MATHEMATICS OF COMPUTATION
Volume 87, Number 313, September 2018, Pages 2461–2482
http://dx.doi.org/10.1090/mcom/3311
Article electronically published on January 2, 2018

CYCLOTOMIC DIFFERENCE SETS IN FINITE FIELDS

BINZHOU XIA

Abstract. The classical problem of whether mth-powers with or without zero in a finite field $\mathbb{F}_q$ form a difference set has been extensively studied, and is related to many topics, such as flag transitive finite projective planes. In this paper new necessary and sufficient conditions are established including those via a system of polynomial equations on Gauss sums. The author thereby solves the problem for even q which is neglected in the literature, and extends the nonexistence list for even m up to 22. Moreover, conjectures toward the complete classification are posed.

1. Introduction

A subset $D = \{a_1, \ldots, a_k\}$ in a group F of order v is said to be a (v, k, λ)-*difference set* or simply a *difference set* if for each nonidentity $a \in F$ there are exactly λ ordered pairs $(a_s, a_t) \in D \times D$ such that $a_s a_t^{-1} = a$. Given a (v, k, λ)-difference set, we obtain instantly by simple counting that

$$k(k-1) = \lambda(v-1). \tag{1.1}$$

It is straightforward to check that any subset of a group F with size 0, 1, $|F|-1$ or $|F|$ is a $(|F|, k, \lambda)$-difference set with $k - \lambda = 0$ or 1. Conversely, if $k - \lambda = 0$ or 1, then (1.1) implies $k = 0$, 1, $v-1$ or v. For a (v, k, λ)-difference set D, we call the nonnegative integer $n := k - \lambda$ the *order* of D, and say D is *trivial* if $n \leqslant 1$ and *nontrivial* if $n > 1$.

For comprehensive surveys on difference sets, the reader is referred to [7, 18 Part VI] and [16]. In this paper we focus on the case when F is the additive group of a finite field and the nonzero elements in D form a multiplicative subgroup of $F \setminus \{0\}$.

Notation 1.1. Let $q = mf + 1$ be a power of a prime number p with $m, f \in \mathbb{Z}_{>0}$. Denote the set of nonzero mth-powers in $\mathbb{F}_q$ by $H_{q,m}$ and $M_{q,m} := H_{q,m} \cup \{0\}$.

If $H_{q,m}$ is a (q, f, λ)-difference set in $\mathbb{F}_q^+$, then it is called an *mth-cyclotomic difference set* or *mth-power residue difference set*. If $M_{q,m}$ is a $(q, f+1, \lambda)$-difference set in $\mathbb{F}_q^+$, then it is called a *modified mth-cyclotomic difference set* or *modified mth-power residue difference set*. When not specifying the parameters, we will simply call them *cyclotomic difference set* or *modified cyclotomic difference set*, respectively. In view of (1.1), a necessary condition for the cyclotomic (q, f, λ)-difference set is

$$f - 1 = \lambda m, \tag{1.2}$$

Received by the editor September 26, 2015, and, in revised form, November 11, 2016, November 12, 2016, and April 14, 2017.

2010 *Mathematics Subject Classification.* 05B10, 05B25, 11T22, 11T24, 65H10.

Key words and phrases. Difference set, Gauss sum, Jacobi sum, finite projective plane, discrete Fourier transform.

This work was partially supported by NSFC grant (11501011).

while a necessary condition for the modified cyclotomic $(q, f+1, \lambda)$-difference set is

$$f + 1 = \lambda m. \tag{1.3}$$

Research on cyclotomic and modified cyclotomic difference sets dates back to Paley in the 1930s [19] when he used the quadratic residues in a finite field to construct Hadamard matrices. Essentially, he proved that $H_{q,2}$ is a $(q, f, (q-3)/4)$-difference set under the condition $q \equiv 3 \pmod 4$, which is no further restriction than (1.2). Based on this result, it is clear to see that $M_{q,2}$ is a $(q, f+1, (q+1)/4)$-difference set under the condition $q \equiv 3 \pmod 4$, which is no further restriction than (1.3). About ten years after Paley's construction, Chowla [5] discovered a family of nontrivial quartic cyclotomic difference sets in $\mathbb{F}_p$ by showing that $H_{p,4}$ is a difference set when $p = 1 + 4t^2$ for some odd integer t.

In 1953, Lehmer published a paper [17] investigating cyclotomic and modified cyclotomic difference sets in $\mathbb{F}_p$, where she established necessary and sufficient conditions for their existence via cyclotomic numbers and applied these to get fruitful results (see [3, Chapter 2] for an introduction to cyclotomic numbers). She proved that neither $H_{p,m}$ nor $M_{p,m}$ is a nontrivial difference set in $\mathbb{F}_p$ with odd m, and determined all the nontrivial mth-cyclotomic and modified mth-cyclotomic difference sets in $\mathbb{F}_p$ for $4 \leqslant m \leqslant 8$: they are

$$H_{p,4} \text{ with } p = 1 + 4t^2 \text{ for some odd integer } t, \tag{1.4}$$

$$H_{p,8} \text{ with } p = 1 + 8u^2 = 9 + 64v^2 \text{ for some integers } u \text{ and } v, \tag{1.5}$$

$$M_{p,4} \text{ with } p = 9 + 4t^2 \text{ for some odd integer } t, \tag{1.6}$$

$$M_{p,8} \text{ with } p = 49 + 8u^2 = 441 + 64v^2 \text{ for some integers } u \text{ and } v. \tag{1.7}$$

Note that the Pell equation $u^2 - 8v^2 = 1$ coming from (1.5) forces u and v to be odd in order that $1 + 8u^2$ is prime ([17, page 429]), while u is odd and v is even in (1.7) for a similar reason ([17, page 432]). On the other hand, it is not yet known whether there exist infinitely many primes p as in (1.5) or (1.7), although Lehmer noticed that they are quite rare by computation results.

Since Lehmer's significant paper, cyclotomic numbers have been the main tool for studying existence of cyclotomic and modified cyclotomic difference sets. The criterion in terms of cyclotomic numbers established by Lehmer originally in $\mathbb{F}_p$ extends to general finite fields $\mathbb{F}_q$ in the same form, and then it is shown that, if q is odd, the general finite field case does not give more examples than (1.4)–(1.7) for m odd or $4 \leqslant m \leqslant 8$ [14,20]. As for the case when $q = p$, more nonexistence results on mth-cyclotomic and modified cyclotomic difference sets have been proved. They are now known to be nonexistent for $m = 10$ [25], 12 [26], 14 [18], 16 [9], 18 [2] and 20 [11]. Although widely believed that for any larger even m neither $H_{p,m}$ nor $M_{p,m}$ forms a difference set, it has only been proved for some values of m under extra condition: $m \equiv 6 \pmod 8$ with $4 \in H_{p,m}$ [18], and $m = 24$ with $2 \in H_{p,3}$ or $3 \in H_{p,4}$ [10]. One of the difficulties for higher powers is to evaluate the cyclotomic numbers, and also the work is quite laborious when m grows.

In this paper, we alternate the approach by considering the relations that the corresponding Gauss sums must satisfy, which leads to overdetermined systems of polynomial equations. This enables us to determine mth-cyclotomic and modified cyclotomic difference sets in $\mathbb{F}_q$ up to $m = 22$ including even q, and gives insight for general m.

There are definite links between difference sets and other structures (see for example [1]). A remarkable one is that to finite projective planes, which we will illustrate in Subsection 5.3. Physical applications of difference sets can be found in the references listed in [4].

The layout of this paper is as follows. In Section 2 we will discuss preparing results on multiplicative characters and Gauss and Jacobi sums as well as discrete Fourier transform techniques which will be utilized in subsequent sections. In Section 3, we establish new necessary and sufficient conditions for the existence of cyclotomic and modified cyclotomic difference sets in finite fields via multiplicative characters, Jacobi sums and Gauss sums, respectively. Based on these, we obtain results on the existence problem of mth-cyclotomic and modified cyclotomic difference sets in Section 4. It is proved that the only existing one for odd m is the modified 3rd-cyclotomic difference set in $\mathbb{F}_{16}$ (see Theorem 4.1), while the existence for even m implies restrictions on the solutions of certain system of polynomial equations. In the final section, we discuss the computation results for these systems, which yield the determination of existence up to $m = 22$ (see Theorem 5.1) and suggest conjectures toward the complete classification.

2. Preliminaries

First of all, we set up some notation.

Notation 2.1. Let $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ be the unit cycle on the complex plane. Denote $\zeta_r = e^{2\pi i/r}$ for any $r \in \mathbb{Z}_{>0}$. For a field F, let $F^* = F \setminus \{0\}$ be the set of nonzero elements in F, which constitutes a group under multiplication of the field.

2.1. **Multiplicative characters.** Let χ be a character of the multiplicative group $\mathbb{F}_q^*$, i.e., a group homomorphism from $\mathbb{F}_q^*$ to $\mathbb{C}^*$. For any $s \in \mathbb{Z}$, the map χ^s from $\mathbb{F}_q^*$ to $\mathbb{C}^*$ defined by $\chi^s(\alpha) = (\chi(\alpha))^s$ for $\alpha \in \mathbb{F}_q^*$ is also a character of $\mathbb{F}_q^*$. Extend the domain of χ to $\mathbb{F}_q$ by setting

$$\chi(0) = \begin{cases} 1, & \text{if } \chi \text{ is trivial,} \\ 0, & \text{if } \chi \text{ is nontrivial,} \end{cases}$$

and call χ a *multiplicative character* on $\mathbb{F}_q$. For any $s \in \mathbb{Z}$, the character χ^s of $\mathbb{F}_q^*$ is also extended to a multiplicative character on $\mathbb{F}_q$, and by $\chi^s(\alpha)$ we mean the image of $\alpha \in \mathbb{F}_q$ under χ^s rather than $(\chi(\alpha))^s$. Note that the equality $\chi^s(\alpha) = (\chi(\alpha))^s$ may not hold after χ^s is extended to a multiplicative character on $\mathbb{F}_q$. For example, if χ is nontrivial and s is a positive integer such that χ^s is trivial, then $\chi^s(0) = 1 \neq 0 = (\chi(0))^s$.

