On the Nonexistence of Partial Difference Sets by Projections to Finite Fields

Yue Zhou*

Department of Mathematics, National University of Defense Technology, Changsha 410073, China.

Received 30 November 2020; Accepted 13 April 2021

Abstract. In the study of (partial) difference sets and their generalizations in groups \( G \), the most widely used method is to translate their definition into an equation over group ring \( \mathbb{Z}[G] \) and to investigate this equation by applying complex representations of \( G \). In this paper, we investigate the existence of (partial) difference sets in a different way. We project the group ring equations in \( \mathbb{Z}[G] \) to \( \mathbb{Z}[N] \) where \( N \) is a quotient group of \( G \) isomorphic to the additive group of a finite field, and then use polynomials over this finite field to derive some existence conditions.

AMS subject classifications: 05B10, 05E30, 11T06

Key words: Partial difference set, strongly regular graph, finite field.

1 Introduction

Let \( G \) be a finite group of order \( v \) and \( D \) a \( k \)-subset of \( G \). We call \( D \) a \((v,k,\lambda,\mu)\) - partial difference set in \( G \) if the expressions \( d_1d_2^{-1} \), for distinct \( d_1, d_2 \in D \), represent each non-identity element contained in \( D \) exactly \( \lambda \) times and represent each non-identity element not contained in \( D \) exactly \( \mu \) times. In particular, when \( \lambda = \mu \), a partial difference set is just an ordinary difference set.

*Corresponding author. Email address: yue.zhou.ovgu@gmail.com (Y. Zhou)
Usually, (partial) difference sets are studied using the group ring \( \mathbb{Z}[G] \) or \( \mathbb{C}[G] \). Let \( \mathbb{Z}[G] \) denote the set of formal sums \( \sum_{g \in G} a_g g \), where \( a_g \in \mathbb{Z} \) and \( G \) is a multiplicative group. The addition and the multiplication on \( \mathbb{Z}[G] \) are defined by

\[
\sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g)g,
\]

and

\[
\left( \sum_{g \in G} a_g g \right) \cdot \left( \sum_{g \in G} b_g g \right) := \sum_{g \in G} \left( \sum_{h \in G} a_h b_{h^{-1}g} \right)g
\]

for \( \sum_{g \in G} a_g g, \sum_{g \in G} b_g g \in \mathbb{Z}[G] \). Moreover,

\[
\lambda \cdot \left( \sum_{g \in G} a_g g \right) := \sum_{g \in G} (\lambda a_g)g
\]

for \( \lambda \in \mathbb{Z} \) and \( \sum_{g \in G} a_g g \in \mathbb{Z}[G] \).

For an element \( D = \sum_{g \in G} a_g g \in \mathbb{Z}[G] \) and \( t \in \mathbb{Z} \), we define

\[
D(t) := \sum_{g \in G} a_g g^t.
\]

An important case is \( D^{(-1)} = \sum_{g \in G} a_g g^{-1} \). If \( D \) is a subset of \( G \), we identify \( D \) with the group ring element \( \sum_{d \in D} d \). A subset \( D \) in \( G \) is a \((v, k, \lambda, \mu)\)-partial difference set if and only if

\[
DD^{(-1)} = \mu G + (\lambda - \mu)D + \gamma 1_G,
\]

where \( 1_G \) denotes the identity element of \( G \).

When \( \lambda \neq \mu \), i.e. \( D \) is not a difference set, there is always \( D^{(-1)} = D \), see [8]. Note that \( D \) is a partial difference set with \( D^{(-1)} = D \) and \( 1_G \notin D \), if and only if, \( D \) generates a strongly regular graph \( \text{Cay}(G, D) \). Here \( \text{Cay}(G, D) \) is defined to be a graph with the elements in \( G \) as vertices, and in which two vertices \( g \) and \( h \) are adjacent if and only if \( gh^{-1} \in D \). Usually, a partial difference set with \( D^{(-1)} = D \) and \( 1_G \notin D \) is called regular.

Partial difference sets have been intensively investigated for decades. There are many known constructions and necessary conditions on their existence. We refer to [9] for a classical survey. More construction results could be found in [1,10–13]. For existence conditions and classification result, see [2–4,6,15,16].

