Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 14 (2008) 76–84
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On m-ovoids of $\mathcal{W}_3(q)$

A. Cossidente [a], C. Culbert [b], G.L. Ebert [c,*,1], G. Marino [d]

[a] *Dipartimento di Matematica, Università degli Studi della Basilicata, 85100 Potenza, Italy*
[b] *Department of Mathematics, Anne Arundel Community College, Arnold, MD 21002, USA*
[c] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*
[d] *Dipartimento di Matematica e Appl., Università di Napoli "Federico II", 80126 Napoli, Italy*

Received 14 March 2006
Available online 26 May 2006
Communicated by Gary L. Mullen

Abstract

We show that the generalized quadrangle $\mathcal{W}_3(q)$ for odd q has exponentially many $\frac{1}{2}(q+1)$-ovoids, thus implying that the generalized quadrangle $\mathcal{Q}(4,q)$ has exponentially many hemisystems for odd q. For q even, we show that $\mathcal{W}_3(q)$ has m-ovoids for all integers m, $1 \leqslant m \leqslant q$. Stabilizers are determined, and some computer results are given.

Keywords: Symplectic generalized quadrangle; Singer cycle; m-Ovoid

1. Introduction

Let $\mathcal{S} = (P, B, I)$ be a generalized quadrangle of order (s,t). An *m-ovoid* $\mathcal{O}$ of $\mathcal{S}$ is a subset of P such that each line in B contains exactly m points of $\mathcal{O}$. Of course, if $\mathcal{O}$ is an m-ovoid of $\mathcal{S}$, then its complement in P is an $(s+1-m)$-ovoid of $\mathcal{S}$. A 1-ovoid of $\mathcal{S}$ is called an *ovoid* of $\mathcal{S}$. For details and results on ovoids, see [11,15]. If $m = (t+1)/2$, then the dual of an m-ovoid is also called a *hemisystem* of the dual of $\mathcal{S}$. It is easily seen that if $\mathcal{O}$ is an m-ovoid of $\mathcal{S}$ then $|\mathcal{O}| = m(st+1)$ (see [14, Lemma 1]). Moreover, m-ovoids of generalized quadrangles are very important objects because of their connection with strongly regular graphs (see [6,13,14]).

* Corresponding author.
E-mail addresses: cossidente@unibas.it (A. Cossidente), cwculbert@aacc.edu (C. Culbert), ebert@math.udel.edu (G.L. Ebert), giuseppe.marino@unina2.it (G. Marino).
[1] Author gratefully acknowledges the support of NSA grant MDA 904-03-1-0099.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.04.001

The notion of hemisystem first appeared in the celebrated paper [12] of B. Segre completely devoted to the geometry of Hermitian varieties. Segre was interested in hemisystems of the Hermitian surface, which is a generalized quadrangle of order (q^2, q). In particular, he constructed a hemisystem of $\mathcal{H}(3, 9)$. In [8], Cossidente and Penttila found an infinite family of hemisystems of $\mathcal{H}(3, q^2)$, q odd, invariant under the orthogonal group $P\Omega^-(4, q)$, which includes Segre's example.

In this paper we are interested in m-ovoids of the symplectic generalized quadrangle $\mathcal{W}_3(q)$, which has order (q, q). It is well known (see [11]) that $\mathcal{W}_3(q)$, q odd, has no ovoids, which makes it interesting in this case to look for m-ovoids, with $m > 1$. Since $\mathcal{W}_3(q)$ is isomorphic to the dual of $\mathcal{Q}(4, q)$, a $\frac{1}{2}(q + 1)$-ovoid of $\mathcal{W}_3(q)$ for odd q corresponds to a hemisystem of $\mathcal{Q}(4, q)$.

Here we construct several infinite families of $\frac{1}{2}(q + 1)$-ovoids of $\mathcal{W}_3(q)$ (hence infinite families of hemisystems of $\mathcal{Q}(4, q)$) based on the existence of certain line-spreads of $PG(3, q)$, q odd. Some computational results for small q are also provided. In addition, we show that for q even, m-ovoids of $\mathcal{W}_3(q)$ admitting the semidirect product of a cyclic group of order $q^2 + 1$ by a cyclic group of order 4 exist for all integers m, $1 \leqslant m \leqslant q$.

