COUNTER-EXAMPLES TO A PROBLEM OF COHN ON CLASSIFYING CHARACTERS

KWOK-KWONG CHOI AND MAN-KEUNG SIU

ABSTRACT. Let p be a prime and F be a finite field with $q = p^s$ elements. It is well-known that for any nontrivial multiplicative character f of F,

$$\sum_{b\in F} f(b)\overline{f(b+a)} = \begin{cases} q-1 & \text{if } a = 0; \\ -1 & \text{if } a \neq 0. \end{cases}$$

H. Cohn asked whether the converse is true. For the case p is odd and $s = 1$, A. Biró gives a partial positive answer to Cohn's problem. In this note, we give a negative answer to Cohn's problem when $q > 4$ and $s > 1$.

Let p be a prime and $q = p^s$ be a power of p. Throughout this note, F will denote a finite field with q elements. F_p will denote the prime field with p elements. A function $f : F \longrightarrow \mathbb{C}$ is called a nontrivial multiplicative character of F if $f(0) = 0, f(1) = 1$ but $f \not\equiv 1$ on $F^* = F\backslash\{0\}$, and $f(b_1b_2) = f(b_1)f(b_2)\ \forall b_1, b_2 \in F$. In this case, it is well-known that

$$\sum_{b\in F} f(b)\overline{f(b+a)} = \begin{cases} q-1 & \text{if } a = 0; \\ -1 & \text{if } a \neq 0. \end{cases} \qquad (*)$$

H. Cohn asked whether the converse is true [7, p.202]:

> If $f : F \longrightarrow \mathbb{C}$ is such that $f(0) = 0, f(1) = 1, |f(a)| = 1\ \forall a \in F^*$, and $(*)$ holds, must f be a nontrivial multiplicative character of F?

For the case p is odd and $s = 1$, A. Biró gives some partial positive answers to Cohn's problem [2], among which are (1) there are only finitely many such f; (2) if furthermore $f(a) \in \{1, -1\}\ \forall a \in F^*$, then $f = \chi_2$, the Legendre symbol. The second result seems to be part of folklore that appears in different contexts [3, Corollary 1.2; 6, Corollary 2; 8, Result 1.2.9]. In this paper we give instead a NEGATIVE answer to Cohn's problem when $q > 4$ and $s > 1$. When $p = 2, s = 1$, there does not exist any f satisfying $(*)$, so the result is vacuously true. A direct computation of the case $p = 2$ and $s = 2$ shows that the answer to Cohn's problem is in the affirmative for $q = 4$. Therefore, the only unsettled case is when q is an odd prime p and f takes values other than $\{-1, 0, 1\}$.

Example 1. $F = F_3[X]/\langle X^2 - X - 1\rangle = F_3[\alpha] \cong F_9$ where $\alpha = [X]$. Define $f : F \longrightarrow \mathbb{C}$ by $f(0) = 0, f(1) = 1, f(\alpha) = \zeta, f(\alpha^2) = \zeta^7, f(\alpha^3) = \zeta^2, f(\alpha^4) = \zeta^4, f(\alpha^5) = \zeta^5, f(\alpha^6) = \zeta^3, f(\alpha^7) = \zeta^6$, where $\zeta = e^{2\pi i/8}$. Direct checking shows that f satisfies $(*)$. But f is NOT a multiplicative character, e.g. $f(\alpha)^2 = \zeta^2 \neq \zeta^7 = f(\alpha^2)$.

Date: March 13, 2012.

Example 2. F is the same as in Example 1. Define $f : F \longrightarrow \{0, 1, -1\}$ by $f(0) = 0, f(1) = 1, f(\alpha) = f(\alpha^4) = f(\alpha^5) = 1, f(\alpha^2) = f(\alpha^3) = f(\alpha^6) = f(\alpha^7) = -1$. Direct checking shows that f satisfies $(*)$. But f is NOT a multiplicative character, e.g. $f(\alpha)^2 = (1)^2 = 1 \neq -1 = f(\alpha^2)$.

