GAUSS SUMS, JACOBI SUMS, AND p-RANKS OF CYCLIC DIFFERENCE SETS

RONALD EVANS, HENK HOLLMANN, CHRISTIAN KRATTENTHALER, QING XIANG

Abstract. We study quadratic residue difference sets, GMW difference sets, and difference sets arising from monomial hyperovals, all of which are $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference sets in the multiplicative group of the finite field $\mathbb{F}_{2^d}$ of 2^d elements, with $d \geq 2$. We show that, except for a few cases with small d, these difference sets are all pairwise inequivalent. This is accomplished in part by examining their 2-ranks. The 2-ranks of all of these difference sets were previously known, except for those connected with the Segre and Glynn hyperovals. We determine the 2-ranks of the difference sets arising from the Segre and Glynn hyperovals, in the following way. Stickelberger's theorem for Gauss sums is used to reduce the computation of these 2-ranks to a problem of counting certain cyclic binary strings of length d. This counting problem is then solved combinatorially, with the aid of the transfer matrix method. We give further applications of the 2-rank formulas, including the determination of the nonzeros of certain binary cyclic codes, and a criterion in terms of the trace function to decide for which β in $\mathbb{F}_{2^d}^*$ the polynomial $x^6+x+\beta$ has a zero in $\mathbb{F}_{2^d}$, when d is odd.

1. Introduction

Let G be a finite (multiplicative) group of order v. A K-element subset D of G is called a (v, K, λ) *difference set* in G if the list of "differences" $d_1d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, represents each nonidentity element in G exactly λ times. Thus, D is a (v, K, λ) difference set in G if and only if it satisfies the following equation in $\mathbb{Z}[G]$:

$$\left(\sum_{d\in D} d\right)\left(\sum_{d\in D} d^{-1}\right) = (K-\lambda)1_G + \lambda\sum_{g\in G} g, \tag{1.1}$$

where 1_G is the identity element of G. If the group G is cyclic, then D is called a *cyclic* difference set.

We say that the (v, K, λ) difference sets D_1 and D_2 in an Abelian group G are *equivalent* if there exists an automorphism α of G and an element $a \in G$ such that $\alpha(D_1) = D_2a$. In particular, if G is cyclic, then D_1 and D_2 are equivalent if there exists an integer t, $(t, v) = 1$, such that $D_1 = D_2^{(t)}a$ for some $a \in G$, where $D_2^{(t)} = \{d^t \mid d \in D_2\}$.

2000 *Mathematics Subject Classification.* Primary 05B10; Secondary 05A15 05C38 05C90 11L05 11T24 11T71 94B15.

Key words and phrases. Cyclic difference set, monomial hyperoval, Segre hyperoval, Glynn hyperoval, Singer difference set, GMW difference set, quadratic residue difference set, binary cyclic code, finite fields, Teichmüller character, Gauss sum, Jacobi sum, enumeration of cyclic binary strings, transfer matrix method.

Copyright © 1999 by Academic Press.

In the case G is Abelian, using the Fourier inversion formula, we obtain the following standard result in the theory of difference sets [28, p. 323].

Lemma 1.1. *Let G be an Abelian group of order v. A K-subset D is a (v,K,λ) difference set in G if and only if*

$$\chi(D)\overline{\chi(D)} = K - \lambda \tag{1.2}$$

for every nontrivial complex multiplicative character χ of G. Here, $\chi(D)$ stands for $\sum_{d\in D}\chi(d)$.

Difference sets are the same objects as symmetric designs with a regular automorphism group (see [15, p. 243]). Therefore they play an important role in the theory of combinatorial designs. The study of difference sets is also closely related to coding theory, finite geometry, and communication signal designs. We refer the reader to the book of Lander [16] and the paper of Jungnickel [15] for a survey of this subject.

Let $\mathbb{F}_q$ be the finite field with q elements, q being a power of the prime p. Let ξ_p be a fixed complex primitive pth root of unity and let $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi\colon \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi(x) = \xi_p^{\mathrm{Tr}_{q/p}(x)},$$

which is easily seen to be a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi\colon \mathbb{F}_q^* \to \mathbb{C}^*$$

be a multiplicative character of $\mathbb{F}_q^*$. We extend χ to all of $\mathbb{F}_q$ by setting $\chi(0)=0$. Note that $\chi^{q-1}=1$ (the trivial character), so the order of χ is prime to p.

Define the *Gauss sum* by

$$g(\chi) = \sum_{a\in\mathbb{F}_q} \chi(a)\psi(a).$$

One of the elementary properties of Gauss sums is [4, Theorem 1.1.4]

$$g(\chi)\overline{g(\chi)} = q, \quad \text{if} \quad \chi \neq 1. \tag{1.3}$$

If χ_1, χ_2 are two multiplicative characters, we define the *Jacobi sum* by

$$J(\chi_1,\chi_2) = \sum_{a\in\mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

Jacobi sums are closely related to Gauss sums. In fact if $\chi_1\neq 1, \chi_2\neq 1$, and $\chi_1\chi_2\neq 1$, then [4, Theorem 2.1.3]

$$J(\chi_1,\chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2), \tag{1.4}$$

and

$$J(\chi_1,\chi_2)\overline{J(\chi_1,\chi_2)} = q. \tag{1.5}$$

The apparent analogy between (1.2) and {(1.3), (1.5)} suggests that there may be a connection between difference sets and Gauss and Jacobi sums. This is indeed the case. In fact, several authors have investigated difference sets by using Gauss sums and Jacobi sums; for example, see [3], [4, Chapter 5], [32]. However, such investigations deal mostly with power residue difference sets. In Section 2 of this paper, we use Jacobi sums to give a simple new proof that certain sets which Maschietti [21] constructed from hyperovals are cyclic $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ difference sets; see Theorem 2.5. Then in Section 3, we use Stickelberger's theorem on the prime ideal decomposition of Gauss sums to give a new proof of the p-rank formula for Singer difference sets (which include the difference sets arising from regular and translation hyperovals); see Theorem 3.5. The main result of Section 3 is Theorem 3.6, where, again using Stickelberger's theorem, we reduce the problem of computing the 2-ranks of the difference sets arising from Segre and Glynn hyperovals to a problem of counting certain cyclic binary sequences. In Section 4, we solve the counting problem completely, with the aid of the transfer matrix method; see Theorem 4.3. In the case of the Segre hyperovals, this yields an explicit formula for their 2-ranks in terms of Fibonacci numbers; see Corollary 4.4. This explicit formula had been conjectured by Xiang [31]. In the case of the Glynn hyperovals we obtain 5-term recurrence relations for the 2-ranks of the corresponding cyclic difference sets; see Theorems 4.6 and 4.8.

As applications, in Section 5, we determine the nonzeros of the binary cyclic codes which result from the Segre hyperovals, and we give a criterion to decide when the equation $x^6+x+\beta=0$, $\beta\in\mathbb{F}_{2^d}^*$, has two distinct solutions in $\mathbb{F}_{2^d}$, d odd.

The main applications of our results are contained in Section 6. There we show that, except for a few small values of d, the Singer difference sets and the difference sets which arise from the Segre and the Glynn hyperovals are all inequivalent; see Theorem 6.2. This answers a question raised by Maschietti [21]. We also show that difference sets arising from hyperovals are inequivalent to quadratic residue difference sets [15, p. 244] (see Theorem 6.3) and to GMW difference sets [11] (see Theorem 6.8).

Finally, in Section 7, we use the machinery developed in this paper to compute the 2-ranks of certain circulant matrices. These matrices are closely related to incidence matrices corresponding to difference sets arising from hyperovals.

2. Gauss Sums, Jacobi Sums and Cyclic Difference Sets

Singer (1938) (cf. [15, p. 244]) discovered a large class of difference sets which are related to finite projective geometry and to (generalized) Reed-Muller codes (cf. [2, p. 180]). These difference sets L_0, whose construction we give below, have parameters

$$v=\frac{q^d-1}{q-1},\qquad K=\frac{q^{d-1}-1}{q-1},\qquad \lambda=\frac{q^{d-2}-1}{q-1}$$

for $d\geq 2$ and they exist whenever q is a prime power.

The construction is as follows. Let $\mathbb{F}_{q^d}$ be the finite field of q^d elements, $d\geq 2$, and let Tr be the trace from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$. We may take a system L of coset representatives of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^d}^*$ such that Tr maps L into $\{0,1\}$. Write $L=L_0\cup L_1$, where

$$L_0=\{x\in L\mid \mathrm{Tr}(x)=0\},\qquad L_1=\{x\in L\mid \mathrm{Tr}(x)=1\}.$$

The following proof that L_0 is a difference set is due to Yamamoto [33]. We present it here since it is less well-known than the standard one using a Singer cycle, and since we will use it to give a new proof of the p-rank formula for the Singer difference sets (see Theorem 3.5). This proof of Theorem 2.1 is essentially an evaluation of the Eisenstein sum $\chi(L_0)$; see [4, pp. 389, 400].

Theorem 2.1. *With the above notation, L_0 is a $(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1})$ difference set in the quotient group $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$.*

Proof: Let χ be a nontrivial multiplicative character of $\mathbb{F}_{q^d}$ whose restriction to $\mathbb{F}_q^*$ is trivial, so that we may view χ as a character of the quotient group $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$. It is easy to see that every nontrivial character of $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$ can be obtained in this manner. We have

$$\begin{aligned} g(\chi) &= \sum_{y\in\mathbb{F}_{q^d}^*} \chi(y)\xi_p^{\mathrm{Tr}_{q^d/p}(y)} = \sum_{a\in\mathbb{F}_q^*}\sum_{x\in L} \chi(xa)\xi_p^{\mathrm{Tr}_{q^d/p}(xa)} \\ &= \sum_{x\in L}\chi(x)\sum_{a\in\mathbb{F}_q^*}\chi(a)\xi_p^{\mathrm{Tr}_{q/p}(a\,\mathrm{Tr}(x))} \\ &= (q-1)\sum_{x\in L_0}\chi(x) - \sum_{x\in L_1}\chi(x) = q\sum_{x\in L_0}\chi(x) = q\chi(L_0). \end{aligned}$$

By (1.3), we have $\chi(L_0)\overline{\chi(L_0)} = q^{d-2}$. The theorem now follows from Lemma 1.1. $\square$

Remark: When $q=2$, Singer difference sets have parameters $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$, which are a special case of the *Hadamard* parameters $(4n-1, 2n-1, n-1)$ (see [15, p. 244]).

Cyclic $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ difference sets have been extensively studied because of their important applications in communication signal designs (see [10]). Known examples of these difference sets include Singer difference sets, GMW difference sets (see [11]), quadratic residue difference sets [15, p. 244] and the cyclic $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ difference sets constructed recently by Maschietti [21] by using monomial hyperovals.

We proceed to discuss Maschietti's difference sets. An *m-arc* in the projective plane $PG(2,q)$, with q a prime power, is a set of m points, no three of which are collinear. The maximum value of m is $q+1$ or $q+2$, according as q is odd or even. If q is odd, $(q+1)$-arcs are called *ovals*. A celebrated theorem of Segre [25] (see also [14, p. 168]) states that all such ovals are given algebraically by irreducible conics. If q is even, $(q+2)$-arcs are called *hyperovals*. The classic example of a hyperoval is the union of an irreducible conic and its nucleus (see [14, p. 164]).

Two hyperovals are said to be *projectively equivalent* if one hyperoval can be transformed into the other by a projective linear transformation, i.e., by an element from $PGL(3,q)$. By the Fundamental Theorem of Projective Geometry, the group $PGL(3,q)$ of projective linear transformations of $PG(2,q)$ is transitive on quadrangles. Thus every hyperoval can be mapped by an element of $PGL(3,q)$ to a hyperoval containing the *fundamental quadrangle* $(1,0,0), (0,1,0), (0,0,1)$, and $(1,1,1)$. From now on, we will restrict our attention to those hyperovals in $PG(2,q)$ with $q>2$ which contain the fundamental quadrangle. The following result of Segre (see [14, Theorem 8.4.2]) shows that any such hyperoval can be expressed in terms of a *permutation polynomial* over $\mathbb{F}_q$, i.e., a polynomial which, when interpreted as a function, permutes $\mathbb{F}_q$.

Theorem 2.2. (Segre). *Let $q > 2$ be a power of 2. Then any hyperoval in $PG(2,q)$ containing the fundamental quadrangle is equal to a $(q+2)$-arc*

$$D(f) = \{(1, t, f(t)) \mid t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\},$$

where f is a permutation polynomial over $\mathbb{F}_q$ of degree at most $q-2$, satisfying $f(0) = 0, f(1) = 1$, and such that for each $s \in \mathbb{F}_q$,

$$f_s(x) = \begin{cases} \dfrac{f(x+s)+f(s)}{x}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0, \end{cases}$$

is a permutation polynomial.

Conversely, every such set $D(f)$ is a hyperoval.

These polynomials $f(x)$ are also called *o-polynomials*.

A subclass of hyperovals is the set of *monomial hyperovals*. These are hyperovals in $PG(2,2^d)$ projectively equivalent to

$$D(x^k) = \{(1, t, t^k) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0,1,0),(0,0,1)\}.$$

Known examples of monomial hyperovals in $PG(2,2^d)$ include

(2.1) the *regular* hyperoval $D(x^2)$,
(2.2) the *translation* hyperovals $D(x^{2^i})$, where $(d,i) = 1$, $1 < i < d/2$,
(2.3) the *Segre* hyperoval $D(x^6)$, where $d \geq 5$ is odd,
(2.4) the *Glynn* type (I) hyperovals $D(x^{\sigma+\gamma})$, where $d \geq 7$ is odd, $\sigma = 2^{(d+1)/2}$, and $\gamma = 2^{(3d+1)/4}$ if $d \equiv 1 \bmod 4$, whereas $\gamma = 2^{(d+1)/4}$ if $d \equiv 3 \bmod 4$,
(2.5) the *Glynn* type (II) hyperovals $D(x^{3\sigma+4})$, where $d \geq 11$ is odd, and $\sigma = 2^{(d+1)/2}$.

Remark: We have not listed the translation hyperovals for $i = 1$ nor the Segre and Glynn hyperovals for $d = 3$, as these are all projectively equivalent to the regular hyperovals. The translation hyperoval for a given $i > d/2$ is equivalent to the one where i is replaced by $d - i$. The Glynn hyperovals for $d = 5$ are equivalent to translation hyperovals, while the Glynn type (II) hyperovals for $d = 7$ and $d = 9$ are respectively equivalent to the Segre hyperoval $D(x^6)$ and the Glynn type (I) hyperoval $D(x^{160})$. These equivalences all follow from Lemma 2.3 below. It can be shown using Lemma 2.3 that the hyperovals listed in (2.1)–(2.5) are all mutually projectively inequivalent. For example, to show that the Segre hyperovals are inequivalent to the translation hyperovals, one shows that none of 6, 1/6, −5, −1/5, 6/5, or 5/6 (mod $q-1$) can equal a power of 2 (mod $q-1$), where $q = 2^d$ for odd $d \geq 5$. The computations involved are tedious but straightforward.

Glynn [8] conjectured that the hyperovals listed in (2.1)–(2.5) (together with the equivalent hyperovals given by Lemma 2.3 below) comprise *all* monomial hyperovals. This conjecture still remains open. Some progress was made in a recent paper by Cherowitzo and Storme [7].

Lemma 2.3. ([8], [22]) *Let $q > 2$ be a power of 2. Two monomial hyperovals $D(x^j)$ and $D(x^k)$ in $PG(2,q)$ are projectively equivalent if and only if $j \equiv k$, $1/k$, $1-k$, $1/(1-k)$, $k/(k-1)$, or $(k-1)/k$ (mod $q-1$).*

Proof: First, if $D(x^k)$ is a monomial hyperoval in $PG(2,q)$, then it is well known that for any j congruent to k, $1/k$, $1-k$, $1/(1-k)$, $k/(k-1)$, or $(k-1)/k$ modulo $q-1$, $D(x^j)$ is projectively equivalent to $D(x^k)$ (see [8]). Conversely, it follows from [22, Theorem 12.5.3] that if $D(x^j)$ is projectively equivalent to $D(x^k)$, then j is congruent to one of k, $1/k$, $1-k$, $1/(1-k)$, $k/(k-1)$, $(k-1)/k$ modulo $q-1$. This completes the proof. □

Let $\tau\colon \mathbb{F}_{2^d} \to \mathbb{F}_{2^d}$ be defined by

$$\tau(x) = x + x^k,$$

and let $\operatorname{Im}\tau$ be the image of the map τ. We need the following lemma from Maschietti [21]. For the convenience of the reader, we include a proof. In the statement of the lemma, and its proof, we use the convention that points in $PG(2,q)$ are labelled as (z,x,y).

