1. Introduction

An ovoid in a 3-dimensional projective geometry $PG(3, q)$ over the field $GF(q)$, where $q$ is a prime power, is a set of $q^3 + 1$ points no three of which are collinear. Because of their connections with other combinatorial structures ovoids are of interest to mathematicians in a variety of fields; for from an ovoid one can construct an inversive plane [3], a generalised quadrangle [11], and if $q$ is even, a translation plane [13]. In fact the only known finite inversive planes are those arising from ovoids in projective spaces (see [2]). Moreover, there are only two classes of ovoids known, namely the elliptic quadric and, for $q$ even and not a square, the Tits ovoids; these will be described in the next section. If the field order $q$ is odd, then it was shown by Barlotti and Panella (see [3, 1.4.50]) that the only ovoids are the elliptic quadrics. This paper contains a geometrical characterisation of the two known classes of ovoids.

For $q > 2$ ovoids in $PG(3, q)$ are sets of points with no three points collinear of maximal size [8, Theorem 16.1.5]. A plane $\pi$ intersects an ovoid $\mathcal{O}$ in a set $\pi \cap \mathcal{O}$ of points with no three points of $\pi \cap \mathcal{O}$ collinear in $\pi$; in fact the set $\pi \cap \mathcal{O}$ either consists of a single point and $\pi$ is called a tangent plane to $\mathcal{O}$, or has size $q + 1$ and $\pi$ is called a secant plane to $\mathcal{O}$ see [8, Lemma 16.1.6]. In the latter case the set $\pi \cap \mathcal{O}$ is an oval of $\pi$. There have been several results which characterise ovoids by the nature of their (secant) plane sections $\pi \cap \mathcal{O}$. The first of these was due to Barlotti [2]; he showed that an ovoid is an elliptic quadric if and only if all of its plane sections are conics. This was later strengthened by Prohaska and Walker [12]; they showed that elliptic quadrics were characterised by the nature of the plane sections of the set of planes on a single secant line. (Note that a line in $PG(3, q)$ is called an external, tangent, or secant line to an ovoid if it meets the ovoid in zero, one or two points respectively.)

**Theorem (Prohaska and Walker).** Let $\mathcal{O}$ be an ovoid of $PG(3, q)$, where $q > 2$ is even. The $\mathcal{O}$ is an elliptic quadric if and only if all the plane sections on a given secant line are conics.

In 1984 Glynn [4] made an extensive investigation of finite inversive planes of even order and showed that such planes are either Miquelian planes (corresponding to elliptic quadrics), Suzuki–Tits planes (corresponding to Tits ovoids), or of Hering type I.1 (in the Hering classification of inversive planes [2]). Glynn gives a new proof of the theorem of Prohaska and Walker and also shows that an ovoid is an elliptic quadric if and only if all the plane sections on a given secant line are conics. He conjectures that the only ovoids with at least one plane section a conic are the elliptic quadrics.

Received 19 September 1994; revised 23 October 1995.

1991 Mathematics Subject Classification 51E20

We also are interested in the nature of the plane sections of ovoids and in this paper we investigate ovoids whose plane sections belong to the class translation ovals (discussed in Section 4), a class which properly contains both the conics and the ovals which arise as plane sections of Tits ovoids. Our main result is the following.

**Theorem.** Let \( \mathcal{O} \) be an ovoid of \( PG(3,q) \) where \( q > 2 \) is even. The \( \mathcal{O} \) is an elliptic quadric or a Tits ovoid if and only if all the plane sections on a given tangent line are translation ovals, and this tangent line is an axis of one of the ovals.

Our approach differs from that of Prohaska and Walker, and Glynn in that it is based on theorems of Segre and Thas (stated in the next section) which show that an ovoid in \( PG(3,q) \), where \( q > 2 \) is even, is a set of \( q^2 + 1 \) points such that no two are perpendicular with respect to a fixed non-degenerate alternating form on the underlying vector space. Thus we may choose an alternating form, and then for each point \( P \) known to be on an ovoid \( \mathcal{O} \), all the points, apart from \( P \), are known not to be on \( \mathcal{O} \). Suppose that we know that a certain plane section \( \pi \cap \mathcal{O} \) is a translation oval. Our efforts to extract information about \( \mathcal{O} \) from \( \pi \cap \mathcal{O} \) using the alternating form led to a problem about translation ovals in a plane. This is discussed in Section 4 where a partial answer, sufficient for our present purposes, is proved (Proposition 4.6, the ‘External Lines Lemma’). This result about ovals in a plane is crucial for our characterisation of ovoid in 3-space.

We remark that our assumption on the plane sections of \( \mathcal{O} \) allows the translation ovals to vary from plane to plane. Also we do not assume that any automorphisms of the translation ovals lift to automorphisms of the ovoid.

In the next section we describe the known classes of ovoids and discuss Segre’s and Thas’ theorems which relate ovoids and alternating forms. Our methods require detailed computation over \( GF(q) \) and in Section 3 we develop the tools we shall need for this. Section 4 contains a description of translation ovals and their representations by coordinates. It also contains the crucial ‘External Lines Lemma’, which allows us later to put together information about two different secant plane sections of an ovoid. We prove the main result about ovoids in Section 5.

### 2. Ovoids and forms: the known examples

The only known ovoids of \( PG(3,q) \) are the elliptic quadrics and the Tits ovoids. We describe these below.

**Definition 2.1.** The elliptic quadrics. The set of all totally singular one-dimensional subspaces of \( GF(q)^4 \) with respect to a non-singular quadratic form of Witt index 1 is an ovoid of \( PG(3,q) \) called the **elliptic quadric**. The set of all elliptic quadrics in \( PG(3,q) \) forms a single orbit of the collineation group \( PGL(4,q) \) of \( PG(3,q) \) and we may take as our canonical form for an elliptic quadric:

\[
\mathcal{O} = \{(t^2 + st + as^2, 1, s, t) \mid s, t \in GF(q)\} \cup \{(1, 0, 0, 0)\},
\]

where \( x^2 + x + a \) is irreducible over \( GF(q) \). (See [9, Theorem 5.2.4, permuting the entries according to (14)(23)].) The stabiliser in \( PGL(3,q) \), of an elliptic quadric, namely \( PO(4,q) \), acts 3-transitively on the points of the elliptic quadric.
Note that in the canonical form above we are identifying the 4-tuple \( x = (x_1, x_2, x_3, x_4) \) of \( \text{GF}(q)^4 \) with a point of \( \text{PG}(3, q) \), that is the 1-dimensional subspace of \( \text{GF}(q)^4 \) generated by \( x \).

The Tits ovoids are related to symplectic generalised quadrangles so we first describe these. The \( \text{Sp}(4, q) \) generalised quadrangle is the incidence structure with points the (totally isotropic) 1-dimensional subspaces of \( \text{GF}(q)^4 \), and lines the totally isotropic 2-dimensional subspaces of \( \text{GF}(q)^4 \) with respect to a non-degenerate alternating form, with incidence given by inclusion. A polarity \( \phi \) of the \( \text{Sp}(4, q) \) generalised quadrangle is an incidence preserving map which interchanges points and lines such that \( \phi^2 \) is the identity map. A point which is incident with its image under \( \phi \) is called an absolute point of \( \phi \). The \( \text{Sp}(4, q) \) generalised quadrangle admits a polarity if and only if \( q = 2^h \) with \( h \) odd (see [11] for details).

**Definition 2.2.** The Tits ovoids. The set of all absolute points of a polarity of the \( \text{Sp}(4, q) \) generalised quadrangle where \( q = 2^h \) for \( h \) odd and \( h > 1 \), form an ovoid of \( \text{PG}(3, q) \), called a *Tits ovoid*. Let \( \sigma \) be an automorphism of \( \text{GF}(q) \) such that \( \sigma^2 \) is the Frobenius automorphism, and since the set of all Tits ovoids in \( \text{PG}(3, q) \) forms a single orbit of the collineation group \( \text{PGL}(4, q) \) of \( \text{PG}(3, q) \), we may then take as our ‘canonical form’ for a Tits ovoid:

\[
\mathcal{O} = \{(t^s + st + s^t s^2, 1, s, t) | s, t \in \text{GF}(q)\} \cup \{(1, 0, 0, 0)\}
\]

(see [8, Theorem 16.4.5, permuting the entries according to (1 4)(2 3)])]. The stabiliser in \( \text{PGL}(4, q) \) of a Tits ovoid, namely the Suzuki group \( \text{Sz}(q) \), acts 2-transitively on the points of the Tits ovoid.

The link between ovoids in \( \text{PG}(3, q) \) and forms on the underlying vector space \( \text{GF}(q)^3 \) is fundamental for our approach to studying ovoids and is explained via the theorems of Segre and Thas stated below. The statement of Segre’s theorem below involves some knowledge about ovals in \( \text{PG}(2, q) \). Recall that an *oval* is a set of \( q + 1 \) points of \( \text{PG}(2, q) \), no three collinear. For \( q \) odd, an oval is a subset of points, no three collinear, of maximal size, while for \( q \) even when the maximal size of such a set if \( q + 2 \). In fact when \( q \) is even any oval can be extended uniquely to such a maximal set by adding a further point and the uniquely determined extra point is called the *nucleus* of the oval (see [9, Corollary to 8.1.4]).

