Geometric Codes and Hyperovals

Anton Betten
Department of Mathematics
Colorado State University
Fort Collins, CO 80523
U.S.A.

meinem Lehrer Reinhard Laue
zum 60-ten Geburtstag gewidmet

September 20, 2005

Abstract

We address the problem of constructing hyperovals and arcs in Desarguesian projective planes of even order. Our purpose is two-fold. On the one hand, we show the connection to geometric codes, which are the codes spanned by the characteristic vectors of subspaces of a fixed dimension in projective spaces. Using these codes, we deduce a new hyperoval condition. On the other hand, we investigate the question of determining whether or not a given arc can be extended to a hyperoval. To this end, we present two necessary conditions, one of them based on the new hyperoval condition, the other being an application of Hall's Marriage Theorem. Finally, we discuss the relevance of these results to computer searches for hyperovals in Desarguesian projective planes of small even orders.

1 Hyperovals in Projective Planes

Let $\mathrm{PG}(n,q)$ be the projective space of dimension n defined over the field $\mathbb{F}_q$, i.e. the set of subspaces of $\mathbb{F}_q^{n+1}$ ordered by inclusion. Subspaces of ordinary dimension 1, 2, 3, n are called (projective) points, lines, planes, and hyperplanes, respectively. We say that the projective dimension of a subspace is one less than the ordinary dimension as a vector subspace. Hence, projective points, lines, planes, hyperplanes are said to have projective dimension 0, 1, 2 and $n-1$, respectively. $\mathrm{PG}(2,q)$ is also known as the Desarguesian projective plane of order q. Let S be a set of points in $\mathrm{PG}(2,q)$. A line ℓ is called secant, tangent, external with respect to S if the size of $\ell \cap S$ is 2, 1 or 0, respectively. An *arc* in $\mathrm{PG}(2,q)$ is a set S of points, no three collinear. It is not hard to see that $|S| \leq q+2$. Equality can be reached when q is even, in which case S is called a *hyperoval*. A hyperoval admits no tangent lines, i.e. every line is either external or secant. Examples of hyperovals are the $q+1$ points of a conic together with its nucleus, which is the unique point where all tangent lines meet. This is known as the regular hyperoval. For $q \geq 16$, non-regular hyperovals exist.

For $n \geq 2$, the automorphism group of $\mathrm{PG}(n,q)$ is the group of all collineations, which is all the bijective mappings from points of $\mathrm{PG}(n,q)$ to points of $\mathrm{PG}(n,q)$ preserving collinearity (i.e. mapping collinear points to collinear points). It is known (see for instance Artin [1]) that this group is the group of all semilinear maps from $\mathbb{F}_q^{n+1}$ to $\mathbb{F}_q^{n+1}$. We denote this group as $\mathrm{P\Gamma L}(n+1,q)$, and call it the (full) projective group. We say that sets S and T of points of $\mathrm{PG}(n,q)$ are *projectively equivalent* if there exists a map $\gamma \in \mathrm{P\Gamma L}(n+1,q)$ sending S to T.

Clearly, the projective group maps hyperovals to hyperovals. We are interested in the essentially distinct types of hyperovals, i.e. hyperovals which are pairwise not equivalent. An important problem is the question of classifying hyperovals in projective planes $\mathrm{PG}(2,q)$ where $q = 2^h$. This problem has been solved for $h \leq 5$, cf. [9]. Several infinite families (in terms of h) are known. However, for $h \geq 6$, the classification is far from complete.

Let us choose homogeneous coordinates X, Y, Z for $\mathrm{PG}(2,q)$. It is known that any hyperoval can be brought into the form

$$\mathcal{O}_f = \{\langle (f(t), t, 1)\rangle \mid t \in \mathbb{F}_q\} \cup \{\langle (0,1,0)\rangle, \langle (1,0,0)\rangle\}$$

for some function f from $\mathbb{F}_q$ to $\mathbb{F}_q$. This means that for any hyperoval S we can find a semilinear map γ such that $\gamma(S) = \mathcal{O}_f$ for some f. The fact that we require that $\langle(0,1,0)\rangle$ and $\langle(1,0,0)\rangle$ are part of the hyperoval is not much of a restriction. Indeed, any arc consisting of at least 4 points is projectively equivalent to one containing the fundamental quadrangle $\langle(0,1,0)\rangle$, $\langle(1,0,0)\rangle$, $\langle(0,0,1)\rangle$ and $\langle(1,1,1)\rangle$. This is because the group $\mathrm{PGL}(3,q)$ is sharply transitive on ordered quadrangles.

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called an *oval-polynomial* if the set $\mathcal{O}_f$ as defined above is a hyperoval. It is easily seen that an oval-polynomial f is bijective. The name polynomial comes from the fact that any function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be thought of as a polynomial, such that the value of the function at any given point t equals the evaluation of that polynomial at t. See Theorem 3.1 for this.

An example for such a function f is the map $f(t) = t^2$. The corresponding hyperoval is the regular hyperoval which exists for any h. The points of the form $\langle(t^2,t,1)\rangle$ for $t \in \mathbb{F}_q$ together with $\langle(1,0,0)\rangle$ are the points of the conic with equation $XZ = Y^2$, the point $\langle(0,1,0)\rangle$ is the nucleus. If $q = 4$, this yields the 6 points

$$\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,1)\rangle, \langle(\alpha,\alpha^2,1)\rangle, \langle(\alpha^2,\alpha,1)\rangle,$$

where α is a root of $X^2 + X + 1$ over $\mathbb{F}_2$, i.e. $\alpha^2 = \alpha + 1$. It may be depicted as in Figure 1. The diagonal line is the "line at infinity" with equation $Z = 0$. The 4×4 grid represents the 16 points of the affine plane $Z \neq 0$. Notice that not every line in the projective space is shown in the figure. The horizontal lines should extend to the point $\langle(1,0,0)\rangle$ and the vertical lines should meet in $\langle(0,1,0)\rangle$. In addition, there should be an additional 4 lines through any of the remaining points at infinity. The affine points have coordinates $\langle(x,y,1)\rangle$ for $x, y \in \mathbb{F}_4$. More precisely, the intersection point of the vertical line through $\langle(x,0,1)\rangle$ and the horizontal line through $\langle(0,y,1)\rangle$ has the coordinates $\langle(x,y,1)\rangle$.

There are several known conditions for a function f to be an oval-polynomial. The most basic one is known as the *slope-condition*. It says that f is an oval-polynomial if and only if f is bijective, and in addition

$$\frac{f(x)+f(y)}{x+y} \neq \frac{f(x)+f(z)}{x+z}$$

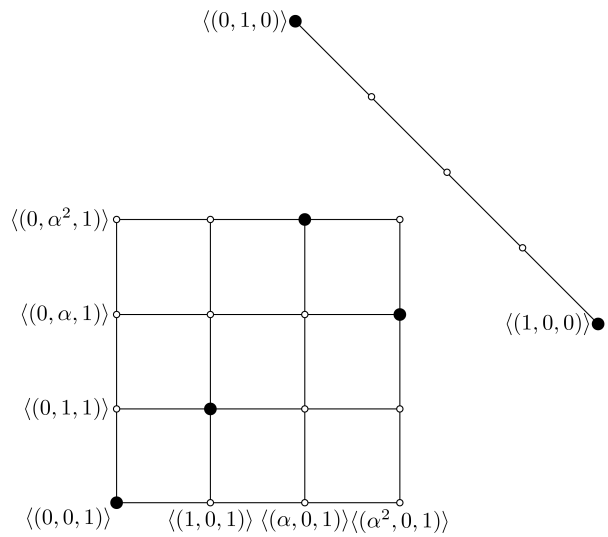

Figure 1: The Regular Hyperoval in $\mathrm{PG}(2,4)$

for all distinct $x, y, z \in \mathbb{F}_q$.

