OVALS IN DESARGUESIAN PLANES

Christine M. O'Keefe
Department of Mathematics
University of Western Australia
Nedlands, W.A. 6009
Australia

ABSTRACT

This paper surveys the known ovals in Desarguesian planes of even order, making use of the connection between ovals and hyperovals. First the known hyperovals are presented, and the inequivalent hyperovals in planes of small order are found. The ovals contained in each of the known hyperovals are determined and presented in a uniform way. Computer searches for new hyperovals are reported.

1. OVALS AND HYPEROVALS

Let $PG(2,q)$ be the Desarguesian projective plane over the field $GF(q)$ of order q, where q is a power of a prime p. An *oval* of $PG(2,q)$ is a set of $q+1$ points, no three of which are collinear. The points of a non-degenerate conic in $PG(2,q)$ form an oval. When q is odd, the converse is true, so that every $(q+1)$-arc is the set of points of a non-degenerate conic ([12; 5, 8.2.4]). When q is even, examples of non-conic ovals are known, and a complete classification of ovals has not yet been effected.

A line of $PG(2,q)$ meets an oval in either 2 points, 1 point or 0 points, in which case it is called a *secant*, a *tangent* or an *external line* respectively. When q is even, the set of tangents to an oval all pass through a common point. This point can be adjoined to the oval to give a set of $q+2$ points, no three collinear. Such a set is called a *hyperoval* and the unique point which is adjoined to an oval to obtain a hyperoval is called the *nucleus* of the oval. An account of ovals and hyperovals appears in Hirschfeld [5].

Given a hyperoval, an oval can be obtained by deleting one of the points of the hyperoval. This deleted point is the nucleus of the resulting oval. There are up to $q+2$ ovals which can be obtained from a hyperoval in this way, but we only distinguish those which are distinct under the action of the automorphism group $P\Gamma L(3,q)$ of $PG(2,q)$. Sets of points which are images of one another under elements of $P\Gamma L(3,q)$ are called *equivalent.*

1.1 Theorem Let $\mathcal{H}$ be a hyperoval in $PG(2,q)$, q even, and let G be the stabiliser of $\mathcal{H}$ in $P\Gamma L(3,q)$. The ovals obtained by deleting the points P and Q of $\mathcal{H}$ are equivalent if and only if P and Q lie in the same orbit of G on $\mathcal{H}$.

Proof: Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be ovals such that

$$\{P\} \cup \mathcal{O}_1 = \mathcal{H} = \{Q\} \cup \mathcal{O}_2.$$

First suppose that $\mathcal{O}_1$ and $\mathcal{O}_2$ are equivalent so that $\sigma(\mathcal{O}_1) = \mathcal{O}_2$ for some element $\sigma \in P\Gamma L(3,q)$. Since σ maps lines to lines, and P and Q are the intersections of the tangents of $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, $\sigma(P) = Q$. Thus

$$\sigma(\mathcal{H}) = \sigma(\{P\}) \cup \sigma(\mathcal{O}_1) = \{Q\} \cup \mathcal{O}_2 = \mathcal{H}$$

so $\sigma \in G$ and thus P and Q are in the same orbit of G on $\mathcal{H}$.

Conversely, suppose that P and Q are in the same orbit of G on $\mathcal{H}$. Then there exists an element $\sigma \in G$ such that $\sigma(P) = Q$. Since σ fixes $\mathcal{H}$, $\sigma(\mathcal{O}_1) = \mathcal{O}_2$ and the result follows.

Thus to study ovals when q is even, it is useful to first find hyperovals, then determine the possible ovals by finding the stabiliser of each hyperoval.

For the rest of the paper we suppose that q is even, so that $q = 2^h$ for some integer h.

2. THE KNOWN HYPEROVALS OF $PG(2,q)$, $q = 2^h$

A polynomial with coefficients in $GF(q)$ which induces a permutation on the elements of $GF(q)$ is called a *permutation polynomial.* There is a useful canonical form for a hyperoval in terms of permutation polynomials, as follows.

