

Crosscorrelation Properties between Perfect Sequences

Dissertation

zur Erlangung des akademischen Grades

**doctor rerum naturalium
(Dr. rer. nat.)**

von Frau Diplom-Mathematikerin Doreen Hertel
geb. am 22.06.1978 in Magdeburg

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg

Gutachter: Prof. Dr. A. Pott
Prof. Dr. K.T. Arasu

eingereicht am: 31. August 2006

Verteidigung am: 21. Dezember 2006

Acknowledgements

I am deeply indebted to Prof. Dr. Alexander Pott for supervising me as a doctoral student, and for his constant support. Prof. Alexander Pott has shared a great deal of his mathematical knowledge with me. He encouraged me from the beginning to present my research work in lectures, and that is another reason I feel really grateful to him.

I wish to thank Prof. Dr. K.T. Arasu for giving me the chance of an educational visit at the Wright State University, Dayton, Ohio, and Prof. Dr. T. Helleseth at the University of Bergen in Norway. Both educational visits provided valuable enlargements of my knowledge while I was studying for a doctorate. With the help of them I was able to develop new ideas for my research work.

I am grateful to Dr. Gohar Kyureghyan as she always lent a ready ear when I had mathematical problems, and helped me with her extensive comments.

Special thanks are given to my parents for encouraging me to study mathematics, and for their constant support during the time I was studying for my degree, and later when I was studying for my doctorate.

I thank Tino for always being by my side.

Abstract

This thesis is an investigation of the crosscorrelation function between perfect sequences of the same period length. The context of the thesis is composed of three parts.

In the first part (Chapter 3 and 4), the crosscorrelation function between perfect sequences of period $4m - 1$ is considered. The concept of Hadamard equivalence is generalised to sequences of period $4m - 1$. We call this extended Hadamard equivalence. Based on this new equivalence, we propose an algorithm to construct perfect sequences of period $4m - 1$. Furthermore, we show that the Hall and Legendre sequences of the same period are extended Hadamard equivalent.

The second part (Chapter 5 and 6) is devoted to the crosscorrelation between perfect sequences of period $2^m - 1$. Sequences of period $2^m - 1$ can be identify with Boolean functions over finite fields. The (usual) Hadamard equivalence is used to express the crosscorrelation between perfect functions of certain families in terms of the crosscorrelation between m -functions, the classical perfect functions. It is proved that certain series of perfect functions obtained from the Dillon-Dobbertin and Gordon-Mills-Welch construction have good crosscorrelation properties.

In the study of the crosscorrelation between m -functions, maximum nonlinear power functions x^d are of interest. The Gold ($d = 2^k + 1$) and Kasami ($d = 2^{2k} - 2^k + 1$) power functions are the most important maximum nonlinear functions. In the last part (Chapter 7) we prove a new property of the Kasami parameter and we give a characterisation of the Gold power mappings in terms of their distance to characteristic functions of subspaces of codimension 1 and 2 in \mathbb{F}_{2^m} .

Contents

1	Introduction	7
1.1	Definitions and Notations	9
1.2	Algebraic Tools	12
1.3	Equivalent Descriptions	15
2	Perfect Sequences	19
2.1	Known Perfect Sequences	19
2.2	Gordon-Mills-Welch Method	22
3	Properties of the Crosscorrelation Function	25
3.1	Dual Sequence	26
3.2	Lower Bounds	29
4	Extended Hadamard Equivalence	35
4.1	(Extended) Hadamard Equivalence	35
4.2	EH-Equivalence of Legendre and Hall Sequences	39
5	Crosscorrelation between Perfect Functions	45
5.1	Properties of the Crosscorrelation Function	45
5.2	Hadamard Equivalence of Functions	48
5.3	Application of Hadamard Equivalence	49
6	Crosscorrelation between Special Perfect Functions	51

6.1	Crosscorrelation between m -Functions	53
6.2	Crosscorrelation between Dillon-Dobbertin Functions	58
6.3	Crosscorrelation between GMW and Dillon-Dobbertin Functions .	61
7	Two Notes on Power Functions	67
7.1	A New Property of the Kasami Power Mappings	67
7.2	A New Characterisation of the Gold Power Mappings	72
	Conclusion	81
	List of Symbols	83
	Index	85
	References	87

Chapter 1

Introduction

Binary periodic sequences with good autocorrelation and crosscorrelation properties are widely used in signal processing. If the autocorrelation properties are optimum and the sequence is balanced, then the sequence is called perfect. In the last few years, the study of perfect sequences has made significant progress. Several new classes of perfect sequences of period $2^m - 1$ have been constructed [5, 28, 30, 31].

The main part of this thesis is an investigation of the crosscorrelation function between perfect sequences of the same period length. The thesis is organised as follows:

In the first chapter, basic definitions are given and the connection between sequences, functions and sets is explained: There is a one-to-one correspondence between binary sequences of period n , sets in a cyclic group G of order n and their characteristic functions $G \rightarrow \{0, 1\}$, respectively. The autocorrelation and crosscorrelation properties are formulated using all these notions. In Chapter 2, all known constructions for perfect sequences are listed and the Gordon-Mills-Welch method for constructing perfect sequences is explained.

In Chapter 3, two slight modified autocorrelation and crosscorrelation functions are given. The first definition implies some interesting autocorrelation properties between a sequence \underline{a} and the sequence obtained from the crosscorrelation coefficients of \underline{a} with a perfect sequence. Using the second definition, a lower bound for the maximum crosscorrelation coefficient (in absolute value) is shown. For the crosscorrelation between perfect sequences, these two definitions are identical.

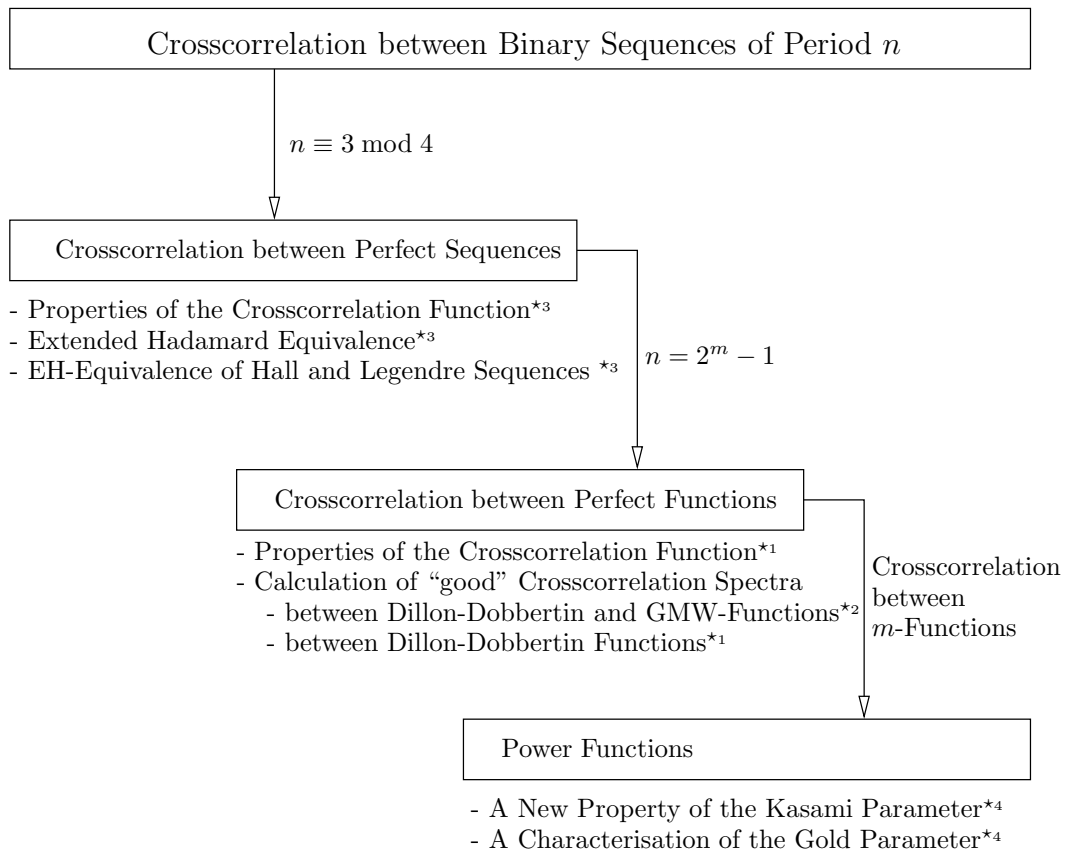
The concept of extended Hadamard equivalence is introduced in Chapter 4. Extended Hadamard equivalence can be used to construct sequences with prescribed autocorrelation properties and it can also be used to prove that a sequence is perfect. It is proved that the Hall and Legendre sequences of the same period length

are extended Hadamard equivalent. Furthermore, it is shown, that the crosscorrelation function between Hall sequences and between Hall and Legendre sequences is reduced to the calculation of cyclotomic numbers. We explicitly calculate the crosscorrelation spectra between these sequences.

Most series of perfect sequences have period $2^m - 1$, i.e. they can be identified with Boolean functions on finite fields of characteristic 2. In Chapter 5, the (classical) Hadamard equivalence is used to express the crosscorrelation function between perfect sequences of certain families with period $2^m - 1$ in terms of the crosscorrelation between m -sequences (the classical perfect sequences), the crosscorrelation of which is well studied. In Chapter 6, the crosscorrelation spectra between perfect sequences from the Dillon-Dobbertin and from the Gordon-Mills-Welch constructions are explicitly calculated, and it is proved that certain series of these sequences have good crosscorrelation properties.

In the study of the crosscorrelation between m -sequences, the Gold and Kasami decimations play an important role. We found a new characterisation of the Gold exponents. Furthermore, an interesting property of the Kasami exponents was proved. These results are presented in Chapter 7.

Overview



Some parts of this thesis are published or accepted for publication. Several parts have been presented at conferences:

- At the international conference “Sequences and their Applications” (SETA ’04) in Seoul/Korea, I presented the topics indicated by \star_1 . The content of my talk is published in the proceedings of the conference [17].
- The topics indicated by \star_2 were content of my talk at the international conference “Sequence Design and its Application in Communications” (IWSDA ’05) in Shimonoseki/Japan. The results are published in the proceedings of the conference [18].
- At the international conference “Sequences and their Applications” (SETA ’06) in Beijing/China I will talk about the topics indicated by \star_3 . The results will be published in the proceedings of the conference [19].
- At the international conference “Finite Geometries” in Irsee/Germany, Prof. Pott will present the results based on the Gold and Kasami exponents, which are indicated by \star_4 . The content will be submitted to the proceedings of that conference.

1.1 Definitions and Notations

A sequence $\underline{a} = (a_i)_{i \geq 0}$ is called **periodic** with **period** n (or n -periodic for short) if $a_i = a_{i+n}$ for all i . Since \underline{a} is n -periodic, its indices may be computed modulo n and \underline{a} can be identified with its fundamental vector (a_0, \dots, a_{n-1}) . The **shift** $\underline{a}^{[t]} = (a_i^{[t]})_{i \geq 0}$ of \underline{a} is defined by $a_i^{[t]} := a_{i+t}$. The fundamental vector of $\underline{a}^{[t]}$ is $(a_t, \dots, a_{n-1}, a_0, \dots, a_{t-1})$, which is a cyclic shift of the fundamental vector of \underline{a} by t positions to the left.

For binary sequence $\underline{a} = (a_i)_{i \geq 0}$ the **autocorrelation** is defined by

$$c_t(\underline{a}) := \sum_{i=0}^{n-1} (-1)^{a_i + a_{i+t}} \quad (1.1)$$

for all t . The autocorrelation coefficients form itself a sequence $(c_t(\underline{a}))_{t \geq 0}$, which is also periodic with period n . The **autocorrelation spectrum** $Sp(\underline{a}) := \{c_t(\underline{a}) | t = 0, \dots, n-1\}$ is the set of all autocorrelation coefficients $c_t(\underline{a})$ of \underline{a} .

Let $v = (v_0, \dots, v_{n-1})$ and $w = (w_0, \dots, w_{n-1})$ be two real vectors of length n . The **Hamming weight** $w_H(v)$ of v is defined by $w_H(v) := |\{i | v_i \neq 0, i = 0, \dots, n-1\}|$ and the **Hamming distance** $d_H(v, w)$ of v and w by $d_H(v, w) := w_H(v - w)$. If

we talk about the Hamming weight (resp. distance) of periodic sequences, then we mean the Hamming weight (resp. distance) of their fundamental vectors.

Let $\bar{\underline{a}} = (\bar{a}_i)_{i \geq 0}$ denote the **binary complement** of \underline{a} defined by $\bar{a}_i := a_i + 1$. Since $c_t(\underline{a}) = n - 2d_H(\underline{a}, \underline{a}^{[t]}) = -(n - 2d_H(\underline{a}, \bar{\underline{a}}^{[t]}))$, formula (1.1) shows: A small autocorrelation coefficient $c_t(\underline{a})$ (in absolute value) implies that $\underline{a}, \underline{a}^{[t]}$ and $\underline{a}, \bar{\underline{a}}^{[t]}$ have large Hamming distance. Thus, the autocorrelation function is a measure for how much a given sequence differs from all its shift.

In this thesis, sequences with autocorrelation coefficients, which are as small as possible, are considered. A sequence \underline{a} with n odd and

$$c_t(\underline{a}) = \begin{cases} -1 & \text{for } 1 \leq t \leq n-1 \\ n & \text{otherwise} \end{cases}$$

is called **perfect**. Perfect sequences can only exist for $n \equiv 3 \pmod{4}$, since $c_t(\underline{a}) \equiv n \pmod{4}$ for all t , which is well known and easy to see (from (1.11) with $c_t(\underline{a}, \underline{a}) = c_t(\underline{a})$). We say a sequence has constant autocorrelation c if the autocorrelation spectrum is two-valued with c and n , since it is trivially $c_0(\underline{a}) = n$.

An n -periodic sequence is called **balanced**, if its Hamming weight is $\frac{n}{2}$ if n is even or $\frac{n \pm 1}{2}$ if n is odd, i.e. the number of ones and zeros in one period is as closed as possible.

For a perfect sequence \underline{a} , we have $\sum_{i=0}^{n-1} (-1)^{a_i} = \pm 1$. In deed,

$$\left(\sum_{i=0}^{n-1} (-1)^{a_i} \right)^2 = \sum_{i=0}^{n-1} \sum_{t=0}^{n-1} (-1)^{a_i + a_{i+t}} = \sum_{t=0}^{n-1} c_t(\underline{a}) = (-1)(n-1) + n = 1,$$

since $c_0(\underline{a}) = n$. Thus, perfect sequences are always balanced.

Note that the autocorrelation function and the balanced property are invariant under the operation taking the binary complement. In the following, for a balanced sequence (and thus for all perfect sequences) \underline{a} we always assume that

$$\sum_{t=0}^{n-1} (-1)^{a_t} = -1, \tag{1.2}$$

otherwise its binary complement is considered. A sequence with property (1.2) has $\frac{n+1}{2}$ entries 1 and $\frac{n-1}{2}$ entries 0 in one period.

The **decimation** $\underline{a}^{(d)} = (a_i^{(d)})_{i \geq 0}$ of an n -periodic sequence \underline{a} is defined by $a_i^{(d)} := a_{id}$. In this thesis, we only consider decimations d with $\gcd(d, n) = 1$.

Two sequences \underline{a} and \underline{b} are called **equivalent**, if \underline{a} can be transformed into \underline{b} by a shift and/or decimation with $\gcd(d, n) = 1$. Equivalent sequences have the same autocorrelation spectrum, since the autocorrelation spectrum is invariant under

the operations shift and decimation with $\gcd(d, n) = 1$. Thus, if we have one perfect sequence, we actually have a whole class of perfect sequences, which are equivalent to the given one.

Two sequences \underline{a} and \underline{b} are called **shift distinct**, if no shift of \underline{a} is equal to \underline{b} , otherwise they are called **shift equivalent**.

An integer d is called a **multiplier** of a sequence \underline{a} , if $\underline{a}^{(d)}$ is shift equivalent to \underline{a} . Obviously, equivalent sequences have the same multipliers. Thus, if two perfect sequences have different multipliers, they cannot be equivalent. For perfect sequences it is proven that there exists a shift \underline{b} of \underline{a} such that $\underline{b}^{(d)} = \underline{b}$ holds for any multiplier of \underline{a} . Without loss of generality, we assume for a perfect sequence that

$$\underline{a}^{(d)} = \underline{a} \quad (1.3)$$

holds for any multiplier d of \underline{a} . In [12] it is shown, that any power of 2 is a multiplier of a perfect sequence with period $n = 2^m - 1$.

The **crosscorrelation** between two sequences $\underline{a} = (a_i)_{i \geq 0}$ and $\underline{b} = (b_i)_{i \geq 0}$ of period n is defined by

$$c_t(\underline{a}, \underline{b}) := \sum_{i=0}^{n-1} (-1)^{a_i + b_{i+t}}. \quad (1.4)$$

The set of all crosscorrelation coefficients $c_t(\underline{a}, \underline{b})$ is called the **crosscorrelation spectrum** $Sp(\underline{a}, \underline{b})$. Since $c_t(\underline{a}, \underline{b}) = n - 2d_H(\underline{a}, \underline{b}^{[t]})$, the maximum crosscorrelation coefficient (in absolute value) is a measure for how much a given sequence \underline{a} can be used to approximate another sequence \underline{b} .

Example 1.1 Let $\underline{a} = (1, 1, 1, 0, 0, 1, 0)$ and $\underline{b} = (1, 1, 0, 1, 0, 0, 1)$ be two sequences of period 7. The sequences are shift distinct. The autocorrelations are given by

$$\begin{array}{c|cccccc} t & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline c_t(\underline{a}) & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\ c_t(\underline{b}) & 7 & -1 & -1 & -1 & -1 & -1 & -1 \end{array},$$

thus, both sequences are perfect. We have

$$\frac{\underline{a}}{\underline{a}^{(2)}} \left| \begin{array}{l} \underline{1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, \dots} \\ \underline{1, 1, 0, 0, 1, 0, 1, \dots} \end{array} \right. \quad \frac{\underline{a}}{\underline{a}^{(3)}} \left| \begin{array}{l} \underline{1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, \dots} \\ \underline{1, 0, 0, 1, 1, 1, 0, \dots} \end{array} \right. ,$$

therefore, 2 is a multiplier of \underline{a} , since $\underline{a}^{(2)} = \underline{a}^{[1]}$, and the sequences \underline{a} and \underline{b} are equivalent, since $\underline{a}^{(3)} = \underline{b}^{[3]}$. The crosscorrelation is given by

$$\frac{t}{c_t(\underline{a}, \underline{b})} \left| \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ -1 & +3 & -1 & -1 & -5 & +3 & +3 \end{array} \right. (= c_{t-3}(\underline{a}, \underline{a}^{(3)})).$$

As mentioned before, the autocorrelation spectrum is invariant under the operations shift, decimation and taking the binary complement. The crosscorrelation spectrum is also invariant if any of the sequences is replaced by a shift. Every crosscorrelation coefficient changes its sign, if one sequence is substituted by its binary complement.

If we use the operation decimation we must be careful: In general, if only one sequence is substituted by one of its decimations, then the crosscorrelation spectrum changes. More precisely, if we know the crosscorrelation between \underline{a} and \underline{b} , then in general we know nothing about the crosscorrelation between $\underline{a}^{(d)}$ and \underline{b} . Obviously, if both sequences \underline{a} and \underline{b} are replaced by $\underline{a}^{(d)}$ and $\underline{b}^{(d)}$, where $\gcd(d, n) = 1$, then the crosscorrelation spectrum does not change.

The notions shift, equivalence, decimation and multiplier we will also use for real periodic sequences.

Another possibility to define an autocorrelation and crosscorrelation function of periodic sequences is the following: Let $\underline{a} = (a_i)_{i \geq 0}$ and $\underline{b} = (b_i)_{i \geq 0}$ be real sequences of period n , i.e. $a_i, b_i \in \mathbb{R}$. The autocorrelation of \underline{a} and the crosscorrelation between \underline{a} and \underline{b} are defined by

$$C_t(\underline{a}) := \sum_{i=0}^{n-1} a_i a_{i+t} \quad \text{and} \quad C_t(\underline{a}, \underline{b}) := \sum_{i=0}^{n-1} a_i b_{i+t}$$

for all t , which is the usual inner product of the fundamental vectors of \underline{a} and $\underline{a}^{[t]}$ and of \underline{a} and $\underline{b}^{[t]}$, respectively. The connection between $C_t(\cdot)$ and $c_t(\cdot)$ for binary sequences \underline{a} and \underline{b} is $c_t(\underline{a}, \underline{b}) = n - 2(w_H(\underline{a}) + w_H(\underline{b}) - 2C_t(\underline{a}, \underline{b}))$ and $c_t(\underline{a}) = n - 4(w_H(\underline{a}) - C_t(\underline{a}))$.

1.2 Algebraic Tools

Relation between Sequences, Sets and Functions

In this thesis, G is always the multiplicatively written cyclic group of order n , i.e. $G = \langle g \rangle$ for an element g in G . A set $D \subset G$ defines a sequence $\underline{a} = (a_i)_{i \geq 0}$ by

$$\underline{a} := \text{seq}(D) \quad \text{with} \quad a_i := 1 \text{ if } g^i \in D \text{ and } a_i := 0 \text{ otherwise.} \quad (1.5)$$

Moreover, a binary sequence \underline{a} of period n defines a set by $\text{supp}(\underline{a}) := \{g^i \in G \mid a_i = 1\}$. The set $\text{supp}(\underline{a})$ is called **support** of \underline{a} in G . The **translate** of D is

defined by $g^t D := \{g^t h \mid h \in D\}$, the **decimation** by $D^{(d)} := \{h^d \mid h \in D\}$ and the **complement** \overline{D} by $\overline{D} := \{h \in G \mid h \notin D\}$. (If $G = (\mathbb{Z}_n, +)$ is an additive group, then we write $D + t$ for a translate and dD for a decimation.)

A sequence \underline{a} can also be identified with a function $f : G \rightarrow \{0, 1\}$, which is defined by

$$f(g^i) := a_i. \quad (1.6)$$

The function f is the characteristic function of $\text{supp}(\underline{a})$ in G . Let $y \in G$, we define the **shift** $f^{[y]}$ by $f^{[y]}(x) := f(yx)$ and the **decimation** $f^{(d)}$ by $f^{(d)}(x) := f(x^d)$ for all $x \in G$.

Let \underline{a} , D and f correspond to each other as defined above (using generator g of G) and let d be an integer such that $\gcd(d, n) = 1$, then the following table translates the different notions of decimation and shift:

	sequence \underline{a}	function f	set $D \subset (G, \cdot)$	$(D \subset (\mathbb{Z}_n, +))$
decimation	$\underline{a}^{(d)}$	$f^{(d)}$	$D^{(1/d)}$	$(d^{-1}D)$
shift	$\underline{a}^{[t]}$	$f^{[g^t]}$	$g^{-t}D$	$(D - gt)$

Note that the transformations depend on the choice of the primitive element g : Changing the primitive element “is” a decimation of the sequence. For $G = (\mathbb{Z}_n, +)$ we choose 1 as the primitive element.

The definitions on sequences, which we have given in Section 1.1, are transferred to functions (resp. to sets): We say a function (resp. a set) has property P , if its corresponding sequence has property P . We can do this, since P is invariant under decimation.

To translate the autocorrelation property to sets, we give some definitions about difference sets. For a thorough investigation of difference sets we refer to [2, 12, 21].

Let $n' \mid n$ and N be a subgroup of G of order n' . Let $D \subseteq G$ such that every element in $G \setminus N$ has exactly λ representations as a difference with elements in D . Elements in N different from the identity have exactly λ' such representations. Any set with this property is called an $(n/n', n', k, \lambda', \lambda)$ -**divisible difference set** in G relative to N .

If $\lambda' = 0$, then we call it a **relative difference set**. In this case, the exceptional subgroup N is called the forbidden subgroup. Moreover, if $n' = 1$, then an $(n, 1, k, 0, \lambda)$ -divisible difference set is called an (n, k, λ) -**difference set** in G .

Note, that for an (n, k, λ) -difference set $D \subset G$ holds that $|D| = k$ and each element in $G \setminus \{0\}$ has exactly λ different descriptions as difference of two elements from D .

If the group G is cyclic and D is a (divisible) difference set in G , then D is called a **cyclic** (divisible) difference set.

Groups and Finite Fields

Given a subset D of G , the same symbol D is also used to denote the corresponding group ring element

$$D = \sum_{x \in D} x \in \mathbb{C}[G]. \quad (1.7)$$

The group G is isomorphic to $(\mathbb{Z}_n, +)$, since G is a cyclic group of order n . Let $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid x \text{ is invertible modulo } n\}$. If n is prime, then \mathbb{Z}_n is a finite field with multiplicative group \mathbb{Z}_n^* . If $n = p^m - 1$ and p is prime, then $(\mathbb{Z}_n, +)$ is isomorphic to $\mathbb{F}_{p^m}^*$, where \mathbb{F}_{p^m} denotes the finite field with p^m elements and $\mathbb{F}_{p^m}^*$ its multiplicative group.

Any binary sequence of period $n = 2^m - 1$ describes a function $f : \mathbb{F}_{2^m}^* \rightarrow \mathbb{F}_2$ by (1.6). Conversely any function $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ describes a binary sequence, where the value $f(0)$ is irrelevant. We choose $f(0) \in \{0, 1\}$ such that $\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)} = 0$, which is always possible if f is balanced. Using (1.2), for balanced and therefore for perfect functions it is always assumed that $f(0) = 0$.

