Special Issue (2003), S49–S58

Advances in Geometry

Ovoids of the Hermitian surface in odd characteristic

Luca Giuzzi and Gábor Korchmáros*

Dedicated to Professor Adriano Barlotti on the occasion of his 80th birthday

Abstract. We construct a new ovoid of the polar space arising from the Hermitian surface of $PG(3, q^2)$ with $q \geqslant 5$ odd. The automorphism group Γ of such an ovoid has a normal cyclic subgroup Φ of order $\frac{1}{2}(q+1)$ such that $\Gamma/\Phi \cong PGL(2, q)$. Furthermore, Γ has three orbits on the ovoid, one of size $q+1$ and two of size $\frac{1}{2}q(q-1)(q+1)$.

Key words. Ovoid, Hermitian surface, polar space, automorphism group.

2000 Mathematics Subject Classification. Primary: 51E20, Secondary: 51A50

1 Introduction

The concept of ovoid and its generalisations have played an important role in finite geometry since the fifties. By a beautiful result of A. Barlotti [2] and G. Panella [10], every ovoid in $PG(3, q)$ with q odd is an elliptic quadric. This is a generalisation of Segre's famous theorem [11] stating that every oval in $PG(2, q)$, with q odd, is a conic. Ovoids of finite classical polar spaces have been intensively investigated, especially in the last two decades, see [1], [3], [4], [5], [9], [12], [13], [14] and the recent survey paper [15]. In this paper we are concerned with ovoids of the polar space determined by a non-degenerate Hermitian surface $\mathscr{H}(3, q^2)$ of $PG(3, q^2)$.

An ovoid $\mathcal{O}$ of the polar space arising from $\mathscr{H}(3, q^2)$ is a set of $q^3 + 1$ points in $\mathscr{H}(3, q^2)$ which meets every generator (that is, every line contained in $\mathscr{H}(3, q^2)$) in exactly one point. The intersection of $\mathscr{H}(3, q^2)$ with any non-tangent plane provides an ovoid—namely, the *classical* ovoid of $\mathscr{H}(3, q^2)$. Existence of non-classical ovoids of $\mathscr{H}(3, q^2)$ was pointed out by Payne and Thas [16], who constructed a non-classical ovoid $\mathcal{O}'$ from the classical one $\mathcal{O}$ by replacing the $q+1$ points of $\mathcal{O}$ lying in a chord ℓ by the common points of $\mathscr{H}(3, q^2)$ with the polar line ℓ' of ℓ. A straightforward generalisation of this procedure consists in replacing a number of chords of $\mathcal{O}$, each with its own polar line. The condition for the resulting set to be an ovoid is easily

* The present research was performed within the activity of G.N.S.A.G.A. of the Italian INDAM with the financial support of the Italian Ministry M.I.U.R., project "Strutture geometriche, combinatorica e loro applicazioni", 2001–02.

stated: the replaced chords must pairwise intersect outside of $\mathcal{O}$. The above procedure will be called *derivation* or *multiple derivation* according to one or more chords being replaced.

In this paper, we construct an ovoid $\mathcal{O}$ of $\mathcal{H}(3,q^2)$ for every odd $q \geqslant 5$ which cannot be obtained either by derivation or by multiple derivation. We also determine the automorphism group of $\mathcal{O}$, as given by the subgroup of $\mathrm{PGU}(4,q^2)$ preserving $\mathcal{O}$.

2 Preliminary results on ovoids of the Hermitian surface

Let $\mathcal{H}(3,q^2)$ be a non-degenerate Hermitian surface in $\mathrm{PG}(3,q^2)$. It is well known, see [6, Chapter 19], that $\mathcal{H}(3,q^2)$ can be reduced by a non-singular linear transformation to the canonical form $X_0^q X_3 + X_0 X_3^q + uX_1^{q+1} + vX_2^{q+1} = 0$, where $u, v \in \mathbb{F}_q$ are non-zero elements. The linear collineation group of $\mathrm{PG}(3,q^2)$ preserving $\mathcal{H}(3,q^2)$ is $\mathrm{PGU}(4,q^2)$. See [8] for a classification of the subgroups of $\mathrm{PGU}(4,q^2)$. We shall rely only upon an existence theorem for subgroups of homologies, as stated in the following lemma.

Lemma 2.1. *Let α be a non-tangent plane to $\mathcal{H}(3,q^2)$ and A its pole under the unitary polarity associated with $\mathcal{H}(3,q^2)$. Then the (α, A) homology group of* $\mathrm{PGU}(3,q^2)$, *that is, the maximal subgroup of* $\mathrm{PGU}(3,q^2)$ *consisting of homologies with axis α and centre A, is a cyclic group of order $q+1$.*

We shall also need a characterisation of ovoids which can be obtained by multiple derivation.

