Defence Science Journal, Vol. 67, No. 5, September 2017, pp. 536-541, DOI : 10.14429/dsj.67.10638

On Walsh Spectrum of Cryptographic Boolean Function

Shashi Kant Pandey* and B.K. Dass

Department of Mathematics, University of Delhi, Delhi – 110 007, India
**E-mail: shashikantshvet@gmail.com*

ABSTRACT

Walsh transformation of a Boolean function ascertains a number of cryptographic properties of the Boolean function viz, non-linearity, bentness, regularity, correlation immunity and many more. The functions, for which the numerical value of Walsh spectrum is fixed, constitute a class of Boolean functions known as bent functions. Bent functions possess maximum possible non-linearity and therefore have a significant role in design of cryptographic systems. A number of generalisations of bent function in different domains have been proposed in the literature. General expression for Walsh transformation of generalised bent function (GBF) is derived. Using this condition, a set of Diophantine equations whose solvability is a necessary condition for the existence of GBF is also derived. Examples to demonstrate how these equations can be utilised to establish non-existence and regularity of GBFs is presented.

Keywords: Generalised bent function; Regular bent function; Diophantine equations

1. INTRODUCTION

Bent Boolean functions were introduced by Rothaus[1], in 1976. A bent function is a function of even number of variables which possesses maximum non-linearity. Because of the very nature of possessing the highest possible non-linearity, bent functions drew attention of researchers from varied fields namely cryptography, coding theory, combinatorial design and communication systems. With the advent of generalised Boolean function, the term generalised bent function came into existence. This concept was propounded by Kumar[2], *et al.* in 1985. Generalised bent functions (GBFs) are the generalised bent Boolean functions[10,11,14,15] having a flat generalised Walsh Hadamard spectrum.

Two types of generalised Boolean function are considered. They are type I and type II generalised Boolean functions. For positive integers $n, q \geq 2$ we define a generalised Boolean function of type I as a function $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/q\mathbb{Z}$. We define generalised Walsh Hadamard transform of f as the map from $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}(\zeta)$, given as:

$$W_f(w) = \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)} (-1)^{w.x} \quad (1)$$

where ζ being a primitive q^{th} root of unity in C and $w.x$ being the dot product of vectors w and x defined as $w.x = \sum_{i=0}^{n-1} x_i w_i \bmod q$. It is easy to observe that $W_f(w)$ belongs to the ring of integers $\mathbb{Z}(\zeta)$. For positive integers $n, q \geq 2$, a generalised Boolean function of type II is a function $f : (\mathbb{Z}/q\mathbb{Z})^n \to \mathbb{Z}/q\mathbb{Z}$. In this case the generalised Walsh Hadamard transform of f is given as

$$W_f(w) = \sum_{x \in \mathbb{Z}_q^n} \zeta^{\{f(x) - w.x\}} \quad (2)$$

A generalised Boolean function of type I is said to be a generalised bent function if for every $w \in (\mathbb{Z}/2\mathbb{Z})^n$, we have

$$|W_f(w)| = 2^{\frac{n}{2}} \quad (3)$$

and another generalisation of Boolean function of type II is said to be generalised bent function if for every $w \in (\mathbb{Z}/q\mathbb{Z})^n$,

$$|W_f(w)| = q^{\frac{n}{2}} \quad (4)$$

Given positive integers $n, q \geq 2$, when a generalised Boolean function f of either type is bent, we call it $[n, q]$ GBF. It is easy to observe that for both of the generalised Boolean function $W_f(w) \in \mathbb{Z}(\zeta)$ and only the magnitude value will be different.

It is not always possible to have a $[n, q]$ GBF for every[3,5,6] $q, n \in N, q > 1$. A lot of conditions on n and q have been found under which a $[n, q]$ generalised bent function does not exist. Feng[7,14], *et al.* had shown the non-existence of GBF for some values of q from the properties of solutions of some Diophantine equations they found for GBF.

Detection of non-existence of bent function under different conditions is important[8,9]. Several constructions of bent functions have been proposed in the literatures which are used in crypto design and further work in this direction is going on[10,15]. Knowledge of non-existence of GBF often saves a cryptographer from a futile search for construction in the cases when a bent function ceases to exist.