The most powerful approach for the study of (partial) difference sets is to translate their definition into an equation over group ring \( \mathbb{Z}[G] \) and to investigate
this equation by applying complex representations of $G$. Many existence conditions are obtained in this way. In this paper, we project the group ring equations in $\mathbb{Z}[G]$ to $\mathbb{Z}[N]$ where $N$ is a quotient group of $G$ isomorphic to the additive group of a finite field, and then use polynomials over this finite field to derive some existence conditions of (partial) difference sets and their generalizations. To the best of our knowledge, this approach has never been applied on the existence of (partial) difference sets before. This work is inspired by Kim [5], Zhang, Ge [17], and Qureshi [14] who applied symmetric polynomials over finite fields to disprove the existence of perfect linear Lee codes.

The rest parts of this paper is organized as follows. In Section 2, we introduce some known restrictions on the parameters of a regular partial difference set and a result on finite fields. Then we prove the main results and consider their applications in Section 3.

## 2 Preliminaries

Following the standard notation, we set $v = |G|, k = |D|, \beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$ for a partial difference set $D$. Furthermore, it is easy to check that $\gamma = k - \mu$ if $1_G \notin D$ and $\gamma = k - \lambda$ if $1_G \in D$.

Concerning the existence of partial difference sets, there are many known results. By simply counting argument, one gets the following well known restrictions on the parameter of a regular partial difference set.

**Lemma 2.1.** The parameters of a regular $(v,k,\lambda,\mu)$-partial difference set satisfy

(a) $(v + \beta)^2 - (\Delta - \beta^2)(v-1)$ must be a square;

(b) $k = \left( (v + \beta) \pm \sqrt{(v + \beta)^2 - (\Delta - \beta^2)(v-1)} \right) / 2$;

(c) $\beta$ and $\Delta$ have the same parity; and

(d) if $D \neq \emptyset$ or $G \setminus \{1_G\}$, then $0 \leq \lambda \leq k-1$ and $0 \leq \mu \leq k$.

An automorphism $\tau$ of $G$ is called a multiplier of $D$ if $\tau(D) = D$. When $G$ is abelian and an integer $t$ is such that $\gcd(t,v) = 1$, the map $g \mapsto g^t$ is an automorphism of $G$. For a subset $D$ of $G$, if $D^{(t)} = D$, then $t$ is called a (numerical) multiplier of $D$. As mentioned in the introduction part, for a regular partial difference set, $-1$ is always its multiplier. There are rich numbers of multipliers of abelian partial difference sets by the following result.
Lemma 2.2 (Ma [8]). Let $G$ be an abelian group of order $v$ and $D$ a regular $(v,k,\lambda,\mu)$-partial difference set in $G$. Then $t^2$ is a multiplier of $D$ for any $t$ relatively prime to $v$. Furthermore, if $\Delta$ is a square, then $t$ is a multiplier of $D$ for any $t$ relatively prime to $v$.

Another strong restriction on the parameters of a regular partial difference set is the following one given by Ma [8] by using the Delsarte dual of strongly regular graphs.

Lemma 2.3. If there exists a nontrivial regular $(v,k,\lambda,\mu)$-partial difference set in an abelian group, then $v, \Delta$ and $v^2/\Delta$ have the same prime divisors.

Let $\mathbb{F}_q$ denote a finite field with $q$ elements where $q$ is a power of a prime number $p$. Let $H$ be a subgroup of index $\sigma$ of the multiplicative group of $\mathbb{F}_q$.

Lemma 2.4. Suppose that $\sigma < q - 1$. Let $V$ denote the $\mathbb{F}_q$-vector space consisting of all functions from $H$ to $\mathbb{F}_q$. Then $V$ is isomorphic to $\mathbb{F}_q[X]/(X^{\frac{q-1}{\sigma}} - 1)$.

When $\sigma = 1$, Lemma 2.4 is very close to a well-known result about the functions from $\mathbb{F}_q$ to itself; see [7, Chapter 7] for instance. The proof of Lemma 2.4 is similar.

Proof. First, it is obvious that each polynomial $f \in \mathbb{F}_q[X]$ defines a function $\bar{f}: x \mapsto f(x)$ from $H$ to $\mathbb{F}_q$. Let $\phi$ denote the map $f \mapsto \bar{f}$. It is obvious that $\phi$ is $\mathbb{F}_q$-linear.

