www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. x No. x (2017), pp. xx-xx.

www.ui.ac.ir

BINARY SEQUENCE/ARRAY PAIRS VIA DIFFERENCE SET PAIRS : A RECURSIVE APPROACH

K. T. ARASU*, ANIKA GOYAL AND ABHISHEK PURI

Communicated by Behruz Tayfeh Rezaie

Abstract. Binary array pairs with optimal/ideal correlation values and their algebraic counterparts "difference set pairs" (DSPs) in abelian groups are studied. In addition to generalizing known 1-dimensional (sequences) examples, we provide four new recursive constructions, unifying previously obtained ones. Any further advancements in the construction of binary sequences/arrays with optimal/ideal correlation values (equivalently cyclic/abelian difference sets) would give rise to richer classes of DSPs (and hence binary perfect array pairs). Discrete signals arising from DSPs find applications in cryptography, CDMA systems, radar and wireless communications.

1. Introduction

Binary sequence pairs give rise to a class of discrete signals and hence have received considerable attention by several researchers (e.g. see [1, 2, 3, 4]). Sequence pairs can be used in mismatched filtering systems (see [5] for more on the original discussion on these). Use of discrete signals with desirable correlation properties in cryptography, radar, wireless communications and CDMA (Code Division Multiple Access) is explained at length in [6, 7].

Along the lines of [2, 3], we study the aforementioned objects in a more general set-up (so-called "binary array pairs") via their combinatorial counterparts "difference set pairs in abelian groups".

An r-dimensional "matrix" $\mathbf{A} = (a[j_1, j_2, \ldots, j_r])$ with $0 \leq j_i < s_i, 1 \leq i \leq r$ is called an $s_1 \times s_2 \times \cdots \times s_r$ *array*. We call $v = s_1 s_2 \cdots s_r$ as the *energy* of the array. Such an array is said to be binary if all entries in the array belong to $\{-1, 1\}$. An 1-dimensional array is simply called a sequence.

MSC(2010): Primary: 05B10; Secondary: 05B30, 11T22, 51E30, 94C30.

Keywords: autocorrelation, binary sequence, perfect sequence pair, difference set pair.

Received: 16 February 2015, Accepted: 06 September 2016.

*Corresponding author.

Given two binary arrays $\mathbf{A} = (a[j_1, j_2, \ldots, j_r])$ and $\mathbf{B} = (b[j_1, j_2, \ldots, j_r])$, we define :

(i) 'Auto-correlation' coefficient γ for $\mathbf{A}$ at $(\tau_1, \tau_2, \ldots, \tau_r)$ as follows :

$$\gamma_{\mathbf{A}}(\tau_1, \tau_2, \ldots, \tau_r) = \sum_{j_1=0}^{s_1-1} \cdots \sum_{j_r=0}^{s_r-1} a\,(j_1, j_2, \ldots, j_r)\, a\,(j_1 + \tau_1, j_2 + \tau_2, \ldots, j_r + \tau_r) \tag{1.1}$$

(where the i^{th} index is read modulo s_i.)

(ii) 'Cross-correlation' coefficient γ between array pair $(\mathbf{A}, \mathbf{B})$ at $(\tau_1, \ldots, \tau_r)$ as follows :

$$\gamma_{\mathbf{A},\mathbf{B}}\,(\tau_1, \ldots, \tau_r) = \sum_{j_1=0}^{s_1-1} \cdots \sum_{j_r=0}^{s_r-1} a\,(j_1, j_2, \ldots, j_r)\, b\,(j_1 + \tau_1, j_2 + \tau_2, \ldots, j_r + \tau_r) \tag{1.2}$$

(where the i^{th} index is read modulo s_i.)

It is a well known fact that $\gamma_{\mathbf{A}}(\tau) \equiv v \pmod 4$ for all $\tau \neq 0$ in one dimensional case. (e.g. see [8]).

A $s_1 \times s_2 \times \cdots \times s_r$ binary array $\mathbf{A}$ is said to be 'balanced' if :

$$\{|\ \{(j_1, j_2, \ldots, j_r) | a(j_1, j_2, \ldots, j_r) = 1\}\ |,\ |\ \{(j_1, j_2, \ldots, j_r) | a(j_1, j_2, \ldots, j_r) = -1\}\ |\}$$

$$= \begin{cases} \{\frac{v}{2}\} & if\ v\ is\ even \\ \{\frac{v+1}{2}, \frac{v-1}{2}\} & if\ v\ is\ odd \end{cases} \tag{1.3}$$

A binary array pair $(\mathbf{A}, \mathbf{B})$ is said to be 'balanced' if at least one of $\mathbf{A}$ or $\mathbf{B}$ is balanced.

A binary array $\mathbf{A}$ is said to be ideal if:

$$\gamma_{\mathbf{A}}(\tau_1, \tau_2, \ldots, \tau_r) = \begin{cases} 0 & if\ v \equiv 0 \pmod 4 \\ 1 & if\ v \equiv 1 \pmod 4 \\ -1 & if\ v \equiv 3 \pmod 4 \end{cases} \tag{1.4}$$

for all $(\tau_1, \tau_2, \ldots, \tau_r) \neq (0, 0, \ldots, 0)$.

Such arrays are also referred to as 'perfect' arrays in the literature. For more on these perfect arrays, for instance, refer [9]. A binary array pair $(\mathbf{A}, \mathbf{B})$ is said to be ideal if $\gamma_{\mathbf{A},\mathbf{B}}(\tau_1, \tau_2, \ldots, \tau_r)$ is constant and $\gamma_{\mathbf{A},\mathbf{B}}(\tau_1, \tau_2, \ldots, \tau_r)\ \epsilon\ \{-1, 0, 1\}$ for all $(\tau_1, \tau_2, \ldots, \tau_r) \neq (0, 0, \ldots, 0)$. We will simply denote this constant by γ in the remainder of this paper.