We derive a general expression for Walsh transformation of $[n, q]$generalised bent function and obtain a necessary condition for existence of $[n, q]$GBF. In the later section,

Received : 13 September 2016, Revised : 15 April 2017
Accepted : 20 April 2017, Online published : 19 September 2017

we have shown that for an odd prime q, it is possible to put this necessary condition in form of a system of Diophantine equations. And how the system of equations can be utilised to establish non-existence or regularity of $[n,q]$GBF, q being an odd prime.

2. NECESSARY CONDITION FOR EXISTENCE OF $[n,q]$GBF

A generalised Boolean function f, defined earlier is bent if the magnitude of its Walsh transform i.e., $|W_f(w)|$ is constant. It is equal to $2^{\frac{n}{2}}$ in case of type I functions and $q^{\frac{n}{2}}$ otherwise. In other words, a generalised Boolean function f of type I is bent only if given $w \in (\mathbb{Z}/2\mathbb{Z})^n$, $|W_f(w)| = 2^{\frac{n}{2}}$. Similarly a generalised Boolean function f of type II is bent only when for given $w \in (\mathbb{Z}/q\mathbb{Z})^n$, $|W_f(w)| = q^{\frac{n}{2}}$. We first derive a general expression of Walsh transformation of f and then obtain the necessary condition for existence of GBF using the above relations.

2.1 Walsh Transformation of $[n,q]$GBF

The following theorem expresses Walsh transformation of f as integer linear combination of the quantities

$$\cos\frac{2k\pi}{q}, k = 0,1,...,\left\lfloor \frac{q-1}{2} \right\rfloor$$

Theorem 2.1 Let f be a $[n,q]$generalised Boolean function. Then for given

$$w \in (\mathbb{Z}/q\mathbb{Z})^n$$

$$|W_f(w)|^2 = i_0 + 2\sum_{u=1}^{\left\lfloor \frac{q-1}{2} \right\rfloor} i_u \cos\frac{2\pi u}{q}$$

where $i_0, i_1, ..., i_{\left\lfloor \frac{q-1}{2} \right\rfloor}$ are some positive integers.

Proof: For generalised bent function f, $W_f(w) \in \mathbb{Z}(\zeta)$, where $\zeta = e^{\frac{2i\pi}{q}}$, then there exist positive integers $a_0, a_1, ..., a_{q-1}$ such that

$$W_f(w) = \sum_{i=0}^{q-1} a_i \zeta^i \tag{5}$$

From Eqns. (4) and (5) we have,

$$\sum_{i=0}^{q-1} a_i = q^n \tag{6}$$

Observe that $\overline{\zeta^k} = \zeta^{-k}$ and $\overline{\zeta^k}\zeta^k = |\zeta^k|^2 = 1 \Rightarrow \overline{(\zeta^k)} = \zeta^{-k}$. Therefore,

$$\overline{W_f(w)} = \sum_{i=0}^{q-1} a_i \overline{(\zeta^i)} = \sum_{i=0}^{q-1} a_i \zeta^{-i}$$

We have,

$$\begin{aligned} W_f(w)\overline{W_f(w)} = |W_f(w)^2| &= \sum_{i=0}^{q-1} a_i \zeta^i \cdot \sum_{i=0}^{q-1} a_i \zeta^{-i} \\ &= \sum_{i=0}^{q} \sum_{i=0}^{q-1} a_i a_j \zeta^{i-j} \\ &= \sum_{u=-(q-1)}^{q-1} C_u \zeta^u \\ &= \sum_{-(q-1)}^{-1} C_u \zeta^u + C_0 + \sum_{u=1}^{q-1} C_u \zeta^u \\ &= C_0 + \sum_{u=1}^{q-1} \left(C_{-u} \zeta^{-u} + C_u \zeta^u \right) \end{aligned} \tag{7}$$

where

$$C_u = \begin{cases} \sum_{i=0}^{q-1} a_i a_{i-u} & when \quad u \le 0 \\ \sum_{i=0}^{q-1} a_i^2 & when \quad u = 0 \\ \sum_{i=0}^{q-1} a_i a_{i-u} & when \quad u \ge 0 \end{cases} \tag{8}$$

The coefficients displayed in equation (8) are related as $C_u = C_{-u}$, for all $0 \le u \le q-1$.