2.1 Theorem [5, 8.4.2] A hyperoval $\mathcal{O}$ in $PG(2,q)$ where $q > 2$ is even can be written as

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

where f is a permutation polynomial of degree at most $q-2$ satisfying $f(0) = 0$ and $f(1) = 1$. Further, for each $s \in GF(q)$, the polynomial $f^{(s)}$ where

$$f^{(s)}(x) = \frac{f(x+s)+f(s)}{x}, \qquad f^{(s)}(0) = 0$$

is a permutation polynomial.

If f is a polynomial representing a hyperoval, then $f(0) = 0$ and $f(1) = 1$ imply that f has no constant term and that the sum of the coefficients of f is 1. It is also known that the coefficient of each term of odd power in f is zero (see [14; 5, 8.4.2 Cor 1]). Further restrictions on the coefficients of such a polynomial f are described in [8].

The known hyperovals of $PG(2,q)$ with $q = 2^h$ and $h \geq 2$ are the following:
(1) The regular hyperovals $\mathcal{R} = \mathcal{D}(x^2)$, $h \geq 2$,
(2) the translation hyperovals $\mathcal{T} = \mathcal{D}(x^{2^i})$, where $(i,h) = 1$, $1 < i \leq h-1$ and $h \geq 3$, [13]
(3) the Segre hyperoval $\mathcal{D}(x^6)$, where $h \geq 5$ is odd, [11, 14]
(4) the Lunelli-Sce hyperoval $\mathcal{L} = \mathcal{D}(f)$, where $f(x) = x^{12} + x^{10} + \eta^{11}x^8 + x^6 + \eta^2x^4 + \eta^9x^2$, $q = 16$ and η is a primitive root satisfying $\eta^4 = \eta + 1$, [6]
(5) the Glynn hyperovals $\mathcal{G}_1 = \mathcal{D}(x^{3\sigma+4})$, where $h \geq 7$ is odd and $\sigma^2 \equiv 2 \pmod{q-1}$, [2]
(6) the Glynn hyperovals $\mathcal{G}_2 = \mathcal{D}(x^{\sigma+\lambda})$, where $h \geq 7$ is odd, $\sigma^2 \equiv 2 \pmod{q-1}$, $\lambda^4 \equiv 2 \pmod{q-1}$ and $\lambda^2 \equiv \sigma \pmod{q-1}$, [2]
(7) the Payne hyperovals $\mathcal{P} = \mathcal{D}(x^{1/6} + x^{3/6} + x^{5/6})$, where $h \geq 5$ is odd and the exponents are read modulo $q-1$, [10]
(8) the Cherowitzo hyperovals $\mathcal{C} = \mathcal{D}(x^\sigma + x^{\sigma+2} + x^{3\sigma+4})$, where $h = 5, 7$ or 9 and $\sigma^2 \equiv 2 \pmod{q-1}$ [1].

It is conjectured that the Cherowitzo hyperovals lie in an infinite class, that is, that $\mathcal{D}(x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4})$ is a hyperoval for all odd $h \geq 5$.

Each of the above infinite classes is defined for values of $h \geq 2$ (either all values of h or only odd values of h as appropriate) but the restrictions on h are placed to ensure that when two classes of hyperovals are defined in a plane then they are distinct. To illustrate some of the collapses that can occur, we determine the distinct classes of known hyperovals in planes of small order. We need the following result about hyperovals:

Theorem 2.2 [5, 8.4.3] If $\mathcal{H} = \mathcal{D}(x^{\alpha})$ is a hyperoval, then $\mathcal{D}(x^k)$ is a hyperoval equivalent to $\mathcal{H}$ for $k = 1/\alpha$, $1-\alpha$, $1/(1-\alpha)$, $\alpha/(1-\alpha)$ and $(\alpha-1)/\alpha$.

