J. Austral. Math. Soc. (*Series A*) **51** (1991), 436–447

POLYNOMIALS FOR HYPEROVALS OF DESARGUESIAN PLANES

CHRISTINE M. O'KEEFE and TIM PENTTILA

(Received 27 October 1989; revised 2 March 1990)

Communicated by L. Caccetta

Abstract

This paper studies o-polynomials, that is, polynomials which represent hyperovals in Desarguesian projective planes of even order. We present theoretical restrictions on the form that o-polynomials can have, and we determine the number of o-polynomials corresponding to each of the known classes of hyperovals (other than Cherowitzo's). We use this to give the number of known o-polynomials for the fields of orders 4, 8, 16 and 32. Exploratory computer searches for o-polynomials for fields of small orders greater than 16 are reported.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*) 51 E 20.

1. Theoretical results

Let $PG(2, q)$ be the projective plane over the field $GF(q)$ of order q, where q is a power of a prime p. A *hyperoval* of $PG(2, q)$ is a set of $q+2$ points, no three of which are collinear. An account of hyperovals appears in [5], but here we note a few relevant definitions and results. Firstly, hyperovals exist in $PG(2, q)$ if and only if q is even. A hyperoval is *regular* if it contains $q + 1$ points which are the points of a non-degenerate conic in $PG(2, q)$. Conversely, the points of a non-degenerate conic together with a unique further point called the *nucleus* of the conic provide an example of a hyperoval.

THEOREM 1.1 [5, 8.4.1]. *If $q = 2$ then every hyperoval is regular.*

PROOF. In $PG(2, 2)$ a hyperoval consists of four points, any three of which form a conic.

By the transitivity of the collineation group $P\Gamma L(3, q)$ of $PG(2, q)$ on quadrangles, every hyperoval can be mapped by an element of $P\Gamma L(3, q)$ to one containing the fundamental quadrangle $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ and $(1, 1, 1)$. A hyperoval which is the image under an element of $P\Gamma L(3, q)$ of a hyperoval $\mathscr{H}$ is *equivalent* to $\mathscr{H}$.

We therefore restrict our attention to $PG(2, q)$ with $q > 2$ and consider only hyperovals which contain the fundamental quadrangle. The next result shows that these are related to *permutation polynomials*, that is, polynomials which are permutations when regarded as polynomial functions.

THEOREM 1.2 [5, 8.4.2]. *A hyperoval $\mathscr{O}$ in $PG(2, q)$ where $q > 2$ is even can be written as*

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

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

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

is a permutation polynomial.

Permutation polynomials which arise in this way are called *o-polynomials* following Cherowitzo [1], and o-polynomials arising from equivalent hyperovals will be called *equivalent*. If f is an o-polynomial 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. Other results concerning the terms appearing in an o-polynomial are the following three theorems.

THEOREM 1.3 [14; 5, 8.4.2 COROLLARY 1]. *The coefficient of each term of odd power in an o-polynomial is zero.*

For the next statement we need the following partial ordering $\preceq$ on the set of integers n where $0 \leq n \leq q - 1$. 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. In other words, $b \preceq c$ if and only if all terms appearing in the binary expansion of b also appear in the binary expansion of c.

The main source of importance for this partial ordering is the following version of the binomial theorem in fields of characteristic 2:

$$(x+y)^n = \sum_{i \preceq n} x^i y^{n-i}.$$

Another way of stating this is

$$(x+y)^{\alpha_1+\alpha_2+\cdots+\alpha_k} = \prod_{j=1}^{k} (x^{\alpha_j} + y^{\alpha_j}),$$

where $n = \alpha_1 + \alpha_2 + \cdots + \alpha_k$ and the α_j are distinct powers of 2.

THEOREM 1.4 [3]. *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 $f(x)^b \pmod{x^q - x}$ is zero for all pairs of integers (b, c) satisfying $1 \le b \le c \le q-1$, $b \ne q-1$ and $b \preceq c$.*

Note that the case $b = 1$ gives the result of Theorem 1.3. In addition, this condition can be analysed to give further equations relating the coefficients of f as follows.

THEOREM 1.5. *Let $f(x) = \sum_{i=1}^{q-2} a_i x^i$ and suppose that $\sum_{i=1}^{q-2} a_i = 1$. Then f is an o-polynomial if and only if for all b with $1 \le b \le q-2$ and all c with $b \preceq c$*

$$\sum \prod_{k=1}^{n} a_{i_k}^{\alpha_k} = 0,$$

where $b = \alpha_1 + \alpha_2 + \cdots + \alpha_n$, the α_j are distinct powers of 2 and the sum is over all i_k with $c = \sum_{k=1}^{n} i_k \alpha_k \pmod{q-1}$.

