

Finite Fourier Series and Ovals in $\text{PG}(2, 2^h)$

J. Chris Fisher
Department of Mathematics
University of Regina
Regina, Canada
S4S 0A2

Bernhard Schmidt
School of Physical & Mathematical Sciences
Nanyang Technological University
No. 1 Nanyang Walk, Blk 5, Level 3
Singapore 637616
Republic of Singapore

Abstract

We propose the use of finite Fourier series as an alternative means of representing ovals in projective planes of even order. As an example to illustrate the method's potential, we show that the set $\{w^j + w^{3j} + w^{-3j} : 0 \leq j \leq 2^h\} \subset \text{GF}(2^{2h})$ forms an oval if w is a primitive $(2^h + 1)^{\text{st}}$ root of unity in $\text{GF}(2^{2h})$ and $\text{GF}(2^{2h})$ is viewed as an affine plane over $\text{GF}(2^h)$. For the verification, we only need some elementary "trigonometric identities" and a basic irreducibility lemma that is of independent interest. Finally, we show that our example is the Payne oval when h is odd, and the Adelaide oval when h is even.

AMS Classification: 51E20 , 05B25

1 Introduction

In any finite projective plane of order q , an *oval* is a set of $q + 1$ points, no three of which are collinear. In the classical plane $\text{PG}(2, q)$ over $\text{GF}(q)$, a nondegenerate conic is the prototypical oval. If the order of a plane is even, then the tangents to an oval all pass through a point that is called the *nucleus of the oval*. We call an oval together with its nucleus a *hyperoval*. During the 1950s Beniamino Segre proved that in $\text{PG}(2, q)$,

1. when q is odd then there exist no ovals other than the conics, and

2. when $q = 2^h$ coordinates may be chosen so that the points of a hyperoval are the elements of the set

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

where f is a permutation polynomial of degree at most $q - 2$ for which $f(0) = 0$, $f(1) = 1$, and with the additional property that for all s in $\text{GF}(q)$, the function f_s defined by $f_s(0) := 0$ and $f_s(x) := [f(x + s) + f(s)]/x$ for $x \neq 0$ is a permutation polynomial.

The first result is a deep and surprising theorem, while the second is merely a simple observation that reduces the problem of finding examples of hyperovals to the problem of finding appropriate permutation polynomials. The first result in one stroke completely classified the ovals in planes coordinatized by a finite field of odd characteristic, while the second began a search for examples, a search whose ultimate goal is the classification of the ovals of projective planes over $\text{GF}(2^h)$. For the past 50 years the classification problem has inspired a lively research, with connections to number theory, group theory, and combinatorics as well as to geometry. Progress toward a classification has been surveyed in expository articles [1], [7] and [9]; recent progress has been so rapid that a web page [2] is maintained to report the latest discoveries.

From the start, the study of ovals has grown in step with progress in computational techniques – inspired ideas in combination with ever-faster computers. Perhaps such growth is reaching its limit. The latest examples of hyperovals have permutation polynomials whose presentation requires several lines of typescript. For example, a permutation polynomial for the Payne hyperovals, featured in our main theorem, is

$$f(x) = x^{\frac{5 \cdot 2^h - 4}{6}} + x^{2^{h-1}} + x^{\frac{2^h + 4}{6}}.$$

The permutation polynomial for the Adelaide hyperovals, which also come out of our theorem, is considerably more elaborate (see [2] or [3]). With perhaps further infinite families waiting to be discovered whose permutation polynomials are yet more formidable, the time is certainly ripe for an alternative approach. We propose here the use of finite Fourier series.

In the next two sections we introduce some background and provide a discussion of finite Fourier series to motivate our method of representing ovals. The theory remains in the background in this paper; our goal here is simply to introduce the technique. Only the notation and the lemma from section 2 are required for the main theorem in section 5, which provides an example of the method's effectiveness. Section 4 provides the main tools used in proving the theorem. In section 6 we identify our oval with two known families, and we use our representation to study the oval's automorphism group. The final section proposes some first steps of a possibly broader use of finite Fourier series in the study of hyperovals.

2 Representation of $\text{AG}(2, 2^h)$

In this section, we specify how we identify $\text{AG}(2, 2^h)$ with the field $\text{GF}(2^{2h})$ and state a criterion for collinearity using this representation.

Let h be a positive integer and write $q = 2^h$. Since $\text{GF}(q) \rightarrow \text{GF}(q), z \mapsto z^2 + z$ is a two-to-one mapping there is $\delta \in \text{GF}(q)$ with $z^2 + z \neq \delta \forall z \in \text{GF}(q)$. Hence the polynomial $z^2 + z + \delta$ is irreducible over $\text{GF}(q)$.

