Designs, Codes and Cryptography (2023) 91:293–307
https://doi.org/10.1007/s10623-022-01107-2

New hemisystems of the Hermitian surface

Vincenzo Pallozzi Lavorante[1] · **Valentino Smaldore**[2]

Received: 15 April 2022 / Revised: 12 August 2022 / Accepted: 22 August 2022 /
Published online: 17 September 2022

Abstract

Constructing hemisystems of the Hermitian surface is a well known, apparently difficult, problem in Finite geometry. So far, a few infinite families and some sporadic examples have been constructed. One of the different approaches relies on the Fuhrmann-Torres maximal curve and provides a hemisystem in $PG(3, p^2)$ for every prime p of the form $p = 1+4a^2$, a even. Here we show that this approach also works in $PG(3, p^2)$ for every prime $p = 1+4a^2$, a odd. The resulting hemisystem gives rise to two weight linear codes and strongly regular graphs whose properties are also investigated.

Keywords Hemisystems · Hermitian surface · Maximal curves

Mathematics Subject Classification Primary: 05B25; Secondary: 05E30 · 51E20

1 Introduction

The Hermitian surface $\mathcal{H}_{3,q^2}$ of $PG(3, q^2)$ is the set of all self-dual points of a non-degenerate unitary polarity of $PG(3, q^2)$. Generators of $\mathcal{H}_{3,q^2}$ are totally isotropic subspaces of maximal dimension. A generator of $\mathcal{H}_{3,q^2}$ is a totally isotropic line of $PG(3, q^2)$. The total number of generators of $\mathcal{H}_{3,q^2}$ is $(q^3 + 1)(q + 1)$ and through any point $P \in \mathcal{H}_{3,q^2}$ there exist exactly $q+1$ generators and they are the intersection of $\mathcal{H}_{3,q^2}$ with its tangent plane at P. Therefore, for any divisor m of $q+1$, one can ask whether a symmetric point-generator configuration for a family of generators exists such that each point of $\mathcal{H}_{3,q^2}$ is incident with exactly $(q+1)/m$ generators from the family.

Communicated by G. Korchmaros.

✉ Vincenzo Pallozzi Lavorante
vincenzop@usf.edu

Valentino Smaldore
valentino.smaldore@unibas.it

[1] Department of Mathematics, University of South Florida, Tampa, USA

[2] Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Potenza, Italy

In [17] B. Segre proved that such a symmetric point-generator configuration does not exist for $m \neq 2$, and he introduced the concept of a hemisystem for the case $m = 2$. Therefore, a hemisystem of $\mathcal{H}_{3,q^2}$ consists of $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$, exactly $\frac{1}{2}(q+1)$ for each point on $\mathcal{H}_{3,q^2}$. Segre exhibited a hemisystem for $q = 3$.

Hemisystems are interesting configurations which are connected with important combinatorial objects such as strongly regular graphs, partial quadrangles and 4-class imprimitive cometric Q-antipodal association schemes that are not metric; see [4, 6, 8]. Nevertheless, finding hemisystems is a challenging problem. The first infinite family was constructed almost 50 years after by Cossidente and Penttila [8] who also found a new sporadic example in $\mathcal{H}_{3,25}$. Later on, Bamberg, Giudici and Royle [1] and [2, Section 4.1] constructed more sporadic examples for $q = 7, 9, 11, 17, 19, 23, 27$. In [1] the authors provide a construction method of hemisystems for a class of generalized quadrangles which includes $\mathcal{H}_{3,q^2}$. A hemisystem obtained by this method is left invariant by an elementary abelian group of order q^2 and the Cossidente-Penttila hemisystem can be also obtained in this way. Recently several new infinite families of hemisystems appeared in the literature. Bamberg, Lee, Momihara and Xiang [4] constructed a new infinite family of hemisystems on $\mathcal{H}_{3,q^2}$ for every $q \equiv -1 \pmod 4$ that generalize one of the previously known sporadic examples. Their construction is based on cyclotomic classes of $\mathbb{F}^*_{q^6}$ and involves results on characters and Gauss sums. Cossidente and Pavese [7] constructed, for every odd q, a hemisystem of $\mathcal{H}_{3,q^2}$ invariant by a subgroup of $\mathrm{PGU}(4, q)$ of order $(q+1)q^2$.

The approach introduced in [13] relies on the Fuhrmann-Torres curve over q^2 naturally embedded in $\mathcal{H}_{3,q^2}$. Here the term curve defined over q^2 is used for a (projective, geometrically irreducible, non-singular) algebraic curve $\mathcal{X}$ of $PG(3, q^2)$. Their construction provided a hemisystem of $\mathcal{H}_{3,q}$ whenever $q = p$ is a prime of the form $p = 1 + 4a^2$ for an even integer a. In this paper we investigate the analogous construction for $p = 1 + 4a^2$ with an odd integer a, and show that it produces a hemisystem , as well, for every such p. We mention that a prime number p of the form $p = 1+4a^2$ with an integer a is called a *Landau number*. Since the famous Landau's conjecture, dating back to 1904, is still to be proved (or disproved), it is unknown whether there exists an infinite sequence of such primes, and hence whether an infinite family of hemisystems is obtained or not. What is known so far is that 37 primes up to 51000 with this property exist, namely 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101, 8837, 12101, 13457, 14401, 15377, 15877, 16901, 17957, 21317, 22501, 24337, 25601, 28901, 30977, 32401, 33857, 41617, 42437, 44101, 50177, see [15]. Our main result is stated in the following theorem.

Theorem 1.1 *Let p be a prime number where* $p = 1+4a^2$ *with an odd integer a. Then there exists a hemisystem in the Hermitian surface* $\mathcal{H}_{3,q^2}$ *of* $\mathrm{PG}(3, p^2)$ *which is left invariant by a subgroup of* $\mathrm{PGU}(4, p)$ *isomorphic to* $\mathrm{PSL}(2, p) \times C_{\frac{p+1}{2}}$.

2 Background on Hermitian surfaces, maximal curves and hemisystems

By *algebraic curve defined over* $\mathbb{F}_{q^2}$ we mean a projective, geometrically irreducible, non-singular algebraic curve $\mathcal{X}$ of $\mathrm{PG}(3, q^2)$ viewed as a curve of $\mathrm{PG}(3, \overline{\mathbb{F}}_{q^2})$, where $\overline{\mathbb{F}}_{q^2}$ is the algebraic closure of $\mathbb{F}_{q^2}$. The Hasse-Weil bound gives an upper (and lower) bound for the number of points a curve can have over a finite field. More precisely, given a curve $\mathcal{X}$ defined over $\mathbb{F}_{q^2}$ one has

$$|\mathcal{X}(\mathbb{F}_{q^2})| \le q^2 + 1 + 2g(\mathcal{X})q,$$

where $\mathcal{X}(\mathbb{F}_{q^2})$ is the set of the points whose coordinates are defined over $\mathbb{F}_{q^2}$ and $g(\mathcal{X})$ is the genus of $\mathcal{X}$. An algebraic curve $\mathcal{X}$ defined over $\mathbb{F}_{q^2}$ is $\mathbb{F}_{q^2}$-*maximal* if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound. Our aim is to use the Natural Embedding Theorem of a maximal curve, [14], to construct new families of hemisystems on $\mathcal{H}_{3,q^2}$.