A necessary condition on the oval-polynomial f itself is due to Segre and Bartocci [10]. It states that the polynomial f is even, i.e. the coefficient of X^i is zero for i odd.

Important further necessary and sufficient conditions are due to Glynn [5, 6] (cf. Section 7).

2 Geometric Codes

Let us now present the theory of geometric codes following [7]. Consider a finite projective space $\mathrm{PG}(n,q)$. Let us introduce the Grassmannian of i-subspaces, denoted as

$$\mathbb{G}_i(n,q),$$

to be the set of i-dimensional projective subspaces of $\mathrm{PG}(n,q)$. We abbreviate

$$\theta_n(q) = |\mathbb{G}_0(n,q)| = \frac{q^{n+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^n.$$

Let $C(n,q)$ be the set of mappings from the (projective) points of $\mathrm{PG}(n,q)$ (i.e. from $\mathbb{G}_0(n,q)$) to $\mathbb{F}_q$. We can give the set $C(n,q)$ the structure of a $\mathbb{F}_q$ vector space by using componentwise addition of functions and scalar multiplication. The dimension of $C(n,q)$ as $\mathbb{F}_q$ vector space is $\theta_n(q)$.

A particular class of mappings are the *characteristic functions* of subsets $S \subseteq \mathbb{G}_0(n,q)$ which are defined as

$$\chi_S : \mathbb{G}_0(n,q) \to \mathbb{F}_q,\ \chi_S(P) = \begin{cases} 1 & \iff P \in S \\ 0 & \text{otherwise} \end{cases}$$

So, $\chi_S \in C(n,q)$ for all S but for $q > 2$ not every element of $C(n,q)$ is a characteristic function.

Let $q = p^h$, with p prime. For $i \leq n$, define the subspace

$$\mathcal{C}_i = \mathcal{C}_i(n,q) = \langle \chi_U \mid U \in \mathbb{G}_i(n,q) \rangle$$

of dimension $r_i := r_i(n,q) := \dim \mathcal{C}_i$. We call $\mathcal{C}_1$ the *line-code*, $\mathcal{C}_2$ the *plane-code* etc. A great deal of effort has been spent to compute the dimensions $r_i(n,q)$. The final answer has been given by Hamada [8], and is known as Hamada's formula. It states that

$$r_i(n,q) = \sum_S \prod_{j=0}^{h-1} \sum_{k=0}^{\left\lfloor \frac{s_{j+1}p - s_j}{p} \right\rfloor} (-1)^k \binom{n+1}{k} \binom{n + s_{j+1}p - s_j - kp}{n},$$

where the first sum is over all sequences $S = (s_0, \ldots, s_h)$ of $h+1$ integers s_j such that

$$s_h = s_0,\ i+1 \leq s_j \leq n+1,\ 0 \leq s_{j+1}p - s_j \leq (n+1)(p-1).$$

This result has been interpreted by Glynn and Hirschfeld [7] in terms of basis elements of geometric codes which are the topic of the current article. Also, Bardoe and Sin [2] have given a representation theoretic explanation of this formula.

For our purposes, the spaces which are dual to $\mathcal{C}_i$ (with respect to the standard bilinear form) are of interest:

For $i \leq n$, the *geometric code* of i-spaces is defined as

$$C_i(n,q) = \left\{ f \in C(n,q) \;\middle|\; \sum_{P \in U} f(P) = 0 \text{ for all } U \in \mathbb{G}_i(n,q) \right\}.$$

If n and q are understood, we simply write C_i for $C_i(n,q)$. We let $d_i := d_i(n,q)$ be the dimension of $C_i(n,q)$. Noting that $C_i = \mathcal{C}_i^{\perp}$, we have the dimension formula

$$d_i(n,q) = \theta_n(q) - r_i(n,q).$$

We call C_1 the *dual line-code*, C_2 the *dual plane-code* and so on.

Lemma 2.1 *We have the chain of subspaces*

$$\{\mathbf{0}\} = C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots \subseteq C_n \subseteq C(n,q),$$

where $\mathbf{0}$ *denotes the zero map which is zero on every point of* $\mathrm{PG}(n,q)$. *For the dimensions we have*

$$0 = d_0 \leq d_1 \leq \cdots \leq d_n = \theta_n(q) - 1 < \dim C(n,q) = \theta_n(q).$$

Proof. We show the inclusion $C_i \subseteq C_{i+1}$:

Let $f \in C_i$ and let U be an $(i+1)$-subspace. Inside U, pick an $(i-1)$-dimensional subspace V. Then U/V is two dimensional, and hence there are $q+1$ i-subspaces $W_1, \ldots, W_{q+1}$ in U containing V. These subspaces cover every point of $U \setminus V$ exactly once, whereas the points of V are in each of the W_j. Since $f \in C_i$ we deduce that

$$\sum_{P \in U} f(P) = \sum_{j=1}^{q+1} \underbrace{\sum_{P \in W_j} f(P)}_{=0} = 0,$$

i.e. $f \in C_{i+1}$. Notice that the terms $f(P)$, where $P \in V$, appear $q+1$ times in the second sum, i.e. we overcounted these function values q times. However, this does not change the value of the sum since $q \cdot a = 0$ for any $a \in \mathbb{F}_q$ in characteristic p.

As far as the statement about the dimensions is concerned, we note that the function $\mathbf{1}$ which is one at every point is contained in none of the C_i

(since $\theta_i = 1 + q + \ldots + q^i \equiv 1 \not\equiv 0 \bmod p$, where p is the characteristic of $\mathbb{F}_q$). In particular, C_n is a codimension-one subspace of $C(n,q)$ and $C(n,q)$ is generated by C_n and $\mathbf{1}$ together. $\square$

We remark that Glynn and Hirschfeld compute special cases of the dimensions d_i. For instance, they show that

$$d_1(n,4) = \frac{1}{3}(n+1)(n^2+2n+3). \tag{1}$$

The connection between hyperovals and geometric codes is explained easily. We first recall a result of Glynn [6]:

Lemma 2.2 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function (where $q = 2^h$). The following are equivalent:*

1. *$\mathcal{O}_f$ is hyperoval.*
2. *The $q^2 - q$ lines of $\mathrm{PG}(2,q)$ passing neither through $\langle(0,1,0)\rangle$ nor through $\langle(1,0,0)\rangle$ always intersect $\mathcal{O}_f$ in an even number of points.*

This implies the following.

