# (Hyper)ovals and ovoids in projective spaces

Matthew Brown
Ghent University

Socrates Intensive Course
Finite Geometry and its Applications
Ghent, 3–14 April 2000

## Contents

# 1 Introduction

In 1947 Bose ([4]) considered the application of finite geometries to the theory of confounding in factorial designs. Bose was able to display that such designs could have particular desirable properties by constructing examples from the affine space $AG(n, q)$. In this context an important statistical question (what is the maximum number $m_t(n, q)$ of factors in a symmetrical factorial design where each factor is at $q$ levels and each block contains $q^n$ treatments, while interactions of order $t$ and lower remain unconfounded?) was equivalent to the geometrical question: what is the maximum number $m_t(n, q)$ of points in $PG(n, q)$ such that any $t$ of them span a $PG(t-1, q)$? In particular for the case where $t = 3$ we have: what is the maximum number $m(n, q)$ (omitting the 3 from the notation) of points of $PG(3, q)$ such that any 3 of them span a plane. In other words what is the size of the largest set of points of $PG(n, q)$ with the property that no three are collinear? Bose was able to show that $m(2, q) = q+2$ when $q$ is even and $m(2, q) = q+1$ when $q$ is odd. For $PG(3, q)$ he proved that $m(3, q) = q^2+1$ when $q$ is odd and that $m(3, 2) = 8$. We will see these facts for ourselves later in the notes.

While the statistical considerations are not relevant to us, the geometrical questions remain. Can we construct, characterise and/or classify maximum sized sets of points in $PG(2, q)$ and $PG(3, q)$ such that no three points are collinear?

It should be noted that Bose's paper did not contain a determination of $m(3, q)$ for $q > 2$ and even, that is the maximum size of a set of points of $PG(3, q)$ such that no three are collinear. This was done by Qvist ([63]) where it was shown that $m(3, q) = q^2 + 1$ in this case. In this paper Qvist also showed that $m(2, q)$ is an upper bound for the size of a set of points of a projective plane of order $q$ (not necessarily desarguesian), no three collinear.

Segre called a set of $m(2, q)$ points of a projective plane of order $q$ with the property that no three are collinear an *oval*. A set of $m(3, q) = q^2 + 1$ points of $PG(3, q)$, no three collinear was called an *ovaloid*.

In 1962 Tits ([80]) defined an *ovoid* to be a set of points $\Omega$ in a projective geometry $\mathcal{S}$ (not required to be finite nor desarguesian) such that for any $P \in \Omega$ the union of all lines $\ell$ with $\ell \cap \Omega = \{P\}$ is a hyperplane. In $PG(n, q)$ an ovoid can only exist if $n \leq 3$ (see [15] or Theorem 3.4). It is immediate from the definition of an ovoid that in $PG(3, q)$ it has size $q^2 + 1$ and for a finite projective plane of order $q$ it has size $q + 1$. Thus an ovoid of $PG(3, q)$ is an ovaloid for $q > 2$.

It is straight-forward to see that any set of $q + 1$ points of a projective plane of order $q$ (not necessarily desarguesian), no three collinear, is an ovoid of the plane, and so this is an equivalent definition. Dembowski ([15]), amongst others, called such a set of points an *oval*, differing from the use of the same term by Segre in the case where the order of the projective plane is even. With the adoption of the term oval to mean a set of $q + 1$ points, no three collinear, in a projective plane, a set of $q + 2$ points, no three collinear in a projective plane of even order (an oval in the sense of Segre) became known as a *hyperoval*.

Barlotti ([1, 2]) and Panella ([49]) showed that in $PG(3, q)$, $q > 2$, an ovaloid has the property that for any fixed point of the ovoid the union of the tangent lines forms a plane. That is, the definition of an ovaloid *coincides* with the definition of an ovoid (although Tits had yet to make his definition of an ovoid at the time Barlotti and Panella proved their result). The preceding discussion should hopefully explain the following definitions and put them into an historical context. Many of the results alluded to above will be fleshed out in the work that follows.

**Definition 1.1.** *An* **oval** *of* $\mathrm{PG}(2,q)$ *is a set of* $q+1$ *points no three collinear.*

**Definition 1.2.** *A* **hyperoval** *of* $\mathrm{PG}(2,q)$ *is a set of* $q+2$ *points no three collinear.*

**Definition 1.3.** *An* **ovoid** *of* $\mathrm{PG}(3,q)$*,* $q>2$*, is a set of* $q^2+1$ *points no three collinear.*

It should be noted that the definition of an oval and the definition of a hyperoval apply equally to non-desarguesian projective planes but we shall not be considering such objects here.

# 2 (Hyper)ovals in $\mathrm{PG}(2,q)$

## 2.1 Introduction and preliminaries

In this section we establish some elementary properties of ovals and hyperovals before considering the $q$ odd and $q$ even cases separately. For an excellent introduction to ovals see Chapter 8 of [27].

Following the Bose-Segre approach to (hyper)ovals we make the following definition.

**Definition 2.1.** *A* $k$**-arc** *of* $\mathrm{PG}(2,q)$ *is a set of* $k$ *points no three collinear.*

As introduced in Section 1 we will let $m(2,q)$ denote the maximum size of a $k$-arc.

If $\mathcal{K}$ is a $k$-arc of $\mathrm{PG}(2,q)$ then each line of $\mathrm{PG}(2,q)$ meets $\mathcal{K}$ in either 0, 1 or 2 points and are called, resepctively an *external* line of $\mathcal{K}$, a *tangent* of $\mathcal{K}$ and a *secant* of $\mathcal{K}$.

**Classical Examples:**

(1) The points of $\mathrm{PG}(2,q)$ that are the zeros of an irreducible quadratic form are the points of a $(q+1)$-arc called a *conic*. For instance, let the points of $\mathrm{PG}(2,q)$ have coordinates $(x_0,x_1,x_2)$ and consider the irreducible quadratic form $x_1^2+x_0x_2$. The corresponding conic is

$$\mathcal{C}=\{(1,t,t^2)\,:\,t\in \mathrm{GF}(q)\}\cup\{(0,0,1)\}$$

Note that there is only one equivalence class of conics under the group of $\mathrm{PG}(2,q)$.

(2) For $q$ even, since the square map is an automorphism of the field, it is easy to verify that the point $(0,1,0)$ is on the tangent of $\mathcal{C}$ at each point of $\mathcal{C}$. Hence

$$\mathcal{C}\cup\{(0,1,0)\}=\{(1,t,t^2)\,:\,t\in \mathrm{GF}(q)\}\cup\{(0,0,1),(0,1,0)\}$$

is a hyperoval of $\mathrm{PG}(2,q)$. The point $N(0,1,0)$ is called the *nucleus* of the conic $\mathcal{C}$, and the hyperoval $\mathcal{C}\cup\{N\}$ is called the *regular hyperoval.*

In fact this property of the conic in $\mathrm{PG}(2,q)$, $q$ even, to have all of its tangents intersecting in a point, the nucleus, is true of all ovals when $q$ is even.

**Lemma 2.2.** *Let $\mathcal{O}$ be an oval of* $\mathrm{PG}(2,q)$, *$q$ even. The $q+1$ tangents to $\mathcal{O}$ are concurrent (i.e. intersect in a common point) called the* **nucleus** *of $\mathcal{O}$.*

**Proof.** Let $P$ be any point of $\mathrm{PG}(2,q)$ off $\mathcal{O}$. Since the lines through $P$ partition the points of $\mathcal{O}$ and $q+1$ is odd, $P$ must be on at least one tangent to $\mathcal{O}$. Now let $\ell$ be a secant to $\mathcal{O}$ with $\ell \cap \mathcal{O} = \{Q, R\}$. The tangents of $\mathcal{O}$ at the points $\mathcal{O} \setminus \{Q, R\}$ meet $\ell$ in distinct points. Thus any point not on $\mathcal{O}$ that lies on a secant must lie on exactly one tangent. If we take the intersection of two tangents to $\mathcal{O}$ this point lies on two tangents and so cannot lie on any secants. Consequently it lies on all the tangents to $\mathcal{O}$. $*\square$

This result means that for $q$ even an oval $\mathcal{O}$ can *always* be extended *uniquely* to a hyperoval $\mathcal{H}$. The oval $\mathcal{O}$ is said to *complete* to $\mathcal{H}$. Note that the proof is purely combinatorial and so also applies to non-desarguesian projective planes.

We now prove the Bose result on the maximum size of a $k$-arc in $\mathrm{PG}(2,q)$.

**Lemma 2.3 (Bose [4]).**

$$m(2,q) = \begin{cases} q+1, & \textit{for } q \textit{ odd} \\ q+2, & \textit{for } q \textit{ even} \end{cases}$$

**Proof.** If $q$ is even we have the example of the conic plus its nucleus, so $m(2,q) \geq q+2$. If $\mathcal{H}$ is any hyperoval of $\mathrm{PG}(2,q)$, $q$ even, and $P \in \mathcal{H}$, then each of the $q+1$ lines of $\mathrm{PG}(2,q)$ on $P$ contains a second point of $\mathcal{H}$. Hence there is no way to extend $\mathcal{H}$ to a bigger arc. So $m(2,q) = q+2$ for $q$ even.

Now suppose that $q$ is odd. From the example of the conic we have that $m(2,q) \geq q+1$. So now aiming for a contradiction suppose that there exists a hyperoval $\mathcal{H}$ in $\mathrm{PG}(2,q)$, $q$ odd. $\mathcal{H}$ has no tangents and so if $Q$ is a point of $\mathrm{PG}(2,q)$ not on $\mathcal{H}$ the lines incident with $Q$ are either external to $\mathcal{H}$ or secant to $\mathcal{H}$. Since the lines through $Q$ partition the points of $\mathcal{H}$ it must be that $\mathcal{H}$ contains an even number of points. However $|\mathcal{H}| = q+2$ is odd, a contradiction and so $m(2,q) = q+1$ for $q$ odd. $*\square$

To finish this section we consider the distribution of tangents to an oval of $\mathrm{PG}(2,q)$, $q$ odd, on the points off the oval. In other words the $q$ odd equivalent of Lemma 2.2.

**Lemma 2.4.** *Let $\mathcal{O}$ be an oval of* $\mathrm{PG}(2,q)$, *$q$ odd. Every point off $\mathcal{O}$ is incident with either* $0$ *or* $2$ *tangents to $\mathcal{O}$.*

**Proof.** Let $\ell$ be a tangent to $\mathcal{O}$ at the point $P$. If $Q$ is any other point on $\ell$ the lines through $Q$ partition the $q+1$ points of $\mathcal{O}$. Since $q$ is odd and $Q$ is already incident with one tangent it must be lie on at least one other tangent. Since this is true for each of the $q$ points of $\ell \setminus \{P\}$ and there are $q$ tangents to $\mathcal{O}$, apart from $\ell$, it must be that each point of $\ell \setminus \{P\}$ must be on exactly one other tangent. In other words if a point off $\mathcal{O}$ is on one tangent, then it is on exactly two, and hence the result. $*\square$

This result is also true for non-desarguesian projective planes.

## 2.2 The classification of ovals for $q$ odd

As we saw in the previous section the "behaviour" of ovals for $q$ odd and even is quite different. In fact as we shall see in this section we are able to classify ovals in $\mathrm{PG}(2,q)$,

$q$ odd, as the conics. This contrasts sharply with the $q$ even case where there are a number of infinite families of ovals (and hyperovals) and there is as yet no classification.

The classification in the $q$ odd case is due to Segre ([65, 66]) and is an elegant exercise in classical geometry of $\mathrm{PG}(2, q)$.

To start with, suppose that $\mathcal{K}$ is a $k$ arc with, $k \geq 4$, containing the points $U_0 = (1, 0, 0)$, $U_1 = (0, 1, 0)$ and $U_2 = (0, 0, 1)$. Through each of these points there are $t = q - k + 2$ tangents to $\mathcal{K}$ which have equations $x_1 = a_i x_2$ for $U_0$; $x_2 = b_i x_0$ for $U_1$ and $x_0 = c_i x_1$ for $U_2$ where $i = 1, \ldots, t$. Note that since the lines $x_0 = 0$, $x_1 = 0$ and $x_2 = 0$ are secants of $\mathcal{K}$ it follows that $a_i, b_i, c_i$, $i = 1, \ldots, t$ are all non-zero.

With this setup in mind we present the prelude to the classification theorem the so called "lemma of tangents".

**Lemma 2.5 (Lemma of tangents).** $\prod_{i=1}^{t} a_i b_i c_i = -1$

**Proof.** Let $P = (p_0, p_1, p_2)$ be a point of $\mathcal{K} \setminus \{U_0, U_1, U_2\}$ and so $p_i \neq 0$. The lines $\langle P, U_0 \rangle$, $\langle P, U_1 \rangle$ and $\langle P, U_2 \rangle$ have equations $x_1 = p_1 x_2 / p_2$, $x_2 = p_2 x_0 / p_0$ and $x_0 = p_0 x_1 / p_1$, respectively. In particular $(p_1/p_2) \cdot (p_2/p_0) \cdot (p_0/p_1) = 1$.

Through $U_0$ there are $q - 1$ lines other than $\langle U_0, U_1 \rangle$ and $\langle U_0, U_2 \rangle$, consisting of $t = q - k + 2$ tangents, $x_1 = a_i x_2$ and $k - 3$ secants $x_1 = d_j x_2$. Similarly we denote the tangents and secants to $\mathcal{K}$ on $U_1$ by $x_2 = b_i x_0$ and $x_2 = e_j x_0$ and on $U_2$ by $x_0 = c_i x_1$ and $x_0 = f_j x_1$, respectively, such that the secants with parameters $d_j$, $e_j$ and $f_j$ are concurrent on a point of $\mathcal{K} \setminus \{U_0, U_1, U_2\}$. Since the product of the non-zero elements of $\mathrm{GF}(q)$ is $-1$ we have

$$-1 = \prod a_i \prod d_j = \prod b_i \prod e_j = \prod c_i \prod f_j = \prod a_i b_i c_i \prod d_j e_j f_j.$$

Since $x_1 = d_j x_2$, $x_2 = e_j x_0$ and $x_0 = f_j x_1$ are concurrent on a point of $\mathcal{K} \setminus \{U_0, U_1, U_2\}$ it follows that $d_j e_j f_j = 1$ and so $\prod a_i b_i c_i = -1$. $*\Box$

Now we prove another preparatory lemma, but this time about ovals.

**Lemma 2.6.** *The triangles formed by three points of an oval and the tangents at these points are in perspective.*

**Proof.** Let the three points be $U_0$, $U_1$, $U_2$ and the tangents at the points $x_1 = a x_2$, $x_2 = b x_0$, $x_0 = c x_1$, respectively. Then $abc = -1$ by the lemma of tangents and the result follows. $*\Box$

**Theorem 2.7 (The classification of ovals for $\mathrm{PG}(2, q)$, $q$ odd. Segre [65, 66]).** *In $\mathrm{PG}(2, q)$, $q$ odd, every oval is a conic.*

**Proof.** Let $\mathcal{O}$ be an oval with $U_0, U_1, U_2 \in \mathcal{O}$ and with the point of perspective of the triangles formed by $U_0, U_1, U_2$ and the tangents at $U_0, U_1, U_2$ concurrent at $(1, 1, 1)$. Let $P = (p_0, p_1, p_2) \in \mathcal{O} \setminus \{U_0, U_1, U_2\}$, so $p_0 p_1 p_2 \neq 0$ and let the tangent of $\mathcal{O}$ at $P$ be $\ell = [\ell_1, \ell_2, \ell_3]$ with $\ell_1 \ell_2 \ell_3 \neq 0$. Thus $p_0 \ell_0 + p_1 \ell_1 + p_2 \ell_2 = 0$. Also since $(-1, 1, 1)$, $(1, -1, 1)$ and $(1, 1, -1)$ lie on two tangents apart from $\ell$ by Lemma 2.4 they cannot also be on $\ell$. Thus $-p_0 + p_1 + p_2$, $p_0 - p_1 + p_2$ and $p_0 + p_1 - p_2$ are all non-zero.

By the previous lemma the triangle $PU_1U_2$ and the triangle defined by the tangents at these three points are in perspective. Calculating this condition yields $\ell_1(p_0 +$

$p_1) = \ell_2(p_0 + p_2)$ and similarly by considering triangles $PU_2U_0$ and $PU_0U_1$ we obtain $\ell_2(p_1 + p_2) = \ell_0(p_1 + p_0)$ and $\ell_0(p_2 + p_0) = \ell_1(p_2 + p_1)$, respectively. Hence

$$\ell_0 : \ell_1 : \ell_2 = p_1 + p_2 : p_2 + p_0 : p_0 + p_1.$$

Recall $p_0\ell_0 + p_1\ell_1 + p_2\ell_2 = 0$ which, given the ratios above, is the case if and only if $p_0(p_1+p_2)+p_1(p_2+p_0)+p_2(p_0+p_1) = 0$, i.e. $p_0p_1+p_1p_2+p_2p_0 = 0$. Thus the points of $\mathcal{O}$ satisfy the equation $x_0x_1 + x_1x_2 + x_2x_0 = 0$ and so $\mathcal{O}$ is a conic. $*\square$

An interesting historical aside to the classification of ovals for $q$ odd are the Mathematical Reviews of the relevant articles. In [29] Jarnefelt and Kustaanheimo conjectured that every oval in the plane $\mathrm{PG}(2, q)$, with $q$ odd, is a conic. The reviewer, Marshall Hall Jr, commented "The reviewer finds this conjecture implausible." (Mathematical Review 14,1008d). When reviewing [66] where Segre proved the conjecture Marshall Hall, Jr was again the reviewer and this time wrote "The fact that this conjecture seemed implausible to the reviewer seems to have been at least a partial incentive to the author to undertake this work. It would be very gratifying if further expressions of doubt were as fruitful." (Mathematical Review 17,72g). I'm sure there's a lesson in there somewhere...

