AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **55** (2013), Pages 49–63

Jacobi-like sums and difference sets with Singer parameters

J. F. Dillon

National Security Agency
Fort George G. Meade, MD 20755
U.S.A.
jfdillon@gmail.com

Neeraj Kashyap

Department of Mathematics
Indiana University
Bloomington, IN 47405
U.S.A.
nkashyap@indiana.edu

Dedicated to Kathy Horadam on the happy occasion of her birthday

Abstract

We show that a function $F : \mathbb{F}_{2^m}^{\times} \to \mathbb{C}$ whose multiplicative Fourier coefficients are given by certain character sums, which we call Jacobi-like sums, is in fact the ± 1-valued characteristic function of a difference set in $\mathbb{F}_{2^m}^{\times}$ with Singer parameters. We show further that the difference sets arising from such functions are precisely the so-called DD difference sets constructed by the first author and Hans Dobbertin.

1 Introduction

The purpose of this paper is to give an alternative proof that the sets constructed by Dillon and Dobbertin in [6] are indeed difference sets with Singer parameters. In contrast with the methods employed in that paper, which made use of the Fourier transform on the additive group of the field $\mathbb{F}_{2^m}$, we utilize the more traditional number theoretic approach based on analysis of the multiplicative Fourier coefficients of the sets in question. In fact, our approach is independent of that in [6] and we make explicit use of its results only in the final section of this paper, in which we

prove that the difference sets we have constructed are indeed the same as those constructed there. Similar Jacobi-like sums are used in [1] to construct, for arbitrary primes p, p-ary sequences with ideal autocorrelation and derived cyclic difference sets with Singer parameters.

First, we set some notation. Given a function $f : \mathbb{F}_{2^m}^{\times} \to \mathbb{C}$, we will usually extend f to $\mathbb{F}_{2^m}$ by $f(0) := 0$; in particular, we define $\chi(0) := 0$ for all multiplicative characters χ of $\mathbb{F}_{2^m}^{\times}$. On the extension $\mathbb{F}_{2^m}$ of $\mathbb{F}_2$ we have the trace map $Tr(x)$ defined by

$$Tr(x) := \sum_{j=0}^{m-1} x^{2^j}.$$

If χ is a character of the multiplicative group $\mathbb{F}_{2^m}^{\times}$ we denote by $\mathcal{G}(\chi)$ the Gauss sum

$$\mathcal{G}(\chi) := \sum_{x \in \mathbb{F}_{2^m}} \chi(x)(-1)^{Tr(x)}.$$

Given two multiplicative characters χ and ψ of $\mathbb{F}_{2^m}$, we denote by $\mathcal{J}(\chi, \psi)$ the Jacobi sum

$$\mathcal{J}(\chi, \psi) := \sum_{x \in \mathbb{F}_{2^m}} \chi(x)\psi(1-x).$$

Below we state some basic facts about Gauss and Jacobi sums, proofs of which can be found in [4] and [10].

If χ_0 denotes the principal character of $\mathbb{F}_{2^m}^{\times}$, then $\mathcal{G}(\chi_0) = -1$ by the orthogonality relations for the additive characters of $\mathbb{F}_{2^m}$. If χ is a nonprincipal character of $\mathbb{F}_{2^m}^{\times}$, then

$$|\mathcal{G}(\chi)|^2 = 2^m. \tag{1}$$

If χ and ψ are nonprincipal characters of $\mathbb{F}_{2^m}^{\times}$ whose product $\chi\psi$ is also nonprincipal, then the Jacobi sum $\mathcal{J}(\chi, \psi)$ can be factored into Gauss sums as

$$\mathcal{J}(\chi, \psi) = \frac{\mathcal{G}(\chi)\mathcal{G}(\psi)}{\mathcal{G}(\chi\psi)}, \tag{2}$$

and this factorization, together with (1), immediately yields the identity

$$|\mathcal{J}(\chi, \psi)|^2 = 2^m. \tag{3}$$

A subset D of a group G is called a (v, k, λ)-*difference set* if $|G| = v$, $|D| = k$, and every nonidentity element of G occurs λ times as the difference gh^{-1} of elements g and h of D. If G is a cyclic group, we call D a *cyclic difference set*. This paper is concerned with cyclic difference sets with *Singer parameters* $(v, k, \lambda) = (2^m - 1, 2^{m-1}, 2^{m-2})$. These parameters are named after James Singer [16]. More information about such difference sets can be found in [2, 3, 9, 11, 6]. References for applications of character theory to the study of difference sets include [13, 17, 3, 14, 15, 7, 6]. A comprehensive reference for all aspects of difference sets is [5].

