DAVID G. GLYNN

A CONDITION FOR THE EXISTENCE OF OVALS IN PG(2, q), q EVEN

ABSTRACT. A condition is found that determines whether a polynomial over GF(q) gives an oval in PG(2, q), q even. This shows that the set of all ovals of PG(2, q) corresponds to a certain variety of points of PG($(q-4)/2, q$). The condition improves upon that of Segre and Bartocci, who proved that all the terms of an oval polynomial have even degree. It is suitable for efficient computer searches.

An oval, sometimes called a hyperoval, is a set of $q+2$ points of PG(2, q), $q = 2^h$, such that no three are collinear. Since a k-arc is defined to be a set of k points, with no three being collinear, an oval is also a $(q+2)$-arc. Such a set of points generalizes the properties of a non-degenerate conic plus its nucleus, through which all the tangents of the conic pass. It is an important problem of finite algebraic geometry to classify all the ovals of the plane up to the group of collineations of PG(2, q), which is generated by PGL(3, q) and the h field automorphisms. For the theory of ovals see [3], [5], or [10].

Let the points of PG(2, q) be represented by homogeneous triples (i, j, k) over the finite field GF(q) in the usual way, and similarly let the lines be represented by dual coordinates $[r, s, t]$. Thus (i, j, k) is incident with $[r, s, t]$ if and only if $ir + js + kt = 0$. Consider the diagram in Figure 1.

An oval θ of PG(2, q) may be assumed to take the following form:

$$\theta = \{(0, 1, 0), (0, 0, 1)\} \cup \{(1, t, f(t)) \mid t \in \mathrm{GF}(q)\},$$

where $f(t)$ is a polynomial of degree at most $q-2$ over GF(q).

The condition that we shall find will determine whether or not $f(t)$ gives an oval in PG(2, q). The lines which do not pass through $(0, 1, 0)$ and $(0, 0, 1)$ intersect the oval in either 0 or 2 points ... an even number of points.

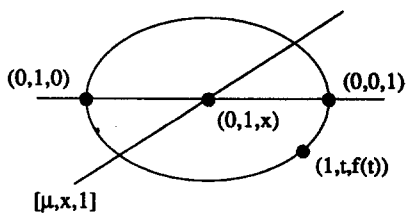

Fig. 1.

Geometriae Dedicata **32**: 247–252, 1989.
© 1989 *by Kluwer Academic Publishers. Printed in the Netherlands.*

LEMMA 1. *θ is an oval if and only if the $q^2 - q$ lines of* PG(2, q) *passing neither through* (0, 1, 0) *nor through* (0, 0, 1) *always intersect θ in an even number of points.*

Proof. If θ is an oval, then all lines of PG(2, q) intersect in 0 or 2 points and thus in an even number of points. Assume the converse. Consider one of the q points P of θ not equal to (0, 1, 0) or (0, 0, 1). Then the $q - 1$ lines which pass through P but not through (0, 1, 0) or (0, 0, 1) all contain at least one further point of θ. Since there *are* only $q - 1$ further points of θ, these $q - 1$ lines each contain exactly two points of θ. Thus $\theta\backslash\{(0, 1, 0)\}$ is a $(q + 1)$-arc. It remains to show that (0, 1, 0) is the nucleus of this $(q + 1)$-arc; i.e. it is the point through which all the tangents of the arc pass. That this is the case follows from the fact that no chords of $\theta\backslash\{(0, 1, 0)\}$ pass through (0, 1, 0), as we have seen above.

Next we find an algebraic condition that determines whether or not a polynomial always has an even number of solutions.

LEMMA 2. *Let $g(t)$ be a polynomial of* GF(q). *Then $g(t) = \mu$ has an even number of solutions $t \in$ GF(q) for all $\mu \in$ GF(q) if and only if the following holds:*

$$\sum g(\lambda)^r = 0 \text{ for all } r = 1, 2, \ldots, q - 1. \text{ (The sum is over all } \lambda \in \mathrm{GF}(q).)$$

Proof. The non-trivial part is to show that the above algebraic condition implies that $g(t) = \mu$ always has an even number of solutions. Let $\Omega = \{\mu | g(t) = \mu \text{ has an odd number of solutions}\}$. Then the sum of the above condition can be reduced to $\lambda \in \Omega$. Now Vandermonde's determinant implies that the vectors $(1, \mu, \mu^2, \ldots, \mu^{q-1})$ are linearly independent for different $\mu \in$ GF(q). However, the above condition implies that the sum of the vectors with $\mu \in \Omega$ is zero. Thus $\Omega = \emptyset$.

Now we convert the combinatorial condition on ovals to an algebraic one.

