ON A PROBLEM OF H. COHN FOR CHARACTER SUMS

TODD COCHRANE, DAVID GARTH, AND ZHIYONG ZHENG

Abstract. Cohn’s problem on character sums (see [6], p. 202) asks whether a multiplicative character on a finite field can be characterized by a kind of two level autocorrelation property. Let \( f \) be a map from a finite field \( F \) to the complex plane such that \( f(0) = 0, f(1) = 1, \) and \( |f(\alpha)| = 1 \) for all \( \alpha \neq 0. \) In this paper we show that if for all \( a, b \in F^* \), we have

\[
(q - 1) \sum_{\alpha \in F} f(b\alpha)\overline{f(\alpha + a)} = -\sum_{\alpha \in F} f(b\alpha)f(\alpha),
\]

then \( f \) is a multiplicative character of \( F. \) We also prove that if \( F \) is a prime field and \( f \) is a real valued function on \( F \) with \( f(0) = 0, f(1) = 1, \) and \( |f(\alpha)| = 1 \) for all \( \alpha \neq 0, \) then \( \sum_{\alpha \in F} f(\alpha)f(\alpha + a) = -1 \) for all \( a \neq 0 \) if and only if \( f \) is the Legendre symbol. These results partially answer Cohn’s problem.

1. Introduction

Let \( F = \mathbb{F}_q \) be the finite field in \( q = p^\gamma \) elements. We say that a complex valued function defined on \( F \) is a Cohn function if \( f(0) = 0, |f(\alpha)| = 1 \) for all \( \alpha \neq 0, \) and for all nonzero \( a \) in \( F, \)

\[
(1.1) \sum_{\alpha \in F} f(\alpha)f(\alpha + a) = -1.
\]

The last condition just means that the out of phase autocorrelations of \( f \) are all equal to -1. For example, if \( f = \theta \chi, \) where \( \theta \) is a complex constant of modulus one and \( \chi \) is a nontrivial multiplicative character on \( F \) (with \( \chi(0) := 0, \) then \( f \) is a Cohn function. In this case the sum in (1.1) is a well known Jacobi sum. The question then arises whether there are any other Cohn functions. This problem was posed by Harvey Cohn in [4], (p. 202).

To the best of our knowledge, there has been no progress on this problem. In this paper, we solve the problem for the special case of real valued functions defined on a prime field \( \mathbb{F}_p \) (see Theorem 2), and we also prove the following related theorem.

Theorem 1. Let \( f \) be a complex valued function on the finite field \( F \) with \( f(0) = 0, f(1) = 1 \) and \( |f(\alpha)| = 1 \) for all \( \alpha \neq 0. \) Then

\[
(1.2) (q - 1) \sum_{\alpha \in F} f(b\alpha)f(\alpha + a) = -\sum_{\alpha \in F} f(b\alpha)f(\alpha),
\]

for all \( a, b \in F^* \) if and only if \( f \) is a nontrivial multiplicative character on \( F. \)
If $f$ is a nontrivial multiplicative character on $F$ then it is easy to see that (1.2) holds for any $a, b \in F^*$. In this case the factor $f(b)$ can be cancelled from both sides of (1.2) and the equation simplifies to (1.1) which, as we noted above, is known to be valid. When $b = 1$ the equality in (1.2) is just the autocorrelation condition (1.1). Thus by Theorem 1, Cohn’s problem is equivalent to the following problem: Let $f$ be a complex valued function on $F$ with $f(0) = 0$, $f(1) = 1$, and $|f(\alpha)| = 1$ for all $\alpha \neq 0$. Then if equality in (1.2) holds when $b = 1$ and $a \in F^*$, does it hold for all $a, b \in F^*$?