A canonical form of $\mathcal{H}_{3,q^2}$ is

$$X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0.$$

The group of projectivities preserving $\mathcal{H}_{3,q^2}$ is isomorphic to the projective unitary group $\mathrm{PGU}(4,q)$ and it acts on the points of $\mathcal{H}_{3,q^2}$ as a permutation group [10]. The number of points of $\mathcal{H}_{3,q^2}$ is $(q^2+1)(q^3+1)$. A hemisystem of $\mathcal{H}_{3,q^2}$ consists of $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$, exactly $\frac{1}{2}(q+1)$ of them through each point of $\mathcal{H}_{3,q^2}$. Up to a change of the projective frame in $\mathrm{PG}(3,q^2)$, the equation of $\mathcal{H}_{3,q^2}$ may also be written in the form

$$\mathcal{H}_{3,q^2}\colon X_1^{q+1} + 2X_2^{q+1} - X_3^qX_0 - X_3X_0^q = 0.$$

In $\mathrm{PG}(2,\overline{\mathbb{F}}_q)$ with homogeneous coordinates $(X:Y:Z)$, the Fuhrmann-Torres curve is the plane curve $\mathcal{F}^+$ of genus $\frac{1}{4}(q-1)^2$ with equation

$$\mathcal{F}^+\colon Y^q - YZ^{q-1} = X^{\frac{q+1}{2}}Z^{\frac{q-1}{2}}.$$

The morphism

$$\varphi\colon \mathcal{F}^+ \to \mathrm{PG}(3,\overline{\mathbb{F}}_q), \quad (X:Y:Z) \mapsto (Z^2 : XZ : YZ : Y^2)$$

defines an embedding (called natural embedding) of $\mathcal{F}^+$ which is a $q+1$ degree curve $\mathcal{X}^+$ whose points (including those defined over $\overline{\mathbb{F}}_q$) are contained in $\mathcal{H}_{3,q^2}$. In particular, $\mathcal{F}^+$ is an $\mathbb{F}_{q^2}$-maximal curve. The twin Fuhrmann-Torres curve is defined by the equation

$$\mathcal{F}^-\colon Y^q - YZ^{q-1} = -X^{\frac{q+1}{2}}Z^{\frac{q-1}{2}}.$$

and the above claims remain valid with respect to the same morphism. For more details see [9].

Some useful properties of the Fuhrmann-Torres curve, also valid for any $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ naturally embedded in $\mathcal{H}_{3,q^2}$, can be found in [13, Sections 2,3,4].

In particular, $\mathcal{X}^+$ is a $q+1$ degree curve lying in the Hermitian surface $\mathcal{H}_{3,q^2}$. Furthermore $\mathcal{X}^+(\mathbb{F}_{q^2})$ is partitioned in Ω and $\mathcal{X}^+(\mathbb{F}_{q^2}) \setminus \Omega = \Delta^+$, where Ω is the set cut out on $\mathcal{X}^+$ by the plane $\pi\colon X_1 = 0$. Note that $|\Omega| = q+1$ and $|\Delta^+| = \frac{1}{2}(q^3-q)$.

Equivalently Ω is the intersection in π of the conic $\mathcal{C}$ with equation $X_0X_3 - X_2^2 = 0$ and the Hermitian curve $\mathcal{H}(2,q^2)$ with equation $X_0^qX_3 + X_0X_3^q - 2X_2^{q+1} = 0$. Moreover, the above properties hold true when $^+$ is replaced by $^-$ and $\mathcal{X}^-$ is the natural embedding of the plane curve $\mathcal{F}^-$. The curves $\mathcal{X}^+$ and $\mathcal{X}^-$ are isomorphic over $\mathbb{F}_{q^2}$ and Ω is the set of common points of $\mathcal{X}^+$ and $\mathcal{X}^-$.

We use classical terminology regarding maximal curves. In particular, a (*real*) *chord* of $\mathcal{X}$ is a line in $\mathrm{PG}(3,q^2)$ which meets $\mathcal{X}(\mathbb{F}_{q^2})$ in at least two distinct point, whereas an *imaginary chord* of $\mathcal{X}$ is a line in $\mathrm{PG}(3,q^2)$ joining a point $P \in \mathcal{X}(\mathbb{F}_{q^4}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ to its conjugate, that is, its Frobenius image.

The key point of the construction below is the following corollary to the NET.

Lemma 2.1 [13, Lemma 3.4] *Let $\mathcal{C}$ be an $\mathbb{F}_{q^2}$-maximal curve naturally embedded in the Hermitian surface $\mathcal{H}_{3,q^2}$. Then*

(i) *No two distinct points in $\mathcal{C}(\mathbb{F}_{q^2})$ are conjugate under the unitary polarity associated with $\mathcal{H}_{3,q^2}$.*
(ii) *Any imaginary chord of $\mathcal{C}$ is a generator of $\mathcal{H}_{3,q^2}$ which is disjoint from $\mathcal{C}$.*
(iii) *For any point $P \in \mathcal{H}_{3,q^2}$ in* PG$(3, q^2)$*, if $P \notin \mathcal{C}(\mathbb{F}_{q^2})$ and Π_P is the tangent plane to $\mathcal{H}_{3,q^2}$ at P, then $\Pi_P \cap \mathcal{C}$ consists of $q+1$ pairwise distinct points which are in $\mathcal{C}(\mathbb{F}_{q^4})$.*

3 The Fuhrmann-Torres construction

From now on let q be a prime $p \equiv 1 \pmod 4$ and let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve. Denote by N_{q^2} the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$.

Let $\mathcal{H}$ denote the set of all imaginary chords of $\mathcal{X}$. Furthermore, for a point $P \in \mathrm{PG}(3, q^2)$ lying in $\mathcal{H}_{3,q^2} \setminus \mathcal{X}(\mathbb{F}_{q^2})$, let $n_P(\mathcal{X})$ denote the number of generators of $\mathcal{H}_{3,q^2}$ through P which contain an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$.

Definition 3.1 A set $\mathcal{M}$ of generators of $\mathcal{H}_{3,q^2}$ is an *half-hemisystem* on $\mathcal{X}$ if the following properties hold:

(A) Each $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$.
(B) For any point $P \in \mathcal{H}_{3,q^2} \setminus \mathcal{X}(\mathbb{F}_{q^2})$ lying in PG$(3, q^2)$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P(\mathcal{X})$ generators through P which contain an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$.

