Noname manuscript No.
(will be inserted by the editor)

A Maiorana-McFarland Construction of a GBF on Galois ring

Shashi Kant Pandey · P.R.Mishra · B.K.Dass

the date of receipt and acceptance should be inserted later

Abstract Bent functions shows some vital properties among all combinatorial objects. Its links in combinatorics, cryptography and coding theory attract the scientific community to construct new class of bent functions. Since the entire characterisation of bent functions is still unexplored but several construction on different algebraic structure is in progress. In this paper we proposed a generalized Maiorana-McFarland construction of bent function from Galois ring.
Keywords: Bent Function, Galois ring, Non Linearity.

1 Introduction

Rothous [1] was proposed the word Bent for the function having flat Walsh transformation. In this paper he showed various properties of bent functions over binary field. The importance of these functions in Cryptography and Coding theory attracts the scientific community very much so from beginning to till today these functions are playing important role in designing and analysing of a cryptosystem. Later Kumar, Scholtz and Welch generalized the function and called it generalized q-arey bent function. Proper characterisation of these functions is still a challenging problem and designing of a bent function gives a lot of clues about inner nature of these functions. Before the construction of a bent function on a specific finite algebraic structure it is always beneficial to differentiate the limitation of the existence and non existence of a q-ary function. A lot of construction is available in this direction on various algebraic

Shashi Kant Pandey · B.K. Dass
Department of Mathematics, University of Delhi, Delhi-110007, India,
E-mail: shashikantshvet@gmail.com
E-mail: dassbk@rediffmail.com

P.R. Mishra
Scientific Analysis Group, Metcalfe House Complex, DRDO, Delhi-110054, India
E-mail: prasanna.r.mishra@gmail.com

structures[2]. In parallel study of these functions people are exploring other functions having almost similar properties viz. planner function, APN functions, PN functions and almost bent functions. A large literature is available about the characterisation of these functions[3].

In this paper we are giving more generalized construction of a bent function based on a ring structure. Here the ring structure is a Galois ring of type $\mathrm{GR}(q^k, n)$, where q, k and n are any positive integers. Further distinguishing a field structure from the Galois ring and proposed a generalized construction over this field. Kai Schmidth explore several bent construction for CDMA code in[4]. He proposed a construction based on the $\mathrm{GR}(2^h, 1)$, where h is any integer. Taking similar practice we proposed a construction which is more general construction from Schmidth.

The background of bent function is available in section 2. The characterisation of Galois ring and the proof of leading theorem is available in section 3. Section 4 contains the description of construction of bent function.

2 Bent Function

The word Bent is first time proposed by Rothous for the functions having a spacial spectral property. Let q, p and n be any two positive integers and ζ_k be the k^{th} root of unity then the Walsh transformation of a function from ${Z_q}^n$ to Z_p is defined as

$$W_f(w) = \sum_{x \in {Z_q}^n} {\zeta_q}^{f(x)} {\zeta_p}^{w.x}, w \in {Z_q}^n \tag{1}$$

Where $w.x = (w_1.x_1 + w_2.x_2 + ... + w_n.x_n) \mod p$ for $w, x \in {Z_q}^n$. $\frac{W_f(w)}{\sqrt{q^n}}$ is called normalised Walsh transformation of f. The values of $W_f(w)$ are called the Walsh coefficient of f. To measure the distance between f and set of all linear and affine functions, these coefficients are useful. So maximum distance can be achievable when we have the optimum minimum value of $|W_f(w)|$. A function f is called bent if the minimum optimum value of $|W_f(w)| = \sqrt{q^n}$ for all $w \in {Z_q}^n$. A function $\hat{\mathrm{f}}$ from ${Z_q}^n$ to Z_p is called dual of f if $W_f(w) = \zeta^{\hat{f}}$. Not always Bent function exist for all integer values of p, q and n. Which makes it more interesting and rare among the combinatorial objects. There are other analogous functions available like planer function, APN, PN function etc. For $p = q = 2$ Bent function always exist for all even values of n and for odd n it may or may not exist. There are several cases available[5] for p, q and n where bent functions do not exist.

