On the nonlinearity of idempotent quadratic functions and the weight distribution of subcodes of Reed-Muller codes

Nurdagül Anbar, Wilfried Meidl, Alev Topuzo˘ Glu

On the nonlinearity of idempotent quadratic functions and the weight distribution of subcodes of Reed-Muller codes

Nurdagül Anbar[1], Wilfried Meidl[2], and Alev Topuzoğlu[3]

[1] Technical University of Denmark, Matematiktorvet, Building 303B, DK-2800, Lyngby, Denmark
nurdagulanbar2@gmail.com
[2] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria
meidlwilfried@gmail.com
[3] Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
alev@sabanciuniv.edu

Abstract. The Walsh transform $\widehat{Q}$ of a quadratic function $Q : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfies $|\widehat{Q}(b)| \in \{0, 2^{\frac{n+s}{2}}\}$ for all $b \in \mathbb{F}_{2^n}$, where $0 \leq s \leq n-1$ is an integer depending on Q. In this article, we investigate two classes of such quadratic Boolean functions which attracted a lot of research interest. For arbitrary integers n we determine the distribution of the parameter s for both of the classes, $\mathcal{C}_1 = \{Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}) \ : \ a_i \in \mathbb{F}_2\}$, and the larger class $\mathcal{C}_2$, defined for even n as $\mathcal{C}_2 = \{Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}) + \mathrm{Tr}_{n/2}(a_{n/2} x^{2^{n/2}+1}) \ : \ a_i \in \mathbb{F}_2\}$. Our results have two main consequences. We obtain the distribution of the nonlinearity for the rotation symmetric quadratic Boolean functions, which have been attracting considerable attention recently. We also present the complete weight distribution of the corresponding subcodes of the second order Reed-Muller codes.

1 Introduction

Omitting linear and constant terms, a quadratic function Q from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be expressed in trace form as

$$Q(x) = Q^{(n)}(x) = \mathrm{Tr_n}\Big(\sum_{i=1}^{\lfloor n/2 \rfloor} a_i x^{2^i+1}\Big), \quad a_i \in \mathbb{F}_{2^n}, \tag{1}$$

where Tr_n denotes the absolute trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. We use the notation $Q^{(n)}$ when we need to specify the integer n. If n is odd, this representation is unique. For even n the coefficient $a_{n/2}$ is taken modulo $\mathbb{F}_{2^{n/2}}$.

The *Walsh transform* $\widehat{f}$ of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the function from $\mathbb{F}_{2^n}$ into the set of integers defined as

$$\widehat{f}(b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr_n}(bx)}.$$

Quadratic Boolean functions belong to the class of *plateaued functions*, for which for every $b \in \mathbb{F}_{2^n}$, the Walsh transform $\widehat{f}(b)$ vanishes or has absolute value $2^{(n+s)/2}$ for some fixed integer $0 \leq s \leq n$. Accordingly we call f *s-plateaued*. Note that $\widehat{f}(b)$ is an integer, hence for any s-plateaued function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, n and s must be of the same parity. Recall that a 0-plateaued function is called *bent*, and depending on n being odd or even, a 1 or 2-plateaued Boolean function is called *semi-bent*. Clearly a Boolean bent function can only exist when n is even.
The *nonlinearity* N_f of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined to be the smallest Hamming distance of f to any affine function, i.e.

$$N_f = \min_{u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_2} |\{x \in \mathbb{F}_{2^n} \ : \ f(x) \neq \mathrm{Tr_n}(ux) + v\}|.$$

The nonlinearity of a Boolean function f can be expressed in terms of the Walsh transform as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}_{2^n}} |\widehat{f}(b)|. \tag{2}$$

By Parseval's identity we have $\sum_{b \in \mathbb{F}_{2^n}} \left|\widehat{f}(b)\right|^2 = 2^{2n}$ for any Boolean function f. As a consequence, bent functions are the Boolean functions attaining the highest possible nonlinearity. Since high nonlinearity is crucial for cryptographic applications, bent functions are of particular interest.
Recall that the rth order Reed-Muller code $R(r, n)$ of length 2^n is defined as

$$R(r, n) = \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_{2^m})) \mid f \in P_r\},$$

where P_r is the set of all polynomials from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ (or from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) of algebraic degree at most r, and $\alpha_1, \alpha_2, \ldots, \alpha_{2^m}$ are the elements of $\mathbb{F}_{2^n}$ (or $\mathbb{F}_2^n$) in some fixed order. The set of quadratic Boolean functions together with the constant and affine functions form the second order Reed-Muller codes.
Classes of quadratic functions (1) which attracted a lot of attention in the last decade are the classes