2. $\frac{1}{2}(q + 1)$-Ovoids of $\mathcal{W}_3(q)$, q odd

Let δ denote a polarity of $\Sigma = PG(3, q)$, where q is an odd prime power. A spread $\mathcal{S}$ of Σ will be called *polarity-paired* with respect to δ provided $\mathcal{S}$ consists of $\frac{1}{2}(q^2 + 1)$ δ-conjugate skew pairs of lines. That is, $\mathcal{S}$ is left invariant by δ, but δ fixes no line of $\mathcal{S}$ and hence $\mathcal{S}$ contains no totally isotropic lines. In this paper we will be concerned with the case when δ is symplectic, although the general situation is certainly of interest. For instance, we have found a polarity pairing for 15 of the 21 projectively inequivalent spreads of $PG(3, 5)$, although only one of the pairings arises from a symplectic polarity.

In this section $\mathcal{W}_3(q)$ will denote the generalized quadrangle consisting of all points of Σ and the totally isotropic lines of some symplectic polarity δ. If A is any subspace of Σ, we will often denote A^δ by $A^\perp$.

Theorem 2.1. *A polarity-paired spread $\mathcal{S}$ of Σ with respect to a symplectic polarity δ gives rise to $2^{(q^2+1)/2}$ $\frac{1}{2}(q + 1)$-ovoids of $\mathcal{W}_3(q)$ (hemisystems of $\mathcal{Q}(4, q)$).*

Proof. Since $\mathcal{S}$ is polarity-paired, we can express $\mathcal{S}$ as a union of $\frac{1}{2}(q^2 + 1)$ conjugate skew pairs of lines. Let $\mathcal{H}$ be a subset of $\mathcal{S}$ of size $\frac{1}{2}(q^2 + 1)$ obtained by selecting one line from each of these conjugate skew pairs, and let $\mathcal{O}$ denote the set of points covered by the lines in $\mathcal{H}$. Thus there are $2^{(q^2+1)/2}$ ways of constructing $\mathcal{O}$. Let $\mathcal{W}_3(q)$ denote the generalized quadrangle associated with the symplectic polarity δ. We claim that $\mathcal{O}$ is a $\frac{1}{2}(q + 1)$-ovoid of $\mathcal{W}_3(q)$.

Let r be any totally isotropic line of δ. Then r is not in the spread $\mathcal{S}$, and hence meets $q + 1$ lines of $\mathcal{S}$ in one point each. But if r meets the spread line ℓ, then r necessarily meets $\ell^\perp$ as well. Since $\{\ell, \ell^\perp\}$ is one of the conjugate skew pairs comprising $\mathcal{S}$, precisely one of these spread lines is in the subset $\mathcal{H}$. Thus r meets $\mathcal{O}$ in exactly $\frac{1}{2}(q + 1)$ points, proving the result. □

We now construct several infinite families of symplectically-paired spreads of Σ. We begin by looking at André spreads. Using left-normalized homogeneous coordinates for Σ, let $\ell_{(x,y)} = \langle (1, 0, x, y), (0, 1, wy, x) \rangle$ for any $x, y \in GF(q)$, where w is some primitive element (hence

a nonsquare) in $GF(q)$. Let $\ell_\infty = \langle (0,0,0,1), (0,0,1,0)\rangle$. Then $\mathcal{S}_0 = \{\ell_\infty\} \cup \{\ell_{(x,y)}\colon\ x, y \in GF(q)\}$ is a regular spread of Σ. Moreover, $\mathcal{R}_t = \{\ell_{(x,y)}\colon\ x^2 - yw^2 = -t\}$ is a regulus contained in $\mathcal{S}_0$ for each $t \in GF(q)^* = GF(q) \setminus \{0\}$. In fact, $\{\mathcal{R}_t\colon\ t \in GF(q)^*\}$ is a linear set of $q-1$ mutually disjoint reguli in $\mathcal{S}_0$ with carriers $\ell_{(0,0)}$ and ℓ_∞ (see [5]). Straightforward computations show that $\mathcal{R}_t^{\text{opp}} = \{m_{(x,y)}\colon\ x^2 - wy^2 = -t\}$ is the opposite regulus to $\mathcal{R}_t$, where $m_{(x,y)} = \langle (1,0,x,y), (0,1,-wy,-x)\rangle$.

Now consider the symplectic polarity δ_k represented by the skew-symmetric matrix

$$A_k = \begin{pmatrix} 0 & k & 0 & 0 \\ -k & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \text{for some fixed } k \in GF(q)^*.$$

Straightforward computations show that for this symplectic polarity,

$$\ell_{(0,0)}^{\perp} = \ell_\infty \quad \text{and} \quad \ell_{(x,y)}^{\perp} = \ell_{(-kx/(x^2-wy^2),-ky/(x^2-wy^2))} \quad \text{for any } (x,y) \neq (0,0).$$