## 2.3 Hyperovals and ovals of $\mathrm{PG}(2, q)$, $q$ even

In the previous section we closed the book on ovals of $\mathrm{PG}(2, q)$, $q$ odd. They are all conics which was proved by some elegant, yet elementary geometry. In contrast the study of hyperovals of $\mathrm{PG}(2, q)$, $q$ even, is a rich, deep and complex field and the subject of much current research. As we shall see later hyperovals have links to many areas of geometry including generalized quadrangles, translation planes, flocks of quadratic cones and $\alpha$-flocks. Indeed many hyperovals are constructed "indirectly" by consideration of related geometrical objects.

We begin by discussing the relationship between hyperovals and ovals. By Lemma 2.2 we know that any oval $\mathcal{O}$ of $\mathrm{PG}(2, q)$, $q$ even, completes to a hyperoval $\mathcal{H}$ by adding the nucleus $N$ of $\mathcal{O}$. On the other hand, if we start with a hyperoval $\mathcal{H}$ and remove a point $N \in \mathcal{H}$, then we are left with an oval $\mathcal{H}\backslash\{N\}$ which has nucleus $N$ and completes to $\mathcal{H}$. Thus one oval gives rise to a further $q + 1$ ovals. If $\mathcal{H}$ is a hyperoval and $\mathcal{O}_1$, $\mathcal{O}_2$ are two ovals constructed from $\mathcal{H}$ by removing the points $N_1$, $N_2$, respectively, then $\mathcal{O}_1$ and $\mathcal{O}_2$ are equivalent in $\mathrm{PG}(2, q)$ if and only if the stabiliser of $\mathcal{H}$ maps $N_1$ to $N_2$.

The one example of a hyperoval that we have encountered thus far is the regular hyperoval consisting of a conic and its nucleus. For $q = 2$ and 4 the group of the regular hyperoval is transitive on the points of the hyperoval so each oval contained in it is a conic. For $q > 4$ the group of the regular hyperoval fixes the nucleus of the conic and so we have two ovals, the conic and the so called pointed conic, which has canonical form $\{(1, t, \sqrt{t}) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\}$. This is our first example of a non-conic oval, but don't worry we'll see more later.

To say much more about hyperovals at all we need a concrete way of describing them in general. The following discussion will provide an algebraic way of representing hyperovals in terms of functions over $\mathrm{GF}(q)$ called o-polynomials. By such considerations we also have an algebraic method for determining if a given set of $q+2$ points of $\mathrm{PG}(2,q)$ is a hyperoval.

By the fundamental theorem of projective geometry any hyperoval of $\mathrm{PG}(2,q)$, $q$ even, is equivalent to an oval $\mathcal{O}$ containing the points $(1,0,0),(0,0,1),(1,1,1)$ and $(0,1,0)$. Consequently we may write $\mathcal{O}$ in the form

$$\mathcal{O} = \mathcal{D}(f) = \{(1,t,f(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,0,1),(0,1,0)\} \tag{1}$$

where $f$ induces a permutation of $\mathrm{GF}(q)$ (and so is called a *permutation polynomial*) such that $f(0)=0$ and $f(1)=1$. Note that from [27, Section 1.3] the natural map from the polynomials over $\mathrm{GF}(q)$ with degree less than $q$ to functions from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ is a bijection. So, as with $f$ above, we will abuse notation and use the same symbol to represent both a function and the unique polynomial of degree less than $q$ that generates the function. If $f(x)=x^n$ for some $n$, then we write $\mathcal{D}(n)$ for $\mathcal{D}(f)$.

Any polynomial with degree less than $q$ that arises from an hyperoval as above will be called an *o-polynomial* (following Cherowitzo [10]).

In the published literature on ovals and hyperovals there is a variance in the use of the notation $\mathcal{D}(f)$. In some cases it is used to refer to a hyperoval, as we are here, but it is also used to refer to the *oval* $\{(1,t,f(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,0,1)\}$ with nucleus $(0,1,0)$ and containing the points $(1,0,0)$ and $(1,1,1)$; or even the oval $\{(1,t,f(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}$, containing the points $(1,0,0)$ and $(1,1,1)$. Since such an oval completes to a hyperoval as in (1) this gives an equivalent definition of an o-polynomial.

Since every hyperoval containing the fundamental quadrangle gives rise to an o-polynomial, it follows that every hyperoval is equivalent to a hyperoval that may be described in this way. However the description is not in general unique as there may be many collineations mapping a given hyperoval "onto" the fundamental quadrangle. This also applies to hyperovals containing the fundamental quadrangle so that it is possible that $\mathcal{D}(f) = \mathcal{D}(f')$, where $f$ and $f'$ are o-polynomials (and $f'$ is *not* the derivative of $f$, so get used to it!) but $f$ and $f'$ are *not* equal.

**Example: The regular hyperoval** The one hyperoval that we have met thus far, the regular hyperoval, can be represented by the o-polynomials $x^2$, $\sqrt{x}$ and $x^{q-2}$. (For a list of all o-polynomials corresponding to the regular hyperoval for $q \geq 8$ see [38].)

We now give two equivalent theorems which provide algebraic conditions for a permutation $f$ to be an o-polynomial. The first is due to Segre ([67, 69], see [27, Theorem 8.22]) while the second is due to Glynn ([21]).

To apply the first theorem it is useful to know whether a given function from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$, $q$ even, is a permutation.

**Theorem 2.8 (Dickson's criterion; see [16] or [27]).** *Let $f$ be a polynomial over $\mathrm{GF}(q)$ with degree less than $q$. Then $f$ defines a permutation of $\mathrm{GF}(q)$ if and only if*

(i) *for $r$ odd and $r \leq -2$, the degree of $f(x)^r$ reduced modulo $x^q - x$ is at most $q-2$;*

(ii) *$f(t)=0$ has exactly one solution in $\mathrm{GF}(q)$.*

Now we present the result of Segre in the form found in [27].

**Theorem 2.9.** *If $q > 2$, a polynomial $f$ is an o-polynomial if and only if*
*(i) $f$ is a permutation polynomial with $f(0) = 0$, $f(1) = 1$; and*
*(ii) for each $s \in \mathrm{GF}(q)$, $f_s$ is a permutation polynomial and $f_s(0) = 0$, where*

$$f_s(x) = \frac{f(x+s) + f(s)}{x}.$$

**Proof.** Condition (i) is equivalent to $\mathcal{D}(f)$ containing the fundamental quadrangle and having the property that no line on $(0,0,1)$ is incident with three points of $\mathcal{D}(f)$. Condition (ii) guarantees that no three of the points of $\mathcal{D}(f) \setminus \{(0,1,0),(0,0,1)\}$ are collinear. $*\square$

The second formulation of o-polynomials due to Glynn is more technical in appearance than that of Segre but has some computational advantages, particularly in the application of computers to searching for o-polynomials.

First we define a partial ordering $\preceq$ on the set of integers $n$ where $0 \leq n \leq q-1$ and $q = 2^h$. If

$$b = \sum_{i=0}^{h-1} b_i 2^i \text{ and } c = \sum_{i=0}^{h-1} c_i 2^i$$

(where each $b_i$ and each $c_i$ is either 0 or 1) then $b \preceq c$ if and only if $b_i \leq c_i$ for all $i$.

**Theorem 2.10 ([21]).** *A polynomial $f$ of degree at most $q-2$ satisfying $f(0) = 0$ and $f(1) = 1$ is an o-polynomial if and only if the coefficient of $x^c$ in $f(x)^b$ (mod $x^q - x$) is zero for all pairs of integers $(b, c)$ satisfying $1 \leq b \leq c \leq q-1$, $b \neq q-1$ and $b \preceq c$.*

Now we state an easy corollary of this result that was first proved by Segre and Bartocci ([64]).

**Corollary 2.11.** *An o-polynomial has only even degree terms.*

**Proof.** Set $b = 1$, then for any odd number $c \leq q-1$ since $1 \preceq c$ the coefficient of $x^c$ is zero. $*\square$

For more detailed information on o-polynomials see Chapter 8 of [27], Cherowitzo [10] and O'Keefe and Penttila [38].

To this point we have met only the regular hyperoval. In the next four sections we shall outline all of the known hyperovals and their constructions.

### 2.3.1 Monomial o-polynomials

In this section we'll look at the monomial o-polynomials, that is o-polynomials of the form $x^n$. By using Theorem 2.9 it is possible to derive necessary and sufficient conditions for the function $x^n$ to be an o-polynomial.

**Theorem 2.12 (See [27, Corollary 8.2.4]).** *In $\mathrm{PG}(2,q)$, with $q$ even and $q > 2$, $\mathcal{D}(n)$ is a hyperoval if and only if*

(i) $(n, q-1) = 1$;

(ii) $(n-1, q-1) = 1$;

(iii) $\frac{(x+1)^n + 1}{x}$ *is a permutation polynomial.*

**Proof.** Condition (i) is equivalent to $x^n$ being a permutation polynomial; condition (ii) is equivalent to condition (ii) of Theorem 2.9 with $s = 0$; and condition (iii) is equivalent to condition (ii) of Theorem 2.9 with $s \neq 0$. $*\square$

It turns out that if a hyperoval may be represented by a monomial hyperoval, then there are a number of different monomial o-polynomials that represent the same hyperoval.

**Theorem 2.13.** *If $x^n$ is an o-polynomial, then so are $x^{1/n}$, $x^{1-n}$, $x^{1/(1-n)}$, $x^{n/(n-1)}$ and $x^{(n-1)/n}$ are also o-polynomials (where the exponents are taken modulo $q-1$). These six o-polynomials give projectively equivalent hyperovals.*

It should be noted that for a given hyperoval with a monomial o-polynomial that these six o-polynomials are not always distinct.

We will now look at the known examples of hyperovals with a monomial o-polynomial.

**The regular hyperoval:** As we have seen, with o-polynomial $x^2$.

**The translation hyperovals, $x^{2^i}$, $(i,h) = 1$:** If $q = 2^h$ then the map $x \mapsto x^{2^i}$ is an automorphism of $\mathrm{GF}(q)$. If in addition $(i,h) = 1$, then $x^{2^i}$ is an o-polynomial called a *translation hyperoval.* The translation hyperovals were constructed by Segre in [67] and the term translation is used because the hyperoval $\{(1,t,t^{2^i}) : t \in \mathrm{GF}(q)\} \cup \{(0,0,1)\}$ is fixed by the elation group of size $q$ whose elements act on points of $\mathrm{PG}(2,q)$ by

$$(x_0, x_1, x_2) \mapsto (x_0, x_1 + t, x_2 + t^{2^i}) \text{ for } t \in \mathrm{GF}(q).$$

This group fixes the points $(0,0,1)$ and $(0,1,0)$ of $\mathcal{D}(f)$, and acts transitively on the rest of the points. The line $x_0 = 0$ is called the *axis* of the hyperoval. The elation group is a *translation group* in the affine plane formed by removing the axis of the hyperoval from $\mathrm{PG}(2,q)$. If $\alpha$ is the automorphism $x \mapsto x^{2^i}$, then we will often use the notation $\mathcal{D}(\alpha)$ to refer to the hyperoval $\{(1,t,t^{2^i}) : t \in \mathrm{GF}(q)\} \cup \{(0,0,1)\}$.

When $(i,h) = 1$ and $i \neq 1, h-1$ the corresponding translation hyperoval is not regular and so gives us examples of irregular hyperovals for $\mathrm{PG}(2,q)$ where $h = 5$ and $h \geq 7$.

Payne ([51]) showed that these are the only hyperovals with an additive o-polynomial (or equivalently the only hyperovals stabilised by such a translation group).

**The Segre hyperoval, $x^6$, $q = 2^{\mathbf{odd}}$:** If $q = 2^h$ and $h$ is odd, then $x^6$ is an o-polynomial. These hyperovals were discovered by Segre in 1962 ([69]), although most of the proofs appeared in [64].

It is a nice, but not trivial, exercise in familiarising oneself with Theorem 2.12 to prove that the Segre Hyperovals are indeed hyperovals.

**The Glynn hyperovals, $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$, with $\sigma^2 \equiv \gamma^4 \equiv 2 \pmod{q-1}$ for $q = 2^{\text{odd}}$:**
If $q = 2^{2e+1}$ (that is $q = 2^{\text{odd}}$), then there exist automorphisms $\sigma$ and $\gamma$ of $\mathrm{GF}(q)$ with $\sigma : x \mapsto x^{2^{e+1}}$ and $\gamma : x \mapsto x^{2^{(e+1)/2}}$ if $e$ is odd and $x \mapsto x^{2^{(3e+2)/2}}$ when $e$ is even. In other words $\sigma^2 \equiv \gamma^4 \equiv 2 \pmod{q-1}$. In 1982 Glynn showed that the monomials $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ are o-polynomials (see [19]).

If Theorem 2.10 of Glynn is applied to a monomial function $x^n$, then we see that it is an o-polynomial if and only if $d \not\preceq nd$, for $d = 1, 2, \ldots, q-2$. This result appears in [19] (and so predates Theorem 2.10) and was used in programming computer searches for monomial o-polynomials for $q$ up to $q = 2^{19}$. By doing this Glynn found the two new types of o-polynomials. To prove that they were infinite families he used Theorem 2.12 and "generalized" the proof of the Segre hyperoval found in [25].

It is worth noting that at the time of their construction the Glynn hyperovals were the first new hyperovals for over twenty years and marked the start of a steady stream of new hyperovals. It was also the first use of a computer in the construction of an infinite family of hyperovals (Lunelli and Sce used a computer to construct their hyperoval in the particular plane $\mathrm{PG}(2, 16)$, see [35]). Although the proofs in [19] are computer free the use of the computer was essential in the discovery of the hyperovals. Computers have also played a large part in the discovery of most of the hyperovals discovered subsequently.

In his paper Glynn also conjectured that
(1) For $\mathrm{PG}(2, q)$, $q = 2^{\text{even}}$, the only hyperovals with a monomial o-polynomial are the translation hyperovals; and
(2) There are no more hyperovals with monomial o-polynomials.

Both conjectures remain open.

These problems are extremely difficult and we now quote a couple of partial results on the problem. The first is a computer result of Glynn extending the classification of monomial o-polynomials in "small" order planes.

**Theorem 2.14 ([21]).** *The only hyperovals with a monomial o-polynomial in the plane* $\mathrm{PG}(2, 2^h)$ *for* $h \le 28$*, are those given by the known constructions.*

It seems likely that with the increase in computer power since 1989 this result could be extended to greater $h$. However the fact that no new hyperovals were found for $h \le 28$ suggests that a classification of the monomial hyperovals as the known examples is required and that further computer may not be of much use. (Unless, of course, you think that you can find a new monomial hyperoval!)

The second partial result, due to Cherowitzo and Storme ([13]) considers the binary decompostion of the exponent of a monomial o-polynomial. If we consider the monomial $x^n$ over $\mathrm{GF}(2, 2^h)$ where $n = \sum_{i=0}^{h-1} b_i 2^i$, then $n$ is called a $k$ bit exponent if exactly $k$ of the $b_i$ are non-zero. The translation hyperovals correspond to the one bit exponent case. Cherowitzo and Storme classify those monomial o-polynomials with a two bit exponent as the known examples (i.e. the Segre hyperoval and the first family of Glynn).

### 2.3.2 The Lunelli-Sce hyperoval in $\mathrm{PG}(2,16)$, "sporadic" O'Keefe-Penttila hyperoval in $\mathrm{PG}(2,32)$ and hyperovals in $\mathrm{PG}(2,64)$

In 1958 Lunelli and Sce ([35]) found by computer search an irregular hyperoval in $\mathrm{PG}(2,16)$. This showed that $\mathrm{PG}(2,16)$ is the smallest order desarguesian plane to contain an irregular hyperoval (since it was known that $\mathrm{PG}(2,4)$ and $\mathrm{PG}(2,8)$ contain only regular hyperovals as we shall see later). The Lunelli-Sce hyperoval may be written as $\mathcal{L} = \mathcal{D}(f)$ with

$$f(x) = x^{12} + x^{10} + \eta^{11}x^8 + x^6 + \eta^2x^4 + \eta^9x^2$$

where $\eta$ is a primitive element of $\mathrm{GF}(q)$ satisfying $\eta^4 = \eta + 1$.

The hyperoval $\mathcal{L}$ has the nice property that its group is transitive on its points. Hyperovals with this property have been classified by Korchmaros ([33]) as the $\mathcal{L}$ and the regular hyperovals in $\mathrm{PG}(2,2)$ and $\mathrm{PG}(2,4)$.

For many years it was unclear whether $\mathcal{L}$ was contained in an infinite family of hyperovals or was in some sense sporadic. In 1996 Cherowitzo, Penttila, Pinneri and Royle resolved this problem by constructing the "Subiaco" infinite family of hyperovals which contained the Lunelli-Sce hyperoval. We shall deal with the Subiaco hyperovals in due course.

In 1991 with the aid of a computer O'Keefe and Penttila searched in $\mathrm{PG}(2,32)$ for hyperovals under hypotheses on the divisor of the automorphism group of a putative hyperoval. They constructed a hyperoval with o-polynomial

$$\begin{aligned} f(x) &= x^4 + x^{16} + x^{28} + \beta^{11}(x^6 + x^{10} + x^{14} + x^{18} + x^{22} + x^{26}) \\ &\quad + \beta^{20}(x^8 + x^{20}) + \beta^6(x^{12} + x^{24}), \end{aligned}$$

where $\beta$ is a primitive element of $\mathrm{GF}(32)$ satisfying $\beta^5 = \beta^2 + 1$. The O'Keefe-Penttila hyperoval has a small automorphism group of order 3. One of the intriguing properties of the O'Keefe-Penttila hyperoval is its reluctance to be a member of an infinite family. It is known to not be a member of any of the existing infinite families of hyperovals, but further is also known not to arise by general construction methods that yield all other (known) hyperovals. We shall discus these general construction methods later.

In $\mathrm{PG}(2,2)$, $\mathrm{PG}(2,4)$ and $\mathrm{PG}(2,8)$ all hyperovals are regular (as we shall see later). For $\mathrm{PG}(2,2^h)$, $h = 5$ and $h \geq 7$ the translation hyperovals provide examples of irregular hyperovals. For many years after the construction of the translation hyperovals by Segre in 1957 it was unknown if there exists a non-regular hyperoval in the remaining case $\mathrm{PG}(2,64)$. Almost forty years after the construction of the translation hyperovals Penttila and Pinneri ([58]) found two irregular families of hyperovals in $\mathrm{PG}(2,64)$. These two hyperovals were later placed in the Subiaco family. Following this, Penttila and Royle ([60]) found another irregular hyperoval in $\mathrm{PG}(2,64)$, which later became part of the Adelaide family.

