COMBINATORICA
Bolyai Society – Springer-Verlag

Combinatorica 24pp.
DOI: 10.1007/s00493-016-3525-4

A NEW INFINITE FAMILY OF HEMISYSTEMS OF THE HERMITIAN SURFACE

JOHN BAMBERG, MELISSA LEE, KOJI MOMIHARA, QING XIANG

Received November 4, 2015
Revised April 5, 2016

In this paper, we construct an infinite family of hemisystems of the Hermitian surface $\mathsf{H}(3,q^2)$. In particular, we show that for every odd prime power q congruent to 3 modulo 4, there exists a hemisystem of $\mathsf{H}(3,q^2)$ admitting $C_{(q^3+1)/4}{:}C_3$.

1. Introduction

A hemisystem of a generalized quadrangle of order (q^2,q), q odd, is a set of lines $\mathcal{H}$ containing half of the lines on every point. Hemisystems are of interest because they give rise to strongly regular graphs, partial quadrangles and 4-class imprimitive cometric Q-antipodal association schemes that are not metric [14]. For a prime power q, the *classical* generalized quadrangle of order (q^2,q) is the Hermitian surface $\mathsf{H}(3,q^2)$ with automorphism group $\mathsf{P\Gamma U}(4,q)$. An *m-cover* of a generalized quadrangle is a set of lines such that every point is incident with m lines from this set. For instance, a *spread* is a 1-cover and a hemisystem of $\mathsf{H}(3,q^2)$ has $m=(q+1)/2$. It was shown by Segre [12] that the only nontrivial m-covers of $\mathsf{H}(3,q^2)$, q odd, are hemisystems and he gave an example on $\mathsf{H}(3,3^2)$. Bruen and Hirschfeld [7] showed that there

Mathematics Subject Classification (2010): 05B25; 05E30, 51E12

The first author acknowledges the support of the Australian Research Council Future Fellowship FT120100036.

The second author acknowledges the support of a Hackett Postgraduate Research Scholarship.

The third author acknowledges the support by JSPS under Grant-in-Aid for Young Scientists (B) 25800093 and Scientific Research (B) 15H03636.

The fourth author acknowledges the support of an NSF grant DMS-1600850.

are no nontrivial m-covers of $\mathsf{H}(3,q^2)$ when q is even. Segre's example of a hemisystem remained the only example of a hemisystem for thirty years, and so it was reasonable for Thas [13] in 1995 to pose a conjecture that Segre's example was the only one. In 2005, Cossidente and Penttila [8] disproved this conjecture by showing the existence of a hemisystem on $\mathsf{H}(3,q^2)$, q odd, admitting $\mathsf{P\Omega}^-(4,q)$ for each odd prime power q. Cossidente and Penttila [8, Remark 4.4] also found by computer search a hemisystem of $\mathsf{H}(3,7^2)$ with full stabilizer in $\mathsf{P\Gamma U}(4,7)$ a metacyclic group of order 516, and a hemisystem of $\mathsf{H}(3,9^2)$, with full stabilizer in $\mathsf{P\Gamma U}(4,9)$ a metacyclic group of order 876. Bamberg, Giudici and Royle [2, Section 4.1] found that the pattern continues (except, curiously, for q congruent to 1 modulo 12) by finding for each $q\in\{11,17,19,23,27\}$ a hemisystem of $\mathsf{H}(3,q^2)$ admitting a cyclic group of order q^2-q+1. In this paper, we construct an infinite family of hemisystems that generalize the examples above where q is congruent to 3 modulo 4.

Theorem 1.1. *There is a hemisystem of* $\mathsf{H}(3,q^2)$ *for every prime power* $q\equiv 3 \pmod 4$*, each admitting* $C_{(q^3+1)/4}{:}C_3$.

We also prove that this infinite family of hemisystems yields new hemisystems beyond the small known examples. We note from [2] that for $q=3$, our construction gives a hemisystem that is projectively equivalent to Segre's hemisystem, and for $q=7$, the hemisystem is equivalent to that given in [8, Remark 4.4].

Our construction is based on initially identifying a hemisystem of $\mathsf{H}(3,q^2)$ with its dual[1] set of points of the elliptic quadric $\mathcal{Q}^-(5,q)$. A hemisystem (of points) of $\mathcal{Q}^-(5,q)$ in this context is defined as a set of points $\mathcal{M}$ containing half of the points on every line. The technique used to construct these hemisystems is remarkably similar to the technique used in [10] to construct $\frac{(q^2-1)}{2}$-tight sets of $\mathcal{Q}^+(5,q)$, otherwise known via the Klein correspondence as *Cameron-Liebler line classes* of $\mathsf{PG}(3,q)$ with parameter $\frac{(q^2-1)}{2}$. The construction in this paper is essentially a cyclotomic construction, that is, the hemisystem of $\mathcal{Q}^-(5,q)$ we are going to construct is a union of cyclotomic classes of $\mathbb{F}_{q^6}^* = \mathbb{F}_{q^6}\setminus\{0\}$. The first step is to give a finite field model of $\mathcal{Q}^-(5,q)$ for $q\equiv 3 \pmod 4$: we view $\mathbb{F}_{q^6}$ as a 6-dimensional vector space over $\mathbb{F}_q$ and define $\mathcal{Q}^-(5,q)$ (using the underlying vectors instead of projective points) as the nonzero vectors in the zero-set of the quadratic form $\mathrm{Tr}_{q^3/q}(x^{q^3+1})$ defined on $\mathbb{F}_{q^6}$, where $\mathrm{Tr}_{q^3/q}$ is the trace from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$. Note that in this setting, $\mathcal{Q}^-(5,q)$ is also a union of $4(q+1)$ cyclotomic classes of

[1] By interchanging the roles of points and lines of a generalized quadrangle we obtain another generalized quadrangle, the *dual*.

index $4(q^2+q+1)$ of $\mathbb{F}_{q^6}^*$. Of course, this field model and the cyclotomic interpretation of $\mathcal{Q}^-(5,q)$ are well known. In order to construct a hemisystem of $\mathcal{Q}^-(5,q)$, we need to choose half of the cyclotomic classes involved in the definition of $\mathcal{Q}^-(5,q)$. The difficulty lies in deciding which half to choose. We overcome this difficulty by using a partition of a conic in $\mathsf{PG}(2,q)$ first discovered in [10]. This partition of a conic in $\mathsf{PG}(2,q)$ gives us a way to choose half of the cyclotomic classes involved in the definition of $\mathcal{Q}^-(5,q)$, yielding a hemisystem of points of $\mathcal{Q}^-(5,q)$. The proof that our choice indeed works for each $q \equiv 3 \pmod 4$ relies on computations of (additive) character values of the subset of chosen vectors using Gauss sums.

The paper is structured as follows: in Section 2, we give the requisite background on generalized quadrangles (particularly the elliptic quadric $\mathcal{Q}^-(5,q)$), m-ovoids, strongly regular graphs, Cayley graphs, and Gauss sums. Then in Sections 3 and 4 we work towards describing the new hemisystems and giving a proof of Theorem 1.1. Finally, we show that the hemisystems we have constructed are indeed new.

2. Preliminaries

2.1. Generalized quadrangles and m-ovoids

A generalized quadrangle of order (s,t) is a point-line incidence structure obeying the following axioms.

- Any two points are incident with at most one line.
- Every line is incident with $s+1$ points.
- Every point is incident with $t+1$ lines.
- Given a point P and a line ℓ that are not incident, there is a unique point Q on ℓ that is collinear to P.

The dual of a generalized quadrangle of order (s,t) is a generalized quadrangle of order (t,s). The family of generalized quadrangles that we are mainly interested in are the Hermitian surfaces $\mathsf{H}(3,q^2)$, where q is a prime power. We define $\mathsf{H}(3,q^2)$ to be comprised of the set of totally isotropic points and lines of a non-degenerate Hermitian form on $\mathsf{PG}(3,q^2)$; which results in a generalized quadrangle of order (q^2,q). The dual of $\mathsf{H}(3,q^2)$ is a generalized quadrangle of order (q,q^2), isomorphic to the geometry of totally singular points and lines of an elliptic quadric $\mathcal{Q}^-(5,q)$ arising from a non-singular quadratic form of minus type on $\mathsf{PG}(5,q)$.

We will be working almost exclusively in this dual setting. Let $m \geq 1$ be an integer. A set of points is said to be an *m-ovoid* of $\mathcal{Q}^-(5,q)$ if every

line of $\mathcal{Q}^-(5,q)$ meets the set in m points. Note that an m-ovoid is the dual concept to an m-cover of lines (i.e., upon interchanging the roles of points and lines), and in particular from the above results, a nontrivial m-ovoid of $\mathcal{Q}^-(5,q)$ must have $m=(q+1)/2$. The following lemma follows directly from [3, Lemma 1].