Thus δ_k leaves invariant the regular spread $\mathcal{S}_0$, maps the regulus $\mathcal{R}_t$ to the regulus $\mathcal{R}_{k^2/t}$, and thus leaves invariant the regulus $\mathcal{R}_t$ if and only if $t = k$ or $t = -k$. More precisely, the regulus $\mathcal{R}_k$ is fixed linewise, while the $q+1$ lines of the regulus $\mathcal{R}_{-k}$ are paired off by δ_k (no lines of $\mathcal{R}_{-k}$ are fixed). The remaining $q-3$ reguli $\mathcal{R}_t$ in the above linear set are paired off by δ_k. As

$$m_{(x,y)}^{\perp} = m_{(kx/(x^2-wy^2),ky/(x^2-wy^2))},$$

we see that δ_k maps the regulus $\mathcal{R}_t^{\text{opp}}$ to the regulus $\mathcal{R}_{k^2/t}^{\text{opp}}$. Thus $\mathcal{R}_k^{\text{opp}}$ and $\mathcal{R}_{-k}^{\text{opp}}$ are left invariant, but this time $\mathcal{R}_{-k}^{\text{opp}}$ is fixed linewise while all lines of $\mathcal{R}_k^{\text{opp}}$ are paired off.

Recall that an André spread of Σ is obtained by reversing a linear set of j mutually disjoint reguli in a regular spread, where *reversing* a regulus means replacing the lines of the regulus by the lines of its opposite regulus, and a set of reguli in a regular spread is called *linear* if the associated hyperbolic quadrics have a common conjugate pair of skew lines. Such an André spread is said to have *index* j. In general, not all André spreads of a given index j are projectively equivalent. A Hall spread of Σ is an André spread of index 1, and it is uniquely determined up to projective equivalence. Since reversing a linear set of $q-1$ disjoint reguli in a regular spread yields another regular spread, without loss of generality one only studies André spreads of index j for $1 \leqslant j \leqslant \frac{1}{2}(q-1)$.

Theorem 2.2. *For every odd index j, with $1 \leqslant j \leqslant \frac{1}{2}(q-1)$, there is an André spread of index j which is symplectically-paired.*

Proof. Using the above notation, consider the symplectic polarity δ_k for some fixed $k \in GF(q)^*$. Construct an André spread $\mathcal{S}$ by starting with the above regular spread $\mathcal{S}_0$ and reversing the regulus $\mathcal{R}_k$ and also reversing each regulus in a collection of $(j-1)/2$ pairs of reguli $\{\mathcal{R}_t, \mathcal{R}_{k^2/t}\}$, where $t \neq \pm k$. The action of δ_k described above implies that the André spread $\mathcal{S}$ of index j will indeed be left invariant by δ_k with no fixed lines. That is, $\mathcal{S}$ will be symplectically-paired. □

Corollary 2.3. *The Hall spread is symplectically-paired.*

Corollary 2.4. *If $q \equiv 3 \pmod 4$, then the regular nearfield spread of Σ is symplectically-paired.*

Proof. The regular nearfield spread of Σ is obtained by reversing a linear subset of $(q-1)/2$ reguli $\mathcal{R}_t$ in a regular spread $\mathcal{S}_0$, where the subscripts t are all the nonsquares (or, equivalently, all the nonzero squares) of $GF(q)$. Since $q \equiv 3 \pmod 4$, we have that $(q-1)/2$ is odd. If we choose k to be a nonsquare in $GF(q)$, then δ_k will pair the regulus $\mathcal{R}_t$, where t is a nonsquare, with the regulus $\mathcal{R}_{k^2/t}$, where k^2/t is also a nonsquare. Note that $-k$ will be a nonzero square since $q \equiv 3 \pmod 4$. Hence, using the technique described in the proof of Theorem 2.2, we see that the regular nearfield spread obtained by reversing all reguli $\mathcal{R}_t$ with t a nonsquare in $GF(q)$ is symplectically-paired by δ_k. □

We next consider spreads of Σ corresponding to non-Desarguesian flag-transitive affine planes of odd order q^2. We will describe such spreads in terms of the field model. That is, we view $GF(q^4)$ as a 4-dimensional vector space over its subfield $GF(q)$, and use this vector space to model Σ. The points of Σ are identified with the field elements $\beta^0, \beta^1, \beta^2, \ldots, \beta^{q^3+q^2+q}$, where β is a primitive element of $GF(q^4)$ and thus $w = \beta^{q^3+q^2+q+1}$ is a primitive element of the subfield $GF(q)$. Multiplication by β induces a Singer cycle on the points and planes of Σ, and we will let $[L]$ denote the orbit of the line L under the Singer subgroup of order $\frac{1}{2}(q^2+1)$ induced by multiplication by $\beta^{2(q+1)}$. Moreover, we let $\beta^d L^q$ denote the image of the line L under the collineation of Σ induced by the mapping $x \mapsto \beta^d x^q$ for some positive integer d. Finally, we let L_s denote the line $\langle \beta^0, \beta^{s(q+1)} \rangle$, for any integer s with $1 \leqslant s \leqslant q^2$.

