Different method for counting the number of Quadratic functions with prescribed spectra

Arnab Ganguly[1] and Sankhadip Roy[2*]
[1] *Comscore, Reston, Virginia, United States and*
[2] *Department of Basic Science and Humanities, University of Engineering and Management, Kolkata-160, India*

In this correspondence we study a class of quadratic binary functions $\mathcal{F}_{2,n}$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, which are well-known to have plateaued Walsh spectrum; i.e., for each $b \in \mathbb{F}_{2^n}$ the Walsh transform $\hat{f}(b)$ satisfies $|\hat{f}(b)|^2 \in \{0, 2^{(n+s)}\}$ for some integer $0 \le s \le n-1$. For the type of integers $n = q_1 q_2$, where q_1, q_2 are two different odd primes, we determine possible values of s and present some enumeration results for counting the number of quadratic functions having those particular form of s.

Keywords: Quadratic Boolean functions, s-plateaued functions, self-reciprocal polynomials.

I. INTRODUCTION

In this correspondence we consider quadratic Boolean functions $\mathcal{F}_{p,n} : \mathbb{F}_{p^n} \to \mathbb{F}_p$, given in trace form: defined by

$$\mathcal{F}_{p,n}(x) = Tr(\sum_{i=0}^{k} a_i x^{p^i+1}), \tag{1}$$

where p is any prime, the coefficients $a_0, \ldots, a_k \in \mathbb{F}_p$, and Tr denotes the absolute trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
The *Walsh Transform* (or the *Fourier Transform*) of a p-ary function
$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ at $a \in \mathbb{F}_{p^n}$ is

$$\hat{f}(a) = \sum_{x \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x)-Tr(ax)}, \tag{2}$$

where ε_p is p-th root of unity. The *Walsh spectrum* of f is the set $\{\hat{f}(a) : a \in \mathbb{F}_{p^n}\}$. It is well-known that for each $a \in \mathbb{F}_{p^n}$ the Walsh transform $\hat{f}(a)$ satisfies $|\hat{f}(b)|^2 \in \{0, p^{(n+s)}\}$, where $0 \le s \le n-1$ is an integer. Since s is uniquely determined by a given quadratic function f, we call f *s-plateaued.*

For $p = 2$ it is obvious from (2) that $\hat{f}(a)$ for any $a \in \mathbb{F}_{2^n}$ is an integer. Therefore, the well-known bent functions or 0-plateaued functions are only defined for even n when $p = 2$. 1 or 2-plateaued functions are called semi-bent. Of course, in that case n and s need to have the same parity. Semi-bent functions have been studied widely especially for their importance in cryptography, see [1, 2, 4–6], and the references therein.

*Communication address: Email:sankhadip.roy@uem.edu.in

The question we address here are the following: for given prime p and an integer n, determine the integers s giving s-plateaued $\mathcal{F}_{p,n}$ and enumerate such $\mathcal{F}_{p,n}$ for some particular form of s.

Using standard Welch-squaring techniques one can see that the integer s is the dimension over $\mathbb{F}_p$ of the kernel of the linear transformation defined on $\mathbb{F}_{p^n}$ by

$$L(x) = \sum_{i=0}^{k} (a_i x^{p^i} + a_i^{p^{n-i}} x^{p^{n-i}}),$$

where $k = \lfloor (n-1)/2 \rfloor$ when $p = 2$ and $k = \lfloor n/2 \rfloor$ when $p \ge 3$. Also the kernel of L has dimension s if and only if the associates $A(x)$ of $L(x)$ and $x^n - 1$ of $x^{p^n} - x$, respectively, satisfy (see [7])

$$\deg(\gcd(A(x), x^n - 1)) = s. \tag{3}$$

The associate $A(x)$ corresponding to $\mathcal{F}_n$ in (1) is

$$A(x) = \sum_{i=0}^{k} (a_i x^i + a_i x^{n-i}) = x^{i_0} h(x), \tag{4}$$

where i_0 is the smallest integer such that $a_{i_0} \ne 0$, i.e., $h(0) \ne 0$, and $h(x) \in \mathbb{F}_p[x]$ is the self-reciprocal polynomial

$$h(x) = \sum_{i=i_0}^{k} a_i (x^{i-i_0} + x^{n-i_0-i})$$

of degree $n - 2i_0$.

II. PRELIMINARIES

In this section we discuss some results on self-reciprocal polynomials over finite fields. Recall that a polynomial $F(x)$ with non-zero constant term and of degree m over a finite field $\mathbb{F}_{p^r}$ is self-reciprocal if $F(x) = x^m F(1/x)$. We refer to [3, 7–9] for further reading. But we need to mention few important results on self-reciprocal polynomials.