A few results for the case $\gamma = -1$ are given in [10]. In addition to providing some generalized results for case $\gamma = -1$, we investigate the remaining two cases i.e. $\gamma = 0$ and $\gamma = 1$. We shall point out that higher magnitude values of γ are possible only in few cases of v, if we require the condition of array pair being balanced.

The equivalence of binary perfect/ideal arrays and their algebraic counterparts so-called 'difference sets' is a well studied notion, further details of which, for instance, can be found in [8, 11]. We shall confine our attention only to the case of binary array pairs with constant γ and their equivalent algebraic objects 'difference set pairs' as discussed in [3].

Let G be an additionally written abelian group of order v. Let A and B be subsets of G, of size k and k' respectively. Let $|\ A \cap B\ | = e$. If the list/multiset of differences $(x - y \mid x \in A\ and\ y \in B,\ x \neq y)$ contains each non-zero element exactly λ times, then we call (A, B) a difference set pair (DSP) in G with parameters (v, k, k', e, λ).

The notion of difference sets is very important in the general area of discrete mathematics and algebraic combinatorics, having immense applications in communication engineering. For more on this, we refer the reader to the encyclopedian book [12].

If (A, B) is a (v, k, k, k, λ) difference set pair (DSP) in G with $A = B$, then A is simply called a (v, k, λ) difference set in G.

The following theorem is essentially due to [3].

Theorem 1.1. *There exists a $s_1 \times s_2 \times \cdots \times s_r$ binary array pair $(\boldsymbol{A}, \boldsymbol{B})$ with constant cross-correlation value $\gamma = \gamma_{A,B}(\tau_1, \tau_2, \ldots, \tau_r)$ for all $\tau_i \not\equiv 0 \pmod{s_i}, 1 \leq i \leq r$ if and only if there exists a DSP (A, B) in $G = Z_{s_1} \times Z_{s_2} \times \cdots \times Z_{s_r}$.*

Remark 1.2. The equivalence of the aforementioned theorem is achieved by the following bijection:
$\mathbf{A} = (a(j_1, j_2, \ldots, j_r))_{0 \leq j_i \leq s_i - 1, 1 \leq i \leq r} \quad \overleftrightarrow{\nu}$
$A = \{(j_1, j_2, \ldots, j_r) \mid a(j_1, j_2, \ldots, j_r) = -1\} \subseteq Z_{s_1} \times Z_{s_2} \times \cdots \times Z_{s_r}$

Remark 1.3. The parameters for the DSP (A, B) of theorem 1.1 are :
(v, k, k', e, λ)
where $v = s_1 s_2 \cdots s_r$, $k = \mid A \mid$, $k' = \mid B \mid$,
where $A = \nu(\mathbf{A})$ and $B = \nu(\mathbf{B})$,
$e = \mid A \cap B \mid$ and λ is determined by the equations :

$$kk' = e + \lambda(v - 1) \tag{1.5}$$

$$\gamma = v - 2(k + k') + 4\lambda \tag{1.6}$$

We shall refer to this constant γ as *correlation constant.*

Remark 1.4. The most general version of theorem 1.1 as given above is new but it is a mundane generalization of the $\gamma = 0$ case given in [3] and the higher dimensional analog of the 'sequence' (1-dimensional) version studied in [2].

Remark 1.5. Neither of the requirements 'balanced' and/or 'ideal/perfect' is essential in theorem 1.1 which is much more general.

Remark 1.6. We define a DSP (A, B) to be balanced (respectively ideal/perfect) if the corresponding binary array pair $(\mathbf{A}, \mathbf{B})$ is balanced (respectively ideal/perfect).

We organize this paper as follows: Section 2 provides the basic results required for the remainder of the paper. The main section (Section 3) gives several construction techniques (many of them being recursive) of DSPs, generalizing previously known constructions. While our main thrust may seem to be directed toward balanced and ideal cases, most of our results hold for arbitrary DSPs in general. Section 4 is devoted to the possible candidate objects, which could be used as 'plug-ins' in our recursive theorems. In the concluding section (Section 5), we point out the inter-connections between our results and those of others found in the literature.

All the DSP constructions we provide in this paper, in turn, yield binary array pairs in view of Theorem 1.1. We shall only state our results in the language of DSPs; restating our DSP constructions as their binary sequence/array pairs is straight forward and we omit it.

2. Preliminaries

Many authors use the notion of Hall-polynomials (see [13]) to paraphrase the concept of sequence/array pairs. We opt to make use of group rings instead, for reasons of brevity, simplicity and elegance. Both approaches can be easily shown to be mathematically equivalent.

Let G be a multiplicatively written abelian group of order v, R any subring of the field of complex numbers and RG the group ring of G over R.
For any subset S of G, we let S also denote the group ring element:

$$S = \sum_{x \in S} x \in RG$$

where the coefficient of x on the right hand side is 1 or 0, according as x is in S or not. We use the same letter S to denote 'subset' and 'group ring element ', causing no confusion as the context would make the meaning clear.
For

$$A = \sum_{g \in G} a_g.g \in RG$$

and $t \in \mathbb{Z}$, we define

$$A^{(t)} = \sum_{g \in G} a_g.g^t$$

Remark 2.1. For

$$A = \sum_{g \in G} a_g.g \in \mathbb{Z}G,$$

it is easy to see that

$$AG = \left(\sum_{g \in G} a_g \right) G \in \mathbb{Z}G \tag{2.1}$$

In particular, for any subset S of G,

$$SG = |S|G \in \mathbb{Z}G \tag{2.2}$$

The following proposition is straight forward:

