

On ovoids of $PG(3, q)$

Simeon Ball *

Department of Mathematics,
Queen Mary College, University of London,
Mile End Road, London E1 4NS,
United Kingdom

Current address:

Departament de Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya,
Jordi Girona 1–3, Mòdul C3,
08034 Barcelona,
Spain
`simeon@mat.upc.es`

13 January 2005

Abstract

We give necessary and sufficient conditions that a polynomial $f(x, y)$ gives an ovoid of $PG(3, q)$. Furthermore by considering Rédei polynomials associated to ovoids of $PG(3, q)$ we obtain sets of equations relating the coefficients of $f(x, y)$. One such set of equations implies that if $x^i y^j$ occurs as a term in $f(x, y) + xy$ then i and j must have disjoint binary expansions.

1 Introduction

An *inversive plane* is an incidence structure of points and circles which satisfy the following axioms.

- (I1) Three distinct points are incident with exactly one circle.

*The author was supported by a British EPSRC Fellowship No. AF/990-480 during the period when the main part of this research was undertaken. It was completed with the support of the Ministerio de Ciencia y Tecnología, España.

- (I2) If P and Q are two points and c is a circle incident with P and not incident with Q then there is exactly one circle d incident with P and Q such that $c \cap d = \{P\}$.
- (I3) There are at least two circles and every circle has at least three points.

For any point P of an inversive plane the points $\neq P$ and the circles incident with P form an affine plane. If the inversive plane is finite then all these affine planes have the same order; this integer is the order of the inversive plane. An inversive plane of order n has $n^2 + 1$ points and $n(n^2 + 1)$ circles; every circle is incident with $n + 1$ points and any two points are incident with $n + 1$ circles. For more details concerning inversive planes see [4].

An *ovoid of $PG(3, q)$* \mathcal{O} is a set of points in $PG(3, q)$ satisfying the following properties.

- (O1) Any line is incident with at most two points of \mathcal{O} .
- (O2) For any $P \in \mathcal{O}$, the union of all lines l with $l \cap \mathcal{O} = \{P\}$ is a plane.

The points and the non-tangent plane sections of an ovoid of $PG(3, q)$ form an inversive plane. In 1963 Dembowski [4] proved the following partial converse:

Theorem 1.1 Every inversive plane of even order n is isomorphic to the system of points and plane sections of an ovoid in $PG(3, n)$. □

The classification of inversive planes would follow then from the classification of ovoids in $PG(3, q)$ when q is even. However we only have the following classification result due independently to Barlotti [1] and Panella [13].

Theorem 1.2 Every ovoid in $PG(3, q)$, with q odd, is an elliptic quadric. □

The known ovoids of $PG(3, q)$ when q is even are of two types; they are the elliptic quadrics which occur for all q and the Tits ovoids [18], which only occur when $q > 2$ is a non-square.

Let $W(q)$ be the generalised quadrangle whose points are the points of $PG(3, q)$ and whose lines are the totally isotropic lines of a symplectic form, see [15]. An ovoid $\bar{\mathcal{O}}$ of $W(q)$ is a set of points with the property that every line is incident with exactly one point of $\bar{\mathcal{O}}$.

A non-tangent planar section $\pi \cap \mathcal{O}$ of an ovoid \mathcal{O} in $PG(3, q)$ is a set of $q + 1$ points with at most two points incident with any line. Such a set is called an *oval*.

An oval in $PG(2, q)$ with q even has the property that all tangent lines are incident with a common point, called the *nucleus* of the oval.

In [16] Segre proved the following.

Theorem 1.3 Let \mathcal{O} be an ovoid of $PG(3, q)$, q even. Then \mathcal{O} determines a symplectic polarity that interchanges each point P of the ovoid with its tangent plane (the plane whose intersection with \mathcal{O} is P) and interchanges each secant plane π with nucleus of the oval $\pi \cap \mathcal{O}$. \square

In other words, when q is even, an ovoid of $PG(3, q)$ is an ovoid of some $W(q)$, defined in $PG(3, q)$. In [17] This proved the converse.

Theorem 1.4 An ovoid of $W(q)$ defined in $PG(3, q)$, q even, is an ovoid of $PG(3, q)$. \square

The classification of inversive planes of even order is equivalent to the classification of ovoids in $PG(3, q)$ with q even, which in turn is equivalent to the classification of ovoids in $W(q)$.

Let us fix a symplectic (alternating) form

$$(\langle x_0, x_1, x_2, x_3 \rangle, \langle y_0, y_1, y_2, y_3 \rangle) = x_0y_2 + y_0x_2 + x_1y_3 + y_1x_3$$

and consider ovoids of the $W(q)$, q even, that this form defines.

We can assume that an ovoid contains the points $\langle 0, 0, 1, 0 \rangle$ and $\langle 1, 0, 0, 0 \rangle$. The plane $X_0 = 0$ is the polar plane of the point $\langle 0, 0, 1, 0 \rangle$ and hence contains no other points of the ovoid. If the points $\langle 1, x, a, y \rangle$ and $\langle 1, x, b, y \rangle$ are both points of the ovoid then since any line of $W(q)$ is incident with exactly one point of the ovoid, $a = b$. Hence there is a polynomial $f(x, y)$ such that the points of the ovoid are

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, x, f(x, y), y \rangle \mid x, y \in GF(q)\},$$

and $f(0, 0) = 0$.

A polynomial $f(X, Y)$ that gives an ovoid of $W(q)$, arising from the form above, will be called an *ovoid polynomial*.

The known examples of ovoid polynomials (see [7]) are those that give elliptic quadrics

$$f(x, y) = xy + ax^2 + by^2,$$

where $ax^2 + x + b$ is irreducible over $GF(q)$ and those that give Tits ovoids

$$f(x, y) = xy + [(cx + dy)^{\sigma+2} + (ax + by)^\sigma + acx^2 + bdy^2]/(ad + bc),$$

where $ad + bc \neq 0$ and $\sigma = \sqrt{2q} > 2$.

In $PG(3, 8)$ ovoids are either elliptic quadrics or Tits ovoids, Fellegara [5]. In $PG(3, 16)$ ovoids are elliptic quadrics, first classified by O’Keefe and Penttila with the aid of a computer in [10], and without a computer by the same authors in [11]. In $PG(3, 32)$ ovoids are either elliptic quadrics or Tits ovoids; this classification was obtained by O’Keefe, Penttila and Royle with the aid of a computer [12].

The following theorem is from Brown [2].

Theorem 1.5 An ovoid of $PG(3, q)$ that has a conic as a planar section is an elliptic quadric. \square

A pointed conic of $PG(2, q)$, q even, is an oval projectively equivalent to the set of points

$$\{(0, 1, 0)\} \cup \{(x, x^{q/2}, 1) \mid x \in GF(q)\}.$$

The following theorem is from Brown [3].

Theorem 1.6 An ovoid of $PG(3, q)$, q even, that has a pointed conic as a planar section is either an elliptic quadric in $PG(3, 4)$ or a Tits ovoid in $PG(3, 8)$. \square

In [7] Glynn also provides us with necessary and sufficient conditions for $f(x, y)$ to be an ovoid polynomial. When we talk about the coefficient of $x^b y^c$ in $f(x, y)^k$ we mean the coefficient of $x^b y^c$ in $f(x, y)^k$ modulo $x^q = x$ and $y^q = y$. We are working over $GF(q)$ where q is even, so all binomial coefficients are evaluated modulo 2. The following is a reformulation of Glynn’s theorem which does not require us to mention i -good functions.