Lemma 2.2. *Let $\mathcal{O}'$ be an ovoid of $\mathcal{H}(3,q^2)$. A necessary and sufficient condition for $\mathcal{O}'$ to be obtainable from a classical ovoid $\mathcal{O}$ of $\mathcal{H}(3,q^2)$ through multiple derivation is that $\mathcal{O}'$ is preserved by the (α, A) homology group of* $\mathrm{PGU}(3,q^2)$ *for a non-tangent plane α and its pole A.*

Proof. Choose a pair (α, A) consisting of a non-tangent plane α to $\mathcal{H}(3,q^2)$ and the pole A of α under the unitary polarity associated with $\mathcal{H}(3,q^2)$. Let $\mathcal{O}$ be the classical ovoid given by all common points of $\mathcal{H}(3,q^2)$ and α. Denote by Ψ the homology group of $\mathrm{PGU}(3,q^2)$ with axis α and centre A. It is easily verified that if an ovoid $\mathcal{O}'$ arises from $\mathcal{O}$ by (multiple) derivation, then Ψ preserves $\mathcal{O}'$. Conversely, we prove that if Ψ preserves an ovoid $\mathcal{O}'$ different from $\mathcal{O}$, then $\mathcal{O}'$ can be obtained from $\mathcal{O}$ by (multiple) derivation. Let $P \in \mathcal{O}'$ be a point not on α. Then the orbit of P under Ψ consists of the common points of $\mathcal{H}(3,q^2)$ and the line ℓ' joining A and P. Hence, $\mathcal{H}(3,q^2) \cap \ell'$ is contained in $\mathcal{O}'$. Let now $\ell_1', \dots, \ell_m'$ be the lines through A which meet $\mathcal{O}'$ outside α, and let $\ell_1, \dots, \ell_m$ be their corresponding polar lines. The latter lines are chords of the Hermitian curve $\mathcal{H}(2,q^2) = \mathcal{O}$, cut out on $\mathcal{H}(3,q^2)$ by the plane α, and any two of them intersect outside $\mathcal{H}(2,q^2)$. This proves that $\mathcal{O}'$ arises from $\mathcal{O}$ by multiple derivation. □

3 The construction

We assume $q \geqslant 5$ to be odd and write the equation of the Hermitian surface $\mathscr{H}(3, q^2)$ in its canonical form

$$X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0. \tag{3.1}$$

The starting point of our construction is the following lemma.

Lemma 3.1. *Let* (x, y) *satisfy the relation*

$$y^q + y + x^{(q+1)/2} = 0. \tag{3.2}$$

Then the point $(1, x, y, y^2)$ *lies on* $\mathscr{H}(3, q^2)$.

Proof. If (x, y) satisfies (3.2), then the polynomial identity

$$(Y^q + Y - X^{(q+1)/2})(Y^q + Y + X^{(q+1)/2}) = Y^{2q} + 2Y^{q+1} + Y^2 - X^{q+1}$$

implies that $y^{2q} + 2y^{q+1} + y^2 - x^{q+1} = 0$. The geometric interpretation of this equation is that the point $(1, x, y, y^2)$ lies on $\mathscr{H}(3, q^2)$. □

Lemma 3.2. *Let* $x \in \mathbb{F}_{q^2}^*$. *Then Equation* (3.2) *has either* q *or* 0 *solutions in* $y \in \mathbb{F}_{q^2}$, *according as* x *is a square or a non-square in* $\mathbb{F}_{q^2}$.

Proof. We first prove that if (x, y), with $x, y \in \mathbb{F}_{q^2}$, satisfies (3.2), then x is the square of an element of $\mathbb{F}_{q^2}$. The assertion holds trivially for $x = 0$; hence, we may assume that $x \neq 0$. Since $y^q + y \in \mathbb{F}_q$, we have $-x^{(q+1)/2} \in \mathbb{F}_q$, whence $(x^{(q+1)/2})^{q-1} = 1$. On the other hand, $x \neq 0$ is a square in $\mathbb{F}_{q^2}$ if and only if $x^{(q^2-1)/2} = 1$, which proves the assertion. Conversely, let x be a square element of $\mathbb{F}_{q^2}$, and take $\xi \in \mathbb{F}_{q^2}$ such that $x = \xi^2$. By [7, 1.19], the equation $y^q + y = \xi^{q+1}$ has exactly q solutions in $\mathbb{F}_{q^2}$. Hence, $y^q + y = x^{(q+1)/2}$ holds for exactly q values $y \in \mathbb{F}_{q^2}$. This completes the proof. □

Let Σ denote the set of all pairs (x, y) with $x, y \in \mathbb{F}_{q^2}$ satisfying (3.2).