**Theorem 2.3** [2, 1.4.54]. Let \( \mathcal{O} \) be an ovoid of \( \text{PG}(3, q) \) where \( q \) is even and \( q > 2 \). Then \( \mathcal{O} \) determines a symplectic polarity \( \sigma \) of \( \text{PG}(3, q) \) which interchanges each tangent plane of \( \mathcal{O} \) with its point of tangency, and each secant plane \( \pi \) of \( \mathcal{O} \) with the nucleus of the oval \( \mathcal{O} \cap \mathcal{O} \) of \( \mathcal{O} \).

**Corollary to 2.3.** For distinct points \( P_1 \) and \( P_2 \), we have that \( P_1 \) is incident with \( P_2 \) if and only if the line \( P_1 P_2 \) is tangent to \( \mathcal{O} \).

**Proof of Corollary.** This is clear if \( P_2 \) lies on \( \mathcal{O} \) since in that case \( P_2 \) is the tangent plane to \( \mathcal{O} \) at \( P_2 \). If \( P_2 \) is not on \( \mathcal{O} \) then \( P_2 \) is the nucleus of the oval \( \mathcal{O} \cap \mathcal{O} \). Thus every line on \( P_2 \) in the plane \( P_2 \) is tangent to \( \mathcal{O} \) and hence a tangent to \( \mathcal{O} \). Conversely if \( P_1 P_2 \) is tangent to \( \mathcal{O} \) at \( Q \), say, then we have just shown that \( P_2 \) is incident with \( Q \) and hence \( Q \) is incident with \( P_2 \); thus the line \( P_1 P_2 = P_2 Q \) lies in \( P_2 \) so \( P_1 \) is incident with \( P_2 \).
It follows from Segre’s Theorem 2.3 that an ovoid \( \mathcal{O} \) of \( \text{PG}(3, q) \) with \( q \) even, \( q > 2 \), determines, up to a scalar multiple, a non-degenerate alternating form \( \langle \cdot, \cdot \rangle \) on \( \text{GF}(q)^3 \) such that for each point \( P = \langle v \rangle \), where \( v \) is a non-zero element of \( \text{GF}(q)^4 \), the ‘perp’ \( P^\perp = \langle w | \langle v, w \rangle = 0 \rangle \) of \( P \) is equal to \( P^\perp \). Details of this is given in [3, 1.4.38]. We note that the form is unique up to a scalar multiple since the perps for all points on \( \mathcal{O} \) are determined by \( \mathcal{O} \) and hence the perps for five points, no four coplanar are determined.

It follows from the corollary that two points are perpendicular with respect to this form if and only if they lie on a tangent line to the ovoid. In particular, no two points of the ovoid are perpendicular. A converse to this statement also holds.

**Theorem 2.4** (Thas [13]). A set of \( q^2 + 1 \) points of \( \text{PG}(3, q) \), with \( q \) even and \( q > 2 \), such that no two are perpendicular with respect to a fixed non-degenerate alternating form is an ovoid of \( \text{PG}(3, q) \).

Thus the study of ovoids of \( \text{PG}(3, q) \), where \( q \) is even and \( q > 2 \), is equivalent to the study of sets \( q^2 + 1 \) points of \( \text{PG}(3, q) \) such that no two are perpendicular with respect to a fixed non-degenerate alternating form on the underlying \( \text{GF}(q)^4 \).

3. Computation in \( \text{GF}(q) \): the trace map and an exponential version

We shall need to compute within the field \( \text{GF}(q) \) for \( q \) even, with functions \( f: \text{GF}(q) \to \text{GF}(q) \), and with the trace map, \( \text{trace}: \text{GF}(q) \to \text{GF}(q) \). In this section we develop the computational tools we shall use later in the paper. It will prove to be very convenient to use an exponential notation for functions \( f \) of the form \( f: x \mapsto x^n \) with \( n \) an integer, that is, for monomial functions. We set this up as follows for \( q = p^h \) with \( p \) any prime.

The natural map from polynomials to polynomial functions is a ring homomorphism from \( \text{GF}(q)[x] \) onto the ring of all functions \( \text{GF}(q) \to \text{GF}(q) \) (with pointwise operations) with kernel the principal ideal generated by \( x^q - x \). It follows that, for integers \( m \) and \( n \) the polynomials \( x^m \) and \( x^n \) map to the same function if and only if either \( m = n = 0 \) or both \( m \) and \( n \) are non-zero and \( m \equiv n \) (mod \( q - 1 \)). For this reason we set \( Z_{q-1} = \{1, 2, \ldots, q-1\} \).

3.1. The exponential version

For \( n \in Z_{q-1} \) we denote the functions \( x \mapsto x^n \) (for \( x \) in \( \text{GF}(q) \)) by \( n \). With this convention, for \( m, n \in Z_{q-1} \) we denote by \( m + n \) the pointwise product of the functions \( x \mapsto x^m \) and \( x \mapsto x^n \), while \( nm \) is their composition. If \( u \) is a unit of \( Z_{q-1} \) we denote its inverse in \( Z_{q-1} \) by \( 1/u \) (since \( Z_{q-1} \) is commutative). Now \( u \) is a unit in \( Z_{q-1} \) if and only if the function \( x \mapsto x^u \) is invertible and in this case \( 1/u \) denotes the inverse function.

The automorphisms of \( \text{GF}(q) \) for \( q = p^h \), are the powers \( p^i \) with \( 1 \leq i < q \), that is, with \( 0 \leq i < h \). The generators \( \alpha \) of the automorphism group \( \text{Aut} \text{GF}(q) \) are the powers \( p^i \) of \( p \) with \( i \) coprime to \( h \). In this case \( \alpha - 1 = p^i - 1 \) is coprime to \( p^h - 1 \) so that \( \alpha - 1 \) is a unit in \( Z_{q-1} \). The product \( \alpha/(\alpha - 1) \) of \( \alpha \) and the inverse \( 1/(\alpha - 1) \) of \( \alpha - 1 \), for \( \alpha \) a generator of the automorphism group, plays a crucial role in our work. Now \( \alpha/(\alpha - 1)-1 = 1/(\alpha - 1) \) is a unit of \( Z_{q-1} \), and

\[
\left( \frac{\alpha}{\alpha - 1} \right) / \left( \frac{\alpha}{\alpha - 1} - 1 \right) = \alpha.
\]
Thus if \( n \in \mathbb{Z}_{q-1} \) is such that \( n-1 \) is a unit in \( \mathbb{Z}_{q-1} \) and if for some \( t \in \text{GF}(q) \) we have

\[
t^\frac{n}{(q-1)} = t^n,
\]

then

\[
t^a = t^{b/(n-1)}.
\]

In particular, if \( \beta \) is also a generator of \( \text{Aut} \text{GF}(q) \) and

\[
t^\frac{\beta}{(q-1)} = t^\beta/(\beta-1)
\]

then

\[
t^a = t^b.
\]

This fact will be useful later in the paper.

Next we introduce the trace map and collect together some of its properties in Proposition 3.2. For \( q = 2^h \) the map trace: \( \text{GF}(q) \rightarrow \text{GF}(2) \) is defined by

\[
\text{trace}(x) = \sum_{0 \leq i < h} x^i \quad \text{for } x \in \text{GF}(q).
\]

**Proposition 3.2.** (1) The trace map is additive, that is, for all \( x, y \in \text{GF}(q) \), we have \( \text{trace}(x+y) = \text{trace}(x) + \text{trace}(y) \).

(2) The trace map is invariant under automorphisms of \( \text{GF}(q) \), that is, for each \( x \in \text{GF}(q) \) and \( \alpha \in \text{Aut} \text{GF}(q) \), we have \( \text{trace}(\alpha x) = \text{trace}(x) \).

(3) The kernel \( K \) of the trace map is a subgroup of \( (\text{GF}(q), +) \) of index 2 and trace has image \( \text{GF}(2) \).

(4) The kernel \( K \) is automorphism invariant, that is, \( K^\alpha = K \) for all \( \alpha \in \text{Aut} \text{GF}(q) \).

(5) There are \( q-1 \) subgroups of \( (\text{GF}(q), +) \) of index 2, namely, \( aK \) for \( a \in \text{GF}(q) \setminus \{0\} \). In particular if \( aK = bK \) then \( a = b \).

(6) The only subgroup of \( (\text{GF}(q), +) \) of index 2 which is automorphism invariant is \( K \).

(7) For \( \alpha \in \text{Aut} \text{GF}(q) \), the set \( \{x + x^\alpha | x \in \text{GF}(q)\} \subseteq K \) with equality if and only if \( \alpha \) generates \( \text{Aut} \text{GF}(q) \).

(8) For \( a, b \in \text{GF}(q) \setminus \{0\} \), and \( \alpha \) a generator of \( \text{Aut} \text{GF}(q) \), we have

\[
\langle at^a + bt^b | t \in \text{GF}(q) \rangle = a^{1/(q-1)} b^{\alpha/(q-1)} K.
\]

(9) For \( a \in \text{GF}(q) \), \( x^2 + x + a \) is irreducible over \( \text{GF}(q) \) if and only if \( \text{trace}(a) = 1 \).

**Proof.** Set \( A = \text{Aut} \text{GF}(q) \). Then for \( x \in \text{GF}(q) \), we have \( \text{trace}(x) = \sum_{\alpha \in A} x^\alpha \).

(1) Since trace is the sum of additive maps trace is itself additive.