Theorem 1.7 Let $q = 2^h$. The polynomial $f(x, y)$ is an ovoid polynomial if and only if

- (A) $f(x, y) = 0$ if and only if $(x, y) = (0, 0)$.
- (B) for all $1 \leq k \leq q - 2$ and $0 \leq b, c \leq q - 1$, where $s = k - b - c$ modulo $q - 1$ and $1 \leq s \leq q - 1$, one of the following occurs.
 - (i) The coefficient of $x^b y^c$ in $f(x, y)^k$ is zero.
 - (ii) There exists an r with $0 \leq r \leq h - 1$ such that $\binom{b}{2^r} = \binom{c}{2^r} = \binom{q-1-k}{2^r} = \binom{s}{2^r} = 0$.
 - (iii) $b, c, q - 1 - k$ and s have mutually disjoint binary expansions.
 - (iv) $b = c = k$ and the coefficient of $(xy)^k$ in $f(x, y)^k$ is 1.

□

Throughout the article q will be even and so all binomial coefficients will be evaluated modulo 2. Lucas' Theorem, in this case, says that

$$\binom{a}{b} = \binom{a_0}{b_0} \binom{a_1}{b_1} \cdots \binom{a_r}{b_r} \pmod{2},$$

where $a = \sum_{i=0}^r a_i 2^i$ and $b = \sum_{i=0}^r b_i 2^i$.

Note that $\binom{a}{2^s} = a_s$ and $\binom{q-1-b}{a} = 1$ if and only if a and b have disjoint binomial expansions. Note also that $\binom{q-1-b+k}{k} = \binom{b}{k}$ since that left-hand side is 1 if and only if $b_r = 1$ whenever $k_r = 1$ which is if and only if $\binom{b}{k} = 1$.

In this article we will prove the following necessary and sufficient conditions for $f(x, y)$ to be an ovoid polynomial.

Theorem 2.2 $f(x, y)$ is an ovoid polynomial if and only if for all $y, a \in GF(q)$ the coefficient of x^b in $(f(y, x) + xy)^k$ and $(f(x, y + ax) + xy)^k$ is zero whenever $\binom{b}{k} \neq 0$ unless $b = k = q - 1$ in which case it is 1. □

We will also prove other necessary conditions on the coefficients including the following corollary.

Corollary 6.2 If the coefficient of $x^i y^j$ in $f(x, y) + xy$ is non-zero then i and j have disjoint binary expansions. □

Finally, proofs of the classification for $q = 8$ and $q = 16$ have been included. As opposed to previous classification results for ovoids [10, 11, 12], the classifications are obtained independent of the classification of ovals. It is my hope that the technique used here will offer an approach to the classification of ovoids in fields of higher order where the classification of ovals would appear to be out of reach.

2 Necessary and Sufficient Conditions

The following lemma is a slight modification of the theorem in [6]. Recall that when we talk about the coefficient of x^b in $f(x)^k$ we mean the coefficient of x^b in $f(x)^k \pmod{x^q = x}$ and that all binomial coefficients are evaluated modulo 2. To make the formulas more legible we will sometimes suppress the arguments of the polynomials. e.g $\sigma(Z)$ maybe appear as σ if the argument is clear.

Lemma 2.1 The set of $q + 1$ points of $PG(2, q)$

$$\{(x, f(x), 1) \mid x \in GF(q)\} \cup \{(0, 1, 0)\}$$

is an oval with nucleus $\langle 1, 0, 0 \rangle$ if and only if the coefficient of x^b in $f(x)^k$ is zero whenever $q > k > 0$ and $\binom{b}{k} \neq 0$ unless $b = k = q - 1$ in which case it is 1.

Proof. Consider the Rédei polynomial of the function f defined in two indeterminates by

$$R(T, Z) := \prod_{x \in GF(q)} (T + xZ + f(x)) = \sum_{j=0}^q \sigma_{q-j}(Z) T^j.$$

The number of points of the oval incident with the line $zX + Y = b$ is the number of $x \in GF(q)$ such that $zx + f(x) = b$ which is the number of times $T + b$ occurs as a factor of $R(T, z)$.

If $z \neq 0$ then this number is zero or two and the polynomial $R(T, z)$ is a square in T , and therefore for j odd $\sigma_j(z) = 0$.

If $z = 0$ each factor of $R(T, 0)$ is distinct and therefore $R(T, 0) = T^q + T$. In particular $\sigma_{q-1}(0) = 1$.

The degree of σ_j is at most j by definition so for $j < q - 1$ and j odd $\sigma_j \equiv 0$. The polynomial σ_{q-1} is zero for all $Z = z \neq 0$ and $\sigma_{q-1}(0) = 1$, hence $\sigma_{q-1} \equiv Z^{q-1} + 1$.

Differentiate the reverse Rédei polynomial

$$T^q R(T^{-1}, Z) = \prod_{x \in GF(q)} (1 + (xZ + f(x))T) = \sum_{j=0}^q \sigma_j T^j$$

with respect to T ,

$$\left(\sum_{j=0}^q \sigma_j T^j \right) \left(\sum_{x \in GF(q)} \frac{xZ + f(x)}{1 + (xZ + f(x))T} \right) = \sigma_{q-1} T^{q-2}.$$

Write the rational function as an infinite sum and multiply by T to get the identity

$$\left(\sum_{j=0}^q \sigma_j T^j \right) \left(\sum_{j=1}^{\infty} \pi_j(Z) T^j \right) = \sigma_{q-1} T^{q-1},$$

where

$$\pi_j(Z) = \sum_{x \in GF(q)} (xZ + f(x))^j.$$

By definition $\sigma_0 = 1$ and so $\pi_j(Z) \equiv 0$ for $0 < j < q - 1$ and $\pi_{q-1} = \sigma_{q-1} = Z^{q-1} + 1$.

Now for $j < q - 1$

$$\pi_j(Z) = \sum_{k=0}^j \binom{j}{k} \left(\sum_{x \in GF(q)} x^{j-k} f(x)^k \right) Z^{j-k},$$

which is identically zero if and only if the coefficient of $x^{q-1-j+k}$ in $f(x)^k$ is zero whenever $\binom{j}{k} \neq 0$ and $j < q-1$, which is if and only if the coefficient of x^b in $f(x)^k$ is zero whenever $\binom{q-1-b+k}{k} = \binom{b}{k} \neq 0$ and $b > k$.

And

$$\pi_{q-1}(Z) = \sum_{b=0}^{q-1} \left(\sum_{x \in GF(q)} x^{q-1-b} f(x)^b \right) Z^{q-1-b},$$

which is identically equal to $Z^{q-1} + 1$ if and only if the coefficient of x^b in $f(x)^b$ is zero for $b < q-1$ and the coefficient of x^{q-1} in $f(x)^{q-1}$ is 1.

This completes the forward implication.

The argument in reverse is straightforward up until the point where we differentiate the reverse Rédei polynomial. The $\pi_j \equiv 0$ for $j < q-1$ imply that $\sigma_j \equiv 0$ for j odd and it follows then that $\sigma_{q-1} = \pi_{q-1} = Z^{q-1} + 1$. Now when we put $Z = z \neq 0$ in the Rédei polynomial we see that it is a square in T and therefore every line not incident with $\langle 1, 0, 0 \rangle$ is incident with an even number of the points

$$\{\langle x, f(x), 1 \rangle \mid x \in GF(q)\} \cup \{\langle 0, 1, 0 \rangle\}.$$

For $a \in GF(q)$, consider lines through the point $\langle a, f(a), 1 \rangle$. Each of the q lines incident with $\langle a, f(a), 1 \rangle$, not incident with $\langle 1, 0, 0 \rangle$, contains exactly one of the points

$$\{\langle x, f(x), 1 \rangle \mid x \neq a\} \cup \{\langle 0, 1, 0 \rangle\}.$$

Hence the line $\langle (1, 0, 0), (a, f(a), 1) \rangle$ is incident with only one of the points

$$\{\langle x, f(x), 1 \rangle \mid x \in GF(q)\} \cup \{\langle 0, 1, 0 \rangle\},$$

namely $\langle a, f(a), 1 \rangle$. So this set is an oval with nucleus $\langle 1, 0, 0 \rangle$.