PROOF. The polynomial $f(x)^b$ is

$$\left(\sum_{i=1}^{q-2} a_i x^i\right)^{\alpha_1+\alpha_2+\cdots+\alpha_n} = \prod_{j=1}^{n} \left(\sum_{i=1}^{q-2} a_i^{\alpha_j} x^{i\alpha_j}\right).$$

By Theorem 1.4, if $b \preceq c$ then the coefficient of x^c in the right hand-side is zero; so

$$\sum \prod_{k} a_{i_k}^{\alpha_k} = 0.$$

When investigating o-polynomials, two coefficients can often be assumed

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

to be equal. More precisely,

THEOREM 1.6. *Let* $f(x) = \sum_{k=1}^{(q-2)/2} a_{2k}x^{2k}$ *be an o-polynomial such that for some* i *and* j, *with* $i-j$ *coprime to* $q-1$, $a_{2i} \neq 0$ *and* $a_{2j} \neq 0$. *Then* f *is equivalent to an o-polynomial* $g(x) = \sum_{k=1}^{(q-2)/2} b_{2k}x^{2k}$ *with* $b_{2i} = b_{2j}$ *and, for all* k, $b_{2k} = 0$ *if and only if* $a_{2k} = 0$.

PROOF. Let $f(x) = \sum_{k=1}^{(q-2)/2} a_{2k}x^{2k}$ with $a_{2i} \neq 0$, $a_{2j} \neq 0$ and $(i-j, q-1) = 1$. The hyperoval $\mathscr{D}(f)$ is mapped by the homography with matrix

$$\mathscr{M}_s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & s^{-1} & 0 \\ 0 & 0 & f(s)^{-1} \end{pmatrix}, \quad s \in GF(q) - \{0\}$$

to a hyperoval $\mathscr{M}_s(\mathscr{D}(f))$ which still contains the fundamental quadrangle, since $\mathscr{M}_s$ fixes the points $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ and maps the point $(1, s, f(s))$ to $(1,1,1)$. Thus the o-polynomial f_s of $\mathscr{M}_s(\mathscr{D}(f))$ is equivalent to f. Since

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & s^{-1} & 0 \\ 0 & 0 & f(s)^{-1} \end{pmatrix} \begin{pmatrix} 1 \\ t \\ f(t) \end{pmatrix} = \begin{pmatrix} 1 \\ s^{-1}t \\ f(s)^{-1}f(t) \end{pmatrix} = \begin{pmatrix} 1 \\ u \\ f(s)^{-1}f(su) \end{pmatrix}$$

this o-polynomial is

$$f_s(x) = f(s)^{-1}f(sx) = \left(\sum_{k=1}^{(q-2)/2} a_{2k}s^{2k} \right)^{-1} \sum_{k=1}^{(q-2)/2} a_{2k}s^{2k}x^{2k}.$$

The ratio of the coefficient of x^{2i} to the coefficient of x^{2j} in f_s is $s^{2(i-j)}(a_{2i}/a_{2j})$ for $s \in GF(q) - \{0\}$. Since $(i-j, q-1) = 1$, the ratio takes on $q-1$ distinct non-zero values in the $q-1$ o-polynomials f_s equivalent to f, and the result follows.

When conducting a computer search for o-polynomials and using this theorem, each o-polynomial with $a_{2i} = a_{2j}$, non-zero, gives rise to $q-1$ o-polynomials. The number of o-polynomials can be enough to characterize the hyperovals by using the ideas of Theorem 1.8 below.

COROLLARY. *A binomial o-polynomial* $f(x) = ax^{2i} + bx^{2j}$ *has* $(i-j, q-1) \neq 1$. *In particular, if* $q-1$ *is a prime then there are no binomial o-polynomials representing hyperovals in* $PG(2, q)$.

PROOF. Suppose that $f(x) = ax^{2i} + bx^{2j}$ is a binomial o-polynomial for $PG(2, q)$ and that $(i-j, q-1) = 1$. The theorem implies that f is

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

equivalent to the o-polynomial $f_s(x) = ax^{2i} + ax^{2j}$. But $f_s(1) = 1$ means that $a + a = 1$, a contradiction since when q is even, $a + a = 0$ for any $a \in GF(q)$.