### 2.3.3 Hyperovals from a flock of a quadratic cone

In this section we describe the construction of a family of hyperovals from a flock of a quadratic cone. Flocks of a quadratic cone which link certain elation generalized quadrangles of order $(q^2, q)$, with translation planes and in the even case with hyperovals has been one of the most productive and intriguing areas of finite geometry of the last decade. We will give a brief overview of the area leading to the construction of hyperovals.

A *quadratic cone* $\mathcal{K}$ is a cone in $\mathrm{PG}(3, q)$ which has as its vertex a point $V$ of $\mathrm{PG}(3, q)$ and for its base a conic in a plane of $\mathrm{PG}(3, q)$ not containing $V$. The canonical example is given by the equation $x_1^2 + x_0x_2 = 0$ which has vertex $(0, 0, 0, 1)$. A *flock* of a quadratic cone $\mathcal{K}$ is a set of $q$ planes of $\mathrm{PG}(3, q)$, not containing the vertex of $\mathcal{K}$, which pairwise do not intersect in a point of $\mathcal{K}$. The elements of a flock partition the set of points of the quadratic cone minus the vertex. In 1976 Walker ([83]) and Thas independently proved that corresponding to a flock of a quadratic cone is a translation plane (of dimension at most two over its kernel). In 1987 Thas ([75]) showed that to a flock of a quadratic cone there corresponds an elation generalized quadrangle of order $(q^2, q)$ by linking the flock with previously known constructions for generalized quadrangles. We shall now briefly outline the construction of these generalized quadrangles.

In [31] (see [56, 8.2]) Kantor gave a construction method for a GQ of order $(s, t)$ from group cosets. Let $G$ be a group of order $s^2t$ and let $\mathcal{F} = \{S_0, S_1, \ldots, S_t\}$ be a family of $t + 1$ subgroups of $G$, each of order $s$, such that for each $i = 0, \ldots, t$ there is a subgroup $S_i^*$ of $G$ of order $st$ containing $S_i$ and satisfying:

K1 $S_iS_j \cap S_k = \{1\}$ for distinct $i, j, k$ and

K2 $S_i^* \cap S_j = \{1\}$ for distinct $i, j$.

Such a family $\mathcal{F}$ is called a *4-gonal family for $G$*. The subgroup $S_i^*$ is called the *tangent space of $G$ at $S_i$*. From such a family Kantor gave a construction of a GQ $\mathcal{S}(\mathcal{F})$ of order $(s, t)$:

*points:* (i) elements of $G$, (ii) cosets $S_i^*g$ for $g \in G$ and $i = 0, \ldots, t$, and (iii) a symbol $(\infty)$;

*lines:* (a) cosets $S_i^*g$ for $g \in G$ and $i = 0, \ldots, t$, and (b) the symbols $[S_i]$, $i = 0, \ldots, t$.

*Incidence:* inherited from the group $G$ and also a line $[S_i]$ of type (b) is incident with the points $S_i^*g$, $g \in G$, and the point $(\infty)$.

As a familiarisation exercise the reader may want to verify that the conditions K1 and K2 do in fact ensure that $\mathcal{S}(\mathcal{F})$ is a GQ of order $(s, t)$.

In [32] Kantor presented an algebraic formulation of the construction for a particular group $G$ of order $q^5$, $q$ odd, giving rise to elation generalized quadrangles of order $(q^2, q)$. Payne ([52]) gave the equivalent formulation for $q$ even, and in [75], Thas unified the odd and even case by showing the relation to flocks of a quadratic cone. In [52] Payne also showed that in the $q$ even case the GQ of order $(q^2, q)$ possesses a family $\{\mathcal{S}_0, \ldots, \mathcal{S}_q\}$ of $q + 1$ subquadrangles each of order $(q, q)$ and that with each of these subquadrangles is associated an oval $\mathcal{O}_i$, $i = 0, \ldots, q$, and hence a hyperoval.

(It is implicit in the paper of Payne that the subquadrangle $\mathcal{S}_i$ is isomorphic to the quadrangle $T_2(\mathcal{O}_i)$ of Tits.)

We will now present some of the details of the construction of the elation generalized quadrangle of order $(q^2, q)$, the subquadrangles of order $(q, q)$ and the associated ovals. Note that the construction we present is specialised to the $q$ even case.

Let $\mathcal{C} = \left\{ A_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$ be a collection of $2 \times 2$ matrices, indexed by the elements of $\mathrm{GF}(q)$, with the property that for distinct $s, t \in \mathrm{GF}(q)$ the matrix $A_s - A_t$ is anisotropic, that is $\underline{u}(A_s - A_t)\underline{u}^T = 0$ if and only if $\underline{u} = 0$. Such a family of matrices is called a $q$-clan (following Payne [53]). We see from the definition that the map $t \mapsto y_t$ is a permutation of $\mathrm{GF}(q)$ for if $y_s = y_t$ for some $s, t \in \mathrm{GF}(q)$, $s \neq t$, then the matrix $A_s - A_t$ is either the zero matrix or $\underline{u} = (\sqrt{z_s + z_t}, \sqrt{x_s + x_t})$ is a non-zero solution to $\underline{u}(A_s - A_t)\underline{u}^T = 0$. Clearly $t \mapsto x_t$ and $t \mapsto z_t$ must also be permutations of $\mathrm{GF}(q)$. Hence we can reparametrise the $q$-clan and assume

$$A_t = \begin{pmatrix} x_t & t^{1/2} \\ 0 & z_t \end{pmatrix}.$$

The *trace* map from $\mathrm{GF}(2^h) \to \mathrm{GF}(2)$ is defined to be $x \mapsto x + x^2 + \ldots + x^{2^{h-1}}$. So following Cherowitzo, Penttila, Pinneri and Royle [12] we can assume that elements of a $q$-clan, $q$ even, have the form

$$A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & \kappa g(t) \end{pmatrix},$$

where $\mathrm{trace}(\kappa) = 1$, $f(0) = g(0) = 0$, $f(1) = g(1) = 1$ and

$$\mathrm{trace}\left(\frac{\kappa(f(s) + f(t))(g(s) + g(t))}{s + t}\right) = 1$$

for all $s, t \in \mathrm{GF}(q)$ with $s \neq t$. (This last trace condition is the equivalent of $A_s - A_t$ being anisotropic.)

A $q$-clan in this form (said to be *normalised*) is used to define a 4-gonal family for the group $G = \{(\alpha, c, \beta) : \alpha, \beta \in \mathrm{GF}(q)^2, c \in \mathrm{GF}(q)\}$ with group operation

$$(\alpha, c, \beta)(\alpha', c', \beta') = (\alpha + \alpha', c + c' + \beta \circ \alpha', \beta + \beta'),$$

where $\beta \circ \alpha = \sqrt{\beta^T P \alpha}$, with $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. The 4-gonal family consists of the subgroups

$$\begin{aligned} A(\infty) &= \{(0, 0, \beta) : \beta \in \mathrm{GF}(q)^2\} \text{ and} \\ A(t) &= \{(\alpha, \sqrt{\alpha^T A_t \alpha}, t^{1/2}\alpha) : \alpha \in \mathrm{GF}(q)^2\}, \quad t \in \mathrm{GF}(q), \end{aligned}$$

with tangent spaces

$$\begin{aligned} A^*(\infty) &= \{(0, c, \beta) : \beta \in \mathrm{GF}(q)^2, c \in \mathrm{GF}(q)\} \text{ and} \\ A^*(t) &= \{(\alpha, c, t^{1/2}\alpha) : \alpha \in \mathrm{GF}(q)^2, c \in \mathrm{GF}(q)\}, \quad t \in \mathrm{GF}(q). \end{aligned}$$

(To see that this is a 4-gonal family refer to [56, 10.4].) The GQ constructed from this 4-gonal family by the Kantor construction is a GQ of order $(q^2, q)$ and will be called $\mathcal{S}$.

Payne and Maneri ([54]) defined a subgroup $G_\alpha$, for a fixed $\alpha \in \mathrm{GF}(q)^2 \setminus \{(0,0)\}$, of order $q^3$ of $G$ which, when intersected with the the 4-gonal family above, gives a 4-gonal family of $G_\alpha$ corresponding to a GQ $\mathcal{S}_\alpha$ of order $(q,q)$. Since the 4-gonal family for $\mathcal{S}_\alpha$ is a sub-family of that for $\mathcal{S}$ it follows that $\mathcal{S}_\alpha$ is a subquadrangle of $\mathcal{S}$.

In particular the group $G_\alpha$ is defined to be $G_\alpha = \{(x\alpha, z, y\alpha) : x, y, z \in \mathrm{GF}(q)\}$ and the 4-gonal family for $G_\alpha$ consists of the subgroups

$$\begin{aligned} A_\alpha(\infty) = G_\alpha \cap A(\infty) &= \{0, 0, y\alpha) : y \in \mathrm{GF}(q)\} \\ A_\alpha(t) = G_\alpha \cap A(t) &= \{(x\alpha, x\sqrt{\alpha^T A_t \alpha}, xt^{1/2}\alpha) : x \in \mathrm{GF}(q)\}. \end{aligned}$$

The tangent space of $G_\alpha$ at $A_\alpha(t)$, $t \in \mathrm{GF}(q) \cup \{(\infty)\}$ is given by $A^*_\alpha(t) = G_\alpha \cap A^*(t)$.

Now an inspection of the definition of $G_\alpha$ reveals that $G_\alpha = G_{\alpha'}$ if and only if $\alpha = \lambda\alpha'$ for some $\lambda \in \mathrm{GF}(q) \setminus \{0\}$. Thus there are $q+1$ subgroups $G_\alpha$ and correspondingly $q+1$ subquadrangles $\mathcal{S}_\alpha$ (although while there are $q+1$ of these subquadrangles they are not in general non-isomorphic).

Interestingly we can make $G_\alpha$ a three-dimensional vector space over $\mathrm{GF}(q)$ by introducing the scalar multiplication

$$k(x\alpha, x\sqrt{\alpha^T A_t \alpha}, xt^{1/2}\alpha) = (kx\alpha, kx\sqrt{\alpha^T A_t \alpha}, kxt^{1/2}\alpha).$$

Then the map $(x\alpha, z, y\alpha) \mapsto (x, y, z)$ from $G_\alpha$ to $\mathrm{PG}(2,q)$ gives $G_\alpha$ the canonical form of a desarguesian projective plane. Under this map $A_\alpha(\infty) \mapsto (0,1,0)$ and $A_\alpha(t) \mapsto (1, t^{1/2}, \sqrt{\alpha^T A_t \alpha})$. Let

$$\mathcal{O}_\alpha = \{(1, t^{1/2}, \sqrt{\alpha^T A_t \alpha}) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}.$$

In [52] Payne made the important observation that the 4-gonal family condition K1 forces the set $\mathcal{O}_\alpha$ to be an oval of $\mathrm{PG}(2,q)$. (It is also implicit in [52] that the subquadrangle $\mathcal{S}_\alpha$ is isomorphic to $T_2(\mathcal{O}_\alpha)$.)

So we now have $q+1$ ovals popping out of the $q$-clan construction of a GQ of order $(q^2, q)$ and its subquadrangles. If we put the ovals $\mathcal{O}_\alpha$ into a canonical form we obtain the $q+1$ ovals

$$\begin{aligned} \mathcal{O}_\infty &= \{(1, t, f_\infty(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\} \text{ and} \\ \mathcal{O}_s &= \{(1, t, f_s(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}, \quad s \in \mathrm{GF}(q) \end{aligned}$$

where not only is $\{f_s : s \in \mathrm{GF}(q)\} \cup \{f_\infty\}$ a set of $q+1$ *o-polynomials* but also the set satisfies the equation

$$f_s(t) = \frac{f_0(t) + \kappa s f_\infty(t) + s^{1/2}t^{1/2}}{1 + \kappa s + s^{1/2}}$$

for some $\kappa \in \mathrm{GF}(q)$ with $\mathrm{trace}(\kappa) = 1$. A family of ovals $\{\mathcal{O}_\infty\} \cup \{\mathcal{O}_s : s \in \mathrm{GF}(q)\}$ as above where $f_\infty$, $f_s$, $s \in \mathrm{GF}(q)$ satisfy the above equation is called a *herd* of ovals (Cherowitzo, Penttila, Pinneri and Royle ([12]) are responsible for this term).

Also from [12] we have the following theorem which summarises the above rather algebraic discussion of the links between $q$-clans and ovals.

**Theorem 2.15 ([12]).** *A herd of ovals gives rise to a (normalised) q-clan*

$$\left\{ \begin{pmatrix} f_0(t) & t^{1/2} \\ 0 & \kappa f_\infty(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\},$$

*and conversely such a normalised q-clan gives rise to a herd of ovals.*

We prefaced the discussion leading to the preceding theorem by mentioning the correspondence between flocks and the GQs constructed via $q$-clans. We have omitted mentioning flocks as they are not directly required in the generation of the ovals, however as a pivotal result in the establishment of the field of study it is worth presenting the following theorem due to Thas.

**Theorem 2.16 ([75, 2.5.3]).** *The set* $\mathcal{C} = \left\{ \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$ *is a q-clan if and only if the planes* $x_t X_0 + z_t X_1 + y_t X_2 + X_3 = 0$, $t \in \mathrm{GF}(q)$, *define a flock of the quadratic cone with equation* $X_0 X_1 = X_2^2$.

We reiterate that this result applies to $q$-clan GQ constructions for both $q$ odd and even. It should also be noted that Thas has contributed much to the geometric understanding of the constructions of the flock or $q$-clan GQs and of the herd of ovals. In [77] Thas gives a construction of the GQ from the flock and in [78] for the $q$ even case provides constructions of the ovals in a herd from the corresponding flock. As however most of the work in the area has been algebraic in nature, and particularly the hyper(oval) constructions, we have chosen to emphasise this more.

We are now in a position to present the hyperovals constructed via the connection with flocks and generalized quadrangles.

**The Payne hyperovals, $q = 2^h$, $h$ odd:** In [52] Payne showed that the set $\left\{ \begin{pmatrix} t^{1/6} & t^{1/2} \\ 0 & t^{5/6} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$ is a $q$-clan. For $q > 8$ the corresponding herd consists of 2 equivalent ovals completing to the Segre hyperoval $\mathcal{D}(6)$ and $q-1$ equivalent ovals completing to the hyperoval $\mathcal{D}(f)$ with

$$f(x) = x^{1/6} + x^{3/6} + x^{1/2}.$$

**The Subiaco hyperovals, $q = 2^h$:** In [12] Cherowitzo, Penttila, Pinneri and Royle showed that

$$\mathcal{C} = \mathcal{C}_\delta = \left\{ \begin{pmatrix} f_0(t) & t^{1/2} \\ 0 & \kappa g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\},$$

is a $q$-clan where, for some $\delta \in \mathrm{GF}(q)$ with $\delta^2 + \delta + 1 \neq 0$ and $\mathrm{trace}(1/\delta) = 1$, we have

$$\begin{aligned}
\kappa &= \frac{\delta^2 + \delta^5 + \delta^{1/2}}{\delta(1 + \delta + \delta^2)} \\
f_0(t) &= \frac{\delta^2(t^4 + t) + \delta^2(1 + \delta + \delta^2)(t^3 + t^2)}{(t^2 + \delta t + 1)^2} + t^{1/2} \quad \text{and} \\
g(t) &= \frac{\delta^4 t^4 + \delta^3(1 + \delta^2 + \delta^4)t^3 + \delta^3(1 + \delta^2)t}{(\delta^2 + \delta^5 + \delta^{1/2})(t^2 + \delta t + 1)^2} + \frac{\delta^{1/2}}{(\delta^2 + \delta^5 + \delta^{1/2})} t^{1/2}.
\end{aligned}$$

So from this the Subiaco o-polynomial is

$$f(x) = \frac{\delta^2(x^4+x)+\delta^2(1+\delta+\delta^2)(x^3+x^2)}{(x^2+\delta x+1)^2} + x^{1/2},$$

whenever we have $\delta \in \mathrm{GF}(q)$ such that $\mathrm{trace}(1/\delta) = 1$ and $\delta \notin \mathrm{GF}(4)$, for $h \equiv 2 \pmod 4$.

This o-polynomial gives rise to two inequivalent hyperovals when $h \equiv 2 \pmod 4$ and to a unique hyperoval when $h \not\equiv 2 \pmod 4$.

For $q \neq 2$ the Subiaco hyperoval(s) are not regular, for $q = 32$ they are Payne hyperovals and for $q > 32$ they are inequivalent to the members of the infinite families of hyperovals we have discussed thus far. It is known that the only hyperovals in $\mathrm{PG}(2,16)$ are the regular hyperoval and the Lunelli-Sce hyperoval (see [23, 39]) and hence the Subiaco family includes the Lunelli-Sce hyperoval in $\mathrm{PG}(2,16)$. In the case $q = 64$, the two classes of Subiaco hyperovals are those discovered by Penttila and Pinneri. For $q = 128, 256$ they are the hyperovals discovered by Penttila and Royle ([60]).

**The Adelaide hyperovals, $q = 2^h$, $h$ even:** If you were under the impression that the forms of the Subiaco $q$-clan and o-polynomial were complicated, then you will find the Adelaide hyperovals even more remarkable. In work *just* finished Cherowitzo, O'Keefe and Penttila [14] constructed the Adelaide $q$-clans and hyperovals. (In fact their construction is much more general, but we shall discuss this later.)