In Eqn. (8) for $u = 0$, the equality holds, for $u > 0$ we have

$$C_{-u} = \sum_{i=0}^{q-1-u} a_i a_{i+u} = \sum_{i'=0}^{q-1} a_{i'} a_{i'-u} = C_u \text{ , using } i' = i - u$$

and for $u < 0$

$$C_{-u} = \sum_{i=-u}^{q-1} a_i a_{i+u} = \sum_{i'=0}^{q-1-u} a_{i'} a_{i'-u} = C_u \text{ , using } i' = i + u$$

Now for $q = 2k+1$, where k is any positive integer, Eqn. (7) can be written as

$$\begin{aligned} |W_f(w)|^2 &= C_0 + \sum_{u=1}^{q-1} C_u \left(\zeta^{-u} + \zeta^u \right) \\ &= C_0 + 2\sum_{u=1}^{q-1} C_u \Re\left(\zeta^u\right) \\ &= C_0 + 2\left(\sum_{u=1}^{k} C_u \Re\left(\zeta^u\right) + \sum_{u=k+1}^{2k} C_u \Re\left(\zeta^u\right) \right) \\ &= C_0 + 2\left(\sum_{u=1}^{k} C_u \Re\left(\zeta^u\right) + \sum_{u=k}^{1} C_{q-u} \Re\left(\zeta^u\right) \right) \text{ using } u = q - u' \\ &= C_0 + 2\left(\sum_{u=1}^{k} \left(C_u + C_{q-u}\right) \Re\left(\zeta^u\right) \right) \text{ using} \\ &\qquad \left(\Re\left(\zeta^u\right) = \Re\left(\zeta^{q-u}\right) \right) \\ &= C_0 + 2\left(\sum_{u=1}^{\frac{(q-1)}{2}} \left(C_u + C_{q-u}\right) \cos\frac{2\pi u}{q} \right) \end{aligned} \tag{9}$$

Similarly for $q = 2k$, where k is any positive integer, Eqn. (7) can be written as

$$\begin{aligned} |W_f(w)|^2 &= C_0 + \sum_{u=1}^{q-1} C_u \left(\zeta^{-u} + \zeta^u \right) \\ &= C_0 + 2\sum_{u=1}^{q-1} C_u \Re\left(\zeta^u\right) \end{aligned}$$

$$= C_0 + 2\left(\sum_{u=1}^{k-1} C_u \Re\left(\zeta^u\right) + C_{\frac{q}{2}} \Re\left(\zeta^{\frac{q}{2}}\right) \sum_{u'=k-1}^{1} C_{q-u'} \Re\left(\zeta^{q-u'}\right)\right)$$

$$= C_0 + 2C_{\frac{q}{2}} + 2\left(\sum_{u=1}^{k-1} C_u \Re\left(\zeta^u\right) + \sum_{u=1}^{k-1} C_{q-u} \Re\left(\zeta^{q-u}\right)\right);$$

$$\Re\left(\zeta^{\frac{q}{2}}\right) = 1,\ C_u = C_{q-u}$$

$$= C_0 + 2rC_{\frac{q}{2}} + 2\sum_{u=1}^{\frac{q-1}{2}} \left(C_u + C_{q-u}\right)\cos\frac{2\pi u}{q}. \quad (10)$$

Now combining Eqns. (9) and (10) we can write

$$\left|W_f\left(w\right)\right|^2 = i_0 + 2\sum_{u=1}^{\left\lceil\frac{q-1}{2}\right\rceil} i_u \cos\frac{2\pi u}{q} \quad (11)$$

where $i_0 = C_0 + 2rC_{\frac{q}{2}}$ for $r \in (0,1), r \equiv (q-1) \bmod (2)$ and $i_u = C_u + C_{q-u}$ for $u = 1,2,...,\left\lceil\frac{q-1}{2}\right\rceil$.

Corollary 1. The necessary and sufficient condition that a $[n,q]$ generalised Boolean function f is bent, is that for all $w \in Z_q^n$, the coefficients $C_0, C_1, ..., C_{q-1}$ as computed in theorem 2.1 satisfy the condition

$$t^n = i_0 + 2\sum_{u=1}^{\left\lceil\frac{q-1}{2}\right\rceil} i_u \cos\frac{2\pi u}{q} \quad (12)$$

where $i_0, i_1, ..., i_{\left\lceil\frac{q-1}{2}\right\rceil}$ are as defined in Eqn. (11) and t can be 2 or q according as f is of type I or type II function.

Proof: The property of Walsh spectrum follows the proof.