□

Theorem 2.2¹ Let $q > 2$ be even. The polynomial $f(x, y)$ is an ovoid polynomial if and only if for all $y, a \in GF(q)$ the coefficient of x^b in $(f(y, x) + xy)^k$ and $(f(x, y + ax) + xy)^k$ is zero whenever $q > k > 0$ and $\binom{b}{k} \neq 0$ unless $b = k = q-1$ in which case it is 1.

Proof. Suppose that $f(x, y)$ is an ovoid polynomial and let \mathcal{O} be the ovoid

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, x, f(x, y), y \rangle \mid x, y \in GF(q)\}.$$

Let y and $a \in GF(q)$ and consider the plane

$$X_3 = yX_0 + aX_1.$$

¹I am indebted to Michel Lavrauw for simplifying both the original statement and proof of this theorem.

Its intersection with \mathcal{O} is

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, x, f(x, y + ax), y + ax \rangle \mid x \in GF(q)\}.$$

By Theorem 1.4 this set of $q + 1$ points is an oval. The symplectic form tells us that this oval has nucleus $\langle 0, 1, y, a \rangle$. Let us introduce a change of coordinates that fixes X_0 and X_1 and puts $X_2^* = X_2 + yX_1$ and $X_3^* = yX_0 + aX_1 + X_3$. Then in this new frame the intersection is the oval

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, x, f(x, y + ax) + xy, 0 \rangle \mid x \in GF(q)\},$$

and it has nucleus $\langle 0, 1, 0, 0 \rangle$. Lemma 2.1 now implies that the coefficient of x^b in $(f(x, y + ax) + xy)^k$, is zero whenever $\binom{b}{k} \neq 0$ and $k > 0$ unless $b = k = q - 1$ in which case it is 1.

To complete the forward implication we have to consider the planes $X_1 = aX_0$ where $a \in GF(q)$. This plane intersects the ovoid in the oval

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, a, f(a, y), y \rangle \mid y \in GF(q)\},$$

with nucleus $\langle 0, 0, a, 1 \rangle$. Again we introduce a change of coordinates that fixes X_0 and X_3 and puts $X_1^* = X_1 + aX_0$ and $X_2^* = X_2 + aX_3$. Then in this new frame the intersection is the oval

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, 0, f(a, y) + ay, y \rangle \mid y \in GF(q)\},$$

and it has nucleus $\langle 0, 0, 0, 1 \rangle$. Now we apply Lemma 2.1 again and replace a with y and y with x to conclude that the coefficient of x^b in $(f(y, x) + xy)^k$, is zero whenever $\binom{b}{k} \neq 0$ and $k > 0$ unless $b = k = q - 1$ in which case it is 1.

The reverse implication almost follows directly by the following the above argument in reverse. Since the conditions to follow the reverse implication in Lemma 2.1 hold, we have that every plane that contains the point $\langle 0, 0, 1, 0 \rangle$ intersects the set

$$\{\langle 0, 0, 1, 0 \rangle\} \cup \{\langle 1, x, f(x, y), y \rangle \mid x, y \in GF(q)\}$$

in an oval. The only plane that we have not considered is the plane $X_0 = 0$ but this is clearly a tangent plane. Now every line is contained in one of these planes and so we conclude that every line is incident with at most two points of this set of $q^2 + 1$ points. Counting (point, plane) pairs and (point, point, plane) triples one can deduce that each plane is incident with 1 or $q + 1$ points of the set and so (O2) is satisfied and this set of points is an ovoid of $PG(3, q)$. The reverse implication of Lemma 2.1 tells us the nucleus of each of the oval sections of the ovoid and that the ovoid is also an ovoid of $W(q)$.

□

The following corollary was first proven by Glynn in [7].

Corollary 2.3 If $f(x, y)$ is an ovoid polynomial then $f(x, y) = xy + s(x, y)^2$ for some polynomial $s(x, y)$ of total degree at most $q/2 - 1$.

Proof. Let

$$f(x, y) + xy = \sum_{i,j=0}^{q-1} c_{i,j} x^i y^j.$$

Theorem 2.2 with $k = 1$ implies that the coefficient of x^b in

$$f(x, y + ax) + xy = \sum_{i,j=0}^{q-1} c_{i,j} x^i (y + ax)^j = \sum_{i,j=0}^{q-1} \sum_{k=0}^j \binom{j}{k} c_{i,j} x^{i+k} y^{j-k} a^k,$$

is zero whenever b is odd. Therefore the coefficient of $x^i y^j a^0$, which is $c_{i,j}$, is zero whenever i is odd. By reversing the role of x and y we conclude that $c_{i,j}$ is zero whenever j is odd. The coefficient of $x^{i+k} y^0 a^k$, which is $c_{i,k}$, is zero whenever $i + k \geq q$ and $i + k$ is even, (so $i + k$ modulo $q - 1$ is odd).

□

The j -th Hasse derivative of a polynomial $g(x) = \sum c_i x^i$ is $\partial^j g = \sum \binom{i}{j} c_i x^{i-j}$.

Lemma 2.4 If

$$f(x, y) = xy + \sum_{i,j=0}^{q-2} c_{i,j} x^i y^j = \sum_{i=0}^{q-2} \psi_i(y) x^i + xy$$

then

$$f(x, y + ax) = \sum_{i=0}^{q-2} \bar{\psi}_i(y, a) x^i + xy,$$

where for $i > 2$

$$\bar{\psi}_i(y, a) = \sum_{j=0}^{q-2-i} \partial^j \tau_{i+j}(a) y^j,$$

$$\bar{\psi}_2(y, a) = a + \sum_{j=0}^{q-4} \partial^j \tau_{j+2}(a) y^j$$

and

$$\tau_r(a) = \sum_{k=0}^r c_{r-k,k} a^k.$$

Proof. Firstly note that

$$\partial^j \tau_{i+j} = \sum_{k=j}^{i+j} \binom{k}{j} c_{i+j-k,k} a^{k-j} = \sum_{k=0}^i \binom{k+j}{j} c_{i-k,k+j} a^k.$$

By Corollary 2.3 we can write

$$\begin{aligned}
f(x, y + ax) &= xy + ax^2 + \sum_{j=0}^{q-2} \sum_{i=0}^{q-2-j} c_{i,j} x^i (y + ax)^j \\
&= xy + ax^2 + \sum_{j=0}^{q-2} \sum_{i=0}^{q-2-j} \sum_{k=0}^j \binom{j}{j-k} c_{i,j} a^k x^{i+k} y^{j-k} \\
&= xy + ax^2 + \sum_{k=0}^{q-2} \sum_{j=k}^{q-2} \sum_{i=k}^{q-2+k-j} \binom{j}{j-k} c_{i-k,j} a^k x^i y^{j-k} \\
&= xy + ax^2 + \sum_{k=0}^{q-2} \sum_{j=0}^{q-2-k} \sum_{i=k}^{q-2-j} \binom{j+k}{j} c_{i-k,j+k} a^k x^i y^j \\
&= xy + ax^2 + \sum_{i=0}^{q-2} \sum_{j=0}^{q-2-i} \sum_{k=0}^i \binom{j+k}{j} c_{i-k,j+k} a^k x^i y^j.
\end{aligned}$$