Through this section, we will evaluate some multiplicative character sums, which turns out to play a central role in the subsequent section. For any nontrivial multiplicative character χ on $\mathbb{F}_q$, it is well known (see for example [3, Page 9]) that

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = 0 \tag{2.1}$$

Lemma 2.2. *Let χ be a multiplicative character of order m on $\mathbb{F}_q$ and $s \in \mathbb{Z}$. Then*

$$\sum_{\beta,\gamma \in H_{q,m}} \chi^s(\beta - \gamma) = f \sum_{\alpha \in H_{q,m}} \chi^s(1 - \alpha).$$

Proof.

$$\sum_{\beta,\gamma\in H_{q,m}}\chi^s(\beta-\gamma)=\sum_{\beta\in H_{q,m}}\sum_{\gamma\in H_{q,m}}\chi^s(1-\beta^{-1}\gamma)$$
$$=\sum_{\beta\in H_{q,m}}\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)=f\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha).\qquad\square$$

Notation 2.3. For any multiplicative character χ of order m on $\mathbb{F}_q$ and $\gamma\in\mathbb{F}_q^*$, let $A_{\chi,\gamma}=\{\alpha\in H_{q,m}\mid\chi(1-\alpha)=\chi(\gamma)\}$, $B_{q,m,\gamma}=\{(\alpha,\beta)\in H_{q,m}\times H_{q,m}\mid\alpha-\beta=\gamma\}$ and $C_{q,m,\gamma}=\{(\alpha,\beta)\in M_{q,m}\times M_{q,m}\mid\alpha-\beta=\gamma\}$.

The following lemma is apparent.

Lemma 2.4. *Let χ be a multiplicative character of order m on $\mathbb{F}_q$ and $\gamma\in\mathbb{F}_q^*$. Then the following statements hold.*

(a) $(\alpha,\beta)\mapsto\alpha^{-1}\beta$ *is a bijection from $B_{q,m,\gamma}$ to $A_{\chi,\gamma}$. In particular, $|A_{\chi,\gamma}|=|B_{q,m,\gamma}|$.*
(b) $|C_{q,m,\gamma}|=|B_{q,m,\gamma}|+|C_{q,m,\gamma}\cap(H_{q,m}\times\{0\})|+|C_{q,m,\gamma}\cap(\{0\}\times H_{q,m})|$.

We express the multiplicative character sum in the next lemma in terms of $|A_{\chi,\gamma}|$.

Lemma 2.5. *Let χ be a multiplicative character of order m on $\mathbb{F}_q$ and $\gamma\in\mathbb{F}_q^*$. Then*

$$\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)=m|A_{\chi,\gamma}|+1.$$

Proof. We have

$$\begin{aligned}&\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)\\&=\sum_{\alpha\in H_{q,m}}\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\chi^s(1-\alpha)\\&=\sum_{\alpha\in H_{q,m}\setminus\{1\}}\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\chi^s(1-\alpha)+\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\chi^s(0)\\&=\sum_{\substack{\alpha\in H_{q,m}\setminus\{1\}\\ \chi(1-\alpha)=\chi(\gamma)}}\sum_{s=0}^{m-1}1+\sum_{\substack{\alpha\in H_{q,m}\setminus\{1\}\\ \chi(1-\alpha)\neq\chi(\gamma)}}\sum_{s=0}^{m-1}\left(\frac{\chi(1-\alpha)}{\chi(\gamma)}\right)^s+\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\chi^s(0).\end{aligned}$$

For any $\alpha\in H_{q,m}\setminus\{1\}$ such that $\chi(1-\alpha)\neq\chi(\gamma)$,

$$\sum_{s=0}^{m-1}\left(\frac{\chi(1-\alpha)}{\chi(\gamma)}\right)^s=\frac{\left(\frac{\chi(1-\alpha)}{\chi(\gamma)}\right)^m-1}{\frac{\chi(1-\alpha)}{\chi(\gamma)}-1}=\frac{1-1}{\frac{\chi(1-\alpha)}{\chi(\gamma)}-1}=0.$$

Hence it follows that

$$\begin{aligned}\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha) &= \sum_{\substack{\alpha\in H_{q,m}\setminus\{1\}\\ \chi(1-\alpha)=\chi(\gamma)}}\sum_{s=0}^{m-1}+\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\chi^s(0)\\ &= \sum_{\substack{\alpha\in H_{q,m}\setminus\{1\}\\ \chi(1-\alpha)=\chi(\gamma)}} m+\chi^0(\gamma)\chi^0(0)\\ &= \sum_{\substack{\alpha\in H_{q,m}\\ \chi(1-\alpha)=\chi(\gamma)}} m+1 = m|A_{\chi,\gamma}|+1. \qquad \square\end{aligned}$$

2.2. **Gauss and Jacobi sums.** For a multiplicative character χ on $\mathbb{F}_q$, the *Gauss sum* $G_q(\chi)$ is defined by

$$G_q(\chi)=\sum_{\alpha\in\mathbb{F}_q}\chi(\alpha)\zeta_p^{\mathrm{tr}(\alpha)},$$

where tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. For multiplicative characters χ,ψ on $\mathbb{F}_q$, the *Jacobi sum* $J_q(\chi,\psi)$ is defined by

$$J_q(\chi,\psi)=\sum_{\alpha\in\mathbb{F}_q}\chi(\alpha)\psi(1-\alpha).$$

It is immediate from the definition that $J_q(\psi,\chi)=J_q(\chi,\psi)$.

We only list here some basic facts about Gauss and Jacobi sums which will be used in the sequel, and refer to [3, Chapters 1 and 2] for their proof and more properties of Gauss and Jacobi sums.

Proposition 2.6. *Let χ be a multiplicative character of order m on $\mathbb{F}_q$, and $s,t\in\mathbb{Z}$. Then the following statements hold.*

(a)
$$|G_q(\chi^s)|=\begin{cases}\sqrt{q}, & \text{if } s\not\equiv 0 \pmod m,\\ 0, & \text{if } s\equiv 0 \pmod m.\end{cases}$$

(b) *If $s\not\equiv 0 \pmod m$, then*
$$G_q(\chi^s)G_q(\chi^{-s})=\chi^s(-1)q.$$

(c) *If $s\not\equiv 0 \pmod m$ or $t\not\equiv 0 \pmod m$, then*
$$J_q(\chi^s,\chi^t)=\begin{cases}G_q(\chi^s)G_q(\chi^t)/G_q(\chi^{s+t}), & \text{if } s+t\not\equiv 0 \pmod m,\\ -\chi^s(-1), & \text{if } s+t\equiv 0 \pmod m.\end{cases}$$

(d) *If m is even and $s\not\equiv 0 \pmod m$, then*
$$\chi^s(4)J_q(\chi^s,\chi^s)=J_q(\chi^s,\chi^{m/2}).$$

The following lemma evaluates sums of Jacobi sums with one character fixed.

Lemma 2.7. *Let χ be a multiplicative character of order m on $\mathbb{F}_q$. If $s\not\equiv 0 \pmod m$, then*

$$\sum_{t=1}^{m-1}J_q(\chi^s,\chi^t)=1+m\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha).$$

Proof. Note that

$$\begin{aligned}\sum_{t=1}^{m-1} J_q(\chi^s,\chi^t) &= \sum_{t=1}^{m-1}\sum_{\beta\in\mathbb{F}_q}\chi^s(\beta)\chi^t(1-\beta)\\ &= \sum_{\beta\in\mathbb{F}_q}\chi^s(\beta)\sum_{t=1}^{m-1}\chi^t(1-\beta)\\ &= \sum_{1-\beta\in H_{q,m}}\chi^s(\beta)(m-1)+\sum_{1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(\beta)\sum_{t=1}^{m-1}\chi^t(1-\beta)\\ &= \sum_{1-\beta\in H_{q,m}}\chi^s(\beta)(m-1)+\sum_{1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(\beta)\sum_{t=0}^{m-1}\chi^t(1-\beta)\\ &\quad -\sum_{1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(\beta)\chi^0(1-\beta).\end{aligned}$$

For any $\beta\in\mathbb{F}_q$ such that $1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}$, as $\chi(1-\beta)\neq 1$, we have

$$\sum_{t=0}^{m-1}\chi^t(1-\beta)=\frac{(\chi(1-\beta))^m-1}{\chi(1-\beta)-1}=\frac{1-1}{\chi(1-\beta)-1}=0.$$

It follows that

$$\begin{aligned}\sum_{t=1}^{m-1} J_q(\chi^s,\chi^t) &= \sum_{1-\beta\in H_{q,m}}\chi^s(\beta)(m-1)-\sum_{1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(\beta)\chi^0(1-\beta)\\ &=(m-1)\sum_{1-\beta\in H_{q,m}}\chi^s(\beta)-\sum_{1-\beta\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(\beta)\\ &=(m-1)\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)-\sum_{\alpha\in\mathbb{F}_q^*\setminus H_{q,m}}\chi^s(1-\alpha)\\ &=m\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)-\sum_{\alpha\in\mathbb{F}_q^*}\chi^s(1-\alpha)\\ &=m\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)-\sum_{\alpha\in\mathbb{F}_q}\chi^s(1-\alpha)+\chi^s(1)\\ &=1+m\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha).\end{aligned}$$

□

2.3. **Discrete Fourier transform.** For a complex-valued function X on $\mathbb{Z}/r\mathbb{Z}$, the discrete Fourier transform (DFT) of X, denoted by $\hat{X}$, is the complex-valued function on $\mathbb{Z}/r\mathbb{Z}$ defined by

$$\hat{X}(s)=\sum_{t=0}^{r-1}\zeta_r^{-st}X(t),\quad s=0,\dots,r-1.$$

Here are two basic formulae for DFT, the convolution formula and the inverse formula, see for example [21, page 36] for a proof.