Let $f, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be Boolean functions. The **autocorrelation** of f and the **crosscorrelation** between f and g are defined by

$$c_y(f) := \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+f(yx)} \quad \text{and} \quad c_y(f, g) := \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+g(yx)} \quad (1.8)$$

for all $y \in \mathbb{F}_{2^m}$, where we identify \mathbb{F}_2 with $\{0, 1\} \subset \mathbb{C}$. The crosscorrelation spectrum is given by $Sp(f, g) := \{c_y(f, g) \mid y \in \mathbb{F}_{2^m}^*\}$ and the autocorrelation spectrum by $Sp(f) := Sp(f, f)$. Note that $c_0(f, g) = (-1)^{g(0)+f(0)} c_0(f)$. If \underline{a} is the sequence corresponding to f using a primitive element $\alpha \in \mathbb{F}_{2^m}$, then $c_{\alpha^t}(f) = c_t(\underline{a}) + 1$. Furthermore, a function f is **perfect** if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+f(yx)} = \begin{cases} 2^m & \text{if } y = 1 \\ 0 & \text{otherwise.} \end{cases} \quad (1.9)$$

For $m = rs$, we may view \mathbb{F}_{2^s} as a subfield of \mathbb{F}_{2^m} . The **trace** function from \mathbb{F}_{2^m} to \mathbb{F}_{2^s} is the linear mapping $tr_{m/s}$ defined by $tr_{m/s}(x) := \sum_{i=0}^{m-1} x^{2^{si}}$. For $s = 1$ we simply write tr instead of $tr_{m/1}$, and we say tr is the trace function on \mathbb{F}_{2^m} . It is well known that the shifts $tr^{[\beta]}$, $\beta \in \mathbb{F}_{2^m}^*$, and $tr^{[0]}$ are linear, again, and all 2^m linear mappings $\mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ can be represented like this. The linear functions $tr^{[\beta]}$, $\beta \in \mathbb{F}_{2^m}^*$, are the classical perfect functions.

Let $F : \mathbb{F}_{2^m} \rightarrow \mathbb{C}$ be a function, the **Walsh transform** [15] (also called **Hadamard transform**) $\mathcal{W}(F)$ of F is the mapping $\mathbb{F}_{2^m} \rightarrow \mathbb{C}$ defined by

$$\mathcal{W}(F)(y) := \sum_{x \in \mathbb{F}_{2^m}} F(x)(-1)^{\text{tr}(yx)}.$$

If $F(x) = (-1)^{f(x)}$, we simply write $\mathcal{W}(f)$ instead of $\mathcal{W}(F)$. If g is the *trace* function, then

$$\mathcal{W}(f)(y) = c_y(f, g). \quad (1.10)$$

Thus, the Walsh transform $\mathcal{W}(f)$ is equal to the crosscorrelation function between f and the linear functions.

1.3 Equivalent Descriptions

In this section, some equivalent descriptions for the autocorrelation and crosscorrelation function of binary sequences are considered.

Proposition 1.2 *Let $G = \langle g \rangle$ and $D, E \subset G$ with $|G| = n$ and $|D| = |E| = k$. Then the following statements are equivalent:*

- (1) *We have $|D \cap g^t E| = \lambda_t$ for all $t = 0, \dots, n-1$.*
- (2) *The sequences $\underline{a} := \text{seq}(D)$ and $\underline{b} := \text{seq}(E)$ have crosscorrelation $c_{-t}(\underline{a}, \underline{b}) = n - 4(k - \lambda_t)$.*
- (3) *We have $DE^{(-1)} = \sum_{t=0}^{n-1} \lambda_t g^t$ in the group ring $\mathbb{C}[G]$.*

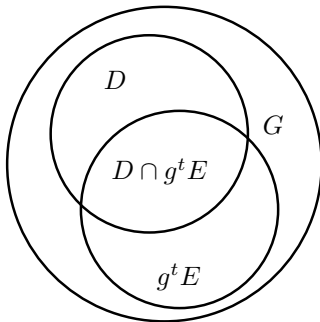
Proof.

(1) \iff (2)

The crosscorrelation coefficient $c_t(\underline{a}, \underline{b})$ is an integer, which we may interpret also in terms of the intersection between certain sets. We have

$$c_{-t}(\underline{a}, \underline{b}) = n - 4(k - \lambda_t), \quad (1.11)$$

since



$$\begin{aligned} c_{-t}(\underline{a}, \underline{b}) &= \sum_{i=0}^{n-1} (-1)^{a_i + b_{i-t}} \\ &= |\{i \mid a_i = b_{i-t}, 0 \leq i \leq n-1\}| \\ &\quad - |\{i \mid a_i \neq b_{i-t}, 0 \leq i \leq n-1\}| \\ &= n - 2|\{i \mid a_i \neq b_{i-t}, 0 \leq i \leq n-1\}| \\ &= n - 2(|D| + |g^t E| - 2|D \cap g^t E|) \\ &= n - 4(k - \lambda_t) \end{aligned}$$

and $|D| = |g^t E| = k$.

(1) \iff (3)

Let $D = \sum_{d \in D} d$ and $E = \sum_{d' \in E} d'$ in $\mathbb{C}[G]$. We have

$$DE^{(-1)} = \sum_{d \in D} \sum_{d' \in E} dd'^{-1} = \sum_{t=0}^{n-1} \lambda_t g^t,$$

where λ_t is the number of pairs (d, d') with $d \in D$ and $d' \in E$ such that $dd'^{-1} = g^t$. It is $d = g^t d'$ for λ_t pairs (d, d') . Therefore $|D \cap g^t E| = \lambda_t$ and vice versa. \square

The notions above are useful for the analysis of crosscorrelation functions between perfect sequences. For perfect sequences we have the following equivalent descriptions.

Corollary 1.3 (Equivalent Description) *Let $G = \langle g \rangle$ and $D \subset G$ with $|G| = n$ and $|D| = k$. Then the following statements are equivalent:*

- (1) *The set D is an (n, k, λ) -difference set in G .*
- (2) *We have $|D \cap g^t D| = \lambda$ for all $t = 1, \dots, n-1$.*
- (3) *The sequence $\underline{a} := \text{seq}(D)$ has constant autocorrelation $c = n - 4(k - \lambda)$.*
- (4) *We have $DD^{(-1)} = (k - \lambda) + \lambda G$ in the group ring $\mathbb{C}[G]$.*

Proof. The equivalence of (2), (3) and (4) follows from Proposition 1.2 with $D = E$ and $c_t(\underline{a}) = c_t(\underline{a}, \underline{a})$. We still have to show that (1) is equivalent to another item.

(1) \iff (2)

Let $h \in (D \cap g^t D)$, then $g^t d = h = d'$ for some $d, d' \in D$, hence $g^t = d' d^{-1}$. Thus, $\lambda_t := |D \cap g^t D|$ is the number of difference pairs (d, d') with $d, d' \in D$ such that $d' d^{-1} = g^t$. The intersection size λ_t is constant if and only if the number of these difference pairs is constant. \square

Perfect sequences of period $n = 4t - 1$ and (1.2) are in one-to-one correspondence to the notions above with $k = 2t$ and $\lambda = t$. A cyclic $(4t - 1, 2t, t)$ -difference set is called **Paley type difference set** and if t is a power of 2, then it is called a **Singer type difference set**. A cyclic $((2^m - 1)/(2^s - 1), 2^s - 1, 2^{m-s}, 0, 2^{m-2s})$ -relative difference set is called a **relative Singer type difference set**.

Corollary 1.4 *Let $G = \langle g \rangle$ and $D \subset G$ with $|G| = n$ and $|D| = k$. Then D is an $(n/n', n', k, \lambda', \lambda)$ -divisible difference set if and only if*

$$DD^{(-1)} = (k - \lambda') + \lambda \sum_{g \in G \setminus N} g + \lambda' \sum_{h \in N} h. \quad (1.12)$$

There is another interesting connection of perfect sequences to Hadamard matrices:

Let A be an $n' \times n'$ -matrix with entries ± 1 . If A satisfies $AA^T = n'I$, where I is the identity matrix, then A is called a **Hadamard matrix**. For a recent survey on Hadamard matrices, see [35], for instance.

Let $\underline{a} = (a_i)_{i \geq 0}$. Then the matrix $B = (b_{i,j})_{i,j=0,\dots,n-1}$ with $b_{i,j} := ((-1)^{a_j+i})$ satisfies $BB^T = (n-c)I + cJ$, where J is the matrix with all entries 1, if and only if \underline{a} has constant autocorrelation c , since $(BB^T)_{i,j} = c_0(\underline{a}^{[i]}, \underline{a}^{[j]}) = c_{j-i}(\underline{a})$.

For perfect binary sequences we have the following proposition:

Proposition 1.5 *Let $\underline{a} = (a_i)_{i \geq 0}$ be a perfect sequence of period n and $n' = n+1$. Then the $n' \times n'$ -Matrix A defined by*

$$A := \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & (-1)^{a_0} & (-1)^{a_1} & (-1)^{a_2} & \cdots & (-1)^{a_{n-1}} \\ 1 & (-1)^{a_1} & (-1)^{a_2} & (-1)^{a_3} & \cdots & (-1)^{a_0} \\ 1 & (-1)^{a_2} & (-1)^{a_3} & (-1)^{a_4} & \cdots & (-1)^{a_1} \\ \vdots & \vdots & & & \ddots & \vdots \\ 1 & (-1)^{a_{n-1}} & (-1)^{a_0} & (-1)^{a_2} & \cdots & (-1)^{a_{n-2}} \end{pmatrix}$$

is a Hadamard matrix.

Note, that A is the matrix, which is obtained by extending B with all-one first column and row.

Proof. Let $v = (1, \dots, 1)$ of length n' and $\langle \cdot, \cdot \rangle$ denote the inner product. We have $(AA^T)_{0,0} = \langle v, v \rangle = n'$ and $(AA^T)_{i,j} = 1 + \sum_{t=0}^{n-1} (-1)^{a_t} = 0$ if either i or j is 0, since \underline{a} satisfies (1.2). For $i, j = 1, \dots, n-1$ we get

$$(AA^T)_{i,j} = 1 + c_0(\underline{a}^{[i]}, \underline{a}^{[j]}) = 1 + c_{j-i}(\underline{a}) = \begin{cases} n' & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

since \underline{a} is perfect. Indeed, $AA^T = n'I$. □

Chapter 2

Perfect Sequences

2.1 Known Perfect Sequences

Let $G = \langle g \rangle$ be a cyclic group of order n . In Section 1.2, we have shown that binary sequences of period n correspond to sets $D \subseteq G$ by

$$\underline{a}_D := seq(D).$$

We are now going to describe the known constructions for perfect sequences in terms of their corresponding sets, which are Paley type difference sets. In general, the constructions produce inequivalent perfect sequences.

Let $n = ef + 1$ be prime power and let z be a primitive element in \mathbb{F}_n^* . The **cyclotomic classes** are defined by

$$C_i^{(e)} := \{z^j \mid j \equiv i \pmod{e}\}. \quad (2.1)$$

Let $n = 4m - 1$. From number theory three constructions are known for perfect sequences [34]:

- (a) **Legendre Sequences (Paley [33], 1933)**: Let n be a prime and $G = (\mathbb{Z}_n, +)$. The Legendre sequence \underline{a}_D is formed by the non-zero quadratic residue

$$D := G \setminus C_0^{(2)}.$$

- (b) **Hall Sequences (Hall [12], 1957)**: Let $n = 4t^2 + 27$ be a prime and $G = (\mathbb{Z}_n, +)$. The Hall (sextic residue) sequence \underline{a}_D is defined by

$$D := G \setminus (C_0^{(6)} \cup C_1^{(6)} \cup C_3^{(6)}).$$

- (c) **Twin Prime Sequence (Sprott and Stanton [39], 1958)**: Let p and $p+2$ be odd primes, $n = p(p+2)$ and $G = (\mathbb{Z}_p \times \mathbb{Z}_{p+2}, +)$. The twin prime sequence \underline{a}_D is defined by

$$D := G \setminus \{(x, y) \mid x, y \text{ are both non-zero squares or } x, y \text{ both are non-squares or } y = 0\}.$$

Let $n = 2^m - 1$, then \mathbb{Z}_n is isomorphic to $\mathbb{F}_{2^m}^*$. In the following, let $G = \mathbb{F}_{2^m}^*$, then:

- (1) **m -Sequences (Singer [38], 1938)**

Let tr be the trace function on \mathbb{F}_{2^m} . The sequence \underline{a}_D defined by

$$D := \{x \in \mathbb{F}_{2^m}^* \mid tr(x) = 1\}$$

is called maximal length linear shift register sequence (m -sequence).

- (2) **GMW-Sequences (Gordon, Mills & Welch [11], 1962)**

Let $m = rs$ and let f be a perfect function on \mathbb{F}_{2^s} . The sequence \underline{a}_D defined by

$$D := \{x \in \mathbb{F}_{2^m}^* \mid f(tr_{rs/s}(x)) = 1\}$$

is called GMW-sequence.

- (3) **Maschietti Sequences (Maschietti [28], 1998)**

Let $k < m$ be integers such that $\gcd(k, 2^m - 1) = 1$ and $x \mapsto x + x^k$ is a 2-to-1 mapping on \mathbb{F}_{2^m} . The sequence \underline{a}_{D_k} defined by

$$D_k := \mathbb{F}_{2^m}^* \setminus \{x + x^k \mid x \in \mathbb{F}_{2^m}^*\}$$

is called Maschietti sequence.

- (4) **NCY-Sequences (No, Chung & Yun [30], 1998)**

Let $m = 3k \pm 1$ and $d := 2^{2k} - 2^k + 1$. The sequence \underline{a}_D with

$$D := \{(x+1)^d + x^d \mid x \in \mathbb{F}_{2^m}^*\}$$

is called a No-Chung-Yun sequence (NCY-sequence).

- (5) **DD-Sequences (Dillon & Dobbertin [5], 1999)**

Let $k < m$ be integers such that $\gcd(k, m) = 1$ and let $d := 2^{2k} - 2^k + 1$. The sequence \underline{a}_{D_k} with

$$D_k := \mathbb{F}_{2^m}^* \setminus \{(x+1)^d + x^d + 1 \mid x \in \mathbb{F}_{2^m}^*\}$$

is called a Dillon-Dobbertin sequence (DD-sequence).

Note that we get from every construction above a whole class of perfect sequences by equivalence. In the following, if we talk about the crosscorrelation for example between Hall and Legendre sequences, then we mean also the crosscorrelation of their decimations. In particular, if we say that we look at the crosscorrelation between Hall sequences, then we mean the crosscorrelation between the Hall sequence with its decimations.

Some comments are in order:

The Singer construction is the classical construction for perfect sequences. In the literature, m -sequences are also known as pseudorandom sequences or as pseudonoise sequences. A decimation $tr^{(d)}$ with $\gcd(d, 2^m - 1) = 1$ describes an m -sequence, too, since the decimation d only changes the choice of the primitive element. We call all functions f with $f(x) = tr(\beta x^d)$ **m -functions**, if $\beta \in \mathbb{F}_{2^m}^*$ and $\gcd(d, 2^m - 1) = 1$.

If $f \equiv tr_{s/1}^{(2^i)}$ for some i , then the GMW-sequence reduces to an m -sequence. For $f = tr^{(d)}$ with $\gcd(d, 2^s - 1) = 1$ the resulting sequences are the so called classical GMW-sequences.

For the Maschietti's construction, up to equivalence the following k are known, for which $x \mapsto x + x^k$ is a 2-to-1 mapping: $k = 2$ (Singer), $k = 6$ (Segre [36]) and $k = 3 \cdot 2^{\frac{m+1}{2}} + 4$ and $k = 2^{\frac{m+1}{2}} + 2^t$ with $4t \equiv 1 \pmod{m}$ (Glynn [7]). It is an open conjecture, whether this list of k 's is already complete. Furthermore note, that the Singer sequence is identical to an m -sequence and the Segre sequence is identical to the Dillon-Dobbertin sequence with $k = 2$, see [5].

The Dillon-Dobbertin construction differs from the No-Chung-Yun construction just by adding 1. Note that adding 1 is an operation in the additive group of \mathbb{F}_{2^m} , but D_k is considered as a subset in the multiplicative group of \mathbb{F}_{2^m} . This makes the difference in the number of inequivalent perfect sequences obtained from these constructions: According to k with $\gcd(k, m) = 1$, there exists $\frac{\phi(m)}{2}$ inequivalent Dillon-Dobbertin sequences, where ϕ is the Euler-totient function. If $k = 1$ the Dillon-Dobbertin sequence is identical to an m -sequence.

Up to equivalence for fixed m , the No-Chung-Yun construction produces one perfect sequence and the Maschietti produces at most four different sequences. For the GMW construction, the more prime divisors m has, the more inequivalent perfect sequences are obtained. For the Dillon-Dobbertin construction, it is just the opposite; the less prime divisors m has, the more inequivalent perfect sequences are obtained.

Today, there are no sporadic examples of perfect sequences (for $m \leq 11$ and $n = 2^m - 1$ a complete computer search was done), i.e. every known perfect sequence belongs to a series given by any of the constructions above. It is not

known if other perfect sequences exist, which are inequivalent to the known ones.

2.2 Gordon-Mills-Welch Method

Relative difference sets are important for constructions of perfect sequences. The next theorem shows how to get new (relative) difference sets from given (relative) difference sets.

Theorem 2.1 (Gordon-Mills-Welch Method) *Let G be a group of order n and $n'|n$ and $n''|n'$. Let N be a subgroup of G of order n' and N' be a subgroup of N of order n'' . Moreover, let D be an $(n/n', n', k, 0, \lambda)$ -relative difference in G with the forbidden subgroup N and let D' an $(n'/n'', n'', k', 0, \lambda')$ -relative difference set in N with $\lambda'k = \lambda k'^2$. Then the set E defined by the group ring element $E := DD'$ is an $(n/n'', n'', kk', 0, \lambda'k)$ -relative difference set in G .*

Proof. We identify D and D' with elements in the group ring $\mathbb{C}[G]$, see Section 1.2. Note, that $DD' = \sum_{g \in D} \sum_{h \in D'} gh = \sum_{g \in G} \lambda_g g$, where $\lambda_g \in \{0, 1\}$. Assume, that there exists $g, g' \in D$ and $h, h' \in D'$ such that $gh = g'h'$. Since $D' \subset N$ we get $g'g^{-1} = hh'^{-1} \in N$. The set N is the forbidden subgroup of the difference set D , hence $g'g^{-1}$ is the identity in G , thus $g = g'$. This implies $\lambda_g \in \{0, 1\}$ for all $g \in G$ and $|E| = |D| \cdot |D'| = kk'$.

Using the notation in Section 1.3, we get

$$\begin{aligned}
EE^{(-1)} &= DD'(DD')^{(-1)} \\
&= (DD^{(-1)})(D'D'^{(-1)}) \\
&\stackrel{(1.12)}{=} \left(k + \lambda \sum_{g \in G \setminus N} g\right) \left(k' + \lambda' \sum_{h \in N \setminus N'} h\right) \\
&= k'k + \lambda'k \sum_{h \in N \setminus N'} h + k'\lambda \sum_{g \in G \setminus N} g + \lambda\lambda' \sum_{h \in N \setminus N'} \sum_{g \in G \setminus N} hg \\
&= kk' + \lambda'k \sum_{h \in N \setminus N'} h + \left(k'\lambda + \lambda\lambda'(n' - n'')\right) \sum_{g' \in G \setminus N} g'.
\end{aligned}$$

The last step follows, since $hg \in G \setminus N$ holds for all $h \in N \setminus N'$ and $g \in G \setminus N$ and for fix elements $g' \in G \setminus N$ and $h \in N \setminus N'$ exists one element $g \in G \setminus N$ such that $hg = g'$, hence any element g' in $G \setminus N$ has $|N \setminus N'| = n' - n''$ such presentations.

Since D' is a relative difference set, it follows easily (double counting) that $\lambda'(n' - n'') = k'(k' - 1)$. Thus, $k'\lambda + \lambda\lambda'(n' - n'') = k'\lambda + \lambda k'(k' - 1) = \lambda k'^2$. Using our assumption we get

$$EE^{(-1)} = kk' + \lambda'k \sum_{h \in N \setminus N'} h + \lambda'k \sum_{g \in G \setminus N} g = kk' + \lambda'k \sum_{g \in G \setminus N} g.$$

Equation (1.12) shows that E is an $(n/n'', n'', kk', 0, \lambda'k)$ -divisible difference set, and therefore a relative difference set. \square

The only known relative Singer type difference sets are equivalent to sets given by the next proposition and applying iterative the Gordon-Mills-Welch method to such sets.

Proposition 2.2 (Relative Singer difference sets) *Let $m = rs$ and let $tr_{m/s}$ be the trace function from \mathbb{F}_{2^m} to \mathbb{F}_{2^s} . The set D defined by*

$$D := \{x \in \mathbb{F}_{2^m}^* \mid tr_{m/s}(x) = 1\}$$

is an $((2^m - 1)/(2^s - 1), 2^s - 1, 2^{m-s}, 0, 2^{m-2s})$ -relative difference set in $\mathbb{F}_{2^m}^$ with the forbidden subgroup $\mathbb{F}_{2^s}^*$.*

Proof. We have $|D| = 2^{m-s}$, since $tr_{m/s}$ is linear and the dimension of the kernel is 2^{m-s} . Let

$$DD^{(-1)} = \sum_{x \in D} \sum_{y \in D} xy^{-1} = \sum_{z \in \mathbb{F}_{2^m}^*} \lambda_z z.$$

If $z = 1$, then $\lambda_1 = 2^{m-s}$, since $xy^{-1} = 1$ for $|D| = 2^{m-s}$ times. If $z \in \mathbb{F}_{2^s}^* \setminus \{1\}$, then $\lambda_z = 0$. Assume $xy^{-1} = z$ for some $x, y \in D$, then $1 = tr_{m/s}(x) = tr_{m/s}(zy) = z \cdot tr_{m/s}(y) = z$, which is a contradiction. Now, let $z \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*$, then $\lambda_z = 2^{m-2s}$, since $tr_{m/s}$ is a linear function and the dimension of its kernel is 2^{m-s} , i.e.

$$\begin{aligned} & |\{y \in D \mid tr_{m/s}(y) = 1 = tr_{m/s}(zy)\}| = \\ & = 2^{-s} |\{y \in \mathbb{F}_{2^m} \mid tr_{m/s}(y) = tr_{m/s}(zy)\}| \\ & = 2^{-s} |\{y \in \mathbb{F}_{2^m} \mid tr_{m/s}((z+1)y) = 0\}| \\ & = 2^{m-2s}. \end{aligned}$$

Finally we have

$$DD^{(-1)} = 2^{m-s} + 2^{m-2s} \sum_{x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} x,$$

thus, D is a relative difference sets with parameters $((2^m - 1)/(2^s - 1), 2^s - 1, 2^{m-s}, 0, 2^{m-2s})$. \square

Example 2.3 *Let $\underline{a} = (110100010000000)$ and $\underline{b} = (110)(= (b_0, b_1, b_2))$. Then \underline{a} correspond to an $(15/3, 3, 4, 0, 2)$ -relative difference set D and \underline{b} to an $(3, 2, 1)$ -difference set D' . We get by the Gordon-Mills-Welch method:*

$$\begin{array}{r|cccccccccccccc}
& b_0 \cdot \underline{a}^{[0]} & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
+ & b_1 \cdot \underline{a}^{[5]} & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
+ & b_2 \cdot \underline{a}^{[10]} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
\underline{c} & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{array}$$

The sequence \underline{c} correspond to DD' , which is an $(15, 8, 4)$ -difference set, thus \underline{c} is perfect. We see that the Gordon-Mills-Welch method "increases" the sequence \underline{a} using the smaller perfect sequence \underline{b} such that the resulting sequence is perfect.

Chapter 3

Properties of the Crosscorrelation Function

In this chapter, we introduce two slightly modified autocorrelation and crosscorrelation definitions. For the first definition, we get that the modified crosscorrelation coefficient sequence has special autocorrelation properties. Using the second definition a lower bound for the maximum crosscorrelation coefficient $c_t(\underline{a}, \underline{b})$ between perfect sequences is shown.

In the following it is always assumed that a balanced and therefore a perfect sequence satisfies (1.2). We denote by

$$w(\underline{a}) := \sum_{i=0}^{n-1} (-1)^{a_i}$$

the difference between the numbers of 0's and 1's in one period of \underline{a} . Note, that equivalent sequences have the same difference. Using (1.2) we get for balanced and therefore for perfect sequences \underline{a} that $w(\underline{a}) = -1$. In general, we have

$$\sum_{t=0}^{n-1} c_t(\underline{a}, \underline{b}) = \sum_{t=0}^{n-1} \sum_{i=0}^{n-1} (-1)^{a_i + b_{i+t}} = \sum_{i=0}^{n-1} (-1)^{a_i} \sum_{t=0}^{n-1} (-1)^{b_{i+t}} = w(\underline{a})w(\underline{b})$$

and therefore follows

$$\sum_{t=0}^{n-1} c_t(\underline{a}) = w(\underline{a})^2 \quad \text{and} \quad \sum_{t=0}^{n-1} c_t(\underline{a}, \underline{b}) = -w(\underline{a}) \quad (3.1)$$

for a balanced (resp. perfect) sequence \underline{b} . Thus, $w(\underline{a})$ is unique defined by the crosscorrelation coefficients between \underline{a} and a perfect sequence \underline{b} .

3.1 Dual Sequence

We define a modified autocorrelation and crosscorrelation function for binary sequences \underline{a} and \underline{b} of period n by

$$c'_t(\underline{a}) := c_t(\underline{a}) + w(\underline{a})^2 \quad \text{and} \quad c'_t(\underline{a}, \underline{b}) := c_t(\underline{a}, \underline{b}) + w(\underline{a})w(\underline{b})$$

for all $t = 0, \dots, n-1$, respectively. Note that

$$\sum_{t=0}^{n-1} c'_t(\underline{a}) = (n+1)w(\underline{a})^2 \quad \text{and} \quad \sum_{t=0}^{n-1} c'_t(\underline{a}, \underline{b}) = -(n+1)w(\underline{a}) \quad (3.2)$$

for a balanced (resp. perfect) sequence \underline{b} . Thus, two sequences have the same autocorrelation if and only if they have the same modified autocorrelation. Furthermore, $w(\underline{a})$ is uniquely defined by the modified crosscorrelation coefficients $c'_t(\underline{a}, \underline{b})$ between \underline{a} and a perfect sequence \underline{b} . Let $Sp'(\underline{a}, \underline{b}) := \{c'_t(\underline{a}, \underline{b}) | t = 0, \dots, n-1\}$ and $Sp'(\underline{a}) := Sp'(\underline{a}, \underline{a})$ denote the modified crosscorrelation and autocorrelation spectrum. If \underline{a} and \underline{b} are balanced, using (1.2) we simply get

$$c'_t(\underline{a}) = c_t(\underline{a}) + 1 \quad \text{and} \quad c'_t(\underline{a}, \underline{b}) = c_t(\underline{a}, \underline{b}) + 1. \quad (3.3)$$

For a perfect sequence \underline{a} we have

$$c'_t(\underline{a}) = \begin{cases} 0 & \text{if } t \not\equiv 0 \pmod{n} \\ n+1 & \text{if } t \equiv 0 \pmod{n}. \end{cases} \quad (3.4)$$

The next proposition gives the inversion formula of the modified crosscorrelation function. This shows that a sequence \underline{a} is uniquely defined by a perfect sequence \underline{d} and their crosscorrelation coefficients $c'_t(\underline{a}, \underline{d})$. Since (3.2) holds, the next proposition implies that a sequence \underline{a} is uniquely defined by a perfect sequence \underline{d} and their crosscorrelation coefficients $c_t(\underline{a}, \underline{d})$.