□

3 The classification when $q = 8$

By Corollary 2.3 we can write

$$f(x, y) = xy + \psi_0 + \psi_2 x^2 + \psi_4 x^4 + \psi_6 x^6$$

where $\psi_j(y)$ is a square in y of degree at most $6 - j$. Lemma 2.4 and Theorem 2.2 with $k = 3$ and $b = 3$ and 7 respectively give

$$\overline{\psi_2} \overline{\psi_4}^2 + \overline{\psi_2}^2 \overline{\psi_6} = 0 \quad (1)$$

and

$$\overline{\psi_6} \overline{\psi_4}^2 + \overline{\psi_2} \overline{\psi_6}^2 = 0, \quad (2)$$

for all $y, a \in GF(8)$ where

$$\overline{\psi_2} = a + \tau_2 + \partial^2 \tau_4 y^2 + \partial^4 \tau_6 y^4,$$

$$\overline{\psi_4} = \tau_4 + \partial^2 \tau_6 y^2,$$

and

$$\overline{\psi_6} = \tau_6.$$

The degree of (2) in y is just 4 and so for all $a \in GF(8)$ the coefficients of y^0 , y^2 and y^4 are zero;

$$\begin{aligned}\tau_4^2\tau_6 + (a + \tau_2)\tau_6^2 &= 0 \\ \tau_6^2\partial^2\tau_4 &= 0 \\ \tau_6(\partial^2\tau_6)^2 + \tau_6^2(\partial^4\tau_6) &= 0.\end{aligned}$$

Let us consider first the case $\tau_6 \neq 0$. The last equation has degree 14 and is a square in a and so is identically zero. The polynomial $\partial^2\tau_6$ is a 4-th power of degree 4 so we can write $\partial^2\tau_6 = (\gamma + \delta a)^4$ for some γ and δ . The polynomial $\partial^4\tau_6$ divides $\partial^2\tau_6$ and has degree 2 so for some ε we have that $\partial^4\tau_6 = \varepsilon(\gamma + \delta a)^2$. Hence

$$\tau_6 = (\gamma + \delta a)^6/\varepsilon.$$

The equation $\partial^2\tau_4 = 0$ implies that τ_4 is a 4-th power of degree at most 4 and so

$$\tau_4 = (\alpha + \beta a)^4/\varepsilon$$

for some $\alpha, \beta \in GF(8)$. All that remains is to solve for τ_2 from the remaining equation which tells us that for all $a \in GF(q)$

$$(\gamma + \delta a)^6(\alpha + \beta a) + \varepsilon(a + \tau_2)(\gamma + \delta a)^{12} = 0.$$

Hence

$$(\gamma + \delta a)(\alpha + \beta a) + \varepsilon(a + \tau_2) = 0$$

and since it has degree just 2 in a it is identically zero. Now since we know that τ_2 is a square we conclude that

$$\tau_2 = (\alpha\gamma + \beta\delta a^2)/\varepsilon$$

and that $\varepsilon = \alpha\delta + \beta\gamma$. Therefore

$$f(x, y) = xy + [(\gamma x + \delta y)^6 + (\alpha x + \beta y)^4 + \alpha\gamma x^2 + \beta\delta y^2]/(\alpha\delta + \beta\gamma),$$

which is the general form of a Tits ovoid.

The case $\tau_6 = 0$ is easy. We have that $\bar{\psi}_6 = 0$ and from equation (1) that

$$\tau_4(a + \tau_2) = 0.$$

Now $\tau_2 = \alpha + \beta a^2$ for some α and $\beta \in GF(8)$ and so $\tau_4 = 0$. Hence

$$f(x, y) = xy + \alpha x^2 + \beta y^2$$

and the ovoid is an elliptic quadric.

4 Rédei polynomials

Consider the (reverse) Rédei polynomial defined in three variables by

$$\rho(T, Y, Z) := \prod_{x \in GF(q)} (1 + (xZ + f(x, Y))T) = \sum_{j=0}^q \sigma_j(Y, Z)T^j.$$

Lemma 4.1 If the polynomial $f(X, Y)$ is an ovoid polynomial then for all $y \neq z \in GF(q)$

- (i) $\rho(T, y, z)$ = a square in T that divides $1 + T^{2q-2}$,
- (ii) $\rho(T, y, z)\rho(T, z, y) = 1 + T^{2q-2}$,
- (iii) $\rho(T, y, y) = 1 + T^{q-1}$.

Proof. The set of points

$$\{(0, 0, 1, 0)\} \cup \{(1, x, f(x, y), y) \mid x \in GF(q)\}$$

is the intersection of the ovoid with the plane $X_3 = yX_0$, and they form an oval section of the ovoid with nucleus $\langle 0, 1, y, 0 \rangle$. Again we apply a change of coordinates that fixes all the coordinates with the exception of $X_3^* = X_3 + yX_0$. Then in the new frame the intersection with the ovoid is oval

$$\{(0, 0, 1, 0)\} \cup \{(1, x, f(x, y), 0) \mid x \in GF(q)\},$$

and the nucleus is $\langle 0, 1, y, 0 \rangle$. Now (i) and (iii) follow as in the proof of Lemma 2.1.

For $y \neq z$, the polynomials $\rho(T, y, z)$ and $\rho(T, z, y)$ have a common factor if and only if there exists an x and $s \in GF(q)$ such that $xz + f(x, y) = sy + f(s, z)$. However the points $\langle 1, x, f(x, y), y \rangle$ and $\langle 1, s, f(s, z), z \rangle$ are distinct points of an ovoid of the $W(q)$ and so

$$\langle \langle 1, x, f(x, y), y \rangle, \langle 1, s, f(s, z), z \rangle \rangle = xz + f(x, y) + sy + f(s, z) \neq 0.$$

Hence the polynomials $\rho(T, y, z)$ and $\rho(T, z, y)$ have distinct factors. Now (i) implies (ii).

□

Lemma 4.1 implies that $\sigma_j(y, Z)$ is identically zero whenever j is odd and $j < q - 1$ and the polynomial $\sigma_{q-1}(y, Z) = (Z^q + Z)/(Z + y)$.

Differentiating $\rho(T, y, Z)$ with respect to T we get

$$\rho(T, y, Z) \left(\sum_{x \in GF(q)} \frac{xZ + f(x, y)}{1 + (xZ + f(x, y))T} \right) = \sigma_{q-1}(y, Z)T^{q-2}$$

and by writing the quotient as an infinite sum and multiplying through by T

$$\rho(T, y, Z) \left(\sum_{j=1}^{\infty} \pi_j(y, Z)T^j \right) = (Z^q + Z)T^{q-1}/(Z + y),$$

where

$$\pi_j(y, Z) = \sum_{x \in GF(q)} (xZ + f(x, y))^j.$$

The polynomial $\rho(T, y, Z)$ has constant term 1 and so $\pi_j(y, Z) \equiv 0$ for $j < q - 1$ and every $\pi_j(y, Z)$ is divisible by $(Z^q + Z)/(Z + y)$. Also for k odd and $k < q - 1$ we have that $\pi_{q-1+k}(y, Z) \equiv \pi_{(q-1+k)/2}(y, Z)^2 \equiv 0$. Define

$$\tilde{\sigma}_j(y, Z) := (Z + y)\pi_{j+q-1}(y, Z)/(Z^q + Z).$$

Rewriting the above we have that

$$\left(\sum_{j=0}^q \sigma_j(y, Z)T^j \right) \left(\sum_{j=0}^{\infty} \tilde{\sigma}_j(y, Z)T^j \right) = 1. \quad (3)$$

Lemma 4.2 For all $y, z \in GF(q)$ and $j \leq q$

$$\sigma_j(y, z) = \tilde{\sigma}_j(z, y).$$

Proof. If $y \neq z$ then Lemma 4.1 (ii) implies that $\rho(T, z, y) = \sum_{j=0}^q \tilde{\sigma}_j(y, z)T^j$ and the lemma is proved. If $y = z$ then $\sigma_j(y, y) = \tilde{\sigma}_j(y, y) = 0$ for $j \neq 0$ or $q - 1$ and for $j = 0$ or $q - 1$ they are both 1.