Note that $\mathcal{M}$ consists of $\frac{1}{2}(q+1)N_{q^2}$ generators and $\mathcal{H}$ of $\frac{1}{2}(q^2+q)(q^2-q-2g(\mathcal{X}))$ generators of $\mathcal{H}_{3,q^2}$. Therefore $\mathcal{M} \cup \mathcal{H}$ has exactly $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$.

Result 3.2 [13, Proposition 4.1] *$\mathcal{M} \cup \mathcal{H}$ is a hemisystem of $\mathcal{H}_{3,q^2}$.*

Let $\mathfrak{G}$ be a subgroup of Aut$(\mathcal{X})$ and $o_1, \ldots, o_r$ be the $\mathfrak{G}$-orbits on $\mathcal{X}(\mathbb{F}_{q^2})$. Let $\mathcal{G}$ be the set of all generators meeting $\mathcal{X}^+$. Moreover, for $1 \le j \le r$, let $\mathcal{G}_j$ denote the set of all generators of $\mathcal{H}_{3,q^2}$ meeting o_j. Note that $\mathfrak{G}$ leaves each $\mathcal{G}_j$ invariant.

Result 3.3 [13, Proposition 4.2] *With the above notation, assume that the subgroup $\mathfrak{G}$ fulfills the hypothesis:*

(C) *$\mathfrak{G}$ has a subgroup $\mathfrak{h}$ of index 2 such that $\mathfrak{G}$ and $\mathfrak{h}$ have the same orbits $o_1, \ldots, o_r$ on $\mathcal{X}(\mathbb{F}_{q^2})$.*
(D) *For any $1 \le j \le r$, $\mathfrak{G}$ acts transitively on $\mathcal{G}_j$ while $\mathfrak{h}$ has two orbits on $\mathcal{G}_j$.*

Let $P \notin \mathcal{X}(\mathbb{F}_{q^2})$ be a point lying on a generator in $\mathcal{G}$, if

(E) *there is an element in $\mathfrak{G}_P$ not in $\mathfrak{h}_P$,*

then P satisfies (B).

From [13, Lemma 5.1] $\mathcal{G}$ is also the set of all generators meeting $\mathcal{X}^-$. In particular, $\mathcal{G}$ splits into two subset

$$\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2, \tag{3.1}$$

where $\mathcal{G}_2$ is the set of the $(q+1)^2$ generators meeting Ω, while $\mathcal{G}_1$ is the set of the $\frac{1}{2}(q^3-q)(q+1)$ generators meeting both Δ^+ and Δ^-. Thus, the following characterization of $\mathcal{G}$ is very useful.

Result 3.4 [13, Lemma 5.3] *The generator set $\mathcal{G}_1$ consists of all the lines $g_{u,v,s,t}$ spanned by the points $P_{u,v} = (1 : u : v : v^2) \in \Delta^+$ and $Q_{s,t} = (1 : s : t : t^2) \in \Delta^-$ such that*

$$\mathcal{F}\colon\ F(v,t) = (v+t)^{q+1} - 2(vt + (vt)^q) = 0$$

and

$$u^{\frac{q+1}{2}} = v^q - v, \quad -s^{\frac{q+1}{2}} = t^q - t, \quad u^q s = (t - v^q)^2.$$

Result 3.5 [13, Lemma 5.4] Aut$(\mathcal{F})$ *contains a subgroup $\Psi \cong \mathrm{PGL}(2,q)$ that acts faithfully on the set $\mathcal{F}(\mathbb{F}_{q^2}) \setminus \mathcal{F}(\mathbb{F}_q)$ as a sharply transitive permutation group.*

4 Automorphisms preserving $\mathcal{G}$ and $\mathcal{X}^+$

In this subsection we recall the main results about the group-theoretic properties involving, $\mathcal{X}^+$, $\mathcal{X}^-$ and $\mathcal{G}$; see [13, Section 5]. The authors showed that Ψ contains a subgroup Γ which acts sharply transitively on $\mathcal{G}_1$. Furthermore, Γ has a unique index 2 subgroup Φ such that

$$\Phi \cong PSL(2,q) \times C_{\frac{q+1}{2}}.$$

In particular, Φ has two orbits on $\mathcal{G}_1$, namely $\mathcal{M}_1$ and $\mathcal{M}_2$.

In terms of subgroups of PGU$(4,q)$, the following holds.

Result 4.1 [13, Lemma 5.7] *The group* PGU$(4,q)$ *has a subgroup $\mathfrak{G}$ with the following properties:*

(i) *$\mathfrak{G}$ is an automorphism group of $\mathcal{X}^+$ and $\mathcal{X}^-$;*
(ii) *$\mathfrak{G}$ preserves Δ^+, Δ^-, Ω and $\mathcal{G}_1$;*
(iii) *$\mathfrak{G}$ acts faithfully on Δ^+, Δ^- and $\mathcal{G}_1$;*
(iv) *the collineation group induced by $\mathfrak{G}$ on π is $\mathfrak{G}/Z(\mathfrak{G}) \cong \mathrm{PGL}(2,q)$ with $Z(\mathfrak{G}) \cong C_{\frac{q+1}{2}}$;*
(v) *the permutation representation of $\mathfrak{G}$ on $\mathcal{G}_1$ is Γ; in particular $\mathfrak{G} \cong \Gamma$;*
(vi) *$\mathfrak{G}/Z(\mathfrak{G})$ acts on Ω as $\mathrm{PGL}(2,q)$ in its 3-transitive permutation representation.*

Furthermore, $\mathfrak{G}$ has an index 2 subgroup $\mathfrak{h}$ isomorphic to $\mathrm{PSL}(2,q) \times C_{\frac{q+1}{2}}$.

With the above notation, in the isomorphism $\mathfrak{G} \cong \Gamma$, $\mathfrak{h}$ and Φ correspond.

Result 4.2 [13, Lemma 5.9] *The elements of order 2 in $\mathfrak{h}$ are skew perspectivities, while those in $\mathfrak{G} \setminus \mathfrak{h}$ are homologies. Furthermore, the linear collineation $\mathfrak{w}$, defined by*

$$\boldsymbol{W} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

interchanges $\mathcal{X}^+$ with $\mathcal{X}^-$ and the linear group generated by $\mathfrak{G}$ and $\mathfrak{w}$ is the direct product $\mathfrak{G} \times \langle \mathfrak{w} \rangle$.