Lemma 2.1. *Let $\mathcal{M}$ be a set of $m(q^3+1)$ points in $\mathcal{Q}^-(5,q)$. Then, $\mathcal{M}$ is an m-ovoid of $\mathcal{Q}^-(5,q)$ if and only if*

$$|P^\perp \cap \mathcal{M}| = \begin{cases} (m-1)(q^2+1)+1, & \text{if } P \in \mathcal{M}, \\ m(q^2+1), & \text{otherwise.} \end{cases}$$

Here $\perp$ is the polarity defined by the elliptic quadric $\mathcal{Q}^-(5,q)$.

The above result makes it possible to use projective two-intersection sets for constructing m-ovoids. A two-intersection set $\mathcal{K}$ is a set of points in $\mathsf{PG}(n,q)$ such that every hyperplane of $\mathsf{PG}(n,q)$ is incident with either h_1 or h_2 points of $\mathcal{K}$. We call h_1 and h_2 *intersection numbers*. A related concept to a two-intersection set is an intriguing set. A set $\mathcal{I}$ of points of a generalized quadrangle is called *intriguing* if there are integers k_1 and k_2 such that the number of points of $\mathcal{I}$ collinear to an arbitrary point P of the generalized quadrangle is k_1 if $P\in\mathcal{I}$, and k_2 otherwise.

2.2. Strongly regular graphs and Cayley graphs

A (v,k,λ,μ) *strongly regular graph* is a simple undirected regular graph on v vertices with valency k satisfying the following: for any two adjacent (resp. nonadjacent) vertices x and y there are exactly λ (resp. μ) vertices adjacent to both x and y. It is known that a graph with valency k, not complete or edgeless, is strongly regular if and only if its adjacency matrix has exactly two restricted eigenvalues. Here, we say that an eigenvalue of the adjacency matrix is *restricted* if it has an eigenvector perpendicular to the all-ones vector.

Let G be a finite abelian group and D be an inverse-closed subset of $G\setminus\{0\}$. We define a graph $\mathrm{Cay}(G,D)$ with the elements of G as its vertices; two vertices x and y are adjacent if and only if $x-y\in D$. The graph $\mathrm{Cay}(G,D)$ is called a *Cayley graph* on G with connection set D. The eigenvalues of $\mathrm{Cay}(G,D)$ are given by $\psi(D)$, $\psi\in\widehat{G}$, where $\widehat{G}$ is the *dual group* consisting of all characters of G. Using the aforementioned spectral characterization of strongly regular graphs, we see that $\mathrm{Cay}(G,D)$ with connection set $D(\neq\varnothing,G)$ is strongly regular if and only if $\psi(D)$, $\psi\in\widehat{G}\setminus\{1\}$, take exactly two

values, say α_1 and α_2. We note that if $\mathrm{Cay}(G,D)$ is strongly regular with two restricted eigenvalues α_1 and α_2, then the sets $\{\psi \in \widehat{G}\colon \psi(D)=\alpha_i\}$, $i=1,2$, also form connection sets of strongly regular Cayley graphs on $\widehat{G}$; one is the complement of another in $\widehat{G}\setminus\{1\}$, and each of these sets is called the *dual* of D.

For a nonzero vector $x\in\mathbb{F}_q^6$, we use $\langle x\rangle$ to denote the projective point in $\mathsf{PG}(5,q)$ corresponding to the one-dimensional subspace over $\mathbb{F}_q$ spanned by x. In this paper, we will use the following relation between certain intriguing sets and strongly regular graphs: For an intriguing set $\mathcal{M}$ in $\mathcal{Q}^-(5,q)$, define $D:=\{\lambda x\colon \lambda\in\mathbb{F}_q^*, \langle x\rangle\in\mathcal{M}\}$, which is a subset of $(\mathbb{F}_q^6,+)$. Then the Cayley graph with vertex set $(\mathbb{F}_q^6,+)$ and connection set D is strongly regular. Its restricted eigenvalues can be determined as follows. Let ψ be a nontrivial additive character of $\mathbb{F}_q^6$. Then ψ is principal on a unique hyperplane $P^\perp$ for some $P\in\mathsf{PG}(5,q)$. We have

$$\begin{aligned}\psi(D) &= \sum_{\langle x\rangle\in\mathcal{M}}\sum_{\lambda\in\mathbb{F}_q^*}\psi(\lambda x) = \sum_{\langle x\rangle\in\mathcal{M}}(q\mathbb{1}_{P^\perp}(\langle x\rangle)-1)\\ &= -|\mathcal{M}|+q|P^\perp\cap\mathcal{M}| = \begin{cases}-q^3+m(q-1), & \text{if } P\in\mathcal{M},\\ m(q-1), & \text{otherwise,}\end{cases}\end{aligned}$$

where for a subset S of the points, $\mathbb{1}_S$ is the characteristic function taking value 1 on elements of S and value 0 elsewhere. Conversely, for each hyperplane $P^\perp$ of $\mathsf{PG}(5,q)$, we can find a nontrivial character ψ that is principal on $P^\perp$, and the size of $P^\perp\cap\mathcal{M}$ can be computed from $\psi(D)$. Therefore, the character values of D reflect the intersection properties of $\mathcal{M}$ with the hyperplanes of $\mathsf{PG}(5,q)$. To summarize, we have the following result.

Result 2.2. *Let $\mathcal{M}$ be a set of $m(q^3+1)$ points in $\mathcal{Q}^-(5,q)$. Define*

$$D:=\{\lambda x\colon \lambda\in\mathbb{F}_q^*, \langle x\rangle\in\mathcal{M}\}\subset(\mathbb{F}_q^6,+). \tag{2.1}$$

Then, $\mathcal{M}$ is an m-ovoid of $\mathcal{Q}^-(5,q)$ if and only if for any $P\in\mathsf{PG}(5,q)$

$$\psi(D)=\begin{cases}-q^3+m(q-1), & \text{if } P\in\mathcal{M},\\ m(q-1), & \text{otherwise,}\end{cases}$$

where ψ is any nontrivial character of $\mathbb{F}_q^6$ that is principal on the hyperplane $P^\perp$.

2.3. A finite field model of the elliptic quadric $\mathcal{Q}^-(5,q)$

We will use the following model of $\mathcal{Q}^-(5,q)$. We view $\mathbb{F}_{q^6}$ as a 6-dimensional vector space over $\mathbb{F}_q$. We define the trace function $\mathrm{Tr}_{q^n/q}\colon \mathbb{F}_{q^n} \to \mathbb{F}_q$ by $\mathrm{Tr}_{q^n/q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$. Define a quadratic form $Q\colon \mathbb{F}_{q^6} \to \mathbb{F}_q$ by

$$Q(x) := \mathrm{Tr}_{q^3/q}(x^{q^3+1}).$$

The quadratic form Q is clearly elliptic and the projective points corresponding to the nonzero vectors of $\{x \in \mathbb{F}_{q^6} \mid Q(x) = 0\}$ form an elliptic quadric. This will be our model for $\mathcal{Q}^-(5,q)$. Note that for a point $P = \langle x \rangle$, its polar hyperplane $P^\perp$ is given by $P^\perp = \{\langle y \rangle\colon \mathrm{Tr}_{q^6/q}(yx^{q^3}) = 0\}$.

Let $\psi_{\mathbb{F}_{q^6}}$ and $\psi_{\mathbb{F}_q}$ be the canonical additive characters of $\mathbb{F}_{q^6}$ and $\mathbb{F}_q$, respectively. Then, each nontrivial additive character ψ_a of $\mathbb{F}_{q^6}$ has the form

$$\psi_a(x) = \psi_{\mathbb{F}_{q^6}}(ax) = \psi_{\mathbb{F}_q}(\mathrm{Tr}_{q^6/q}(ax)),\ x \in \mathbb{F}_{q^6}, \tag{2.2}$$

where $a \in \mathbb{F}_{q^6}^*$. Since ψ_a is principal on the hyperplane $\{\langle x \rangle\colon \mathrm{Tr}_{q^6/q}(ax) = 0\} = P^\perp$ with $P = \langle a^{q^3} \rangle$, the character sum condition in Result 2.2 can be more explicitly rewritten as

$$\psi_a(D) = \begin{cases} -q^3 + m(q-1), & \text{if } a^{q^3} \in D, \\ m(q-1), & \text{otherwise.} \end{cases} \tag{2.3}$$

2.4. Gauss sums

We need some preparation for computing (additive) character values of a subset of vectors of $\mathbb{F}_{q^n}$. For a multiplicative character χ and the canonical additive character ψ of $\mathbb{F}_q$, define the *Gauss sum* by

$$G_q(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x).$$

The following are some basic properties of Gauss sums:

(i) $G_q(\chi)\overline{G_q(\chi)} = q$ if χ is nontrivial;
(ii) $G_q(\chi^{-1}) = \chi(-1)\overline{G_q(\chi)}$;
(iii) $G_q(\chi) = -1$ if χ is trivial.