□

5 Waring's formula

To make use of Lemma 4.2 we need to be able to calculate $\sigma_j(y, z)$ and in theory Waring's formula allows us to do this.

Waring's formula [9, pp.30] relates power sums with symmetric functions and says that

$$\pi_k = \sum \frac{(i_1 + i_2 + \dots + i_n - 1)!k}{i_1!i_2! \dots i_n!} \sigma_1^{i_1} \sigma_2^{i_2} \dots \sigma_n^{i_n},$$

where the sum runs over all combinations $i_1 + 2i_2 + \dots + ni_n = k$.

In the previous section we saw that $\pi_k = 0$ for $k < q - 1$ and $\pi_{q-1+k} = 0$ when $k < q - 1$ is odd, so we are only interested in the formula when $q - 1 \leq k < 2q - 2$ and k is odd. In this case each term in the right-hand side of the formula must have a σ_{q-1} as this is the only σ_j that is not zero when j is odd.

$$\pi_{q-1+k} = \sigma_{q-1} \sum \frac{(i_1 + i_2 + \dots + i_{n-1})!}{i_1! i_2! \dots i_{n-1}!} \sigma_1^{i_1} \sigma_2^{i_2} \dots \sigma_{n-1}^{i_{n-1}},$$

where the sum runs over all combinations $i_1 + 2i_2 + \dots + (n-1)i_{n-1} = k$. By definition $\tilde{\sigma}_k = \pi_{q-1+k}/\sigma_{q-1}$ so we conclude that

$$\tilde{\sigma}_k = \sum \frac{(i_1 + i_2 + \dots + i_{n-1})!}{i_1! i_2! \dots i_{n-1}!} \sigma_1^{i_1} \sigma_2^{i_2} \dots \sigma_{n-1}^{i_{n-1}}. \quad (4)$$

Consider equation (3). We could easily let both sums be infinite (defining $\sigma_j = 0$ for $j > q$) and then this equation would be identical if we replace $\tilde{\sigma}_j$ with σ_j and vice-versa. Waring's formula derives from this equation, so we can reverse the role of the σ_j 's and the $\tilde{\sigma}_j$'s in (4) and get the formula

$$\sigma_k = \sum \frac{(i_1 + i_2 + \dots + i_{n-1})!}{i_1! i_2! \dots i_{n-1}!} \tilde{\sigma}_1^{i_1} \tilde{\sigma}_2^{i_2} \dots \tilde{\sigma}_{n-1}^{i_{n-1}}.$$

Denote the coefficient of x^i in $f(x, y)^j$ by $\phi_{i,j}(y)$.

Lemma 5.1 The following hold for $0 < k \leq q$ and k even.

(i)

$$\tilde{\sigma}_k(y, Z) = (Z + y) \left(\sum_{i=1}^{k-1} \binom{k-1}{i} \phi_{q-1-k+i,i}(y) Z^{k-1-i} \right)$$

and the terms of highest degree are

$$\begin{aligned} \tilde{\sigma}_k(y, Z) &= (Z + y)(\psi_{q-k}(y)Z^{k-2} + \psi_{q-k/2}(y)^2 Z^{k-3} \\ &+ \binom{k-1}{3} \phi_{q-k+2,3}(y)Z^{k-4} + \psi_{q-k/4}(y)^4 Z^{k-5} \\ &+ \binom{k-1}{5} \phi_{q-k+4,5}(y)Z^{k-6} + \dots). \end{aligned}$$

(ii)

$$\begin{aligned}
\sigma_k(y, Z) &= (Z + y)(\psi_{q-k}(y)Z^{k-2} \\
&+ [\binom{k-1}{3}\phi_{q-k+2,3}(y) + y\psi_{q-k/2}(y)^2 + \sum_{2m+n=k} \psi_{q-m}(y)^2\psi_{q-n}(y)]Z^{k-4} \\
&+ [\binom{k-1}{5}\phi_{q-k+4,5}(y) + y^2 \sum_{2m+n=k} \psi_{q-m}(y)^2\psi_{q-n}(y) + \\
&\sum_{2m+n=k} \binom{n-1}{3}\psi_{q-m}(y)^2\phi_{q-n+2,3}(y)]Z^{k-6} + \dots)
\end{aligned}$$

Proof. By definition we have that

$$(Z^q + Z)\tilde{\sigma}_k(y, Z) = (Z + y)\pi_{k+q-1}(y, Z).$$

Also

$$\begin{aligned}
\pi_{k+q-1}(y, Z) &= \sum_{x \in GF(q)} (xZ + f(x, y))^{k+q-1} \\
&= \sum_{x \in GF(q)} (xZ^q + f(x, y))(xZ + f(x, y))^{k-1} \\
&= \sum_{i=0}^{k-1} \binom{k-1}{i} \sum_{x \in GF(q)} x^{k-i} f(x, y)^i Z^{q+k-1-i} + x^{k-1-i} f(x, y)^{i+1} Z^{k-1-i}.
\end{aligned}$$

Hence

$$\pi_{k+q-1}(y, Z) = (Z^q + Z) \sum_{i=1}^{k-1} \binom{k-1}{i} \phi_{q-1-k+i, i} Z^{k-1-i}$$

which gives the first part of (i).

Recall that by Cororally 2.3 we have that $\psi_k = 0$ when k is odd. For the second part of (i) expand the sum and note that $\phi_{q-k-1,0} = 0$, $\phi_{q-k,1} = \psi_{q-k}$ and $\binom{k-1}{2}\phi_{q-k+1,2} = \binom{k-1}{2}\psi_{q-k/2}^2 = \psi_{q-k/2}^2$. If $k = 2 \pmod{4}$ then $\phi_{q-k+3,4} = \psi_{(2q-k+2)/4}^4$ which is zero unless $k = 2 \pmod{8}$. If $k = 0 \pmod{4}$ then $\phi_{q-k+3,4} = \psi_{q-k/4}^4$. Hence $\binom{k-1}{4}\phi_{q-k+3,4} = \psi_{q-k/4}^4$.

Note that the degree in Z of $\tilde{\sigma}_k(y, Z)$ is at most $k-1$. Therefore to calculate the terms of degree at least $k-5$ in Z in σ_k it is enough to consider the following terms

$$\sigma_k = \tilde{\sigma}_k + \tilde{\sigma}_{k/2}^2 + \sum_{2m+n=k} \tilde{\sigma}_m^2 \tilde{\sigma}_n + \tilde{\sigma}_{k/4}^4 + \sum_{4m+n=k} \tilde{\sigma}_m^4 \tilde{\sigma}_n + \dots$$

and compute using (i). This calculation makes repeated use of the fact that $\psi_k = 0$ when k is odd. For example, in the computation of the coefficient of Z^{q-5} , one needs that if $\binom{n-1}{2}\psi_{q-n/2} \neq 0$ then $n = 0 \pmod{4}$, which implies that $\binom{n-1}{2} = 1$ and so

$$\sum_{2m+n=k} \binom{n-1}{2} \psi_{q-m}^2 \psi_{q-n/2}^2 = \sum_{2m+2r=k} \psi_{q-m}^2 \psi_{q-r}^2 = \psi_{q-k/4}^2 \psi_{q-k/4}^2 = \psi_{q-k/4}^4.$$

□

6 Necessary conditions

In this section we shall apply the calculations in Lemma 5.1 to Lemma 4.2 and get conditions on the coefficients of an ovoid polynomial $f(X, Y)$.