We associate the point (x, y) of the affine plane $\text{AG}(2, q)$ with the element $z = x + iy$ of $\text{GF}(q^2)$, where we have fixed i to be a root of a quadratic equation

$$z^2 + z + \delta = 0.$$

We call y the *imaginary part* or *y-coordinate* of z and denote it by $\Im(z)$. Since $i + 1$ is the second root of $z^2 + z + \delta$, the conjugate of i must be $i^q = i + 1$. Thus the conjugate of $z = x + iy$ is

$$z^q = (x + y) + iy. \tag{1}$$

For the verification of our main theorem, the following well known result is useful.

Lemma 1 *Considered as points of $\text{AG}(2, q)$, elements T, U, V of $\text{GF}(q^2)$ are collinear if and only if*

$$\Im(TU^q + UV^q + VT^q) = 0.$$

Proof Write $T = a + ib, U = c + id, V = e + if$. Then $\Im(TU^q + UV^q + VT^q) = bc + ad + de + cf + fa + eb$. Furthermore, T, U, V are collinear if and only if

$$\begin{vmatrix} c + a & e + a \\ d + b & f + b \end{vmatrix} = 0.$$

But this determinant equals $bc + ad + de + cf + fa + eb$. \square

3 Finite Fourier Series

It will be convenient to consider an oval of $\text{AG}(2, q)$ to be a particular type of $(q + 1)$ -gon: an *ordered* set of $q + 1$ points,

$$\mathbf{P} = (p_0, p_1, \dots, p_q)$$

with $p_i \in \text{GF}(q^2)$. In this way the oval \mathbf{P} is a vector in a $(q + 1)$ -dimensional vector space over $\text{GF}(q^2)$. More correctly, an oval is represented by $(q + 1)!$ vectors, one for each way of ordering its points. The advantage of using ordered point sets is that we may identify a *linear combination of point sets* with the linear combination of the corresponding vectors. Taking our cue from Fourier analysis, we see that a natural basis for this vector space will be the “regular $(q + 1)$ -gons”; the oval will be written as a linear combination of these basis elements, with the scalars being the associated finite Fourier coefficients. To define the regular $(q + 1)$ -gons, we fix w to be a primitive $(q + 1)^{st}$ root of unity in the field $\text{GF}(q^2)$. The powers of w will be points on a unit circle $(c(t), s(t))$, where we use the notation $c(t)$ and $s(t)$ to suggest their relationship to the cosine and sine functions; more precisely, we define $c(t)$ and $s(t)$ by

$$w^t = c(t) + is(t), \quad 0 \leq t \leq q.$$

Thus, using (1), we have

$$1 = w^t w^{qt} = [c(t) + is(t)][c(t) + s(t) + is(t)] = c^2(t) + c(t)s(t) + \delta s^2(t) \quad (2)$$

for every t . This means that the *unit circle* of $\text{AG}(2, q)$ consists of the points $(c(t), s(t))$ of the ellipse $x^2 + xy + \delta y^2 + 1 = 0$.

Definition 2 The k -regular $(q+1)$ -gon in $\text{AG}(2, q)$ is the ordered set

$$(1, w^k, w^{2k}, \dots, w^{qk}).$$

Thus, the k -regular $(q+1)$ -gon is the analogue of the regular polygon of the Euclidean plane whose vertices are points evenly spaced around the unit circle, with adjacent vertices subtending the angle $2k\pi/(q+1)$ at the center. Note that its vertices can be repeated; for example, the 0-regular 9-gon consists of the point 1 repeated nine times, while the 3-regular 9-gon is a 3-fold repeated triangle. What is relevant here is that the k -regular $(q+1)$ -gons form a basis for complex $(q+1)$ -space. This claim is actually a restatement of a standard and easily verified fact about finite Fourier series (see [11] or [12], for example). More precisely, for a $(q+1)$ -gon $\mathbf{P} = (p_0, p_1, \dots, p_q)$ there exists a unique set $\alpha_0, \dots, \alpha_q$ of $q+1$ elements of $\text{GF}(q^2)$, the *finite Fourier coefficients* of \mathbf{P} , so that

$$p_j = \sum_{k=0}^q \alpha_k w^{jk} \quad (3)$$

for $j = 0, \dots, q$. This is immediately clear since the coefficient matrix of (3), when considered as a system of linear equations in the unknowns $\alpha_0, \dots, \alpha_q$, is a nonsingular Vandermonde matrix. Furthermore, since

$$\sum_{j=0}^q w^{jt} = \begin{cases} 1, & \text{if } t \equiv 0 \pmod{q+1}, \\ 0 & \text{otherwise,} \end{cases}$$

we have

$$\begin{aligned} \alpha_k &= \sum_{r=0}^q \alpha_r \sum_{j=0}^q w^{j(r-k)} \\ &= \sum_{j=0}^q \left(\sum_{r=0}^q \alpha_r w^{jr} \right) w^{-jk} \\ &= \sum_{j=0}^q p_j w^{-jk}. \end{aligned} \quad (4)$$

