ON THE SPECTRA OF QUADRATIC FUNCTIONS

by

CANAN KAŞIKCI

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University
Fall 2014

ON THE SPECTRA OF QUADRATIC FUNCTIONS

APPROVED BY

Prof. Dr. Alev Topuzoğlu .....
(Thesis Supervisor)

Assoc. Prof. Dr. Wilfried Meidl .....
(Thesis Co-supervisor)

Assoc. Prof. Dr. Cem Güneri .....

Assoc. Prof. Dr. Albert Levi .....

Prof. Dr. Henning Stichtenoth .....

DATE OF APPROVAL: .....

©Canan Kaşıkcı 2015
All Rights Reserved

ON THE SPECTRA OF QUADRATIC FUNCTIONS

Canan Kaşıkcı

Mathematics, PhD Thesis, 2015

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Thesis Co-Supervisor: Assoc. Prof. Dr. Wilfried Meidl

Keywords: Quadratic functions, Walsh Transform, expected value, variance, nonlinearity, discrete Fourier transform.

Abstract

Study of quadratic forms goes back to the 18th century. They attracted particular interest in the last decades also because of their applications. Indeed, there is an interaction between quadratic functions, cryptography and coding theory via their relation with Boolean bent/semi-bent functions, sequences, and various types of codes.

The Walsh transform $\widehat{f}$ of a quadratic function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ satisfies $|\widehat{f}(y)| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for all $y \in \mathbb{F}_{p^n}$ and for an integer $0 \leq s < n$. In other words quadratic functions form a subclass of the so-called plateaued functions. The value of s is 0 for example, in the case of the well-known bent functions, hence bent functions are 0-plateued.

In this thesis we study quadratic functions $\mathcal{F}_{p,n} = \sum_{i=0}^{k} Tr_n(a_i x^{p^i+1})$ given in trace form with the restriction that $a_i \in \mathbb{F}_p$, $0 \leq i \leq k$. Extensive work on quadratic functions with such restrictions on coefficients shows that they have many interesting features.

In this work we determine the expected value for the parameter s for such quadratic functions, for many classes of integers n. Our exact formulas confirm that on average the value of s is small, and hence the average nonlinearity of this class of quadratic functions is high when $p = 2$.

KUADRATIK FONKSIYONLARIN SPEKTRUMU ÜZERINE

Canan Kaşıkcı

Matematik, Doktora Tezi, 2015

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu
Tez Eş Danışmanı: Doç. Dr. Wilfried Meidl

Anahtar Kelimeler: Kuadratik fonksiyonlar, Walsh dönüşümü, beklenen değer, varyans, doğrusalsızlık, kesikli Fourier dönüşümü

Özet

Kuadratik fonksiyonlara ait çalışmalar 18. yüzyıla kadar gitmektedir. Son yıllarda uygulamaları sebebiyle bu fonksiyonlara ilgi daha da artmıştır. Gerçekten de kuadratik fonksiyonlar, şifreleme ve kodlama teorisi, ikili bükük/yarı bükük fonksiyonlar, diziler ve bazı kodlarla yakından bağlantılıdır.

Kuadratik bir fonksiyonun Walsh dönüşümlerinin mutlak değeri $0 \leq s < n$ aralığındaki bir tam sayı s için 0 veya $p^{\frac{n+s}{2}}$ değerini alır. Başka bir deyişle kuadratik fonksiyonlar basamaklı fonksiyonların bir alt sınıfını oluşturmaktadır. Bükük fonksiyonlar örneğinde s'nin aldığı değer sıfırdır, yani bükük fonksiyonlar 0-basamaklı fonksiyonlardır.

Bu tezde trace formunda $\mathcal{F}_{p,n} = \sum_{i=0}^{k} Tr_n(a_i x^{p^i+1})$ verilmiş olan kuadratik fonksiyonlardan katsayıları $a_i \in \mathbb{F}_p$, $0 \leq i \leq k$ şartını sağlayanlar çalışılmıştır. Katsayılar üzerinde benzer koşulları sağlayan kuadratik fonksiyonlara dair yapılmış olan geniş araştırmalar bu fonksiyonların dikkat çeken özelliklerini göstermiştir.

Bu tezde birçok n tamsayı sınıfı için bahsi geçen kuadratik fonksiyonların s parametresinin beklenen değeri belirlenmiştir. Bulunan formüller ortalama olarak s değerinin küçük olduğunu ve böylece $p = 2$ için bu kuadratik fonksiyon sınıfının ortalama doğrusalsızlığının yüksek olduğunu doğrulamıştır.

to my family

Acknowledgments

First of all, I would like to thank to the Mathematics Program of Sabancı University for supporting me and creating a warm and friendly atmosphere that I enjoyed all through my studies. I would gratefully like to thank my supervisors Alev Topuzoğlu and Wilfried Meidl for their encouragement and guidance at all stages of my work. Last but by no means least, I would like to thank my family with all my heart for all their love and encouragement that I received all through my life, and to my dear friends Nurdagül Anbar, Duygu Karaoğlan Altop, Barış Altop and Ayça Çesmelioğlu for their support and friendship.

Table of Contents

CHAPTER 1

INTRODUCTION

In this chapter, we present basic concepts concerning quadratic functions, Walsh transorm and plateaued functions. For further details we refer to [33], [2]. We assume basic knowledge on finite fields. Therefore, other than recalling the definition and basic properties of the trace function, we do not give further information on finite fields. We close this chapter with some remarks on applications of quadratic/plateaued functions.

1.1 Quadratic Functions

We start by recalling the absolute trace map between finite fields. Let p be a prime, $n > 1$ be an integer. The trace map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined by

$$Tr(x) = x + x^p + x^{p^2} + ... + x^{p^{n-1}}$$

Note that the trace map is $\mathbb{F}_p$-linear and surjective. It is balanced in the sense that for every $c \in \mathbb{F}_p$, there exist p^{n-1} preimages in $\mathbb{F}_{p^n}$.

Let n be a positive integer. A Boolean function $f(x)$ of n-variables is a function from the set $\mathbb{F}_2^n$ of all binary vectors $x = (x_1, ..., x_n)$ of length n to the field $\mathbb{F}_2$. The *Hamming weight* $wt(f)$ of an n-variable Boolean function is the size of its *support*, i.e. $wt(f) = supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. The function f is balanced if it has *Hamming weight* 2^{n-1}. The *Hamming distance* between two n-variable Boolean functions f and g is the size of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$, that is, it is $wt(f+g)$. The domain $\mathbb{F}_2^n$ can be endowed with the structure of the field $\mathbb{F}_{2^n}$. Boolean functions can be represented in different ways. We introduce the ones mostly used in coding theory, cryptography and communications with advantage, since they provide uniquely determined parameters.

Proposition 1.1.1 Every n-variable Boolean function f can be represented uniquely

by a multivariate polynomial, i.e, f is a polynomial mapping over $\mathbb{F}_2$ of the form

$$f(x) = \sum_{I \subseteq \{1,...,n\}} a_I \left(\prod_{i \in I} x_i \right) \in \mathbb{F}_2 \left[x_1, ..., x_n \right] / ({x_1}^2 + x_1, ..., {x_n}^2 + x_n). \tag{1.1}$$

Definition 1.1.1 This representation (1.1) of a Boolean function f is called *algebraic normal form(ANF)* of f. The terms $\prod_{i \in I} x_i$ are monomials while the coefficients $a_I \in \mathbb{F}_2$.

Definition 1.1.2 The *algebraic degree* $d^\circ f$ of f given in the form 1.1 is defined to be the highest degree of the monomial with non-zero coefficients, i.e.,

$$d^\circ f = \{max\, |I| : a_I \neq 0\}$$

.

Proposition 1.1.2 Let $\mathbb{F}_2^n$ be identified with the field $\mathbb{F}_{2^n}$ and let f be an n-variable Boolean function with even weight (i.e., of algebraic degree at most $n-1$). There exists a unique representation of f as a univariate polynomial mapping of the form

$$f(x) = \sum_{j \in \Gamma_n} Tr_{\mathbb{F}_{2^{o(j)}}/\mathbb{F}_2} \left(A_j x^j \right), x \in \mathbb{F}_{2^n}, \tag{1.2}$$

where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 (mod $2^n - 1$) and $o(j)$ is the size of each cyclotomic coset containing j, $A_j \in \mathbb{F}_{2^{o(j)}}$ and $Tr_{\mathbb{F}_{2^{o(j)}}/\mathbb{F}_2}$ is the trace function from $\mathbb{F}_{2^{o(j)}}$ to $\mathbb{F}_2$.

Definition 1.1.3 The representation (1.2) is called the trace representation (or univariate representation) of f.

Definition 1.1.4 A function is *affine*, respectively *quadratic* if it has algebraic degree at most 1, respectively 2.

Proposition 1.1.3 Let f be given by its trace representation (1.2). Then f has algebraic degree $\max\limits_{j \in \Gamma_n | A_j \neq 0} w_2(j)$, where $w_2(j)$ is the Hamming weight of the binary expansion of j.

Proposition 1.1.4 The algebraic degree of an n-variable Boolean function f is the maximum dimension of the subspaces $\{x \in \mathbb{F}_2^n | supp(x) \subseteq I\}$, where I is any subset of $\{1, ..., n\}$, on which f takes the value 1 an odd number of times.

Now we present similar results for p-ary functions, for $p \geq 3$. Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary function. If $\mathbb{F}_p^n$ is identified with the field $\mathbb{F}_{p^n}$, all p-ary functions can be described by $Tr_n(F(x))$ for some function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ of degree at most $p^n - 1$. This is called the *univariate representation* of f. On the other hand, a p-ary function can naturally be represented as a multinomial in $x_1, ..., x_n$ also, where the variables x_i occur with the exponent at most $p - 1$. This is called the *multivariate representation* or *algebraic normal form(ANF)*. This representation is unique. The *algebraic degree* of a p-ary function is the degree of the polynomial giving its multivariate representation.

The univariate representation mentioned above is not unique. However a unique univariate form of a p-ary function, called the trace representation can be given as follows:

$$f(x) = \sum_{j \in \Gamma_n} Tr_{o(j)} \left(A_j x^j \right) + A_{p^n-1} x^{p^n-1}, \tag{1.3}$$

where Γ_n is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $p^n - 1$ and $o(j)$ is the size of the cyclotomic coset containing j, $A_j \in \mathbb{F}_{p^{o(j)}}$ and $A_{p^n-1} \in \mathbb{F}_p$. The algebraic degree of f is equal to $\max\limits_{j \in \Gamma_n | A_j \neq 0} w_p(j)$, where $w_p(j)$ is the weight of the p-ary expansion of j. Now omitting linear and constant terms, a p-ary quadratic function, i.e., a function of algebraic degree 2 has an algebraic normal form

$$f(x_1, x_2, ..., x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j, a_{ij} \in \mathbb{F}_p. \tag{1.4}$$

The corresponding trace representation

$$f(x) = \sum_{1 \leq i,j \leq n-1} Tr \left(\alpha_{ij} x^{p^i + p^j} \right), \alpha_{ij} \in \mathbb{F}_{p^n} \tag{1.5}$$

can be written as

$$f(x) = Tr(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}), \quad a_i \in \mathbb{F}_{p^n}. \tag{1.6}$$

If n is odd, this representation is unique. For even n the coefficient $a_{n/2}$ needs to be taken modulo $K = \{a \in \mathbb{F}_{p^n} \mid \mathrm{Tr_{n/(n/2)}}(a) = 0\}$, where $\mathrm{Tr_{n/k}}$ denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$; $Tr_{n/k}(x) = x + x^p + .. + x^{p^{n/k-1}}$.

1.2 Walsh Transform

The *Walsh transform* (or *Fourier transform*) of a Boolean/p-ary function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined as

$$\widehat{f}(y) = \sum_{x \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x)-Tr(yx)}, \quad \varepsilon_p = e^{2\pi i/p}.$$

The set $\left\{\widehat{f}(y) : y \in \mathbb{F}_{p^n}\right\}$ is called the *Walsh spectrum* of f, or just spectrum of f.

Proposition 1.2.1 Every Boolean/p-ary function satisfies

$$\sum_{y \in \mathbb{F}_{p^n}} |\widehat{f}(y)|^2 = p^{2n},$$

which is the well known Parseval's relation.

Remark:In case $p = 2$, if $\left|\widehat{f}(y)\right|$ is "large" the values of $f(x)$ agree with $Tr(yx)$ (if $\widehat{f}(y) > 0$) or $Tr(yx) + 1$ (if $\widehat{f}(y) < 0$) for many $x \in \mathbb{F}_{2^n}$. In other words, f is well approximated by a linear function. This remark motivates the following notion:

$$\mathcal{L}(f) = \max\{\left|\widehat{f}(y)\right| : y \in \mathbb{F}_{2^n}\}$$

Note that if $\mathcal{L}(f)$ is "small", the Boolean function f is far from being linear, i.e. it is nonlinear.

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.

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

For $p = 2$, the nonlinearity of f can be expressed in terms of the Walsh transform as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}_{2^n}} |\widehat{f}(y)|. \tag{1.7}$$

1.3 Plateaued Functions

Definition 1.3.1 Let $p \geq 3$. A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a *(p-ary) bent function* or (*generalized bent function*) if all its Walsh coefficients satisfy $|\widehat{f}(y)|^2 = p^n$. A bent function f is *regular* if for every $y \in \mathbb{F}_p^n$, the normalized Walsh coefficient $p^{-n/2}\widehat{f}(y)$ is equal to a complex p-th root of unity, i.e., $p^{-n/2}\widehat{f}(y) = {\epsilon_p}^{f^*(y)}$ for some function $f^* : \mathbb{F}_p^n \to \mathbb{F}_p$. A bent function f is *weakly regular* if there exits a complex number u having unit magnitude such that $up^{-n/2}\widehat{f}(y) = {\epsilon_p}^{f^*(y)}$ for all $y \in \mathbb{F}_p^n$.

Definition 1.3.2 A boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is *bent* if

$$|\widehat{f}(y)| = \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+y.x} \right| = 2^{n/2} \tag{1.8}$$

for all $y \in \mathbb{F}_2^n$.

In the Boolean case the dimension n must be even, since $\widehat{f}(y)$ is an integer. A Boolean bent function is trivially regular.

Theorem 1.3.3 The normalized Walsh coefficients of a p-ary bent function f satisfies

$$p^{-n/2}\widehat{f}(y) = \begin{cases} \pm {\epsilon_p}^{f^*(y)} & \text{if n is even or n is odd and p} \equiv 1(\text{mod4}) \\ \pm i{\epsilon_p}^{f^*(y)} & \text{if n is odd and p} \equiv 3(\text{mod4}) \end{cases}$$

for $p \geq 3$, and ± 1 for $p = 2$.

Regular bent functions can exist only when n is even or when n is odd and $p \equiv 1 \bmod 4$. For a weakly regular bent function, the constant u can only be equal to ± 1 and $\pm i$. Boolean bent functions were introduced by Rothaus in [35]. These are the functions attaining the highest possible nonlinearity. In other words, they have the maximal possible Hamming distance from the class of all affine functions. Now we present some fundamental classes of bent functions. The following is a complete list of Boolean bent functions on $\mathbb{F}_2^{2m}$ for $1 \leq m \leq 3$ up to equivalence see [35]:

1. x_1x_2 for $m = 1$,
2. $x_1x_2 + x_3x_4$ for $m = 2$,
3. $x_1x_4 + x_2x_5 + x_3x_6 = F_3$,
4. $F_3 + x_1x_2x_3 = F_4$,
5. $F_4 + x_2x_4x_6 + x_1x_2 + x_4x_6 = F_5$,
6. $F_5 + x_3x_4x_5 + x_1x_2 + x_3x_5 + x_4x_5 = F_6$.