$$\mathcal{C}_1 = \{Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}) \ : \ a_i \in \mathbb{F}_2\},$$

and for even n

$$\mathcal{C}_2 = \{Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}) + \mathrm{Tr_{n/2}}(a_{n/2} x^{2^{n/2}+1}) \ : \ a_i \in \mathbb{F}_2, 1 \leq i \leq n/2\},$$

where all coefficients are in $\mathbb{F}_2$, see the articles [3, 4, 6–10]. If n is odd, then $\mathcal{C}_1$ is the class of the *idempotent* quadratic Boolean functions, which are defined by the property $Q(x^2) = Q(x)$ for all $x \in \mathbb{F}_{2^n}$. For even n the class of the idempotent quadratic Boolean functions is $\mathcal{C}_2$. As observed in [2] there is a nonlinearity preserving one-to-one correspondence between the set of idempotent quadratic

functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and the set of *rotation symmetric* quadratic functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Hence many results on idempotent quadratic functions also yield results on rotation symmetric quadratic functions, which makes the classes $\mathcal{C}_1$ and $\mathcal{C}_2$ even more interesting.
In this work we continue the research on these classes of quadratic functions. For technical reasons we include the 0-function, for which all coefficients a_i are zero in both sets $\mathcal{C}_1$ and $\mathcal{C}_2$. Being constant, the zero function is n-plateaued.
We now introduce

$$\mathcal{C} = \{Q^{(n)}(x) \ : \ Q^{(n)}(x) \in \mathcal{C}_1 \text{ for odd } n \text{ and } Q^{(n)}(x) \in \mathcal{C}_2 \text{ for even } n\}.$$

With this notation, $\mathcal{C}$ is the set of idempotent quadratic functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
The study of the Walsh spectrum of quadratic Boolean functions in $\mathcal{C}_1$ has been initiated in [7], where the authors determine all n for which all such quadratic Boolean functions are semi-bent. This result was extended in [3]. In the articles [6, 10] bent functions in $\mathcal{C}_2$ are constructed. The problem of counting the bent functions in $\mathcal{C}_2$ was solved in [10] for special classes of integers n. Enumeration results on Boolean quadratic functions in $\mathcal{C}_1$ with a large value of s have been obtained in the paper [4]. With methods originally used in the analysis of the linear complexity of periodic sequences (see [5]), far reaching counting results for the set $\mathcal{C}_1$ have been obtained in [8, 9]. In [8], the number $\mathcal{N}_n(s)$ of s-plateaued quadratic functions in $\mathcal{C}_1$ has been determined for $n = 2^m$, $m \geq 1$ and all possible values of s. The *generating polynomial* $\mathcal{G}_n(z)$, defined by

$$\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t,$$

was considered in [9] in order to describe $\mathcal{N}_n(s)$. This generating polynomial has been determined as a product of polynomials for all odd integers n and also for $n = 2m$, m odd. In particular, explicit formulas for the number of semi-bent functions in $\mathcal{C}_1$ have been obtained for such n. We remark that unlike $\mathcal{C}_2$, the set $\mathcal{C}_1$ does not contain bent functions.
In this work we extend the above results to functions in $\mathcal{C}_1$ and $\mathcal{C}_2$ for any arbitrary n, by determining,

(i) the generating polynomial $\mathcal{G}_n(z)$ for any (even) number n,
(ii) the generating polynomial $\mathcal{H}_n(z) = \sum_{t=0}^{n} \mathcal{M}_n(n-t) z^t$ for the number $\mathcal{M}_n(s)$ of s-plateaued functions in $\mathcal{C}_2$.

We therefore describe the distribution of the parameter s in the sets $\mathcal{C}_1$ and $\mathcal{C}_2$, hence completely determine the distribution of the nonlinearity in $\mathcal{C}_1$ and $\mathcal{C}_2$. In particular, we obtain the number of bent functions in the set $\mathcal{C}_2$ for arbitrary (even) integers n.
As mentioned above, there is a nonlinearity preserving one-to-one correspondence between the set of idempotent quadratic functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and the set of rotation symmetric quadratic functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Therefore we obtain

the distribution of the nonlinearity of rotation symmetric quadratic functions. We also analyse the subcodes of the second order Reed-Muller code obtained from $\mathcal{C}_1$ and $\mathcal{C}_2$, and present the weight distribution for both subcodes of $R(2,n)$.

