ON MAXIMAL PERIOD LINEAR SEQUENCES AND THEIR CROSSCORRELATION FUNCTIONS

by

CANAN KAŞIKCI

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

Sabanci University
Spring 2006

ON MAXIMAL PERIOD LINEAR SEQUENCES AND THEIR CROSSCORRELATION FUNCTIONS

APPROVED BY

Assist. Prof. Dr. Cem Güneri ....
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu ....

Prof. Dr. Henning Stichtenoth ....

Prof. Dr. Albert Erkip ....

Assist. Prof. Dr. Erkay Savaş ....

DATE OF APPROVAL: ....

to my family

ON MAXIMAL PERIOD LINEAR SEQUENCES AND THEIR CROSSCORRELATION FUNCTIONS

Canan Kaşıkcı

Mathematics, Master of Science Thesis, 2006

Thesis Supervisor: Assist. Prof. Dr. Cem Güneri

Keywords: m-sequence, crosscorrelation, cyclic code, McEliece's theorem, nonlinear functions.

Abstract

For an n^{th} order linear recurring sequence over the finite field $\mathbb{F}_p$, the largest possible period is $p^n - 1$. When such a sequence attains this upper bound as its period, it is called a maximal period linear sequence, or m-sequence in short. Interest in such sequences originated from applications. Indeed, there is an interaction between m-sequences, coding theory and cryptography via the relation with cyclic codes, Boolean functions, etc. One of the main goals is to construct a pair of binary m-sequences whose crosscorrelation takes few values, preferably with small magnitude. By a theorem of Helleseth, the crosscorrelation function takes at least three values. Hence, existence and construction of sequences with 3-valued crosscorrelation is of particular interest. This is also the main theme of our work.

The aim of this thesis is to introduce foundational material on m-sequences, explain the relations with other topics mentioned above, and to present proofs of three conjectures on the existence/nonexistence of 3-valued crosscorrelation functions for binary m-sequences. These conjectures are due to Sarwate-Pursley, Helleseth and Welch and were proved by McGuire-Calderbank, Calderbank-McGuire-Poonen-Rubinstein and Canteaut-Charpin-Dobbertin respectively.

MAKSİMUM PERİODLU DOĞRUSAL DİZİLER VE ÇAPRAZ İLİNTİ FONKSİYONLARI

Canan Kaşıkcı

Matematik, Yüksek Lisans Tezi, 2006

Tez Danışmanı: Yar. Doç. Cem Güneri

Anahtar Kelimeler: m-dizisi, çapraz ilinti, devirsel kod, McEliece'in teoremi, doğrusal olmayan fonksiyon.

Özet

Mertebesi n olan ve sonlu $\mathbb{F}_p$ cismi üzerinde tanımlı bir doğrusal yinelemeli dizi için mümkün en büyük period $(p^n - 1)$'dir. Periodu bu üst sınıra eşit olan böyle dizilere maksimum periodlu doğrusal diziler ya da kısaca m-dizileri denir. Bu tip dizilere olan ilgi uygulamalardan kaynaklanmıştır. Gerçektende m-dizileri, kodlama teorisi ve şifreleme konuları devirsel kodlar, Boole fonksiyonları, vb. ilişkilerle yakın temas halindedirler. En önemli amaçlardan biri çapraz ilinti fonksiyonları az sayıda, ve tercihen küçük, değerlere sahip ikili m-diziler inşasıdır. Helleseth'in teoremine göre çapraz ilinti fonksiyonu genelde en azından üç tane değere sahiptir. Dolayısıyla 3-değerli çapraz ilinti fonksiyonlarının varlığı ve inşası çok ilgi uyandırır. Bu aynı zamanda bizim çalışmamızın da ana temasıdır.

Bu tezin amacı m-dizilerinin temel konularına giriş yapmak, yukarda bahsi geçen diğer konularla olan ilişkileri açıklamak ve 3-değerli çapraz ilinti fonksiyonlarının varlığı üzerine yapılmış üç farklı önsavın ispatlarını vermektir. Bu önsavlar Sarwate-Pursley, Helleseth ve Welch'e ait olup ispatları sırasıyla McGuire-Calderbank, Calderbank-McGuire-Poonen-Rubinstein ve Canteaut-Charpin-Dobbertin tarafından verilmiştir.

Acknowledgments

First of all, I would like to thank to the Mathematics Program of Sabancı University for supporting me and creating a warm and friendly atmosphere that I enjoyed all through my studies. I would gratefully like to thank my supervisor Cem Güneri for his encouragement and guidance at all stages of my work. Last but by no means least, I would like to thank my family with all my heart for all their love and encouragement that I received all through my life, and to my dear friends Güler, Bahar, Başak, Cenk, Ali for their support and friendship.

Contents

CHAPTER 1

INTRODUCTION

In this section, we present foundational material on m-sequences, cyclic codes and the relations between two subjects. For m-sequences, our references are [11] and [13], whereas we refer to [16] for coding theory parts. We assume basic knowledge on finite fields. Therefore, other than recalling the definition and basic properties of the trace function, we do not give further information on finite fields.

1.1 Linear Recurring Sequences and m-Sequences

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

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

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

Definition 1.1.1. Let n be a positive integer, and let $c_1, ..., c_n$ be elements of $\mathbb{F}_p$. A sequence $s_0, s_1 ...$ of elements of $\mathbb{F}_p$ satisfying the recurrence relation

$$s_t = c_1 s_{t-1} + c_2 s_{t-2} + ... + c_n s_{t-n} \tag{1.1}$$

for all $t \geq n$ is called an *n^{th}-order linear recurring sequence over* $\mathbb{F}_p$. The terms $s_0, s_1, ..., s_{n-1}$ which determine the rest of the sequence together with the recurrence relation are called *initial values.*

Given a sequence (s_t), the least positive integer r for which $s_{t+r} = s_t$ for all $t \geq 0$ is called the *period* of (s_t). Sequences for which such a number r exists are called *periodic.* It is easy to see that an n^{th} order linear recurring sequence is "ultimately periodic" (i.e. there exists t_o, r such that $s_{t+r} = s_t$ for all $t \geq t_o$) with period $r \leq p^n - 1$.

Definition 1.1.2. Given the recurrence relation (1.1) the polynomial $f(x)$

$$f(x) = x^n - c_1 x^{n-1} - c_2 x^{n-2} - \ldots - c_n \ \in \ \mathbb{F}_p[x] \tag{1.2}$$

is called the *characteristic polynomial* of the corresponding linear recurring sequence.

Characteristic polynomial yields a trace representation for its recurring sequence:

Theorem 1.1.1. *If the characteristic polynomial $f(x)$ is irreducible of degree n, then for any $\theta \in \mathbb{F}_{p^n}$, the sequence (s_t) defined by $s_t = Tr(\theta\alpha^t)$, where α is a root of $f(x)$, satisfies the recurrence relation (1.1). Conversely, given a sequence (s_t) satisfying the linear recurrence relation (1.1), there exists a unique $\theta \in \mathbb{F}_{p^n}$ such that $s_t = Tr(\theta\alpha^t)$ holds.*

Proof. Since α is a root of the characteristic polynomial we have

$$\alpha^n = \sum_{i=1}^{n} c_i \alpha^{n-i}.$$

Consider

$$s_t = Tr(\theta\alpha^t) = Tr(\theta\alpha^{t-n}\alpha^n) = Tr(\theta\alpha^{t-n}\sum_{i=1}^{n} c_i\alpha^{n-i}) = \sum_{i=1}^{n} Tr(c_i\theta\alpha^{t-i})$$

$$= \sum_{i=1}^{n} c_i Tr(\theta\alpha^{t-i}) = \sum_{i=1}^{n} c_i s_{t-i}.$$

Thus $s_t = Tr(\theta\alpha^t)$ satisfies the recurrence relation. For the converse, first note that there are exactly p^n distinct solutions corresponding to the p^n choices for the initial values $s_0, s_1, ..., s_{n-1}$. There are also p^n solutions to the recurrence (1.1) in the form $s_t = Tr(\theta\alpha^t)$ corresponding to the p^n choices for θ. We have to show that these p^n solutions are distinct. Suppose that for distinct $\theta_1, \theta_2 \in \mathbb{F}_{p^n}$, we have $Tr(\theta_1\alpha^t) = Tr(\theta_2\alpha^t)$ for all t or equivalently $Tr((\theta_1 - \theta_2)\alpha^t) = 0$ for all t. Since $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, having $\theta_1 \neq \theta_2$ implies that the trace map is identically zero. This is a contradiction. So, the sequences must be distinct. □

Definition 1.1.3. Two solutions s_t and v_t of the linear recurrence relation are *cyclically equivalent* if there exists $i > 0$ such that $v_t = s_{t+i}$ for all $t \geq 0$.

Remark 1.1.1. When the characteristic polynomial of the recurrence relation is irreducible we have $s_t = Tr(\theta\alpha^t)$ and $v_t = Tr(\theta'\alpha^t)$. Then cyclic equivalence of s_t and v_t implies that $Tr(\theta'\alpha^t) = Tr(\theta\alpha^{t+i})$, that is $Tr((\theta' - \theta\alpha^i)\alpha^t) = 0$. Hence $\theta' = \theta\alpha^i$ and the elements θ, θ' which produce cyclically equivalent sequences must be contained in the same coset of the subgroup $H = \{1, \alpha, \alpha^2, ..., \alpha^{ord(\alpha)-1}\}$ of $\mathbb{F}_{p^n}^*$. So the number of equivalence classes (with respect to cyclic equivalence) is equal to $|\mathbb{F}_{p^n}^* : H| = \frac{p^n-1}{ord(\alpha)}$. Thus, when the characteristic polynomial is primitive all solutions to the recurrence are cyclically equivalent.

Theorem 1.1.2. *Let $s_0, s_1, ...$ be a nonzero linear recurring sequence over $\mathbb{F}_p$. Suppose that the corresponding characteristic polynomial $f(x)$ is irreducible over $\mathbb{F}_p$ with $f(0) \neq 0$. Then the sequence is periodic with period $ord(f(x))$, where $ord(f(x))$ is the least positive integer e such that $f(x)$ divides $x^e - 1$.*

Definition 1.1.4. A nonzero linear recurring sequence $s_0, s_1, ...$ over $\mathbb{F}_p$ whose characteristic polynomial is a primitive polynomial over $\mathbb{F}_p$ is called a *maximal period linear sequence (m-sequence)* over $\mathbb{F}_p$.

Note that by Theorem 1.1.2, the period of an n^{th} order m-sequence over $\mathbb{F}_p$ is $p^n - 1$. Also note that an m-sequence (s_t) can be represented as

$$s_t = Tr(\theta\gamma^t) \tag{1.3}$$

where $\theta \in \mathbb{F}_{p^n}^*$ and γ is root of the characteristic polynomial of (s_t). Hence, γ is a primitive element of $\mathbb{F}_{p^n}$.

Theorem 1.1.3. *There exist $\frac{\varphi(p^n-1)}{n}$ maximal linear sequences of n^{th} order which are not equivalent under cyclic shifts.*

Proof. We observed that the solutions of a recurrence relation which has a primitive characteristic polynomial are cyclically equivalent, that is two maximal linear sequences with period $p^n - 1$ will be cyclically equivalent if and only if they are the solutions of the same n^{th} order linear recurrence relation over $\mathbb{F}_p$. Thus the number of maximal linear sequences will be the number of primitive polynomials of degree n over $\mathbb{F}_p$. □

Definition 1.1.5. Given a sequence (s_t) and any integer $d \geq 1$.A d^{th} *decimation* of (s_t) is a sequence (r_t) which is obtained by taking every d^{th} term from (s_t), i.e. $r_t = s_{td}$ for all $t \geq 0$.

Theorem 1.1.4. *Let (s_t) be an m-sequence of period $p^n - 1$. Then (s_{td}) is an m-sequence if and only if $(d, p^n - 1) = 1$.*

Proof. Since (s_t) is an m-sequence, we have $s_t = Tr(\theta\gamma^t)$, where $\theta \in \mathbb{F}_{p^n}^*$ and $\langle\gamma\rangle = \mathbb{F}_{p^n}^*$. Note that $r_t = s_{td} = Tr(\theta\gamma^{td})$ is an m-sequence if and only if $\langle\gamma^d\rangle = \mathbb{F}_{p^n}^*$, which holds if and only if $(d, p^n - 1) = 1$. □

Theorem 1.1.5. *Let s_t and v_t be two different m-sequences of period $p^n - 1$. Then there exist integers k and d where $(d, p^n - 1) = 1$ such that $v_{t+k} = s_{dt}$.*

Proof. After suitable shifts for both s_t and v_t we can obtain, $s_{t+\tau_1} = s_t^{'} = Tr(\gamma^t)$ and $v_{t+\tau_2} = v_t^{'} = Tr(\beta^t)$ where γ, β are the roots of the corresponding characteristic polynomials. Now choose $(d, p^n - 1) = 1$ such that $\beta = \gamma^d$. Then we have $v_t^{'} = s_{dt}^{'}$, which implies $v_{t+\tau_2} = s_{dt+d\tau_1}$. Now replacing t by $t - \tau_1$, we will have $s_{dt} = v_{t-\tau_1+\tau_2}$. □

Remark 1.1.2. For many purposes, shifting a given sequence cyclically is not important. Therefore, Theorem 1.1.5 essentially says that two m-sequences are related via a suitable decimation d.

Let ξ be a primitive complex p^{th} root of unity. Recall that the *canonical additive character* of $\mathbb{F}_{p^n}$ is defined as

$$\chi(x) = \xi^{Tr(x)}$$

where $x \in \mathbb{F}_{p^n}$. Properties of the trace function implies that,

$$\chi(x + y) = \chi(x)\chi(y) \text{ and } \chi(x^p) = \chi(x).$$

Another well-known fact is the following:

$$\sum_{a \, \in \, \mathbb{F}_{p^n}} \chi(ax) = \begin{cases} p^n & \text{if } x = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Definition 1.1.6. Let (s_t) and (v_t) be sequences over $\mathbb{F}_p$ with period ϵ, and let ξ be a primitive complex p^{th} root of unity. Then the *crosscorrelation function* $\Theta_{s,v}$ between the sequences s_t and v_t is defined for $l = 0, ..., \epsilon - 1$ as

$$\Theta_{s,v}(l) = \sum_{t=0}^{\epsilon-1} \xi^{s_{t-l} - v_t}.$$

Remark 1.1.3. For binary sequences s_t and v_t of period ϵ we have

$$\Theta_{s,v}(l) = \sum_{t=0}^{\epsilon-1} (-1)^{s_{t-l} - v_t},$$

which is the number of agreements minus the number of disagreements between the bits of s_{t-l} and v_t over the period ϵ.