Lemma 3.3. *The set* Σ *has size* $\frac{1}{2}q(q^2 + 1)$.

Proof. The number of squares in $\mathbb{F}_{q^2}$, zero included, is $(q^2 + 1)/2$. Thus, the assertion follows from Lemma 3.2 together with a counting argument. □

We embed Σ in $\mathrm{PG}(3, q^2)$ by means of the map $\varphi : (1, x, y) \mapsto (1, x, y, y^2)$. Some properties of the embedded set are collected in the following two lemmas.

Lemma 3.4. *Let* Δ *be the set of all points* $(1, x, y, y^2)$ *of* $\mathrm{PG}(3, q^2)$ *with* $(x, y) \in \Sigma$, *together with the point* $(0, 0, 0, 1)$. *Then*

I) Δ *has size* $\frac{1}{2}(q^3 + q + 2)$;

II) *The plane* π *with equation* $X_1 = 0$ *intersects* Δ *in a set* Δ_1 *of size* $q + 1$. *The set* Δ_1 *is the complete intersection in* π *of the conic* $\mathscr{C}$ *with equation* $X_0X_3 - X_2^2 = 0$ *and the Hermitian curve* $\mathscr{H}(2, q^2)$ *with equation* $X_0^qX_3 + X_0X_3^q + 2X_2^{q+1} = 0$;

III) *The Baer involution* $\beta := (X_0, X_2, X_3) \mapsto (X_0^q, -X_2^q, X_3^q)$ *of* π *preserves both* $\mathscr{C}$ *and* $\mathscr{H}(2, q^2)$. *The associated Baer subplane* π_0 *of* π *meets* $\mathscr{H}(2, q^2)$ *in* Δ_1;

IV) Δ_1 *lies in* π_0 *and consists of all the points of a conic* $\mathscr{C}_0$ *of* π_0.

Proof. The lemma is a consequence of straightforward computations. □

Lemma 3.5. *The point* $U = (0, 1, 0, 0)$ *is not in* Δ. *Furthermore,*

i) *A line through* U *meets* Δ *in either* $\frac{1}{2}(q+1)$ *or* 1 *or* 0 *points. More precisely, there are exactly* $q^2 - q$ *lines through* U *sharing* $\frac{1}{2}(q+1)$ *points with* Δ, *and* $q + 1$ *lines having just one point in* Δ. *The former lines meet the plane* π *in the points of the conic* $\mathscr{C}$ *not lying on* Δ_1; *the latter in the points of* Δ_1;

ii) *A plane through* U *meets* Δ *in either* $q + 1$ *or* $\frac{1}{2}(q+1)$ *or* 0 *points*;

iii) *A plane missing* U *meets* Δ *in at most* $q^2 + 1$ *points.*

Proof. In order to prove ii), take a point $P(1, x, y, y^2)$ in Δ and consider the line ℓ through U and P. The point $P_t(1, x+t, y, y^2)$, for $t \in \mathbb{F}_{q^2}$, is a common point of ℓ and Δ if and only if $y^q + y + (x+t)^{(q+1)/2} = 0$. By (3.2) this occurs when $(x+t)^{(q+1)/2} = x^{(q+1)/2}$. For $x = 0$, this implies $t = 0$. Hence, in this case, P is the only common point of ℓ and Δ. In particular, $P \in \Delta_1$. For $x \neq 0$, we obtain $(1 + t/x)^{(q+1)/2} = 1$. Since all the $\frac{1}{2}(q+1)$-st roots of unity are contained in $\mathbb{F}_{q^2}$ and they are pairwise distinct, ℓ contains exactly $\frac{1}{2}(q+1)$ points from Δ. The common point of ℓ and π is the point $(1, 0, y, y^2)$ which lies on $\mathscr{C}$, but does not belong to Δ_1. Let now α be the plane through U with equation $u_0X_0 + u_2X_2 + u_3X_3 = 0$; a point $P(1, x, y, y^2)$ of Δ lies in α if and only if $u_0 + u_2y + u_3y^2 = 0$. Since for every $y \in \mathbb{F}_{q^2}$, Equation (3.2) has exactly $\frac{1}{2}(q+1)$ solutions in $x \in \mathbb{F}_{q^2}$, statement ii) follows. To prove iii), consider a plane β which meets any line through U in exactly one point. By statement i), there are at most $q^2 + 1$ lines through U containing a point of Δ. Hence, $q^2 + 1$ is an upper bound for the number of points in common between β and Δ. This proves statement iii). □

We need some more notation. For $q \equiv 1 \pmod 4$, denote by Δ' the set of all points in $\mathscr{H}(2, q^2) \setminus \Delta_1$ which are covered by chords of $\mathscr{C}_0$. For $q \equiv 3 \pmod 4$, Δ' will denote the set of all points in $\mathscr{H}(2, q^2)$ which are covered by external lines to $\mathscr{C}_0$ in π_0. Clearly, Δ' has size $\frac{1}{2}q(q+1)(q-1)$. Several properties of $\Delta \cup \Delta'$ can be deduced from Lemma 3.5. However, we just state one which will be used in Section 5.