3 Galois Ring

The Galois ring is much similar as Galois field but there are some difference between the two algebraic structure. Specially they differ from the multiplicative

operation point of view. The major difference is that the division is not possible in general in a Galois ring whereas all the elements of a Galois field have their multiplicative inverse. The availability of multiplicative inverse gives a lot of analogous representation of an element in a Galois field. A Galois Ring have also various representation but many of the representation are remain unexplored.

Let p be a prime number n, m be any positive integers. The Galois ring $\mathrm{G}(p^n, m)$ is the extension of the ring Z_{p^n} of degree m. If g is a monic basic irreducible polynomial over Z_p^n of degree m then $\mathrm{GR}(p^n, m)$ can be seen as $Z_{p^n}[X]/ < g >$ having p^{mn} elements. Hence $\mathrm{GR}(p, m)$ is equivalent to the Galois field of order p^m. Let η be the primitive element in $\mathrm{GR}(p^n, m)$ of order $p^m - 1$ and $T_n = \{0, 1, \eta, \eta^2, ..., \eta^{p^m-2}\}$ is the Teichmuller set. Every element of $\mathrm{GR}(p^n, m)$ can be represented in two different way, for any $z \in GR(p^n, m)$
The multiplicative form:

$$z = \sum_{i=1}^{n} p^{i-1} t_i, t_i \in T_n \tag{2}$$

The additive form:

$$z = \sum_{i=0}^{n} a_i \eta^i, a_i \in Z_{p^n} \tag{3}$$

The set of Teichmuller representatives in $GR(p^n, 1)$ can also be seen as

$$F = \{z \in Z_{p^n} : z^{p^n} = z\}$$

So the multiplicative form of an element of $GR(p^n, 1)$ is basically its uniquely written p-adic expansion. Now we define two operations on F by $a \oplus b = (a + b)^{p^{n-1}}$ and $a \otimes b = a.b \mod p^n$ for all $a, b \in F$.

Lemma 1 *Let p be any prime and z be any integer, if $p \nmid z$ then $p^n \nmid z$.*

Lemma 2 *Let p be any prime and z be any integer, if $p \mid z$ then $p \nmid z^{p^n-1} - 1$.*

Theorem 31. *For any prime p,$(F, \oplus, \otimes)$ is a field and $|F| = p$.*

Proof It is clear that $0 \in F$. Now let any $0 \neq z \in F$. Then

$$z(z^{p^n-1} - 1) = 0 \tag{4}$$

Case1. If $p \nmid z$:
By Lemma1., p^n and z are relatively prime. Hence there exist two integers a, b such that

$$ap^n + bz = 1 \tag{5}$$

Taking modulo with p^n both side we get the multiplicative inverse of z in F.
Case2. If $p \mid z$:

By Lemma2. and above argument $z^{p^n-1}-1$ has multiplicative inverse. Therefore by the argument of equation 4 and 5, $z=0$. Hence in any case $0 \neq z \in F$, then z is a unit in Z_{p^n}. Note that units in Z_{p^n} form a group. Moreover ,if $Z^{\star}_{p^n}$ denote the group of units in Z_{p^n} then

$$Z^{\star}_{p^n} \cong C_{p-1} \oplus C_{p^{n-1}}. \tag{6}$$

Where C_n denotes the cyclic group of order n and $\oplus$ is the direct sum. Again, if $0 \neq z \in F$, then z is a unit and hence by equation 4, $z^{p^n-1}=1$. So the multiplicative order of z should also divides p^n-1. By equation 6 ,multiplicative order of z should also divides $(p-1)(p^{n-1})$. Which implies that multiplicative order of z divides $p-1$. Hence

$$z \in Z_{p-1} \subseteq C_{p-1} \oplus C_{p^{n-1}}$$

Or via any isomorphism ϕ on $Z^{\star}_{p^n}$

$$\phi(F-\{0\}) \subseteq Z_{p-1}$$

Now conversely suppose that $z \in C_{p-1} \subseteq C_{p-1} \oplus Z_{p^{n-1}}$. Note that Z_{p-1} is a subgroup of an isomorphic image of units of Z_{p^n}. Hence $z^{p-1}=1$. Thus $z^p = z \implies z^{p^2} = z^p = z$. Inductively $z^{p^n} = z \implies Z_{p-1} \subseteq F$ via isomorphism. Thus we have shown that $F-\{0\} \cong Z_{p-1}$. Hence $|F| = p$ as $0 \in F$.