Proposition 2.8. *The following statements hold.*

(a) *If W, X and Y are complex-valued functions on $\mathbb{Z}/r\mathbb{Z}$ with*

$$W(s) = \sum_{t=0}^{r-1} X(t)Y(s-t), \quad s = 0, \dots, r-1,$$

then $\hat{W}(s) = \hat{X}(s)\hat{Y}(s)$ for all $s \in \mathbb{Z}/r\mathbb{Z}$.

(b) *If X is a complex-valued function on $\mathbb{Z}/r\mathbb{Z}$, then $X(s) = \hat{\hat{X}}(-s)/r$ for all $s \in \mathbb{Z}/r\mathbb{Z}$. In particular, DFT is an isomorphism on the complex vector space of complex-valued functions on $\mathbb{Z}/r\mathbb{Z}$.*

We note that since complex-valued functions on $\mathbb{Z}/r\mathbb{Z}$ are determined by their values on the r points $0, \dots, r-1$, Proposition 2.8 can be translated into the language of r-dimensional complex vectors. This will be more convenient to apply in cases.

3. Necessary and sufficient conditions

3.1. **Cyclotomic difference sets.** Before we give the existence criterions for cyclotomic difference sets, recall the necessary condition (1.2) for cyclotomic (q, f, λ)-difference sets.

Theorem 3.1. *Suppose $f - 1 = \lambda m$ and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $H_{q,m}$ is a (q, f, λ)-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{\alpha \in H_{q,m}} \chi^s(1-\alpha) = 0, \quad s = 1, \dots, m-1. \tag{3.1}$$

Proof. First suppose that $H_{q,m}$ is a (q, f, λ)-difference set. In view of (2.1) we then have for $s = 1, \dots, m-1$ that

$$\sum_{\beta,\gamma \in H_{q,m}} \chi^s(\beta - \gamma) = \sum_{\substack{\beta,\gamma \in H_{q,m} \\ \beta \neq \gamma}} \chi^s(\beta - \gamma) = \lambda \sum_{\alpha \in \mathbb{F}_q^*} \chi^s(\alpha) = 0.$$

This leads to (3.1) by Lemma 2.2.

Next suppose that (3.1) holds. Let γ be an arbitrary element in $\mathbb{F}_q^*$. Then

$$\sum_{s=0}^{m-1} \chi^{-s}(\gamma) \sum_{\alpha \in H_{q,m}} \chi^s(1-\alpha) = \sum_{\alpha \in H_{q,m}} \chi^0(1-\alpha) = f.$$

It follows that $|A_{\chi,\gamma}| = (f-1)/m = \lambda$ by Lemma 2.5, and so $|B_{q,m,\gamma}| = \lambda$ according to Lemma 2.4(a). By the definition of difference sets, this completes the proof. □

Combining Lemma 2.7 and Theorem 3.1 we obtain a necessary and sufficient condition of cyclotomic difference sets via Jacobi sums.

Theorem 3.2. *Suppose $f - 1 = \lambda m$, and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $H_{q,m}$ is a (q, f, λ)-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{t=1}^{m-1} J_q(\chi^s, \chi^t) = 1, \quad s = 1, \dots, m-1. \tag{3.2}$$

In light of Proposition 2.6(c), (3.2) can be rewritten by Gauss sums.

Theorem 3.3. *Suppose $f-1=\lambda m$, and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $H_{q,m}$ is a (q,f,λ)-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{\substack{t=1\\ t\neq s}}^{m-1}\chi^t(-1)G_q(\chi^t)G_q(\chi^{s-t})=(1+\chi^s(-1))G_q(\chi^s),\quad s=1,\dots,m-1. \tag{3.3}$$

Proof. Utilizing Proposition 2.6, we reformulate (3.2) to

$$\sum_{\substack{t=1\\ s+t\neq m}}^{m-1}\frac{G_q(\chi^s)G_q(\chi^t)}{G_q(\chi^{s+t})}-\chi^s(-1)=1,\quad s=1,\dots,m-1,$$

which is equivalent to

$$\sum_{\substack{t=1\\ t\neq m-s}}^{m-1}\frac{\chi^t(-1)G_q(\chi^t)G_q(\chi^{m-s-t})}{G_q(\chi^{m-s})}=1+\chi^s(-1),\quad s=1,\dots,m-1.$$

After multiplying both sides by $G_q(\chi^{m-s})$ and replacing s by $m-s$, this turns out to be (3.3). Hence the theorem follows by Theorem 3.2. □

3.2. **Modified cyclotomic difference sets.** Parallel with cyclotomic difference sets we can establish existence criterions for modified cyclotomic difference sets. Recall the necessary condition (1.3) for the modified cyclotomic $(q,f+1,\lambda)$-difference sets.

Theorem 3.4. *Suppose $f+1=\lambda m$, and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $M_{q,m}$ is a $(q,f+1,\lambda)$-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)=-1-\chi^s(-1),\quad s=1,\dots,m-1. \tag{3.4}$$

Proof. First suppose that $M_{q,m}$ is a $(q,f+1,\lambda)$-difference set. Then for $s=1,\dots,m-1$,

$$\sum_{\beta,\gamma\in M_{q,m}}\chi^s(\beta-\gamma)=\sum_{\substack{\beta,\gamma\in M_{q,m}\\ \beta\neq\gamma}}\chi^s(\beta-\gamma)=\lambda\sum_{\alpha\in\mathbb{F}_q^*}\chi^s(\alpha)=0.$$

On the other hand,

$$\begin{aligned}\sum_{\beta,\gamma\in M_{q,m}}\chi^s(\beta-\gamma)&=\sum_{\beta,\gamma\in H_{q,m}}\chi^s(\beta-\gamma)+\sum_{\beta\in H_{q,m}}\chi^s(\beta)+\sum_{\gamma\in H_{q,m}}\chi^s(-\gamma)\\&=\sum_{\beta,\gamma\in H_{q,m}}\chi^s(\beta-\gamma)+f+f\chi^s(-1).\end{aligned}$$

Hence

$$\sum_{\beta,\gamma\in H_{q,m}}\chi^s(\beta-\gamma)=-f(1+\chi^s(-1)),\quad s=1,\dots,m-1,$$

and thus we get (3.4) by virtue of Lemma 2.2.

Now suppose conversely that (3.4) holds. Let γ be an arbitrary element in $\mathbb{F}_q^*$. Then

$$\sum_{s=0}^{m-1}\chi^{-s}(\gamma)\sum_{\alpha\in H_{q,m}}\chi^s(1-\alpha)=f-\sum_{s=1}^{m-1}\chi^{-s}(\gamma)(1+\chi^s(-1)).$$

We thereby deduce from Lemmas 2.4 and 2.5 that

$$m|B_{q,m,\gamma}| + 1 = f - \sum_{s=1}^{m-1} \chi^{-s}(\gamma)(1 + \chi^s(-1)). \tag{3.5}$$

Recall that $C_{q,m,\gamma} = \{(\alpha, \beta) \in M_{q,m} \times M_{q,m} \mid \alpha - \beta = \gamma\}$. It suffices to show $|C_{q,m,\gamma}| = \lambda$ by the definition of difference set. Observe that $\chi(\gamma) \neq 1$ implies $|C_{q,m,\gamma} \cap (H_{q,m} \times \{0\})| = 0$ while $\chi(\gamma) \neq \chi(-1)$ implies $|C_{q,m,\gamma} \cap (\{0\} \times H_{q,m})| = 0$. The cases for $\chi(\gamma)$ are divided into the following four.

Case 1. $\chi(\gamma) \neq 1$ or $\chi(-1)$. In this case

$$\sum_{s=1}^{m-1} \chi^{-s}(\gamma)(1 + \chi^s(-1)) = -2,$$

whence (3.5) gives $|B_{q,m,\gamma}| = \lambda$. We then conclude $|C_{q,m,\gamma}| = |B_{q,m,\gamma}| = \lambda$ viewing Lemma 2.4(b).

Case 2. $\chi(\gamma) = 1 \neq \chi(-1)$. Then (3.5) gives $m|B_{q,m,\gamma}| + 1 = f - (m - 1 - 1)$, i.e., $|B_{q,m,\gamma}| = \lambda - 1$. Moreover,

$$C_{q,m,\gamma} \cap (H_{q,m} \times \{0\}) = \{(\gamma, 0)\}, \tag{3.6}$$

so $|C_{q,m,\gamma}| = |B_{q,m,\gamma}| + 1 = \lambda$ by Lemma 2.4(b).