2 Preliminaries

In this section we summarize basic tools that we use to obtain our results. In Sections 2 and 3, functions Q are assumed to be in $\mathcal{C}_1$ or $\mathcal{C}_2$. Let n be odd and let $Q(x) \in \mathcal{C}_1$, i.e. $Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{(n-1)/2} a_i x^{2^i+1})$, $a_i \in \mathbb{F}_2$. Then we can assign to Q the polynomial

$$A(x) = \sum_{i=1}^{(n-1)/2} (a_i x^i + a_i x^{n-i})$$

of degree at most $n-1$. When n is even we consider $Q(x) \in \mathcal{C}_2$; $Q(x) = \mathrm{Tr_n}(\sum_{i=1}^{n/2-1} a_i x^{2^i+1}) + \mathrm{Tr_{n/2}}(a_{n/2} x^{2^{n/2}+1})$, $a_i \in \mathbb{F}_2$, and the associated polynomial

$$A(x) = \sum_{i=1}^{n/2-1} (a_i x^i + a_i x^{n-i}) + a_{n/2} x^{n/2}$$

of degree at most $n-1$. Then the quadratic Boolean function $Q \in \mathcal{C}$ is s-plateaued, with

$$s = \deg(\gcd(x^n+1, A(x))),$$

see [8]. We observe that $A(x) = x^d h(x)$, where d is a positive integer and h is a self-reciprocal polynomial of degree $n-2d$. Hence $\gcd(x^n+1, A(x))$ is also self-reciprocal, and $A(x)$ can be written as

$$A(x) = x^d f(x) g(x),$$

where f is a self-reciprocal divisor of x^n+1 of degree s, and g is a self-reciprocal polynomial with degree smaller than $n-s$, satisfying $\gcd(g, (x^n+1)/f) = 1$. Obviously the factorization of x^n+1 into self-reciprocal factors plays an important role. In accordance with [8, 9], for a prime power q, we call a self-reciprocal polynomial $f \in \mathbb{F}_q[x]$ *prime self-reciprocal* if

(i) f is irreducible over $\mathbb{F}_q$, or
(ii) $f = ugg^*$, where g is irreducible over $\mathbb{F}_q$, the polynomial $g^* \neq g$ is the reciprocal of g and $u \in \mathbb{F}_q^*$ is a constant.

To analyze the factorization of x^n+1 into prime self-reciprocal polynomials, we recall the canonical factorization of x^n+1 into irreducible polynomials. Since $x^n+1 = (x^{n_1}+1)^{2^v}$ if $n = n_1 2^v$, n_1 odd, we can assume that n is odd. Let α be a primitive nth root of unity in an extension field of $\mathbb{F}_2$, and let $C_j =$

$\{j2^k \bmod n \ : \ k \in \mathbb{N}\}$ be the *cyclotomic coset* of j modulo n (relative to powers of 2). Then $x^n + 1 \in \mathbb{F}_2[x]$ can be factorized into irreducible polynomials as

$$x^n + 1 = \prod_{t=1}^{h} f_t(x) \quad \text{with} \quad f_t(x) = \prod_{i \in C_{j_t}} (x - \alpha^i),$$

where $C_{j_1}, \ldots, C_{j_h}$ are the distinct cyclotomic cosets modulo n.
In [8, 9] it is observed that an irreducible factor $f_t(x) = \prod_{i \in C_{j_t}} (x - \alpha^i)$ of $x^n + 1$ is self-reciprocal if and only if C_{j_t} contains with i, its additive inverse $-i$ modulo n. Otherwise there exists a cyclotomic coset C_{-j_t}, which consists of the additive inverses of the elements of C_{j_t}, and the polynomial $f_t^*(x) = \prod_{i \in C_{-j_t}} (x - \alpha^i)$ is the reciprocal of f_t. In this case $f_t f_t^*$ is a prime self-reciprocal divisor of $x^n + 1$. Most of our results are expressed in terms of the degrees of the prime self-reciprocal factors of $x^n + 1$. We remark that by Lemma 2 in [8], the cardinalities of the cyclotomic cosets modulo n, and the degrees of the prime self-reciprocal divisors of $x^n + 1$ can be obtained directly from the factorization of n.

