Technical University of Denmark

DTU

Idempotent and p-potent quadratic functions: distribution of nonlinearity and co-dimension

Anbar Meidl, Nurdagül; Meidl, Wilfried Meidl; Topuzoglu, Alev

Link back to DTU Orbit

DTU Library
Technical Information Center of Denmark

Idempotent and p-potent quadratic functions: Distribution of nonlinearity and co-dimension

This paper is dedicated to the memory of Tosun Terzioğlu

Nurdagül Anbar · Wilfried Meidl · Alev Topuzoğlu

Abstract The Walsh transform $\widehat{Q}$ of a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ satisfies $|\widehat{Q}(b)| \in \{0, p^{\frac{n+s}{2}}\}$ for all $b \in \mathbb{F}_{p^n}$, where $0 \le s \le n-1$ is an integer depending on Q. In this article, we study the following three classes of quadratic functions of wide interest. The class $\mathcal{C}_1$ is defined for arbitrary n as $\mathcal{C}_1 = \{Q(x) = \mathrm{Tr}_n(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}) \; : \; a_i \in \mathbb{F}_2\}$, and the larger class $\mathcal{C}_2$ is defined for even n as $\mathcal{C}_2 = \{Q(x) = \mathrm{Tr}_n(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}) + \mathrm{Tr}_{n/2}(a_{n/2} x^{2^{n/2}+1}) \; : \; a_i \in \mathbb{F}_2\}$. For an odd prime p, the subclass $\mathcal{D}$ of all p-ary quadratic functions is defined as $\mathcal{D} = \{Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}) \; : \; a_i \in \mathbb{F}_p\}$. We determine the generating function for the distribution of the parameter s for $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{D}$. As a consequence we completely describe the distribution of the nonlinearity for the rotation symmetric quadratic Boolean functions, and in the case $p > 2$, the distribution of the co-dimension for the rotation symmetric quadratic p-ary functions, which have been attracting considerable attention recently. Our results also facilitate obtaining closed formulas for the number of such quadratic functions with prescribed s for small values of s, and hence extend earlier results on this topic. We also present the complete weight distribution of the subcodes of the second order Reed-Muller codes corresponding to $\mathcal{C}_1$ and $\mathcal{C}_2$ in terms of a generating function.

Nurdagül Anbar
Technical University of Denmark, Matematiktorvet, Building 303B, DK-2800, Lyngby, Denmark
E-mail: nurdagulanbar2@gmail.com

Wilfried Meidl
Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria
E-mail: meidlwilfried

Alev Topuzoğlu
Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey.
E-mail: alev@sabanciuniv.edu

1 Introduction

Let p be a prime and let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then we can write f in polynomial form, for instance as the trace of a polynomial of degree at most $p^n - 1$. Clearly such a representation is not unique. Recall that the *algebraic degree* of f is the largest p-ary weight of an exponent in a polynomial representation of f. In this article we deal with functions Q from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of algebraic degree 2, which we call *quadratic functions*. The *degree* of a function on $\mathbb{F}_{p^n}$ will always refer to the polynomial degree, i.e. to the largest exponent of its (unique) representation as a polynomial of degree at most $p^n - 1$.

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

$$Q(x) = \mathrm{Tr}_{\mathrm{n}}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right) \ , \quad a_i \in \mathbb{F}_{p^n} \ , \tag{1}$$

where Tr_n denotes the absolute trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. When n is odd, this representation is unique. For even n the coefficient $a_{n/2}$ is taken modulo the additive subgroup $G = \{x \in \mathbb{F}_{p^n} \ : \ \mathrm{Tr}_{n/2}^n(x) = 0\}$ of $\mathbb{F}_{p^n}$, where $\mathrm{Tr}_{n/2}^n$ denotes the relative trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^{n/2}}$. Furthermore, if $p = 2$, then $a_0 = 0$, hence i in the summation in (1) ranges over $1 \le i \le \lfloor n/2 \rfloor$, since $a_0 x^2$ is a linear term.

The *Walsh transform* $\widehat{f}$ of a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the function from $\mathbb{F}_{p^n}$ into the set of complex numbers defined as

$$\widehat{f}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \mathrm{Tr}_n(bx)} \ ,$$

where $\epsilon_p = e^{2\pi i/p}$ is a complex p-th root of unity.

Quadratic functions belong to the class of *plateaued functions*, for which for every $b \in \mathbb{F}_{p^n}$, the Walsh transform $\widehat{f}(b)$ vanishes or has absolute value $p^{(n+s)/2}$ for some fixed integer $0 \le s \le n$. Accordingly we call f *s-plateaued*. Note that if $p = 2$, then $\epsilon_p = -1$, and $\widehat{f}(b)$ 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 from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called *bent*. Clearly a Boolean bent function can exist only when n is even. When p is odd, a 1-plateaued function is called *semi-bent*. A Boolean function f is called semi-bent, if f is 1 or 2-plateaued, depending on the parity of n.

The *nonlinearity* N_f of a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined to be the smallest Hamming distance of f to any affine function, i.e.

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

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

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

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, Boolean bent functions are the Boolean functions attaining the highest possible nonlinearity. Since high nonlinearity is crucial for cryptographic applications, Boolean bent functions are of particular interest.

Recall that the rth order Reed-Muller code $R(r, n)$ of length 2^n is defined as

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

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 $\alpha_1, \alpha_2, \ldots, \alpha_{2^n}$ 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.

In this work we focus on the subclasses of the set of quadratic functions given in Equation (1), obtained by restricting the coefficients to the prime subfield. Namely, for $p = 2$ we consider $\mathcal{C}_1$ and the larger class $\mathcal{C}_2$ defined as

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

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

Note that $\mathcal{C}_1$ is defined for arbitrary n, while $\mathcal{C}_2$ is defined for even n only. These two classes of Boolean functions have attracted significant attention in the last decade, see the articles [5, 6, 9, 11–13, 15–17]. For $p > 2$ we put

$$\mathcal{D} = \left\{ Q(x) = \mathrm{Tr_n}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} \right) : a_i \in \mathbb{F}_p \right\} .$$

The class $\mathcal{D}$ has also been studied previously, see [11, 12, 14–16].

The study of the Walsh spectrum of quadratic functions in $\mathcal{C}_1$ and $\mathcal{D}$ has been initiated in [12], where the authors determine all n for which all such

quadratic functions are semi-bent. This result was extended in [5] for $\mathcal{C}_1$. In the articles [9,17] bent functions in $\mathcal{C}_2$ are constructed.

Enumeration of functions in $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{D}$ for particular values of s has been a challenging problem. In [17] the number of bent functions in $\mathcal{C}_2$ was obtained for some special classes of n. Counting results on Boolean quadratic functions in $\mathcal{C}_1$ with a large value of s have been obtained in the paper [6]. Far reaching enumeration results for the sets $\mathcal{C}_1$ and $\mathcal{D}$ have been obtained in [11, 15,16] by the use of methods originally employed in the analysis of the linear complexity of periodic sequences, such as the method in [7].

Let us denote the number of s-plateaued quadratic functions in $\mathcal{C}_1$ and $\mathcal{D}$ by $\mathcal{N}_n(s)$ and $\mathcal{N}_n^{(p)}(s)$, respectively. In [15], the number $\mathcal{N}_n(s)$ has been determined for $n = 2^m$, $m \geq 1$, and all possible values of s, with combinatorial methods. In [16], $\mathcal{N}_n(s)$ and $\mathcal{N}_n^{(p)}(s)$ are described by the use of *generating polynomials* $\mathcal{G}_n(z)$ and $\mathcal{G}_n^{(p)}(z)$, defined by

$$\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t)z^t \quad \text{and} \quad \mathcal{G}_n^{(p)}(z) = \sum_{t=0}^{n} \mathcal{N}_n^{(p)}(n-t)z^t \ .$$

In the cases of odd n and $n = 2m$ for an odd m, the polynomial $\mathcal{G}_n(z)$ is determined as a product of polynomials, see [16]. Similarly $\mathcal{G}_n^{(p)}(z)$ is obtained for n with $\gcd(n,p) = 1$ in [4,16]. In particular, explicit formulas for the number of bent functions in $\mathcal{D}$ and of semi-bent functions in $\mathcal{C}_1$ are given for such n. For a result on the number of semi-bent functions in $\mathcal{C}_2$ we may refer to the recent article [13]. The average behaviour of the Walsh transform for many classes of functions in $\mathcal{C}_1$ and $\mathcal{D}$ is analysed in [11]. We remark that unlike $\mathcal{C}_2$, the set $\mathcal{C}_1$ does not contain bent functions.

We note that the main results in [16] are obtained by using the discrete Fourier transform. This method is only applicable when $\gcd(n,p) = 1$. Hence the study of the case $\gcd(n,p) > 1$ necessitates different methods. Moreover the discrete Fourier transform can not be used for the analysis of the the important class $\mathcal{C}_2$. In order to obtain $\mathcal{G}_n(z)$ when $n = 2m$ for odd m, a modification of the method that was used to analyse linear complexity of sequences in [7] was first employed in [16]. However the arguments in [16] heavily rely on the property, specific to the case studied in that paper, that the multiplicity of 1 as a root of $\gcd(x^n + 1, A(x))$ is exactly 2, where $A(x)$ is defined as in (3).

In this work we present the solution of the enumeration problem in full generality. We first extend the above results to functions in $\mathcal{C}_1$ and $\mathcal{C}_2$ *for arbitrary n and all possible s*, by determining,

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

Finally we adapt our method to the considerably more complicated case of functions in $\mathcal{D}$, and determine

(iii) the generating polynomial $\mathcal{G}_n^{(p)}(z)$ for any number n, $\gcd(n,p) > 1$.