Case 3. $\chi(\gamma) = \chi(-1) \neq 1$. In this case, (3.5) leads to $|B_{q,m,\gamma}| = \lambda - 1$, and it follows by Lemma 2.4(b) that $|C_{q,m,\gamma}| = |B_{q,m,\gamma}| + 1 = \lambda$ since

$$C_{q,m,\gamma} \cap (\{0\} \times H_{q,m}) = \{(0, -\gamma)\}. \tag{3.7}$$

Case 4. $\chi(\gamma) = 1 = \chi(-1)$. In this case, (3.5) leads to $|B_{q,m,\gamma}| = \lambda - 2$, and it follows by Lemma 2.4(b) that $|C_{q,m,\gamma}| = |B_{q,m,\gamma}| + 2 = \lambda$ since we have both (3.6) and (3.7).

□

Combination of Lemma 2.7 and Theorem 3.4 leads to a necessary and sufficient condition of modified cyclotomic difference sets via Jacobi sums.

Theorem 3.5. *Suppose $f + 1 = \lambda m$, and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $M_{q,m}$ is a $(q, f + 1, \lambda)$-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{t=1}^{m-1} J_q(\chi^s, \chi^t) = 1 - m - m\chi^s(-1), \quad s = 1, \ldots, m - 1. \tag{3.8}$$

Along the same lines as Theorem 3.3, we can reformulate (3.8) by Gauss sums as follows.

Theorem 3.6. *Suppose $f + 1 = \lambda m$, and let χ be a multiplicative character of order m on $\mathbb{F}_q$. Then $M_{q,m}$ is a $(q, f + 1, \lambda)$-difference set in $\mathbb{F}_q$ if and only if*

$$\sum_{\substack{t=1 \\ t \neq s}}^{m-1} \chi^t(-1) G_q(\chi^t) G_q(\chi^{s-t}) = (1-m)(1+\chi^s(-1)) G_q(\chi^s), \quad s = 1, \ldots, m-1. \tag{3.9}$$

4. Existence conditions via polynomial equations

4.1. **System on g-level.** We investigate the existence problem for cyclotomic and modified cyclotomic difference sets based on the criterions obtained in the previous section.

First we embark on the case when m is odd. It is already known in this case that neither $H_{q,m}$ nor $M_{q,m}$ form a nontrivial difference set in $\mathbb{F}_q$ if q is odd [20, Chapter 1, Part 1]. However, the parity argument for cyclotomic numbers used to prove this fact does not appeal to even q's. In Theorem 4.1 below, we deal with the case when m is odd in a uniform way for both even and odd q's. It turns out that the only existent one is $M_{16,3}$, which is not mentioned in the literature.

Theorem 4.1. *Suppose that m is odd. Then the following statements hold.*

(a) *$H_{q,m}$ is never a nontrivial difference set in $\mathbb{F}_q$.*
(b) *$M_{q,m}$ is a nontrivial difference set in $\mathbb{F}_q$ if and only if $(q,m)=(16,3)$.*

Proof. Suppose that $H_{q,m}$ or $M_{q,m}$ is a nontrivial difference set. As a consequence, both m and f are greater than 1. Let χ be a multiplicative character of order m on $\mathbb{F}_q$. Define a function g on $\mathbb{Z}/m\mathbb{Z}$ by

$$g(s)=G_q(\chi^s)/\sqrt{q},\quad s=1,\dots,m-1,$$

and

$$g(0)=\begin{cases}-1/\sqrt{q}, & \text{if } H_{q,m} \text{ is a nontrivial difference set,}\\ (m-1)/\sqrt{q}, & \text{if } M_{q,m} \text{ is a nontrivial difference set.}\end{cases}$$

Noticing $\chi(-1)=1$ as m is odd, we have

$$\sum_{t=0}^{m-1} g(t)g(s-t)=0,\quad s=1,\dots,m-1 \tag{4.1}$$

by Theorems 3.3 and 3.6, and

$$g(s)g(-s)=1,\quad s=1,\dots,m-1 \tag{4.2}$$

by Proposition 2.6(b). Define a complex-valued function W on $\mathbb{Z}/m\mathbb{Z}$ by

$$W(s)=\sum_{t=0}^{m-1} g(t)g(s-t),\quad s\in\mathbb{Z}.$$

It follows that $W(1)=\cdots=W(m-1)=0$ and

$$W(0)=g(0)^2+\sum_{t=1}^{m-1} g(t)g(-t)=g(0)^2+m-1.$$

Relying on Proposition 2.8 we have

$$\hat{g}(s)^2=\hat{W}(s)=\sum_{t=0}^{m-1}\zeta_m^{-st}W(t)=W(0)=g(0)^2+m-1,\quad s\in\mathbb{Z},$$

$$\sum_{r=0}^{m-1}\zeta_m^{sr}\hat{g}(r)\sum_{t=0}^{m-1}\zeta_m^{-st}\hat{g}(t)=\hat{\hat{g}}(-s)\hat{\hat{g}}(s)=m^2g(s)g(-s)=m^2,\quad s=1,\dots,m-1 \tag{4.3}$$

and

$$\sum_{s=0}^{m-1} \hat{g}(s) = \hat{\hat{g}}(0) = mg(0). \tag{4.4}$$

Therefore, $\hat{g}(s) = \varepsilon(s)\sqrt{g(0)^2 + m - 1}$ with $\varepsilon(s) = \pm 1$ for $s \in \mathbb{Z}$, and substituting this into (4.3) and (4.4) we get

$$\sum_{r=0}^{m-1} \zeta_m^{sr} \varepsilon(r) \sum_{t=0}^{m-1} \zeta_m^{-st} \varepsilon(t) = \frac{m^2}{g(0)^2 + m - 1}, \quad s = 1, \ldots, m-1 \tag{4.5}$$

and

$$\sum_{s=0}^{m-1} \varepsilon(s) = \frac{mg(0)}{\sqrt{g(0)^2 + m - 1}}. \tag{4.6}$$

Note that $\sum_{s=0}^{m-1} \varepsilon(s)$ is an odd integer as m is odd. We proceed according to the three cases below.

Case 1. $H_{q,m}$ is a nontrivial difference set. We deduce from (4.6) that

$$\left(\frac{mg(0)}{\sqrt{g(0)^2 + m - 1}} \right)^2 \geqslant 1,$$

i.e., $g(0)^2 \geqslant 1/(m+1)$. This yields $q \leqslant m + 1$, which violates the condition $f > 1$.

Case 2. $p > 2$ and $M_{q,m}$ is a nontrivial difference set. In this case,

$$\frac{m^2(m-1)}{m-1+q} = \left(\frac{mg(0)}{\sqrt{g(0)^2 + m - 1}} \right)^2$$

is an odd integer by (4.6). However, this is a contradiction as $m - 1$ is even and $m - 1 + q$ is odd.

Case 3. $p = 2$ and $M_{q,m}$ is a nontrivial difference set. Suppose $M_{q,m}$ is a $(q, f+1, \lambda)$-difference set. Then $q = mf + 1 = \lambda m^2 - m + 1$ by (1.3). In view of (4.5),

$$\frac{q}{\lambda(m-1)} = \frac{m^2}{g(0)^2 + m - 1}$$

is an algebraic integer, and thus an integer as it is rational. On the other hand, $(m-1)/\lambda = m^2(m-1)/(m-1+q)$ is an odd integer as shown in the previous case. We thereby conclude that $\lambda = m - 1$ is a power of 2, whence $q = \lambda m^2 - m + 1 = (m-1)^2(m+1)$. This implies that $m + 1$ is also a power of 2, so we have $m = 3$. Thus $\lambda = 2$ and $q = 16$.

Conversely, consider $\mathbb{F}_{16}$ as the splitting field of $x^4 + x + 1$ over $\mathbb{F}_2$. Let ω be a root of $x^4 + x + 1 = 0$ in $\mathbb{F}_{16}$ and χ be a multiplicative character on $\mathbb{F}_{16}$ such that $\chi(\omega) = \zeta_3$. It is easy to check that $1 - \omega^3 = \omega^{14}$, $1 - \omega^6 = \omega^{13}$, $1 - \omega^9 = \omega^7$ and $1 - \omega^{12} = \omega^{11}$. Now for $s = 1, 2$

$$\sum_{\alpha \in H_{16,3}} \chi^s(1 - \alpha) = \sum_{t=0}^{4} \chi^s(1 - \omega^{3t}) = \zeta_3^{2s} + \zeta_3^s + \zeta_3^s + \zeta_3^{2s} = -2.$$

Thus $M_{16,3}$ is a $(16, 6, 2)$-difference set by Theorem 3.4.

□

During the proof of Theorem 4.1, it is the relations of Gauss sums, with no need to evaluate them, from (3.3) and (3.9) as well as Proposition 2.6 that rule out the possibility of cyclotomic and modified cyclotomic difference sets. This suggests us to approach the case when m is even in the same vein, namely studying the relations that Gauss sums necessarily satisfy.

Theorem 4.2. *Suppose m is even. If $H_{q,m}$ or $M_{q,m}$ is a difference set in $\mathbb{F}_q$, then the system of equations*

$$\begin{cases} \sum_{t=0}^{2s}(-1)^t g_t g_{2s-t} + \sum_{t=2s+1}^{m-1}(-1)^t g_t g_{m+2s-t} = 0, \quad s = 1, \ldots, \frac{m}{2} - 1, \\ g_s g_{m-s} = (-1)^s, \quad s = 1, \ldots, \frac{m}{2}, \\ h^s g_s g_{\frac{m}{2}+s} = g_{2s} g_{\frac{m}{2}}, \quad s = 1, \ldots, \frac{m}{2} - 1, \\ h^{\frac{m}{2}} = 1 \end{cases} \tag{4.7}$$

in the unknowns $g_0, g_1, \ldots, g_{m-1}, h$ has a solution in $\mathbb{R} \times (\mathbb{S}^1)^m$ with $g_0 = -1/\sqrt{q}$ or $(m-1)/\sqrt{q}$, respectively.