We identify a function $F : \mathbb{F}_{2^m}^\times \to \mathbb{C}$ with a corresponding element F of the group algebra $\mathbb{C}\mathbb{F}_{2^m}^\times$ by

$$F := \sum_{x \in \mathbb{F}_{2^m}^\times} F(x)x.$$

The adjoint of F acting on $\mathbb{C}\mathbb{F}_{2^m}^\times$ by left multiplication is left multiplication by

$$F^* = \sum_{x \in \mathbb{F}_{2^m}^\times} \overline{F(x)}x^{-1} \in \mathbb{C}\mathbb{F}_{2^m}^\times.$$

Each character χ of $\mathbb{F}_{2^m}^\times$ extends linearly to all of $\mathbb{C}\mathbb{F}_{2^m}^\times$ by

$$\chi(F) := \sum_{x \in \mathbb{F}_{2^m}^\times} F(x)\chi(x);$$

we have the identity

$$\overline{\chi(F)} = \chi(F^*).$$

Characteristic functions of difference sets with Singer parameters must satisfy certain identities in the group algebra, stated in the following lemma. We forego its proof as it is simply an appeal to definitions.

Lemma 1. *Let $f : \mathbb{F}_{2^m} \to \{0, 1\}$ with $f(0) = 0$. Put $F := (-1)^f$. The following statements are equivalent:*

1. *the support D of f is a difference set in $\mathbb{F}_{2^m}^\times$ with Singer parameters $(v, k, \lambda) = (2^m - 1, 2^{m-1}, 2^{m-2})$;*
2. *$FF^* = 2^m - \sum_{x \in \mathbb{F}_{2^m}^\times} x$ in $\mathbb{C}\mathbb{F}_{2^m}^\times$;*
3. *$\chi_0(F) = -1$ and $|\chi(F)|^2 = 2^m$ for all nonprincipal characters χ of $\mathbb{F}_{2^m}^\times$;*
4. *the matrix $[F(xy)]_{x,y \in \mathbb{F}_{2^m}}$ is a Hadamard matrix.*

The main goal of this paper is the following theorem, which we shall prove in the next section.

Theorem 1. *Let k and m be relatively prime positive integers. Define a function $F : \mathbb{F}_{2^m}^\times \to \mathbb{C}$ by its Fourier coefficients:*

$$\chi(F) := \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}. \tag{4}$$

Then F is the ± 1-valued characteristic function of a difference set with Singer parameters.

In analogy with (2), we call the sums (4) *Jacobi-like sums*. The conclusion of Theorem 1 is item 1 of Lemma 1; but the property (1) of Gauss sums and the fact that $\gcd(2^k+1, 2^m-1) = \gcd(3, 2^m-1)$ make it clear that the function F of Theorem 1 satisfies the equivalent item 3 of Lemma 1. Thus, the difficulty in proving the Theorem lies in showing that F, which is defined as a complex-valued function by its Fourier coefficients, satisfies the hypothesis of Lemma 1; i.e. it takes only the values ± 1.

The final section of this paper will address the question of whether or not the construction of Theorem 1 gives rise to previously unknown difference sets. The answer is "No".

Theorem 2. *For k a positive integer relatively prime to m, put $d := 4^k - 2^k + 1$ and let $\Delta : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be the map*

$$\Delta(x) := (x+1)^d + x^d + 1.$$

Let $D := \mathbb{F}_{2^m} \backslash \Delta(\mathbb{F}_{2^m})$. The function $F : \mathbb{F}_{2^m}^\times \to \mathbb{C}$ given by (4) is in fact the ± 1-valued characteristic function of D.

The construction in Theorem 2 of the difference sets D is precisely the one given in [6]. Thus Theorem 1 merely constitutes a new proof that the sets D are indeed cyclic difference sets with Singer parameters. In a way, the order in which the theorems are presented is a bit deceptive since it was the construction of [6] which led to our study of the Jacobi-like sums. On the other hand, defining a function F on $\mathbb{F}_{2^m}^\times$ so that the character sums $\chi(F)$, as expressions in Gauss sums, are guaranteed to satisfy the requisite $|\chi(F)|^2 = 2^m$ has the potential for being a rich source of difference sets.

2 Construction of the difference sets

The purpose of this section is to prove Theorem 1. To that end let $F : \mathbb{F}_{2^m}^\times \to \mathbb{C}$ be defined by (4). First, note that F can be recovered explicitly from its multiplicative Fourier coefficients by Fourier inversion.

$$F(x) := \frac{1}{2^m - 1} \sum_{\chi} \chi(F)\overline{\chi}(x). \tag{5}$$

Given (4), it is clear that, for each $x \in \mathbb{F}_{2^m}^\times$, $F(x) \in \mathbb{Q}(\zeta_{2^m-1})$ where ζ_{2^m-1} is a primitive $(2^m-1)^{st}$ root of unity. The first step of the proof is to show that $F(x)$ is an algebraic integer.