Lemma 2.4. *Let $q = 2^d$. The $(q+2)$-set $D(x^k) = \{(1,t,t^k) \mid t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$ in $PG(2,q)$ is a hyperoval if and only if $(k,q-1) = 1$ and τ is a two-to-one map from $\mathbb{F}_q$ into itself.*

Proof: If $D(x^k)$ is a hyperoval, then x^k is a permutation polynomial on $\mathbb{F}_q$, so $(k,q-1) = 1$. Furthermore, any affine line $y = x + a$ $(a \in \mathbb{F}_q)$ meets $D(x^k)$ at either 0 or 2 distinct points, which implies that $x^k + x + a = 0$ has either 0 or 2 distinct solutions in $\mathbb{F}_q$, that is, the map τ is two-to-one.

Conversely, if τ is two-to-one, then the equation $x^k + x = 0$ has exactly two solutions, namely 0 and 1. Hence, there is no $(k-1)$th root of 1 distinct from 1 in $\mathbb{F}_q$, so that $(k-1,q-1) = 1$.

It is straightforward to show that a line of $PG(2,q)$ with homogeneous equation $cy = ax + bz$, with $abc = 0$, intersects $D(x^k)$ at either 0 or 2 points. It remains to show that the line $y = ax + bz$, with $ab \neq 0$, intersects $D(x^k)$ at either 0 or 2 points.

It is clear that there are no intersection points $(0,x,y)$ of the line with $D(x^k)$. Thus set $z = 1$ and consider the affine equation $x^k = ax + b$. We must show that this equation has 0 or 2 solutions. This follows from the hypothesis that τ is two-to-one, as can be seen after making the change of variable $x = a^{\frac{1}{k-1}}x'$. This completes the proof. □

Remark: From Lemma 2.4 and its proof, it follows that when $D(x^k)$ is a hyperoval in $PG(2,q)$, with $q = 2^d$, then k and $k-1$ are both relatively prime to $q-1$.

Using the geometry of hyperovals, Maschietti [21] proved that if $D(x^k)$ is a hyperoval in $PG(2,2^d)$, then

$$D_{k,d} = \operatorname{Im}\tau \setminus \{0\}$$

is a $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ difference set in $\mathbb{F}_{2^d}^*$. In the following theorem, we give a simpler proof using Jacobi sums.

Theorem 2.5. *Let $q = 2^d$. If $D(x^k) = \{(1,t,t^k) \mid t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$ is a hyperoval in $PG(2,q)$, then $D_{k,d} = \operatorname{Im}\tau \setminus \{0\}$ is a $(q-1, q/2-1, q/4-1)$ difference set in $\mathbb{F}_q^*$.*

Proof: Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$. Since $D(x^k)$ is a hyperoval, τ is two-to-one by Lemma 2.4, and we have

$$\chi(D_{k,d}) = \frac{1}{2}\sum_{x\in\mathbb{F}_q}\chi(x+x^k) = \frac{1}{2}\sum_{x\in\mathbb{F}_q}\chi(x)\chi(1+x^{k-1}).$$

By the previous remark, $(k-1, q-1) = 1$, so there exists a multiplicative character ϕ of $\mathbb{F}_q$ such that $\chi = \phi^{k-1}$. Hence

$$\chi(D_{k,d}) = \frac{1}{2}\sum_{x\in\mathbb{F}_q}\phi(x^{k-1})\chi(1+x^{k-1}) = \frac{1}{2}J(\phi,\chi). \tag{2.6}$$

Noting that $\phi\chi = \phi^k$ is nontrivial, we have, by (1.5), $\chi(D_{k,d})\overline{\chi(D_{k,d})} = 2^{d-2}$. Now the theorem follows from Lemma 1.1. □

The following proposition shows that two projectively equivalent monomial hyperovals give rise to two equivalent cyclic difference sets under the construction of Theorem 2.5.

Proposition 2.6. *Let $q = 2^d$, $q > 2$. If $D(x^k)$ and $D(x^j)$ are two projectively equivalent monomial hyperovals in $PG(2, q)$, then the corresponding difference sets $D_{k,d}$ and $D_{j,d}$ constructed in Theorem 2.5 are equivalent.*

Proof: By Lemma 2.4, we know that j is congruent to one of k, $1/k$, $1-k$, $1/(1-k)$, $k/(k-1)$, $(k-1)/k$ modulo $q-1$. Now direct calculation shows that

$$D_{\frac{k}{k-1},d} = D_{\frac{k-1}{k},d} = D_{k,d}^{(k-1)}, \tag{2.7}$$

$$D_{1-k,d} = D_{\frac{1}{1-k},d} = D_{k,d}^{(\frac{1-k}{k})}, \tag{2.8}$$

$$D_{\frac{1}{k},d} = D_{k,d}, \tag{2.9}$$

where $D^{(t)} = \{d^t \mid d \in D\}$. For example, to prove (2.7), write $c = x + x^k$, make the variable change $x = c/y$, then multiply both sides by y^k. This completes the proof of the proposition. □

The difference sets arising from the regular and translation hyperovals $D(x^{2^i})$ are the Singer difference sets $\{y \in \mathbb{F}_{2^d}^* \mid \mathrm{Tr}(y) = 0\}$. This follows from Lemma 2.4 and Hilbert's Theorem 90 [17, p. 56]. It is an interesting problem to determine whether the cyclic difference sets arising from the Segre and Glynn hyperovals are inequivalent to each other and to the previously known ones (such as Singer difference sets, quadratic residue difference sets, GMW difference sets). We approach these problems by studying the 2-ranks (as defined in Section 3) of these cyclic difference sets. Our conclusions are presented in Theorems 6.2, 6.3, and 6.8.

3. Stickelberger's Theorem and the p-ranks of Cyclic Difference Sets

We start this section by reviewing a few standard notions from design theory. We refer the reader to [15, p. 243] for details and more information.

Let G be a (multiplicative) Abelian group of order v, and let D be a (v, K, λ) difference set in G. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a (v, K, λ) symmetric design with a regular automorphism group G, where the set $\mathcal{P}$ of *points* of $\mathcal{D}$ is G, and where the set $\mathcal{B}$ of *blocks* of $\mathcal{D}$ is

$\{gD \mid g \in G\}$. (As it turns out, the blocks are all distinct.) This design is usually called the *development* of D. The incidence matrix of $\mathcal{D}$ is the matrix A whose rows are indexed by the blocks B of $\mathcal{D}$ and whose columns are indexed by the points g of $\mathcal{D}$, where the entry $A_{B,g}$ in row B and column g is 1 if $g \in B$, and 0 otherwise.

The *p-ary code* of D, denoted $\mathcal{C}_p(D)$, is defined to be the row space of A over $\mathbb{F}_p$, the field of p elements. This code is also the p-ary code of $\mathcal{D}$, denoted by $\mathcal{C}_p(\mathcal{D})$. The $\mathbb{F}_p$-dimension of $\mathcal{C}_p(D)$ is usually called the *p-rank* of the difference set D. We shall also denote it by $\operatorname{rank}_p\mathcal{D}$. It is well-known that $\mathcal{C}_p(D)$ is of interest only if $p \mid (K-\lambda)$; see [5] or [15, p. 297]. So from now on, we always assume that $p \mid (K-\lambda)$.

The p-ranks of difference sets have been studied extensively for several reasons. First, if D_1 and D_2 are two equivalent (v,K,λ) difference sets in an Abelian group G, then the p-ranks of D_1 and D_2 are the same. Therefore, the p-ranks can help us to distinguish two inequivalent difference sets.

Secondly, let D be a cyclic (v,K,λ) difference set in $\mathbb{Z}/v\mathbb{Z}$ with $2|(K-\lambda)$. Corresponding to D is the *characteristic sequence* $\{a_i\}_{0\le i\le v-1}$ given by $a_i = 1$ if $i \in D$, and $a_i = 0$ otherwise. This sequence has a two-level autocorrelation function (see [10, p. 62]). The *linear complexity* (or *linear span*) of $\{a_i\}$ is the smallest degree of a linear shift register over $\mathbb{F}_2$ which is capable of generating $\{a_i\}$. It turns out that the linear complexity of $\{a_i\}$ is the same as the 2-rank of D. Therefore, the study of 2-ranks of cyclic difference sets is important for communications and cryptographic applications; see [10].

A third reason is provided by Theorem 3.2 below. MacWilliams and Mann [19], Goethals and Delsarte [9], and Smith [26] proved that the p-rank of the $((q^d-1)/(q-1),(q^{d-1}-1)/(q-1),(q^{d-2}-1)/(q-1))$ Singer difference set is $\binom{p+d-2}{d-1}^s+1$, where $q=p^s$ for prime p. Subsequently, Hamada [12] made the following conjecture.

Conjecture 3.1. *Let $\mathcal{D}$ be a symmetric design with Singer parameters $((q^d-1)/(q-1),(q^{d-1}-1)/(q-1),(q^{d-2}-1)/(q-1))$, where $q=p^s$. Then one has*

$$\operatorname{rank}_p\mathcal{D} \ge \binom{p+d-2}{d-1}^s + 1,$$

with equality if and only if $\mathcal{D}$ is the development of a classical Singer difference set.

This conjecture still remains open. But Hamada and Ohmori [13] proved the following interesting result in this direction.

Theorem 3.2. *Let $\mathcal{D}$ be a symmetric design with parameters $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$. Then $\mathcal{D}$ is the development of the cyclic Singer difference set with these parameters if and only if* $\operatorname{rank}_2\mathcal{D} = d+1$.

In Theorem 3.5, we will give a simple new proof of the p-rank formula for the classical Singer difference sets. Our approach is different from previous ones in that it uses Gauss and Jacobi sums, and Stickelberger's theorem on the prime ideal factorization of Gauss sums.

We first quote a result (Theorem 3.3) of MacWilliams and Mann [19]. For the convenience of the reader, we include a proof here.

Let $B = \sum_{g\in G} b_g g$ be an element of the group algebra $F[G]$, where G is an Abelian group and F is a field. We associate with B the matrix $(b_{g(g')^{-1}})$, whose rows and columns are labeled by the group elements g and g'. The rank of $(b_{g(g')^{-1}})$ is called the *rank* of B. We remark that in particular, if $B = \sum_{g\in D} g$, where D is a (v, K, λ) difference set in G, then the p-rank of D, i.e., the $\mathbb{F}_p$-dimension of the code $\mathcal{C}_p(D)$, is the same as the rank of B over $\mathbb{F}_p$. The reason is that the rows and columns of the incidence matrix of the development of D can be arranged so that the incidence matrix is the transpose $(b_{g(g')^{-1}})^T$ of the matrix $(b_{g(g')^{-1}})$.

Theorem 3.3. *Let G be an Abelian group of order v and exponent v^*, let F be a field of characteristic p not dividing v which contains the v^*th roots of unity, and let $B = \sum_{g\in G} b_g g$ be an element of the group algebra $F[G]$. Then the rank of B over F is equal to the number of characters $\chi : G \to F^*$ satisfying $\chi(B) \neq 0$, where $\chi(B) = \sum_{g\in G} b_g \chi(g)$.*

Proof: Let $\big(\chi(g)\big)$ be a matrix whose rows are labeled by the v characters χ and whose columns are labeled by the v group elements g, so that the entry in row χ and column g is $\chi(g)$. This matrix is nonsingular since $\frac{1}{v}\big(\chi(g)\big)\big(\chi(g^{-1})\big)^T$ is the identity matrix. The result now follows from the identity

$$\big(\chi(g)\big)\big(b_{g(g')^{-1}}\big)\big(\chi(g^{-1})\big)^T = v \cdot \operatorname{diag}\big(\chi(B)\big).$$

□

We will also need Stickelberger's result (Theorem 3.4) on the prime ideal decomposition of Gauss sums. We first introduce some notation.

Let p be a prime, $q = p^s$, and let ξ_{q-1} be a (complex) primitive $(q-1)$th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let $\omega_\mathfrak{p}$ be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega_\mathfrak{p} : \mathbb{F}_q^* \to \{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\}$$

satisfying

$$\omega_\mathfrak{p}(\alpha) \pmod{\mathfrak{p}} = \alpha, \tag{3.1}$$

for all α in $\mathbb{F}_q^*$. The Teichmüller character $\omega_\mathfrak{p}$ has order $q-1$; hence it generates all multiplicative characters of $\mathbb{F}_q$.

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{p}$. For an integer a, let $s(a) = v_\mathfrak{P}(g(\omega_\mathfrak{p}^{-a}))$, where $v_\mathfrak{P}$ is the $\mathfrak{P}$-adic valuation. Thus $\mathfrak{P}^{s(a)} \,||\, g(\omega_\mathfrak{p}^{-a})$. The following evaluation of $s(a)$ is due to Stickelberger (see [4, p. 344], [29, p. 96]).

Theorem 3.4. *Let p be a prime, and $q = p^s$. For an integer a not divisible by $q-1$, let $a_0 + a_1 p + a_2 p^2 + \cdots + a_{s-1}p^{s-1}$, $0 \le a_i \le p-1$, be the p-adic expansion of the reduction of a modulo $q-1$. Then*

$$s(a) = a_0 + a_1 + \cdots + a_{s-1},$$

that is, $s(a)$ is the sum of the p-adic digits of the reduction of a modulo $q-1$.

An easily proved consequence of Theorem 3.4 is the formula [4, p. 347], [29, p. 98]

$$s(a) = \frac{p-1}{q-1}\sum_{i=0}^{s-1} L(ap^i), \tag{3.2}$$

where $L(x)$ is the reduction of x modulo $q-1$.

We are now ready to give a new proof of the p-rank formula for Singer difference sets.

Theorem 3.5. *For $q = p^s$, let L_0 be the $(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1})$ difference set in the quotient group $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$, as in Theorem 2.1. Then the p-rank of L_0 is*

$$\binom{p+d-2}{d-1}^s + 1.$$

Proof: For $\mathfrak{p}$ a prime ideal in $\mathbb{Z}[\xi_{q^d-1}]$ lying over p, let $\omega_\mathfrak{p}$ be the Teichmüller character on $\mathbb{F}_{q^d}$ and let $\chi = \omega_\mathfrak{p}^{-(q-1)}$. Then χ is a generator of the character group of $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$. From the proof of Theorem 2.1, we know that for each a, $0 < a < \frac{q^d-1}{q-1}$,

$$q \cdot \chi^a(L_0) = g(\chi^a). \tag{3.3}$$

Note that if χ_0 is the trivial character, then $\chi_0(L_0) = |L_0| \not\equiv 0 \pmod p$. Thus by the definition (3.1) of the Teichmüller character and Theorem 3.3, the p-rank of L_0 is $1 + A(q,d)$, where $A(q,d)$ is the number of χ^a, $0 < a < (q^d-1)/(q-1)$, such that $\chi^a(L_0) \pmod{\mathfrak{p}} \neq 0$.

Let $\mathfrak{P}$ be the prime of $\mathbb{Z}[\xi_{q^d-1}, \xi_p]$ lying above $\mathfrak{p}$. Since $\mathfrak{P} \mid \chi^a(L_0)$ if and only if $\mathfrak{p} \mid \chi^a(L_0)$, $A(q,d)$ is equal to the number of χ^a, $0 < a < (q^d-1)/(q-1)$, such that $\mathfrak{P} \nmid \chi^a(L_0)$.

By the definition of $s(a)$ (with q^d in place of q), $\mathfrak{P}^{s((q-1)a)} \,||\, g(\chi^a)$. Since $\mathfrak{P}^{(p-1)s} \,||\, q$, we see from (3.3) that $A(q,d)$ is equal to the number of a, $0 < a < (q^d-1)/(q-1)$, such that $s((q-1)a) = (p-1)s$, which, in turn, is equal to the number of x, $0 < x < q^d - 1$, $(q-1) \mid x$, such that $s(x) = (p-1)s$.