Theorem 6.1 (i) The coefficient of y^j in $\psi_{q-k}(y)$ is zero if $\binom{k-1}{j} = 0$.

(ii) The coefficient of y^j in

$$\sum_{2m+n=k} \psi_{q-m}^2 \psi_{q-n}$$

is zero if $k \equiv 2(4)$ and $\binom{k-1}{j} = 0$.

(iii) The coefficient of y^j in

$$\sum_{2m+n=k} \psi_{q-m}^2 \psi_{q-n}$$

is zero if $k \equiv 2(8)$ and $\binom{k-1}{j+2} = 0$.

(iv) The coefficient of y^j in

$$\sum_{2m+n=q-k+2} \psi_m^2 \psi_n + y^2 \psi_{q-k}$$

is zero if $k \equiv 0(4)$ and $\binom{k-1}{j} = 0$.

Proof.

By Lemma 4.2 we have that for all $y, z \in GF(q)$ and $k \leq q$

$$\sigma_k(y, z) = \tilde{\sigma}_k(z, y).$$

By Lemma 5.1 this gives

$$(z + y)(\psi_{q-k}(y)z^{k-2} +$$

$$\begin{aligned}
& + \left[\binom{k-1}{3} \phi_{q-k+2,3}(y) + y \psi_{q-k/2}(y)^2 + \sum_{2m+n=k} \psi_{q-m}(y)^2 \psi_{q-n}(y) \right] z^{k-4} \\
& + \left[\binom{k-1}{5} \phi_{q-k+4,5}(y) + y^2 \sum_{2m+n=k} \psi_{q-m}(y)^2 \psi_{q-n}(y) + \right. \\
& \quad \left. \sum_{2m+n=k} \binom{n-1}{3} \psi_{q-m}(y)^2 \phi_{q-n+2,3}(y) \right] z^{k-6} + \dots \\
& = (z+y) \left(\sum_{i=1}^{k-1} \binom{k-1}{i} \phi_{q-1-k+i,i}(z) y^{k-1-i} \right)
\end{aligned}$$

for all $y, z \in GF(q)$. This equation has terms in y (and z) of degree at most $q-1$ and is therefore an identity.

- (i) This follows by considering the coefficient of $(z+y)y^j z^{k-2}$.
- (ii) This follows by considering the coefficient of $(z+y)y^j z^{k-4}$ and noting that $\binom{k-1}{3} = 0$ and $\psi_{q-k/2} = 0$ when $k \equiv 2(4)$.
- (iii) This follows by considering the coefficient of $(z+y)y^{j+2} z^{k-6}$. Note that $k \equiv 2(8)$ implies that $\binom{k-1}{5} = 0$ and

$$\sum_{2m+n=k} \binom{n-1}{3} \psi_{q-m}(y)^2 \phi_{q-n+2,3}(y)$$

is equal to zero because $\psi_{q-m} \neq 0$ implies that $m \equiv 0(2)$ and $2m+n=k$ implies that $n \equiv 2(4)$, whence $\binom{n-1}{3} = 0$.

- (iv) This follows by considering the coefficient of $(z+y)y^j z^{k-4}$ and noting that $\binom{k-1}{3} = 1$ when $k \equiv 0(4)$ and

$$\phi_{q-k+2,3}(y) = \sum_{2m+n=q-k+2} \psi_m^2 \psi_n + y^2 \psi_{q-k} + y \psi_{q-k/2}^2 + \sum_{2m+n=k} \psi_{q-m}^2 \psi_{q-n}.$$

□

Corollary 6.2 If the coefficient of $x^i y^j$ in $f(x, y) + xy$ is non-zero then i and j have disjoint binary expansions.

Proof.

This follows directly from Theorem 6.1 (i). The coefficient of y^j in ψ_i is the coefficient of $x^i y^j$ in $f(x, y)$ and is zero if $\binom{q-1-i}{j} = 0$. Now note that $\binom{q-1-i}{j} \neq 0$ if and only if i and j have disjoint binary expansions.

□

Theorem 6.3 For all $a \in GF(q)$

(i) the coefficient of y^j in $\bar{\psi}_{q-k}$ is zero if $\binom{k-1}{j} = 0$.

(ii) the coefficient of y^j in

$$\sum_{2m+n=k} \bar{\psi}_{q-m}^2 \bar{\psi}_{q-n}$$

is zero if $k \equiv 2(4)$ and $\binom{k-1}{j} = 0$;

(iii) the coefficient of y^j in

$$\sum_{2m+n=k} \bar{\psi}_{q-m}^2 \bar{\psi}_{q-n}$$

is zero if $k \equiv 2(8)$ and $\binom{k-1}{j+2} = 0$;

(iv) the coefficient of y^j in

$$\sum_{2m+n=q-k+2} \bar{\psi}_m^2 \bar{\psi}_n + y^2 \bar{\psi}_{q-k}$$

is zero if $k \equiv 0(4)$ and $\binom{k-1}{j} = 0$.

Proof. In Section 4, Section 5 and this section we could replace $f(x, y)$ with $f(x, y + ax)$ and follow the same arguments. This theorem is then a repeat of Theorem 6.1.

□

Corollary 6.4 If $\binom{i}{j} = 0$ then the polynomials

$$\partial^j \tau_i \equiv 0.$$

Proof. By Theorem 6.3 (i) and Lemma 2.4 we have that $\partial^j \tau_{q-k+j} = 0$ if $\binom{k-1}{j} = 0$. It is identically zero since it has degree less than q and is zero for all $a \in GF(q)$. Put $i = q - k + j$ and note that $\binom{q-i+j-1}{j} = \binom{i}{j}$.

□

Note that if $2^r | i$ then τ_i is a 2^r -th power.

Corollary 6.5 For all a the polynomial in y

$$\bar{\psi}_{q-2}^2 \bar{\psi}_{q-6} + \bar{\psi}_{q-4}^2 \bar{\psi}_{q-2}$$

is identically zero.

Proof. By Lemma 2.4 and Corollary 6.2 the polynomials

$$\bar{\psi}_{q-2}(y, a) = \tau_{q-2}(a),$$

$$\bar{\psi}_{q-4}(y, a) = \tau_{q-4}(a) + \partial^2 \tau_{q-2}(a) y^2$$

and

$$\bar{\psi}_{q-6}(y, a) = \tau_{q-6}(a) + \partial^4 \tau_{q-2}(a) y^4.$$

Hence as a polynomial in y

$$\bar{\psi}_{q-2}^2 \bar{\psi}_{q-6} + \bar{\psi}_{q-4}^2 \bar{\psi}_{q-2}$$

has terms of degree zero and 4. By Theorem 6.3 (ii) and (iii) with $k = 10$ both of these coefficients are zero for all $a \in GF(q)$.