As discussed in [4], for every odd integer s with $1 \leqslant s \leqslant q^2$ and $s \neq \frac{1}{2}(q^2+1)$, there is an odd integer d (which is unique modulo $q+1$) such that $[L_s] \cup [\beta^d L_s^q]$ is a non-regular spread of Σ admitting a transitive collineation group and hence corresponds to a non-Desarguesian flag-transitive affine plane of (odd) order q^2. In fact, the collineation ϕ induced by the map $x \mapsto \beta^d x^q$ joins the above two half-spreads and thus gives the transitive action on the resulting spread. Moreover, as shown in [3], for $q \equiv 3 \pmod 4$ there is a unique equivalence class of such spreads in which $L_s^q = \beta^t L_s$ for some positive integer t. Hence the resulting spread, called "special" in [3], looks like $\mathcal{S}_s = [L_s] \cup [\beta^{t+d} L_s]$ where s and d are odd integers. In fact, since $\phi^2(L_s) = \beta^d(\beta^d L_s^q)^q = \beta^d(\beta^{t+d} L_s)^q = \beta^{(t+d)(q+1)} L_s \in [L_s]$, necessarily $t+d$ is even and thus t must also be an odd integer.

To show that this "special" spread is symplectically-paired, we need some technical lemmas. In what follows, T will denote the trace from $GF(q^4)$ to $GF(q)$.

Lemma 2.5. *Using the above notation, there exists some integer j such that $z = \beta^{2j(q+1)+(t+d)} \in GF(q^2)^*$.*

Proof. Since β^{q^2+1} is a primitive element of $GF(q^2)$, we must find some integer j such that $2j(q+1) + (t+d) \equiv 0 \pmod{q^2+1}$. As shown above, $t+d$ is an even integer. Hence the above congruence may be rewritten as $j(q+1) \equiv -\frac{1}{2}(t+d) \pmod{\frac{1}{2}(q^2+1)}$. Since $\gcd(q+1, \frac{1}{2}(q^2+1)) = 1$, there is a solution for j, which is unique modulo $\frac{1}{2}(q^2+1)$. □

Lemma 2.6. *Using the above notation, let $\gamma = \beta^{s(q+1)}$ and let z denote the nonzero element of $GF(q^2)$ guaranteed to exist by Lemma 2.5. Then there exists some nonzero element $a \in GF(q^4)$ such that $T(az(\gamma - \gamma^{q^2})) = 0$.*

Proof. Let $g = \gamma - \gamma^{q^2}$. Since $s \neq \frac{1}{2}(q^2+1)$, we know $\gamma \notin GF(q^2)$ and thus $g \neq 0$. Choose any nonzero x in $GF(q^4)$ such that $T(x) = 0$. Then $a = x/(zg)$ satisfies the conditions stated in the lemma. □

Note that there are many choices for the element a in the above lemma. We now consider the alternating bilinear form defined on the vector space $GF(q^4)$ over its subfield $GF(q)$ given by $B(x, y) = T(a(x^{q^2}y - xy^{q^2}))$, where a is some nonzero element of $GF(q^4)$ satisfying the condition in Lemma 2.6. Then B induces a symplectic polarity δ_a on Σ. We wish to show that δ_a leaves the "special" spread $\mathcal{S}_s = [L_s] \cup [\beta^{t+d}L_s]$ invariant without fixing any of its lines. Using all the above notation, the lines of $[L_s]$ are $\langle \beta^{2i(q+1)}, \beta^{2i(q+1)}\gamma \rangle$ for $i = 0, 1, 2, \ldots, \frac{1}{2}(q^2-1)$, and the lines of $[\beta^{t+d}L_s]$ are $\langle z\beta^{2i(q+1)}, \gamma z\beta^{2i(q+1)} \rangle$ for $i = 0, 1, 2, \ldots, \frac{1}{2}(q^2-1)$.