Let $\mathrm{GF}(q^2)$ be a quadratic extension of $\mathrm{GF}(q)$ with $q = 2^e$. Let $\beta \in \mathrm{GF}(q^2) \setminus \{1\}$ be such that $\beta^{q+1} = 1$, and let $T(x) = x + x^q$ for all $x \in \mathrm{GF}(q^2)$. Let $\kappa \in \mathrm{GF}(q)$ and the functions $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ be defined by:

$$\kappa = \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1$$

$$f(t) = f_{m,\beta}(t) = \frac{T(\beta^m)(t+1)}{T(\beta)} + \frac{T((\beta t + \beta^q)^m)}{T(\beta)(t + T(\beta)t^{1/2}+1)^{m-1}} + t^{1/2}$$

and

$$\kappa g(t) = \kappa g_{m,\beta}(t) = \frac{T(\beta^m)}{T(\beta)} t + \frac{T((\beta^2 t + 1)^m)}{T(\beta)T(\beta^m)(t + T(\beta)t^{1/2}+1)^{m-1}} + \frac{1}{T(\beta^m)} t^{1/2}$$

and let

$$\mathcal{C} = \left\{ \begin{pmatrix} f(t) & t^{1/2} \\ 0 & \kappa g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}.$$

If $q = 2^e$ with $e > 2$ even and $m \equiv \pm\frac{q-1}{3} \pmod{q+1}$ then $\mathcal{C}$ is a $q$-clan, which we call the *Adelaide* $q$-clan, for all $\beta$.

So from this the Adelaide o-polynomial is

$$f(x) = \frac{T(\beta^m)(x+1)}{T(\beta)} + \frac{T((\beta x + \beta^q)^m)}{T(\beta)(x + T(\beta)x^{1/2}+1)^{m-1}} + x^{1/2},$$

where $\beta \in \mathrm{GF}(q^2) \setminus \{1\}$ such that $\beta^{q+1} = 1$.

The Adelaide hyperoval is known to be new for $q = 64$ and $q = 256$ and for $q = 2^h$, $h > 6$, Cherowitzo, O'Keefe, Penttila show that the Adelaide hyperoval is either new or a Subiaco hyperoval. There is a great deal of evidence however to suggest that the Adelaide hyperovals are in general new, which we shall discuss soon.

In the above we have only included the $q$-clans that give hyperovals not previously constructed by other methods and listed earlier. There are two $q$-clans, for $q$ even that we did not mention above. The first is the *classical* $q$-clan, for $q$ even, whose associated ovals are all conics and whose associated flock is the linear flock (that is, take a line not intersecting the cone and take the planes through that line not containing the vertex of the cone). The other is the so called FTWKB (Fisher-Thas-Walker-Kantor-Betten) $q$-clan, for $q = 2^{\mathrm{odd}}$, where the associated ovals are conics for $q = 2$ and for $q \geq 8$ all equivalent to the translation oval $\{(1, t, t^4) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\}$. The beauty of the Cherowitzo, O'Keefe, Penttila construction of the Adelaide $q$-clans is that, as they show, it extends to all of the known $q$-clans, $q$ even, by adjusting $m$ and $\beta$, although we won't give the details here. This new work is truly impressive.

In their paper Cherowitzo, O'Keefe and Penttila also show that GQs from the Adelaide $q$-clans are new. From this it follows that the associated flocks and translation planes are also new. These results together with the facts that the ovals are new in the cases $q = 64$ and $q = 256$ accessible by computer suggest the Adelaide hyperovals are new, although this is *yet* to be proved.

**General remark:** As the reader may have noticed the area of flock, $q$-clan, GQ, herds of hyperovals research is complex and we have been able only to scratch the surface. As a general survey on the area the reader is encouraged to read Johnson and Payne [30].

### 2.3.4 Hyperovals from $\alpha$-flocks

Let $q = 2^h$, $h$ odd and let $\sigma$ be the automorphism of $\mathrm{GF}(q)$ such that $\sigma^2 \equiv 2 \pmod{q-1}$. Then in the cases $h = 5, 7$ and $9$ Cherowitzo ([10]) proved that the function

$$f(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$$

was a new o-polynomial and conjectured that it was an o-polynomial for general $h$ odd. In [11] Cherowitzo proved this using $\alpha$-flocks.

Let $\alpha$ be a generator of the automorphism group of $\mathrm{GF}(q)$ and let $\mathcal{K}_\alpha$ be a cone in $\mathrm{PG}(3, q)$ with vertex a point and base an oval equivalent to $\{(1, t, t^{\alpha}) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\}$, the canonical version having equation $x_1^{\alpha} = x_0 x_2^{\alpha-1}$. (Such an oval is called a *translation oval* and completes to the translation hyperoval $\mathcal{D}(\alpha)$.) Analogous to the definition of a flock of a quadratic cone, an *$\alpha$-flock* is a set of $q$ planes of $\mathrm{PG}(3, q)$, not containing the vertex of $\mathcal{K}_\alpha$, which pairwise do not intersect in a point of $\mathcal{K}_\alpha$. The crucial theorem of Cherowitzo's paper [11], which we present in a different formulation to the original, is

**Theorem 2.17.** *If the set of planes of* PG$(3, q)$ *given by the equations* $\{f(t)x_0 + t^{1/\alpha}x_1 + g(t)x_2 + x_3 = 0 : t \in \mathrm{GF}(q)\}$ *is a (normalised)* $\alpha$*-flock, then* $f(t)$ *is an o-polynomial.*

Using this Cherowitzo was able to prove that his examples of hyperovals did extend to an infinite family of hyperovals with the o-polynomial given above.

It should be noted that the definition of $\alpha$-flocks includes that of flocks and that an oval in a herd of a flock extends to a hyperoval with an o-polynomial as in Theorem 2.17. Cherowitzo also showed that both of the Glynn hyperovals (see page 10 had o-polynomials arising from an $\alpha$-flock, for $\alpha = \sigma$.

This means all known hyperovals *except* the O'Keefe-Penttila hyperoval in PG$(2, 32)$ are associated in the above way with an $\alpha$-flock. So either the O'Keefe-Penttila oval is truly sporadic (and note that sporadic is not a well defined term!) or there are new construction methods of hyperovals to be discovered that include it.

### 2.3.5 Automorphism groups of hyperovals

We won't be discussing the automorphism groups of the known hyperovals here, but will merely point the reader in the direction of the appropriate references. The paper of O'Keefe and Penttila, [42], contains proofs and references of proofs for the automorphism groups of the regular, Segre, Glynn and Payne infinite families of hyperovals. The automorphism group of the Subiaco hyperovals has been determined by Payne, Penttila, Pinneri [55] and O'Keefe and Thas [47]. For the group of the Cherowitzo hyperoval in PG$(2, 32)$ see O'Keefe, Penttila, Praeger [45] and for some results on the group in general see O'Keefe, Thas [47]. Finally the determination of the group of the O'Keefe-Penttila hyperoval in PG$(2, 32)$ is contained in O'Keefe and Penttila [40].

### 2.3.6 The classification of hyperovals in small order spaces

**PG$(2,2)$, PG$(2,4)$ and PG$(2,8)$:** In PG$(2, 2)$ any three non-collinear points form a conic and since a hyperoval consists of four points every hyperoval must be a conic plus its nucleus, that is a regular hyperoval.

For PG$(2, q)$, $q \geq 4$, we know that through any five points of PG$(2, q)$, no three collinear, there is a conic of the plane ([27, Corollary 7.5]). Hence for PG$(2, 4)$ a hyperoval has six points any five of which form a conic. Thus every hyperoval is regular.

In PG$(2, 8)$ the Segre hyperoval $\mathcal{D}(6)$ and the translation hyperoval $\mathcal{D}(4)$ are regular (by Theorem 2.13). If $f$ is any o-polynomial the degree of $f$ is either 2, 4 or 6 (since it must have even degree). If the degree is 2 then we must have $x^2$, if the degree is 4 then $f$ is additive and so must be $x^4$. If the degree is 6 it is possible to show that the hyperoval must be Segre.

**PG$(2,16)$:** In [23] Hall showed, with the aid of computer, that there were two projectively distinct hyperovals in PG$(2, 16)$: the regular hyperoval and the Lunelli-Sce hyperoval. In [39] O'Keefe and Penttila proved the result without the aid of a computer. First they calculated an upper bound for the number of different o-polynomials over GF(16) and then by investigating the possible automorphism groups of hyperovals in PG(2, 16) showed that the o-polynomials from a putative new hyperoval plus the o-polynomials from the regular and Lunelli-Sce hyperovals would exceed the upper bound.

PG(2, 32)**:** In [59] Penttila and Royle devised a simple yet ingenious method of labelling arcs in PG(2, $q$) which allowed them to write an efficient computer program to search for hyperovals in PG(2, 32). Their results showed that there are six projectively distinct hyperovals in PG(2, 32): the regular hyperoval, the translation hyperoval $\mathcal{D}(4)$, the Segre hyperoval, the Payne hyperoval $\mathcal{D}(x^6 + x^{16} + x^{28})$, the Cherowitzo hyperoval $\mathcal{D}(x^8 + x^{10} + x^{28})$ and the mysterious O'Keefe-Penttila hyperoval $\mathcal{D}(x^4 + x^{16} + x^{28} + \beta^{11}(x^6 + x^{10} + x^{14} + x^{18} + x^{22} + x^{26}) + \beta^{20}(x^8 + x^{20}) + \beta^6(x^{12} + x^{24}))$, where $\beta$ is a primitive root of GF(32) satisfying $\beta^5 = \beta^2 + 1$.

Note that while the Glynn hyperovals are defined for PG(2, 32) in this case they are both equivalent to the translation hyperoval $\mathcal{D}(4)$.

### 2.3.7 A summary of the known hyperovals

In this final section on hyperoval we present a table listing the known hyperovals. The idea and format of the table have been "borrowed" from the hyperoval web site of Cherowitzo ([9]) which is an *excellent* reference for information on hyperovals.

**The Known Hyperovals in PG(2, $2^h$)**

| Name | O-Polynomial | Field Restriction | Section |
|---|---|---|---|
| Regular | $f(x) = x^2$ | None | Section 2.3.1 |
| Translation | $f(x) = x^{2^i}$, $(i, h) = 1$ | None | Section 2.3.1 |
| Segre | $f(x) = x^6$ | $h$ odd | Section 2.3.1 |
| Glynn I | $f(x) = x^{3\sigma+4}$, $\sigma^2 \equiv 2$ | $h$ odd | Section 2.3.1 |
| Glynn II | $f(x) = x^{\sigma+\gamma}$, $\sigma^2 = \gamma^4 \equiv 2$ | $h$ odd | Section 2.3.1 |
| Payne | $f(x) = x^{3/6} + x^{5/6} + x^{1/2}$ | $h$ odd | Section 2.3.3 |
| Subiaco | See Section 2.3.3 | None | Section 2.3.3 |
| Cherowitzo | $f(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$, $\sigma^2 \equiv 2$ | $h$ odd | Section 2.3.4 |
| Adelaide | See Section 2.3.3 | $h$ even | Section 2.3.3 |
| O'Keefe-Penttila | See Section 2.3.2 | $h = 5$ | Section 2.3.2 |

# 3 Ovoids of $\mathrm{PG}(3, q)$

It has been claimed that ovoids of $\mathrm{PG}(3, q)$ are the centre of the geometrical universe. While this may be debatable (to some) there is no denying the richness and elegance of ovoids and their many connections to other areas of finite geometry. For example from an ovoid of $\mathrm{PG}(3, q)$ may be constructed a GQ of order $(q, q^2)$ (due to Tits, see [15]) and an inversive plane. In fact in the case where $q$ is even inversive planes are equivalent to ovoids (see [15, 6.2]). Other objects constructed from ovoids include spreads, translation planes, unitals of translation planes ([8]), maximal arcs and partial geometries (see [74]). However in these notes our interest will be directly in results on ovoids and the theory of ovoids rather than these related geometrical structures.

For an excellent survey on ovoids see [36]. For general results on ovoids as well as details on the elliptic quadric ovoid, the Tits ovoid and the classification of ovoids for $q$ odd see [26, Chapter 16].

In this section we shall expand upon our discussion in Section 1. In particular we shall prove some properties of an ovaloid of $\mathrm{PG}(3, q)$ (the Segre definition), and also properties of ovoids of $\mathrm{PG}(n, q)$ (the Tits definition). This will allow us to show the equivalence of an ovaloid of $\mathrm{PG}(3, q)$ and an ovoid of $\mathrm{PG}(3, q)$ for $q > 2$. We shall summarise the discussion by giving the most common "contemporary" definition of an ovoid and its properties.

First we discuss ovaloids, that is a set of points of $\mathrm{PG}(3, q)$, no three collinear, of maximal size. We begin with a definition of Segre.

**Definition 3.1.** *A $k$-cap of $\mathrm{PG}(3, q)$ is a set of $k$ points no three collinear.*

An ovaloid is a $k$-arc of maximum size. Using the Bose notation introduced in Section 1 let $m(3, q)$ denote this maximum size of a $k$-cap in $\mathrm{PG}(3, q)$. We shall show that for $q > 2$ that $m(3, q) = q^2 + 1$, which was first proved by Bose ([4]) for $q$ odd, Seiden ([70]) for $q = 4$ and Qvist ([63]) for $q > 2$ and even. The first step in the process is to show that there is a $k$-cap that satisfies the bound, i.e. with $k = q^2 + 1$.

**The classical examples: elliptic quadrics.** A non-singular quadric of $\mathrm{PG}(3, q)$ of elliptic type, called an *elliptic quadric*, is a set of $q^2+1$ points no three collinear. There is a single orbit of elliptic quadrics under the group of $\mathrm{PG}(3, q)$ and the canonical example is given by the equation $x_0^2 + x_0x_1 + ax_1^2 + x_2x_3 = 0$, where $a$ is an element of $\mathrm{GF}(q)$ such that $x^2 + x + a$ is irreducible over $\mathrm{GF}(q)$. As a set of points this is

$$\{(s, t, s^2 + st + at^2, 1) \,:\, s, t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1, 0)\}.$$

An elliptic quadric defines a polarity of $\mathrm{PG}(3, q)$ (see [28, Chapter 22]) under which a point of the elliptic quadric is mapped to the plane consisting of the tangents to the elliptic quadric at that point. Hence the elliptic quadric is an example of an ovoid of $\mathrm{PG}(3, q)$.

Note that every secant plane section of an elliptic quadric is a conic.

**Theorem 3.2.** *[[4] $q$ odd, [70] $q = 4$, [63] $q$ even] The size of an ovaloid $\mathcal{O}$ is $q^2 + 1$ for $q > 2$.*

**Proof.** Suppose $q$ is odd. Let $P$ and $Q$ be two points of $\mathcal{O}$ and $\ell$ the line that they span. Considering the intersection of each of the planes on $\ell$ with $\mathcal{O}$ we have $|\mathcal{O}| \leq (q+1)(q-1)+2 = q^2+1$, and since we know that the elliptic quadric satisfies the bound we have equality.

The $q$ even case is a little trickier. Suppose that there is no line of $\mathrm{PG}(3,q)$ that is tangent to $\mathcal{O}$. Let $P$ and $Q$ be two points on $\mathcal{O}$ and $\ell$ the line they span. Each of the planes on $\ell$ must intersect $\mathcal{O}$ in a hyperoval and so $|\mathcal{O}| = (q+1)q+2 = q^2+q+2$. Let $R$ be a point not on $\mathcal{O}$. $R$ is incident with $(q^2+q+2)/2$ secants to $\mathcal{O}$ and each plane on $R$ either meets $\mathcal{O}$ in a hyperoval or meets $\mathcal{O}$ in no points. Hence counting incident pairs $(\ell, \pi)$ where $\ell$ is a secant on $R$ and $\pi$ a plane (necessarily meeting $\mathcal{O}$ in a hyperoval) we obtain

$$(\frac{q}{2}+1)k = \frac{q^2+q+2}{2}(q+1),$$

where $k$ is the number of planes incident with $R$ meeting $\mathcal{O}$ in a hyperoval. It follows that $q = 2$. Thus if $q \neq 2$ there exists a tangent $m$ to $\mathcal{O}$ at some point $X$ say. Considering the planes about $m$ we see that $|\mathcal{O}| \leq (q+1)q+1 = q^2+q+1$. If each plane about $m$ meets $\mathcal{O}$ in at most $q$ points we have $|\mathcal{O}| \leq (q+1)(q-1)+1 \leq q^2+1$ (as required) so suppose there is a plane $\pi$ on $m$ meeting $\mathcal{O}$ in an oval. Let $N$ be the nucleus of the oval in $\pi$. If $N$ lies on only tangents to $\mathcal{O}$ we may extend $\mathcal{O}$ by adding $N$ and so $N$ must lie on at least one secant, $n$ say. Each plane on $n$ meets $\pi$ in a tangent to $\mathcal{O}$ and so meets $\mathcal{O}$ in at most $q+1$ points. Considering the planes about $n$ we see thus see that $|\mathcal{O}| \leq (q+1)(q-1)+2 = q^2+1$. $*\square$

Now we see that an equivalent definition of an ovaloid, for $q > 2$, is a set of $q^2+1$ points no three collinear. We show that such a set of points is also an ovoid of $\mathrm{PG}(3,q)$, that is the union of the tangents to a point of an ovaloid form a plane.

**Theorem 3.3 ([1, 2, 49]).** *Let $\mathcal{O}$ be an ovaloid of* $\mathrm{PG}(3,q)$*, $q > 2$, then*

(i) *for $P \in \mathcal{O}$ the union of all the tangents on $P$ is a plane; and*

(ii) *exactly $q^2+1$ planes of* $\mathrm{PG}(3,q)$ *meet $\mathcal{O}$ in a unique point and the other $q^3+q$ planes meet $\mathcal{O}$ in an oval.*

**Proof.** (i) For $q$ odd let $P, Q$ be two points of $\mathcal{O}$. Since for $q$ odd each plane of $\mathrm{PG}(3,q)$ can meet $\mathcal{O}$ in at most $q+1$ points it follows that each of the planes about the line spanned by $P$ and $Q$ meets $\mathcal{O}$ in exactly $q+1$ points, that is an oval. Thus a secant line can only lie on planes meeting $\mathcal{O}$ in an oval. Let $\ell_1, \ell_2$ be two tangents to $\mathcal{O}$ at $P$ and let $\pi$ be the plane they span. Since $\pi$ contains two tangents to $\mathcal{O}$ at $P$ it cannot meet $\mathcal{O}$ in an oval and so it cannot contain any secants. Thus $\pi \cap \mathcal{O} = \{P\}$ and $\pi$ is the union of all tangents on $P$.