Lemma 3.6. *With the notation above,*

i) *The plane* $X_1 = 0$ *meets* $\Delta \cup \Delta'$ *in* $\frac{1}{2}(q^3 + q + 2)$ *points; any other plane of* $\mathrm{PG}(3, q^2)$ *has at most* $q^2 + q + 2$ *points in common with* $\Delta \cup \Delta'$;

ii) *A line through* U *meets* $\Delta \cup \Delta'$ *in either* $\frac{1}{2}(q+1)$ *or* 1 *or* 0 *points. More precisely, there are exactly* $q^2 - q$ *lines through* U *sharing* $\frac{1}{2}(q+1)$ *points with* $\Delta \cup \Delta'$, *and* $\frac{1}{2}(q^3 + q + 2)$ *having just one point in* $\Delta \cup \Delta'$. *The former lines meet* π *in the points of the conic* $\mathscr{C}$ *which are not in* Δ_1; *the latter meet* π *in the points of* $\Delta_1 \cup \Delta'$.

The main result of this paper is the following.

Theorem 3.7. *The set* $\Delta \cup \Delta'$ *is an ovoid of* $\mathscr{H}(3, q^2)$ *which cannot be obtained from a Hermitian curve by means of multiple derivation.*

The proof of Theorem 3.7 is postponed till Section 5. Meanwhile, we state and prove some properties of the collineation group of $\Delta \cup \Delta'$ which will play a role in its proof.

4 The subgroup of $\mathbf{PGU(4, q^2)}$ preserving $\Delta \cup \Delta'$

The linear collineation group of $\mathrm{PG}(3, q^2)$ preserving $\mathscr{H}(3, q^2)$ is $\mathrm{PGU}(4, q^2)$. First, we determine the subgroup of $\mathrm{PGU}(4, q^2)$ which preserves Δ. In doing so, we shall be dealing with several collineations from $\mathrm{PGU}(4, q^2)$.

For any $a \in \mathbb{F}_{q^2}$, with $a^q + a = 0$, and for any square μ in $\mathbb{F}_{q^2}$, let

$$T_a := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ a & 0 & 1 & 0 \\ a^2 & 0 & 2a & 1 \end{pmatrix}; \quad M_\mu := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu^{(q+1)/2} & 0 \\ 0 & 0 & 0 & \mu^{(q+1)} \end{pmatrix}.$$

Denote by $[T_a]$ and $[M_\mu]$ the linear collineations associated with the matrices T_a and M_μ, respectively.

It is easily verified that $\mathbf{T} = \{[T_a] \mid a \in \mathbb{F}_{q^2}\}$ is an elementary Abelian group of order q, while $\mathbf{M} = \{[M_\mu] \mid \mu \in \mathbb{F}_{q^2}^*\}$ is a cyclic group of order $\frac{1}{2}(q^2 - 1)$. Furthermore, the group generated by $\mathbf{T}$ and $\mathbf{M}$ is the semidirect product $\mathbf{T} \rtimes \mathbf{M}$.

For any non-zero square λ in $\mathbb{F}_q^*$, let

$$L_\lambda := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Again, $[L_\lambda]$ is the linear collineation associated to the matrix L_λ. Clearly, $\mathbf{L} = \{[L_\lambda] \mid \lambda \in \mathbb{F}_q^*\}$ is a cyclic group of order $(q+1)/2$. Finally, let

$$N := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and $[N]$ be the associated linear collineation; the collineation group $\mathbf{N}$ generated by $[N]$ has order 2.

Lemma 4.1. *Let Γ be the the group generated by all of the above linear collineations. Then*

i) Γ *preserves both* $\mathscr{H}(3, q^2)$ *and* Δ;

ii) Γ *has two orbits on* Δ. *One is* Δ_1 *and the other, say* Δ_2, *has size* $\frac{1}{2}q(q-1)(q+1)$;

iii) Γ *acts on* Δ_1 *as a sharply* 3-*transitive permutation group*;

iv) *The subgroup* Φ *of* Γ *fixing* Δ_1 *pointwise is a cyclic group of order* $\frac{1}{2}(q+1)$ *and* $\Gamma/\Phi \cong \mathrm{PGL}(2, q)$;

v) Γ *has order* $\frac{1}{2}q(q-1)(q+1)^2$.