Lemma 2.3 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function (where $q = 2^h$). The following are equivalent:*

1. *$\mathcal{O}_f$ is hyperoval.*
2. *$\chi_f \in C_1(2,q)$ (here, $\chi_f = \chi_{\mathcal{O}_f}$).*

Proof. Since hyperovals admit no tangent lines, the inner product

$$\left\langle \chi_f, \chi_\ell \right\rangle$$

is either zero or two for any line ℓ. Since we are in characteristic two, this means that χ_f is orthogonal to χ_ℓ for any line ℓ, i.e. that $\chi_f \in C_1(2,q)$.

Conversely, if $\chi_f \in C_1(2,q)$ then the $q^2 - q$ lines of $\mathrm{PG}(2,q)$ passing neither through $\langle(0,1,0)\rangle$ nor through $\langle(1,0,0)\rangle$ always intersect $\mathcal{O}_f$ in an even number of points. By Lemma 2.2, this implies that $\mathcal{O}_f$ is a hyperoval. $\square$

Summarizing, we are left with the problem of finding functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that the characteristic function $\chi_f = \chi_{\mathcal{O}_f}$ is an element of the dual line-code $C_1(2,q)$. In order to decide such questions, we need to develop the theory of geometric codes further. For this, we first need to express the elements of $C(n,q)$ as multivariate polynomials.

3 Function Theory on Projective Spaces

For sets A and B we denote by $\mathrm{map}(A, B)$ the set of mappings from A to B. If f and g are elements of $\mathrm{map}(A, B)$, we write $f \equiv g$ if $f(t) = g(t)$ for all $t \in A$. Also, for elements $g_1, \ldots, g_r$ of a ring R, we denote by $\mathrm{I}(g_1, \ldots, g_r)$ the ideal which is generated by the elements g_i, where $i = 1, \ldots, r$. Furthermore, we denote by $\mathbb{F}_q^\times$ the set of non-zero elements of the field $\mathbb{F}_q$. The following result is part of the folklore. The last three equations can be found in Glynn [5].

Theorem 3.1 *The homomorphism*

$$\varphi : \mathbb{F}_q[X] \to \mathrm{map}(\mathbb{F}_q, \mathbb{F}_q),\ f \mapsto \{t \mapsto f(t)\}$$

is surjective. Its kernel is the ideal which is generated by $X^q - X$. If f and g are polynomials in $\mathbb{F}_q[X]$ then

$$\varphi(f) \equiv \varphi(g) \iff f - g \in \mathrm{I}(X^q - X) \iff f \equiv g \mod X^q - X.$$

We call a polynomial reduced *if* $\deg(g) \leq q-1$. *Define the reduction function as follows: for $a = e(q-1) + s$ with $0 \leq s < q-1$, let*

$$r(a) = \begin{cases} 0 & \text{if } a = 0 \\ q-1 & \text{if } e > 0 \text{ and } a = e(q-1) \\ s & \text{otherwise} \end{cases}$$

If $f = \sum_i a_i X^i \in \mathbb{F}_q[X]$, then $g = \sum_i a_i X^{r(i)} \in \mathbb{F}_q[X]$ is the unique reduced polynomial $g \in \mathbb{F}_q[X]$ with $\varphi(f) \equiv \varphi(g)$. Let $f \in \mathrm{map}(\mathbb{F}_q, \mathbb{F}_q)$. The unique reduced polynomial g with $f \equiv \varphi(g)$ is $g = \sum_{i=0}^{q-1} a_i X^i$ with

$$\begin{aligned} a_0 &= f(0), \\ a_i &= -\sum_{s \in \mathbb{F}_q^\times} f(s) s^{-i},\ 1 \leq i \leq q-2, \\ a_{q-1} &= -\sum_{s \in \mathbb{F}_q} f(s). \end{aligned}$$

Next, we wish to express the elements of $C(n, q) = \mathrm{map}(\mathbb{G}_0(n, q), \mathbb{F}_q)$ as multivariate polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]$. The value of a point $P = \langle (z_0, \ldots, z_n) \rangle$ should be the value of the polynomial when we substitute $X_i =$

z_i. Of course, not every polynomial defines a function on projective space. In order to have a well-defined map, we need that the polynomial consists of monomials

$$c_{a_0,\ldots,a_n} X_0^{a_0} \cdots X_n^{a_n}$$

of degree divisible by $q-1$. Formally, if we write

$$f(X_0,\ldots,X_n) = \sum_{a_0,\ldots,a_n} c_{a_0,\ldots,a_n} X_0^{a_0} \cdots X_n^{a_n},$$

then $c_{a_0,\ldots,a_n} = 0$ unless $q-1$ divides $\sum_{i=0}^n a_i$.

Let S_n be the group of all permutations of the n-element set $\{0,1,\ldots,n-1\}$. This group is also known as the *symmetric group of degree* n. The group S_n acts on the polynomials in $\mathbb{F}_q[X_0,\ldots,X_{n-1}]$ as follows. For $\pi \in S_n$ and $f(X_0,\ldots,X_{n-1}) \in \mathbb{F}_q[X_0,\ldots,X_{n-1}]$ we set

$$\pi \cdot f(X_0,\ldots,X_{n-1}) = f(X_{\pi^{-1}(0)},\ldots,X_{\pi^{-1}(n-1)}).$$

A polynomial $f \in \mathbb{F}_q[X_0,\ldots,X_{n-1}]$ is said to be *symmetric* if $\pi \cdot f = f$ for all $\pi \in S_n$. Two classes of symmetric polynomials are as follows. The *elementary symmetric polynomial* of degree i is defined to be the sum of all products of i of the indeterminates, i.e.

$$\begin{aligned}
e_0 &= 1,\\
e_1 &= X_0 + \cdots + X_{n-1},\\
e_i &= \sum_{0 \le a_1 < a_2 < \cdots < a_i < n} X_{a_1} X_{a_2} \cdots X_{a_i},\\
e_n &= X_0 X_1 \cdots X_{n-1}.
\end{aligned}$$

A *partition* of an integer d is a weakly decreasing sequence of nonnegative integers

$$\lambda_0 \ge \lambda_1 \ge \cdots \ge \lambda_r$$

such that $\lambda_0 + \cdots + \lambda_r = d$. The λ_i are called the *parts* of the partition. We do not distinguish between partitions which differ only in the number of zeros in the end. Since the number of variables is fixed, we restrict ourselves to partitions $\lambda = (\lambda_0,\ldots,\lambda_{n-1})$ with at most n nonzero parts. For such a

partition λ, the *monomial symmetric polynomial* is the polynomial defined as

$$m_\lambda = \sum_{\alpha \sim \lambda} X^\alpha.$$

Here, α runs through all sequences of n integers which are rearrangements of λ. Also, we use the convention that for a sequence $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ we define X^α to be the monomial

$$X_0^{\alpha_0} \cdots X_{n-1}^{\alpha_{n-1}}.$$

Thus, the monomial symmetric polynomial for a partition λ of an integer d is a homogeneous polynomial of degree d. To simplify notation, let us denote a partition $\lambda = (\lambda_0, \ldots, \lambda_r)$ as

$$\lambda = (1^{m_1}, 2^{m_2}, \ldots),$$

where m_i is the number of parts of λ which are equal to i. We remark that the empty partition with no parts is denoted as $()$. The monomial symmetric polynomial indexed by the empty partition is by definition $m_{()} = 1$.