The first hint that finite Fourier series might be applicable to the study of ovals was the observation that any ellipse of $\text{AG}(2, q)$, q even or odd, can be represented by the series whose j th point is

$$p_j = aw^j + bw^{-j} + c$$

where $a, b, c \in \text{GF}(q^2)$, $a^{q+1} \neq b^{q+1}$. This means that an ellipse has only three nonzero Fourier coefficients: $\alpha_0 = c$, $\alpha_1 = a$, $\alpha_q = b$. The element c is the center of gravity of the

$q + 1$ points of the ellipse. The condition $a^{q+1} \neq b^{q+1}$ avoids the situation where the $q + 1$ points are collinear. It is a straightforward exercise to confirm directly that these points satisfy the equation of an ellipse, although a deeper explanation is provided by the theory of affinely regular polygons (see [4], Theorem 2). The natural question is: Do other ovals have particularly nice Fourier representations?

We turned to the computer to find all ovals whose Fourier series have only three or four nonzero coefficients. It turned out that, up to affine transformations, all such ovals have the form $\mathbf{P} = (p_0, p_1, \dots, p_q)$ with

$$p_j = w^j + aw^{jk} + bw^{-jk}, \quad a, b \in \text{GF}(q^2), \quad k = 2, 3, \dots, q/2.$$

Only certain choices of a and b yield ovals. We found that for the planes $\text{AG}(2, q)$, $q = 8, 16, 32, 64, 128$, aside from conics, the only ovals we get in this way are

$$\mathcal{O}_r = \{w^j + w^{3j+2r} + w^{-3j-4r}, j = 0, \dots, q\}, \quad r = 0, 1, \dots, q. \quad (5)$$

Note that, for fixed q , the ovals \mathcal{O}_r , $r = 0, 1, \dots, q$, are all equivalent:

$$\begin{aligned} \mathcal{O}_r &= \{w^j + w^{3j+2r} + w^{-3j-4r}, j = 0, \dots, q\} \\ &= \{w^{j-r} + w^{3(j-r)+2r} + w^{-3(j-r)-4r}, j = 0, \dots, q\} \\ &= \{w^{-r}(w^j + w^{3j} + w^{-3j}), j = 0, \dots, q\} \\ &= w^{-r}\mathcal{O}_0. \end{aligned}$$

In fact, \mathcal{O}_0 is an oval in $\text{AG}(2, 2^h)$ for all h . To prove this we use a finite analogue of trigonometry.

4 Trigonometric Identities for $\text{GF}(2^{2h})$

We collect here the tools used in our proof of the main theorem. All one needs here from section 2 are the identities

$$i^2 = i + \delta, \quad (6)$$

$$w^t = c(t) + is(t), \quad (7)$$

$$\delta s^2(t) = 1 + c^2(t) + c(t)s(t) \quad (8)$$

From these we will derive a list of “trigonometric identities” followed by a brief verification. Our treatment follows [10], section 2, where further details can be found. An alternative approach to trigonometry by way of vectors is the subject of [6]. With a third approach, S.E. Payne and J.A. Thas [8] recently used such identities to help find the automorphism group of the Adelaide ovals.

Recall from section 2 that the domain of the functions $c(t)$ and $s(t)$ consists of the integers modulo 2^h+1 ; addition and multiplication of “angles” are reduced modulo 2^h+1 , so that $t/2$ always has a well-defined value.

Double and half angle formulas

$$c(2t) = 1 + c(t)s(t) \quad (9)$$

$$c^2(t/2) = \frac{1 + c^2(t)}{s(t)} \quad (10)$$

$$s(2t) = s^2(t) \quad (11)$$

$$s^2(t/2) = s(t) \quad (12)$$

Triple angle formulas

$$c(3t) = c(t) + s(t) + c(t)s^2(t) \quad (13)$$

$$s(3t) = s(t) + s^3(t) \quad (14)$$

Formulas involving angle sums and differences

$$c(t+u) = c(t)c(u) + s(t)s(u)\delta \quad (15)$$

$$s(t+u) = c(t)s(u) + c(u)s(t) + s(t)s(u) \quad (16)$$

$$c(t-u) = c(t)c(u) + c(t)s(u) + s(t)s(u)\delta \quad (17)$$

$$s(t-u) = s(t)c(u) + c(t)s(u) = s(u-t) = c(t-u) + c(u-t) \quad (18)$$

$$c(t)s(u) = c(t+u) + c(t-u) \quad (19)$$

$$c(t) + c(u) = c\left(\frac{t+u}{2}\right) s\left(\frac{t-u}{2}\right) \quad (20)$$