Let γ be a fixed primitive element of $\mathbb{F}_q$ and k a positive integer dividing $q-1$. For $0 \leqslant i \leqslant k-1$ we set $C_i^{(k,q)} = \gamma^i C_0$, where C_0 is the subgroup of index k of $\mathbb{F}_q^*$. The *Gauss periods* associated with these cyclotomic classes are defined by $\psi(C_i^{(k,q)}) := \sum_{x \in C_i^{(k,q)}} \psi(x)$, $0 \leqslant i \leqslant k-1$, where ψ is the canonical additive character of $\mathbb{F}_q$. As described in the introduction, since we take a union of cyclotomic classes of index $k = 4(q^2+q+1)$ of $\mathbb{F}_{q^6}$ as a subset D of (2.1), we need to compute a sum of Gauss periods. By orthogonality of characters, the Gauss periods can be expressed as a linear combination of Gauss sums:

$$\psi(C_i^{(k,q)}) = \frac{1}{k} \sum_{j=0}^{k-1} G_q(\chi^j) \chi^{-j}(\gamma^i), \ 0 \leqslant i \leqslant k-1, \tag{2.4}$$

where χ is any fixed multiplicative character of order k of $\mathbb{F}_q$.

Theorem 2.3. ([15, Theorem 1]) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_{q^n}$ and χ' be its restriction to $\mathbb{F}_q$. Take a system L of representatives of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ such that $\mathrm{Tr}_{q^n/q}$ maps L onto $\{0,1\} \subset \mathbb{F}_q$. Partition L into two parts:*

$$L_0 = \{x \in L \colon \mathrm{Tr}_{q^n/q}(x) = 0\} \text{ and } L_1 = \{x \in L \colon \mathrm{Tr}_{q^n/q}(x) = 1\}.$$

Then,

$$\sum_{x \in L_1} \chi(x) = \begin{cases} G_{q^n}(\chi)/G_q(\chi'), & \text{if } \chi' \text{ is nontrivial,} \\ -G_{q^n}(\chi)/q, & \text{otherwise.} \end{cases}$$

Theorem 2.4. ([6, Theorem 11.6.3]) *Let p be a prime. Suppose that $m > 2$ and p is semi-primitive modulo m, i.e., there exists a positive integer s such that $p^s \equiv -1 \pmod{m}$. Choose s minimal and write $f = 2st$ for any positive integer t. Let χ_m be a multiplicative character of order m of $\mathbb{F}_{p^f}$. Then,*

$$p^{-f/2} G_{p^f}(\chi_m) = \begin{cases} (-1)^{t-1}, & \text{if } p = 2, \\ (-1)^{t-1+(p^s+1)t/m}, & \text{if } p > 2. \end{cases}$$

We will need the *Davenport-Hasse lifting formula*, which is stated below.

Theorem 2.5. ([6, Theorem 11.5.2]) *Let χ' be a nontrivial multiplicative character of $\mathbb{F}_{p^f}$ and let χ be the lift of χ' to $\mathbb{F}_{p^{fs}}$, i.e., $\chi(\alpha) = \chi'(\mathrm{Norm}_{p^{fs}/p^f}(\alpha))$ for $\alpha \in \mathbb{F}_{p^{fs}}$, where $s \geq 2$ is an integer. Then*

$$G_{p^{fs}}(\chi) = (-1)^{s-1} (G_{p^f}(\chi'))^s.$$

The following theorem is often referred to as the *Davenport-Hasse product formula*.

Theorem 2.6. ([6, Theorem 11.3.5]) *Let η be a multiplicative character of order $\ell>1$ of $\mathbb{F}_{p^f}$. For every nontrivial multiplicative character χ of $\mathbb{F}_{p^f}$,*

$$G_{p^f}(\chi)=\frac{G_{p^f}(\chi^\ell)}{\chi^\ell(\ell)}\prod_{i=1}^{\ell-1}\frac{G_{p^f}(\eta^i)}{G_{p^f}(\chi\eta^i)}.$$

The following is the main theorem of this section.

Theorem 2.7. *Let $q=p^f$ be an odd prime power such that $q\equiv 3 \pmod 4$, and let m be an odd positive integer dividing $N=q^2+q+1$. Let χ'_m be a multiplicative character of order m of $\mathbb{F}_{q^3}$ and χ_m be its lift to $\mathbb{F}_{q^6}$, and χ_4 be a multiplicative character of order 4 of $\mathbb{F}_{q^6}$. Then, it holds that $G_{q^6}(\chi_4\chi_m)=G_{q^6}(\chi_4^3\chi_m)$. In particular, it holds that*

$$G_{q^6}(\chi_4\chi_m)=\rho_q G_{q^3}({\chi'}_m^4)G_{q^3}({\chi'}_m^{-2}), \tag{2.5}$$

where $\rho_q=-1$ or 1 depending on whether $q\equiv 3 \pmod 8$ or $q\equiv 7 \pmod 8$.

Proof. First, we have

$$G_{q^6}(\chi_4\chi_m)=G_{q^6}(\chi_4^{q^3}\chi_m^{q^3})=G_{q^6}(\chi_4^3\chi_m).$$

Applying the Davenport-Hasse product formula (Theorem 2.6) with $\ell=4$, $\chi=\chi_4\chi_m$, and $\eta=\chi_4$, we have

$$\begin{aligned} G_{q^6}(\chi_4\chi_m)&=\frac{G_{q^6}(\chi_m^4)G_{q^6}(\chi_4)G_{q^6}(\chi_4^2)G_{q^6}(\chi_4^3)}{\chi_m^4(4)G_{q^6}(\chi_4^2\chi_m)G_{q^6}(\chi_4^3\chi_m)G_{q^6}(\chi_m)}\\ &=q^6\frac{G_{q^6}(\chi_m^4)G_{q^6}(\chi_4^2)}{G_{q^6}(\chi_4^2\chi_m)G_{q^6}(\chi_4\chi_m)G_{q^6}(\chi_m)}. \end{aligned} \tag{2.6}$$

On the other hand, we have

$$G_{q^6}(\chi_4^2\chi_m)=\frac{G_{q^6}(\chi_m^2)G_{q^6}(\chi_4^2)}{\chi_m^2(2)G_{q^6}(\chi_m)}=\frac{G_{q^6}(\chi_m^2)G_{q^6}(\chi_4^2)}{G_{q^6}(\chi_m)}. \tag{2.7}$$

By substituting (2.7) into (2.6), we have

$$G_{q^6}(\chi_4\chi_m)^2=q^6\frac{G_{q^6}(\chi_m^4)}{G_{q^6}(\chi_m^2)}=G_{q^6}(\chi_m^4)G_{q^6}(\chi_m^{-2}). \tag{2.8}$$

Then, by the Davenport-Hasse lifting formula (Theorem 2.5), Eq. (2.8) is reformulated as

$$G_{q^6}(\chi_4\chi_m)^2 = G_{q^3}(\chi'^4_m)^2 G_{q^3}(\chi'^{-2}_m)^2,$$

i.e.,

$$G_{q^6}(\chi_4\chi_m) = \rho G_{q^3}(\chi'^4_m) G_{q^3}(\chi'^{-2}_m)$$

for some $\rho \in \{-1, 1\}$.

Now, we determine the sign of ρ by induction. Write $m = \ell p_1$, where ℓ is a positive integer and p_1 is an odd prime. First we consider the case where $\ell = 1$, i.e., $m = p_1$. Take the reduction of $G_{q^6}(\chi_4\chi_{p_1})^{p_1}$ modulo p_1:

$$\begin{aligned} G_{q^6}(\chi_4\chi_{p_1})^{p_1} &\equiv \sum_{z\in\mathbb{F}^*_{q^6}} \chi_4^{p_1}\chi_{p_1}^{p_1}(z)\psi(p_1 z) \pmod{p_1} \\ &= \sum_{z\in\mathbb{F}^*_{q^6}} \chi_4^{-p_1}(p_1)\chi_4^{p_1}(p_1 z)\psi(p_1 z) \\ &= G_{q^6}(\chi_4^{p_1}) = G_{q^6}(\chi_4). \end{aligned} \tag{2.9}$$

By Theorem 2.4, we have $G_{q^6}(\chi_4) = \rho_q q^3$, where $\rho_q = -1$ or 1 depending on whether $q \equiv 3 \pmod 8$ or $q \equiv 7 \pmod 8$. On the other hand,

$$\begin{aligned} G_{q^6}(\chi_4\chi_{p_1})^{p_1} &= \left(\rho G_{q^3}(\chi'^4_{p_1}) G_{q^3}(\chi'^{-2}_{p_1})\right)^{p_1} \\ &= \rho^{p_1} G_{q^3}(\chi'^4_{p_1})^{p_1} G_{q^3}(\chi'^{-2}_{p_1})^{p_1} \equiv \rho \pmod{p_1}. \end{aligned} \tag{2.10}$$

Hence, by Eqs. (2.9) and (2.10), we have $\rho \equiv \rho_q q^3 \pmod{p_1}$. Since $p_1 \mid (q^3-1)$, we obtain $\rho = \rho_q$.