From corollary 1, it is clear that if we find at least one $w \in (\mathbb{Z}/q\mathbb{Z})^n$, for which Eqn. (12) is not satisfied then f is not a GBF. In other words, the emptiness of the solution set of Eqn. (12) ensures the non-existence of GBF. The following corollary tells this condition in a precise mathematical form.

Corollary 2. An $[n,q]$ type GBF does not exist if it is not possible to find the coefficients $i_0, i_1, ..., i_{\left\lceil\frac{q-1}{2}\right\rceil}$ satisfying Eqn. (12) corresponding to a set of positive integers $a_0, a_1, ..., a_{q-1}$ satisfying the relation

$$\sum_{i=1}^{q-1} a_i = t^n$$

The following theorems viz Theorem 2.2 and Theorem 2.3 are needed for formulation of Diophantine equations. Though the proof of Theorem 2.2 is straightforward, we produce it here for readability. Furthermore we are also making use of an expression arising out of the proof, for our subsequent calculations. For proof of Theorem 2.3, one may refer to[13].

Theorem 2.2 For any positive integers n, q we have

$$\cos\frac{2\pi u}{q} = g\left(\cos\frac{2\pi}{q}\right)$$

where g is an integer polynomial of degree u.

Proof: By De Moivre's theorem we know that

$$\cos\frac{2\pi u}{q} + i\sin\frac{2\pi u}{q} = \left(\cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}\right)^u$$

$$= \sum_{r=0}^{u} \binom{u}{r} \left(\cos\frac{2\pi}{q}\right)^r i\sin^{u-r}\frac{2\pi}{q}$$

Comparing real and imaginary part

$$\cos\frac{2\pi u}{q} = \sum_{r=0}^{u} (-1)^k \binom{u}{2k} \left(\cos\frac{2\pi}{q}\right)^{u-2k} \left(1-\cos^2\frac{2\pi}{q}\right)^k$$

Now we can see in the binomial expansion of $\left(1-\cos^2\frac{2\pi}{q}\right)^k$ the maximum degree of $\cos\frac{2\pi u}{q}$ is $2k$. In the above equality the maximum degree of $\cos\frac{2\pi u}{q}$ will go to u. So the degree of $\cos\frac{2\pi u}{q}$, will be u.

Theorem 2.3 For prime $q > 2$, Minimal polynomial of $\sin\frac{2\pi u}{q}$ and $\cos\frac{2\pi u}{q}$ is $P(x)$, of degree $q-1$ and $Q(x)$ of degree $(q-1)/2$, respectively[13] where,

$$P(x) = \sum_{k=0}^{\frac{q-1}{2}} (-1)^k {}_{2k+1}{}^qC \left(1-x^2\right)^{\left(\frac{q-1}{2}\right)-k} x^{2k}$$

and

$$Q(x) = P\left(\sqrt{\left(\frac{1-x}{2}\right)}\right)$$

Note that the minimal polynomial given in the above theorem need not be monic. In the next section we show how the necessary and sufficient conditions together convert to Diophantine equations when q is an odd prime.

3. NECESSARY CONDITION IN TERMS OF DIOPHANTINE EQUATIONS FOR ODD PRIME q

In corollary 2 we have discussed the necessary condition for existence of an $[n,q]$GBF. Now, we relate that necessary condition in terms of Diophantine equations for the case when q is an odd prime. For an odd prime, the minimal polynomial $Q(x)$of $\cos\frac{2\pi}{q}$, as given in Theorem 2.3

$$Q(x) = P\left(\sqrt{\frac{1-x}{2}}\right)$$

$$= \sum_{k=0}^{\frac{q-1}{2}} (-1)^k \binom{q}{2k+1} \left(1-\left(\sqrt{\frac{1-x}{2}}\right)^2\right)^{\left(\frac{q-1}{2}\right)-k} \left(\sqrt{\frac{1-x}{2}}\right)^{2k}$$

$$= \sum_{k=0}^{\frac{q-1}{2}} (-1)^k \binom{q}{2k+1} \left(1-\left(\frac{1-x}{2}\right)\right)^{\left(\frac{q-1}{2}\right)-k} \left(\frac{1-x}{2}\right)^k \quad (13)$$

Using Corollary 1 and Theorem 2.2 we have

$$0 = -t^n + i_0 + 2\sum_{u=1}^{\left\lceil \frac{q-1}{2} \right\rceil} i_u \sum_{k=0}^{\left\lfloor \frac{u}{2} \right\rfloor} (-1)^k \binom{u}{2k} \left(\cos\frac{2\pi}{q}\right)^{u-2k} \left(1-\cos^2\frac{2\pi}{q}\right)^k \quad (14)$$

