PARTIAL SPREADS AND HYPERBENT FUNCTIONS IN ODD CHARACTERISTIC

by

Hui Yi Lu
B.Sc., Simon Fraser University, 2008

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN THE DEPARTMENT
OF
MATHEMATICS

SIMON FRASER UNIVERSITY
Summer 2011

APPROVAL

Name:	Hui Yi Lu
Degree:	Master of Science
Title of Thesis:	Partial Spreads And Hyperbent Functions in Odd Characteristic
Examining Committee:	Dr. Marni Mishna (Chair)

____

Dr. Petr Lisonek, Senior Supervisor

____

Dr. Jonathan Jedwab, Supervisor

____

Dr. Stephen Choi, Examiner

Date Approved: June 9, 2011

Declaration of Partial Copyright Licence

Abstract

We study bent functions which are as different as possible from linear functions. Functions that remain bent under all bijective monomial substitutions are called hyperbent.

In Chapter 2 we introduce partial spreads to construct a family of bent functions on vector spaces of even dimension over a finite field. This generalizes the construction given by Dillon for fields of characteristic 2. In Chapter 3 we use finite fields to introduce an explicit family of functions in the trace form whose hyperbentness can be tested using results of Chapter 2. This test is more efficient than using the definition of a bent function. It is an analogue of a result by Charpin and Gong for characteristic 2.

The motivation for studying bent functions is their important role in cryptography and coding theory. For example, the CAST cipher constructed using bent functions is approved for use by the Canadian government.

Acknowledgments

I would like to express my sincere gratitude to Simon Fraser University and the Department of Mathematics for having me as a student and supporting me with Graduate Fellowships and teaching appointments. I would also like to thank Province of British Columbia for awarding me the Pacific Century Graduate Scholarship and thank for the Research Assistantships from Petr Lisonek's NSERC grant that allowed me to do research on combinatorics and finite fields and attend numerous conferences.

On the personal note first and foremost, I would like to thank my supervisor Dr. Petr Lisonek. Thank you for being patient and encouraging and for guiding me through this entire process; I could not ask for a better advisor.

To my committee members for reading this thesis and making suggestions for possible improvements.

To Lin Qi for keeping me in your heart.

To Sulin for everything you mean to me.

To all my family for believing in me and for making me what I am today.

Finally, I would like to thank my parents for giving me all their love and supporting me with whatever they have.

Contents

List of Figures

Chapter 1

Background

1.1 Introduction

Throughout this thesis we assume knowledge of finite fields. The readers seeking details about the proofs of some theorems that are used without proof can refer to [16] and [4].

In 1974 John F. Dillon in his PhD thesis proved that certain kinds of binary functions defined by partial spreads are bent with the help of difference sets in the binary case. Our first result is an extension of Dillon's result. The functions we deal with are p-ary instead of binary.

In 2006, T. Helleseth and A. Kholosha proved theorems about a family of monomial (with exactly one term) bent functions $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$, where p is an odd prime [9]. In 2008, P. Charpin and G. Gong proved theorems about a family of multinomial binary bent functions [2]. With the inspiration of these two papers, we get the second result of our thesis: a method that is faster to find a family of multinomial p-ary bent functions defined by trace functions than using the definition.

In this chapter, we will provide knowledge that is needed to prove theorems in later chapters such as group algebra, Dickson polynomials and characters. We will also explain why a bent function is highly nonlinear and its applications.

1.2 Linear Algebra

It is very important for the study of bent functions to determine if a function is linear or far away from linear. This section contains basic knowledge about linear algebra for later use.

First, let us define some symbols.

Let p be a prime. Let $\mathbb{F}_{p^n}$ be the finite field of order p^n, for positive integer n. Let $\mathbb{F}_p^n$ be the n-dimensional vector space over the field $\mathbb{F}_p$. Let the exponents be the elements in $\mathbb{F}_p$, where $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$.

Definition 1.2.1. *Let S be a set. We use $\#S$ to denote the cardinality of S.*

For n a positive integer, let ζ_n be a primitive nth root of unity, $\zeta_n = e^{2\pi i/n}$.

Definition 1.2.2. *Let V be a vector space with dimension n over a field K. An* inner product *on V is a mapping from $V \times V$ to K which assigns to each ordered pair of vectors (a, b) a scalar $(a|b)$ in K such that for all $a, b, c \in V$*

(1) $(a+b|c) = (a|c) + (b|c)$,

(2) $(a|b) = (b|a)$,

(3) $(ka|b) = k(a|b)$ for $k \in K$,

(4) if $(a|x) = 0$ for all $x \in V$, then a is the zero vector of V.

A well known example of an inner product on $\mathbb{F}_p^n$ is the *dot product* $(a|b) = a \cdot b = \sum_{i=1}^n a_i b_i$ where $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$. We will see another example of an inner product shortly. Let us first observe some general properties of an inner product.

Theorem 1.2.3. *Let v be a nonzero vector in $\mathbb{F}_p^n$. Then $\#\{\alpha \in \mathbb{F}_p^n : (\alpha|v) = j\} = p^{n-1}$, for all $j \in \mathbb{F}_p$.*

Proof. Let $D = \{\alpha \in \mathbb{F}_p^n : (\alpha|v) = 0\}$. By Definition 1.2.2, D is a subspace of $\mathbb{F}_p^n$. By the fact that if $(\alpha|v) = 0$ for all $\alpha \in \mathbb{F}_p^n$ then $v = 0$, we have $D \neq \mathbb{F}_p^n$. So $\#D \leq p^{n-1}$. The cosets of D each have the form $D + \beta = \{\alpha + \beta : \alpha \in D\}$. Then $(\gamma|v) = (\beta|v)$ for all $\gamma \in D + \beta$. For β_1 and β_2 not in the same coset, $(\beta_1|v) \neq (\beta_2|v)$, because otherwise $(\beta_1 - \beta_2|v) = 0$ implies $\beta_1 - \beta_2 \in D$ and $\beta_1 = \beta_1 - \beta_2 + \beta_2 \in D + \beta_2$, which is a contradiction. There are p choices for the value $(\beta|v)$ where $\beta \in \mathbb{F}_p^n$. So $\#D = p^{n-1}$ and the cardinality of each coset of D is p^{n-1}. Hence $\#\{\alpha \in \mathbb{F}_p^n : (\alpha|v) = j\} = p^{n-1}$, for all $j \in \mathbb{F}_p$. □

The following theorem is an application of Theorem 1.2.3.

Theorem 1.2.4. *Let $V = \mathbb{F}_p^n$, a vector space. Then $\sum_{c \in V} \zeta_p^{(c|b)} = 0$ for b nonzero.*

Proof. By Theorem 1.2.3, $\sum_{c \in V} \zeta_p^{(c|b)}$ is a multiple of $1 + \zeta_p + \cdots + \zeta_p^{p-1}$. We have the property that $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$. So the result follows. □

We reserve the following definition and theorem for later use.

Definition 1.2.5. *Let W_1 and W_2 be finite-dimensional subspaces of a vector space V. We define $W_1 + W_2 = \{g_1 + g_2 : g_1 \in W_1, g_2 \in W_2\}$.*

Note: For W_1 and W_2 being finite-dimensional subspaces of a vector space V, $W_1 \cap W_2$ and $W_1 + W_2$ are subspaces of V.

Theorem 1.2.6. *(Theorem 6, Chapter 2 in [11]) If W_1 and W_2 are finite-dimensional subspaces of a vector space V, then*

$$\dim W_1 + \dim W_2 = \dim(W_1 \cap W_2) + \dim(W_1 + W_2).$$

Definition 1.2.7. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$. If $f(x+y) = f(x) + f(y)$ and $f(cx) = cf(x)$ for all $x, y \in \mathbb{F}_p^n$ and all $c \in \mathbb{F}_p$, then f is called* linear.

Next, we will find all the linear functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$.