Proof. A straightforward computation shows that each of the above linear collineations preserves both $\mathscr{H}(3, q^2)$ and Δ. This proves the first assertion. Next, take any square $x \in \mathbb{F}_{q^2}$. Following Lemma 3.4, let $\Delta(x)$ be the set of the q points $P_y = (1, x, y, y^2)$, satisfying $y^q + y = x^{(q+1)/2}$, $y \in \mathbb{F}_{q^2}$. Then $\Delta_1 = \Delta(0) \cup P_\infty(0, 0, 0, 1)$. Further, let $\Delta_2 = \bigcup \Delta(x)$, where the union is over the set of non-zero squares of $\mathbb{F}_{q^2}$. Then $|\Delta_2| = \frac{1}{2}q(q^2 - 1)$ and $\Delta = \Delta_1 \cup \Delta_2$. To prove that Δ_2 is a full orbit under Γ, take any two points in Δ_2, say $P = (1, x, y, y^2)$ and $Q = (1, x', y', y'^2)$. Since both x and x' are non-zero squares in $\mathbb{F}_{q^2}$, their ratio $\mu = x/x'$ is also a non-zero square element of $\mathbb{F}_{q^2}$. The collineation $[M_\mu]$ maps Q onto a point $R = (1, x, \bar{y}, \bar{y}^2) \in \Delta_2$. For $a = y - \bar{y}$, the collineation $[T_a]$ takes R onto P. This proves the assertion. We now show that Γ induces on Δ_1 a 3-transitive permutation group. This depends on the following remarks: the group $\mathbf{T}$ fixes P_∞ and acts transitively on the remaining q points in Δ_1, whereas $\mathbf{M}$ fixes both P_0 and P_∞ and acts transitively on the remaining $q - 1$ points in Δ_1. Hence, $\mathbf{T} \rtimes \mathbf{M}$ acts on $\Delta_1 \setminus \{P_\infty\}$ as a sharply 2-transitive permutation group whose one-point stabiliser is cyclic. Furthermore, $[N]$ interchanges P_0 and P_∞. Following the notation of Lemma 3.4, let Φ be the normal subgroup of Γ which fixes π pointwise. Any collineation of Φ is associated with a diagonal matrix of type

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \rho & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

with $\rho \in \mathbb{F}_{q^2}^*$; such collineation preserves Δ if and only if $\rho^{(q+1)/2} = 1$. This shows that $\Phi = \mathbf{L}$. Hence, Φ is a cyclic group of order $(q+1)/2$. Let $G = \Gamma/\Phi$ be the linear collineation group induced by Γ on π. Then G is the linear collineation group of π which preserves Δ_1. Actually, G also preserves the Baer subplane π_0 as defined in III) of Lemma 3.4, since the associated Baer involution β centralises G. By IV) of Lemma 3.4, G is a linear collineation group of π_0 which acts 3-transitively on a conic $\mathscr{C}_0$ of π_0. Thus, $G \cong \mathrm{PGL}(2,q)$ acts on $\mathscr{C}_0$ as $\mathrm{PGL}(2,q)$ in its unique sharply 3-transitive permutation representation. In particular, G has order $q(q-1)(q+1)$, and hence v) holds. □

In the previous proof, we have also shown that Γ coincides with the subgroup of $\mathrm{PGU}(4,q^2)$ which preserves both Δ_1 and Δ_2. Actually, this result can be improved with little more effort.

Lemma 4.2. *The group* Γ *is the subgroup of* $\mathrm{PGU}(4,q^2)$ *which preserves* Δ.

Proof. Assume, to the contrary, that the subgroup of $\mathrm{PGU}(4,q^2)$ which preserves Δ acts transitively on Δ. Then the size of Δ should divide the order of $\mathrm{PGU}(3,q^2)$, that is, $\frac{1}{2}(q+1)(q^2-q+2)$ should divide $q^6(q+1)^3(q-1)^2(q^2-q+1)$. Let d be a prime divisor of q^2-q+2. Thus d divides $(q-1)^2(q+1)^3$ too. This is possible only for $d=2$. Hence, $q^2+q-2=2^m$ for an integer $m \geqslant 1$. We show that this cannot occur for $q \geqslant 5$. First, assume that $m=2n$ is even and write $q^2-q+2=2^{2n}$ in the equivalent form $(2^{n+1}+(2q-1))(2^{n+1}-(2q-1))=7$, whence $2^{n+1}+2q-1=7$ and $2^{n+1}-(2q-1)=1$. This only occurs for $q=2$, $n=1$. For the case $m=2n+1$, write $q^2-q+2=2^{2n+1}$ as $q(q-1)=2(2^n+1)(2^n-1)$. This yields $kq=2^n \pm 1$ and $\frac{1}{2k}(q-1)=2^n \mp 1$ for a divisor k of $q-1$. Then $kq-\frac{1}{2k}(q-1)=2$, which is only possible for $q=3$, $n=1$ and $k=1$, since $kq-\frac{1}{2k}(q-1)>(q-1)\left(k-\frac{1}{k}\right)>\frac{1}{2}k(q-1)$. □