This implies that $\cos\frac{2\pi}{q}$ also satisfies a polynomial $R(x)$ of integer coefficients where

$$R(x) = -t^n + i_0 + 2\sum_{u=1}^{\left\lceil \frac{q-1}{2} \right\rceil} i_u \sum_{k=0}^{\left\lfloor \frac{u}{2} \right\rfloor} (-1)^k \binom{u}{2k} (x)^{u-2k} \left(1-x^2\right)^k \quad (15)$$

Now for odd prime q the maximum power of the indeterminate x in Eqn. (15) will be u and the consequently maximum value of u will be $(q-1)/2$. Therefore the maximum power of x in $R(x)$ is $(q-1)/2$. From Theorem 2.3

Degree of $Q(x) = (q-1)/2 =$ Degree of $R(x)$

Since $Q(x)$ is the minimal polynomial of $\cos\frac{2\pi}{q}$ for some non-zero integers α and β we have

$\alpha R(x) = \beta Q(x)$

where α and β are chosen in a way that the highest degree coefficient of and $\beta Q(x)$ are equal. As $\alpha R(x) - \beta Q(x)$ essentially a zero polynomial, equating coefficients of $\alpha R(x) - \beta Q(x)$ to zero will give us a set of $(q-1)/2$ Diophantine equations in $a_0, a_1 ..., a_{q-1}$ We can put $x = 0,1,2,...$ alternatively in $\alpha R(x) - \beta Q(x)$ to obtain Diophantine equations.

In the next section we show the non-existence result of GBF from the Diophantine equation approach. However the results are not new but the method is totally different from those available in the literature.

3.1 Non-existence of $[n,5]$ GBFs of Type I

For $[n,5]$ GBF of type I, we have from Corollary 1.

$$2^n = i_0 + 2i_1\cos\frac{2\pi}{5} + 2i_2\cos\frac{4\pi}{5} \quad (16)$$

where

$$i_0 = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_0^2$$
$$i_1 = a_1a_0 + a_2a_1 + a_3a_2 + a_4a_3 + a_4a_0$$
$$i_2 = a_2a_0 + a_3a_1 + a_4a_2 + a_3a_0 + a_1a_4$$

Putting $\cos\frac{4\pi}{5} = 2\cos^2\frac{2\pi}{5} - 1$ in Eqn. (16) we have

$$0 = -2^n + i_0 - 2i_2 + 2i_1\cos\frac{2\pi}{5} + 4i_2\cos^2\frac{2\pi}{5} \quad (17)$$

It is clear from Eqn. (17) that $\cos\frac{2\pi}{5}$ satisfies polynomial of integer coefficients of degree 2, therefore we have

$R(x) = 4i_2x^2 + 2i_1x - 2^n + i_0 - 2i_2$

from Eqn. (13) we have

$Q(x) = 4x^2 + 2x - 1$

The highest power coefficient of $Q(x)$ and $R(x)$ are 4 and $4i_2$, respectively. Therefore $i_2Q(x) - R(x)$ must be a zero polynomial. Equating coefficients of $i_2Q(x) - R(x)$ to zero we have

$$2^n = i_0 - i_2 \quad (18)$$

$$i_1 = i_2 \quad (19)$$

Now from Eqn. (6) we have

$(a_0 + a_1 + a_2 + a_3 + a_4)^2 = 2^{2n}$

Which implies that,

$$\Rightarrow i_0 + 2i_1 + 2i_2 = 2^{2n} \quad (20)$$

For existence of GBF we have to check the integer solutions of above non-linear Diophantine equations.

Solving Eqns. (18), (19), and (20) we get

$$i_0 = \frac{4.2^n + 2^{2n}}{5} \text{ and } i_1 = i_2 = \frac{4.2^n - 2^{2n}}{5}$$

To find existence of GBF, we have to find the solution set of the polynomial Diophantine[16] equations given as

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 = \frac{4.2^n + 2^{2n}}{5} \quad (21)$$

$$a_1a_0 + a_2a_1 + a_3a_2 + a_4a_3 + a_4a_0 = \frac{2^{2n} - 2^n}{5} \quad (22)$$

$$a_2a_0 + a_3a_1 + a_4a_2 + a_3a_0 + a_4a_1 = \frac{2^{2n} - 2^n}{5} \quad (23)$$

It is clear from Eqn. (22) that 5 must divide $2^{2n} - 2^n$.