Example 3. $F = F_2[X]/\langle X^4 + X^3 + 1\rangle = F_2[\alpha] \cong F_{16}$ where $\alpha = [X]$. Define $f : F \longrightarrow \mathbb{C}$ by $f(0) = 0, f(1) = 1, f(\alpha^5) = f(\alpha^{10}) = 1, f(\alpha^4) = f(\alpha^9) = f(\alpha^{14}) = \omega, f(\alpha^3) = f(\alpha^8) = f(\alpha^{13}) = \omega^2, f(\alpha) = f(\alpha^6) = f(\alpha^{11}) = \xi, f(\alpha^2) = f(\alpha^7) = f(\alpha^{12}) = -\xi$, where $\omega = e^{2\pi i/3}, \xi = e^{2\pi i/2000}$. Direct checking shows that f satisfies $(*)$. But f is NOT a multiplicative character, e.g. $f(\alpha^2) = -\xi \neq \xi^2 = f(\alpha)^2$.

Example 1, Example 2 and Example 3 are respectively specific instances of three classes of counter-examples to Cohn's problem. We will state each class as a theorem below (see Theorems 2, 3, 4).

For abbreviation we denote by $(**)$ the condition that $f : F \longrightarrow \mathbb{C}$ is such that $f(0) = 0, f(1) = 1, |f(a)| = 1\ \forall a \in F^*$ and $(*)$ holds. A counter-example to Cohn's problem is then a function $f : F \longrightarrow \mathbb{C}$ satisfying $(**)$ which is not a multiplicative character of F.

Lemma 1. *If $\varphi : F \longrightarrow F$ is an additive bijection with $\varphi(1) = 1$ (thence $\varphi|_{F_p}$ is the identity), then $f \circ \varphi$ satisfies $(**)$ whenever f satisfies $(**)$.*

Proof. Since φ is an additive bijection, we have

$$\sum_{b\in F}(f\circ\varphi)(b)\overline{(f\circ\varphi)(b+a)} = \sum_{b\in F} f(\varphi(b))\overline{f(\varphi(b)+\varphi(a))} = \sum_{b\in F} f(b)\overline{f(b+\varphi(a))}.$$

Hence $f \circ \varphi$ satisfies $(**)$ whenever f satisfies $(**)$. □

Let T be the set of all additive bijections $\varphi : F \longrightarrow F$ such that $\varphi(1) = 1$. There are totally $(p^s - 1)(p^s - p)\cdots(p^s - p^{s-1})$ bases for F, regarded as an s-dimensional vector space over F_p. Elements of T can be identified with those bases up to multiplication by an element of F^*. Hence

$$|T| = (p^s - p)(p^s - p^2)\cdots(p^s - p^{s-1}).$$

Theorem 2. *For every $q = p^s > 4$ and $s > 1$, there exists an additive bijection $\varphi : F \longrightarrow F$ in T which is not multiplicative. Hence there exists a function $f : F \longrightarrow \mathbb{C}$ satisfying $(**)$ which is not a multiplicative character of F.*

Proof. We shall give two proofs to the first assertion. The first proof allows us to construct φ explicitly but the second proof is simpler using a counting argument.

Let $F = F_p[X]/\langle P(X)\rangle$ and $F' = F_p[X]/\langle Q(X)\rangle$ where $P(X), Q(X)$ are DISTINCT irreducible polynomials of degree s over F_p. Write $F = F_p[\alpha], F' = F_p[\beta]$ where $\alpha = X$ modulo $P(X)$ and $\beta = X$ modulo $Q(X)$. Define $\varphi : F \longrightarrow F'$ by

$$\varphi(a_0 + a_1\alpha + \cdot + a_{s-1}\alpha^{s-1}) = a_0 + a_1\beta + \cdot + a_{s-1}\beta^{s-1}.$$

φ is an additive bijection which is not multiplicative. Indeed, let $P(X) = X^s - p(X)$ and $Q(X) = X^s - q(X)$ with $p(X), q(X)$ being distinct polynomials of degree at most $s - 1$ over F_p, then

$$\varphi(\alpha^s) = \varphi(p(\alpha)) = p(\beta) \neq \beta^s = \varphi(\alpha)^s.$$

Since F is isomorphic to F', we can regard φ as an additive bijection on F. Thus we are able to construct a non-multiplicative φ in T whenever there are at least

two distinct irreducible polynomials over F_p, which is guaranteed by the conditions $p^s > 4$ and $s > 1$.