Theorem 2.7. *The spread $\mathcal{S}_s$ is symplectically-paired by the polarity δ_a.*

Proof. Temporarily fix the integer i, where $i \in \{0, 1, 2, \ldots, \frac{1}{2}(q^2-1)\}$. To simplify the notation, we let $x = \beta^{2i(q+1)}$, and thus $x^{q^2+1} = w^{2i} \in GF(q)$. It follows from our above description of $\mathcal{S}_s$ that it suffices to show δ_a maps the line $\langle x, x\gamma \rangle$ to the line $\langle zx, \gamma zx \rangle$. To accomplish this we must show that $B(x, zx) = B(x, \gamma zx) = B(x\gamma, zx) = B(x\gamma, \gamma zx) = 0$. But these four computations follow immediately from Lemmas 2.5, 2.6, and the fact that $w^{2i} \in GF(q)$. □

Corollary 2.8. *For any prime power q with $q \equiv 3 \pmod 4$, there is a $\frac{1}{2}(q+1)$-ovoid of $\mathcal{W}_3(q)$ which admits a cyclic group of order q^2+1.*

Proof. Let $\mathcal{W}_3(q)$ be the incidence structure consisting of the points of Σ and the totally isotropic lines with respect to the symplectic polarity δ_a of Theorem 2.7, and let O_s denote the set of points covered by the lines in the half-spread $[L_s]$ of $\mathcal{S}_s$. The proof of Theorem 2.7, together with Theorem 2.1, show that O_s is indeed a $\frac{1}{2}(q+1)$-ovoid in $\mathcal{W}_3(q)$. Let $\mathcal{G}$ denote the subgroup of $PGL(4, q)$ leaving invariant the set of isotropic lines of δ_a. We view $\mathcal{G}$ as the automorphism group of $\mathcal{W}_3(q)$ (note that it is slightly larger than $PSp(4, q)$). Straightforward computations show that Singer cyclic subgroup G of order q^2+1 induced by multiplication by β^{q+1} is a subgroup of $\mathcal{G}$. Moreover, G leaves O_s invariant since O_s is a union of G-orbits, as described in [4]. □

It should be noted that the collineation in $\mathcal{G}$ induced by the map $x \mapsto x^{q^2}$ also leaves O_s invariant, and thus O_s has a stabilizer of order at least $2(q^2+1)$. For $q = 7, 11$ and 19 this subgroup of order $2(q^2+1)$ is the full stabilizer of O_s, as verified by Magma [7] computations. It seems likely that this is always the case for $q > 3$ and $q \equiv 3 \pmod 4$.

Using Theorems 2.2 and 2.7, we now have several infinite families of symplectically-paired spreads of Σ, each such spread yielding exponentially many $\frac{1}{2}(q+1)$-ovoids of $\mathcal{W}_3(q)$ by Theorem 2.1. For small values of q, we are able to sort out the projective equivalences among these ovoids, as we now do.

For $q = 3$, there is only one non-regular spread of Σ up to projective equivalence, namely the Hall spread. We know that this spread is symplectically-paired by Corollary 2.3 (or by Theorem 2.7, as it turns out). Taking such a symplectic polarity, one can construct 2^5 2-ovoids of $W_3(3)$ as indicated by Theorem 2.1. Magma [7] computations show that all such 2-ovoids are projectively equivalent under the group $\mathcal{G}$. The full stabilizer in $\mathcal{G}$ of such a 2-ovoid is isomorphic

to the symmetric group of degree 5. This stabilizer acts transitively on the points of the 2-ovoid and has two orbits on the lines of $W_3(3)$, one of size 10 (which is a regular spread of $W_3(3)$) and one of size 30. However, it should be noted that the Hall spread of $PG(3,3)$ is a sporadic example in that this spread admits a non-solvable group acting transitively on its lines, and hence the stabilizer of this 2-ovoid is undoubtedly atypical.

For $q=5$, the Hall spread of Σ yields 2^{13} 3-ovoids of $W_3(5)$ as above. Magma [7] computations show that under the group $\mathcal{G}$ one obtains 16 projectively distinct 3-ovoids; namely, one with a trivial stabilizer, four with a stabilizer of order 2, two with a stabilizer of order 3, five with a stabilizer of order 6, one with a stabilizer of order 9, one with a stabilizer of order 10, one with a stabilizer of order 18, and one with a stabilizer of order 30.

For $q=7$, Theorems 2.2 and 2.7 allow us to work with the Hall spread, the regular nearfield spread, a non-nearfield André spread of index 3, and the "special" transitive spread of Σ. These symplectically-paired spreads are mutually inequivalent, and each spread yields 2^{25} 4-ovoids of $W_3(7)$. There are two (complementary) 4-ovoids obtained from the "special" spread that have a stabilizer of order 100 (a semidirect product of a cyclic group of order 50 by a cyclic group of order 2) as in Corollary 2.8, but most of the other 4-ovoids have very small stabilizers. Starting with the Hall spread of $PG(3,7)$, extensive (but not exhaustive) searching with Magma [7] found 4-ovoids with stabilizers of orders $1, 2, 3, 4$ and 6. For the other symplectically-paired spreads of $PG(3,7)$, random searching found 4-ovoids with stabilizers only of size 1 or 2. It should also be noted that most of these 4-ovoids are mutually inequivalent under the group $\mathcal{G}$, independent of the starting spread. In random samples of size 100 for a given spread, typically 99 or all 100 were found to be mutually inequivalent.

