *hemisystem*, since through each point we consider exactly the half of the generators.

In [5], B. Segre introduced the notion of hemisystems and proved the following theorem:

Theorem 0.3 (Segre's Theorem) *Let $\mathscr{U}_3$ be an Hermitian surface. If q is odd, all the m-regular systems on $\mathscr{U}_3$ are hemistystems.*

In [5] was also constructed the first example, $q = 3$, unique up to isomorphism.

The construction of new hemisystem was an open problem for almost 50 years, and it was conjectured the non existence of hemisystems while $q \neq 3$. But later, in [3], it was constructed by A. Cossidente and T. Penttila an infinite family of hemisystems stabilized by a group isomorphic to $PSL(2,q^2)$. Since then, they were exhibited other constructions of sporadic examples and new infinite families of hemisystem by several authors using different approachs. In [4], considering the Fuhrmann-Torres curve over q^2 naturally embedded in $\mathscr{U}_3$, it is constructed a family of hemiststems in $PG(3,p^2)$, while $p = 1+16a^2$, with an odd integer a. In this talk we investigate the analog construction for $p = 1+4a^2$. The main result is stated in the following theorem.

Theorem 0.4 *Let p be a prime number where $p = 1+4a^2$ with an integer a. Then there exists a hemisystem in the Hermitian surface $\mathscr{U}_3$ of $PG(3,p^2)$ which is left invariant by a subgroup of $PGU(4,p)$ isomorphic to $PSL(2,p) \times C_{\frac{p+1}{2}}$.*

An m-regular system on the Hermitian surface provides an m-ovoid $\mathscr{O}$ on the elliptic quadric $Q^-(5,q)$ which is the image of $\mathscr{U}_3$ via the *Klein correspondence*. In turn, an m-ovoids gives rise to a projective $(m(q^{r+1}+$

$1), 6, m(q^r+1), m(q^r+1)-q^r)$-set and it produces via *linear representation* in $AG(6,q)$, see [1, Theorem 11], a strongly regular graph with parameters:

$$(q^6, m(q-1)(q^3+1), m(q-1)(3+m(q-1))-q^2, m(q-1)(m(q-1)+1)).$$

Since $m=\frac{q+1}{2}$ we get a strongly regular graph with parameters $(q^6, \frac{(q^3+1)(q^2-1)}{2}, \frac{q^4-5}{4}, \frac{q^4-1}{4})$, and the $\left(\frac{q+1}{2}\right)$-ovoid $\mathscr{O}$ is a projective $(\frac{(q^3+1)(q+1)}{2}, 6, \frac{(q^2+1)(q+1)}{2}, \frac{(q^3-q^2+q+1)}{2})$-set. Theorem (0.1) allows us to see this projective set as a $[\frac{(q^3+1)(q+1)}{2}, 6]$-linear two-weight code with weights $w_1=\frac{q^2(q^2-1)}{2}$ and $w_2=\frac{q^2(q^2+1)}{2}$.

Joint work with Vincenzo Pallozzi Lavorante.

References

[1] J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, Journal of Combinatorial Theory A, 114(7), pp. 1293-1314, 2007.

[2] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, Bulletin of the London Mathematical Society, 18, pp. 97-122, 1986.

[3] A. Cossidente, T. Penttila, Hemisystems on the Hermitian surface, Journal of the London Mathematical Society, 72(2), pp. 731-741, 2005.

[4] G. Korchmáros, G. P. Nagy, P. Speziali, Hemisystems of the Hermitian surface, Journal of Combinatorial Theory A, 165, pp. 408-439, 2019.

[5] B. Segre, Forme e geometrie hermitiane, con paricolare riguardo al caso finito, Annali di Matematica Pura ed Applicata, 70(1), pp. 1-201, 1965.

Keywords: Hermitian surfaces, hemisystems, strongly regular graphs, two-weight codes