Proposition 2.2. *Let G be an abelian group of order v and A and B be subsets of G of size k and k' respectively. Then (A, B) is a (v, k, k', e, λ) DSP in G if and only if*

$$AB^{(-1)} = A^{(-1)}B = e + \lambda(G - 1) \text{ in } \mathbb{Z}G. \tag{2.3}$$

(Here 1 denotes the identity element of G)

Corollary 2.3. *Let G be an abelian group of order v and D a subset of G of size k. Then D is a (v, k, λ) difference set in G if and only if*

$$DD^{(-1)} = (k - \lambda) + \lambda G \text{ in } \mathbb{Z}G. \tag{2.4}$$

We warn the reader that we do all our group ring calculations in $\mathbb{Z}G$ assuming G as a *multiplicative* group. From now on, S and N would denote 'squares' and 'non-squares' in the finite field $GF(q)$. Although $G = GF(q)$ is an *additive* group, we shall treat S and N as objects in $\mathbb{Z}G$ and use *multiplicative* operations. This misuse of notations is not uncommon in the theory of difference sets and must not cause any confusion.

We also require the further class of objects that generalize 'difference sets'.

Proposition 2.4. *Let G be a multiplicatively written abelian group of order v and $D \subseteq G$, $|D| = k$. Assume that $1 \notin D$. D is said to be a (v, k, λ, μ) partial difference set (PDS) in G if $D = D^{(-1)}$ and*

$$DD^{(-1)} = D^2 = k + \lambda D + \mu(G - D - 1) \text{ in } \mathbb{Z}G. \tag{2.5}$$

The following class of PDS is well-known (see the survey article [14]).

Example 2.5. *Let q be a prime power, $q \equiv 1 \pmod 4$. Let $GF(q)$ denote the finite field with q elements. Fix a primitive element α of $GF(q)$, define*
$S = \{\alpha^{2i} | i = 0, 1, \ldots, \frac{q-3}{2}\}$
$N = \{\alpha^{2j+1} | j = 0, 1, \ldots, \frac{q-3}{2}\}$
Thus S and N consist of 'squares' and 'non squares' of $GF(q)|\{0\}$. It is well known that S and N are PDS in $G = (GF(q), +)$ with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. Hence the following equations hold in $\mathbb{Z}G$:

$$SS^{(-1)} = S^2 = \frac{q-1}{2} + \frac{q-5}{4}S + \frac{q-1}{4}N \tag{2.6}$$

$$NN^{(-1)} = N^2 = \frac{q-1}{2} + \frac{q-5}{4}N + \frac{q-1}{4}S \tag{2.7}$$

Also

$$S = S^{(-1)} \tag{2.8}$$

$$N = N^{(-1)} \tag{2.9}$$

and

$$1 + S + N = G \tag{2.10}$$

The '1-dimensional/sequence' version of the following proposition is given as [2, Lemma 2] which can also be found in [3]. We now present its higher dimensional/array analog.

Proposition 2.6. *Let (A, B) be a (v, k, k', e, λ) DSP in an abelian group G whose correlation constant is γ. Then:*
i)$(G - A, B)$ is a $(v, v - k, k', k' - e, k' - \lambda)$ DSP in G with correlation constant $-\gamma$.
ii)$(A, G - B)$ is a $(v, k, v - k', k - e, k - \lambda)$ DSP in G with correlation constant $-\gamma$.
iii)$(G - A, G - B)$ is a $(v, v - k, v - k', e + v - (k + k'), \lambda + v - (k + k'))$ DSP in G with correlation constant γ.

Proof. Earlier proofs of this proposition(the 'sequence' version) made use of 'correlation' calculations. We opt to provide a more transparent proof using group rings which holds for all 'dimensions'. We shall only prove (iii) (Proofs of (i) and (ii) follow the same approach).
We compute,
$(G - A)(G - B)^{(-1)}$
$= GG - AG - B^{(-1)}G + AB^{(-1)}$
$= vG - kG - k'G + (e + \lambda(G - 1))$ using proposition 2.2 Simplification of this expression yields the desired result, noting that the assertion on the correlation constant follows from calculating the expression for γ given in equation (6). □

Remark 2.7. *We call the DSP pairs $(A, B), (G-A, B), (A, G-B), (G-A, G-B)$ as pairwise equivalent. More specifically, $(G - A, B)$ is 'left complement' equivalent to (A, B); $(A, G - B)$ is 'right complement' equivalent to (A, B) and $(G - A, G - B)$ is 'complement' equivalent to (A, B).*

Next, we give two concrete and explicit examples of DSPs that arise from a finite field of order q. These results must be well known (see [10] for instance).

Theorem 2.8. *With notations as in Example 2.5,*
i) (S, N) forms a DSP in (GF(q),+) with parameters $(4m + 1, 2m, 2m, 0, m)$ whose $\gamma = 1$.
ii) $(1 + S, S)$ forms a DSP in (GF(q),+) with parameters $(4m + 1, 2m + 1, 2m, 2m, m)$ whose $\gamma = -1$.

Proof. i) Follows by computing $SN^{(-1)}$ and simplifying it, using equations $(12) - (16)$.
Part (ii) is an easy consequence of parts (i) and (ii) of Proposition 2.6. □

Theorem 2.8 dealt with prime power q, $q \equiv 1 \pmod 4$. We close this section with the '$q \equiv 3 \pmod 4$' analog of Theorem 2.8. We shall state (without proof) a more general result that holds for 'all' difference sets with Paley parameters, in addition to the classical squares and non-squares in $GF(q)$, $q \equiv 3 \pmod 4$.