We next consider the case where $\ell > 1$. Write $\ell = p_2\ell'$ with p_2 a prime, and let $\chi_{\ell' p_1} := \chi_m^{p_2}$. Assume that

$$G_{q^6}(\chi_4\chi_{\ell' p_1}) = \rho_q G_{q^3}(\chi'^4_{\ell' p_1}) G_{q^3}(\chi'^{-2}_{\ell' p_1}).$$

Then, we have

$$G_{q^6}(\chi_4\chi_m)^{p_2} \equiv \sum_{z\in\mathbb{F}^*_{q^6}} \chi_4^{p_2}\chi_m^{p_2}(z)\psi(p_2 z) \pmod{p_2} = G_{q^6}(\chi_4\chi_{\ell' p_1}).$$

On the other hand,

$$\begin{aligned} G_{q^6}(\chi_4\chi_m)^{p_2} &= \rho G_{q^3}(\chi'^4_m)^{p_2} G_{q^3}(\chi'^{-2}_m)^{p_2} \\ &\equiv \rho G_{q^3}(\chi'^4_{\ell' p_1}) G_{q^3}(\chi'^{-2}_{\ell' p_1}) \pmod{p_2}. \end{aligned}$$

This implies that $\rho = \rho_q$. This completes the proof of the theorem. ∎

Corollary 2.8. *With the same notation as in Theorem 2.7, it holds that*

$$G_{q^6}(\chi_4\chi_m) = \rho_q \frac{q^3 G_{q^3}(\chi_2'\chi_m'^2)}{G_{q^3}(\chi_2')},$$

where χ_2' is the quadratic character of $\mathbb{F}_{q^3}$.

Proof. Applying the Davenport-Hasse product formula with $\ell = 2$, $\chi = \chi_2'\chi_m'^2$ and $\eta = \chi_2'$, we have

$$G_{q^3}(\chi_2'\chi_m'^2) = \frac{G_{q^3}(\chi_2')}{q^3} G_{q^3}(\chi_m'^4) G_{q^3}(\chi_m'^{-2}).$$

Then, Eq. (2.5) of Theorem 2.7 is reformulated as

$$G_{q^6}(\chi_4\chi_m) = \rho_q \frac{q^3 G_{q^3}(\chi_2'\chi_m'^2)}{G_{q^3}(\chi_2')}.$$

This completes the proof. ∎

3. The beginnings of a construction: a partition of a conic in $\mathsf{PG}(2,q)$

Let ω be a primitive element of $\mathbb{F}_{q^3}$ and $N := q^2+q+1$. Viewing $\mathbb{F}_{q^3}$ as a 3-dimensional vector space over $\mathbb{F}_q$, we will use $\mathbb{F}_{q^3}$ as the underlying vector space of $\mathsf{PG}(2,q)$. The points of $\mathsf{PG}(2,q)$ are $\langle\omega^i\rangle$, $0 \leqslant i \leqslant N-1$, and the lines of $\mathsf{PG}(2,q)$ are

$$L_c := \{\langle x\rangle \colon \mathrm{Tr}_{q^3/q}(\omega^c x) = 0\}, \tag{3.1}$$

where $0 \leqslant c \leqslant N-1$. Of course, $\langle\omega^i\rangle = \langle\omega^{i+jN}\rangle$ and $L_c = L_{c+jN}$, for any i, j and c.

Define a quadratic form $f\colon \mathbb{F}_{q^3} \to \mathbb{F}_q$ by $f(x) := \mathrm{Tr}_{q^3/q}(x^2)$. The associated bilinear form $B\colon \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \to \mathbb{F}_q$ is given by $B(x,y) = 2\,\mathrm{Tr}_{q^3/q}(xy)$. It is clear that B is nondegenerate. Therefore f defines a conic $\mathcal{Q}$ in $\mathsf{PG}(2,q)$, which contains $q+1$ points. Consequently, each line l of $\mathsf{PG}(2,q)$ meets $\mathcal{Q}$ in 0, 1 or 2 points, and l is called an *exterior*, *tangent* or *secant line* accordingly. Also it is known that each point $P \in \mathsf{PG}(2,q) \setminus \mathcal{Q}$ is on either 0 or 2 tangent lines to $\mathcal{Q}$, and P is called an *interior* or *exterior point* accordingly.

Consider the following subset of $\mathbb{Z}_N$:

$$I_{\mathcal{Q}} := \{i \colon 0 \leqslant i \leqslant N-1,\ \mathrm{Tr}_{q^3/q}(\omega^{2i}) = 0\} = \{d_0, d_1, \ldots, d_q\}, \tag{3.2}$$

where the elements are numbered in any (unspecified) order. That is, $\mathcal{Q} = \{\langle \omega^{d_i} \rangle \colon 0 \leqslant i \leqslant q\}$. Furthermore, consider the following subset (a so-called *Singer difference set*) of $\mathbb{Z}_N$:

$$S := \{i \pmod N \colon \mathrm{Tr}_{q^3/q}(\omega^i) = 0\}. \tag{3.3}$$

That is, $L_0 = \{\langle \omega^i \rangle \colon i \in S\}$. Then, it is clear that $I_{\mathcal{Q}} \equiv 2^{-1} S \pmod N$.

For $x \in \mathbb{F}_{q^3}$, we define the sign of x, $\mathrm{sgn}(x) \in \{0, 1, -1\}$, by

$$\mathrm{sgn}(x) = \begin{cases} 1, & \text{if } x \text{ is a nonzero square,} \\ -1, & \text{if } x \text{ is a nonsquare,} \\ 0, & \text{if } x = 0. \end{cases} \tag{3.4}$$

Lemma 3.1. *With the above notation, we have the following.*

1. *The polarity of* $\mathsf{PG}(2,q)$ *induced by* $\mathcal{Q}$ *interchanges* $\langle \omega^c \rangle$ *and* L_c. *In particular, it maps points on* $\mathcal{Q}$ *to tangent lines, and exterior (resp. interior) points to secant (resp. exterior) lines.*
2. *For any point* $P = \langle x \rangle$ *off* $\mathcal{Q}$, P *is exterior (resp. interior) if and only if* $\mathrm{sgn}(f(x)) = \epsilon$ *(resp.* $-\epsilon$*), where* $\epsilon = 1$ *or* -1 *depending on whether* $q \equiv 1 \pmod 4$ *or* $3 \pmod 4$.

Proof. For the proof of (1), we refer the reader to [11]. For the proof of (2) in the case where $q \equiv 1 \pmod 4$, see [10, Lemma 3.3]. The case $q \equiv 3 \pmod 4$ can be proved in a similar way. ∎

By Lemma 3.1,

$$\begin{aligned} L_c \text{ is tangent} &\Leftrightarrow \mathrm{sgn}(f(\omega^c)) = 0 \Leftrightarrow |(S - c) \cap I_{\mathcal{Q}}| = 1, \\ L_c \text{ is exterior} &\Leftrightarrow \mathrm{sgn}(f(\omega^c)) = -\epsilon \Leftrightarrow |(S - c) \cap I_{\mathcal{Q}}| = 0, \\ L_c \text{ is secant} &\Leftrightarrow \mathrm{sgn}(f(\omega^c)) = \epsilon \Leftrightarrow |(S - c) \cap I_{\mathcal{Q}}| = 2. \end{aligned}$$

Define $D_1 := \bigcup_{i \in I_{\mathcal{Q}}} C_i^{(N,q^3)}$, where $C_i^{(N,q^3)}$ is represented by $\langle \omega^i \rangle$. Then, D_1 takes exactly three nontrivial character values:

$$\begin{aligned} \sum_{i \in I_{\mathcal{Q}}} \psi_{\mathbb{F}_{q^3}}(\omega^c C_i^{(N,q^3)}) &= \sum_{i \in I_{\mathcal{Q}}} \psi_{\mathbb{F}_q}(\mathrm{Tr}_{q^3/q}(\omega^{c+i}) \mathbb{F}_q^*) = q|(S - c) \cap I_{\mathcal{Q}}| - (q+1) \\ &= \begin{cases} -1, & \text{if } c \pmod N \in I_{\mathcal{Q}}, \\ -1 + \epsilon q, & \text{if } c \pmod N \in I_s, \\ -1 - \epsilon q, & \text{if } c \pmod N \in I_n, \end{cases} \end{aligned} \tag{3.5}$$

where $I_s := \{i \pmod N \colon \mathrm{Tr}_{q^3/q}(\omega^{2i}) \in C_0^{(2,q)}\}$ and $I_n := \{i \pmod N \colon \mathrm{Tr}_{q^3/q}(\omega^{2i}) \in C_1^{(2,q)}\}$.