For example, $q = 8$ and $q = 32$ have $q - 1$ prime so hyperovals in $PG(2, 8)$ or $PG(2, 32)$ can never have a binomial o-polynomial.

An o-polynomial defined over a proper subfield has further restrictions, as remarked in [3].

THEOREM 1.7. *If f is an o-polynomial for $PG(2, q^r)$ with coefficients in $GF(q)$ then f is congruent to an o-polynomial for $PG(2, q)$ modulo $x^{2q} + x^2$.*

PROOF. If f is considered to be a polynomial over $GF(q)$, then it is an o-polynomial for $PG(2, q)$, since it defines a set of points, no three collinear, of the correct cardinality. It follows that $f \equiv g \pmod{x^q + x}$ for some o-polynomial g for $PG(2, q)$. By Theorem 1.3 both f and g are squares, say $f = f_1^2$ and $g = g_1^2$. Now $f_1(a)^2 = g_1(a)^2$ for all $a \in GF(q)$, so $f_1(a) = g_1(a)$ for all $a \in GF(q)$. Therefore $f_1 \equiv g_1 \pmod{x^q + x}$; so $f_1^2 \equiv g_1^2 \pmod{x^{2q} + x^2}$. (In fact $f(x) = g(x) + r(x)^2(x^{2q} + x^2)$ for some polynomial $r(x)$, since f is a square.)

Another useful observation, due to Cherowitzo [1], is that if $\sum_{i=1}^{(q-1)/2} a_{2i}x^{2i}$ is an o-polynomial then $\sum_{i=1}^{(q-1)/2} a_{2i}^{\alpha}x^{2i}$ is an equivalent o-polynomial, where α is any automorphism of $GF(q)$.

These results can be used to conduct a computer search for o-polynomials, particularly in small fields. An exhaustive list of o-polynomials for a given value of q constitutes a means of characterization of the hyperovals of $PG(2, q)$ for that value of q. For this purpose, it is useful to know how many o-polynomials are equivalent to a given o-polynomial. This depends on the particular hyperoval, as is shown in the next result.

THEOREM 1.8. *Let $\mathscr{H}$ be a hyperoval of $PG(2, q)$ where $q = 2^h$ and $h \geq 2$, containing the fundamental quadrangle $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ and $(1, 1, 1)$. Let the o-polynomial of $\mathscr{H}$ be f and let G denote the stabiliser of $\mathscr{H}$ in $P\Gamma L(3, q)$. Then the number of o-polynomials equivalent to f is*

$$\frac{h(q+2)(q+1)q(q-1)}{|G|}.$$

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

PROOF. The o-polynomials equivalent to f are precisely the o-polynomials associated with the hyperovals which are images under $P\Gamma L(3, q)$ of $\mathscr{H}$ and which contain the fundamental quadrangle. We find the number of such hyperovals by counting in two ways the pairs $(\mathscr{H}', Q)$ where $\mathscr{H}'$ is an image under $P\Gamma L(3, q)$ of $\mathscr{H}$ and Q is a quadrangle contained in $\mathscr{H}'$. Letting N denote the number of hyperovals containing a fixed quadrangle Q which are images under $P\Gamma L(3, q)$ of $\mathscr{H}$, we obtain

$$|P\Gamma L(3, q): G|.\binom{q+2}{4} = \frac{(q^2+q+1)(q^2+q)q^2(q-1)^2}{4!}.N$$

and the result follows.

COROLLARY. *Table 1 displays, for each of the known hyperovals $\mathscr{H}$, the order $|G(\mathscr{H})|$ of the stabiliser of that hyperoval and hence the number $N(\mathscr{H})$ of equivalent o-polynomials representing that hyperoval. For the details, see* [9]. *The known hyperovals of $PG(2, q)$. $q = 2^h \geq 4$, are the following:*

(1) *the regular hyperovals $\mathscr{R} = \mathscr{D}(x^2)$;*

(2) *the translation hyperovals $\mathscr{T} = \mathscr{D}(x^{2^i})$, where $(i, h) = 1$,* [12];

(3) *the hyperoval $\mathscr{D}(x^6)$, where $h \geq 5$ is odd,* [13, 14];

(4) *the Lunelli-Sce hyperoval $\mathscr{L} = \mathscr{D}(f)$, 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 $\mathscr{G}_1 = \mathscr{D}(x^{3\sigma+4})$, where $h \geq 7$ is odd and $\sigma^2 \equiv 2 \pmod{q-1}$,* [2]:

(6) *the Glynn hyperovals $\mathscr{G}_2 = \mathscr{D}(x^{\sigma+\lambda})$, 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 $\mathscr{P} = \mathscr{D}(x^{1/6} + x^{3/6} + x^{5/6})$, where $h \geq 5$ is odd and the exponents are read modulo $q-1$,* [10];

(8) *the Cherowitzo hyperovals $\mathscr{C} = \mathscr{D}(x^\sigma + x^{\sigma+2} + x^{3\sigma+4})$, where $h = 5, 7$ or 9 and $\sigma^2 \equiv 2 \pmod{q-1}$,* [1].