Theorem 2.9. *Let D be a $(4m-1, 2m-1, m-1)$ difference set (with Paley parameters) in any abelian group G of order $4m - 1$. Then*
i) (D, D) is a $(4m - 1, 2m - 1, 2m - 1, 2m - 1, m - 1)$ DSP in G whose $\gamma = -1$.
ii) $(G - D, D)$ is a $(4m - 1, 2m, 2m - 1, 0, m)$ DSP in G whose $\gamma = 1$.

3. New difference set pairs from old ones

Although our primary interest would be directed towards balanced and ideal DSPs, we shall obtain more general constructions of DSPs, from which we obtain balanced and ideal examples, as special cases. We begin this section by investigating the cases $\gamma \in \{0, 1, -1\}$, characterizing the parameters of the corresponding DSPs. We point out that the case $\gamma = -1$ is dealt with in [10] which inspired some of our results.

Higher values of $|\gamma|$ in the balanced case for DSPs would result in a very limited number of feasible parameters (This can be seen using elementary arithmetic). We would be remiss if we failed to give due credit to the ingenious work of [15], whose recursive constructions motivated us to pursue this research.

3.1. $\gamma = 0$. The following proposition provides the parameter characterization of balanced and ideal DSPs with $\gamma = 0$.

Proposition 3.1. *There exists a balanced and ideal (v, k, k', e, λ) DSP with $\gamma = 0$ if and only if $k = \frac{v}{2}$, $k' = 2\lambda$, $e = \lambda$*

Proof. The desired conclusions follow easily from (5) and (6) by setting $k = \frac{v}{2}$ and $\gamma = 0$. □

Our next theorem provides a striking contrast to the other DSP cases with $\gamma \neq 0$ and the difference set problem with $\gamma = 0$. While the existence problem for the latter cases is parameter dependent, the former ones that pertain to balanced and ideal DSP with $\gamma = 0$ will be shown to exist *for all* λ and v.

Theorem 3.2. *In any abelian group G of even order v, there exists a balanced and ideal DSP (A, B) with parameters $(v, \frac{v}{2}, 2\lambda, \lambda, \lambda)$ for all λ satisfying $\lambda \leq \frac{v}{2}$.*
(Note: The requirement $\lambda \leq \frac{v}{2}$ is essential.)

Proof. Let H be a subgroup of G of index 2, i.e., $|H| = \frac{v}{2}$. Let C be any subset of H with $|C| = \lambda$ and D any subset of $G - H$ (the complement of H in G) with $|D| = \lambda$.
Define $A = H$ and $B = C \cup D$. Using elementary group theory, one obtains $AB^{(-1)} = \lambda + \lambda(G - 1)$, as desired. □

3.2. $\gamma = 1$ and $\gamma = -1$. We now provide the parameter characterization of balanced and ideal DSPs with $\gamma = 1$ followed by $\gamma = -1$.

Proposition 3.3. *If there exists a balanced and ideal (v, k, k', e, λ) DSP in an abelian group of order v with $\gamma = 1$, then*
$k = \frac{v-1}{2}$, $k' = 2\lambda$, $e = 0$ *or*
$k = \frac{v+1}{2}$, $k' = 2\lambda - 1$, $e = 2\lambda - (\frac{v+1}{2})$

Proof. Identical to the proof as in proposition 3.1 by setting $k = \frac{v \mp 1}{2}$ and $\gamma = 1$. □

Proposition 3.4. *If there exists a balanced and ideal (v, k, k', e, λ) DSP in an abelian group of order v with $\gamma = -1$, then*
$k = \frac{v-1}{2}, k' = 2\lambda + 1, e = \frac{v-1}{2}$ *or*
$k = \frac{v+1}{2}, k' = 2\lambda, e = 2\lambda$

Proof. Similar to proposition 3.3. □

3.3. **Some new recursive constructions.** It's a commonplace to make use of 'Kronecker' product in the construction of orthogonal matrices and the like (also their algebraic counterparts difference sets etc.). Some recent publications (e.g. [2, 10, 15]) implicitly use this idea and we follow suit by providing four new recursive constructions of DSPs from old ones via 'Kronecker-like' products. In what follows we freely make use of group ring notations as explained in section 2.

Theorem 3.5. *Let (A, B) be a DSP with parameters $(v,\ k,\ k',\ e,\ \lambda)$ in an abelian group G of order v. Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1,\ 2m,\ m)$ (complementary Paley parameters), whence*

$$EE^{(-1)} = m + mH \tag{3.1}$$

Let

$$C = EA + (H - E)(G - A) \tag{3.2}$$

and

$$D = EB \tag{3.3}$$

Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m-1),\ (2m-1)v + k,\ 2mk',\ 2me,\ 2m\lambda) \tag{3.4}$$

if and only if $k' = 2\lambda$, in which case the new DSP (C,D) also satisfies the same condition, thereby making this construction recursive.

Proof. Verification of the first three parameters of (C, D) is quite straight forward. To obtain last two parameters, we compute
$CD^{(-1)} = [EA + (H - E)(G - A)](EB)^{(-1)}$ *[using (18) and (19)]*
$= EE^{(-1)}AB^{(-1)} + (H - E)E^{(-1)}(G - A)B^{(-1)}$
$= 2EE^{(-1)}AB^{(-1)} + 2mk'GH - 2mHAB^{(-1)} - k'EE^{(-1)}G$ *[using (8)]*
$= 2m(e - \lambda) + (2m\lambda - mk')G + (mk')GH$ *[using (9),(17)]*
In order for (C, D) to be a DSP in $G \times H$, we require that the coefficient of G in previous equation to be 0; therefore we get $k' = 2\lambda$, which completes the proof. □

We now apply theorem 3.5 to some balanced and ideal cases.

Theorem 3.6. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v}{2}, 2\lambda, \lambda, \lambda)$ in an abelian group G of order v (with $\gamma = 0$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1, 2m, m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H - E)(G - A)$ and $D = EB$. Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m-1), \frac{v(4m-1)}{2}, 4m\lambda, 2m\lambda, 2m\lambda) \tag{3.5}$$

with $\gamma = 0$.