We therefore completely describe the distribution of the parameter s in the set $\mathcal{C}_2$, and in the sets $\mathcal{C}_1$ and $\mathcal{D}$ in all remaining cases. This also yields the distribution of the nonlinearity in $\mathcal{C}_1$ and $\mathcal{C}_2$ in full generality. In particular, one can obtain the number of bent functions in the sets $\mathcal{C}_2$ and $\mathcal{D}$, or the number of semi-bent functions in $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{D}$ for arbitrary integers n.

Remark 1 The classes $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{D}$ have additional properties that we explain below. A Boolean function f, defined over $\mathbb{F}_{2^n}$ is *idempotent* if it satisfies $f(x^2) = f(x)$ for all $x \in \mathbb{F}_{2^n}$. The set of idempotent quadratic functions coincides with $\mathcal{C}_1$ when n is odd, and it coincides with $\mathcal{C}_2$ when n is even. For an odd prime p, one can similarly define a *p-potent* function as a function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ that satisfies $f(x^p) = f(x)$ for all $x \in \mathbb{F}_{p^n}$. As one would expect, the set of p-potent quadratic functions coincides with $\mathcal{D}$. It is observed in [3] that 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 $\mathbb{F}_2$. (Note that only even n is considered in [3], but the same applies to the case of odd n.) Following the arguments of [3], one can show that this property extends to any prime $p \geq 2$ and hence there is a one-to-one correspondence between the set $\mathcal{D}$ and the set of rotation symmetric quadratic functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, which preserves the parameter s. Hence many results on idempotent and p-potent quadratic functions also yield results on rotation symmetric quadratic functions, which add to the interest in the classes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{D}$.

Having obtained the distribution of s in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{D}$, we are able to give the distribution of the nonlinearity of rotation symmetric quadratic functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, and the distribution of the co-dimension of rotation symmetric quadratic functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, for odd p. 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. We essentially follow the notation of [15,16]. For technical reasons we include the 0-function, for which all coefficients a_i are zero, in all sets $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{D}$. Being constant, the zero function is n-plateaued.

Let $Q(x)$ be in $\mathcal{C}_1$, i.e. $Q(x) = \mathrm{Tr}_\mathrm{n}(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1})$, $a_i \in \mathbb{F}_2$. We associate to Q, the polynomial

$$A(x) = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} (a_i x^i + a_i x^{n-i}) \tag{3}$$

of degree at most $n - 1$. For even n we consider $Q(x) \in \mathcal{C}_2$, i.e. $Q(x) = \mathrm{Tr}_\mathrm{n}(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}) + \mathrm{Tr}_{\mathrm{n}/2}(a_{n/2} x^{2^{n/2}+1})$, $a_i \in \mathbb{F}_2$, and the associated poly-

nomial

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

of degree at most $n - 1$.

When p is odd and n is arbitrary we consider $Q(x) \in \mathcal{D}$, i.e. the quadratic function of the form $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, and the associated polynomial

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} (a_i x^i + a_i x^{n-i})$$

of degree at most n. With the standard Welch squaring method of the Walsh transform, one can easily see that in all three cases, the quadratic function Q is s-plateaued if and only if

$$s = \deg \left(\gcd(x^n - 1, A(x)) \right) ,$$

see also [8,12,14,17]. We observe that $A(x) = x^d h(x)$, where d is a non-negative integer and h is a self-reciprocal polynomial of degree $n - 2d$. Note that d is a positive integer in the case $p = 2$. When $Q(x) \in \mathcal{C}_1$ or $Q(x) \in \mathcal{C}_2$, and hence Q is a Boolean function, the polynomial $\gcd(x^n + 1, A(x))$ 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 $\gcd(g, (x^n + 1)/f) = 1$. When p is odd, then $x^n - 1 = (x-1)\psi(x)$, where $\psi(x) = 1 + x + \cdots + x^{n-1} \in \mathbb{F}_p[x]$ is self-reciprocal. Hence $\gcd(x^n - 1, A(x)) = (x-1)^\epsilon f(x)$, $\epsilon \in \{0, 1\}$, for a self-reciprocal divisor f of $x^n - 1$. Thus $A(x)$ can be written as

$$A(x) = x^d (x-1)^\epsilon f(x) g(x) ,$$

where g satisfies $\gcd(g, (x^n - 1)/((x-1)^\epsilon f)) = 1$.

Obviously the factorization of $x^n + 1$ and $\psi(x)$ into self-reciprocal factors plays an important role. In accordance with [15,16], 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 analyse the factorization of $x^n + 1$ and $(x^n - 1)/(x-1)$ into prime self-reciprocal polynomials, we recall the canonical factorization of $x^n - 1$ into irreducible polynomials. Since $x^n - 1 = (x^m - 1)^{p^v}$ if $n = mp^v$, $\gcd(m, p) = 1$, we can assume that n and p are relatively prime. Let α be a primitive nth root of unity in an extension field of $\mathbb{F}_p$, and let $C_j = \{jp^k \bmod n : k \in \mathbb{N}\}$ be the

cyclotomic coset of j modulo n (relative to powers of p). Then $x^n - 1 \in \mathbb{F}_p[x]$ 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.

It is observed in [15,16] that, when p is odd, an irreducible factor $f_t(x) = \prod_{i \in C_{j_t}} (x - \alpha^i)$ of $x^n - 1$, different from $x - 1$, 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 $f_t^*(x) = \prod_{i \in C_{-j_t}} (x - \alpha^i)$, which 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 [15], 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.

As explained above our aim is to determine the generating polynomials $\mathcal{G}_n(z)$ and $\mathcal{H}_n(z)$ for even n, and $\mathcal{G}_n^{(p)}(z)$ for $n = p^v m$, $v > 0$. This enables us to solve the problem of enumerating quadratic functions in the sets $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{D}$ with prescribed s. We adapt the number theoretical approach used in [16, Section V], by which the generating polynomial $\mathcal{G}_n(z)$ is obtained to yield the number of s-plateaued quadratic functions in $\mathcal{C}_1$ for the two cases; odd n and $n = 2m$, where m is odd. We start by giving some definitions and lemmas.

For a (self-reciprocal) polynomial $f \in \mathbb{F}_p[x]$ we define

$C(f) := \{g \in \mathbb{F}_p[x] \mid g$ is self-reciprocal, $\deg(g)$ is even, and $\deg(g) < \deg(f)\}$,
$K(f) := \{g \in C(f) \mid \gcd(g(x), f(x)) = 1\}$, and
$\phi_p(f) := |K(f)|$.

Let f be a monic self-reciprocal polynomial in $\mathbb{F}_p[x]$ with even degree. Let $f = r_1^{e_1} \cdots r_k^{e_k}$ be the factorization of f into distinct monic self-reciprocal polynomials all of *even degree*, i.e. either $r_1 = (x+1)^2$ and r_j, $2 \le j \le k$, are prime self-reciprocal polynomials, or r_j is prime self-reciprocal for all $1 \le j \le k$. Then we define the (following variant of the Möbius) function μ_p as

$$\mu_p(f) := \begin{cases} (-1)^k & \text{if } e_1 = \cdots = e_k = 1, \\ 0 & \text{otherwise.} \end{cases}$$

As for the classical Möbius function on the set of positive integers, we have

$$\sum_{d|f} \mu_p(d) = \begin{cases} 1 & \text{if } f = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where the summation is over all monic self-reciprocal divisors d of f of even degree.

Remark 2 Compare μ_p with the "Möbius function" used in [16], which is defined on the set of all self-reciprocal polynomials. Here considering the Möbius function on the set of self-reciprocal polynomials of *even degree*, where the set of the prime elements is 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 $\mathcal{G}_n(z)$, $\mathcal{H}_n(z)$ and $\mathcal{G}_n^{(p)}(z)$ in full generality.

The next lemma is Lemma 8 in [16], except that the condition on a self-reciprocal polynomial "not to be divisible by $x+1$" is replaced by the condition that it is of "even degree". The proof is similar to the one in [16] with this slight modification and hence we omit it.

Lemma 1 *[16, Lemma 8] Let $f \in \mathbb{F}_p[x]$ be a monic self-reciprocal polynomial whose degree is a positive even integer. Then*

$$\sum_{d|f} \phi_p(d) = p^{\frac{\deg(f)}{2}} - 1 \; ,$$

where the sum runs over all monic self-reciprocal divisors d of f of even degree.

The next lemma is again similar to Lemma 9 in [16], except that polynomials involved are of even degree. We give the proof for the convenience of the reader.

Lemma 2 *[16, Lemma 9] Let $f, f_1, f_2 \in \mathbb{F}_p[x]$ be monic self-reciprocal polynomials whose degrees are positive even integers.*

(i) We have

$$\phi_p(f) = \sum_{d|f} \mu_p(d) p^{\frac{\deg(f) - \deg(d)}{2}} \; ,$$

where the sum runs over all monic self-reciprocal divisors d of f of even degree.

(ii) If $f = f_1 f_2$ such that $\gcd(f_1, f_2) = 1$, then

$$\phi_p(f) = \phi_p(f_1)\phi_p(f_2) \; .$$

Proof. Taking the summation over all monic self-reciprocal divisors d of f of even degree, by Lemma 1 we get

$$\sum_{d|f} \mu_p(d)\left(p^{\frac{\deg(f)-\deg(d)}{2}} - 1\right) = \sum_{d|f} \mu_p\left(\frac{f}{d}\right)\left(p^{\frac{\deg(d)}{2}} - 1\right)$$

$$= \sum_{d|f} \mu_p\left(\frac{f}{d}\right)\sum_{d_1|d} \phi_p(d_1) = \sum_{d_1|f} \phi_p(d_1)\sum_{g|\frac{f}{d_1}} \mu_p(g) = \phi_p(f) \; ,$$

where in the last step we use the fact that the inner sum is 1 for $d_1 = f$ and 0 otherwise. With

$$\phi_p(f) = \sum_{d|f} \mu_p(d)\left(p^{\frac{\deg(f)-\deg(d)}{2}} - 1\right)$$

$$= \sum_{d|f} \mu_p(d) p^{\frac{\deg(f)-\deg(d)}{2}} - \sum_{d|f} \mu_p(d) = \sum_{d|f} \mu_p(d) p^{\frac{\deg(f)-\deg(d)}{2}},$$

we finish the proof for (i).