$$s(t)s(u) = s(t+u) + s(t-u) \quad (21)$$

$$s(t) + s(u) = s\left(\frac{t+u}{2}\right) s\left(\frac{t-u}{2}\right) \quad (22)$$

$$s(t)s(u)s(v) = s(t+u+v) + s(-t+u+v) + s(t-u+v) + s(t+u-v) \quad (23)$$

$$s(t) + s(u) + s(v) = s\left(\frac{t+u}{2}\right) s\left(\frac{u+v}{2}\right) s\left(\frac{v+t}{2}\right) + s(t+u+v) \quad (24)$$

Proof of (9) through (12)

$$w^{2t} \stackrel{(6)}{=} (c^2(t) + s^2(t)\delta) + s^2(t)i$$

$$\stackrel{(8)}{=} (1 + c(t)s(t)) + (s^2(t))i$$

This shows (9), (11) and (12). To get (10), we compute

$$\begin{aligned} c(t/2)^2 &\stackrel{(9)}{=} \left(\frac{c(t)+1}{s(t/2)}\right)^2 \\ &= \frac{c(t)^2 + 1}{s(t/2)^2} \\ &\stackrel{(12)}{=} \frac{c(t)^2 + 1}{s(t)} \end{aligned}$$

Proof of (13) and (14)

$$\begin{aligned} w^{3t} &\stackrel{(6)}{=} (c(t) + c^2(t)s(t) + s^3(t)\delta) + (s(t) + s^3(t))i \\ &\stackrel{(8)}{=} (c(t) + s(t) + c(t)s^2(t)) + (s(t) + s^3(t))i \end{aligned}$$

Proof of (15) through (24)

$$\begin{aligned} w^t w^u &= (c(t) + s(t)i)(c(u) + s(u)i) \\ &= (c(t)c(u) + s(t)s(u)\delta + (c(t)s(u) + c(u)s(t) + s(t)s(u))i) \\ \\ w^t w^{-u} &= w^t (w^u)^q \\ &= (c(t) + s(t)i)(c(u) + s(u) + s(u)i) \\ &= (c(t)c(u) + c(t)s(u) + s(t)s(u)\delta) + (s(t)c(u) + c(t)s(u))i \end{aligned}$$

This proves (15) through (18). The remaining identities follow from (15-18) and the observation $s(-t) = s(t)$ for all t . \square

We use the following notation:

$$f_\alpha := x^2 + x + \alpha \in \text{GF}(2^h)[x] \quad \text{for } \alpha \in \text{GF}(2^h).$$

Note that f_α is a two-to-one mapping on $\text{GF}(2^h)$ and thus $|f_\alpha(\text{GF}(2^h))| = 2^{h-1}$. The following is well known, see [5] section 1.4, (iii). For the convenience of the reader, we include a proof.

Lemma 3 *The polynomial $f_{\alpha+\beta}$ is irreducible over $\text{GF}(2^h)$ if and only if exactly one of f_α , f_β is irreducible over $\text{GF}(2^h)$.*

Proof The sufficiency of the conditions is obvious. Necessity: If both f_α and f_β have roots in $\text{GF}(2^h)$ then so has $f_{\alpha+\beta}$ and thus is reducible. If f_α and f_β are both irreducible then their images on $\text{GF}(2^h)$ both do not contain 0 and hence intersect. Thus there are $a, b \in \text{GF}(2^h)$ with $a^2 + a + \alpha = b^2 + b + \beta$, i.e. $(a+b)^2 + (a+b) + \alpha + \beta = 0$. This shows that $f_{\alpha+\beta}$ is reducible. \square

To prove our main theorem, we need one basic lemma, a result that seems to be of interest in its own right. In fact, it was observed also in [8] (cf. section 5), where the authors need it for computations similar to ours.

Lemma 4 *For any nonzero element s of $\text{GF}(2^h)$, the quadratic polynomial $z^2 + sz + 1$ is irreducible over $\text{GF}(2^h)$, if and only if s is the nonzero y -coordinate of a point of the unit circle $ww^q = 1$ in $\text{AG}(2, 2^h)$.*

Proof Note that $z^2 + sz + 1$ is irreducible over $\text{GF}(2^h)$ if and only if f_{1/s^2} is irreducible over $\text{GF}(2^h)$ (put $z = sx$). By Lemma 3, f_{1/s^2} is irreducible if and only if $f_{\delta+1/s^2}$ is reducible since f_δ is irreducible by the choice of δ . But $f_{\delta+1/s^2}$ is reducible if and only if $z^2 + sz + \delta s^2 + 1$ is reducible (put $x = z/s$). This is the case if and only if there is $c \in \text{GF}(2^h)$ with $c^2 + sc + \delta c^2 + 1 = 0$. By (2) this holds if and only if s is the nonzero y -coordinate of a point of the unit circle in $\text{AG}(2, 2^h)$. \square