Proposition 3.1 *Let $\underline{a} = (a_i)_{i \geq 0}$ and $\underline{d} = (d_i)_{i \geq 0}$ be binary sequences of period n and \underline{d} be perfect. Then*

$$(-1)^{a_t} = \frac{1}{n+1} \left(\sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d}) (-1)^{d_{k+t}} \right). \quad (3.5)$$

Proof. Simple transformations of the right hand side of equation (3.5) yield

$$\sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d}) (-1)^{d_{k+t}} = \sum_{k=0}^{n-1} (c_k(\underline{a}, \underline{d}) + \underbrace{w(\underline{a})w(\underline{d})}_{=-1}) (-1)^{d_{k+t}}$$

$$\begin{aligned}
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} (-1)^{a_i+d_{i+k}+d_{k+t}} - w(\underline{a}) \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{k+t}}}_{=w(\underline{d})=-1} \\
&= \sum_{i=0}^{n-1} (-1)^{a_i} \underbrace{\left(\sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{k+t}} + 1 \right)}_{\stackrel{(3.3)}{=}c'_{t-i}(\underline{d})} - w(\underline{a}) + w(\underline{a}) \\
&\stackrel{(3.4)}{=} (n+1) \cdot (-1)^{at},
\end{aligned}$$

since \underline{d} is perfect. □

Let \underline{d} be a perfect sequence. The real sequence $\underline{a}^{\underline{d}} = (a_i^{\underline{d}})_{i \geq 0}$ defined by

$$a_i^{\underline{d}} := c'_i(\underline{a}, \underline{d})$$

is called the **dual sequence** of \underline{a} with respect to \underline{d} . The next proposition shows the connection between the crosscorrelation between two sequences \underline{a} and \underline{b} and the crosscorrelation between their dual sequences with respect to the same perfect sequence.

Proposition 3.2 (Duality) *Let $\underline{a}, \underline{b}$ and \underline{d} be binary sequences of period n and \underline{d} be perfect. Then*

$$c'_t(\underline{a}, \underline{b}) = \frac{1}{n+1} \left(\sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d}) c'_{k-t}(\underline{b}, \underline{d}) \right) \quad (3.6)$$

holds for all $t = 0, \dots, n-1$.

Proof. Let $\underline{a} = (a_i)_{i \geq 0}$, $\underline{b} = (b_i)_{i \geq 0}$ and $\underline{d} = (d_i)_{i \geq 0}$. We expand

$$\begin{aligned}
&\sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d}) c'_{k-t}(\underline{b}, \underline{d}) \\
&= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} (-1)^{a_i+d_{i+k}} + \underbrace{w(\underline{a}) w(\underline{d})}_{=-1} \right) \cdot \left(\sum_{j=0}^{n-1} (-1)^{b_j+d_{j+k-t}} + \underbrace{w(\underline{b}) w(\underline{d})}_{=-1} \right) \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} \sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{j+k-t}} \\
&\quad - w(\underline{b}) \underbrace{\sum_{i=0}^{n-1} (-1)^{a_i}}_{=w(\underline{a})} \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{i+k}}}_{=w(\underline{d})=-1} - w(\underline{a}) \underbrace{\sum_{i=0}^{n-1} (-1)^{b_i}}_{=w(\underline{b})} \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{i+k-t}}}_{=w(\underline{d})=-1} + \sum_{k=0}^{n-1} w(\underline{a}) w(\underline{b}) \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} \sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{j+k-t}} + (n+2)w(\underline{a})w(\underline{b})
\end{aligned}$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} \underbrace{\left(\sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{j+k-t}} + 1 \right)}_{\stackrel{(3.3)}{=} c'_{j-t-i}(\underline{d})} + (n+1)w(\underline{a})w(\underline{b}).$$

Using (3.4) we get

$$\begin{aligned} \sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d}) c'_{k-t}(\underline{b}, \underline{d}) &= (n+1) \sum_{i=0}^{n-1} (-1)^{a_i+b_{i+t}} + (n+1)w(\underline{a})w(\underline{b}) \\ &= (n+1)c'_t(\underline{a}, \underline{b}). \end{aligned}$$

□

Corollary 3.3 *Let \underline{a} and \underline{d} be binary sequences of period n and \underline{d} be perfect. Then*

$$c'_t(\underline{a}) = \frac{1}{n+1} C_t(\underline{a}^{\underline{d}}) \quad (3.7)$$

holds for all $t = 0, \dots, n-1$. In particular, $Sp'(\underline{a})$ is two-valued if and only if $\{C_t(\underline{a}^{\underline{d}}) | t = 0, \dots, n-1\}$ is two-valued.

Proof. Proposition 3.2 shows that $(n+1)c'_t(\underline{a}, \underline{b}) = C_{-t}(\underline{a}^{\underline{d}}, \underline{b}^{\underline{d}})$ holds for all t . Thus, the autocorrelation of a sequence \underline{a} and the autocorrelation of its dual sequences $\underline{a}^{\underline{d}}$ is equal up to the factor $n+1$, since $(n+1)c'_t(\underline{a}) = C_{-t}(\underline{a}^{\underline{d}}) = C_t(\underline{a}^{\underline{d}})$. □

Three-valued Crosscorrelation Spectra and Ternary Sequences

It is interesting to search for crosscorrelation spectra, which contain only a few different values. Crosscorrelation spectra of the form $\{\pm c, 0\}$ play an important role. More precisely, let \underline{a} and \underline{d} be binary sequences and \underline{d} be perfect. Furthermore, let the crosscorrelation spectrum $Sp'(\underline{a}, \underline{d})$ be three-valued with $\pm c$ and 0. Then the ternary sequence $\underline{b} = (b_i)_{i \geq 0}$ obtained from the dual sequence $\underline{a}^{\underline{d}}$ by

$$b_i := \frac{c'_i(\underline{a}, \underline{d})}{c}$$

has also special autocorrelation property

$$C_i(\underline{b}) = \frac{n+1}{c^2} c'_i(\underline{a}),$$

since \underline{d} is perfect [37]. Thus, \underline{b} has a two-level autocorrelation spectrum if \underline{a} has a two-valued autocorrelation spectrum.

3.2 Lower Bounds

In this section, we search for a lower bound for the maximum crosscorrelation coefficient $c_t(\underline{a}, \underline{b})$. Motivated by formula (3.3) we define a slight modified auto-correlation of \underline{a} and crosscorrelation between \underline{a} and \underline{b} by

$$c_t^*(\underline{a}) := c_t(\underline{a}) + 1 \quad \text{and} \quad c_t^*(\underline{a}, \underline{b}) := c_t(\underline{a}, \underline{b}) + 1$$

for all $t = 0, \dots, n-1$, respectively, and $w^*(\underline{a}) := w(\underline{a}) + 1$. Note that for perfect sequences the definitions of $c'_t()$ and $c_t^*()$ are identical. Let $Sp^*(\underline{a}, \underline{b}) := \{c_t^*(\underline{a}, \underline{b}) | t = 0, \dots, n-1\}$ and $Sp^*(\underline{a}) := Sp^*(\underline{a}, \underline{a})$ denote the modified crosscorrelation and autocorrelation spectrum. Using (1.2) we get analogically to (3.4) that a perfect sequence \underline{a} yields

$$c_t^*(\underline{a}) = \begin{cases} 0 & \text{if } t \not\equiv 0 \pmod{n} \\ n+1 & \text{if } t \equiv 0 \pmod{n}, \end{cases} \quad (3.8)$$

since $c'_t(\underline{a}) = c_t^*(\underline{a})$ holds for a perfect sequence.

The next two propositions are well-known for sequences defined over finite fields of characteristic 2: Let \underline{a} and \underline{b} be sequences of period $n = 2^m - 1$ and f and g their corresponding functions with $f(0) = g(0) = 0$ using the primitive element α , then $c_t^*(\underline{a}, \underline{b}) = c_{\alpha^t}(f, g)$.

At first we see that a sequence \underline{a} is also unique defined by a perfect sequence \underline{d} and their crosscorrelation coefficients $c_t^*(\underline{a}, \underline{d})$, since $w(\underline{a})$ and therefore $w^*(\underline{a})$ is uniquely defined by the crosscorrelation coefficient with a perfect sequence by (3.1).

Proposition 3.4 *Let $\underline{a} = (a_i)_{i \geq 0}$ and $\underline{d} = (d_i)_{i \geq 0}$ be binary sequences of period n and \underline{d} be perfect. Then*

$$(-1)^{a_t} = \frac{1}{n+1} \left(\sum_{k=0}^{n-1} c_k^*(\underline{a}, \underline{d}) (-1)^{d_{k+t}} + w^*(\underline{a}) \right). \quad (3.9)$$

Proof. We simply transform the right hand side of equation (3.9) and we get

$$\begin{aligned} \sum_{k=0}^{n-1} c_k^*(\underline{a}, \underline{d}) (-1)^{d_{k+t}} &= \sum_{k=0}^{n-1} (c_k(\underline{a}, \underline{d}) + 1) (-1)^{d_{k+t}} \\ &= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} (-1)^{a_i + d_{i+k} + d_{k+t}} + \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{k+t}}}_{=-1} \end{aligned}$$

$$\begin{aligned}
&= \sum_{i=0}^{n-1} (-1)^{a_i} \underbrace{\left(\sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{k+t}} + 1 \right)}_{=c_{t-i}^*(\underline{d})} - \sum_{j=0}^{n-1} (-1)^{a_j} - 1 \\
&\stackrel{(3.8)}{=} (n+1) \cdot (-1)^{a_t} - w^*(\underline{a}),
\end{aligned}$$

since \underline{d} is perfect. □

Proposition 3.5 (Generalised Parseval formula) *Let $\underline{a}, \underline{b}$ and \underline{d} be binary sequences of period n and \underline{d} be perfect. Then*

$$c_t^*(\underline{a}, \underline{b}) = \frac{1}{n+1} \left(\sum_{k=0}^{n-1} c_k^*(\underline{a}, \underline{d}) c_{k-t}^*(\underline{b}, \underline{d}) + w^*(\underline{a}) w^*(\underline{b}) \right). \quad (3.10)$$

Proof. Let $\underline{a} = (a_i)_{i \geq 0}$, $\underline{b} = (b_i)_{i \geq 0}$ and $\underline{d} = (d_i)_{i \geq 0}$. We expand

$$\begin{aligned}
&\sum_{k=0}^{n-1} c_k^*(\underline{a}, \underline{d}) c_{k-t}^*(\underline{b}, \underline{d}) \\
&= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} (-1)^{a_i+d_{i+k}} + 1 \right) \cdot \left(\sum_{j=0}^{n-1} (-1)^{b_j+d_{j+k-t}} + 1 \right) \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} \sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{j+k-t}} \\
&\quad + \sum_{i=0}^{n-1} (-1)^{a_i} \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{i+k}}}_{=-1} + \sum_{j=0}^{n-1} (-1)^{b_j} \underbrace{\sum_{k=0}^{n-1} (-1)^{d_{j+k-t}}}_{=-1} + n \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} \underbrace{\left(\sum_{k=0}^{n-1} (-1)^{d_{i+k}+d_{j+k-t}} + 1 \right)}_{=c_{j-t-i}^*(\underline{d})} + n + 1 \\
&\quad - \left(\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{a_i+b_j} + \sum_{i=0}^{n-1} (-1)^{a_i} + \sum_{j=0}^{n-1} (-1)^{b_j} + 1 \right),
\end{aligned}$$

where we insert $0 = \sum_{i,j=0}^{n-1} (-1)^{a_i+b_j} + 1 - (\sum_{i,j=0}^{n-1} (-1)^{a_i+b_j} + 1)$. Since \underline{d} is perfect we get

$$\begin{aligned}
&\sum_{k=0}^{n-1} c_k^*(\underline{a}, \underline{d}) c_{k-t}^*(\underline{b}, \underline{d}) \\
&= (n+1) \left(\sum_{i=0}^{n-1} (-1)^{a_i+b_{i+t}} + 1 \right) - \left(\sum_{i=0}^{n-1} (-1)^{a_i} + 1 \right) \left(\sum_{j=0}^{n-1} (-1)^{b_j} + 1 \right) \\
&= (n+1) c_t^*(\underline{a}, \underline{b}) - w^*(\underline{a}) w^*(\underline{b}).
\end{aligned}$$

□

Some basic properties of the crosscorrelation function between binary sequences are summarised:

Proposition 3.6 *Let \underline{a} and \underline{b} be binary sequences of period n and let d be an integer such that $\gcd(d, n) = 1$.*

(1) *It is $c_t^*(\underline{a}^{(d)}, \underline{b}) = c_{dt}^*(\underline{a}, \underline{b}^{(1/d)})$ and $c_t^*(\underline{a}, \underline{b}) = c_{-t}^*(\underline{b}, \underline{a})$.*

(2) *If d is a multiplier of \underline{a} , then $Sp^*(\underline{a}^{(d)}, \underline{b}) = Sp^*(\underline{a}, \underline{b})$.*

(3) *If \underline{b} is perfect, then*

$$\sum_{t=0}^{n-1} c_t^*(\underline{a}, \underline{b}) = (n+1) - w^*(\underline{a}).$$

(4) *If \underline{b} is perfect, then*

$$\sum_{t=0}^{n-1} (c_t^*(\underline{a}, \underline{b}))^2 = (n+1)^2 - w^*(\underline{a})^2.$$

(5) *If \underline{a} and \underline{b} are perfect, then*

$$\sum_{t=0}^{n-1} c_t^*(\underline{a}, \underline{b})c_{t+k}^*(\underline{a}, \underline{b}) = \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod{n} \\ (n+1)^2 & \text{if } k \equiv 0 \pmod{n}. \end{cases}$$

Proof: Let $\underline{a} = (a_i)_{i \geq 0}$ and $\underline{b} = (b_i)_{i \geq 0}$.

(1) Since $\gcd(d, n) = 1$ the integer d is invertible modulo n . We have

$$c_t^*(\underline{a}^{(d)}, \underline{b}) = \sum_{i=0}^{n-1} (-1)^{a_{di} + b_{i+t}} + 1 = \sum_{i=0}^{n-1} (-1)^{a_i + b_{(i+dt)/d}} + 1 = c_{dt}^*(\underline{a}, \underline{b}^{(1/d)}).$$

Trivially we have

$$c_t^*(\underline{a}, \underline{b}) = \sum_{i=0}^{n-1} (-1)^{a_i + b_{i+t}} + 1 = \sum_{i=0}^{n-1} (-1)^{b_i + a_{i-t}} + 1 = c_{-t}^*(\underline{b}, \underline{a}).$$

(2) Since d is a multiplier, we have $a_{di} = a_{i+k}$ for some k and

$$c_t^*(\underline{a}^{(d)}, \underline{b}) = \sum_{i=0}^{n-1} (-1)^{a_{di} + b_{i+t}} + 1 = \sum_{i=0}^{n-1} (-1)^{a_{i+k} + b_{i+t}} + 1 = c_{t-k}^*(\underline{a}, \underline{b}).$$

(3) Since \underline{b} is perfect, we get

$$\begin{aligned} \sum_{t=0}^{n-1} c_t^*(\underline{a}, \underline{b}) &= \sum_{t=0}^{n-1} \left(\sum_{i=0}^{n-1} (-1)^{a_i + b_{i+t}} + 1 \right) \\ &= \sum_{i=0}^{n-1} (-1)^{a_i} \underbrace{\sum_{t=0}^{n-1} (-1)^{b_{i+t}}}_{=-1} + n \\ &= n + 1 - w^*(\underline{a}). \end{aligned}$$

(4) Since \underline{b} is perfect, the generalised Parseval formula shows

$$\sum_{t=0}^{n-1} (c_t^*(\underline{a}, \underline{b}))^2 \stackrel{(3.10)}{=} (n+1)c_0^*(\underline{a}, \underline{a}) - w^*(\underline{a})^2 = (n+1)^2 - w^*(\underline{a})^2.$$

(5) Since \underline{a} and \underline{b} are perfect, using the generalised Parseval formula we have

$$\begin{aligned} \sum_{t=0}^{n-1} c_t^*(\underline{a}, \underline{b})c_{t+k}^*(\underline{a}, \underline{b}) &\stackrel{(3.10)}{=} (n+1)c_{-k}^*(\underline{a}, \underline{a}) - w^*(\underline{a})^2 \\ &\stackrel{(3.8)}{=} \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod{n} \\ (n+1)^2 & \text{if } k \equiv 0 \pmod{n}. \end{cases} \end{aligned}$$

□

Lower Bound for the Maximal Crosscorrelation Coefficient

We are interested in perfect sequences \underline{a} and \underline{b} , for which the Hamming distance $d_H(\underline{a}, \underline{b}^{[t]})$ and $d_H(\underline{a}, \bar{\underline{b}}^{[t]})$ are as large as possible for all $t = 0, \dots, n-1$. It is easy to see that $d_H(\underline{a}, \underline{b}) = n - d_H(\underline{a}, \bar{\underline{b}})$.

For two binary sequences \underline{a} and \underline{b} with period n , it follows that $c_t(\underline{a}, \underline{b}) = n - 2d_H(\underline{a}, \underline{b}^{[t]})$ and $c_t(\underline{a}, \bar{\underline{b}}) = n - 2d_H(\underline{a}, \bar{\underline{b}}^{[t]}) = -(n - 2d_H(\underline{a}, \underline{b}^{[t]}))$ holds for all $t = 0, \dots, n-1$. Hence we try to find sequences \underline{a} and \underline{b} such that

$$\mathcal{M}(\underline{a}, \underline{b}) := \max_{t \in \{0, \dots, n-1\}} |c_t(\underline{a}, \underline{b}) + 1|$$

is as small as possible. In $\mathcal{M}(\cdot, \cdot)$ we add a one only for a better handling: We can use the definition $c_t^*(\cdot, \cdot)$ and the properties listed in Proposition 3.6. The maximal crosscorrelation coefficient (in absolute value) is a measure for how much \underline{a} can be used to approximate \underline{b} . We are interested in a lower bound for the maximum crosscorrelation coefficient between two perfect sequences. The next proposition gives a lower bound for the maximum crosscorrelation coefficient between two binary sequences, if one sequence is perfect.

Theorem 3.7 *Let \underline{a} and \underline{b} be binary sequences of period n and \underline{b} be perfect. Then*

$$\mathcal{M}(\underline{a}, \underline{b}) \geq \sqrt{\frac{(n+1)^2 - w^*(\underline{a})^2}{n}}. \quad (3.11)$$

Proof. We have $\sum_{t=0}^{n-1} (c_t(\underline{a}, \underline{b}) + 1)^2 = (n+1)^2 - w^*(\underline{a})^2$ by (4) in Proposition 3.6. The sum on the left hand side contains n non-negative terms. □

Example 3.8 *Let $\underline{b} = 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \dots$ of period 15, then \underline{b} is perfect. We list two sequences, for which the bound (3.11) is tight.*

Let $\underline{a} = 0, 0, 0, 0, 0, 0, 0, 0, \dots$, then $c_t(\underline{a}, \underline{b}) + 1 = w(\underline{b}) + 1 = 0$ for all t and $w^*(\underline{a}) = n + 1$ and therefore $\mathcal{M}(\underline{a}, \underline{b}) = 0$.

Let $\underline{c} = 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, \dots$, then

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$c_t(\underline{c}, \underline{b})$	-5	3	3	3	-5	3	3	3	-5	3	3	-5	3	3	-5

and $w(\underline{c}) = 15 - 2 \cdot 10 = -5$. Note, that $|c_t(\underline{c}, \underline{b}) + 1| = |w^*(\underline{c})| = \sqrt{n+1} = 4$. The bound (3.11) is tight with $\mathcal{M}(\underline{c}, \underline{b}) = 4$.

The example shows that in general the bound (3.11) is best possible. If we additionally assume that $|w^*(\underline{a})|$ is bounded, then we get a larger bound.

Corollary 3.9 *Let \underline{a} and \underline{b} be binary sequences of period n and let \underline{b} be perfect. If $|w^*(\underline{a})| \leq \sqrt{n+1}$, then*

$$\mathcal{M}(\underline{a}, \underline{b}) \geq \sqrt{n+1}. \quad (3.12)$$

In particular, if \underline{a} is balanced or perfect, then $\mathcal{M}(\underline{a}, \underline{b}) > \sqrt{n+1}$.

Chapter 4

Extended Hadamard Equivalence

New classes of perfect sequences of period $2^m - 1$ have been found in [5] by Dillon and Dobbertin. For this remarkable result, a new type of equivalence between sequences with period $2^m - 1$ has been defined. The powerful tool employed in [5] is the Hadamard equivalence. The fundamental issue is that Hadamard equivalent sequences have the same autocorrelation spectrum. This concept has been generalised by Gong and Golomb [9]. Based on this equivalence, in [9] a method is given to construct new perfect sequences of period $2^m - 1$. All recently discovered perfect sequences of period $2^m - 1$ are Hadamard equivalent to m -sequences, when m is odd. Unfortunately, no new perfect sequences have been found by this method for $m \leq 17$.

In Section 4.1, the concept of Hadamard equivalence is outlined and a generalisation of Hadamard equivalence is introduced to sequences of period $n = 4m - 1$. We call this extended Hadamard equivalence. It turns out that extended Hadamard equivalent sequences have the same autocorrelation spectrum. In Section 4.2, it is proved that the Legendre and the Hall sequences of the same period are extended Hadamard equivalent. The proof also shows that all crosscorrelation coefficient between Hall sequences and between Hall and Legendre sequences are determinate by cyclotomic numbers. We explicitly list all crosscorrelation spectra between these sequences.

4.1 (Extended) Hadamard Equivalence

The crosscorrelation is used to develop a method to construct sequences with specified autocorrelation properties. This method can also be applied to prove that certain sequences are perfect. The basic idea is a generalisation of the Hadamard equivalence introduced in [5]. Hadamard equivalence has been used

for sequences of period $2^m - 1$. The specific feature of sequences with period $2^m - 1$ is that they can be identified with functions $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$, see Section 1.2.

We outline the concept of Hadamard equivalence: Let $f, g, h_1, h_2 : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be functions, $z \in \mathbb{F}_{2^m}^*$ and d be an integer with $\gcd(d, 2^m - 1) = 1$ such that

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x) + h_1(y^d x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{g(x) + h_2(z y x)} \quad (4.1)$$

holds for all $y \in \mathbb{F}_{2^m}$. Then

- [4, 5]: If $h_1 = h_2$ is the trace function, then the functions f and g are called **Hadamard equivalent**. In particular, if f is perfect, then g is perfect, too. Hadamard equivalence is a powerful tool to prove that functions are perfect. The main idea in the proofs given in [4, 5] is, that certain functions are Hadamard equivalent to m -functions.
- [9]: If $h_1 = h_2$ is an arbitrary perfect function, then the functions f and g have the same autocorrelation spectra. In particular, if f is perfect, then g is perfect, too. Using this slight generalisation of Hadamard equivalence, an algorithm for constructing perfect functions is developed. Unfortunately, no new perfect functions have been found for $m \leq 17$.

We generalise the idea of Hadamard equivalence to sequences of period $n = 4m - 1$. We call this extended Hadamard equivalence. Based on this new equivalence, we propose an algorithm to construct perfect sequences of period $n = 4m - 1$.

Two binary sequences \underline{a} and \underline{b} of period $n = 4m - 1$ are called **extended Hadamard equivalent (EH-equivalent)**, if there exist two perfect sequences \underline{d} and \underline{e} and integers s, t with $\gcd(s, n) = 1$ such that

$$c_k(\underline{a}, \underline{d}) = c_{sk+t}(\underline{b}, \underline{e}) \quad (\text{resp. } c_k^*(\underline{a}, \underline{d}) = c_{sk+t}^*(\underline{b}, \underline{e})) \quad (4.2)$$

holds for all k . With (3.1) it follows for EH-equivalent sequences \underline{a} and \underline{b} that $w(\underline{a}) = w(\underline{b})$. Thus, (4.2) is equivalent to

$$c'_k(\underline{a}, \underline{d}) = c'_{sk+t}(\underline{b}, \underline{e}), \quad (4.3)$$

since (3.2) holds. In other words, \underline{a} and \underline{b} are EH-equivalent if and only if there exists perfect sequences \underline{d} and \underline{e} such that the dual sequences $\underline{a}^{\underline{d}}$ and $\underline{b}^{\underline{e}}$ are equivalent, i.e.

$$a_k^{\underline{d}} = b_{sk+t}^{\underline{e}} \quad (4.4)$$

for some integers t and s with $\gcd(s, n) = 1$.

Note that two arbitrary perfect sequences \underline{a} and \underline{b} are EH-equivalent, since (4.2) holds for $\underline{d} := \underline{a}$ and $\underline{e} := \underline{b}$. We call it trivial EH-equivalence, otherwise nontrivial EH-equivalence. In the following if we talk about EH-equivalence we always mean nontrivial EH-equivalence.