(2) For \( \alpha \in A \) we have \( \alpha A = A \) and so for all \( x \in \text{GF}(q) \), we have

\[
\text{trace}(x) = \sum_{\beta \in A} x^{\alpha \beta} = \sum_{\beta \in A} x^\beta = \text{trace}(x).
\]

(3) Since trace(\( x \)), considered as an element of \( \text{GF}(2)[x] \), has degree less than \( q \) it follows that trace: \( \text{GF}(q) \rightarrow \text{GF}(2) \) is not the zero map. Thus, as trace is additive, Part (3) follows.

(4) If \( x \in K \) then \( x^2 \in K \) for \( \alpha \in A \).

(5) The subgroups of \( (\text{GF}(q), +) \) of index 2 can be identified with the hyperplanes of the projective geometry \( \text{PG}(h-1, 2) \) and the multiplicative group \( \text{GF}(q)^* \) of \( \text{GF}(q) \) acts regularly on the points and hence also on the hyperplanes of \( \text{PG}(h-1, 2) \). Thus there are \( q-1 \) such subgroups, each of which is of the form \( aK \) for some \( a \in \text{GF}(q)^* \), and if \( aK = bK \) then \( a = b \).
(6) For \( z \in A \) and \( a \in \text{GF}(q)^\ast \), it follows that \((aK)^\ast = a^2 K^\ast = a^4 K\) and so \((aK)^\ast = aK\) if and only if \((a^4)^\ast = a\) by (5). Thus \(aK\) is automorphism invariant if and only if \((a^4)^\ast = a\) for each \( z \in A \), which in turn holds if and only if \( a \in \text{GF}(2) \setminus \{0\} = \{1\} \), that is, \(aK = K\).

(7) For \( z \in A \) and \( x \in \text{GF}(q) \) it follows from (1) and (2) that \( \text{trace}(x^2 + x^2) = \text{trace}(x) + \text{trace}(x^2) = 0 \), so that \( \{x + x^2 \mid x \in \text{GF}(q)\} \subseteq K \). Now the map \( x \mapsto x + x^2 \) is additive with kernel the fixed field of \( z \), and so the image of this map, 
\[
\{x + x^2 \mid x \in \text{GF}(q)\},
\]
has size \( |K| = q/2 \) if and only if the fixed field of \( z \) is \( \text{GF}(2) \), that is, if and only if \( z \) generates \( A \).

(8) We have
\[
\{a^t + bt \mid t \in \text{GF}(q)\} = a\{t^2 + (a^{-1}b) t \mid t \in \text{GF}(q)\}
\]
\[
= a\{(a^{-1}b)^{(q-1)} s + (a^{-1}b)(a^{-1}b)^{(q-1)} x \mid s, x \in \text{GF}(q)\}
\]
\[
= a^{-1(q-1)} b x^{q-1} \{s^2 + s \mid s, x \in \text{GF}(q)\}
\]
\[
= a^{-1(q-1)} b x^{q-1} \text{K} \quad \text{by Part (7)}.
\]

(9) For \( a \in \text{GF}(q) \), the polynomial \( x^2 + x + a \) is irreducible over \( \text{GF}(q) \) if and only if \( x^2 + x + a \) has no zeros in \( \text{GF}(q) \), which in turn is true if and only if \( a \notin \{x + x^2 \mid x \in \text{GF}(q)\} \). Since the Frobenius map \( x \mapsto x^2 \) generates \( A \), it follows that \( \{x + x^2 \mid x \in \text{GF}(q)\} = K \), and by Part (3), \( a \notin K \) if and only if \( \text{trace}(a) = 1 \).

Part 9 of Proposition 3.2 will prove useful when we are working with the canonical forms for the known ovoids given in Section 2.

**Proposition 3.3.** Suppose that \( \text{trace}\left( \sum_{i=1}^{q-1} a_i x^i \right) = 0 \) for all \( x \in \text{GF}(q) \) with \( q \) even, where trace is the trace map \( \text{GF}(q) \to \text{GF}(2) \). Then, for all \( i \) with \( 1 \leq i \leq q-1 \), we have
\[
\sum_{a \in \text{Aut}(\text{GF}(q))} a_i^{q-1} = 0,
\]
using the exponential convention on the subscripts.

*Proof.* Now
\[
\text{trace}\left( \sum_{i=1}^{q-1} a_i x^i \right) = \sum_{i=1}^{q-1} \text{trace}(a_i, x^i) = \sum_{i=1}^{q-1} \sum_{a \in \text{Aut}(\text{GF}(q))} a_i^{q-1} x^{ia}
\]
\[
= \sum_{j=1}^{q-1} \left( \sum_{a \in \text{Aut}(\text{GF}(q))} a_i^{q-1} \right) x^{ij} \pmod{x^q + x}.
\]
So \( \text{trace}\left( \sum_{i=1}^{q-1} a_i x^i \right) = 0 \) for all \( x \in \text{GF}(q) \) if and only if
\[
\sum_{a \in \text{Aut}(\text{GF}(q))} a_i^{q-1} = 0,
\]
for all \( j \) with \( 1 \leq j \leq q-1 \).

The next four technical lemmas will be used in Section 5 in the characterisation of the known ovoids. Proposition 3.3 is needed for the proof of the first lemma, where it also may help to recall that, for \( q = 2^h \), each positive integer less than \( q \) has a unique binary expansion \( \sum_{0 \leq i < h} a_i 2^i \), where the \( a_i \) are 0 or 1.
Lemma 3.4. Suppose that \( \alpha \) is a generator of \( \text{Aut} \, GF(q) \), where \( q = 2^h \). Then

\[
\text{trace}((x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1) = 0
\]

for all \( x \in GF(q) \) if and only if \( \alpha = 2 \) or \( \alpha^2 = 2 \).

Proof. Suppose that (1) holds for all \( x \in GF(q) \). Since \( \alpha \) generates \( \text{Aut} \, GF(q) \) there is a smallest positive integer \( i \) such that \( \alpha^i = 2 \). Hence \( (\alpha - 1)(1 + \alpha + \cdots + \alpha^{i-1}) = (\alpha^i - 1) = 1 \) and it follows that \( \alpha/(\alpha - 1) = \alpha + \alpha^2 + \cdots + \alpha^i \). Hence

\[
(x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1 = (x+1)^i(x+1)^{\frac{q(x-1)}{2}}(x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1
\]

\[
= (x^i + 1)(x^i + 1)(x^i + 1) + x^{\frac{q(x-1)}{2}} + 1
\]

\[
= \sum x^n,
\]

where the sum is over all \( n \) which are (using the exponential convention) sums of a non-empty proper subset of \( \{ \alpha, \alpha^2, \ldots, \alpha^i \} \). Suppose that \( i > 1 \). We claim that the only powers of \( 2 \) (mod \( q-1 \)) occurring as exponents in this summation are \( \alpha, \alpha^2, \ldots, \alpha^i \). Now \( \alpha = 2^l \) for some \( 1 \leq a < h \) relatively prime to \( h \). Suppose for some \( X = \{k_1, \ldots, k_d\} \subseteq \{1, 2, \ldots, \ell\} \) that \( \sum_{k \in X} 2^{k^2} = 2^j \) (mod \( q-1 \)) for some \( 0 \leq j < h \). There are distinct integers \( l_1, \ldots, l_d \) such that, for each \( 1 \leq m \leq d \), we have \( 0 < l_m < h \) and \( l_m \equiv ak_m \) (mod \( h \)). Then \( \sum_{m=1}^{d} 2^{l_m} = 2^j \) (mod \( q-1 \)), and, as both sides of this congruence lie between 0 and \( q-2 \), we have \( \sum_{m=1}^{d} 2^{l_m} = 2^j \). It follows that \( X = \{k_1\} \) and \( 2^j = 2^h \equiv 2^{\alpha h} = \alpha^j \) (mod \( q-1 \)). Thus there are exactly \( i \) powers of \( 2 \) occurring as exponents in the summation, and by Proposition 3.3 this number \( i \) must be even.

Now suppose that \( i > 2 \). We claim that the only sums of two powers of \( 2 \) of the form \( 2^j + 2^{j+a} \), where \( 0 \leq j < h \) and \( \alpha = 2^a \), occurring as exponents in the summation are \( \alpha + \alpha^2, \alpha^2 + \alpha^3, \ldots, \alpha^{i-1} + \alpha^i \). With the notation of the previous paragraph suppose that

\[
\sum 2^{l_m} = \sum 2^{ak_m} = 2^j + 2^{j+a} = 2^j + 2^j \pmod{q-1},
\]

where \( j + a \equiv l \) (mod \( h \)) for \( 0 \leq l < h \). We deduce as above that \( X = \{k_1, k_2 = k_1 + 1\} \) with \( 2^j = \alpha^j \) and \( 2^{j+a} = \alpha^{j+1} \), proving our claim. By Proposition 3.3 the number \( i-1 \) of terms of the form \( \alpha^j + \alpha^{j+1} \) must be even. This is a contradiction. Hence \( i \leq 2 \), that is \( \alpha = 2 \) or \( \alpha^2 = 2 \).