Result 4.3 [13, Lemma 5.11] *$\mathfrak{G}$ acts transitively on $\mathcal{G}_2$ while $\mathfrak{h}$ has two orbits on $\mathcal{G}_2$.*

From the result of this section, the following theorem follows

Theorem 4.4 [13, Theorem 5.13] *Conditions* (C) *and* (D) *are fulfilled for $\mathcal{X} = \mathcal{X}^+$, with $\Gamma = \mathfrak{G}$ and $\Phi = \mathfrak{h}$.*

More precisely, $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ with $\mathcal{G}_1 = \mathcal{M}_1 \cup \mathcal{M}'_1$ and $\mathcal{G}_2 = \mathcal{M}_2 \cup \mathcal{M}'_2$, where $\mathcal{G}_1$ and $\mathcal{G}_2$ are the $\mathfrak{G}$-orbits on $\mathcal{G}$ whereas $\mathcal{M}_1, \mathcal{M}'_1, \mathcal{M}_2, \mathcal{M}'_2$ are the $\mathfrak{h}$-orbits on $\mathcal{G}_1$ and $\mathcal{G}_2$ respectively. This notation fits with [13, Section 5].

5 Points satisfying condition (E)

The plane $\pi : X_1 = 0$ can be seen as the projective plane $\mathrm{PG}(2, q^2)$, with homogeneous coordinates $(X_0 : X_2 : X_3)$. Then $\mathcal{C}$ is the conic of equation $X_0X_3 - X_2^2 = 0$ and Ω is the set of points of $\mathcal{C}$ lying in the (canonical Baer) subplane $\mathrm{PG}(2, q)$.

The points in $\mathrm{PG}(2, q^2) \setminus \mathrm{PG}(2, q)$ are of three types with respect to the lines of $\mathrm{PG}(2, q)$, i.e.

(I) points of a unique line disjoint from Ω which meets $\mathcal{C}$ in two distinct points both in $\mathrm{PG}(2, q^2) \setminus \mathrm{PG}(2, q)$;
(II) points of a unique line meeting Ω in two distinct points;
(III) points of a unique line which is tangent to $\mathcal{C}$ with tangency point on Ω.

Points of type (I) - (II) and points in $\mathrm{PG}(2, q)$ satisfy condition (B), as can be readily seen in the next result.

Result 5.1 [13, Theorem 6.1] *If the projection of $P \in \mathcal{H}_{3,q^2}$ on π is a point P' of type* (I) - (II) *or $P' \in \mathrm{PG}(2, q)$, then condition* (E) *is fulfilled for $\mathcal{X} = \mathcal{X}^+$, $\Gamma = \mathfrak{G}$ and $\Phi = \mathfrak{h}$.*

6 Condition (B) for case (III) and $p \equiv 5 \pmod 8$

Condition (B) is not always satisfied in Case (III), that is, for points P whose projection from $X_\infty = (0, 1, 0, 0)$ on π is a point P' lying on a tangent l to $\mathcal{C}$. Our goal is to show that [13, Theorem 7.1], proven for $p \equiv 1 \pmod 8$, remains true for $p \equiv 5 \pmod 8$, extending their results to the case $p \equiv 1 \pmod 4$.

For this reason, from now on, we assume q be a prime $p \equiv 5 \pmod 8$.

Theorem 6.1 *Condition (B) for Case (III) is satisfied if and only if the number N_q of $\mathbb{F}_q$-rational points of the elliptic curve with affine equation $Y^2 = X^3 - X$ equals either $q - 1$, or $q + 3$.*

We need few steps before to prove Theorem 6.1. To begin with, we have to prove the following theorem.

Theorem 6.2 *Let n_q be the number of $\xi \in \mathbb{F}_q$ for which $f(\xi) = \xi^4 - 48\xi^2 + 64$ is a square in $\mathbb{F}_q$. Condition (B) for Case (III) is satisfied if and only if n_q equals either $\frac{1}{2}(q + 1)$ or $\frac{1}{2}(q - 3)$.*

The proof of Theorem 6.2 is carried out by a series of lemmas.

Since $q \equiv 5 \pmod 8$, 2 is not a square in $\mathbb{F}_q$.

Let h and $-h$ be the square roots of 2 in $\mathbb{F}_{q^2}$. In particular we have that $h^q + h = 0$ and $(\pm h)^{q+1} = -2$. Moreover h is a non-square in $\mathbb{F}_{q^2}$.

Moreover $h^{(q-1)/2} = \alpha \in \mathbb{F}_q$, with $\alpha^2 = -1$. Thus, $\alpha \notin \Box_q$ and $(1+\alpha)(1-\alpha) = 2 \notin \Box_q$.

Since $\mathfrak{G}$ is transitive on Ω, the point $O = (1 : 0 : 0 : 0)$ may be assumed to be the tangency point of l. Then l has equation $X_1 = 0$, $X_3 = 0$, and $P = (a_0 : a_1 : a_2 : 0)$ with

$a_1 \neq 0$ and $a_1^{q+1} + 2a_2^{q+1} = 0$. If $a_0 = 0$ then $P = (0 : d : 1 : 0)$ with $d^{q+1} + 2 = 0$ and his projection to $\pi : X_1 = 0$ is $P' = (0 : 1 : 0)$, which is a point in PG$(2, q)$. By Result 5.1 the case $a_0 = 0$ can be dismissed and $a_0 = 1$ may be assumed.

Therefore, after the dehomogenization with respect to X_0, consider the affine coordinates (X, Y, Z) for a point in PG$(3, q^2)$.
We may limit ourselves to a point $P = (a, b, 0)$ such that $a^{q+1} + 2b^{q+1} = 0$. The latter equation holds for $a = \pm h^2$ and $b = h$. Then we may choose

$$P = (2\varepsilon, h, 0), \quad \text{where } \varepsilon \in \{-1, 1\}$$

and we can carry out the case $\varepsilon = 1$ and $\varepsilon = -1$ simultaneously.

6.1 Case of $\mathcal{G}_1$

We keep up our notation $P_{u,v} = (u, v, v^2)$ for a point in Δ^+. The following lemmas are analogous to those in [13, section 7.1].

Lemma 6.3 *Let $v \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then there exists $u \in \mathbb{F}_{q^2}$ such that the line joining P at $P_{u,v}$ is a generator of $\mathcal{H}_{3,q^2}$ if and only if*

$$(v^2 + 2hv)^{\frac{q+1}{2}} = 2\varepsilon(v^q - v). \tag{6.1}$$

If (6.1) holds, then u is uniquely determined by v.

Proof The line $l = PP_{u,v}$ is a generator if and only if $P_{u,v}$ lies on the tangent plane to $\mathcal{H}_{3,q^2}$ at P. This implies

$$u = \frac{v^2 + 2hv}{2\varepsilon}. \tag{6.2}$$

and since $P_{u,v} \in \Delta^+$ then $u^{\frac{q+1}{2}} = v^q - v$ and l is a generator. The converse follows from the proof of [13, Lemma 7.4]. □

Lemma 6.1 can be extended to $Q_{s,t} \in \Delta^-$, providing that u, v are replaced by s, t and Equations (6.1), (6.2) by

$$(t^2 + 2ht)^{\frac{q+1}{2}} = -2\varepsilon(t^q - t) \tag{6.3}$$

and

$$s = \frac{t^2 + 2ht}{2\varepsilon}. \tag{6.4}$$

Furthermore P, $P_{u,v}$ and $Q_{s,t}$ are collinear if and only if

$$\begin{cases} 2\varepsilon(t^2 - v^2) = t^2u - v^2s, \\ vt - h(v + t) = 0. \end{cases} \tag{6.5}$$

Therefore, the following lemma holds.