When $q = 4$ we have $h = 2$ and there are no irregular translation hyperovals. As h is even, there are no other known hyperovals. When $q = 8$ we have $h = 3$ and $2^2 = 4 = 1/2$ so there are no irregular translation hyperovals. Also there are no irregular Segre hyperovals as $6 = 1 - 2$. We find that $\sigma = 4$ and $\lambda = 2$ which imply $\sigma + \lambda = 6$ and $3\sigma + 4 = 2$ so the Glynn hyperovals are regular hyperovals. Also $1/6 = 6$ so the Payne and the Cherowitzo hyperovals are both $\mathcal{D}(x^2 + x^4 + x^6)$, which can be shown to be equivalent to $\mathcal{D}(x^2)$ (see [8, 1.11]). In fact,

Theorem 2.3 [5, 8.4.1] Every hyperoval of $PG(2,4)$ and $PG(2,8)$ is regular, so is of the form $\mathcal{D}(x^2)$.

When $q = 16$ there are regular hyperovals and Lunelli-Sce hyperovals known. Since $h = 4$ and $2^3 = 8 = 1/2$ there are no irregular translation hyperovals, and actually the following is true:

Theorem 2.4 [4, 7] In $PG(2,16)$ all hyperovals are either regular or are Lunelli-Sce hyperovals.

This theorem, first proved with the aid of a computer in [4], has recently been proved without a computer.

When $q = 32$ we have $h = 5$ and since $8 = 1/4$ and $16 = 1/2$ the only irregular translation hyperoval is $\mathcal{D}(x^4)$. We find that $\sigma = 8$ and $\lambda = 16$, giving $3\sigma + 4 = 28 = 1 - 4$ and $\sigma + \lambda = 24 = 1 - 8$ so the Glynn hyperovals are both irregular translation. Also, $1/6 = 26$ so that:

2.5 In $PG(2, 32)$ the known hyperovals are either regular $\mathcal{D}(x^2)$, irregular translation $\mathcal{D}(x^4)$, Segre $\mathcal{D}(x^6)$, Payne $\mathcal{D}(x^6 + x^{16} + x^{26})$ or Cherowitzo $\mathcal{D}(x^8 + x^{10} + x^{28})$.

When $q = 64$ we have $h = 6$ so apart from regular hyperovals there may be irregular translation hyperovals for $i = 5$. But $2^5 = 32 = 1/2$ which gives the result:

2.6 In $PG(2, 64)$ all known hyperovals are regular.

In $PG(2, 128)$ the above classes of known hyperovals are distinct (note that class (4) is not defined).

3. THE OVALS OF $PG(2, q)$, $q = 2^h$

We now return to the problem of determining the ovals contained in a given hyperoval $\mathcal{H}$. This determination depends on the orbits of the stabiliser of the hyperoval as shown in Section 1. It has been shown in [9] that, except in the case that $\mathcal{H}$ is one of $\mathcal{P}$ and $\mathcal{C}$, the orbits on $\mathcal{H}$ of the stabiliser $G(\mathcal{H})$ are unions of the sets:

- $X = \{(1, 0, 0)\}$;
- $Y = \{(0, 1, 0)\}$;
- $Z = \{(0, 0, 1)\}$ and
- $\mathcal{F} = \{(1, t, f(t)) : t \in GF(q)\backslash\{0\}\}$.

The Table 1 displays, for each of the known hyperovals $\mathcal{H}$, apart from $\mathcal{P}$ and $\mathcal{C}$, the order $\mid G(\mathcal{H}) \mid$ of the stabiliser of that hyperoval in $P\Gamma L(3, q)$ and the orbits of the stabiliser on $\mathcal{H}$. The hyperovals $\mathcal{P}$ and $\mathcal{C}$ are dealt with separately. For the details, see [9].