Conversely if \( \alpha = 2 \) then \( \alpha/(\alpha - 1) = 2 \), so \( (x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1 = (x+1)^i + x^i + 1 = x^i + 1 + x^i + 1 = 0 \) and hence \( \text{trace}((x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1) = 0 \) for all \( x \in GF(q) \). Similarly if \( \alpha^2 = 2 \) then \( \alpha/(\alpha - 1) = \alpha + \alpha^2 = \alpha + 2 \), so

\[
(x+1)^{\frac{q(x-1)}{2}} + x^{\frac{q(x-1)}{2}} + 1 = (x+1)^{i+2} + x^{i+2} + 1
\]

\[
= (x^i + 1)(x^i + 1)(x^i + 1) + x^i + 1 + x^i + 1 = x^i + x^i.
\]

for all \( x \in GF(q) \) we have \( \text{trace}(x^2 + x^2) = \text{trace}(x^3) + \text{trace}(x^3) = \text{trace}(x) + \text{trace}(x) = 0 \).
Lemma 3.5. Let $q = 2^h$ and let $n$ be a positive integer. If for some $a \in \text{GF}(q) \setminus \{0\}$ either
(1) $\text{trace}(ax^n) = 0$ for all $x \in \text{GF}(q)$, or
(2) $\text{trace}(ax^n) = 1$ for all $x \in \text{GF}(q) \setminus \{0\}$,
then for some integer $i$ with $0 < i < h$ it follows that $n(2^i - 1) \equiv 0 \pmod{q - 1}$.

Proof. (1) By Proposition 3.3, $nx \equiv n \pmod{q - 1}$, for some $\alpha \in \text{Aut GF}(q)$ with $\alpha \neq 1$.
(2) If trace$(b) = 1$, then trace$(ax^n + bx^{n-1}) = 0$, for all $x \in \text{GF}(q)$. So, by Proposition 3.3, $nx \equiv n \pmod{q - 1}$, for some $\alpha \in \text{Aut GF}(q)$ with $\alpha \neq 1$.

Lemma 3.6. Suppose that $q$ is even and $\alpha$ is a generator of $\text{Aut GF}(q)$. If $\alpha/(\alpha - 1)$ is an automorphism then $\alpha$ is the Frobenius map, that is, $\alpha = 2$.

Proof. Since $\alpha$ generates $\text{Aut GF}(q)$ there is a smallest integer $i$ for which $\alpha^i = 2$. Then $x/\alpha = 2$ whence $1/(\alpha - 1) = 1 + x + \cdots + x^{i-1}$. Thus $\alpha/(\alpha - 1) = \alpha + \alpha^2 + \cdots + \alpha^i$. Now $\alpha/(\alpha - 1)$ is an automorphism if and only if, using the exponential convention, $\alpha/(\alpha - 1)$ is congruent to a power of 2 modulo $q - 1$, and $\alpha + \alpha^2 + \cdots + \alpha^i$ is congruent to a power of 2 modulo $q - 1$ if and only if $i = 1$ (arguing as in the proof of Lemma 3.4), that is, $\alpha = 2$.

Lemma 3.7. Let $\alpha$ and $\beta$ be generators of $\text{Aut GF}(q)$, where $q = 2^h$, and suppose that either
(1) $(\alpha/(\alpha - 1) - \beta/(\beta - 1))(2^i - 1) \equiv 0 \pmod{q - 1}$, or
(2) $(\alpha/(\alpha - 1) - \beta)(2^i - 1) \equiv 0 \pmod{q - 1}$
for some $i$ with $0 < i < h$. Then $\alpha = \beta$ and in Case (2), $\alpha = 2$.

Proof. Since $\alpha$ generates $\text{Aut GF}(q)$ it follows that $\alpha = 2^j$ for some $0 < j < h$ relatively prime to $h$. Thus $\alpha - 1 = 2^j - 1$ is a unit in $\mathbb{Z}_{2^h-1}$, and similarly $\beta - 1$, and hence $(\alpha - 1)(\beta - 1)$, are units in $\mathbb{Z}_{2^h-1}$. Suppose that (1) holds. Then, multiplying by $(\alpha - 1)(\beta - 1)$ we have $(\beta - \alpha)(\beta - 1) \equiv 0 \pmod{q - 1}$, and hence $\beta^2 + \alpha \equiv \alpha^2 + \beta \pmod{q - 1}$. By the uniqueness of the binary expression, $(\beta^2, \alpha) = (\alpha^2, \beta)$ (interpreting $\beta^2$ and $\alpha^2$ as powers of 2 less than $q$). Since $\alpha \neq \alpha^2$ it follows that $\alpha = \beta$.

Now suppose that (2) holds. Then multiplying by $(\alpha - 1)$ gives $(\alpha + \beta - \alpha \beta)(\alpha - 1) \equiv 0 \pmod{q - 1}$. Hence $\alpha^2 + \beta^2 + \alpha \beta \equiv \alpha + \beta + \alpha \beta^2 \pmod{q - 1}$, and we interpret each side of this congruence as a sum of three positive powers of 2, each less than $q$. If, on each side, the three terms were distinct powers of 2, then we would have $\{\alpha^2, \beta^2, \alpha \beta\} = \{\alpha, \beta, \alpha \beta^2\}$, but this is not the case since $\alpha \beta$ does lie in the second set. Thus on at least one side of the congruence two of the terms are equal. It follows that either $\alpha = \beta$ or one of $\alpha$ and $\beta$ lies in $\{2^i, 2^{h-i}\}$. In the latter case, as $\alpha$ and $\beta$ generate $\text{Aut GF}(q)$, the integer $i$ must be relatively prime, so $\alpha/(\alpha - 1) \equiv \beta(\mod q - 1)$; by Lemma 3.6, $\alpha = \beta = 2$. In the former case the congruence becomes $\alpha^2 + \alpha \beta \equiv 2\alpha + \alpha^2 2^i \pmod{q - 1}$, so $\{\alpha^2 + \alpha \beta, \alpha^2\} = \{2\alpha, \alpha^2 2^i\}$ and hence $\alpha = 2$.

4. Translation ovals

We recall that an oval in $\text{PG}(2,q)$ is a set of $q + 1$ points, no three collinear. An important class of ovals is the class of conics. (A conic is the set of all totally singular one dimensional subspaces of $\text{GF}(q)^2$ with respect to a non-singular quadratic form, see [7, Lemma 7.2.3]...) In 1955 Segre (see [7, Theorem 8.2.47]) proved that for $q$ odd
every oval in $\text{PG}(2,q)$ is a conic. However for $q$ even the ovals of $\text{PG}(2,q)$ have not been classified. One important class which includes the conics is the class of translation ovals and it is this class which we use in this paper.

**Definition 4.1.** A translation oval $\mathcal{O}$ of $\text{PG}(2,q)$ with $q$ even, is an oval which is invariant under a group $E$ of elations of order $q$ such that all the elations in $E$ have a common axis $l$. (An elation $\sigma$ of $\text{PG}(2,q)$ is a collineation such that, for some incident point $p$ and line $l$, the collineation $\sigma$ fixes all points of $l$ and all lines on $p$; in addition $p$ is called a centre of $\sigma$ and $l$ is called an axis of $\sigma$.) The line $l$ is a tangent to $\mathcal{O}$ and is called an axis of $\mathcal{O}$.

For a conic $\mathcal{O}$ every tangent line to $\mathcal{O}$ is an axis (that is an axis of a suitable elation group of order $q$), and indeed any translation oval with at least two axes is a conic (see [7]). On the other hand there are many translation ovals which are not conics, and hence which have exactly one axis. We need some notation to facilitate their description.

**Definition 4.2.** The $D$ notation. For $f : \text{GF}(q) \to \text{GF}(q)$ set

$$D(f) = \{(1,t,f(t)) \mid t \in \text{GF}(q)\} \cup \{(0,0,1)\}.$$ 

Here the triples $(1,t,f(t))$ and $(0,0,1)$ denote points of $\text{PG}(2,q)$ (that is, 1-dimensional subspaces of $\text{GF}(q)^3$). We shall denote elements of $\text{GF}(q)^3$ by column vectors

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = [x_1,x_2,x_3]' .$$

A matrix $M \in \text{GL}(3,q)$ will then induce a map $M : \text{GF}(q)^3 \to \text{GF}(q)^3$ by $v \mapsto Mv$, which in turn will induce a map $M : \text{PG}(2,q) \to \text{PG}(2,q)$ which is a collineation.

**Theorem 4.3** (Payne [10]). Let $\mathcal{O}$ be an oval of $\text{PG}(2,q)$, where $q$ is even, and let $l$ be a tangent line to $\mathcal{O}$. Then the following are equivalent.

1. The oval $\mathcal{O}$ is a translation oval with axis $l$.
2. There is a collineation of $\text{PG}(2,q)$ which maps $\mathcal{O}$ to $D(\alpha)$ and $l$ to $\{(0,x,y) \mid x,y \in \text{GF}(q)\}$.

3. There is a collineation of $\text{PG}(2,q)$ induced by a matrix in $\text{GL}(3,q)$ which maps $\mathcal{O}$ to $D(\alpha)$ and $l$ to $\{(0,x,y) \mid x,y \in \text{GF}(q)\}$ for some generator $\alpha$ of $\text{Aut} \text{GF}(q)$.

4. If $P_1$, $P_2$, $P_3$, $P_4$ are four points of $\mathcal{O}$ not on $l$, and if $P_1P_2 \cap P_3P_4 \subseteq l$ then $P_1P_3 \cap P_2P_4 \subseteq l$.

(To see that (1) and (4) are equivalent, apply the results concerning existence of elations in Hall [5].)