As $a^{\frac{q-1}{\sigma}} - 1 = 0$ for each $a \in H$, the ideal $(X^{\frac{q-1}{\sigma}} - 1)$ belongs to the kernel of $\phi$. Since $|H| = \frac{q-1}{\sigma}$, the dimension of $V$ is $\dim_{\mathbb{F}_q}(V) = \frac{q-1}{\sigma}$. It also equals the size of $\{1, X, X^2, \ldots, X^{\frac{q-1}{\sigma}}\}$ which spans $\mathbb{F}_q[X]/(X^{\frac{q-1}{\sigma}} - 1)$. Therefore, $V$ is isomorphic to $\mathbb{F}_q[X]/(X^{\frac{q-1}{\sigma}} - 1)$.

Theorem 2.1. Suppose that $\sigma < q - 1$. Let $y_1, \ldots, y_s \in H$. Suppose that

$$\sum_{i=1}^{s} y_i^j = 0$$

for $j = 1, \ldots, \frac{q-1}{\sigma} - 1$. Then there is a constant $C$ such that $C \equiv \#\{i : y_i = h\} \pmod{p}$ for all $h \in H$.

Proof. Let $h_a = 1 - (X-a)^{q-1}$. Then

$$h_a(x) = \begin{cases} 1, & x = a, \\ 0, & x \neq a. \end{cases}$$
Let \( \hat{h}_a \) denote the polynomial \( h_a \pmod{X^{q-1} - 1} \). Clearly, \( \deg(\hat{h}_a) < \frac{q-1}{\sigma} \). By Lemma 2.4, \( \{\hat{h}_a : a \in H\} \) is a basis of \( \mathbb{F}_q[X]/(X^{q-1} - 1) \) over \( \mathbb{F}_q \). By computation, for \( a \in H \),

\[
h_a = 1 - (X-a)^{q-1} = 1 - \sum_{i=0}^{q-1} a^{q-1-i} X^i
\]

\[
\equiv 1 - X^{q-1} - \sum_{j=0}^{\frac{q-1}{\sigma}-1} \sum_{k=0}^{j} a^{q-1-j-k} \frac{q-1}{\sigma} X^j \pmod{X^{\frac{q-1}{\sigma}} - 1}
\]

\[
\equiv - \sum_{j=0}^{\frac{q-1}{\sigma}-1} \sum_{k=0}^{j} a^{q-1-j} X^j \pmod{X^{\frac{q-1}{\sigma}} - 1},
\]

which means

\[
\hat{h}_a = - \sum_{j=0}^{\frac{q-1}{\sigma}-1} \sigma a^{q-1-j} X^j. \tag{2.1}
\]

Define \( f_H = \sum_{a \in H} \hat{h}_a \). Then \( \deg(f_H) < \frac{q-1}{\sigma} \) and \( f_H(x) = 1 \) for all \( x \in H \). By Lemma 2.4, we have \( f_H = 1 \in \mathbb{F}_q[X] \). By (2.1),

\[
1 = - \sum_{a \in H} \sum_{j=0}^{\frac{q-1}{\sigma}-1} \sigma a^{q-1-j} X^j.
\]

Therefore, \( \sigma \sum_{a \in H} a^j = 0 \) for \( j = 1, \ldots, \frac{q-1}{\sigma} - 1 \). As \( \gcd(\sigma, q) = 1 \), we obtain

\[
\sum_{a \in H} a^j = 0 \tag{2.2}
\]

for \( j = 1, \ldots, \frac{q-1}{\sigma} - 1 \).

Now let \( g = \sum_{i=1}^s \hat{h}_{y_i} \) which implies \( \deg(g) < \frac{q-1}{\sigma} \). By (2.1), we have

\[
g = - \sum_{i=1}^s \sum_{j=0}^{\frac{q-1}{\sigma}-1} \sigma y_i^{q-1-j} X^j = - \sigma \sum_{j=0}^{\frac{q-1}{\sigma}-1} \left( \sum_{i=1}^s y_i^{q-1-j} \right) X^j = -\sigma s,
\]

where the last equality is from the assumption that \( \sum_{i=1}^s y_i^j = 0 \) for \( j = 1, \ldots, \frac{q-1}{\sigma} - 1 \). Therefore,

\[
g = -\sigma s \sum_{a \in H} \hat{h}_a.
\]
As \( \{ \hat{h}_a : a \in H \} \) is a basis of \( \mathbb{F}_q[X]/(X^{q+1} - 1) \) over \( \mathbb{F}_q \), each \( a \in H \) must appear in \( y_1, \cdots, y_s \) for the same number of times modulo \( p \).