If $\gcd(f_1, f_2) = 1$, then $\mu_p(f_1 f_2) = \mu_p(f_1)\mu_p(f_2)$. Taking the summation over all monic self-reciprocal divisors d_i of f_i with $\deg(d_i)$ is even, $i = 1, 2$, we then have

$$\phi_p(f_1)\phi_p(f_2) = \sum_{d_1|f_1} \mu_p(d_1) p^{\frac{\deg(f_1)-\deg(d_1)}{2}} \sum_{d_2|f_2} \mu_p(d_2) p^{\frac{\deg(f_2)-\deg(d_2)}{2}}$$

$$= \sum_{\substack{d_1|f_1 \\ d_2|f_2}} \mu_p(d_1 d_2) p^{\frac{\deg(f_1 f_2)-\deg(d_1 d_2)}{2}} = \sum_{d|f} \mu_p(d) p^{\frac{\deg(f)-\deg(d)}{2}} \ ,$$

which shows (ii). □

For an integer t, we define $\mathcal{N}_n(f; t)$ by

$$\mathcal{N}_n(f; t) = \begin{cases} 1 & \text{if } t = 0 \\ \sum_{d|f, \deg(d)=t} \phi_p(d) & \text{if } t > 0 \text{ is even} \\ 0 & \text{otherwise,} \end{cases} \tag{4}$$

where the above sum runs over all monic self-reciprocal divisors d of f of degree t. Then we define the generating function $\mathcal{G}_n(f; z)$ for the distribution of the values $\mathcal{N}_n(f; t)$ by

$$\mathcal{G}_n(f; z) = \sum \mathcal{N}_n(f; t) z^t \ .$$

We note that $\mathcal{G}_n(f; z)$ is a polynomial by definition of $\mathcal{N}_n(f; t)$.

The next lemma and its proof resemble Lemma 10 in [16] for $p = 2$.

Lemma 3 *[16, Lemma 10] Let $f = f_1 f_2$ for two self-reciprocal polynomials f_1, f_2 of even degree. If $\gcd(f_1, f_2) = 1$, then*

$$\mathcal{G}_n(f; z) = \mathcal{G}_n(f_1; z)\mathcal{G}_n(f_2; z) \ .$$

Proof. We have to show that for each $t \geq 0$,

$$\mathcal{N}_n(f; t) = \sum_{0 \leq t_1 \leq t} \mathcal{N}_n(f_1; t_1)\mathcal{N}_n(f_2; t - t_1) \ .$$

For $t = 0$, $t > \deg(f)$ and t odd this is trivial. Assume that $1 \leq t \leq \deg(f)$ is even. Taking into account that $\phi_p(1) = 0$, by Lemma 2(ii), and the definition of $\mathcal{N}_n(f; t)$ we obtain

$$\sum_{0 \leq t_1 \leq t} \mathcal{N}_n(f_1; t_1)\mathcal{N}_n(f_2; t - t_1) = \mathcal{N}_n(f_1; 0)\mathcal{N}_n(f_2; t) + \mathcal{N}_n(f_1; t)\mathcal{N}_n(f_2; 0)$$

$$+ \sum_{\substack{1 < t_1 < t-1 \\ \text{even}}} \sum_{\substack{d_1|f_1 \\ \deg(d_1)=t_1}} \phi_p(d_1) \sum_{\substack{d_2|f_2 \\ \deg(d_2)=t-t_1}} \phi_p(d_2)$$

$$= \mathcal{N}_n(f_2; t) + \mathcal{N}_n(f_1; t) + \sum_{\substack{1 < t_1 < t-1 \\ \text{even}}} \sum_{\substack{d_1|f_1; \deg(d_1)=t_1 \\ d_2|f_2; \deg(d_2)=t-t_1}} \phi_p(d_1 d_2)$$

$$= \mathcal{N}_n(f_2; t) + \mathcal{N}_n(f_1; t) + \sum_{\substack{d|f \\ \deg(d)=t}} \phi_p(d) - \sum_{\substack{d_1|f_1 \\ \deg(d_1)=t}} \phi_p(d_1) - \sum_{\substack{d_2|f_2 \\ \deg(d_2)=t}} \phi_p(d_2)$$

$$= \mathcal{N}_n(f; t).$$

$\square$

Lemma 4 *Let r be a prime self-reciprocal polynomial of even degree. Then*

$$\mathcal{G}_n(r^k; z) = 1 + \sum_{j=1}^{k} (p^{\frac{\deg(r^j)}{2}} - p^{\frac{\deg(r^j)-\deg(r)}{2}}) z^{j\deg(r)}.$$

For an even integer k we have

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

Proof. If r is a prime self-reciprocal polynomial of even degree, then

$$\mathcal{G}_n(r^k; z) = \sum_{t:\text{ even}} \mathcal{N}_n(r^k; t) z^t = 1 + \sum_{t:\text{ even},\, t>0} \left(\sum_{d|r^k;\, \deg(d)=t} \phi_p(d) \right) z^t$$

$$= 1 + \sum_{j=1}^{k} \phi_p(r^j) z^{j\deg(r)} = 1 + \sum_{j=1}^{k} \left(\sum_{d|r^j} \mu_p(d) p^{\frac{\deg(r^j)-\deg(d)}{2}} \right) z^{j\deg(r)}$$

$$= 1 + \sum_{j=1}^{k} \left(p^{\frac{\deg(r^j)}{2}} - p^{\frac{\deg(r^j)-\deg(r)}{2}} \right) z^{j\deg(r)}.$$

The expression for $\mathcal{G}_n(((x-1)^2)^{k/2}; z)$ follows as a special case, and $\mathcal{G}_n(((x+1)^2)^{k/2}; z)$ is determined in the same way since the sum in (4) is over self-reciprocal polynomials d of even degree dividing f, and $\mathcal{N}(f; t) = 0$ for odd t. $\square$

3 Distribution of the nonlinearity in $\mathcal{C}_1$ and $\mathcal{C}_2$

Our aim in this section is to determine both $\mathcal{G}_n(z)$ and $\mathcal{H}_n(z)$ for all (even) integers n. By Remark 1, this does not only enable us to completely describe the distribution of the nonlinearity for the set of idempotent quadratic Boolean functions, but also for the set of rotation symmetric quadratic Boolean functions.

We first express our counting functions $\mathcal{N}_n(s)$ and $\mathcal{M}_n(s)$ in terms of $\mathcal{N}(f; t)$.

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*

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

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 associated 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 $\gcd(g, (x^n + 1)/f_1(x)) = 1$. 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. $\square$

The following is the main theorem of this section.

Theorem 1 *Let $n = 2^v m$, m odd, $v > 0$, and let $x^n + 1 = (x+1)^{2^v} r_1^{2^v} \cdots r_k^{2^v}$, where $r_1, \ldots, r_k$ are prime self-reciprocal polynomials of even degree. We set*

$$G_i(z) := 1 + \sum_{j=1}^{2^v} \left(2^{\frac{j \deg(r_i)}{2}} - 2^{\frac{(j-1) \deg(r_i)}{2}} \right) z^{j \deg(r_i)} \ .$$

Then the generating polynomial $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n - t) z^t$ is given by

$$\mathcal{G}_n(z) = \left(1 + \sum_{j=1}^{2^{v-1}-1} 2^{j-1} z^{2j} \right) \prod_{i=1}^{k} G_i(z) \ ,$$

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

$$\mathcal{H}_n(z) = \left(1 + \sum_{j=1}^{2^{v-1}} 2^{j-1} z^{2j} \right) \prod_{i=1}^{k} G_i(z) \ .$$

Proof. By Proposition 1 and Lemma 3 we have

$$\mathcal{G}_n(z) = \mathcal{G}_n\left(\frac{x^n+1}{x^2+1}; z\right) = \mathcal{G}_n((x+1)^{2(2^{v-1}-1)}; z)\prod_{i=1}^{k}\mathcal{G}_n(r_i^{2^v}; z)\ ,$$

and

$$\mathcal{H}_n(z) = \mathcal{G}_n(x^n+1; z) = \mathcal{G}_n((x+1)^{2(2^{v-1})}; z)\prod_{i=1}^{k}\mathcal{G}_n(r_i^{2^v}; z)\ .$$

For a prime self-reciprocal polynomial r of even degree, Lemma 4 for $p = 2$ gives

$$\mathcal{G}_n(r^{2^v}; z) = 1 + \sum_{j=1}^{2^v}(2^{\frac{j\deg(r)}{2}} - 2^{\frac{(j-1)\deg(r)}{2}})z^{j\deg(r)},\ \text{and}$$

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

Combining those formulas yields the assertion.   □

Remark 3 Putting $v = 1$ and $m > 1$ in Theorem 1, one obtains $\mathcal{G}_n(z)$ in Theorem 5(ii) of [16]. Note that the Theorem 5(ii) in [16] 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 [15].

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 [9,17], 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 $n = 2^v m$, m odd, $v > 0$, and let $x^n+1 = (x+1)^{2^v} r_1^{2^v} \ldots r_k^{2^v}$, where $r_1, \cdots, r_k$ are prime self-reciprocal polynomials of even degree. Then the number of bent functions in $\mathcal{C}_2$ is*

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

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

Similarly one may obtain $\mathcal{M}_n(s)$ and $\mathcal{N}_n(s)$ for other small values of s. The number of semi-bent function in $\mathcal{C}_1$ for even n, and in $\mathcal{C}_2$ is presented in the next corollary. Note that the number of semi-bent functions in $\mathcal{C}_1$ when n is odd is given in [16, Corollary 7].

