Non-existence of \([n, 5]\) type Generalized Bent Functions

Shashi Kant Pandey  
Department of Mathematics,  
University of Delhi,  
Delhi-110007, India;  
P.R Mishra  
Scientific Analysis Group,  
Metcalfe House Complex, DRDO,  
Delhi-110054, India†  
B.K Dass  
Department of Mathematics,  
University of Delhi,  
Delhi-110007, India‡

September 14, 2014

Abstract

Search of rich boolean function for designing a good cryptosystem is most important. In this search from the infinite domain of integers, cases where rejection of integers for the existence of Generalized bent function is very helpfull. With the help of some necessary condition of GBF here we show the non existence of \([n,5]\) type Generalized Bent functions.

Keywords: Generalized Bent Function, Non Linearity.

\(^*\)shashikantshvet@gmail.com  
\(^†\)prasanna.r.mishra@gmail.com  
\(^‡\)dassbk@rediffmail.com
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 generalized Boolean function, the term generalized bent function came into existence. The concept was propounded by P. V. Kumar, R. A. Scholtz, and L. R. Welch [2] in 1985. Generalized bent functions are the generalized Boolean functions having a flat generalized Walsh Hadamard spectrum.

For positive integers $q, n$, $q \geq 2$ we define a generalized Boolean function as a function $f : (\mathbb{Z}/q\mathbb{Z})^n \rightarrow \mathbb{Z}/q\mathbb{Z}$. We define Generalized Walsh Hadamard transform of $f$ as the map from $(\mathbb{Z}/q\mathbb{Z})^n \rightarrow \mathbb{Z}(\zeta)$ given as

$$W_f(w) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}^n} \zeta^{f(x) - w \cdot x}$$  \hspace{1cm} (1)

$\zeta$ being a primitive $q^{th}$ root of unity in $\mathbb{C}$ and $w \cdot x$ being the dot product of vectors $w$ and $x$ defined as $w \cdot x = \sum_{i=0}^{n-1} x_i w_i \pmod{q}$. It is easy to observe that $W_f(w)$ belongs to the ring of integers $\mathbb{Z}(\zeta)$.

A generalized Boolean function $f : (\mathbb{Z}/q\mathbb{Z})^n \rightarrow \mathbb{Z}/q\mathbb{Z}$ is said to be a generalized bent function if for every $w \in (\mathbb{Z}/q\mathbb{Z})^n$, we have

$$|W_f(w)| = q^{n/2}. \hspace{1cm} (2)$$

We call $f$ an $[n,q]$ type generalized bent function.

It is not possible to have an $[n,q]$ type generalized bent function for every $q, n \in \mathbb{N}, q > 1$. A lot of conditions on $n$ and $q$ have been found under which an $[n,q]$ type generalized bent function does not exist. In the next section we discuss some of the conditions when an $[n,q]$ type generalized bent function does not exist. In section 3 we discuss a our approach towards finding condition for non-existence of generalized bent function. Using the approach we show that for all values of $n$ and $q = 5$, generalized bent functions do not exist.

2 Non-existence of $[n,q]$ type bent functions

Rothus [1] proved for the case when $q = 2$, that there exist a Bent function if and only if $n$ is even. Later [2] Kumar et al. constructed a generalized
Bent function for the case $n$ is even or $q \neq 2(1+2k)$, for some $k \in \mathbb{N}$. So far, there is no any generalized construction known for odd $n$. However, for odd $n$, there are many cases in which non-existence of generalized bent functions has been shown. Below are some more conditions where the non-existence of generalized bent function have been established:

Let $2 \nmid n \geq 1$ and $q = 2N, 2 \nmid N \geq 3$ \textsuperscript{[8]}

1. There exist an integer $s \geq 1$ such that $2^s \equiv -1 \pmod{N}$.

2. $n = 1, N = 7$

3. $n = 1, N = p^e$ where $e \geq 1$ $p$ is a prime, $p \equiv 7 \pmod{8}$ and $p \neq 7$.

4. $n = 1, N$ has prime factorization that $N = \prod p_i^{s_i}$ and for each $i$ there exist $s_i \leq 1$ such that $p_i^{s_i} \equiv -1 \pmod{\frac{N}{p_i}}$.