The stabiliser of the Payne hyperoval $\mathcal{P}$ has order $2h$ and has about $q/(2\log_2 q)$ orbits on the points of $\mathcal{P}$. These are $\{(0, 0, 1)\}$, $\{(1, 1, 1)\}$, $\{(1, 0, 0), (0, 1, 0)\}$ and

hyperoval	$\mid G(\mathcal{H}) \mid$	orbits on $\mathcal{H}$
regular $\mathcal{R}$, $q = 2,4$	$(q+2)(q+1)q(q-1)h$	$\mathcal{F} \cup X \cup Y \cup Z$
Lunelli-Sce $\mathcal{L}$, $q = 16$	$(q+2)2h = 144$	$\mathcal{F} \cup X \cup Y \cup Z$
regular $\mathcal{R}$, $q \geq 8$	$(q+1)q(q-1)h$	$\mathcal{F} \cup X \cup Z$, Y
$\mathcal{D}(x^6)$, $q = 32$	$3(q-1)h = 465$	$\mathcal{F}$, $X \cup Y \cup Z$
Glynn $\mathcal{G}_2$, $q = 128$	$3(q-1)h = 2667$	$\mathcal{F}$, $X \cup Y \cup Z$
irregular translation $\mathcal{T}$	$q(q-1)h$	$\mathcal{F} \cup X$, Y, Z
$\mathcal{D}(x^6)$, $q \geq 128$	$(q-1)h$	$\mathcal{F}$, X, Y, Z
Glynn $\mathcal{G}_1$	$(q-1)h$	$\mathcal{F}$, X, Y, Z
Glynn $\mathcal{G}_2$, $q > 128$	$(q-1)h$	$\mathcal{F}$, X, Y, Z

Table 1

sets

$$\mathcal{O}_n = \left\{ \left(1, w^{n2^i}, f(w^{n2^i})\right) : i = 1, \ldots, h \right\} \cup \left\{ \left(w^{n2^i}, 1, f(w^{n2^i})\right) : i = 1, \ldots, h \right\}$$

of size $2d$ where d divides h and w is a primitive element of $GF(q)$. The automorphic collineations stabilise the Cherowitzo hyperoval $\mathcal{C}$, so the stabiliser of $\mathcal{C}$ has order divisible by h. The orbits of the stabiliser on the points of $\mathcal{C}$ are unions of the following sets: $\{(0,0,1)\}$, $\{(1,1,1)\}$, $\{(1,0,0)\}$, $\{(0,1,0)\}$ and

$$\mathcal{O}_n = \left\{ \left(1, w^{n2^i}, f(w^{n2^i})\right) : i = 1, \ldots, h \right\}.$$

By Theorem 1.1 the number of orbits is the number of inequivalent ovals obtained by deleting a point of $\mathcal{H}$. Incidentally the orbits of the stabiliser of a hyperoval on its points and on unordered pairs of its points are also of interest in constructing generalized quadrangles (see [10]).

We now have the number of inequivalent ovals contained in each of the known hyperovals (except the Cherowitzo hyperovals). We proceed to a uniform way of describing these ovals. As in the case of hyperovals, there is a useful form for an oval $\mathcal{O}$. This is obtained by completing the oval to a hyperoval then using the canonical form for the hyperoval, but ensuring that the nucleus of the oval is the point (0,1,0). The oval is then written as

$$\mathcal{E}(f) = \{(1, t, f(t)) : t \in GF(q)\} \cup \{(0,0,1)\}$$

where f is a permutation polynomial of degree at most $q-2$ satisfying $f(0)=0$ and $f(1)=1$. Further, for each $s \in GF(q)$, the polynomial $f^{(s)}$ where

$$f^{(s)}(x) = \frac{f(x+s)+f(s)}{x}, \qquad f^{(s)}(0)=0$$

is a permutation polynomial.

To obtain each of the ovals contained in a given hyperoval $\mathcal{H}$ in this form, we need to choose a point of each orbit of the stabiliser, then map this to the point $(0,1,0)$ with an element of $P\Gamma L(3,q)$, ensuring that the resulting image of $\mathcal{H}$ contains the fundamental quadrangle. The image of $\mathcal{H}$ can be written as $\mathcal{H}' = \mathcal{D}(g)$ and the corresponding oval is $\mathcal{E}(g) = \{(1,t,g(t)) : t \in GF(q)\} \cup \{(0,0,1)\}$ and has nucleus $(0,1,0)$ as required. This representation is not necessarily unique.