□

7 The classification when $q = 16$

By Theorem 2.2 with $k = 3$ and $b = 15$ and 11 we have that

$$\bar{\psi}_{14}^2 \bar{\psi}_2 + \bar{\psi}_{12}^2 \bar{\psi}_6 + \bar{\psi}_{10}^3 + \bar{\psi}_8^2 \bar{\psi}_{14} = 0 \quad (5)$$

and

$$\bar{\psi}_{12}^2 \bar{\psi}_2 + \bar{\psi}_{10}^2 \bar{\psi}_6 + \bar{\psi}_8^2 \bar{\psi}_{10} + \bar{\psi}_6^2 \bar{\psi}_{14} = 0 \quad (6)$$

Let us first do the case $\bar{\psi}_{14} = \tau_{14} \neq 0$. By Corollary 6.5 we have that

$$\bar{\psi}_{14}^2 \bar{\psi}_{10} + \bar{\psi}_{12}^2 \bar{\psi}_{14} = 0. \quad (7)$$

If we look at $\bar{\psi}_{12}^2 \bar{\psi}_{14}(5) + \bar{\psi}_{14}^3(6)$ and apply Corollary 6.5 where possible we obtain the equation

$$\bar{\psi}_{14}(\bar{\psi}_{10}^2 + \bar{\psi}_6 \bar{\psi}_{14}) = 0. \quad (8)$$

Now from Lemma 2.4 and Corollary 6.2 the polynomials

$$\bar{\psi}_{14}(y, a) = \tau_{14}(a),$$

$$\bar{\psi}_{10}(y, a) = \tau_{10}(a) + \partial^4 \tau_{14}(a) y^4$$

and

$$\bar{\psi}_6(y, a) = \tau_6(a) + \partial^8 \tau_{14}(a) y^8.$$

The polynomial $\tau_{14}(a) = \sum_{j=0}^{14} c_{14-j,j} a^j$ has degree 14. By considering the coefficient of y^8 the polynomial

$$\tau_{14}((\partial^4 \tau_{14})^2 + \tau_{14}(\partial^8 \tau_{14}))$$

is zero for all $a \in GF(16)$. By calculating the terms of highest degree directly we see that it is of degree at most 30 and it is also a square. Hence it is identically zero and

$$(\partial^4 \tau_{14})^2 + \tau_{14}(\partial^8 \tau_{14}) \equiv 0. \quad (9)$$

The coefficient of y^4 in equation (7) tells us that

$$\tau_{14}((\partial^2 \tau_{14})^2 + \tau_{14} \partial^4 \tau_{14})$$

is zero for all $a \in GF(16)$. Hence

$$\tau_{14} \partial^8 \tau_{14} ((\partial^2 \tau_{14})^2 + \tau_{14}(\partial^4 \tau_{14}))$$

and

$$\partial^4 \tau_{14} ((\partial^2 \tau_{14})^2 + \tau_{14}(\partial^4 \tau_{14}))$$

is zero for all $a \in GF(16)$. This polynomial has degree at most 30 and is a square and hence is identically zero.

If $\partial^4 \tau_{14} \equiv 0$ then $\partial^4 \tau_{14} = \sum_{j=0}^{14} \binom{j}{4} c_{14-j,j} a^{j-4} \equiv 0$ and $c_{14-j,j} = 0$ for $j = 4, 6, 12, 14$. Now we could have started all the calculations with $f(x, y) = \sum c_{j,i} x^i y^j$. If we would again have that $\partial^4 \tau_{14} \equiv 0$ then $\sum_{j=0}^{14} \binom{j}{4} c_{j,14-j} = 0$ and $c_{14-j,j} = 0$ for $j = 0, 2, 8, 10$, which would then give $\tau_{14} \equiv 0$. So we can assume that $\partial^4 \tau_{14} \not\equiv 0$ in at least one of the cases and deduce that

$$\tau_{14} \partial^4 \tau_{14} \equiv (\partial^2 \tau_{14})^2.$$

The polynomial $\partial^2 \tau_{14}$ is a 4-th power of degree 12 and so over some field extension there exist linear polynomials u, v and w such that $\partial^2 \tau_{14} = (uvw)^4$. The polynomial $\partial^4 \tau_{14}$ divides $(uvw)^8$, it has (possibly) non-zero terms of degree 0, 2, 8 and 10 and so $\partial^4 \tau_{14} = v^8 w^2$ choosing u, v and w suitably. Hence $\tau_{14} = w^6 u^8$ and we can assume that one of u and w is monic so let us assume that it is w , i.e. assume $\partial w = 1$. Note that u and w have coefficients in $GF(16)$ since τ_{14} does. Substituting into equation (9) gives

$$w^4 u^{16} + w^{12} u^8 (\partial u)^8 = 0$$

and hence for some non-zero $\gamma \in GF(16)$

$$\tau_{14} = \gamma w^{14}.$$

The coefficient of y^0 in equation (7) and equation (8) tell us that

$$\tau_{14}(\tau_{12}^2 + \tau_{10}\tau_{14}) = 0$$

and

$$\tau_{14}(\tau_{10}^2 + \tau_6\tau_{14}) = 0$$

for all $a \in GF(16)$. Hence

$$\gamma w^2(\tau_{12}^2 + \gamma w^{14}\tau_{10}) = 0$$

and

$$\gamma w^2(\tau_{10}^2 + \gamma w^{14}\tau_6) = 0.$$

Both of these equations have degree less than 32 and are squares and hence are both identically zero. Now this implies that w^7 divides τ_{10} which since it is a square is in fact divisible by w^8 . This then implies that w^{22} divides τ_{12}^2 which is an 8-th power, by Corollary 6.4, and hence is in fact divisible by w^{24} . We conclude that for some $\beta \in GF(16)$,

$$\tau_{12} = \gamma\beta w^{12},$$

$$\tau_{10} = \gamma\beta^2 w^{10}$$

and

$$\tau_6 = \gamma\beta^4 w^6.$$

The coefficient of y^0 in equation (5) now simplifies to give

$$\gamma^2 w^{28}(\tau_2 + a) + \gamma w^{14}\tau_8^2 = 0$$

from which it follows that

$$\tau_8 \equiv (\gamma(\tau_2 + a)/w)^8.$$

Finally we need two more of the equations from Theorem 2.2, the equations with $k = 3$ and $b = 7$ and with $k = 5$ and $b = 13$;

$$\overline{\psi}_{10}^2 \overline{\psi}_2 + \overline{\psi}_8^2 \overline{\psi}_6 + \overline{\psi}_6^2 \overline{\psi}_{10} + \overline{\psi}_4^2 \overline{\psi}_{14} = 0 \quad (10)$$

and

$$\overline{\psi}_6^4 \overline{\psi}_4 + \overline{\psi}_{12}^4 \overline{\psi}_{10} + \overline{\psi}_4^4 \overline{\psi}_{12} + \overline{\psi}_{14}^4 \overline{\psi}_2 = 0. \quad (11)$$

The coefficient of y^0 in equation (10) gives

$$\tau_4 = \gamma\beta^5 w^4$$

and the coefficient of y^0 in equation (11) gives

$$\tau_2 + a = \gamma\beta^6 w^2.$$

However this is impossible since τ_2 is a square in the variable a .

We can assume now that $\bar{\psi}_{14} = \tau_{14} = 0$ and that $\bar{\psi}_{12} \equiv \tau_{12} \neq 0$. Equation (6) and equation (5) become

$$\bar{\psi}_{12}^2 \bar{\psi}_2 + \bar{\psi}_{10}^2 \bar{\psi}_6 + \bar{\psi}_8^2 \bar{\psi}_{10} = 0 \quad (12)$$

and

$$\bar{\psi}_{12}^2 \bar{\psi}_6 + \bar{\psi}_{10}^3 = 0 \quad (13)$$

respectively. $\bar{\psi}_2$ has a single term of degree 1 in a and hence is not identically zero and so equation (12) implies that $\bar{\psi}_{10} \neq 0$. Hence $\tau_{10} \neq 0$. If $\partial^8 \tau_{10} = 0$ then $c_{2,8} = c_{0,10} = 0$. If we then replace $f(x, y)$ by $f(y, x)$ in all the preceding and have again that $\partial^8 \tau_{10} = 0$ we would have that $c_{8,2} = c_{10,0} = 0$ and that $\tau_{10} = 0$. Hence in at least one of the cases we can assume that $\partial^8 \tau_{10} \neq 0$.