Let $\mathscr{H}$ be a hyperoval containing the fundamental quadrangle Q and with o-polynomial f. The group of projectivities which stabilises Q has order 24, and any of its elements maps $\mathscr{H}$ to an equivalent hyperoval. Using this observation, Cherowitzo [1] gives a list of images of the point $(1, t, f(t))$ which implicitly define 24 o-polynomials equivalent to f. In particular he finds the o-polynomials of Theorem 1.9.

THEOREM 1.9 [1]. *The following polynomials g are o-polynomials equivalent to a given o-polynomial f:*

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

Table 1

hyperoval	$\lvert G(\mathscr{H})\rvert$	$N(\mathscr{H})$
regular $\mathscr{R}$, $q = 2, 4$	$(q+2)(q+1)q(q-1)h$	1
regular $\mathscr{R}$, $q \geq 8$	$(q+1)q(q-1)h$	$q+2$
irregular translation $\mathscr{T}$	$q(q-1)h$	$(q+2)(q+1)$
$\mathscr{D}(x^6)$, $q = 32$	$3(q-1)h = 465$	$(q+2)(q+1)q/3 = 11968$
$\mathscr{D}(x^6)$, $q \geq 128$	$(q-1)h$	$(q+2)(q+1)q$
Lunelli-Sce $\mathscr{L}$, $q = 16$	$(q+2)2h = 144$	$(q+1)q(q-1)/2 = 2040$
Glynn $\mathscr{G}_1$	$(q-1)h$	$(q+2)(q+1)/q$
Glynn $\mathscr{G}_2$, $q = 128$	$3(q-1)h = 2667$	$(q+2)(q+1)q/3$
Glynn $\mathscr{G}_2$, $q > 128$	$(q-1)h$	$(q+2)(q+1)q$
Payne $\mathscr{P}$	$2h$	$(q+2)(q+1)q(q-1)/2$
Cherowitzo $\mathscr{C}$, $q = 32$	$h = 5$	$(q+2)(q+1)q(q-1)$
Cherowitzo $\mathscr{C}$, $q \geq 128$	divisible by h	$\leq (q+2)(q+1)q(q-1)$

(2) $g(x) = f^{-1}(x)$;
(5) $g(x) = xf(1/x)$, $g(0) = 0$;
(6) $g(x) = f(x+1) + 1$;
(11) $g(x) = (x+1)f(1/(x+1)) + 1$, $g(1) = 1$;
(12) $g(x) = x + xf(1 + (1/x))$, $g(0) = 0$;
(16) $g(x) = x + (x+1)f(x/(x+1))$, $g(1) = 1$;

as well as each of the above with f replaced by f^{-1}. (Here the numbering follows that of [1, *Result* 2]).

If we now consider projectivities fixing $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ pointwise but not necessarily fixing the point $(1, 1, 1)$ we obtain the following.

THEOREM 1.10. *If f is an o-polynomial then the following $q-1$ polynomials f_s are o-polynomials equivalent to f:*

$$f_s(x) = f(s)^{-1} f(sx), \text{ for } s \in GF(q) - \{0\}.$$

PROOF. The homographies with matrix $\mathscr{M}_s$, $s \in GF(q) - \{0\}$, introduced in Theorem 1.6 map the hyperoval $\mathscr{D}(f)$ to equivalent hyperovals containing the fundamental quadrangle and hence give $q-1$ o-polynomials f_s equivalent to f as in the statement of the theorem.