The following monomial functions $f(x) = Tr(\alpha x^d)$ are bent on $\mathbb{F}_{2^n}$ with $n = 2m$:

1. $d = 2^k + 1$ with $n/gcd(k, n)$ being even and $\alpha \notin y^d : y \in \mathbb{F}_{2^n}$ ([18]);
2. $d = r(2^m - 1)$ with $gcd(r, 2^m + 1) = 1$ and $\alpha \in \mathbb{F}_{2^m}$ being -1 of the Kloosterman sum ([7]);

3. $d = 2^{2k} - 2^k + 1$ with $gcd(k, n) = 1$ and $\alpha \notin y^3 : y \in \mathbb{F}_{2^n}$ ([25], [11]);

4. $d = (2^k + 1)^2$ with $n = 4k$ and k odd, $\alpha \in \omega\mathbb{F}_{2^k}$ with $\omega \in \mathbb{F}_4\mathbb{F}_2$ ([8], [26]);

5. $d = 2^{2k} + 2^k + 1$ with $n = 6k$ and $k > 1$, $\alpha \in \mathbb{F}_{2^{3k}}$ with $Tr_{\mathbb{F}_{2^{3k}}/\mathbb{F}_{2^k}}(\alpha) = 0$ ([1]).

A positive integer d (always understood modulo $2^n - 1$ with $n = 2m$) is a *Niho exponent* if $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. The following are the examples of bent functions consisting of one or more Niho exponents:

1. Quadratic Functions $Tr_m(ax^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$.

2. Binomials of the form $f(x) = Tr_n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, where $2d_1 \equiv 2^m + 1 \pmod{2^n - 1}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^*$ are such that $(\alpha_1 + {\alpha_2}^{2^m})^2 = {\alpha_2}^{2^m+1}$ ([12]).

Definition 1.3.4 A function f, mapping $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called an *(s-)plateaued function* if for every $y \in \mathbb{F}_p^n$, the Walsh transform $\widehat{f}(y)$ vanishes or has absolute value $p^{(n+s)/2}$ for some fixed integer $0 \leq s \leq n$. The case $s = 0$ corresponds to bent functions.

As mentioned above, in case $p = 2$ since $\widehat{f}(y)$ is an integer for every $y \in \mathbb{F}_{2^n}$, 0-plateaued functions, i.e., Boolean bent functions are only defined for even n. If f is an s-plateaued Boolean function, $s > 0$, then n and s need to be of the same parity. Depending on n being odd or even, 1 or 2-plateaued functions are called *semi-bent*. When p is odd the term semi-bent refers to 1-plateaued functions. Quadratic functions are s-plateaued for some integer s, with $0 \leq s \leq n - 1$.

Theorem 1.3.5 [3] Let f be the quadratic p-ary function

$$f(x) = Tr_n\left(\sum_{i=0}^{l} a_i x^{p^i+1}\right),$$

and let $L(z)$ be the linearized polynomial

$$L(z) = \sum_{i=0}^{l} \left({a_i}^{p^l} z^{p^{l+i}} + {a_i}^{p^{l-i}} z^{p^{l-i}}\right).$$

The square of the Walsh transform of f takes the absolute values 0 and p^{n+s}, where s is the dimension of the kernel of the linear transformation on $\mathbb{F}_{p^n}$ defined by $L(z)$.

Proof: With the standard Welch-squaring technique we obtain

$$\begin{aligned}\left|\widehat{f}(-b)\right|^2 &= \sum_{x,y\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(y)+Tr_n(b(x-y))} \\ &= \sum_{y,z\in\mathbb{F}_{p^n}} \varepsilon_p^{f(y+z)-f(y)+Tr_n(bz)} \\ &= \sum_{z\in\mathbb{F}_{p^n}} \varepsilon_p^{f(z)+Tr_n(bz)} \sum_{y\in\mathbb{F}_{p^n}} \varepsilon_p^{f(y+z)-f(y)-f(z)}.\end{aligned}$$

Observe that

$$\begin{aligned}f(y+z)-f(y)-f(z) &= Tr_n\left(\sum_{i=0}^{l} a_i\left((y+z)^{p^i+1}-y^{p^i+1}-z^{p^i+1}\right)\right) \\ &= Tr_n\left(\sum_{i=0}^{l} a_i\left(yz^{p^i}+y^{p^i}z\right)\right) \\ &= Tr_n\left(y^{p^l}\sum_{i=0}^{l}\left({a_i}^{p^l}z^{p^{l+i}}+{a_i}^{p^{l-i}}z^{p^{l-i}}\right)\right) \\ &= Tr_n(y^{p^l}L(z)).\end{aligned}$$

Consequently

$$\begin{aligned}\left|\widehat{f}(-b)\right|^2 &= \sum_{z\in\mathbb{F}_{p^n}} \varepsilon_p^{f(z)+Tr_n(bz)} \sum_{y^{p^l}\in\mathbb{F}_{p^n}} \varepsilon_p^{Tr_n(yL(z))} \\ &= p^n \sum_{z\in\mathbb{F}_{p^n}\, L(z)=0} \varepsilon_p^{f(z)+Tr_n(bz)} \\ &= \begin{cases} p^{n+s} & \text{if } f(z)+Tr_n(bz)\equiv 0 \text{ on } ker(L) \\ 0 & \text{otherwise}\end{cases}\end{aligned}$$

since $f(z)+Tr_n(bz)$ is linear on the kernel of L. □

In this thesis we focus on the class of quadratic functions $\mathcal{F}_{p,n}:\mathbb{F}_{p^n}\to\mathbb{F}_p$ given in trace form, i.e.,

$$\mathcal{F}_{p,n}(x)=Tr_n\left(\sum_{i=0}^{k} a_i x^{p^i+1}\right), \tag{1.9}$$

where p is any prime, and the coefficients $a_0,\ldots,a_k$ are in the prime field $\mathbb{F}_p$. If p is odd, then functions of the form (1.9) have a unique representation as

$$\mathcal{F}_{p,n}(x)=Tr_n\left(\sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{p^i+1}\right). \tag{1.10}$$

If $p = 2$, then for even n we have $x^{2^{n/2}+1} \in \mathbb{F}_{2^{n/2}}$ and $Tr_n(x^{2^{n/2}+1} = 0)$ for all $x \in \mathbb{F}_2^n$. Every function of the form (1.9) has then a unique representation as

$$\mathcal{F}_{2,n}(x) = Tr_n\left(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}\right), \tag{1.11}$$

see Theorem 1.2 in [13].

1.4 Linear Complexity, Discrete Fourier Transform, Applications

Let $S = s_0, s_1, s_2, \ldots$ be a sequence with terms in the prime field $\mathbb{F}_p$. S is said to be *n-periodic* if $s_i = s_{i+n}$. Since an n-periodic sequence is determined by the terms in one period, we can completely describe S as $S = (s_0, s_1, \ldots, s_{n-1})^\infty$. For an n-periodic sequence $S = (s_0, s_1, \ldots, s_{n-1})^\infty$, the *generating polynomial* $S_n(x)$ of S is defined as $S_n(x) = s_0 + s_1 x + \ldots + s_{n-1}x^{n-1}$.

Definition 1.4.1 Let $S = (s_0, s_1, ..., s_{n-1})^\infty$ be an n-periodic sequence over $\mathbb{F}_p$. The *linear complexity* $L(s)$ of S is the smallest nonnegative integer c for which there exit coefficients $d_1, d_2, \ldots, d_c \in \mathbb{F}_p$ such that

$$s_j + d_1 s_{j-1} + \ldots + d_c s_{j-c} = 0,$$

for all $j \geq c$.

Lemma 1.4.2 [10] Let $S = (s_0, s_1, \ldots, s_{n-1})^\infty$ be an n-periodic sequence over $\mathbb{F}_p$. The *linear complexity* $L(S)$ of S is given by

$$L(S) = n - \deg(\gcd(S_n(x), x^n - 1)), \tag{1.12}$$

where $S_n(x) = s_0 + s_1 x + \ldots + s_{n-1}x^{n-1}$ is the generating polynomial of the sequence S.

Definition 1.4.3 Suppose that $\gcd(n, p) = 1$ and let α be a primitive nth root of unity in an extension field of $\mathbb{F}_p$. The *discrete Fourier transform* (DFT) of an n-tuple $s = (s_0, s_1, \ldots, s_{n-1})$ over $\mathbb{F}_p$ is the n-tuple $\mathcal{S} = (\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$ over $\mathbb{F}_p(\alpha)$ defined by

$$S = V \cdot s$$

where the n-tuples s and S are written as column vectors and $V = (v_{ij})$, $0 \leq i, j \leq n-1$, is the invertible $n \times n$ Vandermonde matrix with $v_{ij} = \alpha^{ij}$.

The discrete Fourier trasform has been used to study the linear complexity of n-periodic sequences. Next theorem describes this connection.

Theorem 1.4.4 *(Blahut's Theorem)* [29] Suppose $\gcd(n, p) = 1$ and let α be a primitive nth root of unity in some extension field of $\mathbb{F}_p$. Then the linear complexity of an n-periodic sequence $S = (s_0, s_1, \ldots, s_{n-1})^\infty$ is equal to the Hamming weight of the discrete Fourier transform of S.

So (1.12) becomes

$$\deg(\gcd(S_n(x), x^n - 1)) = n - Hw(\mathcal{S}), \tag{1.13}$$

where $\mathcal{S} = (\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$ with $\mathcal{S}_j = S(\alpha^j)$.

Quadratic functions have been extensively studied in the last decades. They are used for the construction of functions, sequences with favourable properties for applications in cryptography and coding theory. In [9] quadratic functions have been employed to construct nonquadratic Boolean bent and semi-bent functions. In ([3], [4], [5]) infinite classes of not weakly regular bent functions for arbitrary dimension n and primes $p \geq 3$ have been constructed and analysed with the help of quadratic functions. In coding theory quadratic functions form the second order Reed-Muller codes.

The functions $\mathcal{F}_{p,n}$ and their Walsh spectra are of great interest. For instance, one may ask the following questions (see [30]):

- Given s, determine n, such that all $\mathcal{F}_{p,n}$ are s-plateaued.
- Given n, find possible s, such that there exists a function $\mathcal{F}_{p,n}$, which is s-plateaued.
- Given n and s, construct $\mathcal{F}_{p,n}$, which is s-plateaued.
- Given n, for any s, enumarate all $\mathcal{F}_{p,n}$, which are s-plateaued.
- Given n, determine the expected value for the parameter s.

In [23] the authors showed that the only odd integers n such that all non-zero functions $\mathcal{F}_{2,n}$ are semi-bent are a certain kind of primes. In other words given $s = 1$, they determined n, such that all $\mathcal{F}_{2,n}$ are 1-plateaued. In [9] the authors characterized the set of even n such that all $\mathcal{F}_{2,n}$ are semi-bent, i.e., 2-plateaued. In fact, they showed

that unless $n = 4$, there is no n for which all $\mathcal{F}_{2,n}$ semi-bent. Recently in [30] the first two questions are answered for any $p \geq 2$, see Chapter 2.

Moreover in [30] for all s and odd n, relatively prime to p, theorems 2.3.1, 2.3.2 provide constructions for $\mathcal{F}_{p,n}$ which are s-plateaued.

The problem of enumerating $\mathcal{F}_{p,n}$ with prescribed Walsh spectrum was first addressed in [22], [23]. Similarly for the case $p = 2$, some enumeration results were obtained by the use of self-reciprocal polynomials in [14]. In [30] enumeration results were given for a class of integers n, for $n = 2^m$ for $p = 2$ and $n = q^m$ for primes $p, q \geq 3$ where p is a primitive root modulo q^2. These enumeration results were significantly improved in [31].

CHAPTER 2

CONSTRUCTION of sPLATEAUED FUNCTIONS

Recently new tools have been introduced to the study of the class of quadratic functions $\mathcal{F}_{p,n}$. Indeed, the use of self-reciprocal polynomials and the linear complexity of sequences in [30], [31] opened up a new area of research. In this thesis we heavily use these methods, which we introduce in this chapter.

2.1 Factorization of $\mathbf{x^n - 1}$, Self Reciprocal Polynomials, Cyclotomic Cosets

From now on $\mathcal{F}_{p,n}$ denotes a function of the form (1.10) and (1.11) respectively, depending on p being odd or even. Recall that $k = \lfloor (n-1)/2 \rfloor$ when $p = 2$ and $k = \lfloor n/2 \rfloor$ when $p \geq 3$.

Definition 2.1.1 A polynomial of the form

$$L(x) = \sum_{i=0}^{k} \alpha_i x^{p^i}$$

with coefficients in an extension field $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ is called a *p-polynomial* over $\mathbb{F}_{p^n}$.

Definition 2.1.2 The polynomials

$$l(x) = \sum_{i=0}^{k} \alpha_i x^i \text{ and } L(x) = \sum_{i=0}^{k} \alpha_i x^{p^i}$$

over $\mathbb{F}_{p^n}$ are called *p-associates* of each other.

Theorem 2.1.3 [27] Let $L_1(x)$ and $L(x)$ be linearized polynomials (i.e. p-polynomials) over $\mathbb{F}_p$ with p-associates $l_1(x)$ and $l(x)$, then $L_1(x)$ divides $L(x)$ if and only if $l_1(x)$ divides $l(x)$.

Using the standard Welch-squaring technique we have shown that(see theorem 1.3.5) the integer s is the dimension over $\mathbb{F}_p$ of the kernel of the linear transformation defined on $\mathbb{F}_{p^n}$ by

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

i.e., $\gcd(x^{p^n} - x, L(x))$ has degree p^s.

Equivalently, the kernel of L has dimension s if and only if the p-associates $A(x)$ and $x^n - 1$ of $L(x)$ and $x^{p^n} - x$, respectively, satisfy

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

This follows immediately from Theorem 2.1.3 and from the fact that $a_i \in \mathbb{F}_p$ for all $i \geq 0$. The associate $A(x)$ corresponding to $\mathcal{F}_{p,n}$ in (1.9) is

$$A(x) = \sum_{i=0}^{k} \left(a_i x^i + a_i x^{n-i} \right) = x^{i_0} g(x), \tag{2.1}$$

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

$$g(x) = \sum_{i=i_0}^{k} a_i \left(x^{i-i_0} + x^{n-i_0-i} \right) \tag{2.2}$$

of degree $n - 2i_0$. Thus the value of s is determined by

$$s = \deg(\gcd(A(x), x^n - 1)) = \deg(\gcd(g(x), x^n - 1)). \tag{2.3}$$

We note that in case $p = 2$ one has

$$\gcd\left(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i (x^i + x^{n-i}), x^n + 1 \right) = \gcd\left(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i (x^i + x^{n-i}) + a_0 (x^n + 1), x^n + 1 \right). \tag{2.4}$$

In other words, a_0 does not effect the value of s.

Definition 2.1.4 A polynomial $F(x)$ with non-zero constant term and of degree m over a finite field $\mathbb{F}_{p^r}$ is called *self reciprocal* if $F(x) = x^m F(\frac{1}{x})$.

The following lemma gives the basic properties of self-reciprocal polynomials, see [21], [27], [30].

Lemma 2.1.5 Let $F \in \mathbb{F}_{p^r}[x]$.

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

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

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

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

By Lemma 2.1.5(iv), in the case $p = 2$, if $A(x) \in \mathbb{F}_2[x]$ is self-reciprocal, then $gcd(x^n + 1, A(x))$ is self-reciprocal since $x^n + 1$ is self-reciprocal.
In case $p \geq 3$ we have

$$\gcd(x^n - 1, A(x)) = (x-1)^\epsilon h(x), \epsilon \in \{0, 1\},$$

for a self-reciprocal divisor $h(x) \in \mathbb{F}_p[x]$ of $\Psi_n(x) = (x^n - 1)/x - 1$. In what follows we use the notation of [30] and put

$$\Psi_n(x) = \begin{cases} x^n + 1 & \text{if } p = 2 \\ \frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + ... + 1 & \text{if } p \geq 3 \end{cases}$$

According to p being even or odd, we have

$$\gcd(x^n + 1, A(x)) = \text{gdc}(\Psi_n(x), A(x))$$

or

$$\gcd(x^n - 1, A(x)) = (x-1)^\epsilon \gcd(\Psi_n(x), A(x)), \epsilon \in \{0, 1\},$$

respectively. We therefore need to determine the self-reciprocal factors of $\Psi_n(x)$. For this purpose we recall cyclotomic cosets, corresponding factorization of $x^n - 1$ into irreducibles and introduce prime self-reciprocal polynomials over a finite field.

Definition 2.1.6 Let $\gcd(n, p) = 1$. The set $C_j = \left\{jp^k \bmod n, k \in \mathbb{N}\right\}$ is called the *cyclotomic coset* of j modulo n (relative to powers of p).