### 3 Main results

Let \( G \) be a group with the identity element \( 1_G \). By setting \( \beta = \lambda - \mu \), from (1.1) we have

\[
DD^{(-1)} = \mu G + \beta D + \gamma 1_G
\]

for some \( \mu, \beta, \gamma \in \mathbb{Z} \). It is clear that the coefficient of each element on the right hand side of (3.1) must be equal to or larger than 0. In particular, if \( \beta = 0 \), then \( D \) is a difference set.

Suppose that \( G \) has a quotient group \( N \) which is isomorphic to the additive group of \( \mathbb{F}_p^\times \), where \( p \) is a prime number. This implies that there is a normal subgroup \( H \leq G \) of order \( m \), \( N = G/H \) and \( |G| = mp^n \). Let \( \rho \) be the natural homomorphism from \( G \) to \( N \). Then we can derive the following equation from (3.1):

\[
\rho(D) \rho \left( D^{(-1)} \right) = \mu mN + \beta \rho(D) + \gamma 1_N,
\]

(3.2)

where \( 1_N \) is the identity element in \( N \).

Suppose that \( t \in \mathbb{Z} \) with \( p \nmid t \) is a numerical multiplier fixing \( \rho(D) \), i.e. \( \rho(D)^{(t)} = \rho(D) \). Let \( \sigma = \text{ord}_p(t) \). Thus the nonzero elements in \( \rho(D) \) can be written as the union of the orbits of elements under the action of \( a \mapsto at \). As \( N \) is an elementary abelian \( p \)-group, all these orbits containing non-identity elements are of the same length \( \sigma \) and \( \sigma \mid p-1 \).

Now, we rewrite group \( N \) additively and use 0 to denote the identity element. In this way, the action of the multiplier \( t \) is given by \( x \mapsto xt \) and

\[
\rho(D) = \{ * 0^{\text{r times}} 0 * \} \bigcup \{ * x_it^j : i = 1, \ldots, s, j = 0, \ldots, \sigma - 1 * \},
\]

(3.3)

where \( x_1, \cdots, x_s \in N \setminus \{0\} \) and they are not necessarily different. It is clear that \( |D| = r + s\sigma \) and \( r \leq m \).

For each \( u \in N \), we define \( C_u := \# \{ d \in D : \rho(D) = u \} \). Let \( \bar{u} \) be the image of \( u \in \mathbb{F}_p^\times \) under the canonical homomorphism from \( \mathbb{F}_p^\times \) to \( \mathbb{F}_p^\times / \langle t \rangle \). Then we can define \( C_{\bar{u}} = C_u \), because \( C_u = C_{ut^j} \) for each \( j = 0, \ldots, \sigma - 1 \) by (3.3). Therefore

\[
|D| = \sigma \sum_{\bar{u} \in \mathbb{F}_p^\times / \langle t \rangle} C_{\bar{u}} + C_0,
\]

and \( C_0 = r \).
The difference list of $\rho(D)$ is the multiset
\[\{ * x - y : x, y \in \rho(D) * \},\]
which is the union of the multisets
\[
\begin{align*}
&\{ * 0, \cdots, 0 * \}, \{ * \pm x, t^u : 1 \leq i \leq s, 0 \leq u \leq \sigma - 1 * \}, \\
&\{ * x_i t^u - x_j t^v : 1 \leq i, j \leq s, 0 \leq u, v \leq \sigma - 1 * \}.
\end{align*}
\]

**Theorem 3.1.** Define the following collection of conditions

(a) $p \nmid 2 | D | - \beta$ and $2 | \sigma$;
(b) $p \nmid 2 | D | - \beta$, $2 | \sigma$ and $p \mid \beta$;
(c) $p \mid 2 | D | - \beta$, $2 | \sigma$ and $p \nmid \beta$;
(d) $p \mid 2 | D | - \beta$, $2 | \sigma$ and $p \nmid \beta$;
(e) $p \mid 2 | D | - \beta$, $2 | \sigma$ and $p \mid \beta$.