Proof. Immediate by putting the values $k = \frac{v}{2}$, $k' = 2\lambda$, $e = \lambda$ in theorem 3.5. □

Theorem 3.7. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v-1}{2}, 2\lambda, 0, \lambda)$ in an abelian group G of order v (with $\gamma = 1$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1, 2m, m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H - E)(G - A)$ and $D = EB$. Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m-1), \frac{v(4m-1)-1}{2}, 4m\lambda, 0, 2m\lambda) \tag{3.6}$$

with $\gamma = 1$.

Proof. Put $k = \frac{v-1}{2}$, $k' = 2\lambda$, $e = 0$ in theorem 3.5. □

Theorem 3.8. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v+1}{2}, 2\lambda, 2\lambda, \lambda)$ in an abelian group G of order v (with $\gamma = -1$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1, 2m, m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H - E)(G - A)$ and $D = EB$. Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m-1), \frac{v(4m-1)+1}{2}, 4m\lambda, 4m\lambda, 2m\lambda) \tag{3.7}$$

with $\gamma = -1$.

Proof. Put $k = \frac{v+1}{2}$, $k' = 2\lambda$, $e = 2\lambda$ in theorem 3.5 to get the desired results. □

We now make a variation of the general theme that gave us our recursive constructions of the earlier theorems in this section by replacing the 'Paley-type' difference sets E by so-called partial difference sets PDSs (For more on PDSs, we refer the reader to [14]).

Theorem 3.9. *Let (A, B) be a DSP with parameters (v, k, k', e, λ) in an abelian group G of order v. Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1, 2m, m-1, m)$, whence*

$$EE^{(-1)} = 2m + (m-1)E + m\bar{E} \tag{3.8}$$

$$\bar{E}\bar{E}^{(-1)} = 2m + (m-1)\bar{E} + mE \tag{3.9}$$

$$E = E^{(-1)} \tag{3.10}$$

$$\bar{E} = \bar{E}^{(-1)} \tag{3.11}$$

$$1 + E + \bar{E} = H \tag{3.12}$$

Let

$$C = (1+E)A + \bar{E}(G-A) \tag{3.13}$$

and

$$D{=}EB$$

Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m+1),\ 2mv+k,\ 2mk',\ 2me,\ 2m\lambda) \tag{3.14}$$

if and only if $k' = 2\lambda$, which makes the resulting DSP (C,D) to satisfy the same condition and thus makes this construction recursive.

Proof. Verification of the first three parameters of the candidate DSP (C, D) is quite straight forward. To obtain last two parameters, we compute
$CD^{(-1)} = [(1+E)A + \bar{E}(G-A)](EB)^{(-1)}$ *[using (29) and (19)]*
$= [(1+E)A + (H-E-1)(G-A)]E^{(-1)}B^{(-1)}$ *[using (28)]*
$= (1+E)E^{(-1)}AB^{(-1)} + (H-E-1)E^{(-1)}(G-A)B^{(-1)}$
$= 2m(e-\lambda) + (2m\lambda - mk')G + (mk')GH$ *[using (9), (24), (25), (26), (27)]*
In order for (C, D) to be a DSP in $G \times H$, it is required that the coefficient of G in the previous expression is 0; therefore we get $k' = 2\lambda$, which completes the proof. □

As before, our next task is to obtain special cases of theorem 3.9.

Theorem 3.10. *Let (A, B) be a balanced and ideal DSP with parameters $(v,\ \frac{v}{2},\ 2\lambda,\ \lambda,\ \lambda)$ in an abelian group of order v (with $\gamma = 0$). Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1,\ 2m,\ m-1,\ m)$, whence*

$$EE^{(-1)} = 2m + (m-1)E + m\bar{E}$$
$$\bar{E}\bar{E}^{(-1)} = 2m + (m-1)\bar{E} + mE$$
$$E = E^{(-1)}$$
$$\bar{E} = \bar{E}^{(-1)}$$
$$1 + E + \bar{E} = H$$

Let $C = (1+E)A + \bar{E}(G-A)$ and $D = EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters:

$$(v(4m+1), \frac{v(4m+1)}{2}, 4m\lambda, 2m\lambda, 2m\lambda) \tag{3.15}$$

with $\gamma = 0$.

Proof. It is elementary by putting the values $k = \frac{v}{2}$, $k' = 2\lambda$, $e = \lambda$ in theorem 3.9. □

Theorem 3.11. *Let* (A, B) *be a balanced and ideal DSP with parameters* $(v,\ \frac{v-1}{2},\ 2\lambda,\ 0,\ \lambda)$ *in an abelian group of order* v *(with* $\gamma = 1$*). Let* E *be a partial difference set in an abelian group* H *of order* $4m+1$ *with parameters* $(4m+1,\ 2m,\ m-1,\ m)$*, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let $C = (1+E)A + \bar{E}(G-A)$ *and* $D = EB$*. Then* (C, D) *is a balanced and ideal DSP in* $G \times H$ *with parameters:*

$$(v(4m+1), \frac{v(4m+1)-1}{2}, 4m\lambda, 0, 2m\lambda) \tag{3.16}$$

with $\gamma = 1$.