For each of the known hyperovals except the Payne and Cherowitzo hyperovals, there are at most 4 orbits of the stabiliser and each contains at least one of the fundamental points. Thus we need use only (some of) the fundamental points (1,0,0), (0,1,0), (0,0,1) and (1,1,1) to determine the ovals contained in each hyperoval, and the maps we require are the identity together with the maps:

(1) $(a,b,c) \mapsto (b,c,a)$,

(2) $(a,b,c) \mapsto (c,b,a)$, and

(3) $(a,b,c) \mapsto (a+b,b,b+c)$.

These maps were considered in [1], where it is shown that they map the hyperoval $\mathcal{D}(f)$ to the equivalent hyperoval $\mathcal{D}(g)$ where

(1) $g(x) = xf(1/x)$;

(2) $g(x) = f^{-1}(x)$;

(3) $g(x) = (x+1)f(x/x+1)+x$.

Using these means we have:

3.1 The following hyperovals give rise to the inequivalent ovals $\mathcal{E}(g)$ as indicated in Table 2. (For convenience an oval $\mathcal{E}(x^n)$ for some n will be denoted by $\mathcal{E}(n)$.)

The expressions for the ovals contained in the Payne and Cherowitzo hyperovals are more complicated as there are more than four orbits of the stabiliser of the

hyperoval $\mathcal{H}$	ovals in $\mathcal{H}$
regular $\mathcal{R}$, $q = 2, 4$	$\mathcal{E}(2)$
Lunelli-Sce $\mathcal{L}$, $q = 16$	$\mathcal{E}(f(x))$
regular $\mathcal{R}$, $q \geq 8$	$\mathcal{E}(2)$, $\mathcal{E}(1/2)$
$\mathcal{D}(x^6)$, $q = 32$	$\mathcal{E}(6)$, $\mathcal{E}(26)$
Glynn $\mathcal{G}_2$, $q = 128$	$\mathcal{E}(20)$, $\mathcal{E}(108)$
irregular translation $\mathcal{T}$	$\mathcal{E}(2^i)$, $\mathcal{E}(1/2^i)$, $\mathcal{E}(1 - 2^i)$
$\mathcal{D}(x^6)$, $q \geq 128$	$\mathcal{E}(6)$, $\mathcal{E}(1/6)$, $\mathcal{E}(1-6)$, $\mathcal{E}((x+1)(x/(x+1))^6 + x)$
Glynn $\mathcal{G}_1$	$\mathcal{E}(3\sigma + 4)$, $\mathcal{E}(1/(3\sigma + 4))$,
	$\mathcal{E}(1 - (3\sigma + 4))$, $\mathcal{E}((x+1)(x/(x+1))^{3\sigma+4} + x)$
Glynn $\mathcal{G}_2$, $q > 128$	$\mathcal{E}(\sigma + \lambda)$, $\mathcal{E}(1/(\sigma + \lambda))$,
	$\mathcal{E}(1 - (\sigma + \lambda))$, $\mathcal{E}((x+1)(x/(x+1))^{\sigma+\lambda} + x)$

Table 2

hyperoval on its points.

Once the orders of the stabilisers of the various hyperovals are known, and the lengths of the orbits of these stabilisers on the hyperovals are found, it is easy to calculate the orders of the stabilisers of the known ovals.

3.2 Theorem Let $\mathcal{O}$ be an oval of $PG(2,q)$, q even, with nucleus P so that $\mathcal{H} = \mathcal{O} \cup \{P\}$ is a hyperoval. Let G be the stabiliser in $P\Gamma L(3,q)$ of $\mathcal{H}$, and suppose that the orbit of G on $\mathcal{H}$ which contains P has n points. Then the stabiliser J in $P\Gamma L(3,q)$ of $\mathcal{O}$ has order $\mid G \mid /n$.