Definition 2.1.7 A self-reciprocal polynomial $f \in \mathbb{F}_q[x]$ is called *prime self-reciprocal* if either f itself is irreducible over $\mathbb{F}_q$, or $f = ugg^*$, 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.

We remark that for $n = p^v n_1$ and $\gcd(n_1, p) = 1$, one has $x^n - 1 = (x^{n_1} - 1)^{p^v}$. Thus for analysing the prime self-reciprocal factors of $x^n - 1$, one may assume that $\gcd(n, p) = 1$. Assuming $(n, p) = 1$, the canonical factorization of $x^n - 1 \in \mathbb{F}_p[x]$ into irreducible polynomials is

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

where α is a primitive nth root of unity and $C_{j_1}, \ldots, C_{j_h}$ are the distinct cyclotomic cosets modulo n. Recall also that for $n \geq 3$,

$$x^n - 1 = \prod_{m|n} Q_m,$$

where Q_m denotes the m-th cyclotomic polynomial. The cyclotomic polynomial Q_m factors into irreducible polynomials $f_1, ..., f_{\varphi(m)/d} \in \mathbb{F}_p[x]$, each of degree d, where $d = ord_m p$, and φ denotes the Euler φ-function. Here $ord_m p$ denotes the smallest integer l, such that $p^l \equiv 1$ mod m. More precisely we have

$$Q_m = f_1 ... f_{\varphi(m)/d} \quad \text{with} \quad f_t(x) = \prod_{j \in C_t} (x - \alpha^j), \tag{2.5}$$

where $C_1, \ldots, C_{\varphi(m)/d}$ are the cyclotomic cosets modulo n relative to powers of p, containing the elements of the form n/mi with $\gcd(m, i) = 1$. Next lemma provides a useful tool to determine self-reciprocal factors of a cyclotomic polynomial Q_m. We denote the 2-adic valuation of an integer l by $\upsilon(l)$, i.e., $2^{\upsilon(l)}$ is the largest power of 2 which divides l.

Lemma 2.1.8 [30] Let $m = {q_1}^{e_1} {q_2}^{e_2} ... {q_k}^{e_k}$ be odd, relatively prime to p, $d_i = ord_{q_i} p$, $1 \leq i \leq k$, and $d = ord_m p$. Suppose the irreducible factors of Q_m are $f_1, ..., f_{\varphi(m)/d}$.

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

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

By lemma 2.1.8 we see that the polynomial $f_t(x)$ in (2.5) is self-reciprocal, thus prime self-reciprocal if and only if C_{j_t}, containing the integer j_t, also contains its inverse $-j_t$ modulo m. If this is not the case, then there is another cyclotomic coset $C_{j_{t'}} = C_{n-j_t}$ consisting of inverses of the elements of C_{j_t}. Then $f_{t'} = f_{t^*}$ is the reciprocal of f_t and $f = f_t f_{t'}$ is prime self-reciprocal.

Example 2.1.1 Factorization of $x^n - 1$ into self-reciprocal polynomials when $p = 2$, $n = 3.5^2 = 75$ The cyclotomic cosets are:
$C_{j_1} = C_1 = \{1, 2, 4, 8, 16, 32, 64, 53, 31, 62, 49, 23, 46, 17, 34, 68, 61, 47, 19, 38\}$
$C_{j_2} = C_7 = \{7, 14, 28, 56, 37, 74, 73, 71, 67, 59, 43, 11, 22, 44, 13, 26, 52, 29, 58, 41\}$
$C_{j_3} = C_5 = \{5, 10, 20, 40\}$ $C_{j_4} = C_{35} = \{35, 70, 65, 55\}$
$C_{j_5} = C_3 = \{3, 6, 12, 24, 48, 21, 42, 9, 18, 36, 72, 69, 63, 51, 27, 54, 33, 66, 57, 39\}$
$C_{j_6} = C_{15} = \{15, 30, 60, 45\}$
$C_{j_7} = C_{25} = \{25, 50\}$ $C_0 = \{0\}$
For a primitive 45th root of unity α we put

$$f_t(x) = \prod_{i \in C_{j_t}} \left(x - \alpha^i\right),$$

$t = 1, ..., 7$. Then

$$x^{75} + 1 = (x + 1)Q_{75}Q_{25}Q_{15}Q_5Q_3,$$

with $Q_{75} = f_1 f_2$, $Q_{25} = f_5$, $Q_{15} = f_3 f_4$, $Q_5 = f_6$, $Q_3 = f_7$. The irreducible polynomials $(x + 1), f_5 = r_1, f_6 = r_2, f_7 = r_3$ are self-reciprocal, hence prime self-reciprocal but f_1, f_2, f_3, f_4 are not. We have $f_2 = {f_1}^*$ and $f_4 = {f_3}^*$. Hence $f_1 f_2 = r_4$ and $f_3 f_4 = r_5$ are the other prime self-reciprocal factors of $x^{75} + 1$.
Therefore $x^{75} + 1 = (x + 1)r_1 r_2 r_3 r_4 r_5$ factors into 6 prime self-reciprocal factors which are of degrees $1, 2, 4, 8, 20, 40$.

Corollary 2.1.9 Let $n = q_{e_1} q_{e_2} ... q_{e_k}$ be odd, relatively prime to p, and $d_i = ord_{q_i} p$, $1 \leq i \leq k$. Recall that $\Psi_n(x) = x^n + 1$ if $p = 2$ and $\Psi_n(x) = (x^n - 1)/x - 1$ if $p > 2$. All the irreducible factors of $\Psi_n(x)$ are self-reciprocal if and only if $\upsilon(d_1) = \upsilon(d_2) = ... = \upsilon(d_k) > 0$.

The following proposition from [30] shows that for given n and p the possible values of s are determined by the degrees of prime self-reciprocal factors of $\Psi_n(x)$.

Proposition 2.1.1 (i) Let $n = 2^v n_1$, $\gcd(n_1, 2) = 1$, and let $x^n + 1 = {r_1}^{2^v} {r_2}^{2^v} ... {r_k}^{2^v}$ be the canonical factorization of $x^n + 1$ into prime self-reciprocal polynomials over $\mathbb{F}_2$. Without lost of generality we put $r_1 = x + 1$. If $\mathcal{F}_{2,n} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a function of the form 1.11, then $\mathcal{F}_{2,n}$ is s-plateaued, where s is of the form

$$s = e_1 + \sum_{j=2}^{k} e_j deg(r_j), 0 \leq e_j \leq 2^v, j = 2, ..., k,$$

with $e_1 = 1$ when n is odd and $2 \leq e_1 \leq p^v$ is even when n is even.

(ii) For an odd prime p let $n = p^v n_1$, $\gcd(n_1, p) = 1$, and let $\Psi_n = {r_1}^{\frac{p^v-1}{2}} {r_2}^{p^v} ... {r_k}^{p^v}$ be the canonical factorization of $\Psi_n = \frac{(x^n-1)}{(x-1)}$ into prime self-reciprocal polynomials over $\mathbb{F}_p$, where $r_1(x) = x^2 - 2x + 1$. The function $\mathcal{F}_{p,n}$ is s-plateaued for an integer s of the form

$$s = \epsilon + \sum_{j=1}^{k} e_j deg(r_j), \epsilon \in \{0, 1\}, 0 \leq e_1 \leq (p^v - 1)/2), 0 \leq e_j \leq p^v, j = 2, ..., k.$$

Proof:

(i) We use the equation $s = \deg(\gcd(g(x), x^n - 1))$. The polynomial $g(x) \in \mathbb{F}_2[x]$ is self-reciprocal, hence by Lemma 2.1.5(iv), we have

$$\gcd(g(x), x^n + 1) = {r_1}^{e_1} {r_2}^{e_2} ... {r_k}^{e_k}$$

for some integers $0 \leq e_j \leq 2^v$. If n is odd, hence $v = 0$, then $e_1 = 1$. Note that $e_1 > 0$ since $g(x)$ is always divisible by $x + 1$. If n is even, then e_1 must be an even integer between 2 and 2^v, since s and n must be of same parity and the degrees of prime self-reciprocal polynomials $r_2, ...r_k$ are even.

(ii) Again, $g(x) \in \mathbb{F}_p[x]$ is self-reciprocal, and hence by Lemma 2.1.5(iv), we have

$$\gcd(g(x), x^n - 1) = (x - 1)^\epsilon \gcd(g(x), \Psi_n(x)) = (x - 1)^\epsilon {r_1}^{e_1} {r_2}^{e_2} ... {r_k}^{e_k},$$

where $\epsilon \in \{0, 1\}$, and $0 \leq e_1 \leq (p^v - 1)/2)$, $0 \leq e_j \leq p^v$, $j = 2, ..., k$. Now Equation 2.3 implies the result.

□

2.2 Existence of $s$plateaued functions

The following result of [30] gives a criteria for existence of s-plateaued functions.

Theorem 2.2.1 Let n be an arbitrary integer relatively prime to $p \geq 3$. There exists an s-plateaued quadratic function $\mathcal{F}_{p,n}$ if and only if

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

Proof: Let $h(x)$ be a self-reciprocal divisor of $x^n - 1$ of degree s. If n is odd, then $x+1$ cannot divide h, hence s must be even. We then put

$$h(x) = (x+1)g(x), i_o = (n - \deg(g(x)))/2$$

and obtain $A(x)$ as in 2.1. If n is even, then $x+1$ divides $x^n - 1$, and the degree s of $h(x)$ may be odd or even, depending on $x+1$ dividing $h(x)$ or not. If s is even we put $h(x) = g(x)$, otherwise we choose $h(x) = (x+1)g(x)$. In the latter case $x+1$ does not divide $(x^n-1)/h$. We then set $i_o = (n - deg(g(x)))/2$ and obtain $A(x)$ as in 2.1 giving rise to an s-plateaued function. If $x^n - 1$ has a self-reciprocal divisor $h(x)$ of degrees $s-1$, we put $h^{'}(x) = h(x)(x^2 - 2x + 1)$, and then obtain $A(x)$ as above. Note that in this case we have $\gcd(A(x), x^n - 1) = (x-1)h(x)$. We remark that the degree of $g(x)$ is at most n when $s < n-1$.
Conversely, if $\deg(\gcd(A(x), x^n - 1)) = s$ then there is a self-reciprocal factor $h(x)$ of $x^n - 1$ satisfying

$$\deg(\gcd(A(x), h(x))) = s \text{ or } \deg(\gcd(A(x), h(x))) = s-1 \text{ and } A(1) = 0.$$

Note that then 1 must be a double root of $A(x)$, however $\gcd(p, n) = 1$ implies that $(x-1)^2$ does not divide $x^n - 1$. □
The existence criteria for the case $p = 2$ is as follows.

Theorem 2.2.2 Let n be an arbitrary integer. There exists an s-plateaued quadratic function $\mathcal{F}_{2,n}$ if and only if $x^n + 1$ has a self-reciprocal factor $h(x)$ of degree $s \leq n-2$, where s and n are of the same parity, and $(x+1)|h(x)$. If $x^n + 1$ has such a factor $h(x)$, then $(x+1)^2|h(x)$ if n is even.

Proof: Proof of the first part is immediate. That $h(x)$ is divisible by $x+1$ or $(x+1)^2$ depending on n being odd or even, follows from $A(1) = 0$, implying $(x+1)|\gcd(x^n + 1, A(x))$. Note that when n is even, $(x+1)^2$ must be a factor of $h(x)$ because of Lemma 2.1.5(ii),(iii). □

This theorem immediately answers one of the questions raised on Section 1.4.

Corollary 2.2.3 Let $p \geq 3$. There is no $n \geq 3$ such that all $\mathcal{F}_{p,n}$ are bent or semi-bent.

Proof: The polynomial $x^n - 1$ has the self-reciprocal factor $\Psi_n(x) = x^{n-1} + x^{n-2} + ... + 1$ for any n, always yielding an $(n-1)$-plateaued quadratic function $\mathcal{F}_{p,n}$. □

Theorem 2.2.4 [32] Let $N(2e)$ denote the number of self-reciprocal irreducible monic polynomials of degree $2e$ over $\mathbb{F}_p$. Then

$$N(2e) = \begin{cases} \frac{1}{2e}(p^e - 1) & p \text{ odd and } e = 2^a,\ a \geq 0 \\ \frac{1}{2e} \sum\limits_{d|e, d \text{ odd}} \mu(d) p^{e/d} & \text{otherwise} \end{cases}$$

where $\mu(z)$ denotes the Möbius function on integers.

This result of Meyn [32] on self-reciprocal irreducible monic polynomials, together with the above theorem yields the following result.

Corollary 2.2.5 Let $n = p^m + 1$. Then there is an s-plateaued $\mathcal{F}_{p,n}$ if and only if $s < n$ is of the form

$$s = \epsilon + 2 \sum_{e|m, m/e \text{ odd}} a_e e,$$

with $\epsilon = 1$ when $p = 2$ and $\epsilon \in \{0, 1\}$ when $p > 2$, and for some $0 \leq a_e \leq N(2e)$, where $N(2e)$ is the number of monic, self-reciprocal irreducible polynomials over $\mathbb{F}_p$ of fixed degree $2e$.

For a given n the next theorem of [30] enables to determine all possible values of s such that an s-plateaued function $\mathcal{F}_{p,n}$ exits.

Theorem 2.2.6 Let $p \geq 2$, and $q_1, q_2, ..., q_k \geq 3$ be distinct primes, relatively prime to p. Suppose $n = q_1 q_2 ... q_k$, $d_i = ord_{q_i} p$, $1 \leq i \leq k$ and $ord_n p = d$. There exits an s-plateaued function $\mathcal{F}_{p,n}$ if and only if $s < n$ is of the form given in one of the following

cases (i)-(iv). For $I \subset \{1, 2, ..., k\}$, put $n_I = \prod_{i \in I} q_i$ and $d_I = lcm\{d_i : i \in I\}$. Let $M = \{I : I \subset \{1, 2, ..., k\}, I \neq 0\}$. Throughout $\epsilon = 1$ if $p = 2$ and $\epsilon \in \{0, 1\}$ if p is odd.

(i) If $v(d_1) = v(d_2) = ... = v(d_k) > 0$, then

$$s = \epsilon + \sum_{I \in M} k_I d_I,$$

with $0 \leq k_I \leq \varphi(n_I)/d_I$.

(ii) Suppose $v(d_i) > 0$ for $1 \leq i \leq k$ and $v(d_i) \neq v(d_j)$ for some $1 \leq i \neq j \leq k$. Let $M_1 = \{I \in M : |I| \geq 2, v(d_i) = v(d_j) \text{ for every } i, j \in I\} \cup \{I \in M : |I| = 1\}$ and $M_2 = M \setminus M_1$, then

$$s = \epsilon + \sum_{I \in M_1} k_I d_I + 2 \sum_{I \in M_2} k_I d_I,$$

where $0 \leq k_I \leq \varphi(n_I)/d_I$ for $I \in M_1$ and $0 \leq k_I \leq \varphi(n_I)/2d_I$ for $I \in M_2$.

(iii) If $v(d_1) = v(d_2) = ... = v(d_k) = 0$, then

$$s = \epsilon + 2 \sum_{I \in M} k_I d_I,$$

with $0 \leq k_I \leq \varphi(n_I)/2d_I$.

(iv) Suppose (after a possible change of order of $q_1, q_2, ..., q_k$) $v(d_i) > 0$ for $1 \leq i \leq k_1 < k$ and $v(d_i) = 0$ for $k_1 + 1 \leq i \leq k$. Let $\bar{M} = \{I : I \subset \{1, 2, ...k_1\}, I \neq 0\}$, $\bar{M}_1 = \left\{I \in \bar{M} : |I| \geq 2, v(d_i) = v(d_j) \text{ for every } i, j \in I\right\} \cup \left\{I \in \bar{M} : |I| = 1\right\}$ and $\bar{M}_2 = M \setminus \bar{M}_1$, then

$$s = \epsilon + \sum_{I \in \bar{M}_1} k_I d_I + 2 \sum_{I \in \bar{M}_2} k_I d_I$$

where $0 \leq k_I \leq \varphi(n_I)/d_I$ for $I \in \bar{M}_1$ and $0 \leq k_I \leq \varphi(n_I)/2d_I$ for $\in \bar{M}_2$.