Lemma 1.2.8. *Let $(a|b)$ be an inner product. Define $f_a : \mathbb{F}_p^n \to \mathbb{F}_p$ as $f(x) = (a|x)$ for some $a \in \mathbb{F}_p^n$. Then $\{f_a : a \in \mathbb{F}_p^n\}$ is exactly the set of linear functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ and has cardinality p^n.*

Proof. Suppose f is linear. Let B be a basis of $\mathbb{F}_p^n$. By Definition 1.2.7, f is defined by B. If for each $b \in B$, we assign an element in $\mathbb{F}_p$ to $f(b)$, then f is uniquely defined. We have p different elements in $\mathbb{F}_p$ and n distinct elements in B. So there are p^n distinct linear functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. Let D be the set of functions of the form f_a where $a \in \mathbb{F}_p^n$. Thus $\#D \leq p^n$ and by Definition 1.2.2, each function in D is linear. Assume there exist $a \in \mathbb{F}_p^n$ and $b \in \mathbb{F}_p^n$ such that $(a|x) = (b|x)$ for all $x \in \mathbb{F}_p^n$. We have $(a-b|x) = 0$ for all $x \in \mathbb{F}_p^n$. Thus $a = b$ by Definition 1.2.2. So $\#D = p^n$. Hence the result follows. □

1.3 Finite Fields

In this section, we will list some basic facts about finite fields.

Let us first define some notations.

Let $\mathbb{F}_{p^n}^*$ denote $\mathbb{F}_{p^n} \setminus \{0\}$. We will use the notation $(\mathbb{F}_{p^n}, +)$ to denote the *additive group* of the field $\mathbb{F}_{p^n}$ and $(\mathbb{F}_{p^n}^*, \cdot)$ to denote the *multiplicative group* of the field $\mathbb{F}_{p^n}$.

The following theorem is well-known and the proof can be found in many books.

Theorem 1.3.1. *Let p be a prime and n be a positive integer. Let a be in some finite field. Then $a^{p^n} = a$ if and only if $a \in \mathbb{F}_{p^n}$.*

Note: The finite field of p^n elements is unique.

Proof. Assume $a \in \mathbb{F}_{p^n}$. If $a = 0$, then $a^{p^n} = a$. If $a \neq 0$, then $a \in (\mathbb{F}_{p^n}^*, \cdot)$ and the order of a divides $p^n - 1$. Hence $a^{p^n} = a$.

Conversely, assume $a^{p^n} = a$. The polynomial $x^{p^n} - x$ has p^n roots. There are p^n distinct elements b in $\mathbb{F}_{p^n}$ such that $b^{p^n} = b$ and $x^{p^n} - x$ has p^n roots, so all the roots are in $\mathbb{F}_{p^n}$. Therefore, if $a^{p^n} = a$, then $a \in \mathbb{F}_{p^n}$. □

The following theorem shows that theorems proved over $\mathbb{F}_p^n$ can be used for proving theorems over $(\mathbb{F}_{p^n}, +)$.

Theorem 1.3.2. *We can view $(\mathbb{F}_{p^n}, +)$ as the vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$.*

Proof. We represent each element in $(\mathbb{F}_{p^n}, +)$ as a polynomial of the form $f(x) = a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in \mathbb{F}_p$ for all $i = 0, \ldots, n-1$. Then $(\mathbb{F}_{p^n}, +)$ is closed under addition and multiplication by scalars in $\mathbb{F}_p$. The proofs of $(\mathbb{F}_{p^n}, +)$ satisfying other axioms of a vector space are trivial. Hence we can view $(\mathbb{F}_{p^n}, +)$ as the vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$ with a basis $\{1, x, x^2, \ldots, x^{n-1}\}$. □

Definition 1.3.3. *[16] Let k and n be positive integers such that $k|n$. We define the* trace function *$T_k^n : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ as*

$$T_k^n(\beta) = \sum_{l=0}^{n/k-1} \beta^{p^{kl}}.$$

Proposition 1.3.4. *(Theorem 2.26 in [16]) Let m and b be positive integers. The trace functions over $\mathbb{F}_{p^{bm}}$ satisfy $T_1^{bm}(x) = T_1^m(T_m^{bm}(x))$.*

Theorem 1.3.5. *(Theorem 2.23 in [16]) Let $K = \mathbb{F}_p$ and $F = \mathbb{F}_{p^n}$. Then the trace function T_1^n satisfies the following properties:*

(i) $T_1^n(\alpha+\beta) = T_1^n(\alpha) + T_1^n(\beta)$ for all α, $\beta \in F$;

(ii) $T_1^n(c\alpha) = cT_1^n(\alpha)$ for all $c \in K$, $\alpha \in F$;

(iii) $T_1^n(a) = na$ for all $a \in K$;

(iv) $T_1^n(\alpha^p) = T_1^n(\alpha)$ for all $\alpha \in F$.

Proof. (i) We use the fact that $(\alpha+\beta)^{p^j} = \alpha^{p^j} + \beta^{p^j}$ for all integers $j \geq 0$ to get

$$\begin{aligned} T_1^n(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^p + \cdots + (\alpha+\beta)^{p^{n-1}} \\ &= \alpha+\beta+\alpha^p+\beta^p+\cdots+\alpha^{p^{n-1}}+\beta^{p^{n-1}} \\ &= T_1^n(\alpha)+T_1^n(\beta). \end{aligned}$$

(ii) We use the fact $c^{p^j} = c$ for $c \in K$ and all integers $j \geq 0$ to get

$$\begin{aligned} T_1^n(c\alpha) &= c\alpha + (c\alpha)^p + \cdots + (c\alpha)^{p^{n-1}} \\ &= c\alpha + c\alpha^p + \cdots + c\alpha^{p^{n-1}} \\ &= cT_1^n(\alpha). \end{aligned}$$

(iii)We use the fact $a^{p^j} = a$ for $a \in K$ and all integers $j \geq 0$ to get

$$\begin{aligned} T_1^n(a) &= a + a^p + \cdots + a^{p^{n-1}} \\ &= a + a + \cdots + a \\ &= na. \end{aligned}$$

(iv) We use the fact $\alpha^{p^n} = \alpha$ to get

$$\begin{aligned} T_1^n(\alpha^p) &= \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^n} \\ &= \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} + \alpha \\ &= T_1^n(\alpha). \end{aligned}$$

□

Theorem 1.3.6. *For $\alpha \in \mathbb{F}_{p^n}$, $T_1^n(\alpha) = 0$ if and only if there exists some $\beta \in \mathbb{F}_{p^n}$ such that $\alpha = \beta^p - \beta$. Furthermore, $\#\{\alpha \in \mathbb{F}_{p^n} : T_1^n(\alpha) = j\} = p^{n-1}$, for all j in $\mathbb{F}_p$.*

Proof. By Theorem 1.3.5, if $\alpha = \beta^p - \beta$ then $T_1^n(\alpha) = 0$. Conversely, given $T_1^n(\alpha) = 0$, we let β be a root of $x^p - x - \alpha$. Then $\beta^p - \beta = \alpha$. The thing left to be proved is that $\beta \in \mathbb{F}_{p^n}$.

$$\begin{aligned} 0 = T_1^n(\alpha) &= \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}} \\ &= \beta^p - \beta + \beta^{p^2} - \beta^p + \cdots + \beta^{p^n} - \beta^{p^{n-1}} \\ &= \beta^{p^n} - \beta. \end{aligned}$$

By Theorem 1.3.1, we have $\beta \in \mathbb{F}_{p^n}$.