The second proof is simpler but not constructive. It is well-known that there are $\phi(p^s - 1)$ multiplicative characters which are injective. It can also be shown that when $p^s > 4$ and $s > 1$, $|T| > \phi(p^s - 1)$. Hence there is at least some φ in T which is not multiplicative.

To prove the second assertion, we take a nontrivial multiplicative character $\chi : F \longrightarrow \mathbb{C}$ which is injective (e.g. let χ send a generator of the multiplicative group F^* to $e^{2\pi i/(q-1)}$) and define $f : F \longrightarrow \mathbb{C}$ by $f = \chi \circ \varphi$. From Lemma 1, f satisfies $(**)$ since χ satisfies $(**)$. Since φ is not multiplicative, there is $l > 1$ such that $\varphi(\alpha^l) \neq \varphi(\alpha)^l$. Thus

$$f(\alpha^l) = \chi(\varphi(\alpha^l)) \neq \chi(\varphi(\alpha)^l) = [\chi\varphi(\alpha)]^l = f(\alpha)^l,$$

so f is not a multiplicative character of F. □

Biró's second result shows that the answer to Cohn's problem is affirmative if we further assume $f(a) \in \{1, -1\}\ \forall a \in F_p^*$. The following theorem gives counter-examples for this case when p is an odd prime and $s > 1$.

Theorem 3. *Let p be an odd prime and $q = p^s$ with $s \geq 2$. There exists a function $f : F \longrightarrow \{0, 1, -1\}$ satisfying $(**)$ which is not a multiplicative character of F.*

Proof. Since p is odd, F has a unique quadratic character χ_2 with $\chi_2(a) = 0, 1$ or -1 according to a is 0, square or non-square in F. For any φ in T, by Lemma 1 $f = \chi_2 \circ \varphi$ satisfies $(**)$ since χ_2 satisfies $(**)$. If f is a multiplicative character, then $f = \chi_2$ by uniqueness. Hence, it suffices to find some φ in T such that $\chi_2 \circ \varphi \neq \chi_2$. To this end choose a non-square $\alpha \in F^* \backslash F_p^*$ and a square $\beta \in F^* \backslash F_p^*$, possible since q is odd and $s \geq 2$. For example, we can take α to be any generator of F^* and $\beta = \alpha^2$. Extend $\{1, \alpha\}$ and $\{1, \beta\}$ respectively to two bases for F over F_p. Define φ in T sending α to β. Then $\chi_2 \circ \varphi(\alpha) = \chi_2(\beta) = 1 \neq -1 = \chi_2(\alpha)$. □

Biró's first result shows that there are only finitely many functions $f : F_p \longrightarrow \mathbb{C}$ satisfying $(**)$. The following theorem gives infinitely many counter-examples to Cohn's problem when $q > 4$ is a square. This will also dash the hope for a relaxed positive answer to Cohn's problem which allows f to be the composite of a multiplicative character with some φ in T. Write $q = Q^2$ and express $F = E[X]/\langle X^2 - X - K\rangle$ where $X^2 - X - K$ is an irreducible polynomial over $E = \{0, k_1, \cdots, k_{Q-1}\}$, the finite field with Q elements (by choosing $K \in E$ such that K is not of the form $a^2 - a$ for some $a \in E$). Then $F = E[\alpha]$ where $\alpha = X$ modulo $X^2 - X - K$. Let $C = F^*/E^*$. We may choose the coset representatives in such a way that

$$C = \{[1], [\alpha], [\alpha + k_1], \cdots, [\alpha + k_{Q-1}]\}.$$

Theorem 4. *Let F be a finite field with $q = Q^2 > 4$. Let C be defined as above. Then any $f : C \longrightarrow \mathbb{C}$ for which $f(1) = 1, |f(c)| = 1\ \forall c \in C$ and $\sum_{c\in C} f(c) = 0$ extends to a function on F satisfying $(**)$. Hence there are uncountably many $f : F \longrightarrow \mathbb{C}$ satisfying $(**)$ which are not multiplicative characters.*

