Indian J. Pure Appl. Math., **51**(1): 233-249, March 2020
© Indian National Science Academy DOI: 10.1007/s13226-020-0397-5

POLYNOMIAL CRITERION FOR ABELIAN DIFFERENCE SETS

Pradipkumar H. Keskar and Priyanka Kumari

Department of Mathematics, Birla Intitute of Technology and Science,
Pilani (Pilani Campus), Pilani 333 031, *India*
e-mails: keskar@pilani.bits-pilani.ac.in;
priyanka.kumari@pilani.bits-pilani.ac.in

(*Received* 25 *August* 2017; *after final revision* 17 *August* 2018;
accepted 21 *January* 2019)

Difference sets are subsets of a group satisfying certain combinatorial property with respect to the group operation. They can be characterized using an equality in the group ring of the corresponding group. In this paper, we exploit the special structure of the group ring of an Abelian group to establish a one-to one correspondence of the class of difference sets with specific parameters in that group with the set of all complex solutions of a specified system of polynomial equations. The correspondence also develops some tests for a Boolean function to be a bent function.

Key words : Difference set; group ring; point representation; ideal membership; bent function.

2010 Mathematics Subject Classification: 05B10, 11T71, 13P99

1. Introduction

For a finite group G of order v and nonnegative integers k, λ, a subset D of G is called a (v, k, λ) *difference set* in G if for every $g \in G \setminus \{e\}$,

$$|\{(d_1, d_2) \in D \times D \,:\, g = d_1 d_2^{-1}\}| = \lambda \text{ and } |D| = k,$$

where e is the identity of G. Moreover, if G is abelian then D is called an *abelian difference set*. The notion of a difference set was introduced independently by Singer [10] and Bose [2] while investigating finite geometries and (statistical) design of experiments respectively. Later the ideas were found fruitful having several relations to areas such as coding theory and cryptography. Bent functions, which are cryptographically significant, are characterized on page 95 of [11] in terms of difference sets as follows. For an even positive integer $t > 2$, a Boolean function of t variables $\big($that is, a function from $(\mathbb{Z}/2\mathbb{Z})^t$ to $(\mathbb{Z}/2\mathbb{Z})\big)$ is a bent function if and only if its support is a $\big(2^t, 2^{(t-1)} \pm 2^{(t-2)/2}, 2^{(t-2)} \pm 2^{(t-2)/2}\big)$ difference set in $(\mathbb{Z}/2\mathbb{Z})^t$(where signs are chosen consistently). Hence the construction, characterization, equivalence of difference sets is a useful exercise having applications for the analysis of bent functions.

Among the different tools used to study difference sets are symmetric designs and group rings. In this paper, we will be concerned with the characterization of a difference set using an equality in a group ring, which we now describe.

Let G be a finite group and R be a commutative ring with unit element 1 different from its additive identity 0. The *group ring* RG of G over R is the ring

$$RG = \{\sum_{g\in G} r_g g : r_g \in R\}$$

where $\sum_{g\in G} r_g g = \sum_{g\in G} r_g^* g \iff r_g = r_g^*$ for all $g \in G$, with the addition defined by $\sum_{g\in G} r_g g + \sum_{g\in G} r_g^* g = \sum_{g\in G}(r_g + r_g^*)g$ and the multiplication defined by $\Big(\sum_{g\in G} r_g g\Big)\Big(\sum_{g\in G} r_g^* g\Big) = \sum_{g\in G}(\sum_{xy=g} r_x r_y^*)g$.

For any $D \subset G$, we denote $\sum_{g\in D} g \in RG$ by D again and $\sum_{g\in D} g^{-1} \in RG$ by $D^{(-1)}$. The following is a characterization of a difference set in a finite group G.

Group Ring Criterion : Let G be a finite group of order v and k, λ be nonnegative integers with $k \leq v$. Then $D \subset G$ is a (v, k, λ) difference set in G if and only if as elements of $\mathbb{C}G$, we have $DD^{(-1)} = \lambda G + (k - \lambda)e$, where e is the identity element of G.

(In most of the literature, for instance [1], the characterization is proved under extra assumption that $|D| = k$. This assumption can be seen to be superfluous, as it is implied by either of the above two conditions. It is enough to note that if $DD^{(-1)} = \lambda G + (k - \lambda)e$, then by comparing the coefficient of e on both sides, we get $|D| = k$.)

In this paper, we exploit the structure of the group ring of an abelian finite group G as an affine $\mathbb{C}$-algebra to obtain two algebraic criteria for a subset of G to be a (v, k, λ) difference set. The first criterion, Theorem 2.2 of Section 2, is in terms of an ideal membership problem. The second, Theorem 3.2 of Section 3, is via verification of some polynomial equations. These processes can also be crystalised to give tests for a subset of an abelian group to be a (v, k, λ) difference set. The first test is verifiable using ideal theory or algebra softwares like Macaulay 2, while the second test is verifiable by explicit computations with complex numbers, especially the roots of unity. Section 4 deals with generalization of these criteria to generalized difference sets. We illustrate the use of the criteria for difference sets through some examples in Section 5. The first two illustrate these tests for difference sets. The third illustrates how the polynomial criterion can be used to prove that a quadratic Boolean function is a bent function. In a future work we plan to explore the more of potential applications of these methods to the theory of bent functions.

Ideal theoretic methods, in particular Gröbner basis methods, are being widely applied to several problems in Science and Engineering, see [4]. More specifically, we can find their applications to Combinatorics in [5-7, 9]. In this paper, we introduce these methods to study difference sets.

2. Ideal Membership Problem for Abelian Difference Sets

Let G be a finite abelian group. Then $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_t}$ where $C_{n_l} = \langle g_l \rangle$ is a cyclic group of order n_l. Let $R = \mathbb{C}[X_1, \ldots, X_t]$, I be ideal $(X_1^{n_1} - 1, \ldots, X_t^{n_t} - 1)$ of R and $S = \{(i_1, \ldots, i_t) \in \mathbb{Z}^t : 0 \leq i_l \leq n_l - 1 \text{ for all } 1 \leq l \leq t\}$. Regarding the structure of $\mathbb{C}G$, we have the following:

***Theorem* 2.1** — *Let $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_t}$ where $C_{n_l} = \langle g_l \rangle$ is a cyclic group of order n_l. Then the map $\phi_G : \frac{R}{I} \to \mathbb{C}G$ defined by*

$$\phi_G(f(X_1, \ldots, X_t) + I) = f(g_1, \ldots, g_t)$$

is an isomorphism of $\frac{R}{I}$ onto $\mathbb{C}G$, where

$$\begin{aligned} f(g_1, \ldots, g_t) &= \sum_{(i_1,\ldots,i_t) \in \mathbb{Z}^t} c_{i_1 \cdots i_t} g_1^{i_1} \cdots g_t^{i_t} \\ \textit{for } f(X_1, \ldots, X_t) &= \sum_{(i_1,\ldots,i_t) \in \mathbb{Z}^t} c_{i_1 \cdots i_t} X_1^{i_1} \cdots X_t^{i_t} \\ \textit{with } c_{i_1 \cdots i_t} &\in \mathbb{C} \textit{ for all } (i_1, \ldots, i_t) \in \mathbb{Z}^t. \end{aligned}$$