Given $\alpha \in \mathbb{F}_{p^n}$. $T_1^n(\alpha) = 0$ if and only if $\alpha = \beta^p - \beta$ for some $\beta \in \mathbb{F}_{p^n}$. Claim: $\alpha = \beta^p - \beta$ for some $\beta \in \mathbb{F}_{p^n}$ if and only if $\alpha = \beta^p - \beta$ for exactly p distinct $\beta \in \mathbb{F}_{p^n}$. ($\Leftarrow$) is trivial. ($\Rightarrow$) Assume $\alpha = \beta^p - \beta$ for some $\beta \in \mathbb{F}_{p^n}$. Then for each $k \in \mathbb{F}_p$, $(\beta + k)^p - (\beta + k) = \beta^p + k^p - \beta - k = \beta^p + k - \beta - k = \beta^p - \beta$. And $\beta + k_1 \neq \beta + k_2$ for $k_1 \neq k_2$. Thus there at least p distinct β such that $\alpha = \beta^p - \beta$. Also $x^p - x - \alpha = 0$ has at most p solutions. So we proved the claim. Hence $\#\{\alpha \in \mathbb{F}_{p^n} : T_1^n(\alpha) = 0\} = p^{n-1}$, for all $j \in \mathbb{F}_p$. □

The following proposition shows that it is possible to define an inner product using a trace function.

Proposition 1.3.7. *For a, $b \in \mathbb{F}_{p^n}$, the mapping $(a,b) \mapsto T_1^n(ab)$ is an inner product on $(\mathbb{F}_{p^n}, +)$.*

Proof. Remember that $(\mathbb{F}_{p^n}, +)$ can be viewed as the vector space $\mathbb{F}_p^n$. By Theorem 1.3.5 and field axioms, the first three conditions for an inner product are satisfied. For the last condition, assume $T_1^n(ax) = 0$ for all $x \in \mathbb{F}_{p^n}$. Suppose $a \neq 0$. The map $x \mapsto ax$ is a bijection. By Theorem 1.3.6, $T_1^n(ax)$ is not always equal to 0, which is a contradiction. So $a = 0$. □

1.4 Dickson Polynomials

The main reference on Dickson polynomials is the book [15]. Let R be a commutative ring with identity. A *Dickson polynomial* is defined by

$$D'_r(x,a) = \sum_{i=0}^{\lfloor r/2 \rfloor} \frac{r}{r-i} \binom{r-i}{i} (-a)^i x^{r-2i}, \tag{1.1}$$

where r is a positive integer and $a \in R$ and $\lfloor r/2 \rfloor$ means the largest integer that is less than or equal to $r/2$.

Note: For $i \in \{0, \dots, \lfloor r/2 \rfloor\}$,

$$\frac{r}{r-i}\binom{r-i}{i} \tag{1.2}$$

is an integer, because Dickson polynomials can be defined recursively as follows: For $n \geq 0$

$$D'_{r+2}(x,a) = xD'_{r+1}(x,a) - aD'_r(x,a),$$

with initial values $D'_0(x,a) = 2$ and $D'_1(x,a) = x$. By induction on r, we get that (1.2) is an integer.

From the book [15], the following properties are needed for later use. We let $D_r(x) = D'_r(x,1)$.

Proposition 1.4.1. *(Equation (2.1) [15]) For Dickson polynomials $D_r \in \mathbb{F}_p[x]$, $D_r(x + x^{-1}) = x^r + x^{-r}$, for any positive integer r, i.e., $R = \mathbb{F}_p$.*

Proof. Follows from formula in Theorem 1.1 in [15]. □

Definition 1.4.2. *Let n be an integer. If f is a polynomial with coefficient in $\mathbb{F}_{p^n}$, f is called* a permutation polynomial *of $\mathbb{F}_{p^n}$ if the associated function $f : c \mapsto f(c)$ from $\mathbb{F}_{p^n}$ into itself permutes the elements of $\mathbb{F}_{p^n}$.*

Proposition 1.4.3. *(Theorem 3.2 [15]) Let m be a positive integer. The Dickson polynomial $D_r(x)$ is a permutation polynomial of $\mathbb{F}_{p^m}$ if and only if* $\gcd(r, p^{2m} - 1) = 1$.

1.5 Characters

In this section, we define characters and prove some theorems about characters. We also introduce the Kloosterman sums.

Let G be a finite abelian group. A *character* of G is a homomorphism from G into the group of complex numbers of absolute value 1. A *trivial character* of G is the character of G denoted by χ_0 and defined by $\chi_0(g) = 1$ for all $g \in G$. A *nontrivial character* is a character that is not trivial. An *additive character* of $\mathbb{F}_{p^n}$ is a character of $(\mathbb{F}_{p^n}, +)$.

Recall that $\zeta_s = e^{2\pi i/s}$.

Theorem 1.5.1. *(Theorem 5.7 [16]) For any character χ of $(\mathbb{F}_{p^n},+)$, there exists some $c \in \mathbb{F}_{p^n}$ such that $\chi(u) = \chi_c(u) = \zeta_p^{T_1^n(cu)}$, for all $u \in \mathbb{F}_{p^n}$. When $c = 1$ we call the character the* canonical additive character *of $\mathbb{F}_{p^n}$.*

Let G be a finite abelian group. Let $G^{\curlywedge}$ be the group of characters of G where the group operation in $G^{\curlywedge}$ is multiplication and χ_0 is the identity element of $G^{\curlywedge}$. Then we have:

Theorem 1.5.2. *[16] Let G be a finite abelian group. The group $G^{\curlywedge}$ is isomorphic to G.*

The following theorems are used for proving Theorem 1.5.5.

Theorem 1.5.3. *[16] Let G be a finite abelian group. If χ is a nontrivial character of G, then*

$$\sum_{g \in G} \chi(g) = 0. \tag{1.3}$$

Proof. Since χ is nontrivial, there exists $h \in G$ with $\chi(h) \neq 1$. Then

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

because as g runs through G, so does hg. Thus we have $(\chi(h) - 1) \sum_{g \in G} \chi(g)$ =0, which implies equation (1.3). □

Theorem 1.5.4. *(Corollary 5.3 [16]) For any two distinct elements g_1, $g_2 \in G$ there exists a character χ of G with $\chi(g_1) \neq \chi(g_2)$.*

Theorem 1.5.5. *If $g \in G$ with $g \neq 1_G$, the identity element in G, then*

$$\sum_{\chi \in G^{\curlywedge}} \chi(g) = 0. \tag{1.4}$$

Proof. If $g \neq 1_G$ then by Theorem 1.5.4 there exists χ such that $\chi(g) \neq \chi(1_G) = 1$. Define $\widehat{g}(\phi) = \phi(g)$ for $\phi \in G^{\curlywedge}$. Then $\widehat{g}$ is a nontrivial character of $G^{\curlywedge}$. By Theorem 1.5.3, we get Equation (1.4). □

We have been equipped with all the necessary knowledge about characters. Now we can define the Kloosterman sum.

Some definitions found in the literature are:

(1) The *Kloosterman sum* is the sum

$$K'_{p^m}(\chi;a,b)=\sum_{x\in\mathbb{F}^*_{p^m}}\chi(ax^{-1}+bx),$$

for $a,b\in\mathbb{F}_{p^m}$ such that $a\neq 0$ and for χ a nontrivial additive character of $\mathbb{F}_{p^m}$.

(2) The *Kloosterman sum* is the sum

$$K''_{p^m}(d)=\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{T_1^m(x^{-1}+dx)}, \tag{1.5}$$

for $d\in\mathbb{F}_{p^m}$.