$\Rightarrow 2^{2n} \equiv 2^n \bmod (5)$

$\Rightarrow 2^n \equiv 1 \bmod (5)$ as $\gcd(2^n, 5) = 1$

$\Rightarrow$ must be a multiple of 4 as the order of 2 in $\mathbb{Z}_5^*$ is 4. Therefore the possible values of n for which we can expect solutions of the system of Diophantine equations are for $n = 4,8,12$ and so on.

Exhaustively we checked that there are no solutions to the system of equations for $n = 4,8$ and 12, therefor $[n,5]$ GBF do not exist for $n < 16$.

Apart from an establishing non-existence, this approach can also be used to prove regularity of GBF. In the following section we prove regularity of GBF in a case not reported earlier.

3.2 Regular Bent Function

A generalised bent function $f : (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})$ is called regular bent function if each of its Walsh coefficient value can be written as

$W_f(w) = q^{n/2}\zeta^{g(w)}$

where g is any q valued function. Function g is also called dual of f. Generalised bent functions are not always regular. For $q = 2$ a bent function is always regular Boolean function. Kumar[2], *et. al.* had shown the existence of regular bent function for various values of q and n. Our analysis determines a new case for the existence of regular bent functions. Next two theorems demonstrate the existence of regular bent functions for $n = 2$ and $q = 5$.

Theorem 3.1[11] Let $n = 2k$ where k and h are any two positive integers, q is any prime number then there always

exist a GBF $f:(\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q^h\mathbb{Z})$.

Theorem 3.2 A generalised bent function $f:(\mathbb{Z}/5\mathbb{Z})^2 \to (\mathbb{Z}/5\mathbb{Z})$ is always regular.

Proof: Theorem 3.1 ensures existence of GBFs from $(\mathbb{Z}/5\mathbb{Z})^n \to (\mathbb{Z}/5\mathbb{Z})$. Simplifying Eqn. (15) for we can obtain the corresponding Diophantine equations. Consequently Eqns. (18), (19), and (20) for $t=5$ and $n=2$ can be rewritten as

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 = 145 \quad (24)$$

$$a_0a_1 + a_2a_1 + a_3a_2 + a_4a_3 + a_4a_0 = 120 \quad (25)$$

$$a_0a_2 + a_3a_1 + a_4a_2 + a_3a_0 + a_4a_1 = 120 \quad (26)$$

We have computed the solutions of the above system of equations using exhaustive search. The set of solutions for (a_0,a_1,a_2,a_3,a_4) can be written as $\{(1,6,6,6,6),(6,1,6,6,6),(6,6,1,6,6),(6,6,6,1,6),(6,6,6,6,1)\}$

So according to each of above solutions the Walsh coefficients at any can be written in only five different ways i.e.

$$1+6\zeta+6\zeta^2+6\zeta^3+6\zeta^4;$$
$$6+\zeta+6\zeta^2+6\zeta^3+6\zeta^4;$$
$$6+6\zeta+\zeta^2+6\zeta^3+6\zeta^4;$$
$$6+6\zeta+6\zeta^2+\zeta^3+6\zeta^4;$$
$$6+6\zeta+6\zeta^2+6\zeta^3+\zeta^4;$$

Using the property of ζ or the 5th roots of unity i.e.

$$1+\zeta+\zeta^2+\zeta^3+\zeta^4=0$$

All possible different values of Walsh transformations can be written as

$$\{-5\zeta^0,-5\zeta^1,-5\zeta^2,-5\zeta^3,-5\zeta^4\}$$

From these expressions of $W_f(w)$ for all $w\in(\mathbb{Z}/5\mathbb{Z})^n$ and any 5-valued function f^* we can say that

$$W_f(x) = -5\zeta^{f^*(x)}$$

Hence we can say that *f* is regular where *f* * is dual of *f*.

4. CONCLUSION

In this paper a new approach for generalised Boolean function which is based on formulation of Diophantine equations is proposed. We have also shown by examples how this approach can be utilised to prove nonexistence of GBF or to prove regularity of GBF. We hope that this method will help to detect more cases when a GBF is regular or it ceases to exist.