Part 4 of the theorem is of interest only in that it provides a synthetic definition of a translation oval. The automorphism $\alpha$ is uniquely determined by $\mathcal{O}$ and is called the automorphism associated with $\mathcal{O}$. Indeed translation ovals with different automorphisms lie in different orbits under the action of the collineation group of
PG(2, q). For $\mathcal{C}$ a conic, the automorphism associated with $\mathcal{C}$ is the Frobenius automorphism $x = 2$ and so the class of conics in PG(2, q) is the orbit containing $D(2)$. Next we record some information about the stabiliser in $\text{GL}(3, q)$ of a translation oval $D(x)$. The proof is straightforward computation and is omitted.

**Lemma 4.4.** Let $x$ be a generator of $\text{Aut} \, GF(q)$, where $q$ is even, and let $G$ be the stabiliser of $D(x)$ in $\text{GL}(3, q)$. Then $G$ has subgroups

$$D = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t^2 \end{bmatrix} \mid t \in GF(q) \setminus \{0\} \right\}, \quad E = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ 0 & t^2 & 0 \end{bmatrix} \mid t \in GF(q) \right\}.$$  

(1) The subgroup $E$ is an elation group of order $q$ with axis

$$l = \{[0, x, y] \mid x, y \in GF(q)\}.$$  

(2) The orbits of the group $\langle D, E \rangle$ generated by $D$ and $E$ on the points of PG(2, q) are

$$\Delta_1 = \{(0, 1, 0)\} \quad \text{(the nucleus of } D(x)),$$

$$\Delta_2 = \{(0, 0, 1)\} \quad \text{(the point of } D(x) \text{ on the axis } l),$$

$$\Delta_3 = \{(0, 1, t) \mid t \in GF(q) \setminus \{0\}\} \quad \text{(the other } q-1 \text{ points of } l),$$

$$\Delta_4 = \{(1, t, t^2) \mid t \in GF(q)\} \quad \text{(the other } q \text{ points of } D(x),$$

and

$$\Delta_5 \quad \text{the remaining } q^2-q \text{ points.}$$

In order to use this information about $D(x)$ we examine images of translation ovals under collineations of PG(2, q).

**Lemma 4.5.** Suppose that $\mathcal{C}$ is a translation oval of PG(2, q) for $q$ even, with associated automorphism $x$ and containing the point $(0,0,1)$. Let the line $l = \{[0, x, y] \mid x, y \in GF(q)\}$.

(1) Suppose that $\mathcal{C}$ has nucleus $(0, 1, 0)$. Then $\mathcal{C} = D(f)$ for some $f: GF(q) \to GF(q)$. If $l$ is an axis of $\mathcal{C}$ then $f(t) = a + bt^q$ for some $a, b \in GF(q)$ with $b \neq 0$, while if $l$ is not an axis of $\mathcal{C}$ then $f(t) = a + bt(t+c)^{q(q-1)}$ for some $a, b, c \in GF(q)$ with $b \neq 0$.

(2) Suppose that $\mathcal{C}$ has nucleus $(0, 1, a)$ for some $a \in GF(q) \setminus \{0\}$, and that $l$ is an axis of $\mathcal{C}$. Then $\mathcal{C} = D(f)$, where

$$f(t) = c + at + bt^q$$

for some $b, c \in GF(q)$ with $b \neq 0$.

**Proof.** (1) By Theorem 4.3 there is a matrix $M \in \text{GL}(3, q)$ such that $M(D(x)) = \mathcal{C}$. Since $M$ maps the nucleus $(0, 1, 0)$ of $D(x)$ to the nucleus of $\mathcal{C}$ we have

$$M \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ e \\ 0 \end{bmatrix}$$

for some non-zero $e$ in $GF(q)$. Suppose that $l$ is an axis of $\mathcal{C}$. If $\mathcal{C}$ is a conic the stabiliser of $\mathcal{C}$ is transitive on tangent lines to $\mathcal{C}$ so we may assume that $M$ fixes $l$. On
the other hand if \( \mathcal{C} \) is not a conic, then \( l \) is the unique axis of both \( D(z) \) and \( \mathcal{C} \) and again \( M \) fixes \( l \). Thus \( M \) fixes \( l \) and since \((0,0,1)\) is the point of intersection of \( l \) and \( D(z) \), and also of \( l \) and \( \mathcal{C} \), it follows that

\[
M = \begin{bmatrix}
0 \\
0 \\
1
\end{bmatrix} = \begin{bmatrix}
0 \\
0 \\
g
\end{bmatrix}
\]

for some non-zero \( g \) in \( \text{GF}(q) \). Further the \((1,1)\) entry of \( M \) must be non-zero since \( M \) fixes \( l \), and, since all scalar matrices in \( \text{GL}(3,q) \) act trivially on \( \text{PG}(2,q) \), we may assume that the \((1,1)\) entry of \( M \) is 1. Thus for some \( d, h \in \text{GF}(q) \) we have

\[
M = \begin{bmatrix}
1 & 0 & 0 \\
d & e & 0 \\
h & 0 & g
\end{bmatrix}.
\]

Then \( M \) maps the point \((1,t,t^2)\) to the point \((1,d+et, h+gt^2)\). Setting \( s = d+et \) we have \( t = e^{-1}(s+d) \) so that \( h+gt^2 = h+g(e^{-1}d)^3+ge^{-s}s^2 \). Then setting \( a = h+g(e^{-1}d)^3 \) and \( b = ge^{-s} \) we obtain

\[
M(D(z)) = \{(1,s,a+bs^2) | s \in \text{GF}(q)\} \cup \{(0,0,1)\}.
\]

Suppose \( l \) is not an axis of \( \mathcal{C} \). Then \( M \) maps the point \((1,t,t^2)\) of \( D(z) \) to \((0,0,1)\) for some \( t \in \text{GF}(q) \). Set

\[
L = \begin{bmatrix}
1 & 0 & 0 \\
t & 1 & 0 \\
1 & 0 & 0
\end{bmatrix}.
\]

Then \( ML^{-1} \) fixes the points \((0,1,0)\) and \((0,0,1)\) and therefore, on multiplying by a scalar matrix if necessary, we have

\[
ML^{-1} = \begin{bmatrix}
1 & 0 & 0 \\
c & e & 0 \\
a & 0 & g
\end{bmatrix},
\]

for some \( a, c, e, g \in \text{GF}(q) \) with \( e \) and \( g \) non-zero. So

\[
M(D(z)) = ML^{-1}(L(D(z)))
\]

\[
= ML^{-1}(((s^3+t^2, s+t, 1) | s \in \text{GF}(q)) \cup \{(0,0,1)\})
\]

\[
= ML^{-1}(((u^2, u, 1) | u \in \text{GF}(q)) \cup \{(0,0,1)\})
\]

\[
= ML^{-1}(((1,v,v^{2/(q-1)}) | v \in \text{GF}(q)) \cup \{(0,0,1)\}) \quad \text{(on setting } v = u^{1-2})
\]

\[
= \{(1,c+ev, a+ge^{2/(q-1)}) | v \in \text{GF}(q)\} \cup \{(0,0,1)\}
\]

\[
= \{(1,w,a+g((e^{-1}(w+c))^{2/(q-1)}) | w \in \text{GF}(q)\} \cup \{(0,0,1)\}.
\]

Thus setting \( b = ge^{-2/(q-1)} \) we have \( M(D(z)) = D(f) \) with \( f(w) = a+b(w+c)^{2/(q-1)} \).

(2) This part follows from part (1) on applying the matrix

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & a & 1
\end{bmatrix}.
\]
We complete this section by discussing and proving the External Lines Lemma (Proposition 4.6), which allows us to put together information about two different secant plane sections of an ovoid. Suppose that $\mathcal{O}$ is an ovoid in $PG(3, q)$ for $q$ even, with associated non-degenerate alternating form as described in Section 2. Further suppose, as is the case in this paper, that we have a secant plane $\pi$ such that $\pi \cap \mathcal{O}$ is a known oval. Let $N$ be the nucleus of $\pi \cap \mathcal{O}$ so that $N = N'$. If $\pi'$ is a secant plane to $\mathcal{O}$ on $N$, distinct from $\pi$, then $\pi \cap \pi'$ is the tangent line to the oval $\pi \cap \mathcal{O}$ on $N$ (for every line in $\pi$ on $N$ is a tangent line to $\pi \cap \mathcal{O}$ and hence to $\mathcal{O}$). Let $P$ be a point on $\pi \cap \mathcal{O}$ but not in $\pi'$. Then $P^\perp$ is the tangent plane to $\mathcal{O}$ at $P$ and hence contains the tangent line to $\pi \cap \mathcal{O}$ at $P$ which in turn contains the point $N$. Thus $P^\perp \cap \pi'$ is a line in $\pi'$ on $N$. Since $P^\perp$ meets $\mathcal{O}$ only in the point $P$ and since $P$ is not in $\pi'$ it follows that $P^\perp \cap \pi'$ is an external line to $\mathcal{O}$.

For each of the $q + 1$ lines $l$ in $\pi'$ on $N$ the line $l^\perp$ lies in $N^\perp = \pi$ and contains $(\pi')^\perp = N'$, the nucleus of $\pi' \cap \mathcal{O}$. Similarly for each of the $q + 1$ lines $l$ in $\pi$ on $N'$ the line $l^\perp$ is a line in $\pi'$ on $N$. Since $N' = (\pi')^\perp \neq \pi' = N$, there are exactly $q/2$ (secant) lines $l$ in $\pi$ on $N'$ meeting $\pi \cap \mathcal{O}$ in points off $\pi \cap \pi'$ (for $\pi \cap \pi'$ is a tangent line to $\mathcal{O}$), and the perps $l^\perp$ of these lines form a set of $q/2$ lines in $\pi'$ on $N$.