Corollary 2 *Let $n = 2^v m$, m odd, $v > 0$, and let $x^n + 1 = (x+1)^{2^v} r_1^{2^v} \dots r_k^{2^v}$, where $r_1, \cdots, r_k$ are prime self-reciprocal polynomials of even degree. The number of semi-bent functions in $\mathcal{C}_1$ is*

$$\mathcal{N}_n(2) = 2^{2^{v-1}-2} \prod_{i=1}^{k} \left(2^{\frac{2^v \deg(r_i)}{2}} - 2^{\frac{(2^v - 1)\deg(r_i)}{2}} \right).$$

The number of semi-bent functions in $\mathcal{C}_2$ is

- $\mathcal{M}_n(2) = \mathcal{N}_n(2)$ *if 3 does not divide n,*
- $\mathcal{M}_n(2) = \mathcal{N}_n(2) + 2^{2^{v-1}-1}2^{2^v-2} \prod_{r_i \neq x^2+x+1}^{k} \left(2^{\frac{2^v \deg(r_i)}{2}} - 2^{\frac{(2^v - 1)\deg(r_i)}{2}} \right)$ *if*
  3 *divides n.*

Proof. The corollary follows from Theorem 1 with the observation that x^2+x+1 divides $x^n - 1$ if and only if 3 divides n. □

Remark 4 In [13, Theorem 12], for $n \equiv 0 \mod 3$ an expression for the number $\mathcal{K}$ of semi-bent functions in $\mathcal{C}_2 \setminus C_1$ is given, which involves a Möbius function on the set of monic self-reciprocal polynomials. Our formula

$$\mathcal{K} = 2^{2^{v-1}-1}2^{2^v-2} \prod_{r_i \neq x^2+x+1}^{k} \left(2^{\frac{2^v \deg(r_i)}{2}} - 2^{\frac{(2^v - 1)\deg(r_i)}{2}} \right)$$

is more explicit.

Remark 5 To completely describe the nonlinearity distribution in $\mathcal{C}_1$ and $\mathcal{C}_2$ it is inevitable to consider the generating polynomials. Otherwise, in order to determine $\mathcal{N}_n(s)$ or $\mathcal{M}_n(s)$ for a specific s, one would first have to find *all* possible ways of expressing 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 the set of affine functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by $\mathcal{A} = \{\text{Tr}_n(bx) + c \; : \; b \in \mathbb{F}_{2^n}, \; c \in \mathbb{F}_2\}$. 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 $\mathcal{A}$.

The weight distribution of other subcodes of $R(2, n)$ containing $R(1, n)$ has been investigated in [1, 10]. More precisely, the authors determine the weight distribution of some extended cyclic codes of length 2^n with special generator

polynomials in terms of Gaussian coefficients. In our work, we are interested in the classes of subcodes generated by the cosets of $R(1, n)$ containing rotation symmetric functions. We emphasize that these classes of subcodes are different than the ones investigated in [1,10]. For example, the punctured code (the reverse operation of extending code) of our corresponding subcodes is not cyclic.

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 [2] by explicit, quite involved formulas. Here we focus on the subcodes of $R(2, n)$, obtained from the sets $\mathcal{C}_1$ and $\mathcal{C}_2$, 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,

$$\mathcal{W}_{\mathcal{C}_1}(z) = \sum_{k=0}^n A_k^{\mathcal{C}_1} z^k = \sum_{k=0}^n \mathcal{N}_n(n - k)2^k z^k = \mathcal{G}_n(2z) ,$$

$$\mathcal{W}_{\mathcal{C}_2}(z) = \sum_{k=0}^n A_k^{\mathcal{C}_2} z^k = \sum_{k=0}^n \mathcal{M}_n(n - k)2^k z^k = \mathcal{H}_n(2z) . \tag{5}$$

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

$$A^{\mathcal{C}_1} = \sum_{k=0}^n \mathcal{N}_n(n - k)(2^{n+1} - 2^{k+1}) = 2^{n+1}\sum_{k=0}^n \mathcal{N}_n(n - k) - 2\sum_{k=0}^n \mathcal{N}_n(n - k)2^k$$

$$= 2^{n+1}\mathcal{G}_n(1) - 2\mathcal{G}_n(2) .$$

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 $\bar{R}_{\mathcal{C}}$.

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*

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

where

$$W_i(z) = 1 + \sum_{j=1}^{2^t} \left(2^{\frac{3j\deg(r_i)}{2}} - 2^{\frac{(3j-1)\deg(r_i)}{2}}\right) z^{j\deg(r_i)} \ ,$$

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

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

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

Proof. By using (5), the formulas for $\mathcal{W}_{\mathcal{C}_1}(z)$ and $\mathcal{W}_{\mathcal{C}_2}(z)$ follow from the generating function $\mathcal{G}_n(z) = \prod_{i=1}^{l} \left[1 + (2^{\deg(r_i)/2} - 1)z^{\deg(r_i)}\right]$ when n is odd (see Theorem 5(i) in [16]) 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 $2^{n+1}\mathcal{H}_n(1) - 2\mathcal{H}_n(2)$. $\quad\square$

Remark 6 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 $k = \sum_{r_i \in \{r_1,\ldots,r_l\}} \deg(r_i)$, for $r = \min\{\deg(r_i)\}_{i=1}^{l}$ 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.

Remark 7 We emphasize that in order to describe the weight distribution of the codes that we study, it is not possible to avoid the use of generating polynomials. Note that every explicit formula for the number of codewords with a given weight should depend on all possible ways of expressing the corresponding parameter s as a sum of degrees of polynomials in the prime self-reciprocal factorization of $x^n + 1$. Hence such formulas for general n cannot be given unless the degrees of these divisors follow a particular pattern. Description of the weight distribution via a generating polynomial is for these codes the best one can expect.

5 Enumeration of s-plateaued quadratic functions for odd characteristic

In this section we apply our method to quadratic functions in $\mathcal{D}$. Recall that results on $\mathcal{D}$ translate to results on the set of rotation symmetric functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. As we will see, determining the generating function in odd characteristic is considerably more involved. We can restrict ourselves to the case $\gcd(n, p) > 1$ since the case $\gcd(n, p) = 1$ is dealt with in [16] with a different method which employs discrete Fourier transform. We emphasize that the method of [16] is not applicable to the case $\gcd(n, p) > 1$.

Recall that to $Q(x) = \mathrm{Tr}_n \left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i + 1} \right) \in \mathcal{D}$, the associate is

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \left(a_i x^i + a_i x^{n-i} \right) ,$$

which is a polynomial of degree at most n. We treat the cases of odd and even n separately.

The case of odd n

In this case the factorization of $x^n - 1$ into prime self-reciprocal divisors is given by

$$x^n - 1 = (x - 1)^{p^v} r_1^{p^v} \cdots r_k^{p^v} .$$

Firstly we note that $x^n - 1$ is not divisible by $x + 1$ as n is an odd integer, and hence each r_i, $1 \le i \le k$, is a prime self-reciprocal polynomial of even degree. Write $A(x)$ as

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \left(a_i x^i + a_i x^{n-i} \right) = x^c h(x) ,$$

where $h(x)$ is a self-reciprocal polynomial of degree $n - 2c$. Since n is odd, also the degree of h is odd, and hence $x + 1$ is a factor of $A(x)$. In fact, $x + 1$ must appear as an odd power in the factorization of $A(x)$. In particular,

$$A(x) = x^c (x + 1) \varrho(x)$$

for a self-reciprocal polynomial $\varrho(x)$ of even degree $n - 2c - 1$. As a consequence,

$$\gcd(A(x), x^n - 1) = \gcd(\varrho(x), x^n - 1) = (x - 1)^\epsilon f_1(x) ,$$

for a self-reciprocal polynomial f_1 of even degree, and some $\epsilon \in \{0, 1\}$. That is,

$$\varrho(x) = (x - 1)^\epsilon f_1(x) g_1(x) \text{ with } \gcd\left(\frac{x^n - 1}{(x - 1)^\epsilon f_1(x)}, g_1(x) \right) = 1 .$$

We will frequently use the following observation, which immediately follows from the definition of ϕ_p.

Proposition 2 *For a self-reciprocal polynomial d of even degree we have*

$$\phi_p((x \pm 1)d) = \phi_p((x \pm 1)^2 d) \ .$$

We now represent the counting function $\mathcal{N}_n^{(p)}(s)$ in terms of the function $\mathcal{N}_n(f;t)$ in (4). The arguments are more complicated than in the even characteristic case, for instance, here the distinction between odd and even n is required. As we see in the proposition below, for odd n we also need to consider odd and even s separately. In the next subsection, where n is even, we have to treat four cases.