Set
\[
M = \begin{cases} 
\max \left\{ \ell : p \mid \left( \frac{2i\sigma}{l} \right) \text{ for each even } i \in [1, \ell] \right\} & \text{for (c)}, \\
\max \left\{ \ell : p \mid \left( \frac{2i\sigma}{l} \right) \text{ for each } i \in [1, \ell] \right\} & \text{for (d) and (e)}. 
\end{cases}
\]

Suppose that there is a $D \subseteq G$ such that (3.2) holds.

(A) If (a) or (b) holds, then there is a constant $C$ such that $C \bar{u} \equiv C \mod p$ for all $\bar{u} \in \mathbb{F}_{p^n}^* / \langle t \rangle$.

(B) If $p^n - 1 \nmid s \sigma$, $M \geq \max \{ s - p, \frac{s - 1}{2} \}$ and one of (c) to (e) holds, then $p \mid s$.

(C) If $p^n - 1 \mid s \sigma$, $M \geq \max \{ s - p, \frac{s - 1}{2} \}$, each of $p, s - 1$ and $\frac{p^n - 1}{\sigma}$ is odd and one of (c) to (e) holds, then $p \mid s$.

**Proof.** We view every element in $\mathbb{N}$ as an element in the finite field $\mathbb{F}_{p^n}$. By (2.2),
\[
\sum_{\alpha \in \mathbb{F}_{p^n}} \alpha^l = \begin{cases} 
0, & p^n - 1 \nmid l, \\
-1, & p^n - 1 \mid l.
\end{cases}
\]
Computing the sum of the $l$-th power of each element on every side of (3.2), we get
\[
\sum_{u,v,i} (x_i t^u - x_j t^v)^l + r \sum_{i,u} (\pm x_i t^u)^l = \mu m \sum_{\alpha \in \mathbb{F}_p} \alpha^l + \beta \sum_{i,u} (x_i t^u)^l,
\]
which means
\[
\sum_{u,v,i} (x_i t^u - x_j t^v)^l + r \sum_{i,u} (\pm x_i t^u)^l - \beta \sum_{i,u} (x_i t^u)^l = \begin{cases} 0, & \text{if } \sigma = 0, \\ \pm m, & \text{if } \sigma = \pm 1. \end{cases} \tag{3.5}
\]
We denote the left hand side of (3.5) by $f_l(X)$, where $X := (x_1, \ldots, x_s)$.
Furthermore, by (2.2), we have
\[
\sum_{u=0}^{\sigma-1} t^{ul} = \begin{cases} \sigma, & \sigma \mid l, \\ 0, & \sigma \nmid l. \end{cases} \tag{3.6}
\]
Following the standard notation for symmetric functions, we use $p_l(X)$ to denote the power sum symmetric polynomials $\sum_{i=1}^s x_i^l$ evaluated at $(x_1, \cdots, x_s)$. Expand $f_l(X)$ for $l = 0, 1, \ldots, p^a - 1$,
\[
f_l(X) = \sum_{u,v,i} t^{ul} \sum_{v,i,j} (x_i - x_j t^{v-u})^l + r (1 + (-1)^l) \sum_{u} t^{ul} \sum_{i} x_i^l - \beta \sum_{u,v,i} t^{ul} \sum_{i} x_i^l
\]
\[
= \sum_{u,v,i} t^{ul} \sum_{v,i,j} \left( \begin{array}{c} l \\ k \end{array} \right) (-t^{v-u})^k x_i^{l-k} x_j^k + \left( r (1 + (-1)^l) - \beta \right) \sum_{u,v,i} t^{ul} p_l(X)
\]
\[
= \sum_{k=0}^{l} (-1)^k \left( \begin{array}{c} l \\ k \end{array} \right) \left( \sum_{u,v} t^{ul-uk+vk} \right) p_{l-k}(X) p_k(X) + \left( r (1 + (-1)^l) - \beta \right) \sum_{u,v,i} t^{ul} p_l(X)
\]
\[
= \left( \sum_{u,v} t^{ul} p_0(X) + (-1)^l \sum_{u,v} t^{vl} p_0(X) + \left( r (1 + (-1)^l) - \beta \right) \sum_{u,v,i} t^{ul} \right) p_l(X)
\]
\[
+ \sum_{k=1}^{l-1} (-1)^k \left( \begin{array}{c} l \\ k \end{array} \right) \left( \sum_{u,v} t^{ul-k} \sum_{v} t^{vk} \right) p_{l-k}(X) p_k(X).
\]
If $\sigma \nmid l$, then, by (3.6), $f_l(X) = 0$; if $l = w \sigma$ for some $w \in \mathbb{Z}^+$, then, by (3.6), the above equation becomes
\[
f_{w\sigma}(X) = \left( \sigma^2 p_0(X) + (-1)^w \sigma^2 p_0(X) + r \sigma (1 + (-1)^w \sigma) - \beta \sigma \right) p_{w\sigma}(X) \tag{3.7}
\]
\[
+ \sum_{i=1}^{w-1} (-1)^i \left( \begin{array}{c} w \sigma \\ i \sigma \end{array} \right) \sigma^2 p_{(w-i)\sigma}(X) p_{i\sigma}(X)
\]
By (3.8), recursively we can show that