 ©2019 Society for Makers, Artist ,Researchers and Technologists

Lemma 1 ([10])**.** *Let $F \in \mathbb{F}_{p^r}[x]$.*

(i) Let F be irreducible and of degree ≥ 2. F is self-reciprocal if and only if the set of roots of F is closed under inversion.

(ii) If F is self-reciprocal and $G \in \mathbb{F}_{p^r}[x]$, then FG is self-reciprocal if and only if G is self-reciprocal.

(iii) If F is an irreducible self-reciprocal polynomial of degree $m \geq 2$, then m is even.

(iv) If $F, G \in \mathbb{F}_{p^r}[x]$ are self-reciprocal, then $\gcd(F(x), G(x))$ is self-reciprocal.

Obviously when $p = 2$ the polynomial $x^n + 1 \in \mathbb{F}_2[x]$ is self-reciprocal, hence if $A(x) \in \mathbb{F}_2[x]$ is self-reciprocal, then $\gcd(x^n + 1, A(x))$ is self-reciprocal by Lemma 1(iv).

From equations (3),(4) and properties of self-reciprocal polynomials we have the following two theorems.

Theorem 1. *Let n be an arbitrary integer relatively prime to $p \geq 3$. There exists an s-plateaued quadratic function $\mathcal{F}_{p,n}$ if and only if*

1. *$x^n - 1$ has a self-reciprocal factor $h(x)$ of degree s, or*
2. *$x^n - 1$ has a self-reciprocal factor $h(x)$ of degree $s - 1$ where $s < n - 1$.*

Theorems 1 and (3) show that in order to determine the integers s for which there exists an s-plateaued function $\mathcal{F}_{p,n}$, we need to find self-reciprocal factors of $x^n - 1$. Hence we need to see the factorization of cyclotomic polynomials.

Suppose $n \geq 3$, and consider

$$x^n - 1 = \prod_{m|n} \mathcal{Q}_m, \tag{5}$$

where $\mathcal{Q}_m$ denotes the m-th cyclotomic polynomial. We then factorize $\mathcal{Q}_m$ into irreducibles $f_1 \cdots f_{\varphi(m)/d} \in \mathbb{F}_p[x]$, each of degree d, where $d = ord_m p$, and φ denotes the Euler-φ function. Here $ord_m p$ denotes the smallest integer l, such that $p^l \equiv 1 \bmod m$. We therefore have

$$\mathcal{Q}_m = f_1 \cdots f_{\varphi(m)/d} \quad \text{with} \quad f_t(x) = \prod_{j \in C_t} (x - \alpha^j), \tag{6}$$

where α is a primitive mth root of unity over $\mathbb{F}_{p^n}$, and $C_1, \ldots, C_{\varphi(m)/d}$ are the cyclotomic cosets modulo m relative to powers of p, containing the elements relatively prime to m, i.e., $C_1 = \langle p \rangle$ is the subgroup of $\mathbb{Z}_m^*$ generated by p, and $C_2, \ldots, C_{\varphi(m)/d}$ are its cosets.

Let $\nu(l)$ denote the p-adic valuation of an integer l, i.e., $p^{\nu(l)}$ is the largest power of p which divides l. In our result we will only consider the case $p = 2$.The following lemma is about the irreducible factors of $\mathcal{Q}_m$.

Lemma 2 ([10])**.** *Let $m = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$ be odd, relatively prime to p, $d_i = ord_{q_i} p$, $1 \leq i \leq k$, and $d = ord_m p$. Suppose the irreducible factors of $\mathcal{Q}_m$ are $f_1, \ldots, f_{\varphi(m)/d}$. Then*

(i) The polynomials $f_1, \ldots, f_{\varphi(m)/d}$ are self-reciprocal if and only if $\nu(d_1) = \nu(d_2) = \cdots = \nu(d_k) > 0$. In particular, if m is a prime, then $f_1, \ldots, f_{(m-1)/d}$ are self-reciprocal if and only if d is even.

(ii) If $\nu(d_i) \neq \nu(d_j)$ for some $1 \leq i, j \leq k$, then none of the polynomials f_t, $1 \leq t \leq \varphi(m)/d$, is self-reciprocal, and for each t, $1 \leq t \leq \varphi(m)/d$, there exists a unique $t' \neq t$, $1 \leq t' \leq \varphi(m)/d$, such that the product $f_t f_{t'}$ is self-reciprocal.

We need one more lemma for $p = 2$ before we state the main result.The proof is obviou.

Lemma 3. *The number of self-reciprocal polynomials over $\mathbb{F}_2$ of degree n is $2^{\frac{n}{2}}$ if n is even and $2^{\frac{n-1}{2}}$ if n is odd.*

III. MAIN RESULT

For $p = 2$ we have the following enumeration result.