For x with $0 < x < q^d - 1$, write $x = \sum_{j=0}^{d-1} \sum_{i=0}^{s-1} x_{i,j} p^i q^j$, $0 \le x_{i,j} < p$. By (3.2) (with q^d in place of q),

$$s(x) = \frac{p-1}{q^d-1} \sum_{j=0}^{d-1} \sum_{i=0}^{s-1} L(xp^i q^j), \tag{3.4}$$

where $L(y)$ denotes the reduction of y modulo $q^d - 1$. Suppose that $(q-1) \mid x$ and $s(x) = (p-1)s$. Then, by (3.4),

$$(q^d-1)s = \sum_{j=0}^{d-1} \sum_{i=0}^{s-1} L(xp^i q^j). \tag{3.5}$$

Since

$$0 < \sum_{j=0}^{d-1} L(xp^i q^j) \equiv \sum_{j=0}^{d-1} xp^i q^j \equiv 0 \pmod{q^d - 1},$$

it follows that $\sum_{j=0}^{d-1} L(xp^i q^j) \ge q^d - 1$ for each i. Thus, by (3.5),

$$\sum_{j=0}^{d-1} L(xp^i q^j) = q^d - 1 \tag{3.6}$$

for each i. Write $x = a_0 + a_1 q + \cdots + a_{d-1}q^{d-1}$, where $a_j = \sum_{i=0}^{s-1} x_{i,j}p^i$, $0 \le j \le d-1$. Then by (3.6) with $i = 0$, we have $a_0 + a_1 + \cdots + a_{d-1} = q - 1$. Thus $\sum_{j=0}^{d-1} x_{0,j} \ge p - 1$. Similarly, by (3.6) for general i, we obtain

$$\sum_{j=0}^{d-1} x_{i,j} \ge p - 1 \tag{3.7}$$

for *all* i. As

$$(p-1)s \le \sum_{i=0}^{s-1}\sum_{j=0}^{d-1} x_{i,j} = s(x) = (p-1)s,$$

it follows that equality holds in (3.7) for each i. The equation $\sum_{j=0}^{d-1} x_{i,j} = p - 1$, $0 \le x_{i,j} < p$, has $\binom{p+d-2}{d-1}$ solutions for each i, $0 \le i < s$. Therefore $A(q,d) = \binom{p+d-2}{d-1}^s$. This completes the proof. $\square$

Next we show how to compute the 2-ranks of those cyclic difference sets $D_{k,d}$ arising from monomial hyperovals in Section 2. For succinctness, we will actually state the theorem in terms of the 2-rank of the complement $\overline{D_{k,d}}$. (It follows easily from (1.1) that if D is a (v, K, λ) difference set in G then the complement $\overline{D}$ of D in G is a $(v, v-K, \lambda - 2K + v)$ difference set in G.) This is just a matter of convenience, as the 2-rank of the difference set $D_{k,d}$ is exactly 1 more than the 2-rank of the complement $\overline{D_{k,d}}$ (see the proof of Theorem 3.6).

Theorem 3.6. *Let $D_{k,d}$ be the $(2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$ cyclic difference set in $\mathbb{F}_{2^d}^*$ constructed from the hyperoval $D(x^k)$ as in Theorem 2.5, and let $\overline{D_{k,d}}$ be the complement of $D_{k,d}$ in $\mathbb{F}_{2^d}^*$. Then the 2-rank of $\overline{D_{k,d}}$ is equal to the number of a's, $0 < a < 2^d - 1$, such that*

$$s(a) + s((k-1)a) = s(ka) + 1, \tag{3.8}$$

where $s(a)$ is as defined above Theorem 3.4 with $q = 2^d$.

Proof: For $\mathfrak{p}$ a prime ideal in $\mathbb{Z}[\xi_{2^d-1}]$ lying over 2, let $\omega = \omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_{2^d}$. By (2.6), we see that for each a, $0 < a < 2^d - 1$,

$$-2 \cdot \omega^{-(k-1)a}\left(\overline{D_{k,d}}\right) = J(\omega^{-a}, \omega^{-(k-1)a}). \tag{3.9}$$

By the definition of $s(a)$ (with $q = 2^d$) and (1.4),

$$\mathfrak{p}^{s(a)+s((k-1)a)-s(ka)} \,||\, J(\omega^{-a}, \omega^{-(k-1)a}). \tag{3.10}$$

Since $\mathfrak{p}\,||\,2$, we see from (3.9) that the number of a's, $0 < a < 2^d - 1$, such that $\omega^{-(k-1)a}\left(\overline{D_{k,d}}\right) \pmod{\mathfrak{p}} \ne 0$, is equal to the number of a's, $0 < a < 2^d - 1$, such that $s(a) + s((k-1)a) = s(ka) + 1$. Since the cardinality of $\overline{D_{k,d}}$ is $2^{d-1} \equiv 0 \pmod 2$, $\chi_0(\overline{D_{k,d}}) \pmod{\mathfrak{p}}$ equals 0 for the trivial character χ_0. (In contrast, $\chi_0(D_{k,d}) \pmod{\mathfrak{p}}$ equals 1, which is why we prefer to state the theorem in terms of $\overline{D_{k,d}}$.) Thus, by Theorem 3.3, we see that the 2-rank of $\overline{D_{k,d}}$ is equal to the number of a's, $0 < a < 2^d - 1$, for which $s(a) + s((k-1)a) = s(ka) + 1$. This completes the proof. $\square$

Let $B_k(d)$ be the number of a's, $0 < a < 2^d - 1$, for which $s(a) + s((k-1)a) = s(ka) + 1$. By the above theorem, in order to compute the 2-rank of $D_{k,d}$, we need to compute $B_k(d)$. We will discuss the determination of $B_k(d)$ in the next section. But first of all, we observe that $B_k(d)$ is always a multiple of d. We state this as a lemma.

Lemma 3.7. *Let $B_k(d)$ be the number of a's, $0 < a < 2^d - 1$, for which $s(a) + s((k-1)a) = s(ka) + 1$. Then $d \mid B_k(d)$.*

Proof: For any a, $0 < a < 2^d - 1$, it follows easily from (3.2) that

$$s(a) + s((k-1)a) - s(ka) = \sum_{i=0}^{d-1} \left(\left\lfloor \frac{2^i ka}{2^d - 1} \right\rfloor - \left\lfloor \frac{2^i a}{2^d - 1} \right\rfloor - \left\lfloor \frac{2^i (k-1)a}{2^d - 1} \right\rfloor \right), \tag{3.11}$$

where $\lfloor x \rfloor$ denotes the greatest integer $\le x$ (see [4, p. 349], [29, p. 98]).

Clearly, if a is a solution to $s(a) + s((k-1)a) = s(ka) + 1$, then $a \cdot 2^j$ is also a solution, for all j, $0 \le j \le d-1$. We contend that $a \cdot 2^j$, $j = 0, 1, \ldots, d-1$, are necessarily *distinct* modulo $2^d - 1$. If they were not distinct, then the sum on i in (3.11) would have more than one term equal to 1, contradicting the fact that $s(a) + s((k-1)a) - s(ka) = 1$. This completes the proof. □

4. Enumeration of Cyclic Binary Strings and Computation of 2-ranks

Let d be an integer ≥ 2. In this section, we are concerned with determining explicitly the 2-ranks of the difference sets $\overline{D_{k,d}}$ corresponding to the hyperovals $D(x^k)$ (which, by the remark preceding Theorem 3.6, is equivalent to determining the 2-ranks of the difference sets $D_{k,d}$ themselves). By Theorem 3.6, the 2-rank of $\overline{D_{k,d}}$ equals the number $B_k(d)$ of solutions a, $0 < a < 2^d - 1$, to equation (3.8). The case of the difference sets arising from the translation and the regular hyperovals is already covered by Theorem 3.5, as these difference sets are instances of Singer difference sets (see the last paragraph of Section 2). Hence, we concentrate on the difference sets arising from the Segre and the Glynn hyperovals. Most of the time we will not actually deal with the number $B_k(d)$ of solutions itself, but with the quantity $A_k(d) = B_k(d)/d$. For the convenience of the reader we have listed the first few values for $A_6(d)$ (the Segre case, see (2.3)), for $A_{\sigma+\gamma}(d)$ (the Glynn type (I) case, see (2.4)), and for $A_{3\sigma+4}(d)$ (the Glynn type (II) case, see (2.5)). These values were originally found by the computer algebra package MAGMA [6].

d	3	5	7	9	11	13	15	17	19	21	23	25
$A_6(d)$	1	3	5	9	15	25	41	67	109	177	287	465
$A_{\sigma+\gamma}(d)$	1	1	3	7	13	23	45	87	167	321	619	1193
$A_{3\sigma+4}(d)$	1	1	5	7	21	37	89	173	383	777	1665	3441

Table 1

When we entered the values from the table into the *Maple* package `gfun` [23], we were able to guess a linear recurrence for the numbers $A_k(d)$ in each of the three cases. These recurrences are established by rather elaborate combinatorial arguments in Theorems 4.3, 4.6 and 4.8. Consequently, we obtain explicit formulas for the 2-ranks of the difference sets $D_{k,d}$ corresponding to the Segre and Glynn hyperovals $D(x^k)$; see Corollaries 4.4, 4.7 and 4.9.

Table 1 suggests that for $d \geq 15$ the 2-ranks $A_6(d)$ for the Segre case are the smallest, while the 2-ranks $A_{3\sigma+4}(d)$ for the Glynn type (II) case are the largest. This observation is established in Lemma 6.1.

Our first goal is to determine $B_6(d)$ explicitly in terms of Fibonacci numbers. The result, Theorem 4.3, was conjectured by Xiang [31].

Given any integer x not divisible by $2^d - 1$, recall that by Theorem 3.4 with $q = 2^d$, $s(x)$ equals the number of 1's in the binary representation of x reduced modulo $2^d - 1$. Now, the binary representation of $2x \bmod 2^d - 1$ is simply the rotation of the binary representation of $x \bmod 2^d - 1$ by "one step", i.e., all the digits are moved one step to the left, with a 1 that would be moved beyond the leftmost place moved ("rotated") to the rightmost place. This implies that $s(x) = s(2x)$. Therefore, given any solution to (3.8), multiples of the solution by powers of 2 will also give solutions to (3.8).

Proposition 4.1. *Let d be an integer ≥ 2. The binary representations of all the solutions $a \bmod 2^d - 1$ to the equation*

$$s(a) + s(5a) = s(6a) + 1 \tag{4.1}$$

can be constructed by the following procedure:

Step 1. Form all the possible binary strings of length $\leq d$ by concatenating blocks of the form 01, 0011, 00111, *subject to the following restrictions:*

(A) *In a string of length $< d$, the rightmost block must be* 01, *and the block* 00111 *must not occur.*

(B) *In a string of length d, the block* 00111 *occurs exactly once, namely, as the rightmost block.* (*In particular, strings of length d can only occur for odd d.*)

Step 2. Given a string of length k obtained through Step 1, append $(d-k)$ 0's on the left to form a string of length d.

Step 3. All the solutions $a \bmod 2^d - 1$ to (4.1), *or rather their binary representations, are obtained by forming all possible rotations of the strings that were constructed in Step 2.*

Before we move on to a proof of the proposition, we illustrate this construction by an example.

Example 4.2. Let $d = 9$. Then all possible strings formed in Step 1 are (the bars indicate separation of blocks)

$$\begin{gathered} 01,\ 01|01,\ 01|01|01,\ 01|01|01|01,\ 0011|01, \\ 0011|01|01,\ 01|0011|01,\ 01|01|00111,\ 0011|00111. \end{gathered} \tag{4.2}$$

Hence, according to Steps 2 and 3, the solutions $a \bmod 2^d - 1$ to (4.1), in binary notation, are all the possible rotations of

$$\begin{gathered} 000000001,\ 000000101,\ 000010101,\ 001010101,\ 000001101, \\ 000110101,\ 001001101,\ 010100111,\ 001100111. \end{gathered} \tag{4.3}$$

Therefore, the solutions are

$$1, 5, 21, 85, 13, 53, 77, 167, 103,$$

and their multiples by powers of 2, for a total of $9 \cdot 9 = 81$ solutions.

Proof of Proposition 4.1. It is straightforward to check that the numbers obtained by the proposed construction are indeed solutions to (4.1). We leave this to the reader.

It remains to be shown that there cannot be other solutions to (4.1). We do this by performing a case-by-case analysis which rules out all other possibilities.

From now on, when we talk about some number $x \bmod 2^d - 1$, we always assume that x is reduced mod $2^d - 1$ to a number between 0 and $2^d - 2$. When we refer to a, $5a$, and $6a$, these numbers are to be viewed mod $2^d - 1$.

Before we start our case-by-case analysis, it is helpful to recall what we would like to achieve. We want to find each number a such that the number of 1's in the binary representation of $6a$ is exactly one less than the number of 1's in the binary representation of a plus the number of 1's in the binary representation of $5a$.

On the other hand, by carrying out the addition $a + 5a = 6a \pmod{2^d - 1}$, we see that the number of 1's in the binary representation of $6a$ can be at most the total of the number of 1's in the binary representations of a and $5a$ minus the number of instances of a 1 occurring at the same place in a and $5a$. To give an example, if $d = 5$, and if $a = 11010$, so $5a = 00110$, then the number of 1's in $6a$ can be at most $3 + 2 - 1 = 4$. (The number of 1's in the binary representation of a is 3, the number of 1's in the binary representation of $5a$ is 2, and there is a 1 in both a and $5a$ in the second position from the right.) In fact, $6a = 00001$, so the number of 1's in $6a$ is even less.

Thus we can limit our search to a's for which there is *exactly one* such instance of a 1 in the same position in a and $5a$. In particular, if we detect *two* such instances in a and $5a$, then a cannot be a solution to (4.1). To guarantee that the number of 1's in the binary representation of $6a$ is *exactly* one less (as opposed to two or more less), we must have a 0 in both a and $5a$ in the position which is immediately to the left of the position where 1 occurs in both a and $5a$.

In the analysis that follows, it does not matter whether we consider a or $2^m a$, for a positive integer m. In terms of binary representations this means that it does not matter whether we consider the binary representation of a or any cyclic permutation of it.

Now we turn to our case-by-case analysis. Since Proposition 4.1 is easily checked for the cases $d = 2, 3, 4, 5$, we may assume in the following that $d \geq 6$.

Case 1. The block 11111 *occurs in the binary representation of* a. Suppose that 11111 occurs in the binary representation of a. Then, since $5a = a + 4a$, we have

$$\begin{array}{rl} a = & \ldots.11111.. \\ 4a = & ..11111\ldots. \\ \hline 5a = & \ldots.11\ldots.. \end{array}$$

So, there are two instances of 1's in the same position in a and $5a$. Hence, a cannot be a solution to (4.1).

Case 2. The block 1111 *occurs in the binary representation of* a. Since we already ruled out that 11111 occurs, we may assume that there is a 0 before, and a 0 after 1111. We have

$$\begin{array}{rl} a = & \ldots.011110.. \\ 4a = & ..011110\ldots. \\ \hline 5a = & \ldots\ldots.\underline{\ }\ldots. \end{array}$$

Now, if in the underlined position there is no 1 carrying over from the right, then the addition would give

$$\begin{array}{rl} a = & \ldots.011110.. \\ 4a = & ..011110\ldots. \\ \hline 5a = & \ldots..101\ldots. \end{array}$$

Again we are encountering two positions with 1's in both a and $5a$, and thus a cannot be a solution to (4.1).

On the other hand, if a 1 does carry over, then we have

$$\begin{array}{rl} a = & \ldots.011110.. \\ 4a = & ..011110\ldots. \\ \hline 5a = & \ldots..110\ldots. \end{array}$$

So again, a cannot be a solution to (4.1).

Case 3. The block 111 *occurs in the binary representation of* a. Since we already ruled out that 1111 occurs, we may assume that there is a 0 before, and a 0 after 111. We have

$$\begin{array}{rl} a = & \ldots.01110.. \\ 4a = & ..01110\ldots. \\ \hline 5a = & \ldots\ldots\ldots.. \end{array}$$

If to the left of the block 01110 we would have a 1,

$$\begin{array}{rl} a = & \ldots.101110.. \\ 4a = & ..101110\ldots. \\ \hline 5a = & \ldots\ldots.\underline{\ }\ldots. \end{array}$$

then, regardless of whether a 1 carries over to the underlined position or not (see Case 2 for an analogous consideration), we would obtain two positions with 1's in both a and $5a$, and so a cannot be a solution to (4.1).

Therefore, the only way to have the block 111 is in the form $\ldots 001110 \ldots.$

Case 4. The block 0110 *occurs in the binary representation of* a. Let us first assume that we have a 1 on the left of this block, so that we encounter

$$\begin{array}{rl} a = & \ldots.10110.. \\ 4a = & ..10110\ldots. \\ \hline 5a = & \ldots\ldots\underline{\ }\ldots. \end{array}$$

Now, if no 1 carries over to the underlined position, then we have

$$\begin{array}{rl} a = & \ldots.10110.. \\ 4a = & ..10110\ldots. \\ \hline 5a = & \ldots..1\underline{1}\ldots. \end{array}$$

So, there is a 1 in that position in both a and $5a$, and there is a 1 just left of that position in $5a$. By what we observed earlier, such a number a cannot be a solution to (4.1). If 1 does carry over to the underlined position, then we have

$$\begin{array}{rl} a = & \dots x10110\,.\,. \\ 4a = & .\,.10110\dots. \\ \hline 5a = & \dots y10\underline{0}\dots. \end{array}$$

where either x or y equals 1. Again, a cannot be a solution to (4.1).

Therefore, the only way to have a block 0110 is in the form $\dots 00110\dots$.

At this point, let us summarize our observations. The conclusions from the considerations in Cases 1–4 are that the (cyclic) binary strings of length d for a that we are looking for must be built out of the blocks 00111, 0011, and 01, with possibly filling 0's placed in between.

It is not difficult to see that it is only possible to insert filling 0's in one place in a (cyclic) binary string. For, otherwise we would have at least two instances of a 1 in the same place in a and $5a$. For the same reason, if a block 00111 occurs, then it can appear only once, and no filling 0's are allowed. Finally, it is easy to see that an all 0 string, or a string built out of blocks of the form 0011 plus filling 0's, or a string where filling 0's are adjacent to two consecutive 1's, does not give a solution to (4.1). All the remaining possibilities are indeed covered by the construction in the statement of Proposition 4.1. This concludes the proof of the proposition. □

Proposition 4.1 yields the following formula for the number $B_6(d)$ of solutions to (4.1).