Remark 3.2. We define the following subsets of $\mathbb{F}_{q^3}$:

$$D_0 := \{0\},\ D_1 := \bigcup_{i\in I_{\mathcal{Q}}} C_i^{(N,q^3)},\ D_2 := \bigcup_{i\in I_s} C_i^{(N,q^3)},\ D_3 := \bigcup_{i\in I_n} C_i^{(N,q^3)}.$$

In the language of association schemes, the Cayley graphs $\mathrm{Cay}(\mathbb{F}_{q^3}, D_i)$, $i=0,1,2,3$, form a three-class association scheme on $\mathbb{F}_{q^3}$. See [5].

We will consider a partition of D_1. For $d_0 \in I_{\mathcal{Q}}$, we define

$$\mathcal{X} := \{\omega^{d_i} \mathrm{Tr}_{q^3/q}(\omega^{d_0+d_i})\colon 1 \leqslant i \leqslant q\} \cup \{2\omega^{d_0}\}$$

and

$$X := \{\log_\omega(x) \pmod{2N}\colon x \in \mathcal{X}\} \subset \mathbb{Z}_{2N}.$$

It is clear that $X \equiv I_{\mathcal{Q}} \pmod N$. We list a few properties of the set X below.

Remark 3.3. (i) ([10, Lemma 3.4]) If we use any other d_i in place of d_0 in the definition of $\mathcal{X}$, then the resulting set X' satisfies $X' \equiv X \pmod{2N}$ or $X' \equiv X+N \pmod{2N}$.

(ii) ([10, Remark 3.5]) The set X is invariant under multiplication by q modulo $2N$.

The set X was used to construct $\frac{(q^2-1)}{2}$-tight sets of $\mathcal{Q}^+(5,q)$ in [10]. We note that $\frac{(q^2-1)}{2}$-tight sets of $\mathcal{Q}^+(5,q)$ were independently constructed in [9]. Surprisingly, X is also behind our new $(q+1)/2$-ovoids of $\mathcal{Q}^-(5,q)$.

The set X can be expressed as

$$X = 2S_1'' \cup (2S_2'' + N) \pmod{2N} \tag{3.6}$$

for some $S_1'', S_2'' \subseteq \mathbb{Z}_N$ with $|S_1''|+|S_2''| = q+1$. That is, we are partitioning X into the *even* and *odd* parts. Define $S_i' \equiv 2S_i'' \pmod N$ and $S_i \equiv 2S_i' \pmod N$ for $i=1,2$. Then, $S_1' \cup S_2' \equiv I_{\mathcal{Q}} \pmod N$ and $S_1 \cup S_2 \equiv S \pmod N$, i.e., X induces partitions of the conic $\mathcal{Q}$ and the line L_0, respectively. We will use this partition S_1, S_2 of S to define our $(q+1)/2$-ovoids in the next section. Consider the following partition of D_1:

$$D_{1,1} := \bigcup_{i\in X} C_i^{(2N,q^3)} \text{ and } D_{1,2} := \bigcup_{i\in X+N} C_i^{(2N,q^3)}.$$

Theorem 3.4. ([10, Theorem 3.7, Remark 3.8]) *With notation as above, the set $D_{1,1}$ takes exactly four nontrivial character values, that is,*

$$\psi_{\mathbb{F}_{q^3}}(\omega^c D_{1,1}) = \begin{cases} \frac{-1+\eta(2)qG_q(\eta)}{2}, & \text{if } c \pmod N \in I_Q \text{ and } c \pmod{2N} \in X, \\ \frac{-1-\eta(2)qG_q(\eta)}{2}, & \text{if } c \pmod N \in I_Q \text{ and } c \pmod{2N} \in X+N, \\ \frac{-1+\epsilon q}{2}, & \text{if } c \pmod N \in I_s, \\ \frac{-1-\epsilon q}{2}, & \text{if } c \pmod N \in I_n, \end{cases}$$

where η is the quadratic character of $\mathbb{F}_q$.

Remark 3.5. (i) In [10], the authors treated only the case where $q \equiv 1 \pmod 4$ of Theorem 3.4. The case $q \equiv 3 \pmod 4$ can be proved in a similar way.

(ii) In the language of association schemes, the Cayley graphs $\mathrm{Cay}(\mathbb{F}_{q^3}, D_i)$, $i = 0, 2, 3$, and $\mathrm{Cay}(\mathbb{F}_{q^3}, D_{1,j})$, $j = 1, 2$, form a four-class association scheme on $\mathbb{F}_{q^3}$, which is a fission scheme of the scheme mentioned in Remark 3.2.

4. New $\frac{q+1}{2}$-ovoids of $\mathcal{Q}^-(5,q)$

In the rest of this paper, we assume that $q \equiv 3 \pmod 4$ is a prime power. In this section, we give a construction of $\frac{q+1}{2}$-ovoids of $\mathcal{Q}^-(5,q)$.

4.1. Construction of $\frac{q+1}{2}$-ovoids of $\mathcal{Q}^-(5,q)$

Consider the following bilinear form from $\mathbb{F}_{q^6}^2$ to $\mathbb{F}_q$:

$$B(x,y) := \mathrm{Tr}_{q^6/q}(xy^{q^3}).$$

This form is symmetric and defines an elliptic orthogonal space isomorphic to $\mathcal{Q}^-(5,q)$, where the associated quadratic form is given by $Q(x) = \mathrm{Tr}_{q^3/q}(x^{q^3+1})$. We now define a subset D of the elliptic quadric $\{x \in \mathbb{F}_{q^6}^* \colon \mathrm{Tr}_{q^3/q}(x^{q^3+1}) = 0\}$.

Construction 4.1. *Let S_1, S_2 be the partition of the Singer difference set S defined by S_1'', S_2'' of (3.6). Let $J_1 := \{0,3\}$ and $J_2 := \{1,2\}$, and put*

$$I := \{Ni - (q+1)j \pmod{4N} \colon (i,j) \in (J_1 \times S_1) \cup (J_2 \times S_2)\}.$$

Now, define

$$D := \bigcup_{i \in I} C_i^{(4N,q^6)},$$

where $C_i^{(4N,q^6)} := \gamma^i C_0$ *with* C_0 *the subgroup of index* $4N$ *of* $\mathbb{F}_{q^6}^*$ *and* γ *a fixed primitive element of* $\mathbb{F}_{q^6}$ *such that* $\gamma^{q^3+1} = \omega$ *(where* ω *was defined in Section 3).*

It is clear that $|D| = (q^3+1)(q^2-1)/2$. Furthermore, D is a subset of $\{x \in \mathbb{F}_{q^6} : \mathrm{Tr}_{q^3/q}(x^{q^3+1}) = 0\}$. In fact, for any $x = \gamma^{Ni-(q+1)j+s} \in D$ with $\gamma^s \in C_0^{(4N,q^6)}$

$$\begin{aligned}\mathrm{Tr}_{q^3/q}(\gamma^{(Ni-(q+1)j+s)(q^3+1)}) &= \mathrm{Tr}_{q^3/q}(\omega^{Ni-(q+1)j+s}) \\ &= \omega^{Ni+s-Nj}\,\mathrm{Tr}_{q^3/q}(\omega^{Nj-(q+1)j}) \\ &= \omega^{Ni+s-Nj}\,\mathrm{Tr}_{q^3/q}(\omega^j) = 0.\end{aligned}$$

The following is our main theorem which will be proved in the next section.

Theorem 4.2. *The set* $\mathcal{M}$ *of points in* $\mathsf{PG}(5,q)$ *corresponding to* D *(defined in Construction 4.1) forms a* $(q+1)/2$*-ovoid of* $\mathcal{Q}^-(5,q)$.

4.2. Computations of character values

By Result 2.2, we only need to show that the (additive) character values of D take the prescribed values. In particular, it suffices to show that for all $\gamma^a \in \mathbb{F}_{q^6}^*$,

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D) = \begin{cases} -q^3 + \frac{q^2-1}{2}, & \text{if } \gamma^{aq^3} \in D, \\ \frac{q^2-1}{2}, & \text{otherwise,} \end{cases}$$

where $\psi_{\mathbb{F}_{q^6}}$ is the canonical additive character of $\mathbb{F}_{q^6}$.