Proposition 1.5.6. *We have for $a,b\in\mathbb{F}_{p^m}$ such that $a\neq 0$ and for χ a nontrivial additive character of $\mathbb{F}_{p^m}$, there exists $d\in\mathbb{F}_{p^m}$ such that $K'_{p^m}(\chi;a,b)=K''_{p^m}(d)$.*

Proof. Any nontrivial additive character of $\mathbb{F}_{p^m}$ can be written as $\chi_c(x)=\zeta_p^{T_1^m(cx)}$, where $c\neq 0$ by Theorem 1.5.1. Assume $a\neq 0$, thus

$$\begin{aligned}K'_{p^m}(\chi;a,b)&=\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{T_1^m(acx^{-1}+cbx)}\\&=\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{T_1^m((a^{-1}c^{-1}x)^{-1}+cbx)}\\&=\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{T_1^m(x^{-1}+cbacx)}\\&=\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{T_1^m(x^{-1}+c^2abx)}.\end{aligned} \tag{1.6}$$

Equation (1.6) holds by the bijection $x\mapsto a^{-1}c^{-1}x$. Let $d=c^2ab$. Hence $K'_{p^m}(\chi;a,b)=K''_{p^m}(d)$. □

In this thesis we use the following definition of Kloosterman sum, which appears to be the most common definition at the present time.

Definition 1.5.7. *The* Kloosterman sum *is the mapping $K_{p^m}:\mathbb{F}_{p^m}\to\mathbb{R}$ defined by*

$$K_{p^m}(d)=\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{T_1^m(x^{-1}+dx)}. \tag{1.7}$$

In (1.7) we let $0^{-1} = 0$. Note that $K_{p^m}(d) = K''_{p^m}(d) + 1$. To see that K_{p^m} maps to $\mathbb{R}$, regroup the summation by pairs $\{x, -x\}$, recall that $T_1^m(-u) = -T_1^m(u)$ and note that $\zeta_p^k + \zeta_p^{-k} \in \mathbb{R}$ for $k \in \mathbb{F}_p$. For $p = 2, 3$, $K_{p^m}(d)$ is an integer for each d but this is not the case in general for $p > 3$.

1.6 Group Algebras

Group algebra is a key ingredient to prove theorems in Chapter 2. In this section, we will introduce some theorems that are based on well-known group algebra.

Let $\mathbb{C}$ denote the field of complex numbers. Let $\bar{z}$ be the *complex conjugate* of $z \in \mathbb{C}$.

Throughout Section 1.6 we work exclusively with finite abelian groups.

Definition 1.6.1. *Let G be a finite abelian group written multiplicatively. The* group algebra $\mathbb{C}[G]$ *of G over the field of complex numbers $\mathbb{C}$ is the set of elements of the form:*

$$A = \sum_{g \in G} a_g g,\ a_g \in \mathbb{C},$$

with addition being defined component-wise; i.e.

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

and multiplication being defined as:

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g,h \in G} a_g b_h gh.$$

Definition 1.6.2. *For any $A = \sum_{g \in G} a_g g$ denote $A^{(-1)} = \sum_{g \in G} a_g g^{-1}$, which is clearly in $\mathbb{C}[G]$.*

Definition 1.6.3. *Let $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$ and $B = \sum_{h \in G} b_h h \in \mathbb{C}[G]$. Let χ be a character of G. We define $\chi(A) = \sum_{g \in G} a_g \chi(g)$.*

Proposition 1.6.4. *Let $A, B \in \mathbb{C}[G]$. Let χ be a character of G. Then $\chi(AB) = \chi(A)\chi(B)$.*

Proof. Let $A = \sum_{g \in G} a_g g$ and $B = \sum_{h \in G} b_h h$, where $a_g, b_h \in \mathbb{C}$. By the property that a character is a homomorphism, we have that

$$\begin{aligned}
\chi(AB) &= \chi(\sum_{g,h \in G} a_g b_h gh) \\
&= \sum_{g,h \in G} a_g b_h \chi(gh) \\
&= \sum_{g,h \in G} a_g b_h \chi(g)\chi(h) = \chi(A)\chi(B).
\end{aligned}$$

□

Theorem 1.6.5. *Let $A = \sum_{g \in G} a_g g$ and $B = \sum_{g \in G} b_g g$ be group algebra elements of $\mathbb{C}[G]$. If $\chi(A) = \chi(B)$ for all characters χ of G, then $A = B$.*

Proof. For each $h \in G$, we have

$$\begin{align}
1/|G| \sum_{\chi \in G^{\curlywedge}} \chi(A)\chi(h^{-1}) &= 1/|G| \sum_{\chi \in G^{\curlywedge}} \sum_{g \in G} a_g \chi(g)\chi(h^{-1}) \tag{1.8} \\
&= 1/|G| \sum_{g \in G} a_g \sum_{\chi \in G^{\curlywedge}} \chi(gh^{-1}) \tag{1.9} \\
&= a_h. \tag{1.10}
\end{align}$$

Equation (1.10) holds because $\sum_{\chi \in G^{\curlywedge}} \chi(gh^{-1}) = 0$ except for $g = h$, when it is $|G|$. Hence $\chi(A) = \chi(B)$ for all characters χ of G implies $a_h = b_h$, for all $h \in G$. So $A = B$. □

Remark: By a slight abuse of notation we identify a subset of G with the corresponding element of $\mathbb{C}[G]$ that is, for $D \subset G$ we also denote $D = \sum_{g \in D} g$ as an element of $\mathbb{C}[G]$. Note: on the left hand side D is a group algebra element in $\mathbb{C}[G]$ and on the right hand side, D is a set.

Theorem 1.6.6. *Assume G is an abelian group of order v. Let D be a group algebra element of $\mathbb{C}[G]$. Suppose that there is an $n \in \mathbb{C}$ such that $\chi(D) = n$ for all nontrivial characters of G. Then*

$$D = n + \frac{\chi_0(D) - n}{v} G.$$

Proof. Recall χ_0 is the trivial character. Define λ to satisfy $\chi_0(D) = n + \lambda v$ and then set $E = n + \lambda G$. We can do that because we can always find a $\lambda \in \mathbb{C}$ such that $n + \lambda v = \chi_0(D)$. We have $\chi(E) = n = \chi(D)$ for any nontrivial character χ, and $\chi_0(E) = \chi_0(D)$. So by Theorem 1.6.5, $D = E = n + \lambda G$, where $\lambda = \frac{\chi_0(D) - n}{v}$. □

Definition 1.6.7. *Let $D = \sum_{g \in G} d_g g$, where $d_g \in \mathbb{C}$, be an element of $\mathbb{C}[G]$. We define $[D]$ as a matrix: $[D](g,h) = d_{gh^{-1}}$.*

Remark: Here we did not use the standard indices for entries of a matrix. Instead, we let g and h (the elements in G) be the indices.

The following are some properties of matrices defined in Definition 1.6.7.

Theorem 1.6.8. *Let A and B be elements of $\mathbb{C}[G]$. Then:*
(i) $[AB] = [A][B]$, (ii) $[A+B] = [A] + [B]$, and (iii) $[A][B] = [B][A]$.

Proof. Let $A = \sum_{g \in G} a_g g$ and $B = \sum_{g \in G} b_g g$. We have

$$AB = \sum_{g \in G} \sum_{h \in G} a_g b_h gh.$$

Then $[AB](g,h) = \sum_{ij^{-1} = gh^{-1}} a_i b_{j^{-1}} = \sum_{r \in G} a_{gr^{-1}} b_{rh^{-1}} = [A][B](g,h)$. So $[AB] = [A][B]$.

Part (ii) follows from $[A+B](g,h) = a_{gh^{-1}} + b_{gh^{-1}} = [A](g,h) + [B](g,h)$.

Part (iii) follows from $[AB] = [BA]$ (since the group is abelian) and part (i). □

Theorem 1.6.9. *Let $D = \sum_{g \in G} d_g g$ be an element of $\mathbb{C}[G]$. Then $[D^{(-1)}] = [D]^T$.*

Proof. We have $[D^{(-1)}](g,h) = d_{(gh^{-1})^{-1}} = d_{hg^{-1}} = [D](h,g) = [D]^T(g,h)$. □

1.7 Nonlinear Functions

In this section, we will define bent functions as the most nonlinear functions.