\[ p \quad \text{in which the last equality holds because } p_0(X) = s \text{ and } |D| = r + s. \]

In particular, for \( w = 1 \),

\[ f_{\sigma}(X) = \sigma(1 + (-1)^{w\sigma}) - \beta) p_{w\sigma}(X). \]

If \( w\sigma \) is odd which implies that \( \sigma \) is also odd, then \((-1)^{w\sigma} = -(w-i)^{\sigma}\) whence (3.7) equals \(-\beta p_{w\sigma}(X)\). If \( w\sigma \) is even, then by (3.7)

\[ f_{w\sigma}(X) = \sigma(2|D| - \beta) p_{w\sigma}(X) + \sum_{i=1}^{w-1} (-1)^{w\sigma + 1} (w\sigma) p_{\sigma(w-i)\sigma}(X) p_{i\sigma}(X). \]

Noting that \( p \mid \sigma \), by (3.5), the above discussion leads to

\[
0 = \begin{cases} 
\beta p_{w\sigma}(X), & \text{if } 2 \nmid w\sigma, \\
(2|D| - \beta) p_{w\sigma}(X) + \sum_{i=1}^{w-1} (-1)^{w\sigma + 1} (w\sigma) p_{\sigma(w-i)\sigma}(X) p_{i\sigma}(X), & \text{if } 2 \nmid w\sigma, w \geq 2, \\
(2|D| - \beta) p_{w}(X), & \text{if } 2 \mid \sigma, w = 1 
\end{cases} \tag{3.8}
\]

for \( 1 \leq w < \frac{p^2 - 1}{\sigma} \).

**Claim.** If (a) or (b) holds, then \( p_{i\sigma}(X) = 0 \) for \( i = 1,2,\ldots,\frac{p^2 - 1}{\sigma} - 1 \); if one of (c), (d) and (e) holds, then \( p_{i\sigma}(X) = 0 \) for \( i = 1,2,\ldots,M \).

**Proof.** Next we divide the proof of the claim above into two cases depending on the parity of \( \sigma \).

**Case (i) \( \sigma \) is odd (Conditions (b), (c) and (d)).** First we consider the case \( p \nmid \beta \). By (3.8), \( p_{i\sigma}(X) = 0 \) for each odd integer \( i \). In particular, \( p_{\sigma}(X) = 0 \).

If \( p \mid 2|D| - \beta \), then by taking \( w = 2 \) and \( p_{\sigma}(X) = 0 \) in (3.8) we get \( p_{2\sigma}(X) = 0 \). Recursively we can show that \( p_{i\sigma}(X) = 0 \) for \( i = 4,5,6,\ldots,\frac{p^2 - 1}{\sigma} - 1 \).