3. m-Ovoids of $\mathcal{W}_3(q)$, q even

For q even it is well known that $\mathcal{W}_3(q)$ possesses ovoids. From [1], no two disjoint ovoids of $\mathcal{W}_3(q)$ exist and hence there is no hope of glueing together ovoids to form m-ovoids. Nonetheless, in [9] it is shown (dually) that 2-ovoids of $\mathcal{W}_3(q)$ exist for all even q. We now show the existence of m-ovoids in $\mathcal{W}_3(q)$, q even, for all integers m, with $1 \leqslant m \leqslant q$.

Again we use the field model for $PG(3,q)$, as described in Section 2. We also use the Singer subgroup G of order q^2+1 induced by multiplication by β^{q+1}. As described in [10], the G-orbits (on points) partition the points of $\Sigma = PG(3,q)$ into $q+1$ elliptic quadrics. Label these G-orbits as $\Omega_0, \Omega_1, \Omega_2, \ldots, \Omega_q$, where Ω_i denotes the points of Σ corresponding to the field elements $\beta^{s(q+1)+i}$ for $s = 0, 1, 2, \ldots, q^2$. Recall that two nonzero field elements from $GF(q^4)$ represent the same projective point if and only if they are $GF(q)$-scalar multiples of one another. As shown in [10], for even q, every line of Σ is either tangent to each of these G-orbits or else tangent to exactly one of them and hence secant to $q/2$ of them. There are precisely q^2+1 lines of Σ tangent to each of the G-orbits, and they form a regular spread $\mathcal{S}_0$ of Σ. In fact, in this setting, $\mathcal{S}_0$ is represented by $L, \beta L, \beta^2 L, \ldots, \beta^{q^2} L$, where $L = GF(q^2)$ is the unique subfield of order q^2. We begin with a technical lemma, where again trace will always mean the trace from $GF(q^4)$ to $GF(q)$, and this trace will be denoted by T.

Lemma 3.1. *Using the above notation with q even, the field elements which are powers of $\xi = \beta^{q+1}$ and have trace 0 are precisely the nonzero elements of the subfield $GF(q)$.*

Proof. Suppose $T(\xi^b) = 0$ for some integer b. Letting $y = \xi^b$, we have $y + y^q + y^{q^2} + y^{q^3} = 0$ and thus $y + y^{q^2} = (y + y^{q^2})^q$ since q is even. This implies that $y + y^{q^2} \in GF(q)$.

Now $y^{q^2} = \beta^{bq^2(q+1)} = w^b/y$, where $w = \beta^{(q+1)(q^2+1)}$ is a primitive element of $GF(q)$. Hence $y + w^b/y = (y^2 + w^b)/y \in GF(q)$ and y satisfies some monic quadratic polynomial with coefficients in $GF(q)$. Therefore $y = \xi^b = \beta^{b(q+1)} \in GF(q^2)$ and $(q^2+1) \mid b(q+1)$. As q is even, $\gcd(q+1, q^2+1) = 1$ and $(q^2+1) \mid b$. That is, $y = \xi^b \in GF(q)^*$. As every element of $GF(q)$ has trace 0 for q even, the result follows. □

We now show that the only tangent lines to Ω_0 which meet Ω_i and Ω_{q+1-i}, for some $i \in \{1, 2, 3, \ldots, q/2\}$, are the lines of the regular spread $\mathcal{S}_0$.

Lemma 3.2. *Consider the line $\ell = \langle \beta^{t(q+1)+q+1-i}, \beta^{s(q+1)+i} \rangle$ meeting the ovoid Ω_i and the ovoid Ω_{q+1-i} in at least one point each, for some $i \in \{1, 2, 3, \ldots, q/2\}$ and some $s, t \in \{0, 1, 2, \ldots, q^2\}$. Then ℓ is tangent to Ω_0 if and only if $\ell \in \mathcal{S}_0$.*

Proof. A point $\langle \beta^{t(q+1)+q+1-i} + a\beta^{s(q+1)+i} \rangle$ of ℓ, for some $a \in GF(q)^*$, lies in Ω_0 if and only if $(\beta^{t(q+1)+q+1-i} + a\beta^{s(q+1)+i})^{q^2+1} \in GF(q)$. Expanding, we obtain the equivalent condition that $w^{t+1}/\gamma^i + (\zeta + \zeta^{q^2})a + \gamma^i w^s a^2 \in GF(q)$, where $\gamma = \beta^{q^2+1}$ is a primitive element of $GF(q^2)$, $w = \beta^{(q+1)(q^2+1)}$ is a primitive element of $GF(q)$, and $\zeta = \beta^{((t+1)q^2 - i(q-1)+s)(q+1)}$. Using the fact that q is even, this condition is, in turn, equivalent to the equation

$$\left(\gamma^i + \gamma^{iq}\right) w^s a^2 + T(\zeta)a + w^{t+1}\left(\frac{1}{\gamma^i} + \frac{1}{\gamma^{iq}}\right) = 0.$$