Proof : First we show that ϕ_G is well defined. Assume $f_1(X_1, \ldots, X_t) + I = f_2(X_1, \ldots, X_t) + I$ for $f_1 = f_1(X_1, \ldots, X_t)$ and $f_2 = f_2(X_1, \ldots, X_t) \in R$. Then $f_1 - f_2 \in I$ and hence

$$f_1(X_1, \ldots, X_t) - f_2(X_1, \ldots, X_t) = \sum_{l=1}^{t} (X_l^{n_l} - 1) u_l(X_1, \ldots, X_t)$$

for $u_1(X_1, \ldots, X_t), \ldots, u_t(X_1, \ldots, X_t) \in R$. This, in turn, implies that

$$f_1(g_1, \ldots, g_t) - f_2(g_1, \ldots, g_t) = \sum_{l=1}^{t} (g_l^{n_l} - 1) u_l(g_1, \ldots, g_t) = 0$$

as $g_l^{n_l} - 1 = 0$ for all $1 \leq l \leq t$. Hence $\phi_G(f_1 + I) = \phi_G(f_2 + I)$, therefore ϕ_G is well defined.

Next, ϕ_G is clearly $\mathbb{C}-$algebra homomorphism onto $\mathbb{C}G$.

Now $\mathbb{C}G$ has dimension $n_1 \cdots n_t$ as $\mathbb{C}-$vector space, as $\{g_1^{i_1} \cdots g_t^{i_t} : 0 \leq i_l \leq n_l - 1$ for all $1 \leq l \leq t\}$ is a basis for $\mathbb{C}G$. Also $\frac{R}{I}$ has dimension $n_1 \cdots n_t$ as $\{X_1^{i_1} \cdots X_t^{i_t} : 0 \leq i_l \leq n_l - 1$ for all $1 \leq l \leq t\}$ is a basis for $\frac{R}{I}$. This shows that ϕ_G is an isomorphism. □

As a consequence of Theorem 2.1, we can make several identifications. First, the group ring $\mathbb{C}G$ can be identified with the affine space $\mathbb{C}^{n_1 \cdots n_t}$ by identifying $\sum_{(i_1,\ldots,i_t)\in S} \alpha_{i_1 \cdots i_t} g_1^{i_1} \cdots g_t^{i_t}$ with $(\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S)$ in a fixed order on S, say lexicographic order. Second, any subset T of G can be identified with the point in $\mathbb{C}^{n_1 \cdots n_t}$ corresponding to $\sum_{g \in T} g \in \mathbb{C}G$; it will be called *the point representation (or characteristic point) of* T and it is a vertex of the unit hypercube of $\mathbb{C}^{n_1 \cdots n_t}$. Third, T can also be represented by the unique polynomial $f = f(X_1, \ldots, X_t) \in R$ such that $\phi_G(f + I) = \left(\sum_{g\in T} g\right)$ and either $f = 0$ or $\deg_{X_l}(f) < n_l$ for all $1 \leq l \leq t$. We call f the *polynomial representation of* T and denote it by $\rho_G(T)$ or $\rho_G(T)(X_1, \ldots, X_t)$.

Here onwards, by using the isomorphism of G with $C_{n_1} \times \cdots \times C_{n_t}$ and fixed isomorphisms of C_{n_l} with $\left(\frac{\mathbb{Z}}{n_l\mathbb{Z}}\right)$ for all $1 \leq l \leq t$, we will identify G with $\prod_{l=1}^{t} \left(\frac{\mathbb{Z}}{n_l\mathbb{Z}}\right)$. Moreover for any $T \subset G$, we let $T^* = \{(i_1, \ldots i_t) \in S : (i_1 + n_1\mathbb{Z}, \ldots, i_t + n_t\mathbb{Z}) \in T\}$.

The above relationships can be captured by the following equalities :

For any T $\subset G$

$$\begin{aligned}\rho_G(T) &= \sum_{(i_1,\ldots,i_t)\in T^*} X_1^{i_1} \cdots X_t^{i_t} \qquad (2.1*)\\ &= \sum_{(i_1,\ldots,i_t)\in S} \alpha_{i_1 \cdots i_t} X_1^{i_1} \cdots X_t^{i_t}\end{aligned}$$

where $(\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S)$ is a point representation of T.

Using these representations, Group Ring Criterion of Section 1 can be rephrased as an ideal membership problem (refer p. 94 of [4]) in $\mathbb{C}[X_1, \ldots, X_t]$ as follows.

Theorem 2.2 — *Let $\kappa_D = \kappa_D(X_1, \ldots, X_t) \in \mathbb{C}[X_1, \ldots, X_t]$ be defined by*

$$\begin{aligned}\kappa_D = &\left(\sum_{(i_1,\ldots,i_t)\in D^*} X_1^{i_1} \cdots X_t^{i_t}\right)\left(\sum_{(i_1,\ldots,i_t)\in D^*} X_1^{n_1-i_1} \cdots X_t^{n_t-i_t}\right)\\ &-\lambda\left(\sum_{(i_1,\ldots,i_t)\in S} X_1^{i_1} \cdots X_t^{i_t}\right) - (k-\lambda).\end{aligned}$$

Then a subset $D \subset G$ is a (v, k, λ) difference set in G if and only if $\kappa_D \in I$.

PROOF :

$$\begin{aligned}\phi_G(\kappa_D+I) = &\left(\sum_{(i_1,\ldots,i_t)\in D^*} g_1^{i_1}\cdots g_t^{i_t}\right)\left(\sum_{(i_1,\ldots,i_t)\in D^*} g_1^{n_1-i_1}\cdots g_t^{n_t-i_t}\right)\\ &-\lambda\left(\sum_{(i_1,\ldots,i_t)\in S} g_1^{i_1}\cdots g_t^{i_t}\right)-(k-\lambda)\\ =&\left(\sum_{(i_1,\ldots,i_t)\in D^*} g_1^{i_1}\cdots g_t^{i_t}\right)\left(\sum_{(i_1,\ldots,i_t)\in D^*} g_1^{-i_1}\cdots g_t^{-i_t}\right)\\ &-\lambda\left(\sum_{(i_1,\ldots,i_t)\in S} g_1^{i_1}\cdots g_t^{i_t}\right)-(k-\lambda)\\ =&DD^{(-1)}-\lambda G-(k-\lambda).\end{aligned}$$

Now

D is a (v,k,λ) difference set in G
$\Leftrightarrow DD^{(-1)}-\lambda G-(k-\lambda)=0$
$\Leftrightarrow \phi_G(\kappa_D+I)=0 \Leftrightarrow \kappa_D+I=0$
$\Leftrightarrow \kappa_D\in I.\square$

Note : Alternatively we can write

$$\begin{aligned}\kappa_D = &\left(\sum_{(i_1,\ldots,i_t)\in S}\alpha_{i_1\ldots i_t}X_1^{i_1}\ldots X_t^{i_t}\right)\left(\sum_{(i_1,\ldots,i_t)\in S}\alpha_{i_1\ldots i_t}X_1^{n_1-i_1}\ldots X_t^{n_t-i_t}\right)\\ &-\lambda\left(\sum_{(i_1,\cdots,i_t)\in S}X_1^{i_1}\cdots X_t^{i_t}\right)-(k-\lambda).\end{aligned}$$

where $\alpha=(\alpha_{i_1\ldots i_t}:(i_1,\ldots,i_t)\in S)$ is the point representation of D.