3 Distribution of the nonlinearity

The generating polynomial $\mathcal{G}_n(z)$ for the number of s-plateaued quadratic functions in $\mathcal{C}_1$ has been determined in [8, 9] for all odd integers n, and also for even integers of the form $n = 2^m$, $m \geq 1$, and $n = 2m$, for odd m. Recall that for odd n, $\mathcal{C}_1$ is the set of idempotent quadratic functions. Our aim in this section is to determine both generating polynomials, $\mathcal{G}_n(z)$ and $\mathcal{H}_n(z)$ for all (even) integers n. This enables us to completely describe the distribution of the nonlinearity for the sets $\mathcal{C}_1$ and $\mathcal{C}_2$, and hence the set of the idempotent quadratic functions, for all integers n. Because of the observation of [2], that the nonlinearity distribution of the idempotent quadratic functions is the same as that of the rotation symmetric quadratic functions in n variables, we also give the complete distribution of the nonlinearity of the rotation symmetric quadratic functions. (Only even n is considered in [2], but the same applies to the case of odd n.)
We adapt the number theoretical approach in [9, Section V]. Let S_2 be the set of self-reciprocal polynomials in $\mathbb{F}_2[x]$. For a polynomial $f \in \mathbb{F}_2[x]$ we define

$$\begin{aligned} C(f) &= \{g \in S_2 \ : \ \deg(g) \text{ is even and } \deg(g) < \deg(f)\}, \\ K(f) &= \{g \in C(f) \ : \ \gcd(g(x), f(x)) = 1\}, \text{ and} \\ \phi_2(f) &= |K(f)|. \end{aligned}$$

Following the notation of [9], for a polynomial $f \in S_2$ we put

$$\mathcal{N}(f;t) := \begin{cases} 1 & \text{if } t = 0, \\ 0 & \text{if } t \text{ is odd}, \\ \sum_{d|f \text{ and } \deg(d)=t} \phi_2(d) & \text{otherwise} \end{cases}$$

and

$$\mathcal{G}_n(f;z) := \sum_{t \geq 0} \mathcal{N}(f;t) z^t \ .$$

Proposition 1. *Let n be even and let $\mathcal{N}_n(s)$ and $\mathcal{M}_n(s)$ be the number of s-plateaued quadratic functions in $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Then*

$$\mathcal{N}_n(s) = \mathcal{N}_n(\frac{x^n+1}{(x+1)^2}; n-s) \quad \textit{and} \quad \mathcal{M}_n(s) = \mathcal{N}_n(x^n+1; n-s).$$

Proof. The statement is clear when $n-s$ is zero or odd. Suppose $n-s>0$ is even. First we consider quadratic functions $Q \in \mathcal{C}_1$. For the corresponding associate polynomial $A(x)$ we have $\gcd(A(x), x^n+1) = (x+1)^2 f_1(x)$ for some self-reciprocal divisor f_1 of $(x^n+1)/(x^2+1)$ of degree $s-2$; i.e.

$$A(x) = x^c(x+1)^2 f_1(x) g(x)$$

for an integer $c \geq 1$ and a self-reciprocal polynomial g of even degree less than $n-s$, which is relatively prime to $d(x) = \frac{x^n+1}{(x+1)^2 f_1(x)}$. In other words, g is any of the $\phi_2(d)$ polynomials in $K(d)$. To determine the number $\mathcal{N}_n(s)$ we consider all divisors $(x+1)^2 f_1(x)$ of x^n+1 of degree s, or equivalently, all divisors $d(x)$ of $(x^n+1)/(x^2+1)$ of degree $n-s$. Hence we obtain $\mathcal{N}_n(s)$ as

$$\mathcal{N}_n(s) = \sum_{d \mid \frac{x^n+1}{(x+1)^2} \text{ and } \deg(d)=n-s} \phi_2(d) \ .$$

If $Q \in \mathcal{C}_2$, then the corresponding associate polynomial $A(x)$ satisfies $\gcd(A(x), x^n+1) = f_1(x)$, where f_1 is a self-reciprocal polynomial of degree s; i.e.

$$A(x) = x^c f_1(x) g(x)$$

for an integer $c \geq 1$ and a self-reciprocal polynomial g of even degree less than $n-s$, with $\gcd(g, \frac{x^n+1}{f_1(x)}) = 1$. Therefore $g \in K(d)$. As a consequence, the number of s-plateaued quadratic functions in $\mathcal{C}_2$ is

$$\mathcal{M}_n(s) = \sum_{d \mid (x^n+1) \text{ and } \deg(d)=n-s} \phi_2(d) \ ,$$

which finishes the proof. □

The following is the main theorem of this section. We sketch its proof.