The coefficient of y^8 in equation (12) gives

$$\tau_{12}^2 (\partial^8 \tau_{10}) + \tau_{10} (\partial^4 \tau_{12})^2 = 0 \quad (14)$$

for all $a \in GF(16)$ and is identically zero since it is a square and of degree at most 26. Now $\partial^4 \tau_{12}$ is divisible by w^8 for some monic polynomial w linear in a (it is an 8-th power of degree at most 8) and since $\partial^8 \tau_{10}$ has degree at most two, w^{14} divides τ_{12}^2 and since it is a 8-th power w^{16} divides τ_{12}^2 .

The coefficient of y^0 in equation (13) gives

$$\tau_6 \tau_{12}^2 + \tau_{10}^3 \equiv 0 \quad (15)$$

and it follows from this equation that w^{16} divides τ_{10}^3 and hence that w^6 divides τ_{10} . Again from equation (14) we now have that w^{20} divides τ_{12}^2 which equation (15) implies w^7 divides τ_{10} . Again from equation (14) we now have that w^{21} divides τ_{12}^2 and since it is a 8-th power that w^{24} divides τ_{12}^2 . Hence there is some non-zero $\gamma \in GF(q)$ such that

$$\tau_{12} = \gamma w^{12}.$$

There is some monic polynomial u , linear in a and some constant $\beta \neq 0$ such that

$$\tau_{10} = \gamma \beta w^8 u^2$$

and from equation (15) that

$$\tau_6 = \gamma \beta^3 u^6.$$

Theorem 2.2 with $k = 5$ and $b = 15$ gives

$$\bar{\psi}_6^5 + \bar{\psi}_{12}^5 = 0$$

and the coefficient of y^0 tells us that $\gamma^5\beta^{15}u^{30} + \gamma^5w^{60} = 0$. Reduce modulo $u^{16} = u$ and $w^{16} = w$ and we get $u^{15} = w^{15}$. Therefore, since they are both linear, monic and have the same zero, $u = w$.

Now the coefficient of y^0 in equation (12) gives

$$(\tau_2 + a)\gamma^2w^{24} + \gamma^3\beta^5w^{26} + \gamma\beta w^{10}\tau_8^2 = 0$$

for all $a \in GF(q)$.

Theorem 2.2 with $k = 3$ and $b = 3$ gives

$$\bar{\psi}_2\bar{\psi}_8^2 + \bar{\psi}_6^3 + \bar{\psi}_{10}\bar{\psi}_4 = 0$$

from which the coefficient of y^0 tells us

$$(\tau_2 + a)\tau_8^2 + \gamma^3\beta^9w^3 + \gamma\beta w^{10}\tau_4^2 = 0$$

for all $a \in GF(q)$.

By Corollary 6.4 τ_4 is a 4-th power, so these equations imply that

$$\tau_4^2 = \gamma^2\beta^8w^8 + \beta^{-2}w^4(\tau_2 + a)(a + \tau_2 + \gamma\beta^5w^2)$$

is an 8-th power and so $(\tau_2 + a)(a + \tau_2 + \gamma\beta^5w^2)$ should be divisible by w^4 which it is not, since τ_2 is a square in the variable a .

Finally if $\bar{\psi}_{14} = \bar{\psi}_{12} \equiv 0$ then from equation (13) $\bar{\psi}_{10} \equiv 0$. Theorem 2.2 with $k = 3$ and $b = 7$ gives

$$\bar{\psi}_6\bar{\psi}_8^2 = 0$$

and with $k = 3$ and $b = 3$ gives

$$\bar{\psi}_2\bar{\psi}_8^2 + \bar{\psi}_6^3 = 0. \tag{16}$$

Hence $\bar{\psi}_6 \equiv 0$ and the coefficient of y^0 in equation (16) gives

$$(\tau_2 + a)\tau_8^2 = 0$$

from which it immediately follows that $\tau_8 \equiv 0$.

Theorem 2.2 with $k = 5$ and $b = 5$ implies that $\bar{\psi}_4 \equiv 0$ and hence $\tau_4 \equiv 0$.

The only non-zero τ_j is now τ_2 and so

$$f(x, y) = xy + \alpha x^2 + \beta y^2.$$

Hence the only ovoids of $PG(3, 16)$ are the elliptic quadrics.

8 Final comments

It seems that if we follow the same attack for the case $q = 32$ we have problems almost immediately. We would like to be able to show that $\tau_{30} = \gamma w^{30}$ for some monic linear polynomial w . However the (differential) equations that I can deduce from Theorem 2.2 and Corollary 6.5 are of too high degree to conclude any polynomial identities for τ_{30} . For example, it is true that from Corollary 6.5 that

$$\tau_{30}((\partial^2 \tau_{30})^2 + \tau_{30} \partial^4 \tau_{30})$$

is a square and is zero for all $a \in GF(32)$. But the polynomial has degree 86 so we cannot conclude that it is identically zero.

Finally, I would like to thank both referees for their comments and suggestions, they were greatly appreciated.

References

- [1] A. Barlotti, Un'estensione del teorema di Segre-Kustaanheimo, *Boll. Un. Mat. Ital.*, bf 10, (1955), 96–98.
- [2] M. R. Brown, Ovoids of $PG(3, q)$, q even, with a conic section, *J. London Math. Soc.*, **62**, (2000), 569–582.
- [3] M. R. Brown, The determination of ovoids of $PG(3, q)$ containing a pointed conic, *J. Geom.*, **67**, (2000), 61–72.
- [4] P. Dembowski, Inversive planes of even order, *Bull. Amer. Math. Soc.*, **69**, 1963, 850–854.
- [5] G. Fellegara, Gli ovaloidi di uno spazio tridimensionale di Galois di ordine 8, *Atti. Accad. Naz. Lincei Rend.*, **32**, (1962), 170–176.
- [6] D. G. Glynn, A condition for the existence of ovals in $PG(2, q)$, q even, *Geom. Dedicata*, **32**, (1989), 247–252.
- [7] D. G. Glynn, A condition for the existence of ovoids in $PG(3, q)$, q even. In [G. Faina and G. Tallini, eds. *Giornate di Geometria Combinatoria*, Perugia 1993], pp.213–225.
- [8] D. G. Glynn, Plane representations of ovoids, *Bull. Belg. Math. Soc.* **5** (1998), 275–286.
- [9] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edition, Cambridge, 1997.

- [10] C. M. O’Keefe and T. Penttila, Ovoids of $PG(3, 16)$ are elliptic quadrics, *J. Geom*, **38**, (1990), 95–106.
- [11] C. M. O’Keefe and T. Penttila, Ovoids of $PG(3, 16)$ are elliptic quadrics, II, *J. Geom*, **44**, (1992), 140–159.
- [12] C. M. O’Keefe, T. Penttila and G. F. Royle, Classification of ovoids in $PG(3, 32)$, *J. Geom*, **50**, (1994), 143–150.
- [13] G. Panella, Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, *Boll. Un. Mat. Ital.*, **10**, (1955), 507–513.
- [14] T. Penttila and C. E. Praeger, Ovoids and translation ovals, *J. London Math. Soc.*, **56**, (1997), 607–624.
- [15] S. E. Payne and J. A. Thas, *Finite generalized quadrangles*, Pitman, London, 1984.
- [16] B. Segre, On complete caps and ovaloids in three-dimensional Galois spaces of charactersitic two, *Acta Arith.*, **5**, (1959), 315–332.
- [17] J. A. Thas, Ovoidal translation planes, *Arch. Math.*, **23**, (1972), 110–112.
- [18] J. Tits, Ovoides et groupes de Suzuki, *Arch. Math.*, **13**, (1962), 187–198.