LEMMA 3. *The $q^2 - q$ lines of* PG(2, q) *passing neither through* (0, 1, 0) *nor through* (0, 0, 1) *always intersect θ in an even number of points if and only if the following condition holds:*

$$\sum (f(\lambda) + \lambda x)^r = 0 \text{ for all } r = 1, 2, \ldots, q - 1 \text{ and for all } x \in \mathrm{GF}(q),$$
$$\text{except } (x, r) = (0, q - 1), \text{ where the sum is over all } \lambda \in \mathrm{GF}(q).$$

Proof. A general line not passing through (0, 1, 0) or (0, 0, 1) has coordinates $[\mu, x, 1]$, $x \neq 0$. See Figure 1. The condition that this line contains a point $(1, t, f(t))$ of θ is $f(t) + tx = \mu$. Hence, for all $x \in \mathrm{GF}(q)\backslash\{0\}$, the equation above follows from Lemma 2. When x is zero, the fact that $f(t)$ is a permutation polynomial is equivalent to the above condition plus the fact that $f(t) = 0$ if and

only if $t = 0$. See [2] or [3] for a statement of Dickson's criterion. This is the case if θ is an oval, because the lines passing through $(0, 1, 0)$ each intersect θ in one further point.

We can now finally prove the main result.

THEOREM. *θ is an oval if and only if the following condition holds: the coefficient of t^a in $[f(t)]^b$ (modulo $t^q - t$) is zero, for all pairs of integers (a, b) with $1 \leqslant b \leqslant a \leqslant q-1, b \neq q-1$, and with the binary expansion of a containing the binary expansion of b. Thus $b \ll a$ below.*

This is just a generalization of the condition for oval functions t^k given in [3]. Also, the condition for $b = 1$ is just the condition of Segre and Bartocci [10], that all the powers of t are even.

Proof. Consider the condition of Lemma 3 with $r < q - 1$ as a polynomial in x. The binomial expansion, in the case of characteristic 2, is obtained via the binary partial order [3], which we denote here by the symbol $\ll$. Thus two integers u, v with $0 \leqslant u \leqslant q-1$ and $0 \leqslant v \leqslant q-1$ satisfy $u \ll v$, if and only if the binary expansion of u is 'dominated' by the binary expansion of v if and only if t^u occurs in the expansion of $(1 + t)^v$. Thus the condition with $r < q - 1$ becomes

$$\sum\left(\sum f(\lambda)^{r-s}\lambda^s x^s\right) = 0 \quad \text{for all } r = 1, 2, \ldots, q-2,$$

where the outer sum is over all $\lambda \in \mathrm{GF}(q)$ and the inner sum is over the integers s with $0 \leqslant s \ll r$. Since this is true for all x the coefficient of x^i is zero for all $0 \leqslant i \leqslant q-2$. Thus

$$\sum f(\lambda)^{r-i}\lambda^i = 0 \quad \text{for all } 0 \leqslant i \ll r \leqslant q-2, \text{ where the sum is over all } \lambda \in \mathrm{GF}(q).$$

The condition with $r = q - 1$ is

$$\sum\left(\sum f(\lambda)^{r-s}\lambda^s x^s\right) = 0 \quad \text{when } x \neq 0.$$

When $x = 0$, $\Sigma f(\lambda)^{q-1} = 1$, because $f(t)$ is a permutation polynomial and $\mu^{q-1} = 1$ if $\mu \neq 0$. Thus

$$\sum (f(\lambda) + \lambda x)^{q-1} = x^{q-1} - 1 \quad \text{for all } x \in \mathrm{GF}(q).$$

Considering the coefficient of x^i in this case gives

$$\sum f(\lambda)^{q-1} = \sum \lambda^{q-1} = 1, \quad \text{which is true anyway, and}$$

$$\sum f(\lambda)^{q-1-i}\lambda^i = 0 \quad \text{for all } 1 \leqslant i \leqslant q-2, \text{ where the sums are over all } \lambda \in \mathrm{GF}(q).$$

Putting the above conditions together we obtain

$$\sum f(\lambda)^{r-i}\lambda^i = 0 \quad \text{for all } 0 \leqslant i \leqslant r \leqslant q-1,$$
$$\text{and } (r,i) \neq (0,q-1) \text{ or } (q-1,q-1),$$
$$\text{where the sum is over all } \lambda \in \mathrm{GF}(q).$$

Thus the coefficient of t^{-i} in $f(t)^{r-i}$ is zero for these values of r and i. See, [2] or [3] for the evaluation of the coefficients of a polynomial. So the theorem has been proved.

COROLLARY 1. *If the coefficients of a polynomial are over a subfield of* GF(q), *we are able to determine, by evaluating the powers of* $f(t)$ *up to* $q-2$ *and by calculations only in that subfield, whether it is an oval polynomial. Also, since the condition for fixed* $b = k$ *implies the condition for fixed* $b = \alpha k$, *for all the* h *automorphisms* α *of* GF(q), *it is only necessary to calculate one of the powers of* $f(t)$ *in* $\{\alpha k \mid \alpha \in \mathrm{Aut}(\mathrm{GF}(q))\}$.

COROLLARY 2. *The condition with fixed* $b = 1$ *implies that all the terms of* $f(t)$ *have even degree. Since we may assume, without loss of generality, that* $f(0) = 0$, *i.e. that the constant term of* $f(t)$ *is zero, there are* $(q-2)/2$ *possible remaining non-zero coefficients. Thus the oval polynomials are mapped into the points of an algebraic variety of the coefficient space* PG($(q-4)/2, q$). *For example, in the case* $q = 8$ *it may be calculated that this variety is a non-degenerate conic plus nucleus in* PG(2, 8).