Theorem 4.3. *Write $A_6(d) = B_6(d)/d$, where $B_6(d)$ is the number of solutions mod $2^d - 1$ to equation* (4.1). *Then for $d \geq 6$, $A_6(d)$ satisfies the recurrence*

$$A_6(d) = A_6(d-2) + A_6(d-4) + 1, \tag{4.4}$$

with initial conditions $A_6(2) = 0$, $A_6(3) = 1$, $A_6(4) = 1$, $A_6(5) = 3$. Equivalently, for any positive integer m we have $B_6(2m) = 2m(F_m - 1)$ and $B_6(2m+1) = (2m+1)(2F_m - 1)$, where F_n is the n-th Fibonacci number ($F_0 = F_1 = 1$).

Proof: Clearly, the recurrence (4.4) can be viewed as a recurrence for the number $B_6(d)/d$ of strings that are constructed in Step 1 of Proposition 4.1, i.e., before appending 0's and rotating the obtained strings of length d. (There are $B_6(d)/d$ such strings, since due to the particular form of the strings, all the d rotations in Step 3 are indeed different from each other.)

On the basis of this observation, it is easy to demonstrate the recurrence (4.4). For, given d, the strings that are constructed in Step 1 can be separated into three sets: first, there is the string 01 of length 2, then there is the set of strings of length greater than 2 with leftmost block 01, and finally there is the set of strings with leftmost block 0011. The former set of strings can be obtained by performing Step 1 with d replaced by $d-2$ and then appending 01 to the left of each of the obtained strings. The latter set of strings can be obtained by performing Step 1 with d replaced by $d-4$ and then appending 0011 to the left of each of the obtained strings. Summing, we obtain the recurrence (4.4) for $B_6(d)/d$.

From the recurrence, the explicit formulas for $B_6(d)$ in terms of Fibonacci numbers follow immediately. $\square$

As a corollary, we have the following result on the 2-ranks of those cyclic difference sets constructed from the Segre hyperovals.

Corollary 4.4. *Let d be an odd integer, $d \geq 5$, and let $D_{6,d}$ be the $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference set in $\mathbb{F}_{2^d}^*$ corresponding to the Segre hyperoval $D(x^6)$, as in Theorem 2.5 with $k=6$. Let $\overline{D_{6,d}}$ be the complement of $D_{6,d}$ in $\mathbb{F}_{2^d}^*$. Then the 2-rank $B_6(d)$ of $\overline{D_{6,d}}$ is equal to $d(2F_{(d-1)/2}-1)$, where F_n is the nth Fibonacci number ($F_0 = F_1 = 1$).*

Proof: This is immediate from Theorem 3.6 and Theorem 4.3. $\square$

Next we turn to the computation of the 2-ranks of the cyclic difference set arising from the two types of Glynn hyperovals. According to Theorem 3.6, (2.4) and (2.5), we need to compute the number $B_k(d)$ of solutions a mod 2^d-1 to

$$s(a) + s((k-1)a) = s(ka) + 1, \tag{4.5}$$

where d is odd, $d \geq 7$, and $k = \sigma + \gamma$ or $k = 3\sigma + 4$, with $\sigma = 2^{(d+1)/2}$, and $\gamma = 2^{(3d+1)/4}$ if $d \equiv 1 \bmod 4$, whereas $\gamma = 2^{(d+1)/4}$ if $d \equiv 3 \bmod 4$. These are much more difficult problems than the counting problem in the case $k=6$. We resolve them in Theorems 4.6 and 4.8 by making appeal to the so-called "transfer matrix method" (see [27, Sec. 4.7]). (We could have proved Theorem 4.3 by means of the transfer matrix method as well. We preferred to take the more direct approach via Proposition 4.1.)

In the proofs of Theorems 4.6 and 4.8, we will make use of the result (in the folklore) that when it is known (by some abstract means) that a sequence satisfies *some* linear recurrence, and when a bound for the order of the recurrence is also known, then one needs only to check a certain number of special instances of a *specific* recurrence to prove that the sequence satisfies this recurrence "always". We give the precise statement in the lemma below. For the sake of completeness, we also supply a proof.

Lemma 4.5. *Let $(f_n)_{n\geq 0}$ be a sequence of complex numbers. Suppose that we know that the generating function $\sum_{n\geq 0} f_n z^n$ for the sequence is rational, i.e., that it equals $p(z)/q(z)$, where $p(z)$ and $q(z)$ are polynomials in z, and that the degree of the numerator, $p(z)$, is at most P, and the degree of the denominator, $q(z)$, is at most Q. If the sequence (f_n) satisfies the recurrence*

$$\sum_{i=0}^{k} a_i f_{n-i} = c \tag{4.6}$$

for $n = n_0, \dots, N$, where $n_0 \geq k$, $N = \max\{P+k+1, Q+n_0\}$, and where $a_0, a_1 \dots, a_k$ and c are some given complex numbers, then the recurrence (4.6) is satisfied for all $n \geq n_0$.

Proof: Since (4.6) is satisfied for $n = n_0, \dots, N$, we have

$$a(z) \sum_{n\geq 0} f_n z^n = r(z) + c/(1-z) + z^{N+1} S(z), \tag{4.7}$$

where $a(z) = \sum_{i=0}^{k} a_i z^i$, $r(z)$ is a polynomial of degree less than n_0, and $S(z)$ is some formal power series, the coefficients of which "measure" how (4.6) fails for $n > N$. In particular, $S(z)$ vanishes if and only if (4.6) holds for *all* $n \ge n_0$. Now we multiply both sides of (4.7) by $(1-z)q(z)$. This gives

$$(1-z)a(z)p(z) = (1-z)q(z)r(z) + cq(z) + z^{N+1}(1-z)q(z)S(z).$$

In this equation, the term on the left-hand side and the first two terms on the right-hand side all have degree less than $N+1$. It follows that $z^{N+1}(1-z)q(z)S(z) = 0$, whence $S(z) = 0$. This completes the proof. □

Now we are ready to determine the number of solutions to (4.5) for the Glynn cases. We start with the Glynn type (II) case because it is easier to handle.

Theorem 4.6. *Let d be an odd integer, $d \ge 3$. Let $B_{3\sigma+4}(d)$ be defined as in the first paragraph of this section, and let $A_{3\sigma+4}(d) = B_{3\sigma+4}(d)/d$. Then*

$$A_{3\sigma+4}(d) = A_{3\sigma+4}(d-2) + 3A_{3\sigma+4}(d-4) - A_{3\sigma+4}(d-6) - A_{3\sigma+4}(d-8) + 1, \qquad (4.8)$$

for all odd d, $d \ge 11$, with initial values as given in Table 1.

Proof: First of all, from the proof of Proposition 4.1, we see that the solutions a, $0 < a < 2^d - 1$, to equation (4.5) are characterized by the following property (the pertinent considerations in the proof of Proposition 4.1 are valid for generic k, i.e., they do not restrict to the case $k = 6$):

(4.9) There is exactly one instance of a 1 occurring at the same place in a and $(k-1)a$, and immediately to the left of those 1's there is a 0 in both a and $(k-1)a$,

where we view a and $(k-1)a \pmod{2^d - 1}$ as binary strings of length d.

We are actually concerned not with the number $B_k(d)$ of *all* solutions to (4.5), but rather with $A_k(d) = B_k(d)/d$. Since any solution a immediately gives rise to d solutions by forming all possible rotations of a, we may, without loss of generality, restrict our attention to those solutions a where the instance of a 1 imposed by (4.9) occurs exactly in the *middle* of the string. The number $A_k(d)$ then is the number of these *special* solutions.

Now, for a proof of the theorem, we define a bijection between these special solutions to (4.5) (with $k = 3\sigma + 4$, where $\sigma = 2^{(d+1)/2}$) and a set of closed walks in a certain directed graph D. As we demonstrate at the end, it then follows from first principles that the generating function for the number of these closed walks, and hence for the number of solutions to (4.5), is rational (see also [27, Sec. 4.7]). Finally, we check (4.8) for enough (odd) values of d so that Lemma 4.5 will imply that (4.8) has to hold for *all* odd $d \ge 11$.

In order to motivate the construction of the aforementioned directed graph D, we analyse, for a given special solution a to (4.5), the computation of $(k-1)a$ and ka mod $2^d - 1$. Let $d = 2r - 1$, with $r \ge 2$, and let the binary representation of a be $a_{2r-2} \dots a_1 a_0$. Since $k - 1 = 3\sigma + 3 = 3 \cdot 2^{(d+1)/2} + 3 = 2^{r+1} + 2^r + 2 + 1$, we may compute $(k-1)a$ and

$ka = (k-1)a + a \bmod 2^d - 1$ as follows:

$$\begin{array}{rccccccc}
a = & a_{2r-2} & \dots & a_r & a_{r-1} & a_{r-2} & \dots & a_0 \\
2a = & a_{2r-3} & \dots & a_{r-1} & a_{r-2} & a_{r-3} & \dots & a_{2r-2} \\
2^{r+1}a = & a_{r-3} & \dots & a_{2r-2} & a_{2r-3} & a_{2r-4} & \dots & a_{r-2} \\
2^r a = & a_{r-2} & \dots & a_0 & a_{2r-2} & a_{2r-3} & \dots & a_{r-1} \\ \hline
(k-1)a = & y_{2r-2} & \dots & y_r & y_{r-1} & y_{r-2} & \dots & y_0 \\
a = & a_{2r-2} & \dots & a_r & a_{r-1} & a_{r-2} & \dots & a_0 \\ \hline
ka = & z_{2r-2} & \dots & z_r & z_{r-1} & z_{r-2} & \dots & z_0
\end{array} \tag{4.10}$$

where

$$a_i + a_{i-1} + a_{r+i-2} + a_{r+i-1} + b_{i-1} = y_i + 2b_i, \quad \text{for } i = 0, 1, \dots, 2r-2, \tag{4.11}$$

$$y_i + a_i + c_{i-1} = z_i + 2c_i, \quad \text{for } i = 0, 1, \dots, 2r-2, \tag{4.12}$$

for some integers b_i, c_i with $0 \le b_i \le 3$, $i = 0, 1, \dots, 2r-2$, $c_{r-1} = 1$, and $c_i = 0$ for $i = 0, 1, \dots, r-2, r, \dots, 2r-2$, with the convention that indices are read modulo $2r-1$ throughout. The integer b_i is the carry-over from the ith place to the $(i+1)$th during the addition that gives $(k-1)a$ in (4.10), while c_i is the carry-over from the ith place to the $(i+1)$th during the addition of $(k-1)a$ and a in (4.10) that gives ka. Here, places are counted from the right starting with 0; for example, in the top row of (4.10), the digit a_0 is in the 0th place and the digit a_1 is in the 1th place. (Indeed, as is not difficult to see, there is a unique such choice of b_i's and c_i's which satisfy (4.11) and (4.12) such that the y_i's and z_i's are the digits in the additions given by (4.10).) Equation (4.12), together with the above assignments for the c_i's, reflects the conditions imposed by (4.9) with the 1's in the middle place.

The subsequent considerations become more transparent, if in (4.11) and (4.12) we perform a relabelling. Given a sequence $(x_i)_{i=0,\dots,2r-2}$, where (x_i) can be any of (a_i), (b_i), (c_i), (y_i), or (z_i), define the new sequence $(\tilde{x}_j)_{j=0,\dots,2r-2}$ by $\tilde{x}_j := x_{(r-1)j}$. Note that since $(r-1, d) = (r-1, 2r-1) = 1$, the sequence $(\tilde{x}_j)_{j=0,\dots,2r-2}$ is a permutation of $(x_i)_{i=0,\dots,2r-2}$ (recall that indices are read modulo $2r-1$). Now, by putting $i = (r-1)j$, equations (4.11) and (4.12) read, in terms of the transformed sequences,

$$\tilde{a}_j + \tilde{a}_{j+2} + \tilde{a}_{j+3} + \tilde{a}_{j+1} + \tilde{b}_{j+2} = \tilde{y}_j + 2\tilde{b}_j, \quad \text{for } j = 0, 1, \dots, 2r-2, \tag{4.13}$$

$$\tilde{y}_j + \tilde{a}_j + \tilde{c}_{j+2} = \tilde{z}_j + 2\tilde{c}_j, \quad \text{for } j = 0, 1, \dots, 2r-2, \tag{4.14}$$

where $\tilde{b}_j$, $\tilde{c}_j$ are integers with $0 \le \tilde{b}_j \le 3$, $j = 0, 1, \dots, 2r-2$, $\tilde{c}_1 = 1$, and $\tilde{c}_j = 0$ for $j = 0, 2, 3, \dots, 2r-2$, where again all indices are viewed modulo $2r-1$.

Construct a directed graph D as follows. The set of vertices of D is the set of all vectors $(a', a'', a''', b', b'', c', c'')$ with $0 \le a', a'', a''' \le 1$, $0 \le b', b'' \le 3$, and $0 \le c', c'' \le 1$.

Corresponding to any special solution a, $0 < a < 2^d - 1$, to equation (4.5) with $k = 3\sigma + 4$, define (in the notation of (4.13)–(4.14)) the $2r-1$ vertices

$$v_j = (\tilde{a}_j, \tilde{a}_{j+1}, \tilde{a}_{j+2}, \tilde{b}_j, \tilde{b}_{j+1}, \tilde{c}_j, \tilde{c}_{j+1}), \tag{4.15}$$

$0 \le j \le 2r-2$. Our construction of the directed edges will be motivated by the desire to obtain, via equations (4.13) and (4.14), a bijection between the special solutions a and certain closed walks in D of length $d = 2r - 1$. A solution a will correspond to the walk

$$v_0 \ \to\ v_1 \ \to\ v_2 \ \to \cdots \to\ v_{2r-2} \ \to\ v_0, \tag{4.16}$$

and vice versa.

We connect a vertex $(a', a'', a''', b', b'', c', c'')$ to a vertex $(A', A'', A''', B', B'', C', C'')$ by a directed edge if and only if

$$a'' = A', \tag{4.17}$$

$$a''' = A'', \tag{4.18}$$

$$b'' = B', \tag{4.19}$$

$$c'' = C', \tag{4.20}$$

$$Y := (a' + a''' + A''' + a'' + B'' - 2b') \in \{0, 1\}, \tag{4.21}$$

$$(Y + a' + C'' - 2c') \in \{0, 1\}. \tag{4.22}$$

To motivate the construction of such directed edges, the reader should think of $(a', a'', a''', b', b'', c', c'')$ and $(A', A'', A''', B', B'', C', C'')$ as $v_j = (\tilde a_j, \tilde a_{j+1}, \tilde a_{j+2}, \tilde b_j, \tilde b_{j+1}, \tilde c_j, \tilde c_{j+1})$ and $v_{j+1} = (\tilde a_{j+1}, \tilde a_{j+2}, \tilde a_{j+3}, \tilde b_{j+1}, \tilde b_{j+2}, \tilde c_{j+1}, \tilde c_{j+2})$, respectively, $j = 0, 1, \dots, 2r - 2$, and should observe that (4.21) reflects (4.13), and that (4.22) reflects (4.14).

Define the sets V_0, V_1, V_2 as the sets of vertices $(a', a'', a''', b', b'', c', c'')$ for which (c', c'') equals $(0, 0)$, $(0, 1)$, $(1, 0)$, respectively. With these definitions, we claim that for odd $d \ge 3$ the special solutions a, $0 < a < 2^d - 1$, to equation (4.5) with $k = 3\sigma + 4$ are in bijection with the *special* closed walks of length d which start in V_1, in the first step move to V_2, and from there on visit only vertices from V_0, until they return to the starting vertex from V_1. We leave it to the reader to check the claim in detail, as this is a straightforward task (cf. (4.16) and (4.15)).

Finally, let $\boldsymbol{A}_{ij}$ be the adjacency matrix of D restricted to the information about edges from V_i to V_j, $i, j \in \{0, 1, 2\}$, that is, $\boldsymbol{A}_{ij}$ is the matrix with rows labelled by the vertices from V_i and columns labelled by the vertices from V_j, with an entry 1 in some row and column whenever that particular vertex of V_i is connected to that particular vertex of V_j, all other entries being 0. Then, by basic principles (which are easily verified from scratch), the number of the above defined special closed walks of length d is equal to the trace of $\boldsymbol{A}_{12}\boldsymbol{A}_{20}\boldsymbol{A}_{00}^{d-3}\boldsymbol{A}_{01}$. Hence, by means of our bijection between special solutions to (4.5) and special closed walks in D, we have

$$\begin{aligned}\sum_{r\ge 2} A_{3\cdot 2^r+4}(2r-1) z^{r-2} &= \operatorname{tr}\left(\sum_{j=0}^{\infty} \boldsymbol{A}_{12}\boldsymbol{A}_{20}\boldsymbol{A}_{00}^{2j}\boldsymbol{A}_{01} z^j\right)\\ &= \operatorname{tr}\left(\boldsymbol{A}_{12}\boldsymbol{A}_{20}(\boldsymbol{I} - \boldsymbol{A}_{00}^2 z)^{-1}\boldsymbol{A}_{01}\right).\end{aligned} \tag{4.23}$$

We would be done if we could compute the expression on the right-hand side of (4.23). However, the matrix $\boldsymbol{A}_{00}$ is a 128×128 matrix, and with today's technology it is still not easy to compute the inverse of a 128×128 matrix, such as $(\boldsymbol{I} - \boldsymbol{A}_{00}^2 z)$, which has the indeterminate z sitting inside. We circumvent this difficulty by appealing to Lemma 4.5.