The following theorem is an extension of results which can be found in [7]. The description of the kernel in terms of generators seems to be new. Also, the expression of the function χ_P given here is a little simpler than the one presented in [7].

Theorem 3.2 *Let $\mathcal{R}_{n,q}^{(d)}$ be the set of polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]$ which are homogeneous of degree d. Let $\mathcal{F}_{n,q} = \oplus_i \mathcal{R}_{n,q}^{(i(q-1))}$ be the ring of polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]$ whose monomials are of degree a multiple of $q-1$. The homomorphism*

$$\psi_n : \mathcal{F}_{n,q} \to C(n,q), f \mapsto \{\langle (z_0, \ldots, z_n) \rangle \mapsto f(z_0, \ldots, z_n)\}$$

is well-defined and surjective. Let $\mathcal{I}_{n,q}$ be the ideal of $\mathcal{F}_{n,q}$ which is generated by the elements

$$(X_{i_1}^q - X_{i_1}) X_{i_2} \cdots X_{i_{q-1}},$$

for all choices of indices $0 \leq i_1, i_2, \ldots, i_{q-1} \leq n$ together with the element

$$\sum_{s=0}^{n+1} (-1)^s m_{((q-1)^s)}$$

with $m_{((q-1)^0)} = m_{()} = 1$. *Then* $\mathcal{I}_{n,q}$ *is the kernel of* ψ_n *and therefore we have that*

$$\psi_n(f) \equiv \psi_n(g) \iff f - g \in \mathcal{I}_{n,q}$$

for any two $f, g \in \mathcal{F}_{n,q}$. *A basis for* $C(n,q)$ *is given by the set*

$$\mathcal{B}_{n,q} = \left\{ \psi_n(X_0^{a_0} \cdots X_n^{a_n}) \middle| 0 \leq a_i \leq q-1, \text{ not all } a_i = 0, (q-1) \mid \sum_{i=0}^{n} a_i \right\}$$

The polynomials which are in the linear span of $\mathcal{B}_{n,q}$ *are said to be* reduced. *A different basis of* $C(n,q)$ *is given by the characteristic functions of points: for a point* $P = \langle (z_0, \ldots, z_n) \rangle \in \mathrm{PG}(n,q)$ *and an index* j *for which* $z_j \neq 0$, χ_P *can be written as*

$$\chi_P = \psi_n \left(\prod_{i \in \{0,1,\ldots,n\} \setminus \{j\}} \left(1 - (z_j X_i - z_i X_j)^{q-1}\right) \right).$$

Notice that this expression for χ_P *is usually not reduced.*

Proof. The relations of the form $(X_{i_1}^q - X_{i_1}) X_{i_2} \cdots X_{i_{q-1}}$ are homogeneous of degree $2(q-1)$ and therefore lie in $\mathcal{F}_{n,q}$. They are elements of the kernel of ψ_n since

$$\begin{aligned} & \psi_n((X_{i_1}^q - X_{i_1}) X_{i_2} \cdots X_{i_{q-1}}) \equiv 0 \\ \iff \quad & \psi_n(X_{i_1}^q X_{i_2} \cdots X_{i_{q-1}}) \equiv \psi_n(X_{i_1} X_{i_2} \cdots X_{i_{q-1}}) \end{aligned}$$

which is clearly true. Next, we show that $\psi_n(\sum_{s=0}^{n+1} (-1)^s m_{((q-1)^s)}) \equiv 0$. To this end, let $P = \langle (z_0, \ldots, z_n) \rangle$ be any point. Let $0 \leq i_1 < i_2 < \cdots < i_k \leq n$ be the set of indices with $z_{i_j} \neq 0$ for $j = 1, \ldots, k$. Then $m_{((q-1)^s)}(z_0, \ldots, z_n) = 0$ for $s > k$. Otherwise, if $s \leq k$ then

$$m_{((q-1)^s)}(z_0, \ldots, z_n) = \binom{k}{s}$$

since $z^{q-1} = 1$ for any $z \in \mathbb{F}_q^\times$. Therefore,

$$\sum_{s=0}^{n+1} (-1)^s m_{((q-1)^s)}(z_0, \ldots, z_n) = \sum_{s=0}^{k} (-1)^s \binom{k}{s} = 0.$$

This shows that $\mathcal{I}_{n,q} \leq \ker \psi_n$. Looking at the set $\mathcal{B}_{n,q}$ shows that the given elements are linearly independent modulo $\mathcal{I}$. Since the size of $\mathcal{B}_{n,q}$ is $(q^{n+1} - 1)/(q-1) = \theta_n(q) = \dim C(n,q)$, we must have $\mathcal{I}_{n,q} = \ker \psi_n$.

Next, we verify that χ_P is indeed the characteristic function of the point $P = \langle (z_0, \ldots, z_n) \rangle$. For this, let $Q = \langle (x_0, \ldots, x_n) \rangle$ be any point of $\mathrm{PG}(n,q)$. Recall that j is chosen such that $z_j \neq 0$. Then

$$\begin{aligned} z_j x_i - z_i x_j = 0 &\iff z_j x_i = z_i x_j \\ &\iff \begin{cases} \exists \lambda \in \mathbb{F}_q : \ x_i = \lambda z_i \wedge x_j = \lambda z_j \\ \text{or} \quad x_i = z_i = 0 \end{cases} \end{aligned}$$

so that

$$1 - (z_j x_i - z_i x_j)^{q-1} = \begin{cases} 1 & \text{if} \begin{cases} \exists \lambda \in \mathbb{F}_q : \ x_i = \lambda z_i \wedge x_j = \lambda z_j \\ \text{or} \quad x_i = z_i = 0 \end{cases} \\ 0 & \text{otherwise} \end{cases}$$

and therefore

$$\begin{aligned} &\prod_{i \in \{1,\ldots,n\} \setminus \{j\}} \left(1 - (z_j x_i - z_i x_j)^{q-1}\right) \\ &\qquad = \begin{cases} 1 & \text{if} \begin{cases} \exists \lambda \in \mathbb{F}_q : \ x_i = \lambda z_i \ \forall i \\ \text{or} \quad x_i = z_i = 0 \ \forall i \neq j \end{cases} \\ 0 & \text{otherwise} \end{cases} \\ &\qquad = \begin{cases} 1 & \text{if } \exists \lambda \in \mathbb{F}_q^\times : Q = \lambda P \text{ or } Q = \langle (0, \ldots, 0) \rangle \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

But $Q = \langle (0, \ldots, 0) \rangle$ cannot happen and $Q = \lambda P$ for $\lambda \neq 0$ means that P and Q are the same projective point. This proves that χ_P is indeed the characteristic function of the point P. $\square$

We remark that is is common practice to omit reference to the functions φ and ψ_n, respectively. Thus one simply identifies the elements of the corresponding polynomial factor ring with the functions they induce on $\mathrm{PG}(n,q)$. From now on, we will do the same. We then write $f \equiv g$ for polynomials f and g if $f - g$ is in the kernel of the corresponding map, i.e. if $f(a) = g(a)$ for all a in the domain.