Proof. Let χ be a multiplicative character of order m on $\mathbb{F}_q$,

$$g_s = G_q(\chi^s)/\sqrt{q}, \quad s = 1, \ldots, m-1,$$

$$g_0 = \begin{cases} -1/\sqrt{q}, & \text{if } H_{q,m} \text{ is a difference set,} \\ (m-1)/\sqrt{q}, & \text{if } M_{q,m} \text{ is a difference set,} \end{cases}$$

and $h = \chi(4)$. Since m is even, we derive from (1.2) and (1.3) that f is odd, and thus $\chi(-1) = -1$. It follows from Theorems 3.3 and 3.6 that

$$\sum_{t=0}^{s}(-1)^t g_t g_{s-t} + \sum_{t=s+1}^{m-1}(-1)^t g_t g_{m+s-t} = 0, \quad s = 1, \ldots, m-1.$$

In particular, taking even s gives the first line of (4.7). By Proposition 2.6 we have $|g_1| = \cdots = |g_{m-1}| = 1$,

$$g_s g_{m-s} = (-1)^s, \quad s = 1, \ldots, m-1$$

and

$$h^s \frac{g_s g_s}{g_{2s}} = \frac{g_s g_{\frac{m}{2}}}{g_{\frac{m}{2}+s}}, \quad s = 1, \ldots, \frac{m}{2} - 1. \tag{4.8}$$

Hence the second line of (4.7) holds, and (4.8) implies the third line of (4.7). Finally, $h = \chi^2(2)$ satisfies $h^{m/2} = 1$ and $|h| = 1$. This completes the proof. □

For an even m, we call (4.7) the *system of order m on g-level*. Note that if we count the subscript of g modulo m in the system of order m on g-level, then the first line of (4.7) can be written more concisely as

$$\sum_{t=0}^{m-1}(-1)^t g_t g_{2s-t} = 0, \quad s = 1, \ldots, \frac{m}{2} - 1.$$

Notation 4.3. Denote the affine variety consisting of solutions $(g_0, g_1, \ldots, g_{m-1}, h) \in \mathbb{C}^{m+1}$ to the system of order m on g-level by L_m.

Here are some observations on L_m.

Proposition 4.4. *Suppose that m is even.*

(a) *If $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$, then $(-g_0, -g_1, \ldots, -g_{m-1}, h) \in L_m$.*
(b) *If $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$, then for any integer r,*

$$(g_0, \zeta_m^r g_1, \ldots, \zeta_m^{(m-1)r} g_{m-1}, h) \in L_m.$$

(c) *If $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$, then for any integer r which is coprime to m, $(g_0, g_r, \ldots, g_{(m-1)r}, h)$ with subscripts modulo m lies in L_m.*
(d) *There exists $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$ such that $g_0 = m/2 - 1$; if $m+1$ is a prime power then there exists $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$ such that $g_0^2 = 1/(m+1)$. In particular, L_m is nonempty.*

Proof. Parts (a)–(c) are straightforward. We only need to prove (d). If $m \equiv 0 \pmod 4$, then take $g_0 = m/2 - 1$,

$$g_s = (-1)^{\frac{(s-1)(s-2)}{2}} \zeta_{\frac{m}{2}}^s, \quad s = 1, \ldots, m-1$$

and $h = -1$. If $m \equiv 2 \pmod 4$, then take $g_0 = (-1)^{(m+6)(m-6)/32}(m/2 - 1)$,

$$g_s = (-1)^{\frac{(4s+m+2)(4s+m-2)}{32}} \zeta_{2m}^s, \quad s = 1, \ldots, m-1$$

and $h = 1$. One verifies directly that $(g_0, g_1, \ldots, g_{m-1}, h)$ is a solution of (4.7) with $g_0 = \pm(m/2 - 1)$. Thus by part (a) we conclude that (4.7) has a solution with $g_0 = m/2 - 1$. Now suppose that $m+1$ is a prime power. Then $\{1\}$ is an mth-cyclotomic $(m+1, 1, 0)$-difference set in $\mathbb{F}_{m+1}$. By Theorem 4.2, (4.7) has a solution $(g_0, g_1, \ldots, g_{m-1}, h)$ with $g_0^2 = 1/(m+1)$. □

Theorem 4.5. *Suppose that m is even.*

(a) *If each $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m \cap (\mathbb{R}^* \times (\mathbb{S}^1)^m)$ satisfies $g_0^2 \geqslant 1/(m+1)$, then $H_{q,m}$ is not a nontrivial difference set in $\mathbb{F}_q$.*
(b) *If each $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m \cap (\mathbb{R}^* \times (\mathbb{S}^1)^m)$ satisfies either $g_0^2 \geqslant 1$ or $g_0^2 = 1/(m+1)$, then neither $H_{q,m}$ nor $M_{q,m}$ is a nontrivial difference set in $\mathbb{F}_q$.*

Proof. First we prove part (a). Suppose that $H_{q,m}$ is a nontrivial difference set in $\mathbb{F}_q$. Then as Theorem 4.2 asserts, (4.7) has a solution $(g_0, g_1, \ldots, g_{m-1}, h) \in \mathbb{R} \times (\mathbb{S}^1)^m$ such that $g_0 = -1/\sqrt{q}$. However, $g_0^2 \geqslant 1/(m+1)$, whence $q = m+1$. It follows that $f = 1$ and thus $H_{q,m}$ is a trivial difference set. This contradiction shows that (a) is true.

Now we turn to the proof for part (b). Under the assumption in (b), since we can deduce that $g_0^2 \geqslant 1/(m+1)$, $H_{q,m}$ is not a nontrivial difference set in $\mathbb{F}_q$. Suppose that $M_{q,m}$ is a nontrivial $(q, f+1, \lambda)$-difference set in $\mathbb{F}_q$. By Theorem 4.2, (4.7) has a solution $(g_0, g_1, \ldots, g_{m-1}, h) \in \mathbb{R} \times (\mathbb{S}^1)^m$ such that $g_0 = (m-1)/\sqrt{q}$. Viewing (1.3), we then have

$$g_0^2 = \frac{(m-1)^2}{q} = \frac{(m-1)^2}{mf+1} = \frac{(m-1)^2}{m(\lambda m - 1) + 1} = \frac{(m-1)^2}{\lambda m^2 - m + 1} < \frac{(m-1)^2}{m^2 - 2m + 1} = 1.$$

Hence the assumption in (b) forces $g_0^2 = 1/(m+1)$, i.e., $q = (m-1)^2(m+1)$. This implies that $m-1$ and $m+1$ are both powers of p. If $m > 2$, then $p = 2$ since $2 = (m+1) - (m-1)$ is divisible by p, but this results in a contradiction that m is odd as m divides $q - 1$. When $m = 2$, however, we get $q = 3$ and $|M_{q,m}| = 2$, contrary to the assumption that $M_{q,m}$ is a nontrivial difference set. Thus (b) holds. □

4.2. **System on $(\hat{g},\theta)$-level.** Assume that m is even for the rest of the section. In this subsection, we apply DFT to the system on g-level, which will lead to equivalent systems. Given an integer θ, we introduce the system of equations

$$\begin{cases} m^2\hat{g}_s\hat{g}_{\frac{m}{2}+s} = \left(\sum_{t=0}^{m-1}\hat{g}_t\right)^2 + m^2(m-1), \quad s=0,\dots,\frac{m}{2}-1,\\ m\sum_{t=0}^{m-1}\hat{g}_t\hat{g}_{s+t} = \left(\sum_{t=0}^{m-1}\hat{g}_t\right)^2 - m^2, \quad s=0,\dots,\frac{m}{2}-1,\\ \sum_{t=0}^{m-1}(-1)^t\hat{g}_t\hat{g}_{2s-2\theta-t} = \left(\hat{g}_s+\hat{g}_{\frac{m}{2}+s}\right)\sum_{t=0}^{m-1}(-1)^t\hat{g}_t, \quad s=0,\dots,\frac{m}{2}-1, \end{cases} \tag{4.9}$$

in the unknowns $\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1}$, where subscripts of $\hat{g}$'s are counted modulo m, and call it the *system of order m on $(\hat{g},\theta)$-level*.

Notation 4.6. For any $\theta\in\mathbb{Z}$, denote the affine variety consisting of solutions $(\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1})\in\mathbb{C}^m$ to the system of order m on $(\hat{g},\theta)$-level by $\hat{L}_{m,\theta}$.

The following proposition holds readily.

Proposition 4.7. *Let θ and θ' be integers.*

(a) *If $\theta'\equiv\theta \pmod{m/2}$, then $\hat{L}_{m,\theta'}=\hat{L}_{m,\theta}$.*
(b) *If $(\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1})\in\hat{L}_{m,\theta}$, then $(-\hat{g}_0,-\hat{g}_1,\dots,-\hat{g}_{m-1})\in\hat{L}_{m,\theta}$.*
(c) *If $(\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1})\in\hat{L}_{m,\theta}$ and r is an integer which is coprime to m, then $(\hat{g}_0,\hat{g}_r,\dots,\hat{g}_{(m-1)r})$ with subscripts modulo m lies in $\hat{L}_{m,r\theta}$.*

Theorem 4.8. *The map given by*

$$g_s = \frac{1}{m}\sum_{t=0}^{m-1}\zeta_m^{st}\hat{g}_t, \quad s=0,1,\dots,m-1 \tag{4.10}$$

and $h=\zeta_{m/2}^{\theta}$ is a bijection from $\bigcup_{\theta=0}^{m/2-1}\hat{L}_{m,\theta}$ to L_m.