Lemma 6.4 *Let $v, t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $F(v, t) = 0$. If the line through $P_{u,v} \in \Delta^+$ and $Q_{s,t} \in \Delta^-$ is a generator through P, then*

$$vt - h(v + t) = 0 \tag{6.6}$$

holds.

We now count the number of generators in $\mathcal{G}_1$ which pass through P.

Lemma 6.5 *Equation (6.1) has exactly $\frac{1}{2}(q+1)$ solutions in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.*

Proof Let $r = vh^{-1}$. We obtain:

$$(r^2+2r)^{\frac{q+1}{2}} = \varepsilon h(r^q + r).$$

Hence,

$$(r^2+2r)^{\frac{q^2-1}{2}} = -1$$

and then r^2+2r is a non-square of $\mathbb{F}_{q^2}$. Thus, there exists $z \in \mathbb{F}_{q^2}{}^*$ such that $r^2+2r = hz^2$. Now the system is

$$\begin{cases} hz^2 = r^2+2r \\ \alpha hz^{q+1} = \varepsilon h(r^q + r) \end{cases} \tag{6.7}$$

. Let $\lambda = zr^{-1}$, so that

$$\begin{cases} h\lambda^2 r = r+2, \\ \alpha(\lambda r)^{q+1} = \varepsilon(r^q + r). \end{cases} \tag{6.8}$$

Since $r = 2/(h\lambda^2 - 1)$ we obtain

$$4\alpha\lambda^{q+1} - 2\varepsilon(h\lambda^2-1) - 2\varepsilon(h\lambda^2-1)^q = 0. \tag{6.9}$$

Now if $\lambda = \lambda_1 + h\lambda_2$, with $\lambda_1, \lambda_2 \in \mathbb{F}_q$, Equation (6.9) reads

$$\alpha\lambda_1^2 - 2\alpha\lambda_2^2 - 4\varepsilon\lambda_1\lambda_2 + \varepsilon = 0. \tag{6.10}$$

Since the determinant of the matrix of the quadratic form associated to (6.10) is -2ε, that quadratic form is the equation of an irreducible conic of $\mathrm{PG}(2,q)$. Thus, we have exactly $q+1$ solutions λ of (6.9): if λ is a solution, then $-\lambda$ is too, hence we have $\frac{q+1}{2}$ values for both r and v.

Every solution v of (6.1) is in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In fact, if $(hr)^q = hr$ then $r^q = -r$ and $\lambda r = 0$, which contradicts the first equation of (6.8). □

Note that $\alpha = h^{\frac{q-1}{2}}$ is a non-square of $\mathbb{F}_q$.

Lemma 6.6 *For every solution $v = v_1 + hv_2$ of (6.1),*

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1v_2 + v_1) \notin \Box_q.$$

Proof Consider System (6.7) and let $z = z_1 + hz_2$ and $r = r_1 + hr_2$. Then

$$\begin{cases} z_1^2 + 2z_2^2 = 2r_1r_2 + 2r_2 \\ \alpha z_1^2 - 2\alpha z_2^2 = 2\varepsilon r_1. \end{cases} \tag{6.11}$$

Summing the two equations we have:

$$\alpha z_1^2 = \alpha r_2(r_1+1) + \varepsilon r_1.$$

Since $\alpha^2 = -1$ and $q \equiv 5 \pmod 8$, it follows $\alpha \notin \Box_q$ and then

$$\alpha r_2(r_1+1) + \varepsilon r_1$$

is a non-square of $\mathbb{F}_q$. With $v_2 = r_1$ and $v_1 = 2r_2$ we obtain

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1) \notin \square_q.$$

□

Our next step is to characterize the generators of $\mathcal{G}_1$ through P.

To begin with, we need some notions of number theory, which would allow us to simplify the notation we will use. Note that $(2+h)^{\frac{q+1}{2}} = \lambda h$, where,

$$\lambda = (2+h)^{\frac{q+1}{2}} h^{-1} = [(1+h)h]^{\frac{q+1}{2}} h^{-1} = (1+h)^{\frac{q+1}{2}} h^{\frac{q-1}{2}}. \tag{6.12}$$

Since

$$\lambda^2 = (1+h)^{q+1} 2^{\frac{q-1}{2}} = (1+h)(1-h)(-1) = 1,$$

we have $\lambda = \pm 1$. Applying the Frobenius map to (6.12) gives

$$\lambda = (1-h)^{\frac{q+1}{2}} (-h)^{\frac{q-1}{2}}.$$

Hence λ is independent of the choice of h as a square root of 2.

Proposition 6.7 *We have*

$$\lambda = \begin{cases} 1, & q \equiv 13 \pmod{16} \\ -1, & q \equiv 5 \pmod{16} \end{cases}$$

Proof See Appendix A. □

Let

$$\chi := \begin{cases} -1, & \text{if either } \varepsilon = 1 \text{ and } q \equiv 13 \pmod{16} \text{ or } \varepsilon = -1 \text{ and } q \equiv 5 \pmod{16} \\ 1, & \text{if either } \varepsilon = 1 \text{ and } q \equiv 5 \pmod{16} \text{ or } \varepsilon = -1 \text{ and } q \equiv 13 \pmod{16} \end{cases}$$

According to Proposition 6.7, we have $\lambda\chi = -\varepsilon$ and hence

$$(2 \pm \chi h)^{\frac{q+1}{2}} = \pm\chi\lambda h = \mp\varepsilon h. \tag{6.13}$$

Furthermore,

$$v_0 := -2(h - 2\chi), \quad u_0 := \frac{4}{\varepsilon}(2 - \chi h)$$

and

$$t_0 := -2(h + 2\chi), \quad s_0 := \frac{4}{\varepsilon}(2 + \chi h)$$

Equation (6.13) implies

$$v_0^q - v_0 = 4h = u_0^{\frac{q+1}{2}}. \tag{6.14}$$

and

$$u_0^q s_0 = 16(2 - h\chi)^2 = (t_0 - v_0^q)^2.$$

Furthermore,

$$(v_0 + t_0)^{q+1} = -32 = 2(t_0 v_0 + (t_0 v_0)^q)$$

Therefore, $F(v_0, t_0) = 0$. Thus, from Result 3.4, the line through P_{u_0,v_0} and Q_{s_0,t_0} is a generator $g_0 \in \mathcal{G}_1$. Moreover the following hold:

$$u_0 = \frac{v_0^2 + 2hv_0}{2\varepsilon}, \quad s_0 = \frac{t_0^2 + 2ht_0}{2\varepsilon}$$

showing that g_0 passes through P.