From now on we assume that the sequences (s_t) and (v_t) are m-sequences of period $p^n - 1$. We can assume that after suitable shifts, $s_t = Tr(\gamma^t)$, where γ is a primitive element of $\mathbb{F}_{p^n}$, and $v_t = s_{dt}$ for an integer d with $(d, p^n - 1) = 1$. Then the crosscorrelation function between s_t and v_t will be denoted as $\Theta_d(l)$ for $l = 0, ..., p^n - 2$ and we have

$$\Theta_d(l) = \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-l})-Tr(\gamma^{dt})} = \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-l}-\gamma^{dt})} = \sum_{x\in\mathbb{F}_{p^n}^*} \xi^{Tr(yx-x^d)} = \sum_{x\in\mathbb{F}_{p^n}^*} \chi(yx - x^d)$$

where χ is the canonical additive character and $y = \gamma^{-l}$.

Remark 1.1.4. Since which of the sequences is shifted relative to the other does not matter, and replacing the element y with $-y$ will not change the values of the crosscorrelation funcion, we also have

$$\Theta_d(l) = \sum_{x\in\mathbb{F}_{p^n}^*} \chi(x - yx^d) = \sum_{x\in\mathbb{F}_{p^n}^*} \chi(x + yx^d)$$

where $y = \gamma^{-dl}$.

Remark 1.1.5. When we have $d = 1$, that is (s_t) and (v_t) are the same m-sequences, $\Theta_1(l) = \sum_{x\in\mathbb{F}_{p^n}^*} \chi(x(1-y))$ denotes the *autocorrelation* function. By the properties of canonical additive character we have

$$\Theta_1(l) = \begin{cases} p^n - 1 & \text{if } y = 1 \\ -1 & \text{otherwise} \end{cases}$$

Since $y = \gamma^{-dl}$, we have

$$\Theta_1(l) = \begin{cases} p^n - 1 & \text{if } l \equiv 0 \bmod (p^n - 1) \\ -1 & \text{otherwise} \end{cases}$$

1.2 Cyclic Codes

Let $\mathbb{F}_q$ denote the finite field with q elements. Let $\mathbb{F}_q^n$ be the n-dimensional vector space whose elements are the n-tuples $(c_0, c_1, ..., c_{n-1})$ where $c_i \in \mathbb{F}_q$. A *linear code* C is a subspace of $\mathbb{F}_q^n$. The elements of C are called *codewords*. The *length* of C is n and the *dimension* of C is its dimension as a vector space over $\mathbb{F}_q$. A linear code of length n and dimension k over $\mathbb{F}_q$ is denoted by $[n, k]_q$. For any linear code $C \subseteq \mathbb{F}_q^n$, we define the *dual code* $C^\perp \subseteq \mathbb{F}_q^n$ by

$$C^\perp = \left\{ d \in \mathbb{F}_q^n : d.c = 0, \forall c \in C \right\}.$$

Note that $C^\perp$ is an $[n, n-k]_q$ linear code. Now, we introduce a metric on $\mathbb{F}_q^n$, which will be used to define another important parameter of a linear code. For $x = (x_1, ..., x_n)$

and $y = (y_1, ..., y_n)$, define the *Hamming distance* by

$$d(x, y) = |\{1 \leq i \leq n : x_i \neq y_i\}|\,.$$

The *Hamming weight* $w(x)$ is the number of nonzero coordinates of x. For a given linear code C in $\mathbb{F}_q^n$ we define its *minimum distance* as

$$d(C) = \min\{w(c) : c \in C \backslash \{0\}\}$$

Let C be an $[n, k]_q$ code. The sequence $A_0, A_1, ..., A_n$ is called the *weight distribution* of C, where

$$A_i = |\{x \ \in \ C : \ w(x) = i\}|\,.$$

Another way to present weights of C is by forming the polynomial

$$W_C(x) = \sum_{i=0}^{n} A_i x^i.$$

Definition 1.2.1. A linear code C in $\mathbb{F}_q^n$ is called *cyclic* if $(c_0, c_1, ..., c_{n-1}) \in C$ implies $(c_{n-1}, c_0, ..., c_{n-2}) \in C$.

Considering the isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/(x^n - 1)$ given by

$$a = (a_0, a_1, ..., a_{n-1}) \longmapsto a(x) = \sum_{i=0}^{n-1} a_i x^i$$

we can view any code C as a subset of $\mathbb{F}_q[x]/(x^n-1)$, where the codeword a is identified by the polynomial $a(x)$.

Theorem 1.2.1. *A linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$.*

Since $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal ring every nonzero ideal C is generated by a monic polynomial $g(x)$ of lowest degree in the ideal. Note that $g(x)$ divides $x^n - 1$.

Definition 1.2.2. Let $C = \langle g(x) \rangle$ be a cyclic code. Then $g(x)$ is called the *generator polynomial* of C and $h(x) = \frac{x^n-1}{g(x)}$ is called *the parity check polynomial* of C. We have $\dim(C) = n - \deg(g(x))$.

It is easy to see that the dual code of a cyclic code ia also cyclic. One can easily show that the generator polynomial of $C^\perp$ is $\frac{x^k h(x^{-1})}{h(0)}$, where $h(x)$ is the parity check polynomial of C and $k = \deg h$. Throughout this thesis we will assume that $(n, q) = 1$.

In fact we will usually have $n = q^m - 1$ where $m > 1$. This implies that $x^n - 1$ (and hence $g(x)$) is separable. If $\langle \alpha \rangle = \mathbb{F}_{q^m}^*$, then $x^n - 1 = \prod_{s \in S} m_{\alpha^s}(x)$, where the product is taken over a set S of representatives of the q-cyclotomic cosets modulo n, i.e. $m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i)$ where $C_s = \{s, sq, sq^2, ..., sq^{r-1}\} \pmod{n}$ and r is the smallest integer such that $sq^r \equiv s \pmod{n}$. Therefore, $g(x)$ is the product of some of these minimal polynomials, whose indices come from a subset I of S. Then $\{\alpha^i : i \in I\}$ is called the set of *basic zeros* of the cyclic code C, whereas the set $\{\alpha^i : i \notin I\}$ will be the set of *basic nonzeros* of C. From the generator polynomial of $C^\perp$, it is clear that $\{\alpha^{-i} : i \notin I\}$ is the *basic zero set* of $C^\perp$. We obtain the *zero* (resp. *nonzero*) set of C by listing all of the basic zeros (resp. basic nonzeros) together with their $\mathbb{F}_q$-conjugates.

We finish our survey on cyclic codes with an important result of McEliece which puts constraints on possible weights in a cyclic code. This theorem will be frequently used in Chapters 3 and 4. We refer to [12] for the proof.

Theorem 1.2.2. *Let C be a binary cyclic code, and let l be the smallest number such that $l+1$ nonzeros of C (with repetitions allowed) have product 1. Then the weight of every codeword in C is divisible by 2^l, and there is at least one weight which is not divisible by 2^{l+1}.*

At the end of this section, we will explain an equivalent form of this theorem for certain cyclic codes of interest.

1.3 Relations Between Binary m-sequences and Cyclic Codes

To begin with let α be a primitive of $\mathbb{F}_{2^m}$. Let $m_i(x)$ be the minimal polynomial of α_i and set $h_i(x) = \frac{x^{2^m-1}-1}{m_i(x)}$ and $h_i^* = x^{\deg h_i} h_i(x^{-1})$. We will consider the binary cyclic code C_i of length $n = 2^m - 1$ with generator polynomial $m_i(x)$, i.e. cyclic code with the basic zero α^i. Note that $\dim C_i = n - d_i$ where $d_i = \deg(m_i(x))$. The dual code $C_i^\perp$ of consists of codewords which are multiples of h_i^*.

Definition 1.3.1. Binary cyclic code C_1 of length $n = 2^m - 1$ with generator polynomial $m_1(x)$ is called *the Hamming code.* The dual code $C_1^\perp$ is called *the simplex code.*

We note that C_1 is an $[n, n-m, 3]_2$ code and ever nonzero codeword in the simplex code has weigth 2^{m-1}. In fact, any cyclic code with the parameters mentioned above is "equivalent" to the Hamming code, i.e. can be obtained from the Hamming code by a permutation of coordinates. We refer to [[16], Section 1.8] for the proofs of these facts. Hence if $(i, n) = 1$, $C_i = \langle m_i(x) \rangle$ can also be considered as the Hamming code.

Cyclic codes have a natural trace representation, which make the relation with m-sequences and their crosscorrelation possible. We refer to [[20], Proposition 2.1] for the proof of the following theorem:

Theorem 1.3.1. *Let C be a q-ary cyclic code of length $q^m - 1$ such that $\{\alpha^{i_1}, ..., \alpha^{i_s}\}$ is a basic zero set for $C^{\perp}$, where α is a primitive element of $\mathbb{F}_{q^m}$. For every codeword $c \in C$, there exist $\lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m}$ such that if $f(t) = \lambda_1 t^{i_1} + ... + \lambda_s t^{i_s}$, then,*

$$c = \big(Tr(f(\alpha^0)), Tr(f(\alpha^1)), Tr(f(\alpha^2)), ..., Tr(f(\alpha^{q^m-2}))\big) \tag{1.4}$$

where Tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by $Tr(a) = a + a^q + ... + a^{q^{m-1}}$.

If the use the notation $(Tr(\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}))_{x \in \mathbb{F}^*_{q^m}}$ for the codeword c in 1.4, then Theorem 1.3.1 implies that

$$C = \left\{ \big(Tr(\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s})\big)_{x \in \mathbb{F}^*_{q^m}} : \lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m} \right\}.$$

Note that the trace representation of the binary simplex code is

$$C_1^{\perp} = \left\{ (Tr(\lambda x))_{x \in \mathbb{F}^*_{2^m}} : \lambda \in \mathbb{F}_{2^m} \right\}.$$

By Equation 1.3, we establish the first relation between binary m-sequences and cyclic codes.

Proposition 1.3.1. *For $n = 2^m - 1$, a period of an n^{th} order binary m-sequence is a codeword of the binary simplex code of length n.*

The second relation will be between the crosscorrelation function and the weight distribution of a certain binary cyclic code. For this let $d > 1$ with $(d, 2^m - 1) = 1$ and consider the code $C_{1,d}$ with the generator polynomial $m_1(x) m_d(x)$. Then, $C_{1,d}^{\perp}$ has the following trace representation:

$$C_{1,d}^{\perp} = \left\{ \big(Tr(\lambda_1 x + \lambda_2 x^d)\big)_{x \in \mathbb{F}^*_{2^m}} : \lambda_1, \lambda_2 \in \mathbb{F}_{2^m} \right\} \tag{1.5}$$

Now, consider the binary m-sequences u and v, differing by d^{th} decimation, with $u_i = Tr(\beta_1 \alpha^i)$ and $v_i = Tr(\beta_1 \alpha^{id})$, where $\alpha = \langle \mathbb{F}^*_{2^m} \rangle$, $\beta_1 \in \mathbb{F}^*_{2^m}$ and d is the same as above. Then,

$$\begin{aligned} \Theta_{u,v}(l) &= \sum_{i=0}^{2^m-2} (-1)^{u_i + v_{i+l}} \\ &= \sum_{i=0}^{2^m-2} (-1)^{Tr(\beta_1 \alpha^i + \beta_1 \alpha^{dl} \alpha^{id})}. \end{aligned}$$

Note that as l runs through the period, $\beta_1 \alpha^{dl}$ runs through all nonzero elements of $\mathbb{F}_{2^m}^*$. Also note that

$$\Theta_{u,v}(l) = \Theta_d(l) = n - 2w\left(\left(Tr(\beta_1 x + \beta_1 \alpha^{dl} x^d)\right)_{x \in \mathbb{F}_{2^m}^*}\right). \tag{1.6}$$

So, the values of the crosscorrelation function decides the weights of $(2^m - 1)$-many codewords in $C_{1,d}^{\perp}$ with $\lambda_1 \neq 0, \lambda_2 \neq 0$ in the notation of 1.5. Since changing β_1 only causes u to be cyclically shifted, the crosscorrelation remains unchanged. Hence, all other codewords in 1.5 with any $\lambda_1 \neq 0, \lambda_2 \neq 0$ will have weight which are related to $\Theta_{u,v}$ via 1.6, i.e. nonzero values of the crosscorrelation and the nonzero weights of any codeword in $C_{1,d}^{\perp}$ with $\lambda_1 \neq 0 \neq \lambda_2$ are in one to one correspondence. Finally, when $\lambda_1 = 0$ or $\lambda_2 = 0$, the resulting codewords in $C_{1,d}^{\perp}$ belong to the simplex code and their weight is 2^{m-1}. Hence, we have the following:

Theorem 1.3.2. *Deciding the crosscorrelation spectrum of two binary m-sequences related via decimation d is equivalent to computing the weight enumeration of the binary cyclic code $C_{1,d}^{\perp}$.*

We will end this section with the equivalent statements of McEliece's theorem for the cyclic code ${C_{1,d}}^{\perp}$. Now the nonzeros of ${C_{1,d}}^{\perp}$ are the elements $\alpha^{-i}, \alpha^{-id}$ for $i \in \{1, 2, 4, ..., 2^{m-1}\}$, where α is a primitive element of $\mathbb{F}_{2^m}$. Subsets of these nonzeros will have product 1 when corresponding exponents sum up to zero modulo $2^m - 1$. To see this clearly, $l + 1$ nonzeros of ${C_{1,d}}^{\perp}$ will have product 1 if and only if

$$\prod_{k \in I_1 \cup I_2} \alpha^{-k} = 1$$

where $I_1 \subset Cl(1)$ and $I_2 \subset Cl(d)$ with $|I_1| + |I_2| = l + 1$, where

$$Cl(a) = \left\{a, 2a, 2^2 a ..., 2^{m_a - 1} a\right\},$$

where m_a is the smallest integer such that $2^{m_a} a \equiv a \bmod (2^m - 1)$, which implies

$$\sum_{k \in I_1 \cup I_2} k \equiv 0 \pmod{2^m - 1}.$$

Considet the binary expansions of the positive integers u and v

$$\sum_{i=0}^{m-1} u_i 2^i \text{ and } \sum_{i=0}^{m-1} v_i 2^i.$$

Suppose that

$$u_i = \begin{cases} 1 & \text{if } 2^i d \bmod (2^m - 1) \in I_2 \\ 0 & \text{otherwise} \end{cases}$$

$$v_i = \begin{cases} 1 & \text{if } 2^i \ \mathrm{mod}(2^m-1) \ \in I_1 \\ 0 & \text{otherwise} \end{cases}$$

Then we will have

$$\sum_{k \in I_1 \cup I_2} k \equiv \sum_{i=0}^{m-1} u_i 2^i d \ + \ \sum_{i=0}^{m-1} v_i 2^i \equiv 0(mod\ 2^m - 1)$$

Thus, if for all (u, v) such that $0 \leq u, v \leq 2^m - 1$, and $ud + v \equiv 0 \bmod (2^m - 1)$, we have $w(u) + w(v) \geq l + 1$ and writing $v \leq 2^m - 1$ as $v = 2^m - 1 - ud$, we have the other equivalent statement, if for all u such that $0 \leq u \leq 2^m - 1$, $w(ut) \leq w(u) + m - 1 - l$ holds then by Thm.1.2.2 all the weights in ${C_{1,d}}^{\perp}$ are divisible by 2^l yet there is at least one weight which is not divisible by 2^{l+1}.