We now turn our attention to Δ'.

Lemma 4.3. *The group* Γ *preserves* Δ'. *More precisely*, Δ' *is an orbit under* Γ.

Proof. Using the notation of Lemma 3.4, Γ preserves the plane π and induces on π a linear collineation group $G \cong \mathrm{PGL}(2,q)$ that leaves both $\mathscr{C}_0$ and $\mathscr{H}(2,q^2)$ invariant. In particular, Γ preserves the set of all chords of $\mathscr{C}_0$, as well as that of external lines to $\mathscr{C}_0$. Hence, it leaves Δ' invariant. To prove that G is transitive on Δ', it is enough to show that the stabiliser G_P of a point $P \in H(2,q^2)\backslash\Delta_1$ has order 2. As $P \notin \pi_0$, there is only one line of π_0 through P, say ℓ. Since tangents to $\mathscr{C}_0$ are also tangents to $\mathscr{H}(2,q^2)$, ℓ is either a chord of $\mathscr{C}_0$ or an external line to $\mathscr{C}_0$. Thus, the stabiliser G_ℓ of ℓ is a dihedral group $D_{q\pm1}$ of order $2(q\pm1)$, where $+$ or $-$ occurs depending on whether ℓ is an external line or a chord. The central involution of $D_{q\pm1}$ fixes ℓ pointwise, whereas each of the $q\pm1$ non-central involutions of $D_{q\pm1}$ has exactly two fixed points, both in π_0, hence distinct from P. Choose now any element $g \in D_{q\pm1}$ of order greater than 2. To complete the proof we have to show that $g(P) \neq P$. If ℓ is an external line to $\mathscr{C}_0$, then g has no fixed point on ℓ; when ℓ is a chord, g fixes the common points of ℓ and $\mathscr{C}_0$ but no other point on ℓ. □

Our final result is the following theorem.

Theorem 4.4. *The group* Γ *is the subgroup of* $\mathrm{PGU}(4,q^2)$ *which preserves* $\Delta \cup \Delta'$.

Proof. By virtue of the last two Lemmas, we have only to prove that any collineation $g \in \mathrm{PGU}(3,q^2)$ preserving $\Delta \cup \Delta'$ must also preserve Δ. By i) of Lemma 3.6, g preserves the plane π with equation $X_1 = 0$. Since $U = (0,1,0,0)$ is the pole of π with respect to the unitary polarity associated with $\mathscr{H}(3,q^2)$, it turns out that g fixes U. By ii) of Lemma 3.6, g preserves the conic $\mathscr{C}$ of π. Since g preserves $\mathscr{H}(2,q^2) = \mathscr{H}(3,q^2) \cap \pi$ and $\Delta_1 = \mathscr{H}(2,q^2) \cap \mathscr{C} = \mathscr{C}_0$, it follows that g preserves both Δ_1 and $\mathscr{C} \backslash \Delta_1$. Again, by ii) of Lemma 3.6, the latter assertion yields that g preserves not only Δ_1 but also $\Delta \backslash \Delta_1$. This can only happen if g preserves Δ. □

5 The proof of Theorem 3.7

We keep our previous notation. We first prove that $\mathscr{O} = \Delta \cup \Delta'$ is an ovoid. Since $\mathscr{O}$ has the right size, $q^3 + 1$, it is enough to show that no two distinct points in $\mathscr{O}$ are conjugate under the unitary polarity associated with $\mathscr{H}(3,q^2)$. As $\Delta_1 \cup \Delta_2$ lies in the plane π, which is not tangent to $\mathscr{H}(3,q^2)$, our assertion is true for any two distinct points in $\Delta_1 \cup \Delta'$. It remains to prove that no point $P \in \Delta_2 = \Delta \backslash \Delta_1$ is conjugate to another point in $\Delta \cup \Delta'$. Since, by ii) of Lemma 4.1, Γ acts transitively on Δ_2, we may assume $P\left(1,1,-\frac{1}{2},\frac{1}{4}\right)$. The plane α_P, tangent to $\mathscr{H}(3,q^2)$ at P, has equation $X_0 - 4X_1 - 4X_2 + 4X_3 = 0$. We have to verify that both of the following statements hold:

i) α_P has no points in Δ except P;

ii) α_P meets π in a line disjoint from $\Delta_1 \cup \Delta'$.