We show how each generator g passing through P can be obtained from g_0. If $g = P_{u,v}Q_{s,t}$ is a line through P, then, by Lemma 6.4, $F(v, t) = 0$ and $vt = h(v + t)$. Now for α, β, γ and $\delta \in \mathbb{F}_q$, with $\alpha\delta - \beta\gamma \neq 0$, write

$$v = \frac{\alpha v_0 + \beta}{\gamma v_0 + \delta}, \quad t = \frac{\alpha t_0 + \beta}{\gamma t_0 + \delta}.$$

From $v_0 t_0 = -8$ and $v_0 + t_0 = -4h$, we may write Equation (6.6) as

$$\begin{aligned} 8\alpha\gamma &= 2\alpha\beta + \beta\delta, \\ \beta^2 &= 8(\alpha^2 - \alpha\delta - \beta\gamma). \end{aligned} \tag{6.15}$$

Our aim is to show that these equations hold if and only if α, β, γ and δ depend on a unique parameter $\xi \in \mathbb{F}_q \cup \{\infty\}$. To begin with, let $\delta \neq 0$. Then $\alpha \neq 0$. The first equation in (6.15) forces

$$\gamma = \frac{(2\alpha + 1)\beta}{8\alpha}.$$

Together with the other equation, we have

$$8\alpha^3 - 3\alpha\beta^2 - 8\alpha^2 - \beta^2 = 0.$$

Let $\xi = \beta\alpha^{-1}$. This implies $\alpha^2(8\alpha - 3\alpha\xi^2 - 8 - \xi^2) = 0$. Therefore

$$\alpha = \frac{\xi^2 + 8}{8 - \xi^2},$$

and the assertion follows for $\delta \neq 0$. For $\delta = 0$ we may assume $\beta = 1$. If $\alpha \neq 0$ then $\gamma = 1/4$ and $8\alpha^2 = -1$, which is impossible as -1 is a square in $\mathbb{F}_q$ while 8 is not. When $\delta = \alpha = 0$ and $\beta = 1$, then $\gamma = \frac{-1}{8}$.

Therefore,

$$v = v_\xi = \frac{(\xi^2 + 8)v_0 + (\xi^2 + 8)\xi}{\frac{\xi}{8}(-\xi^2 + 24)v_0 + 8 - 3\xi^2}, \quad v_\infty = \frac{1}{-\frac{1}{8}v_0} = -2(h + 2\chi). \tag{6.16}$$

Let A_ξ and A_∞ be two matrices in $GL(2, \mathbb{F}_q)$ representing the fractional linear maps v_ξ and v_∞. Thus,

$$\det(A_\xi) = \frac{(\xi^2 + 8)(\xi^4 - 48\xi^2 + 64)}{8}, \quad \det(A_\infty) = (8)^{-1}. \tag{6.17}$$

These equations remain true for t_0 and t:

$$t = t_\xi = \frac{(\xi^2 + 8)t_0 + (\xi^2 + 8)\xi}{\frac{\xi}{8}(-\xi^2 + 24)t_0 + 8 - 3\xi^2}, \quad t_\infty = \frac{1}{-\frac{1}{8}t_0} = -2(h - 2\mathcal{X}). \tag{6.18}$$

Next we show that Lemma 6.6 imposes a condition on ξ in (6.16).

Lemma 6.8 $\xi^2 + 8$ *is a square in* $\mathbb{F}_q$.

Proof To use Lemma 6.6 we rewrite $\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1)$ in terms of ξ. This requires a certain amount of straightforward and tedious computations that we omit. From (6.16), we have

$$v = \frac{4(\xi^2+8)}{\chi 16 - \chi 2\xi^2 + h(8 - \chi 8\xi + \xi^2)} \tag{6.19}$$

and

$$v_1 = \frac{-4(\chi 16 - \chi 2\xi^2)(8+\xi^2)}{k}, \quad v_2 = \frac{-4(8+\xi^2)(8-\chi 8\xi + \xi^2)}{k} \tag{6.20}$$

where $k = 128 + \chi 256\xi - 224\xi^2 + \chi 32\xi^3 + 2\xi^4$.
Then,

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1) = \frac{2(1-\chi\varepsilon\alpha)(8+\xi^2)((-16+16\alpha)+(8+32\alpha)\xi+(6+10\alpha)\xi^2+\xi^3)^2}{(64-128\xi-112\xi^2-16\xi^3+\xi^4)^2} \tag{6.21}$$

Note that $(1+\alpha)(1-\alpha)=2$ and that $1+\alpha \in \Box_q$ if and only if $q \equiv 13 \pmod{16}$. In fact,

$$1+\alpha = \pm h^{\frac{q+3}{4}} \in \Box_q \iff h^{\frac{(q-1)(q+3)}{8}} = 1$$

and in this case $1-\alpha$ is a non-square in $\mathbb{F}_q$.

Since $\chi\varepsilon = 1$ when $q \equiv 5 \pmod{16}$ and $\chi\varepsilon = -1$ when $q \equiv 13 \pmod{16}$, we get that $1 - \chi\varepsilon\alpha$ is always a square in $\mathbb{F}_q$. Hence $\xi^2 + 8 \in \Box_q$. □

To state a corollary of Lemmas 6.5, 6.6 and 6.8, the partition of $\mathbb{F}_q \cup \{\infty\}$ into two subsets $\Sigma_1 \cup \{\infty\}$ and Σ_2 is useful, where $x \in \Sigma_1 \cup \{\infty\}$ or $x \in \Sigma_2$ according as $x^2 + 8 \in \Box_q$ or not.

Proposition 6.9 *Let $P = (2\varepsilon, h, 0) \in \mathcal{H}_{3,q^2}$ with $h^2 = 2$. Then the generators in $\mathcal{G}_1$ through the point P which meet $\mathcal{X}^+$ are as many as $n_P = \frac{1}{2}(q+1)$. They are precisely the lines g_ξ joining P to $P_{u,v} = (u, v, v^2)$ with u, v as in equation (6.2) and (6.16), where ξ ranges over the set $\Sigma_1 \cup \{\infty\}$.*

6.2 Case of $\mathcal{G}_2$

This case requires much less effort. The tangent plane π_P at $P = (2\varepsilon : h : 0)$ meets π in the line r of equation $2h^q Y + Z = 0$. Since $\mathcal{C}$ has equation $Z = Y^2$ in π, the only common points of r and $\mathcal{C}$ are $(0:0:0)$ and $Q = (0 : 2h : 8)$, with $Q \notin \Omega$ as $h \notin \mathbb{F}_q$. Then we have the following result.