Proof. First of all, we note that (4.10) gives a one-to-one correspondence between the points $(g_0,g_1,\dots,g_{m-1})$ and $(\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1})$ in $\mathbb{C}^m$.

Suppose $(g_0,g_1,\dots,g_{m-1},h)\in L_m$. Then $h=\zeta_{m/2}^{\theta}$ for some $\theta\in\{0,1,\dots,m/2-1\}$ since $h^{m/2}=1$, and (4.10) determines a point $(\hat{g}_0,\hat{g}_1,\dots,\hat{g}_{m-1})\in\mathbb{C}^m$. Define a function g on $\mathbb{Z}/m\mathbb{Z}$ by letting $g(s)=g_t$ whenever $s\equiv t \pmod{m}$, $t=0,\dots,m-1$. According to Proposition 2.8(b) and (4.10) we get that $\hat{g}(s)=\hat{g}_t$ whenever $s\equiv t \pmod{m}$, $t=0,\dots,m-1$. For each $s\in\mathbb{Z}$, let

$$W(s)=\sum_{t=0}^{m-1}(-1)^t g(t)g(s-t).$$

One readily sees that W is a function on $\mathbb{Z}/m\mathbb{Z}$, and $W(s)=0$ when s is odd. It then follows by (4.7) that $W(1)=\cdots=W(m-1)=0$ and

$$W(0)=g(0)^2+\sum_{t=1}^{m-1}(-1)^t g(t)g(-t)=g(0)^2+m-1.$$

In light of Proposition 2.8 we have

$$\hat{g}(s)\hat{g}\left(\frac{m}{2}+s\right)=\hat{W}(s)=\sum_{t=0}^{m-1}\zeta_m^{-st}W(t)=W(0)=g(0)^2+m-1, \quad s\in\mathbb{Z}$$

and

$$g(0) = \frac{1}{m}\hat{g}(0) = \frac{1}{m}\sum_{t=0}^{m-1}\hat{g}(t),$$

whence

$$m^2\hat{g}(s)\hat{g}\left(\frac{m}{2}+s\right) = \left(\sum_{t=0}^{m-1}\hat{g}(t)\right)^2 + m^2(m-1), \quad s \in \mathbb{Z}.$$

Moreover, direct calculation leads to

$$m\sum_{t=0}^{m-1}\hat{g}(t)\hat{g}(s+t) = m^2g(0)^2 - m^2 = \left(\sum_{t=0}^{m-1}\hat{g}(t)\right)^2 - m^2, \quad s \not\equiv \frac{m}{2} \pmod{m}$$

and

$$\sum_{t=0}^{m-1}(-1)^t\hat{g}(t)\hat{g}(2s-2\theta-t) = \left(\hat{g}(s)+\hat{g}\left(\frac{m}{2}+s\right)\right)\sum_{t=0}^{m-1}(-1)^t\hat{g}(t), \quad s \in \mathbb{Z}.$$

Hence $(\hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{m-1}) = (\hat{g}(0), \hat{g}(1), \ldots, \hat{g}(m-1))$ satisfies (4.9), i.e.,

$$(\hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{m-1}) \in \hat{L}_{m,\theta}.$$

Conversely, suppose $(\hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{m-1}) \in \hat{L}_{m,\theta}$ for some $\theta \in \{0, 1, \ldots, m/2-1\}$ and $(g_0, g_1, \ldots, g_{m-1}, h) \in \mathbb{C}^{m+1}$ is given by (4.10) and $h = \zeta_{m/2}^{\theta}$. We aim to show that $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$. The equation $h^{m/2} = 1$ is clearly satisfied. Since $\sum_{t=0}^{m-1}\hat{g}_t = mg_0$, one derives from (4.9) that

$$\begin{cases} \hat{g}_s\hat{g}_{\frac{m}{2}+s} = g_0^2 + m - 1, \quad s \in \mathbb{Z}, \\ \sum\limits_{t=0}^{m-1}\hat{g}_t\hat{g}_{s+t} = mg_0^2 - m, \quad s \not\equiv \frac{m}{2} \pmod{m}, \\ \sum\limits_{t=0}^{m-1}(-1)^t\hat{g}_t\hat{g}_{2s-2\theta-t} = \left(\hat{g}_s + \hat{g}_{\frac{m}{2}+s}\right)\sum\limits_{t=0}^{m-1}(-1)^t\hat{g}_t, \quad s \in \mathbb{Z}, \end{cases}$$

where subscripts of $\hat{g}$ are counted modulo m. If we also count the subscripts of g modulo m, then for $s = 1, \ldots, m/2-1$

$$\begin{aligned} \sum_{t=0}^{m-1}(-1)^t g_t g_{2s-t} =& \frac{1}{m^2}\sum_{t=0}^{m-1}(-1)^t\sum_{r=0}^{m-1}\zeta_m^{tr}\hat{g}_r\sum_{r=0}^{m-1}\zeta_m^{(2s-t)j}\hat{g}_j \\ =& \frac{1}{m^2}\sum_{r=0}^{m-1}\sum_{j=0}^{m-1}\zeta_m^{2sj}\hat{g}_r\hat{g}_j\sum_{t=0}^{m-1}\zeta_m^{(m/2+r-j)t} \\ =& \frac{1}{m}\sum_{r=0}^{m-1}\zeta_m^{2s(m/2+r)}\hat{g}_r\hat{g}_{\frac{m}{2}+r} \\ =& \frac{g_0^2+m-1}{m}\sum_{r=0}^{m-1}\zeta_m^{2sr} \\ =& 0. \end{aligned}$$

Thus the first line of (4.7) holds. For $s = 1, \ldots, m/2$,

$$\begin{aligned} g_s g_{m-s} =& \frac{1}{m^2} \sum_{r=0}^{m-1} \zeta_m^{sr} \hat{g}_r \sum_{t=0}^{m-1} \zeta_m^{(m-s)t} \hat{g}_t \\ =& \frac{1}{m^2} \sum_{r=0}^{m-1} \sum_{t=0}^{m-1} \zeta_m^{s(r-t)} \hat{g}_r \hat{g}_t \\ =& \frac{1}{m^2} \sum_{j=0}^{m-1} \zeta_m^{sj} \sum_{t=0}^{m-1} \hat{g}_{j+t} \hat{g}_t \\ =& \frac{mg_0^2 - m}{m^2} \sum_{\substack{j=0 \\ j \neq m/2}}^{m-1} \zeta_m^{sj} + \frac{(-1)^s}{m^2} \sum_{t=0}^{m-1} \hat{g}_t \hat{g}_{\frac{m}{2}+t} \\ =& -\frac{mg_0^2 - m}{m^2}(-1)^s + \frac{g_0^2 + m - 1}{m}(-1)^s \\ =& (-1)^s, \end{aligned}$$

which proves the second line of (4.7). Similarly, one can show that

$$h^s g_s g_{m+s} = \frac{1}{m^2} \sum_{r=0}^{m/2-1} \zeta_m^{2sr} \left(\hat{g}_r + \hat{g}_{\frac{m}{2}+r} \right) \sum_{t=0}^{m-1} (-1)^t \hat{g}_t = g_{2s} g_{\frac{m}{2}}$$

for $s = 1, \ldots, m/2 - 1$, and so the third line of (4.7) is satisfied. This completes our proof. □

Theorem 4.8 roughly says that the system of order m on g-level decomposes into $m/2$ systems on $(\hat{g}, \theta)$-level of the same order. This helps to reduce computation in the next section when m gets large. In fact, we avoid the high degree equation $h^{m/2} = 1$ in the the system of order m on g-level and instead solve $\tau(m/2)$ systems of order m on $(\hat{g}, \theta)$-level, where τ is the number-of-divisors function. To illustrate it in more detail, we need the following number-theoretic result.

Lemma 4.9. *Let θ be an integer. Then there exists a prime number $r > m$ such that $r\theta \equiv \gcd(\theta, m/2) \pmod{m/2}$.*

Proof. Let $\ell = m/2$, $d = \gcd(\theta, \ell)$, $\theta_0 = \theta/d$ and $\ell_0 = \ell/d$. Then $\gcd(\theta_0, \ell_0) = 1$, and so there exists an integer s such that $s\theta_0 \equiv 1 \pmod{\ell_0}$. As $\gcd(s, \ell_0) = 1$, by Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers congruent to s modulo ℓ_0. In particular, there is a prime number $r > m$ such that $r \equiv s \pmod{\ell_0}$. It follows that $r\theta_0 \equiv 1 \pmod{\ell_0}$. Consequently, $r\theta_0 d \equiv d \pmod{\ell_0 d}$, which turns out to be $r\theta \equiv d \pmod{\ell}$, as desired. □

Combining Lemma 4.9 with parts (a) and (c) of Proposition 4.7 we see that, among the systems of order m on $(\hat{g}, \theta)$-level for all integers θ, it suffices to solve for θ being the divisors of $m/2$. By computation in this $\tau(m/2)$ systems on $(\hat{g}, \theta)$-level, we get all the information for the system of order m on g-level via Theorem 4.8. This is carried out in the next section up to $m = 22$.

5. Computation results and conjectures

5.1. **Results for $m \leqslant 22$.** One of the main tools for solving systems of polynomial equations is the *Gröbner basis* computation. Generally speaking, a Gröbner basis

is a particular kind of generating set of an ideal in a polynomial ring. (The reader is referred to [8] for the explicit definition and an introduction to this topic.) Once a Gröbner basis is computed, it is easy to know many important properties of the ideal and the associated algebraic variety, such as the dimension [8, §3 Chapter 9].