Let $Q = (1,x,y,y^2) \in \Delta_2$ be a point of α_P. Then by Lemma 3.2, $x = \xi^2$ with $\xi \in \mathbb{F}_{q^2}$. In this case, both $1 - 4\xi^2 - 4y + 4y^2 = 0$ and $y^q + y + \xi^{q+1} = 0$. The former equation gives $y = \pm\frac{1}{2}(2\xi + 1)$; it follows that $(\pm\xi^q - 1)(\pm\xi - 1) = 0$. This yields $\xi = \pm 1$. Thus, $x = 1$ and either $y = -\frac{1}{2}$, or $y = \frac{3}{2}$. As q is odd, the latter condition is impossible. Hence, Q is the only common point of α and Δ_2.

To verify ii), we consider the line $\ell = \alpha_P \cap \pi$ with equation $X_0 - 4X_2 + 4X_3 = 0$, and we show that ℓ is disjoint from Δ'.

We first deal with the case $q \equiv 1 \pmod 4$. For any chord r of $\mathscr{C}_0$, compute the coordinates of the point $R = \ell \cap r$. Let $R_1 = (1,u,u^2)$ and $R_2 = (1,v,v^2)$, with $u^q + u = 0$, $v^q + v = 0$, be the common points of r and $\mathscr{C}_0$. Since r has equation $uvX_0 - (u+v)X_2 + X_3 = 0$, we have $R = (4(u+v-1), 4uv-1, 4uv-u-v)$. Let

$$f = 4(u+v-1)^q(4uv-u-v) + 4(u+v-1)(4uv-u-v)^q + 2(4uv-1)^{q+1}.$$

Then $f = 0$ if and only if $R \in \mathscr{H}(2,q^2)$. By a straightforward computation,

$$\begin{aligned} f &= 4(u+v-1)^q(u+v-4uv) + 4(u+v-1)(u+v-4uv)^q \\ &\quad + 2(4uv-1)^{q+1} = 4(1+4v^2)u^2 - 16vu + 4v^2 + 1. \end{aligned}$$

This shows that $f = 0$ implies that

$$u = \frac{4v + (4v^2 - 1)j}{2(1 + 4v^2)}, \quad j^2 = -1. \tag{5.1}$$

As $q \equiv 1 \pmod 4$, we have $j^q = j$. Taking $u^q + u = 0$, $v^q + v = 0$ into account, we see that $f = 0$ yields

$$0 = u^q + u = \frac{4v - 1}{2(1 + 4v)}(j + j^q).$$

Therefore, $q \equiv 1 \pmod 4$ implies $f \neq 0$ and ii) follows for this case.

If $q \equiv 3 \pmod 4$, we have to consider an external line r to $\mathscr{C}_0$. Since r meets $\mathscr{C}$ in two distinct points, r can be regarded as the line joining the point $R_1(1, u, u^2)$, with $u^q + u \neq 0$, and its image $R_2(1, -u^q, u^{2q})$ under the Baer involution associated with π_0, see statement III) of Lemma 3.4. Hence, r has equation $X_3 + (u^q - u)X_2 - u^{q+1}X_0 = 0$. The common point of r and ℓ is $R = (4(u^q - u + 1), 4u^{q+1} + 1, 4u^{q+1} - u^q + u)$. Let

$$\begin{aligned} f &= 4(u^q - u + 1)^q(4u^{q+1} - u^q + u) \\ &\quad + 4(u^q - u + 1)(4u^{q+1} - u^q + u)^q + 2(4u^{q+1} + 1)^{q+1}. \end{aligned}$$

Then $R \in \mathscr{H}(2, q^2)$ if and only if $f = 0$. By a direct computation $f = 2[4(u^q + u)^2 + (4u^{q+1} + 1)^2]$. Therefore, $f = 0$ implies that $2(u^q + u) = j(4u^{q+1} + 1)$ with $j^2 = -1$, whence $4u^{q+1} + 1 \neq 0$ and

$$j = 2\frac{u^q + u}{4u^{q+1} + 1}.$$

This yields $j \in \mathbb{F}_q$, contradicting $q \equiv 3 \pmod 4$, and completes the proof of ii).