Let χ_4, χ_N, and χ_{4N} be multiplicative characters of order 4, N, and $4N$ of $\mathbb{F}_{q^6}$, respectively. By the orthogonality of characters, we have

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D) = \frac{1}{4N} \sum_{h=0}^{4N-1} G_{q^6}(\chi_{4N}^h) \sum_{i \in I} \chi_{4N}^{-h}(\gamma^{a+i}). \tag{4.1}$$

Since $\gcd(4,N)=1$, χ_{4N}^h is uniquely expressed as $\chi_4^{h_1}\chi_N^{h_2}$ for some $(h_1,h_2)\in \mathbb{Z}_4\times\mathbb{Z}_N$. Then, the right hand side of Eq. (4.1) is rewritten as

$$\frac{1}{4N}\sum_{h_1=0,1,2,3}\sum_{h_2=0}^{N-1} G_{q^6}(\chi_4^{h_1}\chi_N^{h_2})\left(\sum_{j\in J_1}\sum_{s\in S_1}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a-(q+1)s}) + \sum_{j\in J_2}\sum_{s\in S_2}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a-(q+1)s})\right). \tag{4.2}$$

By noting that each S_i is invariant under multiplication by q modulo N, we have

$$\begin{aligned}
&\psi_{\mathbb{F}_{q^6}}(\gamma^a D)\\
&= \frac{1}{4N}\sum_{h_1=0,1,2,3}\sum_{h_2=0}^{N-1} G_{q^6}(\chi_4^{h_1}\chi_N^{h_2})\left(\sum_{j\in\{0,3\}}\sum_{s\in S_1}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a+q^2s}) + \sum_{j\in\{1,2\}}\sum_{s\in S_2}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a+q^2s})\right)\\
&= \frac{1}{4N}\sum_{h_1=0,1,2,3}\sum_{h_2=0}^{N-1} G_{q^6}(\chi_4^{h_1}\chi_N^{h_2})\left(\sum_{j\in\{0,3\}}\sum_{s\in S_1}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a+s}) + \sum_{j\in\{1,2\}}\sum_{s\in S_2}\chi_4^{-h_1}(\gamma^{a+Nj})\chi_N^{-h_2}(\gamma^{a+s})\right).
\end{aligned} \tag{4.3}$$

We compute the right hand side of Eq. (4.3) by dividing it into the three partial sums: P_1, P_2 and P_3, where P_1 is the contribution of the summands with $h_1=0$, P_2 is the contribution of the summands with $h_1=2$, and P_3 is the contribution of the summands with $h_1=1$ or 3. That is, we have

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D) = P_1 + P_2 + P_3. \tag{4.4}$$

It is clear that $P_2=0$ since

$$\sum_{j\in\{0,3\}}\chi_4^{-2}(\gamma^{a+Nj}) = \sum_{j\in\{1,2\}}\chi_4^{-2}(\gamma^{a+Nj}) = 0.$$

We consider the partial sum P_1.

Lemma 4.3. *It holds that*

$$P_1 = \begin{cases} \frac{-q^3+q^2-1}{2}, & \text{if } a \in S \pmod N, \\ \frac{q^2-1}{2}, & \text{if } a \notin S \pmod N. \end{cases}$$

Proof. We compute

$$P_1 = \frac{1}{2N} \sum_{h_2=0}^{N-1} G_{q^6}(\chi_N^{h_2}) \sum_{s \in S} \chi_N^{-h_2}(\gamma^{a+s}). \tag{4.5}$$

Let χ'_N be the multiplicative character of order N of $\mathbb{F}_{q^3}$ such that χ_N is the lift of χ'_N. Since

$$G_{q^3}(\chi'^{-h_2}_N) = q \sum_{s \in S} \chi'^{-h_2}_N(\omega^s) = q \sum_{s \in S} \chi_N^{-h_2}(\gamma^s)$$

and

$$G_{q^6}(\chi_N^{h_2}) = -G_{q^3}(\chi'^{h_2}_N)^2$$

by Theorems 2.3 and 2.5, respectively, continuing from (4.5), we have

$$\begin{aligned} P_1 + \frac{q+1}{2N} &= -\frac{1}{2Nq} \sum_{h_2=1}^{N-1} G_{q^3}(\chi'^{h_2}_N)^2 G_{q^3}(\chi'^{-h_2}_N) \chi'^{-h_2}_N(\omega^a) \\ &= -\frac{q^2}{2N} \sum_{h_2=1}^{N-1} G_{q^3}(\chi'^{h_2}_N) \chi'^{-h_2}_N(\omega^a) \\ &= -\frac{q^3}{2N} \sum_{h_2=0}^{N-1} \sum_{s \in S} \chi'^{-h_2}_N(\omega^{-s+a}) + \frac{q^3(q+1)}{2N} \\ &= \begin{cases} \frac{q^3(q+1)}{2N} - \frac{q^3}{2}, & \text{if } a \in S \pmod N, \\ \frac{q^3(q+1)}{2N}, & \text{if } a \notin S \pmod N. \end{cases} \end{aligned}$$

The conclusion of the lemma now follows. ∎

Next, we evaluate the partial sum P_3. Recall that $S'_i \equiv 2^{-1} S_i \pmod N$, $S''_i \equiv 2^{-1} S'_i \pmod N$, $i = 1, 2$, and

$$X = 2S''_1 \cup (2S''_2 + N) \pmod{2N}.$$

Lemma 4.4. *Let* $b \equiv 4^{-1}a \pmod N$ *and* $c \equiv 2b \pmod{2N}$. *Then, it holds that*

(4.6)
$$P_3 = \frac{\rho_q \delta_a q^3}{G_{q^3}(\chi'_2)} \psi_{\mathbb{F}_{q^3}} \left(\omega^c \bigcup_{t \in X} C_t^{(2N,q^3)} \right) - \frac{\rho_q \delta_a q^3}{2G_{q^3}(\chi'_2)} \psi_{\mathbb{F}_{q^3}} \left(\omega^c \bigcup_{t \in I_{\mathcal{Q}}} C_t^{(N,q^3)} \right).$$

where $\psi_{\mathbb{F}_{q^3}}$ *is the canonical additive character of* $\mathbb{F}_{q^3}$ *and* $\delta_a = 1$ *or* -1 *depending on whether* $a \equiv 0,1 \pmod 4$ *or* $a \equiv 2,3 \pmod 4$.

Proof. We have

$$\begin{aligned} P_3 = \frac{1}{4N} \sum_{h_2=0}^{N-1} G_{q^6}(\chi_4 \chi_N^{h_2}) \Bigg(& \sum_{j \in \{0,3\}} \sum_{s \in S_1} \chi_4^{-1}(\gamma^{a+Nj}) \chi_N^{-h_2}(\gamma^{a+s}) \\ & + \sum_{j \in \{1,2\}} \sum_{s \in S_2} \chi_4^{-1}(\gamma^{a+Nj}) \chi_N^{-h_2}(\gamma^{a+s}) \Bigg) \\ + \frac{1}{4N} \sum_{h_2=0}^{N-1} G_{q^6}(\chi_4^3 \chi_N^{h_2}) \Bigg(& \sum_{j \in \{0,3\}} \sum_{s \in S_1} \chi_4(\gamma^{a+Nj}) \chi_N^{-h_2}(\gamma^{a+s}) \\ & + \sum_{j \in \{1,2\}} \sum_{s \in S_2} \chi_4(\gamma^{a+Nj}) \chi_N^{-h_2}(\gamma^{a+s}) \Bigg). \end{aligned}$$

Noting that $G_{q^6}(\chi_4 \chi_N^{h_2}) = G_{q^6}(\chi_4^3 \chi_N^{h_2})$ by Theorem 2.7, we have

$$\begin{aligned} P_3 = \frac{\delta_a}{2N} \sum_{h_2=1}^{N-1} G_{q^6}(\chi_4 \chi_N^{h_2}) \left(\sum_{s \in S_1} \chi_N^{-h_2}(\gamma^{a+s}) - \sum_{s \in S_2} \chi_N^{-h_2}(\gamma^{a+s}) \right) \\ + \frac{\delta_a}{2N} G_{q^6}(\chi_4)(|S_1| - |S_2|), \end{aligned} \tag{4.7}$$

where $\delta_a = 1$ or -1 depending on whether $a \equiv 0,1 \pmod 4$ or $a \equiv 2,3 \pmod 4$. Note that $G_{q^6}(\chi_4) = \rho_q q^3$ by Theorem 2.4. We now compute the former

summand of (4.7). Applying Theorem 2.7, we have

(4.8)
$$\begin{aligned}
&\sum_{h_2=1}^{N-1} G_{q^6}(\chi_4\chi_N^{h_2})\left(\sum_{s\in S_1}\chi_N^{-h_2}(\gamma^{a+s})-\sum_{s\in S_2}\chi_N^{-h_2}(\gamma^{a+s})\right)\\
&=\frac{\rho_q q^3}{G_{q^3}(\chi_2')}\sum_{h_2=1}^{N-1} G_{q^3}(\chi_2'\chi_N'^{2h_2})\left(\sum_{s\in S_1}\chi_N'^{-h_2}(\omega^{a+s})-\sum_{s\in S_2}\chi_N'^{-h_2}(\omega^{a+s})\right)\\
&=\frac{\rho_q q^3}{G_{q^3}(\chi_2')}\sum_{h_2=1}^{N-1} G_{q^3}(\chi_2'\chi_N'^{2h_2})\chi_N'^{-2h_2}(\omega^{2b})\left(\sum_{s\in S_1'}\chi_N'^{-2h_2}(\omega^{s})-\sum_{s\in S_2'}\chi_N'^{-2h_2}(\omega^{s})\right)\\
&=\frac{\rho_q q^3}{G_{q^3}(\chi'_2)}\sum_{h_2=1}^{N-1} G_{q^3}(\chi_2'\chi_N'^{2h_2})\sum_{t\in X}\chi_2'\chi_N'^{-2h_2}(\omega^{t+c}).
\end{aligned}$$