Here we apply a state-of-the-art algorithm of Faugère [12] called *F4* to compute Gröbner bases of the systems of order m on $(\hat{g}, \theta)$-level with $m = 6$, 10, 12, 14, 16, 18, 20 and 22 performed in MAPLE 14. For each m, we only compute for θ being a divisor of $m/2$ (when $\theta = m/2$ it is equivalent to put $\theta = 0$). It turns out that in these computed cases, $\hat{L}_{m,\theta}$ is a finite set, and thus each $(\hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{m-1})$ satisfies

$$F_{m,\theta}\left(\frac{1}{m}\sum_{t=0}^{m-1}\hat{g}_t\right) = 0$$

for some univariate polynomial[1] $F_{m,\theta}(x)$ listed in Tables 5.1–8 ($F_{m,\theta}(x) = 1$ indicates that $\hat{L}_{m,\theta}$ is empty). Now for $m = 6$, 10, 12, 14, 16, 18, 20 and 22, Theorem 4.8 in conjunction with Lemma 4.9 and parts (a) and (c) of Proposition 4.7 implies that each $(g_0, g_1, \ldots, g_{m-1}, h)$ satisfies $F_m(g_0) = 0$, where

$$F_m(x) = \prod_{\theta \mid n} F_{m,\theta}(x).$$

We list $F_m(x)$ for these values of m in Table 9[2].

TABLE 1. $F_{6,\theta}(x)$

θ	0	1
$F_{6,\theta}(x)$	$(x-2)(x+2)$	$7x^2-1$

TABLE 2. $F_{10,\theta}(x)$

θ	0	1
$F_{10,\theta}(x)$	$x(x-4)(x+4)$	$11x^2-1$

TABLE 3. $F_{12,\theta}(x)$

θ	0	1	2	3
$F_{12,\theta}(x)$	1	$13x^2-1$	1	$(x-3)(x+3)(x-5)(x+5)(5x-7)(5x+7)$

TABLE 4. $F_{14,\theta}(x)$

θ	0	1
$F_{14,\theta}(x)$	$(x-6)(x+6)(4x^2+3)$	1

[1]One can find them by the command **Groebner[UnivariatePolynomial]** in MAPLE 14.

[2]To find $F_m(x)$, one may also compute directly in the system of order m on g-level. However, the author's PC failed to compute a Gröbner basis for the system on g-level when $m = 22$ as it is too memory-consuming.

TABLE 5. $F_{16,\theta}(x)$

θ	0	1	2	4
$F_{16,\theta}(x)$	$(7x-17)(7x+17)$	1	$17x^2-1$	$(x-7)(x+7)$

TABLE 6. $F_{18,\theta}(x)$

θ	0	1	3
$F_{18,\theta}(x)$	$x(x-8)(x+8)$	$19x^2-1$	1

TABLE 7. $F_{20,\theta}(x)$

θ	0	1	2	5
$F_{20,\theta}(x)$	1	1	1	$(x-7)(x+7)(x-9)(x+9)(9x-31)$ $\cdot(9x+31)(13x-67)(13x+67)$

TABLE 8. $F_{22,\theta}(x)$

θ	0	1
$F_{22,\theta}(x)$	$(x-10)(x+10)(4x^4-60x^2+243)$	$23x^2-1$

TABLE 9. $F_m(x)$

m	$F_m(x)$
6	$(x-2)(x+2)(7x^2-1)$
10	$x(x-4)(x+4)(11x^2-1)$
12	$(x-3)(x+3)(x-5)(x+5)(5x-7)(5x+7)(13x^2-1)$
14	$(x-6)(x+6)(4x^2+3)$
16	$(x-7)(x+7)(7x-17)(7x+17)(17x^2-1)$
18	$x(x-8)(x+8)(19x^2-1)$
20	$(x-7)(x+7)(x-9)(x+9)(9x-31)(9x+31)(13x-67)(13x+67)$
22	$(x-10)(x+10)(4x^4-60x^2+243)(23x^2-1)$

Due to the these computation results we have the following theorem.

Theorem 5.1. *If $m \leqslant 22$ is an even integer other than 2, 4 or 8, then neither $H_{q,m}$ nor $M_{q,m}$ forms a nontrivial difference set in $\mathbb{F}_q$.*

Proof. Let $(g_0, g_1, \ldots, g_{m-1}, h)$ be any point in $L_m \cap (\mathbb{R}^* \times \mathbb{C}^m)$. Then $F_m(g_0) = 0$ with $F_m(x)$ lying in Table 9. Note that $4x^4 - 60x^2 + 243 = 0$ has no solution in $\mathbb{R}$. We infer from Table 9 that either $g_0^2 \geqslant 1$ or $g_0^2 = 1/(m+1)$. Accordingly, neither $H_{q,m}$ nor $M_{q,m}$ forms a nontrivial difference set in $\mathbb{F}_q$ by Theorem 4.5(b). □

5.2. **Conjectural classification.** Let us summarize what has been known so far about the existence of nontrivial mth-cyclotomic and modified cyclotomic difference sets in $\mathbb{F}_q$. First, the case when m is odd is dealt with in Theorem 4.1: only $M_{16,3}$ arises as a difference set. Second, for even values of m up to 8, all the nontrivial mth-cyclotomic and modified cyclotomic difference sets in $\mathbb{F}_q$ have been determined due to Paley [19], Hall [14] and Storer [20]: they are the quadratic case with $q \equiv 3 \pmod 4$ and quartic and octic case with $q = p$ as in (1.4)–(1.7). For even values of m from 10 to 22, $H_{q,m}$ and $M_{q,m}$ do not form nontrivial difference sets any more as shown in Theorem 5.1. Now we pose a conjectural classification.

Conjecture 5.2. $H_{q,m}$ is a nontrivial difference set in $\mathbb{F}_q$ if and only if one of the following appears:

(a) $m = 2$ and $q \equiv 3 \pmod 4$;
(b) $m = 4$ and $q = p = 1 + 4t^2$ for some odd integer t;
(c) $m = 8$ and $q = p = 1 + 8u^2 = 9 + 64v^2$ for some odd integers u and v.

$M_{q,m}$ is a nontrivial difference set in $\mathbb{F}_q$ if and only if one of the following appears:

(a') $m = 2$ and $q \equiv 3 \pmod 4$;
(b') $m = 3$ and $q = 16$;
(c') $m = 4$ and $q = p = 9 + 4t^2$ for some odd integer t;
(d') $m = 8$ and $q = p = 49 + 8u^2 = 441 + 64v^2$ for some odd integer u and even integer v.

We have seen that Conjecture 5.2 is true for odd m and even $m \leqslant 22$. In fact, our verification for even values of m up to 22 other than 2, 4 or 8 builds on the computation results that the assumptions of both (a) and (b) in Theorem 4.5 hold for these m's. Viewing this, we address the following conjecture, whose latter part obviously implies the former.

Conjecture 5.3. Suppose that m is even and $m \neq 2$, 4 or 8.

(a) Each $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m \cap (\mathbb{R}^* \times (\mathbb{S}^1)^m)$ satisfies $g_0^2 \geqslant 1/(m+1)$.
(b) Each $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m \cap (\mathbb{R}^* \times (\mathbb{S}^1)^m)$ satisfies either $g_0^2 \geqslant 1$ or $g_0^2 = 1/(m+1)$.

By the benefit of Theorem 4.5, it provides a possible way to tackle Conjecture 5.2 for higher powers by verifying Conjecture 5.3 for larger m: if Conjecture 5.3(b) is true, then Conjecture 5.2 is true; if part (a) of Conjecture 5.3 is true then at least the statement about $H_{q,m}$ in Conjecture 5.2 holds. From the author's viewpoint, it is quite possible that, like the computation results in the previous subsection, each $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$ satisfies the inequalities in Conjecture 5.3. In other words, it would probably suffice to compute the Gröbner basis for (4.7) or (4.9) for even $m \geqslant 24$.

5.3. **Flag-transitive projective planes.** A *finite projective plane* of order n, where $n \in \mathbb{Z}_{>1}$, is a point-line incidence structure satisfying:

(i) each line contains exactly $n+1$ points and each point is contained in exactly $n+1$ lines;
(ii) any two distinct lines intersect in exactly one point and any two distinct points are contained in exactly one line.

The incident point-line pairs are called *flags*. A permutation on the point set preserving the lines and flags is called a *collineation* or *automorphism*. If the collineation group of a finite projective plane acts 2-transitively on the points, then it is said to be 2-*transitive*. If the collineation group of a finite projective plane acts transitively on the flags, then it is said to be *flag-transitive*. Note that 2-transitive finite projective planes are always flag-transitive because two distinct points determine a line.

From the definition of difference sets one sees that each $(v, k, 1)$-difference set D in an abelian group F gives rise to a finite projective plane once we call elements of F points and $\{D + a \mid a \in F\}$ lines. For such consideration, $(v, k, 1)$-difference sets are also called *planar difference sets*. A finite projective plane coordinatized by a finite

field is said to be *Desarguesian* since Moufang revealed its equivalence to a certain configurational property named in honor of G. Desargues (see for example [15]). An elegant and celebrated theorem of Wagner [24] asserts that every finite 2-transitive projective plane is Desarguesian, which actually classifies the 2-transitive projective planes. Toward a generalization of Wagner's theorem, a conjecture was made that every finite flag-transitive projective plane is Desarguesian. This conjecture has received attention of wide scope and is still open as it is attributed to the existence problem of related planar difference sets by Proposition 5.4 below. For more about the history of this longstanding conjecture including Proposition 5.4; see [22, 23].