Proposition 4.1 *Let \underline{a} and \underline{b} be binary sequences of period $n = 4m - 1$. If \underline{a} and \underline{b} are EH-equivalent, then the autocorrelation spectra of \underline{a} and \underline{b} are equal.*

Proof. If \underline{a} and \underline{b} are EH-equivalent, then there exists two perfect sequences \underline{d} and \underline{e} and integers s, t with $\gcd(s, n) = 1$ such that (4.3) holds. Since $c'_i(\underline{a}) = c'_i(\underline{a}, \underline{a})$, by Proposition 3.2 we get

$$\begin{aligned} (n+1)c'_i(\underline{a}) &= \sum_{k=0}^{n-1} c'_k(\underline{a}, \underline{d})c'_{k-i}(\underline{a}, \underline{d}) \\ &= \sum_{k=0}^{n-1} c'_{sk+t}(\underline{b}, \underline{e})c'_{s(k-i)+t}(\underline{b}, \underline{e}) \\ &= \sum_{k=0}^{n-1} c'_k(\underline{b}, \underline{e})c'_{k-si}(\underline{b}, \underline{e}) \\ &= (n+1)c'_{si}(\underline{b}), \end{aligned}$$

thus, $Sp'(\underline{a}) = Sp'(\underline{b})$. Since $w(\underline{a}) = w(\underline{b})$ holds for EH-equivalent sequences, we get $Sp(\underline{a}) = Sp(\underline{b})$. \square

Let $\underline{a} = (a_i)_{i \geq 0}$, $\underline{d} = (d_i)_{i \geq 0}$ and $\underline{e} = (e_i)_{i \geq 0}$ be binary sequences of period $n = 4m - 1$ and let \underline{d} and \underline{e} be perfect. Let z_1, z_2, z_3 be integers with $\gcd(z_i, n) = 1$, $i = 1, 2, 3$, such that

$$\left(\sum_{k=0}^{n-1} c_{z_2 k}^*(\underline{a}^{(z_1)}, \underline{d}) (-1)^{e_{k+i}^{(z_3)}} + w^*(\underline{a}) \right) \in \{\pm(n+1)\}. \quad (4.5)$$

Then the binary sequence $\underline{b} = (b_i)_{i \geq 0}$ defined by

$$(-1)^{b_i} = \frac{1}{n+1} \left(\sum_{k=0}^{n-1} c_{z_2 k}^*(\underline{a}^{(z_1)}, \underline{d}) (-1)^{e_{k+i}^{(z_3)}} + w^*(\underline{a}) \right) \quad (4.6)$$

is called **realisation** of $\underline{a}, \underline{d}, \underline{e}$ by the triple (z_1, z_2, z_3) .

Theorem 4.2 *Let $\underline{a}, \underline{d}$ and \underline{e} be binary sequences of period $n = 4m - 1$ and let \underline{d} and \underline{e} be perfect. Let z_1, z_2, z_3 be integers with $\gcd(z_i, n) = 1$, $i = 1, 2, 3$, such that (4.5) holds. Then the sequence $\underline{b} = (b_i)_{i \geq 0}$ defined by (4.6) and the sequence \underline{a} have the same autocorrelation spectrum.*

Note that the sequence \underline{b} is uniquely defined by the perfect sequence $\underline{e}^{(z_3)}$ and its crosscorrelation coefficients $c_k^*(\underline{b}, \underline{e}^{(z_3)})$ ($:= c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d})$), see Proposition 3.4.

Proof. We show that the sequences $\underline{a}^{(z_1)}$ and \underline{b} are EH-equivalent. Then the sequences \underline{a} and \underline{b} have the same autocorrelation spectrum, since \underline{a} is equivalent to $\underline{a}^{(z_1)}$. We get

$$\begin{aligned}
& (n+1)c_i(\underline{b}, \underline{e}^{(z_3)}) \\
&= (n+1) \sum_{j=0}^{n-1} (-1)^{b_j + e_{j+i}^{(z_3)}} \\
&= \sum_{j=0}^{n-1} \left(\sum_{k=0}^{n-1} c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d}) (-1)^{e_{k+j}^{(z_3)} + e_{j+i}^{(z_3)}} + w^*(\underline{a}) \right) (-1)^{e_{j+i}^{(z_3)}} \\
&= \sum_{k=0}^{n-1} c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d}) \sum_{j=0}^{n-1} (-1)^{e_{k+j}^{(z_3)} + e_{j+i}^{(z_3)}} + w^*(\underline{a}) \underbrace{\sum_{j=0}^{n-1} (-1)^{e_{j+i}^{(z_3)}}}_{=-1} \\
&= \sum_{k=0}^{n-1} c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d}) \left(\underbrace{\sum_{j=0}^{n-1} (-1)^{e_{k+j}^{(z_3)} + e_{j+i}^{(z_3)}}}_{=c_{i-k}^*(\underline{e}^{(z_3)})} + 1 \right) - \sum_{k=0}^{n-1} c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d}) - w^*(\underline{a}) \\
&= (n+1)c_{z_2i}^*(\underline{a}^{(z_1)}, \underline{d}) - \sum_{k=0}^{n-1} c_{z_2k}^*(\underline{a}^{(z_1)}, \underline{d}) - w^*(\underline{a}),
\end{aligned}$$

since \underline{e} is perfect. Since \underline{d} is perfect, we get from (3) in Proposition 3.6 that $(n+1)c_i(\underline{b}, \underline{e}^{(z_3)}) = (n+1)c_{z_2i}^*(\underline{a}^{(z_1)}, \underline{d}) - (n+1) = (n+1)c_{z_2i}(\underline{a}^{(z_1)}, \underline{d})$. \square

A method to construct sequences with specified autocorrelation properties based on Theorem 4.2 is the following: Take three shift distinct perfect sequences and check for all possible integers $z_i, i = 1, 2, 3$, if a realisation of these sequences exists. The drawback of this algorithm is that three perfect sequences, which are pairwise shift distinct, are needed. If the given sequences are not pairwise shift distinct, then the resulting sequence is a shift of one of the given sequences.

Note that if \underline{b} is a realisation of $\underline{a}, \underline{d}, \underline{e}$ by (z_1, z_2, z_3) , then $\underline{b}^{(1/z_3)}$ is a realisation of $\underline{a}, \underline{d}, \underline{e}$ by $(z_1, z_2/z_3, 1)$, since $c_t(\underline{b}, \underline{e}^{(z_3)}) = c_{z_3t}(\underline{b}^{(1/z_3)}, \underline{e})$. Thus, if we search for a new perfect sequence, which is not equivalent to the known one, without loss of generality we can choose $z_3 = 1$.

In the case $n = 4m - 1$ and m is not a power of 2, there exists at least three (known) shift distinct sequences if $n = 4t^2 + 27$ prime: called Hall and Legendre sequences. Note that for fix prime $n = 4t^2 + 27$ we have six shift distinct Hall sequences and two Legendre sequences. Using Hall and Legendre sequences the algorithm gives no new perfect sequences for $n = 4t^2 + 27$ and $t \leq 77$, but another interesting result is discovered, which is presented in the next section.

In the following we use the notion of EH-equivalence very generously. If we say

for example that the Hall and Legendre sequences are EH-equivalent, then we mean that an equivalent sequence of the Hall sequence is EH-equivalent to an equivalent sequence of the Legendre sequence.

4.2 EH-Equivalence of Legendre and Hall Sequences

Let $n = ef + 1$ be prime. We fix z as a primitive element in \mathbb{Z}_n^* . The cyclotomic classes $C_i^{(e)}$ in \mathbb{Z}_n defined by (2.1) are pairwise disjoint for $i = 0, \dots, e - 1$, and their union is \mathbb{Z}_n^* . Furthermore, $C_{i+ke}^{(e)} = C_i^{(e)}$ for all integers k , thus we consider the indices modulo e .

Let $n = 4t^2 + 27$ be prime. We recall, the Hall sequence $\underline{s}_{QR} := seq(\overline{QR})$ and the Legendre sequence $\underline{s}_H := seq(\overline{H})$ are given by

$$QR := C_0^{(2)} \quad \text{and} \quad H := C_0^{(6)} \cup C_1^{(6)} \cup C_3^{(6)}. \quad (4.7)$$

It is easy to see from the definitions of the sets QR and H , that the sequences \underline{s}_{QR} and \underline{s}_H are not equivalent. Therefore note that every square modulo n is a multiplier of \underline{s}_{QR} and the only multipliers of \underline{s}_H are the sixth powers modulo n . Since z^2 is a multiplier of \underline{s}_{QR} and not of \underline{s}_H , the corresponding sequences cannot be equivalent. The integer z^2 is not a multiplier of \underline{s}_H , because $c_0(\underline{s}_H^{(z^2)}, \underline{s}_H) = -n + 2 + 4|z^{-2}H \cap H| = -(n - 4)/3 \notin \{-1, n\}$ and therefore $\underline{s}_H^{(z^2)}$ cannot be a shift of \underline{s}_H .

Theorem 4.3 *The Hall and Legendre sequences of the same period length are EH-equivalent. More precisely, we have*

$$c_{zk}(\underline{s}_H^{(z)}, \underline{s}_H) = c_k(\underline{s}_{QR}, \underline{s}_H) \quad (4.8)$$

for all $k = 0, \dots, n - 1$. In other words, the Legendre sequence is a realisation of the Hall sequence by $(z, z, 1)$.

Proof. Let \underline{a} and \underline{b} be perfect sequences of period n corresponding to $\overline{A}, \overline{B} \subset \mathbb{Z}_n$. Then $|A| = |B| = \frac{n-1}{2}$ by (1.2). Using the well known correspondence between sets and binary sequences we get

$$\begin{aligned} c_t(\underline{a}, \underline{b}) &= n - 2|\{i \mid a_i \neq b_{i+t}, i = 0, \dots, n - 1\}| \\ &= n - 2(|A| + |B| - 2|\{i \mid a_i = b_{i+t} = 0, i = 0, \dots, n - 1\}|) \\ &= n - 2\left(\frac{n-1}{2} + \frac{n-1}{2} - 2|\{i \mid a_i = b_{i+t} = 0, i = 0, \dots, n - 1\}|\right) \\ &= -n + 2 + 4|(B - t) \cap A|. \end{aligned}$$

Thus,

$$\begin{aligned} c_{zk}(\underline{\mathfrak{S}}_H^{(z)}, \underline{\mathfrak{S}}_H) &= -n + 2 + 4|(H - zk) \cap z^{-1}H| \quad \text{and} \\ c_k(\underline{\mathfrak{S}}_{QR}, \underline{\mathfrak{S}}_H) &= -n + 2 + 4|(H - k) \cap QR| \end{aligned} \quad (4.9)$$

holds for all $k = 0, \dots, n-1$. We simply write C_i for $C_i^{(6)}$. Note, that z is the primitive element used to define QR and H , thus

$$z^i QR = C_i \cup C_{i+2} \cup C_{i+4} \quad \text{and} \quad z^j H = C_j \cup C_{j+1} \cup C_{j+3}. \quad (4.10)$$

For $k = 0$ we get $c_0(\underline{\mathfrak{S}}_H^{(z)}, \underline{\mathfrak{S}}_H) = -n + 2 + 4|C_0| = c_0(\underline{\mathfrak{S}}_{QR}, \underline{\mathfrak{S}}_H)$. Let $k \neq 0$, then $k = -z^{-i}$ for some i , since z is a primitive element in \mathbb{Z}_n^* . We get from (4.9), that (4.8) holds if and only if

$$|(H + z^{-i+1}) \cap z^{-1}H| = |(H + z^{-i}) \cap QR| \quad (4.11)$$

holds for all $i = 0, \dots, n-1$. We have $(H + z^{-i+1}) \cap z^{-1}H = z^{-i+1}((z^{i-1}H + 1) \cap z^{i-2}H)$ and $(H + z^{-i}) \cap QR = z^{-i}((z^i H + 1) \cap z^i QR)$. Thus, from (4.10) it follows that (4.11) holds if and only if $h_i = q_i$ for all $i = 0, \dots, 5$, where

$$h_i := |(z^{i-1}H + 1) \cap z^{i-2}H| \quad \text{and} \quad q_i := |(z^i H + 1) \cap z^i QR|. \quad (4.12)$$

We explicitly calculate h_i and q_i . In general we have

$$((C_{i_1} \dot{\cup} C_{i_2} \dot{\cup} C_{i_3}) + 1) \cap (C_{j_1} \dot{\cup} C_{j_2} \dot{\cup} C_{j_3}) = \bigcup_{\substack{r=1,2,3 \\ s=1,2,3}} ((C_{i_r} + 1) \cap C_{j_s})$$

since the C_{i_j} 's are pairwise disjoint. For fixed i and j , the cyclotomic number (i, j) is defined as the number of solutions of the equation $z_i + 1 = z_j$ with $z_i \in C_i$ and $z_j \in C_j$, i.e.

$$(i, j) = |(C_i + 1) \cap C_j|,$$

see [40] for more information about cyclotomic numbers in particular in connection with difference sets. We have

$$|((C_{i_1} \cup C_{i_2} \cup C_{i_3}) + 1) \cap (C_{j_1} \cup C_{j_2} \cup C_{j_3})| = \sum_{\substack{r=1,2,3 \\ s=1,2,3}} (i_r, j_s) \quad (4.13)$$

and therefore we get from (4.10) that

$$h_i = \sum_{\substack{r=0,2,5 \\ s=1,4,5}} (i+r, i+s) \quad \text{and} \quad q_i = \sum_{\substack{r=0,1,3 \\ s=0,2,4}} (i+r, i+s).$$

For $n = 4t^2 + 27$ prime the cyclotomic numbers are known. If $n = 4t^2 + 27$ is prime, then $\gcd(t, 3) = 1$. We have $n-1 \equiv 0 \pmod{6}$ and $n-1 \equiv 6 \pmod{12}$, since

2 and 3 divides $n - 1$ and 4 is not a divider of $n - 1$. Thus, $n = 6f + 1$ with f is odd. In this case the 36 cyclotomic numbers (i, j) are given by

$i \backslash j$	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	E	C	I
2	H	J	G	F	I	B
3	A	G	H	A	G	H
4	G	F	I	B	H	J
5	H	I	E	C	I	G

(4.14)

where

$$\begin{aligned}
9 \cdot A &:= t^2 - 4 \cdot t' + 4 \\
9 \cdot B &:= t^2 - t' + 16 \\
9 \cdot C &:= t^2 - t' + 16 = 9 \cdot B \\
9 \cdot D &:= t^2 + 8 \cdot t' + 7 \\
9 \cdot E &:= t^2 - t' - 2 \\
9 \cdot F &:= t^2 - t' - 2 = 9 \cdot E \\
9 \cdot G &:= t^2 + 2 \cdot t' + 10 \\
9 \cdot H &:= t^2 + 2 \cdot t' + 1 \\
9 \cdot I &:= t^2 - t' + 7 \\
9 \cdot J &:= t^2 - t' + 7 = 9 \cdot J
\end{aligned}
\tag{4.15}$$

and $t' = -t$ if $t \equiv 1 \pmod{3}$ and $t' = t$ if $t \equiv 2 \pmod{3}$. We get

$$\begin{aligned}
q_0 &= A + C + E + G + I + C + A + H + G = t^2 + \frac{22}{3} - \frac{2t'}{3} = B + E + F + J + I + B + I + I + G = h_0 \\
q_1 &= H + E + I + J + F + B + F + B + J = t^2 + \frac{16}{3} - \frac{2t'}{3} = A + C + F + G + I + I + A + H + H = h_1 \\
q_2 &= H + G + I + A + H + G + H + E + I = t^2 + \frac{13}{3} + \frac{t'}{3} = G + H + E + H + J + F + G + F + B = h_2 \\
q_3 &= B + D + F + G + A + H + F + B + J = t^2 + \frac{19}{3} + \frac{t'}{3} = J + G + I + G + H + G + I + E + I = h_3 \\
q_4 &= G + I + C + G + I + H + H + E + I = t^2 + \frac{19}{3} + \frac{t'}{3} = C + D + F + H + A + H + I + B + J = h_4 \\
q_5 &= B + D + F + J + F + B + I + C + G = t^2 + \frac{25}{3} + \frac{t'}{3} = G + E + C + G + B + H + H + C + I = h_5
\end{aligned}$$

□

The proof shows that one can explicitly calculate the intersection size and therefore the crosscorrelation coefficients between Hall sequences and between Hall and Legendre sequences by cyclotomic numbers.

Theorem 4.4 *Let $n = 4t^2 + 27$ be prime and let \underline{s}_H be the Hall sequence defined by (4.7) with the primitive element z in \mathbb{Z}_n^* . Then*

$$\begin{aligned}
Sp(\underline{s}_H^{(z)}, \underline{s}_H) &= \left\{ \frac{-4t^2-23}{3}, \frac{13-8t'}{3}, \frac{-11-8t'}{3}, \frac{-23+4t'}{3}, \frac{1+4t'}{3}, \frac{25+4t'}{3} \right\} \text{ and} \\
Sp(\underline{s}_H^{(z^3)}, \underline{s}_H) &= \left\{ \frac{4t^2+29}{3}, \frac{5-4t'}{3}, \frac{-19+8t'}{3}, \frac{17-4t'}{3}, \frac{-19-4t'}{3}, \frac{17+8t'}{3}, \frac{-7-4t'}{3} \right\},
\end{aligned}$$

where $t' = -t$ if $t \equiv 1 \pmod{3}$ and $t' = t$ if $t \equiv 2 \pmod{3}$. Furthermore, any crosscorrelation spectrum between Hall sequences, where the sequences are shift distinct, and between Legendre and Hall sequences belongs to one of these spectra.

Proof. We have the notation above. Since $\underline{s}_H^{(z^{6r+s})} = \underline{s}_H^{(z^s)}$, we have at most five different crosscorrelation spectra between shift distinct Hall sequences. Furthermore, $Sp(\underline{s}_H^{(z^i)}, \underline{s}_H) = Sp(\underline{s}_H, \underline{s}_H^{(z^{-i})}) = Sp(\underline{s}_H^{(z^{-i})}, \underline{s}_H)$ shows, that we have at most three different crosscorrelation spectra. The proof of Theorem 4.3 shows, that the crosscorrelation coefficients are constant on the cyclotomic classes C_i 's. We have

$$Sp(\underline{s}_H^{(z^l)}, \underline{s}_H) = \{ c_0(\underline{s}_H^{(z^l)}, \underline{s}_H) \} \cup \{ c_{z^k}(\underline{s}_H^{(z^l)}, \underline{s}_H) \mid k = 0, \dots, 5 \}$$

for all $l = 1, 2, 3$. Since $H = C_0 \cup C_1 \cup C_3$ and $|C_i| = \frac{n-1}{6}$ for all i we have

$$\begin{aligned} c_0(\underline{s}_H^{(z^l)}, \underline{s}_H) &= -n + 2 + 4|z^{-l}H \cap H| \\ &= \begin{cases} -n + 2 + 4\frac{n-1}{6} & \text{if } l = 1, 2 \\ -n + 2 + 4\frac{n-1}{3} & \text{if } l = 3 \end{cases} \\ &= \begin{cases} \frac{-4t^2-23}{3} & \text{if } l = 1, 2 \\ \frac{4t^2+29}{3} & \text{if } l = 3. \end{cases} \end{aligned}$$

We transform

$$\begin{aligned} c_{-z^{-k}}(\underline{s}_H^{(z^{-l})}, \underline{s}_H) &= -n + 2 + 4|(H + z^{-k}) \cap z^l H| \\ &= -n + 2 + 4|z^{-k}((z^k H + 1) \cap z^{l+k} H)| \\ &= -n + 2 + 4|(z^k H + 1) \cap z^{l+k} H|. \end{aligned}$$

Using (4.13), by the definition of H we get

$$h_{l,k} := |(z^k H + 1) \cap z^{l+k} H| = \sum_{i,j=0,1,3} (i+k, j+l+k).$$

By (4.14) and (4.15) we can explicitly calculate the crosscorrelation spectra given in the theorem, since $Sp(\underline{s}_H^{(z^l)}, \underline{s}_H) = \{ c_0(\underline{s}_H^{(z^l)}, \underline{s}_H) \} \cup \{ -n+2+4h_{l,k} \mid k = 0, \dots, 5 \}$ for all $l = 1, 2, 3$. Let $H_l := \{h_{l,k} \mid k = 0, \dots, 5\}$, then

$$\begin{aligned} H_1 &:= \{4J + 2E + G + 2B, E + 2J + 2H + 2A + G + B, 2G + 2H + J + 3E + B, \\ &\quad 4J + 3G + H + E, 2H + 2J + 2B + A + D + E, 3B + E + 2H + J + 2G\} \\ H_2 &:= \{2E + 2B + 2G + J + 2H, 4J + B + 3G + H, E + 2J + 2H + 2A + G + B, \\ &\quad 2E + 2B + 2G + J + 2H, 4J + 2E + G + 2B, B + D + 2E + 2J + 2H + A\} \\ H_3 &:= \{2B + 4J + 2H + E, B + 4H + 2G + A + E, 3A + 2G + E + 2B + D, \\ &\quad 2E + 4J + 2H + B, 3E + 3B + 2G + D, D + 2E + 3A + B + 2G\}. \end{aligned}$$

By (4.15), finally we get $Sp(\underline{s}_H^{(z)}, \underline{s}_H) = Sp(\underline{s}_H^{(z^2)}, \underline{s}_H)$ and the crosscorrelation coefficients listed in Theorem 4.4.

We have only two Legendre sequences, which are shift distinct, namely \underline{s}_{QR} and $\underline{s}_{QR}^{(z)}$. Note that $\underline{s}_{QR}^{(z)}$ and $\bar{\underline{s}}_{QR}$ differs just in one position. We already know from Theorem 4.3 that $Sp(\underline{s}_{QR}, \underline{s}_H) = Sp(\underline{s}_H^{(z)}, \underline{s}_H)$. Furthermore, we have $Sp(\underline{s}_{QR}^{(z)}, \underline{s}_H) = Sp(\underline{s}_H^{(z^3)}, \underline{s}_H)$, since

$$\frac{n-1}{2} = |(H - z^k)| = |(H - z^k) \cap C_0^{(2)}| + |(H - z^k) \cap C_1^{(2)}| + |(H - z^k) \cap \{0\}|$$

and $|(H - z^k) \cap \{0\}| = 1$ if $z^k \in H$ and 0 otherwise. Thus,

$$\begin{aligned} c_{z^k}(\underline{s}_{QR}^{(z)}, \underline{s}_H) &= -n + 2 + 4|(H - z^k) \cap C_1^{(2)}| \\ &= -n + 2 + 4\left(\frac{n-1}{2} - |(H - z^k) \cap C_0^{(2)}| - |(H - z^k) \cap \{0\}|\right) \\ &= n - 4|(H - z^k) \cap C_0^{(2)}| - 4|(H - z^k) \cap \{0\}| \\ &= 2 - c_{z^k}(\underline{s}_{QR}, \underline{s}_H) - 4|(H - z^k) \cap \{0\}| \\ &= \begin{cases} -2 - c_{z^k}(\underline{s}_{QR}, \underline{s}_H) & \text{if } k \equiv 0, 1, 3 \pmod{6} \\ 2 - c_{z^k}(\underline{s}_{QR}, \underline{s}_H) & \text{if } k \equiv 2, 4, 5 \pmod{6} \end{cases} \end{aligned}$$

and $c_0(\underline{s}_{QR}^{(z)}, \underline{s}_H) = 2 - c_0(\underline{s}_{QR}, \underline{s}_H)$. Finally, we get $Sp(\underline{s}_{QR}^{(z)}, \underline{s}_H) = Sp(\underline{s}_H^{(z^3)}, \underline{s}_H)$. \square

Chapter 5

Crosscorrelation between Perfect Functions

In the following, we restrict our considerations to the description of sequences with period $n = 2^m - 1$ via functions $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$. With assumption (1.2) for balanced and therefore for perfect functions, we always have $f(0) = 0$.

In Section 5.1, basic properties for the crosscorrelation between perfect functions are listed. The known results for Hadamard equivalent sequences are presented in Section 5.2 and in Section 5.3 it is shown how to use Hadamard equivalence to write the crosscorrelation between certain perfect functions in terms of the crosscorrelation between m -functions.

5.1 Properties of the Crosscorrelation Function

Proposition 3.6 is now translated into the notation for functions. Note, that if f and g are the corresponding functions of the sequences \underline{a} and \underline{b} using the primitive element α , then $c_t(\underline{a}, \underline{b}) = c_{\alpha^t}(f, g) - (-1)^{f(0)+g(0)}$ for all $t = 0, \dots, n - 1$. Without loss of generality in the following we always assume that $f(0) = g(0) = 0$, otherwise we consider their complements. Now, we have $c_{\alpha^t}(f, g) = c_t^*(\underline{a}, \underline{b})$ for all $t = 0, \dots, n - 1$.

Additionally it is known that 2 is always a multiplier of a perfect sequence with period $n = 2^m - 1$, and therefore of a perfect function [12]. Using (1.3) for perfect functions f we assume

$$f^{(2^i)} = f. \quad (5.1)$$

Proposition 5.1 *Let $f, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be functions, $\gcd(d, 2^m - 1) = 1$ and $y \in \mathbb{F}_{2^m}^*$.*

- (1) We have $c_y(f^{(d)}, g) = c_{y^{1/d}}(f, g^{(1/d)})$ and $c_y(f, g) = c_{y^{-1}}(g, f)$.
- (2) Let g be perfect. Using (5.1), then $c_y(f, g^{(2^i)}) = c_y(f, g)$.
- (3) Let f and g be perfect. Using (5.1), then $c_{y^{2^i}}(f, g) = c_y(f, g)$.
- (4) If g is perfect, then $\sum_{y \in \mathbb{F}_{2^m}} c_y(f, g) = 2^m$.
- (5) If g is perfect, then $\sum_{y \in \mathbb{F}_{2^m}} (c_y(f, g))^2 = 2^{2m}$.
- (6) If f and g are perfect, then $\sum_{y \in \mathbb{F}_{2^m}} c_y(f, g) c_{ay}(f, g) = \begin{cases} 0 & \text{if } a \in \mathbb{F}_{2^m} \setminus \{1\} \\ 2^{2m} & \text{if } a = 1. \end{cases}$

We write the generalised Parseval formula (3.10) in functional representation: Let $f, h, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be functions and let g be perfect, then

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)} (-1)^{h(x)} = \frac{1}{2^m} \sum_{y \in \mathbb{F}_{2^m}} c_y(f, g) c_y(h, g). \quad (5.2)$$

If g is the trace function, then (5.2) is called the (usual) **Parseval formula**, i.e.

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+h(x)} = \frac{1}{2^m} \sum_{y \in \mathbb{F}_{2^m}} \mathcal{W}(f)(y) \cdot \mathcal{W}(h)(y).$$

since $\mathcal{W}(f)(y) = c_y(f, tr)$.