For $q$ even let $P \in \mathcal{O}$ and let $\ell$ be a tangent to $\mathcal{O}$ on $P$. In the proof of Theorem 3.2 we saw that there must exist a plane $\pi$ on $\ell$ such that $\pi \cap \mathcal{O}$ is a $q+1$ arc with nucleus $N$ and that $N$ lies on some secant $n$. Each plane on $n$ contains a tangent on $N$ by intersection with $\pi$. It follows that each plane on $n$ meets $\mathcal{O}$ in an oval. In such a plane $N$ lies on a unique tangent which must be the intersection of the plane with $\pi$. Hence all of the tangents on $N$ lie in $\pi$. So any plane on $\ell$, not $\pi$, that contains a second point $Q$ of $\mathcal{O}$ contains a secant $\langle N, Q\rangle$ and so meets $\mathcal{O}$ in an oval. So we see that any plane on $\ell$ meets $\mathcal{O}$ in exactly $P$ or in an oval from which it must be that the tangents on $P$ form a plane.

(ii) From (i) each point of $\mathcal{O}$ has a unique tangent plane. Also any other plane on a tangent must meet $\mathcal{O}$ in an oval. Counting reveals that this is all the planes of $\mathrm{PG}(3, q)$. $*\square$

A plane meeting an ovoid in an oval is called a *secant plane*. An oval that is the intersection of an ovoid and a secant plane of the ovoid is called a *secant plane section* or an *oval section*.

By Theorem 3.3 an ovaloid of $\mathrm{PG}(3, q)$ is also an ovoid as defined by Tits. We now see that the Tits definition of an ovoid in $\mathrm{PG}(n, q)$ can only be realised when $n \leq 3$.

**Theorem 3.4.** *([80], see [15]) If* $\mathrm{PG}(n, q)$ *has an ovoid* $\Omega$*, then*

(i) $|\Omega| = q^{n-1} + 1$*; and*

(ii) $n \leq 3$

**Sketch Proof.** (i) If $P \in \Omega$ there are $(q^{n-1} - 1)/(q - 1)$ tangents on $P$ and hence $q^{n-1}$ secants.
(ii) The conic and elliptic quadric provide examples of ovoids for $n = 2, 3$, so assume $n > 3$. On any point of $\Omega$ there is one tangent hyperplane and the rest of the hyperplanes intersect $\Omega$ in an ovoid (of the hyperplane). Now counting incident pairs (point of $\Omega$, non-tangent hyperplane) we have

$$\frac{(q^{n-1} + 1)(q^n - q)}{q - 1} = k(q^{n-1} + 1),$$

where $k$ is the total number of hyperplanes intersecting $\Omega$ in an ovoid. This provides a contradiction (exercise). $*\square$

This result means that there is something very special about the study of $k$-caps of maximal size in $\mathrm{PG}(3, q)$ as opposed to any other dimension of projective space.

As a summary of the above discussion we now give the defintion (seen in Section 1) and properties of an ovoid of $\mathrm{PG}(3, q)$, $q > 2$, that we shall be using from this point.

**Definition 1.3.** An *ovoid* of $\mathrm{PG}(3, q)$ is a set of $q^2 + 1$ points no three collinear.

We shall usually use $\Omega$ as notation for an ovoid of $\mathrm{PG}(3, q)$.

**Theorem 3.5.** (i) *Ovoids exist for all* $\mathrm{PG}(3, q)$.

(ii) *For $q > 2$ an ovoid is a maximum size of a set of points of* $\mathrm{PG}(3, q)$ *no three collinear.*

(iii) *The union of all tangents on a fixed point of an ovoid is a plane.*

(iv) *Let $\Omega$ be an ovoid of* $\mathrm{PG}(3, q)$. *Then exactly $q^2 + 1$ planes of* $\mathrm{PG}(3, q)$ *meet $\Omega$ in a unique point and the other $q^3 + q$ planes meet $\Omega$ in an oval.*

In all of the theorems and definitions to date we usually apply the condition that $q > 2$, as this case is a little different. As a postscript to this section we will discuss how and why it is different.

**Theorem 3.6.** *The largest $k$-cap in* PG(3, 2) *has $k = 8$, that is $m(3, 2) = 8 > 2^2 + 1$.*

**Proof.** The complement of a hyperplane in PG(3, 2) is a set of 8 points no three collinear. On any point of PG(3, 2) there are 7 lines and so the maximum *possible* size for a $k$-cap is 8. $*\square$

An elliptic quadric of PG(3, 2) is an ovoid, however in this case it is not a maximal sized set of point no three collinear.

## 3.1 The classification of ovoids of PG(3, q), q odd

We now look at the classification of ovoids of PG(3, $q$) for $q$ odd. Analogously to the case of ovals in PG(2, $q$) the classification of ovoids as classical, in this case elliptic quadrics, occurred early in the study of ovoids and is achieved by some elementary geometry. The classification of ovoids for $q$ odd relies directly on the classification of ovals for $q$ odd. Using this we can assume that every secant plane section of an ovoid is a conic, which is a very strong condition (we shall see later that in fact when $q$ is even we need only *one* conic section to force the ovoid to be an elliptic quadric). The result was proved independently in 1955 by Barlotti ([1]) and Panella ([49]). Barlotti showed that if all oval sections of an ovoid in PG(3, $q$), $q$ odd, are conics then the ovoid is an elliptic quadric. He then noticed that this characterisation was valid also for $q$ even resulting in the following theorem.

**Theorem 3.7 (Barlotti [2]).** *Let $\Omega$ be an ovoid of* PG(3, $q$) *with $q > 2$. If every secant plane section of $\Omega$ is a conic, then $\Omega$ is an elliptic quadric.*

**Proof.** First we consider the case $q = 3$ and so $|\Omega| = 10$. Let $\ell$ be a line of PG(3, 3) exterior to $\Omega$. Then of the four planes on $\ell$ two, $\pi_1$ and $\pi_2$, meet $\Omega$ in a conic and two, $\pi_3$ and $\pi_4$, are tangent to $\Omega$. Let $\pi_1 \cap \Omega = \mathcal{C}_1$ and $\pi_2 \cap \Omega = \mathcal{C}_2$ and let $\pi_3$, $\pi_4$ be tangent at $P_3$ and $P_4$, respectively. The nine points $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \{P_3\}$ define an elliptic quadric $\mathcal{E}$, we want to show that $P_4 \in \mathcal{E}$ so that $\Omega = \mathcal{E}$. Suppose that $\mathcal{E} \neq \Omega$ and so $P_4 \notin \mathcal{E}$ and $\mathcal{E} \setminus \Omega = \{X\}$ for some point $X$. Since $\mathcal{E}$ and $\Omega$ are maximal sized sets of points no three collinear it must be that the line $m = \langle P_4, X\rangle$ contains a further point $Y$ of $\mathcal{E} \cap \Omega$, i.e. $m$ is a secant to both $\mathcal{E}$ and $\Omega$. Each plane on $m$ meets both $\mathcal{E}$ and $\Omega$ in a conic and for a given plane its intersection with $\mathcal{E}$ and its intersection with $\Omega$ have three (out of four) points in common. So let $\pi$ be a plane on $m$, with $\pi \cap \mathcal{E} = \mathcal{C}$, $\pi \cap \Omega = \mathcal{C}'$ and $\mathcal{C} \cap \mathcal{C}' = \{Y, A, B\}$. The line $\langle A, B\rangle$ cannot contain $P_4$, $Y$ or $X$ and so must meet $m$ in the remaining point of $M$, $Q$ say. It follows that $Q$ lies on no tangents of $\mathcal{E}$ or $\Omega$, which is a contradiction. Hence $\Omega = \mathcal{E}$ is an elliptic quadric.

Now suppose that $q \geq 4$. Let $P_1$ and $P_2$ be two points of $\Omega$ and $\ell$ the line they span. Let $\pi_1$ and $\pi_2$ be two planes containing $\ell$ and hence meeting $\Omega$ in conics, $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Let $P_1, P_2, P_3, P_4, P_5$ be five distinct points of $\mathcal{C}_1$ and $P_1, P_2, Q_3, Q_4, Q_5$ five distinct points of $\mathcal{C}_2$. Let $R$ be any point of $\Omega$ not on $\pi_1$ or $\pi_2$ and $\mathcal{Q}$ the unique quadric containing the points $P_1, P_2, P_3, P_4, P_5, Q_1, Q_2, Q_3, R$. Since five points in a plane determine a unique conic (see [27, Corollary 7.5]) it follows that $\mathcal{Q}$ must contain $\mathcal{C}_1$ and $\mathcal{C}_2$ (since $\pi_1 \cap \mathcal{Q}$ and $\pi_2 \cap \mathcal{Q}$ are conics). From this we know that the tangents to both $\mathcal{C}_1$ and $\mathcal{C}_2$ at the point $P_1$ are tangents to both $\Omega$ and $\mathcal{Q}$. Hence $\Omega$ and $\mathcal{Q}$ have the same tangent plane at $P_1$, and similarly for $P_2$.

Now let $\pi_3$ be the plane $\langle \ell, R\rangle$ and $\mathcal{C}_3$ the conic $\pi_3 \cap \Omega$. Since $\mathcal{C}_3$ and $\mathcal{Q} \cap \pi_3$ (also a conic) share the points $P_1, P_2, R$ *and* tangents to $P_1$ and $P_2$ this is enough to force $\mathcal{C}_3$ to be contained in $\mathcal{Q}$ (elementary exercise in quadrics).

All that remains now is to show that any point $P \in \Omega$ not on $\pi_1$, $\pi_2$ or $\pi_3$ is contained in $\mathcal{Q}$. Let $\pi$ be a plane containing $\langle P, P_1\rangle$ but not $P_2$ nor the tangents to $\mathcal{C}_1$ and $\mathcal{C}_2$ at $P_1$. It follows that $\pi$ must meet each of $\pi_1$, $\pi_2$ and $\pi_3$ in a secant and hence contain a second point, other than $P_1$, of $\pi_1$, $\pi_2$ and $\pi_3$. Since these three points are in $\mathcal{Q}$ we have that the conic $\pi \cap \Omega$ shares with $\pi \cap \mathcal{Q}$ four points and the tangent at $P_1$ and so must be contained in $\mathcal{Q}$. Hence $P \in \mathcal{Q}$ and $\Omega = \mathcal{Q}$ which must be an elliptic quadric. $*\square$

## 3.2 Ovoids of $\mathrm{PG}(3, q)$, $q$ even

In the previous section we saw that as with the $q$ odd case for ovals the ovoids of $\mathrm{PG}(3, q)$ for $q$ odd were shown to be classical by some elegant yet straight-forward projective geometry. We now direct our attention once again to the more complicated and mysterious $q$ even case. We shall start with some fundamental general results for ovoids in the $q$ even case, then give the construction of the only known non-classical ovoid: the Tits ovoid. Following this we shall outline general characterisation results and classification results for small order spaces.

### 3.2.1 Symplectic polarities, the generalized quadrangle $W(q)$ and ovoids

The *dual space* of $\mathrm{PG}(3, q)$ is the projective three space labelled $\mathrm{PG}(3, q)^\wedge$ with pointset the set of planes of $\mathrm{PG}(3, q)$; lineset the set of lines of $\mathrm{PG}(3, q)$; with planes the points of $\mathrm{PG}(3, q)$ and incidence induced from $\mathrm{PG}(3, q)$. A *polarity* of $\mathrm{PG}(3, q)$ is a map from the set of subspaces of $\mathrm{PG}(3, q)$ onto itself that maps points to planes, lines to lines, planes to planes, preserves incidence *and* has order 2. In other words a polarity is a special kind of isomorphism from $\mathrm{PG}(3, q)$ to $\mathrm{PG}(3, q)^\wedge$. A point, line or plane of $\mathrm{PG}(3, q)$ is *absolute* with respect to a polarity if it is incident with its own image under the polarity. The *symplectic polarity* of $\mathrm{PG}(3, q)$ is a polarity with the property that every point (and hence every plane) is absolute. The canonical form of the symplectic polarity of $\mathrm{PG}(3, q)$ acts on points/planes by

$$(p_0, p_1, p_2, p_3) \longleftrightarrow p_1x_0 - p_0x_1 + p_3x_2 - p_2x_3 = 0.$$

The map of the polarity on the lines is induced by the action on points/planes. Two points span an absolute line with respect to the canonical symplectic polarity if their coordinates satisfy

$$x_0y_1 - x_1y_0 + x_2y_3 - x_3y_2 = 0.$$

Of course in the $q$ even case with which we will be dealing we can dispense with the minus sign. For more on polarities of projective spaces see [15, 1.4] and [27].

The set of absolute lines of a symplectic polarity forms a linear complex of lines of $\mathrm{PG}(3, q)$ (see [26, 15]). The incidence structure of absolute points and lines of the symplectic polarity is the *generalized quadrangle* $W(q)$ of order $(q, q)$. Since the polarity is symplectic *all* of the points of $\mathrm{PG}(3, q)$ are absolute and so $W(q)$ consists of all of the points of $\mathrm{PG}(3, q)$ and a subset of the lines of $\mathrm{PG}(3, q)$. (For more on generalized quadrangles see [56] and [76].)

One of the most fundamental results on ovoids of $\mathrm{PG}(3, q)$, $q$ even, is the construction of a symplectic polarity from an ovoid.

**Theorem 3.8 (Segre [68]).** *Let $\Omega$ be an ovoid of $\mathrm{PG}(3, q)$ where $q > 2$ is even. Then $\Omega$ determines a symplectic polarity of $\mathrm{PG}(3, q)$ which interchanges each tangent plane of $\Omega$ with its point of tangency and interchanges each secant plane $\pi$ with the nucleus of the oval $\pi \cap \Omega$.*

Importantly this result allows us to make use of the theory of generalized quadrangles in studying ovoids. An *ovoid* $\mathcal{R}$ of a generalized quadrangle $\mathcal{S}$ of order $(q, q)$ is a set of points of $\mathcal{S}$ such that each line of $\mathcal{S}$ is incident with a unique point of the set. It follows that $|\mathcal{R}| = q^2 + 1$ and that $\mathcal{R}$ may be thought of as a set of $q^2 + 1$ points of $\mathcal{S}$ no *two* collinear. From Theorem 3.8 we have that the GQ $W(q)$ associated with an ovoid $\Omega$ of $\mathrm{PG}(3, q)$ is all of the points of $\mathrm{PG}(3, q)$ and the lines that are tangent to $\Omega$. Hence an ovoid $\Omega$ of $\mathrm{PG}(3, q)$ is an ovoid of the *generalized quadrangle* $W(q)$ constructed from the associated symplectic polarity. It should be noted that since $\mathrm{P\Gamma L}(4, q)$ is transitive on linear complexes given an ovoid $\Omega$ of $\mathrm{PG}(3, q)$ and a $W(q)$ defined in $\mathrm{PG}(3, q)$, there is an ovoid projectively equivalent to $\Omega$ that is an ovoid of $W(q)$.

In 1972 Thas proved another fundamental result on ovoids, a converse to Theorem 3.8.

**Theorem 3.9 (Thas [72]).** *Let $W(q)$ be the generalized quadrangle arising as the set of absolute points and lines of a symplectic polarity of $\mathrm{PG}(3, q)$, $q$ even. If $\Omega$ is an ovoid of $W(q)$, then it is also an ovoid of $\mathrm{PG}(3, q)$.*

Having discussed some basic results on ovoids of $\mathrm{PG}(3, q)$, $q$ even, we now move onto the construction of the only non-classical ovoid, the Tits ovoid.

### 3.2.2 The Tits ovoid

In this section we will outline the construction of the Tits ovoid. We begin by discussing polarities of $W(q)$. A *polarity* of $W(q) = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a map $\phi : \mathcal{P} \cup \mathcal{B} \rightarrow \mathcal{P} \cup \mathcal{B}$, such that $\phi$ maps points to lines, lines to points, preserves incidence *and* has order two. A polarity of $W(q)$ is particularly nice for the following reason.

**Theorem 3.10 (Tits [81]).** *Let $\phi$ be a polarity of $W(q)$. The set of absolute points of $\phi$ is an ovoid of $\mathrm{PG}(3, q)$.*

Tits also established the following result.

**Theorem 3.11 (Tits [81]).** *Suppose that $q = 2^h$. Then $W(q)$ possesses a polarity if and only if $h$ is odd, and in this case all polarities of $W(q)$ are equivalent.*

It should be noted that the actual construction of the Tits ovoid was in [79].

(Note that the above results generalises to GQs in the sense that if a GQ of order $(s, s)$ has a polarity then $2s$ is square and also the set of absolute points of the polarity is an ovoid of the GQ ([50], see [56, 1.8.2])).

The unique ovoid of $\mathrm{PG}(3, q)$, $q = 2^{2^{2e+1}}$, that arises in this manner is the Tits ovoid. The canonical form of the Tits ovoid is

$$\{(1, st + s^{\sigma+2} + t^{\sigma}, s, t) \, : \, s, t \in \mathrm{GF}(q)\} \cup \{(0, 1, 0, 0)\},$$

where $\sigma : x \mapsto x^{2^{e+1}}$. The $W(q)$ associated with the ovoid is defined by the form $x_0y_1 + x_1y_0 + x_2y_3 + x_3y_2 = 0$.

We will now give a brief outline of the specific construction of the Tits ovoid. Embed $\mathrm{PG}(3, q)$ in $\mathrm{PG}(5, q)$. Using the Klein correspondence (see [26, Chapter 15]) the lines of $\mathrm{PG}(3, q)$ are mapped onto the points of a non-singular hyperbolic quadric of $\mathrm{PG}(5, q)$. The lines of $W(q)$ are mapped onto the points of a non-singular parabolic quadric $Q(4, q)$ in a four-dimensional subspace of $\mathrm{PG}(5, q)$. The points of $W(q)$ are mapped onto the lines of $Q(4, q)$ (giving a duality from the GQ $W(q)$ to the GQ $Q(4, q)$). Since $q$ is even the quadric $Q(4, q)$ has a nucleus $N$ and so we project $Q(4, q)$ from $N$ onto the points and lines of $W(q)'$ (equivalent to $W(q)$) in $\mathrm{PG}(3, q)$ (here we need to have embedded $\mathrm{PG}(3, q)$ such that $N$ is not contained in it). Applying a collineation of $\mathrm{PG}(3, q)$ we can map $W(q)'$ to $W(q)$. Let this whole process above be the map $\psi$.