Proof: If an element $\sigma \in P\Gamma L(3,q)$ stabilises $\mathcal{O}$ then it stabilises P and hence $\mathcal{H}$, so that J is a subgroup of G. In fact J is that subgroup of G which fixes P, which has order $\mid G \mid$ divided by the length of the orbit of G on $\mathcal{H}$ containing P.

4. COMPUTER SEARCHES FOR HYPEROVALS

The polynomials over $GF(q)$ which could represent hyperovals are of the form $f(x) = \sum_{i=1}^{(q-2)/2} a_{2i}x^{2i}$ where $\sum_{i=1}^{(q-2)/2} a_{2i} = 1$. There are easily programmed tests which can be applied to such a polynomial to determine whether or not it represents a hyperoval ([1, 2, 3]). In fact the Lunelli-Sce hyperoval, the two classes of Glynn hyperovals and the Cherowitzo hyperovals were first discovered by computer searches.

The following spaces of polynomials over $GF(q)$ have been searched for polynomials which represent hyperovals. In each case, any polynomials found correspond to a hyperoval belonging to one of the known classes.

(1) $PG(2,32)$

- polynomials with coefficients in GF(2) ([1, 3]);
- polynomials with one term ([2]);
- polynomials with 2 to 4 terms ([8]);
- some polynomials with 5 terms ([8]).

(2) $PG(2,64)$

- polynomials with coefficients in GF(2) ([3, 8]);
- some polynomials with coefficients in GF(4) ([3, 8]);
- polynomials with one term ([2, 8]).
- polynomials with 2 to 3 terms ([8]);

(3) $PG(2,128)$

- polynomials with one term ([2]);
- polynomials with 3 terms and coefficients in $GF(2)$ ([1]);

(4) $PG(2,256)$

- polynomials with one term ([2]);
- the 2040 polynomials which represent the Lunelli-Sce hyperoval with coefficients (from $GF(16)$) considered as elements of $GF(256)$ ([8]);

(5) $PG(2,512)$

- polynomials with one term ([2]);
- polynomials with 3 terms and coefficents in $GF(2)$ whose exponents occur as monomial o-polynomials ([1]);

(5) $PG(2, 2^h)$, $h \leq 28$

- polynomials with one term ([2, 3]).

Acknowledgement: The author acknowledges the support of an ARC Research Fellowship.

5. REFERENCES

[1] W. Cherowitzo, Hyperovals in Desarguesian planes of even order, Annals Disc. Math. 37 (1988) 87–94.

[2] D.G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, in: L.R.A. Casse, ed., Combinatorial Mathematics X Lecture Notes in Mathematics 1036 (Springer, 1983) 217–229.

[3] D.G. Glynn, A condition for the existence of ovals in $PG(2, q)$, q even, to appear, Geometriae Dedicata.

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

[5] J.W.P. Hirschfeld, Projective geometries over finite fields (Oxford University Press, 1979).

[6] 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)

[7] C.M. O'Keefe and T. Penttila, Hyperovals in $PG(2, 16)$, submitted.

[8] C.M. O'Keefe and T. Penttila, Polynomials for hyperovals of Desarguesian planes, submitted.

[9] C.M. O'Keefe and T. Penttila, Symmetries of arcs, in preparation.

[10] S.E. Payne, A new infinite family of generalized quadrangles, Congressus Numerantium 49 (1985) 115–128.

[11] B. Segre, Ovali e curve σ nei piani di Galois di caratteristica due, Atti Accad. Naz. Lincei Rend. (8) 32 (1962) 785–790.

[12] B. Segre, Ovals in a finite projective plane, Can. J.Math. 7 (1955) 414–416.

[13] B. Segre, Sui k-archi nei piani finiti di caratteristica 2, Revue de Math. Pures Appl. 2 (1957) 289–300.

[14] B. Segre and U. Bartocci, Ovali ed altre curve nei piani di Galois di caratteristica due, Acta Arith. 8 (1971) 423–449.