We showed above that each of these lines $l^\perp$ is external to $\pi' \cap \mathcal{O}$ (consider the point $P$ in the previous paragraph to lie in $l \cap \mathcal{O}$). Thus the set:

$$\{P^\perp \cap \pi' \mid P \in \pi \cap \mathcal{O}, P \not\in \pi'\}$$

of $q/2$ lines is the complete set of lines of $\pi'$ on $N$ which are external to $\mathcal{O}$.

To determine all possibilities for the oval $\pi \cap \mathcal{O}$ we must answer the following question about $PG(2, q)$.

Suppose that we are given a point $N$ of $PG(2, q)$ with $q$ even, a set $S$ of $q/2$ lines on $N$, and a point $M$ distinct from $N$ and not on any lines of $S$. Which ovals have $M$ as nucleus and $S$ as their set of external lines on $N$?

A partial answer to this question for translation ovals is given in Proposition 4.6, the External Lines Lemma. This result is the key to our later results. A better answer to the question above would lead to more general characterisations of ovoids, and perhaps even to new constructions of ovoids.

**Proposition 4.6 (The External Lines Lemma).** Let $\mathcal{O}$ be a translation oval of $PG(2, q)$ for $q$ even, with nucleus $N$, and let $l$ be an axis of $\mathcal{O}$. Let $P$ be the point of $\mathcal{O}$ on $l$ and let $Q$ be another point of $l$, distinct from $P$ and $N$. Suppose that $\mathcal{O}'$ is a translation oval containing $P$ such that its nucleus $N'$ is a point on $l$ distinct from $Q$. If every line on $Q$ external to $\mathcal{O}$ is also external to $\mathcal{O}'$ then $l$ is an axis of $\mathcal{O}'$.

**Proof.** By Theorem 4.3 we may assume that $\mathcal{O}$ is $D(z)$ (hence that the nucleus $N$ is $(0, 1, 0)$, that $l$ is $[0, x, y]^T$ $x, y \in GF(q)$), (and hence that $P$ is $(0, 0, 1)$), and that there is a matrix $M$ taking $\mathcal{O}'$ to $D(\beta)$, where $z$ and $\beta$ are generators of $\text{Aut} GF(q)$. Also, since by Lemma 4.4 the $q − 1$ points of $l$ distinct from $P$ and $N$ form an orbit of the stabiliser of $D(z)$ in $PG(2, q)$, we may assume that $Q = (0, 1, 1)$. If the image $MQ$ of $Q$ lies on $l$ then, as $M$ maps $N'$, the nucleus of $\mathcal{O}'$, to $N = (0, 1, 0)$, the nucleus of $D(\beta)$, it follows that $M$ maps $l$ (which is the line on $N'$ and $Q$) to the line on $N$ and $MQ$, that is $ML = l$. Thus if $MQ$ lies on $l$ then, as $l$ is an axis of $D(\beta)$, $l$ is an axis of $\mathcal{O}'$.

Assume then that $MQ$ is not on $l$. Since by Lemma 4.4 the set of all points not on $l$ or $D(\beta)$ is an orbit of the stabiliser of $D(\beta)$ in $GL(3, q)$ we may assume that $MQ$ is $(1, 1, 0)$. 
Now a line on \( Q \) external to \( \mathcal{O} \) is of the form

\[
l_a = \{[x_1, x_2, x_3] \mid ax_1 + x_2 + x_3 = 0\}
\]

with \( a \neq X = \langle t + t^e \mid t \in GF(q) \rangle \), that is, \( a \neq K \), the kernel of the trace map, by Proposition 3.2(7). Similarly a line on \( MQ = (1, 1, 0) \) external to \( D(\beta) \) is of the form

\[
m_b = \{[x_1, x_2, x_3] \mid x_1 + x_2 + bx_3 = 0\}
\]

with \( b \neq \{t^e + t^e \mid t \in GF(q) \} \). We have

\[
M[l_a \mid a \neq K] = \{m_b \mid b \neq X\}
\]

since the lines on \( Q \) external to \( \mathcal{O} \) are external to \( \mathcal{O}' \).

Now as \( N' \) is a point on \( l \) distinct from \( P \) and \( Q \), we have \( N' = (0, 1, c) \) for some \( c \neq 1 \). Moreover \( M \) maps \( N' \) to \( N = (0, 1, 0), Q = (0, 1, 1) \) to \( MQ = (1, 1, 0) \) and \( P = (0, 0, 1) = l \cap \mathcal{O}' \), to \( MI \cap D(\beta) = (1, 0, 0) \) (since \( MI \) is the line on \( N = MN' \) and \( MQ \)).

It follows that

\[
M = \begin{bmatrix}
    m_{11} & m_{12} & m_{13} \\
    m_{21} & m_{22} & 0 \\
    m_{31} & 0 & 0
\end{bmatrix}
\]

for some \( m_i \in GF(q) \) with \( m_{22} = m_{12} + m_{13} \) and \( m_{12} + cm_{13} = 0 \). Now \( M \) maps \( l_a \) to \( m_b \) where \( b = (m_{11} + m_{13})/m_{31}, e = (m_{11} + m_{21})/m_{31}, \) noting that \( m_{31} \) is non-zero since \( M \) is non-singular. Then \( M \) maps \( l_a \) to \( m_b \) where \( b = da + e \). Hence \( X = dK + e \).

Now \( 0 \in X \) (since \( m_0 \) contains \( P \)) and so \( d^{-1} e \in K \). Then by Proposition 3.2(5) we have \( X = dK \). Moreover by definition \( X = \{t^e + t^e \mid t \in GF(q) \} \), which is invariant under \( \text{Aut} \, GF(q) \), and hence by Proposition 3.2(6), \( X = K \). It follows from Proposition 3.3 that \( \beta / (\beta - 1) \) is an automorphism, and then from Lemma 3.6 that \( \beta = 2 \). Thus \( \mathcal{O}' \) is a conic and all tangent lines are axes. In particular \( l \) is an axis of \( \mathcal{O}' \).

**Remark 4.7.** The hypothesis that \( \mathcal{O}' \) be a translation oval in Proposition 4.6 is necessary, as shown by the Lunelli-Sce oval in \( PG(2, 16) \) [9].

5. Ovoids

As a consequence of Theorem 2.3 and 2.4 ovoids are closely connected with alternating forms. Our aim is to use partial knowledge of an ovoid to gain information about the whole ovoid. For this we exhibit the form explicitly. Suppose that \( \mathcal{O} \) is an ovoid in \( PG(3, q) \) with \( q \) even, and \( P_1, P_2, P_3, P_4 \) are four points not lying together in a plane such that the lines \( P_1P_3, P_2P_3, P_2P_4 \) and \( P_1P_4 \) are tangent lines of \( \mathcal{O} \).

Then, by the Corollary to Theorem 2.3 and the remarks following it, \( P_1 \perp P_2 \perp P_3 \perp P_4 \) with respect to the form determined by \( \mathcal{O} \). There is a collineation \( \mu \) taking \( P_1 \) to \( (1, 0, 0, 0) \), \( P_2 \) to \( (0, 1, 0, 0) \), \( P_3 \) to \( (0, 0, 1, 0) \) and \( P_4 \) to \( (0, 0, 0, 1) \). The image of \( \mathcal{O} \) under this collineation determines, up to a scalar multiple, the form

\[(x, y) = ax_1y_2 + ax_2y_1 + bx_3y_4 + bx_4y_3\]

for some \( a, b \in GF(q) \), since with respect to this form we have

\[\mu(P_i) \perp \mu(P_j) \perp \mu(P_k) \perp \mu(P_l)\]

and the form is alternating. By working a little harder we can obtain a better result and this is the content of the following somewhat technical lemma.
Lemma 5.1. Suppose that \( \mathcal{O} \) is an ovoid of PG(3, q) with \( q \) even, and that \( \pi \) is a plane such that \( \pi \cap \mathcal{O} \) is a translation oval. Let \( P_3 \) be the nucleus of \( \pi \cap \mathcal{O} \) and let \( P_1 \) be a point such that \( l = P_1 P_3 \) is an axis of \( \pi \cap \mathcal{O} \). Finally let \( P' \) be a plane on \( P_1 \) but not on \( P_3 \). Then there is a collineation \( \mu \) taking \( P_1 \) to \((0,0,0,0)\), \( P_3 \) to \((0,0,0,1)\), \( \pi \) to

\[
\{[x_1, x_2, 0, x_3] \mid x_1, x_2, x_3 \in GF(q)\},
\]

and \( \pi' \) to

\[
\{[x_1, x_2, x_3, 0] \mid x_1, x_2, x_3 \in GF(q)\},
\]

such that \((0,1,0,0)\) and \((1,1,0,1)\) lie in \( \mu(\pi \cap \mathcal{O}) \), and the alternating form determined, up to scalar multiple, by \( \mu(\mathcal{O}) \) is

\[
(x,y) = x_1 y_2 + x_2 y_1 + x_3 y_4 + x_4 y_3.
\]

(Recall that elements of \( GF(q)^4 \) are denoted by column vectors \([x_1, x_2, x_3, x_4]^t\) while points of \( PG(3,q) \), that is, 1-dimensional subspaces of \( GF(q)^4 \), are denoted by 4-tuples \((x_1, x_2, x_3, x_4)\).