We call a character χ of $\mathbb{F}_{2^m}^\times$ *degenerate* if $\chi^3 = \chi_0$. Since $\gcd(2^k+1, 2^m-1) = \gcd(3, 2^m-1)$ and $\mathcal{G}(\chi_0) = -1$, if χ is degenerate then $\chi(F)$ is simply a Gauss sum and is therefore an algebraic integer. To prove the claim for nondegenerate characters we make use of the Davenport-Hasse formulas, stated below; for proofs see [4].

Theorem 3. (Davenport-Hasse product formula.) *Given a character ψ of $\mathbb{F}_q^\times$ of order $l > 1$, for any character χ of $\mathbb{F}_q^\times$, put*

$$N(l,\chi) := \frac{\chi^l(l)\mathcal{G}(\chi)}{\mathcal{G}(\chi^l)} \prod_{j=1}^{l-1} \frac{\mathcal{G}(\chi\psi^j)}{\mathcal{G}(\psi^j)}. \tag{6}$$

For each $l > 0$ and each character χ of $\mathbb{F}_q^\times$, $N(l,\chi) = 1$.

Theorem 4. (Davenport-Hasse forumula for lifted Gauss sums.) *A character χ on $\mathbb{F}_q^\times$ induces a character $\tilde{\chi}$ on the multiplicative group of any extension $\mathbb{F}_{q^s}$ via composition with the norm map $\mathbb{F}_{q^s} \to \mathbb{F}_q$. Denote by $\mathcal{G}_{\mathbb{F}_{q^s}}(\tilde{\chi})$ and $\mathcal{G}_{\mathbb{F}_q}(\chi)$ the Gauss sums over the corresponding fields. Then*

$$\mathcal{G}_{\mathbb{F}_{q^s}}(\tilde{\chi}) = (-1)^{s-1}\mathcal{G}_{\mathbb{F}_q}(\chi)^s.$$

Suppose first that χ is a nondegenerate character on $\mathbb{F}_{2^m}^\times$ where m is even. In particular, this means that there is a cubic character ψ of $\mathbb{F}_{2^m}^\times$. For a function F as defined by (4), the Davenport-Hasse product formula gives the following identity.

$$\chi(F)^2 = \overline{\mathcal{J}(\chi\psi, \chi^{2^k}\psi^2)\mathcal{J}(\chi^{2^k}\psi, \chi\psi^2)}. \tag{7}$$

To see this, consider the expression

$$\begin{aligned}
\chi(F)^2 &= \frac{\chi(F)^2}{N(3,\chi)^2} \\
&= \frac{\mathcal{G}(\chi)^2\mathcal{G}(\chi^{2^k+1})^2}{\mathcal{G}(\chi^3)^2} \cdot \frac{\mathcal{G}(\psi)^2\mathcal{G}(\chi^3)^2\mathcal{G}(\psi^2)^2}{\chi^3(3)^2\mathcal{G}(\chi)^2\mathcal{G}(\chi\psi)^2\mathcal{G}(\chi\psi^2)^2} \\
&= \frac{\mathcal{G}(\chi^{2^k+1})^2\mathcal{G}(\psi)^2\mathcal{G}(\psi^2)^2}{\mathcal{G}(\chi\psi)^2\mathcal{G}(\chi\psi^2)^2} \\
&= 2^{2m}\frac{\mathcal{G}(\chi^{2^k+1})^2}{\mathcal{G}(\chi\psi)^2\mathcal{G}(\chi\psi^2)^2}.
\end{aligned}$$

Applying the automorphism $x \mapsto x^{2^k}$ on $\mathbb{F}_{2^m}$ gives

$$\mathcal{G}(\chi\psi) = \mathcal{G}((\chi\psi)^{2^k}) = \mathcal{G}(\chi^{2^k}\psi^2),$$

since k is relatively prime to m and therefore is odd. Similarly

$$\mathcal{G}(\chi\psi^2) = \mathcal{G}(\chi^{2^k}\psi).$$

Thus

$$\chi(F)^2 = 2^{2m}\frac{\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi\psi)\mathcal{G}(\chi^{2^k}\psi^2)} \cdot \frac{\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^{2^k}\psi)\mathcal{G}(\chi\psi^2)},$$

yielding (7) by (2) and (3).