REFERENCES

1. Rothaus, O.S. On 'bent' functions. *J. Combinatorial Theory Ser. A* , 1976, **20**(3), 300--305. doi: 10.1016/0097-3165(76)90024-8
2. Kumar, P.V.; Scholtz, R.A. & Welch, L.R. Generalized bent functions and their properties. *J. Combin. Theory Ser. A*, 1985, **40**(1), 90-107. doi: 10.1016/0097-3165(85)90049-4
3. Pei, Ding Yi. On nonexistence of generalized bent functions. Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), 165-172, Lecture Notes in Pure and *Appl. Math.,* 141, *Dekker, New York,* 1993.
4. Akyildiz, Ersan; Güloğlu, Ismail Ş. & İkeda, Masatoshi. A note of generalized bent functions. *J. Pure Appl. Algebra*, 1996, **106**(1), 1-9. doi: 10.1016/0022-4049(94)00006-9
5. Ikeda, Masatoshi. A remark on the non-existence of generalized bent functions. Number theory and its applications (Ankara, 1996), 109-119, Lecture Notes in Pure and Appl. Math., 204, Dekker, New York, 1999.
6. Feng, Keqin. Generalized bent functions and class group of imaginary quadratic fields. *Sci. China Ser. A* 2001, **44**(5), 562-570. doi:10.1007/BF02876704
7. Feng, Keqin & Liu, Fengmei. New results on the nonexistence of generalized bent functions. *IEEE Trans. Inform. Theory,* 2003, **49**(11), 3066-3071. doi:10.1109/TIT.2003.818388
8. Liu, Fengmei; Ma, Zhi & Feng, Keqin. New results on non-existence of generalized bent functions. II. *Sci. China Ser. A* 2002, **45**(6), 721-730. doi: 10.1360/02ys9079
9. Feng, Ke Qin & Liu, Feng Mei. Non-existence of some generalized bent functions. *Acta Math. Sin. (Engl. Ser.),* 2003, **19** (1), 39-50. doi: 10.1007/s10114-002-0228-0
10. Tokareva, N.N. Generalizations of bent functions: A survey of publications. *Translated Diskretn. Anal. Issled. Oper.,* 2010, **17**(1), 34-64. (Russian). doi: 10.1134/S1990478911010133
11. Pandey, S.K.; Mishra P.R. & Dass, B.K. A Maiorana-McFarland Construction of a GBF on Galois ring, ePrint Archive, 2016/097.
12. Gangopadhyay, Sugata; Pasalic, Enes & Stănică, Pantelimon. A note on generalized bent criteria for Boolean functions. *IEEE Trans. Inform. Theory,* 2013, **59**(5), 3233-3236. doi: 10.1109/TIT.2012.2235908
13. Beslin, Scott & De Angelis, Valerio. The Minimal Polynomials of $\sin\frac{2n\pi}{p}$ and $\cos\frac{2n\pi}{p}$. *Math. Mag.,* 2004, **77**(2), 146-149.
14. Liu, Feng Mei & Yue, Qin. The relationship between the nonexistence of generalized bent functions and Diophantine equations. *Acta Math. Sin. (Engl. Ser.)* 2011, **27** (6), 1173-1186. doi:10.1007/s10114-011-8198-8
15. Zhou, Zhengchun; Li, Nian; Fan, Cuiling & Helleseth, Tor. Linear codes with two or three weights from quadratic bent functions. *Des. Codes Cryptogr.,* 2016, **81**(2), 283-295. doi 10.1007/s10623-015-0144-9
16. Tripathi, A.; Harris & Kwong, C.H. Some necessary conditions for a real polynomial to have only real roots. *Crux Mathematicorum Mathe. Mayhem*, 2004, **30**(1), 102-105.

CONTRIBUTORS

Mr Shashi Kant Pandey has obtained his Master of science (Mathematics) in 2009, from Banaras Hindu University, Varanasi and currently pursuing his Ph.D. from Department of Mathematics, Delhi University. His area of interest include: Cryptography, Boolean function, Information theory, Combinatorics and discrete mathematics.
The work of this manuscript is part of his PhD thesis under the supervision of Prof. B.K. Dass.

Dr B.K. Dass is a retired professor and Head, Department of Mathematics and dean, Faculty of Mathematical sciences of University of Delhi. He earned two research degrees viz. Ph.D. in 1975 and D.Sc. in 1983. His research interests include: Coding theory, Information theory, Cryptography, Applied algebra and discrete mathematics. He has published over 100 research papers and edited 7 books.