A lower bound for the maximum crosscorrelation coefficient

$$\mathcal{M}(f, g) := \max_{y \in \mathbb{F}_{2^m}} |c_y(f, g)|$$

is given by

$$\mathcal{M}(f, g) \geq 2^{\frac{m}{2}}, \quad (5.3)$$

if g is perfect. Furthermore, if f is balanced or perfect, then $\mathcal{M}(f, g) > 2^{m/2}$. This follows from Theorem 3.7 and Corollary 3.9, since $\mathcal{M}(f, g) = \max |\{c_t^*(\underline{a}, \underline{b}) | t = 0, \dots, n-1\} \cup \{w^*(\underline{a})\}|$ yields for the corresponding sequences \underline{a} and \underline{b} of f and g .

If g is linear, then (5.3) states nothing new. The **linearity** of f is the maximum Walsh coefficient (in absolute value) of f . Thus, the crosscorrelation of a function f with the trace function is related to the linearity of the function f . The maximum Walsh coefficient of a function $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ is $\max_{y \in \mathbb{F}_{2^m}} |\mathcal{W}(f)(y)| \geq 2^{m/2}$, where equality occurs if and only if f is bent [15].

Since bent functions are not balanced, we have $\max_{y \in \mathbb{F}_{2^m}^*} |\mathcal{W}(f)(y)| > 2^{m/2}$ for balanced functions f . In the case, where f and g are both m -functions, it is

well-known that $\mathcal{M}(f, g) \geq 2^{(m+1)/2}$. The bound (5.3) seems to be bad if f and g are both perfect. We have no examples of perfect functions f and g with $\mathcal{M}(f, g) < 2^{(m+1)/2}$, hence we ask ourself:

Question 5.2 *Let f and g be two perfect functions. Is it true, that*

$$\mathcal{M}(f, g) \geq 2^{\frac{m+1}{2}} ? \quad (5.4)$$

Minimal Number of Different Crosscorrelation Values

Proposition 5.3 *Let $f, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be two perfect functions, whose corresponding sequences \underline{a} and \underline{b} are shift distinct. Then their crosscorrelation spectrum contains at least three different values.*

In [13] Helleseht proved this for m -functions, but the proof is also true for arbitrary perfect functions.

Proof. Note that $c_0(f, g) = c_0(f) = 0$ for a perfect function f . Assume, contrary to the statement, that a and b are the only crosscorrelation coefficients. Then it follows by (4) and (5) in Proposition 5.1 that

$$\begin{aligned} x + y &= 2^m - 1 \\ xa + yb &= 2^m \\ xa^2 + yb^2 &= 2^{2m}, \end{aligned}$$

where x and y are the multiplicities of the crosscorrelation coefficients. We have $a \neq 0 \neq b$ otherwise $a = 2^m$ or $b = 2^m$ and then the sequences are shift equivalent. Without loss of generality we get from the first line that x is even and y is odd. Let i and x' be integers such that $x = 2^i x'$ and x' is odd, thus $i \geq 1$. Let j, k and a', b' be integers such that $a = 2^j a'$, $b = 2^k b'$ and a', b' are odd. We get

$$\begin{aligned} 2^{i+j} x' a' + 2^k y b' &= 2^m \\ 2^{i+2j} x' a'^2 + 2^{2k} y b'^2 &= 2^{2m}. \end{aligned}$$

It follows, that $i+j = k$, otherwise the left hand side of the first line is not a power of 2, but also that $i+2j = 2k$, otherwise the left hand side of the second line is not a power of 2. This gives a contradiction to $i \geq 1$. Thus, the crosscorrelation spectrum contains more than two values. \square

Proposition 5.4 : *Let $f, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be functions and let g be perfect. Let the crosscorrelation spectrum between f and g be three-valued with $\pm c$ and 0 and*

$c_0(f) = 0$. Then $c = 2^{(m+k)/2}$ with $k \in \mathbb{N}_0$ and the multiplicities are:

crosscorrelation value	multiplicity	
0	$2^m - 2^{m-k} - 1$	(5.5)
$+2^{\frac{m+k}{2}}$	$2^{m-1-k} + 2^{\frac{m-k}{2}-1}$	
$-2^{\frac{m+k}{2}}$	$2^{m-1-k} - 2^{\frac{m-k}{2}-1}$.	

Proof. Let x denote the number of crosscorrelation coefficient $\pm c$. From (6) in Proposition 5.1 we get $2^{2m} = \sum_{y \in \mathbb{F}_{2^m}} (c_y(f, g))^2 = c^2 x$. This shows that c^2 has divide 2^{2m} , and therefore c is a power of 2.

By (5.3) we have $c \geq 2^{m/2}$. Let $c = 2^{(m+k)/2}$ for some integer $k \geq 0$ and $z_i := |\{y \in \mathbb{F}_{2^m}^* | c_y(f, g) = i\}|$. Obviously we have

$$z_0 + z_c + z_{-c} = 2^m - 1. \quad (5.6)$$

Since g is perfect, by (5) in Proposition 5.1 we get $2^m = \sum_{y \in \mathbb{F}_{2^m}} c_y(f, g) = (z_c - z_{-c}) \cdot 2^{(m+k)/2}$, thus

$$z_c - z_{-c} = 2^{\frac{m-k}{2}}. \quad (5.7)$$

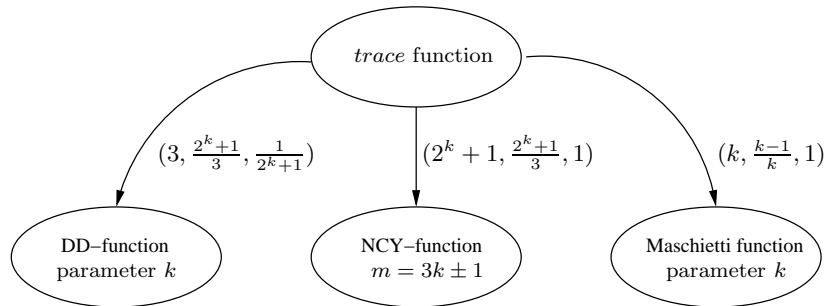
By (6) in Proposition 5.1 we get $2^{2m} = \sum_{z \in \mathbb{F}_{2^m}} (c_z(f, g))^2 = (z_c + z_{-c}) \cdot 2^{m+k}$, therefore

$$z_c + z_{-c} = 2^{m-k}. \quad (5.8)$$

The equations (5.6), (5.7) and (5.8) show the multiplicities in (5.5). \square

5.2 Hadamard Equivalence of Functions

An exhaustive search was performed to compute all functions $\mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ that are (extended) Hadamard equivalent to linear functions for odd $m \leq 17$ [9]. For $m = 7$ see Example 5.5. For $9 \leq m \leq 17$, those which are (extended) Hadamard equivalent to the trace functions are the Maschietti, the NCY and the DD-functions. Let m be odd, then we have the following realisations by (z_1, z_2, z_3) :

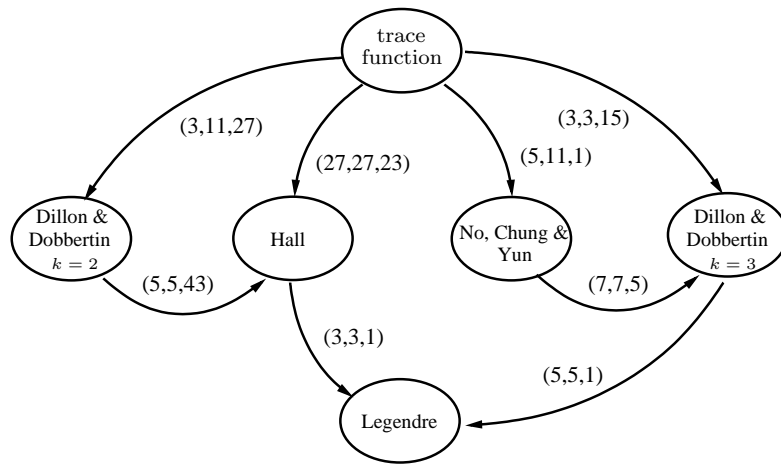


where z_1, z_2 and z_3 are defined by

$$(-1)^{g(z)} = \frac{1}{2^m} \left(\sum_{x \in \mathbb{F}_{2^m}} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(x^{z_1})+f(xy^{z_2})+f(yz^{z_3})} \right) \quad (5.9)$$

and the arrow begins at the starting function f and ends at the resulting function g , see [4, 5]. In other words, the usual Hadamard equivalence, which is introduced in [4, 5], means that the new perfect functions are realisations of the trace function.

Example 5.5 [9] *We start with the trace function and compute all realisations by formula (5.9). For $m = 7$ we get by computations the following realisations:*



For $m = 7$ there exist up to equivalence six classes of perfect functions. It is an interesting phenomenon that we get all these perfect functions by iterations of (5.9).

5.3 Application of Hadamard Equivalence

In the following, Hadamard equivalence is used to write the crosscorrelation coefficients of arbitrary perfect functions in terms of Walsh coefficients of m -functions. This is possible for the crosscorrelation function of perfect functions $f^{(s)}$ and g , if there exist integers d and d' , which are coprime to $2^m - 1$, such that $f^{(d)}$ and $g^{(d')}$ are Hadamard equivalent to m -functions.

Theorem 5.6 *Let $f, g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be perfect functions, and let s be an integer such that $\gcd(s, 2^m - 1) = 1$. Let $\mathcal{W}(f^{(d)})(x) = \mathcal{W}(tr^{(k)})(\beta x^l)$ and $\mathcal{W}(g^{(d')})(x) =$*

$\mathcal{W}(tr^{(k')})(\beta'x^{l'})$ for all $x \in \mathbb{F}_{2^m}$ and some integers l, l', d, d', k, k' , where d, d', k, k' are coprime to $2^m - 1$. Then

$$\begin{aligned} c_a(f^{(s)}, g) &= \\ &= \frac{1}{2^{2m}} \sum_{x, z \in \mathbb{F}_{2^m}} \mathcal{W}(tr^{(k)})(\beta x^l) \cdot \mathcal{W}(tr^{(k')})(\beta' x^{l'}) \cdot \mathcal{W}(tr^{(t)})(a^{1/d'} z x^{-1/t}), \end{aligned}$$

where $t := d's/d$.

Theorem 5.6 shows that the problem to determine the crosscorrelation between certain perfect functions is related to the problem to determine the crosscorrelation between the trace function and its decimations $tr^{(d)}$. Even this is a very difficult problem. It has been investigated for many years and still many questions are open, see [14] for instance.

Proof of Theorem 5.6. Let $a \neq 0$. Formula (5.2) with the perfect function $tr^{(s/d)}$ is applied in the first step and with $tr^{(1/d')}$ in the second step:

$$\begin{aligned} 2^{2m} c_a(f^{(s)}, g) &= \\ &= 2^{2m} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x^s) + g(ax)} \\ &\stackrel{(5.2)}{=} 2^m \sum_{x \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(y^s) + tr(x^{s/d} y^{s/d})} \right) \left(\sum_{z \in \mathbb{F}_{2^m}} (-1)^{g(az) + tr(x^{s/d} z^{s/d})} \right) \\ &= 2^m \sum_{x \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(y^d) + tr(xy)} \right) \left(\sum_{z \in \mathbb{F}_{2^m}} (-1)^{g(z) + tr(a^{-s/d} x z^{s/d})} \right) \\ &\stackrel{(5.2)}{=} \sum_{x \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(y^d) + tr(xy)} \right) \\ &\quad \cdot \left(\sum_{z \in \mathbb{F}_{2^m}} \sum_{v \in \mathbb{F}_{2^m}} (-1)^{g(v) + tr(z^{1/d'} v^{1/d'})} \sum_{w \in \mathbb{F}_{2^m}} (-1)^{tr(a^{-s/d} x w^{s/d}) + tr(z^{1/d'} w^{1/d'})} \right). \end{aligned}$$

We substitute $z^{1/d'}$ by z and w by $ax^{-d/s} w^{d'}$ and get

$$\begin{aligned} 2^{2m} c_a(f^{(s)}, g) &= \\ &= \sum_{x, z \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(y^d) + tr(xy)} \right) \left(\sum_{v \in \mathbb{F}_{2^m}} (-1)^{g^{(d')}(v) + tr(zv)} \right) \\ &\quad \cdot \left(\sum_{w \in \mathbb{F}_{2^m}} (-1)^{tr(w^{d' \cdot s/d}) + tr(a^{1/d'} z x^{-d/(d' \cdot s)} w)} \right) \\ &= \sum_{x, z \in \mathbb{F}_{2^m}} \mathcal{W}(f^{(d)})(x) \cdot \mathcal{W}(g^{(d')})(y) \cdot \mathcal{W}(tr^{(d' s/d)})(a^{1/d'} z x^{-d/(d' s)}). \end{aligned}$$

Using the assumptions, Theorem 5.6 is proved. \square

Chapter 6

Crosscorrelation between Special Perfect Functions

An overview over the research on the crosscorrelation between perfect functions:

- The crosscorrelation between m -functions was first examined 1968. Today they are the most examined and best-known crosscorrelation functions. But there are still many questions open [15].
- The crosscorrelation between an m -function and a GMW-function was analysed 1985 by Games [6]. A strong condition was that the two functions were considered without decimations. This condition was partly removed 1990 in [23] by Chan, Goresky and Klapper.
- Antweiler has shown in 1994 that the calculation of the crosscorrelation between arbitrary GMW-functions can be reduced to the crosscorrelation of m -functions [1].
- The crosscorrelation between an m -function and a Maschietti function without decimations is examined in [4], between an m -function and a No-Chung-Yun function without decimations in [4, 5] and the crosscorrelation between an m -function and a decimated Dillon-Dobbertin function with one particular exponent in [5]. These calculations were used to prove that the Maschietti, No-Chung-Yun and Dillon-Dobbertin construction produce perfect functions. Gong and Yu [10] looked at the crosscorrelation between these functions and get new exponents for decimations, where the crosscorrelation spectrum is three- or five-valued.
- In this thesis, I consider the crosscorrelation function between Dillon-Dobbertin functions [17] and between Dillon-Dobbertin and Gordon-Mills-Welch functions [18].

Cross-Correlation	<i>m</i> -function	GMW-function	Mas.-function	NCY-function	DD-function
<i>m</i> -function	1968 Gold [8], Kasami [22], Welch [41], Niho [29]	1985 Games [6]	1998 Dillon [4]	1998 Dillon & Dobbertin [4, 5]	1999 Dillon & Dobbertin [5]
GMW-function	—	1993 Chan, Goresky & Klapper [24] 1994 Antweiler [1]	?	?	2006 Section 6.3 published in [18]
Mas.-function	—	—	?	?	?
NCY-function	—	—	—	?	?
DD-function	—	—	—	—	2004 Section 6.2 published in [17]

The table gives an overview of important steps in the research of the crosscorrelation between the known perfect functions.

In this chapter, new results on the crosscorrelation between Dillon-Dobbertin functions and between Dillon-Dobbertin functions and GMW-functions are presented. We have used the fact that the crosscorrelation between these perfect functions is reduced to the crosscorrelation between m -functions, when m is odd, because many results are known on the crosscorrelation between m -functions.

In Section 5.1, some known results on the crosscorrelation between m -functions are listed. These results are used to prove our results on the crosscorrelation between Dillon-Dobbertin functions in Section 6.2 and on the crosscorrelation between Dillon-Dobbertin functions and GMW-functions in Section 6.3.

Some assumptions

In the following perfect functions with nice crosscorrelation properties are considered: With respect to Question 5.2 it is possible that the case $\mathcal{M}(f, g) = 2^{\frac{m+1}{2}}$ is optimum. Hence we are looking for pairs of functions f and g with $\mathcal{M}(f, g) = 2^{\frac{m+1}{2}}$, so we restrict our considerations to the case m odd.

If we explicitly list the crosscorrelation spectrum of two functions, note that:

1. It is always $n = 2^m - 1$ and $\gcd(d, n) = 1$.
2. By (1) in Proposition 3.6 follows $Sp(f^{(d)}, g^{(d')}) = Sp(f^{(d/d')}, g)$ for all d, d' . Therefore, it is enough to write down only the decimations of one function.
3. With respect to (2) in Proposition 3.6, the smallest decimation d in $\{2^i d \bmod 2^m - 1 \mid i = 0, \dots, m - 1\}$ is listed.

6.1 Crosscorrelation between m -Functions

The crosscorrelation between m -functions is the most analysed and best known crosscorrelation function. In this section, an overview over some known results of the crosscorrelation between m -functions is given [13, 14, 15].

Let $\varphi : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ be a function and let $\varphi_\beta(x) := \text{tr}(\beta\varphi(x))$ be the so called **coordinate function** from \mathbb{F}_{2^m} to \mathbb{F}_2 . If φ is a power function x^d , then $\varphi_\beta(x) = \text{tr}^{[\beta]}(x^d)$. Thus, m -functions correspondent to coordinate functions of power functions x^d , if $\gcd(d, 2^m - 1) = 1$.

The maximum

$$\mathcal{N}(\varphi) := \max_{\beta, \gamma \in \mathbb{F}_{2^m}, \beta \neq 0} \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right| \quad (6.1)$$

is called the **linearity** of φ . In the case of power mappings with $\gcd(d, 2^m - 1) = 1$, the computation of the linearity simplifies. We have

$$\begin{aligned} \mathcal{N}(\varphi) &= \max_{\gamma, \beta \in \mathbb{F}_{2^m}, \beta \neq 0} \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\gamma \cdot x + \beta \cdot x^d)} \right| \\ &= \max_{\alpha, \eta \in \mathbb{F}_{2^m}, \eta \neq 0} \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\alpha(\eta \cdot x) + (\eta \cdot x)^d)} \right| \\ &= \max_{\alpha \in \mathbb{F}_{2^m}} \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\alpha x + x^d)} \right| \\ &= \mathcal{M}(\text{tr}^{(d)}, \text{tr}), \end{aligned} \quad (6.2)$$

where we put $\beta = \eta^d$ and $\gamma = \alpha\eta$ and finally we note, that ηx runs through \mathbb{F}_{2^m} if x does. This observation implies some connections between the linearity of power mappings and the crosscorrelation between m -functions. Note that a lower bound for the linearity of a power function x^d is also a lower bound for the maximum crosscorrelation coefficient between $\text{tr}^{(d)}$ and tr .

Proposition 6.1 *Let $\varphi : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ be a function, then*

$$\mathcal{N}(\varphi) \geq 2^{(m+1)/2}. \quad (6.3)$$

Proof. In generally, we have $\sum_{v \in M} v^2 \leq w \sum_{v \in M} v$, where M is a finite set with non-negative integers and $w := \max_{v \in M} v$. We use this and take v to be $(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)})^2$ and get

$$\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^4 \leq \mathcal{N}(\varphi)^2 \cdot \sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^2. \quad (6.4)$$

Note that $\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\gamma \cdot x)} = 0$ if $\gamma \neq 0$ and 2^m otherwise, since the trace function is balanced. We calculate the sum on the right hand side of (6.4). In the first step we insert $0 = \sum_{\gamma \in \mathbb{F}_{2^m}} (\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\gamma x)})^2 - 2^{2m}$ and get

$$\begin{aligned} &\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^2 \\ &= \sum_{\beta, \gamma \in \mathbb{F}_{2^m}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^2 - 2^{2m} \\ &= \sum_{\beta, \gamma, x, y \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x) + \varphi(y)) + \gamma(x+y))} - 2^{2m} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\beta, x, y \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x)+\varphi(y)))} \underbrace{\sum_{\gamma \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\gamma(x+y))}}_{= \begin{cases} 2^m & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}} - 2^{2m} \\
&= 2^m \sum_{\beta, x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x)+\varphi(x)))} - 2^{2m} \\
&= 2^{3m} - 2^{2m}.
\end{aligned}$$

For the left hand side of (6.4) we calculate a lower bound by

$$\begin{aligned}
&\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^4 \\
&= \sum_{\beta, \gamma \in \mathbb{F}_{2^m}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^4 - 2^{4m} \\
&= \sum_{\beta, x, y, z, v \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x)+\varphi(y)+\varphi(z)+\varphi(v)))} \underbrace{\sum_{\gamma \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\gamma(x+y+z+v))}}_{= \begin{cases} 2^m & \text{if } v = x + y + z \\ 0 & \text{otherwise} \end{cases}} - 2^{4m} \\
&= 2^m \sum_{x, y, z \in \mathbb{F}_{2^m}} \left(\sum_{\beta \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x)+\varphi(y)+\varphi(z)+\varphi(x+y+z)))} \right) - 2^{4m} \\
&= 2^m \sum_{x, y, z \in \mathbb{F}_{2^m}} \left(\sum_{\beta \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta(\varphi(x)+\varphi(x+y)+\varphi(z)+\varphi(y+z)))} \right) - 2^{4m},
\end{aligned}$$

where y is replaced by $x + y$. Since tr is perfect we get

$$\begin{aligned}
&\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \right)^4 \\
&= 2^{2m} |\{ (x, y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid \varphi(x) + \varphi(x+y) = \varphi(z) + \varphi(y+z) \}| - 2^{4m} \\
&\geq 2^{2m} (2^{2m+1} + 2^{2m} - 2^{m+1}) - 2^{4m} \\
&= 2^{4m+1} - 2^{3m+1},
\end{aligned}$$

because $(H_1 \dot{\cup} H_2 \dot{\cup} H_3) \subseteq \{ (x, y, z) \mid \varphi(x) + \varphi(x+y) = \varphi(z) + \varphi(y+z) \}$, where

$$\begin{aligned}
H_1 &:= \{ (x, y, x) \mid x, y \in \mathbb{F}_{2^m} \} \\
H_2 &:= \{ (x, y, x+y) \mid x, y \in \mathbb{F}_{2^m}, y \neq 0 \} \\
H_3 &:= \{ (x, 0, y) \mid x, y \in \mathbb{F}_{2^m}, x \neq y \}.
\end{aligned}$$

The sets $H_i, i = 1, 2, 3$, are pairwise disjoint and the cardinality is $|H_1| = 2^{2m}$ and $|H_2| = |H_3| = 2^m(2^m - 1)$. Using (6.4) we get $\mathcal{N}(\varphi)^2 \geq 2^{m+1}$. \square

Proposition 6.2 *Let $\mathcal{N}(\varphi) = 2^{(m+1)/2}$, then*

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)} \in \{\pm 2^{(m+1)/2}, 0\}$$

for all $\beta \in \mathbb{F}_{2^m}^*$ and $\gamma \in \mathbb{F}_{2^m}$.

Proof: Since $(\mathcal{N}(\varphi))^2 = 2^{m+1}$ equality occurs in (6.4). Hence we have for all $\beta \in \mathbb{F}_{2^m}^*$ and $\gamma \in \mathbb{F}_{2^m}$ that $(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta \cdot \varphi(x) + \gamma \cdot x)})^2 \in \{0, 2^{m+1}\}$. \square

A function φ is called **maximum nonlinear** or **almost bent**, if $\mathcal{N}(\varphi) = 2^{(m+1)/2}$. Note, that maximum nonlinear functions only exist for m odd. A function φ is called **almost perfect nonlinear** (APN) if the function $\varphi(x+y) + \varphi(x)$ is a 2-to-1 mapping for all $y \in \mathbb{F}_{2^m}^*$.

The proof of Proposition 6.1 shows that maximum nonlinear functions are almost perfect nonlinear, since $|\{(x, y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid \varphi(x) + \varphi(x+z) = \varphi(y) + \varphi(y+z)\}| = 2^{2m+1} + 2^{2m} - 2^{m+1}$ holds for maximum nonlinear functions, hence φ is almost perfect nonlinear.

Corollary 6.3 *Let tr be the trace function, then*

$$\mathcal{M}(tr^{(d)}, tr) \geq 2^{(m+1)/2}. \quad (6.5)$$

If $\mathcal{M}(tr^{(d)}, tr) = 2^{(m+1)/2}$, then $Sp(tr^{(d)}, tr) = \{\pm 2^{(m+1)/2}, 0\}$ and the multiplicities are given in (5.5).

Proof. The results follow from Proposition 6.1 and 6.2 with (6.2). \square

Note that for power functions φ the sum on the left hand side in (6.4) reduces to

$$\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta x^d + \gamma x)} \right)^4 = (2^m - 1) \sum_{\gamma \in \mathbb{F}_{2^m}} c_\gamma(tr^{(d)}, tr)^4$$

and the sum on the right hand side to

$$\sum_{\substack{\beta, \gamma \in \mathbb{F}_{2^m} \\ \beta \neq 0}} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\beta x^d + \gamma x)} \right)^2 = (2^m - 1) \sum_{\gamma \in \mathbb{F}_{2^m}} c_\gamma(tr^{(d)}, tr)^2,$$

since $\beta^{1/d}x$ runs through \mathbb{F}_{2^m} if x does. Thus, the proof of Proposition 6.1 shows $\sum_{x \in \mathbb{F}_{2^m}} c_x(tr^{(d)}, tr)^4 \geq 2^{3m+1}$ and $\sum_{x \in \mathbb{F}_{2^m}} c_x(tr^{(d)}, tr)^2 = 2^{2m}$ and

$$\begin{aligned} & \sum_{x \in \mathbb{F}_{2^m}} c_x(tr^{(d)}, tr)^4 = \\ & = 2^{2m} |\{(y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid y^d + (y+1)^d = x^d + (x+1)^d\}|. \end{aligned} \quad (6.6)$$

The sum over all squares of the crosscorrelation coefficients between arbitrary perfect functions is always 2^{2m} , see (5) in Proposition 5.1. But for arbitrary perfect functions it is not true that the sum over the 4-th powers of the crosscorrelation coefficients is greater or equal to 2^{3m+1} . Thus, this proof cannot be generalised to attach Question 5.2. Furthermore, the second statement in Corollary 6.3 is not true for the crosscorrelation between arbitrary perfect functions. The next example gives a counter-example.

Example 6.4 Let $m = 7$ and b_k be the Dillon-Dobbertin function defined in Chapter 2 with parameter k . We choose $k = 3$ and get $\mathcal{M}(b_3^{(19)}, b_3) = 2^{(m+1)/2} = 2^4$, but

$$\begin{aligned} \sum_{x \in \mathbb{F}_{2^m}} c_x(b_3^{(19)}, b_3)^4 &= 21 \cdot 16^4 + 28 \cdot 8^4 + 21 \cdot 0 + 28 \cdot 8^4 + 29 \cdot 16^4 \\ &= 3.506.176 < 4.194304 = 2^{3 \cdot 7 + 1}. \end{aligned}$$

Furthermore, the crosscorrelation spectrum is five-valued, i.e. $Sp(b_3^{(19)}, b_3) = \{-2^4(21), -2^3(28), 0(21), 2^3(28), 2^4(29)\}$, where the numbers in brackets are the multiplicities.