1.7.1 General Characteristic

In 1976, Rothaus introduced the definition of binary bent functions in [20]. In 1985, Kumar, Scholtz and Welch generalized the definition of bent functions to p-ary in [14]. Recall $\zeta_p = e^{2\pi i/p}$. Then we give the following definitions:

Definition 1.7.1. *For any function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and a fixed inner product $(x|y)$ on $\mathbb{F}_p^n$ we define the* Walsh transform *of f to be the mapping $\widehat{f} : \mathbb{F}_p^n \to \mathbb{C}$ such that*

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)-(a|x)}$$

and we call $\widehat{f}(a)$ a Walsh coefficient.

Definition 1.7.2. *The* Walsh spectrum *of a function f is defined as the multiset $\{\widehat{f}(a) : a \in \mathbb{F}_p^n\}$.*

Definition 1.7.3. *For any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, we state its* extended Walsh transform

$$\widehat{f}(a,k) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)-T_1^n(ax^k)},$$

where $a \in \mathbb{F}_{p^n}$ and $\gcd(k, p^n - 1) = 1$.

By the triangle inequality, $|\widehat{f}(b)| \leq p^n$ for all $b \in \mathbb{F}_p^n$. By Corollary 1.2.8, if f is linear, then $f(x) = (a|x)$ for some a and hence $\widehat{f}(a) = p^n$. So it is natural to think the most nonlinear function should satisfy the condition that $|\widehat{f}(a)|$ is small for all $a \in \mathbb{F}_p^n$.

Throughout the rest of the thesis, we will denote *any* inner product by $x \cdot y$. This is not necessarily the dot product. We use this simplified notation in order to simplify the formulas.

We have Parseval's Identity as follows:

Theorem 1.7.4. *For all $f : \mathbb{F}_p^n \to \mathbb{F}_p$, we have $\sum_{a \in \mathbb{F}_p^n} |\widehat{f}(a)|^2 = p^{2n}$.*

Proof. We have

$$\begin{aligned}
\sum_{a \in \mathbb{F}_p^n} |\widehat{f}(a)|^2 &= \sum_{a \in \mathbb{F}_p^n} |\sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)-a\cdot x}|^2 \\
&= \sum_{a \in \mathbb{F}_p^n} \left(\sum_{x,y \in \mathbb{F}_p^n} \zeta_p^{f(x)-a\cdot x} \overline{\zeta_p^{f(y)-a\cdot y}} \right) \\
&= \sum_{a \in \mathbb{F}_p^n} \left(\sum_{x,y \in \mathbb{F}_p^n} \zeta_p^{f(x)-f(y)-a\cdot x+a\cdot y} \right)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{x,y\in\mathbb{F}_p^n} \zeta_p^{f(x)-f(y)} \left(\sum_{a\in\mathbb{F}_p^n} \zeta_p^{-a\cdot x+a\cdot y}\right) \\
&= \sum_{x\neq y\in\mathbb{F}_p^n} \zeta_p^{f(x)-f(y)} \left(\sum_{a\in\mathbb{F}_p^n} \zeta_p^{-a\cdot x+a\cdot y}\right) + \sum_{x=y\in\mathbb{F}_p^n} \zeta_p^{f(x)-f(y)} \left(\sum_{a\in\mathbb{F}_p^n} \zeta_p^{-a\cdot x+a\cdot y}\right) \\
&= 0+p^{2n}.
\end{aligned}$$

The above proof uses Theorem 1.2.4. □

If $|\widehat{f}(a)|^2 = p^n$ for all a, then we minimize over f the maximum value over a of $|\widehat{f}(a)|$ to be $p^{n/2}$, which makes f the most nonlinear. Let us prove this.

Assume that $\max|\widehat{f}(a)| < p^{n/2}$, i.e. for all a, we have $|\widehat{f}(a)| < p^{n/2}$. So $\sum_{a\in\mathbb{F}_p^n} |\widehat{f}(a)|^2 < p^{2n}$. This contradicts Parseval's identity.

Then the most nonlinear functions are defined as follows:

Definition 1.7.5. *[14] If $|\widehat{f}(a)| = p^{n/2}$ for each $a \in \mathbb{F}_p^n$, then f is called* bent.

Rothaus [20] defined bent functions for $p = 2$ in 1976. Note that n must be even if $p = 2$, since $\widehat{f}(a)$ is then an integer for all a. In 1985, Kumar, Scholtz and Welch [14] generalized bent functions to the case of arbitrary p. For $p > 2$, bent functions exist also for odd n, as illustrated by the following example.

Example 1.7.6. Let $f : \mathbb{F}_3 \to \mathbb{F}_3$ be defined as $f(1) = 0$, $f(2) = 0$ and $f(0) = 1$ and the inner product is the dot product. We have $|\widehat{f}(1)| = |\zeta_3^2 + \zeta_3 + \zeta_3| = \sqrt{3}$, $|\widehat{f}(2)| = |\zeta_3 + \zeta_3^2 + \zeta_3| = \sqrt{3}$ and $|\widehat{f}(0)| = |1+1+\zeta_3| = \sqrt{3}$. So f is bent.

Lemma 1.7.7. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$, $c \in \mathbb{F}_p$ and let $f' : \mathbb{F}_p^n \to \mathbb{F}_p$ be defined by $f'(x) = f(x)+c$ for each x. Then f is bent if and only if f' is bent.*

Proof. For all $a \in \mathbb{F}_p^n$,

$$|\widehat{f'}(a)| = |\sum_{x\in\mathbb{F}_p^m} \zeta_p^{f'(x)-a\cdot x}| = |\sum_{x\in\mathbb{F}_p^m} \zeta_p^{f(x)+c-a\cdot x}| = |\zeta_p^c \widehat{f}(a)| = |\widehat{f}(a)|.$$

Apply Definition 1.7.5. The result follows. □

It follows from Lemma 1.7.7 that without loss of generality one could restrict attention to bent functions that satisfy $f(0) = 0$. This is the case throughout Chapter 3.

In 2001, A. M. Youssef and G. Gong defined the hyperbent functions as follows.

Definition 1.7.8. *[23] A function f is* hyperbent *if the square of the absolute value of its extended Walsh transform only takes the value p^n.*

In cryptography, an S-Box (Substitution-box) is a basic component of symmetric key algorithms which performs substitution. In 1999, G. Gong and S. W. Golomb in [8] proposed that S-box should not be approximated by bijective monomials (i.e. functions in the form $Tr(\lambda x^c) + e$, $\gcd(c, p^n - 1) = 1$). A bent function achieves the maximal minimum distance to all affine functions (i.e., functions in the form $Tr(\lambda x) + e$). However, this does not guarantee that a bent function cannot be approximated by bijective monomials. Hyperbent functions make up for the shortcoming of bent functions in this sense.

The potential applications for p-ary bent functions ($p > 2$) are in cryptographic components of non-binary information technologies. In most information storage and transmission technologies, more than two levels of signals are possible. We can represent these signal levels by $0, 1, 2, \ldots, p-1$. Another reason for studying bent functions with $p > 2$ is that we may gain a new perspective on the important binary case ($p = 2$).

1.8 Applications

Because of their highly nonlinear property, bent functions are widely used in cryptography and coding theory, for example in the construction of block ciphers. A block cipher is a symmetric key cipher which obtains its ciphertext as follows: $y_1 y_2 \ldots = e_K(x_1) e_K(x_2) \ldots$, where $x_i's$ are plaintext blocks of the same length, $y_i's$ are ciphertext blocks of the same length and e_K is the encryption function (depending on the secret key K) that is often implemented as a substitution-permutation network [21, Chapter 3]. We can use bent functions to construct the cipher to make the cipher more secure. For example, the CAST-128 block cipher is constructed using bent functions. This cipher is used by PGP and by the Canadian government, where Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits. The full 16 rounds are used when the key size is longer than 80 bits. Components include large 8×32-bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations.