3. SYSTEM OF POLYNOMIAL EQUATIONS FOR DIFFERENCE SETS IN AN ABELIAN GROUP

The results of Section 2 can be rephrased to provide a criterion for (v,k,λ) difference sets in an abelian group of order v in terms of some polynomial equations. More specifically, we will find a set of polynomials in $\mathbb{C}\left[\{A_{i_1\cdots i_t}:(i_1,\ldots,i_t)\in S\}\right]$ whose zero set in $\mathbb{C}^{n_1\cdots n_t}$ is exactly the set of all the point representations of all (v,k,λ) difference sets in G.

First some terminology and preparation. For any $J \subset \mathbb{C}[X_1, \ldots, X_t]$, let $V(J) = \{(x_1, \ldots, x_t) \in \mathbb{C}^t : f(x_1, \ldots, x_t) = 0$ for all $f(X_1, \ldots, X_t) \in J\}$. For any $W \subset \mathbb{C}^t$, let $I(W) = \{f(X_1, \ldots, X_t) \in \mathbb{C}[X_1, \ldots, X_t] : f(x_1, \ldots, x_t) = 0$ for all $(x_1, \ldots, x_t) \in W\}$. Then it can easily be seen that $I(W)$ is an ideal in $\mathbb{C}[X_1, \ldots, X_t]$. For any ideal J of $\mathbb{C}[X_1, \ldots, X_t]$, the radical of J is given by $\sqrt{J} = \{f = f(X_1, \ldots, X_t) \in \mathbb{C}[X_1, \ldots, X_t] : f^n \in J$ for some positive integer $n\}$. It can be seen that for any ideal J of $\mathbb{C}[X_1, \ldots, X_t]$, $\sqrt{J}$ is an ideal of $\mathbb{C}[X_1, \ldots, X_t]$. An ideal J of $\mathbb{C}[X_1, \ldots, X_t]$ is called a radical ideal if $\sqrt{J} = J$. For the following famous theorem, see [4], p. 175.

***Theorem* 3.1** — *(Hilbert Nullstellensatz). If J is any ideal of $\mathbb{C}[X_1, \ldots, X_t]$ then $I(V(J)) = \sqrt{J}$.*

We will use the following corollary of Hilbert Nullstellensatz.

Corollary 3.1 — Let $f = f(X_1, \ldots, X_t) \in \mathbb{C}[X_1, \ldots, X_t]$ and J be a radical ideal of $\mathbb{C}[X_1, \ldots, X_t]$. Then $f \in J$ if and only if $f(x_1, \ldots, x_t) = 0$ for all $(x_1, \ldots, x_t) \in V(J)$.

In order to use Corollary 3.1, we prove the following:

Lemma 3.1 — The ideal $I = (X_1^{n_1} - 1, \ldots, X_t^{n_t} - 1)$ of $\mathbb{C}[X_1, \ldots, X_t]$ is a radical ideal.

PROOF : Clearly $I \subset \sqrt{I}$. Now let $f(X_1, \ldots, X_t) \in \sqrt{I}$ be any element. We want to show that $f = f(X_1, \ldots, X_t) \in I$. We can write

$$f(X_1, \ldots, X_t) = g(X_1, \ldots, X_t) + r(X_1, \ldots, X_t)$$

such that $g(X_1, \ldots, X_t) \in I$ and $r(X_1, \ldots, X_t) \in \mathbb{C}[X_1, \ldots, X_t]$ satisfies $r(X_1, \ldots, X_t) = 0$ or $\deg_{X_i} r(X_1, \ldots, X_t) < n_i$ for all $i = 1, 2, \ldots, t$.

It is enough to show that $r(X_1, \ldots, X_t) = 0$. We can write

$$r(X_1, \ldots, X_t) = \sum_{j=0}^{n_t - 1} r_j(X_1, \ldots, X_{t-1}) X_t^j$$

with $r_j(X_1, \ldots, X_{t-1}) \in \mathbb{C}[X_1, \ldots, X_{t-1}]$ such that for any $0 \leq j < n_t$, we have $r_j(X_1, \ldots, X_{t-1}) = 0$ or $\deg_{X_i} r_j(X_1, \ldots, X_{t-1}) < n_i$ for all $1 \leq i \leq t-1$. Consider any $(\xi_1, \ldots, \xi_{t-1}) \in \mathbb{C}^{t-1}$ with $\xi_i^{n_i} = 1$ for all $1 \leq i \leq t-1$. Since $f \in \sqrt{I} = I(V(I))$ and for all $0 \leq l \leq n_t - 1$, $\left(\xi_1, \ldots, \xi_{t-1}, e^{\frac{2\pi i l}{n_t}}\right) \in V(I)$, we have $f\left(\xi_1, \ldots, \xi_{t-1}, e^{\frac{2\pi i l}{n_t}}\right) = 0$. Moreover, since $g \in I$, $g\left(\xi_1, \ldots, \xi_{t-1}, e^{\frac{2\pi i l}{n_t}}\right) = 0$ for all $0 \leq l \leq n_t - 1$. Thus $r\left(\xi_1, \ldots, \xi_{t-1}, e^{\frac{2\pi i l}{n_t}}\right) = 0$ for all $l = 0, 1, \ldots, n_t - 1$. Assume $r(\xi_1, \ldots, \xi_{t-1}, X_t) \neq 0$. Since $\deg_{X_t} r(\xi_1, \ldots, \xi_{t-1}, X_t) < n_t$ and it has n_t distinct roots, we get a contradiction. Hence $r(\xi_1, \ldots, \xi_{t-1}, X_t) = 0$ and therefore for any

$0 \leq j < n_t$, we have $r_j(\xi_1, \ldots, \xi_{t-1}) = 0$ for any $(\xi_1, \ldots, \xi_{t-1}) \in \mathbb{C}^{t-1}$ with $\xi_i^{n_i} = 1$ for all $i = 1, 2, \ldots, t-1$. Iterating the argument with r replaced by r_j etc, we get that $r = 0$. □

Now we are prepared to discuss the main result of this paper. Let Δ denote the polynomial ring $\mathbb{C}[X_1, \ldots, X_t][\{A_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S\}]$ in $n_1 \cdots n_t$ independent variables $A_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S$ over $\mathbb{C}[X_1, \ldots, X_t]$ and let $U = \{(\xi_1, \ldots, \xi_t) \in \mathbb{C}^t : \xi_i^{n_i} = 1 \text{ for all } 1 \leq i \leq t\}$. To simplify the notation, let $A = (A_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S)$, $X = (X_1, \ldots, X_t)$. Also if $\alpha_{i_1 \cdots i_t} \in \mathbb{C}$ for all $(i_1, \ldots, i_t) \in S$, we let $\alpha = (\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S) \in \mathbb{C}^{n_1 \cdots n_t}$. Then we have the following:

Theorem 3.2 — *Let $\Psi = \Psi(X, A) \in \Delta$ be defined by*

$$\Psi = \left(\sum_{(i_1, \ldots, i_t) \in S} A_{i_1 \cdots i_t} X_1^{i_1} \cdots X_t^{i_t} \right) \left(\sum_{(i_1, \ldots, i_t) \in S} A_{i_1 \cdots i_t} X_1^{n_1 - i_1} \cdots X_t^{n_t - i_t} \right)$$
$$- \lambda \left(\sum_{(i_1, \ldots, i_t) \in S} X_1^{i_1} \cdots X_t^{i_t} \right) - (k - \lambda)$$

Then we have the following :

(1) For $\alpha = (\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S) \in \mathbb{C}^{n_1 \cdots n_t}$, α is a point representation of a subset of G if and only if α satisfies the system $P_{i_1 \cdots i_t}(A) = 0, (i_1, \ldots, i_t) \in S$ of polynomial equations where for $(i_1, \ldots, i_t) \in S, P_{i_1 \cdots i_t}(A) = A_{i_1 \cdots i_t}^2 - A_{i_1 \cdots i_t}$.

(2) For $\alpha = (\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S) \in \mathbb{C}^{n_1 \cdots n_t}$, α is a point representation of a (v, k, λ) difference set in G if and only if α satisfies the equations $P_{i_1 \cdots i_t}(A) = 0$ for all $(i_1, \ldots, i_t) \in S$, and $\Psi(\xi, A) = 0$ for all $\xi = (\xi_1, \ldots, \xi_t) \in U$.

PROOF : Note that (1) follows, as for any $\alpha = (\alpha_{i_1 \cdots i_t} : (i_1, \ldots, i_t) \in S) \in \mathbb{C}^{n_1 \cdots n_t}$,

$P_{i_1 \cdots i_t}(\alpha) = 0$ for all $(i_1, \ldots, i_t) \in S$
$\Leftrightarrow \alpha_{i_1 \cdots i_t} \in \{0, 1\}$ for all $(i_1, \ldots, i_t) \in S$
$\Leftrightarrow \alpha$ is a point representation of $D \subset G$ where
$D = \{(i_1 + n_1\mathbb{Z}, \ldots, i_t + n_t\mathbb{Z}) : (i_1, \ldots, i_t) \in S \text{ and } \alpha_{i_1 \cdots i_t} = 1\}$.

To prove (2), first note that $\kappa_D(X_1, \ldots, X_t) = \Psi(X, \alpha)$ where α is the point representation of

$D \subset G$. Thus, for any $\alpha \in \mathbb{C}^{n_1 \cdots n_t}$,

$$\begin{aligned}
&\alpha \text{ is a point representation of a } (v,k,\lambda) \text{ difference set D in } G \\
&\overset{\text{Theorem 2.2}}{\iff} \alpha \text{ is a point representation of } D \subset G \text{ and} \\
&\qquad \kappa_D(X_1,\ldots,X_t) \in I \\
&\iff \alpha \text{ is a point representation of } D \subset G \text{ and} \\
&\qquad \Psi(X,\alpha) \in I \\
&\overset{\text{by Theorem 3.2 (1)}}{\iff} P_{i_1 \cdots i_t}(\alpha) = 0 \text{ for all } (i_1,\ldots,i_t) \in S \text{ and} \\
&\qquad \Psi(X,\alpha) \in I \\
&\overset{\text{Theorem 3.1, Lemma 3.1}}{\iff} P_{i_1 \cdots i_t}(\alpha) = 0 \text{ for all } (i_1,\ldots,i_t) \in S \text{ and} \\
&\qquad \Psi(X,\alpha) \in I(V(I)) \\
&\overset{\text{since } U=V(I)}{\iff} P_{i_1 \cdots i_t}(\alpha) = 0 \text{ for all } (i_1,\ldots,i_t) \in S \text{ and} \\
&\qquad \Psi(\xi,\alpha) = 0 \text{ for all } \xi \in U. \square
\end{aligned}$$

Note : The ideas of this section are analogous to interpolation of polynomials, in the sense that every postulation of a zero of a polynomial puts a condition on the parameters occurring in its coefficients.

Remark on $\mathbb{C}$-algebra homomorphisms

For any $\xi = (\xi_1,\ldots,\xi_t) \in U$, let $\theta_{(\xi_1,\ldots,\xi_t)} : \mathbb{C}[X_1,\ldots,X_t] \to \mathbb{C}$ be a $\mathbb{C}$-algebra homomorphism defined by $\theta_{(\xi_1,\ldots,\xi_t)}(f(X_1,\ldots,X_t)) = f(\xi_1,\ldots,\xi_t)$ and let $\theta^{\Delta}_{(\xi_1,\ldots,\xi_t)} : \Delta \to \Delta$ be the unique extension of $\theta_{(\xi_1,\ldots,\xi_t)}$ to a $\mathbb{C}$-algebra homomorphism such that $\theta^{\Delta}_{(\xi_1,\ldots,\xi_t)}(A_{i_1 \cdots i_t}) = A_{i_1 \cdots i_t}$ for all $(i_1,\ldots,i_t) \in S$. That is, for any $\Omega(X,A) \in \Delta$,

$$\theta^{\Delta}_{(\xi_1,\ldots,\xi_t)}(\Omega(X,A) = \Omega(\xi,A).$$

Moreover, for any $\alpha \in \mathbb{C}^{n_1 \cdots n_t}$, let $\tau_\alpha : \Delta \to \mathbb{C}[X_1,\ldots,X_t]$ be a ring homomorphism defined by $\tau_\alpha(\Omega(X,A)) = \Omega(X,\alpha)$ for all $\Omega(X,A) \in \Delta$. Note that if α is the point representation of $D \subset G$ and $\xi = (\xi_1,\ldots,\xi_t) \in U$,

$$\begin{aligned}
\kappa_D(X_1,\ldots,X_t) &= \tau_\alpha(\Psi(X,A)), \\
\Psi(\xi,A) &= \theta^{\Delta}_{(\xi_1,\ldots,\xi_t)}(\Psi(X,A)), \\
\Psi(\xi,\alpha) &= \theta_{(\xi_1,\ldots,\xi_t)}(\tau_\alpha(\Psi(X,A))) = \theta_{(\xi_1,\ldots,\xi_t)}(\kappa_D(X_1,\ldots,X_t)) \\
\Psi(\xi,\alpha) &= \tau_\alpha\Big(\theta^{\Delta}_{(\xi_1,\ldots,\xi_t)}(\Psi(X,A)\Big) = \tau_\alpha(\Psi(\xi,A)).
\end{aligned}$$

Hence, in view of (2.1$*$), it follows that if α is the point representation of $D \subset G$ and $\xi = (\xi_1, \dots, \xi_t) \in U$, then

$$\begin{aligned}\Psi(\xi,\alpha) =& \theta_{(\xi_1,\dots,\xi_t)}(\tau_\alpha(\Psi(X,A)))\\ =&\theta_{(\xi_1,\dots,\xi_t)}\left(\rho_G(D)\right)\theta_{(\xi_1,\dots,\xi_t)}\left(\rho_G(D^{(-1)})\right)\\ &-\lambda\,\theta_{(\xi_1,\dots,\xi_t)}\left(\rho_G(G)\right)-(k-\lambda).\end{aligned} \tag{3.1$*$}$$