Proof. Similar to theorem 3.10 by putting the values $k = \frac{v-1}{2}$, $k' = 2\lambda$, $e = 0$. □

Theorem 3.12. *Let* (A, B) *be a balanced and ideal DSP with parameters* $(v,\ \frac{v+1}{2},\ 2\lambda,\ 2\lambda,\ \lambda)$ *in an abelian group* G *of order* v *(with* $\gamma = -1$*). Let* E *be a partial difference set in an abelian group* H *of order* $4m+1$ *with parameters* $(4m+1,\ 2m,\ m-1,\ m)$*, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let $C = (1+E)A + \bar{E}(G-A)$ *and* $D = EB$*. Then* (C, D) *is a balanced and ideal DSP in* $G \times H$ *with parameters:*

$$(v(4m+1), \frac{v(4m+1)+1}{2}, 4m\lambda, 4m\lambda, 2m\lambda) \tag{3.17}$$

with $\gamma = -1$.

Proof. Similar to theorem 3.10 by substituting $k = \frac{v+1}{2}$, $k' = 2\lambda$, $e = 2\lambda$. □

Our last set of 'recursive' theorems is now proven (theorems 3.13 and theorems 3.17) by slightly modifying the second set D in the DSP (C, D) of theorems 3.5 and theorems 3.9, resulting in 'new' constraints on the parameters of the plug-in DSPs (A,B).

Theorem 3.13. *Let (A, B) be a DSP with parameters (v, k, k', e, λ) in an abelian group G of order v. Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1,\ 2m,\ m)$, whence*

$$EE^{(-1)} = m + mH$$

Let

$$C = EA + (H - E)(G - A)$$

and

$$D = (H - E)G + EB \tag{3.18}$$

Then (C, D) is a DSP in $G \times H$ with parameters

$$(v(4m-1),\ (2m-1)v + k,\ (2m-1)v + 2mk',\ k - v + m(v + k' + 2(e - \lambda)),\ k - v + m(v + k')) \tag{3.19}$$

if and only if $v = 2k + k' - 2\lambda$, with the resulting DSP (C,D) satisfying the same condition and making this construction recursive.

Proof. First three parameters of (C, D) can be verified by using basic mathematics. To verify the last two parameters, we compute:
$CD^{(-1)} = [EA + (H - E)(G - A)][(H - E)G + EB]^{(-1)}$ *[using (18), (34)]*
$= [EA + (H - E)(G - A)][(H - E^{(-1)})G + E^{(-1)}B^{(-1)}]$
$= E(H - E^{(-1)})AG + EE^{(-1)}AB^{(-1)} + (H - E)(H - E^{(-1)})(G - A)B^{(-1)} + (H - E)E^{(-1)}(G - A)B^{(-1)}$
$= 2m(e - \lambda) + m(v - 2k - k' + 2\lambda)G + (k - v + m(v + k'))GH$ *[using (9), (17)]*
In order for (C, D) to be a DSP in $G \times H$, the coefficient of G in previous expression must be 0, therefore we get $v = 2k + k' - 2\lambda$, which is the required result. □

We now provide some specialized cases of theorem 3.13 which are applicable for balanced and ideal plug-in DSPs.

Theorem 3.14. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v}{2}, 2\lambda, \lambda, \lambda)$ in an abelian group G of order v (with $\gamma = 0$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1,\ 2m,\ m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H - E)(G - A)$ and $D = (H - E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters

$$(v(4m-1), \frac{v(4m-1)}{2}, (2m-1)v + 4m\lambda, \frac{(2m-1)v + 4m\lambda}{2}, \frac{(2m-1)v + 4m\lambda}{2}) \tag{3.20}$$

with $\gamma = 0$.

Proof. Can be easily obtained by putting $k = \frac{v}{2}$, $k' = 2\lambda$, $e = \lambda$ in the results of theorem 3.13. □

Theorem 3.15. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v+1}{2}, 2\lambda-1, 2\lambda-\frac{v+1}{2}, \lambda)$ in an abelian group G of order v (with $\gamma = 1$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1,\ 2m,\ m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H-E)(G-A)$ and $D = (H-E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters

$$(v(4m-1), \frac{(4m-1)v+1}{2}, 2m(v+2\lambda-1)-v, \frac{4m(2\lambda-1)-v+1}{2}, \frac{2m(v+2\lambda-1)-v+1}{2}) \tag{3.21}$$

with $\gamma = 1$.

Proof. Similar by substituting $k = \frac{v+1}{2}$, $k' = 2\lambda-1$, $e = 2\lambda-\frac{v+1}{2}$ in the results of theorem 3.13. □

Theorem 3.16. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v-1}{2}, 2\lambda+1, \frac{v-1}{2}, \lambda)$ in an abelian group G of order v (with $\gamma = -1$). Let E be a difference set in an abelian group H of order $4m-1$ with parameters $(4m-1,\ 2m,\ m)$, whence*

$$EE^{(-1)} = m + mH$$

Let $C = EA + (H-E)(G-A)$ and $D = (H-E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters

$$(v(4m-1), \frac{(4m-1)v-1}{2}, 2m(v+2\lambda+1)-v, \frac{(4m-1)v-1}{2}, \frac{2m(v+2\lambda+1)-v-1}{2}) \tag{3.22}$$

with $\gamma = -1$

Proof. Similar by putting $k = \frac{v-1}{2}$, $k' = 2\lambda+1$, $e = \frac{v-1}{2}$ in the results of theorem 3.13. □

Our final recursive construction for general DSPs is given in :

Theorem 3.17. *Let (A, B) be a DSP with parameters (v, k, k', e, λ) in an abelian group G of order v. Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1, 2m, m-1, m)$, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let

$$C = (1+E)A + \bar{E}(G-A)$$

and

$$D = (H-E)G + EB$$

Then (C, D) is a DSP in $G \times H$ with parameters:

$$(v(4m+1), 2mv+k, (2m+1)v+2mk', 2m(e-\lambda)+k+m(v+k'), k+m(v+k')) \tag{3.23}$$

if and only if $v = k'+2k-2\lambda$, where the new DSP (C, D) obtained as a result follows the same condition as the plug-in DSP and thereby make this construction recursive.