Proof: If $v(d_1) = v(d_2) = ... = v(d_k) > 0$, all the irreducible factors of $\Psi_n(x)$ are self-reciprocal and hence any divisor of $\Psi_n(x)$ is self-reciprocal. On the other hand if If $v(d_1) = v(d_2) = ... = v(d_k) = 0$, then none of the irreducible factors of $\Psi_n(x)$ are self-reciprocal, therefore together with their reciprocals they give rise to self-reciprocal divisors of $\Psi_{n_I}(x)$, $I \in M$. Hence one obtains $\varphi(n_I)/2d_I$ self-reciprocal factors of $\Psi_{n_I}(x)$, each of degree $2d_I$, for any $I \in M$. In the other two cases one needs to consider appropriate subsets of M_1 and $\bar{M}_1$ of M, where irreducible factors of $\Psi_{n_I}(x)$ are self-reciprocal for each $I \in M_1$ and $I \in \bar{M}_1$. Again for $I \in M_2$ and $I \in \bar{M}_2$, none of the

irreducible factors of $\Psi_{n_I}(x)$ are self-reciprocal hence the corresponding degrees must be multiplied by two, and the ranges of k_I must be restricted to $0 \leq k_I \leq \varphi(n_I)/2d_I$.

Corollary 2.2.7 Let $p = 2$, n be an odd prime with $ord_n 2 = d$.

1. If d is even, then there exits an s-plateaued quadratic function $\mathcal{F}_{2,n}$ if and only if $s = kd + 1$ for some $0 \leq k \leq [(n-1)/d] - 1$.

2. If d is odd, then there exits an s-plateaued quadratic function $\mathcal{F}_{2,n}$ if and only if $s = 2kd + 1$ for some $0 \leq k \leq [(n-1)/(2d)] - 1$.

2.3 Construction

The following two theorems describe the construction of s-plateaued quadratic functions for the cases $p = 2$ and $p \geq 3$ respectively.

Theorem 2.3.1 [30] Let $p = 2$, n arbitrary, and $s \leq n - 2$ be an integer, known to give rise to an s-plateaued function $\mathcal{F}_{2,n}$. Suppose $h_1 = x + 1, h_2, ..., h_k \in \mathbb{F}_2[x]$ are self-reciprocal factors of $x^n + 1$, with $\deg(h_1) + \deg(h_2) + ... + \deg(h_k) = s$. Put $h(x) = h_1 h_2 ... h_k$. If $s = n - 2$ let $l(x) = 1$. If $s \leq n - 4$ let $l(x) \in \mathbb{F}_2[x]$ be a self-reciprocal polynomial of even degree satisfying $\gcd(l(x), x^n + 1/h(x)) = 1$, and $\deg(h(x)l(x)) \leq n - 2$. For $g(x) = h(x)l(x)$, and $i_o = (n - \deg(g(x)))/2$, let $A(x) = x^{i_o} g(x) = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^i + a_i x^{n-i} \in \mathbb{F}_2[x]$. Then

$$\mathcal{F}_{2,n}(x) = Tr_n \left(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1} \right)$$

is s-plateaued, where a_0 can be chosen to be 0 or 1.

Proof: By Theorem 2.2.1, the polynomial $x + 1$ must divide $h(x)$. Hence $h_1 = x + 1$. Since s, n must be of the same parity when $p = 2$, and $\deg(l(x))$ is even, we have $2|(n - \deg(g(x)))$, and $i_o \geq 1$. This implies $A(0) = 0$. Recall that we can choose a_0 to be 0 or 1, see equation 2.4. □

Theorem 2.3.2 [30] Let $p \geq 3$, n be odd, relatively prime to p, and $s < n$ be an integer, known to give rise to an s-plateaued function $\mathcal{F}_{p,n}$. Suppose $h_1, h_2, ..., h_k \in \mathbb{F}_p[x]$ are self-reciprocal factors of $x^n - 1$, with $\deg(h_1) + \deg(h_2) + ... + \deg(h_k) = s$. Put $h(x) = h_1 h_2 ... h_k$, and let $l(x) \in \mathbb{F}_p[x]$ be a self-reciprocal poynomial, satisfying

$\gcd(l(x), \Psi_n(x)/h(x)) = 1$, and $\deg(h(x)l(x)) \leq n$ and $2|(n - \deg(h(x)l(x)))$. For $g(x) = h(x)l(x)$, and $i_o = (n - \deg(g(x)))/2$, let $A(x) = x^{i_o}g(x) = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^i + a_i x^{n-i} \in \mathbb{F}_p[x]$. Then

$$\mathcal{F}_{p,n}(x) = Tr_n \left(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^{p^i+1} \right)$$

is s-plateaued.

Proof: In case $p \geq 3$, and n is odd, $\deg(h(x)) = s$ must be even. Hence $l(x)$ needs to be a self-reciprocal polynomial of odd degree, i.e., $x + 1$ must divide $l(x)$ in order that the integer i_o is well-defined. We note that $x+1$ does not divide $x^n - 1$, therefore a polynomial $l(x)$ satisfying the conditions of the theorem exits. Then $A(x)$ is of the required form giving rise to an s-plateaued function $\mathcal{F}_{p,n}$. □

Example 2.3.1 Let $p = 2$ and $n = 21$. $x^{21} + 1 = (x + 1)Q_{21}Q_7Q_3$

$$x^{21}+1 = (x+1)(x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1)(x^6+x^5+x^4+x^3+x^2+1)(x^2+x+1)$$

$$x^{21}+1 = (x+1)(x^6+x^5+x^4+x^2+1)(x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+1)(x^2+x+1)$$

Pick the self-reciprocal polynomials $h_1 = (x + 1)$, $h_2 = (x^2 + x + 1)$ and get $h(x) = h_1(x)h_2(x) = x^3 + 1$ of degree $3 \leq n - 4(= 17)$.
For $l(x)$, i.e., a self-reciprocal polynomial of even degree satisfying

$$\gcd(l(x), x^n + 1/h(x)) = 1, \text{ and } \deg(h(x)l(x)) \leq n - 2,$$

choose $l(x) = x^6 + x^5 + x + 1$ to obtain

$$g(x) = h(x)l(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1.$$

Then $i_0 = 6$ and $A(x) = x^{i_0}g(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6$, and therefore $Tr_{21}\left(x^{2^6+1} + x^{2^7+1} + x^{2^9+1} + x^{2^{10}+1}\right)$ is 3-plateaued.

We end this chapter by pointing out a connection between the integer s and the linear complexity of an n-periodic sequence, which was observed in Section 1.4. We recall that the *linear complexity* $L(S)$ of an n-periodic sequence $S = (s_0, s_1, ..., s_{n-1})^\infty$ over $\mathbb{F}_p$ is given by

$$L(S) = n - \deg(\gcd(S_n(x), x^n - 1)),$$

where $S_n(x) = s_0 + s_1x + ... + s_{n-1}x^{n-1}$ is the generating polynomial of the sequence S.

Lemma 2.3.3 Let $f(x) = Tr_n\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right)$, $a_i \in \mathbb{F}_p$, and let $A(x)$ be the corresponding associate $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i})$. Then f is s-plateaued with $s = n - L$, where L is the linear complexity of the n-periodic sequence over $\mathbb{F}_p$ with generating polynomial

$$\bar{A(x)} = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0. \tag{2.6}$$

Proof: Since $s = \gcd(A(x), x^n - 1) = \gcd(A(x) \bmod (x^n - 1), x^n - 1)$ and

$$A(x) = a_0(x^n - 1) + \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0 = a_0(x^n - 1) + \bar{A(x)},$$

we have $s = gcd(\bar{A(x)}, x^n - 1)$. Since $\deg(\bar{A(x)}) \leq n - 1$, the polynomial $\bar{A(x)}$ can be seen as the generating polynomial of an n-periodic sequence over $\mathbb{F}_p$, and the assertion follows from Equation 1.12. □

CHAPTER 3

EXPECTED VALUE

This chapter contains the main results of this thesis. Recall that for every quadratic function $\mathcal{F}_{p,n} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we have $|\widehat{f}(y)| \in \{0, p^{\frac{n+s}{2}}\}$ for some integer $0 \leq s < n$ depending on $\mathcal{F}_{p,n}$. By using various methods we determine the expected value $E(s)$ for the parameter s and for several classes of integers n. In Section 3.2 we present $E(s)$ for the case $n = p^m$, $m \geq 1$, where the values of $\mathcal{N}_n(s)$ are known explicitly. In Section 3.3 we employ DFT to determine $E(s)$ for the case $\gcd(n, p) = 1$. With a number theoretical method, in Section 3.4 we obtain $E(s)$ for the case $p = 2$ where $n = 2m$ and m is odd. Note that this case is particularly important for applications. Our exact formulas confirm that on average the value for s is small. For the case $p = 2$ this corresponds to a high average nonlinearity.

3.1 Results on $\mathcal{N}_{\mathbf{n}}(\mathbf{s})$

Throughout this chapter we denote the number of s-plateaued quadratic functions $\mathcal{F}_{p,n}$ by $\mathcal{N}_n(s)$. Suppose that $\gcd(n, p) = 1$, and α is a primitive nth root of unity in an extension field of $\mathbb{F}_p$. First we recall the *Blahut's Theorem* which states that the linear complexity of an n-periodic sequence S can be obtained as the Hamming weight of the DFT of S, see Section 1.4. Our aim is to use DFT to analyse the Walsh transform of quadratic functions (1.10). Now we recall Lemma 2.3.3 that described the relation between the value for s and DFT of an n-tuple obtained from the coefficients of (1.10). Hence we are interested in the nature of the DFT of coefficient vectors of polynomials $\bar{A}(x) \in \mathbb{F}_p[x]$ that are as in (2.6), i.e. of the DFT of n-tuples over $\mathbb{F}_p$ of the form

$$\mathbf{a} = \begin{cases} (2a_0, a_1, \ldots, a_{(n-1)/2}, a_{(n-1)/2}, \ldots, a_1) & : \quad n \text{ odd} \\ (2a_0, a_1, \ldots, a_{n/2-1}, 2a_{n/2}, a_{n/2-1}, \ldots, a_1) & : \quad n \text{ even.} \end{cases} \tag{3.1}$$

The following lemma in [31] completely describes the nature of the DFT of n-tuples of the form (3.1).

Lemma 3.1.1 Let $\gcd(p,n) = 1$ and $\bar{A}(x)$ be as in (2.6). Consider the cyclotomic coset C_j of j modulo n for $0 \leq j \leq n-1$. Suppose that $0 \leq k \leq n-1$ is an element of C_j, i.e., $k \equiv jp^r \bmod n$ for some $r \geq 0$. Then

(i) $\bar{A}(\alpha^k) = \bar{A}(\alpha^j)^{p^r}$,

(ii) $\bar{A}(\alpha^{-j}) = \bar{A}(\alpha^j)$,

(iii) $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j}}$, where $l_j = |C_j|$. If $j \notin \{0, n/2\}$ and $-j \in C_j$, then $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j/2}}$.

(iv) $\bar{A}(1) = 0$, if $p = 2$.

Proof: If $|C_j| = l_j$, and hence $jp^{l_j} = j \bmod n$, for every polynomial $\bar{A}(x) \in \mathbb{F}_p[x]$ and a primitive nth root of unity α we have,

$$(\bar{A}(\alpha^j))^{p^{l_j}} = \bar{A}(\alpha^{jp^{l_j}}) = \bar{A}(\alpha^j).$$

Consequently, $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j}}$. Furthermore, when $k \equiv jp^r \bmod n$, we get

$$\bar{A}(\alpha^k) = \bar{A}(\alpha^{jp^r}) = (\bar{A}(\alpha^j))^{p^r}.$$

Thus (i) and the first part of (iii) are proved. When $\bar{A}(x)$ is of the form (2.6), we have

$$\begin{aligned} \bar{A}(\alpha^j) &= 2a_0 + \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(\alpha^{ji} + \alpha^{j(n-i)}) \\ &= 2a_0 + \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(\alpha^{-j(n-i)} + \alpha^{-ji}) = \bar{A}(\alpha^{-j}), \end{aligned} \tag{3.2}$$

which shows (ii). If $j \notin \{0, n/2\}$, where $j = n/2$ only occurs when n is even and hence $p \neq 2$, then $-j \in C_j$ implies that l_j is even and $-j \equiv jp^{l_j/2} \bmod n$. By (3.2) we obtain

$$\bar{A}(\alpha^j)^{p^{l_j/2}} = \bar{A}(\alpha^{jp^{l_j/2}}) = \bar{A}(\alpha^{-j}) = \bar{A}(\alpha^j).$$

Therefore $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j/2}}$. Part (iv) is trivial.

In accordance with the terminology in [31], we call n-tuples over $\mathbb{F}_p(\alpha)$ that satisfy the properties described in Lemma 3.1.1 as n-tuples in *sfdt-form* (or a *symmetric frequency domain tuple*). Lemma 3.1.1 enables the following characterization of n-tuples in sfdt-form:

- Suppose $1 \leq j \leq n-1$, $j \neq n/2$ is an integer such that the cyclotomic coset C_j containing j also contains $-j$ modulo n. Then $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{|C_j|/2}}$ determines $\bar{A}(\alpha^d)$ for all $d \in C_j$; $\bar{A}(1) \in \mathbb{F}_p$; $\bar{A}(\alpha^{n/2}) = \bar{A}(-1) \in \mathbb{F}_p$ if n is even.

- Suppose $1 \leq j \leq n-1$ is an integer such that the cyclotomic coset C_j containing j does not contain $-j$ modulo n. Then $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{|C_j|}}$ determines $\bar{A}(\alpha^d)$ for all $d \in C_j \cup C_{-j}$.

Example 3.1.1 $p = 2$, $n = 3.5^2$

The cyclotomic cosets for which $C_j = C_{-j}$, i.e., the ones containing the inverses are $C_0 = \{0\}$, $C_{25} = \{25, 50\}$, $C_{15} = \{15, 30, 60, 45\}$ and
$C_3 = \{3, 6, 12, 24, 48, 21, 42, 9, 18, 36, 72, 69, 63, 51, 27, 54, 33, 66, 57, 39\}$ with cardinalities $1, 2, 4, 20$.
$C_1 = \{1, 2, 4, 8, 16, 32, 64, 53, 31, 62, 49, 23, 46, 17, 34, 68, 61, 47, 19, 38\}$ and $C_7 = C_{-1}$ have cardinalities 20 which give a possible contribution of 40 to the Hamming weight. Similarly $C_5 = \{5, 10, 20, 40\}$ and $C_{35} = C_{-5}$ have cardinalities 4, which give a possible contribution of 8 to the Hamming weight. These numbers coincide with degrees of the prime-self reciprocal factors of $x^{75} + 1$, see Example 2.1.1.

The following theorem plays a key role in the enumeration of s-plateaued quadratic functions (1.10) for prescribed s, by using discrete Fourier transform.

Theorem 3.1.2 [31, Theorem 3] There is a one to one correspondence between n-tuples over $\mathbb{F}_p$ of the form (3.1) and n-tuples $\mathcal{A}$ over $\mathbb{F}_p(\alpha)$ in sfdt-form.