Alternatively, as a consequence of the conclusions of Theorem 3.2, for a subset D of G, D is a (v, k, λ) difference set if and only if

$$\begin{aligned}&\rho_G(D)(\xi_1,\dots,\xi_t)\rho_G(D^{-1})(\xi_1,\dots,\xi_t)-\lambda\rho_G(G)(\xi_1,\dots,\xi_t)-(k-\lambda)=0\\ &\text{for all } (\xi_1,\dots,\xi_t)\in U.\end{aligned} \tag{3.2$*$}$$

Sharpening of Ryser Condition : A necessary condition for the existence of (v, k, λ) difference set is $\lambda(v-1) = k(k-1)$, as discovered by Ryser. Note that this condition is nothing but $\theta^{\Delta}_{(\xi_1,\dots,\xi_t)}(\Psi)(\alpha) = 0$ for $(\xi_1, \dots, \xi_t) = (1, \dots, 1)$, where α is the point representation of some set $D \subset G$ of size k. The condition is clearly not sufficient. However, when an abelian group G of order v is given as a direct sum of cyclic groups, the necessary as well as sufficient condition for existence of a (v, k, λ) difference set in G is the consistency of the system of equations $P_{i_1\cdots i_t}(A) = 0$ for all $(i_1, \dots, i_t) \in S$ and $\theta^{\Delta}_{(\xi_1,\dots,\xi_t)}(\Psi)(A) = 0$ for all $(\xi_1, \dots, \xi_t) \in U$ in the variables $A = (A_{i_1\cdots i_t} : (i_1, \dots, i_t) \in S)$. In the parlance of Gröbner bases (see page 171 of [4]), the condition be reformulated as:

Gröbner Basis Version of Existence Problem : There exists a (v, k, λ) difference set in G if and only if the reduced Gröbner basis (in any monomial order) of the ideal generated by $P_{i_1\cdots i_t}(A)$ for all $(i_1, \dots, i_t) \in S$ and $\theta^{\Delta}_{(\xi_1,\dots,\xi_t)}(\Psi)(A)$ for all $(\xi_1, \dots, \xi_t) \in U$ in $\mathbb{C}\left[\{A_{i_1\cdots i_t} : (i_1, \dots, i_t) \in S\}\right]$ is not equal to $\{1\}$.

4. Generalization of the Criteria

The criteria developed in Sections 2 and 3 can be generalized to generalized difference sets in finite abelian groups. Following [3], we proceed to define a generalized difference set thus. For a finite group G_0 of order v, let $D_0, M_0 \subset G_0$ be such that $|D_0| = k > 1, |M_0| > 0$. For any $g \in G_0$, let $\lambda_g = |\{(d_1, d_2) \in D_0 \times D_0 : g = d_1 d_2^{-1}\}|$. If λ_1, λ_2 are nonnegative integers, D_0 is called a $(v, |M_0|, k, \lambda_1, \lambda_2)$-*generalized difference set* of G_0 related to M_0 if for any nonidentity element $g \in G_0$

$$\lambda_g = \begin{cases} \lambda_1, & \text{if } g \in M_0;\\ \lambda_2, & \text{if } g \notin M_0.\end{cases}$$

This is a generalization of a difference set in the following sense. If $M_0 = \{e\}$ for the identity element e of G_0 and $\lambda_1 = 0$ then any $(v, |M_0|, k, \lambda_1, \lambda_2)$-generalized difference set of G_0 related to M_0 is exactly a (v, k, λ_2) difference set of G_0. Other special cases of generalized difference set give several important variations of a difference set in G_0. For instance, if M_0 is a subgroup of G_0 and $\lambda_1 = 0$, then D_0 is called a $(v, |M_0|, k, \lambda_2)$ *relative difference set* of G_0 with relative to M_0. We say D_0 is a $(v, k, \lambda_1, \lambda_2)$ partial difference set in G_0 if $M_0 = D_0$. Generalized difference sets are helpful in computation of autocorrelation of certain arrays, see [3]. Partial difference sets have connections with strongly regular graphs, see [8]. With this in mind, we state the polynomial criterion for the generalized difference sets as a consequence of the group ring criterion ([3], Theorem 2), the proof is analogous to Theorem 3.2.

***Theorem* 4.1** — *Let $M \subset G$ and let $\Psi^* = \Psi^*(X, A) \in \Delta$ be defined by*

$$\Psi^* = \begin{cases} \left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S} A_{i_1\cdots i_t} X_1^{i_1}\cdots X_t^{i_t}\right)\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S} A_{i_1\cdots i_t} X_1^{n_1-i_1}\cdots X_t^{n_t-i_t}\right) \\ -\lambda_1\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in M^*} X_1^{i_1}\cdots X_t^{i_t}\right) \\ -\lambda_2\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S\setminus M^*} X_1^{i_1}\cdots X_t^{i_t}\right) - (k-\lambda_1), & if\ e \in M; \\ \\ \left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S} A_{i_1\cdots i_t} X_1^{i_1}\cdots X_t^{i_t}\right)\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S} A_{i_1\cdots i_t} X_1^{n_1-i_1}\cdots X_t^{n_t-i_t}\right) \\ -\lambda_1\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in M^*} X_1^{i_1}\cdots X_t^{i_t}\right) \\ -\lambda_2\left(\displaystyle\sum_{(i_1,\ldots,i_t)\in S\setminus M^*} X_1^{i_1}\cdots X_t^{i_t}\right) - (k-\lambda_2), & if\ e \notin M. \end{cases}$$

Then we have the following :

For $\alpha = (\alpha_{i_1\ldots i_t} : (i_1, \ldots, i_t) \in S) \in \mathbb{C}^{n_1\cdots n_t}$, α is a point representation of a $(v, |M|, k, \lambda_1, \lambda_2)$ generalized difference set in G related to M if and only if $P_{i_1\cdots i_t}(\alpha) = 0$ for all $(i_1, \ldots, i_t) \in S$ and $\Psi^*(\xi, \alpha) = 0$ for all $\xi = (\xi_1, \ldots, \xi_t) \in U$.

5. Illustrations of the Criteria

In this section, we illustrate the use of the criteria developed in Sections 2 and 3. The purpose of the illustrations is just to show how the ideas developed in previous sections can potentially be used.

As the outcomes of these illustrations are well known or can be proved by other means, some of the arguments, which are repetitive in nature, are left to the reader.

Illustration 1 :

Let $G = \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$. We verify that the subset $D = \{(0,1),(0,2),(0,3),(1,0),(2,0),(3,0)\}$ of G is a $(16,6,2)$ difference set in G.