Put the value of (4.8) as T. Let $\chi'_{2N}:=\chi_2'\chi_N'$, which is a multiplicative character of order $2N$ of $\mathbb{F}_{q^3}$. Then, we have

(4.9)
$$\begin{aligned}
T&=\frac{\rho_q q^3}{G_{q^3}(\chi'_2)}\sum_{h:\ \text{odd};h\neq N} G_{q^3}(\chi_{2N}'^{h})\sum_{t\in X}\chi_{2N}'^{-h}(\omega^{t+c})\\
&=\frac{\rho_q q^3}{G_{q^3}(\chi'_2)}\sum_{h=0}^{2N-1} G_{q^3}(\chi_{2N}'^{h})\sum_{t\in X}\chi_{2N}'^{-h}(\omega^{t+c})\\
&\quad-\frac{\rho_q q^3}{G_{q^3}(\chi'_2)}\sum_{h=0}^{N-1} G_{q^3}(\chi_{2N}'^{2h})\sum_{t\in X}\chi_{2N}'^{-2h}(\omega^{t+c})\\
&\quad-\frac{\rho_q q^3}{G_{q^3}(\chi'_2)}G_{q^3}(\chi_{2N}'^{N})\sum_{t\in X}\chi_{2N}'^{-N}(\omega^{t+c}).
\end{aligned}$$

By the orthogonality of characters, we have

$$\sum_{h=0}^{2N-1} G_{q^3}(\chi_{2N}'^{h})\sum_{t\in X}\chi_{2N}'^{-h}(\omega^{t+c})=2N\psi_{\mathbb{F}_{q^3}}\left(\omega^c\bigcup_{t\in X}C_t^{(2N,q^3)}\right).$$

Furthermore, noting that $X\equiv I_{\mathcal{Q}}\pmod N$, we have

$$\sum_{h=0}^{N-1} G_{q^3}(\chi_{2N}'^{2h})\sum_{t\in X}\chi_{2N}'^{-2h}(\omega^{t+c})=N\psi_{\mathbb{F}_{q^3}}\left(\omega^c\bigcup_{t\in I_{\mathcal{Q}}}C_t^{(N,q^3)}\right).$$

Finally, the last term of (4.9) is computed as

$$-\rho_q q^3(|S_1|-|S_2|).$$

Summing up, we have (4.6) of this lemma. ∎

We are now ready to prove our main theorem.

Proof of Theorem 4.2. Recall that $\psi_{\mathbb{F}_{q^6}}(\gamma^a D)=P_1+P_2+P_3$ as in (4.4), where $P_2=0$, and P_1 and P_3 are computed in Lemmas 4.3 and 4.4, respectively. By (3.5) and Theorem 3.4, we have

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D)=\begin{cases}\frac{-q^3+q^2-1}{2}, & \text{if } a \pmod N \in S,\\ \frac{q^2-1}{2}, & \text{if } a \pmod N \notin S,\end{cases}$$

$$+\frac{\rho_q\delta_a q^3}{G_{q^3}(\chi'_2)}\psi_{\mathbb{F}_{q^3}}\left(\omega^c\bigcup_{t\in X}C_t^{(2N,q^3)}\right)-\frac{\rho_q\delta_a q^3}{2G_{q^3}(\chi'_2)}\psi_{\mathbb{F}_{q^3}}\left(\omega^c\bigcup_{t\in I_{\mathcal{Q}}}C_t^{(N,q^3)}\right)$$

$$=\begin{cases}\frac{-q^3+q^2-1}{2}, & \text{if } a \pmod N \in S,\\ \frac{q^2-1}{2}, & \text{if } a \pmod N \notin S,\end{cases}$$

$$+\frac{\rho_q\delta_a q^3}{G_{q^3}(\chi'_2)}\cdot\begin{cases}\frac{-1+\eta(2)qG_q(\eta)}{2}, & \text{if } c \pmod N \in I_{\mathcal{Q}} \text{ and } c \pmod{2N} \in X,\\ \frac{-1-\eta(2)qG_q(\eta)}{2}, & \text{if } c \pmod N \in I_{\mathcal{Q}} \text{ and } c \pmod{2N} \in X+N,\\ -\frac{q+1}{2}, & \text{if } c \pmod N \in I_s,\\ \frac{q-1}{2}, & \text{if } c \pmod N \in I_n,\end{cases}$$

$$-\frac{\rho_q\delta_a q^3}{2G_{q^3}(\chi'_2)}\cdot\begin{cases}-1, & \text{if } c \pmod N \in I_{\mathcal{Q}},\\ -q-1, & \text{if } c \pmod N \in I_s,\\ q-1, & \text{if } c \pmod N \in I_n.\end{cases}$$

We remark the following facts:

$$\begin{aligned} c \pmod N \in I_{\mathcal{Q}} &\Leftrightarrow a \pmod N \in S,\\ c \pmod{2N} \in X &\Leftrightarrow a \pmod N \in S_1,\\ c \pmod{2N} \in X+N &\Leftrightarrow a \pmod N \in S_2.\end{aligned}$$

Then, we have

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D)=\begin{cases}\frac{-q^3+q^2-1}{2}+\frac{\rho_q\delta_a\eta(2)q^4G_q(\eta)}{2G_{q^3}(\chi'_2)}, & \text{if } a \pmod N \in S_1,\\ \frac{-q^3+q^2-1}{2}-\frac{\rho_q\delta_a\eta(2)q^4G_q(\eta)}{2G_{q^3}(\chi'_2)}, & \text{if } a \pmod N \in S_2,\\ \frac{q^2-1}{2}, & \text{if } a \pmod N \notin S.\end{cases}$$

Note that $\eta(2)=-1$ or 1 depending on $q\equiv 3 \pmod 8$ or $q\equiv 7 \pmod 8$. Furthermore, by $G_{q^3}(\chi_2')^2=-q^3$ and $G_{q^3}(\chi_2')=G_q(\eta)^3$, we have

$$\frac{\rho_q\eta(2)q^4G_q(\eta)}{G_{q^3}(\chi_2')} = -qG_q(\eta)G_{q^3}(\chi_2') = -qG_q(\eta)^4 = -q^3.$$

Hence,

$$\psi_{\mathbb{F}_{q^6}}(\gamma^a D) = \begin{cases} -q^3+\frac{q^2-1}{2}, & \text{if } a \pmod N \in S_1 \text{ and } a\equiv 0,1 \pmod 4, \text{ or} \\ & a \pmod N \in S_2 \text{ and } a\equiv 2,3 \pmod 4, \\ \frac{q^2-1}{2}, & \text{if } a \pmod N \notin S,\ a \pmod N \in S_1 \text{ and} \\ & a\equiv 2,3 \pmod 4, \\ & \text{or } a \pmod N \in S_2 \text{ and } a\equiv 0,1 \pmod 4. \end{cases}$$

Thus, D takes exactly two nontrivial character values, i.e., the Cayley graph $\mathrm{Cay}(\mathbb{F}_{q^6},D)$ is strongly regular.

Finally, we show that $\psi_{\mathbb{F}_{q^6}}(\gamma^a D)=-q^3+\frac{q^2-1}{2}$ if and only if $\gamma^{aq^3}\in D$. To do this, we determine the dual of D explicitly. Let $K_1:=\{0,1\}$ and $K_2:=\{2,3\}$. Define

$$J := \{Ni-(q+1)j \pmod{4N} \colon (i,j)\in (K_1\times S_1)\cup(K_2\times S_2)\}$$

and $E := \bigcup_{i\in J} C_i^{(4N,q^6)}$. Then, E is obviously the dual of D. Hence, $\psi_{\mathbb{F}_{q^6}}(\gamma^a D) = -q^3+\frac{q^2-1}{2}$ if and only if $\gamma^a\in E$. Since $q^3I\equiv J \pmod{4N}$, we obtain the assertion. The proof of the theorem is now complete. ∎

5. On groups and equivalence with known examples

From our construction, it is not difficult to identify a subgroup of the stabilizer of a hemisystem arising from Construction 4.1.