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

THEOREM 1.11. *When $q \geq 8$ the $q+2$ equivalent o-polynomials representing a regular hyperoval are exactly*

(1) *the 3 monomials x^2, $x^{1/2}$ and x^{-1},*

(2) *the $q-1$ polynomials*

$$g_s(x) = \sum_{i=1}^{(q-2)/2} (s+1)s^{2i-1}x^{2i}, \qquad \text{for } s \in GF(q) - \{0\}.$$

PROOF. A regular hyperoval is represented by the o-polynomial $f(x) = x^2$. The other two monomials listed in (1) are o-polynomials equivalent to x^2 by Theorem 1.9 (2) and (5). It can be verified that these three are distinct for $q \geq 8$. By Theorem 1.9 (11), the regular hyperoval is also represented by the o-polynomial

$$g(x) = (x+1)f(1/(x+1)) + 1 = \frac{(x+1)}{(x+1)^2} + 1 = \frac{x}{x+1} \text{ and } g(1) = 1.$$

The o-polynomial g can also be expressed as $g(x) = (x+1)^{q-2} + 1 = \sum_{i=1}^{(q-2)/2} x^{2i}$. It now follows from Theorem 1.10 that g is equivalent to the o-polynomials

$$g_s(x) = \frac{s+1}{s} \sum_{i=1}^{(q-2)/2} (sx)^{2i} = \sum_{i=1}^{(q-2)/2} (s+1)s^{2i-1}x^{2i}.$$

By Corollary (2) to Theorem 1.8 there are $q+2$ o-polynomials equivalent to f, and the proof is complete.

2. *O*-polynomials for $PG(2, 4)$ and $PG(2, 8)$

THEOREM 2.1. *In $PG(2, 4)$ every hyperoval is regular. In particular, there is a unique o-polynomial $f(x) = x^2$ for $PG(2, 4)$.*

PROOF. A hyperoval in $PG(2, 4)$ has six points, any five of which uniquely determine a conic. By Theorems 1.2 and 1.3, an o-polynomial for $PG(2, 4)$ has only terms with even powers of x appearing, has degree at most $q-2 = 2$ and has the sum of coefficients equal to 1. Since $f(x) = x^2$ is an o-polynomial the result follows.

COROLLARY. *The stabiliser of a regular hyperoval in $PG(2, 4)$ has order 720, is isomorphic to S_6 and acts naturally on the points of the hyperoval.*

PROOF. By Theorem 1.4 and (2) above, the stabiliser G of a regular hyperoval $\mathscr{H}$ in $PG(2, 4)$ has order $2(4+2)(4+1)4(4-1)$. We have a

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

homomorphism from G into S_6 with kernel the pointwise stabiliser of $\mathscr{H}$, which is trivial. To see that it is onto, note that the orders of G and S_6 are equal.

THEOREM 2.2. *In $PG(2, 8)$ every hyperoval is regular. The o-polynomials for $PG(2, 8)$ are $a_6x^6+a_4x^4+a_2x^2$ where the values of a_6, a_4, a_2 are given in Table 2. $GF(8)$ has primitive root ε where $\varepsilon^3 = \varepsilon^2 + 1$, and so $\varepsilon^7 = 1$.*

Table 2

a_6	0	0	ε^3	ε^3	ε^5	ε^5	ε^6	ε^6	ε^7	ε^7
a_4	0	ε^7	ε^1	ε^4	ε^2	ε^4	ε^1	ε^2	0	ε^7
a_2	ε^7	0	ε^6	ε^5	ε^6	ε^3	ε^3	ε^5	0	ε^7

PROOF. By Theorems 1.2 and 1.3, an o-polynomial for $PG(2, 8)$ is of the form $a_6x^6+a_4x^4+a_2x^2$ where $a_6+a_4+a_2 = 1$. Consider the equations of Theorem 1.5 for the cases $b = 3$, $c = 3$ and $b = 3$, $c = 7$, which are

$$a_4^2a_2 + a_2^2a_6 = 0 \quad \text{and} \quad a_6^2a_2 + a_4^2a_6 = 0$$

respectively. There are 10 solutions (a_6, a_4, a_2) with $a_2 + a_4 + a_6 = 1$ to this system of equations. This can be seen by noting that the system can be rewritten as $(a_4^2+a_2a_6)a_2 = 0$ and $(a_4^2+a_2a_6)a_6 = 0$ so that the solutions are the point $(0, 1, 0)$ together with the points of the conic $a_4^2 = a_2a_6$. Since Theorem 1.11 constructs 10 o-polynomials representing regular hyperovals, it follows that they are the only o-polynomials for $PG(2, 8)$.

Note the curious fact mentioned by Glynn [3] that the triples (a_6, a_4, a_2) with $a_6x^6+a_4x^4+a_2x^2$ an o-polynomial themselves form a regular hyperoval in $PG(2, 8)$.