To further explain condition (1.2), we note the following identity, which can be obtained readily by a regrouping of terms: For any complex valued function $f$ on $F$ and nonzero $b \in F$ we have

$$|\sum_{\alpha \in F} f(\alpha)|^2 = \sum_{\alpha \in F} f(b\alpha \overline{f(\alpha)}) + \sum_{a \in F^*} \{\sum_{\alpha \in F} f(b\alpha)f(\alpha + a)\}.$$  

In particular, taking $b = 1$ we see that for any Cohn function $f$, we must have $\sum_{\alpha \in F} f(\alpha) = 0$. We also see that (1.2) holds for arbitrary $a, b \in F^*$ if and only if $\sum_{\alpha \in F} f(\alpha) = 0$ and the value of the sum on the left hand side of (1.2) does not depend on $a$.

Next, we consider the special case that $F$ is a prime field and $f$ is real valued. In this case we are able to completely solve the problem of Cohn.

**Theorem 2.** Let $p$ be an odd prime and $f$ be a real valued function on $F_p$ with $f(0) = 0$, $f(1) = 1$, and $f(\alpha) = \pm 1$ for all $\alpha \neq 0$. Then

$$\sum_{\alpha \in F} f(\alpha)f(\alpha + a) = -1,$$

for all nonzero $a \in F$ if and only if $f$ is the Legendre symbol on $F_p$.

We note that for any finite field $F$ of characteristic 2 and any real valued function $f$ on $F$ satisfying $f(0) = 0$ and $f(\alpha) = \pm 1$ for all nonzero $\alpha \in F$, we trivially cannot have $\sum_{\alpha \in F} f(\alpha) = 0$. Thus there are no real valued Cohn functions on such fields.

**2. Finite Fourier Transforms**

Let $F$ be the finite field in $q = p^\gamma$ elements and let $tr$ denote the trace map from $F$ to $F_p$. We denote by $\psi$ the nontrivial additive character of $F$ given by $\psi(\alpha) = e(tr(\alpha)/p)$. Let $f$ be any complex valued function on $F$. The finite Fourier transform $FTf$ of $f$ is the complex valued function on $F$ given by

$$\text{(2.1)} \quad FTf(a) = \sum_{\alpha \in F} f(\alpha)\psi(a\alpha), \quad \text{for } a \in F.$$

The inversion formula

$$f(a) = \frac{1}{q} \sum_{\alpha \in F} FTf(\alpha)\psi(-\alpha a),$$

allows us to recover $f$ from $FTf$. In particular if $\chi = \chi_0$, the trivial multiplicative character on $F$ (with $\chi_0(0) := 0$), then

$$\text{(2.2)} \quad FT\chi_0(a) = \begin{cases} 
q - 1, & \text{if } a = 0; \\
-1, & \text{if } a \neq 0.
\end{cases}$$
If $\chi$ is a nontrivial multiplicative character on $F$ (with $\chi(0) := 0$), then $FT\chi$ is just a Gauss sum, and we have $|FT\chi| = \sqrt{q}\chi_0$, that is,

(2.3) \[ |FT\chi(a)| = \begin{cases} 0 & \text{if } a = 0; \\ \sqrt{q} & \text{if } a \neq 0. \end{cases} \]

In Lemma 2.2 below we observe that the autocorrelation condition (1.1) is equivalent to (2.3) and thus if the only Cohn functions with $f(1) = 1$ are nontrivial multiplicative characters then formula (2.3) becomes a characteristic property of a nontrivial multiplicative character. In order to prove this equivalence we need a few elementary properties of the finite Fourier transform. First we recall that if $f_1 \ast f_2$ is the convolution of two functions $f_1, f_2$ on $F$, defined by

$$f_1 \ast f_2(\alpha) = \sum_{\alpha_1 + \alpha_2 = \alpha} f_1(\alpha_1)f_2(\alpha_2),$$

then $FT(f_1 \ast f_2) = (FTf_1)(FTf_2)$. Let $f^*$ be the function defined by

$$f^*(\alpha) = \overline{f(-\alpha)}.$$

It is easy to verify that

(2.4) \[ FTf^* = \overline{FTf}. \]

In this context the autocorrelation condition (1.1) is just the statement that for any nonzero $a \in F$, $(f \ast f^*)(a) = -1$, that is, $f \ast f^* = FT\chi_0$ on $F^*$.