CHAPTER 2

PROPERTIES OF CROSSCORRELATION FUNCTION

This section is devoted to some important properties of the crosscorrelation function. The main result (Theorem 2.2.1) states that the crosscorrelation function takes at least 3 values. This theorem and other results are due to Helleseth (see [8]).

Other than Helleseth's paper [8], we refer to PhD dissertations of Niho and Trachtenberg ([15], [19]) for more foundational material on m-sequences. For a more recent account of the current state of research on the topic, we refer to the PhD thesis of Rosendahl, [17]. We note that the crosscorrelation with exactly three values will be our main focus in the remaining chapters.

2.1 Preliminary Identities

We start with a theorem which states basic properties of the crosscorrelation function.

Theorem 2.1.1. *We have*

(i) $\Theta_d(l)$ *is real valued for all* $l = 0, ..., p^n - 2$.

(ii) *The values and the number of occurrences of each value of* $\Theta_d(l)$ *are independent of the choice* ξ.

(iii) $\Theta_{dp^j}(l) = \Theta_d(l)$, *i.e. crosscorrelation takes the same value on the p-cyclotomic coset of d.*

(iv) $\Theta_d(lp^j) = \Theta_d(l)$, *i.e. crosscorrelation is the same for those shifts which are in the same p-cyclotomic coset.*

(v) $\sum_{l=0}^{p^n-2} \Theta_d(l) = 1$.

Proof. **(i)** $\Theta_d(l) = \sum_{t=0}^{p^n-2} \xi^{s_{t-l}-v_t}$. For $p = 2$, $\xi = -1$ and hence the result follows. For $p > 2$, $p^n - 1$ is even. Assume that $s_t = Tr(\alpha^t)$ for all t, where α is primitive in

$\mathbb{F}_{p^n}$. Then, $s_{t+\frac{p^n-1}{2}} = Tr(\alpha^t\alpha^{\frac{p^n-1}{2}}) = -Tr(\alpha^t) = -s_t$. Hence we have $s_t = -s_{t+\frac{p^n-1}{2}}$, $v_t = -v_{t+\frac{p^n-1}{2}}$. Thus, the first half of the period is the negative of second half relative to any starting point. So,

$$\begin{aligned}
\Theta_d(l) &= \sum_{t=1}^{p^n-1} \xi^{s_{t-l}-v_t} \\
&= \sum_{t=1}^{\frac{p^n-1}{2}} \xi^{s_{t-l}-v_t} + \sum_{t=\frac{p^n+1}{2}}^{p^n-1} \xi^{s_{t-l}-v_t} \\
&= \sum_{t=1}^{\frac{p^n-1}{2}} \xi^{s_{t-l}-v_t} + \xi^{-s_{t-l}+v_t} \\
&= \sum_{t=1}^{\frac{p^n-1}{2}} \xi^{s_{t-l}-v_t} + (\xi^{-1})^{s_{t-l}-v_t} \\
&= 2Re\sum_{t=1}^{\frac{p^n-1}{2}} \xi^{s_{t-l}-v_t}.
\end{aligned}$$

(ii) Let $s_t = Tr(\theta\alpha^t)$, where $\theta \in \mathbb{F}_{p^n}^*$, and α is a primitive element of $\mathbb{F}_{p^n}^*$. Set $\theta = \alpha^i$, then we have $s_t = Tr(\alpha^{t+i})$. For integers k with $1 < k < p$, consider $ks_t = Tr(k\theta\alpha^t)$. Letting $k\theta = \alpha^{i+\tau}$, we obtain $ks_t = Tr(\alpha^{t+i+\tau}) = s_{t+\tau}$, which implies that multiplying an m-sequence with an integer k gives a cyclic shift of the same sequence. In $\Theta_d(l) = \sum_{t=0}^{p^n-2} \xi^{s_{t-l}-v_t}$, replace ξ with ξ^k where $1 < k < p$. Then

$$\begin{aligned}
\Theta_d(l) &= \sum_{t=1}^{p^n-1} \xi^{k(s_{t-l}-v_t)} \\
&= \sum_{t=1}^{p^n-1} \xi^{ks_{t-l}-kv_t} \\
&= \sum_{t=1}^{p^n-1} \xi^{s_{t-l+\tau}-v_{t+\sigma}} \\
&= \Theta_d(l^{'}) \text{ where } l^{'} = l + \sigma - \tau.
\end{aligned}$$

(iii) For $s_{t-l} = Tr(\gamma^{t-l})$ and $v_t = Tr(\gamma^{dt}) = s_{dt}$ where γ is primitive in $\mathbb{F}_{p^n}$, consider

$$\begin{aligned}
\Theta_{dp^j}(l) &= \sum_{t=0}^{p^n-2} \xi^{s_{t-l}-v_t} \\
&= \sum_{t=0}^{p^n-2} \xi^{s_{t-l}-s_{dp^j t}} \\
&= \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-l})-Tr(\gamma^{dp^j t})} \\
&= \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-l})-Tr(\gamma^{dt})} \\
&= \sum_{t=0}^{p^n-2} \xi^{s_{t-l}-s_{dt}} \\
&= \Theta_d(l),
\end{aligned}$$

since $Tr(x) = Tr(x^p)$.

(iv) For $s_{t-l} = Tr(\gamma^{t-l})$ and $v_t = Tr(\gamma^{dt}) = s_{dt}$ where γ is primitive in $\mathbb{F}_{p^n}$, consider

$$\begin{aligned}
\Theta_d(lp^j) &= \sum_{t=0}^{p^n-2} \xi^{s_{t-lp^j}-v_t} \\
&= \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-lp^j})-Tr(\gamma^{dt})} \\
&= \sum_{t=0}^{p^n-2} \xi^{Tr(\gamma^{t-l})-Tr(\gamma^{dt})} \\
&= \Theta_d(l),
\end{aligned}$$

since $Tr(x) = Tr(x^p)$.

(v) Assume that $s_t = Tr(\alpha^t)$ and $v_t = s_{td} = Tr(\alpha^{td})$, where α is primitive in $\mathbb{F}_{p^n}$. Then

$$\begin{aligned}
\sum_{l=0}^{p^n-2}\sum_{t=0}^{p^n-2} \xi^{s_{t-l}-v_t} &= \sum_{l=0}^{p^n-2}\sum_{t=0}^{p^n-2} \xi^{Tr(\alpha^{t-l}-\alpha^{td})} \\
&= \sum_{y\in\mathbb{F}_{p^n}^*}\sum_{x\in\mathbb{F}_{p^n}^*} \xi^{Tr(yx-x^d)} \text{ where } y = \alpha^t \\
&= \sum_{x\in\mathbb{F}_{p^n}^*} \xi^{Tr(x^d)} \sum_{y\in\mathbb{F}_{p^n}^*} \xi^{Tr(yx)} \\
&= \sum_{x\in\mathbb{F}_{p^n}^*} \xi^{Tr(x^d)} \left(\sum_{y\in\mathbb{F}_{p^n}} \xi^{Tr(yx)} - 1 \right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x\in\mathbb{F}^*_{p^n}} \xi^{Tr(x^d)}\left(p^{n-1}\sum_{y_1\in\mathbb{F}_p}\xi^{Tr(y_1)}-1\right)\\
&= \sum_{x\in\mathbb{F}^*_{p^n}} \xi^{Tr(x^d)}(-1)\\
&= -\sum_{x\in\mathbb{F}^*_{p^n}} \xi^{Tr(x)} = -\sum_{x\in\mathbb{F}_{p^n}} \xi^{Tr(x)} - 1\\
&= -p^{n-1}\sum_{x\in\mathbb{F}_p}\xi^{Tr(x)} - 1 = 1.
\end{aligned}
$$

Note that we used the fact that the absolute trace function is balanced, the powers of a primitive p^{th} root of unity sum up to zero and the map $f(x) = x^d$ is one to one since $(d, p^n - 1) = 1$.

□

The following theorem and its consequences will be of great use in computing crosscorrelation values.

Theorem 2.1.2. *We have*

$$\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l+\tau_1)...\Theta_d(l+\tau_{m-1}) = -(p^n-1)^{m-1} + 2(-1)^{m-1} + c_m^{(\tau_1,...,\tau_{m-1})}p^{2n},$$

where ${c_m}^{(\tau_1,...,\tau_{m-1})}$ *is the number of solutions to the following two equations:*

$$\alpha^{-\tau_1}x_1 + \alpha^{-\tau_2}x_2 + ... + \alpha^{-\tau_{m-1}}x_{m-1} + 1 = 0$$

$${x_1}^d + {x_2}^d + ... + {x_{m-1}}^d + 1 = 0$$

where $x_i \in \mathbb{F}^*_{p^n}$ *for* $i = 0, 1, ..., m-1$.

Proof. Consider the following sets:

$$
\begin{aligned}
K &= \left\{(x_0, x_1, ..., x_{m-1}) : x_i \in \mathbb{F}^*_{p^n}\right\},\\
K_1 &= \left\{(x_0, x_1, ..., x_{m-1}) \in K : x_0 + \alpha^{-\tau_1}x_1 + \alpha^{-\tau_2}x_2 + ... + \alpha^{-\tau_{m-1}}x_{m-1} = 0\right\}\\
K_2 &= \left\{(x_0, x_1, ..., x_{m-1}) \in K : {x_0}^d + {x_1}^d + {x_2}^d + ... + {x_{m-1}}^d = 0\right\}
\end{aligned}
$$

Recall that the crosscorrelation function is,

$$\Theta_d(l) = \sum_{x\in\mathbb{F}^*_{p^n}} \xi^{Tr(cx-x^d)},$$

where $c = \alpha^{-l}$ for some primitive element $\alpha \in \mathbb{F}_{p^n}$ and $\xi \neq 1$ is a complex p^{th} root of unity. So, for $i = 1, ..., m-1$ we have

$$\Theta_d(l+\tau_i) = \sum_{x\in\mathbb{F}^*_{p^n}} \xi^{Tr(\alpha^{-(l+\tau_i)}x - x^d)}.$$

For simplicity let $S(y) = \xi^{Tr(y)}$, then

$$\begin{aligned}
&\sum_{l=0}^{p^n-2} \Theta_d(l)\Theta_d(l+\tau_1)...\Theta_d(l+\tau_{m-1}) \\
=& \sum_{l=0}^{p^n-2} \left(\sum_{x_0 \in \mathbb{F}_{p^n}^*} S(\alpha^{-l}x_0 - {x_0}^d) \right) ... \left(\sum_{x_{m-1} \in \mathbb{F}_{p^n}^*} S(\alpha^{-(l+\tau_{m-1})}x_{m-1} - {x_{m-1}}^d) \right) \\
=& \sum_{l=0}^{p^n-2} \sum_{K} S(\alpha^{-l}x_0 - {x_0}^d)...S(\alpha^{-(l+\tau_{m-1})}x_{m-1} - {x_{m-1}}^d) \\
=& \sum_{l=0}^{p^n-2} \sum_{K} S(\alpha^{-l}x_0 - {x_0}^d + ... + \alpha^{-(l+\tau_{m-1})}x_{m-1} - {x_{m-1}}^d) \\
=& \sum_{l=0}^{p^n-2} \sum_{K} S(\alpha^{-l}(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1}) - ({x_0}^d + {x_1}^d + ... + x_{m-1}^d)) \\
=& \sum_{K} \sum_{l=0}^{p^n-2} S(\alpha^{-l}(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1}) - ({x_0}^d + {x_1}^d + ... + x_{m-1}^d)) \\
=& \sum_{K} \sum_{y \in \mathbb{F}_{p^n}^*} S(y(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1}) - ({x_0}^d + {x_1}^d + ... + x_{m-1}^d)).
\end{aligned}$$

Using the sets K, K_1, K_2, seperate the sum into four parts as follows:

$$= \sum_{K-(K_1 \cup K_2)} \sum_{y \in \mathbb{F}_{p^n}^*} S(y(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1}) - ({x_0}^d + {x_1}^d + ... + x_{m-1}^d))$$

$$+ \sum_{K_1-K_2} \sum_{y \in \mathbb{F}_{p^n}^*} S(-({x_0}^d + {x_1}^d + ... + {x_{m-1}}^d))$$

$$+ \sum_{K_2-K_1} \sum_{y \in \mathbb{F}_{p^n}^*} S(y(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1})) + \sum_{K_1 \cap K_2} \sum_{y \in \mathbb{F}_{p^n}^*} S(0).$$

In the first sum, set

$$a_x = x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1} \neq 0 \quad \text{and}$$

$$b_x = {x_0}^d + {x_1}^d + ... + {x_{m-1}}^d \neq 0.$$

Then we have

$$\begin{aligned}
\sum_{K-(K_1 \cup K_2)} \sum_{y \in \mathbb{F}_{p^n}^*} S(ya_x - b_x) &= \sum_{K-(K_1 \cup K_2)} \sum_{y \in \mathbb{F}_{p^n}^*} \xi^{Tr(ya_x) - Tr(b_x)} \\
&= \sum_{K-(K_1 \cup K_2)} \xi^{Tr(-b_x)} \sum_{y \in \mathbb{F}_{p^n}^*} \xi^{Tr(ya_x)}
\end{aligned}$$

Since $a_x \neq 0$, as y runs through $\mathbb{F}_{p^n}^*$ so does $y_1 = ya_x$. Thus, for the inner sum, we have

$$\sum_{y_1 \in \mathbb{F}_{p^n}^*} \xi^{Tr(y_1)} = \sum_{y_1 \in \mathbb{F}_{p^n}} \xi^{Tr(y_1)} - 1 = p^{n-1} \sum_{y_2 \in \mathbb{F}_p} \xi^{y_2} - 1 = -1.$$

Note that we used the fact that the absolute trace function is balanced and the powers of a primitive p^{th} root of unity sum up to zero. If $(x_0, ..., x_{m-1}) \in K - (K_1 \cup K_2)$ and $z \in \mathbb{F}_{p^n}^*$, then $(zx_0, ..., zx_{m-1})$ is also contained in $K - (K_1 \cup K_2)$. So consider the sum

$$\sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}^*} S(-(z^d {x_0}^d + ... + z^d {x_{m-1}}^d)) = \sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}^*} S(-z^d({x_0}^d + ... + {x_{m-1}}^d)).$$