Proof: Let $C_{j_1} = C_0 = \{0\}, C_{j_2}, \ldots, C_{j_h}$ be the distinct cyclotomic cosets modulo n relative to powers of p satisfying $C_k = C_{-k}$. Note that if n is even and hence p is odd, then $C_{n/2} = \{n/2\}$ is among them. Furthermore let $C_{j_{h+1}}, C_{-j_{h+1}}, \ldots, C_{j_{h+m}}, C_{-j_{h+m}}$ be the remaining $2m$ distinct cyclotomic cosets. Denote by l_i the cardinality of the cyclotomic coset C_{j_i}, $1 \leq i \leq h+m$. By Lemma 3.1.1, an n-tuple in sfdt-form is determined by $h+m$ entries as follows. The entries corresponding to C_{j_i}, $i = 1, \ldots, h$ are the elements of the field $\mathbb{F}_{p^{l_i/2}}$, except for the coset $C_0 = \{0\} = C_{j_1}$ and also $C_{n/2}$ if n is even. The entries corresponding to C_{j_i}, $i = h+1, \ldots, h+m$, are the elements of $\mathbb{F}_{p^{l_i}}$. First we consider the case that $p \geq 3$ and n is odd. Then by simple counting

arguments, the number Ω of n-tuples in sfdt-form is given by

$$\begin{aligned}\Omega &= pp^{l_2/2}\cdots p^{l_h/2}\cdot p^{l_{h+1}}\cdots p^{l_{h+m}}\\ &= pp^{\frac{1}{2}(l_2+\cdots+l_h+2l_{h+1}+2l_{h+m})} = pp^{(n-1)/2} = p^{(n+1)/2}.\end{aligned}$$

The number Ω agrees with the number of all n-tuples over $\mathbb{F}_p$ of the form (3.1) when n is odd. The same holds for the case $p = 2$ and odd n, where $\Omega = 2^{(n-1)/2}$, and the case $p \geq 3$ and even n, where $\Omega = p^{(n/2)+1}$. Since the DFT is invertible, we obtain a bijection from the set of n-tuples of the form (3.1) onto the set of n-tuples in sfdt-form. As a consequence of Theorem 3.1.2, we can count s-plateaued functions $\mathcal{F}_{p,n}$, by counting n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form with Hamming weight $n-s$. Applying this method, in Corollaries 3–6 in [31], explicit formulas for the counting function $\mathcal{N}_n(s)$ have been presented when the factorization of x^n-1 in $\mathbb{F}_p[x]$ is particularly simple. The following cases are covered :

- $n = q$, where q a prime different from p,

- $n = q^k$, where $q \neq p$ is a prime such that p is a primitive root modulo q^2,

and for $p = 2$,

- $n = 2^m - 1$, where m is an odd prime,

- $n = 3q$, where q is a prime and the order of 2 modulo q is odd.

In particular the number $\mathcal{N}_n(0)$ of bent functions has been determined for all $p \geq 3$ and n with $\gcd(n, p) = 1$. For $p = 2$ the number $\mathcal{N}_n(1)$ of semi-bent functions has been given for all odd integers n, see [31, Corollary 7].

To describe the counting function $\mathcal{N}_n(s)$ for $\gcd(n, p) = 1$, the univariate polynomial $\mathcal{G}_n(z)$ in the variable z is considered. $\mathcal{G}_n(z)$ is defined by

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

and is called the *generating polynomial* for $\mathcal{N}_n(s)$. The generating polynomial has been determined as a product of polynomials for odd n with $\gcd(n, p) = 1$ in [31], and for even n relatively prime to p in [6]. We restate those results in the following theorem.

Theorem 3.1.3 [6, 31]

(i) Let $p = 2$, n be odd, and $x^n + 1 = (x + 1)r_1 \cdots r_k$ be the factorization of $x^n + 1$ into prime self-reciprocal polynomials over $\mathbb{F}_2$. Then $\mathcal{G}_n(z)$ is given by

$$\mathcal{G}_n(z) = \prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1)z^{\deg(r_j)}\right].$$

(ii) Let $p \geq 3$, $\gcd(n, p) = 1$. Suppose the polynomial $x^n - 1$ is factorized as $x^n - 1 = (x - 1)r_1 \cdots r_k$ or $x^n - 1 = (x - 1)(x + 1)r_1 \cdots r_k$ for odd or even n respectively, where $r_1, \ldots, r_k$ are self-reciprocal polynomials of degree ≥ 2. Then $\mathcal{G}_n(z)$ is given by

$$\mathcal{G}_n(z) = (1 + (p - 1)z)^{\delta} \prod_{j=1}^{k} \left[1 + (p^{\frac{\deg(r_j)}{2}} - 1)z^{\deg(r_j)}\right].$$

Here $\delta = 1$ if n is odd, and $\delta = 2$ if n is even.

Proof: We show that the coefficient of z^t in $\mathcal{G}_n(z)$ is $\mathcal{N}_n(n - t)$. Note that $\mathcal{N}_n(n - t)$ is the number of n-tuples $(\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$ in sfdt-form with Hamming weight t.
If $p = 2$, then the Hamming weight of an n-tuple in sfdt-form is given as $\sum_{i \in I} \deg(r_j)$ for a subset I of $\{1, \ldots, k\}$. Let $\Omega(t)$ be the set of subsets I of $\{1, \ldots, k\}$ for which $\sum_{j \in I} \deg(r_j) = t$. Since the entry in an n-tuple in sfdt-form which corresponds to a self-reciprocal factor of $x^n + 1$ of degree $\deg(r_j) > 1$ is an element of $\mathbb{F}_{2^{\deg(r_j)/2}}$, for an (even) integer t, the number of n-tuples in sfdt-form with Hamming weight t is determined by

$$\sum_{I \in \Omega(t)} \prod_{j \in I} (2^{\frac{\deg(r_j)}{2}} - 1).$$

This coincides with the coefficient of z^t in the polynomial

$$\prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1)z^{\deg(r_j)}\right].$$

If p is odd, then the Hamming weight of an n-tuple in sfdt-form is $\delta_0 + \sum_{i \in I} \deg(r_j)$ if n is odd, and $\delta_0 + \delta_{n/2} + \sum_{i \in I} \deg(r_j)$ if n is even, for a subset I of $\{1, \ldots, k\}$. Here $\delta_0 = 0$ ($\delta_{n/2} = 0$) if and only if $\mathcal{S}_0$ ($\mathcal{S}_{n/2}$), belonging to $\mathbb{F}_p$, is 0. Therefore we have to multiply the polynomial

$$\prod_{j=1}^{k} \left[1 + (p^{\frac{\deg(r_j)}{2}} - 1)z^{\deg(r_j)}\right]$$

with $(1+(p-1)z)$ when n is odd and with $(1+(p-1)z)^2$ when n is even. $\square$

We should point out that in these calculations we take $a_0 = 0$ in (1.10) when $p = 2$, unlike in [31], where a_0 is not necessarily zero. As a consequence, the formulas in [31] contain an additional factor 2 for $p = 2$.

The method of the DFT is not applicable if $\gcd(n, p) \neq 1$. For this purpose, in [31, Section V], a number theoretical method has been introduced and the generating polynomial $\mathcal{G}_n(z)$ for the important case $p = 2$ has been presented for $n = 2m$ and odd m. We state this result below. The tools used to obtain it will be described in Section 3.4 where we determine the expected value for the parameter s.

Theorem 3.1.4 [31, Theorem 5] Let $p = 2$, $n = 2m$, m be odd, and $x^n + 1 = (x+1)^2 r_1^2 \cdots r_k^2$ be the canonical factorization of $x^n + 1$ into prime self-reciprocal polynomials. Then the generating polynomial $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t$ is given by

$$\mathcal{G}_n(z) = \prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} + (2^{\deg(r_j)} - 2^{\frac{\deg(r_j)}{2}}) z^{2\deg(r_j)} \right].$$

3.2 The case $\mathbf{n = p^m}$

In [30], $\mathcal{N}_n(s)$ has been determined for $p = 2$ and $n = 2^m$, $m \geq 1$, by using the Games-Chan algorithm [17], which was designed to determine the linear complexity of binary 2^m-periodic sequences. With a direct calculation, the analog result for odd p and $n = p^m$, $m \geq 1$, has been obtained in [31]. We recall these results in the following propositions.

Proposition 3.2.1 [30, Theorem 2] Let $p = 2$ and $n = 2^m$. Then

$$\mathcal{N}_n(s) = \begin{cases} 2^{2^{m-1}-1-k} & : \quad s = 2k, k = 1, \ldots, 2^{m-1} - 1, \\ 1 & : \quad s = 2^m, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

Proposition 3.2.2 [31, Theorem 1] Let $p \geq 3$ and $n = p^m$. Then

$$\mathcal{N}_n(s) = \begin{cases} (p-1)p^{\frac{p^m-s-1}{2}} & : \quad s \text{ even}, \ 0 \leq s \leq p^m - 1, \\ 1 & : \quad s = p^m, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

We can use Proposition 3.2.1 and Proposition 3.2.2 to evaluate $E(s)$ for $n = p^m$.

Theorem 3.2.1 Let $p = 2$. If $n = 2^m$, then the expected value $E(s)$ of the parameter s for a quadratic function as in (1.11) is

$$E(s) = 4 - \frac{1}{2^{2^{m-1}-2}}.$$

Proof: By Proposition 3.2.1 and the observation that the total number of Boolean quadratic functions (1.10) is $2^{(n/2)-1}$, we obtain that

$$E(s) = \frac{1}{2^{\frac{n}{2}-1}} \left(\sum_{k=1}^{2^{m-1}-1} 2^{2^{m-1}-1-k} 2k + 2^m \right) = \frac{1}{2^{2^{m-1}-1}} \left(2^{2^{m-1}} \sum_{k=1}^{2^{m-1}-1} \frac{k}{2^k} + 2^m \right).$$

Look at the sum $\sum_{k=1}^{a} \frac{k}{2^k}$ up to a:

$$\begin{aligned}
\sum_{k=1}^{a} \frac{k}{2^k} &= \frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \frac{4}{16} + \ldots + \frac{a}{2^a} \\
&= \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \left(\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16}\right) \\
&\quad + \ldots + \overbrace{\left(\frac{1}{2^a} + \frac{1}{2^a} + \ldots + \frac{1}{2^a}\right)}^{a \text{ times}} \\
&= \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^a}\right) + \left(\frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^a}\right) + \left(\frac{1}{8} + \frac{1}{16} + \ldots + \frac{1}{2^a}\right) \\
&\quad + \ldots + \frac{1}{2^a}
\end{aligned}$$

Take $a = 5$, check the sum,

$$\begin{aligned}
\sum_{k=1}^{5} \frac{k}{2^k} &= \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \left(\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16}\right) \\
&\quad \left(\frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32}\right) \\
&= \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32}\right) + \left(\frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32}\right) + \left(\frac{1}{8} + \frac{1}{16} + \frac{1}{32}\right) \\
&\quad + \left(\frac{1}{16} + \frac{1}{32}\right) + \frac{1}{32} \\
&= \frac{31}{32} + \frac{15}{32} + \frac{7}{32} + \frac{3}{32} + \frac{1}{32} \\
&= \frac{2^5 - 1}{32} + \frac{2^4 - 1}{32} + \frac{2^3 - 1}{32} + \frac{2^2 - 1}{32} + \frac{2^1 - 1}{32} \\
&= \frac{(2^5 + 2^4 + 2^3 + 2^2 + 2) - 5}{2^5} \\
&= \frac{2\left(2^5 - 1\right) - 5}{2^5} \\
&= \frac{2^{5+1} - 2 - 5}{2^a}
\end{aligned}$$

By induction on a we get

$$\sum_{k=1}^{a} \frac{k}{2^k} = \frac{2^{a+1} - 2 - a}{2^a}$$

So we obtain

$$\begin{aligned} E(s) &= \frac{1}{2^{2^{m-1}-1}} \left(2^{2^{m-1}} \frac{2^{2^{m-1}} - 2 - (2^{m-1} - 1)}{2^{2^{m-1}-1}} + 2^m \right) \\ &= \frac{1}{2^{2^{m-1}-1}} \left(2^{2^{m-1}+1} - 2 \cdot 2 - 2(2^{m-1} - 1) + 2^m \right) \\ &= \frac{1}{2^{2^{m-1}-1}} \left(2^{2^{m-1}+1} - 2 \right) = 4 - \frac{1}{2^{2^{m-1}-2}}. \end{aligned}$$

□

By Equation 1.7, the nonlinearity of a Boolean function can be determined from its Walsh spectrum. Hence Theorem 3.2.1 also points towards a high average nonlinearity.

Theorem 3.2.2 Let p be an odd prime and $n = p^m$. Then the expected value $E(s)$ of the parameter s for a quadratic function (1.10) is given by

$$E(s) = \frac{2}{p-1} - \frac{1}{p^{\frac{n+1}{2}}} \frac{p+1}{p-1}.$$

Proof: By Proposition 3.2.2 we have

$$\begin{aligned} E(s) &= \frac{1}{p^{\frac{n+1}{2}}} \left(\sum_{k=0}^{\frac{p^m-1}{2}} (p-1) p^{\frac{p^m-2k-1}{2}} 2k + p^m \right) \\ &= \frac{2(p-1)}{p} \sum_{k=0}^{\frac{p^m-1}{2}} \frac{k}{p^k} + \frac{p^m}{p^{\frac{n+1}{2}}}. \end{aligned}$$

Set it up to a:

$$\begin{aligned} \sum_{k=1}^{a} \frac{k}{p^k} &= \frac{1}{p} + \frac{2}{p^2} + \frac{3}{p^3} + \frac{4}{p^4} + \ldots + \frac{a}{p^a} \\ &= \frac{1}{p} + \left(\frac{1}{p^2} + \frac{1}{p^2} \right) + \left(\frac{1}{p^3} + \frac{1}{p^3} + \frac{1}{3} \right) + \ldots + \overbrace{\left(\frac{1}{p^a} + \frac{1}{p^a} + \ldots + \frac{1}{p^a} \right)}^{a \text{ times}} \\ &= \left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots + \frac{1}{p^a} \right) + \left(\frac{1}{p^2} + \frac{1}{p^3} + \ldots + \frac{1}{p^a} \right) \\ &\quad + \left(\frac{1}{p^3} + \frac{1}{p^4} + \ldots + \frac{1}{p^a} \right) + \ldots + \frac{1}{p^a} \end{aligned}$$

Take $a = 5$, check the sum,

$$\begin{aligned}
\sum_{k=1}^{5} \frac{k}{p^k} &= \frac{1}{p} + \left(\frac{1}{p^2} + \frac{1}{p^2}\right) + \left(\frac{1}{p^3} + \frac{1}{p^3} + \frac{1}{p^3}\right) + \left(\frac{1}{p^4} + \frac{1}{p^4} + \frac{1}{p^4} + \frac{1}{p^4}\right) \\
&\quad + \left(\frac{1}{p^5} + \frac{1}{p^5} + \frac{1}{p^5} + \frac{1}{p^5} + \frac{1}{p^5}\right) \\
&= \left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \frac{1}{p^5}\right) + \left(\frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \frac{1}{p^5}\right) + \left(\frac{1}{p^3} + \frac{1}{p^4} + \frac{1}{p^5}\right) \\
&\quad + \left(\frac{1}{p^4} + \frac{1}{p^5}\right) + \frac{1}{p^5} \\
&= \frac{p^4 + p^3 + p^2 + p + 1}{p^5} + \frac{p^3 + p^2 + p + 1}{p^5} + \frac{p^2 + p + 1}{p^5} + \frac{p + 1}{p^5} + \frac{1}{p^5} \\
&= \frac{\left(\frac{p^5-1}{p-1}\right) + \left(\frac{p^4-1}{p-1}\right) + \left(\frac{p^3-1}{p-1}\right) + \left(\frac{p^2-1}{p-1}\right) + \left(\frac{p-1}{p-1}\right)}{p^5} \\
&= \frac{(p^5 + p^4 + p^3 + p^2 + p) - 5}{(p-1)\,p^5} \\
&= \frac{p\,(p^5 - 1)}{(p-1)^2\,p^5} - \frac{5}{(p-1)\,p^5}
\end{aligned}$$

By induction on a we get

$$\sum_{k=1}^{a} \frac{k}{p^k} = \frac{p\,(p^a - 1)}{(p-1)^2\,p^a} - \frac{a}{(p-1)\,p^a}$$

Thus with $a = \frac{p^m-1}{2} = \frac{n-1}{2}$, we get

$$\begin{aligned}
E(s) &= \frac{2(p-1)}{p}\left(\frac{p\,(p^a - 1)}{(p-1)^2\,p^a} - \frac{a}{(p-1)\,p^a}\right) + \frac{p^m}{p^{a+1}} \\
&= \frac{2p(p^a - 1)}{(p-1)p^{a+1}} - \frac{2a}{p^{a+1}} + \frac{2a+1}{p^{a+1}} \\
&= \frac{2}{p-1} - \frac{2p}{(p-1)p^{a+1}} + \frac{1}{p^{a+1}} = \frac{2}{p-1} - \frac{1}{p^{a+1}}\frac{p+1}{p-1},
\end{aligned}$$

which completes the proof. □

3.3 The case $\gcd(\mathbf{n}, \mathbf{p}) = \mathbf{1}$

As pointed out in Section 3.1, when $\gcd(n, p) = 1$, then the number $\mathcal{N}_n(s)$ of s-plateaued quadratic functions (1.10) is the number of n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form with Hamming weight $n - s$. Hence the expected value for s can be obtained from the expected Hamming weight of an n-tuple in sfdt-form. Since the nature of the n-tuples in sfdt-form depends on the properties of the cyclotomic cosets modulo n, we may express the expected value $E(s)$ in terms of the cardinalities of the cyclotomic cosets modulo n relative to the powers of p.