On the right-hand side of (4.23) we have the trace of a matrix, all the entries of which are rational in z. Hence, the right-hand side, and so also the left-hand side, is rational in z. Taking into account that the matrix $\boldsymbol{A}_{00}$ is a 128×128 matrix, we see that we may write the left-hand side as $p(z)/q(z)$ where the degree of $p(z)$ is at most 127 and the degree of $q(z)$ is at most 128. Now we are in the position to invoke Lemma 4.5, with $n_0 = k = 4$, $P = 127$, $Q = 128$, once we are able to verify the recurrence (4.8) for $d = 11, 13, \dots, 267$. In view of our characterization of $A_{3\sigma+4}(d) = A_{3\cdot 2^r+4}(2r-1)$ as the trace of $\boldsymbol{A}_{12}\boldsymbol{A}_{20}\boldsymbol{A}_{00}^{d-3}\boldsymbol{A}_{01}$, this is routinely performed on a computer[1].

Thus, the proof of the theorem is complete. □

By combining Theorems 4.6 and 3.6, we are now able to precisely determine the 2-ranks of the difference sets corresponding to the Glynn type (II) hyperovals.

Corollary 4.7. *Let d be an odd integer, $d \ge 3$, and set $\sigma = 2^{(d+1)/2}$. Let $D_{3\sigma+4,d}$ be the $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference set in $\mathbb{F}_{2^d}^*$ corresponding to the Glynn type (II) hyperoval $D(x^{3\sigma+4})$, as in Theorem 2.5. Let $\overline{D_{3\sigma+4,d}}$ be the complement of $D_{3\sigma+4,d}$ in $\mathbb{F}_{2^d}^*$. Then the 2-rank $B_{3\sigma+4}(d)$ of $\overline{D_{3\sigma+4,d}}$ equals $dA_{3\sigma+4}(d)$, where $A_{3\sigma+4}(3) = 1$, $A_{3\sigma+4}(5) = 1$, $A_{3\sigma+4}(7) = 5$, $A_{3\sigma+4}(9) = 7$, and for $d \ge 11$, $A_{3\sigma+4}(d)$ satisfies the recurrence (4.8).*

Next we turn to the Glynn type (I) case.

Theorem 4.8. *Let d be an odd integer, $d \ge 3$. Let $B_{\sigma+\gamma}(d)$ be defined as in the first paragraph of this section, and let $A_{\sigma+\gamma}(d) = B_{\sigma+\gamma}(d)/d$. Then*

$$A_{\sigma+\gamma}(d) = A_{\sigma+\gamma}(d-2) + A_{\sigma+\gamma}(d-4) + A_{\sigma+\gamma}(d-6) + A_{\sigma+\gamma}(d-8) - 1, \tag{4.24}$$

for all odd d, $d \ge 13$, with initial values as given in Table 1.

Proof: We proceed in the spirit of the proof of Theorem 4.6. Here we regard $A_{\sigma+\gamma}(d)$ as the number of special solutions a, $0 < a < 2^d - 1$, to (4.5) (where $k = \sigma + \gamma$) with the instance of a 1 imposed by (4.9) occurring exactly at the mth place if $d = 4m-1$, and exactly at the $(3m+1)$th place if $d = 4m+1$ (where, again, we count places from the right starting with 0). We will define a bijection between these special solutions and certain closed walks in a directed graph D.

We distinguish between the cases $d = 4m-1$ and $d = 4m+1$, noting that γ is defined differently in these two cases (see (2.4)).

First let $d = 4m-1$, $m \ge 2$. In this case we have $\sigma = 2^{2m}$ and $\gamma = 2^m$, by (2.4).

We analyse, for a given special solution a to (4.5), the computation of $(k-1)a$ and $ka \bmod 2^d - 1 = 2^{4m-1} - 1$. Let the binary representation of a be $a_{4m-2} \dots a_1 a_0$. Since $k = \sigma + \gamma = 2^{2m} + 2^m$, we may compute ka in the following two ways:

$$\begin{array}{r} 2^{2m}a = \\ 2^m a = \\ ka = \end{array} \begin{array}{cccccccccccc} a_{2m-2} & \dots & a_m & a_{m-1} & \dots & a_0 & a_{4m-2} & \dots & a_{3m-1} & a_{3m-2} & \dots & a_{2m-1} \\ a_{3m-2} & \dots & a_{2m} & a_{2m-1} & \dots & a_m & a_{m-1} & \dots & a_0 & a_{4m-2} & \dots & a_{3m-1} \\ \hline z_{4m-2} & \dots & z_{3m} & z_{3m-1} & \dots & z_{2m} & z_{2m-1} & \dots & z_m & z_{m-1} & \dots & z_0 \end{array} \begin{array}{l} \left.\vphantom{\begin{array}{c} a \\ a \end{array}}\right\} + \\ \\ \end{array} \tag{4.25}$$

[1] *Maple* and *Mathematica* codes for generating the matrices $\boldsymbol{A}_{00}$, $\boldsymbol{A}_{01}$, $\boldsymbol{A}_{12}$, $\boldsymbol{A}_{20}$ can be obtained on request from the authors, or by WWW at `http://radon.mat.univie.ac.at/People/kratt/artikel/glynn.html`. The verification of (4.8) for $d = 11, 13, \dots, 267$ took 8 minutes on a Pentium with 133 MHz.

and

$$\left.\begin{array}{r|ccccccccccc} (k-1)a= & y_{4m-2} & \dots & y_{3m} & y_{3m-1} & \dots & y_{2m} & y_{2m-1} & \dots & y_m & y_{m-1} & \dots & y_0 \\ a= & a_{4m-2} & \dots & a_{3m} & a_{3m-1} & \dots & a_{2m} & a_{2m-1} & \dots & a_m & a_{m-1} & \dots & a_0 \\ \hline ka= & z_{4m-2} & \dots & z_{3m} & z_{3m-1} & \dots & z_{2m} & z_{2m-1} & \dots & z_m & z_{m-1} & \dots & z_0 \end{array}\right\}+ \tag{4.26}$$

where

$$a_i + a_{m+i} + b_{2m+i-1} = z_{2m+i} + 2b_{2m+i}, \quad \text{for } i = 0, 1, \dots, 4m-2, \tag{4.27}$$

$$y_{2m+i} + a_{2m+i} + c_{2m+i-1} = z_{2m+i} + 2c_{2m+i}, \quad \text{for } i = 0, 1, \dots, 4m-2, \tag{4.28}$$

for some integers b_i, c_i with $0 \le b_i \le 1$, $i = 0, 1, \dots, 4m-2$, $c_m = 1$, and $c_i = 0$ for $i = 0, 1, \dots, m-1, m+1, \dots, 4m-2$, with the convention that indices are read modulo $4m-1$ throughout. The integer b_i is the carry-over from the ith place to the $(i+1)$th during the addition displayed in (4.25) that gives ka, while c_i is the carry-over from the ith place to the $(i+1)$th during the addition displayed in (4.26) that gives ka. (Again, it is not difficult to see that there is a unique such choice of b_i's and c_i's which satisfy (4.27) and (4.28) such that the y_i's and z_i's are the digits in the additions given by (4.25) and (4.26).) Equation (4.28), together with the above assignments for the c_i's, reflects the conditions imposed by (4.9) with the 1's in the mth place.

Next, as in the proof of Theorem 4.6, we perform an appropriate relabelling of indices. Given a sequence $(x_i)_{i=0,\dots,4m-2}$, where (x_i) can be any of (a_i), (b_i), (c_i), (y_i), or (z_i), define the new sequence $(\tilde{x}_j)_{j=0,\dots,4m-2}$ by $\tilde{x}_j := x_{mj}$. Note that since $(m, d) = (m, 4m-1) = 1$, the sequence $(\tilde{x}_j)_{j=0,\dots,4m-2}$ is a permutation of $(x_i)_{i=0,\dots,4m-2}$ (recall that indices are read modulo $4m-1$). Now, by putting $i = mj$, equations (4.27) and (4.28) read, in terms of the transformed sequences,

$$\tilde{a}_j + \tilde{a}_{j+1} + \tilde{b}_{j-2} = \tilde{z}_{j+2} + 2\tilde{b}_{j+2}, \quad \text{for } j = 0, 1, \dots, 4m-2, \tag{4.29}$$

$$\tilde{y}_{j+2} + \tilde{a}_{j+2} + \tilde{c}_{j-2} = \tilde{z}_{j+2} + 2\tilde{c}_{j+2}, \quad \text{for } j = 0, 1, \dots, 4m-2, \tag{4.30}$$

where $0 \le \tilde{b}_j \le 1$, $j = 0, 1, \dots, 4m-2$, $\tilde{c}_1 = 1$, and $\tilde{c}_j = 0$ for $j = 0, 2, 3, \dots, 4m-2$, where again all indices are viewed modulo $4m-1$.

We now interrupt the proof for the case $d = 4m-1$ and turn for a moment to the case $d = 4m+1$, $m \ge 1$. Then we have $\sigma = 2^{2m+1}$ and $\gamma = 2^{3m+1}$, by (2.4).

Again, we analyse, for a given special solution a to (4.5), the computation of $(k-1)a$ and $ka \bmod 2^d - 1 = 2^{4m+1} - 1$. Let the binary representation of a be $a_{4m} \dots a_1 a_0$. Since $k = \sigma + \gamma = 2^{2m+1} + 2^{3m+1}$, we may compute ka in the following two ways:

$$\left.\begin{array}{r|ccccccccccc} 2^{3m+1}a= & a_{m-1} & \dots & a_0 & a_{4m} & \dots & a_{3m+1} & a_{3m} & \dots & a_{2m+1} & a_{2m} & \dots & a_m \\ 2^{2m+1}a= & a_{2m-1} & \dots & a_m & a_{m-1} & \dots & a_0 & a_{4m} & \dots & a_{3m+1} & a_{3m} & \dots & a_{2m} \\ \hline ka= & z_{4m} & \dots & z_{3m+1} & z_{3m} & \dots & z_{2m+1} & z_{2m} & \dots & z_{m+1} & z_m & \dots & z_0 \end{array}\right\}+ \tag{4.31}$$

and

$$\left.\begin{array}{r|ccccccccccc} (k-1)a= & y_{4m} & \dots & y_{3m+1} & y_{3m} & \dots & y_{2m+1} & y_{2m} & \dots & y_{m+1} & y_m & \dots & y_0 \\ a= & a_{4m} & \dots & a_{3m+1} & a_{3m} & \dots & a_{2m+1} & a_{2m} & \dots & a_{m+1} & a_m & \dots & a_0 \\ \hline ka= & z_{4m} & \dots & z_{3m+1} & z_{3m} & \dots & z_{2m+1} & z_{2m} & \dots & z_{m+1} & z_m & \dots & z_0 \end{array}\right\}+ \tag{4.32}$$

where

$$a_i + a_{i-m} + b_{2m+i} = z_{2m+i+1} + 2b_{2m+i+1}, \quad \text{for } i = 0, 1, \dots, 4m, \tag{4.33}$$
$$y_{2m+i+1} + a_{2m+i+1} + c_{2m+i} = z_{2m+i+1} + 2c_{2m+i+1}, \quad \text{for } i = 0, 1, \dots, 4m, \tag{4.34}$$

for some integers b_i, c_i with $0 \le b_i \le 1$, $i = 0, 1, \dots, 4m$, $c_{3m+1} = 1$, and $c_i = 0$ for $i = 0, 1, \dots, 3m, 3m+2, \dots, 4m$, with the convention that indices are read modulo $4m+1$ throughout. The integer b_i is the carry-over from the ith place to the $(i+1)$th during the addition displayed in (4.31) that gives ka, while c_i is the carry-over from the ith place to the $(i+1)$th during the addition displayed in (4.32) that gives ka. (As in the similar places before, there is a unique such choice of b_i's and c_i's which satisfy (4.33) and (4.34) such that the y_i's and z_i's are the digits in the additions given by (4.31) and (4.32).) Equation (4.34), together with the above assignments for the c_i's, reflects the conditions imposed by (4.9) with the 1's in the $(3m+1)$th place.

Next, we perform an appropriate relabelling of indices. Here, given a sequence $(x_i)_{i=0,\dots,4m}$, where (x_i) can be any of (a_i), (b_i), (c_i), (y_i), or (z_i), define the new sequence $(\tilde{x}_j)_{j=0,\dots,4m}$ by $\tilde{x}_j := x_{-mj}$. (Note the difference from the previous relabelling.) Note that since $(-m, d) = (m, 4m+1) = 1$, the sequence $(\tilde{x}_j)_{j=0,\dots,4m}$ is a permutation of $(x_i)_{i=0,\dots,4m}$. Now, by putting $i = -mj$, equations (4.33) and (4.34) read, in terms of the transformed sequences,

$$\tilde{a}_j + \tilde{a}_{j+1} + \tilde{b}_{j-2} = \tilde{z}_{j+2} + 2\tilde{b}_{j+2}, \quad \text{for } j = 0, 1, \dots, 4m, \tag{4.35}$$
$$\tilde{y}_{j+2} + \tilde{a}_{j+2} + \tilde{c}_{j-2} = \tilde{z}_{j+2} + 2\tilde{c}_{j+2}, \quad \text{for } j = 0, 1, \dots, 4m, \tag{4.36}$$

where $0 \le \tilde{b}_j \le 1$, $j = 0, 1, \dots, 4m$, $\tilde{c}_1 = 1$, and $\tilde{c}_j = 0$ for $j = 0, 2, 3, \dots, 4m$, where again all indices are viewed modulo $4m+1$.

Very conveniently, equations (4.35)-(4.36) are identical with equations (4.29)-(4.30), so that from now on we can treat the cases $d = 4m-1$ and $d = 4m+1$ simultaneously.

Construct a directed graph D as follows. The set of vertices of D is the set of all vectors $(a', a'', b', b'', b''', b'''', c', c'', c''', c'''')$ with $0 \le a', a'', b', b'', b''', b'''', c', c'', c''', c'''' \le 1$.

Corresponding to a special solution a, $0 < a < 2^d - 1$, to (4.5) with $k = \sigma + \gamma$, define (in the notation of (4.29)–(4.30)/(4.35)–(4.36)) the d vertices

$$v_j = (\tilde{a}_j, \tilde{a}_{j+1}, \tilde{b}_{j-2}, \tilde{b}_{j-1}, \tilde{b}_j, \tilde{b}_{j+1}, \tilde{c}_{j-2}, \tilde{c}_{j-1}, \tilde{c}_j, \tilde{c}_{j+1}), \tag{4.37}$$

$0 \le j \le d-1$. Our construction of the directed edges will be motivated by the desire to obtain, via equations (4.29) and (4.30), a bijection between the special solutions a and certain closed walks in D of length d. A solution a will correspond to the walk

$$v_0 \to v_1 \to \cdots \to v_{d-1} \to v_0, \tag{4.38}$$

and vice versa.

We connect a vertex $(a', a'', b', b'', b''', b'''', c', c'', c''', c'''')$ to a vertex $(A', A'', B', B'', B''', B'''', C', C'', C''', C'''')$ by a directed edge if and only if

$$a'' = A', \tag{4.39}$$
$$b'' = B', \tag{4.40}$$
$$b''' = B'', \tag{4.41}$$
$$b'''' = B''', \tag{4.42}$$
$$c'' = C', \tag{4.43}$$
$$c''' = C'', \tag{4.44}$$
$$c'''' = C''', \tag{4.45}$$
$$Z := (a' + a'' + b' - 2B'''') \in \{0, 1\}, \tag{4.46}$$
$$(Z + 2C'''' - A'' - c') \in \{0, 1\}. \tag{4.47}$$

The reader should think of $(a', a'', b', b'', b''', b'''', c', c'', c''', c'''')$ and $(A', A'', B', B'', B''', B'''', C', C'', C''', C'''')$ as $v_j = (\tilde a_j, \tilde a_{j+1}, \tilde b_{j-2}, \tilde b_{j-1}, \tilde b_j, \tilde b_{j+1}, \tilde c_{j-2}, \tilde c_{j-1}, \tilde c_j, \tilde c_{j+1})$ and $v_{j+1} = (\tilde a_{j+1}, \tilde a_{j+2}, \tilde b_{j-1}, \tilde b_j, \tilde b_{j+1}, \tilde b_{j+2}, \tilde c_{j-1}, \tilde c_j, \tilde c_{j+1}, \tilde c_{j+2})$, respectively, $j = 0, 1, \dots, d-1$. Equation (4.46) reflects (4.29)/(4.35), and equation (4.47) reflects (4.30)/(4.36).