There are many results of non-existence based on Field descent method and condition (1) explored by Feng et.al. Jiang and Deng used the property of cyclotomic field $\mathbb{Q}(\zeta_{23e})$ to show the non-existence of bent functions for the case where $p = 2 \times 23^e$ and $n = 3$. Feng et.al. had shown many of non-existence results for Bent functions where all $p_i$s are primes and $n$ satisfied some conditions. Some of them are

(a) $N = p^e, p \equiv 7 \pmod{8}$ and $n \leq \frac{m}{n}$ where $m$ is smallest odd positive integer such that $x^2 + p\pi y^2 = 2^{m+2}$ has $\mathbb{Z}$-solution and $s = \frac{\phi(N)}{2f}$ $f$ is the order of 2 \pmod{N}.

(b) $N = p_1p_2^2, p_1 \equiv 3 \pmod{4}, p_2 \equiv 5 \pmod{8}, \left(\frac{p_1}{p_2}\right) = -1$.

(c) $N = p_1p_2^2, p_1 \equiv 3 \pmod{4}, p_2 \equiv 2^{\lambda+1} \pmod{2^{\lambda+1}}, \left(\frac{p_1}{p_2}\right) = -1, \left(\frac{2}{p_2}\right) \neq 1$.

(d) $N = p_1p_2, p_1 \equiv p_2 \equiv 7 \pmod{8}, \left(\frac{p_1}{p_2}\right) = -1$.

(e) $N = p_1p_2, p_1 \equiv 3 \pmod{8}, p_2 \equiv 7 \pmod{8}, \left(\frac{p_2}{p_1}\right) = -1$.

(f) $N = p_1p_2, p_1 \equiv 3 \pmod{8}, p_2 \equiv 7 \pmod{8}, \left(\frac{p_1}{p_2}\right) = -1$.

(g) $N = p_1p_2^2, p_1 \equiv 2^{\lambda+1} \pmod{2^{\lambda+1}}, \lambda \geq 3, p_2 \equiv 7 \pmod{8}, \left(\frac{p_1}{p_2}\right) = 1, \left(\frac{2}{p_2}\right) \neq 1, \left(\frac{2}{p_2}\right) \neq 1$.

(h) $N = p_1p_2, p_1 \equiv 5 \pmod{8}, p_2 \equiv 3 \pmod{4}, \left(\frac{p_1}{p_2}\right) = 1, \left(\frac{p_2}{p_1}\right) \neq 1$.

3
3 Our Approach

To show that a generalized Boolean function $f: (\mathbb{Z}/q\mathbb{Z})^n \to \mathbb{Z}/q\mathbb{Z}$ is bent, we have to show that it satisfy condition (2). In other words, to show that $f$ is not bent, we have to show that there exists $w \in (\mathbb{Z}/q\mathbb{Z})^n$ such that $|W_f(w)| \neq q^{n/2}$.

If we are able to prove that for a particular set of values of $q$ and $n$, if for any $f: (\mathbb{Z}/q\mathbb{Z})^n \to \mathbb{Z}/q\mathbb{Z}$,

$$|W_f(w)| \neq q^{n/2} \forall w \in (\mathbb{Z}/q\mathbb{Z})^n,$$

the non-existence of $[n,q]$ bent functions is guaranteed for the given set. Below we derive a necessary and sufficient condition for existence of $[n,q]$ type Generalized bent function.

Let $f$ be an $[n,q]$ type generalized bent function satisfying criterion (2). As $|W_f(w)| \in \mathbb{Z}(\zeta)$, $\zeta = e^{\frac{2\pi k}{q}}$, there exist integers $a_0, a_1, \ldots, a_{q-1}$ such that

$$W_f(w) = \sum_{i=0}^{q-1} a_i \zeta^i. \quad (3)$$

Form (1) and (3) we have,

$$\sum_{i=0}^{q-1} a_i = q^n. \quad (4)$$

Observe that $\tilde{\zeta}^k = \zeta^{-k}$ as $|\zeta^k|^2 = 1 \implies \tilde{\zeta}^k = \zeta^{-k}$. Therefore,

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

for odd primes $q$ we have,

$$W_f(w)\overline{W_f(w)} = |W_f(w)|^2 = \sum_{i=0}^{q-1} a_i \zeta^i \cdot \sum_{i=0}^{q-1} a_i \zeta^{-i}$$

$$= \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} a_i a_j \zeta^{i-j}$$

$$= i_0 + i_1 R(\zeta) + \ldots + i_{q-1} R(\zeta^{q-1}), \quad (5)$$

where $R(\zeta)$ is the real part of $\zeta$ and $i_l$ are some integers for $0 \leq l \leq \frac{q-1}{2}$.