5 The Main Theorem

Theorem 5 *The point set $\mathcal{O}_0 = \{w^j + w^{3j} + w^{-3j} : 0 \leq j \leq 2^h\}$ is an oval of $\text{AG}(2, 2^h)$ whose nucleus is the origin.*

Proof Write $p_j = w^j + w^{3j} + w^{-3j}$. Since $w^{3j} + w^{-3j} = (c(3j) + c(3j) + s(3j)) + (s(3j) + s(3j))i = s(3j)$, we have

$$p_j = c(j) + s(3j) + s(j)i. \quad (25)$$

Let $0 \leq t < u < v \leq 2^h$ be arbitrary. We have to show that p_t, p_u and p_v are not collinear. By Lemma 1 this is equivalent to

$$\Im(p_t p_u^q + p_u p_v^q + p_v p_t^q) \neq 0. \quad (26)$$

Note that, using (25),

$$\begin{aligned} \Im(p_j p_k^q) &= \Im[(c(j) + s(3j) + s(j)i)(c(k) + s(k) + s(3k) + s(k)i)] \\ &= c(j)s(k) + s(3j)s(k) + s(j)c(k) + s(j)s(3k). \end{aligned}$$

Hence the collinearity of p_t, p_u, p_v is equivalent to

$$\begin{aligned} &s(3t)[s(u) + s(v)] + s(3u)[s(t) + s(v)] + s(3v)[s(u) + s(t)] \\ &= c(t)[s(u) + s(v)] + c(u)[s(t) + s(v)] + c(v)[s(u) + s(t)] \end{aligned} \quad (27)$$

We must therefore show that (27) *never* holds. We first compute the left hand side of (27):

$$\begin{aligned} &s(3t)[s(u) + s(v)] + s(3u)[s(t) + s(v)] + s(3v)[s(u) + s(t)] \\ \stackrel{(14)}{=} &s^3(t)[s(u) + s(v)] + s^3(u)[s(t) + s(v)] + s^3(v)[s(u) + s(t)] \\ = &(s(t) + s(u))(s(t) + s(v))(s(u) + s(v))(s(t) + s(u) + s(v)) \\ \stackrel{(22),(24)}{=} &s\left(\frac{t+u}{2}\right)s\left(\frac{t-v}{2}\right)s\left(\frac{t+v}{2}\right)s\left(\frac{t-u}{2}\right)s\left(\frac{u+v}{2}\right)s\left(\frac{u-v}{2}\right)[s\left(\frac{t+u}{2}\right)s\left(\frac{u+v}{2}\right)s\left(\frac{v+t}{2}\right) + s(t+u+v)] \end{aligned}$$

Note $s(x) = 0$ if and only if $x \equiv 0 \pmod{2^h + 1}$. For the right hand side of (27) we get

$$\begin{aligned} &c(t)[s(u) + s(v)] + c(u)[s(t) + s(v)] + c(v)[s(u) + s(t)] \\ = &(c(t)s(u) + c(u)s(t)) + (c(u)s(v) + c(v)s(u)) + (c(v)s(t) + c(t)s(v)) \\ \stackrel{(18)}{=} &s(t-u) + s(u-v) + s(v-t) \\ \stackrel{(24)}{=} &s\left(\frac{t-u}{2}\right)s\left(\frac{u-v}{2}\right)s\left(\frac{v-t}{2}\right) + s(0) \\ = &s\left(\frac{t-u}{2}\right)s\left(\frac{u-v}{2}\right)s\left(\frac{v-t}{2}\right). \end{aligned}$$

Since $t < u < v$, the last product cannot equal zero, so (27) is equivalent to

$$s\left(\frac{t+u}{2}\right)s\left(\frac{t+v}{2}\right)s\left(\frac{u+v}{2}\right)[s\left(\frac{t+u}{2}\right)s\left(\frac{u+v}{2}\right)s\left(\frac{v+t}{2}\right) + s(t+u+v)] = 1 \quad (28)$$