Proposition 3 *Let n be an odd integer such that the p-adic valuation of n is $v_p(n) = v$. The number $\mathcal{N}_n^{(p)}(s)$ of quadratic s-plateaued functions in $\mathcal{D}$ is given by*

$$\mathcal{N}_n^{(p)}(s) = \begin{cases} \mathcal{N}_n(\frac{x^n-1}{(x-1)^{p^v}}; n-s) & \textit{if s is odd,} \\ \mathcal{N}_n((x-1)(x^n-1); n-s+1) - \mathcal{N}_n(\frac{x^n-1}{(x-1)^{p^v}}; n-s+1) & \textit{if s is even.} \end{cases}$$

Proof Suppose that $\gcd(A(x), x^n - 1) = (x-1)f_1(x)$, i.e. $\epsilon = 1$. This holds if only if s is odd. In this case, $\deg(g_1)$ is odd and $g_1(x)$ is divisible by $(x-1)$ since $\varrho(x)$ is a self-reciprocal polynomial of even degree, i.e. $g_1(x) = (x-1)g(x)$ for some self-reciprocal polynomial g of even degree. Furthermore we know that $\gcd(\frac{x^n-1}{(x-1)f_1(x)}, g_1(x)) = 1$, and therefore $x - 1$ is not a factor of $\frac{x^n-1}{(x-1)f_1(x)}$. Consequently, $(x - 1)^{p^v-1}$ must divide $f_1(x)$. Hence $h(x)$ can be expressed as

$$h(x) = (x+1)(x-1)^{p^v+1}f(x)g(x) \ \text{ with } \ \gcd\left(\frac{x^n-1}{(x-1)^{p^v}f(x)}, g(x)\right) = 1 \ ,$$

where g is a self-reciprocal polynomial of even degree smaller than $n - s$, and hence $g \in K\left(\frac{x^n-1}{(x-1)^{p^v}f(x)}\right)$. Furthermore, each divisor d of $\frac{x^n-1}{(x-1)^{p^v}}$ of degree $n - s$ uniquely determines $f(x)$. As a result, there exist

$$\sum_{d \mid \frac{x^n-1}{(x-1)^{p^v}}; \ \deg(d)=n-s} \phi_p(d) = \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}}; n-s\right)$$

s-plateaued quadratic functions in $\mathcal{D}$ if s is odd. Now we consider the case of even s, i.e. $\epsilon = 0$ and $\gcd(A(x), x^n - 1) = f(x)$, where the multiplicity of $x - 1$ in f is even. As a result, $\frac{x^n-1}{f(x)}$ is divisible by $x - 1$, which implies that $g(x)$ is not divisible by $x - 1$. In this case,

$$h(x) = (x+1)f(x)g(x) \ \text{ with } \ \gcd\left(\frac{x^n-1}{f(x)}, g(x)\right) = 1 \ ,$$

i.e. $g \in K\left(\frac{x^n-1}{f(x)}\right) = K\left((x-1)\frac{x^n-1}{f(x)}\right)$ by Proposition 2. Furthermore for any self-reciprocal divisor d of $x^n - 1$ of degree $n-s-1$, the factor $(x-1)d$ uniquely

determines f. Hence there are

$$\sum_{(x-1)d|x^n-1;\ \deg(d)=n-s-1} \phi_p((x-1)d)$$

$$= \sum_{(x-1)^2d|(x-1)(x^n-1);\ \deg(d)=n-s-1} \phi_p((x-1)^2d)$$

s-plateaued functions in $\mathcal{D}$ in the case of even s, where d runs over all monic self-reciprocal divisors of x^n-1. In order to determine the last sum, we separate the set

$$S = \{d\ :\ d \text{ is monic, self-reciprocal, } d|(x-1)(x^n-1),\ \deg(d) = n-s+1\}$$

into two disjoint subsets. The set $\mathcal{S}_1$ consists of elements of S which are divisible by $x-1$, and $\mathcal{S}_2$ is the complement, i.e.

$$\mathcal{S}_1 = \{d\ :\ d = (x-1)^2k \in S,\ k \text{ is self-reciprocal},\ \deg(k) = n-s-1\},$$

$$\mathcal{S}_2 = \left\{d\ :\ d \in S,\ d\Big|\frac{x^n-1}{(x-1)^{p^v}}\right\}.$$

Then

$$\sum_{d\in S_1} \phi_p(d) = \sum_{d\in S} \phi_p(d) - \sum_{d\in S_2} \phi_p(d)\ ,$$

or equivalently

$$\sum_{(x-1)^2d|(x-1)(x^n-1);\ \deg(d)=n-s-1} \phi_p((x-1)^2d)$$

$$= \sum_{d|(x-1)(x^n-1);\ \deg(d)=n-s+1} \phi_p(d) - \sum_{d|\frac{x^n-1}{(x-1)^{p^v}};\ \deg(d)=n-s+1} \phi_p(d)$$

$$= \mathcal{N}_n((x-1)(x^n-1); n-s+1) - \mathcal{N}_n\Big(\frac{x^n-1}{(x-1)^{p^v}}; n-s+1\Big)\ .$$

Remark 8 Note that from the proof of Proposition 3, we see that $s \geq p^v$ if s is odd.

Theorem 3 *Let n be an odd integer and let $x^n-1 = (x-1)^{p^v} r_1^{p^v}\cdots r_k^{p^v}$ be the factorization of x^n-1 into distinct prime self-reciprocal polynomials. Then $\mathcal{G}_n^{(p)} = \sum_{t=0}^n \mathcal{N}_n^{(p)}(n-t)z^t$ is given by*

$$\mathcal{G}_n^{(p)}(z) = \left(1 + \sum_{j=1}^{\frac{p^v+1}{2}} p^{j-1}(p-1)z^{2j-1}\right)\prod_{i=1}^k G_i(z)\ ,$$

where

$$G_i(z) = 1 + \sum_{j=1}^{p^v}\Big(p^{\frac{\deg(r_i^j)}{2}} - p^{\frac{\deg(r_i^j)-\deg(r_i)}{2}}\Big)z^{j\deg(r_i)}\ .$$

Proof We can express the generating function as

$$
\begin{aligned}
\mathcal{G}_n^{(p)}(z) &= \sum_{t:\,\text{even}} \mathcal{N}_n^{(p)}(n-t)z^t + \sum_{t:\,\text{odd}} \mathcal{N}_n^{(p)}(n-t)z^t \\
&= \sum_{t:\,\text{even}} \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t\right)z^t + \sum_{t:\,\text{odd}} \left(\mathcal{N}_n((x-1)(x^n-1);t+1) - \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t+1\right)\right)z^t \\
&= \sum_{t:\,\text{even}} \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t\right)z^t + \frac{1}{z}\sum_{t:\,\text{odd}} \left(\mathcal{N}_n((x-1)(x^n-1);t+1) - \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t+1\right)\right)z^{t+1} \\
&= \sum_{t:\,\text{even}} \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t\right)z^t + \frac{1}{z}\left[\sum_{t:\,\text{even}} \left(\mathcal{N}_n((x-1)(x^n-1);t) - \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};t\right)\right)z^t\right] \\
&= \mathcal{G}_n\left(\frac{x^n-1}{(x-1)^{p^v}};z\right) + \frac{1}{z}\left[\mathcal{G}_n((x-1)(x^n-1);z) - \mathcal{G}_n\left(\frac{x^n-1}{(x-1)^{p^v}};z\right)\right] \\
&= \prod_{i=1}^{k} \mathcal{G}_n(r_i^{p^v};z)\left(1 - \frac{1}{z} + \frac{1}{z}\mathcal{G}_n((x-1)^{p^v+1};z)\right).
\end{aligned}
$$

Note that in the fourth equality we added and subtracted $\mathcal{N}_n((x-1)(x^n-1);0) = \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}};0\right) = 1$. In the last equality we used Lemma 3. We then obtain the claimed formula by Lemma 4.

The case of even n

In this case the factorization of $x^n - 1$ is given by

$$
x^n - 1 = (x-1)^{p^v}(x+1)^{p^v}r_1^{p^v}\cdots r_k^{p^v} ,
$$

for some distinct prime self-reciprocal polynomials r_i, $1 \le i \le k$, of even degree. Now

$$
A(x) = \sum_{i=0}^{n/2}(a_i x^i + a_i x^{n-i}) = x^c h(x) ,
$$

where $h(x)$ is self-reciprocal, and of even degree $n-2c$. For the $\gcd(A(x), x^n-1)$ we have

$$
\gcd(A(x), x^n - 1) = \gcd(h(x), x^n - 1) = (x-1)^\epsilon(x+1)^\delta f_1(x) , \qquad (7)
$$

for a self-reciprocal polynomial f_1 of even degree, and elements $\epsilon, \delta \in \{0,1\}$. Consequently,

$$
h(x) = (x-1)^\epsilon(x+1)^\delta f_1(x)g_1(x), \text{ with } \gcd\left(\frac{x^n-1}{(x-1)^\epsilon(x+1)^\delta f_1(x)}, g_1(x)\right) = 1 .
$$

We now have to distinguish four cases depending on the values of ϵ and δ in (7).

(i) Let $\epsilon = \delta = 1$, i.e., $\gcd(A(x), x^n - 1) = \gcd(h(x), x^n - 1) = (x - 1)(x + 1)f_1(x)$. In this case, s is even and the self-reciprocal polynomial h of even degree is given by

$$h(x) = (x - 1)(x + 1)f_1(x)(x - 1)(x + 1)g(x)$$

$$\text{with } \gcd\left((x - 1)(x + 1)g(x), \frac{x^n - 1}{(x - 1)(x + 1)f_1}\right) = 1 \ ,$$

where $g(x)$ is a self-reciprocal polynomial of degree $\leq n - s - 2$. As a result, $f_1(x) = (x - 1)^{p^v - 1}(x + 1)^{p^v - 1}f(x)$ for a self-reciprocal polynomial f of even degree (which of course is a product of some r_i's). As a consequence,

$$h(x) = (x - 1)^{p^v + 1}(x + 1)^{p^v + 1}f(x)g(x) \ ,$$

for some self-reciprocal polynomial g. Note that $\deg(g)$ is an even integer smaller than $n - s$ and $\gcd\left(g, \frac{x^n - 1}{(x-1)^{p^v}(x+1)^{p^v}f(x)}\right) = 1$. Recalling that $\deg\left(\frac{x^n - 1}{(x-1)^{p^v}(x+1)^{p^v}f(x)}\right) = n - s$, we see that $g \in K\left(\frac{x^n - 1}{(x-1)^{p^v}(x+1)^{p^v}f(x)}\right)$. Furthermore each divisor d of $\frac{x^n - 1}{(x-1)^{p^v}(x+1)^{p^v}}$ of degree $n - s$ uniquely determines f, and hence there exist

$$\sum_{d \mid \frac{x^n - 1}{(x-1)^{p^v}(x+1)^{p^v}}; \, \deg(d) = n - s} \phi_p(d)$$

such polynomials h.