For m odd, note that applying the automorphism $x \mapsto x^{2^{m-k}}$ gives

$$\mathcal{G}(\chi^{2^k+1}) = \mathcal{G}(\chi^{2^{m-k}+1}),$$

so the function defined by (4) for k is the same as that defined for $m-k$. Thus we may assume without loss of generality that k is odd. Let χ be a nondegenerate character of $\mathbb{F}_{2^m}^\times$ and denote by $\tilde{\chi}$ its lift to $\mathbb{F}_{2^{2m}}^\times$. Then the order of $\tilde{\chi}$ is the same as that of χ and thus $\tilde{\chi}$ is a nondegenerate character of $\mathbb{F}_{2^{2m}}^\times$. By Theorem 4 and (7) we obtain the following identity.

$$\chi(F)^4 = \overline{\mathcal{J}(\chi'\psi, (\chi')^{2^k}\psi^2)\mathcal{J}((\chi')^{2^k}\psi, \chi'\psi^2)} \tag{8}$$

The identities (7) and (8) prove that each $\chi(F)$ is an algebraic integer in $\mathbb{Q}(\zeta_{2^m-1})$.

Let n be an integer relatively prime to 2^m-1 and let σ denote the automorphism $\zeta_{2^m-1} \mapsto \zeta_{2^m-1}^n$ of $\mathbb{Q}(\zeta_{2^m-1})$. Then for any $x \in \mathbb{F}_{2^m}^\times$, by (5),

$$\begin{aligned}\sigma\left((2^m-1)F(x)\right) &= \sum_\chi \chi^n(F)\overline{\chi}^n(x)\\ &= \sum_\chi \chi(F)\overline{\chi}(x)\\ &= (2^m-1)F(x).\end{aligned}$$

Since $(2^m-1)F(x)$ is an algebraic integer in $\mathbb{Q}(\zeta_{2^m-1})$ invariant under the Galois group, it is a rational integer.

Similarly, considering explicitly the expression of (4) and separating the contribution of the degenerate characters from that of the non-degenerate ones, we obtain

$$\begin{aligned}F(x) &= \frac{1}{2^m-1}\sum_\chi \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}\overline{\chi}(x)\\ &= \frac{1}{2^m-1}\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\overline{\chi}(x) + \frac{1}{2^m(2^m-1)}\sum_{\chi^3\neq\chi_0}\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\overline{\chi}(x).\end{aligned}$$

Adding to and subtracting from the above expression the term

$$\frac{1}{2^m(2^m-1)}\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\overline{\chi}(x) = \frac{1}{2^m(2^m-1)}\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\overline{\chi}(x),$$

gives the identity

$$F(x) = \frac{1}{2^m-1}\left(\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\overline{\chi}(x) - \frac{1}{2^m}\mathcal{G}(\chi)\overline{\chi}(x)\right) + \frac{1}{2^m}\gamma(x),$$

where

$$\gamma(x) := \frac{1}{2^m-1}\sum_{\chi}\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\overline{\chi}(x).$$

Noting that

$$\frac{1}{2^m-1}\sum_{\chi^3=\chi_0}\left(\mathcal{G}(\chi)\overline{\chi}(x)-\frac{1}{2^m}\mathcal{G}(\chi)\overline{\chi}(x)\right)=\frac{1}{2^m-1}\sum_{\chi^3=\chi_0}\frac{2^m-1}{2^m}\mathcal{G}(\chi)\overline{\chi}(x),$$

we have

$$F(x)=\frac{1}{2^m}\left(\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\overline{\chi}(x)+\gamma(x)\right), \tag{9}$$

where

$$\begin{aligned}\gamma(x)&=\frac{1}{2^m-1}\sum_{\chi}\overline{\chi}(x)\sum_{u,v,w}\chi(uv^{2^k+1}w^{-3})(-1)^{Tr(u+v+w)}\\&=\frac{1}{2^m-1}\sum_{u,v,w}(-1)^{Tr(u+v+w)}\sum_{\chi}\chi(uv^{2^k+1}w^{-3})\overline{\chi}(x)\\&=\sum_{uv^{2^k+1}w^{-3}=x}(-1)^{Tr(u+v+w)}.\end{aligned}$$

Thus $\gamma(x)\in\mathbb{Z}$ for all $x\in\mathbb{F}_{2^m}^{\times}$. Furthermore, the sum

$$\sum_{\chi^3=\chi_0}\mathcal{G}(\chi)\overline{\chi}(x)$$

is invariant under the action of the Galois group of $\mathbb{Q}(\zeta_{2^m-1})$ over $\mathbb{Q}$ and thus that sum is also a rational integer. Therefore, by (9), $2^mF(x)\in\mathbb{Z}$.
Since $(2^m-1)F(x)$ and $2^mF(x)$ are in $\mathbb{Z}$ for all $x\in\mathbb{F}_{2^m}^{\times}$, we deduce that $F(x)$ is a rational integer for all x.
By Plancherel's theorem, since $|\chi(F)|^2=2^m$ for $\chi\neq\chi_0$, and $|\chi_0(F)|^2=1$, we have

$$\sum_{x\in\mathbb{F}_{2^m}^{\times}}F(x)^2=2^m-1.$$

The terms in the sum are all integers and are 2^m-1 in number. Thus in order to show that F takes values ±1 it suffices to show that if $x\in\mathbb{F}_{2^m}^{\times}$ then $F(x)\neq0$.