Finally, assume by way of contradiction that $\mathscr{O}$ is obtained by a multiple derivation. According to Lemma 2.2, there is a homology group Ψ of order $q + 1$ preserving $\mathscr{O}$. Let α be its axis; the pole A of α is the centre of the elements of Ψ. By Theorem 4.4, Ψ is a subgroup of Γ; hence, it preserves π. However, Ψ is not a subgroup of Φ, since, by iv) of Lemma 4.1, the subgroup Φ of Γ fixing π pointwise has order $\frac{1}{2}(q + 1)$. In particular, $\alpha \neq \pi$. Hence, Ψ acts faithfully on π. In other words, the linear collineation group H induced by Ψ on π has order $q + 1$. Actually, H is a homology group of π whose axis is the common line of α and π and whose centre is the point of intersection of π and the line joining A and U. By ii) of Lemma 3.5, H preserves the conic $\mathscr{C}$ of π. This leads to a contradiction, as no homology of order $t > 2$ preserves a conic.

References

[1] R. D. Baker, G. L. Ebert, G. Korchmáros, T. Szőnyi, Orthogonally divergent spreads of Hermitian curves. In: *Finite geometry and combinatorics* (*Deinze*, 1992), volume 191 of *London Math. Soc. Lecture Note Ser.*, 17–30, Cambridge Univ. Press 1993. MR 94k:51013 Zbl 0804.51013

[2] A. Barlotti, Un'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital.* (3) **10** (1955), 498–506. MR 17,776b Zbl 0066.38901

[3] A. E. Brouwer, H. A. Wilbrink, Ovoids and fans in the generalized quadrangle $Q(4,2)$. *Geom. Dedicata* **36** (1990), 121–124. MR 91h:51007 Zbl 0716.51007

[4] A. Cossidente, G. Korchmáros, Transitive ovoids of the Hermitian surface of $\mathrm{PG}(3,q^2)$, with q even. *J. Combin. Theory Ser. A.* **101** (2003), 117–130.

[5] A. Gunawardena, Primitive ovoids in $O_8^+(q)$. *J. Combin. Theory Ser. A* **89** (2000), 70–76. MR 2000i:51025 Zbl 0961.51007

[6] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*. Oxford Univ. Press 1985. MR 87j:51013 Zbl 0574.51001

[7] J. W. P. Hirschfeld, *Projective geometries over finite fields*. Oxford Univ. Press 1998. MR 99b:51006 Zbl 0899.51002

[8] W. M. Kantor, R. A. Liebler, The rank 3 permutation representations of the finite classical groups. *Trans. Amer. Math. Soc.* **271** (1982), 1–71. MR 84h:20040 Zbl 0514.20033

[9] P. B. Kleidman, The 2-transitive ovoids. *J. Algebra* **117** (1988), 117–135. MR 89j:51008 Zbl 0652.51013

[10] G. Panella, Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital.* (3) **10** (1955), 507–513. MR 17,776c Zbl 0066.38902

[11] B. Segre, Ovals in a finite projective plane. *Canad. J. Math.* **7** (1955), 414–416. MR 17,72g Zbl 0065.13402

[12] B. Segre, Forme e geometrie hermitiane, con particolare riguardo al caso finito. *Ann. Mat. Pura Appl.* (4) **70** (1965), 1–201. MR 35 #4802 Zbl 0146.16703

[13] J. A. Thas, Ovoids and spreads of finite classical polar spaces. *Geom. Dedicata* **10** (1981), 135–143. MR 82g:05031 Zbl 0458.51010

[14] J. A. Thas, Old and new results on spreads and ovoids of finite classical polar spaces. In: *Combinatorics* '90 (*Gaeta*, 1990), volume 52 of *Ann. Discrete Math.*, 529–544, North-Holland 1992. MR 93h:51005 Zbl 0767.51004

[15] J. A. Thas, Ovoids, spreads and m-systems of finite classical polar spaces. In: *Surveys in combinatorics*, 2001 (*Sussex*), volume 288 of *London Math. Soc. Lecture Note Ser.*, 241–267, Cambridge Univ. Press 2001. MR 2003a:51003 Zbl 0986.51005

[16] J. A. Thas, S. E. Payne, Spreads and ovoids in finite generalized quadrangles. *Geom. Dedicata* **52** (1994), 227–253. MR 95m:51005 Zbl 0804.51007

Received 30 December, 2002

L. Giuzzi, Dipartimento di Matematica, Università degli Studi di Brescia, via Valotti 9, 25133 Brescia, Italy
Email: giuzzi@ing.unibs.it, giuzzi@dmf.unicatt.it

G. Korchmáros, Dipartimento di Matematica, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy
Email: korchmaros@unibas.it