The remainder of the proof proceeds just like the proof of Theorem 4.6. We define sets V_0, V_1, V_2, V_3, V_4 as the sets of vertices $(a', a'', b', b'', b''', b'''', c', c'', c''', c'''')$ for which (c', c'', c''', c'''') equals $(0,0,0,0)$, $(0,0,0,1)$, $(0,0,1,0)$, $(0,1,0,0)$, $(1,0,0,0)$, respectively. As is easy to see, for odd $d \ge 3$ the special solutions a, $0 < a < 2^d - 1$, to equation (4.5) with $k = \sigma + \gamma$ are in bijection with the closed walks of length d which start in V_1, in the first step move to V_2, in the next step move to V_3, then move to V_4, and from there on visit only vertices from V_0, until they return to the starting vertex from V_1. In an analogous manner we define matrices $\boldsymbol{A}_{12}$, $\boldsymbol{A}_{23}$, $\boldsymbol{A}_{34}$, $\boldsymbol{A}_{40}$, $\boldsymbol{A}_{00}$ and $\boldsymbol{A}_{01}$, and obtain a rational expression for the generating function for the sequence $(A_{\sigma+\gamma}(2r+1))_{r\ge2}$ in the form

$$\sum_{r\ge2} A_{\sigma+\gamma}(2r+1) z^{r-2} = \operatorname{tr}\left(\sum_{j=0}^{\infty} \boldsymbol{A}_{12}\boldsymbol{A}_{23}\boldsymbol{A}_{34}\boldsymbol{A}_{40}\boldsymbol{A}_{00}^{2j}\boldsymbol{A}_{01} z^j\right)$$
$$= \operatorname{tr}\left(\boldsymbol{A}_{12}\boldsymbol{A}_{23}\boldsymbol{A}_{34}\boldsymbol{A}_{40}(\boldsymbol{I} - \boldsymbol{A}_{00}^2 z)^{-1}\boldsymbol{A}_{01}\right).$$

This time the matrix $\boldsymbol{A}_{00}$, the adjacency matrix of D restricted to V_0, is a 64×64 matrix. Therefore, in order to invoke Lemma 4.5, it suffices to verify the recurrence (4.24) for $d = 13, 15, \dots, 141$. This is again routinely performed on a computer[2]. This establishes (4.24) for *all* odd d, $d \ge 13$.

Now the proof of the theorem is complete. □

[2] *Maple* and *Mathematica* codes for generating the matrices $\boldsymbol{A}_{00}$, $\boldsymbol{A}_{01}$, $\boldsymbol{A}_{12}$, $\boldsymbol{A}_{23}$, $\boldsymbol{A}_{34}$, $\boldsymbol{A}_{40}$ can be obtained on request from the authors, or by WWW at `http://radon.mat.univie.ac.at/People/kratt/artikel/glynn.html`. The verification of (4.24) for $d = 13, 15, \dots, 141$ took 15 seconds on a Pentium with 133 MHz.

By combining Theorems 4.8 and 3.6, we are now able to precisely determine the 2-ranks of the difference sets corresponding to the Glynn type (I) hyperovals.

Corollary 4.9. *Let d be an odd integer, $d \geq 3$, and set $\sigma = 2^{(d+1)/2}$, $\gamma = 2^{(3d+1)/4}$ if $d \equiv 1 \bmod 4$, and $\gamma = 2^{(d+1)/4}$ if $d \equiv 3 \bmod 4$. Let $D_{\sigma+\gamma,d}$ be the $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference set in $\mathbb{F}_{2^d}^*$ corresponding to the Glynn type (I) hyperoval $D(x^{\sigma+\gamma})$, as in Theorem 2.5. Let $\overline{D_{\sigma+\gamma,d}}$ be the complement of $D_{\sigma+\gamma,d}$ in $\mathbb{F}_{2^d}^*$. Then the 2-rank $B_{\sigma+\gamma}(d)$ of $\overline{D_{\sigma+\gamma,d}}$ equals $dA_{\sigma+\gamma}(d)$, where $A_{\sigma+\gamma}(3) = 1$, $A_{\sigma+\gamma}(5) = 1$, $A_{\sigma+\gamma}(7) = 3$, $A_{\sigma+\gamma}(9) = 7$, $A_{\sigma+\gamma}(11) = 13$, and for $d \geq 13$, $A_{\sigma+\gamma}(d)$ satisfies the recurrence* (4.24).

5. Binary cyclic codes of difference sets arising from Segre hyperovals

The next two propositions give some further applications of Proposition 4.1. Let $\mathcal{C}_2(D_{6,d})$ be the binary cyclic code of $D_{6,d}$, as defined near the beginning of Section 3. Define $\theta(x)$ (viewed as a polynomial over $\mathbb{F}_2$) by

$$\theta(x) = \sum_{j=0}^{2^d-2} b_j x^j,$$

where $b_0, b_1, \dots, b_{2^d-2}$ denotes the characteristic sequence of $D_{6,d}$. By suitably ordering the elements of $D_{6,d}$, we may choose a (fixed) generator α of $\mathbb{F}_{2^d}^*$ such that $b_j = 1$ if and only if $\alpha^j \in D_{6,d}$. The significance of $\theta(x)$ is that its greatest common divisor with $x^{2^d-1} - 1$ is the generator polynomial of the binary cyclic code $\mathcal{C}_2(D_{6,d})$. The zeros of $\theta(x)$ in $\mathbb{F}_{2^d}^*$ (i.e., the zeros of the generator polynomial) are called the *zeros* of $\mathcal{C}_2(D_{6,d})$. The remaining elements of $\mathbb{F}_{2^d}^*$ are called the *nonzeros* of $\mathcal{C}_2(D_{6,d})$. Observe that for such a nonzero u, we have $\theta(u) = 1$, since $D_{6,d}$ is invariant under the d automorphisms of $\mathbb{F}_{2^d}$.

Proposition 5.1. *Let d be an odd integer, $d \geq 3$, and let $D_{6,d}$ be the $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference set in $\mathbb{F}_{2^d}^*$ corresponding to the Segre hyperoval $D(x^6)$, as in Theorem* 2.5 *with $k = 6$. Let $\mathcal{C}_2(D_{6,d})$ be the binary cyclic code of $D_{6,d}$. Then the nonzeros of $\mathcal{C}_2(D_{6,d})$ are* 1, *α^{-5a}, where α is the primitive element of $\mathbb{F}_{2^d}^*$ defined above, and a runs through all the solutions of* (4.1) *given explicitly in Proposition* 4.1.

Proof: Clearly 1 is a nonzero of $\mathcal{C}_2(D_{6,d})$ because the cardinality of $D_{6,d}$ is odd. For $\mathfrak{p}$ a prime ideal in $\mathbb{Z}[\xi_{2^d-1}]$ lying over 2, let $\omega = \omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_{2^d}$. By definition of $\theta(x)$ and α, we see that α^i, $0 < i \leq 2^d-2$ is a nonzero of $\mathcal{C}_2(D_{6,d})$ if and only if $\omega^i(D_{6,d}) \pmod{\mathfrak{p}} \neq 0$. From the proof of Theorem 3.6, we see that for $0 < a \leq 2^d-2$, $\omega^{-5a}(D_{6,d}) \pmod{\mathfrak{p}} \neq 0$ if and only if $s(a) + s(5a) = s(6a) + 1$. Therefore the nonzeros of $\mathcal{C}_2(D_{6,d})$ are $1, \alpha^{-5a}$, where a runs through the solutions of (4.1). This completes the proof. □

Example 5.2. Let $D_{6,9}$ be the $(2^9-1, 2^8-1, 2^7-1)$ cyclic difference set in $\mathbb{F}_{2^9}^*$ corresponding to the Segre hyperoval $D(x^6)$, as in Theorem 2.5 with $k = 6$. Let $\mathcal{C}_2(D_{6,9})$ be the binary cyclic code of $D_{6,9}$. By Proposition 5.1 and Example 4.2, we know that the nonzeros of $\mathcal{C}_2(D_{6,9})$ are 1, $\alpha^{-5\cdot 2^i}$, $\alpha^{-25\cdot 2^i}$, $\alpha^{-77\cdot 2^i}$, $\alpha^{-117\cdot 2^i}$, $\alpha^{-9\cdot 2^i}$, $\alpha^{-19\cdot 2^i}$, $\alpha^{-7\cdot 2^i}$, $\alpha^{-37\cdot 2^i}$, and α^{-2^i}, where $i = 0, 1, 2, \dots, 8$. A simple computation shows that α^{501j}, $j = 341, 342, 343, \dots, 408$, are zeros of $\mathcal{C}_2(D_{6,9})$. By the BCH-bound [20, p. 201], the code $\mathcal{C}_2(D_{6,9})$ is a 34-error correcting code of length 511 and dimension 82 over $\mathbb{F}_2$, (with minimum distance at least 69).

Let d be an odd integer, $d \geq 3$. Let a be an integer with $1 \leq a \leq 2^d - 2$, and let r be the smallest positive integer such that $2^{r+1}a \equiv a \pmod{2^d-1}$. The *cyclotomic coset* containing a consists of $\{a, 2a, 2^2a, \dots, 2^ra\}$. The solutions of (4.1) can be partitioned into $A_6(d)$ disjoint cyclotomic cosets, each of cardinality d. Let J be a complete set of cyclotomic coset representatives of the solutions of (4.1). We can give a criterion involving trace to decide when the equation $x^6 + x + \beta = 0$, $\beta \in \mathbb{F}_{2^d}^*$, has two distinct solutions (as opposed to no solutions) in $\mathbb{F}_{2^d}$.

Proposition 5.3. *Let d be an odd integer, $d \geq 3$. Then $x^6 + x + \beta = 0$, $\beta \in \mathbb{F}_{2^d}^*$, has two distinct solutions in $\mathbb{F}_{2^d}$ if and only if $\mathrm{Tr}(\sum_{a\in J} \beta^{5a}) = 0$, where Tr is the trace from $\mathbb{F}_{2^d}$ to $\mathbb{F}_2$, and J is defined above.*

Proof: By Fourier inversion and the definition of $\theta(x)$,

$$(2^d - 1)b_j = \sum_{i=0}^{2^d-2} \theta(\alpha^{-i})\alpha^{ij},$$

for each j with $0 \leq j \leq 2^d - 2$. By Proposition 5.1, $\theta(\alpha^{-i})$ equals 1 if $i = 0$ or $i = 5a$, and otherwise $\theta(\alpha^{-i})$ equals 0, where a runs through the solutions of (4.1). The result now follows with $\beta = \alpha^j$. □

Example 5.4. Let $d = 9$. By Example 4.2, $J = \{1, 5, 21, 85, 13, 53, 77, 167, 103\}$ is a complete set of cyclotomic coset representatives of the solutions of (4.1). Therefore $x^6 + x + \beta = 0$, $\beta \in \mathbb{F}_{2^9}^*$, has two distinct solutions in $\mathbb{F}_{2^9}$ if and only if $\mathrm{Tr}(\beta + \beta^5 + \beta^7 + \beta^9 + \beta^{19} + \beta^{25} + \beta^{37} + \beta^{77} + \beta^{117}) = 0$.

It is interesting to compare Proposition 5.3 with the result (following from Hilbert's Theorem 90) that $x^2 + x + \beta = 0$, $\beta \in \mathbb{F}_{2^d}^*$ has two solutions in $\mathbb{F}_{2^d}$ if and only if $\mathrm{Tr}(\beta) = 0$.

6. Inequivalence of difference sets arising from hyperovals, quadratic residue difference sets, and GMW difference sets

In the next theorem, we answer a question raised by Maschietti [21] by showing that the difference sets $D_{k,d}$ arising from the hyperovals in (2.1), (2.3), (2.4), (2.5) are all inequivalent to each other. The difference sets arising from the hyperovals in (2.1)–(2.2) are of course equivalent for the same d, since as we showed at the end of Section 2, they are all Singer difference sets.

We precede the statement of the theorem by the following auxiliary result which is of independent interest. It relates the magnitudes of the 2-ranks of the difference sets arising from Segre and Glynn hyperovals.

Lemma 6.1. *With $A_k(d)$ as defined at the beginning of Section 4, we have for each odd $d \geq 15$ that*

$$A_{3\sigma+4}(d) > A_{\sigma+\gamma}(d) > A_6(d), \tag{6.1}$$

i.e., the 2-ranks of the difference sets that arise from Glynn type (II) hyperovals dominate the 2-ranks of the difference sets that arise from Glynn type (I) hyperovals, which in turn dominate the 2-ranks of the difference sets arising from Segre hyperovals.

Proof: Since $A_6(d) = 2F_{(d-1)/2} - 1$ by Theorem 4.3, it follows that

$$A_6(d) = \tfrac{2}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{(d+1)/2} - \tfrac{2}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{(d+1)/2} - 1.$$

Note that $(1+\sqrt{5})/2 = 1.6181\ldots$

Solving the recurrence (4.24), we obtain

$$A_{\sigma+\gamma}(d) = a_1\omega_1^{(d+1)/2} + a_2\omega_2^{(d+1)/2} + a_3\omega_3^{(d+1)/2} + a_4\omega_4^{(d+1)/2} + a_5,$$

where $\omega_1, \omega_2, \omega_3, \omega_4$ are four distinct complex zeros of the polynomial $z^4 - z^3 - z^2 - z - 1$, and where a_1, a_2, a_3, a_4, a_5 are explicitly known complex numbers. The zero with greatest absolute value is ω_1, say, where $|\omega_1| = 1.927561975\ldots$

Solving the recurrence (4.8), we obtain

$$A_{3\sigma+4}(d) = b_1\rho_1^{(d+1)/2} + b_2\rho_2^{(d+1)/2} + b_3\rho_3^{(d+1)/2} + b_4\rho_4^{(d+1)/2} + b_5,$$

where $\rho_1, \rho_2, \rho_3, \rho_4$ are four distinct complex zeros of the polynomial $z^4 - z^3 - 3z^2 + z + 1$, and where b_1, b_2, b_3, b_4, b_5 are explicitly known complex numbers. The zero with greatest absolute value is ρ_1, say, where $|\rho_1| = 2.095293985\ldots$

From these formulas, we see that for odd $d > 25$,

$$A_{3\sigma+4}(d) > \tfrac{1}{3}2^{(d+1)/2} > A_{\sigma+\gamma}(d) > (1.6181)^{(d+1)/2} > A_6(d).$$

Appealing to Table 1, we see that (6.1) holds for odd $d \geq 15$.

This completes the proof. □

Theorem 6.2. *The difference sets $D_{k,d}$ arising from the hyperovals in* (2.1), (2.3), (2.4), (2.5) *are all inequivalent.*

Proof: It suffices to show that the 2-ranks of the complements $\overline{D_{k,d}}$ in question are distinct. Since the difference set $D_{k,d}$ arising from a regular hyperoval is a Singer difference set, the 2-rank of its complement equals d, by Theorem 3.5 and the remarks following Theorem 3.5. By Corollary 4.4, the 2-rank of $\overline{D_{6,d}}$ is $dA_6(d) = d(2F_{(d-1)/2} - 1)$, which exceeds d for $d \geq 5$. This show the inequivalence for the cases (2.1) and (2.3). By Table 1 and Lemma 6.1, the 2-ranks in all the cases must be distinct.

This completes the proof. □

Let Q_d denote the quadratic residue cyclic $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ difference set in $\mathbb{F}_{2^d}^*$ [15, p. 244]. Thus, $2^d - 1$ must be a prime, and $Q_d = \{\alpha^r : r$ is a square mod $2^d - 1$, $0 < r < 2^d - 1\}$, where α generates the group $\mathbb{F}_{2^d}^*$. It is easily checked that Q_2 and Q_3 are equivalent to difference sets arising from the regular hyperoval, while Q_5 is equivalent to the difference set arising from the Segre hyperoval. We now show that for (odd) $d \geq 7$, the sets Q_d are inequivalent to difference sets arising from hyperovals.

Theorem 6.3. *Let $d \geq 7$ be odd. Then the quadratic residue difference sets Q_d are inequivalent to the difference sets $D_{k,d}$ arising from the hyperovals in* (2.1)–(2.5).