Write $w = t + u + v$ and $z = s\left(\frac{t+u}{2}\right)s\left(\frac{t+v}{2}\right)s\left(\frac{u+v}{2}\right)$. Then (28) reads

$$z^2 + s(w)z + 1 = 0. \quad (29)$$

If $w \not\equiv 0 \pmod{2^h + 1}$, then (29) has no solution z by Lemma 4 since $s(w)$ is a nonzero y -coordinate of a point on the unit circle. Now assume $w \equiv 0 \pmod{2^h + 1}$. Then $s(u+v) = s(-t) = s(t)$, $s(v+t) = s(-u) = s(u)$ and thus

$$\begin{aligned}
z^2 &= [s(\frac{t+u}{2})s(\frac{t+v}{2})s(\frac{u+v}{2})]^2 \\
&\stackrel{(11)}{=} s(t+u)s(u+v)s(v+t) \\
&= s(t+u)s(t)s(u) \\
&\stackrel{(21)}{=} s(t+u)[s(t+u) + s(t-u)] \\
&= s^2(t+u) + s(t-u)s(t+u).
\end{aligned}$$

Since $s(t-u)$ is a nonzero y -coordinate of a point of the unit circle, Lemma 4 implies $z^2 \neq 1$. Since $s(w) = s(0) = 0$ this shows that (29) has no solution.

In summary, we have shown that (28) and hence (27) never holds. This completes the proof that \mathcal{O}_0 is an oval.

It remains to prove that 0 is the nucleus of \mathcal{O}_0 . Assume to the contrary that two points of the oval, p_t and p_u , are collinear with 0. Then (27) with $c(v) = s(v) = 0$ implies

$$\begin{aligned}
0 &= c(t)s(u) + c(u)s(t) + s(3t)s(u) + s(3u)s(t) \\
&\stackrel{(18),(14)}{=} s(t-u) + (s^3(t) + s(t))s(u) + s(t)(s^3(u) + s(u)) \\
&= s(t-u) + s(t)s(u)(s^2(t) + s^2(u)) \\
&= s(t-u) + s(t)s(u)(s(t) + s(u))^2 \\
&\stackrel{(21),(22)}{=} s(t-u) + (s(t+u) + s(t-u))s^2(\frac{t+u}{2})s^2(\frac{t-u}{2}) \\
&\stackrel{(11)}{=} s(t-u) + (s(t+u) + s(t-u))s(t+u)s(t-u) \\
&= s(t-u)(1 + s^2(t+u) + s(t-u)s(t+u)).
\end{aligned}$$

As we saw earlier in the proof, $1 + s^2(t+u) + s(t-u)s(t+u)$ cannot be zero and, of course, neither can $s(t-u)$. We therefore conclude that no two points of the oval can be collinear with 0, and the theorem is proved. \square

6 Payne and Adelaide ovals and their automorphism group

The ovals described in the previous section are not new. When h is odd they belong to the family discovered by Stanley Payne in 1985; when h is even they belong to the Adelaide family. This development comes as a double surprise: first it is somewhat surprising that what was believed to be two families turns out to be just one; second, it is very surprising that there should be such an easy description of these families. The Adelaide hyperovals in particular caused enormous difficulties, with nearly nine years separating their discovery by computer search in 1995 from the proof that they constitute an infinite family [3]. One can easily identify our ovals after having determined the equation their points must satisfy.

Lemma 6 *The points of the oval \mathcal{O}_0 satisfy the sixth degree equation*

$$y^6 + y^4 + xy + x^2 + \delta y^2 + 1 = 0$$

where δ is chosen as described in section 2.

Proof We saw in the proof of Theorem 5 that points of the oval are in the form $(x, y) = (c + s^3 + s, s)$ where c and s satisfy (8). Plugging $s = y$ and $c = x + y^3 + y$ into (8) produces the desired sixth degree equation. \square

If we replace x respectively y by x/z respectively y/z and multiply by z^6 we get our equation in projective coordinates:

$$y^6 + y^4 z^2 + z^4(xy + x^2 + \delta y^2) + z^6 = 0.$$

We prove that our oval belongs to the Payne and Adelaide families by showing that the sixth degree equation satisfied by the points of our oval is projectively equivalent to equations that had previously been obtained for the known families.

Theorem 7 *The hyperoval $\mathcal{O}_o \cup \{0\}$ is the Payne hyperoval when h is odd, and the Adelaide hyperoval when h is even.*

Proof When h is odd, we can take $\delta = 1$. The equation used by Thas, Payne and Gevaert in [13] to represent the Payne ovals is $v^6 = tu(t+u+v)^4$. Set $t = x+y$, $u = x$, and $v = y+z$ into their equation to reduce it to ours (with $\delta = 1$).

When h is even, to represent the Adelaide oval, Payne and Thas ([8], Lemma 5.1) used the equation $s^2 v^6 = (t+v)^4(t^2 + stu + u^2)$, where $s = w + w^{-1}$ and w is defined in our section 2. Set $t = y$, $u = sx$, and $v = y+z$ to reduce their equation to ours with $\delta = 1 + 1/s^2$.