Since $b_x = {x_0}^d + {x_1}^d + ... + {x_{m-1}}^d \neq 0$, $z^d b_x$ runs through $\mathbb{F}_{p^n}^*$ as z runs through $\mathbb{F}_{p^n}^*$. Moreover, the map $f(z) = z^d$ is one to one since $(d, p^n - 1) = 1$. Combining these we obtain the following:

$$\begin{aligned}\sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}^*} S(-z^d b_x) &= \sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}^*} S(z^d) = \sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}^*} S(z) \\ &= \sum_{K-(K_1\cup K_2), z\in\mathbb{F}_{p^n}} S(z) - 1 = \sum_{K-(K_1\cup K_2)} -1.\end{aligned}$$

So for the first sum we have

$$\begin{aligned}&\sum_{K-(K_1\cup K_2)} \sum_{y\in\mathbb{F}_{p^n}^*} S(y(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1}) - ({x_0}^d + {x_1}^d + ... + x_{m-1}^d)) \\ = &\ \frac{|K| - |K_1 \cup K_2|}{p^n - 1}.\end{aligned}$$

For the second and third sums the above arguments also apply. So we obtain respectively,

$$\begin{aligned}\sum_{K_1-K_2} \sum_{y\in\mathbb{F}_{p^n}^*} S(-({x_0}^d + {x_1}^d + ... + {x_{m-1}}^d)) &= \frac{(p^n-1)|K_1 - K_2|(-1)}{p^n - 1}, \\ \sum_{K_2-K_1} \sum_{y\in\mathbb{F}_{p^n}^*} S(y(x_0 + \alpha^{-\tau_1}x_1 + ... + \alpha^{-\tau_{m-1}}x_{m-1})) &= \sum_{K_2-K_1} -1.\end{aligned}$$

Therefore,

$$\begin{aligned}&\sum_{l=0}^{p^n-2} \Theta_d(l)\Theta_d(l+\tau_1)...\Theta_d(l+\tau_{m-1}) \\ = &\ \frac{|K| - |K_1 \cup K_2|}{p^n - 1} + \frac{(p^n-1)|K_1 - K_2|(-1)}{p^n - 1} + |K_2 - K_1|(-1) + (p^n - 1)|K_1 \cap K_2|, \\ = &\ \frac{1}{p^n - 1}\left(|K| - (p^n)(|K_1| + |K_2|) + (p^n)^2|K_1 \cap K_2|\right).\end{aligned}$$

Note that $|K_1| = |K_2|$ since $(d, p^n - 1) = 1$ and $(y_0, ..., y_{m-1}) \in K_1$ if and only if $({y_0}^{d^{-1}}, ..., \alpha^{-\tau_{m-1}d^{-1}}{y_{m-1}}^{d^{-1}}) \in K_2$. For $d = 1$ and $\tau_1 = \tau_2 = ... = \tau_{m-1} = 0$, we will have $|K_1| = |K_2| = |K_1 \cap K_2|$. Thus, we obtain,

$$\sum_{l=0}^{p^n-2} \Theta_1(l)^m = \frac{1}{p^n - 1}\left(|K| - 2p^n|K_1| + (p^n)^2|K_1|\right).$$

The left hand sum corresponds to autocorrelation function. For $l = 0$, $\Theta_1(l) = p^n - 1$ and $\Theta_1(l) = -1$ otherwise. So we have,

$$\begin{aligned}(p^n-1)^m + (-1)^m(p^n-2) &= \frac{1}{p^n-1}\left((p^n-1)^m - 2p^n|K_1| + (p^n)^2|K_1|\right),\\ |K_1| &= (p^n-1)\frac{(p^n-1)^{m-1}+(-1)^m}{p^n}.\end{aligned}$$

Therefore, by substituting the values for $|K|$ and $|K_1|$, we have

$$\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l+\tau_1)...\Theta_d(l+\tau_{m-1}) = -(p^n-1)^{m-1} + 2(-1)^{m-1} + (p^n)^2\frac{|K_1\cap K_2|}{p^n-1},$$

where $\frac{|K_1\cap K_2|}{p^n-1}$ is the number of solutions of the following equations

$$\alpha^{-\tau_1}x_1 + \alpha^{-\tau_2}x_2 + ... + \alpha^{-\tau_{m-1}}x_{m-1} + 1 = 0$$

$${x_1}^d + {x_2}^d + ... + {x_{m-1}}^d + 1 = 0$$

with $x_i \in \mathbb{F}_{p^n}^*$ for $i = 0, 1, ..., m-1$. This concludes the proof. □

Corollary 2.1.1. *We have*

$$\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l-\tau) = \begin{cases} p^{2n}-p^n-1 & \textit{when } \tau\equiv 0 \pmod{p^n-1}\\ -(p^n+1) & \textit{when } \tau\not\equiv 0 \pmod{p^n-1}\end{cases}$$

Proof. By Theorem 2.1.2 we have

$$\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l-\tau) = -(p^n-1) + 2(-1) + p^{2n}{c_2}^{(\tau)}$$

where ${c_2}^{(\tau)}$ is the number of solutions to $\alpha^{-\tau}x_1 + 1 = 0$ and ${x_1}^d + 1 = 0$ with $x_1 \in \mathbb{F}_{p^n}^*$. These two equations imply that $\alpha^{d\tau} = 1$ and thus $d\tau \equiv 0 \bmod (p^n-1)$. Since $(d, p^n-1) = 1$, we have $\tau \equiv 0 \bmod (p^n-1)$. Therefore, if $\tau \equiv 0 \bmod (p^n-1)$ we have ${c_2}^\tau = 1$, and otherwise ${c_2}^\tau = 0$. □

Corollary 2.1.2. *We have*

$$\sum_{l=0}^{p^n-2}(\Theta_d(l)+1)^3 = p^{2n}b_3$$

where b_3 is the number of solutions of the equations

$$x + y + 1 = 0,$$

$$x^d + y^d + 1 = 0$$

with $x, y \in \mathbb{F}_{p^n}$.

Proof. Using Theorems 2.1.1 and 2.1.2, we have

$$\begin{aligned}\sum_{l=0}^{p^n-2}(\Theta_d(l)+1)^3 &= \sum_{l=0}^{p^n-2}(\Theta_d(l))^3+3\sum_{l=0}^{p^n-2}(\Theta_d(l))^2+3\sum_{l=0}^{p^n-2}(\Theta_d(l))+\sum_{l=0}^{p^n-2}1\\ &= -(p^n-1)^2+2+p^{2n}{c_3}^{(0,0,0)}+3(p^{2n}-p^n-1)+3+(p^n-1)\\ &= p^{2n}\left(2+{c_3}^{(0,0,0)}\right)\end{aligned}$$

where ${c_3}^{(0,0,0)}$ denotes the number of common solutions of the equations

$$x_1+x_2+1=0 \text{ and } {x_1}^d+{x_2}^d+1=0$$

for $x_1,x_2\in\mathbb{F}_{p^n}^*$. Considering the number of solutions corresponding to the cases $x_1=0$ and $x_2=0$, which is 2, and setting $b_3={c_3}^{(0,0,0)}+2$ we obtain the result. □

2.2 On the Values of the Crosscorrelation Function

The following is the main theorem of this chapter and it is due to Helleseth([[8], Theorem 4.1])

Theorem 2.2.1. *$\Theta_d(l)$ has at least three distinct values for $l=0,1,...,p^n-2$ if and only if $d\notin\{1,p,...,p^{n-1}\}$.*

Proof. Suppose $d\in\{1,p,...,p^{n-1}\}$. Then $\Theta_d(l)$ takes on only two values -1 and p^n-1 which are the values of the autocorrelation function since $\Theta_1(l)=\Theta_{p^j}(l)$ for $j=1,2,...,n-1$, by Theorem 2.1.1. So, we assume $d\notin\{1,p,...,p^{n-1}\}$. Suppose on the contrary that $\Theta_d(l)$ takes on two values a and b with occurences r_1 and r_2 respectively. Recall the following

$$\sum_{l=0}^{p^n-2}\Theta_d(l)=1 \text{ and } \sum_{l=0}^{p^n-2}\Theta_d(l)^2=p^{2n}-p^n-1,$$

(cf. Theorem 2.1.1 and Corollary 2.1.1). Using the above equations we obtain,

$$\begin{aligned}r_1+r_2 &= p^n-1,\\ r_1a+r_2b &= 1,\\ r_1a^2+r_2b^2 &= p^{2n}-p^n-1.\end{aligned}$$

By eliminating r_1 and r_2 we obtain

$$\begin{aligned}ab(p^n-1)-b &= a-p^{2n}+p^n+1,\\ ab(p^n-1)^2-(b+a)(p^n-1) &= (p^n-1)(-p^{2n}+p^n+1),\\ ((p^n-1)a-1)((p^n-1)b-1) &= p^{2n}(2-p^n),\\ (p^na-(a+1))(p^nb-(b+1)) &= p^{2n}(2-p^n). \qquad (2.1)\end{aligned}$$

Since ξ is a primitive p^{th} root of unity, the ring of integers of $\mathbb{Q}(\xi)$ is $\mathbb{Z}[\xi]$ ([[10] Proposition 13.12.10]). Since $\{1, \xi, \xi^2, ..., \xi^{p-2}\}$ forms an integral basis for $\mathbb{Q}(\xi)$ and $a, b \in \mathbb{Q}(\xi)$, we have

$$a = \sum_{i=0}^{p-2} u_i \xi^i \text{ and } b = \sum_{i=0}^{p-2} v_i \xi^i$$

where $u_i, v_i \in \mathbb{Z}$. Note that we must have $|u_i| \leq p^n - 1$ and $|v_i| \leq p^n - 1$ for $i = 0, 1, ..., p-2$ because of the definitions of a and b. Let $\pi = 1 - \xi$, and note the obvious equality of $\mathbb{Z}[\xi]$ and $\mathbb{Z}[\pi]$. By [[10]Proposition 13.2.7], the ideals (p) and $(\pi)^{p-1}$ coincide. In the following, $\pi^r || (a+1)$ will mean that $a + 1 \in (\pi)^r - (\pi)^{r+1}$. Suppose $\pi^r || (a+1)$ and $\pi^s || (b+1)$ for some r and s. We consider the following three cases:

Case 1 $\underline{r \geq n_1 = (p-1)n \text{ or } s \geq n_1 = (p-1)n.}$

Then $a + 1 \in (\pi)^r \subset (\pi)^{(p-1)n} = (p)^n$, which implies that $a + 1 = p^n a_1$ with $a_1 = c_0 + c_1\xi + ... + c_{p-2}\xi^{p-2} \in \mathbb{Z}[\xi]$. Thus,

$$a = p^n c_0 - 1 + p^n \left(c_1\xi + ... + c_{p-2}\xi^{p-2}\right).$$

Note that we must have $p^n c_0 - 1 \leq p^n - 1$ and $p^n c_i \leq p^n - 1$ for $i = 1, ..., p-2$. Hence, $c_1 = c_2 = ... = c_{p-2} = 0$ and $c_0 = 1$. Thus, we have $a = p^n - 1$ but this value corresponds to the value taken by the autocorrelation function, that is we must have $d \in \{1, p, ..., p^{n-1}\}$. This is a contradiction to our hypotheses. Similar argument works if $s \geq n_1 = (p-1)n$, too.

Case 2 $\underline{r < n_1 = (p-1)n \text{ and } s < n_1 = (p-1)n.}$

Since $a + 1 \in (\pi)^r - (\pi)^{r+1}$ and $b + 1 \in (\pi)^s - (\pi)^{s+1}$ we have $a + 1 = \pi^r a_1$ where $a_1 \notin (\pi)$ and $b + 1 = \pi^s b_1$ where $b_1 \notin (\pi)$. Similarly since the ideals (p) and $(\pi)^{p-1}$ coincide, we have $p^n = \pi^{n_1} z_1$ where $z_1 \notin (\pi)$. Now substituting these values in (2.1) we obtain

$$\pi^{r+s}(\pi^{n_1-r}z_1 a - a_1)(\pi^{n_1-s}z_1 b - b_1) = \pi^{2n_1}{z_1}^2(2 - p^n).$$

Since $r + s + 1 < 2n_1$, we have $(\pi)^{2n_1} \subset (\pi)^{r+s+1}$. Note that the left hand side of the equation belongs to $(\pi)^{r+s} - (\pi)^{r+s+1}$, and right hand side belongs to $(\pi)^{2n_1}$. This is a contradiction to $(\pi)^{2n_1} \subset (\pi)^{r+s+1}$.

Case 3 $\underline{a + 1 = 0 \text{ or } b + 1 = 0.}$

From (2.1), for $a = -1$ we obtain $b = p^n - 1$. This gives the same contradiction as in Case 1. Similarly for $b + 1 = 0$ case.

□

We have seen in Theorem 2.1.1 that the crosscorrelation function is real valued. The following decides when it is integer valued.