If \( p \mid 2|D| - \beta \), then by taking \( w = 4 \) in (3.8) we get \((-1)^{2\sigma} \frac{4^\sigma}{2\sigma} p_{2\sigma}(X) = 0 \) because \( p_{\sigma}(X) = p_{2\sigma}(X) = 0 \). If \( p \mid \frac{4^\sigma}{\sigma} \), then \( p_{2\sigma}(X) = 0 \). It is not difficult to show recursively that if \( p \mid \frac{2^\sigma}{i\sigma} \) for each even integer \( i \) between 1 and \( M \), then \( p_{i\sigma}(X) = 0 \) for these \( i \)'s.

Second we consider the case \( p \mid \beta \). Clearly there is nothing interesting in (3.8) for odd \( w \). In this case, we need the condition that \( p \mid 2|D| - \beta \). Plugging \( w = 2 \),
into (3.8), we obtain \(-\binom{2\ell}{\sigma}\sigma p_{\sigma}^2(X) = 0\). Similarly as in the previous paragraph, if \(p \mid \binom{2\ell}{\sigma}\) for \(i = 1, 2, \ldots, M\), then \(p_{\sigma^i}(X) = 0\) for \(i = 1, 2, \ldots, M\).

**Case (ii)** \(\sigma\) is even (Conditions (a) and (e)). Now (3.8) can only provide us

\[
0 = (2|D| - \beta) p_{\sigma^e}(X) + \sum_{i = 1}^{w-1} \binom{\sigma^e}{i\sigma} \sigma p_{(w-i)e}(X)p_{i\sigma}(X).
\]

If \(p \nmid 2|D| - \beta\), then we can again recursively show that \(p_{i\sigma}(X) = 0\) for \(i = 1, \ldots, p^r - 1\); if \(p \mid 2|D| - \beta\), under the condition that \(p \mid \binom{2\ell}{\sigma}\) for \(i = 1, 2, \ldots, M\), we have \(p_{i\sigma}(X) = 0\) for \(i = 1, 2, \ldots, M\). Therefore, we have finished the proof of Claim. \(\square\)

The statement for Condition (A) is a direct consequence of Claim and Theorem 2.1.

Next we prove the theorem under Condition (B) or (C). Let \(e_k(X^\sigma)\) be the \(k\)-th elementary symmetric polynomials evaluated at \(x_1^\sigma, \ldots, x_s^\sigma\). By assumption, we know that \(p_{i\sigma}(X) = 0\) for \(i = 1, \ldots, M\). By Newton’s identities on \(x_1^\sigma, x_2^\sigma, \ldots, x_s^\sigma\), we have

\[
ke_k(X^\sigma) = e_{k-1}(X^\sigma)p_{\sigma^e}(X) + \cdots + (-1)^{i-1}e_{k-i}(X^\sigma)p_{i\sigma}(X) + \cdots + (-1)^{k-1}p_{ke}(X) = 0
\]

for every \(1 \leq k \leq M\). It is clear that if \(p \nmid k\), then \(e_k(X^\sigma) = 0\). By the assumption \(M \geq \max\{s - p, \frac{s - 1}{2}\}\) which means \(s - M - 1 \leq \min\{p - 1, M\}\), we have \(e_k(X^\sigma) = 0\) for \(k \leq s - M - 1\) whence

\[
se_s(X^\sigma) = e_s(X^\sigma)p_{\sigma^e}(X) + \cdots + (-1)^{M-1}e_{s-M}(X^\sigma)p_{M\sigma^e}(X) + \cdots + (-1)^s p_{se}(X) = (-1)^{s-1}p_{se}(X)
\]

\[
= \begin{cases} 
0, & p^a - 1 \nmid s\sigma, \\
(-1)^{s-1}s, & p^a - 1 \mid s\sigma.
\end{cases}
\]

Assume, by way of contradiction, that \(p \nmid s\).

If \(p^a - 1 \nmid s\sigma\), then \(e_s(X^\sigma) = 0\). However, \(e_s(X^\sigma) = (x_1 \cdots x_s)^\sigma\) which cannot be 0 because all \(x_i\)'s are nonzero. It is a contradiction. Therefore, \(p\) must divide \(s\).