In the next proposition, the known maximum nonlinear power functions are listed.

Proposition 6.5 [15] Let m be odd and s be an integer such that $\gcd(s, m) = 1$. The crosscorrelation spectrum $Sp(tr^{(d)}, tr)$ is three-valued with the values stated in (5.5) with $k = 1$ if d is

$$\begin{aligned} d &= 2^s + 1 \quad \text{the Gold parameter,} \\ d &= 2^{2s} - 2^s + 1 \quad \text{the Kasami parameter,} \\ d &= 2^{(m-1)/2} + 3 \quad \text{the Welch parameter or} \\ d &= 2^{(m-1)/2} + 2^r - 1 \quad \text{with } 4r \equiv 1 \pmod{m} \quad \text{the Niho parameter.} \end{aligned}$$

Note that the three-valued crosscorrelation spectrum $\{\pm 2^{(m+1)/2}, 0\}$ between m -functions is best possible with respect to the maximal crosscorrelation coefficient (see Corollary 6.3) and with respect to the smallest number of values in the crosscorrelation spectrum (see Proposition 5.3).

There are some more interesting properties of the crosscorrelation function between m -functions.

Proposition 6.6 [13] The crosscorrelation spectrum $Sp(tr^{(d)}, tr)$ has at least three different values if and only if $d \notin \{1, 2, \dots, 2^{m-1}\}$.

Proof: Proposition 5.3 implies $Sp(tr^{(d)}, tr)$ is at least three-valued if $tr^{(d)}$ and tr produce shift distinct sequences. Assume $tr^{(d)}$ gives a shift of tr , then there exists an integer t such that $\sum_{i=0}^{m-1} (\alpha^t x)^{2^i} \equiv tr^{(1)}(\alpha^t x) \equiv tr^{(d)}(x) \equiv \sum_{i=0}^{m-1} x^{2^i d} \pmod{(x^{2^m-1} - 1)}$ holds for a primitive element α in $\mathbb{F}_{2^m}^*$. Comparing to the exponents, it follows

$$\{2^i + t \pmod{2^m - 1} \mid i = 0, \dots, m-1\} = \{2^i d \pmod{2^m - 1} \mid i = 0, \dots, m-1\}. \quad (6.7)$$

If (6.7) holds, then $2^i + t \equiv d \pmod{2^m - 1}$ and $2^j + t \equiv 2d \pmod{2^m - 1}$ for some $i \neq j$. It follows $2^j - d \equiv d - t \equiv 2^i \pmod{2^m - 1}$, which only holds if d is a power of 2. \square

Corollary 6.7 *The only multipliers of m -functions are the powers of 2.*

6.2 Crosscorrelation between Dillon-Dobbertin Functions

In this section, the crosscorrelation between Dillon-Dobbertin functions f and g with $\mathcal{M}(f, g) = 2^{(m+1)/2}$ is considered. Let b_k denote the DD-function with parameter k . For $m \leq 17$ odd, all functions $b_k^{(s)}$ and b_l with $\mathcal{M}(b_k^{(s)}, b_l) = 2^{\frac{m+1}{2}}$ are listed, which were found by computer calculations:

m	k	l	$1/s$	
5	1	2	1	\star_2
5	1	2	5	\star_1
5	1	2	7	\star_3
7	1	2	1	\star_2
7	1	2	5	\star_1
7	1	2	43	
7	1	3	1	\star_2
7	1	3	9	\star_1
7	1	3	15	
7	1	3	27	
7	1	3	43	
7	2	3	1	\star_2
7	2	3	27	
7	3	3	19	\circ_1
9	1	2	5	\star_1
9	1	4	17	\star_1
11	1	2	5	\star_1
11	1	3	1	\star_2

m	k	l	$1/s$	
11	1	3	9	\star_1
11	1	4	1	\star_2
11	1	4	17	\star_1
11	1	5	33	\star_1
11	2	3	1	\star_2
11	2	5	1	\star_2
11	4	5	1	\star_2
13	1	2	5	\star_1
13	1	3	1	\star_2
13	1	3	9	\star_1
13	1	4	1	\star_2
13	1	4	17	\star_1
13	1	5	33	\star_1
13	1	6	65	\star_1
13	2	5	1	\star_2
13	2	6	1	\star_2
13	3	4	1	\star_2
13	5	6	1	\star_2

m	k	l	$1/s$	
15	1	2	5	\star_1
15	1	4	17	\star_1
15	1	7	129	\star_1
17	1	2	5	\star_1
17	1	3	1	\star_2
17	1	3	9	\star_1
17	1	4	17	\star_1
17	1	5	33	\star_1
17	1	6	1	\star_2
17	1	6	65	\star_1
17	1	7	129	\star_1
17	1	8	257	\star_1
17	2	5	1	\star_2
17	2	6	1	\star_2
17	3	8	1	\star_2
17	4	5	1	\star_2
17	4	7	1	\star_2
17	7	8	1	\star_2

The case $k = l = 1$ is not considered, because it describes the crosscorrelation between m -functions. It is interesting that in all cases listed in the table, except the case \circ_1 , the crosscorrelation spectrum is three-valued with the values $\pm 2^{\frac{m+1}{2}}$ and 0 and the multiplicities from Proposition 5.4. In the case \circ_1 the crosscorrelation spectrum is $Sp(b_3^{(1/19)}, b_3) = \{-16(21), -8(28), 0(21), 8(28), 16(29)\}$, where the numbers in the brackets are the multiplicities, see also Example 6.4.

Any value in the table represents a whole class of values, which also have the same crosscorrelation spectrum. In addition to the assumptions already made, we only list the values k and l such that $1 \leq k \leq l \leq \frac{m-1}{2}$, since $b_k = b_{m-k}$.

The values in the table indicated by a star can be explained. It is not only shown that the maximal crosscorrelation coefficient is $2^{(m+1)/2}$, but it is also proved that these crosscorrelation spectra contain only the three values $\pm 2^{(m+1)/2}$ and 0: For some special k, l and s the crosscorrelation between $b_k^{(s)}$ and b_l is equivalent to the Walsh transform of $tr^{(d)}$, where $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$ with $\gcd(k, m) = 1$. The Walsh spectrum of such functions $tr^{(d)}$ is three-valued with $\pm 2^{\frac{m+1}{2}}$ and 0, see Proposition 6.5.

The following highly nontrivial result is the major step in [5] to prove that b_k is a perfect function.

Result 6.8 (Dillon and Dobbertin [5]) *Let m be odd and $\gcd(k, m) = 1$, then*

$$\mathcal{W}(b_k^{(2^k+1)})(y) = \mathcal{W}(tr^{(3)})(y^{(2^k+1)/3}) \quad \text{for all } y \in \mathbb{F}_{2^m}.$$

Result 6.8 explains all entries in the table indicated by \star_1 , since $c_y(b_k^{(s)}, b_1) = \mathcal{W}(b_k^{(s)})(y)$. In particular, we have

$$c_y(b_k^{(2^k+1)}, b_1) \in \{\pm 2^{(m+1)/2}, 0\}.$$

The following theorem shows that the crosscorrelation between DD-functions without decimations is equal to the Walsh transform of certain m -functions.

Theorem 6.9 *Let m be odd and $\gcd(k, m) = \gcd(l, m) = 1$, then*

$$c_y(b_k, b_l) = \mathcal{W}(tr^{((2^k+1)/(2^l+1)}))(y^{-1/(2^k+1)}) \quad \text{for all } y \in \mathbb{F}_{2^m}.$$

Corollary 6.10 *Let m be odd and $\gcd(k, m) = \gcd(l, m) = 1$. Then $\mathcal{M}(b_k, b_l) = 2^{(m+1)/2}$ if and only if the function $x \mapsto x^{(2^k+1)/(2^l+1)}$ is maximal nonlinear.*

The following corollary explains all entries in the table indicated by \star_2 , since $(2^{3k} + 1)/(2^k + 1) = 2^{2k} - 2^k + 1$ is the Kasami exponent.

Corollary 6.11 *Let $m \equiv \pm 1 \pmod{3}$ and $\gcd(l, m) = 1$, then*

$$c_y(b_{3l}, b_l) \in \{\pm 2^{(m+1)/2}, 0\} \quad \text{for all } y \in \mathbb{F}_{2^m}.$$

Proof of Theorem 6.9. First, each crosscorrelation coefficient between two DD-functions is written in terms of crosscorrelation coefficients between m -functions. From Theorem 5.6 with Result 6.8 follows

$$c_a(b_k^{(s)}, b_l) = \sum_{x, z \in \mathbb{F}_{2^m}} \mathcal{W}(tr^{(3)})(x^{(2^k+1)/3}) \cdot \mathcal{W}(tr^{(3)})(z^{(2^l+1)/3} a^{-1/3}) \cdot \mathcal{W}(tr^{(t)})(xz^{-1/t})$$

where $t := (2^k + 1)/s(2^l + 1)$. This shows that the calculation of the crosscorrelation between two DD-functions is related to the calculation of the crosscorrelation between m -functions, when m is odd.

Let $s = 1$ and $c_b := \mathcal{W}(tr^{(t)})(b)$ where $t := (2^k + 1)/(2^l + 1)$. We transform

$$\begin{aligned} 2^{2m} c_a(b_k, b_l) &= \\ &= \sum_{x, z \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^3 + x^{(2^k+1)/3} y)} \right) \left(\sum_{w \in \mathbb{F}_{2^m}} (-1)^{tr(w^3 + z^{(2^l+1)/3} a^{-1/3} w)} \right) \\ &\quad \cdot \underbrace{\left(\sum_{v \in \mathbb{F}_{2^m}} (-1)^{tr(v^{(2^k+1)/(2^l+1)} + xz^{-(2^l+1)/(2^k+1)} v)} \right)}_{=c_b \text{ with } x=bz^{(2^l+1)/(2^k+1)}} \\ &= \sum_{b, z \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^3 + b^{(2^k+1)/3} z^{(2^l+1)/3} y)} \right) \\ &\quad \cdot \left(\sum_{w \in \mathbb{F}_{2^m}} (-1)^{tr(w^3 + z^{(2^l+1)/3} a^{-1/3} w)} \right) c_b \\ &= \sum_{b, w \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^3 + w^3)} \right) \underbrace{\left(\sum_{z \in \mathbb{F}_{2^m}} (-1)^{tr(z(b^{(2^k+1)/3} y + a^{-1/3} w))} \right)}_{= \begin{cases} 2^m & \text{if } w = a^{1/3} y b^{(2^k+1)/3} \\ 0 & \text{otherwise} \end{cases}} c_b \\ &= \sum_{b \in \mathbb{F}_{2^m}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^3 + ay^3 b^{(2^k+1)})} \right) c_b 2^m \\ &= \sum_{b \in \mathbb{F}_{2^m}} \underbrace{\left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y(1+ab^{(2^k+1)}))} \right)}_{= \begin{cases} 2^m & \text{if } b = a^{-1/(2^k+1)} \\ 0 & \text{otherwise} \end{cases}} c_b 2^m \\ &= 2^{2m} c_{a^{-1/(2^k+1)}}. \end{aligned}$$

We obtain $c_a(b_k, b_l) = \mathcal{W}(tr^{((2^k+1)/(2^l+1))})(a^{-1/(2^k+1)})$. □

Also \star_3 is explained. It is known that b_2 describes the quadratic residue sequence of period 31, and $b_2 = b_2^{(7)}$ since 7 is a quadratic residue modulo 31. Thus, for

$m = 5$ follows $Sp(b_2^{(7)}, b_1) = Sp(b_2, b_1)$, which is three-valued with $\pm 2^{(m+1)/2}$ and 0 by Corollary 6.11.

We would like to finish this section with some questions related to the table above and our results.

Question 6.12 *Do there exist more examples of Dillon-Dobbertin functions $b_k^{(s)}$ and b_l with $\mathcal{M}(b_k^{(s)}, b_l) = 2^{(m+1)/2}$ and the crosscorrelation spectrum is not three-valued, except the case \circ_1 in the table?*

The ternary sequences (see Section 3.2) corresponding to the crosscorrelation between DD-functions, which are indicated by a star in the table above, are not new. These ternary sequences are equivalent to the ternary sequences obtained from the crosscorrelation between m -functions. For $m = 7$, there are two more inequivalent ternary sequences (the open cases), which are not equivalent to ternary sequences corresponding to the crosscorrelation between m -functions.

Question 6.13 *Do there exist other DD-functions with a three-valued crosscorrelation spectrum and the corresponding ternary sequence is not equivalent to the known ones?*

Question 6.14 *Let b_k and $b_l^{(s)}$ be DD-functions. If $c_y(b_k^{(s)}, b_l) \in \{\pm 2^{(m+1)/2}, 0\}$ for all $y \in \mathbb{F}_{2^m}$, does this imply that $x \mapsto x^{s(2^k+1)/(2^l+1)}$ is maximum nonlinear?*

It is easy to see, that the converse is not true: Let $m = 11, k = 2, l = 3$ and $s = 9$, then $x^{s(2^k+1)/(2^l+1)} = x^5$ is maximum nonlinear, but the crosscorrelation spectrum $Sp(b_2, b_3^{(9)})$ contains more than three values.

In the case $s = 1$ the answer to Question 6.14 is yes and we even have "if and only if", see Corollary 6.10.

6.3 Crosscorrelation between GMW and Dillon-Dobbertin Functions

In this section, the crosscorrelation between DD-functions and GMW-functions is considered. We recall the following notations: Let $b_k : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be the Dillon-Dobbertin function with parameter k , and let $g_{s,e} : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be the GMW-function defined by $g_{s,e}(x) = tr_{s/1}(tr_{m/s}(x)^e)$, where $s|m$ and $\gcd(e, 2^s - 1) = 1$.

Note that the crosscorrelation function between $b_k^{(2^i d)}$ and $g_{s, 2^j e}$ is the same for all $i, j = 0, \dots, m - 1$ by definition.

In the following let $k \neq 1$ and $e \neq 1$, because b_1 and $g_{s,1}$ are m -functions. For $m \leq 15$ odd, we compute all crosscorrelation spectra $Sp(b_k^{(d)}, g_{s,e})$, but we get neither $\mathcal{M}(b_k^{(d)}, g_{s,e}) = 2^{(m+1)/2}$ nor a three-valued crosscorrelation spectrum. In the next table we list all crosscorrelation spectra, which contain at most five values.

m	s	k	d	e	$Sp(b_k^{(d)}, g_{s,e})$	
9	3	2	1	3	$\{-32, 0, 32, 64\}$	
9	3	2	5	3	$\{-64, -32, 0, 32\}$	*
9	3	4	1	3	$\{-32, 0, 32, 64\}$	
9	3	4	17	3	$\{-64, -32, 0, 32\}$	*
15	3	2	5	3	$\{-512, -256, 0, 256, 512\}$	*
15	3	4	17	3	$\{-512, -256, 0, 256, 512\}$	*
15	3	7	129	3	$\{-512, -256, 0, 256, 512\}$	*
15	5	4	1	3	$\{-512, -256, 0, 256, 512\}$	
15	5	4	1	11	$\{-512, -256, 0, 256, 512\}$	
15	5	4	17	3	$\{-1024, -256, 0, 256\}$	*

For the cases indicated by a star we can control the maximum crosscorrelation coefficient. Therefore, we write the crosscorrelation between $b_k^{(d)}$ and $g_{s,e}$ in terms of Walsh coefficients of m -functions and GMW-functions.

Theorem 6.15 *Let $m = rs$ be odd, $\gcd(k, m) = \gcd(d, 2^m - 1) = 1$. Then*

$$c_a(b_k^{(d)}, g_{s,e}) = \frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} \mathcal{W}(tr_{m/1}^{(3)}(x^{\frac{2^k+1}{3}})) \cdot \mathcal{W}(g_{s,e}^{(\frac{2^k+1}{d})})(a^{-\frac{d}{2^k+1}}x).$$

for all $a \in \mathbb{F}_{2^m}^*$.

Proof. We use formula (5.2) with the perfect function $tr_{m/1}^{(\frac{d}{2^k+1})}$ and get

$$\begin{aligned} c_a(b_k^{(d)}, g_{s,e}) &= \frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} c_x(b_k^{(d)}, tr_{m/1}^{(\frac{d}{2^k+1})}) \cdot c_{a^{-1}x}(g_{s,e}, tr_{m/1}^{(\frac{d}{2^k+1})}) \\ &= \frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} c_x(b_k^{(2^k+1)}, tr_{m/1}) \cdot c_{a^{-\frac{d}{2^k+1}}x}(g_{s,e}^{(\frac{2^k+1}{d})}, tr_{m/1}) \\ &= \frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} \mathcal{W}(b_k^{(2^k+1)})(x) \cdot \mathcal{W}(g_{s,e}^{(\frac{2^k+1}{d})})(a^{-\frac{d}{2^k+1}}x). \end{aligned}$$

Applying Result 6.8 completes the proof of Theorem 6.15. \square

Thus, the crosscorrelation function between a DD-function with a GMW-function is related to the crosscorrelation between m -functions and GMW-functions with

m -functions. It is proved in [1] that the calculation of the crosscorrelation between GMW-functions with m -functions can be reduced to the crosscorrelation between m -functions. Thus, the crosscorrelation between DD-functions with GMW-functions is related to the crosscorrelation between m -functions.

In some cases, we can write the crosscorrelation of GMW-functions with DD-functions in terms of the crosscorrelation between m -functions. Therefore, the next proposition is of interest.

Proposition 6.16 (Gordon, Mills and Welch [11]) *Let $m = rs$. Then*

$$\mathcal{W}(g_{s,e})(y) = \begin{cases} 2^{m-s}\mathcal{W}(tr_{s/1}^{(e)})(y) & \text{if } y \in \mathbb{F}_{2^s} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. In general we have: Let f and g be perfect functions with $f(0) = g(0) = 0$ and let A and B their supports in $\mathbb{F}_{2^m}^*$, then $|A| = |B| = 2^{m-1}$. By Proposition 1.2 we have for all crosscorrelation coefficients that $c_y(f, g) - 1 = n - 4(k - \lambda_{y^{-1}})$ holds for all $y \in \mathbb{F}_{2^m}^*$, where $n = 2^m - 1$ and $k = 2^{m-1}$. Thus

$$c_y(f, g) = 2^m - 4(2^{m-1} - \lambda_{y^{-1}}),$$

where λ_y is defined by $AB^{(-1)} = \sum_{y \in \mathbb{F}_{2^m}^*} \lambda_y y$.

Let $D := \{x \in \mathbb{F}_{2^m}^* \mid tr_{m/s}(x) = 1\}$ and $E := \{y \in \mathbb{F}_{2^s}^* \mid tr_{s/1}(y) = 1\}$. Then D is the relative Singer difference set in $\mathbb{F}_{2^m}^*$ with the forbidden subgroup $\mathbb{F}_{2^s}^*$ and E is the Singer difference set in $\mathbb{F}_{2^s}^*$. Note that the sets $DE^{(d)}$ with $\gcd(d, 2^s - 1) = 1$ are Singer type difference sets in $\mathbb{F}_{2^m}^*$, see Section 2.2. Furthermore, DE correspondent to $tr_{m/1}$ and $DE^{(1/e)}$ to $g_{s,e}$.

Let $E^{(1/e)}E^{(-1)} = \sum_{y \in \mathbb{F}_{2^s}^*} \mu_y y$, then

$$\begin{aligned} (DE^{(1/e)})(DE)^{(-1)} &= DD^{(-1)}E^{(1/e)}E^{(-1)} \\ &\stackrel{(1.12)}{=} (2^{m-s} + 2^{m-2s} \sum_{x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} x) \left(\sum_{y \in \mathbb{F}_{2^s}^*} \mu_y y \right) \\ &= 2^{m-s} \left(\sum_{y \in \mathbb{F}_{2^s}^*} \mu_y y \right) + 2^{m-2s} \sum_{x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} \sum_{y \in \mathbb{F}_{2^s}^*} x \mu_y y. \end{aligned}$$

If $x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*$ and $y \in \mathbb{F}_{2^s}^*$, then $xy \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*$. Now, let $z \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*$. For any $y \in \mathbb{F}_{2^s}^*$ exists one element $x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*$ such that $yx = z$. Thus

$$\sum_{x \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} \sum_{y \in \mathbb{F}_{2^s}^*} x \mu_y y = \sum_{z \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} z \sum_{y \in \mathbb{F}_{2^s}^*} \mu_y.$$

The sum on the right hand side is the number of difference pairs (y, y') with $y, y' \in E$, i.e. $\sum_{y \in \mathbb{F}_{2^s}^*} \mu_y = 2^{s-1} \cdot 2^{s-1}$. Finely we get

$$\begin{aligned} (DE^{(1/e)})(DE)^{(-1)} &= 2^{m-s} \left(\sum_{y \in \mathbb{F}_{2^s}^*} \mu_y y \right) + 2^{m-2s} \cdot (2^{s-1})^2 \sum_{z \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} z \\ &= 2^{m-s} \left(\sum_{y \in \mathbb{F}_{2^s}^*} \mu_y y \right) + 2^{m-2} \sum_{z \in \mathbb{F}_{2^m}^* \setminus \mathbb{F}_{2^s}^*} z. \end{aligned}$$

Let $(DE^{(1/e)})(DE)^{(-1)} = \sum_{x \in \mathbb{F}_{2^m}^*} \lambda_x x$. For the crosscorrelation coefficients follows

$$\begin{aligned} c_y(g_{s,e}, tr_{m/1}) &= 2^m - 4(2^{m-1} - \lambda_{y^{-1}}) \\ &= \begin{cases} 2^m - 4(2^{m-1} - 2^{m-s} \mu_{y^{-1}}) & \text{if } y \in \mathbb{F}_{2^s}^* \\ 2^m - 4(2^{m-1} - 2^{m-2}) & \text{otherwise} \end{cases} \\ &= \begin{cases} 2^{m-s}(2^s - 4(2^{s-1} - \mu_{y^{-1}})) & \text{if } y \in \mathbb{F}_{2^s}^* \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 2^{m-s} c_y(tr_{s/1}^{(e)}, tr_{s/1}) & \text{if } y \in \mathbb{F}_{2^s}^* \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

for all $y \in \mathbb{F}_{2^m}^*$. Since $\mathcal{W}(f)(y) = c_y(f, tr)$ and $\mathcal{W}(g_{s,e})(0) = 0 = \mathcal{W}(tr_{s/1}^{(e)})(0)$ Proposition 6.16 is proved. \square

In Theorem 6.15, we choose $d = 2^k + 1$. Then, by Proposition 6.16, we obtain

$$\begin{aligned} c_a(b_k^{(2^k+1)}, g_{s,e}) &= \frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} \mathcal{W}(tr_{m/1}^{(3)})(ax^{\frac{2^k+1}{3}}) \mathcal{W}(g_{s,e})(x) \\ &= \frac{1}{2^s} \sum_{x \in \mathbb{F}_{2^s}} \mathcal{W}(tr_{m/1}^{(3)})(ax^{\frac{2^k+1}{3}}) \mathcal{W}(tr_{s/1}^{(e)})(x). \end{aligned} \quad (6.8)$$

Now Theorem 6.15 is strengthened for the case $d = 2^k + 1$.

Theorem 6.17 *Let $m = rs$ be odd and k be an integer with $\gcd(k, m) = 1$ and $2^k + 1 \equiv 2^i \cdot 3 \pmod{2^s - 1}$ for some i . Then*

$$c_a(b_k^{(2^k+1)}, g_{s,e}) = c_a^{\frac{2^k+1}{3}}(tr_{m/1}^{(3)}, g_{s,e})$$

for all $a \in \mathbb{F}_{2^m}$.