In summary $\psi$ maps points of $W(q)$ to lines of $W(q)$; lines of $W(q)$ to points of $W(q)$ and preserves incidence. The map $\psi$ is not necessarily a polarity since we do not know if it has order 2. However, if $\phi$ is a polarity, then $\phi \circ \psi^{-1}$ is a collineation of $\mathrm{PG}(3, q)$, so $\phi = T \circ \psi$ for some collineation $T$ of $\mathrm{PG}(3, q)$. Imposing the condition that maps of the form $T \circ \psi$ have order 2 gives us the polarities of $W(q)$ and hence the Tits ovoids. For a more detailed account of the explicit construction of the Tits ovoids see Chapter 16 of [26], although it is good practice to perform the calculations oneself!

In the case $q = 8$ Segre ([68]) constructed the Tits ovoid *before* the construction of the infinite family by Tits. Segre gave conditions for non elliptic quadric ovoids to exist and showed that they were satisfied for $q = 8$ but not for $q = 16$. It was later shown that the conditions are not satisfied for $q > 8$ ([24]). In 1962 Fellegara ([17]) showed that for $q = 8$ the ovoid of Segre and the ovoid of Tits are projectively equivalent.

One of the motivations of the study of Tits into ovoids of $\mathrm{PG}(3, q)$ and construction of the Tits ovoids is the fact that the full group of the ovoid in $\mathrm{PGL}(4, q)$ is $Sz(q)$, the simple group of Suzuki. (See Suzuki [71] for an elegant exposition of the construction and properties of this group.)

**Theorem 3.12 (Tits [79, 82]).** *Let $\Omega$ be the Tits ovoid of $\mathrm{PG}(3, q)$. Then*

(i) *the full stabiliser of $\Omega$ in $\mathrm{PGL}(4, q)$ is the Suzuki simple group $Sz(q)$;*

(ii) *$Sz(q)$ is doubly transitive on $\Omega$;*

(iii) *only the identity of $Sz(q)$ fixes more than two points of $\Omega$;*

(iv) *$Sz(q)$ is transitive on the points of* $\mathrm{PG}(3,q) \setminus \Omega$.

Here we have only touched briefly on the group theoretic aspects of ovoids. For more on groups and ovoids, in particular results characterising ovoids by their automorphism group, see [15, 1.4].

As a final note to this section we make some remarks on a spread of $\mathrm{PG}(3,q)$ associated with the Tits ovoid. Tits proved that the set of absolute points of a polarity of $W(q)$ is an ovoid of $\mathrm{PG}(3,q)$ (see Theorem 3.10) and from this it follows that the set of absolute lines of the polarity is a spread of $\mathrm{PG}(3,q)$. This spread is a spread giving rise to the so called Lüneburg plane [34, 72].

## 3.3 Geometrical characterisations of ovoids and classification of ovoids in small spaces

We now proceed to review known geometrical characterisation results for ovoids and classification results for small $q$. We divide this review into three "generations" of results according, roughly, to the period in which the results were proved and/or the techniques employed. We will mainly be dealing with results characterising ovoids by the nature of their secant plane sections.

### 3.3.1 Generation 1: "Classical" geometry and the GQ $W(q)$

In this section we look at early characterisation results on ovoids which make use of either classical geometrical techniques in $\mathrm{PG}(3,q)$.

We have already seen from Theorem 3.7 of Barlotti that if every secant plane section of an ovoid is a conic, then the ovoid is an elliptic quadric. This result is independent of whether $q$ is odd or even. For $q$ odd since all ovals are conics the classification of ovoids follows. Similarly for $q = 4$. However for $q \geq 8$ and even there are always non-conic ovals so the theorem of Barlotti will not lead to a classification of ovoids in any other case.

In 1959 Segre improved the result of Barlotti to the following.

**Theorem 3.13 (Segre [68]).** *An ovoid of* $\mathrm{PG}(3,q)$*,* $q \geq 8$*, which contains at least* $(q^3 - q^2 + 2q)/2$ *conics must be an elliptic quadric.*

In 1962 Fellegara ([17]) proved, using a computer search, that the only ovoids of $\mathrm{PG}(3,8)$ are the elliptic quadrics and the Tits ovoids. Penttila and Praeger ([61]) proved the same result, computer free, in 1997. We shall mention this work in more detail in the next section.

Next we consider characterisation results relating to bundles, pencils and flocks of an ovoid. Let $\Omega$ be an ovoid of $\mathrm{PG}(3,q)$ and $\ell$ a fixed line of $\mathrm{PG}(3,q)$. First suppose that $\ell$ is a secant to $\Omega$ with $\ell \cap \Omega = \{P, Q\}$. Then each plane on $\ell$ intersects $\Omega$ in an oval. This set of $q+1$ ovals is called a *bundle*. Next supose that $\ell$ is a tangent to $\Omega$, then one of the planes on $\ell$ is tangent to $\Omega$ and the other $q$ meet $\Omega$ in an oval. This set of $q$ ovals is called a *pencil*. Finally let $P, Q$ be any two points of $\Omega$. A partition of $\Omega \setminus \{P, Q\}$ into ovals is called a *flock* of $\Omega$. These definitions arise from the connection of ovoids to inversive planes which we will not discuss here (the reader is referred to the book of Dembowski [15]).

If a flock of $\Omega$ has the property that each plane of an oval in the flock contains a fixed line (necessarily) external to $\Omega$, then the flock is called *linear*. Conversely, taking the intersection with $\Omega$ of secant planes on a fixed external to $\Omega$ gives a (linear) flock. In fact every flock of an ovoid is linear which was proved in the odd case by Orr ([3, 48]) and in the even case by Thas ([18, 73]).

A natural extension of the work of Barlotti and Segre in characterising the elliptic quadric by a number of conic sections was to the bundle, pencil and flock cases. It was proved that if a bundle, a pencil or a flock of an ovoid consists entirely of conics then the ovoid is an elliptic quadric. The bundle result is due to Prohaska and Walker ([62]). In fact they proved a characterisation result on a particular type of spread of $\mathrm{PG}(3, q)$. Since a spread of $\mathrm{PG}(3, q)$ is equivalent to an ovoid of $W(q)$ under a self-duality of $W(q)$ (see [56, 3.2.1] for details of the self-duality), the Prohaska-Walker result may be interpreted as a result on ovoids of $\mathrm{PG}(3, q)$. In particular that if a bundle of an ovoid consists entirely of conics then the ovoid is an elliptic quadric.

The pencil results was proved by Glynn ([20]) in 1984. In this technical paper Glynn performed calculations in an alternative representation of the GQ $W(q)$ to prove results on the automorphism group of an ovoid, related to the Hering classification of inversive planes. As a consequence he was able to prove both the bundle and pencil results.

The flock result was proved by Brown, O'Keefe and Penttila ([7]) in 1999. They considered an ovoid of $W(q)$ with a flock of conics and using the isomorphism betweeen the GQ $W(q)$ and the GQ $Q(4, q)$ considered the equivalent problem in $Q(4, q)$. They employed some elementary quadric geometry to establish the result.

### 3.3.2 Generation 2: The plane equivalent theorem

The second generation of results had its birth in the consideration of the relationship between two secant plane sections of an ovoid that share a tangent. If one of the pair of ovals is known, then we will see that this immediately places geometrical conditions on the second oval.

Recall that an ovoid $\Omega$ of $\mathrm{PG}(3, q)$, $q$ even, defines a symplectic polarity of $\mathrm{PG}(3, q)$. A tangent plane to $\Omega$ is mapped to the point of tangency, and conversely. A secant plane $\pi$ is mapped to the nucleus of the oval $\pi \cap \Omega$, and conversely. The polarity maps a secant line to an external line; an external line to a secant line; and fixes each tangent. So now let $\pi_1$ and $\pi_2$ be secant planes of $\mathcal{O}$ and let $\pi_1 \cap \Omega = \mathcal{O}_1$ and $\pi_2 \cap \Omega = \mathcal{O}_2$ have nuclei $N_1$ and $N_2$, respectively. Suppose further that $\pi_1 \cap \pi_2 = \ell$ is a tangent to $\Omega$ at $P$. It follows that $N_1, N_2 \in \ell$. Consider a line $m$ of $\pi_1$ that is incident with $N_2$ and secant to $\mathcal{O}_1$. The line $m^\perp$ is external to $\Omega$ and also $N_1 \in m^\perp$ and $m^\perp$ is contained in the plane $\pi_2$. In other words, $\perp$ interchanges the set of lines of $N_2$ secant to $\mathcal{O}_1$ with the set of lines in $\pi_2$ incident with $N_1$ and external to $\mathcal{O}_2$. Thus if we know the oval $\mathcal{O}_1$ it immediately places conditions on the form of the oval $\mathcal{O}_2$. The question is how can we make use of this observation?

Penttila and Praeger [61] considered this in the context of translation ovals. A *translation oval* is an oval projectively equivalent to an oval of the form

$$\mathcal{O}(\alpha) = \{(1, t, t^{\alpha}) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\},$$

where $\alpha$ is a generator of $\mathrm{Aut}(\mathrm{GF}(q))$. Note that $\mathcal{O}(\alpha)$ completes to the translation hyperoval $\mathcal{D}(\alpha)$ (see Section 2.3.1). The axis $x_0 = 0$ of $\mathcal{D}(\alpha)$ is also called an *axis* of $\mathcal{O}(\alpha)$ since the group of elations with axis $x_0 = 0$ fixing $\mathcal{D}(\alpha)$ also fixes $\mathcal{O}(\alpha)$. A conic is a translation oval for which every tangent is an axis. For any other translation oval there is a unique axis.

Recalling our earlier discussion of ovals $\mathcal{O}_1, \mathcal{O}_2 \subset \Omega$ sharing a common tangent, Penttila and Praeger considered the case in which $\mathcal{O}_1, \mathcal{O}_2$ are both translation ovals. By cleverly choosing a special homography $T$ of $\mathrm{PG}(3, q)$ that mapped $\pi_2$ to $\pi_1$ they considered two ovals in the plane $\pi_1$. Further $T$ has the properties that $T(\mathcal{O}_2) \cap \mathcal{O}_1 = \{P\}$, $\ell$ is tangent to both ovals and there is a special point $Q$ on $\ell$ such that the external lines to $\mathcal{O}_1$ on $Q$ are *also* external to $T(\mathcal{O}_2)$. This fact relies on both the relationship between $\mathcal{O}_1$ and $\mathcal{O}_2$ discussed earlier and the map $T$. Now that the two ovals are in the same plane use can be made of their special relationship. In particular Penttila and Praeger proved that if $\ell$ is an axis of $\mathcal{O}_1$, then $\ell$ is also an axis of $T(\mathcal{O}_2)$ (the so called external lines lemma). Thus if an ovoid has a pencil of translation ovals with the common tangent being an axis of *one* of the ovals, then it must be an axis of *all* of the ovals in the pencil. Given these much stronger conditions on the elements of the pencil Penttila and Praeger were able to perform calculations to show that the ovoid must be known.

**Theorem 3.14 (Penttila and Praeger [61]).** *Supose that $\Omega$ is an ovoid of $\mathrm{PG}(3, q)$, where $q$ is even, and that $\pi$ is a secant plane such that $\pi \cap \Omega$ is a translation oval. Let $\ell$ be an axis of $\pi \cap \Omega$. Suppose that each secant plane to $\mathcal{O}$ on $\ell$ meets $\Omega$ in a translation oval. Then $\Omega$ is either an elliptic quadric or a Tits ovoid.*

This is the first strong result that characterises *both* the known ovoids and is critical for much of the work on ovoids that has followed it.

In the work of Penttila and Praeger the homography $T$ of $\mathrm{PG}(3, q)$ and the external lines lemma were particular to the translation ovals assumed to be sections of an ovoid. However the idea of the special homography $T$ can be extended.

Consider $\mathcal{O}_1, \mathcal{O}_2 \subset \Omega$ as previously. Let $n$ be a line of $W(q)$ containing $P$ and distinct from $\ell$. Let $T$ be the homography fixing $W(q)$ (commuting with the polarity), fixing $n$ pointwise, fixing each line of $W(q)$ meeting $n$, fixing no point of $W(q)$ *off* $n$, and finally mapping $\pi_2$ to $\pi_1$. (We shall postpone the discussion of the existence of such a homography). Each line of $W(q)$ meeting $n$ contains a unique point of $\Omega$. Since $T$ fixes each line of $W(q)$ meeting $n$, but no point off $n$ it follows that $T(\Omega) \cap \Omega = \{P\}$. Hence $T(\mathcal{O}_2)$ is an oval of $\pi_1$ such that $T(\mathcal{O}_2) \cap \mathcal{O}_1 = \{P\}$. Also since $T$ commutes with $\perp$ the nucleus of $T(\mathcal{O}_2)$ is $N_1$. Now consider a line $m \subset \pi_2$, with $N_1 \in m$ and $m \neq \ell$. Let $X$ be any point of $m \setminus \{N_1\}$ and $Y = X^{\perp} \cap n$. Then $\langle X, Y \rangle$ is the unique line of $W(q)$ on $X$ concurrent with $n$. Since $\langle X, Y \rangle$ is fixed by $T$ it must be that $T(m) = T(\langle N_1, X \rangle) = \langle N_2, Z \rangle$ where $Z = \langle X, Y \rangle \cap \pi_1$. On the other hand $m^{\perp} = \langle N_1, X \rangle^{\perp} = \pi_1 \cap X^{\perp}$. Since $\{Z, N_2\} \subset \pi_1 \cap X^{\perp}$ and $Z \neq N_2$ we have

$m^\perp = \langle Z, N_2 \rangle = T(m)$. This is a key property for the following reason. Consider a line $m$ on $N_1$ secant to the oval $\mathcal{O}_2$. We saw previously that $m^\perp$ is a line containing $N_2$ and external to the oval $\mathcal{O}_1$. Hence the homography $T$ maps the lines on $N_1$ secant to $\mathcal{O}_2$ onto the lines on $N_2$ secant to $T(\mathcal{O}_2)$ and also onto the lines on $N_2$ external to $\mathcal{O}_1$. That is, the lines on $N_2$ secant to $T(\mathcal{O}_2)$ are external to $\mathcal{O}_1$ and vice versa. This property of two ovals in a plane is called compatability.

**Definition 3.15.** *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be ovals of $\mathrm{PG}(2,q)$, and let $Q$ be a point of $\mathrm{PG}(2,q)$ not on either of the ovals and distinct from their nuclei. Then $\mathcal{O}_1$ and $\mathcal{O}_2$ are* compatible *at $Q$ if they have the same nucleus, they have a point $P$ in common, the line $\langle P, Q \rangle$ is a tangent line to each oval and every secant line to $\mathcal{O}_1$ on $Q$ is external to $\mathcal{O}_2$.*

As for the existence of the homography $T$, there are a number of ways to establish this. One possibility is to apply coordinates to the geometry and explicity write down the required matrix. In GQ terms each line of $W(q)$ is an axis of symmetry and $T$ is the symmetry of $W(q)$ with axis $n$ mapping $\pi_2$ to $\pi_1$ (see [56] for the relevant definitions and results). Perhaps the nicest method is to consider the dual $W(q)$. Letting $\wedge$ denote duality, any elation of $\mathrm{PG}(3,q)$ with centres $n^\wedge$ and axis $(n^\wedge)^\perp$ has all the desired properties except (perhaps) mapping $\pi_2$ to $\pi_1$. In $W(q)^\wedge$ the plane $\pi_1$, as a set of lines on $N_1$, is represented as the set of points on a line incident with $\ell^\wedge$ (distinct from $P^\wedge$), and similarly for $\pi_2$. Thus we know that there will be an elation with the desired properties.

The last two descriptions of $T$ are suggestive in the sense that they display a group of order $q$, fixing $P^\perp$ and acting regularly on the other planes about $\ell$. We can use the elements of this group to map each of the ovals arising from the intersection of $\Omega$ with a plane about $\ell$ onto a *fixed* plane on $\ell$. This gives a set of $q$ ovals in the plane. The plane equivalent theorem specifies the compatability between the ovals in this set and also states that we may construct an ovoid from such a set.

**Theorem 3.16 (The Plane Equivalent Theorem, [22] and [57] independently).** *An ovoid of $\mathrm{PG}(3,q)$, $q$ even, is equivalent to a set of $q$ ovals $\mathcal{O}_s$, for $s \in \mathrm{GF}(q)$, of $\mathrm{PG}(2,q)$ all with nucleus $(0,1,0)$, satisfying $\mathcal{O}_s \cap \mathcal{O}_t = \{(0,0,1)\}$ for all $s \neq t$ in $\mathrm{GF}(q)$, and such that $\mathcal{O}_s$ and $\mathcal{O}_t$ are compatible at $P_{s+t} = (0,1,s+t)$. Moreover, each pencil of the ovoid $\Omega$ gives rise to such a set, and for each plane section $\pi \cap \Omega$ of the pencil there is a parameterization of the planes $\pi_s$, $s \in \mathrm{GF}(q)$, of the pencil such that $\pi_0 = \pi$ and there is a homography $M_s : \pi_s \to \pi$ taking $\pi_s \cap \Omega$ and the tangent line of the pencil to the common tangent $[1,0,0]$.*

The set of $q$ ovals in the plane equivalent theorem is called a *fan*.

Penttila proved the result using the group discussed. Glynn used a different representation of the GQ $W(q)$ to deduce five distinct representations of ovoids of $\mathrm{PG}(3,q)$ one of which was the plane equivalent theorem.