Theorem 1. *Let $n = 2^t m$, m odd, $t>0$, and let $x^n+1 = (x+1)^{2^t} r_1^{2^t} \cdots r_l^{2^t}$, where $r_1, \ldots, r_l$ are prime self-reciprocal polynomials of even degree. The generating polynomial $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t$ is given by*

$$\mathcal{G}_n(z) = \left(1 + \sum_{j=1}^{2^{t-1}-1} 2^{j-1} z^{2j}\right) \prod_{i=1}^{l} \left(1 + \sum_{j=1}^{2^t} \left(2^{\frac{j \deg(r_i)}{2}} - 2^{\frac{(j-1)\deg(r_i)}{2}}\right) z^{j \deg(r_i)}\right),$$

and the generating polynomial $\mathcal{H}_n(z) = \sum_{t=0}^{n} \mathcal{M}_n(n-t) z^t$ is given by

$$\mathcal{H}_n(z) = \left(1 + \sum_{j=1}^{2^{t-1}} 2^{j-1} z^{2j}\right) \prod_{i=1}^{l} \left(1 + \sum_{j=1}^{2^t} \left(2^{\frac{j \deg(r_i)}{2}} - 2^{\frac{(j-1)\deg(r_i)}{2}}\right) z^{j \deg(r_i)}\right).$$

Sketch of proof. By Proposition 1 we have

$$\mathcal{G}_n(z) = \mathcal{G}_n(\frac{x^n+1}{x^2+1}; n-s) \quad \text{and} \quad \mathcal{H}_n(z) = \mathcal{G}_n(x^n+1; n-s). \tag{3}$$

From the definitions of $\mathcal{G}_n(f;t)$ and $\mathcal{N}_n(f;t)$, it is obvious that the properties of the function ϕ_2 play a crucial role. Using a Möbius function (and its properties) defined on the union of $\{(x+1)^2\}$ and the set of prime self-reciprocal polynomials of *even* degree, one can show that ϕ_2 is multiplicative, i.e.,

$$\phi_2(f_1 f_2) = \phi_2(f_1)\phi_2(f_2)$$

where $f_1, f_2 \in S_2$ are of even degree with $\gcd(f_1, f_2) = 1$. Furthermore one can derive formulas for $\phi_2(f)$, $f \in S_2$ with even degree, which also involve the Möbius function. In particular we have

$$\phi_2(((x+1)^2)^e) = 2^{e-1} \quad \text{and} \quad \phi_2(r^e) = 2^{\frac{e\deg(r)}{2}}(1 - 2^{-\frac{\deg(r)}{2}}) \tag{4}$$

for a prime self-reciprocal polynomial r of even degree.
By the multiplicativity of ϕ_2 one can show that also $\mathcal{G}_n(f;t)$ is multiplicative. Consequently we can determine $\mathcal{G}_n(z)$ and $\mathcal{H}_n(z)$ by (3) as

$$\mathcal{G}_n(z) = \mathcal{G}_n((x+1)^{2(2^{t-1}-1)}; z) \prod_{i=1}^{l} \mathcal{G}_n(r_i^{2^t}; z), \text{ and}$$
$$\mathcal{H}_n(z) = \mathcal{G}_n((x+1)^{2(2^{t-1})}; z) \prod_{i=1}^{l} \mathcal{G}_n(r_i^{2^t}; z).$$

When r is a prime self-reciprocal polynomial of even degree, (4) implies

$$\begin{aligned}\mathcal{G}_n(r^{2^t}; z) &= \sum_{j=0}^{2^t} \mathcal{N}_n(r^{2^t}; \deg(r^j)) z^{\deg(r^j)} \\ &= 1 + \sum_{j=1}^{2^t} \phi_2(r^j) z^{j\deg(r)} = 1 + \sum_{j=1}^{2^t} (2^{\frac{j\deg(r)}{2}} - 2^{\frac{(j-1)\deg(r)}{2}}) z^{j\deg(r)}.\end{aligned}$$

Moreover, since $\phi_2((x+1)^{2j}) = 2^{j-1}$, we have

$$\mathcal{G}_n(((x+1)^2)^{2^{t-1}}; z) = 1 + \sum_{j=1}^{2^{t-1}} 2^{j-1} z^{2j}$$

for an integer $t > 0$. Combining these formulas yields the assertion. □

Remark 1. Putting $t = 1$ and $m > 1$ in Theorem 1, one obtains $\mathcal{G}_n(z)$ in Theorem 5(ii) of [9]. Note that the Theorem 5(ii) in [9] contains an additional factor 2, since a quadratic function there may also have a linear term. Similarly the expression for $\mathcal{G}_n(z)$ with $m = 1$ gives Theorem 6 in [8].