Method 1 (Ideal Membership Problem) : By Theorem 2.2, we need to see that $\kappa_D(X_1, X_2) \in I = (X_1^4 - 1, X_2^4 - 1)$. This can be done by verifying that the remainder of $\kappa_D(X_1, X_2)$ mod I is 0. The following Macaulay 2 code does this.

```
R= CC[x_1,x_2, MonomialOrder=> Lex]
I=ideal(x_1^4-1,x_2^4-1)
G=(x_1^3+x_1^2+x_1+1)*(x_2^3+x_2^2+x_2+1)
D=x_1^3+x_1^2+x_1+x_2^3+x_2^2+x_2
D1=(x_1^3*x_2^4+x_1^2*x_2^4+x_1*x_2^4+x_1^4*x_2^3
+x_1^4*x_2^2+x_1^4*x_2)
v=16
k=6
lambda=2
D*D1-(k-lambda)-lambda*G
oo%I
```

Method 2 (Polynomial Criterion) : The point representation $\alpha = (\alpha_{ij} : (i,j) \in S)$ of D is given by

$$\begin{aligned} \alpha_{01} = \alpha_{02} = \alpha_{03} = \alpha_{10} = \alpha_{20} = \alpha_{30} &= 1 \\ \alpha_{ij} &= 0 \text{ elsewhere.} \end{aligned}$$

As $\alpha_{ij} \in \{0,1\}$, $P_{ij}(\alpha) = 0, (i,j) \in S$.

Next, we verify that $\theta^{\Delta}_{(\xi_1,\xi_2)}(\Psi)(\alpha) = 0$ for all $(\xi_1, \xi_2) \in U$, where $U = \{\pm 1, \pm i\}^2$.

For sake of brevity, we verify one of the equations of Theorem 3.2 when $(\xi_1, \xi_2) = (i, -i) \in U$. The equations corresponding to the remaining 15 elements of U can be verified to establish that D is a $(16,6,2)$ difference set in G.

Note that $\theta^{\Delta}_{(\xi_1,\xi_2)}(\Psi)(\alpha) = \Psi(i, -i, \alpha)$. Also

$$\begin{aligned}\Psi(u, v, \alpha) = &\left(u^0v^1 + u^0v^2 + u^0v^3 + u^1v^0 + u^2v^0 + u^3v^0\right)\\ &\times \left(u^4v^3 + u^4v^2 + u^4v^1 + u^3v^4 + u^2v^4 + u^1v^4\right)\\ &- 2\left(\sum_{0\leq i\leq 3, 0\leq j\leq 3} u^iv^j\right) - (6-2).\end{aligned}$$

In particular, when $(u, v) = (i, -i)$, since

$$\sum_{0\leq r\leq 3, 0\leq s\leq 3} i^r(-i)^s = \left(\sum_{r=0}^{3} i^r\right)\left(\sum_{s=0}^{3}(-i)^s\right) = (0)(0),$$

we get

$$\begin{aligned}\Psi(i, -i, \alpha) =&(-i-1+i+i-1-i)(i-1-i+i-1-i)\\ &-2(0)-(6-2)\\ =&0.\end{aligned}$$

The reader may also verify directly by definition that D is a $(16, 6, 2)$ difference set in G.

Illustration 2

Let $D = \{(0, 1), (0, 2), (0, 3), (1, 0), (2, 0), (1, 1)\} \subset G = \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$. We can show that D is not a $(16, 6, 2)$ difference set in G just by verifying that $\Psi(1, -1, \alpha) = -4 \neq 0$ for the point representation α of D.

Illustration 3 (An application to bent functions) :

This illustration provides the glimpse of the use of Theorem 3.2 to prove some results about bent functions. Let $t = 2m$ for a positive integer m and $\beta : (\mathbb{Z}/2\mathbb{Z})^t \to (\mathbb{Z}/2\mathbb{Z})$ be a Boolean function defined by $\beta(x_1, \ldots, x_m, y_1, \ldots, y_m) = \sum_{i=1}^{m} x_iy_i$ where $x_i, y_i \in (\mathbb{Z}/2\mathbb{Z})$ are any elements for any $i = 1, \ldots, m$. We illustrate the proof, using Theorem 3.2, that β is a bent function with $|D| = 2^{(t-1)} - 2^{(t-2)/2}$ where $D =$ support of β.

The proof can be given by induction on m. The cases $m = 1, 2, 3$ can be verified easily. For the inductive step, let $m \geq 4$. Then we can write $m = m_1 + m_2$ with min$(m_1, m_2) \geq 2$. For any $i \in \{1, 2\}$, let $t_i = 2m_i$, $G_i = (\mathbb{Z}/2\mathbb{Z})^{t_i}$ and let $\beta_i : G_i \to (\mathbb{Z}/2\mathbb{Z})$ be defined by

$\beta_1(g_1) = \sum_{i=1}^{m_1} x_iy_i$ for any $g_1 \in G_1$, where $g_1 = (x_1, \ldots, x_{m_1}, y_1, \ldots, y_{m_1})$; $x_i, y_j \in (\mathbb{Z}/2\mathbb{Z})$ for all $1 \leq i, j \leq m_1$ and $\beta_2(g_2) = \sum_{i=1}^{m_2} x_{m_1+i}y_{m_1+i}$ for any $g_2 = (x_{m_1+1}, \ldots, x_m, y_{m_1+1}, \ldots, y_m)$;

$x_i, y_j \in (\mathbb{Z}/2\mathbb{Z})$ for all $m_1+1 \leq i, j \leq m$. By induction hypothesis, β_1, β_2 are bent functions with $|D_i| = 2^{(t_i-1)} - 2^{(t_i-2)/2}$ where $D_i =$ support of β_i.

Let $G = G_1 \times G_2$. Identifying $g = (g_1, g_2) \in G$ with $(x_1, \ldots, x_m, y_1, \ldots, y_m) \in (\mathbb{Z}/2\mathbb{Z})^t$, G gets identified with $(\mathbb{Z}/2\mathbb{Z})^t$. Then $\beta(g_1, g_2) = \beta_1(g_1) + \beta_2(g_2)$ for any $g_1 \in G_1, g_2 \in G_2$. We need to show that β is a bent function with domain G and $|D| = 2^{(t-1)} - 2^{(t-2)/2}$ for $D =$ support of β.

We start the proof with:

Observations

(1) Let $H_i \subset G_i = (\mathbb{Z}/2\mathbb{Z})^{r_i}$ for $i \in \{1,2\}$ and let $H = H_1 \times H_2 \subset G_1 \times G_2$. Then

$$\rho_{(G_1 \times G_2)}\left(H_1 \times H_2\right) = \left(\rho_{G_1}(H_1)\right)\left(\rho_{G_2}(H_2)\right).$$

(2) Let $\xi \in \mathbb{C}$ be a primitive n^{th} root of unity. Then $\sum_{i=0}^{n-1} \xi^i = 0$.

(3) By Observations (1) and (2), if $(\xi_1, \ldots, \xi_t) \in \{-1,1\}^t \backslash \{(1, \ldots, 1)\}$, then $\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(G)\right) = \sum_{(i_1,\cdots,i_t)\in S} \xi_1^{i_1} \cdots \xi_t^{i_t} = 0$.