Let P be a prime ideal lying over 2 in $\mathbb{Q}(\zeta_{2^m-1})$. Recall that 2 is unramified in $\mathbb{Q}(\zeta_{2^m-1})$ and the inertial degree of P is m, i.e. $\mathbb{Z}[\zeta_{2^m-1}]/P\cong\mathbb{F}_{2^m}$. Thus there is a character τ of $\mathbb{F}_{2^m}^{\times}$ satisfying

$$\tau(x)\equiv x\ (mod\ P).$$

This character τ is called the Teichmüller character associated with P. Since it is an isomorphism between $\mathbb{F}_{2^m}^{\times}$ and the group of $(2^m-1)^{st}$ roots of unity, τ is a generator for the character group of $\mathbb{F}_{2^m}^{\times}$. Using τ enables us to compute explicitly the valuation of a Gauss sum on $\mathbb{F}_{2^m}$ over P:

Theorem 5. (Stickelberger's theorem.) *Let ν denote the discrete valuation (written additively) induced on $\mathbb{Q}(\zeta_{2^m-1})$ by P, and let τ denote the Teichmüller character associated with P. Given an integer a with $0 \leq a < 2^m - 1$ and binary expansion $a = \sum_{j=0}^{m-1} a_j 2^j$, denote by $s(a)$ its binary weight, i.e. $s(a) = \sum a_i$. Then*

$$\nu\left(\mathcal{G}(\tau^{-a})\right) = s(a).$$

For detailed discussions of this theorem, see e.g. [4, 10, 18].

To complete the proof of Theorem 1 we will show that, given a prime P lying over 2 as above with ν the associated valuation, $\nu(F(x)) = 0$ for all $x \in \mathbb{F}_{2^m}^{\times}$. To prove this, we apply Theorem 5 to (7) and (8). To this end, let m be even and, given a prime P lying over 2 in $\mathbb{Q}(\zeta_{2^m-1})$, let ν be the associated valuation and τ the associated Teichmüller character. Let χ be a nondegenerate character of $\mathbb{F}_{2^m}^{\times}$ and suppose that

$$\nu\left(\mathcal{J}(\chi\psi, \chi^{2^k}\psi^2)\mathcal{J}(\chi^{2^k}\psi, \chi\psi^2)\right) = 0. \tag{10}$$

Then we must have

$$\nu\left(\mathcal{J}(\chi\psi, \chi^{2^k}\psi^2)\right) = 0 = \nu\left(\mathcal{J}(\chi^{2^k}\psi, \chi\psi^2)\right).$$

Writing $\chi = \tau^{-a}$ and choosing as the cubic character ψ the character τ^{-b} where $b := \frac{2^m-1}{3}$, we get by Theorem 5 and (2) that

$$s(a+b) + s(2^k a + 2b) - s((2^k+1)a) = 0 = s(2^k a + b) + s(a + 2b) - s((2^k+1)a).$$

Denote by c, d, and u the residues modulo $2^m - 1$ of $a + b$, $a + 2b$, and $(2^k + 1)a$ respectively. As before, we assume without loss of generality that k is odd, and thus $s(2^k a + 2b) = s(2^k c)$, $s(2^k a + b) = s(2^k d)$. The above equations can be rewritten as

$$s(c) + s(2^k c) - s(u) = 0 = s(d) + s(2^k d) - s(u). \tag{11}$$

In general, the expression $s(u)+s(v)-s(u+v)$ counts the number of carries when adding u and v in their binary expansions; for a nice discussion of this fact, refer to [8]. Reference [7] obtains such expressions by applying Stickelberger's Theorem to classical Jacobi sums which they observe to be the character sums for the difference sets which arise from Maschietti's Theorem on monomial hyperovals [12]. They then go on to demonstrate remarkable combinatorial virtuosity by exactly evaluating these expressions for several known classes of monomial hyperovals, thereby obtaining the 2-ranks of these difference sets and new inequivalence results. We have followed their lead here by applying Stickelberger's Theorem to our Jacobi-like sums; but our aim here is much more modest.