Lemma 2.1. If $f$ is a complex valued function on a finite field $F$, then

(2.5) \[ f \ast f^* = FT\chi_0, \]

if and only if

(2.6) \[ |FTf| = \sqrt{q}\chi_0. \]

Proof. If (2.5) is true, then by (2.4), we have

$$|FTf|^2 = FT(f \ast f^*) = FT(FT(\chi_0)) = q\chi_0,$$

and so (2.6) follows. Conversely, if (2.6) is true, then by (2.4) we have

$$FT(f \ast f^*) = |FTf|^2 = q\chi_0 = FT(FT\chi_0),$$

and thus (2.5) holds true. \[ \square \]

The following lemma is now immediate.

Lemma 2.2. If $f$ is a complex valued function on a finite field $F$ then $f$ is a Cohn function if and only if $|f| = \chi_0$ and $|FTf| = \sqrt{q}\chi_0$.

To prove Theorem 1, we shall make use of the multiplicative Fourier transform. Let $G$ be the group of multiplicative characters on $F$. For any function $f$ on $F$ the multiplicative Fourier transform of $f$, denoted $m(f)$, is a mapping from $G$ into $\mathbb{C}$ given by

(2.7) \[ m(f)(\chi) = \sum_{\alpha \in F} f(\alpha)\chi(\alpha). \]

The following inversion formula is easy to obtain, (see [2], p. 46): For any $\alpha \in F$,

(2.8) \[ f(\alpha) = \frac{1}{q-1} \sum_{\chi \in G} m(f)(\chi)\overline{\chi(\alpha)}. \]
3. Dedekind Determinant

Let $V$ denote the space of all $\mathbb{C}$-valued functions on the finite field $F$, a $q$-dimensional vector space over $\mathbb{C}$. The set of additive characters $\{\psi_a \mid a \in F\}$, where $\psi_a(\alpha) := \psi(aa)$, is a basis for $V$. Another basis is provided by the set $\{\delta_a \mid a \in F\}$ of characteristic functions defined by $\delta_a(\alpha) = 1$ if $\alpha = a$, and $\delta_a(\alpha) = 0$ if $\alpha \neq a$. For $a \in F$ let $T_a : V \to V$ be defined by

$$T_af(\alpha) = f(\alpha + a),$$

for $\alpha \in F$.

For a fixed $f \in V$, let $T_f : V \to V$ be the linear map defined by

$$(3.1) \quad T_f = \sum_{a \in F} f(a)T_a.$$

If $\psi_b$ is an additive character of $F$, it is easy to see that for any $\alpha \in F$,

$$T_f\psi_b(\alpha) = \sum_{a \in F} f(a)\psi_b(\alpha + a) = \psi_b(\alpha)FTf(b),$$

that is, $T_f\psi_b = FTf(b)\psi_b$. This means that $\psi_b$ is an eigenvector of $T_f$ with eigenvalue $FTf(b)$. Therefore, the diagonal matrix $\text{diag} \{FTf(b)\}_{b \in F}$ is the matrix for $T_f$ with respect to the basis $\{\psi_b \mid b \in F\}$. Next, we consider the action of $T_f$ on the basis $\{\delta_b \mid b \in F\}$. We note that for any $\alpha \in F$,

$$T_f\delta_b(\alpha) = \sum_{a \in F} f(a)T_a\delta_b(\alpha)$$

$$= \sum_{a \in F} f(a)\delta_b(\alpha + a)$$

$$= \sum_{a \in F} f(b - a)\delta_b(\alpha).$$

Thus, the matrix for $T_f$ with respect to the basis $\{\delta_b \mid b \in F\}$ is $[f(a-b)]_{a,b \in F}$, (indexing the rows by $a$, and the columns by $b$), and we obtain the following similarity relationship,