If \(p^a - 1 \mid s\sigma\), then \(e_s(X^\sigma) = (x_1 \cdots x_s)^\sigma = (-1)^{s-1}\). As \(\frac{p^a - 1}{\sigma}\) is odd and \(s - 1\) is even, we have

\[
(x_1 \cdots x_s)^{p^a - 1} = -1.
\]
However, as \( p \neq 2 \), this equation cannot hold in \( \mathbb{F}_{p^2} \). Therefore, \( p \) divides \( s \). \( \Box \)

**Remark 3.1.** It is worth pointing out that Theorem 3.1 works also for some generalization of (partial) difference sets, because it only provides necessary conditions for (3.2), not for (1.1). For example, if \( D \subseteq G \) is such that

\[
DD^{(-1)} = \mu G + \beta D + \sum_{i=1}^{w} \gamma_i H_i,
\]

where \( H_i \)'s are subgroups of \( G \). If \( H_i \) is mapped to \( 1 \in \mathbb{N} \) under \( \rho \) for each \( i \), then we get (3.2) again. Thus Theorem 3.1 also works for such a \( D \).

In general, it is not easy to use Theorem 3.1 (B) and (C) to show the nonexistence of \( D \) satisfying (3.1). However, Theorem 3.1 (A) can provide interesting restrictions on the parameters of \( D \) when \( a \) is small and \( p \) is relatively large compared with \( m \). For instance, when \( a=1 \), \( p \) is odd and \( D \) is a regular abelian partial difference set, by Lemma 2.2, we may choose proper \( t \) such that \( \frac{p-1}{\sigma} = 1 \) provided that \( \Delta \) is a square. This covers the most interesting cases, because when \( \Delta \) is a nonsquare, the parameter of an abelian regular partial difference set must be

\[
(v,k,\lambda,\mu,\beta,\Delta) = \left( p^{2s+1}, \frac{p^{2s+1} - 1}{2}, \frac{p^{2s+1} - 5}{4}, -1, p^{2s+1} \right).
\]

By Theorem 3.1 (A), if \( p \nmid 2k - \beta \), then

\[
|D| = (p-1) \cdot C + r
\]

for some \( C,r \in \mathbb{Z}^+ \) such that \( C \leq m \) and \( r < m \). If \( m << p \), then this condition on \( |D| \) is strong enough to exclude many possible value of parameters which even satisfy Lemma 2.1. For instance, \((v,k,\lambda,\mu) = (232,66,40,10)\) meets the conditions in Lemma 2.1. However, if we let \( p = 29 \) and \( m = 8 \), then \( k = 2 \cdot (29-1) + 10 \) with \( r = 10 \geq 8 = m \) and \( p \nmid 2k - \beta = 2 \cdot 66 - 30 = 102 \). Thus, (3.10) is not satisfied and there is no such partial difference sets no matter the group \( G \) is abelian or non-abelian. For \( v = 232 \), by using this approach, we can exclude 109 possible parameters of partial difference sets which satisfy Lemma 2.1. It is clear that a group \( G \) of order 232 = 29 \cdot 8 \) is not necessary abelian. It could be a direct product of the cyclic group \( C_{29} \) of order 29 and the dihedral group of order 8, or the direct product of \( C_{29} \) and the quaternion group.

Unfortunately, for abelian partial difference sets \( D \), Theorem 3.1 (A) is already covered by Lemma 2.3. Precisely speaking, for each \( p \mid v \), Lemma 2.3 tells us that
$p$ must divide $2k - \beta$. To derive this result, suppose the contrary that $p \mid \nu$ and $p \nmid 2k - \beta$. By Lemma 2.1 (b),

$$2k - \beta = \nu \pm \sqrt{(\nu + \beta)^2 - (\Delta - \beta^2)(\nu - 1)}.$$

It follows that

$$p \mid (\nu + \beta)^2 - (\Delta - \beta^2)(\nu - 1) = \nu^2 + \nu \left( \beta^2 + 2\beta - \Delta \right) + \Delta.$$

However, this contradicts Lemma 2.3. Therefore, for each $p \mid \nu$, $p$ always divides $2k - \beta$.

Noting that Lemma 2.3 is only for abelian groups. Therefore, it does not cover Theorem 3.1 for the existence of nonabelian partial difference sets.

**Acknowledgment**

This work is partially supported by Natural Science Foundation of Hunan Province (No. 2019JJ30030) and Training Program for Excellent Young Innovators of Changsha (No. kq1905052).

**References**