Remark 2. Previous results on $\mathcal{G}_n(z)$, obtained in [9], were limited to the cases of odd n and even $n \equiv 2 \mod 4$. The method used there enabled the analysis of the functions $\phi_2(f)$, $\mathcal{N}_n(f;t)$, $\mathcal{G}_n(f;t)$ only for self-reciprocal polynomials f, which did not have $x+1$ as a factor. Similarly the Möbius function in [9] is defined on the set of self-reciprocal polynomials. Here considering the Möbius function on the union of $\{(x+1)^2\}$ and the set of prime self-reciprocal polynomials of *even* degree proved to be advantageous and has facilitated obtaining $\mathcal{G}_n(z)$ and $\mathcal{H}_n(z)$ in full generality.

As a corollary of Theorem 1 we obtain the number $\mathcal{M}_n(0)$ of bent functions in the set $\mathcal{C}_2$ as the coefficient of z^n in $\mathcal{H}_n(z)$ for arbitrary (even) integers n. This complements the results of [6, 10], where $\mathcal{M}_n(0)$ has been presented for the special cases $n = 2^v p^r$, where p is a prime such that the order of 2 modulo p is $p-1$ or $(p-1)/2$.

Corollary 1. *Let $n = 2^t m$, m odd, $t > 0$, and let $x^n + 1 = (x+1)^{2^t} r_1^{2^t} \dots r_l^{2^t}$, where $r_1, \cdots, r_l$ are prime self-reciprocal polynomials of even degree. Then the number of bent functions in $\mathcal{C}_2$ is*

$$\mathcal{M}_n(0) = 2^{2^{t-1}-1} \prod_{i=1}^{l} \left(2^{\frac{2^t \deg(r_i)}{2}} - 2^{\frac{(2^t-1)\deg(r_i)}{2}} \right),$$

which also is the number of rotation symmetric quadratic bent functions in n variables.

Similarly one may obtain $\mathcal{M}_n(s)$ for other very small values of s, see [9, Corollary 7] for the number of semi-bent functions in $\mathcal{C}_1$ when n is odd. To completely describe the nonlinearity distribution in $\mathcal{C}_1$ and $\mathcal{C}_2$ it is inevitable to consider the generating polynomial. To determine $\mathcal{M}_n(s)$ for a specific s individually, one first would have to find *all* possibilities to express s as a sum of degrees of polynomials in the prime self-reciprocal factorization of x^n+1, which for general n is illusive.

4 Weight distribution of subcodes of second order Reed-Muller codes

Let $\mathcal{Q}$ be a set of quadratic functions, which do not contain linear or constant terms. Assume that $\mathcal{Q}$ is closed under addition. Denote by $\mathcal{A} = \{\mathrm{Tr_n}(bx) + c \ : \ b \in \mathbb{F}_{2^n},\ c \in \mathbb{F}_2\}$ the set of affine functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then the set

$$\mathcal{Q} \oplus \mathcal{A} = \{Q(x) + l(x) \ : \ Q \in \mathcal{Q},\ l \in \mathcal{A}\}$$

gives rise to a linear subcode $\bar{R}_{\mathcal{Q}}$ of the second order Reed-Muller code $R(2,n)$, which contains the first order Reed-Muller code $R(1,n)$ as a subcode. Clearly, we can write $\mathcal{Q} \oplus \mathcal{A}$ as the union $\mathcal{Q} \oplus \mathcal{A} = \cup_{Q \in \mathcal{Q}} Q + \mathcal{A}$ of (disjoint) cosets of $\mathcal{A}$. To obtain the weight distribution of the code $\bar{R}_{\mathcal{Q}}$, it is sufficient to know the weight distribution for each of these cosets.