It remains to show that $x^2 + x + 1 + s^{-2}$ is irreducible over $\text{GF}(2^h)$. We use the notation from Lemma 3. Note that $s = (c(1) + s(1)i) + (c(1) + s(1) + s(1)i) = s(1)$ is a nonzero y -coordinate of a point of the unit circle of $\text{AG}(2, 2^h)$. Thus, f_{1/s^2} is irreducible over $\text{GF}(2^h)$ by the proof of Lemma 4. Since h is even, f_1 is reducible over $\text{GF}(2^h)$. Now Lemma 3 implies that $x^2 + x + 1 + s^{-2} = f_{1+1/s^2}$ is indeed irreducible over $\text{GF}(2^h)$. \square

Our representation simplifies somewhat the task of determining the automorphism group of these hyperovals. It is clear that the automorphism $z \mapsto z^2$ of $\text{GF}(2^{2h})$ determines a collineation of the affine plane that permutes the points of the oval \mathcal{O}_0 . This field automorphism induces a cyclic collineation group of order $2h$ that preserves the oval. Note that $z \mapsto z^{2^h}$ can be viewed as complex conjugation in $\text{GF}(2^{2h})$; it represents an affine transformation in $\text{AG}(2, 2^h)$, namely the shear $(x, y) \mapsto (x + y, y)$. This shear and the identity are the only collineations in the stabilizer of the oval that belong to $\text{PGL}(3, 2^h)$; the other $2h - 1$ elements of the stabilizer belong to $\text{PGL}(3, 2^h) \setminus \text{PGL}(3, 2^h)$. To show that when $h \geq 5$ the ovals have no further automorphisms, the authors in [8] and [13] analyzed properties of the oval's sixth degree equation. The hard work lies in showing that the curve is absolutely irreducible. To achieve this goal a key observation, easily verified here, was that the nucleus $(x, y) = (0, 0)$ belongs to the hyperoval but does not satisfy the equation of the oval, while the point at infinity of the line $y = 0$ satisfies the projective equation (and therefore lies on the algebraic curve determined by the oval) but does not belong to the hyperoval.

7 Applications of Fourier series to the study of ovals

One can program a computer to find further examples of ovals with Fourier expansions that have most coefficients equal to zero or, perhaps, that are nice in some other way. Although it might be possible to provide a proof that the computer is finding further infinite families of ovals, this should not be the ultimate goal. More important would be finding a necessary and sufficient condition on the Fourier coefficients for a set of $q + 1$ points to form an oval. Here is a promising approach to that goal.

The first step might be to label the points of a given oval from 0 to q in a “canonical” way. Of the $(q + 1)!$ possible orders, it seems natural to place the nucleus at the origin and use the order inherited from the unit circle: define P_j to be the point of the oval on the line joining the origin to w^j .

Theorem 8 *Let q be a power of 2 and let w be a primitive $(q + 1)$ st root of unity in $\text{GF}(q^2)$. A set $\{p_0, p_1, \dots, p_q\}$ of $q + 1$ points in $\text{GF}(q^2) \setminus \{0\}$ is labeled so that p_j is on the line joining the origin to w^j if and only if the Fourier coefficients of the point set satisfy $\alpha_k = \alpha_{2-k}^q$ where the subscripts are taken modulo $q + 1$.*

Proof Let λ denote the generator of the multiplicative group of the small field $\text{GF}(q)$. Each nonzero element of $\text{GF}(q^2)$ can be uniquely written as $\lambda^b w^c$ for a pair of integers b, c satisfying $0 \leq b < q - 1$ and $0 \leq c < q + 1$. Note that the conjugate of $\lambda^b w^c$ is $(\lambda^b w^c)^q = \lambda^b w^{-c}$. A point p_j is on the line joining 0 to w^j if and only if

$$p_j = \lambda^{b_j} w^j \tag{30}$$

for some b_j , $0 \leq b_j < q - 1$. If (30) holds then (3) yields

$$\begin{aligned} \alpha_k &= \sum_j (\lambda^{b_j} w^j) w^{-jk} = \sum_j \lambda^{b_j} w^{-j(k-1)} \text{ and} \\ \alpha_{2-k} &= \sum_j (\lambda^{b_j} w^j) w^{-j(2-k)} = \sum_j \lambda^{b_j} w^{j(k-1)}. \end{aligned}$$

Thus $\alpha_k = \alpha_{2-k}^q$ as claimed.