Proposition 6.10 *Let $P = (2\varepsilon, h, 0) \in \mathcal{H}_{3,q^2}$, with $h^2 = 2$. Then there is a unique generator through the point P which meets Ω, namely the line l through P and the origin $O = (0:0:0)$.*

From now on, we denote with ℓ^+ and ℓ^- the two generators through P when $\varepsilon = 1$ and $\varepsilon = -1$ respectively.

6.3 Choice of $\mathcal{M}_1$ and $\mathcal{M}_2$

In this last subsection, we are going to choose $\mathcal{M}_1$ and $\mathcal{M}_2$ such that Condition (B) is fulfilled.

We have two different generators g_0's, one for $\varepsilon = 1$, the other for $\varepsilon = -1$:

$$g_0^+ \text{ passing through } P^+(2 : h : 0)$$

and

$$g_0^- \text{ passing through } P^-(-2 : h : 0)$$

Lemma 6.11 *The generators g_0^+ and g_0^- are in different orbits of Φ.*

Proof The linear collineation associated to the matrix $\mathbf{W}$ interchanges the two generators. □

Let r (resp. r') be the number of generators in $\mathcal{M}_1$ (resp. $\mathcal{M}_1'$) through the point P^+ that meet Δ^+. Note that

$$r + r' = \frac{1}{2}(q+1). \tag{6.22}$$

Similarly,

Lemma 6.12 *The generators ℓ^+ and ℓ^- are in different orbits of Φ.*

Proof We use the same arguments of [13, Lemma 7.14]. Indeed, we replace $(\sqrt{-2}b, b, 0)$ and $(-\sqrt{-2}b, b, 0)$ with P^+ and P^- and the proof follows. □

We are ready to choose $\mathcal{M}_1$ and $\mathcal{M}_2$.

- $\mathcal{M}_1$ is the Φ-orbit containing g_0^+.
- $\mathcal{M}_2$ is the Φ-orbit containing ℓ^+ for $r < r'$ and ℓ^- for $r > r'$.

Remark 6.13 As in [13, Proposition 7.15], r' is obtained counting the squares in the value set of the polynomial $f(\xi)$, defined in Theorem 6.2. More precisely, we obtain that the number of $\xi \in \mathbb{F}_q$ for which $f(\xi) \in \square_q$ equals $2r' - 1$.

Therefore we have the following proposition.

Proposition 6.14 *Condition* (B) *for case* (III) *holds if and only if*

$$r = \frac{1}{4}(q-1), \ \textit{and}\ r' = \frac{1}{4}(q+3)$$

or

$$r = \frac{1}{4}(q+3), \ \textit{and}\ r' = \frac{1}{4}(q-1)$$

Proof Note that $n_P = \frac{1}{2}(q+3)$ and that condition (B) holds if and only if half of them is in $\mathcal{M}_1 \cup \mathcal{M}_2$. The choices of r and r' are readily seen. □

Thus, Theorem 6.2 follows.

Since the properties of the plane curve $\mathcal{C}_4$

$$Y^2 = X^4 - 24\omega X^2 + 16\omega^2, \ \text{with } \omega = 2$$

depend only on $q \equiv 1 \pmod 4$, we also get the proof of Theorem 6.1, that is Condition (B) in case (III) is satisfied if and only if the curve $\mathcal{C}_3$

$$Y^2 = X^3 - X$$

has $q - 1$ or $q + 3$ points. For the details, see [13] at the end of Section 7.

7 Proof of Theorem 1.1

We are in the position to work out the case $q = p$ when $p \equiv 1 \pmod 4$. We write $p = \pi\bar{\pi}$, with $\pi \in \mathbb{Z}[i]$. Here, π can be chosen such that $\pi = \alpha_1 + i\alpha_2$ and $\alpha_1 = 1$. From [18, Section 2.2.2], $N_p(\mathcal{C}_3) = q + 1 - 2\alpha_1$. This implies that condition (B) in case (III) is satisfied if and only if

$$p = 1 + 4a^2 \quad \text{and} \quad N_p(\mathcal{C}_3) = q - 1.$$

Therefore, Theorem 1.1 is a corollary of Theorem 4.4, Result 5.1 and Theorem 6.2.

Further computer-aided investigations in the case $q = 5$ showed that the found hemisystem is isomorphic to a sporadic case described in [8], whose full automorphism group is $3.A_7$. In all other cases, there were not other known examples stabilized by $\mathrm{PSL}(2, q) \times C_{\frac{q+1}{2}}$, so the above mentioned sporadic hemisystem should be the first known example in our putative new family.

8 Some applications

In the last section of this chapter we will focus on some applications connected to hemisystems.

8.1 Strongly regular graphs

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 neighbors and any two non-adjacent vertices have μ common neighbors. Every hemisystem gives rise to a strongly regular graph where the vertices of Γ are the lines lying on the surface but not contained in $\mathcal{S}$, and two vertices are adjacent if the lines are incident, with the following parameters: $v = \frac{1}{2}(q^3+1)(q+1), k = \frac{1}{2}(q^2+1)(q-1), \lambda = \frac{1}{2}(q-3), \mu = \frac{1}{2}(q-1)^2, $. The spectrum of Γ can be hence computed. The first eigenvalue is k, of multiplicity 1, and the other two (the restricted eigenvalues) are:

$$\theta_1 = \tfrac{1}{2}\left[(\lambda - \mu) + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right] = q - 1,$$
$$\theta_2 = \tfrac{1}{2}\left[(\lambda - \mu) - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right] = \tfrac{1}{2}(-q^2 + q - 2),$$

of multiplicity

$$m_1 = \tfrac{1}{2}\left[(v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right] = \tfrac{1}{2}(q^4 - q^3 + 2q^2 - q + 1),$$
$$m_2 = \tfrac{1}{2}\left[(v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right] = (q^2+1)(q-1) = 2k,$$

respectively. See [16, Section 1.4].

The hemisystems on the Hermitian surface $\mathcal{H}_{3,p^2}$, for $p = 1 + 4a^2$, constructed in this chapter produce strongly regular graphs Γ with the above parameters for $q = p$. We point out that, in the smallest case $p = 5$, the graph Γ, arising from the sporadic $3.A_7$-stabilized hemisystem, has parameters (378, 52, 1, 8) and spectrum $52, 4^{273}, -11^{104}$. A comparison of Γ with the Cossidente-Penttila strongly regular graph ([8]) with the same parameters, shows that they are cospectral, while a compiter aided search shows that they have different auromorphism groups, so that they are not isomorphic.

8.2 Two-weight codes from strongly regular graphs

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 $|\{w : \exists v \in C \setminus \{\underline{0}\} \quad w(v) = w\}| = 2$. Here we use a result that allows us to construct two-weight codes from hemisystems of $\mathcal{H}(3,q^2)$.