A *stream cipher* generates a keystream $z = z_1 z_2 \cdots$ and uses it to encrypt a plaintext string $x = x_1 x_2 \cdots$ to get ciphertext $y = y_1 y_2 \cdots$ as follows. Encryption is given by

$$y_i = x_i + z_i \pmod 2 \tag{1.11}$$

and decryption is given by $x_i = y_i + z_i \pmod 2$. Here $x_i, y_i, z_i \in \mathbb{F}_2$ for each i and both parties that communicate using the stream cipher have to generate the same key stream $z_1 z_2 \cdots$. This key stream generation is typically done as pseudo-random bit generation starting from a shared secret which is used as the seed of a pseudo-random bit generator.

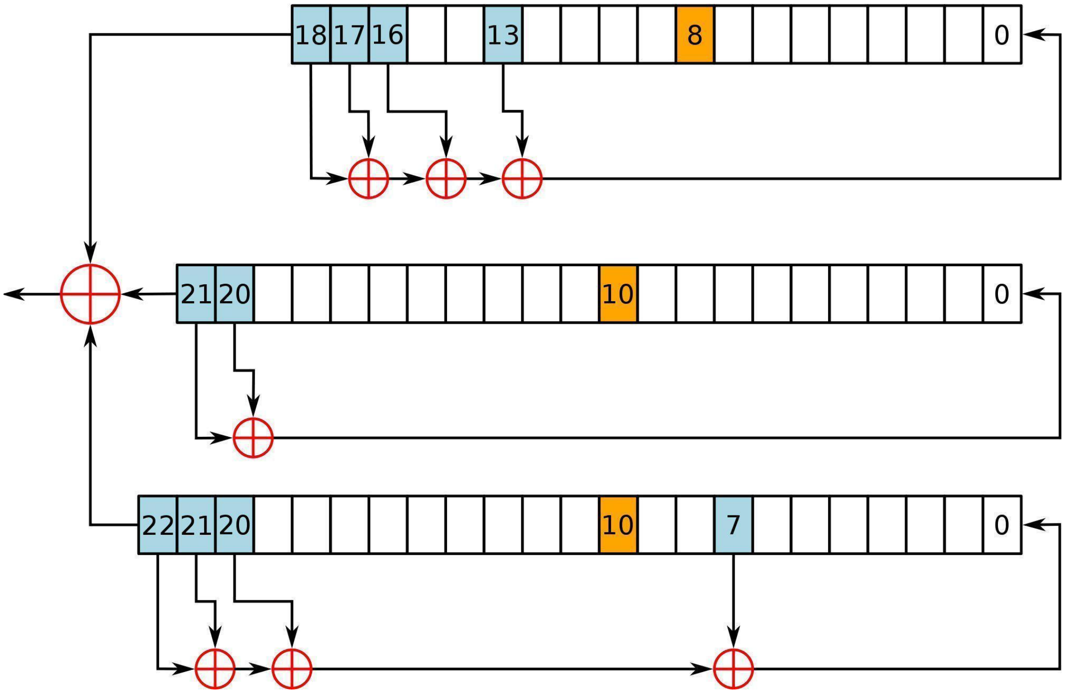
The A5/1 stream cipher is used in GSM mobile telephony standards. Figure 1.1 shows how it works: there are three linear feedback shift registers (LFSR) with 19 bits, 22 bits and 23 bits and their outputs are added together to produce a key stream bit.

Let a_i be the bits generated by the 19-bit LFSR, let b_i be the bits generated by the 22-bit LFSR and let c_i be the bits generated by the 23-bit LFSR for $i = 1, 2, \ldots$. We have $z_i = a_i + b_i + c_i$ for $i = 1, 2, \ldots$. Assume the attacker knows some plaintext bits and corresponding ciphertext bits. Then the corresponding keystream bits can be computed using Equation (1.11).

Let us give a very rough sketch of an attack against A5/1. The details are much more complicated.

Using the LFSR recurrence relation, for each $i > 19$ we can represent a_i as a *linear* combination of $a_1, \ldots, a_{19}$ and similarly for b_i and c_i. Suppose that the attacker knows $z_1, \ldots, z_{64}$. The attacker can solve the system of *linear equations* $z_i = a_i + b_i + c_i$ $(1 \leq i \leq 64)$ for the unknowns $a_1, \ldots, a_{19}, b_1, \ldots, b_{22}, c_1, \ldots, c_{23}$. We give a random numerical example for this in Appendix A.1. As soon as the attacker recovers the contents of the individual LFSRs, the keystream generator is fully compromised. If the attacker knows fewer than 64 consecutive bits z_i, then the linear system will have more than 1 solution and the attacker can try each solution to find the one that works.

The attack described above works only against a simplified version of A5/1. For the actual A5/1 stream cipher, the majority value of the three bits in the middle of the three LFSRs (shown in Figure 1.1) determines which LFSRs advance in the given time instant.



Source: Wikipedia

Figure 1.1: A5/1 key stream generator

However, a “practical” attack against the full version of A5/1 has been given by Chris Paget and Karsten Nohl at the 2009 Black Hat security conference [18].

It should be stressed that from our point of view, the main weakness explored in the attacks mentioned above is due to the use of the $\oplus$ gate in Figure 1.1 to combine the output of the three LFSRs. If a non-linear function was used in that place, the equations for the unknowns $a_1,\ldots,a_{19},b_1,\ldots,b_{22},c_1,\ldots,c_{23}$ would involve polynomials of much higher degree and the system of equations would be much harder to solve than a *linear* system (or impossible to solve due to its huge size). Thus the design of stream ciphers presents one application of bent functions.

Chapter 2

Bent Functions on Partial Spreads

Getting the inspiration from Dillon's thesis [4] for the binary case, we prove theorems on construction of bent functions over $\mathbb{F}_p^{2m}$ for general prime p with the help of partial spreads. Dillon's construction is the special case $p = 2$ of our construction.

2.1 Spreads of Subspaces

Let us start by some definitions. Let m and n be positive integers.

Definition 2.1.1. *An m-*spread *for $\mathbb{F}_p^n$ is a set of pairwise disjoint (except for 0) m- dimensional subspaces of $\mathbb{F}_p^n$ whose union equals $\mathbb{F}_p^n$.*

Definition 2.1.2. *A* partial m-spread *for $\mathbb{F}_p^n$ is a set of pairwise disjoint (except for 0) m-dimensional subspaces of $\mathbb{F}_p^n$.*

Note that a partial m-spread might not be a subset of an m-spread. Counterexamples can be found in [5], Section 1.3. Note also that the term "m-spread" indicates the dimension of the subspaces in the spread.

Theorem 2.1.3. *Let $m|n$. Let $\gamma \in \mathbb{F}_{p^n}$. Consider $(\mathbb{F}_{p^n}, +)$ as an n-dimensional vector space over $\mathbb{F}_p$. Then $\gamma\mathbb{F}_{p^m}$ is a subspace of $(\mathbb{F}_{p^n}, +)$.*

Proof. If $m|n$, then $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$. We have $\gamma\mathbb{F}_{p^m}$ a nonempty subset of $(\mathbb{F}_{p^n}, +)$ since the identity 0 of $(\mathbb{F}_{p^n}, +)$ is in $\gamma\mathbb{F}_{p^m}$. Let $a \in \gamma\mathbb{F}_{p^m}$ and $b \in \gamma\mathbb{F}_{p^m}$. Then $a = \gamma x$ and

$b = \gamma y$ for some $x, y \in \mathbb{F}_{p^m}$. Hence $a + b = \gamma x + \gamma y = \gamma(x + y) \in \gamma\mathbb{F}_{p^m}$. And let $c \in \mathbb{F}_p$. Then $ca = c\gamma x = \gamma(cx) \in \gamma\mathbb{F}_{p^m}$. So $\gamma\mathbb{F}_{p^m}$ is a subspace of $(\mathbb{F}_{p^n}, +)$. □

Theorem 2.1.4. *An m-spread of $\mathbb{F}_p^n$ exists if and only if m divides n.*

Proof. $(\Rightarrow)$ Assume there exists an m-spread of $\mathbb{F}_p^n$. Thus we have $p^m - 1 | p^n - 1$. Assume m does not divide n. Let $n = am + b$, where a is a non-negative integer and b is a positive integer such that $0 < b < m$. Then

$$\begin{aligned} p^n - 1 &\equiv 0 \pmod{p^m - 1} \\ p^{am+b} - 1 &\equiv 0 \pmod{p^m - 1} \\ 1^a \cdot p^b - 1 &\equiv 0 \pmod{p^m - 1}. \end{aligned}$$

But by the condition on b, $0 < p^b - 1 < p^m - 1$. This leads to a contradiction.