Theorem 3.3.1 For an integer n with $\gcd(n,p) = 1$ let $C_{j_1} = \{0\}$, $C_{j_2}, \ldots, C_{j_h}$, $C_{j_{h+1}}, C_{-j_{h+1}}, \ldots, C_{j_{h+m}}, C_{-j_{h+m}}$ be the distinct cyclotomic cosets modulo n relative to powers of p with the properties that $C_{j_i} = C_{-j_i}$ for $1 \leq i \leq h$, and $C_{j_i} \neq C_{-j_i}$ for $h+1 \leq i \leq h+m$. Let l_i, $1 \leq i \leq h+m$, be the cardinality of the cyclotomic coset C_{j_i}. Then the expected value $E(s)$ is given by

$$E(s) = \begin{cases} \frac{1}{p} + \sum_{i=2}^{h} \frac{l_i}{p^{\frac{l_i}{2}}} + \sum_{i=h+1}^{h+m} \frac{2l_i}{p^{l_i}} & : \text{ if } p \geq 3 \text{ and } n \text{ is odd,} \\ 1 + \sum_{i=2}^{h} \frac{l_i}{2^{\frac{l_i}{2}}} + \sum_{i=h+1}^{h+m} \frac{2l_i}{2^{l_i}} & : \text{ if } p = 2 \text{ hence } n \text{ is odd,} \\ \frac{2}{p} + \sum_{i=3}^{h} \frac{l_i}{p^{\frac{l_i}{2}}} + \sum_{i=h+1}^{h+m} \frac{2l_i}{p^{l_i}} & : \text{ if } p \geq 3 \text{ and } n \text{ is even, where} \\ & \quad C_{j_2} = \{n/2\}. \end{cases}$$

Proof: We recall from Section 3.1 that an n-tuple in sfdt-form is completely described by $h+m$ elements $k_1, \ldots, k_h, k_{h+1}, \ldots, k_{h+m}$, where the element k_i is from $\mathbb{F}_{p^{l_i/2}}$ for $1 \leq i \leq h$ and $l_i > 1$, and the element k_i is from $\mathbb{F}_{p^{l_i}}$ for $h+1 \leq i \leq h+m$. For the cyclotomic cosets C_{j_i}, $1 \leq i \leq h$, which contain only one element, we can distinguish 3 cases: If n is odd then only $C_{j_1} = \{0\}$ contains a single element; if $p = 2$ then the corresponding entry k_1 in the n-tuple in sfdt-form is 0, if p is odd then $k_1 \in \mathbb{F}_p$; if n is even and (hence p is odd) then there are two such cyclotomic cosets, $C_{j_1} = \{0\}$ and $C_{j_2} = \{n/2\}$. In both cases the corresponding entry in the n-tuple in sfdt-form is in $\mathbb{F}_p$. We determine $n - E(s) = E(L)$, which by Lemma 2.3.3 is the expected linear complexity of an n-periodic sequence over $\mathbb{F}_p$ with period of the form (3.1). By Theorem 3.1.2, $E(L)$ equals the expected Hamming weight of an n-tuple in sfdt-form. Denoting the set of all n-tuples in sfdt-form by Υ and putting $\Omega = |\Upsilon|$ we have

$$E(L) = \frac{1}{\Omega} \left(\sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} Hw(\mathcal{A}) \right) = \frac{1}{\Omega} \left(\sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} \left(\sum_{\substack{i=1 \\ k_i \neq 0}}^{h} l_i + \sum_{\substack{i=h+1 \\ k_i \neq 0}}^{h+m} 2l_i \right) \right). \tag{3.3}$$

We first consider the case $p \geq 3$ and n is odd. For this case by Equation 3.3 we get

$$\begin{aligned} E(L) &= \frac{1}{p^{\frac{n+1}{2}}} \left(\sum_{\substack{\mathcal{A} \in \boldsymbol{\Upsilon} \\ k_1 \neq 0}} l_1 + \sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} \sum_{\substack{i=2 \\ k_i \neq 0}}^{h} l_i + \sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} \sum_{\substack{i=h+1 \\ k_i \neq 0}}^{h+m} 2l_i \right) \\ &= \frac{1}{p^{\frac{n+1}{2}}} \left(l_1 \sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} 1 + \sum_{i=2}^{h} l_i \sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} 1 + \sum_{i=h+1}^{m+1} 2l_i \sum_{\mathcal{A} \in \boldsymbol{\Upsilon}} 1 \right) \\ &= \frac{1}{p^{\frac{n+1}{2}}} \left(l_1 (p-1) p^{\frac{n+1}{2} - 1} + \sum_{i=2}^{h} l_i (p^{\frac{l_i}{2}} - 1) p^{\frac{n+1-l_i}{2}} \right) \end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{p^{\frac{n+1}{2}}}\left(\sum_{i=h+1}^{m+1} 2l_i(p^{l_i}-1)p^{\frac{n+1}{2}-l_i}\right)\\
=\;& \frac{1}{p^{\frac{n+1}{2}}}\left((p-1)p^{\frac{n+1}{2}-1}+\sum_{i=2}^{h} l_i\left(p^{\frac{n+1}{2}}-p^{\frac{n+1-l_i}{2}}\right)\right)\\
&+\frac{1}{p^{\frac{n+1}{2}}}\left(\sum_{i=h+1}^{m+1} 2l_i\left(p^{\frac{n+1}{2}}-p^{\frac{n+1}{2}-l_i}\right)\right)\\
=\;& \frac{p-1}{p}+\sum_{i=2}^{h} l_i\left(1-\frac{1}{p^{\frac{l_i}{2}}}\right)+\sum_{i=h+1}^{m+1} 2l_i\left(1-\frac{1}{p^{l_i}}\right)\\
=\;& 1-\frac{1}{p}+\sum_{i=2}^{h} l_i-\sum_{i=2}^{h}\frac{l_i}{p^{\frac{l_i}{2}}}+\sum_{i=h+1}^{m+1} 2l_i-\sum_{i=h+1}^{m+1}\frac{2l_i}{p^{l_i}}\\
=\;& \left(1+\sum_{i=2}^{h} l_i+\sum_{i=h+1}^{m+1} 2l_i\right)-\left(\frac{1}{p}+\sum_{i=2}^{h}\frac{l_i}{p^{\frac{l_i}{2}}}+\sum_{i=h+1}^{m+1}\frac{2l_i}{p^{l_i}}\right)\\
=\;& n-\left(\frac{1}{p}+\sum_{i=2}^{h}\frac{l_i}{p^{\frac{l_i}{2}}}+\sum_{i=h+1}^{m+1}\frac{2l_i}{p^{l_i}}\right)
\end{aligned}
$$

which yields the claimed formula for $E(s)$.

If $p=2$, and hence n is odd, then $\Omega = 2^{\frac{n-1}{2}}$ and $k_1 = 0$. From Equation 3.3 we get

$$
\begin{aligned}
E(L) &= \frac{1}{2^{\frac{n-1}{2}}}\left(\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}}\left(\sum_{\substack{i=2\\ k_i\neq 0}}^{h} l_i+\sum_{\substack{i=h+1\\ k_i\neq 0}}^{h+m} 2l_i\right)\right)\\
&= \frac{1}{2^{\frac{n-1}{2}}}\left(\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}}\sum_{\substack{i=2\\ k_i\neq 0}}^{h} l_i+\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}}\sum_{\substack{i=h+1\\ k_i\neq 0}}^{h+m} 2l_i\right)\\
&= \frac{1}{2^{\frac{n-1}{2}}}\left(\sum_{i=2}^{h} l_i\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1+\sum_{i=h+1}^{m+1} 2l_i\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1\right)\\
&= \frac{1}{2^{\frac{n-1}{2}}}\left(\sum_{i=2}^{h} l_i(2^{\frac{l_i}{2}}-1)2^{\frac{n-1-l_i}{2}}+\sum_{i=h+1}^{m+1} 2l_i(2^{l_i}-1)2^{\frac{n-1}{2}-l_i}\right)\\
&= \frac{1}{2^{\frac{n-1}{2}}}\left(\sum_{i=2}^{h} l_i\left(2^{\frac{n-1}{2}}-2^{\frac{n-1-l_i}{2}}\right)+\sum_{i=h+1}^{m+1} 2l_i\left(2^{\frac{n-1}{2}}-2^{\frac{n-1}{2}-l_i}\right)\right)\\
&= \sum_{i=2}^{h} l_i\left(1-\frac{1}{2^{\frac{l_i}{2}}}\right)+\sum_{i=h+1}^{m+1} 2l_i\left(1-\frac{1}{2^{l_i}}\right)\\
&= \sum_{i=2}^{h} l_i-\sum_{i=2}^{h}\frac{l_i}{2^{\frac{l_i}{2}}}+\sum_{i=h+1}^{m+1} 2l_i-\sum_{i=h+1}^{m+1}\frac{2l_i}{2^{l_i}}
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\sum_{i=2}^{h} l_i + \sum_{i=h+1}^{m+1} 2l_i\right) - \left(\sum_{i=2}^{h} \frac{l_i}{2^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{2^{l_i}}\right) \\
&= (n-1) - \left(\sum_{i=2}^{h} \frac{l_i}{2^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{2^{l_i}}\right) \\
&= n - \left(1 + \sum_{i=2}^{h} \frac{l_i}{2^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{2^{l_i}}\right)
\end{aligned}
$$

Finally we consider the case $p \geq 3$ and even n. In this case $\Omega = p^{\frac{n}{2}+1}$ and $k_1, k_2 \in \mathbb{F}_p$. Hence by Equation 3.3 we obtain

$$
\begin{aligned}
E(L) &= \frac{1}{p^{\frac{n}{2}+1}} \left(\sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} \left(\sum_{\substack{i=1 \\ k_i\neq 0}}^{h} l_i + \sum_{\substack{i=h+1 \\ k_i\neq 0}}^{h+m} 2l_i\right)\right) \\
&= \frac{1}{p^{\frac{n}{2}+1}} \left(\sum_{\substack{\mathcal{A}\in\boldsymbol{\Upsilon} \\ k_1\neq 0}} l_1 + \sum_{\substack{\mathcal{A}\in\boldsymbol{\Upsilon} \\ k_2\neq 0}} l_2 + \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} \sum_{\substack{i=3 \\ k_i\neq 0}}^{h} l_i + \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} \sum_{\substack{i=h+1 \\ k_i\neq 0}}^{h+m} 2l_i\right) \\
&= \frac{1}{p^{\frac{n}{2}+1}} \left(l_1 \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1 + l_2 \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1 + \sum_{i=3}^{h} l_i \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1 + \sum_{i=h+1}^{m+1} 2l_i \sum_{\mathcal{A}\in\boldsymbol{\Upsilon}} 1\right) \\
&= \frac{1}{p^{\frac{n}{2}+1}} \left(l_1(p-1)p^{\frac{n}{2}} + l_2(p-1)p^{\frac{n}{2}} + \sum_{i=3}^{h} l_i(p^{\frac{l_i}{2}}-1)p^{\frac{n}{2}+1-\frac{l_i}{2}}\right) \\
&\quad + \frac{1}{p^{\frac{n}{2}+1}} \left(\sum_{i=h+1}^{m+1} 2l_i(p^{l_i}-1)p^{\frac{n}{2}+1-l_i}\right) \\
&= \frac{1}{p^{\frac{n}{2}+1}} \left((p-1)p^{\frac{n}{2}} + (p-1)p^{\frac{n}{2}} + \sum_{i=3}^{h} l_i\left(p^{\frac{n}{2}+1} - p^{\frac{n}{2}+1-\frac{l_i}{2}}\right)\right) \\
&\quad + \frac{1}{p^{\frac{n}{2}+1}} \left(\sum_{i=h+1}^{m+1} 2l_i\left(p^{\frac{n}{2}+1} - p^{\frac{n}{2}+1-l_i}\right)\right) \\
&= \frac{2(p-1)}{p} + \sum_{i=3}^{h} l_i\left(1 - \frac{1}{p^{\frac{l_i}{2}}}\right) + \sum_{i=h+1}^{m+1} 2l_i\left(1 - \frac{1}{p^{l_i}}\right) \\
&= 2 - \frac{2}{p} + \sum_{i=3}^{h} l_i - \sum_{i=3}^{h} \frac{l_i}{p^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} 2l_i - \sum_{i=h+1}^{m+1} \frac{2l_i}{p^{l_i}} \\
&= \left(2 + \sum_{i=3}^{h} l_i + \sum_{i=h+1}^{m+1} 2l_i\right) - \left(\frac{2}{p} + \sum_{i=3}^{h} \frac{l_i}{p^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{p^{l_i}}\right) \\
&= n - \left(\frac{2}{p} + \sum_{i=3}^{h} \frac{l_i}{p^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{p^{l_i}}\right)
\end{aligned}
$$

For several families of integers n we are able to specify the cardinalities of the cyclotomic cosets modulo n. In the following corollaries we present simple formulas for $E(s)$ for such integers n, determined by means of Theorem 3.3.1.

Corollary 3.3.2 Let $p = 2$ and $n = 2^m - 1$ for an odd prime m. Then

$$E(s) = 2 - \frac{1}{2^{m-1}}.$$

Proof: If $p = 2$ and $n = 2^m - 1$ then the cardinality of each cyclotomic coset has to divide m, which is the order of 2 modulo n. Hence there are only cyclotomic cosets of cardinality m and 1. As it is easy to see, $C_0 = \{0\}$ is the only cyclotomic coset of cardinality 1. Hence there are $\frac{2^m-2}{m}$ cyclotomic cosets of odd cardinality m, all of which satisfy $C_j \neq C_{-j}$. By Theorem 3.3.1 we get

$$\begin{aligned} E(L) &= n - \left(1 + \sum_{i=2}^{h} \frac{l_i}{2^{\frac{l_i}{2}}} + \sum_{i=h+1}^{m+1} \frac{2l_i}{2^{l_i}}\right) \\ &= n - \left(1 + \sum_{i=1}^{\frac{2^m-2}{2m}} \frac{2m}{2^m}\right) \\ &= n - \left(1 + \frac{2^m - 2}{2^m}\right) \\ &= n - \left(2 - \frac{1}{2^{m-1}}\right) \end{aligned}$$

□

Corollary 3.3.3 Let $n = q$ be an odd prime different from p, and let d be the order of p modulo q. Then

$$E(s) = \begin{cases} \frac{1}{p} + \frac{q-1}{p^{d/2}} & : \text{ if } p \geq 3 \text{ and } d \text{ is even,} \\ 1 + \frac{q-1}{2^{d/2}} & : \text{ if } p = 2 \text{ and } d \text{ is even,} \\ \frac{1}{p} + \frac{q-1}{p^d} & : \text{ if } p \geq 3 \text{ and } d \text{ is odd,} \\ 1 + \frac{q-1}{2^d} & : \text{ if } p = 2 \text{ and } d \text{ is odd.} \end{cases}$$

Proof: Let $n = q$ be a prime different from p, $d = ord_n p$. Now all $\frac{q-1}{d}$ irreducible divisors of $\frac{x^q-1}{x-1}$ are self-reciprocal if and only if d is even. Equivalently, if d is even, then the cyclotomic cosets C_j, $j \neq 0$, which are all of size d, satisfy $C_j = C_{-j}$. If d

is odd, $\frac{x^q-1}{x-1}$ factors into $\frac{q-1}{2d}$ prime self-reciprocal polynomials all of degree $2d$ where $-j \notin C_j$, $j \neq 0$. We consider the following four cases:

Case 1: $p \geq 3$ and d is even:

$$\begin{aligned} E(L) &= n - \left(\frac{1}{p} + \sum_{i=1}^{\frac{q-1}{d}} \frac{d}{p^{d/2}} \right) \\ &= n - \left(\frac{1}{p} + \frac{q-1}{p^{d/2}} \right) \end{aligned}$$