Let $\mathcal{Q}^-(5,q)$ be the dual of $\mathcal{H}(3,q^2)$. Then a hemisystem of $\mathcal{H}(3,q^2)$ corresponds to a set $\mathcal{O}$ consisting of $\frac{1}{2}(q+1)(q^3+1)$ points of $\mathcal{Q}^-(5,q)$ such that every line of $\mathcal{Q}^-(5,q)$ has $\frac{1}{2}(q+1)$ points in common with $\mathcal{O}$. By [3, Theorem 11], a hyperplane of $\mathrm{PG}(5,q)$ meets $\mathcal{O}$ in either $\frac{1}{2}(q+1)(q^2+1)$ or $\frac{1}{2}(q^3-q^2+q+1)$ points, i.e. $\mathcal{O}$ it is called 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. Hence by [5], the set $\mathcal{O}$ gives rise to a strongly regular graph and a two-weight code.

Result 8.1 [5, Theorems 3.1 and 3.2] *Let Ω a subset of $\mathbb{F}_q^k$, with $\Omega = -\Omega$ and $0 \notin \Omega$, and 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. If $\Sigma = \{\langle \mathbf{v_i} \rangle : i = 1, \ldots, n\}$ is a proper subset of* $\mathrm{PG}(k-1,q)$ *that spans* $\mathrm{PG}(k-1,q)$, *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 $[n,k]$-linear two-weight code with weights w_1 and w_2.*

Corollary 8.2 *It exists a family of $[\frac{1}{2}(q^3+1)(q+1), 6]$-linear two-weight codes with weights $w_1 = \frac{1}{2}q^2(q^2-1)$ and $w_2 = \frac{1}{2}q^2(q^2+1)$.*

Acknowledgements The research of Vincenzo Pallozzi Lavorante was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) and by the National Science Foundation under Grant No. 2127742.

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Appendix A

We provide a proof of Proposition 6.7. Since our proof relies on cyclotomic fields from algebraic number theory, we present it in the form of an appendix.

Let $\mathbb{Q}(\zeta_m)$ the cyclotomic field of mth roots of unity with $\zeta_m = e^{2\pi i/m} \in \mathbb{C}$. In particular, the cyclotomic field $\mathbb{Q}(\zeta_{16})$ contains $\sqrt{2}$ as an integer. Let $\mathfrak{b}$ a prime ideal of $\mathbb{Q}(\zeta_{16})$ such that $\mathfrak{b}$ contains p (i.e. $\mathfrak{b} \mid p$). The extension $\mathfrak{b} \mid p$ is unramified and $\mathbb{Z}[\zeta_{16}]/\mathfrak{b} \cong \mathbb{F}_{p^4}$; see [12, Proposition 13.2.5] and [11, Section 4.5]. Note that $h = \pm\sqrt{2} \pmod{\mathfrak{b}}$. We may assume $h \equiv \sqrt{2} \pmod{\mathfrak{b}}$.

Proof of Proposition 6.7 We do the computation for $q \equiv 13 \pmod{16}$, the proofs for the other cases being analogous.

$$
\begin{aligned}
(1+h)^{\frac{q+1}{2}} h^{\frac{q-1}{2}} &\equiv (1+\sqrt{2})^{\frac{q+1}{2}} (\sqrt{2})^{\frac{q-1}{2}} \pmod{\mathfrak{b}}\\
&= (\sqrt{2}+2)^{\frac{q+1}{2}} \frac{1}{\sqrt{2}}\\
&= (\zeta_8+\zeta_8^{-1}+2)^{\frac{q+1}{2}} \frac{1}{\sqrt{2}}\\
&= (\zeta_{16}+\zeta_{16}^{-1})^{q+1} \frac{1}{\sqrt{2}}\\
&\equiv (\zeta_{16}+\zeta_{16}^{-1})(\zeta_{16}^{13}+\zeta_{16}^{-13}) \frac{1}{\sqrt{2}} \pmod{\mathfrak{b}}\\
&\equiv (\zeta_{16}+\zeta_{16}^{-1})(\zeta_{16}^{-3}+\zeta_{16}^{3}) \frac{1}{\sqrt{2}} \pmod{\mathfrak{b}}\\
&= (\zeta_{16}^{4}+\zeta_{16}^{-2}+\zeta_{16}^{2}+\zeta_{16}^{-4}) \frac{1}{\sqrt{2}}\\
&= (\zeta_8+\zeta_8^{-1}) \frac{1}{\sqrt{2}} = 1 \qquad \square
\end{aligned}
$$

References

1. Bamberg J., Giudici M., Royle G.F.: Every flock generalized quadrangle has a hemisystem. Bull. Lond. Math. Soc. **42**(5), 795–810 (2010).
2. Bamberg J., Giudici M., Royle G.F.: Hemisystems of small flock generalized quadrangles. Des. Codes Crypt. **67**(1), 137–157 (2013).
3. Bamberg J., Kelly S., Law M., Penttila T.: Tight sets and m-ovoids of finite polar spaces. J. Comb. Theory Ser. A **114**(7), 1293–1314 (2007).
4. Bamberg J., Lee M., Momihara K., Xiang Q.: A new infinite family of hemisystems of the hermitian surface. Combinatorica **38**(1), 43–66 (2018).
5. Calderbank R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**(2), 97–122 (1986).
6. Cossidente A.: Combinatorial structures in finite classical polar spaces. Surv. Comb. **440**, 204–237 (2017).
7. Cossidente A., Pavese F.: Intriguing sets of quadrics in pg (5, q). Adv. Geom. **17**(3), 339–345 (2017).
8. Cossidente A., Penttila T.: Hemisystems on the hermitian surface. J. Lond. Math. Soc. **72**(3), 731–741 (2005).
9. Fuhrmann R., Torres F.: The genus of curves over finite fields with many rational points. Manuscr. Math. **89**(1), 103–106 (1996).
10. Hirschfeld J., Korchmáros G., Torres F.: Algebraic Curves Over a Finite Field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton (2013).
11. Hou X.D.: Lectures on Finite Fields, Vol. 190. AMS & Graduate Studies in Mathematics (2018).
12. Kenneth I., Michael R.: A classical introduction to modern number theory. Math. Gaz. **76**(476), 316–317 (1992).
13. Korchmáros G., Nagy G.P., Speziali P.: Hemisystems of the hermitian surface. J. Comb. Theory Ser. A **165**, 408–439 (2019).
14. Korchmáros G., Torres F.: Embedding of a maximal curve in a hermitian variety. Compos. Math. **128**(1), 95–113 (2001).
15. OEIS. http://oeis.org/a002496.
16. Pavese F.: Finite classical polar spaces and their geometry (2021).
17. Segre B.: Forme e geometrie hermitiane, con paricolare riguardo al caso finito. Ann. Mat. **70**, 1–201 (1965).
18. Serre J.-P.: Lectures on $N_X(p)$. CRC Press, Boca Raton (2016).