Proof. Note, that $x^{\frac{2^k+1}{3}} = x^{2^i}$ for all $x \in \mathbb{F}_{2^s}$, since $2^k + 1 \equiv 2^i \cdot 3 \pmod{2^s - 1}$. We transform (6.8) and we obtain

$$\begin{aligned}
c_a(b_k^{(2^k+1)}, g_{s,e}) &= \frac{1}{2^s} \sum_{x \in \mathbb{F}_{2^s}} \left(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr_{m/1}(y^3) + tr_{m/1}(a^{\frac{2^k+1}{3}} x^{2^i} y)} \right) \cdot \left(\sum_{z \in \mathbb{F}_{2^s}} (-1)^{tr_{s/1}(z^e) + tr_{s/1}(xz)} \right) \\
&= \frac{1}{2^s} \sum_{y, z \in \mathbb{F}_{2^s}} (-1)^{tr_{m/1}(y^3) + tr_{s/1}(z^e)} \cdot \underbrace{\sum_{x \in \mathbb{F}_{2^s}} (-1)^{tr_{m/1}(a^{2^{-i} \frac{2^k+1}{3}} x y^{2^{-i}}) + tr_{s/1}(xz)}}_{= \begin{cases} 2^s & \text{if } tr_{m/s}(a^{\frac{2^k+1}{3}} y)^{2^{-i}} = z \\ 0 & \text{otherwise.} \end{cases}} \\
&= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr_{m/1}(x^3) + tr_{s/1}(tr_{m/s}(a^{\frac{2^k+1}{3}} x)^{2^{-i} e})}.
\end{aligned}$$

This proves Theorem 6.17, since $g_{s,e} \equiv g_{s,2^{-i}e}$. \square

In general, if $2^k + 1 \equiv 2^i \cdot 3 \pmod{2^s - 1}$ for some i , then the crosscorrelation spectrum contains many values. But an upper bound for the maximum crosscorrelation coefficient (in absolute value) can be calculated:

Theorem 6.18 *Let $m = rs$ be odd and k be an integer with $\gcd(k, m) = 1$. Let d and e be integers such that x^d is a maximum nonlinear function on \mathbb{F}_{2^m} and y^e is maximum nonlinear on \mathbb{F}_{2^s} . Then*

$$\mathcal{M}(tr_{m/1}^{(d)}, g_{s,e}) \leq 2^{\frac{m+s}{2}}.$$

Proof. We use formula (5.2) with $g = tr_{m/1}$ and then apply Proposition 6.16. We get

$$\begin{aligned}
c_a(tr_{m/1}^{(d)}, g_{s,e}) &= 2^{-m} \sum_{x \in \mathbb{F}_{2^m}} \mathcal{W}(tr_{m/1}^{(d)})(a^{-1}x) \cdot \mathcal{W}(g_{s,e})(x) \\
&= 2^{-s} \sum_{y \in \mathbb{F}_{2^s}} \mathcal{W}(tr_{m/1}^{(d)})(a^{-1}y) \cdot \mathcal{W}(tr_{s/1}^{(e)})(y)
\end{aligned}$$

Since y^e is maximum nonlinear, we have $|\{y \in \mathbb{F}_{2^s} \mid \mathcal{W}(tr_{s/1}^{(e)})(y) \neq 0\}| = 2^{s-1}$. We have $\mathcal{W}(tr_{m/1}^{(d)})(y) \in \{0, \pm 2^{\frac{m+1}{2}}\}$ for all $y \in \mathbb{F}_{2^m}$, since x^d is maximum nonlinear on \mathbb{F}_{2^m} . We obtain $|c_a(tr_{m/1}^{(d)}, g_{s,e})| \leq 2^{-s} \cdot 2^{\frac{m+1}{2}} \cdot 2^{\frac{s+1}{2}} \cdot 2^{s-1} = 2^{\frac{m+s}{2}}$ for all $a \in \mathbb{F}_{2^m}$. \square

The next corollary shows the maximum crosscorrelation coefficient (in absolute value) for the cases in the table above, which are indicated by a star. If $d \equiv 2^i e \pmod{2^s - 1}$ for some i and $d = 2^k + 1$ with $\gcd(k, m) = 1$, then the upper bound is attained:

Corollary 6.19 *Let $m = rs$ be odd and $\gcd(k, m) = 1$. Then*

$$\mathcal{M}(tr_{m/1}^{(2^k+1)}, g_{s,2^k+1}) = 2^{\frac{m+s}{2}}.$$

Proof. For the Gold exponent we have

$$\mathcal{W}(tr_{m/1}^{(2^k+1)})(y) = 2^{\frac{m-s}{2}} (-1)^{\frac{s^2+m^2-2}{8}} \mathcal{W}(tr_{s/1}^{(2^k+1)})(y)$$

for all $y \in \mathbb{F}_{2^s}$, which follows immediately from the fact that

$$\mathcal{W}(tr_{m/1}^{(2^k+1)})(y) = \begin{cases} 2^{\frac{m+1}{2}} (-1)^j & \text{if } y = z^{2^k} + z^{2^{-k}} + 1 \\ 0 & \text{if } tr_{m/1}(y) = 0, \end{cases}$$

where $j := \frac{m^2-1}{8} + tr_{m/1}(z^{2^k+1} + z)$, see [5]. Thus, for $a = 1$ we get

$$|c_1(tr_{m/1}^{(2^k+1)}, g_{s,2^k+1})| = 2^{\frac{m-3s}{2}} \sum_{y \in \mathbb{F}_{2^s}} \left(\mathcal{W}(tr_{s/1}^{(2^k+1)})(y) \right)^2 = 2^{\frac{m+s}{2}}.$$

□

Corollary 6.20 *Let $m = rs$ be odd, let k be an integer with $\gcd(k, m) = 1$ and $2^k + 1 \equiv 2^i \cdot 3 \pmod{2^s - 1}$ for some i and $e = 3$. Then*

$$\mathcal{M}(b_k^{(2^k+1)}, g_{s,3}) = 2^{\frac{m+s}{2}}.$$

Proof. This follows from Theorem 6.17 together with Corollary 6.19. □

We would like to finish this section with some questions.

For $m \leq 15$ odd, we compute all crosscorrelation spectra $Sp(b_k^{(d)}, g_{s,e})$ with $k \neq 1$ and $e \neq 1$, but we neither get $\mathcal{M}(b_k^{(d)}, g_{s,e}) = 2^{(m+1)/2}$ nor a three-valued crosscorrelation spectrum.

Question 6.21 *Does there exist a DD-function b_k , $k \neq 1$, and a GMW-function $g_{s,e}$, $e \neq 1$, such that $\mathcal{M}(b_k^{(d)}, g_{s,e}) = 2^{(m+1)/2}$?*

Question 6.22 *Let m odd. If there exists a DD-function b_k , $k \neq 1$, and a GMW-function $g_{s,e}$, $e \neq 1$, such that their crosscorrelation spectrum is three-valued?*

In the case of Corollary 6.20, the crosscorrelation spectrum consists of just a few values, since m is small. For $m = 21$ many different values are obtained. It is an interesting question to ask, for which numbers m and s the crosscorrelation spectrum contains only a few values.

Chapter 7

Two Notes on Power Functions

There are only four classes of maximum nonlinear power functions known, see Proposition 6.5. The two most important classes are the Gold power mappings and the Kasami power mappings.

In this chapter, some new properties of the Gold and Kasami power mappings are considered. In the first section, some similarities between these two parameters are listed. We prove a new property of the Kasami parameter. In the second section a characterisation of the Gold power mappings in terms of their distance to characteristic functions of subspaces of codimension 1 and 2 in \mathbb{F}_{2^m} is given.

Note that $\gcd(d, 2^m - 1) = 1$ for $d = 2^k + 1$ (Gold parameter) or $d = 2^{2k} - 2^k + 1$ (Kasami parameter), if $\gcd(k, m) = s$ and m/s is odd. It is $\gcd(2k, m) = \gcd(k, m)$ for m/s odd. We get

$$\gcd(2^k + 1, 2^m - 1) = \frac{\gcd((2^k+1)(2^k-1), 2^m-1)}{\gcd(2^k-1, 2^m-1)} = \frac{\gcd(2^{2k}-1, 2^m-1)}{\gcd(2^k-1, 2^m-1)} = \frac{2^{\gcd(2k, m)} - 1}{2^{\gcd(k, m)} - 1} = 1,$$

since $\gcd(2^k + 1, 2^k - 1) = 1$. In the Kasami case, $2^{2k} - 2^k + 1 = \frac{2^{3k} + 1}{2^k + 1}$ and with the equation above we have $\gcd(\frac{2^{3k} + 1}{2^k + 1}, 2^m - 1) = \gcd(2^{3k} + 1, 2^m - 1)$ and

$$\gcd(2^{3k} + 1, 2^m - 1) = \frac{\gcd(2^{6k} - 1, 2^m - 1)}{\gcd(2^{3k} - 1, 2^m - 1)} = \frac{2^{\gcd(6k, m)} - 1}{2^{\gcd(3k, m)} - 1} = 1.$$

7.1 A New Property of the Kasami Power Mappings

The work presented in this section is motivated by the observation that the function \mathbb{F}_{2^m} to \mathbb{F}_{2^m} defined by $x^d + (x + 1)^d + a$ for some $a \in \mathbb{F}_{2^m}$ can be used to construct difference sets. A necessary condition to do so is that the function

$\varphi_d : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ with

$$\varphi_d(x) := x^d + (x+1)^d$$

is a 2^s -to-1 mapping. If $s = 1$, then x^d must be APN. If $\gcd(k, m) = 1$, then the Gold and the Kasami power functions are APN.

Lemma 7.1 *Let the function φ_d be a c -to-1 mapping. Then the function $\varphi_{d'}$ is also a c -to-1 mapping for $d' \equiv 2^i d \pmod{2^m - 1}$ and if $\gcd(d, 2^m - 1) = 1$ for $d' \equiv 1/d \pmod{2^m - 1}$.*

Proof. The case $d' \equiv 2^i d \pmod{2^m - 1}$ is clear, since $\varphi_{2^i d}(x) = \varphi_d(x^{2^i})$. In the case $d' \equiv 1/d \pmod{2^m - 1}$, we have for fix $y \in \mathbb{F}_{2^m}^*$ with $x^d + (x+1)^d = y$, that $x^{1/d} + (x'+1)^{1/d} = y^{-1/d}$ holds for $x' := y^{-1}x^d$, because

$$\begin{aligned} (y^{-1}x^d)^{1/d} + ((y^{-1}x^d) + 1)^{1/d} &= y^{-1/d} && / \cdot y^{1/d} \\ x + (x^d + y)^{1/d} &= 1 && / + x \\ (x^d + y)^{1/d} &= x + 1 && / \wedge d \\ x^d + y &= (x + 1)^d. \end{aligned}$$

□

So far, up to equivalence there is only one value d known, where the function φ_d is a 2^s -to-1 mapping with $s > 1$:

Proposition 7.2 *Let $s = \gcd(k, m)$. The function φ_{2^k+1} is a 2^s -to-1 mapping.*

Proof. This follows from the fact that $\varphi_{2^k+1}(x) = x^{2^k} + x + 1$ is an affine function and the dimension of the kernel of the function $x^{2^k} + x$ is s , see [32]. □

For the Kasami exponent $d = 2^{2k} - 2^k + 1$, it is only known that 1 has exactly 2^s preimages under φ_d , if $s = \gcd(k, m)$, see [16]. In this section it is shown that φ_d is also a 2^s -to-1 mapping if d is the Kasami parameter $d = 2^{2k} - 2^k + 1$ with $\gcd(k, m) = s$ and m/s odd. We hope that this observation can be used to construct more difference sets.

The function φ_d can be used to construct difference sets: We define the set

$$D_{a,d} := \{ \varphi_d(x) + a \mid x \in \mathbb{F}_{2^m}, \varphi_d(x) \neq a \}$$

for $a \in \mathbb{F}_{2^m}$.

Result 7.3 *The set $D_{a,d}$ is an $(2^m - 1, 2^{m-1}, 2^{m-2})$ -difference set in $\mathbb{F}_{2^m}^*$ for*

1. $d = 2^k + 1$ or $d = 1/(2^k + 1)$ with $\gcd(k, m) = 1$ and m odd and $a = 0$. It is easy to show, that in this cases $D_{a,d}$ is the classical Singer difference set.
2. $d = 2^{2k} - 2^k + 1$ with $m = 3k \pm 1$ and $a = 0$. This was conjectured by No, Chung and Yun in [30] and proved by Dillon and Dobbertin in [4, 5].
3. $d = 2^{2k} - 2^k + 1$ with $\gcd(k, m) = 1$ and $a = 1$. This was shown by Dillon and Dobbertin in [5].

This result shows that the Gold and the Kasami exponent may give difference sets in the case $\gcd(k, m) = 1$. Now let us look at the case $\gcd(k, m) > 1$.

It may possible to construct relative difference sets. Relative difference sets are interesting because they can be used to construct difference sets using the Gordon-Mills-Welch method [34], see Chapter 2.

Proposition 7.4 *Let $\gcd(k, m) = s$ and m/s be odd and $a = 0$. Then the set $D_{a,d}$ is an $(\frac{2^m-1}{2^s-1}, 2^s-1, 2^{m-s}, 0, 2^{m-2s})$ -relative difference set in $\mathbb{F}_{2^m}^*$ for $d = 2^k + 1$ and $d = 1/(2^k + 1)$, respectively.*

Proof. The set $D_{0,2^k+1}$ is a relative Singer difference set, since $x \in D_{0,2^k+1}$ if and only if $\text{tr}_{m/s}(x) = 1$ for m/s odd, because $\text{tr}_{m/s}(x^{2^k} + x + 1) = \text{tr}_{m/s}(1) = 1$. Furthermore, $D_{0,1/d} = D_{0,d}^{(-1/d)}$, because $y \in D_{0,d}$ if and only if $y^{-1/d} \in D_{0,1/d}$, which follows from the proof of Lemma 7.1. \square

We have tried to construct such relative difference sets in a similar way. A necessary condition is that we have a 2^s -to-1 mapping. The function φ_d with d is the Kasami parameter has this property.

Theorem 7.5 *Let $\gcd(k, m) = s$ and m/s be odd. Then the function $\varphi_d : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ with $\varphi_d(x) = x^d + (x+1)^d$ and $d = 2^{2k} - 2^k + 1$ is a 2^s -to-1 mapping.*

To prove Theorem 7.5, the following two propositions are needed. The next proposition also shows another property that is shared by the Gold and Kasami exponents.

Proposition 7.6 [15] *Let $s = \gcd(m, k)$ and m/s be odd. Let $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$. Then $\mathcal{W}(\text{tr}^{(d)})$ takes on the following three values:*

value	multiplicity
$2^{(m+s)/2}$	$2^{m-s-1} + 2^{(m-s-2)/2}$
0	$2^m - 2^{m-s}$
$-2^{(m+s)/2}$	$2^{m-s-1} - 2^{(m-s-2)/2}$.

If $|\{x \in \mathbb{F}_{2^m} \mid \varphi_d(x) = y\}| \geq c$ for all $y \in \{\varphi_d(x) \mid x \in \mathbb{F}_{2^m}\}$, then φ_d is called at least a c -to-1 mapping.

Proposition 7.7 *Let d be an integer such that the function φ_d is at least a 2^s -to-1 mapping and the Walsh transform of $tr^{(d)}$ takes just the values $\pm 2^{(m+s)/2}$ and 0. Then the function φ_d is a 2^s -to-1 mapping.*

Note that in the case m odd and $d = 2^{2k} - 2^k + 1$ is the Kasami parameter with $\gcd(k, m) = 1$, the function φ_d is a 2-to-1 mapping, which follows immediately from Proposition 7.7, since any function φ_d is trivially by definition at least a 2-to-1 mapping, and $x^{2^{2k}-2^k+1}$ is maximum nonlinear. For the case $\gcd(k, m) > 1$, it is unapparent that the function $\varphi_{2^{2k}-2^k+1}$ is at least a 2^s -to-1 mapping.

Proof. Since $\mathcal{W}(tr^{(d)})(x) = c_x(tr^{(d)}, tr)$, we have by (6.6) that

$$\sum_{x \in \mathbb{F}_{2^m}} (\mathcal{W}(tr^{(d)})(x))^4 = 2^{2m} |\{(y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid \varphi_d(y) = \varphi_d(z)\}|. \quad (7.1)$$

From Proposition 7.6 we get $(\mathcal{W}(tr^{(d)})(x))^2 = 2^{m+s}$ exactly 2^{m-s} times and $(\mathcal{W}(tr^{(d)})(x))^2 = 0$ otherwise. Therefore, for the left hand side of (7.1) we calculate $\sum_{x \in \mathbb{F}_{2^m}} (\mathcal{W}(tr^{(d)})(x))^4 = (2^{m+s})^2 \cdot 2^{m-s} = 2^{3m+s}$. For the right hand side of (7.1) we have $|\{(y, z) \mid \varphi_d(y) = \varphi_d(z)\}| \geq 2^m \cdot 2^s$, since φ_d maps at least 2^s to 1. Therefore, φ_d must be a 2^s -to-1 mapping. \square

Proof of Theorem 7.5. We define $\phi_d : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ by

$$\phi_d(x) := \frac{1 + x^d}{(1 + x)^d}$$

for all $x \in \mathbb{F}_{2^m} \setminus \{1\}$ and $\phi_d(1) := 1$. If the mapping ϕ_d is at least a 2^s -to-1 mapping, then the mapping φ_d is also at least a 2^s -to-1 mapping, since

$$\varphi_d(0) = \phi_d(1) \quad \text{and} \quad \varphi_d(x) = \phi_d(x^{-1} + 1) \quad \text{for all } x \in \mathbb{F}_{2^m}^*, \quad (7.2)$$

because $\phi_d(x^{-1} + 1) = \frac{1+(x^{-1}+1)^d}{(1+x^{-1}+1)^d} = \frac{1+(x^{-1}+1)^d}{x^{-d}} = x^d + x^d(x^{-1} + 1)^d = x^d + (1 + x)^d$ and $\varphi_d(0) = 1 = \phi_d(1)$.

We show that the mapping $\phi_{2^{2k}-2^k+1}$ is at least a 2^s -to-1 mapping. Let $\alpha \in \mathbb{F}_{2^s}$, then $\phi_{2^{2k}-2^k+1}(\alpha) = 1$, since $\alpha^{2^s} = \alpha$ and therefore $\alpha^{2^{2k}-2^k+1} = \alpha$. Now let $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_{2^s}$. We have

$$\left(\phi_{2^{2k}-2^k+1}(x^{2^k+1})\right)^{2^k+1} = \frac{(1 + x^{2^{3k}+1})^{2^k+1}}{(1 + x^{2^k+1})^{2^{3k}+1}}. \quad (7.3)$$

Let l be an integer with $s \mid \gcd(l, m)$. Note that the function φ_{2^l+1} is at least a 2^s -to-1 mapping, since $\varphi_{2^l+1}(x) + 1$ is linear and the dimension of the kernel of

φ_{2^l+1} is divided by 2^s , i.e. \mathbb{F}_{2^s} is a subset of the kernel of φ_{2^l+1} . Thus, for $x \in \mathbb{F}_{2^m}$ all elements $x + u$, $u \in \mathbb{F}_{2^s}$, have the same image under φ_{2^l+1} .

Now, let $l = 3k$. We define

$$v := \varphi_{2^{k+1}}(\alpha) = \alpha^{2^k} + \alpha + 1 \quad \text{and} \quad w := \varphi_{2^{3k+1}}(\alpha) = \alpha^{2^{3k}} + \alpha + 1.$$

With our considerations above we get that for fixed α all elements $\alpha + u$, $u \in \mathbb{F}_{2^s}$, have the same image under $\varphi_{2^{k+1}}$ and $\varphi_{2^{3k+1}}$. We express v and w by the function ϕ_d . Since (7.2) holds, we get

$$v = \phi_{2^{k+1}}(\beta) = \frac{1 + \beta^{2^k+1}}{(1 + \beta)^{2^k+1}} \quad \text{and} \quad w = \phi_{2^{3k+1}}(\beta) = \frac{1 + \beta^{2^{3k}+1}}{(1 + \beta)^{2^{3k}+1}} \quad (7.4)$$

for all $\beta := (\alpha + u)^{-1} + 1$, $u \in \mathbb{F}_{2^s}$. We transform (7.4) and obtain

$$\begin{aligned} (1 + \beta^{2^{3k}+1})^{2^k+1} &= (w(1 + \beta)^{2^{3k}+1})^{2^k+1} \\ &= w^{2^k+1}((1 + \beta)^{2^k+1})^{2^{3k}+1} \\ &= w^{2^k+1}(v^{-1}(1 + \beta^{2^k+1}))^{2^{3k}+1} \\ &= w^{2^k+1}v^{-(2^{3k}+1)}(1 + \beta^{2^k+1})^{2^{3k}+1}. \end{aligned}$$

We rewrite this equation and get

$$\frac{(1 + \beta^{2^{3k}+1})^{2^k+1}}{(1 + \beta^{2^k+1})^{2^{3k}+1}} = w^{2^k+1}v^{-(2^{3k}+1)}.$$

Therefore, by (7.3) we obtain

$$\phi_{2^{2k-2k+1}}(\gamma) = wv^{-d}$$

for all $\gamma = ((\alpha + u)^{-1} + 1)^{1/(2^k+1)}$, $u \in \mathbb{F}_{2^s}$, since m/s is odd and therefore $\gcd(d, 2^m - 1) = 1$. We have shown that the function $\phi_{2^{2k-2k+1}}$ is at least a 2^s -to-1 mapping.

Therefore, the function $\varphi_{2^{2k-2k+1}}$ is also at least a 2^s -to-1 mapping. Proposition 7.6 together with Proposition 7.7 completes this proof. \square

We have tried to construct relative difference sets of Singer type by using $D_{a,d}$, where d is the Kasami parameter. Computer calculations indicate that $D_{a,d}$ is not a relative difference set in the cases $a = 0$ and $a = 1$.

Question 7.8 *Let $d = 2^{2k} - 2^k + 1$ and $\gcd(k, m) > 1$. Does there exist $a \in \mathbb{F}_{2^m}$ such that $D_{a,d}$ is a relative difference set in $\mathbb{F}_{2^m}^*$?*

7.2 A New Characterisation of the Gold Power Mappings

In this section, a characterisation of the Gold power mappings within the class of maximum nonlinear power mappings is given. The Walsh coefficients are interpreted in terms of the intersection between certain sets. Let

$$\begin{aligned} D_d &:= \{x \in \mathbb{F}_{2^m} \mid \text{tr}(x^d) = 1\} \\ H^i(\alpha) &:= \{x \in \mathbb{F}_{2^m} \mid \text{tr}(\alpha x) = i\} \end{aligned}$$

for $i = 0, 1$. If $\alpha \neq 0$, the sets $H^0(\alpha)$ and $H^1(\alpha)$ are (affine) subspaces of codimension 1 in \mathbb{F}_{2^m} (hyperplanes), i.e. they have size 2^{m-1} . We simply write \mathcal{W}_d for $\mathcal{W}(\text{tr}(x^d))$. For $\alpha \neq 0$, we have

$$\mathcal{W}_d(\alpha) = 2^m - 4|D_d \cap H^0(\alpha)| \quad \text{and} \quad -\mathcal{W}_d(\alpha) = 2^m - 4|D_d \cap H^1(\alpha)|, \quad (7.5)$$

see Section 1.3. Since $|D_d| = 2^{m-1}$, we have $\mathcal{W}_d(0) = 0$. The Walsh spectrum of a maximum nonlinear function is $\{0, \pm 2^{(m+1)/2}\}$, see Proposition 6.2. Therefore, a power mapping x^d with $\gcd(d, 2^m - 1) = 1$ is maximum nonlinear if and only if

$$|D_d \cap H^0(\alpha)|, |D_d \cap H^1(\alpha)| \in \{2^{m-2}, 2^{m-2} \pm 2^{\frac{m-3}{2}}\}$$

for all $\alpha \in \mathbb{F}_{2^m}^*$. This shows that maximum nonlinear power mappings x^d are characterised by the intersection sizes between hyperplanes and D_d .

In this section, the intersection sizes between D_d and (affine) subspaces of codimension 2 are considered. The subspaces are defined by

$$H^{i,j}(\alpha, \beta) := \{x \in \mathbb{F}_{2^m} \mid \text{tr}(\alpha x) = i, \text{tr}(\beta x) = j\}.$$

The Gold power mappings can be characterised in terms of these intersection sizes:

Theorem 7.9 *Let m be odd and let x^d be a maximum nonlinear power function on \mathbb{F}_{2^m} . Then $d = 2^k + 1$ for some integer k with $\gcd(k, m) = 1$ if and only if*

$$|H^{i,j}(\alpha, \beta) \cap D_d| \in \{2^{m-3}, 2^{m-3} \pm 2^{\frac{m-3}{2}}\} \quad (7.6)$$

for all $\alpha, \beta \in \mathbb{F}_{2^m}^*$, $\alpha \neq \beta$, and $i, j \in \mathbb{F}_2$.

The set D_d has some interesting properties: It is the set of 2^{m-1} points in the m -dimensional vector space \mathbb{F}_2^m over \mathbb{F}_2 . If d is a Gold exponent, this set is a non-degenerate quadric, see [8] and [20] for more background on quadrics in vector spaces over finite fields. If m is odd, there is up to equivalence only one

non-degenerate quadric in \mathbb{F}_{2^m} , and the intersection between this quadric and subspaces of codimension 2 must be the three values described in (7.6).

It is natural to ask whether there are values d such that D_d is not a non-degenerate quadric but has the same intersection sizes with hyperplanes. These objects are called by geometers **quasi-quadrics**. Many examples of quasi-quadrics are known, see [3]. Note that all maximum nonlinear power mappings yield quasi-quadrics. We asked the question whether the quasi-quadrics constructed from maximum nonlinear functions may also behave like quadrics if the intersection sizes with subspaces of codimension 2 are considered. The answer, given by Theorem 7.9, is no.

An interesting corollary is the following:

Corollary 7.10 *The only maximum nonlinear power mappings x^d on \mathbb{F}_{2^m} such that D_d is a quadric are the Gold power mappings.*

Before we are going to prove Theorem 7.9, let us mention the following Proposition, which may be of interest in its own:

Proposition 7.11 *Let m be odd and x^d be a maximum nonlinear power mapping on \mathbb{F}_{2^m} with $\gcd(d, m) = 1$. Then*

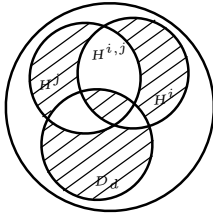
$$|H^{i,j}(\alpha, \beta) \cap D_d| \in \{2^{m-3} + h \cdot 2^{\frac{m-5}{2}} \mid -3 \leq h \leq 3\}, \quad (7.7)$$

where $\alpha, \beta \in \mathbb{F}_{2^m}^*$, $\alpha \neq \beta$.

Proof. We define

$$S^{i,j}(\alpha, \beta) = |H^{i,j}(\alpha, \beta) \cap D_d| \quad \text{and} \quad S^i(\alpha) = |H^i(\alpha) \cap D_d|.$$

Assume $\alpha \neq \beta$, $\alpha, \beta \in \mathbb{F}_{2^m}^*$. Walsh transform can be express by the intersection sizes $S^i(\alpha)$ and $S^{i,j}(\alpha, \beta)$. The picture shows that the Walsh transform (in absolute value) is the difference between the number of elements contained in the white set and the number of elements in the brindled set. We obtain



$$\begin{aligned} |\mathcal{W}_d(\alpha + \beta)| &= \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\alpha x + \beta x + x^d)} \right| \\ &= \left| \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(\alpha x + i + \beta x + j + x^d)} \right| \\ &= 2^m - 2((2^{m-1} - S^i(\alpha) - S^j(\beta) + S^{i,j}(\alpha, \beta)) \\ &\quad + (2^{m-1} - S^i(\alpha) - 2^{m-2} + S^{i,j}(\alpha, \beta)) \\ &\quad + (2^{m-1} - S^j(\beta) - 2^{m-2} + S^{i,j}(\alpha, \beta)) \\ &\quad + S^{i,j}(\alpha, \beta)) \\ &= -2^m + 4S^i(\alpha) + 4S^j(\beta) - 8S^{i,j}(\alpha, \beta). \end{aligned}$$

Because of (7.5), we have $|\mathcal{W}_d(\alpha + \beta)| = 2^m \pm \mathcal{W}_d(\alpha) \pm \mathcal{W}_d(\beta) - 8S^{i,j}(\alpha, \beta)$, hence

$$S^{i,j}(\alpha, \beta) = 2^{m-3} + \frac{1}{8}(\pm\mathcal{W}_d(\alpha + \beta) \pm \mathcal{W}_d(\alpha) \pm \mathcal{W}_d(\beta)). \quad (7.8)$$

This shows that there are only the seven possible values for $S^{i,j}(\alpha, \beta)$ stated in the Proposition. \square

The proof of Theorem 7.9 reduces to the proof of an interesting property of the trace function:

Theorem 7.12 *Let m be odd and $d \in \{3, \dots, 2^m - 2\}$ be odd. Then*

$$\text{tr}(x^d + (x + 1)^d + 1) = 0 \quad (7.9)$$

for all $x \in \mathbb{F}_{2^m}$, if and only if $d = 2^k + 1$ for some $k \in \mathbb{N}$.