Theorem 2. *Let $n = pq$, where p, q are distinct odd primes and $ord_p 2 = d_p, ord_q 2 = d_q$. The integer s for which there exists an s-plateaued quadratic function $\mathcal{F}_{p,n}$ are given as follows: $s < n$ and*

1. *if $\nu(d_p) = \nu(d_q) > 0$, then $s = 1 + k_1 lcm(d_p, d_q) + k_2 d_p + k_3 d_q$, where $0 \leq k_1 \leq \frac{(p-1)(q-1)}{lcm(d_p,d_q)} = \gamma(pq)$, $0 \leq k_2 \leq \frac{(p-1)}{d_p} = \gamma(p), 0 \leq k_3 \leq \frac{(q-1)}{d_q} = \gamma(q)$ and the number of s-plateaued functions for that particular representation of s is*

$$\eta \sum_{m=0}^{l} (-1)^m \sum_{\substack{i+j+k=m \\ N_1 \geq 0}} \lambda 2^{\frac{1}{2} N_1}$$

2. *if $\nu(d_p) > 0, \nu(d_q) > 0$ and $\nu(d_p) \neq \nu(d_q)$, then $s = 1 + 2k_1 lcm(d_p, d_q) + k_2 d_p + k_3 d_q$, where $0 \leq k_1 \leq \frac{(p-1)(q-1)}{2lcm(d_p,d_q)} = \gamma(pq)$, $0 \leq k_2 \leq \frac{(p-1)}{d_p} = \gamma(p), 0 \leq k_3 \leq \frac{(q-1)}{d_q} = \gamma(q)$ and the number of s-plateaued functions for that particular representation of s is*

$$\eta \sum_{m=0}^{l} (-1)^m \sum_{\substack{i+j+k=m \\ N_2 \geq 0}} \lambda 2^{\frac{1}{2} N_2}$$

3. *if $\nu(d_p) > 0, \nu(d_q) = 0$, then $s = 1 + 2k_1 lcm(d_p, d_q) + k_2 d_p + 2k_3 d_q$, where $0 \leq k_1 \leq \frac{(p-1)(q-1)}{2lcm(d_p,d_q)} = \gamma(pq)$, $0 \leq k_2 \leq \frac{(p-1)}{d_p} = \gamma(p), 0 \leq$*

$k_3 \leq \frac{(q-1)}{2d_q} = \gamma(q)$ and the number of s-plateaued functions for that particular representation of s is

$$\eta \sum_{m=0}^{l} (-1)^m \sum_{\substack{i+j+k=m \\ N_3 \geq 0}} \lambda 2^{\frac{1}{2}N_3}$$

4. *if $\nu(d_p) = \nu(d_q) = 0$, then $s = 1 + 2k_1 lcm(d_p, d_q) + 2k_2 d_p + 2k_3 d_q$, where $0 \leq k_1 \leq \frac{(p-1)(q-1)}{2lcm(d_p,d_q)} = \gamma(pq)$, $0 \leq k_2 \leq \frac{(p-1)}{2d_p} = \gamma(p), 0 \leq k_3 \leq \frac{(q-1)}{2d_q} = \gamma(q)$ and the number of s-plateaued functions for that particular representation of s is*

$$\eta \sum_{m=0}^{l} (-1)^m \sum_{\substack{i+j+k=m \\ N_4 \geq 0}} \lambda 2^{\frac{1}{2}N_4}$$

*where $l = \gamma(p) + \gamma(q) + \gamma(pq) - k_1 - k_2 - k_3$,
$\lambda = \binom{\gamma(pq) - k_1}{i}\binom{\gamma(p) - k_2}{j}\binom{\gamma(q) - k_3}{k}$ and
$\eta = \binom{\gamma(pq)}{k_1}\binom{\gamma(p)}{k_2}\binom{\gamma(q)}{k_3}$.
$N_1 = n - 2i_0 - s - ilcm(d_p, d_q) - jd_p - kd_q, N_2 = n - 2i_0 - s - 2ilcm(d_p, d_q) - jd_p - kd_q, N_3 = n - 2i_0 - s - 2ilcm(d_p, d_q) - jd_p - 2kd_q, N_4 = n - 2i_0 - s - 2ilcm(d_p, d_q) - 2jd_p - 2kd_q$.*