We now list all the known classes of ovals in PG($2, q$), q even, by their representative polynomials, together with references. Of course each oval yields many oval polynomials by varying the base points.

(a) x^2: the non-degenerate conic plus nucleus. Classical construction. See, e.g., [5].

(b) x^α: where $\alpha = 2^n$, and $(n, h) = 1$. Constructed by B. Segre. See [8].

(c) x^6: where h is odd. Constructed by B. Segre. See [9].

(d) A 'sporadic' oval in PG(2,16) that is contained in the union of two cubic curves, that are in the same syzygetic pencil [3]. The set of nine points of inflection in common with the two curves is contained in a Baer subplane that is fixed by the group of collineations of the oval. It was constructed by Lunelli and Sce by computer. See [4] and [6]. The author conjectures that general classes of ovals may be constructed by glueing together two cubic curves in a similar way. It may be shown that half the points of any non-degenerate cubic curve form an arc, by considering the abelian group of the curve.

(e) $x^{3\sigma+4}$: where h is odd, and $\sigma^2 \equiv 2 \pmod{q-1}$. Constructed by Glynn. See [3].

(f) $x^{\sigma+\gamma}$: where h is odd and $\gamma^4 \equiv 2 \pmod{q-1}$. Constructed by Glynn. See [3].

(g) $x^{1/6} + x^{1/2} + x^{5/6}$: where h is odd. Constructed by Payne. See [7].

(h)? $\mathrm{ch}(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$: where h is odd. This has been conjectured by W. E. Cherowitzo. Using a connection with the Suzuki–Tits ovoid of PG(3, q), S. E. Payne has shown that $\mathrm{ch}(x)$ is a permutation polynomial, and in joint work Payne and the author have shown that $\mathrm{ch}(x)/x$ is a permutation polynomial. These are necessary conditions that $\mathrm{ch}(x)$ be an oval polynomial and so support the conjecture. The proofs are unpublished at present.

Using the condition of the theorem, the author has written computer programs that have searched for oval polynomials in various planes. The programs were written in the 'C' language with Motorola 68020 assembly instructions to speed up the important operations, such as multiplying two polynomials. The following results have been obtained. The times taken give an indication of the complexity of the various problems. Let $\theta(q, q')$ denote the class of all oval polynomials in PG(2, q) with coefficients over the subfield GF(q') of GF(q).

- The classification of all oval polynomials t^k for $q = 2^h$, $h \leqslant 30$. No ovals, except for those in classes (a), (b), (c), (e), and (f) above, were found. The time for $h = 30$ was about a day.
- $\theta(32, 2)$: 30 seconds: the ovals all come from the known list above. This checks work by W. E. Cherowitzo [1].
- $\theta(64, 2)$: 4 hours: the only ovals are a conic plus nucleus.
- $\theta(64, 4)$: only a partial search was possible and no new ovals were found.

Note that it is possible to prove that an oval polynomial of $\theta(q, q')$, when reduced modulo $x^{q'} - x$, is congruent to a polynomial of $\theta(q', q')$. This knowledge can substantially reduce the size of a computer search.

REFERENCES

1. Cherowitzo, W. E., 'Hyperovals in Desarguesian Planes of Even Order' (to appear).
2. Dickson, L. E., *Linear Groups, with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.
3. Glynn, D. G., 'Two New Sequences of Ovals in Finite Desarguesian Planes of Even Order', in *Combinatorial Mathematics* X, *Springer Lecture Notes in Mathematics* **1036** (1983), 217–229.
4. Hall, M., Jr, 'Ovals in the Desarguesian Plane of Order 16', *Ann. Mat. Pura Appl.* (4) **102** (1975), 159–176.
5. Hirschfeld, J. W. P., *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1979.
6. Lunelli, L. and Sce, M., 'K-archi completi nei piani proiettivi desarguesiani di rango 8 e 16', Centro Calcoli Numerici, Politecnico di Milano, 1958.

7. Payne, S. E., 'A New Infinite Family of Generalized Quadrangles', *Congressus Numerantium* **49** (1985), 115–128.
8. Segre, B., 'Sui k-archi nei piani finiti di caratteristica due', *Revue Math. Pures Appl.* **2** (1957), 289–300.
9. Segre, B., 'Ovali e curve σ nei piani di Galois di caratteristica due', *Atti Accad. Naz. Lincei Rend.* (8) **32** (1962), 785–790.
10. Segre, B. and Bartocci, U., 'Ovali ed altre curve nei piani di Galois di caratteristica due', *Acta Arith.* **18** (1971), 423–449.

Author's address:

David G. Glynn,
University of Canterbury,
Department of Mathematics,
Private Bag, Christchurch 1,
New Zealand.

(Received, November 30, 1988; revised version, June 1, 1989)