Theorem 2.2.2. *$\Theta_d(l) \in \mathbb{Z}$ for $l = 0, 1, ..., p^n - 2$ if and only if $d \equiv 1 \pmod{p-1}$.*

Proof. Define the function

$$C(x) = \sum_{l=0}^{p^n-2} \Theta_d(l) x^l.$$

Let $\beta \neq 1$ be a complex $(p^n-1)^{th}$ root of unity. By inversion, we have

$$\Theta_d(l) = \frac{1}{p^n-1} \sum_{j=0}^{p^n-2} C(\beta^j)\beta^{-lj}.$$

Now that $C(\beta^t)$ belongs to $\mathbb{Q}(\xi\beta)$, since $\Theta_d(l) \in \mathbb{Q}(\xi)$. We are going to show that $C(\beta^t)$ belongs to $\mathbb{Q}(\beta)$ if and only if $d \equiv 1 \pmod{p-1}$. Let α be a primitive root of the characteristic polynomial of the m-sequence. Then $\alpha^{\frac{p^n-1}{p-1}}$ is a primitive element of $\mathbb{F}_p$. The elements of $\mathbb{Q}(\beta)$ are exactly the elements in $\mathbb{Q}(\xi\beta)$ which are fixed under the automorphisms

$$\sigma_i : \xi \to \xi^{\alpha^{i\frac{p^n-1}{p-1}}}$$

for $i = 0, 1, ..., p-2$. We have,

$$\begin{aligned}
\sigma_i(C(\beta^t)) &= \sigma_i\left(\sum_{l=0}^{p^n-2} \Theta_d(l)\beta^{tl}\right) \\
&= \sigma_i\left(\sum_{l=0}^{p^n-2}\sum_{j=0}^{p^n-2} \xi^{Tr(\alpha^{-l}\alpha^j - \alpha^{dj})}\beta^{tl}\right) \\
&= \sum_{l=0}^{p^n-2}\sum_{j=0}^{p^n-2} \xi^{\alpha^{i\frac{p^n-1}{p-1}} Tr(\alpha^{-l}\alpha^j - \alpha^{dj})}\beta^{tl} \\
&= \sum_{l=0}^{p^n-2} \beta^{tl} \sum_{j=0}^{p^n-2} \xi^{\alpha^{i\frac{p^n-1}{p-1}} Tr(\alpha^{-l}\alpha^j - \alpha^{dj})}.
\end{aligned}$$

Since $\alpha^{\frac{p^n-1}{p-1}} \in \mathbb{F}_p$, we have

$$\sigma_i(C(\beta^t)) = \sum_{l=0}^{p^n-2} \beta^{tl} \sum_{j=0}^{p^n-2} \xi^{Tr(\alpha^{-l+j+i\frac{p^n-1}{p-1}} - \alpha^{i\frac{p^n-1}{p-1}+dj})}.$$

Set

$$dj_1 \equiv dj + i\frac{p^n-1}{p-1} \mod (p^n-1)$$

from which we obtain

$$j \equiv j_1 - id^{-1}\frac{p^n-1}{p-1} \mod (p^n-1).$$

By substituting these values we obtain

$$\begin{aligned}
\sigma_i(C(\beta^t)) &= \sum_{l=0}^{p^n-2} \beta^{tl} \sum_{j=0}^{p^n-2} \xi^{Tr(\alpha^{-l+j_1-id^{-1}\frac{p^n-1}{p-1}+i\frac{p^n-1}{p-1}}-\alpha^{dj_1})} \\
&= \sum_{l=0}^{p^n-2} \beta^{tl} \sum_{j=0}^{p^n-2} \xi^{Tr(\alpha^{-(l+i\frac{p^n-1}{p-1}(d^{-1}-1))+j_1}-\alpha^{dj_1})} \\
&= \sum_{l=0}^{p^n-2} \beta^{tl}\Theta_d(l+i\frac{p^n-1}{p-1}(d^{-1}-1)).
\end{aligned}$$

By setting

$$l_1 \equiv l + i(d^{-1}-1)\frac{p^n-1}{p-1} \quad \bmod (p^n-1)$$

and substituting for l, we get

$$\begin{aligned}
\sigma_i(C(\beta^t)) &= \sum_{l_1=0}^{p^n-2} \Theta_d(l_1)\beta^{t(l_1-i(d^{-1}-1)\frac{p^n-1}{p-1})} \\
&= \sum_{l_1=0}^{p^n-2} \Theta_d(l_1)\beta^{tl_1}\beta^{-ti(d^{-1}-1)\frac{p^n-1}{p-1}} \\
&= \beta^{-ti(d^{-1}-1)\frac{p^n-1}{p-1}}C(\beta^t).
\end{aligned}$$

Then, $\sigma_i(C(\beta^t)) = C(\beta^t)$ if and only if $d^{-1} \equiv 1 \pmod{p-1}$ which holds if and only if $d \equiv 1 \pmod{p-1}$. Therefore $C(\beta^t)$ belongs to $\mathbb{Q}(\beta)$ if and only if $d \equiv 1 \pmod{p-1}$.

Assume that $\Theta_d(l)$ is an integer for $l = 0, 1, ..., p^n-2$. Then

$$C(\beta^t) = \sum_{l=0}^{p^n-2} \Theta_d(l)\beta^{tl}$$

is contained in $\mathbb{Q}(\beta)$ for all $t = 0, 1, ..., p^n-2$. This implies $d \equiv 1 \pmod{p-1}$ by the result we just observed.

Conversely assume that $d \equiv 1 \pmod{p-1}$. Then $C(\beta^t)$ belongs to $\mathbb{Q}(\beta)$, which implies that

$$\Theta_d(l) = \frac{1}{p^n-1}\sum_{j=0}^{p^n-2} C(\beta^j)\beta^{-lj}$$

is contained in $\mathbb{Q}(\beta)\cap\mathbb{Q}(\xi) = \mathbb{Q}$. By definition, $\Theta_d(l)$ is also an integer in $\mathbb{Q}(\xi)$. Hence, $\Theta_d(l) \in \mathbb{Z}[\xi] \cap \mathbb{Q} = \mathbb{Z}$, for $l = 0, 1, ..., p^n-1$. □

In the remaining parts of this section, we will state some further general results on the crosscorrelation function.

Theorem 2.2.3. *Let $m \geq 2$, then we have*

$$\sum_{l=0}^{p^n-2} (\Theta_d(l)+1)(\Theta_d(l+\tau_1)+1)...(\Theta_d(l+\tau_{m-1})+1) \equiv 0 \pmod{p^{2n}}.$$

Proof. Opening up the product, we have

$$\sum_{l=0}^{p^n-2} (\Theta_d(l)+1)(\Theta_d(l+\tau_1)+1)\ldots(\Theta_d(l+\tau_{m-1})+1)$$

$$=\sum_{l=0}^{p^n-2} 1+\sum_{l=0}^{p^n-2}\Theta_d(l)+\ldots+\sum_{l=0}^{p^n-2}\Theta_d(l+\tau_{m-1})+\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l+\tau_1)+\ldots+$$

$$\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l+\tau_1)\Theta_d(l+\tau_2)+\ldots+\sum_{l=0}^{p^n-2}\Theta_d(l)\Theta_d(l+\tau_1)\ldots\Theta_d(l+\tau_{m-1}).$$

Using Theorems 2.1.2, 2.1.1 we have

$$\begin{aligned}
&\equiv (p^n-1)+\binom{m}{1}(-(p^n-1)^0+2(-1)^0)+\binom{m}{2}(-(p^n-1)^1+2(-1)^1)\\
&+ \binom{m}{3}(-(p^n-1)^2+2(-1)^2)+\ldots+\binom{m}{m}(-(p^n-1)^{m-1}+2(-1)^{m-1}) \pmod{p^{2n}}.
\end{aligned}$$

Simplifying, we obtain

$$\begin{aligned}
&= (p^n-1)-\sum_{j=1}^{m}\binom{m}{j}(p^n-1)^{j-1}+2\sum_{j=1}^{m}\binom{m}{j}(-1)^{j-1}\\
&= (p^n-1)-\frac{(p^n)^m-1}{p^n-1}+2\frac{(0)^m-1}{-1}\\
&= \frac{p^{2n}-(p^n)^m}{p^n-1}\\
&= p^{2n}\frac{1-(p^n)^{m-2}}{p^n-1}\equiv 0 \pmod{p^{2n}}.
\end{aligned}$$

□

Note that the previous theorem fails for $m=1$ yet we have

$$\sum_{l=0}^{p^n-2}(\Theta_d(l)+1)=p^n$$

by Theorem 2.1.1.

Theorem 2.2.4. *The polynomial*

$$P(x)=\prod_{l=0}^{p^n-2}(x-(\Theta_d(l)+1))$$

has integral coefficients all of which are divisible by p, except the leading coefficient.

Proof. Let $y_l=(\Theta_d(l)+1)$ and consider the polynomial,

$$\prod_{l=0}^{p^n-2}(x-y_l)=x^{p^n-1}+a_{p^n-2}x^{p^n-2}+\ldots+a_1x+a_0.$$

Let E_k denote the corresponding coefficient of x^{p^n-1-k}, and define S_k as

$$S_k = \sum_{l=0}^{p^n-2} y_l^k.$$

Now using Newton identities, we have

$$\begin{aligned}
S_1 - E_1 &= S_1 - a_{p^n-2} = 0, \\
S_2 - S_1E_1 + 2E_2 &= S_2 - S_1a_{p^n-2} + 2a_{p^n-3} = 0, \\
S_3 - S_2E_1 + S_1E_2 - 3E_3 &= S_3 - S_2a_{p^n-2} + S_1a_{p^n-3} - 3a_{p^n-4} = 0 \\
&\vdots \\
S_{p^n-1} &= -\left(\sum_{j=1}^{p^n-2}(-1)^j S_{p^n-1-j}E_j\right) - (-1)^{p^n-1}(p^n-1)E_{p^n-1} \\
&= -\left(\sum_{j=1}^{p^n-2}(-1)^j S_{p^n-1-j}a_{p^n-1-j}\right) - (p^n-1)a_0.
\end{aligned}$$

Now for all $k \geq 1$, using Theorem 2.2.3 we obtain

$$S_k = \sum_{l=0}^{p^n-2}(y_l)^k = \sum_{l=0}^{p^n-2}(\Theta_d(l)+1)^k \equiv 0 \ (mod\ p^n).$$

Therefore, combining the above result with Newton identities we conclude that $a_i \equiv 0 \pmod p$ for $i = 0, 1, ..., p^n - 2$. □

Theorem 2.2.5. $\Theta_d(l) \equiv -1 \pmod \pi$.

Proof. Recall the polynomial

$$P(x) = \prod_{l=0}^{p^n-2}(x - (\Theta_d(l)+1))$$

for $y_l = \Theta_d(l) + 1$ we have $P(y_l) = 0$, that is

$${y_l}^{p^n-1} + a_{p^n-2}{y_l}^{p^n-2} + ... + a_1y_l + a_0 = 0.$$

From Theorem 2.2.4, we have $a_i \equiv 0 \pmod p$ for $i = 0, 1, ..., p^n - 2$, which implies ${y_l}^{p^n-1} \equiv 0 (\text{mod } p)$. Therefore $y_l \equiv 0 \pmod \pi$, and hence $\Theta_d(l) = y_l - 1 \equiv -1 (\text{mod } \pi)$. □

Corollary 2.2.1. *If $\Theta_d(l) \in \mathbb{Z}$, then $\Theta_d(l) \equiv -1 \pmod p$*

Proof. The result follows from Theorem 2.2.5 and using the fact that every rational integer which is divisible by π is also divisible by p. □

We finish this section by noting that a recent Ph.D. Thesis of Rosendahl, contains a list of decimations for which the values of the corresponding crosscorrelation functions and their frequencies are known. It is interesting to see how small the list is which shows the difficulty of the problem (see [[17], Section 2.2]).

CHAPTER 3

CONJECTURES OF HELLESETH AND SARWATE-PURSLEY

As seen in Theorem 2.2.1, the crosscorrelation function between a pair of distinct m-sequences must take on at least three values. In this chapter, we are going to present the impossibility of exactly 3 values for certain cases. Namely, a conjecture made by Sarwate and Pursley [18] suggests that if $m \equiv 0 \pmod 4$, then there are no "preferred" pairs of binary m-sequences with period $n = 2^m - 1$ (i.e. a pair of m-sequences with 3-valued crosscorrelation function which assumes the values $-1, -1 \pm 2^{\lfloor (m+2)/2 \rfloor}$). We present a proof of this conjecture which is to due to McGuire and Calderbank [14]. Secondly, Helleseth claimed in [8] that if m is a power of 2, then there are no pairs of binary m-sequences with a 3-valued crosscorrelation function. In [1], Calderbank, McGuire, Poonen, and Rubinstein proved this conjecture conditionally. We will also present their work. The proofs are similar in spirit and in both of the proofs McEliece's theorem on divisibility of weights in cyclic codes will play a major role. We remind that all sequences are binary in this chapter.

3.1 A proof for the Sarwate-Pursley Conjecture

As mentioned before in Theorem 2.2.1, the crosscorrelation function between two binary $m-$sequences takes on at least three distinct values. For a pair of binary m-sequences the crosscorrelation function is said to be *preferred* if it takes on exactly three values where the values are $-1, -1 \pm 2^{\lfloor (m+2)/2 \rfloor}$ (see [13, Chapter 11]). The aim of this section is to show the nonexistence of preferred pairs of binary m-sequences in certain cases, thereby proving a conjecture of Sarwate-Pursley. Here is the result:

Theorem 3.1.1. *If $m \equiv 0$ (mod 4), then there are no preferred pairs of binary m-sequences.*

Proof. Let C be the binary cyclic code of length $n = 2^m - 1$ whose dual is generated by $h(x) = m_1(x)m_t(x)$, where $(t, n) = 1$. Note that the nonzeros of C are the elements

w^{-i}, w^{-it} for $i \in \{1, 2, 4, ..., 2^{m-1}\}$, where w is a primitive element of $\mathbb{F}_{2^m}$. Suppose that 4 divides m and C is a 3-weight cyclic code of length $n = 2^m - 1$, with weights $w_1 = 2^{m-1} - 2^{m/2}$, $w_2 = 2^{m-1}$, $w_3 = 2^{m-1} + 2^{m/2}$, i.e. those weights corresponding to preferred crosscorrelation values. Since $(t, 2^m - 1) = 1$, t is not congruent to $\{0, 3, 5, 6, 9, 10, 12\}$ mod15. The remaining possible values of t are considered in two cases with respect to the cyclotomic cosets that they belong to.