(ii) Let $\epsilon = 1$ and $\delta = 0$, i.e., $\gcd(A(x), x^n - 1) = \gcd(h(x), x^n - 1) = (x - 1)f_1(x)$. In this case, s is odd and the self-reciprocal polynomial h of even degree is given by

$$h(x) = (x - 1)f_1(x)(x - 1)g(x) \ \text{ with } \ \gcd\left((x - 1)g(x), \frac{x^n - 1}{(x - 1)f_1}\right) = 1 \ ,$$

for some self-reciprocal polynomial g, where $deg(g)$ is even, and smaller than $n - s$. Consequently, $f_1(x) = (x - 1)^{p^v - 1}f(x)$ for some self-reciprocal polynomial f of even degree, and therefore

$$h(x) = (x - 1)^{p^v + 1}f(x)g(x) \ ,$$

where $\gcd\left(g, \frac{x^n - 1}{(x-1)^{p^v}f(x)}\right) = 1$. Since $\frac{x^n - 1}{(x-1)f_1}$ contains the factor $x + 1$, the polynomial g is not divisible by $x + 1$. In particular, $g \in K((x+1)d)$, where $d = \frac{x^n - 1}{(x-1)^{p^v}(x+1)f(x)}$ is a self-reciprocal polynomial of even degree $n - s - 1$. As above, each self-reciprocal divisor d of $\frac{x^n - 1}{(x-1)^{p^v}(x+1)}$ of degree $n - s - 1$ uniquely determines f. Consequently there exist

$$\sum_{d \mid \frac{x^n - 1}{(x-1)^{p^v}(x+1)}; \, \deg(d) = n - s - 1} \phi_p((x + 1)d)$$

such polynomials h.

(iii) The case $\epsilon = 0$ and $\delta = 1$ is very similar. With the same argument as in (ii) we get

$$h(x) = (x+1)f_1(x)(x+1)g(x) \text{ with } \gcd\left((x+1)g(x), \frac{x^n - 1}{(x+1)f_1}\right) = 1 \ ,$$
(8)

for some self-reciprocal polynomial g, where $deg(g)$ is even, smaller than $n - s$, and

$$\sum_{d | \frac{x^n - 1}{(x+1)^{p^v}(x-1)}; \ \deg(d) = n-s-1} \phi_p((x-1)d)$$

is the number of polynomials h of the form (8).

(iv) Let $\epsilon = \delta = 0$, i.e., $\gcd(A(x), x^n - 1) = \gcd(h(x), x^n - 1) = f(x)$ for some self-reciprocal polynomial f of even degree. In this case we see that the self-reciprocal polynomial h is given by

$$h(x) = f(x)g(x) \text{ with } \gcd\left(g(x), \frac{x^n - 1}{f(x)}\right) = 1 \ ,$$

where $g(x)$ is a self-reciprocal polynomial of degree $\leq n-s$. Note that $\frac{x^n - 1}{f(x)}$ is divisible by both $x - 1$ and $x + 1$, so $g(x)$ is not divisible by neither. Therefore

$$h(x) = f(x)g(x) \text{ with } \gcd\left(g(x), (x-1)(x+1)\frac{x^n - 1}{f(x)}\right) = 1 \ , \quad (9)$$

where $g(x)$ is a self-reciprocal polynomial of degree smaller than $n - s + 2$. As for each self-reciprocal divisor d of $x^n - 1$ of degree $n - s$, f is uniquely determined, we can again express the number of polynomials h of the form (9) in terms of ϕ_p as

$$\sum_{(x-1)(x+1)d | (x-1)(x+1)(x^n - 1); \ \deg(d) = n-s} \phi_p((x-1)(x+1)d).$$

Remark 9 From the above observations we conclude that again $s \geq p^v$ if s is odd.

Theorem 4 *Let n be an even integer and let $x^n - 1 = (x-1)^{p^v}(x+1)^{p^v} r_1^{p^v} \cdots r_k^{p^v}$ be the factorization of $x^n - 1$ into distinct prime self-reciprocal polynomials. Then the generating function $\mathcal{G}_n^{(p)}$ is given by*

$$\mathcal{G}_n^{(p)}(z) = \left(1 + \sum_{j=1}^{\frac{p^v + 1}{2}} p^{j-1}(p-1)z^{2j-1}\right)^2 \prod_{i=1}^{k} G_i(z) \ ,$$

where

$$G_i(z) = 1 + \sum_{j=1}^{p^v} (p^{\frac{\deg(r_i^j)}{2}} - p^{\frac{\deg(r_i^j) - \deg(r_i)}{2}}) z^{j \deg(r_i)} \ .$$

Proof First let s be odd, which applies in the cases (ii) and (iii) above. The discussion of these cases imply for $\mathcal{N}_n^{(p)}(s)$ that

$$
\begin{aligned}
\mathcal{N}_n^{(p)}(s) &= \sum_{d|\frac{x^n-1}{(x-1)^{p^v}(x+1)};\, \deg(d)=n-s-1} \phi_p((x+1)d) + \sum_{d|\frac{x^n-1}{(x+1)^{p^v}(x-1)};\, \deg(d)=n-s-1} \phi_p((x-1)d) \\
&= \sum_{d|\frac{x^n-1}{(x-1)^{p^v}(x+1)};\, \deg(d)=n-s-1} \phi_p((x+1)^2 d) + \sum_{d|\frac{x^n-1}{(x+1)^{p^v}(x-1)};\, \deg(d)=n-s-1} \phi_p((x-1)^2 d) \; .
\end{aligned}
\tag{10}
$$

To determine the sum (10) we separate the set

$$
S = \left\{ h \; : \; h \text{ is monic, self-reciprocal, } h \Big| \frac{x^n-1}{(x-1)^{p^v}}, \;\; \deg(h) = n - s + 1 \right\}
$$

into the two disjoint subsets

$$
\begin{aligned}
S_1 &= \{ h \; : \; h \in S \text{ and } \gcd(h, x+1) = 1 \}, \text{ and} \\
S_2 &= \{ h \; : \; h \in S \text{ and } (x+1)|h \}.
\end{aligned}
$$

Note that being self-reciprocal and of even degree, the polynomials h in the set S_2 are divisible by $(x+1)^2$. Then for the first sum in (10) we obtain

$$
\begin{aligned}
\sum_{d|\frac{x^n-1}{(x-1)^{p^v}(x+1)};\, \deg(d)=n-s-1} \phi_p((x+1)^2 d) &= \sum_{h \in S_2} \phi_p(h) \\
&= \sum_{h|\frac{(x+1)(x^n-1)}{(x-1)^{p^v}};\, \deg(h)=n-s+1} \phi_p(h) - \sum_{h \in S_1} \phi_p(h) \\
&= \sum_{h|\frac{(x+1)(x^n-1)}{(x-1)^{p^v}};\, \deg(h)=n-s+1} \phi_p(h) - \sum_{h|\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}};\, \deg(h)=n-s+1} \phi_p(h) \\
&= \mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; n-s+1 \right) - \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s+1 \right).
\end{aligned}
$$

In a similar way, for the second sum in (10) we get

$$
\sum_{d|\frac{x^n-1}{(x+1)^{p^v}(x-1)};\, \deg(d)=n-s-1} \phi_p((x-1)^2 d)
$$

$$
\mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; n-s+1 \right) - \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s+1 \right).
$$

Combining, we obtain

$$
\begin{aligned}
\mathcal{N}_n^{(p)}(s) &= \mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; n-s+1 \right) + \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; n-s+1 \right) \\
&\quad - 2\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s+1 \right)
\end{aligned}
$$

for an odd integer s. Now we consider the case of even s, which corresponds to (i) and (iv). By the above observations,

$$
\begin{aligned}
\mathcal{N}_n^{(p)}(s) &= \sum_{d \mid \frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}};\ \deg(d)=n-s} \phi_p(d) \\
&\quad + \sum_{(x-1)(x+1)d \mid (x-1)(x+1)(x^n-1);\ \deg(d)=n-s} \phi_p((x-1)(x+1)d) \\
&= \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s\right) \\
&\quad + \sum_{(x-1)(x+1)d \mid (x-1)(x+1)(x^n-1);\ \deg(d)=n-s} \phi_p((x-1)(x+1)d).
\end{aligned}
$$

We set $T := \sum_{(x-1)(x+1)d \mid (x-1)(x+1)(x^n-1);\ \deg(d)=n-s} \phi_p((x-1)(x+1)d)$ and

in order to determine T we consider the set

$$S = \{h(x) \ : \ h(x) \text{ is self-reciprocal, } h \mid (x-1)(x+1)(x^n-1), \ \deg(h) = n-s+2\}$$

and its subsets

$$
\begin{aligned}
S_1 &= \{h(x) \ : \ h \in S, \ \gcd(h, x-1) = 1\}, \\
S_2 &= \{h(x) \ : \ h \in S, \ \gcd(h, x+1) = 1\}, \\
S_3 &= \{h(x) \ : \ h \in S, \ \gcd(h, x^2-1) = 1\}.
\end{aligned}
$$

Note that since h is a self-reciprocal polynomial of even degree, h is divisible by $(x \mp 1)^2$ if it is divisible by $x \mp 1$. As a consequence,

$$T = \sum_{h \mid (x-1)(x+1)(x^n-1);\ \deg(h)=n-s+2} \phi_p(h) - \sum_{h \in S_1} \phi_p(h) - \sum_{h \in S_2} \phi_p(h) + \sum_{h \in S_3} \phi_p(h).$$