Proof. If $f : C \longrightarrow \mathbb{C}$ is a function such that $f(1) = 1, |f(c)| = 1\ \forall c \in C$ and $\sum_{c\in C} f(c) = 0$, we extend f to $f : F \longrightarrow \mathbb{C}$ by defining $f(0) = 0$ and $f(b) = f([c])$ whenever $b \in [c]$. By abuse of notation (for convenience) where we confuse $c \in C$

with $[c] \in C$ (actually $c \in F^*$), we may describe f as $f(0) = 0$ and $f(kc) = f(c)\ \forall k \in E^*$. All conditions in $(**)$ are easy to verify except $(*)$ for $a \neq 0$. Now,

$$\begin{aligned}\sum_{b\in F} f(b)\overline{f(b+a)} &= \sum_{b\in F^*} f(b)\overline{f(b+a)} \\ &= \sum_{c\in C}\sum_{k\in E^*} f(kc)\overline{f(kc+a)} \\ &= \sum_{c\in C} f(c) \sum_{k\in E^*} \overline{f(kc+a)}, \text{ since } f(kc) = f(c) \\ &= \sum_{c\in C} f(c) \sum_{k\in E} \overline{f(kc+a)},\end{aligned}$$

because $\sum_{c\in C} f(c) = 0$. Separate the sum into two parts, one part with only the term $f(c)\sum_{k\in E}\overline{f(kc+a)}$ with $a \in [c]$ and the other part with the remaining terms. The first part reduces to $f(a) \sum_{\substack{k\in E\\ kc+a\neq 0}} \overline{f(a)} = \sum_{\substack{k\in E\\ kc+a\neq 0}} 1 = Q-1$, since $kc+a \in [c]\ \forall k \in E$ except when $kc + a = 0$. The second part reduces to

$$\begin{aligned}&\sum_{\substack{c\in C\\ a\notin[c]}} f(c) \sum_{k\in E} \overline{f(kc+a)} \\ =\ &\sum_{\substack{c\in C\\ a\notin[c]}} f(c) \sum_{\substack{c'\in C\\ c'\neq c}} \overline{f(c')}, \text{ since } [kc+a] \text{ are all distinct and } [kc+a] \neq [c] \\ =\ &-\sum_{\substack{c\in C\\ a\notin[c]}} |f(c)|^2 \left(\text{because } \sum_{c\in C} f(c) = 0 \right) \\ =\ &-\sum_{\substack{c\in C\\ a\notin[c]}} 1 = -Q.\end{aligned}$$

Hence, $\sum_{b\in F} f(b)\overline{f(b+a)} = (Q-1) + (-Q) = -1$. To prove the last assertion, we note that there are uncountably many choices of $f([\alpha]), f([\alpha+k_1]), \cdots, f([\alpha+k_{Q-1}])$ on the unit circle in $\mathbb{C}$ when $Q \geq 3$ to make

$$\sum_{c\in C} f(c) = 1 + f([\alpha]) + f([\alpha+k_1]) + \cdots + f([\alpha+k_{Q-1}]) = 0$$

But there are only $\phi(q-1)$ multiplicative characters of F. □

The results so far explained originate from a theorem which deals with a special case. We gratefully acknowledge our debt to Andrew Granville for offering many helpful suggestions and for relentlessly but encouragingly spurring us on starting with that special case. This case (when $q = p^2$) with its complete characterization is stated and explained below.

Theorem 5. *F is the finite field with $q = p^2$ elements with prime field F_p and p is an odd prime. Let $f : F \longrightarrow \mathbb{Z}$ be a function with $f(0) = 0$ and $|f(a)| = 1\ \forall a \in F^*$. Then f satisfies $(*)$ if and only if the following conditions hold: (1) $\sum_{i=1}^{p+1} f(\alpha_i) = 0$; (2) $f(n\alpha_i) = f(\alpha_i)\ \forall n \in F_p^*$, where $[\alpha_1], \cdots, [\alpha_{p+1}]$ form a complete set of cosets of F^* by F_p^*.*

The part on sufficiency has already been done in the proof of Theorem 4 (put $Q = p$). It remains to prove the part on necessity.