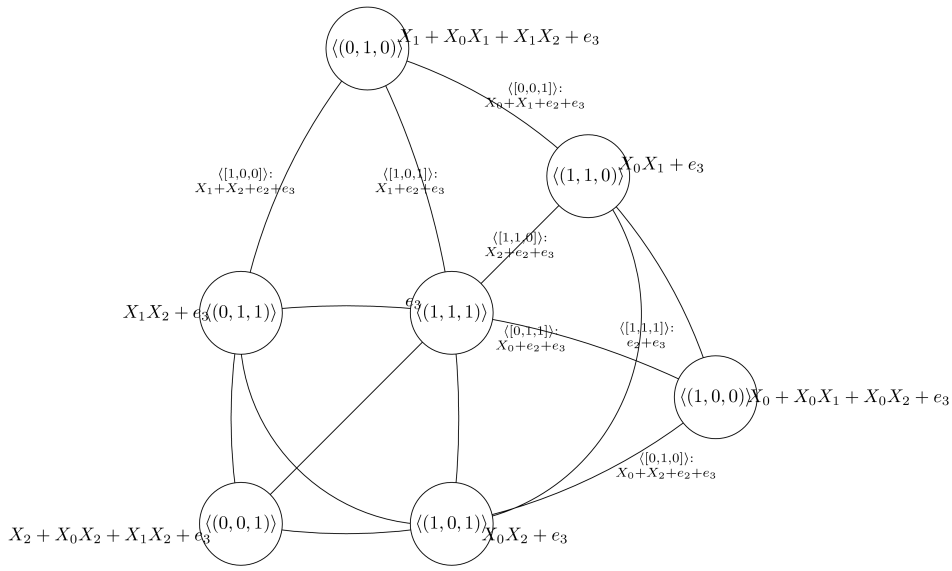

Figure 2: The Characteristic Functions of Points and Lines in $\mathrm{PG}(2,2)$

As an application of the previous theorem, we consider the characteristic functions of points and lines in the projective plane of order 2, see Fig. 2. Here, we denote by $\langle[u,v,z]\rangle$ the line $\{\langle(x,y,z)\rangle \mid xu+yv+zw=0\}$.

The following result due to Delsarte [3] describes the elements in $C_i(n,q)$. The result has been reformulated by Glynn and Hirschfeld in [7], who have translated it into the language of polynomial functions. It is this version which we present here.

Theorem 3.3 *1. A function $\psi \in C(n,q) = \mathrm{map}(\mathbb{G}_0(n,q),\mathbb{F}_q)$ is in $C_i(n,q)$ if and only if it can be written as a sum of monomials, with coefficients in $\mathbb{F}_q$, all of which are in $C_i(n,q)$.*

2. A monomial $t = X_0^{a_0}\cdots X_n^{a_n}$ with $\sum_j a_j \neq 0$ is in $C_i(n,q)$ if and only if there exists an integer j, with $0 \leq j \leq h-1$, such that the degree of t^{p^j} is $d(q-1)$, where $1 \leq d \leq i$, and where the terms in the X_i are reduced via $X_i^q = X_i$.

Let us consider the regular hyperoval in $\mathrm{PG}(2,4)$, for example. Of course, we already know that $f(t) = t^2$ is an oval-polynomial, but we may verify this fact in a different manner. Adding up the characteristic functions of points of $\mathcal{O}_f$ we obtain after some calculations

$$\begin{aligned}
\chi_f &= \sum_{P \in \mathcal{O}_f} \chi_P \\
&= \chi_{\langle(1,0,0)\rangle} + \chi_{\langle(0,1,0)\rangle} + \chi_{\langle(0,0,1)\rangle} + \chi_{\langle(1,1,1)\rangle} + \chi_{\langle(\alpha,\alpha^2,1)\rangle} + \chi_{\langle(\alpha^2,\alpha,1)\rangle} \\
&= X_0^3 + X_1^3 + X_2^3 + X_0X_1X_2 + X_0^2X_1^2X_2^2 \\
&= m_{(3)} + m_{(1^3)} + m_{(2^3)}.
\end{aligned}$$

By Lemma 2.3, we must have $m_{(3)} + m_{(1^3)} + m_{(2^3)} \in C_1(2,4)$. We apply Theorem 3.3 and look at the (reduced) monomials of χ_f. Since

$$(\deg X_i^3)/3 = 1$$

we have $X_i^3 \in C_1(2,4)$ for all i. Since

$$(\deg X_0X_1X_2)/3 = 1$$

we also have $X_i^3 \in C_1(2,4)$. Now we have

$$(\deg X_0^2X_1^2X_2^2)/3 = 2.$$

However,

$$(X_0^2X_1^2X_2^2)^2 = X_0^4X_1^4X_2^4 \equiv X_0X_1X_2$$

and this monomial is in $C_1(2,4)$ as we have seen. Therefore we find that indeed $\chi_f \in C_1(2,4)$.

4 The Hyperoval Condition

Theorem 4.1 *Let f be a map from $\mathbb{F}_q$ to $\mathbb{F}_q$, where $q = 2^h$. Let $\chi_f \in C(2,q)$ be the characteristic function of $\mathcal{O}_f$. Label the points of $\mathrm{PG}(2,q)$ as $P_1, \ldots, P_{q^2+q+1}$. We may think of χ_f as a vector $(x_1, \ldots, x_{q^2+q+1})$ with entries $x_j = 1$ if $P_j \in \mathcal{O}_f$ and $x_j = 0$ otherwise. Let $t_1, \ldots, t_m$ be a list of all reduced monomials $t_i = t = X_0^{a_0}X_1^{a_1}X_2^{a_2}$ with $t \notin C_1(2,q)$. Let $A = (a_{i,j})$ be the $m \times \theta_2(q)$-matrix over $\mathbb{F}_q$ with entries*

$$a_{i,j} = [t_i]\chi_{P_j},$$

i.e. the coefficient of t_i in the characteristic function of the j-th point (after reduction). Then f is an oval-polynomial if and only if

$$A \cdot \chi_f^\top = 0^\top. \tag{2}$$

Using an $\mathbb{F}_2$-basis of $\mathbb{F}_q$, it is possible to rewrite the system (2) over $\mathbb{F}_2$.

Proof. By Lemma 2.3, f is an oval-polynomial if and only if $\chi_f \in C_1(2,q)$. By Theorem 3.3, this is if and only if $[t]\chi_f = 0$ for each $t \notin C_1(2,q)$, i.e. if and only if $A \cdot \chi_f^\top = 0^\top$. □

We remark that $m = \theta_2(q) - d_1(2,q)$.