This result is a powerful tool in proving that many sets of ovals cannot be a pencil of an ovoid. For instance if two ovals are not compatible at a point, then they cannot be in a pencil of an ovoid. Also if $\mathcal{O}$ is an oval contained in an ovoid $\Omega$, then for each tangent $\ell$ to $\mathcal{O}$ we can construct a fan, as in the plane equivalent theorem. Thus for each point

$Q \in \ell$, where $Q$ is not in $\mathcal{O}$ and distinct from the nucleus of $\mathcal{O}$, there must be another oval compatible with $\mathcal{O}$ at $Q$. Hence if an oval $\mathcal{O}$ has *any* point, not in $\mathcal{O}$ and distinct its nucleus, where there is no compatible oval, then $\mathcal{O}$ cannot be contained in an ovoid. Of course the plane equivalent theorem is far more subtle than this application since it refers to ovals *parameterized* and with the point of compatability of two ovals being a point with specified coordinates.

Clearly the consideration of the matching ovals is of great importance in the use of the plane equivalent theorem in classifying/characterising ovoids. We now give concepts and definitions which help with these considerations. These idea were developed by O'Keefe and Penttila in [41, 43, 44]. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be ovals and $P_1$ and $P_2$ be points of $\mathrm{PG}(2,q)$, where $P_1$ is distinct from the points of $\mathcal{O}_1$ and its nucleus and similarly $P_2$ is distinct from the points of $\mathcal{O}_2$ and its nucleus. We say that $(P_1, \mathcal{O}_1)$ *matches* with $(P_2, \mathcal{O}_2)$ if there is a collineation $g$ such that $g(P_1) = P_2$ and $g(\mathcal{O}_1)$ and $\mathcal{O}_2$ are compatible at $P_2$. This definition allows the consideration of matching between two ovals in canonical form rather than compatability for all of the different pairs of ovals.

Next we consider the configuration of a point $P$ not on an oval $\mathcal{O}$ and the three types of lines on $P$; the tangents, secants and external lines of $\mathcal{O}$. The quotient space $\mathrm{PG}(2,q)/P$ is isomorphic to $\mathrm{PG}(1,q)$ so we may give the lines through $P$ parameters from $\mathrm{GF}(q) \cup \{\infty\}$. The set of lines through $P$ consists of 1 tangent, $q/2$ secants and $q/2$ external lines to $\mathcal{O}$. Correspondingly there will be 1 parameter from $\mathrm{GF}(q) \cup \{\infty\}$ for the tangent, $q/2$ to the secants and $q/2$ to the external lines. The set of $q/2$ elements corresponding to the secants is called *the local secant parameter set* of $(P, \mathcal{O})$ and similarly the set of $q/2$ elements corresponding to the external lines is *the local external paramter set* of $(P, \mathcal{O})$.

To make greater use of this observation O'Keefe and Penttila made the following definition. Let $(P, \mathcal{O})$ be a point-oval pair with $P$ not in $\mathcal{O}$ and distinct from its nucleus. Let $G$ be the group induced on the lines through $P$ by $\mathrm{P\Gamma L}(3,q)$, then $G \cong \mathrm{P\Gamma L}(3,q)$. If $H < G$, then the *local stabiliser of* $(P, \mathcal{O})$ *in* $H$ is the subgroup of $H$ fixing the configuration of tangent, external and secant lines to $\mathcal{O}$ on $P$. Note that $\mathcal{O}$ need not be stabilised. The tangent to $\mathcal{O}$ on $P$ *is* fixed and so if we associate with this tangent the parameter $\infty$, then the local stabiliser of $(P, \mathcal{O})$ in $H$ is identified with a subgroup of $\mathrm{A\Gamma L}(1,q)$.

**Lemma 3.17 (O'Keefe and Penttila [41]).** *Suppose that* $(P_1, \mathcal{O}_1)$ *matches with* $(P_2, \mathcal{O}_2)$ *for points* $P_1$ *and* $P_2$ *and ovals* $\mathcal{O}_1$ *and* $\mathcal{O}_2$ *of* $\mathrm{PG}(2,q)$*,* $q$ *even. Then the local stabiliser* $H_1$ *of* $(P_1, \mathcal{O}_1)$ *in* $H$ *is conjugate in* $\mathrm{A\Gamma L}(1,q)$ *to the local stabiliser* $H_2$ *of* $(P_2, \mathcal{O}_2)$ *in* $H$*, for* $H = \mathrm{A\Gamma L}(1,q)$*,* $\mathrm{AGL}(1,q)$ *and* $T$*, where* $T$ *is the group of all translations* $x \mapsto x + b$ *for some* $b \in \mathrm{GF}(q)$*.*

This gives an effective way for establishing that two point-oval pairs do *not* match. Equipped with the above tools we now review a series of classification and characterisation results about ovoids. In all of them the general theme is to eliminate possible oval pairs in a fan until the only possibilities remaining are included in Theorem 3.14, the characterisation theorem of Penttila and Praeger.

**Theorem 3.18 (O'Keefe and Penttila [37, 41]).** *Every ovoid of* $\mathrm{PG}(3,16)$ *is an elliptic quadric.*

O'Keefe and Penttila gave two proofs of this result in separate papers. The first appearing in [37] used extensive computer searches and also relied on Hall's computer assisted classification of the hyperovals of $\mathrm{PG}(2,16)$ ([23]). Subsequent to the publication of the first paper O'Keefe and Penttila produced a hand classification of the hyperovals of $\mathrm{PG}(2,16)$ ([39]) and so a non-computer aided classification of the ovoids of $\mathrm{PG}(3,16)$ was possible.

The only hyperovals in $\mathrm{PG}(2,16)$ are the Lunelli-Sce (Subiaco) hyperoval and the regular hyperoval. This results in three ovals the conic, the $\mathcal{O}(1/2)$ translation oval contained in the regular hyperoval and one oval from the Lunelli-Sce hyperoval. So let $\mathcal{L}$ represent a particular (canonical) Lunelli-Sce oval. In the second paper [41] O'Keefe and Penttila considered matchings with the pair $(P,\mathcal{L})$ for some point $P$. It was not necessary to consider all possible points $P$, only one representative of each orbit of the group of $\mathcal{L}$ on the points off $\mathcal{L}$ and distinct from its nucleus. (Note that this is true in general for any oval in $\mathrm{PG}(2,q)$.) By calculating the local stabiliser of these pairs and eliminating possible matching and applying Lemma 3.17 O'Keefe and Penttila showed that a fan cannot contain a Lunelli-Sce oval. The only other ovals are translation ovals. If an oval is contained in an ovoid, then we may construct a fan on each tangent to the oval. Hence if an ovoid contains all translation ovals, then there will be a fan of the type in Theorem 3.14 and the ovoid is known.

**Theorem 3.19 (O'Keefe, Penttila and Royle [46]).** *Ovoids in* $\mathrm{PG}(3,32)$ *are elliptic quadrics or Tits ovoids.*

**Sketch Proof.** The classification of hyperovals in $\mathrm{PG}(2,32)$ ([59]) revealed that there are 35 ovals in $\mathrm{PG}(2,32)$. Using extensive computer work O'Keefe, Penttila and Royle took a canonical version of each of the 35 ovals, looked at point-oval pairs, for these ovals, and calulated the local secant parameter sets. Of the 35 ovals 32 have a point at which the oval matched with no other oval and so cannot be contained in an ovoid. The remaining ovals were the conic and two translation ovals. So as in the $q=16$ case Theorem 3.14 applies and the result follows. $*\square$

The next two results are based on the same techniques but are considerably more complicated and involve more finesse in the application of matching so we shall just quote the theorems.

**Theorem 3.20 (O'Keefe and Penttila [43]).** *Let* $\Omega$ *be an ovoid of* $\mathrm{PG}(3,q)$ *where* $q>2$ *is even. Then* $\Omega$ *has a pencil of translation ovals if and only if* $\Omega$ *is either an elliptic quadric or a Tits ovoid.*

Recall that in Theorem 3.14 that this result was proved with the extra hypothesis that the common tangent of the pencil was an axis of at least one of the translation ovals. O'Keefe and Penttila proved the remaining case where the common tangent is an axis of none of the ovals.

**Theorem 3.21 (O'Keefe and Penttila [44]).** *Let* $\Omega$ *be an ovoid of* $\mathrm{PG}(3,q)$*,* $q$ *even. If each plane section of* $\Omega$ *is an oval contained in a translation hyperoval, then* $\Omega$ *is either an elliptic quadric or a Tits ovoid.*

The above results perhaps mark the end of the road for these techniques. In terms of classification results for ovoids, a classification result for ovals was first required and in the $PG(3, 32)$ case computer searching. There is (as yet) no classification of ovals in $PG(2, 64)$ and the size of the problem makes it unlikely a computer proof will be available soon. Even given such a classification the matching calculations would probably be a prohibitively large problem.

In terms of characterisation results given the technical nature of the proof of Theorem 3.21 it seems difficult to strengthen the hypotheses using the same techniques. Nevertheless the development of the plane equivalent theorem and related methods reinvigorated the study of ovoids and provided many significant results.

### 3.3.3 The Next Generation: GQs and hypotheses on one secant plane

We now look at two recent theorems due to Brown [5, 6] that characterise ovoids by a *single* oval section. In particular we shall see that if an ovoid contains a conic then it must be an elliptic quadric. This is the first characterisation of one of the known ovoids by a single oval section. We shall also see that if an ovoid contains a $\mathcal{O}(1/2)$ oval (contained in the regular hyperoval), then $q = 4$ and the ovoid is an elliptic quadric or $q = 8$ and it is a Tits ovoid. For $q > 8$ the oval $\mathcal{O}(1/2)$ cannot be contained in an ovoid. This is the first general result of this type (we saw in the classification of ovoids for $q = 16$ and 32 that some ovals cannot be contained in an ovoid).

We saw in the previous section that the techniques employed there would only be extended with considerable difficulty. The single oval section hypothesis requires a different approach. We now give some preliminaries to this approach.

**The GQ $T_2(\mathcal{O})$ of Tits and ovoids of $PG(3, q)$**

Let $\mathcal{O}$ be an oval of $PG(2, q)$ (for the moment $q$ may be odd). Embed $PG(2, q)$ in $PG(3, q)$ and define $T_2(\mathcal{O})$ to be the following incidence structure. The *points* are: (i) the points of $PG(3, q) \setminus PG(2, q)$, called the *affine* points, (ii) the planes of $PG(3, q)$ which meet $PG(2, q)$ in a single point of $\mathcal{O}$ and (iii) a symbol $(\infty)$. The *lines* are: (a) the lines of $PG(3, q)$, not in $PG(2, q)$, which meet $PG(2, q)$ in a single point of $\mathcal{O}$ and (b) the points of $\mathcal{O}$. *Incidence* is as follows: a point of type (i) is incident only with the lines of type (a) which contain it, a point of type (ii) is incident with all lines of type (a) contained in it and with the unique line of type (b) on it and the point of type (iii) is incident with no line of type (a) and with all lines of type (b).

The incidence structure $T_2(\mathcal{O})$ is a GQ of order $(q, q)$. These GQs were first constructed by Tits (see [15]). By [56, 3.2.2] $T_2(\mathcal{O})$ is isomorphic to $Q(4, q)$ if and only if $\mathcal{O}$ is a conic; and it is isomorphic to $W(q)$ if and only if $q$ is even and $\mathcal{O}$ is a conic. So $T_2(\mathcal{O})$ is classical if and only if $\mathcal{O}$ is a conic.

An ovoid of $T_2(\mathcal{O})$ is a set of points such that each line of $T_2(\mathcal{O})$ is incident with exactly one element of the set. Equivalently an ovoid can be thought of as a set of $q^2 + 1$ points no two collinear.

Let $\Omega$ be an ovoid of $PG(3, q)$ and let $\pi$ be a secant plane of $\Omega$ with $\pi \cap \Omega = \mathcal{O}$. If we construct the GQ $T_2(\mathcal{O})$ from $PG(3, q)$, $\pi$ and $\mathcal{O}$ the set $\Omega \setminus \mathcal{O}$ is a set of $q^2 - q$ (affine) points of $T_2(\mathcal{O})$ no two collinear. The points are non-collinear because to be collinear two affine points of $T_2(\mathcal{O})$ must span a projective line that contains a point of $\mathcal{O}$, however this would be a line of $\mathrm{PG}(3,q)$ containing three points of $\Omega$. If to this set we add the $q+1$ tangent planes to $\Omega$ at a point of $\mathcal{O}$, then the resulting set is an ovoid of $T_2(\mathcal{O})$. This gives us the following result.

**Lemma 3.22.** *Let $\Omega$ be an ovoid of $\mathrm{PG}(3,q)$ and $\pi$ a secant plane of $\Omega$ such that $\pi \cap \Omega = \mathcal{O}$. The set*

$$\overline{\Omega} = (\Omega \setminus \mathcal{O}) \cup \{\pi_P : \pi_P \textit{ is the tangent plane to } \Omega \textit{ at } P \in \mathcal{O}\}$$

*is an ovoid of $T_2(\mathcal{O})$.*

Such an ovoid is called a *projective ovoid* of $T_2(\mathcal{O})$. This result is probably "folklore", although most noticably arises in the subquadrangles $T_2(\mathcal{O})$ of the GQ $T_2(\Omega)$ (see [56, 3.1.2 and 2.2.1]).

**Ovoids of $\mathrm{PG}(3,q)$, $q$ even, containing a conic**

The above discussion applies equally for $q$ odd and even, but from this point we shall specialise to the case where $q$ is even and the oval $\mathcal{O}$ in $\Omega$ is a conic $\mathcal{C}$.

By Lemma 3.22 from $\Omega$ we can construct an ovoid $\overline{\Omega}$ of the GQ $T_2(\mathcal{C})$. We noted above that the GQ $T_2(\mathcal{C})$ is isomorphic to the GQ $W(q)$ for $q$ even, so let $\phi$ be an isomorphism from $T_2(\mathcal{C})$ to $W(q)$. Then $\phi(\overline{\Omega})$ is an ovoid of $W(q)$ and by the result of Thas ([72]) also an ovoid of $\mathrm{PG}(3,q)$. Further the ovoid $\phi(\overline{\Omega})$ also contains a conic. So by this process we start with an ovoid $\Omega$ containing a conic and end up with an ovoid $\phi(\overline{\Omega})$ containing a conic. The important point of this is that going from $\Omega$ to $\phi(\overline{\Omega})$ in this way does *not* induce a collineation of $\mathrm{PG}(3,q)$. Thus the fact that $\phi(\overline{\Omega})$ is an ovoid must place strong conditions on the ovoid $\Omega$. To make this point clearer we will use coordinates and make the setting explicit.

We may assume that the symplectic polarity of $\mathrm{PG}(3,q)$ defined by $\Omega$ has form $x_0y_1 + x_1y_0 + x_2y_3 + x_3y_2 = 0$. We may also assume that the plane $\pi$ has equation $x_3 = 0$ and that the conic $\mathcal{C}$ has equation $x_3 = x_0x_1 + x_2^2 = 0$, that is, $\mathcal{C} = \{(1,t^2,t,0) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0,0)\}$ and has nucleus $N = (0,0,1,0)$ (see [7] and [28, Theorem 22.6.6] to justify this normalisation). By Lemma 3.22 we have that

$$\overline{\Omega} = (\Omega \setminus \mathcal{C})) \cup \{[t^2,1,0,t] : t \in \mathrm{GF}(q)\} \cup \{[1,0,0,0]\}$$

is an ovoid of $T_2(\mathcal{C})$.

We now specify the isomorphism $\phi$ from $T_2(\mathcal{C})$ to $W(q)$ in the following lemma.

**Lemma 3.23 (see [5]).** *Let $\pi$ be the plane of $\mathrm{PG}(3,q)$, $q$ even, defined by the equation $x_3 = 0$. Let $\mathcal{C}$ be the conic in $\pi$ defined by the equations $x_3 = x_0x_1 + x_2^2 = 0$, that is*

$$\mathcal{C} = \{(1,t^2,t,0) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0,0)\}$$

*with nucleus $N = (0,0,1,0)$. Construct $T_2(\mathcal{C})$ from $\Sigma$, $\pi$ and $\mathcal{C}$ in the usual manner. Let $W(q)$ be the GQ defined as the singular points and lines of the symplectic polarity of $\mathrm{PG}(3,q)$ with form $x_0y_1+x_1y_0+x_2y_3+x_3y_2 = 0$. Then there exists an isomorphism*

*$\phi$ from $T_2(\mathcal{C})$ to $W(q)$ that acts on the points of $T_2(\mathcal{C})$ by:*

$$\begin{aligned}(x_0, x_1, x_2, 1) &\mapsto (x_0, x_1, x_0x_1 + x_2^2, 1), \ \textit{for } x_0, x_1, x_2 \in \mathrm{GF}(q),\\ [t, 1, 0, s] &\mapsto (1, t, s, 0), \ \textit{for } s, t \in \mathrm{GF}(q).\\ [1, 0, 0, s] &\mapsto (0, 1, s, 0), \ \textit{for } s \in \mathrm{GF}(q),\\ (\infty) &\mapsto (0, 0, 1, 0).\end{aligned}$$

It is reasonably straight-forward to derive this isomorphism by applying coordinates to the proof of [56, 3.2.1].

If we consider $T_2(\mathcal{C})$ and $W(q)$ in the same $\mathrm{PG}(3, q)$, then we see that the ovoid $\phi(\overline{\Omega})$ contains the conic $\mathcal{C}$. Also $\phi$ induces a *quadratic* map on the points of $\mathrm{AG}(3, q) = \mathrm{PG}(3, q) \setminus \pi$, in particular $\phi$ does not induce an automorphism of $\mathrm{AG}(3, q)$. Prima facie there is no reason to assume that $\Omega$ and $\phi(\overline{\Omega})$ are projectively equivalent.