Proof. The unique tangent line in \( \pi \) to \( \pi \cap \mathcal{O} \) on \( P_3 \) is \( l = P_1 P_3 \) since \( P_3 \) is the nucleus of \( \pi \cap \mathcal{O} \). So \( \pi \cap \pi' \) is a secant line to \( \mathcal{O} \) and hence \( \pi' \) is a secant plane to \( \mathcal{O} \).

Let \( P_3 \) be the nucleus of \( \pi' \cap \mathcal{O} \) and let \( P_4 \) be the point different from \( P_1 \) at which the line \( \pi \cap \pi' \) meets \( \mathcal{O} \). Let \( P_{124} \) be a point of \( \pi \cap \mathcal{O} \) not in \( \pi' \) and let \( P_4 \) be the point of intersection of \( l \) and the line \( P_4 P_{124} \).

The plane \( \pi'' = P_3 P_4 P_{124} \) contains the two points \( P_3 \) and \( P_{124} \) of \( \mathcal{O} \), so \( \pi'' \) is a secant plane. Since \( P_4 \) lies in \( \pi'' \), \( \pi'' \) contains a tangent line \( l' \) to \( \mathcal{O} \) on \( P_{14} \); let \( P_{1234} \) be the point of intersection of \( l' \) and the line \( P_4 P_{1234} \).

We claim that no four of \( P_1, P_2, P_3, P_4 \) and \( P_{1234} \) are coplanar. First we note that \( P_3 \) is not in \( \pi \), as \( P_3 \) is the nucleus of \( \pi' \cap \mathcal{O} \) and \( \pi' \cap \pi' \) is a secant line to \( \mathcal{O} \). So \( P_1, P_2, P_3, P_4 \) are not coplanar. Now any plane containing \( P_3 \) and \( P_{1234} \) also contains \( P_{124} \).

Thus if \( P_1, P_2, P_3, P_{124} \) span a plane for some distinct \( i, j \) in \( \{1,2,4\} \), then this plane contains \( P_3 \), \( P_j \) and \( P_{124} \) and hence is the plane \( \pi' \); this is a contradiction as \( P_3 \) is not in \( \pi' \).

Finally \( \pi' = P_1 P_2 P_3 \) does not contain \( P_{1234} \) since the unique tangent line to \( \mathcal{O} \) on \( P_{14} \) in \( \pi' \) is \( l' \) and \( l' = P_{14} P_{1234} \) is a tangent line to \( \mathcal{O} \) different from \( l' \). Thus no four of \( P_1, P_2, P_3, P_4 \) and \( P_{1234} \) are coplanar.

It follows that there is a collineation \( \mu \) taking \( P_1 \) to \((1,0,0,0)\), \( P_2 \) to \((0,1,0,0)\), \( P_3 \) to \((0,0,1,0)\), \( P_4 \) to \((0,0,0,1)\) and \( P_{1234} \) to \((1,1,1,1)\). Hence \( \mu \) takes \( \pi \) to \( P_2 P_3 P_{124} \) to

\[
\{[x_1, x_2, 0, x_3] \mid x_1, x_2, x_3 \in GF(q)\} \quad \text{and} \quad \pi' = P_1 P_3 P_4 \text{ to } \{[x_1, x_2, x_3, 0] \mid x_1, x_2, x_3 \in GF(q)\}.
\]

Now \( P_{124} \) is the point of intersection of \( P_3 P_{124} \) and \( \pi' \) and hence \( \mu(P_{124}) = (1,1,1,1) \).

Thus \((0,1,0,0)\) and \((1,1,0,1)\) lie in \( \mu(\pi' \cap \mathcal{O}) \).

Again \( P_{14} \) is the point of intersection of \( P_2 P_{124} \) and \( l \) and so \( \mu(P_{14}) = (1,0,0,1) \). Then, since the five lines \( P_1 P_3, P_2 P_3, P_2 P_4, P_1 P_4 \) and \( l = P_4 P_1 \), and \( l' = P_{14} P_{1234} \) are all tangents to \( \mathcal{O} \), it follows from the Corollary to Theorem 2.3 that with respect to the form determined by \( \mu(\mathcal{O}), \mu(P_1) \perp \mu(P_2) \perp \mu(P_3) \perp \mu(P_4) \) and \( \mu(P_{124}) \perp \mu(P_{1234}) \). It follows that, up to a scalar multiple, the form is given by \((x,y) = x_1 y_2 + x_2 y_1 + x_3 y_4 + x_4 y_3\).

We are now ready to state our first major result on ovoids. For \( \alpha \in Aut GF(q) \) and a function \( d: GF(q) \to GF(q) \), let \( \mathcal{O}(\alpha, d) \) denote the set

\[
\mathcal{O}(\alpha, d) = \{(t^s + st + d(s), 1, s, t) \mid s, t \in GF(q)\} \cup \{(1,0,0,0)\}.
\]
With this notation the canonical form for an elliptic quadric given in Definition 2.1 is \( \mathcal{C}(2, d) \), where \( d(s) = as^2 \) for some \( a \in \text{GF}(q) \) with trace \( a = 1 \) (by Proposition 3.2(9)), and that for a Tits ovoid given in Definition 2.2 is \( \mathcal{C}(\sigma, \sigma + 2) \) where \( \sigma^2 = 2 \).

**Lemma 5.2.** Suppose that \( \mathcal{C} \) is an ovoid in \( \text{PG}(3, q) \), where \( q = 2^h > 2 \), and that \( \pi \) is a secant plane such that \( \pi \cap \mathcal{C} \) is a translation oval with associated automorphism \( \alpha \).

Let \( l \) be an axis of \( \pi \cap \mathcal{C} \). Suppose that each secant plane to \( \mathcal{C} \) on \( l \) meets \( \mathcal{C} \) in a translation oval. Then there is a collineation of \( \text{PG}(3, q) \) mapping \( \mathcal{C} \) to \( \mathcal{C}(\alpha, d) \) where \( d : \text{GF}(q) \to \text{GF}(q) \) satisfies \( d(0) = 0 \) and

\[
d(a) + d(b) \neq (a + b)^{a-q-1} K
\]

for all \( a, b \in \text{GF}(q) \) with \( a \neq b \), where \( K \) is the kernel of the trace map. Conversely, if \( \alpha \) is a generator of \( \text{Aut} \text{GF}(q) \) and \( d : \text{GF}(q) \to \text{GF}(q) \) has \( d(0) = 0 \) and satisfies (2) for all \( a \neq b \), then \( \mathcal{C}(\alpha, d) \) is an ovoid.

**Proof.** By Lemma 5.1 we may assume that \( \alpha \) is

\[
\{[x_1, x_2, 0, x_3] | x_1, x_2, x_3, x_4 \in \text{GF}(q)\},
\]

that \( l \) is

\[
\{[x_1, 0, 0, x_3] | x_1, x_3 \in \text{GF}(q)\},
\]

that the nucleus of \( \pi \cap \mathcal{C} \) is \( Q = (0, 0, 0, 1) \), that \( l \cap \mathcal{C} \) is \( (1, 0, 0, 0) \), that \( \mathcal{C} \) contains \( (0, 1, 0, 0) \) and \( (1, 1, 0, 1) \) and that the form determined by \( \mathcal{C} \)

\[
(x, y) = x_1y_2 + x_2y_1 + x_3y_4 + x_4y_4.
\]

Now \( \pi \cap \mathcal{C} \) is a translation oval with associated automorphism \( \alpha \), nucleus \( Q = (0, 0, 0, 1) \), axis \( l \), and \( \pi \cap \mathcal{C} \) contains \( (1, 0, 0, 0) \), \( (1, 1, 0, 1) \) and \( (0, 1, 0, 0) \). It follows from Lemma 4.5(a) that

\[
\pi \cap \mathcal{C} = \{(t^2, 1, 0, t) | t \in \text{GF}(q)\} \cup \{(1, 0, 0, 0)\}.
\]

For \( a \in \text{GF}(q) \), let \( \pi_a \) be the plane

\[
\{[x_1, x_2, ax_2, x_3] | x_1, x_2, x_3, x_4 \in \text{GF}(q)\}.
\]

Thus \( \pi_a \) is a plane on \( l \) and with this notation \( \pi_0 = \pi \). The tangent plane to \( \mathcal{C} \) at \( (1, 0, 0, 0) \) is \( (1, 0, 0, 0)^\perp = \{x_1, x_0, x_4 | x_1, x_2, x_3, x_4 \in \text{GF}(q)\} \), so the \( q \) planes \( \pi_a, a \in \text{GF}(q) \), constitute the set of all tangent planes to \( \mathcal{C} \) on \( l \). By hypothesis \( \pi_a \cap \mathcal{C} \) is a translation oval; let \( \beta_a \) denote its associated automorphism. The nucleus of \( \pi_a \cap \mathcal{C} \) is \( \pi_a = (a, 0, 0, 1) \).