Case 2: $p = 2$ and d is even:

$$\begin{aligned} E(L) &= n - \left(1 + \sum_{i=1}^{\frac{q-1}{d}} \frac{d}{2^{d/2}} \right) \\ &= n - \left(1 + \frac{q-1}{2^{d/2}} \right) \end{aligned}$$

Case 3: $p \geq 3$ and d is odd:

$$\begin{aligned} E(L) &= n - \left(\frac{1}{p} + \sum_{i=1}^{\frac{q-1}{2d}} \frac{2d}{p^{d}} \right) \\ &= n - \left(\frac{1}{p} + \frac{q-1}{p^{d}} \right) \end{aligned}$$

Case 4: $p = 2$ and d is odd:

$$\begin{aligned} E(L) &= n - \left(1 + \sum_{i=1}^{\frac{q-1}{2d}} \frac{2d}{2^{d}} \right) \\ &= n - \left(1 + \frac{q-1}{2^{d}} \right) \end{aligned}$$

□

Corollary 3.3.4 Let $n = q^k$, where $q \neq p$ is an odd prime such that p is a primitive root modulo q^2. Then

$$E(s) = \begin{cases} \frac{1}{p} + (q-1) \sum_{i=0}^{k-1} \frac{q^i}{p^{\frac{(q-1)q^i}{2}}} & : \text{ if } p \text{ is odd,} \\ (q-1) \sum_{i=0}^{k-1} \frac{q^i}{2^{\frac{(q-1)q^i}{2}}} & : \text{ if } p = 2. \end{cases}$$

Proof: If p is a primitive root modulo q^2, then all cyclotomic polynomials $\mathcal{Q}_{q^i}$ are irreducible and $x^{q^k}-1=\prod_{i=0}^{k}\mathcal{Q}_{q^i}$ is the canonical factorization of $x^{q^k}-1$. Clearly all $\mathcal{Q}_{q^i}$, $i>0$, are self-reciprocal. Equivalently, other than $\{0\}$, we have k cyclotomic cosets with the cardinalities $(q-1)q^{i-1}$, $1\leq i\leq k$. Each cyclotomic coset contains with j also its inverse $-j$ modulo n. By Theorem 3.3.1 we then get

$$E(s)=\frac{1}{p}+\sum_{i=0}^{k-1}\frac{(q-1)\,q^i}{p^{\frac{(q-1)q^i}{2}}}$$

when p is odd, and

$$E(s)=\sum_{i=0}^{k-1}\frac{(q-1)\,q^i}{2^{\frac{(q-1)q^i}{2}}}$$

when $p=2$. □

We remark that the results in this section confirm that the average value for s is small, which for the case that $p=2$ also points to a large average nonlinearity.

3.4 A number theoretical method

In this section we employ a number theoretical method which was introduced in [31] to determine the generating polynomial $\mathcal{G}_n$ for case $p=2$, and $n=2m$, for odd m. The method is based on a method of Fu et al. [15, 16] for analysing the linear complexity of sequences. Amongst others, in [15, 16] a generating polynomial for the distribution of the linear complexity of sequences has been presented and formulas for the expected value of the linear complexity have been established. We will further develop this method to determine the expected value $E(s)$ for $p=2$, recover $E(s)$ for odd n, and evaluate $E(s)$ for $n=2m$, m odd. Moreover we determine the variance for the parameter s.

We again follow the notation used in [31]. For a prime p let

$$R_p=\{f\in\mathbb{F}_p[x]\ :\ f \text{ is self-reciprocal}\}.$$

Then for a polynomial $f\in\mathbb{F}_p[x]$ we define

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

We next recall some properties of $\phi_p(f)$.

Lemma 3.4.1 [31, Lemma 8] Let $f \in R_p$ be a monic polynomial of positive degree. If f is not divisible by $x+1$, then

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

where the summation is over all monic divisors $d \in R_p$ of f. For $f = 1$ we have $\sum_{d|f} \phi_p(d) = 0$.

Lemma 3.4.2 [31, Lemma 9] Let $f, f_1, f_2 \in R_p$ be monic polynomials of positive degree, not divisible by $x+1$.

(i) If $f = f_1 f_2$ and $\gcd(f_1, f_2) = 1$, then

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

(ii) If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ is the canonical factorization of f into monic prime self-reciprocal polynomials, then

$$\phi_p(f) = p^{\frac{\deg(f)}{2}} \prod_{j=1}^{k} \left(1 - p^{-\frac{\deg(r_j)}{2}}\right).$$

For a self-reciprocal polynomial f that is not divisible by $x+1$ we define

$$\begin{aligned} S_1(f) &= \sum_{d|f} \phi_p(d)\deg(d), \quad \text{and} \\ S_2(f) &= \sum_{d|f} \phi_p(d)(\deg(d))^2, \end{aligned}$$

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

From now on we assume $p = 2$. Our objective is to determine the expected value $E(s)$ for quadratic functions (1.10). In the next proposition we express the expected value and the variance for the parameter s in terms of $S_1(f)$ and $S_2(f)$.

Proposition 3.4.1 (I) Let n be odd. Then the expected value $E(s)$ for the parameter s of a quadratic function (1.10) satisfies

$$E(s) = n - \frac{1}{2^{(n-1)/2}} S_1\left(\frac{x^n+1}{x+1}\right).$$

The variance for the parameter s is given by

$$Var(s) = \frac{1}{2^{(n-1)/2}} S_2\left(\frac{x^n+1}{x+1}\right) - \left(\frac{1}{2^{(n-1)/2}} S_1\left(\frac{x^n+1}{x+1}\right)\right)^2.$$

(II) Let $n = 2m$ for some odd integer m. Then the expected value $E(s)$ for the parameter s of a quadratic function (1.10) satisfies

$$E(s) = n - \frac{1}{2^{n/2-1}} S_1(\frac{x^n+1}{(x+1)^2}).$$

The variance for the parameter s is given by

$$Var(s) = \frac{1}{2^{n/2-1}} S_2(\frac{x^n+1}{(x+1)}^2) - \left(\frac{1}{2^{n/2-1}} S_1(\frac{x^n+1}{(x+1)^2})\right)^2.$$

Proof: Let $A(x)$ be the associate of the linearized polynomial corresponding to $\mathcal{F}_{2,n}$. Then $s = \deg(\gcd(x^n - 1, A(x)))$. We recall that we take the coefficient a_0 in $\mathcal{F}_{2,n}$ to be 0 when $p = 2$, and hence we have $\deg(A) < n$.

(I) If n is odd, then A is of the form

$$A(x) = x^i(x+1)f_1(x)g(x) \tag{3.4}$$

for a self-reciprocal divisor f_1 of $x^n + 1$ of (even) degree $s-1$ and a polynomial g with the following properties: $g(x)$ is a self-reciprocal polynomial of even degree smaller that $n - s$, and $\gcd(\frac{x^n+1}{(x+1)f_1(x)}, g(x)) = 1$. Hence $g \in K(d)$ for $d(x) = \frac{x^n+1}{(x+1)f_1(x)}$, which is a divisor of $(x^n + 1)/(x + 1)$ of degree $n - s$. As a consequence, denoting by $\mathcal{A}(L)$ the number of polynomials A of the form (3.4) (with $\deg(\gcd(A(x), x^n + 1)) = s$), we have for $L = n - s$,

$$\frac{1}{2^{(n-1)/2}} \sum_{s=0}^{n} \mathcal{A}(L)L = \frac{1}{2^{(n-1)/2}} \sum_{d|\frac{x^n+1}{x+1}} \phi_2(d)\deg(d).$$

The formula for the expected value follows from the definition of $S_1(f)$.

For a quadratic function f as in (1.10) let A be the associate of the linearized polynomial corresponding to f, and let $L(f)$ be the linear complexity of the sequence with generating polynomial A. Then with $s = n - L$ we get

$$\begin{aligned} Var(s) &= Var(L) = \frac{1}{2^{(n-1)/2}} \sum_{f\in\mathcal{F}} L(f)^2 - (E(L))^2 \\ &= \frac{1}{2^{(n-1)/2}} \sum_{d|\frac{x^n+1}{x+1}} \phi_2(d)(\deg(d))^2 - \left(\frac{1}{2^{(n-1)/2}} S_1(\frac{x^n+1}{x+1})\right)^2, \end{aligned}$$

which completes the proof for (I).

(II) If $n = 2m$, and m is odd, then $A(x)$ must satisfy $\gcd(A(x), x^n - 1) = (x+1)^2 f_1(x)$, since n and s must be of the same parity. Hence A is of the form

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

for a self-reciprocal divisor f_1 of x^n+1 of (even) degree $s-2$ and a polynomial g with the following properties: $g(x)$ is a self-reciprocal polynomial of even degree smaller that $n-s$, and $\gcd(\frac{x^n+1}{(x+1)^2 f_1(x)}, g(x)) = 1$. Hence $g \in K(d)$ for $d(x) = \frac{x^n+1}{(x+1)^2 f_1(x)}$, which is a divisor of $(x^n+1)/(x+1)^2$ of degree $n-s$. By the same reasoning as in (I) we get the formulas for (II). □

In the following lemmas we present a useful property of the functions $S_1(f)$ and $S_2(f)$.

Lemma 3.4.3 Let f_1, f_2 be self-reciprocal polynomials not divisible by $x+1$ with $\gcd(f_1, f_2) = 1$. Then

$$\frac{1}{2^{\deg(f_1 f_2)/2}} S_1(f_1 f_2) = \frac{1}{2^{\deg(f_1)/2}} S_1(f_1) + \frac{1}{2^{\deg(f_2)/2}} S_1(f_2).$$

Proof:

$$\begin{aligned}
S_1(f_1 f_2) &= \sum_{d | f_1 f_2} \phi_2(d) \deg(d) \\
&= \sum_{d_1 | f_1} \sum_{d_2 | f_2} \phi_2(d_1 d_2)[\deg(d_1) + \deg(d_2)] \\
&\quad + \sum_{d_2 | f_2} \phi_2(d_2) \deg(d_2) + \sum_{d_1 | f_1} \phi_2(d_1) \deg(d_1) \\
&= \sum_{d_1 | f_1} \sum_{d_2 | f_2} \phi(d_1) \phi_2(d_2) \deg(d_1) \\
&\quad + \sum_{d_1 | f_1} \sum_{d_2 | f_2} \phi_2(d_1) \phi_2(d_2) \deg(d_2) + S_1(f_2) + S_1(f_1) \\
&= (\sum_{d_2 | f_2} \phi_2(d_2) + 1) S_1(f_1) + (\sum_{d_1 | f_1} \phi_2(d_1) + 1) S_1(f_2),
\end{aligned}$$

where the summation is over all monic, self-reciprocal divisors of f_1, f_2 and $f_1 f_2$, respectively. By Lemma 3.4.1 we obtain

$$\begin{aligned}
\frac{1}{2^{\deg(f_1 f_2)/2}} S_1(f_1 f_2) &= \frac{1}{2^{\deg(f_1 f_2)/2}} [2^{\deg(f_2)/2} S_1(f_1) + 2^{\deg(f_1)/2} S_1(f_2)] \\
&= \frac{1}{2^{\deg(f_1)/2}} S_1(f_1) + \frac{1}{2^{\deg(f_2)/2}} S_1(f_2).
\end{aligned}$$

□

Lemma 3.4.4 Let f_1, f_2 be self-reciprocal polynomials not divisible by $x+1$ with $\gcd(f_1, f_2) = 1$. Then

$$S_2(f_1 f_2) = S_2(f_1) 2^{\frac{\deg(f_2)}{2}} + S_2(f_2) 2^{\frac{\deg(f_1)}{2}} + 2 S_1(f_1) S_1(f_2).$$

Proof: Again, with the summation over all monic, self-reciprocal divisors of f_1, f_2 and $f_1 f_2$, respectively, we have

$$\begin{aligned}
S_2(f_1 f_2) &= \sum_{d|f_1 f_2} \phi_2(d)\ (\deg(d))^2 \\
&= \sum_{d_1|f_1} \sum_{d_2|f_2} \phi_2(d_1 d_2)[\deg(d_1) + \deg(d_2)]^2 \\
&\quad + \sum_{d_2|f_2} \phi_2(d_2) \deg(d_2)^2 + \sum_{d_1|f_1} \phi_2(d_1) \deg(d_1)^2 \\
&= \sum_{d_1|f_1} \sum_{d_2|f_2} \phi_2(d_1)\phi_2(d_2) \deg(d_1)^2 \\
&\quad + 2 \sum_{d_1|f_1} \sum_{d_2|f_2} \phi_2(d_1)\phi_2(d_2) \deg(d_1) \deg(d_2) \\
&\quad + \sum_{d_1|f_1} \sum_{d_2|f_2} \phi_2(d_1)\phi_2(d_2) \deg(d_2)^2 + S_2(f_2) + S_2(f_1) \\
&= \sum_{d_2|f_2} S_2(f_1)\phi_2(d_2) + 2S_1(f_1)S_1(f_2) \\
&\quad + \sum_{d_1|f_1} S_2(f_2)\phi_2(d_1) + S_2(f_2) + S_2(f_1) \\
&= S_2(f_1)(1 + \sum_{d_2|f_2} \phi_2(d_2)) + S_2(f_2)(1 + \sum_{d_1|f_1} \phi_2(d_1)) + 2S_1(f_1)S_1(f_2) \\
&= S_2(f_1) 2^{\frac{\deg(f_2)}{2}} + S_2(f_2) 2^{\frac{\deg(f_1)}{2}} + 2S_1(f_1)S_1(f_2) \\
&= 2^{\frac{\deg(f_1 f_2)}{2}} \left[\frac{S_2(f_1)}{2^{\deg(f_1)/2}} + \frac{S_2(f_2}{2^{\deg(f_2)/2}} + 2 \frac{S_1(f_1)}{2^{\deg(f_1)/2}} \frac{S_1(f_2)}{2^{\deg(f_2)/2}} \right],
\end{aligned}$$

where in the last step we used Lemma 3.4.1. □

Now we are ready to determine the expected value and the variance for the parameter s in terms of the factorization of $x^n + 1$ into prime self-reciprocal polynomials in $\mathbb{F}_2[x]$. Firstly, in Theorem 3.4.5 we calculate $E(s)$ again for $p = 2$ that we obtained in Theorem 3.3.1. While we represent $E(s)$ in terms of the cardinalities of cyclotomic cosets modulo n in Theorem 3.3.1, we now express $E(s)$ in terms of the degrees of the prime self-reciprocal divisors of $x^n + 1$.