Proposition 5.4. *If there exists a finite non-Desarguesian flag-transitive projective plane of order m with v points, then $v = m^2 + m + 1$ is prime and $H_{v,m}$ is a $(v, m+1, 1)$-difference set in $\mathbb{F}_v$ with $m > 8$.*

An important concept in the theory of difference sets is the so-called *multiplier*. Its idea stems from Hall [13] when investigating the special case of planar difference sets in cyclic groups, and has been generalized to difference sets in an arbitrary group with a lot of outcomes (see the survey [16] for example). Nevertheless, we will focus on the abelian group case for our purposes, where a (*numerical*) *multiplier* of a difference set D in an abelian group F is defined to be an integer t with $\gcd(t, |F|) = 1$ such that $tD = D + a$ for some $a \in F$. The following result is due to Chowla and Ryser [6].

Proposition 5.5. *Let D be a (v, k, λ)-difference set in an abelian group. If t is a prime divisor of $k - \lambda$ with $\gcd(t, v) = 1$ and $t > \lambda$, then t is a multiplier of D.*

In [17, Theorem IV], Lehmer proved that the set of multipliers of a nontrivial cyclotomic difference set in $\mathbb{F}_p$ is the difference set itself. We note that this result can be extended to $\mathbb{F}_q$ along the the same lines of proof. Now suppose that m is even and $H_{q,m}$ is a planar difference set. It follows that f is odd by (1.2), and thus the order $f - 1$ is even. As Proposition 5.5 implies that 2 is a multiplier of $H_{q,m}$, we then have $2 \in H_{q,m}$, and so $\chi(4) = 1$ for any multiplicative character χ of order m on $\mathbb{F}_q$. This allows us to add the equation $h = 1$ to (4.7) in order that $H_{q,m}$ is a planar difference set in $\mathbb{F}_q$. Hence the following theorem holds as a consequence of (1.2) and Proposition 5.4.

Theorem 5.6. *If $H_{q,m}$ is a planar difference set in $\mathbb{F}_q$, then $q = m^2 + m + 1$ with m even and the system of order m on g-level has a solution $(g_0, g_1, \ldots, g_{m-1}, h)$ in $\mathbb{R} \times (\mathbb{S}^1)^m$ with $g_0 = -1/\sqrt{q}$ and $h = 1$. In particular, if there does not exist an even integer $m > 8$ such that $v = m^2 + m + 1$ is prime and the system of order m on g-level has a solution $(g_0, g_1, \ldots, g_{m-1}, h)$ in $\mathbb{R} \times (\mathbb{S}^1)^m$ with $g_0 = -1/\sqrt{v}$ and $h = 1$, then every finite flag-transitive projective plane is Desarguesian.*

5.4. **Other problems on the systems of equations.** Computation results shows that L_m is a finite set when $m \leqslant 22$ is even and $m \neq 2$, 4 or 8. We thus make another conjecture below. Its affirmative solution for each fixed m will result in a conclusion by Theorem 4.2 that there exist at most finitely many q's such that $q \equiv 1 \pmod{m}$ and either $H_{q,m}$ or $M_{q,m}$ is a difference set in $\mathbb{F}_q$ for this m.

Conjecture 5.7. L_m is a finite set for $m \geqslant 24$ even.

Studying whether there exists $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m$ with $g_0 = 0$ is of interest and importance as well. One of the reasons is that it also has connection with finiteness results by the next theorem.

Theorem 5.8. *Suppose that m is even. If $L_m \cap (\{0\} \times (\mathbb{S}^1)^m)$ is empty, then there exist at most finitely many q's such that $q \equiv 1 \pmod{m}$ and either $H_{q,m}$ or $M_{q,m}$ is a difference set in $\mathbb{F}_q$.*

Proof. Let Q be the set of prime powers q such that $q \equiv 1 \pmod{m}$ and $H_{q,m}$ is a difference set in $\mathbb{F}_q$. For each $q \in Q$, there exists a $(g_0(q), g_1(q), \ldots, g_{m-1}(q), h(q)) \in L_m \cap (\mathbb{R} \times (\mathbb{S}^1)^m)$ such that $g_0(q) = -1/\sqrt{q}$ by Theorem 4.2. Suppose Q to be infinite. Then there exists an infinite increasing sequence $(q_n)_{n=1}^{\infty}$ in Q. As $(\mathbb{S}^1)^m$ is bounded and closed, it is compact by the Heine-Borel theorem. Hence the sequence $((g_1(q_n), \ldots, g_{m-1}(q_n), h(q_n)))_{n=1}^{\infty}$ in $(\mathbb{S}^1)^m$ has a subsequence

$$((g_1(q_{n_k}), \ldots, g_{m-1}(q_{n_k}), h(q_{n_k})))_{k=1}^{\infty}$$

which has a limit point, say $(g_1, \ldots, g_{m-1}, h) \in (\mathbb{S}^1)^m$. Since

$$g_0 = \lim_{k\to\infty} g_0(q_{n_k}) = \lim_{k\to\infty} -\frac{1}{\sqrt{q_{n_k}}} = 0$$

and $(g_0(q_{n_k}), g_1(q_{n_k}), \ldots, g_{m-1}(q_{n_k}), h(q_{n_k}))$ satisfies (4.7) for every integer $k \geqslant 1$, taking the limit $k \to \infty$ in each polynomial equation of (4.7) we deduce that $(g_0, g_1, \ldots, g_{m-1}, h)$ satisfies (4.7). This shows that $(g_0, g_1, \ldots, g_{m-1}, h) \in L_m \cap (\{0\} \times (\mathbb{S}^1)^m)$, contrary to the assumption of the theorem. Consequently, Q is finite. Along similar lines one can prove the finiteness of the set of prime powers q such that $q \equiv 1 \pmod{m}$ and $M_{q,m}$ is a difference set in $\mathbb{F}_q$. Thus the theorem is true. □

For the values of m in Table 9, $L_m \cap (\{0\} \times \mathbb{C}^m)$ is nonempty only when $m = 10$ or 18. Hence we would like to ask the following.

Question 5.9. For which even m's is $L_m \cap (\{0\} \times \mathbb{C}^m)$ nonempty?

Acknowledgment

The author would like to thank the anonymous referee for the careful reading and helpful suggestions.

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, Berlin-New York, 1971. MR0282863

[2] L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. **21** (1967), 204–219, DOI 10.2307/2004161. MR0223322

[3] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication. MR1625181

[4] K. Byard, R. Evans, and M. Van Veen, *Lam's power residue addition sets*, Adv. in Appl. Math. **46** (2011), no. 1-4, 94–108, DOI 10.1016/j.aam.2010.09.008. MR2794016

[5] S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 45–46. MR0014119

[6] S. Chowla and H. J. Ryser, *Combinatorial problems*, Canadian J. Math. **2** (1950), 93–99. MR0032551

[7] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, 2nd ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2007. MR2246267

[8] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*: *An introduction to computational algebraic geometry and commutative algebra*, 3rd ed., Undergraduate Texts in Mathematics, Springer, New York, 2007. MR2290010

[9] R. J. Evans, *Bioctic Gauss sums and sixteenth power residue difference sets*, Acta Arith. **38** (1980/81), no. 1, 37–46. MR574123
[10] R. J. Evans, *Twenty-fourth power residue difference sets*, Math. Comp. **40** (1983), no. 162, 677–683, DOI 10.2307/2007541. MR689481
[11] R. Evans, *Nonexistence of twentieth power residue difference sets*, Acta Arith. **89** (1999), no. 4, 397–402. MR1703856
[12] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, DOI 10.1016/S0022-4049(99)00005-5. Effective methods in algebraic geometry (Saint-Malo, 1998). MR1700538
[13] M. Hall Jr., *Cyclic projective Planes*, Duke Math. J. **14** (1947), 1079–1090. MR0023536
[14] M. Hall Jr., *Characters and cyclotomy*, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 31–43. MR0174549
[15] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer-Verlag, New York-Berlin, 1973. Graduate Texts in Mathematics, Vol. 6. MR0333959
[16] D. Jungnickel, *Difference sets*, Contemporary Design Theory, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992, pp. 241–324. MR1178504
[17] E. Lehmer, *On residue difference sets*, Canadian J. Math. **5** (1953), 425–432. MR0056007
[18] J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. **11** (1965/1966), 263–279. MR0193081
[19] R. E. A. C. Paley, On orthogonal matrices. *J. Math. Phys.*, 12 (1933), 311–320.
[20] T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, No. 2, Markham Publishing Co., Chicago, Ill., 1967. MR0217033
[21] A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999. MR1695775
[22] K. Thas, *Finite flag-transitive projective planes: a survey and some remarks*, Discrete Math. **266** (2003), no. 1-3, 417–429, DOI 10.1016/S0012-365X(02)00823-3. MR1991732
[23] K. Thas and D. Zagier, *Finite projective planes, Fermat curves, and Gaussian periods*, J. Eur. Math. Soc. (JEMS) **10** (2008), no. 1, 173–190, DOI 10.4171/JEMS/107. MR2349900
[24] A. Wagner, *On finite affine line transitive planes*, Math. Z. **87** (1965), 1–11, DOI 10.1007/BF01109922. MR0172165
[25] A. L. Whiteman, *The cyclotomic numbers of order ten*, Proc. Sympos. Appl. Math., Vol. 10, American Mathematical Society, Providence, R.I., 1960, pp. 95–111. MR0113851
[26] A. L. Whiteman, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53–76. MR0118709

School of Mathematics and Statistics, University of Western Australia, Crawley 6009, Western Australia, Australia

Current address: School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC 3010, Australia

Email address: binzhoux@unimelb.edu.au