Case 1 $\underline{t \equiv 1, 2, 4, 8 \pmod{15}}$ Suppose that the frequencies of weights w_1, w_2, w_3 in C are N_1, N_2, N_3 respectively. Then the weight enumerator of C is

$$B(z) = 1 + N_1 z^{w_1} + N_2 z^{w_2} + N_3 z^{w_3}.$$

Let $\sum A_i z^i$ be the weight enumerator of $C^\perp$. When we write the first 5 Pless power moments for $n = 2^m - 1$ (see [[16], Section 7.2]), we obtain

$$\begin{aligned}
N_1 + N_2 + N_3 + 1 &= 2^{2m}, \\
1 + w_1 N_1 + w_2 N_2 + w_3 N_3 &= 2^{2m-1}(n - A_1), \\
1 + {w_1}^2 N_1 + {w_2}^2 N_2 + {w_3}^2 N_3 &= 2^{2m-2}\left[n(n+1) - 2nA_1 + 2A_2\right], \\
1 + {w_1}^3 N_1 + {w_2}^3 N_2 + {w_3}^3 N_3 &= 2^{2m-3}\left[n^2(n+3) - (3n^2 + 3n - 2)A_1 + 6nA_2 - 6A_3\right].
\end{aligned}$$

Note that since $m_1(x) | m_1(x) m_t(x)$, $C^\perp$ is a subcode of the binary Hamming code generated by $m_1(x)$, whose minimum distance is 3. Therefore $A_1 = A_2 = 0$. Hence the first three equations above become,

$$\begin{aligned}
N_1 + N_2 + N_3 &= 2^{2m} - 1, \\
1 + w_1 N_1 + w_2 N_2 + w_3 N_3 &= 2^{2m-1} n, \\
1 + {w_1}^2 N_1 + {w_2}^2 N_2 + {w_3}^2 N_3 &= 2^{2m-2} n(n+1).
\end{aligned}$$

Solving this system for N_1, N_2, N_3, and substituting the results in the 4^{th} Pless power moment, we obtain $A_3 = \frac{n}{3}$. Since $C^\perp = \langle m_1(x) m_t(x) \rangle$, for any codeword $c(x) = \sum_{i=0}^{n-1} c_i x^i \in C^\perp$, we have $c(w) = 0$ and $c(w^t) = 0$. Hence $c = (c_0, ..., c_{n-1})$ belongs to $C^\perp$ if and only if

$$\sum_{i=0}^{n-1} c_i w^i = 0 \text{ and } \sum_{i=0}^{n-1} c_i w^{ti} = 0. \tag{3.1}$$

Knowing that $A_3 = \frac{n}{3} > 1$, we conclude that $d(C^\perp) = 3$. A codeword of weight 3 in $C^\perp$ is a cyclic shift of a codeword of weight 3 with a 1 in the first coordinate. So, $c \in C^\perp$ has nonzero coordinates in c_0, c_i, c_j where $i \neq j$. Then, from (3.1), we have

$$1 + w^i + w^j = 0 \text{ and } 1 + w^{it} + w^{jt} = 0.$$

Letting $x = w^i$ and $y = w^j$, we conclude that the equation

$$1 + x^t + y^t = 1 + x^t + (x+1)^t = 0 \tag{3.2}$$

has a solution $x = w^i$ in $\mathbb{F}_{2^m}$ such that $x \neq 0, 1$. We claim that elements of $\mathbb{F}_4$ are solutions of $x^t + (x+1)^t = 1$, for all $t \equiv 1, 2, 4, 8 \pmod{15}$. To see this, let $\alpha \in \mathbb{F}_{2^m}$ with the minimal polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Hence $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Let us write $t = \tilde{t} + 15k$ with $\tilde{t} = 1, 2, 4, 8$. Since $\alpha^3 = 1$, we have $\alpha^t = \alpha^{\tilde{t}}$ for any $t, \tilde{t}$ as above. If $\tilde{t} = 1$, then

$$\alpha^t + (\alpha+1)^t = \alpha + (\alpha + 1) = 1.$$

Similarly α^2 satisfies (3.2). If $\tilde{t} = 2, 4, 8$, then

$$\alpha^t + (\alpha+1)^t = \alpha^{\tilde{t}} + (\alpha+1)^{\tilde{t}} = \alpha^{\tilde{t}} + \alpha^{\tilde{t}} + 1 = 1,$$

since the characteristic is 2. Similarly one can show that α^2 satisfies (3.2) for $\tilde{t} = 2, 4, 8$. So all the elements of $\mathbb{F}_4$ satisfy (3.2) for the given t values as above. Note that we can choose $\alpha = w^{\frac{n}{3}}$ since w is a primitive n^{th} root of unity, i.e. $x = w^{\frac{n}{3}}$ in (3.2). This means there is a codeword $c = (c_0, ..., c_{n-1}) \in C^{\perp}$ with $c_0 = c_{\frac{n}{3}} = c_{\frac{2n}{3}} = 1$. Note that c has exactly $\frac{n}{3}$ shifts and $A_3 = \frac{n}{3}$. Therefore, all of the weight 3 codewords in $C^{\perp}$ must have coordinates in $\mathbb{F}_4$. Equivalently, there exists no $x \in \mathbb{F}_{2^m} \backslash \mathbb{F}_4$ which solves (3.2) for any $t \equiv 1, 2, 4, 8 \pmod{15}$. However, foe a primitive elements β for $\mathbb{F}_{16}$ with $\beta^4 = \beta + 1$ (hence $\beta \in \mathbb{F}_{16} \backslash \mathbb{F}_4$), it is easy to show that β is solution to (3.2) for all $t \equiv 1, 2, 4, 8 \pmod{15}$, which gives a contradiction.

Case 2 $\underline{t \equiv 7, 11, 13, 14 \pmod{15}}$ Note that each of the weights $w_1 = 2^{m-1} - 2^{m/2}$, $w_2 = 2^{m-1}$, $w_3 = 2^{m-1} + 2^{m/2}$ in C is are divisible by $2^{\frac{m}{2}}$. Using McEliece's theorem, we will show the impossibility of this. Let us take $m = 4k$. The nonzeros of C are the elements w^{-i}, w^{-it} for $i \in \{1, 2, 4, ..., 2^{m-1}\}$, where w is a primitive element of $\mathbb{F}_{2^m}$. So if we can find $\frac{m}{2} = 2k$ integers in the set

$$\{1, 2, 4, ..., 2^{m-2}, 2^{m-1}, t, 2t, 4t, ..., 2^{m-1}t\}$$

that sum up to 0 mod $(2^m - 1)$, we will conclude by McEliece's theorem that the highest exponent of 2 that can divide all of the weights in C is $(\frac{m}{2} - 1)$. Note that the congruence $2^u t \equiv -1 \pmod{15}$ has a unique solution for t since $(2^u, 15) = 1$. Here are the solutions:

$$\text{For } u \equiv 0 \pmod{4},\ t \equiv 14 \pmod{15},$$

$$\text{For } u \equiv 1 \pmod{4},\ t \equiv 7 \pmod{15},$$

$$\text{For } u \equiv 2 \text{ (mod4)}, \ t \equiv 11 \text{ (mod15)},$$

$$\text{For } u \equiv 3 \text{ (mod4)}, \ t \equiv 13 \text{ (mod15)}.$$

Consider the following sum of $\frac{m}{2} = 2k$ integers,

$$1 + 2^4 + 2^8 + ... + 2^{4(k-1)} + 2^u t + 2^{u+4} t + 2^{u+8} t + ... + 2^{u+4(k-1)} t$$

$$\begin{aligned} &= (1 + 2^u t)(1 + 2^4 + 2^8 + ... + 2^{4(k-1)}) \\ &= (1 + 2^u t)(\frac{2^{4k} - 1}{2^4 - 1}) \\ &\equiv \ 0 \bmod (2^m - 1) \end{aligned}$$

provided that $2^u t \equiv -1$ (mod15).

Choosing $u \equiv 0, 1, 2, 3$ (mod 4) and $t \equiv 14, 7, 11, 13$ (mod 15) respectively we obtain the desired result for each t in this case. □

3.2 On Helleseth's Conjecture

In his classical paper [8] from 1976, Helleseth conjectured that if m is a power of 2, then there are no pairs of binary m-sequences with a 3-valued crosscorrelation function. Equivalently, there is no binary cyclic code C of length $n = 2^m - 1$ which contains the simplex code and which has 3 weights of the form $2^{m-1} - A, 2^{m-1}, 2^{m-1} + B$. In this section, we will present a proof for this conjecture in the case $A = B$, i.e. symmetric weights or correlation values. The proof is due to Calderbank, McGuire, Poonen, and Rubinstein ([1]). Before, we need a definition.

Definition 3.2.1. Let $a = \sum a_i 2^i$ and $b = \sum b_i 2^i$ be the binary expansions of a and b. Two binary expansions $(a_i), (b_i)$ are said to be *disjoint* if $(a_i, b_i) \neq (1, 1)$ for any i and binary expansion of (a_i) covers (b_i) if $(a_i, b_i) \neq (0, 1)$ for any i.

Remark 3.2.1. For two disjoint binary expansions $(a_i), (b_i)$ we have $w(a+b) = w(a) + w(b)$, where $w(a)$ and $w(b)$ is the number of nonzero terms in the binary expansion of a and b respectively.

Theorem 3.2.1. *If m is a power of 2, then there are no pairs of binary m-sequences of length $n = 2^m - 1$ with crosscorrelation values $-1, -1 \pm 2D$.*

Proof. Let C be the binary cyclic code of length $n = 2^m - 1$ whose dual is generated by $h(x) = m_1(x)m_t(x)$, where $(t, n) = 1$. Assume that the crosscorrelation function assumes the values $-1, -1 \pm 2D$ which implies that the corresponding cyclic code C has weights $w_1 = 2^{m-1} - D, w_2 = 2^{m-1}, w_3 = 2^{m-1} + D$. Let N_1, N_2, N_3 be the number of codewords with weights w_1, w_2, w_3 respectively. Then the weight enumerators of C and $C^{\perp}$ are

$$B(z) = 1 + N_1 z^{w_1} + N_2 z^{w_2} + N_3 z^{w_3} \text{ and } \sum_i A_i z^i.$$

When we write the first 4 Pless power moments for $n = 2^m - 1$, we obtain

$$\begin{aligned}
N_1 + N_2 + N_3 + 1 &= 2^{2m}, \\
1 + w_1 N_1 + w_2 N_2 + w_3 N_3 &= 2^{2m-1}(n - A_1), \\
1 + {w_1}^2 N_1 + {w_2}^2 N_2 + {w_3}^2 N_3 &= 2^{2m-2}\left[n(n+1) - 2nA_1 + 2A_2\right], \\
1 + {w_1}^3 N_1 + {w_2}^3 N_2 + {w_3}^3 N_3 &= 2^{2m-3}\left[n^2(n+3) - (3n^2 + 3n - 2)A_1 + 6nA_2 - 6A_3\right].
\end{aligned}$$

We have $A_1 = A_2 = 0$ for $C^{\perp}$ since $C^{\perp}$ is a subcode of the binary Hamming code, whose minimum distance is 3. Hence,

$$\begin{aligned}
N_1 + N_2 + N_3 &= 2^{2m} - 1, \\
1 + w_1 N_1 + w_2 N_2 + w_3 N_3 &= 2^{2m-1} n, \\
1 + {w_1}^2 N_1 + {w_2}^2 N_2 + {w_3}^2 N_3 &= 2^{2m-2} n(n+1).
\end{aligned}$$

After finding N_1, N_2, N_3 and substituting in the 4^{th} Pless power moment we obtain

$$A_3 = \frac{(2^m - 1)(D^2 - 2^{m-1})}{3 \cdot 2^{m-1}}.$$

This implies that 2^{m-1} divides D^2. Since m is even, we conclude that $2^{\frac{m}{2}}$ divides D. So all the nonzero weights $w_1 = 2^{m-1} - D, w_2 = 2^{m-1}, w_3 = 2^{m-1} + D$ in C will be divisible by $2^{\frac{m}{2}}$. (Note the similarities with the Case 1 in the proof of theorem 3.1.1). Now McEliece's theorem will be used to derive a contradiction to this conclusion. That is we will find at least one weight in C which is not divisible by $2^{\frac{m}{2}}$. To show this we need to find $\frac{m}{2}$ integers from the set $S = \{1, 2, 4, ..., 2^{m-1}, t, 2t, 4t, ..., 2^{m-1}t\}$ that sum up to 0 mod $(2^m - 1)$.

Let $m = 2^s$. In fact it is enough to find $2 \leq r \leq s$ and elements $\alpha_i \in S$ with $i = 1, ..., 2^{r-1}$ such that

$$\alpha_1 + \alpha_2 + ... + \alpha_{2^{r-1}} \equiv 0 \bmod (2^{2^r} - 1).$$

To see why, note that for $r < s$, if

$$\alpha_1 + \alpha_2 + ... + \alpha_{2^{r-1}} \equiv 0 \text{ mod } (2^{2^r} - 1),$$

$$\text{then } \left(\prod_{j=r}^{s-1}(2^{2^j} + 1)\right)(\alpha_1 + \alpha_2 + ... + \alpha_{2^{r-1}}) \equiv 0 \text{ mod } (2^{2^s} - 1).$$

Note that this product expresses 0 as a sum of $(2^{s-1-r+1})(2^{r-1}) = 2^{s-1} = \frac{m}{2}$ elements from the set S.

Let $M = 2^{r-1}$ denote the power of 2 such that $t \equiv 2^j \text{ mod } (2^M - 1)$ for some j, but $t \not\equiv 2^l \text{ mod } (2^{2M} - 1)$ for any l. From the previous observation we need to find $M = 2^{r-1}$ integers $\alpha_1, \alpha_2, ..., \alpha_M$ from the set S such that

$$\sum_{i=1}^{M} \alpha_i \equiv 0 \text{ mod } (2^{2M} - 1).$$

For the positive integers a and b with binary expansions

$$\sum_i a_i 2^i \text{ and } \sum_i b_i 2^i,$$

assume that the following holds:

$$a_i = \begin{cases} 1 & \text{if } 2^i t \in \{\alpha_1, \alpha_2, ..., \alpha_{2^{r-1}}\} \\ 0 & \text{otherwise} \end{cases}$$

$$b_i = \begin{cases} 1 & \text{if } 2^i \in \{\alpha_1, \alpha_2, ..., \alpha_{2^{r-1}}\} \\ 0 & \text{otherwise.} \end{cases}$$

This implies that

$$\sum_{i=1}^{M} \alpha_i \equiv \sum_i a_i 2^i t + \sum_i b_i 2^i \equiv 0 \text{ mod } (2^{2M} - 1).$$

Thus we have $at + b \equiv 0 \pmod{2^{2M} - 1}$. After these observations, it will be enough to find integers a, b with $at+b \equiv 0 \pmod{2^{2M}-1}$ and $w(a)+w(b) = M$, to apply McEliece's theorem to show that there is at least one weight in C which is not divisible by $2^{\frac{m}{2}}$. The integers a, b will be represented with the binary vectors $(a_i), (b_i)$ respectively. Since the code C is determined by the cyclotomic coset $Cl(t)$, by replacing t with $2^{2M-j}t$ we may suppose that $t \equiv 1 \text{ mod}(2^M - 1)$. Thus,

$$t \equiv 1 + k(2^M + 1) \text{ mod}(2^{2M} - 1)$$

for some $1 < k < 2^M + 1$. Consider the first M terms in the binary expansion for $k - 1$ and $2^M - 1 - (k - 1)$, then we have

$$\sum_{i=0}^{M-1} c_i 2^i \text{ and } \sum_{i=0}^{M-1} (1 - c_i) 2^i$$

respectively, that is the first M terms in the binary expansion of $k - 1$ are the complements of the first M terms in the binary expansion of $2^M - 1 - (k - 1)$. Since $k - 1 \leq 2^M - 1$, the $1's$ in the binary expansion of $k - 1$ occur in the first M terms. From

$$k(2^M - 1) = 2^M(k - 1) + (2^M - 1 - (k - 1)),$$

we observe that the binary expansions of $2^M(k - 1)$ and $(2^M - 1 - (k - 1))$ are disjoint and since multiplying $(k - 1)$ with 2^M will just shift the terms c_i to c_{i+M} we have $w(k(2^M - 1)) = M$. After this observation it will be enough to find a and b with disjoint binary expansions, such that

$$a + b = k(2^M - 1) \text{ and } k(a + 1) \equiv 0 \bmod (2^M + 1).$$

Disjoint binary expansions of a and b will imply that

$$w(a + b) = w(k(2^M - 1)) = w(a) + w(b) = M.$$

Moreover $k(a + 1) \equiv 0 \bmod (2^M + 1)$ will imply,

$$\begin{aligned} at + b &\equiv a + b + ak(2^M - 1) \bmod (2^{2M} - 1) \\ &\equiv k(2^M - 1)(a + 1) \bmod (2^{2M} - 1) \\ &\equiv 0 \bmod (2^{2M} - 1) \end{aligned}$$