At the same time, Theorem 7.12 was also proved in [27] and later a more general result, which contains Theorem 7.12, was proved in [25].

Let m be odd. If d satisfies (7.9) and x^d is APN, then $\{x^d + (x + 1)^d | x \in \mathbb{F}_{2^m}\} = \{x | \text{tr}(x) = 1\}$ is an affine hyperplane, since " \supseteq " follows from $|\{x^d + (x + 1)^d | x \in \mathbb{F}_{2^m}\}| = 2^{m-1} = |\{x | \text{tr}(x) = 1\}|$. A function $\varphi : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ with $\{\varphi(x) + \varphi(x + a) | x \in \mathbb{F}_{2^m}\}$ is an hyperplane or a complement of a hyperplane for all $a \in \mathbb{F}_{2^m}^*$ is called **crooked** function. Kyureghyan [26] shows that the only crooked power functions are the Gold power mappings.

The proof of Theorem 7.12 is postponed. First it is shown that it is sufficient to prove Theorem 7.12 in order to check Theorem 7.9.

Let x^d be a maximum nonlinear power function on \mathbb{F}_{2^m} , hence the Walsh spectrum $\{\mathcal{W}_d(\alpha) | \alpha \in \mathbb{F}_{2^m}\}$ contains only the three values $\pm 2^{\frac{m+1}{2}}$ and 0. We assume that (7.6) holds. The function $b : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ is defined as follows

$$b(\alpha) = \begin{cases} 1 & \text{if } \mathcal{W}_d(\alpha) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

If only one value or all values $\mathcal{W}_d(\alpha)$, $\mathcal{W}_d(\beta)$ and $\mathcal{W}_d(\alpha + \beta)$ in equation (7.8) are $\neq 0$, it is impossible that $S^{i,j}(\alpha, \beta) \in \{2^{m-3}, 2^{m-3} \pm 2^{\frac{m-3}{2}}\}$. Therefore, $b(\alpha) + b(\beta) = b(\alpha + \beta)$, hence b is linear and then

$$b(x) = \text{tr}(\gamma x) \quad (= \text{tr}^{[\gamma]}(x))$$

for some $\gamma \in \mathbb{F}_{2^m}^*$. If we think of $\text{tr}(x)$ as an element in \mathbb{C} , we obtain

$$\mathcal{W}(b)(\omega) = \mathcal{W}(\text{tr}^{[\gamma]})(\omega) = \sum_{z \in \mathbb{F}_{2^m}} \text{tr}(\gamma z) \cdot (-1)^{\text{tr}(\omega z)}$$

$$\begin{aligned}
&= \sum_{z \in \mathbb{F}_{2^m}, \text{tr}(\gamma z) = 1} (-1)^{\text{tr}(\omega z)} \\
&= \begin{cases} -2^{m-1} & \text{if } \omega = \gamma \\ 2^{m-1} & \text{if } \omega = 0 \\ 0 & \text{otherwise.} \end{cases} \quad (7.10)
\end{aligned}$$

On the other hand, the function b satisfies

$$b(x) = \frac{1}{2^{m+1}} (\mathcal{W}_d(x))^2.$$

We compute the Walsh transform again:

$$\begin{aligned}
\mathcal{W}(b)(\omega) &= \sum_{z \in \mathbb{F}_{2^m}} \frac{1}{2^{m+1}} (\mathcal{W}_d(z))^2 (-1)^{\text{tr}(\omega z)} \\
&= \frac{1}{2^{m+1}} \sum_{z \in \mathbb{F}_{2^m}} \left(\sum_{x, y \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(zx + x^d + zy + y^d)} \right) (-1)^{\text{tr}(z\omega)} \\
&= \frac{1}{2^{m+1}} \sum_{x, y \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(x^d + y^d)} \underbrace{\sum_{z \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(z(x+y+\omega))}}_{= \begin{cases} 2^m & \text{if } y = \omega + x \\ 0 & \text{otherwise} \end{cases}} \\
&= \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(x^d + (x+\omega)^d)}.
\end{aligned}$$

We compare this with (7.10) and obtain

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(x^d + (x+\omega)^d)} = \begin{cases} -2^m & \text{if } \omega = \gamma \\ 2^m & \text{if } \omega = 0 \\ 0 & \text{otherwise.} \end{cases} \quad (7.11)$$

The case $\omega = \gamma$ implies

$$\text{tr}(x^d + (x + \gamma)^d) = 1 \quad \text{for all } x \in \mathbb{F}_{2^m}. \quad (7.12)$$

We can show that necessarily $\gamma = 1$:

$$\text{tr}((x + \gamma)^d) \stackrel{(7.12)}{=} \text{tr}(x^d) + 1 = \text{tr}(x^{2^l}) + 1 \stackrel{(7.12)}{=} \text{tr}((x^{2^l} + \gamma)^d) = \text{tr}((x + \gamma^{2^{m-l}})^d)$$

for all $l = 0, \dots, m-1$ and $x \in \mathbb{F}_{2^m}$. Thus, we have $\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(x^d + (x + \gamma^{2^l})^d)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{tr}(x^d + (x + \gamma)^d)} = -2^m$ for all l . From the uniqueness of γ in (7.11) we get $\gamma^{2^l} = \gamma$ for all $l = 0, \dots, m-1$, and therefore $\gamma = 1$.

Since m is odd we have $\text{tr}(1) = 1$. Therefore

$$\text{tr}(x^d + (x + 1)^d + 1) = 0 \quad (7.13)$$

for all $x \in \mathbb{F}_{2^m}$. Theorem 7.12 implies that $d = 2^k + 1$ for some $k \in \mathbb{N}$. It is well known that x^d is maximum nonlinear only in the case $\gcd(k, m) = 1$, see Proposition 7.6. Therefore, it is enough to prove Theorem 7.12.

Proof of Theorem 7.12. Let d be an integer. Let $d = \sum_{i=0}^{n-1} d_i 2^i$ be the binary representation of d , then we denote the vector (d_n, \dots, d_0) by \bar{d} and the binary weight of \bar{d} by $w_H(d)$. In Theorem 7.12, all integers d that occur are less than $2^m - 1$, i.e. \bar{d} is a vector of length at most m . By adding 0's, if necessary, we assume that \bar{d} is always a vector of length m . Let $d' \equiv 2^i d \pmod{2^m - 1}$, then $\bar{d}' = \bar{d}^{[i]}$, where the indices are computed modulo m , i.e. we view \bar{d} as a ‘‘cyclic’’ vector, in particular $w_H(d') = w_H(d)$.

Two polynomials $p, q : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ are defined by

$$p(x) := x^d + (x+1)^d + 1 \quad \text{and} \quad q(x) := \text{tr}(p(x)) = \sum_{i=0}^{m-1} (p(x))^{2^i}.$$

Obviously, $q(0) = 0$, therefore we have to show that

$$q(\alpha) = 0 \quad \text{for all } \alpha \in \mathbb{F}_{2^m}^*. \quad (7.14)$$

Let $T = \{t_1, \dots, t_n\}$ denote the set of exponents which occur in p . The multiset $T(t)$ is defined by

$$T(t) = \{0 \leq s \leq 2^m - 2 \mid \bar{s}^{[i]} = \bar{t}, i = 0, \dots, m-1\}.$$

We obtain

$$q(x) = \sum_{t \in T} \sum_{s \in T(t)} x^s.$$

In order to prove (7.14), one must show that every exponent occurs an even number of times in $q(x)$.

If d satisfies (7.13), then each $d' \in \{2^i d \pmod{2^m - 1} \mid i = 0, \dots, m-1\}$ also satisfies (7.13). We choose the smallest odd d' , which satisfies (7.13), and from now on, we denote this element by d . Since $d \geq 3$ is odd, we have $w_H(d) \neq 1$. If $d = 2^k + 1$ is a Gold exponent, then $w_H(d) = 2$ and $q(x)$ satisfies (7.14) (note that $p(x) = x^{2^k} + x$ in this case). Hence we may assume $w_H(d) \geq 3$.

If $w_H(d) = 3$, then $d = 2^k + 2^l + 1$ and $k > l > 0$. For the polynomials p and q we obtain

$$\begin{aligned} p(x) &= x^{2^k+2^l} + x^{2^k+1} + x^{2^l+1} + x^{2^k} + x^{2^l} + x \\ q(x) &= \sum_{i=0}^{m-1} \left((x^{2^k+2^l})^{2^i} + (x^{2^k+1})^{2^i} + (x^{2^l+1})^{2^i} + x^{2^i} \right). \end{aligned}$$

In $p(x)$, the exponents of binary weight 1 (and of binary weight 2) occur three times, therefore we have an odd number of exponents of weight 1 (and of binary weight 2) in $q(x)$, and therefore $q(x)$ cannot satisfy (7.14). This argument can be generalised: If $z = w_H(d)$ then there are precisely $\binom{z}{i}$ exponents t in $p(x)$ with $w_H(t) = i$, $1 \leq t \leq d - 1$. Note that x^d and 1 do not occur in $p(x)$. If z is not a power of 2, at least one of these binomial coefficients is odd (Lucas Theorem). Therefore, we only have to consider the case $z = 2^n$, $n > 1$.

Let v be a binary vector of length m . A **subvector** $w = (w_{m-1}, \dots, w_0)$ of v is a binary vector $w \neq 0, v$ of length m such that $v_i = 0$ implies $w_i = 0$. The set of all subvectors of \bar{d} is the set of the binary vectors of the exponents that occur in $p(x)$, since the polynomials are defined over \mathbb{F}_{2^m} .

In order to show that (7.14) holds, we have to prove that the cardinality of the set

$$S(s) := \{\bar{s}^{[t]} \mid \bar{s}^{[t]} \text{ subvector of } \bar{d}, t = 0, \dots, m - 1\}$$

is even for all $s \in T$. Note, that $S(s)$ is not a multiset. The number $|S(s)|$ is the number of terms in the polynomial p , which are of the form $x^{2^t s}$.

We define a **gap** to be a substring v of the form $0\dots 0$. The number s of 0's in this substring is called the length of the gap, similarly for **runs** which are substrings of the form $1\dots 1$. If $v = (v_i v_{i+1} \dots v_j)$ is a substring, we say that the indices i, \dots, j are contained in v .

By the following algorithm we construct a subvector w of \bar{d} such that $|S(w)|$ is odd. Therefore q does not satisfy (7.14).

Algorithm

Input: binary vector $\bar{d} = (d_{m-1}, \dots, d_0)$ of weight 2^n , $n \in \mathbb{N}$, $n \geq 2$

Output: subvector w of \bar{d} such that $|S(w)|$ is odd

- (1) $z := w_H(d)$;
 $l :=$ maximum length of a run in \bar{d} ;
 $s :=$ multiplicity of a run of length l in \bar{d} ;
 $v :=$ run of length l ;
 $s_{old} := m + 1$; $x_{old} := 0$;
- (2) while (w is not defined) do
- (3) $y := (y_{m-1}, \dots, y_0)$ with

$$y_i = \begin{cases} 1 & \text{if } i \text{ is contained in a substring } v \text{ and } d_i \text{ is 1} \\ 0 & \text{otherwise.} \end{cases}$$
- (4) if $z \neq l \cdot s$ then $w := y$; end if;
- (5) if $z = l \cdot s$ then
 $x :=$ minimum length of a gap between two substrings v in y ;
 $L :=$ gap of length x ;

if $s = 1$ then
 (6) if $s_{old} = m + 1$ then $w := \bar{d} - (0\dots 010)$; end if;
 (7) if $s_{old} \neq m + 1$ then $w := (0\dots 0v_{old}L_{old}v_{old})$; end if;
 end if;
 (8) if $s = 2$ then $w := (0\dots 01Lv)$; end if;
 (9) if $s > 2$ then
 $s_{old} := s$; $l_{old} := l$; $x_{old} := x$; $L_{old} := L$; $v_{old} := v$;
 let v denote a substring of type $(v_{old}Lv_{old}\dots Lv_{old})$ in \bar{d}
 with maximum number of 1's;
 $l :=$ number of 1's in v ;
 $s :=$ multiplicity of v in \bar{d} ;
 end if;
 end if;
 end while;

The algorithm terminates if $z \neq l \cdot s$ or $s \leq 2$. Note, if the case $z \neq l \cdot s$ does not occur then there exists such an s , because $0 < s < s_{old}$ in each step in the algorithm.

Line (4): If $z \neq l \cdot s$, i.e. $y \neq \bar{d}$ and $w = y$ is a subvector of \bar{d} . We have $|S(w)| = 1$, because none of the cyclic shifts $w^{[t]} \neq w$ is a subvector of \bar{d} . Suppose the vector $w^{[t]}$ with $w^{[t]} \neq w$ is a subvector of \bar{d} . Note, that w and $w^{[t]}$ have the same number of 1. If $w^{[t]} \neq w$, then there exists a 1 in \bar{d} and this 1 is in $w^{[t]}$ and not in w . Because $w^{[t]}$ is a cyclic shift of w , this 1 is in a string v , therefore this 1 is in w . This is a contradiction to the definition of w .

Line (5): If $z = l \cdot s$, then $l = 2^{l'}$ and $s = 2^{s'}$. We denote the gaps between the runs v by L_j , $j = 1, \dots, s$. Then \bar{d} has the form

$$\bar{d} = (L_s v L_{s-1} v \dots L_2 v L_1 v).$$

The number of gaps is even. Since m is odd the number of 0's are odd, and therefore, the number of gaps with odd length and the number of gaps with even length is odd. Thus, the maximum and minimum gap have different length. Note, that by the choice of d odd, it follows that L_s is one of the maximum gaps and has length $> x$, the minimum length of a gap.

Line (6): If $z = l \cdot s$ with $s = 1$ and $s_{old} = m + 1$ then $l \geq 4$ and $\bar{d} = (0\dots 01\dots 1)$. For $w = \bar{d} - (0\dots 010)$ we have $|S(w)| = 1$.

Line (7): If $z = l \cdot s$ with $s = 1$ and $s_{old} \neq m + 1$, then $s_{old} \geq 4$. The vector \bar{d} has the form

$$\bar{d} = (L_s v) = (L_{s_{old}} v_{old} L v_{old} \dots L v_{old} L v_{old}),$$

where L is the gap of length x_{old} . We obtain $|S(w)| = s_{old} - 1$ is odd.

Line (8): If $s = 2$, then $\bar{d} = (L_2vL_1v)$. The gap L_2 is longer than the gap L_1 . It is easy to see $|S(w)| = 1$, since $l \geq 2$.

Line (9): The new initialisation for the next while loop. □

Example 7.13 *We illustrate the algorithm with an example. Here we have $m = 23$ and $d = 1 + 2^2 + 2^4 + 2^7 + 2^9 + 2^{11} + 2^{15} + 2^{17}$.*

Input: $\bar{d} = (00000101000101010010101)$

(1) $z := 8; l := 1; s := 8; v := 1; s_{old} := 24; x_{old} := 0;$

(3) $y := \bar{d}$

(5) $x := 1; L := 0;$

(9) $s_{old} := 8; l_{old} := 1; x_{old} := 0; L_{old} := 0; v_{old} := 1;$

$y = (00000\underline{101000101010010101})$

$l := 3; v := 10101; s := 2;$

(3) $y := (0000000000v00v);$

(4) $w := y;$

Output: $w := (00000000000101010010101)$

Conclusion

In this thesis, problems on the crosscorrelation between perfect sequences are solved. A lower bound for the maximum crosscorrelation coefficient (in absolute value) is given and some interesting properties on the dual sequences are shown. Crosscorrelation spectra between perfect sequences of period $4m - 1$, where m is not a power of 2, and of period $2^m - 1$, where m is odd, are calculated, and it is proven that certain series of perfect sequences have good crosscorrelation property. For further research we give some questions in the respective sections.

On the crosscorrelation a new equivalence is defined, called extended Hadamard equivalence. Extended Hadamard equivalence is a generalisation of the Hadamard equivalence, which was developed to prove that certain sequences of period $2^m - 1$ are perfect. Using extended Hadamard equivalence a method is explained to construct sequences with prescribed autocorrelation. In this thesis, we only used this method to search for perfect sequences, but it can also be used to construct sequences which correspond to relative difference sets. For further work, it would be interesting to look for such sequences in order to get new perfect sequences using the Gordon-Mills-Welch method.

Basic Symbol

$\mathbb{N}, \mathbb{Z}, \mathbb{C}$	natural numbers, integers, complex numbers,
\mathbb{Z}_n	residue class ring modulo n ,
$\gcd(\cdot, \cdot)$	greatest common divisor,
$\langle \cdot, \cdot \rangle$	inner product,
$\langle \cdot \rangle$	generate a group,
$\underline{a}, \underline{b}$	sequences,
$w(\cdot)$	difference between 0's and 1's, 25
$w_H(\cdot)$	Hamming weight, 9
$d_H(\cdot, \cdot)$	Hamming distance, 9
$\underline{a}^{[t]}, f^{[y]}$	shift, 9, 13
$\underline{a}^{(d)}, f^{(d)}$	decimation, 10, 13
\bar{a}	complement, 10
\underline{a}^d	dual sequence, 10
$C_t()$	auto- resp. crosscorrelation, 12
$c_t(), c'_t(), c_t^*, c_x()$	auto- resp. crosscorrelation, 9, 11, 14, 26, 29
$Sp(), Sp'(), Sp^*$	auto- resp. crosscorrelation spectrum, 9, 11, 14, 26, 29
\mathbb{F}_{p^m}	finite field with p^m elements,
$\mathbb{F}_{p^m}^*$	multiplicative group of \mathbb{F}_{p^m} ,
$tr, tr_{k \cdot l/k}$	trace function, 14
$\mathcal{M}(\cdot, \cdot)$	maximal crosscorrelation coefficient, 32, 46
$\mathcal{W}(\cdot), \mathcal{W}_d$	Walsh transform, 15, 72
$\mathcal{N}(\cdot)$	linearity, 54
$supp(\cdot)$	support, 12
$seq(\cdot)$	characteristic sequence, 12
$S_1, S_2 \subseteq S$	sets, subsets,
$\overline{S_1}$	complement of S_1 in S ,
$S_1 \cup S_2$	union of S_1 and S_2 ,
$S_1 \dot{\cup} S_2$	disjoint union of S_1 and S_2 ,
$S_1 \cap S_2$	intersection between S_1 and S_2 ,
$S_1 \times S_2$	direct product of S_1 and S_2 ,
$ S $	cardinality of S ,

Index

Sequences,

- autocorrelation, 9, 12
 - modified, 26, 29
 - spectrum, 9
- balanced, 10
- binary complement, 10
- crosscorrelation, 11, 12
 - modified, 26, 29
 - spectrum, 11
- decimation, 10
- dual sequence, 27
- equivalent, 10
- extended Hadamard equivalence, 36
- fundamental vector, 9
- generalised Parseval formula, 30
- Hamming weight, 9
- inverse formula, 29
- multiplier, 11
- perfect, 10
- period, 9
- realisation, 37
- (cyclic) shift, 9
- shift distinct, 11

Functions,

- almost perfect nonlinear (APN), 56
- autocorrelation, 14
- crosscorrelation, 14
- decimation, 13
- Hadamard equivalent, 36
- maximum nonlinear, 56
- m -function, 21
- perfect, 14
- realisation, 48
- shift, 13
- trace function, 14

Walsh transform, 15

Sets, Groups and Fields,

- complement, 13
- cyclotomic class, 19
- decimation, 13
- difference set, 13
 - Paley type difference set, 16
 - Singer type difference set, 16
 - relative difference set, 13
 - (relative) Singer difference set, 23
- translate, 12

Bibliography

- [1] M. Antweiler. Crosscorrelation of p -ary GMW sequences. *IEEE Transactions on Information Theory*, 40(4):1253–1261, 1994.
- [2] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Encyclopedia of Mathematics and its Applications. 69. Cambridge: Cambridge University Press, 1999.
- [3] F. De Clerck, N. Hamilton, C. M. O’Keefe, and T. Penttila. Quasi-quadrics and related structures. *Australas. J. Comb.*, 22:151–166, 2000.
- [4] J.F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography*, 17(1-3):225–235, 1999.
- [5] J.F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.
- [6] R.A. Games. Crosscorrelation of m -sequences and GMW-sequences with the same primitive polynomial. *Discrete Applied Mathematics*, 12:139–146, 1985.
- [7] D. G. Glynn. Two new sequences of ovals in finite Desarguesian planes of even order. *Lecture Notes in Mathematics*, 1036:217–229, 1983.
- [8] R. Gold. Maximal recursive sequences with 3-valued crosscorrelation functions. *IEEE Transactions on Information Theory*, 14:154–156, 1968.
- [9] S. W. Golomb and G. Gong. *Signal design for good correlation. For wireless communication, cryptography, and radar*. Cambridge: Cambridge University Press, 2005.
- [10] G. Gong and N. Y. Yu. Crosscorrelation properties of binary sequences with ideal two-level autocorrelation. *Sequences and Their Applications. Proceedings of the 4th international Conference (SETA’06), Beijing, China, Sept. 24-28, 2006*. Springer Verlag. *Lecture Notes in Computer Science*, 2006.

- [11] B. Gordon, W.H. Mills, and L.R. Welch. Some new difference sets. *Canadian Journal of Mathematics*, 14:614–625, 1962.
- [12] M. Hall. A survey of difference sets. *Proceedings of the American Mathematical Society*, 7:975–986, 1957.
- [13] T. Helleseth. Some results about the crosscorrelation function between two maximal linear sequences. *Discrete Mathematics*, 16:209–232, 1976.
- [14] T. Helleseth. On the crosscorrelation of m -sequences and related sequences with ideal autocorrelation. In *Sequences and their Applications. Proceedings of the 2nd international Conference (SETA '01), Bergen, Norway, May 13-17, 2001*, pages 34–45. Springer Verlag. Discrete Mathematics and Theoretical Computer Science, 2002.
- [15] T. Helleseth and P. V. Kumar. *Sequences with low correlation*, volume 1,2. Handbook of coding theory, North-Holland, Amsterdam, 1998.
- [16] T. Helleseth, J. Lahtonen, and P. Rosendahl. *On certain equations over finite fields and crosscorrelations of m -sequences*, volume 23, pages 169–176. K. Feng, H. Niederreiter and C. Xing, editors, Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic, 2004.
- [17] D. Hertel. Crosscorrelation properties of perfect sequences. In *Sequences and their Applications. Proceedings of the 3rd international Conference (SETA '04), Seoul, Korea, October 24-28, 2004*, pages 208–219. Springer Verlag. Lecture Notes in Computer Science, 2005.
- [18] D. Hertel. Crosscorrelation between GMW and Dillon-Dobbertin sequences. In *Sequence Design and its Application in Communications. Proceedings of the 2nd international Conference (IWSDA '05), Shimonoseki, Japan, Oct. 10-14, 2005*. IEICE Transactions on Fundamentals, 2006.
- [19] D. Hertel. Extended Hadamard equivalence. In *Sequences and their Applications. Proceedings of the 4rd international Conference (SETA '06), Beijing, China, Sept. 24-28, 2006*, pages 119–128. Springer Verlag. Lecture Notes in Computer Science, 2006.
- [20] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.
- [21] D. Jungnickel and A. Pott. Perfect and almost perfect sequences. *Discrete Applied Mathematics*, 95(1-3):331–359, 1999.
- [22] T. Kasami. The weight enumerator for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information Control*, 18:369–394, 1971.

- [23] A. Klapper, A. H. Chan, and M. Goresky. Correlation functions of geometric sequences. In *Advances in Cryptology, Proceedings Workshop, EUROCRYPT'90, Aarhus, Denmark, 1990*, volume 473, pages 214–221. Springer Verlag. Lecture Notes in Computer Science, 1991.
- [24] A. Klapper, A. H. Chan, and M. Goresky. Crosscorrelation of linear and quadratically related geometric sequences and GMW sequences. *Discrete Applied Mathematics*, 46(1):1–20, 1993.
- [25] G. Kyureghyan. Crooked maps in \mathbb{F}_{2^n} . preprint, 2006.
- [26] G. Kyureghyan. The only crooked power functions are $x^{2^k+2^l}$. preprint, 2006.
- [27] P. Langevin and P. Veron. On the non-linearity of power functions. *Designs, Codes Cryptography*, 37(1):31–43, 2005.
- [28] A. Maschietti. Difference sets and hyperovals. *Designs, Codes and Cryptography*, 14(1):89–98, 1998.
- [29] Y. Niho. On maximal comma-free codes. *IEEE Transactions on Information Theory*, 19:580–581, 1973.
- [30] J.S. No, H. Chung, and M.S. Yun. Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z + 1)^d$. *IEEE Transactions on Information Theory*, 44(3):1278–1282, 1998.
- [31] J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal. New binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. *IEEE Transactions on Information Theory*, 44(2):814–817, 1998.
- [32] K. Nyberg. Differentially uniform mappings for cryptography. *Advance in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science*, 765:55–64, 1994.
- [33] R.E.A.C. Paley. On orthogonal matrices. *Journal of Mathematical Physics, Massachusetts Institute of Technology*, 12:311–320, 1933.
- [34] A. Pott. *Finite Geometry and Character Theory*. Lecture Notes in Mathematics 1601. Berlin: Springer-Verlag, 1995.
- [35] J. Seberry and M. Yamada. *Hadamard matrices, sequences, and block designs*, volume 1,2. Contemporary design theory. Collection of Surveys, 1992.
- [36] B. Segre and U. Bartocci. Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.*, 18:423–449, 1971.

- [37] D. A. Shedd and D. V. Sarwate. Construction of sequences with good correlation properties. *IEEE Transactions on Information Theory*, 25:94–97, 1979.
- [38] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43:377–385, 1938.
- [39] D.A. Sprott and R.G. Stanton. A family of difference sets. *Canadian Journal of Mathematics*, 10:73–77, 1958.
- [40] T. Storer. Cyclotomy and difference sets. *Markham Publishing Co, Chicago III*, 1967.
- [41] L.R. Welch. Trace mappings in finite fields and shift register crosscorrelation properties. *Electrical Engineering Department Report, University Southern California*, 1969.