We also note that for h in the set S, $h \in S_1$ if and only if $h \mid (x+1)\frac{x^n-1}{(x-1)^{p^v}}$, $h \in S_2$ if and only if $h \mid (x-1)\frac{x^n-1}{(x+1)^{p^v}}$ and $h \in S_3$ if and only if $h \mid \frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}$. Therefore we can express the sum T as

$$
\begin{aligned}
T &= \sum_{h \mid (x-1)(x+1)(x^n-1);\ \deg(h)=n-s+2} \phi_p(h) - \sum_{h \mid (x+1)\frac{x^n-1}{(x-1)^{p^v}};\ \deg(h)=n-s+2} \phi_p(h) \\
&\quad - \sum_{h \mid (x-1)\frac{x^n-1}{(x+1)^{p^v}};\ \deg(h)=n-s+2} \phi_p(h) + \sum_{h \mid \frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}};\ \deg(h)=n-s+2} \phi_p(h).
\end{aligned}
$$

Hence, for an even integer s

$$
\begin{aligned}
\mathcal{N}_n^{(p)}(s) &= \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s\right) + \mathcal{N}_n\left((x-1)(x+1)(x^n-1); n-s+2\right) \\
&\quad -\mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; n-s+2\right) - \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; n-s+2\right) \\
&\quad +\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; n-s+2\right).
\end{aligned}
$$

From the above equalities we get

$$\mathcal{G}_n^{(p)}(z) = \sum_{t=0}^{n} \mathcal{N}_n^{(p)}(n-t)z^t = \sum_{t:\text{ odd}} \mathcal{N}_n^{(p)}(n-t)z^t + \sum_{t:\text{ even}} \mathcal{N}_n^{(p)}(n-t)z^t$$

$$= \sum_{t:\text{ odd}} \left[\mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t+1 \right) + \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t+1 \right) - 2\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t+1 \right) \right] z^t$$

$$+ \sum_{t:\text{ even}} \left[\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t \right) + \mathcal{N}_n\left((x-1)(x+1)(x^n-1); t+2 \right) - \mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t+2 \right) \right.$$

$$\left. - \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t+2 \right) + \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t+2 \right) \right] z^t$$

$$= \frac{1}{z} \sum_{t:\text{ odd}} \left[\mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t+1 \right) + \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t+1 \right) - 2\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t+1 \right) \right] z^{t+1}$$

$$+ \sum_{t:\text{ even}} \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t \right) z^t + \frac{1}{z^2} \sum_{t:\text{ even}} \left[\mathcal{N}_n\left((x-1)(x+1)(x^n-1); t+2 \right) \right.$$

$$\left. - \mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t+2 \right) - \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t+2 \right) + \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t+2 \right) \right] z^{t+2}$$

$$= \frac{1}{z} \sum_{t:\text{ even}} \left[\mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t \right) + \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t \right) - 2\mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t \right) \right] z^t$$

$$+ \sum_{t:\text{ even}} \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t \right) z^t + \frac{1}{z^2} \sum_{t:\text{ even}} \left[\mathcal{N}_n\left((x-1)(x+1)(x^n-1); t \right) \right.$$

$$\left. - \mathcal{N}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; t \right) - \mathcal{N}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; t \right) + \mathcal{N}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; t \right) \right] z^t$$

$$= \frac{1}{z} \left[\mathcal{G}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; z \right) + \mathcal{G}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; z \right) - 2\mathcal{G}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; z \right) \right]$$

$$+ \mathcal{G}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; z \right) + \frac{1}{z^2} \left[\mathcal{G}_n\left((x-1)(x+1)(x^n-1); z \right) \right.$$

$$\left. - \mathcal{G}_n\left(\frac{(x+1)(x^n-1)}{(x-1)^{p^v}}; z \right) - \mathcal{G}_n\left(\frac{(x-1)(x^n-1)}{(x+1)^{p^v}}; z \right) + \mathcal{G}_n\left(\frac{x^n-1}{(x-1)^{p^v}(x+1)^{p^v}}; z \right) \right]$$

$$= \prod_{i=1}^{k} \mathcal{G}_n(r_i^{p^v}; z) \left(\frac{1}{z} \mathcal{G}_n((x+1)^{p^v+1}; z) + \frac{1}{z} \mathcal{G}_n((x-1)^{p^v+1}; z) - \frac{2}{z} + 1 \right.$$

$$\left. + \frac{1}{z^2} \mathcal{G}_n((x-1)^{p^v+1}(x+1)^{p^v+1}; z) - \frac{1}{z^2} \mathcal{G}_n((x+1)^{p^v+1}; z) - \frac{1}{z^2} \mathcal{G}_n((x-1)^{p^v+1}; z) + \frac{1}{z^2} \right).$$

By Lemma 4 we get

$$\mathcal{G}_n^{(p)}(z) = \prod_{i=1}^{k} \mathcal{G}_n(r_i^{p^v}; z) \left(\frac{2}{z} \mathcal{G}_n((x-1)^{p^v+1}; z) - \frac{2}{z} + 1 + \frac{1}{z^2} \mathcal{G}_n((x-1)^{p^v+1}; z)^2 \right.$$

$$\left. - \frac{2}{z^2} \mathcal{G}_n((x-1)^{p^v+1}; z) + \frac{1}{z^2} \right).$$

Putting

$$
G_i := \mathcal{G}_n(r_i^{p^v}; z) , \quad \text{and} \quad A := \sum_{j=1}^{\frac{p^v+1}{2}} p^{j-1}(p-1)z^{2j} = \mathcal{G}_n((x-1)^{p^v+1}; z) - 1
$$

this yields

$$
\begin{aligned}
\mathcal{G}_n^{(p)}(z) \quad &= \prod_{i=1}^{k} G_i \left[\frac{2}{z}(1+A) - \frac{2}{z} + 1 + \frac{1}{z^2}(1+A)^2 - \frac{2}{z^2}(1+A) + \frac{1}{z^2} \right] \\
&= \left(1 + \frac{A}{z} \right)^2 \prod_{i=1}^{k} G_i.
\end{aligned}
$$

Simplifying and using Lemma 4 we get the desired result.

As an immediate corollary of Theorems 3 and 4 we obtain the number of bent functions in the set $\mathcal{D}$. Note that the case of $\gcd(n, p) = 1$ is covered in [16, Corollary 7].

Corollary 3 *Let the factorization of $x^n - 1$ into distinct prime self-reciprocal polynomials be $x^n - 1 = (x - 1)^{p^v} r_1^{p^v} \cdots r_k^{p^v}$ when n is odd, and $x^n - 1 = (x-1)^{p^v}(x+1)^{p^v} r_1^{p^v} \cdots r_k^{p^v}$ when n is even. Then the number of bent functions in $\mathcal{D}$ is*

$$
\mathcal{N}_n(0) = (p-1)p^{\frac{p^v-1}{2}} \prod_{i=1}^{k} \left(p^{\frac{p^v \deg(r_i)}{2}} - p^{\frac{(p^v-1)\deg(r_i)}{2}} \right) ,
$$

if n is odd, and

$$
\mathcal{N}_n(0) = ((p-1)p^{\frac{p^v-1}{2}})^2 \prod_{i=1}^{k} \left(p^{\frac{p^v \deg(r_i)}{2}} - p^{\frac{(p^v-1)\deg(r_i)}{2}} \right) ,
$$

if n is even.

6 Acknowledgements

References

1. Berlekamp, E.R.: The weight enumerators for certain subcodes of the second order binary Reed-Muller codes. Information and Control 17, 485–500 (1970)
2. Berlekamp, E.R., Sloane, N.: The weight enumerator of second-order Reed-Muller codes. IEEE Trans. Inform. Theory IT-16, 745-751 (1970)
3. 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)
4. Çeşmelioğlu, A., Meidl, W.: Non-weakly regular bent polynomials from vectorial quadratic functions. In: Pott, A., et.al. (eds) Proceedings of the 11th international conference on Finite Fields and their Applications, Contemporary Mathematics, 2015, 83–95
5. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51, 4286–4298 (2005)
6. Fitzgerald, R.W.: Trace forms over finite fields of characteristic 2 with prescribed invariants. Finite Fields Appl. 15, 69–81 (2009)
7. Fu, F.W., Niederreiter, H., Özbudak, F.: Joint linear complexity of multisequences consisting of linear recurring sequences. Cryptogr. Commun. 1, 3–29 (2009)
8. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory 52, 2018–2032 (2006)
9. Hu, H., Feng, D.: On Quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory 53, 2610- 2615 (2007)
10. Kasami T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Information and Control 18, 369–394 (1971)
11. Kaşıkcı, C., Meidl, W., Topuzoğlu, A: Spectra of quadratic functions: Average behaviour and counting functions. Cryptogr. Commun. DOI 10.1007/s12095-015-0142-9
12. 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)
13. Kocak, N., Kocak, O., Özbudak, F., Saygi, Z.: Characterization and enumeration of a class of semi-bent Boolean functions. Int. J. Inform. Coding Theory 3, 39–57 (2015)
14. Li, S., Hu, L., Zeng, X.: Constructions of p-ary quadratic bent functions. Acta Appl. Math. 100, 227–245 (2008)
15. Meidl, W., Topuzoğlu, A.: Quadratic functions with prescribed spectra. Designs, Codes, Cryptogr. 66, 257–273 (2013)
16. Meidl, W., Roy, S., Topuzoğlu, A.: Enumeration of quadratic functions with prescribed Walsh spectrum. IEEE Trans. Inform. Theory 60, 6669–6680 (2014)
17. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory 52, 3291–3299 (2006)

7 Appendix

We give some examples of generating function for $p = 3$.