Now let 2^h be the highest power of 2 dividing $k - 1$. The integers a and b are chosen as $a = 2^{M+h} + 2^h - 1$ and $b = k(2^M - 1) - a$. Then first of all we have

$$k(a + 1) = k2^h(2^M + 1) \equiv 0 \bmod (2^M + 1).$$

Since binary expansion of $a = 2^{M+h} + 2^h - 1$ is covered by $k(2^M - 1)$, a and b have disjoint binary expansions which implies $w(a+b) = w(a) + w(b) = w(k(2^M - 1)) = M$. To sum up we found $M = 2^{r-1}$ elements $\alpha_1, \alpha_2, ..., \alpha_M$ from the set S which sum up to zero modulo $2^r - 1$, then these M elements are used to obtain the congruence

$$\left(\prod_{j=r}^{s-1} (2^{2^j} + 1) \right) (\alpha_1 + \alpha_2 + ... + \alpha_{2^{r-1}}) \equiv 0 \bmod (2^{2^s} - 1)$$

which expresses zero as a sum of $\frac{m}{2}$ elements of S. Thus, by using McEliece's theorem we conclude that there must be at least one codeword in C whose weight is not divisible by $2^{\frac{m}{2}}$ which is a contradiction to the fact that all the nonzero weights in C are $w_1 = 2^{m-1} - D, w_2 = 2^{m-1}, w_3 = 2^{m-1} + D$ are divisible by $2^{\frac{m}{2}}$. □

CHAPTER 4

THE WELCH CONJECTURE

Two of the most important conjectures on m-sequences were finally proved in the beginning of this century. These are Niho and Welch conjectures. Both of them are about decimations yielding 3-valued crosscorrelatin function. Namely, Niho conjecture states that for odd n, say $n = 2m+1$ and $d = 2^{2r} + 2^r - 1$, where $4r + 1 \equiv 0 \pmod{n}$, the crosscorrelation function between a binary m-sequence of length $2^n - 1$ and its decimation by d takes on the three values $-1, -1 \pm 2^{m+1}$, whereas the Welch conjecture states the same conclusion for $n = 2m+1$ and $d = 2^m + 3$. Niho's conjecture was proved by Hollmann and Xiang in [9]. In this paper they also gave a proof of the Welch conjecture. Independently, Canteaut, Charpin, and Dobbertin proved Welch's conjecture in [2]. In this chapter we will present the latter proof of the Welch conjecture. In fact Canteaut, Charpin and Dobbertin proves that the powers functions x^d on $\mathbb{F}_{2^n}$ are maximally nonlinear which is equivalent to Welch conjecture. Therefore, by presenting this proof we will be able to relate the crosscorrelation of binary m-sequences to yet another topic.

As in the proofs of the conjectures in Chapter 3, McEliece's theorem plays a major role in the proof of the Welch conjecture. The proof also relies on some earlier work of the authors. We particularly refer to [3], [4], [7] for a more comprehensive understanding of the subject. Finally throughout this chapter Tr represents the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ where $n = 2m+1$.

4.1 Maximally Nonlinear Power Functions

In this section we introduce the basic notions and facts that are needed to for the proof of the Welch's conjecture.

Definition 4.1.1. A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear **(APN)*** if every equation

$$F(a+t) + F(t) = b \ (a \in \ \mathbb{F}_{2^n}^*, \ b \in \ \mathbb{F}_{2^n})$$

has at most two solutions t in $\mathbb{F}_{2^n}$.

Note that if $F(a+t_o)+F(t_o)=b$, then $F(a+(a+t_o))+F(a+t_o)=b$ as well. Hence the above equation has either no solution or exactly two solutions.

Definition 4.1.2. The *Walsh transform* f^W of a Boolean function $f:\mathbb{F}_{2^n}\longrightarrow\mathbb{F}_2$ is defined by

$$f^W(a)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(f(x)+Tr(ax))}.$$

The values $f^W(a)$ are called the *Walsh coefficients* of f.

Remark 4.1.1. If $\left|f^W(a)\right|$ is "large" the values of $f(x)$ agree with $Tr(ax)$ (if $f^W(a)>0$) or $Tr(ax)+1$ (if $f^W(a)<0$) for many $x\in\mathbb{F}_{2^n}$. In other words, f is well approximated by a linear function.

This remark motivates the following notion:

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

Note that if $\mathcal{L}(f)$ is "small", the Boolean function f is far from being linear, i.e. it is nonlinear. Now, we define the similar notions for a function $F:\mathbb{F}_{2^n}\longrightarrow\mathbb{F}_{2^n}$.

Definition 4.1.3. The *Walsh transform* of $F:\mathbb{F}_{2^n}\longrightarrow\mathbb{F}_{2^n}$ is the collection of all Walsh transforms of $f_s(x)=Tr(sF(x))$, $s\in\mathbb{F}_{2^n}^*$.

Furthermore, we set

$$\mathcal{L}(F)=\max\{\mathcal{L}(f_s):s\in\mathbb{F}_{2^n}^*\}.$$

Definition 4.1.4. The function $F:\mathbb{F}_{2^n}\longrightarrow\mathbb{F}_{2^n}$ is said to be *maximally nonlinear* if it attains the minimal possible value for $\mathcal{L}(F)$.

For $n=2m+1$ this minimum is known to be 2^{m+1}. Furthermore we have the following (see [5], [6]).

Theorem 4.1.1. *For $n=2m+1$, $F:\mathbb{F}_{2^n}\longrightarrow\mathbb{F}_{2^n}$ is maximally nonlinear if and only if the set of values attained by the Walsh transform $W(F)=\{0,\pm 2^{m+1}\}$. Moreover, if F is maximally nonlinear then F is **APN**.*

In the remaining of this section we will show the relation between the Walsh spectrum of power functions and the crosscorrelation of binary m-sequences. Consider the Walsh transform of the power function $F(x)=x^d$, where $(d,2^n-1)=1$,

$$f_s^W(a)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(sx^d+ax)}.$$

Since $(d, 2^n - 1) = 1$, $s = (s^{'})^d$ for some $s^{'} \in \mathbb{F}_{2^n}^*$. Thus we have $sx^d = (s^{'}x)^d$. Now by writing $ax = as^{'}(s^{'})^{-1}x$, and setting $a(s^{'})^{-1} = b$, we have $ax = bs^{'}x$. As x runs through $\mathbb{F}_{2^n}$, so does $y = s^{'}x$. Therefore by substituting y instead of $s^{'}x$, we have

$$f_s^W(a) = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr(y^d + by)}$$

where $b = as^{'} = a\sqrt[d]{s} \in \mathbb{F}_{2^n}$. Note that for $b = 0$, $f_s^W(b) = 0$. Recall the crosscorrelation function between an m-sequence and its d^{th} decimation is given by

$$\Theta_d(l) = \sum_{i=0}^{2^n-2} (-1)^{Tr(\alpha^l x + x^d)} \quad l \in \ \{0, 1, ..., 2^n - 2\}$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Note that as l runs through the set $\{0, 1, ..., 2^n - 2\}$, α^l runs through all the nonzero elements in $\mathbb{F}_{2^n}$. Hence

$$1 + \Theta_d(l) = f_s^W(a),$$

for $a = \alpha^l \sqrt[d]{s} \in \mathbb{F}_{2^n}$. Hence we have proved the following:

Theorem 4.1.2. *Let $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ be the power function $F(x) = x^d$, where $(d, 2^n - 1) = 1$. Then the Walsh spectrum of F and the crosscorrelation function between a binary m-sequence of length $2^n - 1$ and its d^{th} decimation are related by*

$$\{\Theta_d(l) + 1 : \ l = 0, ..., 2^n - 2\} = \left\{f_s^W(a) : \ a, s \in \mathbb{F}_{2^n}\right\}.$$

Thus, Theorem 4.1.1 can be revised for power functions as follows:

Corollary 4.1.1. *A power function $F(x) = x^d$ is maximally nonlinear if and only if the crosscorrelation function between a binary m-sequence of length $2^n - 1$ and its decimation by d takes on exactly the three values $-1, -1 \pm 2^{m+1}$, where $n = 2m + 1$.*

4.2 Proof of the Welch Conjecture

In 1968, Welch conjectured that the power function x^d for $d = 2^m + 3$ is maximally nonlinear or in other words the crosscorrelation function between a binary m-sequence u of length $2^n - 1$ and its decimation v by $d = 2^m + 3$ takes on exactly the three values $-1, -1 \pm 2^{m+1}$. In this section, we will present a proof of this conjecture which is due to Canteaut, Charpin, and Dobbertin [2]. The power functions x^d where $d = 2^m + 3$, m odd are called *Welch power functions.* An important step towards the verification of Welch's conjecture is an earlier result of Dobbertin [7]:

Theorem 4.2.1. *Welch power functions are* ***APN****.*

Recall that **APN** property was implied by maximal nonlinearity. Exact converse of this statement is not true. However, with an extra condition we will be able to write an almost-a-converse statement to this fact. First we need a lemma.

Lemma 4.2.1. *If x^d is* ***APN*** *then the sum of fourth powers of all Walsh coefficients of $Tr(x^d)$ is equal to 2^{3n+1}.*

Proof.

$$\sum_{a\in\mathbb{F}_{2^n}} (f^W(a))^4 = \sum_{a\in\mathbb{F}_{2^n}} \Big(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr(ax+x^d)} \Big)^4$$

$$\begin{aligned}
&= \sum_{a\in\mathbb{F}_{2^n}} \Big(\sum_{x,y,z,w\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+z^d+w^d+a(x+y+z+w))} \Big) \\
&= \sum_{a,x,y,z,w\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+z^d+w^d+a(x+y+z+w))} \\
&= \sum_{x,y,z,w\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+z^d+w^d)} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{Tr(a(x+y+z+w))}.
\end{aligned}$$

If $x+y+z+w \neq 0$ then as a runs through the elements of $\mathbb{F}_{2^n}$ so does $a(x+y+z+w)$. By the properties of canonical additive character, we have

$$\sum_{a\in\mathbb{F}_{2^n}} (-1)^{Tr(a(x+y+z+w))} = \begin{cases} 0 & \text{if } x+y+z+w \neq 0 \\ 2^n & \text{if } x+y+z+w = 0 \end{cases}$$

Hence replacing w with $x+y+z$, we obtain

$$\sum_{a\in\mathbb{F}_{2^n}} (f^W(a))^4 = 2^n \left(\sum_{x,y,z\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+z^d+(x+y+z)^d)} \right)$$

Splitting this sum into two parts for the cases $z=0$ and $z\neq 0$, we get

$$\sum_{a\in\mathbb{F}_{2^n}} (f^W(a))^4 = 2^n \left(\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+(x+y)^d)} \right)$$

$$+2^n \left(\sum_{x,y\in\mathbb{F}_{2^n}} \sum_{z\in\mathbb{F}^*_{2^n}} (-1)^{Tr(z^d((x/z+y/z+1)^d+(x/z)^d+(y/z)^d+1))} \right)$$

$$= 2^n \left(\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{Tr(x^d+y^d+(x+y)^d)} - 2^{2n} \right) + 2^n \left(\sum_{u,v,z\in\mathbb{F}_{2^n}} (-1)^{Tr(z^d((u+v+1)^d+u^d+v^d+1))} \right)$$

where $u = \frac{x}{z}$ and $v = \frac{y}{z}$. Now $(u+v+1)^d + u^d + v^d + 1 = 0$ if and only if either $u = v$ or

$$\left(\frac{1}{u+v}+1\right)^d + \left(\frac{1}{u+v}\right)^d = \left(\frac{u}{u+v}+1\right)^d + \left(\frac{u}{u+v}\right)^d$$

which is obtained by dividing all terms by $(u+v)^d$. Since the power function x^d is **APN** $(x+1)^d + x^d = c$ will have at most two solutions. However for $t = \frac{1}{u+v}$ and $t_1 = \frac{u}{u+v}$ we would have 4 different solutions, so we must have either $u = 1$ or $v = 1$. The number of pairs satisfying $u = v$ or $u = 1$ or $v = 1$ is $3 \cdot (2^n - 1) + 1$. So, we have

$$\sum_{u,v,z \in \mathbb{F}_{2^n}} (-1)^{Tr(z^d((u+v+1)^d + u^d + v^d + 1)} = 2^n(3 \cdot (2^n - 1) + 1)$$

Similarly, split the following into two sums depending on $y = 0$ or $y \neq 0$

$$\begin{aligned} \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr(x^d + y^d + (x+y)^d)} &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(2x^d)} + \sum_{x \in \mathbb{F}_{2^n}, y \in \mathbb{F}^*_{2^n}} (-1)^{Tr(y^d(1 + (\frac{x}{y})^d) + (1 + \frac{x}{y})^d)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(2x^d)} - 2^n + \sum_{u,y \in \mathbb{F}_{2^n}} (-1)^{Tr(y^d(1 + u^d + (1+u)^d))} \end{aligned}$$

where $u = \frac{x}{y}$. Now since x^d is **APN** the equation $u^d + (1+u)^d = 1$ has at most two solutions for u which are $u = 0, 1$. Therefore

$$\sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr(x^d + y^d + (x+y)^d)} = 2^{n+1} \text{ and } \sum_{a \in \mathbb{F}_{2^n}} (f^W(a))^4 = 2^{3n+1}.$$

□

Remark 4.2.1. This result can also be obtained by replacing $f^W(a)$ by $\Theta_{u,v}(l) + 1$ and calculating $\sum_{l=0}^{2^n-2} (\Theta_d(l) + 1)^4$ as in Chapter 2.

Now we are ready to prove the "converse" of the Theorem 4.2.1.