$(\Leftarrow)$ Construction: Let $A = \{\gamma\mathbb{F}_{p^m}^* | \gamma \in \mathbb{F}_{p^n}^*\}$ be the set of cosets of $(\mathbb{F}_{p^m}^*, \cdot)$ in $(\mathbb{F}_{p^n}^*, \cdot)$. So elements in A are pairwise disjoint and the union of elements in A is $\mathbb{F}_{p^n}^*$. From Theorem 2.1.3, $B = \{\gamma\mathbb{F}_{p^m}^* \cup \{0\} | \gamma \in \mathbb{F}_{p^n}^*\}$ is a set of subspaces of $(\mathbb{F}_{p^n}, +)$. So B is an m-spread. Since $(\mathbb{F}_{p^n}, +)$ can be viewed as $\mathbb{F}_p^n$, an m-spread of $\mathbb{F}_p^n$ exists. □

Example 2.1.5. Let $\mathbb{F}_{3^2} = \mathbb{F}_3[x]/(x^2 + 1)$. Then we can find that $\{\{0, 1, 2\}, \{0, x + 2, 2x + 1\}, \{0, x, 2x\}, \{0, 2x + 2, x + 1\}\}$ is a 1-spread of $\mathbb{F}_3^2$ with basis $\{1, x\}$.

Remark: In this thesis, we only deal with the spreads with $n = 2m$. But by Theorem 2.1.4, there is an m-spread on $\mathbb{F}_p^{bm}$ for any b a positive integer. These spreads are also widely used and have their significance. For example, Patterson and Wiedemann construction [19] is the case $n = 3m$, in particular, $m = 5$. They construct a nonlinear function on $\mathbb{F}_2^{15}$.

2.2 Matrix Form of the Walsh Transform

Let p be a prime and let n be a positive integer. Recall that $\zeta_p = e^{2\pi i/p}$.

Again we use the notation $x \cdot y$ for an arbitrary inner product on $\mathbb{F}_p^n$.

Definition 2.2.1. *The* conjugate transpose *of a matrix A with complex entries is the matrix A^* obtained from A by transposition of A and complex conjugation of each entry.*

Definition 2.2.2. *We define the $p^n \times p^n$ matrix M_n, whose row and column indices are the lexicographically ordered vectors of $\mathbb{F}_p^n$, by*

$$M_n(x,y) = \zeta_p^{-x\cdot y}$$

for any $x, y \in \mathbb{F}_p^n$.

Proposition 2.2.3. *Let M_n be as in Definition 2.2.2.*
(i) The inverse of M_n is given by

$$M_n^{-1}(x,y) = p^{-n}\zeta_p^{x\cdot y}$$

for any $x, y \in \mathbb{F}_p^n$.
(ii) We have $M_n = p^n(M_n^{-1})^*$ and $M_n^{-1} = p^{-n}M_n^*$.

Proof. (i) Let M be the matrix defined by $M(x,y) = p^{-n}\zeta_p^{x\cdot y}$. Then

$$\begin{aligned}(M_nM)(x,y) &= \sum_{r\in\mathbb{F}_p^n} M_n(x,r)M(r,y) = \sum_{r\in\mathbb{F}_p^n} \zeta_p^{-x\cdot r}p^{-n}\zeta_p^{r\cdot y} \\ &= \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise,}\end{cases}\end{aligned}$$

by Theorem 1.2.4. So $M = M_n^{-1}$.
(ii) follows from (i). □

Using the lexicographic ordering $w_1, \ldots, w_{p^n}$ of the vectors in $\mathbb{F}_p^n$, which is consistent with Definition 2.2.2, any function $f : \mathbb{F}_p^n \to \mathbb{C}$ is associated with the unique column vector

$$(f(w_1), \ldots, f(w_{p^n}))^T \in \mathbb{C}^{p^n},$$

and vice versa. With a slight abuse of notation we will use *the same symbol* for the function and the column vector corresponding to it.

Similarly as in Definition 2.2.2 we will keep using vectors in $\mathbb{F}_p^n$ as row and column indices of matrices (whenever it is clear from the context).

Definition 2.2.4. *Given $f : \mathbb{F}_p^n \to \mathbb{F}_p$, we define $\tilde{f} : \mathbb{F}_p^n \to \mathbb{C}$ by $\tilde{f}(x) = \zeta_p^{f(x)}$.*

Now we give the matrix form of the Walsh transform which was introduced in Definition 1.7.1:

Proposition 2.2.5. *Suppose M_n is defined using the same inner product that is used in the definition of the Walsh transform. For any $f : \mathbb{F}_p^n \to \mathbb{F}_p$ we have*

$$\hat{f} = M_n \tilde{f}.$$

Proof. Let $w \in \mathbb{F}_p^n$. We have

$$\hat{f}(w) = \sum_u \zeta_p^{f(u)-w\cdot u} = \sum_u \zeta_p^{-w\cdot u} \zeta_p^{f(u)} = (M_n \tilde{f})(w).$$

□

Definition 2.2.6. *With each function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ we associate the $p^n \times p^n$ matrix $[f]$ whose (u,v)-th entry is $\tilde{f}(u-v)$.*

Proposition 2.2.7. *Let f be a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. We have*

$$M_n[f]M_n^{-1} = \mathrm{diag}(\hat{f}(w_1), \hat{f}(w_2), \ldots, \hat{f}(w_{p^n})).$$

Proof. Let $l = s-t$. Then the (u,v)-th entry of $M_n[f]M_n^{-1}$ is

$$\begin{aligned}\sum_{s,t} M_n(u,s)\tilde{f}(s-t)M_n^{-1}(t,v) &= p^{-n}\sum_l \tilde{f}(l)\sum_t \zeta_p^{-u\cdot(l+t)}\zeta_p^{t\cdot v} \\ &= p^{-n}\sum_l \tilde{f}(l)\zeta_p^{-u\cdot l}\sum_t \zeta_p^{t\cdot(v-u)} \\ &= \begin{cases} p^{-n}\cdot \hat{f}(u)\cdot p^n & \text{if } u = v \\ p^{-n}\cdot \hat{f}(u)\cdot 0 & \text{otherwise,} \end{cases}\end{aligned}$$

using Theorem 1.2.4 and Proposition 2.2.5. □

Recall that for any two matrices A, B over $\mathbb{C}$ we have $(AB)^* = B^*A^*$ whenever the product AB is defined.