Example $n = 9 \cdot 13$: In this case, $x^{9 \cdot 13} - 1 = (x-1)^9 r_1^9 r_2^9$ for prime self-reciprocal polynomials r_1, r_2 both of degree 6. By Theorem 3,

$$\mathcal{G}_{9 \cdot 13}^{(3)}(z) = (1 + 2\sum_{j=1}^{5} 3^{j-1} z^{2j-1})(1 + 26\sum_{j=1}^{9} 3^{3(j-1)} z^{6j})^2.$$

Expanding this polynomial we obtain

$\mathcal{G}_{9 \cdot 13}^{(3)}(z) =$

$1 + 2\,z + 6\,z^3 + 18\,z^5 + 52\,z^6 + 158\,z^7 + 474\,z^9 + 936\,z^{11} + 2080\,z^{12} + 6968\,z^{13} + 20904\,z^{15} + 37440\,z^{17}$

$+ 74412\,z^{18} + 261144\,z^{19} + 783432\,z^{21} + 1339416\,z^{23} + 2501928\,z^{24} + 9022104\,z^{25} + 27066312\,z^{27}$

$+ 45034704\,z^{29} + 80857764\,z^{30} + 296819640\,z^{31} + 890458920\,z^{33} + 1455439752\,z^{35} + 2542413744\,z^{36}$

$+ 9451146744\,z^{37} + 28353440232\,z^{39} + 45763447392\,z^{41} + 78345032220\,z^{42} + 293980406616\,z^{43}$

$+ 881941219848\,z^{45} + 1410210579960\,z^{47} + 2377212120504\,z^{48} + 8985055980888\,z^{49} + 26955167942664\,z^{51}$

$+ 42789818169072\,z^{53} + 71255926018836\,z^{54} + 270881306544888\,z^{55} + 812643919634664\,z^{57}$

$+ 1282606668339048\,z^{59} + 1718301299950404\,z^{60} + 7284422604917952\,z^{61} + 21853267814753856\,z^{63}$

$+ 30929423399107272\,z^{65} + 41239231198809696\,z^{66} + 175266732594941208\,z^{67} + 525800197784823624\,z^{69}$

$+ 742306161578574528\,z^{71} + 974276837071879068\,z^{72} + 4175472158879481720\,z^{73} + 12526416476638445160\,z^{75}$

$+ 17536983067293823224\,z^{77} + 22547549657949201288\,z^{78} + 97706048517779872248\,z^{79}$

$+ 293118145553339616744\,z^{81} + 405855893843085623184\,z^{83} + 507319867303857028980\,z^{84}$

$+ 2232207416136970927512\,z^{85} + 6696622248410912782536\,z^{87} + 9131757611469426521640\,z^{89}$

$+ 10958109133763311825968\,z^{90} + 49311491101934903216856\,z^{91} + 147934473305804709650568\,z^{93}$

$+ 197245964407739612867424\,z^{95} + 221901709958707064475852\,z^{96} + 1035541313140632967553976\,z^{97}$

$+ 3106623939421898902661928\,z^{99} + 3994230779256727160565336\,z^{101} + 3994230779256727160565336\,z^{102}$

$+ 1997115389628363580282680\,z^{103} + 5991346168885090740848040\,z^{105} + 7189615402662108889017\,6048\,z^{107}$

$+ 5392211551996581666763203\,6\,z^{108} + 3235326931197949000057922\,16\,z^{109}$

$+ 9705980793593847000173766\,48\,z^{111} + 9705980793593847000173766\,48\,z^{113}$

$+ 2911794238078154100052129\,944\,z^{115} + 8735382714234462300156389\,832\,z^{117}$

Example n = 9 · 14: In this case, $x^{9 \cdot 14} - 1 = (x-1)^9(x+1)^9 r_1^9 r_2^9$ for prime self-reciprocal polynomials r_1, r_2 both of degree 6. By Theorem 4,

$$\mathcal{G}_{9 \cdot 14}^{(3)}(z) = (1 + 2\sum_{j=1}^{5} 3^{j-1} z^{2j-1})^2 (1 + 26\sum_{j=1}^{9} 3^{3(j-1)} z^{6j})^2 =$$

$1 + 4\,z + 4\,z^2 + 12\,z^3 + 24\,z^4 + 36\,z^5 + 160\,z^6 + 316\,z^7 + 640\,z^8 + 948\,z^9 + 2868\,z^{10} + 1872\,z^{11} + 11584\,z^{12}$

$+ 13936\,z^{13} + 39532\,z^{14} + 41808\,z^{15} + 151656\,z^{16} + 74880\,z^{17} + 527472\,z^{18} + 522288\,z^{19} + 1651104\,z^{20}$

$+ 1566864\,z^{21} + 6065280\,z^{22} + 2678832\,z^{23} + 19990152\,z^{24} + 18044208\,z^{25} + 60349536\,z^{26} + 54132624\,z^{27}$

$+ 216985392\,z^{28} + 90069408\,z^{29} + 694967364\,z^{30} + 593639280\,z^{31} + 2055220128\,z^{32} + 1780917840\,z^{33}$

$+ 7295622048\,z^{34} + 2910879504\,z^{35} + 22955416848\,z^{36} + 18902293488\,z^{37} + 66987075168\,z^{38}$

$+ 56706880464\,z^{39} + 235781239824\,z^{40} + 91526894784\,z^{41} + 732961301436\,z^{42} + 587960813232\,z^{43}$

$+ 2119046585760\,z^{44} + 1763882439696\,z^{45} + 7413678477504\,z^{46} + 2820421159920\,z^{47} + 22845411395352\,z^{48}$

$+ 17970111961776\,z^{49} + 65594937833568\,z^{50} + 53910335885328\,z^{51} + 228454113953520\,z^{52}$

$+ 85579636338144\,z^{53} + 699323426602164\,z^{54} + 541762613089776\,z^{55} + 1997341681993632\,z^{56}$

$+ 1625287839269328\,z^{57} + 6931950543389664\,z^{58} + 2565213336678096\,z^{59} + 20712629060085924\,z^{60}$

$+ 14568845209835904\,z^{61} + 58451616870107760\,z^{62} + 43706535629507712\,z^{63} + 198265534609662000\,z^{64}$

$+ 61858846798214544\,z^{65} + 566246366845194672\,z^{66} + 350533465189882416\,z^{67} + 1530609927186590640\,z^{68}$

$+ 1051600395569647248\,z^{69} + 5020083336316641840\,z^{70} + 1484612323157149056\,z^{71}$

$+ 13978909783188828972\,z^{72} + 8350944317758963440\,z^{73} + 36744154998139439136\,z^{74}$

$+ 25052832953276890320\,z^{75} + 120253598175729073536\,z^{76} + 35073966134587646448\,z^{77}$

$+ 333202678278582641256\,z^{78} + 195412097035559744496\,z^{79} + 871838586774035783136\,z^{80}$

$+ 586236291106679233488\,z^{81} + 2840991256901599362288\,z^{82} + 811711787686171246368\,z^{83}$

$+ 7812725956479398246292\,z^{84} + 4464414832273941855024\,z^{85} + 20292794692154281159200\,z^{86}$

$+ 13393244496821825565072\,z^{87} + 65748654802579870955808\,z^{88} + 18263515222938853043280\,z^{89}$

$+ 178982449184800759824144\,z^{90} + 98622982203869806433712\,z^{91} + 460240583618059096690656\,z^{92}$

$+ 295868946611609419301136\,z^{93} + 1479344733058047096505680\,z^{94} + 394491928815479225734848\,z^{95}$

$+ 3969575033705759708956908\,z^{96} + 20710826262812659351079 52\,z^{97} + 10059544184794720256238624\,z^{98}$

$+ 6213247878843797805323856\,z^{99} + 31953846234053817284522688\,z^{100} + 7988461558513454321130672\,z^{101}$

$+ 83878846364391270371872056\,z^{102} + 399423077925672716056533 60\,z^{103}$

$+ 207700000521349812349397472\,z^{104} + 119826923377701814816960080\,z^{105}$

$+ 647065386239589800011584432\,z^{106} + 1437923080532421777803520 96\,z^{107}$

$+ 1635637504105629772251505092\,z^{108} + 647065386239589800011584432\,z^{109}$

$+ 3882392317437538800069506592\,z^{110} + 1941196158718769400034753296\,z^{111}$

$+ 11647176952312616400208519776\,z^{112} + 1941196158718769400034753296\,z^{113}$

$+ 27176746222062771600486546144\,z^{114} + 58235884761563082001042598 88\,z^{115}$

$+ 58235884761563082001042598880\,z^{116} + 17470765428468924600312779664\,z^{117}$

$+ 157236888856220321402815016976\,z^{118} + 31447377771244064280 5630033952\,z^{120}$

$+ 471710666568660964208445050928\,z^{122} + 943421333137321928416890101856\,z^{124}$

$+ 1415131999705982892625335152784\,z^{126}$

Example n = 9 · 20: With $x^{9 \cdot 14} - 1 = (x-1)^9(x+1)^9 r_1^9 r_2^9 r_3^9, r_4^9$, where r_1, r_2, r_3, r_4 are prime self-reciprocal polynomials of degrees $2, 4, 4$ and 8, from

Theorem 4 we obtain

$$\mathcal{G}_{9\cdot20}^{(3)}(z) = (1 + 2\sum_{j=1}^{5} 3^{j-1}z^{2j-1})^2(1 + 2\sum_{j=1}^{9} 3^{j-1}z^{2j})(1 + 8\sum_{j=1}^{9} 3^{2(j-1)}z^{4j})^2(1 + 80\sum_{j=1}^{9} 3^{4(j-1)}z^{8j})$$

Expanding, for instance from the coefficient of z^{99} we see that the number of 81-plateaued functions in $\mathcal{D}$ for $p = 3$ and $n = 9\cdot20$ is 61694647213794052687713 9072. Furthermore we see that the number of bent functions in the set $\mathcal{D}$ is $\mathcal{N}_{9\cdot20}^{(3)} =$ 6054249652811609019026768290053459869736960. Here we omit writing down the whole expanded version of the polynomial $\mathcal{G}_{9\cdot20}^{(3)}$.