As an example, we consider the regular hyperoval in PG(2, 4). At first, we list the reduced monomials $t \notin C_1(2,4)$. From the previous remark and (1) we know that the number of such monomials is $m = \theta_2(4) - d_1(2,4) = 21 - 11 = 10$. Indeed, we find 10 such monomials $X_0^{a_0} X_1^{a_1} X_2^{a_2}$, where (a_0, a_1, a_2) is as in Table 1. Next, we enumerate all points $P_j = \langle (x,y,z) \rangle$ of PG(2, 4). They

i	(a_0, a_1, a_2)
1	$(3,3,0)$
2	$(3,2,1)$
3	$(2,3,1)$
4	$(3,1,2)$
5	$(1,3,2)$
6	$(3,0,3)$
7	$(2,1,3)$
8	$(1,2,3)$
9	$(0,3,3)$
10	$(3,3,3)$

Table 1: The Monomials $X_0^{a_0} X_1^{a_1} X_2^{a_2}$ not in $C_1(2,4)$

are shown in Table 2. Evaluating the characteristic functions χ_{P_j} of points P_j and picking out the coefficients of the monomials $t_i = X_0^{a_0} X_1^{a_1} X_2^{a_2}$ with t_i

j	P_j	j	P_j
1	$\langle(1,0,0)\rangle$	11	$\langle(0,1,1)\rangle$
2	$\langle(0,1,0)\rangle$	12	$\langle(\alpha,1,1)\rangle$
3	$\langle(0,0,1)\rangle$	13	$\langle(\alpha^2,1,1)\rangle$
4	$\langle(1,1,1)\rangle$	14	$\langle(0,\alpha,1)\rangle$
5	$\langle(1,1,0)\rangle$	15	$\langle(1,\alpha,1)\rangle$
6	$\langle(\alpha,1,0)\rangle$	16	$\langle(\alpha,\alpha,1)\rangle$
7	$\langle(\alpha^2,1,0)\rangle$	17	$\langle(\alpha^2,\alpha,1)\rangle$
8	$\langle(1,0,1)\rangle$	18	$\langle(0,\alpha^2,1)\rangle$
9	$\langle(\alpha,0,1)\rangle$	19	$\langle(1,\alpha^2,1)\rangle$
10	$\langle(\alpha^2,0,1)\rangle$	20	$\langle(\alpha,\alpha^2,1)\rangle$
		21	$\langle(\alpha^2,\alpha^2,1)\rangle$

Table 2: The Labeling of Points of $\mathrm{PG}(2,4)$

in the list, we obtain the system

$$\begin{pmatrix}
1&1&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&1&1&\alpha&\alpha&\alpha&\alpha&\alpha^2&\alpha^2&\alpha^2&\alpha^2\\
0&0&0&1&0&0&0&1&\alpha&\alpha^2&0&\alpha&\alpha^2&0&1&\alpha&\alpha^2&0&1&\alpha&\alpha^2\\
0&0&0&1&0&0&0&0&0&0&1&1&1&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha&\alpha&\alpha&\alpha\\
0&0&0&1&0&0&0&1&\alpha^2&\alpha&0&\alpha^2&\alpha&0&1&\alpha^2&\alpha&0&1&\alpha^2&\alpha\\
1&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&\alpha&\alpha^2&0&0&0&0&\alpha&\alpha^2&0&\alpha^2&1&\alpha&0&\alpha&\alpha^2&1\\
0&0&0&1&1&\alpha^2&\alpha&0&0&0&0&\alpha^2&\alpha&0&\alpha&1&\alpha^2&0&\alpha^2&\alpha&1\\
0&1&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}\cdot\chi_f^\top=0^\top.$$

Using the $\mathbb{F}_2$-basis $(1, \alpha)$, we rewrite the system over $\mathbb{F}_2$. This gives

$$\begin{pmatrix}
1&1&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&1&0&0&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&1&0&0&0&1&1&0&0&1&0&0&1&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0&0&1&1\\
1&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&1&0&0&0&0&0&1&0&1&1&0&0&0&1&1\\
0&0&0&0&0&1&1&0&0&0&0&1&1&0&1&0&1&0&1&1&0\\
0&0&0&1&1&1&0&0&0&0&0&1&0&0&0&1&1&0&1&0&1\\
0&0&0&0&0&1&1&0&0&0&0&1&1&0&1&0&1&0&1&1&0\\
0&1&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix} \cdot \chi_f^\top = 0^\top.$$

Row reduction leads to

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&1\\
0&0&1&0&0&0&0&0&0&1&1&0&1&0&1&1&0&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&1&0&0&0&0&1&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&1&1&1&0&1&1&1&0&0&1&0\\
0&0&0&0&0&0&1&0&0&1&1&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&0&1&1&0&1&0\\
0&0&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1
\end{pmatrix} \cdot \chi_f^\top = 0^\top.$$

The function $f : t \mapsto t^2$ is an oval-polynomial, since $\chi_f = (x_1, \ldots, x_{21})$ with $x_1 = x_2 = x_3 = x_4 = x_{17} = x_{20} = 1$ and all other $x_j = 0$ is a solution of (2). The points P_j with $j = 1, 2, 3, 4, 17$ and 20 are just the points of $\mathcal{O}_f$, i.e.

$$\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,1)\rangle, \langle(\alpha^2,\alpha,1)\rangle, \langle(\alpha,\alpha^2,1)\rangle.$$

5 Which Arcs Can Be Completed?

A big problem during the classification of hyperovals is the large number of arcs which do not complete to a hyperoval. In this section, we derive two tests which allow to decide whether an arc can be completed or not. The first one is based on Theorem 4.1. We assume that we are searching for hyperovals by means of the oval-polynomial f. We think of f as a partially defined function, whose domain is a set $D \subseteq \mathbb{F}_q$. Hence we are working not with $\mathcal{O}_f$ but rather with the set

$$\mathcal{O}_{f,D} = \{\langle(f(t), t, 1)\rangle \mid \ t \in D\} \cup \{\langle(0, 1, 0)\rangle, \langle(1, 0, 0)\rangle\}$$

of size $|D| + 2$. We always require that $\mathcal{O}_{f,D}$ is an arc. We express this by saying that f is a *partial oval-polynomial.* We may even assume that $\{0, 1\} \subseteq D$ and $f(0) = 0$ and $f(1) = 1$. Of course, $\mathcal{O}_{f,\mathbb{F}_q} = \mathcal{O}_f$. We say that an arc $\mathcal{O}_{f,D}$ *completes* if the domain of f can be extended to all of $\mathbb{F}_q$, i.e. if there is an arc $\mathcal{O}_{f,\mathbb{F}_q} = \mathcal{O}_f$. Of course, this is equivalent to saying that f can be completed to an oval-polynomial. Let us introduce some notation. For a matrix A and for sets X and Y of row and column indices of A, we denote by $A_{X,Y}$ the submatrix of A which is formed by intersecting the rows with indices in X with the columns indexed by elements of Y. We write $A_{*,Y}$ for the matrix formed by the columns indexed by Y.

Lemma 5.1 (Test 1)
Let $q = 2^h$ and let f be a partial oval-polynomial with domain $D \subseteq \mathbb{F}_q$. Let $\chi_{f,D}$ be the characteristic vector of the arc $\mathcal{O}_{f,D}$. Furthermore, let $\mathcal{S}$ be the set of points which are either in $\mathcal{O}_{f,D}$ or which lie on a secant line of $\mathcal{O}_{f,D}$. Let $\overline{\mathcal{S}}$ be the complement of $\mathcal{S}$ in $\mathbb{G}_0(2, q)$. A necessary condition for completing $\mathcal{O}_{f,D}$ to a hyperoval is the solvability of the $\mathbb{F}_q$-linear inhomogeneous system

$$A_{*,\overline{\mathcal{S}}} \cdot y^\top = A \cdot \chi_{f,D}^\top \tag{3}$$

with a $\{0, 1\}$-vector y, whose entries are indexed by the elements of $\overline{\mathcal{S}}$. Using an $\mathbb{F}_2$ base for $\mathbb{F}_q$, the system (3) may be written as an $\mathbb{F}_2$-linear inhomogeneous system.