Now D_i is a $(2^{t_i}, 2^{(t_i-1)} - 2^{(t_i-2)/2}, 2^{(t_i-2)} - 2^{(t_i-2)/2})$ difference set for $i \in \{1,2\}$. In order to show that β is a bent function, it is enough to show that D satisfies the conditions in Theorem 3.2 (2). Let α be the point representation of D. Then by Theorem 3.2 (1), $P_{i_1\ldots i_t}(\alpha) = 0$ for all $(i_1, \ldots, i_t) \in S$. Using (3.1$*$), we will show that $\Psi(\xi, \alpha) = 0$ for all $\xi = (\xi_1, \ldots, \xi_t) \in U$. Now $D = (D_1 \times \overline{D_2}) \cup (\overline{D_1} \times D_2)$, where $\overline{D_i}$ is the complement of D_i in $(\mathbb{Z}/2\mathbb{Z})^{t_i}$ for all $i \in \{1,2\}$, and the union is disjoint. Hence by Observation (1)

$$\begin{aligned}\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(D)\right) = &\Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(\overline{D_2})\right)\Big)\\ &+\Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(\overline{D_1})\right)\Big)\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)\Big).\end{aligned}$$

Therefore,

$$\begin{aligned}&\Big(\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(D)\right)\Big)^2\\ &= \Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)^2\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(\overline{D_2})\right)\Big)^2\\ &+\Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(\overline{D_1})\right)\Big)^2\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)\Big)^2\\ &+2\Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(\overline{D_2})\right)\Big)\\ &\Big(\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(\overline{D_1})\right)\Big)\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)\Big)\end{aligned} \tag{5.1}$$

We make three cases.

Case (i):

$$(\xi_1,\dots,\xi_{t_1}) \in \{-1,1\}^{t_1} \setminus \{(1,\dots,1)\} \text{ and}$$
$$(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)}) \in \{-1,1\}^{t_2} \setminus \{(1,\dots,1)\}.$$

In view of Observation (3), $\theta_{(\xi_1,\dots,\xi_{t_1})}(\rho_{G_1}(\overline{D_1})) = -\theta_{(\xi_1,\dots,\xi_{t_1})}(\rho_{G_1}(D_1))$ and $\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}$ $(\rho_{G_2}(\overline{D_2})) = -\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}(\rho_{G_2}(D_2))$. Since $n_i = 2$ for all $i = 1,\dots,t_1$ in the equalities of Theorem 3.2, it follows that $\theta_{(\xi_1,\dots,\xi_{t_1})}(\rho_{G_1}(D_1^{(-1)})) = \theta_{(\xi_1,\dots,\xi_{t_1})}(\rho_{G_1}(D_1))$.

Similarly $\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}(\rho_{G_2}(D_2^{(-1)})) = \theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}(\rho_{G_2}(D_2))$ and $\theta_{(\xi_1,\dots,\xi_t)}$ $(\rho_G(D^{(-1)})) = \theta_{(\xi_1,\dots,\xi_t)}(\rho_G(D))$. Since each D_i is a $(2^{t_i}, 2^{(t_i-1)} - 2^{(t_i-2)/2}, 2^{(t_i-2)} - 2^{(t_i-2)/2})$ difference set for $i \in \{1,2\}$, as a consequence of $(3.1*)$ and Observation (3)

$$(\theta_{(\xi_1,\dots,\xi_{t_1})}(\rho_{G_1}(D_1)))^2 = 2^{(t_1-1)} - 2^{(t_1-2)} \text{ and}$$
$$(\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}(\rho_{G_2}(D_2)))^2 = 2^{(t_2-1)} - 2^{(t_2-2)}.$$

Hence by (5.1),

$$\begin{aligned}\Big(\theta_{(\xi_1,\dots,\xi_t)}\left(\rho_G(D)\right)\Big)^2 =&4\Big(\theta_{(\xi_1,\dots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)^2\Big(\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)\Big)^2\\ =&4\left(2^{(t_1-1)} - 2^{(t_1-2)}\right)\left(2^{(t_2-1)} - 2^{(t_2-2)}\right)\\ =&\left(2^{(t-1)} - 2^{(t-2)}\right) = k - \lambda\end{aligned}$$

where $k = 2^{t-1} - 2^{(t-2)/2}, \lambda = 2^{t-2} - 2^{(t-2)/2}$. Since $(\xi_1,\dots,\xi_t) \in \{-1,1\}^t \setminus \{(1,\dots,1)\}$, $\theta_{(\xi_1,\dots,\xi_t)}\left(\rho_G(G)\right) = 0$, and hence, by $(3.1*)$, $\Psi(\xi,\alpha) = 0$ for the point representation α of D.

Case (ii) :

$$(\xi_1,\dots,\xi_{t_1}) = (1,\dots,1) \in \mathbb{C}^{t_1} \text{ and}$$
$$(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)}) \in \{-1,1\}^{t_2} \setminus \{(1,\dots,1)\}.$$

Then

$$\begin{aligned}\theta_{(\xi_1,\dots,\xi_{t_1})}\left(\rho_{G_1}(G_1)\right) =&2^{t_1};\\ \theta_{(\xi_1,\dots,\xi_{t_1})}\left(\rho_{G_1}(\overline{D_1})\right) =&2^{t_1} - \theta_{(\xi_1,\dots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right);\\ \theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(G_2)\right) =&0;\\ \theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(\overline{D_2})\right) =&-\theta_{(\xi_{(t_1+1)},\dots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right).\end{aligned}$$

Hence by (5.1),

$$\begin{aligned}&\Big(\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(D)\right)\Big)^2\\ &=\Big\{\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)^2+\Big(2^{t_1}-\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)^2\\ &-2\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big(2^{t_1}-\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)\Big)\Big\}\Big(\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)\Big)^2.\end{aligned}$$

By (3.1*) and Observation (3), $\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)^2=2^{t_2-1}-2^{t_2-2}$. Also $\theta_{(\xi_1,\ldots,\xi_{t_1})}$ $(\rho_{G_1}(D_1))=|D_1|=2^{t_1-1}-2^{(t_1-2)/2}$. By substituting these in the above expression and then expanding, we get

$$\begin{aligned}&\left(\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(D)\right)\right)^2\\ &=\left(2^{t_2-1}-2^{t_2-2}\right)\left[4\left(2^{t_1-1}-2^{(t_1-2)/2}\right)^2+2^{2t_1}-4(2^{t_1})\left(2^{t_1-1}-2^{(t_1-2)/2}\right)\right]\\ &=\left(2^{t_2-1}-2^{t_2-2}\right)2^{t_1}=(k-\lambda)\end{aligned}$$

where $k=2^{t-1}-2^{(t-2)/2}$ and $\lambda=2^{t-2}-2^{(t-2)/2}$. Since $(\xi_1,\ldots,\xi_t)\neq(1,\ldots,1)$, we see that $\theta_{(\xi_1,\ldots,\xi_t)}\left(\rho_G(G)\right)=0$ and hence by $(3.1*)$, $\Psi(\xi,\alpha)=0$ for the point representation α of D.

Similar argument works when $(\xi_1,\ldots,\xi_{t_1})\in\{-1,1\}^{t_2}\backslash\{(1,\ldots,1)\}$ and $(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})=(1,\ldots,1)\in\mathbb{C}^{t_2}$.