Theorem 3.4.5 For an odd integer n, let $x^n + 1 = (x+1)r_1 \cdots r_k$ be the factorization of $x^n + 1$ into prime self-reciprocal polynomials in $\mathbb{F}_2[x]$. The expected value $E(s)$ is given by

$$E(s) = 1 + \sum_{i=1}^{k} \frac{\deg(r_i)}{2^{\deg(r_i)/2}}.$$

Proof: By Proposition 3.4.1 (I), for $E(L) = n - E(s)$ we have $E(L) = \frac{1}{2^{(n-1)/2}} S_1(\frac{x^n+1}{x+1})$. Applying Lemma 3.4.3 recursively, we get

$$E(L) = \sum_{i=1}^{k} \frac{1}{2^{\deg(r_i)/2}} S_1(r_i). \tag{3.5}$$

By Lemma 3.4.2 (ii), for a prime self-reciprocal polynomial r we have

$$S_1(r) = \phi_2(r)\deg(r) = 2^{\frac{\deg(r)}{2}}(1 - \frac{1}{2^{\frac{\deg(r)}{2}}})\deg(r) = (2^{\frac{\deg(r)}{2}} - 1)\deg(r).$$

Hence $\frac{1}{2^{\deg(r_i)/2}} S_1(r_i) = \deg(r_i) - \frac{\deg(r_i)}{2^{\deg(r_i)/2}}$, $1 \le i \le k$, and by Equation 3.5 we obtain the desired formula. □

Theorem 3.4.6 For an odd integer n, let $x^n + 1 = (x+1)r_1 \cdots r_k$ be the factorization of $x^n + 1$ into prime self-reciprocal polynomials in $\mathbb{F}_2[x]$. The variance $Var(s)$ for s is given by

$$Var(s) = \sum_{i=1}^{k} \frac{\deg(r_i)^2(2^{deg(r_i)/2} - 1)}{2^{\deg(r_i)}}.$$

Proof: By Proposition 3.4.1 (I), we have

$$Var(s) = \frac{1}{2^{(n-1)/2}} S_2(\frac{x^n+1}{x+1}) - \left(\frac{1}{2^{(n-1)/2}} S_1(\frac{x^n+1}{x+1})\right)^2.$$

Applying Lemma 3.4.4 recursively, for $\frac{1}{2^{(n-1)/2}} S_2(\frac{x^n+1}{x+1}) = \frac{1}{2^{(n-1)/2}} S_2(r_1 \cdots r_k)$ we get

$$\frac{1}{2^{(n-1)/2}} S_2(r_1 \cdots r_k) = \sum_{i=1}^{k} \frac{S_2(r_i)}{2^{\deg(r_i)/2}} + 2 \sum_{1 \le i < j \le k} \frac{S_1(r_i)}{2^{\deg(r_i)/2}} \frac{S_1(r_j)}{2^{\deg(r_j)/2}}.$$

Again by a recursive application of Lemma 3.4.3, we obtain

$$\begin{aligned} \left(\frac{1}{2^{(n-1)/2}} S_1(\frac{x^n+1}{x+1})\right)^2 &= \left(\sum_{i=1}^{k} \frac{S_1(r_i)}{2^{\deg(r_i)/2}}\right)^2 \\ &= \sum_{i=1}^{k} \left(\frac{S_1(r_i)}{2^{\deg(r_i)/2}}\right)^2 + 2 \sum_{1 \le i < j \le k} \frac{S_1(r_i)}{2^{\deg(r_i)/2}} \frac{S_1(r_j)}{2^{\deg(r_j)/2}}. \end{aligned}$$

Combining the two formulas, by Lemma 3.4.2 (ii) we get

$$\begin{aligned} Var(s) &= \sum_{i=1}^{k} \frac{S_2(r_i)}{2^{deg(r_i)/2}} - \left(\frac{S_1(r_i)}{2^{deg(r_i)/2}}\right)^2 \\ &= \sum_{i=1}^{k} \frac{S_2(r_i)}{2^{deg(r_i)/2}} - \left(\frac{(2^{deg(r_i)/2-1})deg(r_i)}{2^{degr_i/2}}\right)^2 \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{k} \frac{(2^{\frac{deg(r_i)}{2}} - 1)deg(r_i)^2}{2^{deg(r_i)/2}} - \left(\frac{(2^{deg(r_i)/2-1})deg(r_i)}{2^{degr_i/2}} \right)^2 \\
&= \sum_{i=1}^{k} \frac{deg(r_i)^2(2^{deg(r_i)/2} - 1)}{2^{deg(r_i)}}
\end{aligned}
$$

□

Theorem 3.4.7 For $n = 2m$, m odd, let $x^n + 1 = (x^m + 1)^2 = (x + 1)^2 r_1^2 \cdots r_k^2$ be the factorization of $x^n + 1$ into prime self-reciprocal polynomials in $\mathbb{F}_2[x]$. The expected value $E(s)$ is given by

$$E(s) = 2 + \sum_{i=1}^{k} \left(\frac{\deg(r_i)}{2^{\deg(r_i)/2}} + \frac{\deg(r_i)}{2^{\deg(r_i)}} \right).$$

Proof: By Proposition 3.4.1 (II), for $E(L) = n - E(s)$ we have $E(L) = \frac{1}{2^{n/2-1}} S_1(\frac{x^n+1}{(x+1)^2})$. Applying Lemma 3.4.3 recursively, we get

$$E(L) = \sum_{i=1}^{k} \frac{1}{2^{\deg(r_i)}} S_1({r_i}^2).$$

By Lemma 3.4.2 (ii), for a prime self-reciprocal polynomial r we have

$$
\begin{aligned}
S_1(r^2) &= \sum_{d|r^2} \phi_2(d)\deg(d) = \phi_2(r)\deg(r) + \phi_2(r^2)\deg(r^2) \\
&= S_1(r) + \phi_2(r^2)\deg(r^2) \\
&= \left(2^{\frac{\deg(r)}{2}} - 1\right)\deg(r) + \phi_2(r^2)\deg(r^2) \\
&= \left(2^{\frac{\deg(r)}{2}} - 1\right)\deg(r) + \left(2^{\deg(r)} - 2^{\frac{\deg(r)}{2}}\right)2\deg(r) \\
&= \left(2^{\frac{\deg(r)}{2}} - 1\right)\deg(r)\left(1 + 2^{\frac{\deg(r)}{2}+1}\right). \qquad (3.6)
\end{aligned}
$$

Hence

$$
\begin{aligned}
E(L) &= \sum_{i=1}^{k} \frac{1}{2^{\deg(r_i)}} S_1({r_i}^2) \\
&= \sum_{i=1}^{k} \frac{\deg(r_i)}{2^{\deg(r_i)}} (2^{\frac{\deg(r_i)}{2}} - 1)(1 + 2^{\frac{\deg(r_i)}{2}+1}) \\
&= \sum_{i=1}^{k} \frac{\deg(r_i)}{2^{\deg(r_i)}} (2^{\deg(r_i)+1} - 2^{\frac{\deg(r_i)}{2}} + 1) \\
&= \sum_{i=1}^{k} \deg(r_i)(\frac{2^{\deg(r_i)+1} - 2^{\frac{\deg(r_i)}{2}} - 1}{2^{\deg(r_i)}}) \\
&= \sum_{i=1}^{k} \deg(r_i)(2 - \frac{1}{2^{\deg(r_i)/2}} - \frac{1}{2^{\deg(r_i)}})
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=1}^{k} 2\deg(r_i) - (\sum_{i=1}^{k} \frac{\deg(r_i)}{2^{\deg(r_i)/2}} + \frac{\deg(r_i)}{2^{\deg(r_i)}}) \\
&= n - 2 - (\sum_{i=1}^{k} \frac{\deg(r_i)}{2^{\deg(r_i)/2}} + \frac{\deg(r_i)}{2^{\deg(r_i)}})
\end{aligned}
$$

□

Theorem 3.4.8 For $n = 2m$ and odd m, let $x^n + 1 = (x^m + 1)^2 = (x+1)^2 r_1^2 \cdots r_k^2$ be the factorization of $x^n + 1$ into prime self-reciprocal polynomials in $\mathbb{F}_2[x]$. The variance $Var(s)$ for s is given by

$$
Var(s) = \sum_{i=1}^{k} \frac{\deg(r_i)^2 (2^{3\deg(r_i)/2} + 2^{\deg(r_i)+1} - 2^{\deg(r_i)/2+1} - 1)}{2^{2\deg(r_i)}}.
$$

Proof: We have similar arguments that is used in the proof of Theorem 3.4.6. By Proposition 3.4.1 (II), we have

$$
Var(s) = \frac{1}{2^{n/2-1}} S_2\left(\frac{x^n+1}{(x+1)^2}\right) - \left(\frac{1}{2^{n/2-1}} S_1\left(\frac{x^n+1}{(x+1)^2}\right)\right)^2.
$$

Applying Lemma 3.4.4 recursively, for $\frac{1}{2^{n/2-1}} S_2\left(\frac{x^n+1}{(x+1)^2}\right) = \frac{1}{2^{n/2-1}} S_2({r_1}^2 {r_2}^2 \ldots {r_k}^2)$ we get

$$
\frac{1}{2^{n/2-1}} S_2({r_1}^2 {r_2}^2 \ldots {r_k}^2) = \sum_{i=1}^{k} \frac{S_2({r_i}^2)}{2^{\deg(r_i)}} + 2 \sum_{1 \le i < j \le k} \frac{S_1({r_i}^2)}{2^{\deg(r_i)}} \frac{S_1({r_j}^2)}{2^{\deg(r_j)}}
$$

Again by a recursive application of Lemma 3.4.3, we obtain

$$
\left(\frac{1}{2^{n/2-1}} S_1\left(\frac{x^n+1}{(x+1)^2}\right)\right)^2 = \left(\sum_{i=1}^{k} \frac{S_1(r_i)^2}{2^{\deg(r_i)}}\right)^2 + 2 \sum_{1 \le i < j \le k} \frac{S_1({r_i}^2)}{2^{\deg(r_i)}} \frac{S_1({r_j}^2)}{2^{\deg(r_j)}}
$$

Combining the two formulas, we obtain

$$
Var(s) = \sum_{i=1}^{k} \frac{S_2({r_i}^2)}{2^{\deg(r_i)}} - \left(\frac{S_1({r_i}^2)}{2^{\deg(r_i)}}\right)^2. \tag{3.7}
$$

By Lemma 3.4.2 (ii) we have

$$
\begin{aligned}
S_2(r^2) &= \sum_{d | r^2} \phi_2(d) \deg(d)^2 = \phi_2(r) \deg(r)^2 + \phi_2(r^2)(\deg(r^2))^2 \\
&= S_2(r) + \phi_2(r^2)(\deg(r^2))^2 \\
&= \left(2^{\frac{\deg(r)}{2}} - 1\right) \deg(r)^2 + \phi_2(r^2)(\deg(r^2))^2 \\
&= \left(2^{\frac{\deg(r)}{2}} - 1\right) \deg(r)^2 + \left(2^{\deg(r)} - 2^{\frac{\deg(r)}{2}}\right) (\deg(r^2))^2 \\
&= \deg(r)^2 \left(2^{\deg(r)+2} - 3 \cdot 2^{\frac{\deg(r)}{2}} - 1\right)
\end{aligned}
$$

Combining with Equations 3.6 and 3.7 we get

$$\begin{aligned} Var(s) &= \sum_{i=1}^{k} \frac{\deg(r_i)^2(2^{\deg(r_i)+2} - 3 \cdot 2^{\frac{\deg(r_i)}{2}} - 1)}{2^{\deg(r_i)}} \\ &\quad - \left(\frac{\deg(r_i)(2^{\deg(r_i)+1} - 2^{\frac{\deg(r_i)}{2}} - 1)}{2^{\deg(r_i)}} \right)^2 \\ &= \sum_{i=1}^{k} \frac{\deg(r_i)^2(2^{3\deg(r_i)/2} + 2^{\deg(r_i)+1} - 2^{\deg(r_i)/2+1} - 1)}{2^{2\deg(r_i)}}. \end{aligned}$$

□

Bibliography

[1] Canteaut, A., Charpin, P., Kyureghyan, G. M.: *A new class of monomial bent functions*, Finite Fields Appl. **14**, 221–241, (2008).

[2] Carlet, C. : *Boolean Functions for Cryptography and Error Correcting Codes* (Chapter 8), In Y. Crama and P.L. Hammer, editors, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 257–397, Cambridge University Press, (2010).

[3] Çeşmelioğlu, A., McGuire, G., Meidl, W.: *A construction of weakly and non-weakly regular bent functions*, J. Combin. Theory, Ser. A **119**, 420–429, (2012).

[4] Çeşmelioğlu, A., Meidl, W.: *Bent functions of maximal degree*, IEEE Trans. Inform. Theory **58**, 1186–1190, (2012).

[5] Çeşmelioğlu, A., Meidl, W.: *A Construction of bent functions from plateaued functions*, Designs, Codes, Cryptogr. **66**, 231–242, (2013).

[6] 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, (Magdeburg, 2013), Contemporary Mathematics, to appear.

[7] Charpin, P., Gong, G.: *Hyperbent Functions, Kloosterman Sums, and Dickson Polynomials*, IEEE Trans. Inform. Theory **54**, No. 9, (2008).

[8] Charpin, P., Kyureghyan, G. M.: *Cubic Monomial Bent Functions: A subclass of* $\mathcal{M}$, SIAM J. Discrete Math., **22**, No. 2, 650–665, (2008).

[9] Charpin, P., Pasalic, E., Tavernier, C.: *On bent and semi-bent quadratic Boolean functions*, IEEE Trans. Inform. Theory **51**, 4286–4298, (2005).

[10] Cusick, T., Ding, C., Renvall, A.: *Stream Ciphers and Number Theory*, North Holland Mathematical Library, Elsevier, (2004).

[11] Dillon, J.F., Dobbertin H.: *New cyclic difference sets with Singer parameters*, Finite Fields Appl. **10**, 342–389, (2004).

[12] Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: *Construction of bent functions via Niho power functions*, J. Combin. Theory Ser. A **113**, no. 5, 779–798, (2006).

[13] Fitzgerald, R.W.: *Highly degenerate quadratic forms over finite fields of characteristic* 2, Finite Fields Appl. **11**, 165–181, (2005).

[14] Fitzgerald, R.W.: *Trace forms over finite fields of characteristic* 2 *with prescribed invariants*, Finite Fields Appl. **15**, 69–81, (2009).

[15] Fu, F. W., Niederreiter, H., Özbudak, F.: *Joint linear complexity of multisequences consisting of linear recurring sequences*, Cryptogr. Commun. **1**, 3–29, (2009).

[16] Fu, F. W., Niederreiter, H., Özbudak, F.: *Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences*, Finite Fields Appl. **15**, 475–496, (2009).

[17] Games, R. A., Chan, A. H.: *A fast algorithm for determining the complexity of a binary sequence with period* 2^n, IEEE Trans. Inform. Theory **29**, 144–146, (1983).

[18] Gold, R.:*Maximal Recursive Sequences with* 3*-valued Recursive Cross-Correlation Functions*, IEEE Trans. Inform. Theory **14**, 154–156, (1968).

[19] Helleseth, T., Kholosha, A.: *Monomial and quadratic bent functions over the finite fields of odd characteristic*, IEEE Trans. Inform. Theory **52**, 2018–2032, (2006).

[20] Hu, H., Feng, D.: *On Quadratic bent functions in polynomial forms*, IEEE Trans. Inform. Theory **53**, 2610–2615, (2007).

[21] Jungnickel, D.: *Finite Fields Structure and Arithmetic*, BI Wiss. Verlag Mannheim, Leipzig, Wien, Zurich, 1993.

[22] Khoo, K., Gong, G., Stinson, D.: *A new family of Gold-like sequences*, In: Proceedings of IEEE International Symposium of Information Theory p. 181, (2002).

[23] 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).

[24] Kim, Y.S., Jang, J.W., No, J.S., Helleseth, T.: *On p-ary bent functions defined on finite fields*, In: Mathematical properties of sequences and other combinatorial structures, 65–76, Kluwer, Dordrecht (2002).

[25] Langevin, P., Leander, N. G.: *Monomial bent functions and Stickelbergers theorem*, Finite Fields Appl. **14**, 727–742, (2008).

[26] Leander, N. G.: *Monomial bent functions*, IEEE Trans. Inform. Theory **52**, 738–743, (2006).

[27] Lidl, R., Niederreiter, H.: *Finite Fields, 2nd ed., Encyclopedia Math. Appl.*, vol. 20. Cambridge Univ. Press, Cambridge (1997).

[28] Meidl, W., Niederreiter, H.: *Linear complexity, k-error linear complexity, and the discrete Fourier transform*, J. Comp. **18**, 87–103, (2002).

[29] Meidl, W., Niederreiter, H.: *On the expected value of the linear complexity and the k-error linear complexity of periodic sequences*, IEEE Trans. Inform. Theory **48**, 2817–2825, (2002).

[30] Meidl, W., Topuzoğlu, A.: *Quadratic functions with prescribed spectra*, Designs, Codes, Cryptogr. **66**, 257–273, (2013).

[31] Meidl, W., Roy, S., Topuzoğlu, A.: *Enumeration of quadratic functions with prescribed Walsh spectrum*, IEEE Trans. Inform. Theory **60**, 6669–6680 (2014).

[32] Meyn, H.: *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Algebra Eng. Comm. Comput. **1**, 43–53, (1990).

[33] Mullen G., Panario D.: *Handbook of Finite Fields*, 241–303, Chapman and Hall / CRC, (2013).

[34] Nyberg, K.: *Perfect nonlinear S-boxes*, EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., **547**, 378–386, Springer, Berlin (1991).

[35] Rothaus, O. S. : *On Bent Functions*, J. Combin. Theory Ser. A **20**, no. 3, 300–305, (1976).

[36] Yu, N.Y., Gong, G.: *Constructions of quadratic bent functions in polynomial forms*, IEEE Trans. Inform. Theory **52**, 3291–3299, (2006).