Since $c + 2^k c = u = d + 2^k d$, neither of the sums has any binary carries. If one

writes explicitly

$$c = \sum_{j=0}^{m-1} c_j 2^j,$$
$$d = \sum_{j=0}^{m-1} d_j 2^j,$$
$$u = \sum_{j=0}^{m-1} u_j 2^j,$$

the no-carries condition translates to

$$c_j + c_{j-k} = u_j = d_j + d_{j-k}, \ \forall\ j. \tag{12}$$

Working in the ring $\mathbb{Z}[x]$, we define the polynomials

$$C(x) := \sum_{j=0}^{m-1} c_j x^j,$$
$$D(x) := \sum_{j=0}^{m-1} d_j x^j,$$
$$U(x) := \sum_{j=0}^{m-1} u_j x^j.$$

Here (12) becomes the identity

$$(x^k + 1)\,(C(x) - D(x)) \equiv U(x) - U(x) \equiv 0 \ (mod\ x^m - 1).$$

Since k is relatively prime to m, $gcd(x^k + 1, x^m - 1) = x + 1$ in $\mathbb{Z}[x]$ and so the polynomial $\frac{x^m-1}{x+1}$ must divide $C(x) - D(x)$. However, since the coefficients of $C(x)$ and $D(x)$ are either 0 or 1 and their degree is no greater than $m - 1$, and since

$$\frac{x^m - 1}{x + 1} = \sum_{j=0}^{m-1} (-1)^j x^j,$$

we have

$$C(x) - D(x) = \pm \sum_{j=0}^{m-1} (-1)^j x^j,$$

and thus $c = b$ and $d = 2b$, or $c = 2b$ and $d = b$.

Since k is odd and $c + 2^k c = (2^k + 1)a$, we derive also that

$$2^m - 1 = b + 2b = (2^k + 1)a,$$

and so $\frac{2^m-1}{3}|a$, which means that $\chi^3 = \chi_0$, a contradiction to the non-degeneracy of χ.

Note that when m is odd, we may simply lift to the quadratic extension of $\mathbb{F}_{2^m}$ and carry out the argument there, appealing finally to (8). Thus for any m, if χ is a non-degenerate character of $\mathbb{F}_{2^m}^\times$ and P is any prime lying over 2 in $\mathbb{Q}(\zeta_{2^m-1})$ with associated valuation ν, we have

$$\nu\left(\chi(F)\right) > 0. \tag{13}$$

A straightforward application of Theorem 5 shows that (13) also holds for a cubic character of $\mathbb{F}_{2^m}^\times$. For the principal character, of course, we have

$$\nu\left(\chi_0(F)\right) = 0.$$

Thus by (5) we have that $F(x)$ is odd for all $x \in \mathbb{F}_{2^m}^\times$, completing the proof of Theorem 1.

3 Comparison with older constructions

We now prove Theorem 2. First we recall some notation from [6]. As in the statement of the theorem, let k be a positive integer relatively prime to m and put $d := 4^k - 2^k + 1$. Consider the map $\Delta : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ defined by

$$\Delta(x) := (x+1)^d + x^d + 1.$$

Put $D := \mathbb{F}_{2^m} \backslash \Delta(\mathbb{F}_{2^m})$, let b denote its characteristic function, and put $B := (-1)^b$. We shall now establish the following

Claim 1. $\chi(B) = \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}$ *for all characters* χ *of* $\mathbb{F}_{2^m}^\times$.

Given a function $F : \mathbb{F}_{2^m} \to \mathbb{C}$, we denote by $\widehat{F}$ its additive Fourier transform (or Hadamard transform) given by

$$\widehat{F}(\alpha) := \frac{1}{2^{\frac{m}{2}}} \sum_{x \in \mathbb{F}_{2^m}} F(x)(-1)^{Tr(\alpha x)}.$$

$F \mapsto \widehat{F}$ is a unitary operator on the Hermitian space of complex-valued functions on $\mathbb{F}_{2^m}$ with inner product given by

$$\langle F, G\rangle := \sum_{x \in \mathbb{F}_{2^m}} F(x)\overline{G(x)};$$

and Plancherel's Theorem says

$$< F, G >=< \widehat{F}, \widehat{G} > \forall F, G \in \mathbb{C}^{\mathbb{F}_{2^m}}.$$

It will be useful to compute the Hadamard transforms of multiplicative characters of $\mathbb{F}_{2^m}$. If χ is a character of $\mathbb{F}_{2^m}^{\times}$, which we extend to the entire field by $\chi(0) := 0$, and if $\alpha \neq 0$, then

$$\widehat{\chi}(\alpha) = \frac{1}{2^{\frac{m}{2}}} \sum_{x \in \mathbb{F}_{2^m}} \chi(x)(-1)^{Tr(\alpha x)} = \frac{1}{2^{\frac{m}{2}}} \bar{\chi}(\alpha)\mathcal{G}(\chi). \tag{14}$$

In [6] the first author and Hans Dobbertin proved that if $C_\gamma : \mathbb{F}_{2^m} \to \mathbb{C}$ is defined by

$$C_\gamma(x) := B(\gamma x^{2^k+1}),$$

then

$$\widehat{C_\gamma}(\alpha) = \widehat{S_{3,\gamma}}(\alpha^{\frac{2^k+1}{3}}), \tag{15}$$

where $S_{3,\gamma}(x) := (-1)^{Tr(\gamma x^3)}$.