It can be seen easily that the weight of the codeword c_Q of a (quadratic) function Q can be expressed in terms of the Walsh transform as

$$wt(c_Q) = 2^{n-1} - \frac{1}{2}\widehat{Q}(0) \ .$$

For a quadratic function Q we define $Q_{b,c}(x) = Q(x) + \mathrm{Tr_n}(bx + c)$. Using $\widehat{Q_{b,c}}(0) = (-1)^{\mathrm{Tr_n}(c)}\widehat{Q}(b)$ one can show that the weight distribution of the coset $Q + \mathcal{A}$ for an s-plateaued quadratic function Q is as follows. There are

- 2^{n-s} codewords of weight $2^{n-1} + 2^{\frac{n+s}{2}-1}$,
- 2^{n-s} codewords of weight $2^{n-1} - 2^{\frac{n+s}{2}-1}$, and
- $2^{n+1} - 2^{n-s+1}$ codewords of weight 2^{n-1}.

Hence, if one knows the number of s-plateaued quadratic functions in $\mathcal{Q}$ for every s, one can determine the weight distribution of $\bar{R}_{\mathcal{Q}}$.
If $\mathcal{Q}$ is the set of all quadratic functions, then $\bar{R}_{\mathcal{Q}} = R(2, n)$. The weight distribution of $R(2, n)$ is completely described in [1] by explicit, quite involved formulas. Here we focus on the subcodes of $R(2, n)$, obtained from the set $\mathcal{C}$, in other words from the set of idempotent quadratic functions. Putting $k = n - s$ (which is even), the observations above imply that the only weights that can occur are 2^{n-1} and $2^{n-1} \pm 2^{n-1-\frac{k}{2}}$, $0 \le k \le n$. Moreover, codewords of the weights $2^{n-1} + 2^{n-1-\frac{k}{2}}$ and $2^{n-1} - 2^{n-1-\frac{k}{2}}$ appear the same number of times. Hence to describe the weight distribution of the codes $\bar{R}_{\mathcal{C}}$ we may consider the polynomial $\mathcal{W}_{\mathcal{C}}(z) = \sum_{k=0}^{n} A_k^{\mathcal{C}} z^k$, where $A_k^{\mathcal{C}}$ is the number of codewords in $\bar{R}_{\mathcal{C}}$ of weight $2^{n-1} \pm 2^{n-1-\frac{k}{2}}$. Again by the above observations, $A_k^{\mathcal{C}_1} = \mathcal{N}_n(n-k)2^k$ and $A_k^{\mathcal{C}_2} = \mathcal{M}_n(n-k)2^k$. Consequently,

$$\begin{aligned}
\mathcal{W}_{\mathcal{C}_1}(z) &= \sum_{k=0}^{n} A_k^{\mathcal{C}_1} z^k = \sum_{k=0}^{n} \mathcal{N}_n(n-k)2^k z^k = \mathcal{G}_n(2z), \\
\mathcal{W}_{\mathcal{C}_2}(z) &= \sum_{k=0}^{n} A_k^{\mathcal{C}_2} z^k = \sum_{k=0}^{n} \mathcal{M}_n(n-k)2^k z^k = \mathcal{H}_n(2z). \qquad (5)
\end{aligned}$$

For the number $A^{\mathcal{C}_1}$ of codewords in $\bar{R}_{\mathcal{C}_1}$ of weight 2^{n-1} we have

$$\begin{aligned}
A^{\mathcal{C}_1} &= \sum_{k=0}^{n} \mathcal{N}_n(n-k)(2^{n+1} - 2^{k+1}) = 2^{n+1}\sum_{k=0}^{n} \mathcal{N}_n(n-k) - 2\sum_{k=0}^{n} \mathcal{N}_n(n-k)2^k \\
&= 2^{n+1}\mathcal{G}_n(1) - 2\mathcal{G}_n(2) \ .
\end{aligned}$$

Similarly, $A^{\mathcal{C}_2} = 2^{n+1}\mathcal{H}_n(1) - 2\mathcal{H}_n(2)$.
The following theorem describes the weight distribution of the codes $\bar{R}_{\mathcal{C}}$ completely.