$$\text{diag} \{FTf(a)\}_{a \in F} \sim [f(a-b)]_{a,b \in F}.$$

Lemma 3.1. If $f$ is a function on $F$ with $\sum_{a \in F} f(\alpha) = 0$, then we have

$$(3.2) \quad \text{diag} \{FTf(a)\}_{a \in F^*} \sim [f(a-b) - f(a)]_{a,b \in F^*},$$

and consequently

$$(3.3) \quad \prod_{a \in F^*} FTf(a) = q \cdot \det[f(a-b)]_{a,b \in F^*}.$$

Proof. Let $V_1$ be the $(q - 1)$-dimensional subspace of $V$ consisting of all functions $g$ with $\sum_{a \in F} g(\alpha) = 0$, and let $f$ be a fixed element of $V_1$. It is easy to check that the function $T_f$ maps $V_1$ into $V_1$. Now, $\{\psi_b \mid b \in F^*\}$ is a basis for $V_1$ and the matrix for $T_f$ with respect to this basis is the diagonal matrix $\text{diag} \{FTf(b)\}_{b \in F^*}$. Another basis for $V_1$ can be obtained by shifting the characteristic functions $\delta_b$. For any $b \in F$ let $\eta_b := \delta_b - \frac{1}{q}$. It is easy to see that $\eta_b \in V_1$ for any $b \in F$ and that the set of all $\eta_b$, $b \in F$, spans $V_1$. Moreover, since $\eta_0 = -\sum_{b \in F^*} \eta_b$, it follows that
\{ \eta_b \mid b \in F^* \} \) is a basis for \( V_1 \). Now, since \( f \in V_1 \) it follows that \( T_f \) applied to any constant function is just zero. Thus for any nonzero \( b \),

\[
T_f(\eta_b) = T_f(\delta_b) = \sum_{a \in F} f(b - a)\delta_a = \sum_{a \in F} f(b - a)\eta_a = \sum_{a \in F^*} (f(b - a) - f(b))\eta_a,
\]

and so the matrix for \( T_f \) on \( \{ \eta_b \mid b \in F^* \} \) is \( [f(b - a) - f(a)]_{a,b \in F^*} \). The relationship in (3.2) is now immediate. The determinant of \( [f(b - a) - f(a)]_{a,b \in F^*} \) may be readily calculated by adding the columns of the matrix together. \( \square \)

We consider now the \( (q - 1) \)-dimensional subspace \( W \) of \( V \) defined by

\[
W := \{ f : f \in V \text{ such that } f(0) = 0 \}.
\]

The set of multiplicative characters, \( \{ \chi \} \), is a basis for \( W \). For any \( a \in F^* \) we let \( T_a : W \to W \) be defined by \( T_ag(\alpha) = g(a\alpha) \) for any \( g \in W \), \( \alpha \in F \). For a fixed \( f \in W \), let \( T_f : W \to W \) be the linear map defined by

\[
T_f = \sum_{a \in F} f(a)T_a.
\]

If \( \chi \) is a multiplicative character, it follows that

\[
T_f \chi = m(f)(\chi)\chi,
\]

where \( m(f) \) is the multiplicative Fourier transform given by (2.7). To see this, note that for any \( a \in F \), we have

\[
T_f \chi(\alpha) = \sum_{a \in F} f(a)T_a \chi(\alpha) = \sum_{a \in F} f(a)\chi(a)\chi(\alpha) = m(f)(\chi)\chi(\alpha).
\]

Thus, \( \chi \) is an eigenvector of the linear map \( T_f \) with eigenvalue \( m(f)(\chi) \) and so the matrix for \( T_f \) acting on the basis \( \{ \chi \} \) is the diagonal matrix \( \text{diag} \{ m(f)(\chi) \}_{\chi \in G} \). On the other hand, the matrix of \( T_f \) with respect to the basis \( \{ \delta_b \mid b \in F^* \} \) is \( [f(a^{-1}b)]_{a,b \in F^*} \). We obtain