Theorem 5.1. *Let q be a prime power congruent to 3 modulo 4. Then the hemisystem $\mathcal{M}$ of $\mathcal{Q}^-(5,q)$ arising from Construction 4.1 is stabilized by a subgroup of $\mathsf{P\Gamma O}^-(6,q)$ isomorphic to the metacyclic group $C_{(q^3+1)/4}:C_3$. Moreover:*

(i) The normal cyclic subgroup of order $C_{(q^3+1)/4}$ is induced by right multiplication by $\gamma^{4(q^2+q+1)}$, where γ is a primitive element of $\mathbb{F}_{q^6}$.

(ii) The complementary element of order 3 on top arises from the map $x\mapsto x^{q^2}$.

The known infinite families of examples are

- The Cossidente-Penttila examples, with each example stabilized by $\mathsf{P\Sigma L}(2,q^2)$;
- The BGR-hemisystems arising from the Bamberg-Giudici-Royle (BGR) construction from [1].

The order of $\mathsf{P\Sigma L}(2,q^2)$ is $q^2(q^4-1)\log_p(q)$. So in particular, it is not divisible by q^2-q+1. The generic BGR construction yields many hemisystems, including the Cossidente-Penttila ones. Those that are not of Cossidente-Penttila type have a normal subgroup of order q^2.

Theorem 5.2 ([2, Theorem 3.3]). *Let $\mathcal{H}$ be a BGR-hemisystem of $\mathsf{H}(3,q^2)$. Then the full stabilizer of $\mathcal{H}$ contains $T \rtimes K$, where T is an elementary abelian group of order q^2 and K is a subgroup of $\mathsf{Sp}(4,q)$.*

For many reasons, the exceptional case is $q=3$. Here the stabilizer of the Segre hemisystem is $\mathsf{PSL}(3,4).2$ in its exceptional embedding in $\mathsf{P\Gamma U}(4,3)$. The order of $\mathsf{PSL}(3,4)$ is $20160 = 3^2\cdot(3^2-3+1)\cdot 320$, and it will turn out to be the only occasion when a subgroup M of $\mathsf{PGU}(4,q)$ has order divisible by $q^2(q^2-q+1)$, apart from subgroups containing $\mathsf{SU}(3,q)$. It is not difficult to see that no hemisystems admit $\mathsf{SU}(3,q)$, since this group acts transitively on totally isotropic lines of $\mathsf{H}(3,q^2)$.

The following lemma follows directly from [4, Theorem 4.2].

Lemma 5.3. *Let q be an odd prime power with $q\geqslant 5$. Let M be a maximal subgroup of $\mathsf{PGU}(4,q)$ with order divisible by q^2-q+1. Then M is the stabilizer of a non-degenerate hyperplane and is isomorphic to $\mathsf{GU}(3,q)$.*

Now the order of $\mathsf{GU}(3,q)$ is $q^3(q+1)^2(q^2-1)(q^2-q+1)$. By [4, Theorem 4.1], we have the following:

Lemma 5.4. *Let q be an odd prime power with $q\geqslant 5$. Let M be a maximal subgroup of $\mathsf{GU}(3,q)$ with order divisible by q^2-q+1. Then one of the following occurs:*

(i) $\mathsf{SU}(3,q)\trianglelefteq M$;
(ii) $q=5$ *and* $M\cong 6.S_7$;
(iii) $M\cong\mathsf{\Gamma U}(1,q^3)$.

So if M is a maximal subgroup of $\mathsf{PGU}(4,q)$, q odd and $q\geqslant 5$, with order divisible by $q^2(q^2-q+1)$, then M contains $\mathsf{SU}(3,q)$. Therefore, the m-ovoids we have constructed in this paper are not of BGR type for $q\geqslant 5$.

6. Open problems

In the introduction, we mentioned that there are examples of hemisystems of $\mathsf{H}(3,q^2)$ admitting a cyclic group of order q^2-q+1 for most of the small values of q. In [2, Section 4.1], the computational data, including the orders of the stabilisers of the examples, was presented and which we repeat below:

q	q^2-q+1	Stabiliser
3	7	PSL(3,4).2
5	21	$3\cdot A_7\cdot 2$
7	43	43:6
9	73	73:6
11	111	111:6, 333:3
17	273	273:3
19	343	1715:6
23	507	507:6
27	703	703:3

Notice that there were no examples for $q=13$, nor for $q=25$, and so one might believe that there are no examples for $q\equiv 1 \pmod{12}$. In this paper, we have given a construction for each q congruent to 3 (mod 4), and so an open problem remains whether a similar construction can work for $q\equiv 5,9 \pmod{12}$, say. We have attempted to adapt our methods for q congruent to 1 (mod 4), but to no avail. The essential problem is the computation of Gauss sums. In the case where $q\equiv 3 \pmod 4$, our hemisystem admits $C_{(q^3+1)/4}$, and it was enough to consider Gauss sums of order $4(q^2+q+1)$. But, known examples of hemisystems for $q\equiv 1 \pmod 4$ seem to admit the smaller cyclic group C_{q^2-q+1} instead. Thus, relative to the 3 modulo 4 case, we need to compute Gauss sums of larger order. We could not find an effective way to compute the character values, and furthermore, we do not know what kind of structure is behind the examples. The authors believe a more enlightening distinction could be made in this case: the examples could be further divided according to q modulo 3. It seems the $q\equiv 0 \pmod 3$ examples take on a different nature, and in particular, the field automorphisms fix a unique orbit of C_{q^2-q+1}. Hence, we give the following refinement of the open problem given in [2, Section 4.1]:

Problem 6.1. *Does there exist a hemisystem invariant under a cyclic group of order q^2-q+1 for each odd prime power q satisfying $q\equiv 1 \pmod 4$ and $q\equiv 0,2 \pmod 3$?*

References

[1] J. Bamberg, M. Giudici and G. F. Royle: Every flock generalized quadrangle has a hemisystem, *Bull. Lond. Math. Soc.* **42** (2010), 795–810.

[2] J. Bamberg, M. Giudici and G. F. Royle: Hemisystems of small flock generalized quadrangles, *Des. Codes Cryptogr.* **67** (2013), 137–157.

[3] J. Bamberg, S. Kelly, M. Law and T. Penttila: Tight sets and m-ovoids of finite polar spaces, *J. Combin. Theory Ser. A* **114** (2007), 1293–1314.

[4] J. Bamberg and T. Penttila: Overgroups of cyclic Sylow subgroups of linear groups, *Comm. Algebra* **36** (2008), 2503–2543.

[5] E. Bannai, O. Shimabukuro and H. Tanaka: Finite Euclidean graphs and Ramanujan graphs, *Discrete Mathematics* **309** (2009), 6126–6134.

[6] B. C. Berndt, R. J. Evans and K. S. Williams: *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication.

[7] A. A. Bruen and J. W. P. Hirschfeld: Applications of line geometry over finite fields. II. The Hermitian surface, *Geom. Dedicata* **7** (1978), 333–353.

[8] A. Cossidente and T. Penttila: Hemisystems on the Hermitian surface, *J. London Math. Soc.* **72** (2005), 731–741.

[9] J. De Beule, J. Demeyer, K. Metsch and M. Rodgers: A new family of tight sets in $\mathcal{Q}^+(5,q)$, *Des. Codes Cryptogr.* **78** (2016), 655–678.

[10] T. Feng, K. Momihara and Q. Xiang: Cameron-Liebler line classes with parameter $x=\frac{q^2-1}{2}$, *J. Combin. Theory Ser. A* **133** (2015), 307–338.

[11] J. W. P. Hirschfeld: *Projective geometries over finite fields*, The Clarendon Press, Oxford University Press, New York, 1979, Oxford Mathematical Monographs.

[12] B. Segre: Forme e geometrie hermitiane, con particolare riguardo al caso finito, *Ann. Mat. Pura Appl.* **70** (1965), 1–201.

[13] J. A. Thas: Projective geometry over a finite field, in: *Handbook of incidence geometry*, 295–347, North-Holland, Amsterdam, 1995.

[14] E. R. van Dam, W. J. Martin and M. Muzychuk: Uniformity in association schemes and coherent configurations: cometric Q-antipodal schemes and linked systems, *J. Combin. Theory Ser. A* **120** (2013), 1401–1439.

[15] K. Yamamoto and M. Yamada: Williamson Hadamard matrices and Gauss sums, *J. Math. Soc. Japan* **37** (1985), 703–717.

John Bamberg, Melissa Lee

Centre for the Mathematics of Symmetry and Computation
School of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway, Crawley
W.A. 6009, Australia
John.Bamberg@uwa.edu.au,melissa.lee@research.uwa.edu.au

Koji Momihara

Department of Mathematics
Faculty of Education
Kumamoto University
2-40-1 Kurokami
Kumamoto 860-8555, Japan
momihara@educ.kumamoto-u.ac.jp

Qing Xiang

Department of Mathematical Sciences
University of Delaware
Newark DE 19716, USA
xiang@math.udel.edu