Since the map $\phi$ changes only the $x_2$ coordinate it will fix, as a set of points, the affine part of any plane on the point $(0, 0, 1, 0)$. We now consider the action of $\phi$ in such a plane. To make the situation a little more specific we look at the plane $\pi' : x_1 = x_3$ meeting $\pi$ in the line $\langle(0, 0, 1, 0), (1, 0, 0, 0)\rangle$. The tangent plane to both $\Omega$ and $\phi(\overline{\Omega})$ at the point $(1, 0, 0, 0)$ is $[0, 1, 0, 0]$ (given by the polarity of the ovoids) and so $\pi'$ is a secant plane of both $\Omega$ and $\phi(\overline{\Omega})$. Let $\mathcal{O}_1 = \pi' \cap \Omega$ and $\mathcal{O}_2 = \pi' \cap \phi(\overline{\Omega})$, then $\mathcal{O}_1$ and $\mathcal{O}_2$ share the point $(1, 0, 0, 0)$ and the nucleus $(1, 0, 1, 0)$. Since $\phi$ fixes the affine part of $\pi'$, that is $\pi' \setminus \langle(1, 0, 0, 0), (0, 0, 1, 0)\rangle$, we also have that

$$\phi(\mathcal{O}_1 \setminus \{(1, 0, 0, 0)\}) = \mathcal{O}_2 \setminus \{(1, 0, 0, 0)\},$$

where $\phi$ acts on the affine part of $\pi'$ by

$$(x_0, 1, x_2, 1) \mapsto (x_0, 1, x_0 + x_2^2, 1).$$

Since this map is quadratic in nature it places conditions on both ovals $\mathcal{O}_1$ and $\mathcal{O}_2$.

By representing the ovals using o-polynomials (and omitting the details) we find that $\mathcal{O}_1$ is projectively equivalent to an oval $\{(1, t, f(t)) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\}$ and $\mathcal{O}_2$ to an oval $\{(1, g(t), t) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 1)\}$ where $f, g$ are o-polynomials and

$$g(x) = f(x^{1/2}) + A(x^{1/2} + x); \quad A \in \mathrm{GF}(q) \setminus \{0\} \tag{2}$$

This equation arises because of the quadratic nature of the map $\phi$.

So to find the possibilities for the oval $\mathcal{O}_1 \subset \Omega$ we need to solve the equation (2). The (hopefully) obvious solution is $A = 1$, $f(x) = x^2$, $g(x) = x^{1/2}$. Are there any others?

**Lemma 3.24 (Brown [5]).** *The only solution to*

$$g(x) = f(x^{1/2}) + A(x^{1/2} + x)$$

*for o-polynomials $f$ and $g$ and $A \in \mathrm{GF}(q) \setminus \{0\}$ is $A = 1$, $f(x) = x^2$, $g(x) = x^{1/2}$.*

The proof is hard work. Inductive use of Glynn's theorem (Theorem 2.10) reduces the number of possibly non-zero coefficients of $f$ and $g$ until we are left with the unique solution.

**Corollary 3.25.** *Let $\Omega$ be an ovoid of* $\mathrm{PG}(3,q)$*, $q$ even, and $\pi$ a plane of* $\mathrm{PG}(3,q)$ *such that $\pi \cap \Omega$ is a conic. Then $\Omega$ is an elliptic quadric.*

**Sketch Proof.** By Lemma 3.24 and the discussion preceding it we have that $\pi' \cap \Omega$ is a conic. If we perform this calculation more generally we have the result that any oval section of $\Omega$ sharing a tangent with $\mathcal{C}$ is also a conic. Suppose that $\pi''$ is a secant plane of $\Omega$ such that $\pi'' \cap \Omega = \mathcal{O}''$ does not share a tangent with $\mathcal{C}$. Let $P$ be a point of $\pi'' \cap \pi$ not on $\Omega$, $\ell$ the tangent to $\mathcal{C}$ on $P$ and $\ell''$ the tangent to $\mathcal{O}''$ on $P$. The lines $\ell, \ell''$ span a plane $\pi'''$ and since $\pi'''$ contains two points of $\Omega$ it is a secant plane with $\mathcal{O}''' = \pi''' \cap \Omega$. Now $\mathcal{O}'''$ shares a tangent, $\ell$, with $\mathcal{C}$ and so is a conic. The oval $\mathcal{O}''$ shares a tangent, $\ell''$, with $\mathcal{O}'''$, a conic, and so is also a conic. Hence every oval contained in $\Omega$ is a conic, and so by Theorem 3.7 of Barlotti $\Omega$ is an elliptic quadric. $*\square$

**Ovoids of $\mathrm{PG}(3,q)$ containing a pointed conic**

Pointed conic is a term used for the oval

$$\mathcal{O}(1/2) = \{(1, t, t^{1/2}) \,:\, t \in \mathrm{GF}(q)\} \cup \{(0,0,1)\}.$$

By using ideas similar to those in the conic in an ovoid case, as well as by using GQ theory on the GQ $T_2(\mathcal{O}(1/2))$ and plane geometry Brown ([6]) was able to prove the following theorem.

**Theorem 3.26 (Brown [6]).** *Suppose that $\Omega$ is an ovoid of* $\mathrm{PG}(3,q)$ *where $q > 2$ is even and that $\pi_\infty$ is a secant plane such that $\pi_\infty \cap \Omega$ is a pointed conic. Then either $q = 4$ and $\Omega$ is an elliptic quadric or $q = 8$ and $\Omega$ is a Tits ovoid.*

The proof of this result is a little beyond the scope of these notes so we shall simply encourage the reader to study [6] (when it appears in print).

The significance of this result is that it is the first general result stating that a particular oval may not be contained in an ovoid.

The aim of the part of the notes on ovoids has been to give a historical survey with an emphasis on the most significant geometrical results on ovoids and techniques used to prove them. There are many other “angles” that may be taken on ovoids including group theoretic, coding theoretic and polynomial approaches, not to mention the many geometrical constructions that make use of ovoids. The reader is encouraged to go out and enjoy these.

## References


[1] A. Barlotti, 'Un'estensione del teorema di Segre-Kustaanheimo', *Boll. Un. Mat. Ital.* 10 (1955) 96–98.

[2] A. Barlotti, *Some topics in finite geometrical structures*, Institute of Statistics Mimeo Series No. 439, University of North Carolina, 1965.

[3] D. Betten, '4-dimensionale Translationsebenen mit 8-dimensionaler Kollineationsgruppe', *Geom. Dedicata* 2 (1973) 327–339.

[4] R.C. Bose, 'Mathematical theory of the symmetrical factorial design', *Sankhya* 8 (1947) 107–166.

[5] M.R. Brown, 'Ovoids of $PG(3, q)$, $q$ even, with a conic section', *J. London Math. Soc. (2)*, to appear.

[6] M.R. Brown, 'The determination of ovoids of $PG(3, q)$ containing a pointed conic', *J. Geom.*, to appear.

[7] M.R. Brown, C.M. O'Keefe and T. Penttila, 'Triads, Flocks of Conics and $Q^{-}(5, q)$', *Des. Codes Cryptogr.* 18 (1999) 63–70.

[8] F. Buekenhout, 'Existence of unitals in finite translation planes of order $q^2$ with a kernel of order $q$', *Geom. Dedicata* 5 (1976) 189–194.

[9] W. Cherowitzo, 'Bill Cherowitzo's Hyperoval Page', `http://www-math.cudenver.edu/~wcherowi/research/hyperoval/hypero.html`

[10] W. Cherowitzo, 'Hyperovals in Desarguesian planes of even order', *Ann. Discrete Math.* 37 (1988) 87–94.

[11] W. Cherowitzo, '$\alpha$-Flocks and Hyperovals', *Geom. Dedicata* 72 (1998), 221–246.

[12] W. Cherowitzo, T. Penttila, I. Pinneri, G.F. Royle, 'Flocks and ovals', *Geom. Dedicata* 60 (1996) 17–37.

[13] W. Cherowitzo and L. Storme, '$\alpha$-Flocks with Oval Herds and Monomial Hyperovals,' *Finite Fields and their Applications* 4 (1998) 185-199.

[14] W. Cherowitzo, C.M. O'Keefe and T. Penttila, 'A Unified Construction of Finite Geometries in Characteristic Two', *preprint.*

[15] P. Dembowski, *Finite geometries* (Springer Verlag, Berlin, 1968).

[16] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* Teubner, Leipzig, 1901.

[17] G. Fellegara, 'Gli ovaloidi di uno spazio tridimensionale di Galois di ordine 8, *Atti Accad. Naz. Lincei Rend.* 32 (1962) 170–176.

[18] J.C. Fisher and J.A. Thas, 'Flocks in PG$(3, q)$', *Math. Z.* 169 (1979) 1–11.

[19] D.G. Glynn, 'Two New Sequences of Ovals in Finite Desarguesian Planes of Even Order,' Combinatorial Mathematics X, edited by L.R.A. Casse, pp. 217-229 (Lecture Notes in Mathematics 1036, Springer, 1983).

[20] D.G. Glynn, 'The Hering classification of inversive planes of even order', *Simon Stevin* 58 (1984) 319–353.

[21] D.G. Glynn, 'A condition for the existence of ovals in PG$(2, q)$, $q$ even', *Geom. Dedicata* 32 (1989) 247–252.

[22] D.G. Glynn, Plane representations of ovoids, *Bull. Belg. Math. Soc. Simon Stevin* 5 (1998) 275–286.

[23] M. Hall, Jr., 'Ovals in the Desarguesian plane of order 16', *Ann. Mat. Pura App. (4)* 102 (1975) 159–176.

[24] M. Haring and W. Heise, 'On B. Segre's construction of an ovaloid', *Acta Arith.* 35 (1979) 187–188.

[25] J.W.P. Hirschfeld, 'Rational curves on quadrics over finite fields of characteristic two', *Rend. Mat. Appl.*, 34 (1971) 773–795.

[26] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Clarendon Press, Oxford, 1995.

[27] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1998.

[28] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Clarendon Press, Oxford, 1991.

[29] G. Jarnefelt and P. Kustaanheimo, 'An observation on finite geometries', *Comptes Rendus XI Congr. Math. Scand.*, Trondheim, 166–182.

[30] N.L. Johnson and S.E. Payne, 'Flocks of Laguerre planes and associated geometries' Mostly finite geometries (Iowa City, IA, 1996), 51–122, Lecture Notes in Pure and Appl. Math., 190.

[31] W.M. Kantor, 'Generalized Quadrangles Associated with $G_2(q)$', *J. Combin. Th. Ser. A* 29 (1980) 212–219.

[32] W.M. Kantor, 'Some generalized quadrangles with parameters $(q^2, q)$', *Math. Z.* 192 (1986) 45–50.

[33] G. Korchmaros, 'Gruppi di collineazioni transitivi sui punti di una ovale $[(q + 2)$-arco] di $S_{2,q}$, $q$ pari', *Atti Sem. Mat. Fis. Univ. Modena* 27 (1978) 89–105.

[34] H. Lüneburg, *Die Suzukigruppen und ihre Geometrien*, Springer Verlag, Lecture Notes in Math. no. 10 (1965).

[35] L. Lunelli and M. Sce, '$k$-archi completi nei piani proiettivi desarguesiani di rango 8 e 16', *Centro di Calcoli Numerici Politecnico di Milano*, (1958)

[36] C.M. O'Keefe, 'Ovoids in PG$(3, q)$: a survey', *Discrete Math.* (1–3) 151 (1996) 175–188.

[37] C.M. O'Keefe and T. Penttila, 'Ovoids of PG$(3, 16)$ are elliptic quadrics', *J. Geom* 38 (1990) 95–106.

[38] C.M. O'Keefe and T. Penttila, 'Polynomials for hyperovals of Desarguesian planes', *J. Austral. Math. Soc. (Series A)* 51 (1991) 436–447.

[39] C.M O'Keefe and T. Penttila, 'Hyperovals in PG(2,16)', *Eur. J. Combin.* 12 (1991) 51–59.

[40] C.M. O'Keefe and T. Penttila, 'A new hyperoval in PG(2,32),' *J. Geom.* 44 (1992) 117-139.

[41] C.M. O'Keefe and T. Penttila, 'Ovoids of PG$(3, 16)$ are elliptic quadrics, II', *J. Geom.* 44 (1992) 140–159.

[42] C.M. O'Keefe and T. Penttila, 'Symmetries of Arcs', *J. Combin. Theory Ser. A* 66 (1994), no. 1, 53–67.

[43] C.M. O'Keefe and T. Penttila, 'Ovoids with a Pencil of Translation Ovals', *Geom. Dedicata* 62 (1996) 19–34.

[44] C.M. O'Keefe and T. Penttila, 'Ovals in Translation Hyperovals and Ovoids', *European J. Combin.* 18 (1997) 667–683.

[45] C.M. O'Keefe, T. Penttila and C.E. Praeger, 'Stabilisers of hyperovals in PG(2,32)', in *Advances in Finite Geometries and Designs*, Oxford University Press, Oxford, 1991, pp. 337-357.

[46] C.M. O'Keefe, T. Penttila and G.F. Royle, 'Classification of ovoids in PG$(3, 32)$', *J. Geom.* 50 (1994) 143–150.

[47] C.M. O'Keefe and J.A. Thas, 'Collineations of Subiaco and Cherowitzo hyperovals', *Bull. Belg. Math. Soc. Simon Stevin*, 3 (1996), no. 2, 179-193.

[48] W.F. Orr, *The Miquelian inversive plane* IP$(q)$ *and the associated projective planes*, Ph.D. Thesis, Madison Wisc. 1973.

[49] G. Panella, 'Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito', *Boll. Un. Mat. Ital.* 10 (1955) 507–513.

[50] S.E. Payne, 'Symmetric representations of nondegenerate generalized $n$-gons', *Proc. Amer. Math. Soc.* 19 (1968) 1321–1326.

[51] S.E. Payne, 'A complete determination of translation ovoids in finite Desarguesian planes,' *Atti Accad. Naz. Lincei Rend. (8)* 51 (1971) 328-331.

[52] S.E. Payne, 'A new infinite family of generalized quadrangles', *Congr. Numer.* 49 (1985) 115–128.

[53] S.E. Payne, 'An essay on skew translation generalized quadrangles', *Geom. Dedicata* 32 (1989) 93–118.

[54] S.E. Payne and C.E. Maneri, 'A family of skew-translation generalized quadrangles of even order', *Congress. Numer.* 36 (1982) 127–135.

[55] S.E. Payne, I. Pinneri and T. Penttila, 'Isomorphisms between Subiaco $q$-clan geometries', *Bull. Belgian Math. Soc. Simon Stevin*, 2 (1995), no. 2, 197–222.

[56] S.E. Payne and J.A. Thas, *Finite Generalized Quadrangles*, Pitman, London, 1984.

[57] T. Penttila, A plane representation of ovoids, *Util. Math.*, 56 (1999), 245–250.

[58] T. Penttila and I. Pinneri, 'Irregular Hyperovals in PG(2,64)', *J. Geom.* 51 (1994) 89-100.

[59] T. Penttila and G.F. Royle, 'Classifications of hyperovals in $\mathrm{PG}(2,32)$', *J. Geom* 50 (1994), no. 1–2, 151–158.

[60] T. Penttila and G.F. Royle, 'On hyperovals in small projective planes', *J. Geom.* 54 (1995), no. 1-2, 91–104.

[61] T. Penttila and C.E. Praeger, 'Ovoids and translation ovals' *J. London Math. Soc. (2)* 56 (1997), no. 3, 607–624.

[62] O. Prohaska and M. Walker, 'A note on the Hering type of inversive planes of even order', *Arch. Math.* 28 (1977) 431–432.

[63] B. Qvist, 'Some remarks concerning curves of the second degree in a finite plane', *Ann. Acad. Sci. Fennicae. Ser. A* 1952, (1952) no. 134, 27pp.

[64] B. Segre and U. Bartocci, 'Ovali ed altre curve nei piani di Galois di caratteristica due', *Acta Arith.* 18 (1971) 423–449.

[65] B. Segre, 'Sulle ovali nei piani lineari finiti', *Atti. Accad. Naz. Lincei Rendic.* 17 (1954) 141–142.

[66] B. Segre, 'Ovals in finite projective plane', *Canad. J. Math.* 7 (1955) 414–416.

[67] B. Segre, 'Sui $k$-archi nei piani finiti di caratteristica due', *Rev. Math Pures Appl.* 2 (1957) 289–300.

[68] B. Segre 'On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two', *Acta Arith.* 5 (1959) 282–286.

[69] B. Segre, 'Ovali e curve $\sigma$ nei piani di Galois di caratteristica due', *Naz. Lincei Rend. Cl. Sci. Fis. Nat. Mat. (8)* 32, 785-790.

[70] E. Seiden, 'A theorem in finite projective geometry and an application to statistics', *Proc. Amer. Math. Soc.* 1 (1950) 282–286.

[71] M. Suzuki, 'On a class of doubly transitive groups', *Ann. of Math.* 75 (1962) 105–145.

[72] J.A. Thas, 'Ovoidal translation planes' *Arch. Math.* 23 (1972) 110–112.

[73] J.A. Thas, 'Flocks of finite egglike inversive planes', in: *Finite geometric structures and their applications* (ed. A. Barlotti), Ed. Cremonese Roma (1973) 189–191.

[74] J.A. Thas, 'Construction of maximal arcs and partial geometries', *Geom. Dedicata* 3 (1974) 61–64.

[75] J.A. Thas, 'Generalized Quadrangles and Flocks of Cones', *Europ. J. Combin.* 8 (1987) 441–452.

[76] J.A. Thas, 'Generalized Polygons' in *Handbook of Incidence Geometry, Buildings and Foundations*, (ed. F. Buekenhout), Chapter 9, North-Holland (1995), 383–431.

[77] J.A. Thas, 'Generalized quadrangles of order $(s, s^2)$, III', *J. Combin. Theory Ser. A* 87 (1999) 247–272.

[78] J.A. Thas, 'A result on spreads of the generalized quadrangle $T_2(\mathcal{O})$, with $\mathcal{O}$ an oval arising from a flock, and applications', *preprint*.

[79] J. Tits, 'Les groupes simples de Suzuki et de Ree', *Seminaire Bourbaki*, 3e année No. 210 (1960).

[80] J. Tits, 'Ovoïdes à translations', *Rendic. Mat.* 21 (1962) 37–59.

[81] J. Tits, 'Ovoïdes et groupes de Suzuki', *Arch. Math.* 13 187–198.

[82] J. Tits, 'Une propriété caracteristique des ovoïdes associés aux groupes de Suzuki', *Arch. Math.* 17 (1966) 136–153.

[83] M. Walker, 'A class of translation planes', *Geom. Dedicata* 5 (1976) 135–146.