Since $\zeta = \exp^{\frac{2\pi i}{q}}$, for existence of Bent function above equation can also be
written as

\[ z \times \bar{z} = p^n = i_0 + i_1 \cos \frac{2\pi}{q} + i_2 \cos \frac{4\pi}{q} + \ldots + i_{\frac{q-1}{2}} \cos \frac{2 \times \frac{q-1}{2} \pi}{q}. \quad (6) \]

For the existence of GBF solution of this equation is necessary in the domain of integer. So we are searching for the solution set \{i_0, i_1, \ldots, i_{\frac{q-1}{2}}\} in the integer domain and non-existence of this solution in this domain ensure us the non existence of generalized Bent function.

4 Non existence of \([n, 5]\) type generalized bent function

Based on the necessary and sufficient condition for existence of \([n,q]\) type Generalized bent function derived in previous section we show the case viz., \([n, 5]\) types of generalized bent functions do not exist.

4.1 Non existence of \([n, 5]\) type GBF

For \(q = 5\) condition (5) may be re-written as

\[ 5^n = i_0 + i_1 \cos \frac{2\pi}{5} + i_2 \cos \frac{4\pi}{5} \]

where,

\[
\begin{align*}
i_0 &= a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2, \\
i_1 &= 2(a_1 a_0 + a_2 a_1 + a_3 a_2 + a_4 a_3 + a_4 a_0), \\
i_2 &= 2(a_2 a_0 + a_3 a_2 + a_4 a_2 + a_3 a_0 + a_4 a_1).
\end{align*}
\]

It is known that

\[
\cos \frac{2\pi}{5} = -1 + \sqrt{5} \quad \text{and} \quad \cos \frac{4\pi}{5} = -1 - \sqrt{5} \quad \text{and} \quad \frac{4\pi}{5} = \frac{-1 - \sqrt{5}}{4}
\]

Putting the these values and separating the rational and irrational parts of (7) we get

\[ 5^n = i_0 - \frac{i_1 + i_2}{4}, \quad (8) \]

\[ i_1 = i_2. \quad (9) \]
From (4) we have

\[(a_0 + a_1 + a_2 + a_3 + a_4)^2 = 5^{2n} \]

\[\implies (a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2) + 2(a_1a_0 + a_2a_1 + a_3a_2 + a_4a_3 + a_4a_0)\]

\[+ 2(a_2a_0 + a_3a_2 + a_4a_2 + a_3a_0 + a_4a_1) = 5^{2n} \]

\[\implies i_0 + i_1 + i_2 = 5^{2n}. \quad (10)\]

For existence of GBF we have to check the integral solutions of non-linear system of equations given as,

Solving (8), (9) and (10) we get

\[i_0 = 4 \times 5^{n-1} + 5^{2n-1} \text{ and } i_1 = i_2 = 2(5^{2n-1} - 5^{n-1}) \]

To find existence of GBF, we have to find the solution set of the non-linear system of equations given as

\[a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 = 4 \times 5^{n-1} + 5^{2n-1} \quad (11)\]

\[a_1a_0 + a_2a_1 + a_3a_2 + a_4a_3 + a_4a_0 = (5^{2n-1} - 5^{n-1}) \quad (12)\]

\[a_2a_0 + a_3a_2 + a_4a_2 + a_3a_0 + a_4a_1 = (5^{2n-1} - 5^{n-1}) \quad (13)\]

\[2 \times (11) - 2 \times (12) - 2 \times (13) \text{ gives,} \]

\[
\sum_{i=0}^{4} \sum_{j=i+1}^{4} (a_i - a_j)^2 = 2 \times 5^{n-1}(2 - 5^n) \quad (14)
\]

Left side of (14) is non-negative while RHS is negative for all values of n. Hence solution set of the system is empty which ensures non-existence of \([n, 5]\) GBF.

5 Conclusion

In this way with the formulation of necessary equation for the existence of generalized bent function we show non existence of generalized bent function of type \([n, 5]\).

Acknowledgement

The work of this paper was supported by Dr P.K.Saxena (Director,SAG,DRDO) and Shri A.K.Bhateja(Scientist F,SAG,DRDO). I would like to express my spacial thanks of gratitude to both of them.
References