We first transform $(*)$ into a condition on Tf, the finite Fourier transform of f, viz.

$$Tf(a) = \sum_{b \in F} f(b)\zeta^{-tr(ab)} \ \ \forall a \in F,\ \zeta = \exp(2\pi i/p).$$

(For more properties of Tf, see [4, Chapter 1].) For this part of the discussion, F can be a finite field with p^s elements with no restriction on s.
Standard computation shows that $(*)$ is equivalent to :

$$|Tf(a)|^2 = \begin{cases} 0 & \text{if } a = 0; \\ q & \text{if } a \neq 0. \end{cases}$$

Lemma 6. *Let $f : F \longrightarrow \mathbb{Z}$ be a function satisfying $(*)$ with $f(0) = 0$ and $|f(a)| = 1\ \forall a \in F^*$. When $q \equiv 1 \pmod 4$, $f(a) = f(-a)\ \forall a \in F^*$, so $Tf(a)$ is real $\forall a \in F^*$. When $q \equiv 3 \pmod 4$, $f(a) = -f(-a)\ \forall a \in F^*$, so $Tf(a)$ is purely imaginary $\forall a \in F^*$.*

Proof. Let $g(a) = f(a) + 1$ and $h(a) = \frac{g(a)}{2}$ for all a in F so that $h(a)$ is either 0 or 1 for all $a \in F^*$. Since f and g differ only by a constant, $Tg(a) = Tf(a)\ \forall a \in F^*$ and $Tg(0) = Tf(0) + q = q$. On the other hand, for any $a \in F^*$,

$$\begin{aligned} |Tg(a)|^2 &= \left|1 + 2\sum_{b \in F^*} h(b)\zeta^{-tr(ab)}\right|^2 \\ &= \left\{1 + 2\sum_{b \in F^*} h(b)\zeta^{-tr(ab)}\right\} \times \left\{1 + 2\sum_{b \in F^*} h(-b)\zeta^{-tr(ab)}\right\} \\ &= 1 + 2\sum_{b \in F^*} (h(b) + h(-b))\zeta^{-tr(ab)} + 4\sum_{b \in F} \theta_b \zeta^{-tr(ab)} \end{aligned}$$

where

$$\theta_b = \sum_{\substack{c_1, c_2 \in F^* \\ c_1 - c_2 = b}} h(c_1)h(c_2).$$

Hence from $(*)$, we get

$$q = 1 + 4\sum_{b \in F^*} h(b)^2 + \sum_{b \in F^*} (4\theta_b + 2h(b) + 2h(-b))\zeta^{-tr(ab)} \ \ \forall a \in F^*.$$

Since $h(b)$ is either 0 or 1, we have

$$\sum_{b \in F^*} h(b)^2 = \sum_{b \in F^*} h(b) = \frac{1}{2}\sum_{b \in F^*} f(b) + \frac{1}{2}(q-1) = \frac{1}{2}(q-1).$$

It follows that

$$q - 1 + \sum_{b \in F^*} (4\theta_b + 2h(b) + 2h(-b))\zeta^{-tr(ab)} = 0 \ \ \forall a \in F^*.$$

By the inversion formula of finite Fourier transform, we have

$$4\theta_b + 2h(b) + 2h(-b) = q - 1 \ \ \forall b \in F^*.$$

Thus

$$h(b) + h(-b) \equiv \frac{q-1}{2} \pmod 2 \ \ \forall b \in F^*.$$

This proves our lemma, since $h(b)$ is either 0 or 1. Finally, $\overline{Tf(a)} = Tf^t(a)$ where $f^t(a) = \overline{f(-a)}$, hence $Tf(a)$ is real or imaginary according as $f(-a) = f(a)\ \forall a \in F$ or $f(-a) = -f(a)\ \forall a \in F$. □

Hence,

$$Tf(a) = \begin{cases} \epsilon_a \sqrt{q} & \text{if } p \equiv 1 \pmod 4 \text{ or } p \equiv 3 \pmod 4, s \text{ is even;} \\ \\ \epsilon_a i\sqrt{q} & \text{if } p \equiv 3 \pmod 4, s \text{ is odd.} \end{cases}$$