**Lemma 3.2.** For any \( f \in W \), we have

\[
\text{diag} \{ m(f)(\chi) \}_{\chi \in G} \sim [f(a^{-1}b)]_{a,b \in F^*},
\]

and consequently,

\[
\sum_{\chi \in G} m(f)(\chi) = (q - 1)f(1),
\]

and

\[
\prod_{\chi \in G} m(f)(\chi) = \det [f(a^{-1}b)]_{a,b \in F^*}.
\]

The determinant in (3.8) is called a Dedekind determinant (see [3], p. 89).
4. Proof of Theorem 1

**Lemma 4.1.** If \( f \) is a Cohn function on a finite field \( F \) then the matrix \( [f(a-b)]_{a,b \in F^*} \) is nonsingular.

**Proof.** If \( f \) is a Cohn function on \( F \), then as we noted in the introduction, \( \sum_{\alpha \in F} f(\alpha) = 0 \). It follows from (3.3) that
\[
q \cdot \det [f(a-b)]_{a,b \in F^*} = \prod_{a \in F^*} FTf(a).
\]
But, by Lemma 2.2 we have
\[
|FTf(a)| = \sqrt{q} \quad \text{for} \quad a \neq 0.
\]
It follows that
\[
(4.1) \quad |\det [f(a-b)]_{a,b \in F^*}| = q^{\frac{q-1}{2}},
\]
and therefore the matrix is nonsingular. \( \square \)

Suppose now that \( f \) is a complex valued function with \( f(0) = 0 \), \( f(1) = 1 \) and \( |f(\alpha)| = 1 \) for all \( \alpha \neq 0 \), such that (1.2) holds for all \( a,b \in F^* \). Let
\[
(4.2) \quad A = [f(ab^{-1})]_{a,b \in F^*}, \quad \text{and} \quad B = [f(a-b)]_{a,b \in F^*}.
\]
We will show that \( \text{rank}(A) = 1 \). By Lemma 4.1, we know \( B \) is nonsingular, and so it is enough to show that \( \text{rank}(BA) = 1 \). Let \( BA = [g(a,b)]_{a,b \in F^*} \). In view of (1.2), we have
\[
g(a,b) = \sum_{\alpha \in F^*} f(b^{-1}\alpha)f(a-\alpha)
= \frac{1}{1-q} \sum_{\alpha \in F^*} f(-b^{-1}\alpha)f(\alpha),
\]
a value independent of \( a \). Thus \( \text{rank}(BA) = 1 \). Now by Lemma 3.2, we have
\[
(4.3) \quad \text{rank}(\text{diag } \{m(f)(\chi)\}_{\chi \in G}) = \text{rank}(A) = 1.
\]
Thus, since \( m(f)(\chi_0) = 0 \), there exists a nontrivial multiplicative character \( \rho \) such that
\[
(4.4) \quad m(f)(\chi) = 0 \quad \text{if} \quad \chi \neq \rho \quad \text{and} \quad m(f)(\rho) \neq 0.
\]
It follows from (2.8) that \( f \) is just a multiple of \( \bar{\rho} \). Since \( f \) and \( \bar{\rho} \) take on the same value at one we must have \( f = \bar{\rho} \), identically. This completes the proof of theorem 1.

5. Proof of Theorem 2

Let \( p \) be an odd prime. To prove Theorem 2, we work in the cyclotomic field \( Q(\xi) \), where \( \xi = e^{2\pi i/p} \). The following two lemmas are known.

**Lemma 5.1.** If \( u \) is an algebraic integer all of whose conjugates have absolute value 1, then \( u \) is a root of unity.