The next step is to show that \( l \) is an axis of \( \pi_a \cap \mathcal{C} \) for \( a \neq 0 \) using the External Lines Lemma. To do this we must determine the lines on \( Q \) in \( \pi_a \) external to \( \pi_a \cap \mathcal{C} \). For \( t \in \text{GF}(q) \) set \( P_t = (r^t, 1, 0, t) \), a point on \( \mathcal{C} \) but not in \( \pi_a \). Then \( P_t \cap \mathcal{C} = \{P_t\} \) by Theorem 2.3, so \( P_t \cap \pi_a \) is a line on \( Q \) external to \( \pi_a \cap \mathcal{C} \). Now \( P_t \cap \pi_a \) is

\[
\{[x_1, x_2, ax_2, x_3] | x_1, x_2, x_3, x_4 \in \text{GF}(q), x_1 + x_4 = 0\} = \{[x_2(t^2 + at), x_2, ax_2, x_2] | x_2, x_4 \in \text{GF}(q)\} = \{[dx_2, x_2, ax_2, x_2] | x_2, x_4 \in \text{GF}(q)\},
\]

where \( d \in \text{GF}(q) \) by Proposition 3.2(8), where \( K \) is the kernel of the trace map. Since \( K \) has size \( q/2 \) and there are \( q/2 \) lines on \( Q \) in \( \pi_a \) external to \( \pi_a \cap \mathcal{C} \), it follows that all such lines are of the form \( P_t \cap \pi_a \) for some \( t \) satisfying \( t^2 + at \in \text{GF}(q) \).
Now consider the following oval in $\pi_n$:

$$\mathcal{O}' = \{(t^2 + at + c, 1, a, t) \mid t \in GF(q)\} \cup \{(1, 0, 0, 0)\},$$

where $c \notin a^{z/(q-1)}K$. This in a translation oval as it is the image of $D(x)$ under the map induce by the matrix

$$\begin{bmatrix} c & a & 1 \\ 1 & 0 & 0 \\ a & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$ 

Now $\mathcal{O}'$ has axis $l$, nucleus $(a, 0, 0, 1)$ on $l$, and $l$ meets $\pi_n \cap \mathcal{O}$ and $\mathcal{O}'$ in $(1, 0, 0, 0)$. The lines on $Q$ in $\pi_n$ external to $\mathcal{O}'$ are the lines $\pi_n \cap \sigma_j$ where

$$\sigma_j = \{[dx_2, x_2, x_3, x_4] \mid x_2, x_3, x_4 \in GF(q)\}$$

and $t^2 + at + c \neq d$ for all $t \in GF(q)$. Now $\{t^2 + at \mid t \in GF(q)\} = a^{z/(q-1)}K$ (of size $q/2$) by Proposition 3.2(8) and $c \notin a^{z/(q-1)}K$. So the lines on $Q$ in $\pi_n$ external to $\mathcal{O}'$ are precisely the lines $\pi_n \cap \sigma_j$ for $d \in a^{z/(q-1)}K$, that is, the set of lines on $Q$ in $\pi_n$ external to $\mathcal{O}'$ and the set external to $\pi_n \cap \mathcal{O}$ are the same. Thus by Proposition 4.6, $l$ is an axis of $\pi_n \cap \mathcal{O}$.

It now follows from Lemma 4.5(2) that $\pi_n \cap \mathcal{O}$ is

$$\{(c(a) t^{\beta} + at + d(a), 1, a, t) \mid t \in GF(q)\} \cup \{(1, 0, 0, 0)\}$$

for some $c(a), d(a) \in GF(q)$ with $c(a) \neq 0$.

The points $(s^a, 1, 0, s)$ and $(c(a) t^{\beta} + at + d(a), 1, a, t)$ of $\mathcal{O}$ are not perpendicular with respect to the form determined by $\mathcal{O}$ (by Theorem 2.3 and the remarks following it), and so $s^2 + c(a) t^{\beta} + at + d(a) + as \neq 0$ for all $s$ and $t$ in $GF(q)$, that is, $d(a)$ does not lie in the set

$$X = \{s^2 + c(a) t^{\beta} + a(s + t) \mid s, t \in GF(q)\}.$$ 

Now $X$ is a proper subset of $GF(q)$ which is closed under addition and $X$ contains both

$$\{s^2 + as \mid s \in GF(q)\} = a^{z/(q-1)}K$$

and

$$\{(c(a) t^{\beta} + at \mid t \in GF(q)\} = c(a)^{-1/(\beta_0/(\beta_0+1))}K$$

by Proposition 3.2(8). By Proposition 3.2(5) it follows that

$$a^{z/(q-1)} = c(a)^{-1/(\beta_0/(\beta_0+1))} a^{\beta_0/(\beta_0+1)}$$

which yields

$$c(a) = a^{(z-\beta_0)/(n-1)}$$

(3)

for all non-zero $a$ in $GF(q)$. Again the points $(c(a) s^{\beta} + as + d(a), 1, a, s)$ and $(c(b) t^{\beta} + bt + d(b), 1, b, t)$ of $\mathcal{O}$ are not perpendicular and so

$$c(a) s^{\beta} + as + d(a) + c(b) t^{\beta} + bt + d(b) + at + bs \neq 0$$

(4)

for all $s, t \in GF(q)$. Arguing as above we find that

$$c(a)^{1/(\beta_0/(\beta_0+1))} a^{\beta_0/(\beta_0+1)} = c(b)^{-1/(\beta_0/(\beta_0+1))} (a+b)^{\beta_0/(\beta_0+1)},$$

which yields

$$a^{(z-\beta_0/(1-\beta_0))} b^{(z-\beta_0)/(\beta_0+1)} = (a+b)^{\beta_0/(1-\beta_0)}.$$
If $\beta_a = \beta_b$, then $(ab^{-1})^{(x-\beta_a)(1-x)} = 1$, that is $(ab^{-1})^{(x-\beta_a)}$ is in the fixed field of $\beta_a$. As $\beta_a$ is a generator of $Aut \ GF(q)$, we have $(ab^{-1})^{(x-\beta_a)} = 1$ so that $ab^{-1}$ is an element of the fixed field of $\beta_a x^{-1}$. If $\beta_a = \phi$ then $b^{(x-\beta_a)} = (a+b)^{(x-\beta_a)}$ so that $(a+b)b^{-1}$ is an element of the fixed field of $\beta_a x^{-1}$.

Suppose now that $\beta_a \neq \alpha$ for some $b \neq 0$. Then from the previous paragraph it follows that $||a \in GF(q) \mid \beta_a = \alpha|| \leq q^{1/2}$ (the largest possible order of a proper subfield of $GF(q)$), and also that $||a \in GF(q) \mid \beta_a = \beta_b|| \leq q^{1/2}$. Since there are only $\phi(h)$ generators of $Aut \ GF(q)$ (where $\phi$ is the Euler phi function) it follows that $\phi(h)q^{1/2} \geq q$, so $\phi(h)^2 \geq q = 2^k$, which is a contradiction. Hence $\beta_a = \alpha$ for all $a \neq 0$, and it follows from equation (3) that $c(a) = 1$ for all $a \neq 0$. Thus setting $d(0) = 0$, $c$, which is the union of $\pi_a \cap c$ over all $a$ in $GF(q)$, is the set

$$\{ (t^a + at + d(a), 1, a, t) \mid a, t \in GF(q) \} \cup \{ (1, 0, 0, 0) \},$$

that is, $c = c(\alpha, d)$. Moreover by equation (4)

$$d(a) + d(b) \neq \{ s^a + t^a + (a + b)(s + t) \mid s, t \in GF(q) \},$$

that is, $d(a) + d(b) \neq (a + b)^{x-1} \bar K$ by Proposition 3.2(8).

Conversely it follows from Theorem 2.4 that $c(\alpha, d)$ is an ovoid corresponding to the form

$$(x, y) = x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3$$

if $d$ satisfies (2) for all $a$ and $b$ in $GF(q)$ and $d(0) = 0$.

**THEOREM 5.3.** Suppose that $c$ is an ovoid in $PG(3, q)$, where $q$ is even, $q > 2$, and that $\pi$ is a secant plane such that $\pi \cap c$ is a translation oval. Let $L$ be an axis of $\pi \cap c$. Then all secant planes to $c$ on $l$ meet $c$ in translation ovals if and only if $c$ is an elliptic quadric or a Tits ovoid.

**Proof.** By Lemma 5.2, there is a generator $\alpha$ of $Aut \ GF(q)$ and a function $d$ such that $c = c(\alpha, d)$. Let

$$M_u = \begin{bmatrix} 0 & u^e & u & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & u & 0 & 1 \end{bmatrix}$$

for $u \in GF(q)$. Then

$$M_u \begin{bmatrix} t^a + st + d(s) \\ 1 \\ s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ s \\ t+u \end{bmatrix},$$

so $M_u \cap c = c$. Also, $M_u$ is a translation [2, 6.1] of the inversive plane $\mathcal{I}$ associated with $c$. Moreover, $M = \{ M_u \mid u \in GF(q) \}$ is transitive on the points other than $(0, 0, 0, 1)$ of the oval $\pi_1 \cap c$ of the secant plane $\pi_1 : x_3 = sx_2$ to $c$ on $l$ for each $s \in GF(q)$. Hence $\mathcal{I}$ does not have Hering type I.1. [2, p. 261]. So, by the results of Glynn [4], $c$ is an elliptic quadric or a Tits ovoid.

Note that this is our main theorem stated in the Introduction. Also, since the only ovals of $PG(2, 8)$ are translation ovals [7, Theorem 9.2.3], it follows from Theorem 5.3 that the only ovals of $PG(3, 8)$ are the elliptic quadrics and the Tits ovoids, a result previously obtained by Fellegara [3] by using a computer.
References


Department of Mathematics
The University of Western Australia
Nedlands 6907
Western Australia
Australia

E-mail: penttila@maths.uwa.edu.au
praeger@maths.uwa.edu.au