Theorem 4.2.2. *For an **APN** power function x^d if all Walsh coefficients of $Tr(x^d)$ are divisible by 2^{m+1}, then x^d is maximally nonlinear.*

Proof. Let W_i denote the sequence of absolute values of Walsh coefficients occuring in the Walsh spectrum of $Tr(x^d)$ for $i = 0, 1, ..., k-1$. Now by assumption all Walsh coefficients of $Tr(x^d)$ are divisible by 2^{m+1}. So let $W_i = 2^{m+1}V_i$ where $V_0 = 1$ since $\pm 2^{m-1}$ is in the Walsh spectrum of F and $V_i > 1$ for $1 \leq i < k$. Suppose that each W_i occurs λ_i times. Now if x^d is **APN**, then by Lemma 4.2.1 we have

$$\sum_{i<k} \lambda_i {W_i}^4 = \sum_{i<k} \lambda_i 2^{4m+4} V_i^4 = \sum_{i<k} \lambda_i 2^{2n+2} V_i^4 = 2^{3n+1}.$$

By Theorem 2.1.1 and Corollary 2.1.1,

$$\begin{aligned} \sum_{l=0}^{2^n-2} (\Theta_d(l) + 1)^2 &= \sum_{l=0}^{2^n-2} \left(\Theta_d(l)^2 + 2\Theta_d(l) + 1\right) \\ &= 2^{2n}. \end{aligned}$$

Thus, we have

$$\sum_{i<k} \lambda_i {W_i}^2 = \sum_{i<k} \lambda_i 2^{n+1} V_i^2 = 2^{2n}.$$

Therefore,

$$\sum_{i<k} \lambda_i V_i^4 = \sum_{i<k} \lambda_i V_i^2,$$

or equivalently

$$\sum_{1 \le i<k} \lambda_i (V_i^4 - V_i^2) = 0.$$

Since ${V_i}^4 - V_i^2 > 0$ for all $i \ge 1$, we must have $\lambda_i = 0$ for all $i \ge 1$. Thus $W(x^d) = \{0, \pm 2^{m+1}\}$ and hence x^d is maximally nonlinear by Theorem 4.1.1. □

To prove Welch's conjecture it remains to show that all Walsh coefficients of $Tr(x^d)$ are divisible by 2^{m+1}. This is equivalent to showing that $\Theta_d(l) + 1$ is divisible by 2^{m+1} for all $l = 0, ..., 2^n - 2$, for a binary m-sequence of length $2^n - 1$ and its d^{th} decimation. Hence the weights of every nonzero codeword $c \in C_{1,d}^{\perp}$ will be divisible by 2^m, where $C_{1,d}$ is the cyclic code of length $2^n - 1$ with the generator polynomial $m_1(x)m_d(x)$. Using McEliece's theorem this corresponds to showing for all nonzero $a < 2^n - 1$,

$$w_n(a) + w_n(-ad) \ge m + 1$$

is satisfied. Now for $a \equiv a^{'} \text{mod } (2^n - 1)$ we have $w_n(a) = w(a^{'})$ where $w(a^{'})$ denotes the the Hamming weight of binary expansion of $a^{'}$. Hence, to show that the Welch power function x^d is maximally nonlinear, we have to verify that for all nonzero $a < 2^n - 1$, we have

$$w_n(a) + w_n(-ad) \ge m + 1.$$

Since for all nonzero x, we have $w_n(-x) = 2m + 1 - w_n(x)$, the above statement is equivalent to

$$w_n(ad) - w_n(a) \le m. \qquad (4.1)$$

We can assume that $w_n(a) \le m$. In fact, there exists a pair of integers $i, i+m$ (mod n) such that $a_i = a_{i+m} = 0$, since otherwise we would have $w_n(a) \ge m + 1$. Represent the element a in the form

$$a = b + 2^{m+1}c$$

where $b < 2^m$ and $c < 2^{m-1}$. We have

$$ad = 2^m(b + 6c) + 3b + 2^{2m+1}c,$$

that is

$$ad = (3b + c) + 2^m(b + 6c) \bmod (2^n - 1).$$

Also recall that for arbitrary integers x, y,

$$w(x + y) \leq w(x) + w(y),$$

where equality holds in the case x and y have disjoint binary expansions. This statement also holds for w_n with $x, y < 2^n - 1$. Define a function H for arbitrary integers (finite bit strings) B, C as

$$H(B, C) = w(3B + C) + w(B + 6C) - w(B) - w(C).$$

By the choice of integers $b \leq 2^m - 1$ and $c \leq 2^{m-1} - 1$, b and $2^{m+1}c$ have disjoint binary expansions. Therefore

$$w_n(a) = w(b) + w(c).$$

For $ad = (3b + c) + 2^m(b + 6c) \bmod (2^n - 1)$, we have

$$w_n(ad) \leq w(3b + c) + w(b + 6c).$$

Hence, (4.1) can be written as

$$w_n(ad) - w_n(d) \leq H(b, c). \tag{4.2}$$

We will try to prove (4.2) in the rest of this section. First technical lemmas are needed. We refer to [2] for their proofs.

Lemma 4.2.2. *Let*

$$B = B_5B_4B_3B_2B_1B_0 \text{ and } C = C_5C_4C_3C_2C_1C_0.$$

be bit strings of length 6*, that is integers less than* 64*.*

i) *Then there is some nonzero $r \leq 6$ such that*

$$H(B_{r-1}...B_0, C_{r-1}...C_0) \leq r.$$

ii) *If $B_0 = C_0 = 1$ then there is some nonzero $r \leq 6$, such that*

$$H(B_{r-1}...B_0, C_{r-1}...C_0) < r.$$

For 7*-bit strings $B = B_6B_5B_4B_3B_2B_1B_0$ and $C = C_6C_5C_4C_3C_2C_1C_0$,*

iii) *If* $(B_0, C_0) = (1, 0)$ *then there is some nonzero* $r \leq 7$, *with*

$$H(B_{r-1}...B_0, C_{r-1}...C_0) \leq r,$$

or there is some nonzero $r \leq 6$ *with*

$$H(B_{r-1}...B_0, C_{r-1}...C_0) = r$$

and $(B_r, C_r) \neq (1, 0)$.

Lemma 4.2.3. *Let* $s \geq 1$. *Let*

$$B = B_{s-1}...B_0$$

$$C = C_{s-1}...C_0$$

be bit strings of length s, *that is integers less than* 2^s.

i) *Then*

$$H(B, C) \leq s + 2$$

and $H(B, C) = s + 2$ *implies* $B_0 = 1$, $C_0 = 0$.

ii) *If* $B_{s-1} = 1$ *and* $C_{s-1} = 0$ *then*

$$H(B, C) \leq s + 1$$

and $H(B, C) = s + 1$ *implies* $B_0 \neq C_0$.

iii) *If* $s \geq 2$, $B_{s-1} = 1$, *and* $C_{s-1} = C_{s-2} = 0$, *then* $H(B, C) = s + 1$ *implies* $B_0 = 1$, $C_0 = 0$, *and* $3B + C < 2^{s+1}$.

We are ready to finish the proof of Welch's conjecture.

Theorem 4.2.3. *For the Welch power functions* x^d, *all Walsh coefficients of* $Tr(x^d)$ *are divisible by* 2^{m+1}.

Conclusion of the proof of Theorem 4.2.2. Recall that we reduced the proof to proving (4.2). We study 4 cases:

Case 1 Assume for b, c we have $2^{m-1} \leq b < 2^m$ and $2^{m-2} \leq c < 2^{m-1}$. Since $b \leq 2^m - 1$ and $c \leq 2^{m-1} - 1$ we have $b_{m-1} = 1$ and $c_{m-1} = 0$ which corresponds to the case (ii) in the Lemma 4.2.3, so we have $H(b, c) \leq m + 1$. Now suppose that $H(b, c) = m + 1$. Since $b \geq 2^{m-1}$ and $c \geq 2^{m-2}$, $b + 6c \geq 2^{m+1}$ we have

$$ad \equiv (b + 6c - 2^{m+1})2^m + (3b + c + 1) \bmod (2^{2m+1})$$

which implies that

$$w_n(ad) \leq w(b + 6c - 2^{m+1}) \; + \; w_(3b + c + 1)$$

Moreover since $2^{m+1} \leq b + 6c < 2^{m+2}$, we have $w(b + 6c - 2^{m+1}) = w(b + 6c) - 1$. By the same lemma case (ii) for $H(b, c) = m + 1$ we have $b_0 \neq c_0$, which implies that $3b+c$ is odd. Thus, $w(3b + c + 1) < w(3b + c)$. For $H(b, c) = m + 1$, by combining above results we obtain

$$w_n(ad) \leq w(b + 6c) - 1 + w(3b + c)$$

and since $H(b, c) = w(b + 6c) + w(3b + c) - w_n(a)$ we have

$$w_n(ad) \leq H(b, c) + w_n(a) - 1,$$

which implies

$$w_n(ad) - w_n(a) \leq H(b, c) - 1 \leq m.$$

Case 2 Assume for b, c we have $2^{m-1} \leq b < 2^m$ and $c < 2^{m-2}$. Now since $b \leq 2^m - 1$ and $c \leq 2^{m-2} - 1$ we have $b_{m-1} = 1$ and $c_{m-1} = c_{m-2} = 0$. This corresponds to case (iii) in Lemma 4.2.3, thus we have $H(b, c) \leq m + 1$. Suppose that $H(b, c) = m + 1$, then the same case implies that $b_0 = 1$, $c_0 = 0$ and $3b+c < 2^{m+1}$. For the values b and c given, we have $3b + c > 2^m$, thus $w(3b + c - 2^m) = w(3b + c) - 1$. Since $b_0 = 1$ and $c_0 = 0$, $b + 6c$ is odd. Therefore $w(b + 6c + 1) < w(b + 6c)$. By writing,

$$ad \equiv (b + 6c + 1)2^m \; + \; (3b + c - 2^m) \bmod (2^{2m+1} - 1),$$

we obtain

$$w_n(ad) \leq w(b + 6c + 1) \; + \; w(3b + c - 2^m).$$

By using the above results we have

$$w_n(ad) \leq w(b + 6c) \; + \; w(3b + c) \; - 1,$$

$$w_n(ad) \leq H(b, c) \; + \; w_n(a) \; - 1,$$

and thus

$$w_n(ad) \; - \; w_n(a) \leq m.$$

Case 3 Assume for b, c we have $b < 2^{m-1}$ and $c < 2^{m-2}$. Now if also $b < 2^{m-2}$, by case (i) of Lemma 4.2.3, we have $H(b, c) \leq m$ and since $w_n(ad) - w_n(a) \leq H(b, c)$ we are done. If for b we have $2^{m-2} \leq b < 2^{m-1}$, then $b_{m-2} = 1$ and $c_{m-2} = 0$ which corresponds to the case (ii) of Lemma 4.2.3, where we have $H(b,c) \leq m$, and by $w_n(ad) - w_n(a) \leq H(b,c)$ we obtain the result.

Case 4 Assume for b, c we have $b < 2^{m-1}$ and $2^{m-1} \leq c < 2^m$. Now define $a^{'}$ as

$$a^{'} = 2^{m+1} a \ mod\ (2^{2m+1} - 1) = b2^{m+1} + 2c.$$

Now for $2c$, we have $2^{m-1} \leq 2c < 2^m$. Set $2c = l$. Consider

$$a^{'}d = b2^{2m+1} + 2^m(l + 6b) + 3l$$

and the congruence

$$a^{'}d \equiv (b + 3l - 2^m) \ + \ 2^m(l + 6b + 1).$$

Since $b < 2^{m-1}$ and $2^{m-1} \leq l < 2^m$ we have $b_{m-1} = 0$ and $l_{m-1} = 1$, so by case (ii) of Lemma 4.2.3 we have $H(l,b) \leq m+1$. Suppose that $H(l,b) = m+1$, by the same case we have $b_0 \neq c_0$, which implies that $l + 6b$ is odd, thus $w(l + 6b + 1) < w(l + 6b)$. Note that we have $b + 3l > 2^m$ so $w(b + 3l - 2^m) = w(b + 3l) - 1$. From the congruence above we obtain,

$$w_n(a^{'}d) \leq w(b + 3l - 2^m) \ + \ w(l + 6b + 1).$$

When we combine the results stated above we have,

$$w_n(a^{'}d) \leq w(b + 3l) \ + w(l + 6b) \ - 1.$$

Recall that $H(l,b) = w(3l + b) + w(l + 6b) - w(b) - w(l)$ and $a^{'} = b2^{m+1} + l$. We have $w_n(a^{'}) = w(b) + w(l)$ since the binary expansions of $b2^{m+1}$ and l are disjoint. Thus,

$$w_n(a^{'}d) \leq H(l,b) \ + w_n(a^{'}) \ - 1,$$

$$w_n(a^{'}d) \ - \ w_n(a^{'}) \leq m.$$

Finally using the relations,

$$w_n(a^{'}d) = w_n(ad) \ and \ w_n(a^{'}) = w_n(a)$$

we conclude that

$$w_n(ad) \ - \ w_n(a) \leq m.$$

Combining Theorem 4.2.3 with the fact that Welch power functions are **APN**, and using Theorem 4.2.2, we conclude that Welch power functions are maximally nonlinear. As explained before this is equivalent to the validity of Welch's conjecture.

Bibliography

[1] A.R. Calderbank, G. McGuire, B. Poonen and M. Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-Sequences, IEEE Trans. Inform. Theory, vol. 42, no. 3, 988-990, 1996.

[2] A. Canteaut, P. Charpin and H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, IEEE Trans. Inform. Theory, vol. 46, no.1, 4-8, 2000.

[3] A. Canteaut, P. Charpin, and H. Dobbertin, Weight divisibility of cyclic codes, hihgly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences, SIAM J. Discrete Math., vol.13, no.1, 105-138, 2000.

[4] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutation suitable for DES-like cryptosystems, Des. Codes Cryptogr., vol. 15, no. 2, 125-156, 1998.

[5] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Advances in Cryptology - EUROCRYPT '94, A. De Santis (ed.), Lecture Notes in Comput. Sci., vol.950, 356-365, 1995.

[6] H. Dobbertin, One to One Highly Nonlinear Power Functions on $GF(2^n)$, Appl. Algebra Engrg. Comm. Comput.,vol. 9, no.2, 139-152, 1998.

[7] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Welch Case, IEEE Trans. Inform. Theory, vol.45, 1271-1275, no.4, 1999.

[8] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math., vol.16, no.3, 209-232, 1976.

[9] H. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-Sequences, Finite Fields Appl., vol.7, no.2, 253-286, 2001.

[10] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer, 1990.

[11] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, 1983.

[12] R.J. McEliece, Weight congruences for p-ary cyclic codes, Discrete Math., vol.3, 177-192, 1972.

[13] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer, 1987.

[14] G. McGuire and A.R. Calderbank, Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences, IEEE Trans. Inform. Theory, vol. 41, no. 4, 1153-1155, 1995.

[15] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences, Ph.D. dissertation, Univ. Southern California, 1972.

[16] V. Pless and W.C. Huffman, Fundamentals of error-correcting codes, Cambridge University Press 2003.

[17] P. Rosendahl, Niho type cross-correlation functions and related equations, Ph.D. dissertation, Univ. of Turku, 2004.

[18] D.V. Sarwate and M.B. Pursley, Crosscorrelation properties of pseudo-random and related sequences, Proc. IEEE, vol. 68, no.5, 593-619, 1980.

[19] H.M. Trachtenberg, On the cross-correlation functions of maximal linear recurring sequences, Ph.D. dissertation, Univ. Southern California, 1970.

[20] J. Wolfmann, New bounds on cyclic codes from algebraic curves, Coding Theory and Applications, Toulon, Lecture Notes in Comput. Sci., vol. 388, 47-62, 1989.