**Proof.** See [5], Lemma 11.6. \( \square \)

**Lemma 5.2.** The only roots of unity in \( Q(\xi) \) are \( \pm \xi^s \), with \( s \) a rational integer.

**Proof.** See [5], Lemma 11.4. \( \square \)
Let $f$ be a real valued function on the prime field $\mathbb{F}_p$ with $f(0) = 0$, $f(1) = 1$, $f(\alpha) = \pm 1$ for $\alpha \neq 0$, and such that for any nonzero $a \in F$,
$$\sum_{\alpha \in F} f(\alpha)f(\alpha + a) = -1.$$  
Then $f$ is a real Cohn function on $\mathbb{F}_p$. By Lemma 2.2 we have
\[(5.1) \quad FTf(0) = 0, \quad \text{and} \quad |FTf(\alpha)|^2 = p, \quad \text{for} \alpha \neq 0.\]
Let $\chi_2(\alpha)$ be the Legendre symbol of $\mathbb{F}_p$, namely $\chi_2(0) = 0$, $\chi_2(\alpha) = 1$ if $\alpha \in (\mathbb{F}_p^*)^2$, and $\chi_2(\alpha) = -1$ if $\alpha \notin (\mathbb{F}_p^*)^2$. For $\alpha \neq 0$, let
\[(5.2) \quad \eta(\alpha) = FTf(\alpha)/FT\chi_2(\alpha).\]
By (2.3) we know that $|FT\chi_2(\alpha)|^2 = p$, for $\alpha \neq 0$. Thus if $\alpha \neq 0$, it follows that $|\eta(\alpha)| = 1$. Also, since $f(\alpha) = \pm 1$ for $\alpha \neq 0$, it is easy to see that $\eta(\alpha) \in \mathbb{Q}(\xi)$. We claim that $\eta(\alpha)$ is in fact an algebraic integer in $\mathbb{Q}(\xi)$. To see this, let $<a>$ denote the principal ideal generated by an algebraic integer $a \in \mathbb{Z}[\xi]$. Then (see eg. [1] chapter 13, section 2),
$$<FTf(\alpha) > < FT\chi_2(\alpha)> = < FT\chi_2(\alpha)> = < p > = 1 - \xi >^{p-1},$$
and thus since $1 - \xi >$ is a prime ideal with $1 - \xi >^{p} = 1 - \xi >^{p-1}$. Therefore $\eta(\alpha) \in \mathbb{Z}[\xi].$

Next, we consider the conjugates of $\eta(\alpha)$. The Galois Group $G$ of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$ is the set of automorphisms $\sigma_n : n \in \mathbb{F}_p^*$ defined by $\sigma_n(\xi) = \xi^n$. For any $n \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$ we have $\sigma_n(\psi(b)) = \psi(nb)$ and thus for any $\alpha \in \mathbb{F}_p^*$,
\[(5.3) \quad \sigma_n(\eta(\alpha)) = \sigma_n(FTf(\alpha)/FT\chi_2(\alpha)) = \eta(n\alpha).\]
From the discussion above we see that all conjugates of $\eta(1)$ are algebraic integers of absolute value 1, and so by Lemmas 5.1 and 5.2 we have $\eta(1) = \pm \xi^s = \pm \psi(s)$ for some integer $s$. Then for any $\alpha \neq 0 \in \mathbb{F}_p$, it follows from (5.3) that
$$\eta(\alpha) = \sigma_n(\eta(1)) = \pm \xi^{s\alpha} = \pm \psi(s\alpha).$$
By the definition of $\eta(\alpha)$, (5.2), we have for any $\alpha \in \mathbb{F}_p^*$,
\[(5.4) \quad FTf(\alpha) = \pm \psi(s\alpha)FT\chi_2(\alpha) = \pm FTg(\alpha),\]
where $g$ is the translate of $\chi_2$ given by $g(x) := \chi_2(x - s)$. We note that both sides of (5.4) are zero when $\alpha = 0$. Thus we must have $f = \pm g$ identically on $\mathbb{F}_p$. Since $f(0) = 0$ and $f(1) = 1$ it follows that $f = \chi_2$ identically.

Acknowledgment. The authors are grateful to Professor Bahman Saffari for his valuable suggestions.

References
Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: cochrane@math.ksu.edu

E-mail address: drgarth@math.ksu.edu

Department of Mathematics, Zhongshan University, Guangzhou, P.R. China
E-mail address: addsr03@zsu.edu.cn