Proof. We just prove the first case as all the other cases would have the same arguments.
In case 1, $Q_p(x)$ has $\gamma(p)$,$Q_q(x)$ has $\gamma(q)$ and $Q_{pq}(x)$ has $\gamma(pq)$ irreducible self-reciprocal factors respectively. We need to count the number of self-reciprocal polynomials $g(x)$ of degree $(n - 2i_0)$ such that $\deg(g(x), x^n + 1) = s$. So $g(x) = h(x)f(x)$, where $h(x)$ is product of $(x + 1)$, k_1 irreducible factors of $Q_{pq}(x)$, k_2 irreducible factors of $Q_p(x)$ and k_3 irreducible factors of $Q_q(x)$ and $f(x)$ is self-reciprocal polynomial which doesnot contain any irreducible factor of $Q_p(x), Q_q(x)$ or $Q_{pq}(x)$. Let $f_1(x)$ be the product of remaining irreducible factors of $Q_p(x), Q_q(x)$ and $Q_{pq}(x)$which are not in $h(x)$. Then number of $g = \eta\cdot$ number of f.
Number of $f =$ number of self-reciprocal polynomials of degree $(n - 2i_0 - s)-$
[(number of self-reciprocal polynomials of degree $(n - 2i_0 - s)$with one irreducible factor of $f_1(x)-$ (number of self-reciprocal polynomials of degree $(n - 2i_0 - s)$ with two irreducible factors of $f_1(x)) + \cdots + (-1)^{m+1}$ (number of self-reciprocal polys of deg $(n - 2i_0 - s)$ with m irreducible factors from $f_1(x)) \cdots$]

$$= 2^{\frac{n-2i_0-s}{2}} - [(\binom{\gamma(p) - k_2}{1}2^{\frac{n-2i_0-s-d_p}{2}} + \binom{\gamma(q) - k_3}{1}2^{\frac{n-2i_0-s-d_q}{2}} + \binom{\gamma(pq) - k_1}{1}2^{\frac{n-2i_0-s-lcm(d_p,d_q)}{2}})$$

$$-(\binom{\gamma(p) - k_2}{2}2^{\frac{n-2i_0-s-2d_p}{2}} + \binom{\gamma(q) - k_3}{2}2^{\frac{n-2i_0-s-2d_q}{2}} + \binom{\gamma(pq) - k_1}{2}2^{\frac{n-2i_0-s-2lcm(d_p,d_q)}{2}}$$

$$+\binom{\gamma(p) - k_2}{1}\binom{\gamma(q) - k_3}{1}2^{\frac{n-2i_0-s-d_p-d_q}{2}} + \binom{\gamma(p) - k_2}{1}\binom{\gamma(pq) - k_1}{1}2^{\frac{n-2i_0-s-d_p-lcm(d_p,d_q)}{2}}$$

$$\cdots + \binom{\gamma(pq) - k_1}{1}\binom{\gamma(q) - k_3}{1}2^{\frac{n-2i_0-s-lcm(d_p,d_q)-d_q}{2}})$$

$$+(-1)^{m+1} \sum_{\substack{i+j+k=m \\ N_1 \geq 0}} \lambda 2^{\frac{1}{2}N_1} \cdots] = \sum_{m=0}^{l} (-1)^m \sum_{\substack{i+j+k=m \\ N_1 \geq 0}} \lambda 2^{\frac{1}{2}N_1}$$

where $l = \gamma(p) + \gamma(q) + \gamma(pq) - k_1 - k_2 - k_3$ and
$\lambda = \binom{\gamma(pq) - k_1}{i}\binom{\gamma(p) - k_2}{j}\binom{\gamma(q) - k_3}{k}$ and
$N_1 = n - 2i_0 - s - ilcm(d_p, d_q) - jd_p - kd_q$.

□

[1] C. Carlet and S. Mesnager, A note on Semi-bent Boolean functions, Cryptology ePrint Archive, Report no 486. http://eprint.iacr.org/2010/486.
[2] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51 (2005), 4286–4298.
[3] D. Jungnickel, Finite Fields-Structure and Arithmetic, BI Wiss. Verlag Mannheim, Leipzig, Wien, Zurich, 1993.
[4] K. Khoo, G. Gong, and D. R. Stinson, A new family of Gold-like sequences. In Proceedings of IEEE International Symposium of Information Theory (2002), p. 181.
[5] K. Khoo, G. Gong, D. Stinson, A new characterization of semi-bent and bent functions on finite fields, Designs, Codes and Cryptography 38 (2006), 279–295.
[6] G. Leander, G. McGuire, Construction of bent functions from near-bent functions, Journal of Combinatorial Theory, Series A 116 (2009), 960–970.
[7] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[8] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Eng. Comm. Comput. 1 (1990), 43–53.
[9] H. Stichtenoth, A. Topuzoğlu, Factorization of a class of polynomials over finite fields, Finite Fields Appl. 18 (2011), 108–122.
[10] W. Meidl, S. Roy, A. Topuzoğlu, *Enumeration of Quadratic Functions With Prescribed Walsh Spectrum,* IEEE,Transaction on Info, 60(2014),6669-6680.