Theorem 2. *Let $n = 2^t m$ m odd, and let $x^n + 1 = (x+1)^{2^t} r_1^{2^t} \cdots r_l^{2^t}$ for prime self-reciprocal polynomials $r_1, \ldots, r_l$ of even degree. Then for even n*

$$\mathcal{W}_{\mathcal{C}_2}(z) = \sum_{k=0}^{n} A_k^{\mathcal{C}_2} z^k = \left(1 + \sum_{j=1}^{2^{t-1}} 2^{3j-1} z^{2j}\right) \prod_{i=1}^{l} \left(1 + \sum_{j=1}^{2^t} \left(2^{\frac{3j \deg(r_i)}{2}} - 2^{\frac{(3j-1)\deg(r_i)}{2}}\right) z^{j \deg(r_i)}\right),$$

and

$$A^{\mathcal{C}_2} = 2^{n+1+2^{t-1}} \prod_{i=1}^{l} \left(1 + \sum_{j=1}^{2^t} \left(2^{\frac{j \deg(r_i)}{2}} - 2^{\frac{(j-1)\deg(r_i)}{2}}\right)\right) - \frac{2^{3(2^{t-1}+1)}+6}{7} \prod_{i=1}^{l} \left(1 + \sum_{j=1}^{2^t} \left(2^{\frac{3j \deg(r_i)}{2}} - 2^{\frac{(3j-1)\deg(r_i)}{2}}\right)\right).$$

When $t = 0$, i.e. n is odd, we have

$$\mathcal{W}_{\mathcal{C}_1}(z) = \sum_{k=0}^{n} A_k^{\mathcal{C}_1} z^k = \prod_{i=1}^{l} \left[1 + (2^{3\deg(r_i)/2} - 2^{\deg(r_i)}) z^{\deg(r_i)}\right], \text{ and} \quad (6)$$

$$A^{\mathcal{C}_1} = 2^{\frac{3n+1}{2}} - 2 \prod_{i=1}^{l} \left(1 + (2^{3\deg(r_i)/2} - 2^{\deg(r_i)})\right).$$

Proof. By using (5), the formulas for $\mathcal{W}_{\mathcal{C}_1}(z)$ and $\mathcal{W}_{\mathcal{C}_2}(z)$ follow from $\mathcal{G}_n(z) = \prod_{i=1}^{l} \left[1 + (2^{\deg(r_i)/2} - 1) z^{\deg(r_i)}\right]$ when n is odd (see Theorem 5(i) in [9]) and Theorem 1. The formulas for $A^{\mathcal{C}_1}$ and $A^{\mathcal{C}_2}$ are obtained by expanding $2^{n+1}\mathcal{G}_n(1) - 2\mathcal{G}_n(2)$ and $2^{n+1}\mathcal{H}_n(1) - 2\mathcal{H}_n(2)$. □

Remark 3. When n is odd, the code $\bar{R}_{\mathcal{C}_1}$ has $2^{(3n+1)/2}$ codewords, i.e. $\dim(\bar{R}_{\mathcal{C}_1}) = (3n+1)/2$. Observing that the coefficient of z^k in (6) is not zero if and only if $k = \sum_{r_i \in \{r_1,\ldots,r_l\}} \deg(r_i)$, we conclude that $\bar{R}_{\mathcal{C}_1}$ is a $[2^n, (3n+1)/2, 2^{n-1} - 2^{n-1-\frac{r}{2}}]$ code, where $r = \min\{\deg(r_i)\}_{i=1}^{l}$.

References

1. Berlekamp, E.R., Sloane, N.: The weight enumerator of second-order Reed-Muller codes. IEEE Trans. Inform. Theory IT-16, 745-751 (1970)
2. Carlet, C., Gao, G., Liu, W.: A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. J. Combin. Theory, Series A 127, 161–175 (2014)
3. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51, 4286–4298 (2005)
4. Fitzgerald, R.W.: Trace forms over finite fields of characteristic 2 with prescribed invariants. Finite Fields Appl. 15, 69–81 (2009)
5. Fu, F. W., Niederreiter, H., Özbudak, F.: Joint linear complexity of multisequences consisting of linear recurring sequences. Cryptogr. Commun. 1, 3–29 (2009)
6. Hu, H., Feng, D.: On Quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory 53, 2610- 2615 (2007)
7. Khoo, K., Gong, G., Stinson, D.: A new characterization of semi-bent and bent functions on finite fields. Designs, Codes, Cryptogr. 38, 279–295 (2006)
8. Meidl, W., Topuzoğlu, A.: Quadratic functions with prescribed spectra. Designs, Codes, Cryptogr. 66, 257–273 (2013)
9. Meidl, W., Roy, S., Topuzoğlu, A.: Enumeration of quadratic functions with prescribed Walsh spectrum. IEEE Trans. Inform. Theory 60, 6669–6680 (2014)
10. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory 52, 3291–3299 (2006)