Proof. If f completes, then we have $\chi_f = \chi_{f,D} + z$ where z is some $0, 1$-vector whose support is disjoint from the support of $\chi_{f,D}$. Indeed, we know that the support of z is disjoint from $\mathcal{S}$. Therefore (2) becomes

$$A \cdot \chi_f^\top = A \cdot (\chi_{f,D}^\top + z^\top) = 0,$$

which is equivalent to $A \cdot z^\top = A \cdot \chi_{f,D}^\top$ since we are in characteristic two. Let $y = z_{\overline{\mathcal{S}}}$ be the restriction of z to the entries not in $\mathcal{S}$. The condition now follows by restricting A to the columns in $\overline{\mathcal{S}}$. $\square$

Another test can be derived as follows. Again, we assume that f has been defined on a subset $D \subseteq \mathbb{F}_q$ and that $\mathcal{O}_{f,D}$ is an arc. Also, let $\mathcal{S}$ be the set of points of $\mathcal{O}_{f,D}$ together with the points on secants of $\mathcal{O}_{f,D}$. Let M be the $q \times q$ matrix $M = (m_{y,x})$ whose rows and columns are indexed by elements y and x from $\mathbb{F}_q$. The entries of M correspond to the points $\langle (x, y, 1) \rangle$ of the affine plane $\mathrm{AG}(2, q)$ which results from removing the line $Z = 0$ from $\mathrm{PG}(2, q)$. Fix an ordering of the elements of $\mathbb{F}_q$ and let

$$m_{y,x} = \begin{cases} 0 & \text{if } \langle (x, y, 1) \rangle \in \mathcal{S} \\ 1 & \text{otherwise} \end{cases}$$

Let $E = f(D)$. Let $\overline{D}$ and $\overline{E}$ be the complements of the sets D and E in $\mathbb{F}_q$, respectively. The matrix $M_{\overline{D},\overline{E}}$ defines a bipartite graph Γ as follows. The vertex set of Γ is the disjoint union of the sets $\overline{D}$ and $\overline{E}$. To make the sets disjoint, we form cartesian products with the symbols 1 and 2, respectively. Thus we let the vertices be $\mathcal{V}(\Gamma) = (\overline{D} \times \{1\}) \cup (\overline{E} \times \{2\})$. The set of edges is

$$\mathcal{E}(\Gamma) = \{(y \times \{1\}, x \times \{2\}) \mid y \in \overline{D},\ x \in \overline{E},\ m_{y,x} = 1\}.$$

A *matching* of Γ is a set of edges such that each vertex is incident with exactly one edge of the matching. A necessary and sufficient condition for the existence of a matching is known as Hall's marriage theorem:

Theorem 5.2 *Let Γ be a bipartite graph with vertex set $\mathcal{V}(\Gamma) = V_1 \cup V_2$ and edge set $\mathcal{E}(\Gamma)$. Edges only connect vertices of V_1 with vertices of V_2. We assume that $|V_1| = |V_2|$. A necessary and sufficient condition for the existence of a matching is that for any set $S \subseteq V_1$ the union of the set of neighbors of vertices $x \in S$ is of size at least the size of S.*

We remark that there is an algorithm to construct such a matching provided it exists. If the matching does not exist, the algorithm exhibits a set $S \subseteq V_1$ whose united neighbor set is of insufficient size. Thus the question of whether or not a matching exists is settled. Here, we mean that the answer can be found algorithmically with not too much effort. For a description of this algorithm (which is also known under the name *matchmaker*) we refer to the textbook by van Lint and Wilson [11].

We have the following test:

Lemma 5.3 (Test 2)
The arc $\mathcal{O}_{f,D}$ cannot be completed to a hyperoval unless the bipartite graph Γ which is defined by the matrix $M_{\overline{D},\overline{E}}$ has a matching.

Proof. Consider the pencil of lines trough $\langle(1,0,0)\rangle$ and the pencil of lines through $\langle(0,1,0)\rangle$. These two line pencils define the grid of horizontal and vertical lines in the affine plane. If $\mathcal{O}_{f,D}$ completes, then each of these lines must contain one further (affine) point. In particular, if we restrict to the lines which are not yet secants, then they correspond to the submatrix $M_{\overline{D},\overline{E}}$. An affine point $\langle(x,y,1)\rangle$ can be chosen to extend the arc $\mathcal{O}_{f,D}$ if and only if $m_{y,x}=1$. The fact that we can choose further points on each of the non-secant lines is equivalent to the existence of a matching in the bipartite graph which is defined by the rows and columns of the matrix $M_{\overline{D},\overline{E}}$. $\square$

As an example, consider hyperovals in PG$(2,4)$. We know that we may start with the fundamental quadrangle $\langle(1,0,0)\rangle$, $\langle(0,1,0)\rangle$, $\langle(0,0,1)\rangle$ and $\langle(1,1,1)\rangle$. Thus $D=\{0,1\}$, with $f(0)=0$ and $f(1)=1$, and hence $E=\{0,1\}$. We order the rows and columns of M according to Fig. 1. Thus, rows are indexed by $(\alpha^2,\alpha,1,0)$ whereas columns are indexed by $(0,1,\alpha,\alpha^2)$. We obtain

$$M=\left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

The submatrix $M_{\overline{D},\overline{E}}$ is the 2×2 matrix in the upper right hand corner. We see that this matrix clearly has a matching, corresponding to the points $\langle(\alpha,\alpha^2,1)\rangle$ and $\langle(\alpha^2,\alpha,1)\rangle$. Indeed, these two points complete the fundamental quadrangle to a hyperoval. In particular, we have proved that the hyperoval in PG$(2,4)$ is unique.

6 A Computer Search For Hyperovals

The tests presented in the last section are helpful in facilitating an exhaustive search for all hyperovals in a plane PG$(2,2^h)$ for moderatly large h. Such a search also needs an isomorph rejection algorithm, which was not discussed in this article. Nevertheless, putting the two pieces together, efficient searches

for hyperovals can be performed. The author was able to recalculate the 6 hyperovals in $\mathrm{PG}(2,32)$, a result which was originally obtained by [9] (as mentioned above). For sake of completeness, and since the author feels that this data would otherwise only be available by consulting different research papers, we collect in Table 3 the known hyperovals in planes of order 2^h, $h \leq 5$. This list is known to be complete. We represent the elements of the finite fields $\mathbb{F}_q$ as powers of a primitive element α. The minimum relation satisfied by α is indicated in the table. The column headed "pt-orbits" lists the lengths of orbits of the automorphism group of $\mathcal{O}_f$ in $\mathrm{P\Gamma L}(3,q)$ on the points of $\mathcal{O}_f$.