Proof. First three parameters of (C, D) can be verified easily. For last two parameters, we compute:
$CD^{(-1)} = [(1+E)A + \bar{E}(G-A)][(H-E)G + (EB)]^{(-1)}$ *[using (29), (34)]*
$= [(1+E)A + (H-E-1)(G-A)][(H-E^{(-1)})E^{(-1)}B^{(-1)}G]$ *[using (28)]*
$= 2m(e-\lambda) + (2m\lambda - 2mk - mk' + mv)G + (k+mk'+mv)GH$ *[using (9), (24), (25), (26), (27)]*
In order for (C, D) to be a DSP in $G \times H$, we require the coefficient of G in previous equation to be 0, therefore we get $v = k' + 2k - 2\lambda$, which proves our theorem. □

Now, we provide the final set of special cases of theorem 3.17 .

Theorem 3.18. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v}{2}, 2\lambda, \lambda, \lambda)$ in an abelian group G of order v(with $\gamma = 0$). Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1,\ 2m,\ m-1,\ m)$, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let $C = (1+E)A + \bar{E}(G-A)$ and $D = (H-E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters:

$$(v(4m+1), \frac{v(4m+1)}{2}, v(2m+1)+4m\lambda, v(2m+1)+4m\lambda, \frac{v(2m+1)+4m\lambda}{2}) \tag{3.24}$$

with $\gamma = 0$.

Proof. Can be obtained by putting the values $k = \dfrac{v}{2}$, $k' = 2\lambda$, $e = \lambda$ in the results of theorem 3.17. □

Theorem 3.19. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v+1}{2}, 2\lambda-1, 2\lambda-\frac{v+1}{2}, \lambda)$ in an abelian group of order v(with $\gamma = 1$). Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1,\ 2m,\ m-1,\ m)$, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let $C = (1+E)A + \bar{E}(G-A)$ and $D = (H-E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters:

$$(3.25)\quad (v(4m+1), \frac{v(4m+1)+1}{2}, 2m(2\lambda+v-1)+v, \frac{(v+1)}{2}+2m(2\lambda-1), \frac{(v+1)}{2}+m(2\lambda+v-1))$$

with $\gamma = 1$.

Proof. Elementary and can be obtained by putting $k = \frac{v+1}{2}$, $k' = 2\lambda - 1$, $e = 2\lambda - \frac{v+1}{2}$ in the results of theorem 3.17. □

Theorem 3.20. *Let (A, B) be a balanced and ideal DSP with parameters $(v, \frac{v-1}{2}, 2\lambda+1, \frac{v-1}{2}, \lambda)$ in an abelian group G of order v(with $\gamma = -1$). Let E be a partial difference set in an abelian group H of order $4m+1$ with parameters $(4m+1,\ 2m,\ m-1,\ m)$, whence*

$$\begin{aligned} EE^{(-1)} &= 2m + (m-1)E + m\bar{E} \\ \bar{E}\bar{E}^{(-1)} &= 2m + (m-1)\bar{E} + mE \\ E &= E^{(-1)} \\ \bar{E} &= \bar{E}^{(-1)} \\ 1 + E + \bar{E} &= H \end{aligned}$$

Let $C = (1+E)A + \bar{E}(G-A)$ and $D = (H-E)G + EB$. Then (C, D) is a balanced and ideal DSP in $G \times H$ with parameters:

$$(3.26)\qquad (v(4m+1), \frac{v(4m+1)-1}{2}, 2m(2\lambda+v+1)+v, \frac{v(4m+1)-1}{2}, \frac{(v-1)}{2}+m(2\lambda+v+1))$$

with $\gamma = -1$.

Proof. Simple by putting $k = \frac{v-1}{2}$, $k' = 2\lambda+1$, $e = \frac{v-1}{2}$ in the results of theorem 3.17. □

4. On the plug-in objects

The plug-in objects E (difference sets and partial difference sets) are usually referred to as "Paley-Hadamard" type. These objects E exist in abundance. For more on difference sets, refer [12]. A rich class of such objects in cyclic groups of order $2^r - 1$ can be found in the seminal paper [16]. A nice survey article of partial difference sets is due to [14].

Known 'plug-in' DSPs which could be used as 'input' in all of our recursive constructions are given in [2, 15].

Most of the earlier results on DSPs are given for 'sequences'(1-dimensional array) and almost all of them require the 'Paley-Hadamard' difference sets as the classical examples of "squares in GF(q)". Our recursive theorems are more general, in the sense, any difference set or partial difference set with 'Paley-Hadamard' parameters could be used as 'input' objects. Using this generalized approach in Theorem 3.5, for example, we obtain a class of DSPs which can be used as inputs in all of our recursive theorems.

More such results can be easily stated but we omit the details. We only state one such result to convey our point.

Theorem 4.1. *Let D_i be a $(4n_i - 1, 2n_i, n_i)$ difference set in an abelian group G_i for i=1,2. Define*

$$X = (G_1 - D_1)D_2 + D_1(G_2 - D_2) \tag{4.1}$$

$$Y = D_1 D_2 \tag{4.2}$$

then (X, Y) is a balanced and ideal DSP in $G_1 \times G_2$ with $\gamma = 1$ having parameters

$$((4n_1 - 1)(4n_2 - 1), 8n_1n_2 - 2n_1 - 2n_2, 4n_1n_2, 0, 2n_1n_2) \tag{4.3}$$

Remark 4.2. We note that Theorem 4.1 follows from Theorem 3.5 by taking $A = B = D_1$, $E = D_2$ and observing that (D_1, D_1) is a DSP in G_1 with parameters $(4n_1 - 1, 2n_1, 2n_1, 2n_1, n_1)$.

Remark 4.3. Theorem 4.1 generalizes [2, Theorem 5].