Proof: As χ runs through the (multiplicative) nontrivial characters on $\mathbb{F}_{2^d}^*$, $\chi(Q_d) = \sum_{\beta\in Q_d}\chi(\beta)$ assumes exactly two distinct values z and $\overline{z}$, where z is a complex number and $\overline{z}$ is its complex conjugate. If D is any difference set in $\mathbb{F}_{2^d}^*$ equivalent to Q_d, then as χ runs through the nontrivial characters on $\mathbb{F}_{2^d}^*$, $\chi(D)$ assumes only the values z and $\overline{z}$ up to a factor of a (2^d-1)-th root of unity. Now assume for the purpose of contradiction that the aforementioned D is one of the difference sets $D_{k,d}$ in (2.1)–(2.5). In view of (2.6), it suffices to show that as χ runs through the nontrivial characters on $\mathbb{F}_{2^d}^*$, the principal ideals in $\mathbb{Z}[\xi_{2^d-1}]$ generated by the Jacobi sums $J(\chi,\chi^{k-1})$ assume *more* than two distinct values. Thus, by (3.10), it suffices to show that as a runs through the values $1,2,\dots,2^d-2$, the expression $c(a) := s(a)+s(a(k-1))-s(ak)$ assumes at least three distinct values. One checks this as follows.

For k as in (2.5), $c(1)$, $c(-1)$, and $c(7)$ are distinct. For k as in (2.4), $c(1)$, $c(-1)$, and $c(\sigma+1)$ are distinct. For k as in (2.3), $c(1)$, $c(-1)$, and $c(3)$ are distinct. Finally, for k as in (2.1) or (2.2), $c(1)$, $c(-1)$, and $c(k+1)$ are distinct. This completes the proof. $\square$

Next we consider GMW difference sets [11]. Suppose that d has the factorization $d=uv$ for integers $u,v>1$, and write $q=2^u$ (so that $2^d=q^v$). Let r be an integer strictly between 1 and $q-1$ which is relatively prime to $q-1$ and which is not equal to a power of 2. Define the GMW set

$$G_{d,v,r} = \{y\in\mathbb{F}_{2^d}^* \mid \mathrm{Tr}_{q/2}((\mathrm{Tr}_{q^v/q}(y))^r)=0\},$$

where $\mathrm{Tr}_{q^v/q}$ denotes the trace map from $\mathbb{F}_{q^v}$ to $\mathbb{F}_q$. (We did not allow r to be a power of 2, for otherwise $G_{d,v,r}$ would of course be equivalent to a Singer difference set.) Let w denote the number of 1's in the binary expansion of r (so that $1<w<u$). It is known [24] that $G_{d,v,r}$ is a $(2^d-1,2^{d-1}-1,2^{d-2}-1)$ difference set whose complement has 2-rank uv^w. (For related work over finite fields of characteristic p, see [1].) Theorem 6.8 below shows that the GMW sets $G_{d,v,r}$ are inequivalent to the difference sets $D_{k,d}$ in (2.1)–(2.5). We will first need four lemmas.

Lemma 6.4. *Write $d=uv$ and $q=2^u$ as above. For each nontrivial multiplicative character χ on $\mathbb{F}_{2^d}^*$ we have*

$$\chi(G_{d,v,r}) = \sum_{y\in G_{d,v,r}}\chi(y) = \frac{1}{2}g(\chi)g_1({\chi_1}^{1/r})/g_1(\chi_1),$$

where $1/r$ denotes the inverse of r modulo $q-1$, χ_1 denotes the restriction of χ to $\mathbb{F}_q^*$, and where g and g_1 denote the Gauss sums over $\mathbb{F}_{2^d}^*$ and $\mathbb{F}_q^*$, respectively.

Proof: We have

$$2\chi(G_{d,v,r}) = \sum_{y\in\mathbb{F}_{2^d}^*}\chi(y)(-1)^{\mathrm{Tr}_{q/2}((\mathrm{Tr}_{q^v/q}(y))^r)}.$$

Write

$$T=(q^v-1)/(q-1),$$

and let α be a fixed generator of $\mathbb{F}_{2^d}^*$, so that every $y \in \mathbb{F}_{2^d}^*$ has the form $y = \alpha^{iT+j}$, with $0 \le i < q-1$, $0 \le j < T$. Therefore, since $\alpha^T \in \mathbb{F}_q^*$,

$$2\chi(G_{d,v,r}) = \sum_{j=0}^{T-1} \chi(\alpha^j) \sum_{i=0}^{q-2} \chi^{1/r}(\alpha^{irT})(-1)^{\mathrm{Tr}_{q/2}(\alpha^{irT}(\mathrm{Tr}_{q^v/q}(\alpha^j))^r)}.$$

Thus

$$2\chi(G_{d,v,r}) = A + B,$$

where

$$A = \sum_{j=0}^{T-1} \chi(\alpha^j)\overline{\chi}(\mathrm{Tr}_{q^v/q}(\alpha^j))g_1(\chi_1^{1/r})$$

and

$$B = \sum_{\substack{j=0 \\ \mathrm{Tr}_{q^v/q}(\alpha^j)=0}}^{T-1} \sum_{i=0}^{q-2} \chi(\alpha^{iT+j}) = \sum_{\substack{y \in \mathbb{F}_{2^d}^* \\ \mathrm{Tr}_{q^v/q}(y)=0}} \chi(y).$$

To evaluate A, observe that

$$A = g_1(\chi_1^{1/r}) \sum_{\substack{y \in \mathbb{F}_{2^d}^* \\ \mathrm{Tr}_{q^v/q}(y)=1}} \chi(y).$$

This sum on y is an Eisenstein sum, which is known [4, pp. 391, 400] to equal $g(\chi)/g_1(\chi_1)$ or $-g(\chi)/q$, according as χ_1 is nontrivial or trivial. Thus

$$A = \begin{cases} g_1(\chi_1^{1/r})g(\chi)/g_1(\chi_1), & \text{if } \chi_1 \text{ is nontrivial,} \\ g(\chi)/q, & \text{if } \chi_1 \text{ is trivial.} \end{cases}$$

To evaluate B, observe that B is an Eisenstein sum which is known [4, pp. 389, 391, 400] to equal

$$B = \begin{cases} 0, & \text{if } \chi_1 \text{ is nontrivial,} \\ g(\chi)(q-1)/q, & \text{if } \chi_1 \text{ is trivial.} \end{cases}$$

Adding our evaluations of A and B, we obtain the desired result. $\square$

Lemma 6.5. *Let $v = 3$, $u \ge 7$ with u odd, $q = 2^u$, and $d = uv$. For an integer a not divisible by $q^v - 1$, let $s(a)$ denote the number of 1's in the binary expansion of the reduction of a modulo $q^v - 1$. As in (2.4), define $\sigma = 2^{(d+1)/2}$ and $\gamma = 2^{(3d+1)/4}$ if $d \equiv 1 \bmod 4$, whereas $\gamma = 2^{(d+1)/4}$ if $d \equiv 3 \bmod 4$. Then for $a = (q-1)(\gamma + (-1)^{(d-1)/2})$,*

$$s(a) + s(a(\sigma + \gamma - 1)) - s(a(\sigma + \gamma)) < u.$$

Proof: First suppose that $d \equiv 3 \bmod 4$. Then it may be checked directly that $s(a) = u$, $s(a(\sigma + \gamma - 1)) = (d-1)/2$, and $s(a(\sigma + \gamma)) = (d+1)/2$. The result thus follows in the case $d \equiv 3 \bmod 4$. Next suppose that $d \equiv 1 \bmod 4$. Then it may be checked directly that $s(a) = u$, $s(a(\sigma + \gamma - 1)) = u$, and $s(a(\sigma + \gamma)) = 5(d+3)/12$, and the result again follows. $\square$

Lemma 6.6. *Let $d = uv$ with $v = 3$ and odd $u \geq 3$. Then every GMW difference set $G_{d,3,r}$ is inequivalent to the difference set $D_{\sigma+\gamma,d}$ corresponding to the Glynn type (I) hyperoval.*

Proof: The result is easily checked for $u = 3$ and $u = 5$, because then the 2-ranks of the two kinds of difference sets differ (see Table 1). So let $u \geq 7$. Write $q = 2^u = 2^{d/3}$. Let χ be any nontrivial multiplicative character on $\mathbb{F}_{2^d}^*$ whose restriction χ_1 to $\mathbb{F}_q^*$ is trivial. Thus, if ω is a Teichmüller character (of order $2^d - 1$) on $\mathbb{F}_{2^d}^*$, then $\chi = \omega^{-a}$ for an integer a divisible by $q - 1$.

Suppose that $G_{d,3,r}$ were equivalent to $D_{\sigma+\gamma,d}$. Then it would follow from Lemma 6.4 and (2.6) that

$$J(\chi, \chi^{\sigma+\gamma-1}) = \mu g(\chi^t)$$

for some complex root of unity μ and some integer t relatively prime to $2^d - 1$. Setting $p = 2$ and $d = 3$ in the proof of Theorem 2.1, we see from that proof that $g(\chi^t)$ is divisible by q in the ring of algebraic integers. Thus $J(\chi, \chi^{\sigma+\gamma-1})$ is divisible by q, so that every prime ideal occurring in the factorization of $J(\chi, \chi^{\sigma+\gamma-1})$ over $\mathbb{Z}[\xi_{2^d-1}]$ has an exponent $\geq u$. Thus by (3.10),

$$s(a) + s(a(\sigma + \gamma - 1)) - s(a(\sigma + \gamma)) \geq u$$

for every integer a divisible by $q - 1$. This contradicts Lemma 6.5, and so the proof is complete. □

Lemma 6.7. *Let $u \geq 5$ be odd. Then $A_6(3u)$ is never a power of 3 and $A_6(5u)$ is never a power of 5.*

Proof: By Theorem 4.3, for odd $d > 1$,

$$A_6(d) = 2F_{(d-1)/2} - 1. \tag{6.2}$$

First suppose that $A_6(d)$ is a power of 3 for $d = 3u$. Then, since $A_6(d)$ is different from $3, 9, 27$ (see Table 1), $A_6(d)$ must be divisible by 81. So by (6.2), $d = 57 + 432x$ for some nonnegative integer x. Since F_n (mod 109) has period 108, it follows that $A_6(d)$ (mod 109) has period 216, and hence $A_6(57 + 432x)$ is congruent to 42 modulo 109 for *all* nonnegative integers x. This is a contradiction, since 42 is not a power of 3 modulo 109.

Next suppose that $A_6(d)$ is a power of 5 for $d = 5u$. Then since $A_6(d)$ is different from 5 and 25 (see Table 1), we have $125 \mid A_6(d)$. So by (6.2), we have $d = 585 + 1000y$ for some nonnegative integer y. Since F_n (mod 251) has period 250, it follows that $A_6(d)$ (mod 251) has period 500, and so $A_6(585 + 1000y)$ is congruent to 235 modulo 251 for *all* nonnegative y. This is a contradiction, since 235 is not a power of 5 modulo 251. □

Theorem 6.8. *The GMW difference set $G_{d,v,r}$ is inequivalent to each of the difference sets $D_{k,d}$ arising from the hyperovals in* (2.1)–(2.5).

Proof: As was mentioned following the definition of $G_{d,v,r}$, the complement $\overline{G_{d,v,r}}$ has 2-rank uv^w, where $d = uv$ and $1 < w < u < d$. For k as in (2.1) or (2.2), the difference set $\overline{D_{k,d}}$ has 2-rank d (cf. the proof of Theorem 6.2). Since $u(d/u)^w > d$, it follows that $G_{d,v,r}$ is inequivalent to $D_{k,d}$.

Now let d be an odd composite integer > 5. It is easily checked by extending Table 1 that none of $A_6(d)$, $A_{\sigma+\gamma}(d)$, or $A_{3\sigma+4}(d)$ can equal $(d/u)^{w-1}$ for any $d < 500$. Hence assume $d > 500$. From the proof of Lemma 6.1,

$$A_{3\sigma+4}(d) > \tfrac{1}{4}(2.09)^{(d+1)/2} > 3^{d/3} > (d/u)^{u-2} \geq (d/u)^{w-1}.$$

This completes the proof for k as in (2.5).

Next, let k be as in (2.4). By Lemma 6.6, $G_{d,3,r}$ cannot be equivalent to $D_{\sigma+\gamma,d}$. Hence, assume that $u \leq d/5$. From the proof of Lemma 6.1,

$$A_{\sigma+\gamma}(d) > \tfrac{1}{4}(1.92)^{(d+1)/2} > 5^{d/5} > (d/u)^{u-2} \geq (d/u)^{w-1}.$$

This completes the proof for k as in (2.4).

Finally, let k be as in (2.3), i.e., $k = 6$. By Lemma 6.7, we cannot have $A_6(d)$ equal to $(d/u)^{w-1}$ with $u = d/3$ or $d/5$ or $d/9$. Moreover, $A_6(d)$ cannot equal $(d/u)^{w-1}$ for $u = d/7$, because it follows from Table 1 and the recurrence (4.4) that $A_6(d)$ never equals 7 and is never divisible by 49 for any odd d. Thus assume that $u \leq d/11$. From the proof of Lemma 6.1,

$$A_6(d) > (1.6)^{(d+1)/2} > 11^{d/11} > (d/u)^{u-2} \geq (d/u)^{w-1}.$$

This completes the proof for k as in (2.3), and hence completes the proof of the theorem. □

Remark: In the preceding proof, in order to show the inequivalence of GMW sets $G_{d,3,r}$ and the difference sets $D_{\sigma+\gamma,d}$ arising from the Glynn type (I) hyperovals, we used Lemma 6.6 instead of a 2-rank argument. We do in fact also have a proof[3], which is similar in spirit to the proof of Lemma 6.7, that for odd $u \geq 3$ the number $A_{\sigma+\gamma}(3u)$ is never a power of 3, whence also the 2-ranks of $G_{d,3,r}$ and $D_{\sigma+\gamma,d}$ are distinct. However, we prefer the approach via Lemma 6.6, because the aforementioned proof requires extensive computer calculations, and because Lemma 6.4 is of independent interest.

7. 2-ranks of circulant matrices

For integers $k \geq 3$ and $d \geq 2$, let

$$f(x) = x^k + x^{k-1}, \qquad x \in \mathbb{F}_{2^d}^*.$$

In Theorem 7.5, we will determine the ranks over $\mathbb{F}_2$ of certain circulant matrices M_k, defined as follows. Let α denote a generator of the cyclic group $\mathbb{F}_{2^d}^*$ and define the circulant matrix

$$M_k = (m_{i,j})_{1 \leq i,j \leq 2^d-1} \ ,$$

where $m_{i,j}$ denotes the number of $x \in \mathbb{F}_{2^d}^*$ for which $\alpha^{j-i} = f(x)$. Note that for each k such that $D(x^k)$ is a hyperoval in $PG(2, 2^d)$, we have $M_k = 2A_k$, where A_k is the incidence matrix (defined at the beginning of Section 3) corresponding to the difference set $D_{k,d}$ (defined in Theorem 2.5), the 2-ranks of which we studied in Section 4. This is because the incidence matrix A_k is not affected by changing $\tau(x)$ (as defined before Lemma 2.4) from $x + x^k$ to $x^{k-1} + x^k$, since the difference sets $D_{k,d}$ and $D_{k/(k-1),d}$ are equivalent by Lemma 2.3.

[3]It can be obtained on request from the authors, or by WWW at `http://radon.mat.univie.ac.at/People/kratt/artikel/glynn.html`.

Let $\mathrm{rank}_2(M_k)$ denote the rank of M_k over $\mathbb{F}_2$. In Section 4 we were concerned with the computation of the 2-ranks of incidence matrices A_k. Such a matrix A_k can be viewed as an adjacency matrix of the directed graph where for two vertices u, v in $\mathbb{F}_{2^d}^*$, a directed edge connects u to v if and only if v/u is in the difference set $D_{k,d}$, i.e., if and only if v/u is in the image of τ. The following two theorems exhibit values of k for which the computation of the 2-rank of M_k is also a 2-rank computation for an *adjacency* matrix N_k of a directed graph, where this time u is connected to v if and only if v/u is in the image of f.

Theorem 7.1. *Let $d > 1$ be odd. Let N_5 be the matrix obtained from M_5 by replacing every nonzero entry with* 1. *Then* $\mathrm{rank}_2(N_5) = \mathrm{rank}_2(M_5)$.