We now have all the tools we need to verify Claim 1. We certainly have for all χ

$$\chi(B) = \sum_{x \in \mathbb{F}_{2^m}} \chi(x)B(x).$$

In particular, for the principal character χ_0, we have $\chi_0(B) = -1$ and so Claim 1 holds for χ_0. From now on we assume that $\chi \neq \chi_0$. First we deal with the case that m is odd, in which case

$$\gcd(2^k + 1, 2^m - 1) = 1 = \gcd(3, 2^m - 1).$$

We have

$$\begin{aligned}
\chi(B) &= \sum_{x \in \mathbb{F}_{2^m}} \chi(x)B(x) \\
&= \sum_{x \in \mathbb{F}_{2^m}} \chi(x^{2^k+1})B(x^{2^k+1}) \\
&= \sum_{x \in \mathbb{F}_{2^m}} \chi^{2^k+1}(x)C(x) \\
&= \sum_{\alpha \in \mathbb{F}_{2^m}} \widehat{\chi^{2^k+1}}(\alpha)\widehat{C}(\alpha) \\
&= \sum_{\alpha \in \mathbb{F}_{2^m}} \widehat{\chi^{2^k+1}}(\alpha)\widehat{S_3}(\alpha^{\frac{2^k+1}{3}})
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2^{\frac{m}{2}}} \sum_{\alpha \in \mathbb{F}_{2^m}} \chi^{-(2^k+1)}(\alpha) \mathcal{G}(\chi^{2^k+1}) \widehat{S_3}(\alpha^{\frac{2^k+1}{3}}) \\
&= \frac{1}{2^{\frac{m}{2}}} \mathcal{G}(\chi^{2^k+1}) \sum_{\alpha \in \mathbb{F}_{2^m}} \chi^{-3}(\alpha) \widehat{S_3}(\alpha) \\
&= \frac{1}{2^{\frac{m}{2}}} \mathcal{G}(\chi^{2^k+1}) \sum_{x \in \mathbb{F}_{2^m}} \widehat{\chi^{-3}}(x) S_3(x) \\
&= \frac{1}{2^m} \mathcal{G}(\chi^{2^k+1}) \mathcal{G}(\chi^{-3}) \sum_{x \in \mathbb{F}_{2^m}} \chi^3(x) S_3(x) \\
&= \frac{1}{2^m} \mathcal{G}(\chi^{2^k+1}) \mathcal{G}(\chi^{-3}) \sum_{x \in \mathbb{F}_{2^m}} \chi(x^3)(-1)^{Tr(x^3)} \\
&= \frac{\mathcal{G}(\chi) \mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}.
\end{aligned}
$$

Thus, Claim 1 is true for m odd.

Now suppose that m is even. In this case $\gcd(2^k+1, 2^m-1) = 3$. Since k and $m-k$ lead to the same set D and function B, and we cannot have both k and $m-k$ divisible by 3, we may assume that k satisfies the further condition $\gcd(\frac{2^k+1}{3}, 2^m - 1) = 1$. Since the map $x \mapsto x^{2^k+1}$ is a 3-to-1 homomorphism from $\mathbb{F}_{2^m}^{\times}$ onto the subgroup of cubes we may write

$$
3\chi(B) = \sum_{j,x} \chi(\mu_j x^{2^k+1}) B(\mu_j x^{2^k+1}) = \sum_{j,x} \chi(\mu_j x^{2^k+1}) C_{\mu_j}(x), \tag{16}
$$

where μ_1, μ_2, μ_3 represent the three distinct cosets and x ranges over all of $\mathbb{F}_{2^m}$. We first take care of the case that χ has order 3 so that $\chi^{2^k+1} = \chi^3 = \chi_0$, but $\chi \neq \chi_0$. We have

$$
\begin{aligned}
3\chi(B) &= \sum_j \chi(\mu_j) \sum_{x \in \mathbb{F}_{2^m}} \chi^{2^k+1}(x) C_{\mu_j}(x) \\
&= \sum_j \chi(\mu_j) \sum_{x \in \mathbb{F}_{2^m}^{\times}} C_{\mu_j}(x) \\
&= \sum_j \chi(\mu_j) \left(-C_{\mu_j}(0) + \sum_{x \in \mathbb{F}_{2^m}} C_{\mu_j}(x) \right) \\
&= -B(0) \sum_j \chi(\mu_j) + 2^{\frac{m}{2}} \sum_j \chi(\mu_j) \widehat{C_{\mu_j}}(0).
\end{aligned}
$$