Remark 4.4. It can be easily proved using elementary group ring calculations that the assumption on both D_1 and D_2 being 'Paley-Hadamard' type is essential in Theorem 4.1, i.e., replacing one or both D_i by an arbitrary (v, k, λ) difference set (where $v \neq 4(k - \lambda) - 1$) would not result in DSPs.

5. Conclusion

Theorem(3) of [15] is their main result and has been a motivating factor for our investigation. We have generalized their main result in four directions (also to higher dimensions i.e. r-dimensional arrays, "sequences" being 1-dimensional) providing a recursive construction of DSPs (and hence binary array pairs). The lengths of the underlying binary sequence pairs considered in [15] are "np" where n and p are both primes. The recursive nature of all our constructions would allow more possibilities for 'length/energy' v. All the 'odd length' binary sequence pairs constructed in [2] are contained in our theorems of Section 3. Although [3, 4] consider higher dimensional array pairs, their authors seem to restrict the study to the case $\gamma = 0$; our results are more general than [3, 4], in that we allow other non-zero values of γ. There is virtually no overlap of our results with those given in [17]. But the results of [17] are rather intriguing; they provide a rich class of DSPs with $\gamma = 0$ that are 'nearly-balanced' which may possibly have cryptological applications. We are pleasantly surprised to see in [17], a 'multiplier theorem' proved for DSPs which would serve as an indispensable tool in the 'non-existence' results for DSPs.

Two constructions using cyclotomy of finite field are given in [18]. Our elementary yet more powerful theorem 3.2 supercedes their results which assume the 'length/energy' v to be $2q$, q be a prime power. Our theorem 3.2 fully settles the balanced and ideal case for $\gamma = 0$ (providing explicit construction for *all* v and for *all* λ).

We conclude this paper with the following question :

Are there any other constructions for DSPs

- recursive or not ?
- balanced or not ?
- ideal or not ?

Acknowledgement

The work was partially supported by grants from the AFOSR and NSF. Goyal and Puri's research was carried out while they were summer interns at Wright State University (WSU).They thank the Department of Mathematics and Statistics at WSU for the hospitality and the support provided.

References

[1] F. Mao, T. Jiang, C. lin Zhao and Z. Zhou, Study of pseudorandom binary sequence pairs,*J. Commun.*, **26** (2005) 94–98.

[2] X. Peng, C. Xu and K. T. Arasu, New families of binary sequence pairs with two-level and three-level correlation, *IEEE Trans. Inform. Theory*, **58** (2012) 6968–6978.

[3] C. Q. Xu, Differences set pairs and approach for the study of perfect binary array pairs, *Acta Electron. Sin.*, **29** (2001) 87–89.

[4] X. Zhao, W. He, Z. Wang and S. Jia, The theory of the perfect binary array pairs, *Acta Electron. Sin.*, **27** (1999) 34–37.

[5] H. Rohling and W. Plagge, Mismatched-filter design for periodic binary phased signals, *IEEE Trans. Aerosp. Electron. Syst.*, **25** (1989) 890–897.

[6] S. W. Golomb and G. Gong, *Signal design for good correlation: For wireless communication*, cryptography, and radar. Cambridge University Press, Cambridge, 2005

[7] Q. Li, J. Gao and X. Zhao, *The application of the ZCZ sequence pairs set in QS-CDMA system*, 3rd International Workshop on Signal Design and Its Applications in Communications, 2007 288–291.

[8] D. Jungnickel and A. Pott, Perfect and almost perfect sequences, *Discrete Appl. Math.*, **95** (1999) 331–359.

[9] K. T. Arasu, *Sequences and arrays with desirable correlation properties*, Information Security, Coding Theory and Related Combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur, Amsterdam, **29** (2011) 136–171.

[10] K. T. Arasu, V. Hariharan, D. Hilton and S. K. Sehgal, *On difference set pairs in abelian groups*, (Preprint) 2013.

[11] A. Pott, *Finite geometry and character theory*, Lecture notes in mathematics, pringer-Verlag, Berlin, 1995.

[12] T. Beth, D. Jungnickel and H. Lenz, *Design theory*, Second edition, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1999.

[13] M. Hall, *Combinatorial theory*, Reprint of the 1986 second edition, Wiley Classics Library, A Wiley-Interscience Publication, John Wiley Sons, Inc., New York, 1998.

[14] S. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.*, **4** (1994) 221–261.

[15] P. Ke, W. Yu and Z. Chang, A note on binary sequence pairs with two-level correlation, *Inform. Process. Lett.*, **113** (2013) 811–814.

[16] J. F. Dillon and H. Dobbertin, New cyclic difference sets with singer parameters, *Finite Fields Appl.*, **10** (2004) 342–389.

[17] S.-Y. Jin and H.-Y. Song, Binary sequence pairs with two-level correlation and cyclic difference pairs, *IEICE TRANS. FUNDAMENTALS*, **93** (2010) 2266–2271.

[18] Y.-G. Jia, F.-Z. Ren, Y.-F. Ji, Y.-S. Liu and J. Ren, *Two methods for constructing the difference set pairs*, Published in: Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on, 2010 675–678.

K. T. Arasu
Department of Mathematics and Statistics, Wright State University, Dayton, O.H., 45435, U.S.A.
Email: k.arasu@wright.edu

Anika Goyal
Samsung India Electronics Pvt Ltd, Logix Cyber Park, Plot No. C28-29, Tower D, Sector 62, Noida, 201301, India
Email: anikagoyal13@gmail.com

Abhishek Puri
ThoughtWorks Technologies India, 6th Flr, Bldg. 14B, DLF Cyber Cit, Ph. 3, Gurgaon, Haryana, 122002, India
Email: puri.abhishek14@gmail.com