Proof: It suffices to show that every nonzero entry of M_5 is odd. We will prove the stronger result that for each $c \in \mathbb{F}_{2^d}^*$, the polynomial $g(x) = x^5 + x^4 + c$ has either no zeros, one zero, or three zeros in $\mathbb{F}_{2^d}^*$. First, if $g(x)$ had exactly two zeros in $\mathbb{F}_{2^d}^*$, then $g(x)$ would have an irreducible cubic factor (normal over $\mathbb{F}_{2^d}$), so that $g(x)$ would have five zeros in $\mathbb{F}_{2^{3d}}$. Similarly, if $g(x)$ had four zeros in $\mathbb{F}_{2^d}^*$, then $g(x)$ would have five zeros in $\mathbb{F}_{2^d}^*$. Thus, since $3d$ is odd, it remains to show that $g(x)$ cannot have fives zeros in $\mathbb{F}_{2^d}$ for any odd d. Assume for the purpose of contradiction that $g(x)$ has fives zeros in $\mathbb{F}_{2^d}$. Let z denote one of these zeros. Since c is nonzero, z is not 0 or 1. Over $\mathbb{F}_{2^d}$, we have the factorization $g(x) = (x + z)h(x)$, where

$$h(x) = x^4 + (z + 1)x^3 + (z^2 + z)x^2 + (z^3 + z^2)x + (z^4 + z^3).$$

Note that $h(0)$ is nonzero since $g(0)$ is nonzero. We have

$$q(x) = (z^4 + z^3)^{-1}x^4 h(z/x) = x^4 + x^3 + x^2 + x + w,$$

where $w = z/(z + 1)$. Since $h(x)$ has four zeros in $\mathbb{F}_{2^d}$, so does $q(x)$. Write $q(x) = (x^2 + rx + s)(x^2 + ux + v)$ over $\mathbb{F}_{2^d}$. Since both of these quadratic factors are reducible over $\mathbb{F}_{2^d}$, we have $\mathrm{Tr}(s/r^2) = \mathrm{Tr}(v/u^2) = 0$. Note that r and u are nonzero, since $q(x)$ cannot have multiple zeros over $\mathbb{F}_{2^d}$. We will obtain a contradiction by showing that $\mathrm{Tr}(s/r^2) + \mathrm{Tr}(v/u^2) = 1$. Now, $r + u = 1$, $ru + s + v = 1$, and $su + vr = 1$. Thus $r = 1 + u$, $u^2 + u + v + 1 = s$, and $u^3 + u^2 + uv + u + (v + uv) = 1$. Hence $v = 1 + u + u^2 + u^3$ and $s = u^3$. Therefore

$$s/r^2 = u^3/(1 + u^2) = u + 1/(1 + u) + 1/(1 + u)^2,$$

so that $\mathrm{Tr}(s/r^2) = \mathrm{Tr}(u)$. On the other hand, $v/u^2 = (1/u) + (1/u)^2 + 1 + u$, so that $\mathrm{Tr}(v/u^2) = 1 + \mathrm{Tr}(u)$. Thus $\mathrm{Tr}(v/u^2) + \mathrm{Tr}(s/r^2) = 1$, which yields the desired contradiction. This completes the proof. □

The next theorem shows that the conclusion of Theorem 7.1 is valid for *all* $d > 1$ when the subscript 5 is replaced by any k of the form $2^m - 1$ with $m > 1$.

Theorem 7.2. *Let $d > 1$. Set $k = 2^m - 1$ for an integer $m > 1$, and let N_k be the matrix obtained from M_k by replacing every nonzero entry with* 1. *Then* $\mathrm{rank}_2(N_k) = \mathrm{rank}_2(M_k)$.

Proof: It suffices to show that for each $c \in \mathbb{F}_{2^d}^*$, the polynomial $g(x) = x^k + x^{k-1} + c$ has either no zeros or an odd number of zeros in $\mathbb{F}_{2^d}^*$. Assume that z is a zero of $g(x)$ in

$\mathbb{F}_{2^d}^*$, and note that z is not 0 or 1. We will show that $g(x)$ has an odd number of zeros in $\mathbb{F}_{2^d}^*$. We have the factorization $g(x) = (x+z)h(x)$, where

$$h(x) = x^{k-1} + (z+1)x^{k-2} + (z^2+z)x^{k-3} + \ldots + (z^{k-2}+z^{k-3})x + (z^{k-1}+z^{k-2}).$$

It remains to show that $h(x)$ has an even number of zeros. We have

$$q(x) = (z^{k-1}+z^{k-2})^{-1}x^{k-1}h(z/x) = x^{k-1} + x^{k-2} + \ldots + x + z/(z+1).$$

Since $k = 2^m - 1$, it follows that whenever x is a zero of $q(x)$, so is $x+1$. Thus $q(x)$ and hence $h(x)$ has an even number of zeros. This completes the proof. □

We next give a formula for $\mathrm{rank}_2(M_k)$ in terms of $s(x)$, where $s(x)$ is defined above Theorem 3.4, with $q = 2^d$. Define

$$s^*(x) = \begin{cases} s(x), & \text{if } (2^d-1) \nmid x, \\ d, & \text{if } (2^d-1) \mid x. \end{cases}$$

Theorem 7.3. *For integers $k \geq 3$ and $d \geq 2$, $\mathrm{rank}_2(M_k)$ equals the number of a, $0 < a < 2^d - 1$, for which*

$$s(a) + s((k-1)a) = s^*(ka). \tag{7.1}$$

Proof: The $2^d - 1$ complex eigenvalues of M_k are

$$\sum_{x \in \mathbb{F}_{2^d}^*} \chi(f(x)),$$

where χ ranges over the $2^d - 1$ multiplicative characters on $\mathbb{F}_{2^d}^*$. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\xi_{2^d-1}]$ lying over 2, and let $\omega = \omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_{2^d}^*$. Then $\mathrm{rank}_2(M_k)$ equals the number of a, $0 < a < 2^d - 1$, for which

$$\mathfrak{p} \nmid J(\omega^{-a}, \omega^{-(k-1)a}) = \sum_{x \in \mathbb{F}_{2^d}^*} \omega^{-a}(f(x))$$

(cf. Theorem 3.3). For $0 < a < 2^d - 1$, we have

$$\mathfrak{p}^{s(a)+s((k-1)a)-s^*(ka)} \mid\mid J(\omega^{-a}, \omega^{-(k-1)a})$$

(cf. (3.10)), since $J(\omega^{-a}, \omega^{-(k-1)a})$ is a unit if ka or $(k-1)a$ is divisible by $2^d - 1$. The theorem now follows. □

Let $R_k(d)$ denote the number of solutions a, $0 < a < 2^d - 1$, to equation (7.1). Thus by Theorem 7.3, $R_k(d) = \mathrm{rank}_2(M_k)$. The reader should observe the similarity of the problems of determining $R_k(d)$, the number of solutions a, $0 < a < 2^d - 1$, to equation (7.1), and of determining $B_k(d)$, the number of solutions a, $0 < a < 2^d - 1$, to equation (3.8). In the case of $B_k(d) = dA_k(d)$ we obtained linear recurrences for all relevant values of k (see (4.4), (4.24), (4.8)). The next proposition shows that linear recurrences exist for the $R_k(d)$ as well. We omit the proof, as the proposition can be proved by an approach similar to the one we used in the proofs of Theorems 4.6 and 4.8.

Proposition 7.4. *Let k be a fixed integer ≥ 3. The generating function $\sum_{d\geq 2} R_k(d)z^d$ for the numbers $R_k(d)$ of solutions a, $0 < a < 2^d - 1$, to equation (7.1) is a rational function in z, and, hence, the sequence $(R_k(d))_{d\geq e}$ satisfies a linear recurrence for e large enough.* □

A proof of this proposition in the style of the proofs of Theorems 4.6 and 4.8 also gives bounds on the degrees of the numerator and denominator polynomials of the rational generating function $\sum_{d\geq 2} R_k(d)z^d$. So, this allows us, at least for k not too large, to determine recurrences via the computer, by first computing enough numbers $R_k(d)$ to guess a linear recurrence using `gfun` [23], and then applying Lemma 4.5.

In the next theorem, we determine $R_k(d)$ explicitly for $3 \leq k \leq 9$ by computing the corresponding rational generating functions.

Theorem 7.5. *For $3 \leq k \leq 9$, the generating functions $\sum_{d\geq 2} R_k(d)z^d$ are respectively*

$$\sum_{d\geq 2} R_3(d)z^d = \frac{z^2(2-z)}{(1-z)(1-z-z^2)}, \tag{7.2}$$

$$\sum_{d\geq 2} R_4(d)z^d = \frac{2z^2}{1-z^2}, \tag{7.3}$$

$$\sum_{d\geq 2} R_5(d)z^d = \frac{z^3(3+2z-3z^2)}{(1-z)(1+z^2)(1-z-z^2)}, \tag{7.4}$$

$$\sum_{d\geq 2} R_6(d)z^d = \frac{z^2(2+4z^2)}{1-z^2-z^4}, \tag{7.5}$$

$$\sum_{d\geq 2} R_7(d)z^d = \frac{z^2(2+2z-6z^2-2z^3-2z^4+5z^5)}{(1-z)(1-z-z^3)(1-z^2-z^3)}, \tag{7.6}$$

$$\sum_{d\geq 2} R_8(d)z^d = \frac{6z^3}{1-z^3}, \tag{7.7}$$

$$\sum_{d\geq 2} R_9(d)z^d = \frac{z^2(2-4z+6z^2+2z^3+2z^4-12z^5-2z^6+7z^7)}{(1-z)(1-z-z^2)(1+z^3-z^6)}. \tag{7.8}$$

Proof: These assertions can, in principle, be proved as we described above the statement of the theorem. However, it is instructive to exhibit the solutions to (7.1) in each case explicitly, from which (7.2)–(7.8) then follow easily by means of generating function calculus.

For the description of the solution sets we use a standard notation from the calculus of words (cf. [18]): Given an alphabet $\mathcal{A}$, the set of all words (including the empty word) consisting of letters from $\mathcal{A}$ is denoted by $\mathcal{A}^*$. With that terminology, the solutions to (7.1) in the cases $k = 3, \ldots, 9$ can be described as follows:

For $k = 3$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $\{0, 01\}^* \backslash \{0\}^*$.

For $k = 4$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $\{01\}^*$.

For $k = 5$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $\{0, 001, 0011\}^* \backslash \{0\}^*$.

For $k = 6$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $\{01, 0011\}^*$.

For $k = 7$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $(\{0, 001\}^* \cup \{01, 011\}^*) \backslash \{0\}^*$.

For $k = 8$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $\{001, 011\}^*$.

For $k = 9$, the binary representations of the solutions a to (7.1), $0 < a < 2^d - 1$, are obtained by forming all possible rotations of the strings of length d from the set $(\{0, 00011, 000111\} \cup \{0001, 000101, 00010101, \dots\})^* \backslash \{0\}^*$.

These assertions can be established in a way similar to the proof of Proposition 4.1, with use of the fact that the solutions a to (7.1), $0 < a < 2^d - 1$, are characterized by the property that there is no instance of a 1 occurring in the same place in the binary expansions of a and $(k-1)a \pmod{2^d - 1}$.

The formulas (7.2)–(7.8) for the generating functions follow, as we now demonstrate for the case $k = 5$.

From the above, the binary representation of a solution a to (7.1) with $k = 5$ must be some rotation of a nonzero string of length d obtained by concatenating the blocks 0, 001, and 0011. To identify the block in the *cyclic* binary representation of a which overlaps with the rightmost place of the binary representation of a, we underline the digit in that block where the overlap occurs. We have the following possibilities for such blocks: $\underline{0}$, $\underline{0}01$, $0\underline{0}1$, $00\underline{1}$, $\underline{0}011$, $0\underline{0}11$, $00\underline{1}1$, $001\underline{1}$. Once we have chosen one of these possibilities, we have to "glue" this already chosen block with a (possibly empty) sequence of other blocks from $\{0, 001, 0011\}$ to form a binary string representing a solution to (7.1), where the underlined place is considered as the rightmost place in the string (through appropriate rotation). Hence, in symbolic notation again, the set of all solutions to (7.1) is

$$\big(\{\underline{0}, \underline{0}01, 0\underline{0}1, 00\underline{1}, \underline{0}011, 0\underline{0}11, 00\underline{1}1, 001\underline{1}\} \times \{0, 001, 0011\}^*\big) \backslash \{0\}^*.$$

In particular, a string taken from this set is a solution to (7.1) with corresponding d equal to the length of the string. Since the set $\{\underline{0}, \underline{0}01, 0\underline{0}1, 00\underline{1}, \underline{0}011, 0\underline{0}11, 00\underline{1}1, 001\underline{1}\}$ contains one string of length 1, three strings of length 3, and four strings of length 4, its corresponding generating function is $z + 3z^3 + 4z^4$. Similarly, the set $\{0, 001, 0011\}$ has generating function $z + z^3 + z^4$. Therefore, by elementary "generatingfunctionology" (see [30]), the generating function for the solutions a to (7.1), and, hence, the generating function $\sum_{d \ge 2} R_5(d) z^d$, is given by

$$(z + 3z^3 + 4z^4) \cdot \frac{1}{1 - (z + z^3 + z^4)} - \frac{z}{1 - z}. \tag{7.9}$$

Simplification of expression (7.9) gives (7.4).

We leave the details in the remaining cases to the reader. □

Acknowledgements. The authors are grateful to S. Payne for pointing out the reference [22, Theorem 12.5.3] in the proof of Lemma 2.3, and to Jürgen Bierbrauer for computing a bound for the minimum distance of the code in Example 5.2. The second and fourth authors would like to express their gratitude to the Mathematische Forschungsinstitut Oberwolfach, where they first met and where part of this work initiated. The third author would like to thank the University of California at San Diego for the opportunity to spend a visit in Winter Quarter 1998, which brought together the first and third authors to work on this subject. The research of the fourth author was supported in part by NSA grant MDA 904-97-0104, and a grant from the University of Delaware Research Foundation.

References

[1] M. Antweiler and L. Bömer, *Complex sequences over $GF(p^m)$ with a two-level autocorrelation function and a large linear span*, IEEE Trans. Inform. Theory, **38** (1992), 120–130.

[2] E. F. Assmus, Jr., and J. D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics, 103, Cambridge University Press, Cambridge, 1992.

[3] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory, **11** (1979), 349–398.

[4] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Wiley Interscience, 1998.

[5] W. G. Bridges, M. Hall, and J. L. Hayden, *Codes and designs*, J. Combin. Theory Ser. A **31** (1981), 155–174.

[6] J. Cannon and C. Playoust, *An introduction to MAGMA*, University of Sydney, Australia, 1993.

[7] W. E. Cherowitzo and L. Storme, *α-flocks with oval herds and monomial hyperovals*, preprint.

[8] D. Glynn, *Two new sequences of ovals in finite Desarguesian planes of even order*, Lecture Notes in Mathematics 1036, Springer-Verlag, 1983, 217–229.

[9] J. M. Goethals and P. Delsarte, *On a class of majority logic decodable cyclic codes*, IEEE Trans. Inform. Theory, **14** (1968), 182–188.

[10] S. W. Golomb, *The use of combinatorial structures in communication signal designs*, in: "Applications of Combinatorial Mathematics", Chris Mitchell (ed.), vol. 60, 1997, 59–78.

[11] B. Gordon, W. H. Mills and L. R. Welch, *Some new difference sets*, Canad. J. Math. **14** (1962), 614–625.

[12] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes*, Hiroshima Math. J. **3** (1973), 154–226.

[13] N. Hamada and H. Ohmori, *On the BIB-design having the minimum p-rank*, J. Combin. Theory Ser. A **18** (1975), 131–140.

[14] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields.* Oxford University Press, 1979.

[15] D. Jungnickel, *Difference Sets*, in: "Contemporary Design Theory, A Collection of Surveys", J. Dinitz, D. R. Stinson (eds.), Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley, New York, 1992, 241–324.

[16] E. S. Lander, *Symmetric Designs, An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[18] M. Lothaire, *Combinatorics on words*, 2nd ed., Encyclopedia of Mathematics and Its Applications, vol. 17, Cambridge University Press, Cambridge, 1997.

[19] J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set*, Inform. Control **12** (1968), 474–488.
[20] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.
[21] A. Maschietti, *Difference sets and hyperovals*, Designs, Codes and Crypt. **14** (1998), 89–98.
[22] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Research Notes in Mathematics, **110**, Pitman Pub. Inc., 1984.
[23] B. Salvy and P. Zimmermann, *Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable*, ACM Trans. Math. Software **20** (1994).
[24] R. A. Scholtz and L. R. Welch, *GMW sequences*, IEEE Trans. Inform. Theory **30** (1984), 548–553.
[25] B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.
[26] K. J. C. Smith, *On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry*, J. Combin. Theory **7** (1969), 122–129.
[27] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Wadsworth & Brooks/Cole, Pacific Grove, California, 1986; reprinted by Cambridge University Press, Cambridge, 1997.
[28] R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.
[29] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Springer, 1997.
[30] H. S. Wilf, *generatingfunctionology*, 2nd ed., Academic Press, San Diego, 1994.
[31] Q. Xiang, *On balanced binary sequences with two-level autocorrelation functions*, IEEE Trans. Inform. Theory, to appear.
[32] K. Yamamoto, *On Jacobi sums and difference sets*, J. Combin. Theory Ser. A **3** (1967), 146–181.
[33] K. Yamamoto, *On congruences arising from relative Gauss sums*, in: "Number Theory and Combinatorics", Japan 1984, World Scientific Publ., 1985, 423–446.

Department of Mathematics, University of California, San Diego, La Jolla, California 92093-0112, USA,
E-mail address: revans@euclid.ucsd.edu

Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands,
E-mail address: hollmann@natlab.research.philips.com

Institut für Mathematik, Universität Wien, Strudlhofgasse 4, A-1090 Vienna, Austria,
E-mail address: kratt@pap.univie.ac.at
WWW: http://radon.mat.univie.ac.at/People/kratt

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA,
E-mail address: xiang@math.udel.edu