Since $1 \leqslant i \leqslant q$, we know $\gamma^i \notin GF(q)$ and this is a quadratic equation in the "variable" a with coefficients in $GF(q)$ and nonzero constant term. Hence there is a unique solution for $a \in GF(q)^*$ if and only $T(\zeta) = 0$.

It follows from Lemma 3.1 that $T(\zeta) = 0$ if and only if $\zeta \in GF(q)$, which is equivalent to $(t+1)q^2 - i(q-1) + s \equiv 0 \pmod{q^2+1}$ or $(s+i) - (t+1) \equiv iq \pmod{q^2+1}$. On the other hand $\ell \in \mathcal{S}_0$ if and only if $\beta^{(t+1-s)(q+1)-2i} \in L = GF(q^2)$, which in turn is equivalent to

$$t - s + 1 \equiv 2i/(q+1) \equiv (1-q)i \pmod{q^2+1} \quad \text{for } q \text{ even.}$$

It is now easy to see that the above two congruences are equivalent, and hence the line ℓ is tangent to Ω_0 if and only if $\ell \in \mathcal{S}_0$. □

Since Ω_0 is an ovoid in Σ for q even, the points of Σ together with the tangent lines to Ω_0 form a generalized quadrangle $\mathcal{W}_3(q)$. We again let $\mathcal{G}$ denote the subgroup of $PGL(4, q)$ leaving invariant the lines of $\mathcal{W}_3(q)$ (for q even $\mathcal{G}$ is isomorphic to $PSp(4, q)$), and consider $\mathcal{G}$ as the automorphism group of $\mathcal{W}_3(q)$. We now partition the points of $\Sigma \setminus \Omega_0$ into 2-ovoids of this $\mathcal{W}_3(q)$.

Theorem 3.3. *For even q and any integer $i \in \{1, 2, 3, \ldots, q/2\}$, the set $\mathcal{O}_i = \Omega_i \cup \Omega_{q+1-i}$ is a 2-ovoid of $\mathcal{W}_3(q)$ admitting the semidirect product of a cyclic group of order q^2+1 by a cyclic group of order 4.*

Proof. The lines of $\mathcal{S}_0$, which are lines of $\mathcal{W}_3(q)$, are tangent to each G-orbit, and hence meet $\mathcal{O}_i$ in precisely two points. Any other line of $\mathcal{W}_3(q)$ cannot meet both Ω_i and Ω_{q+1-i} by Theorem 3.2, for any integer $i \in \{1, 2, 3, \ldots, q/2\}$. But every such line is secant to exactly $q/2$ of

the ovoids $\Omega_1, \Omega_2, \Omega_3, \ldots, \Omega_q$ and is disjoint from the other $q/2$ of these ovoids. So it must be the case that any such line is secant to one ovoid from the pair $\{\Omega_i, \Omega_{q+1-i}\}$ and disjoint from the other, for each integer $i \in \{1, 2, 3, \ldots, q/2\}$. Thus $\mathcal{O}_i$ is a 2-ovoid of $\mathcal{W}_3(q)$ for each integer $i \in \{1, 2, 3, \ldots, q/2\}$.

By definition of our $\mathcal{W}_3(q)$, the Singer subgroup G of order q^2+1 is a subgroup of $\mathcal{G}$ that leaves each $\mathcal{O}_i$ invariant. Moreover, the Frobenious map $x \mapsto x^q$ induces a collineation θ of order 4 that leaves the G-orbit Ω_0 invariant and interchanges the G-orbits Ω_i and Ω_{q+1-i}. Thus $\theta \in \mathcal{G}$ and θ stabilizes each 2-ovoid $\mathcal{O}_i$. As the cyclic subgroup generated by θ meets G trivially, the result now follows. □

Corollary 3.4. *For q even, m-ovoids of $\mathcal{W}_3(q)$ admitting the semidirect product of a cyclic group of order q^2+1 by a cyclic group of order 4 exist for all integers m, with $1 \leqslant m \leqslant q$.*

Proof. Since the 2-ovoids $\mathcal{O}_i$ of Theorem 3.3, for $i \in \{1, 2, 3, \ldots, q/2\}$, are mutually disjoint, taking unions we obtain m-ovoids of $\mathcal{W}_3(q)$ for all even m between 2 and q. The result now follows by also including the complementary $(q+1-m)$-ovoids, since all these m-ovoids admit the group described in Theorem 3.3. □

It should be noted that the above corollary implies the existence of $\binom{q/2}{k}$ $2k$-ovoids (and $(q+1-2k)$-ovoids) of $\mathcal{W}_3(q)$ for $k = 1, 2, 3, \ldots, q/2$. In practice these are all mutually inequivalent under $\mathcal{G}$, as verified by Magma [7] for $q = 4, 8$ and 16.