Here $\epsilon_a \in \{1, -1\}$. It is known (see Theorems 5.12 and 5.15 of [5]) that $T\chi_2(1)$ is equal to $(-1)^{s-1}\sqrt{q}$ or $(-1)^{s-1}i^s\sqrt{q}$ according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $T\chi_2(na) = \chi_2(n)Tf(a)$. Thus it follows that $Tf(a) = \epsilon_a\delta(q)T\chi_2(1)$ where

$$\delta(q) = \begin{cases} (-1)^{s-1} & \text{if } p \equiv 1 \pmod 4; \\ (-1)^{s-1}i^{-s} & \text{if } p \equiv 3 \pmod 4 \text{ and } s \text{ is even;} \\ (-1)^{s-1}i^{-(s-1)} & \text{if } p \equiv 3 \pmod 4 \text{ and } s \text{ is odd.} \end{cases}$$

If we let σ_n $(1 \le n \le p-1)$ be the automorphism of $\mathbb{Q}(\zeta)$ which sends ζ to ζ^n, then $\sigma_n(Tf(a)) = Tf(na)$ and $\sigma_n(T\chi_2(a)) = T\chi_2(na)$. Hence

$$\begin{aligned} Tf(na) &= \sigma_n(Tf(a)) = \epsilon_a\delta(q)\sigma_n(T\chi_2(1)) = \epsilon_a\delta(q)T\chi_2(n) \\ &= \epsilon_a\delta(q)\chi_2(n)T\chi_2(1) = \chi_2(n)Tf(a) \end{aligned}$$

because $\delta(q)$ belongs to $\mathbb{Q}$ in all cases. Note that if α is any primitive element of F^*, then $\chi_2 \mid_{F_p^*} \equiv 1$ if and only if $\alpha^{\frac{p^s-1}{p-1}} \in F_p$ is a square, which is true if and only if s is even.

Lemma 7. *Let $f : F \longrightarrow \mathbb{Z}$ be a function satisfying $(*)$ with $f(0) = 0, f(1) = 1$ and $|f(a)| = 1\ \forall a \in F^*$. Then, $f(na) = \chi_2(n)f(a)\ \forall n \in F_p, \forall a \in F$.*

Proof. Since $Tf(na) = \chi_2(n)Tf(a)$, we have

$$\begin{aligned} 0 &= \sum_{b\in F} f(b)\zeta_p^{-tr(nab)} - \sum_{b\in F} \chi_2(n)f(b)\zeta_p^{-tr(ab)} \\ &= \sum_{b\in F} f(n^{-1}b)\zeta_p^{-tr(ab)} - \sum_{b\in F} \chi_2(n)f(b)\zeta_p^{-tr(ab)} \\ &= \sum_{b\in F} (f(n^{-1}b) - \chi_2(n)f(b))\zeta_p^{-tr(ab)} \end{aligned}$$

$\forall n \in F_p$ and $\forall a \in F$. Hence by the inversion formula of finite Fourier transform, we get

$$f(n^{-1}b) - \chi_2(n)f(b) = 0\ \ \forall n \in F_p^*, \forall b \in F$$

and so $f(nb) = \chi_2(n)f(b)$. □

We now come back to the case $q = p^2$, for which $\chi_2 \mid_{F_p^*} \equiv 1$. Conditions (1) and (2) of Theorem 5 follow from Lemma 7 and $Tf(0) = 0$. This completes the proof of Theorem 5.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1980.
[2] A. Biró, *Notes on a Problem of H. Cohn*, J. Number Theory, **22** (1999), No.2, 200-208.
[3] P. Borwein, K.K. Choi and S. Yazdani, *Extremal Property of Fekete Polynomials*, submitted for publication, 1999.
[4] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.
[5] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol 20, Addison-Wesley, Massachusetts, 1983.
[6] S.L. Ma, M.K. Siu and Z. Zheng, *On a problem of Cohn on Character Sums*, preprint, 1996.
[7] H.L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS No. 84, 1994.
[8] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics **1601**, Springer-Verlag, New York, 1995.

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong, SAR, CHINA

E-mail address: choi@maths.hku.hk

E-mail address: mks@maths.hku.hk