7 Note Added In Proof

We remark that the hyperoval condition presented in [6] fails to exclude constant functions as oval-polynomials. Instead, we have the following corrected version:

Theorem 7.1 *Let f be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, where $q = 2^h$. Then $\mathcal{O}_f$ is a hyperoval if and only if*

- $\sum_{x \in \mathbb{F}_q} f(x)^{q-1} = 1$ *and*
- *the coefficient of X^a in*

$$f(X)^b \, mod \, X^q - X$$

is zero for all pairs of integers (a,b) with

$$1 \leq b \prec a \leq q-1, \quad b \neq q-1.$$

Here, for two positive integers a and b with $a = \sum_{i=0}^{h-1} a_i 2^i$ and $b = \sum_{i=0}^{h-1} b_i 2^i$ and $0 \leq a_i, b_i < 2$ $(0 \leq i < h)$ we write

$$b \prec a \iff \Big[b_i = 1 \;\Rightarrow\; a_i = 1 \; \forall i = 0, 1, \ldots, h-1 \Big],$$

i.e. if the binary representation of a "covers" the binary representation of b.

The following two remarks are in order. It has been communicated to the author by both David Glynn and by András Gács that constant functions

are the only counterexamples to the condition presented in [6]. Also, it can be shown that the condition presented in Theorem 4.1 is equivalent to Theorem 7.1. Nevertheless, the version in Theorem 4.1 is a little more general, as it applies also to arcs and hence yields a test as described in Lemma 5.1.

8 Acknowledgements

The author thanks David Glynn, András Gács, Stan Payne and Tom Edgar [4] for fruitful discussions. He also thanks Bob Liebler for pointing out reference [2] to him. Last but certainly not least, he also thanks the two referees for valuable comments and suggestions.

References

[1] E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. Reprint of the 1957 original, A Wiley-Interscience Publication.

[2] M. Bardoe and P. Sin. The permutation modules for $\mathrm{GL}(n+1, \mathbf{F}_q)$ acting on $\mathbf{P}^n(\mathbf{F}_q)$ and $\mathbf{F}_q^{n-1}$. *J. London Math. Soc. (2)*, 61(1):58–80, 2000.

[3] Ph. Delsarte. On cyclic codes that are invariant under the general linear group. *IEEE Trans. Information Theory*, IT-16:760–769, 1970.

[4] T. Edgar. Finite Projective Geometries and Linear Codes, Master's Thesis, Spring 2004, Colorado State University.

[5] D. G. Glynn. Two new sequences of ovals in finite Desarguesian planes of even order. In *Combinatorial mathematics, X (Adelaide, 1982)*, volume 1036 of *Lecture Notes in Math.*, pages 217–229. Springer, Berlin, 1983.

[6] D. G. Glynn. A condition for the existence of ovals in $\mathrm{PG}(2, q), q$ even. *Geom. Dedicata*, 32(2):247–252, 1989.

[7] D. G. Glynn and J. W. P. Hirschfeld. On the classification of geometric codes by polynomial functions. *Des. Codes Cryptogr.*, 6(3):189–204, 1995.

[8] N. Hamada. The rank of the incidence matrix of points and d-flats in finite geometries. *J. Sci. Hiroshima Univ. Ser. A-I Math.*, 32:381–396, 1968.

[9] T. Penttila and G. F. Royle. Classification of hyperovals in $\mathrm{PG}(2, 32)$. *J. Geom.*, 50(1-2):151–158, 1994.

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

[11] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, Cambridge, second edition, 2001.

name	|Aut|	pt-orbits	oval-polynomial
$h=2, \alpha^2=\alpha+1:$			
Regular	720	(6)	X^2
$h=3, \alpha^3=\alpha^2+1:$			
Regular	1512	$(1,9)$	$\alpha^6X^6+\alpha X^4+\alpha^3X^2$
$h=4, \alpha^4=\alpha^3+1:$			
Lunelli,Sce	144	(18)	$X^{12}+X^{10}+\alpha^6X^8+X^6+\alpha^{11}X^4+\alpha X^2$
Regular	16320	$(1,17)$	$\alpha^{13}X^{14}+X^{12}+\alpha^2X^{10}+\alpha^4X^8+\alpha^6X^6+\alpha^8X^4+\alpha^{10}X^2$
$h=5, \alpha^5=\alpha^2+1:$			
Payne	10	$(1^2,2,10^3)$	$\alpha^{21}X^{30}+\alpha^7X^{28}+\alpha^{11}X^{26}+\alpha^7X^{24}+\alpha X^{22}+\alpha^3X^{20}+\alpha^{22}X^{18}+X^{16}+\alpha X^{14}+\alpha^{13}X^{12}+\alpha^{27}X^{10}+\alpha^4X^8+\alpha^{24}X^6+\alpha^{12}X^4+\alpha^{22}X^2$
O'Keefe, Penttila	3	$(1,3^{11})$	$\alpha^{17}X^{30}+\alpha^4X^{28}+X^{26}+\alpha^{16}X^{24}+\alpha^{11}X^{22}+\alpha^{16}X^{20}+\alpha^{20}X^{18}+\alpha^{10}X^{16}+\alpha^{12}X^{14}+\alpha^{29}X^{12}+\alpha^{23}X^{10}+\alpha^5X^8+\alpha^7X^6+\alpha^{19}X^4+\alpha^{19}X^2$
Cherowitzo	5	$(1^4,5^6)$	$X^{30}+\alpha^{16}X^{28}+\alpha^{12}X^{26}+\alpha^{21}X^{24}+\alpha^{30}X^{22}+\alpha^{22}X^{20}+\alpha^{15}X^{18}+\alpha^4X^{16}+\alpha^{29}X^{14}+\alpha^{24}X^{12}+\alpha^{26}X^{10}+\alpha^{14}X^8+\alpha X^6+\alpha^9X^4$
Segre,Bartocci	465	$(3,31)$	$\alpha^4X^{30}+\alpha^{10}X^{28}+\alpha^{16}X^{26}+\alpha^{22}X^{24}+\alpha^{28}X^{22}+\alpha^3X^{20}+\alpha^{14}X^{18}+\alpha^{21}X^{16}+\alpha^{21}X^{14}+\alpha^{25}X^{12}+\alpha^{17}X^{10}+\alpha^{14}X^8+\alpha^{24}X^6+\alpha^2X^2$
Translation (due to Segre)	4960	$(1^2,32)$	$\alpha^3X^{30}+\alpha^{29}X^{28}+\alpha^{24}X^{26}+\alpha^{28}X^{24}+\alpha^2X^{22}+\alpha^{28}X^{20}+\alpha^{23}X^{18}+\alpha^{13}X^{16}+\alpha^{25}X^{14}+\alpha^{20}X^{12}+\alpha^{15}X^{10}+\alpha^{19}X^8+\alpha^{24}X^6+\alpha^{19}X^4+\alpha^{14}X^2$
Regular	163680	$(1,33)$	$\alpha^{19}X^{30}+\alpha^{21}X^{28}+\alpha^{23}X^{26}+\alpha^{25}X^{24}+\alpha^{27}X^{22}+\alpha^{29}X^{20}+X^{18}+\alpha^2X^{16}+\alpha^4X^{14}+\alpha^6X^{12}+\alpha^8X^{10}+\alpha^{10}X^8+\alpha^{12}X^6+\alpha^{14}X^4+\alpha^{16}X^2$

Table 3: The Hyperovals in Planes PG$(2,h)$, $h \leq 5$