4. A generalization of Payne–Thas derivation

A hyperbolic pair $\{\ell, \ell^\perp\}$ of $\mathcal{W}_3(q)$ is a partial 2-ovoid. Indeed, any isotropic line meeting ℓ must meet $\ell^\perp$. In fact, one can check that this partial 2-ovoid is complete. In particular, a 2-ovoid cannot contain a hyperbolic pair.

Using this observation, one can extend the Payne–Thas derivation [11] introduced for the construction of non-classical ovoids of the Hermitian surface to the case of m-ovoids of $\mathcal{W}_3(q)$, q odd, when $m = (q+1)/2$. If the $(q+1)/2$-ovoid $\mathcal{O}$ of $\mathcal{W}_3(q)$ contains a hyperbolic line ℓ, then $\mathcal{O} \setminus \{\ell\} \cup \{\ell^\perp\}$ is again a $(q+1)/2$-ovoid. Indeed, suppose that an m-ovoid $\mathcal{O}$ contains the hyperbolic line ℓ. Since $\ell \cup \ell^\perp$ is a 2-tight set [2, Section 2], it meets any m-ovoid in $2m$ points, and by assumption meets an m-ovoid in $q+1$ points, implying that $m = (q+1)/2$. In this case $\mathcal{O}$ meets $\ell \cup \ell^\perp$ at $2m = q+1$ points, and contains ℓ. Hence $\mathcal{O}$ is disjoint from $\ell^\perp$ and $\mathcal{O} \setminus \{\ell\} \cup \{\ell^\perp\}$ is a $(q+1)/2$-ovoid as desired.

Acknowledgments

The authors would like to thank Tim Penttila for very helpful suggestions and comments, and in particular for pointing out reference [2]. While some of the independently obtained results in this paper overlap work done in [2], the approaches are completely different.

References

[1] B. Bagchi, N.S. Sastry Narasimha, Intersection pattern of the classical ovoids in symplectic 3-space of even order, J. Algebra 126 (1989) 147–160.

[2] J. Bamberg, M. Law, T. Penttila, Tight sets and m-ovoids of generalized quadrangles, submitted for publication.

[3] R.D. Baker, G.L. Ebert, Enumeration of two-dimensional flag-transitive planes, Algebras Groups Geom. 3 (1985) 248–257.
[4] R.D. Baker, G.L. Ebert, Two-dimensional flag-transitive planes revisited, Geom. Dedicata 63 (1996) 1–15.
[5] R.H. Bruck, Construction problems of finite projective planes, in: R.C. Bose, T.A. Dowling (Eds.), Combinatorial Mathematics and Its Applications, Univ. of North Carolina Press, Chapel Hill, 1969, pp. 426–514.
[6] P.J. Cameron, P. Delsarte, J.M. Goethals, Hemisystems, orthogonal configurations, and dissipative conference matrices, Philips J. Res. 34 (1979) 147–162.
[7] J. Cannon, C. Playoust, An Introduction to MAGMA, Univ. of Sydney Press, Sydney, 1993.
[8] A. Cossidente, T. Penttila, Hemisystems on the Hermitian surface, J. London Math. Soc. (2) 72 (2005) 731–741.
[9] K. Drudge, Proper 2-covers of $PG(3, q)$, q even, Geom. Dedicata 80 (2000) 59–64.
[10] G.L. Ebert, Partitioning projective geometries into caps, Canad. J. Math. 37 (1985) 1163–1175.
[11] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, Research Notes Math., vol. 110, Pitman, 1984.
[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, Ovoids and spreads of finite classical polar spaces, Geom. Dedicata 10 (1981) 135–144.
[14] J.A. Thas, Interesting pointsets in generalized quadrangles and partial geometries, Linear Algebra Appl. 114/115 (1989) 103–131.
[15] J.A. Thas, Ovoids, spreads and m-systems of finite classical polar spaces, in: Surveys in Combinatorics, in: London Math. Soc. Lecture Note Ser., vol. 288, Cambridge Univ. Press, 2001, pp. 241–267.