The operation $\otimes$ is same as that of Z_{p^n} so obviously it is closed inder this. From case1. and 2. it is clear that every non zero element of F having multiplicative inverse in F.

Net, let $a, b \in F$. Then $a^{p^n} = a$ and $b^{p^n} = b$. If any of a and b is 0 then $a \oplus b \in F$ is trivial. So assume that $a \neq 0$ and $b \neq 0$ so $a^{p-1} = b^{p-1} = 1 \implies a^p = a$ and $b^p = b$. Also note that,

$$\begin{aligned} (a+b)^p &= a^p + b^p (\mod p) = a + b (\mod p) \\ \implies (a+b)^{p^2} &= (a+b)^p (\mod p) = a + b (\mod p) \end{aligned}$$

Inductively,

$$\begin{aligned} (a+b)^{p^n} &= a + b (\mod p) \\ \implies ((a+b)^{p^n})^{p^{n-1}} &= (a+b)^{p^{n-1}} (\mod p^n) \\ i.e & \\ (a \oplus b)^{p^n} &= a \oplus b \end{aligned}$$

Hence $a \oplus b \in F$. Now to show distribution of $\otimes$ over $\oplus$, Let $c \in F$ then,

$$\begin{aligned} c \otimes a \oplus c \otimes b &= (c \otimes a + c \otimes b)^{p^n} \\ &= c^{p^n} \otimes (a+b)^{p^n} \\ &= c \otimes (a \oplus b) \end{aligned}$$

Thus $(F, \oplus, \otimes)$ is a field of order p.

4 Construction of bent function from Galois Ring

On the basis of selection space of input variables there are other generalization of boolean function is available in litrature [6]. Here we are showing a generalized construction of Bent function from Galois rings.

Theorem 41. *Let π be a permutation on F^k, g be a function from F^k to Z_{p^h}, h and k are any two integers and the function $f : F^{2k} \mapsto Z_{p^h}$ is defined as*

$$f(x, y) = g(x) - p^{h-1}\pi(x).y.$$

Then f is a bent function.

Proof The coefficient walsh transform of f can be written as

$$\begin{aligned} W_f(u, v) &= \sum_{x,y \in F^k} \zeta_{p^h}^{g(x)-p^{h-1}\pi(x).y} \zeta_p^{u.x+v.y} \\ &= \sum_{x \in F^k} \zeta_{p^h}^{g(x)} \zeta_p^{u.x} \sum_{y \in F^k} (\zeta_p)^{(v-\pi(x)).y} \end{aligned}$$

If $\pi(x) \neq v$ then the inner sum will be zero and if $\pi(x) = v$ then the inner sum gives the value p^k. So we can write the walsh coefficient should be

$$W_f(u, v) = p^k \zeta_{p^h}^{g(\pi^{-1}(v))} \zeta_p^{u.\pi^{-1}(v)}$$

Hence f is bent.

References

1. O. S. Rothaus, On Bent functions, J.Comb.Theory(A) 20(1976),300-305.
2. Claude Carlet, A construction of Bent function,London mathematical Society Lecture Note Series 233.
3. Celine Blondeau ,Kaisa Nyberg, Perfect nonlinear function and cryptography, Finite Field and Their Applications 32(2015),120-147.
4. Kai-Uwe Schmidt, Quarternary Constant-Amplitude Codes for Multicode CDMA,arXiv:cs/0611162v2.
5. P.V Kumar, R.A Scholtz, L.R Welch,Generalized bent functions and their properties,Journal of Combinatorial Theory, Series A Volume 40, Issue 1,1985,90-107.
6. N.N.Tokareva, Generalizations of bent functions. A survey,Journal of Applied and Industrial Mathematics, Volume 5, Issue 1,2011,110-129.
7. q-ary Bent Functions Constructed from Chain Rings,Xiang-dong Hou,FINITE FIELDS AND THEIR APPLICATIONS4,5561 (1998).
8. Bjorn Abrahamsson, Architectures for Multiplication in Galois Rings,http://www.ep.liu.se/Linkping University Electronic Press.
9. Javier Gomez-Calderon, Gary L. Mullen, Galois ring and algebraic cryptography, Acta Arithmetica LIX4.1991,317-328.