3. *O*-polynomials for $PG(2, 16)$

By Theorems 1.2 and 1.3, an o-polynomial for $PG(2, 16)$ has the form

$$a_{14}x^{14} + a_{12}x^{12} + a_{10}x^{10} + a_8x^8 + a_6x^6 + a_4x^4 + a_2x^2$$

where $a_i \in GF(16)$ for all i and $a_{14}+a_{12}+a_{10}+a_6+a_4+a_2 = 1$. There are $16^6 = 2^{24}$ *such polynomials, that is, about 17 million. Theorem 1.2 provides*

https://doi.org/10.1017/S1446788700034601 Published online by Cambridge University Press

an easily programmed test of whether or not a given polynomial is an o-polynomial. The output of a program which deals with all the polynomials of the above form is given in [8]. Only 2058 of the polynomials are o-polynomials. This verifies the following result of Hall [4], also obtained by computer.

THEOREM 3.1 [4]. *In* $PG(2, 16)$ *there are two equivalence classes of hyperovals, namely the regular hyperovals giving rise to* 18 *o-polynomials and the hyperovals first constructed by Lunelli and Sce* [6] *which give rise to 2040 o-polynomials.*

COROLLARY. *The stabiliser of a Lunelli-Sce hyperoval in* $PG(2, 16)$ *has order* 144.

PROOF. By Theorem 1.8, the stabiliser has order $4.18.17.16.15/2040$.

In fact the stabiliser of the Lunelli-Sce hyperoval was first found in [11], without using Hall's result. This was used, together with Theorems 1.5 and 1.8 to prove Hall's result without a computer [7].

4. O-polynomials for $PG(2, 32)$

The hyperovals in $PG(2, 32)$ have not yet been classified, and as a consequence the number of o-polynomials for $PG(2, 32)$ is unknown.

There are 5 known classes of hyperovals in $PG(2, 32)$, giving a lower bound on the number of o-polynomials. The regular hyperovals provide 34 o-polynomials, the irregular translation hyperovals provide 1122 and the hyperoval $\mathscr{D}(x^6)$ gives rise to 11,968. The Payne hyperovals provide 556,512 o-polynomials and the Cherowitzo hyperovals give rise to 1,113,024.

The search space for o-polynomials for $PG(2, 32)$ is at present too large for an exhaustive computer search to be justifiable. However, the following smaller searches have been made, with all o-polynomials found coming from one of the above 5 classes:

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

These two searches were repeated, as well as

- polynomials with 2 to 4 terms;
- some polynomials with 5 terms.

5. Computer searches for hyperovals, $q > 32$

The following spaces of polynomials over $GF(q)$ were searched for o-polynomials. In each case, any o-polynomials found correspond to a hyperoval belonging to one of the known classes.

(1) $PG(2, 64)$
- polynomials with coefficients in $GF(2)$ ([3]);
- some polynomials with coefficients in $GF(4)$ ([3]);
- polynomials with one term ([2]);
- polynomials with 2 to 3 terms.

(2) $PG(2, 128)$
- polynomials with one term ([2]);
- polynomials with 3 terms and coefficients in $GF(2)$ ([1]).

(3) $PG(2, 256)$
- polynomials with one term ([2]);
- 2040 o-polynomials for the Lunelli-Sce hyperoval with coefficients (from $GF(16)$) considered as elements of $GF(256)$.

(4) $PG(2, 512)$
- polynomials with one term ([2]);
- polynomials with 3 terms and coefficients 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 first author acknowledges the support of an ARC Research Fellowship.

References

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

[2] 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).

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

[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 $PG(2, 16)$' European J. Combin., to appear.
[8] ——, *Polynomials Representing Hyperovals* (University of Western Australia Research Report, June 1989/26).
[9] ——, 'Symmetries of arcs', submitted.
[10] S. E. Payne, 'A new infinite family of generalized quadrangles', *Congr. Numer.* **49** (1985), 115–128.
[11] S. E. Payne and J. E. Conklin, 'An unusual generalized quadrangle of order sixteen', *J. Combin. Theory Ser. A* **24** (1978), 50–74.
[12] B. Segre, 'Sui k-archi nei piani finiti di caratteristica 2', *Rev. Math. Pures Appl.* **2** (1957), 289–300.
[13] ——, 'Ovali e curve σ nei piani di Galois di caratteristica due', *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) **32** (1962), 785–790.
[14] B. Segre and U. Bartocci, 'Ovali ed altre curve nei piani di Galois di caratteristica due', *Acta Arith.* **8** (1971), 423–449.

The University of Western Australia
Nedlands, W.A. 6009
Australia