Since χ is cubic,

$$
\sum_j \chi(\mu_j) = 0,
$$

and thus by (15) we have

$$\begin{aligned}3\chi(B) &= 2^{\frac{m}{2}}\sum_j \chi(\mu_j)\widehat{S_{3,\mu_j}}(0)\\ &= \sum_j \chi(\mu_j)\sum_{x\in\mathbb{F}_{2^m}}(-1)^{Tr(\mu_j x^3)}\\ &= 3\sum_{x\in\mathbb{F}_{2^m}}\chi(x)(-1)^{Tr(x)}\\ &= 3\mathcal{G}(\chi).\end{aligned}$$

Thus,

$$\chi(B) = \mathcal{G}(\chi) = \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)};$$

so Claim 1 is true if χ has order 3.

Finally, we assume that χ is a non-degenerate character of $\mathbb{F}_{2^m}^{\times}$; i.e. $\chi^3 \neq \chi_0$. Then

$$\begin{aligned}3\chi(B) &= \sum_j \chi(\mu_j)\sum_{x\in\mathbb{F}_{2^m}}\chi^{2^k+1}(x)C_{\mu_j}(x)\\ &= \sum_j \chi(\mu_j)\sum_{\alpha\in\mathbb{F}_{2^m}}\widehat{\chi^{2^k+1}}(\alpha)\widehat{C_{\mu_j}}(\alpha)\\ &= \frac{1}{2^{\frac{m}{2}}}\mathcal{G}(\chi^{2^k+1})\sum_j \chi(\mu_j)\sum_\alpha \chi^{-(2^k+1)}(\alpha)\widehat{S_{3,\mu_j}}(\alpha^{\frac{2^k+1}{3}})\\ &= \frac{1}{2^{\frac{m}{2}}}\mathcal{G}(\chi^{2^k+1})\sum_j \chi(\mu_j)\sum_\alpha \chi^{-3}(\alpha)\widehat{S_{3,\mu_j}}(\alpha)\\ &= \frac{1}{2^{\frac{m}{2}}}\mathcal{G}(\chi^{2^k+1})\sum_j \chi(\mu_j)\sum_{x\in\mathbb{F}_{2^m}}\widehat{\chi^{-3}}(x)S_{3,\mu_j}(x)\\ &= \frac{1}{2^m}\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\sum_j \chi(\mu_j)\sum_{x\in\mathbb{F}_{2^m}}\chi^3(x)S_{3,\mu_j}(x)\\ &= \frac{1}{2^m}\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\sum_{j,x}\chi(\mu_j x^3)(-1)^{Tr(\mu_j x^3)}\\ &= \frac{3}{2^m}\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\mathcal{G}(\chi).\end{aligned}$$

Thus,

$$\begin{aligned}\chi(B) &= 2^{-m}\mathcal{G}(\chi^{2^k+1})\mathcal{G}(\chi^{-3})\mathcal{G}(\chi)\\ &= \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)};\end{aligned}$$

this completes the verification of Claim 1 in all cases.

We have shown that the Fourier transform of function B coincides with that of the function F of Theorem 1; and it follows that the functions B and F must themselves coincide. This completes the proof of Theorem 2.

References

[1] K. T. Arasu, J. F. Dillon and K. J. Player, Character sum factorizations yield perfect sequences, (preprint).

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

[3] L. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics 182, Springer, 1971.

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

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, second ed., 1999.

[6] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields and Their Applications* 10 (2004), 342–389.

[7] R. Evans, H. D. Hollmann, C. Krattenthaler and Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory* 87 (1999), 74–119.

[8] R. J. Friedlander, Factoring factorials, *The Two-Year College Math. Journal* 12 (1981), 12–20.

[9] Marshall Hall Jr, *Combinatorial Theory*, Wiley, second ed., 1986.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math. 84, Springer, 1990.

[11] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lec. Notes 75, Cambridge University Press, 1983.

[12] A. Maschietti, Difference sets and Hyperovals, *Des. Codes Crypto.* 14 (1998), 89–98.

[13] P. Kesava Menon, Difference sets in abelian groups, *Proc. Amer. Math. Soc.* 11 (1960), 368–376.

[14] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Math. 1601, Springer, 1995.

[15] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Math. 1797, Springer, 2002.

[16] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938), 377–385.

[17] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* 15 (1965), 319–346.

[18] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, 1997.

(Received 6 Jan 2012; revised 14 June 2012)