Case (iii):

$$\begin{aligned}(\xi_1,\ldots,\xi_{t_1})&=(1,\ldots,1)\in\mathbb{C}^{t_1}\text{ and}\\ (\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})&=(1,\ldots,1)\in\mathbb{C}^{t_2}.\end{aligned}$$

Then we have

$$\begin{aligned}&\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(D_1)\right)=|D_1|=2^{t_1-1}-2^{(t_1-2)/2};\\ &\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(D_2)\right)=|D_2|=2^{t_2-1}-2^{(t_2-2)/2};\\ &\theta_{(\xi_1,\ldots,\xi_{t_1})}\left(\rho_{G_1}(\overline{D_1})\right)=|\overline{D_1}|=2^{t_1}-2^{t_1-1}+2^{(t_1-2)/2}=2^{t_1-1}+2^{(t_1-2)/2};\\ &\theta_{(\xi_{(t_1+1)},\ldots,\xi_{(t_1+t_2)})}\left(\rho_{G_2}(\overline{D_2})\right)=|\overline{D_2}|=2^{t_2}-2^{t_2-1}+2^{(t_2-2)/2}=2^{t_2-1}+2^{(t_2-2)/2}.\end{aligned}$$

Substituting in (5.1), in view of $(3.1*)$, showing D is a $(2^{t_1+t_2},2^{t_1+t_2-1}-2^{(t_1+t_2-2)/2},2^{t_1+t_2-2}-2^{(t_1+t_2-2)/2})$ difference set reduces to proving the following equality :

If $t_1, t_2 \geq 4$ are even integers then

$$\begin{aligned}
&\left(2^{t_2-1} + 2^{(t_2-2)/2}\right)^2 \left(2^{t_1-1} - 2^{(t_1-2)/2}\right)^2 + \left(2^{t_1-1} + 2^{(t_1-2)/2}\right)^2 \left(2^{t_2-1} - 2^{(t_2-2)/2}\right)^2 \\
&+ 2\left(2^{2t_1-2} - 2^{t_1-2}\right)\left(2^{2t_2-2} - 2^{t_2-2}\right) \\
&= 2^{t_1+t_2}\left(2^{t_1+t_2-2} - 2^{(t_1+t_2-2)/2}\right) + \left(2^{t_1+t_2-1} - 2^{t_1+t_2-2}\right).
\end{aligned}$$

Now to prove this equality,

$$\begin{aligned}
L.H.S. =&\left(2^{2t_1-2} + 2^{t_1-2} - 2^{\frac{3t_1}{2}-1}\right)\left(2^{2t_2-2} + 2^{t_2-2} + 2^{\frac{3t_2}{2}-1}\right) \\
&+ \left(2^{2t_1-2} + 2^{t_1-2} - 2^{\frac{3t_1}{2}-1} + 2\,2^{\frac{3t_1}{2}-1}\right)\left(2^{2t_2-2} + 2^{t_2-2} - 2^{\frac{3t_2}{2}-1}\right) \\
&+ 2\left(2^{2t_1+2t_2-4} - 2^{2t_1+t_2-4} - 2^{t_1+2t_2-4} + 2^{t_1+t_2-4}\right).
\end{aligned}$$

Simplifying further,

$$\begin{aligned}
L.H.S. =&\left(2^{2t_1-2} + 2^{t_1-2} - 2^{\frac{3t_1}{2}-1}\right)\left(2^{2t_2-1} + 2^{t_2-1}\right) + 2^{\frac{3t_1}{2}+2t_2-2} \\
&+ 2^{\frac{3t_1}{2}+t_2-2} - 2^{\frac{3t_1}{2}+\frac{3t_2}{2}-1} + 2^{2t_1+2t_2-3} - 2^{2t_1+t_2-3} \\
&- 2^{t_1+2t_2-3} + 2^{t_1+t_2-3}.
\end{aligned}$$

More simplification gives

$$\begin{aligned}
L.H.S. =&2^{2t_1+2t_2-3} + 2^{2t_1+t_2-3} + 2^{t_1+2t_2-3} + 2^{t_1+t_2-3} - 2^{\frac{3t_1}{2}+2t_2-2} \\
&- 2^{\frac{3t_1}{2}+t_2-2} + 2^{\frac{3t_1}{2}+2t_2-2} + 2^{\frac{3t_1}{2}+t_2-2} - 2^{\frac{3t_1}{2}+\frac{3t_2}{2}-1} \\
&+ 2^{2t_1+2t_2-3} - 2^{2t_1+t_2-3} - 2^{t_1+2t_2-3} + 2^{t_1+t_2-3} \\
=&2^{2t_1+2t_2-2} + 2^{t_1+t_2-2} - 2^{\frac{3t_1}{2}+\frac{3t_2}{2}-1} \\
=&R.H.S.
\end{aligned}$$

This proves that β is a bent function. □

Conclusion

In this paper, we have proved two algebraic criteria for a (v, k, λ) difference set in a given abelian group of order v. Illustrations are provided indicating how they can be applied. Further applications are being planned.

ACKNOWLEDGEMENT

Both the authors thank the support from FIST Programme vide SR/FST/MSI-090/2013 of DST, Govt. of India. The second author thanks UGC, Govt of India for the support under JRF Programme (SR. No. 2061540979, Ref. No. 21/06/2015(1)EU-V R. No. 426800). Both the authors thank S. Gangopadhyay and B. Mandal of IIT, Roorkee for stimulating discussions.

REFERENCES

1. T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, **Vol. 1** Cambridge University Press, Cambridge (1999).
2. R. C. Bose On the construction of balanced incomplete block designs, *Ann. Eugenic.*, **9** (1939), 358-399.
3. X. Cao and D. Sun, Some nonexistence results on generalized difference sets, *Appl. Math. Lett.*, **21**(8) (2008), 797-802.
4. D. Cox, J. Little, and D. O'Shea D. *Ideals, varieties and algorithms*, Springer Verlag, New York Inc (1992).
5. B. Felszeghy, B. Ráth, and L. Rónyai, The lex game and some applications, *J. Symb. Comput.*, **41** (2006), 663-681.
6. B. Felszeghy and L. Rónyai, *Some meeting points of Gröbner bases and combinatorics*, *Algorithmic Algebraic Combinatorics and Gröbner bases*, (M. Klin, G. A. Jones, A. Jurisic, M. Muzychuk, I. Ponomarenko, Editors), Springer-Verlag, Berlin Heidelberg (2009), 207-227.
7. M. Kreuzner and L. Robbiano, *Computational commutative algebra 2*, Springer, (2005).
8. S. Ma, A survey of partial difference sets, *Design Code Cryptogr*, **4** (1994), 221-261.
9. L. Rónyai and T. Mészáros, *Some combinatorial applications of Gröbner bases*, Algebraic informatics (Franz Winkler Ed.), 4th International Conference, CAI 2011, Linz, Proceedings; Springer LNCS 6742, Springer-Verlag, Berlin Heidelberg (2011), 65-83.
10. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377-385.
11. D. R. Stinson, *Combinatorial designs : Construction and analysis,* Springer Verlag, New York Inc (2004).