Conversely, assume $\alpha_k = \alpha_{2-k}^q$ for all k . Write $\alpha_k = \lambda^{d_k} w^{c_k}$. Note that $2 - k$ runs through $0, -1, \dots, (2 - q)/2 \pmod{q + 1}$ when k runs through $2, 3, \dots, (q + 2)/2$. Also note

that $\alpha_1 \in \text{GF}(q)$ since $\alpha_1 = \alpha_{2-1}^q = \alpha_1^q$. This implies

$$\begin{aligned}
p_j &= \alpha_1 w^j + \sum_{k=0}^q \alpha_k w^{jk} \\
&= \alpha_1 w^j + \sum_{k=2}^{(q+2)/2} \alpha_k (w^{jk} + w^{j(2-k)}) \\
&= \alpha_1 w^j + \sum_{k=2}^{(q+2)/2} \lambda^{d_k} \left(w^{c_k+jk} + w^{-c_k+j(2-k)} \right) \\
&= w^j \left(\alpha_1 + \sum_{k=2}^{(q+2)/2} \lambda^{d_k} \left(w^{c_k+j(k-1)} + w^{-c_k-j(k-1)} \right) \right).
\end{aligned}$$

Since $\lambda, \alpha_1 \in \text{GF}(q)$ and $w^t + w^{-t} = w^t + w^{tq} \in \text{GF}(q)$ for all t , this implies $p_j = xw^j$ with $x \in \text{GF}(q)$. Hence (30) holds. \square

Observe that if 0 is the centroid of the points p_j (that is, $0 = \sum p_j$), then $\alpha_0 = \alpha_2 = 0$. Moreover, as we saw in the above proof, α_1 is in $\text{GF}(q)$: $\alpha_1 = \sum \lambda^{d_j}$. Note further that the theorem provides a necessary and sufficient condition for an arbitrary set of $q+2$ points to form a hyperoval: for each of the $q+2$ translations that take one of the given points to the origin, the Fourier series of the set formed by the remaining $q+1$ points has its coefficients paired (with $\alpha_k = \alpha_{2-k}^q$) if and only if the given p_j form a hyperoval. Unfortunately, to apply the theorem one must, for each choice of nucleus, label the remaining $q+1$ points in the appropriate order. There seems to be no obvious relationship among the $q+2$ resulting orderings. We do not yet know if there is a simple underlying pattern; nor do we know if there is some other condition that would enable Fourier series to provide a meaningful classification of ovals. Until such a condition is discovered, the use of Fourier series will be limited to searching for new families of ovals and, perhaps, shedding light on the known ovals.

Acknowledgment This paper was written while the first author was a guest at the University of Augsburg. He is grateful for the kind hospitality of Dieter Jungnickel and his colleagues. We thank Stan Payne and Gordon Royle for their help in identifying our oval.

References

- [1] W. Cherowitzo, Hyperovals in Desarguesian planes : an update, *Discrete Math.* **155** (1996), 31-38.
- [2] W. Cherowitzo, Hyperoval Web Page.
<http://www-math.cudenver.edu/~wcherowi/research/hyperoval/hypero.html>
- [3] W. E. Cherowitzo, C. M. O'Keefe, T. Penttila, A unified construction of finite geometries associated with q-clans in characteristic two. *Adv. Geom.* **3:1** (2003), 1-21.

- [4] J.C. Fisher and R.E. Jamison, Properties of affinely regular polygons, *Geom. Dedicata* **69**:3 (1998) 241-259.
- [5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1979.
- [6] S. Ilkka, *A trigonometric analysis of angles in finite Desarguesian planes*. Report-HTKK-Mat-A44 (Helsinki Univ. of Tech., Institute of Math., SF-02150 Otaniemi, Finland), 1974.
- [7] G. Korchmáros, Old and new results on ovals in finite projective planes, *Surveys in Combinatorics*, 1991 (Guildford, 1991), 41-72, LMS Lect. Note Ser., **166**, Cambridge Univ. Press, Cambridge, 1991.
- [8] S.E. Payne and Joseph A. Thas, The stabilizer of the Adelaide oval. Preprint (March, 2003).
- [9] T. Penttilä, Configurations of ovals. Combinatorics 2002 (Maratea). *J. Geom.* **76** (2003), no. 1-2, 233-255.
- [10] E.M. Schröder, Kreisgeometrische Darstellung metrischer Ebenen und verallgemeinerte Winkel- und Distanzfunktionen, *Abh. Math. Sem. Univ. Hamburg*, **42** (1974), 154-186.
- [11] I.J. Schoenberg, The finite Fourier series and elementary geometry. *Amer. Math. Monthly* **57** (1950), 390-404.
- [12] I.J. Schoenberg, *Mathematical Time Exposures*, Mathematical Association of America, Washington D.C., 1982.
- [13] J.A. Thas, S.E. Payne, H. Gevaert, A family of ovals with few collineations. *European J. Combin.* **9**:4 (1988), 353-362.