Proposition 2.2.8. *Let f be a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. We have*

$$M_n[f][f]^*M_n^{-1} = \mathrm{diag}(|\hat{f}(w_1)|^2, |\hat{f}(w_2)|^2, \ldots, |\hat{f}(w_{p^n})|^2).$$

Proof. Using Proposition 2.2.3 we compute

$$\begin{aligned} M_n[f][f]^*M_n^{-1} &= M_n[f]M_n^{-1}M_n[f]^*M_n^{-1} = M_n[f]M_n^{-1}p^n(M_n^{-1})^*[f]^*p^{-n}M_n^* \\ &= M_n[f]M_n^{-1}(M_n^{-1})^*[f]^*M_n^* = M_n[f]M_n^{-1}\left(M_n[f]M_n^{-1}\right)^*. \end{aligned}$$

Now using Proposition 2.2.7 we get

$$\begin{aligned} &M_n[f]M_n^{-1}\left(M_n[f]M_n^{-1}\right)^* \\ &= \mathrm{diag}(\hat{f}(w_1), \hat{f}(w_2), ..., \hat{f}(w_{p^n}))\mathrm{diag}\left(\overline{\hat{f}(w_1)}, \overline{\hat{f}(w_2)}, ..., \overline{\hat{f}(w_{p^{2m}})}\right) \\ &= \mathrm{diag}(|\hat{f}(w_1)|^2, |\hat{f}(w_2)|^2, ..., |\hat{f}(w_{p^n})|^2). \end{aligned}$$

□

Definition 2.2.9. *Let I_k denote the $k \times k$ identity matrix.*

Theorem 2.2.10. *A function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is bent if and only if $[f][f]^* = p^n I_{p^n}$.*

Proof. By Proposition 2.2.8, f is bent if and only if $M_n[f][f]^*M_n^{-1} = p^n I_{p^n}$ if and only if $[f][f]^* = M_n^{-1}p^n I_{p^n} M_n = p^n I_{p^n}$. □

2.3 The Construction

The following theorem is our first main result about bent functions. In Dillon's thesis [4], difference sets and partial spreads are used to construct bent functions in the binary case. In this section, we use partial spreads to generalize Dillon's result to the p-ary case. Then in the next section we mention the connection between bent functions and relative difference sets for $p > 2$.

Theorem 2.3.1. *Let m be a positive integer. Let $\{S_{ji} | i = 1, 2, ..., p^{m-1}$ and $j \in \mathbb{F}_p^*\}$ be a partial m-spread of $\mathbb{F}_p^{2m}$. For $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ and $j \in \mathbb{F}_p$ denote $D_j := f^{-1}(j)$. Assume that for each $j \in \mathbb{F}_p^*$*

$$D_j = \cup_{i=1}^{p^{m-1}} S_{ji}^*,$$

where $S_{ji}^* := S_{ji} \setminus \{0\}$. Then f is bent.

The following definitions and theorems before the proof of Theorem 2.3.1 all serve for the proof of Theorem 2.3.1.

Definition 2.3.2. *Let m be a positive integer. For any $S \subseteq \mathbb{F}_p^{2m}$, let $\widetilde{S}$ denote the group of characters of $(\mathbb{F}_p^{2m}, +)$ which agree with the trivial character χ_0 on S. That is, $\chi \in \widetilde{S}$ if and only if $\chi(t) = 1$ for each $t \in S$.*

Theorem 2.3.3. *Assume the notations as in Theorem 2.3.1. For $(j,i) \neq (u,v)$, we have $\widetilde{S_{ji}} \cap \widetilde{S_{uv}} = \{\chi_0\}$.*

Proof. Recall $S_{ji} \cap S_{uv} = \{0\}$. So $\dim(S_{ji} \cap S_{uv}) = 0$. By Theorem 1.2.6, $\dim(S_{ji} + S_{uv}) = m + m = 2m$. So $S_{ji} + S_{uv} = \mathbb{F}_p^{2m}$. If $\chi \in \widetilde{S_{ji}} \cap \widetilde{S_{uv}}$, then χ sends all elements in S_{ji} and S_{uv} to 1. Since χ is a homomorphism, $\chi(a+b) = \chi(a)\chi(b) = 1$ for $a \in S_{ji}$ and $b \in S_{uv}$. Thus χ sends all elements in $\mathbb{F}_p^{2m}$ to 1. Hence we have $\widetilde{S_{ji}} \cap \widetilde{S_{uv}} = \{\chi_0\}$. □

Recall for a finite abelian group G, $[D]$ is defined as $[D](g,h) = d_{g-h}$ in Definition 1.6.7.

Lemma 2.3.4. *Assume the notations and conditions as in Theorem 2.3.1. Then $[D_j] = [D_j]^T$ for each $j \in \mathbb{F}_p^*$.*

Proof. (By the definition of m-spread, all coefficients of the element D_j of $\mathbb{C}[G]$ are 1 or 0.) We have $[D_j](g,h) = 1$ if and only if $g - h \in S_{ji}$ for some i if and only if $h - g \in S_{ji}$, which occurs if and only if $[D_j]^T(g,h) = 1$. So $[D_j] = [D_j]^T$. □

Theorem 2.3.5. *Assume the notation as in Theorem 2.3.1 and let $\chi \neq \chi_0$. Then we have*

$$\chi(D_j) = \begin{cases} -p^{m-1} & \textit{if } \chi \notin \widetilde{S}_{ji} \textit{ for all } i \\ (p-1)p^{m-1} & \textit{otherwise.} \end{cases}$$

Proof. By Theorem 1.5.3, we have that $\sum_{g \in S_{ji}} \chi(g) = 0$ for all subgroups S_{ji} of $\mathbb{F}_p^{2m}$ and χ nontrivial on S_{ji}. We know $\#S_{ji}^* = p^m - 1$ for all $i \in \{1, 2, \ldots, p^{m-1}\}$ and all $j \in \mathbb{F}_p^*$. Taking into account Theorem 2.3.3, we have

$$\chi(D_j) = \sum_{i=1}^{p^{m-1}} \sum_{g \in S_{ji}^*} \chi(g) = \begin{cases} p^{m-1}(-1) & \text{if } \chi \notin \widetilde{S}_{ji} \text{ for all } i \\ (p^{m-1}-1)(-1) + (p^m - 1) & \text{otherwise} \end{cases}$$

$$= \begin{cases} -p^{m-1} & \text{if } \chi \notin \widetilde{S}_{ji} \text{ for all } i \\ (p-1)p^{m-1} & \text{otherwise.} \end{cases}$$

□

Lemma 2.3.6. *Assume the notations and conditions in Theorem 2.3.1. For all nontrivial characters χ of $(\mathbb{F}_p^{2m},+)$, if $\chi \notin \widetilde{S}_{ji}$ for all i and j, then*

$$\chi\left(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a\right)=p^m=\chi\left(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b\right).$$

If $\chi \in \widetilde{S}_{ji}$ for some i and j, then

$$\chi(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a)=\zeta_p^j p^m$$

and

$$\chi(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b)=\zeta_p^{-j}p^m.$$

Proof. First recall S_{ji} is an element of a partial m-spread and $\widetilde{S_{ji}}$ is defined in Definition 2.3.2. By Theorem 2.3.5

$$\chi(D_j)=\begin{cases}-p^{m-1} & \text{if } \chi\notin\widetilde{S}_{ji} \text{ for all } i\\ (p-1)p^{m-1} & \text{otherwise.}\end{cases}$$

If $\chi \notin \widetilde{S}_{ji}$ for all i and j, then we calculate

$$\begin{aligned}\chi(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a)&=\sum_{a=1}^{p-1}(\zeta_p^a-1)\chi(D_a) &(2.1)\\ &=(-1-(p-1))(-p^{m-1}) &(2.2)\\ &=p^m. &(2.3)\end{aligned}$$

Recall χ is a homomorphism, $\chi(D)=\sum_{g\in G}d_g\chi(g)$. So Equation (2.1) holds. By the fact that $1+\zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1}=0$, Equation (2.2) holds.

Similarly, $\chi(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b)=p^m$.

On the other hand, if χ is nontrivial and $\chi\in\widetilde{S}_{ji}$, for some (j,i), then

$$\begin{aligned}\chi(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a) &= \sum_{a=1}^{p-1}(\zeta_p^a-1)\chi(D_a)\\ &= \sum_{a=1}^{p-1}\zeta_p^a\chi(D_a)-\sum_{a=1}^{p-1}\chi(D_a)\end{aligned}$$

$$\begin{aligned} &= (-1-\zeta_p^j)(-p^{m-1})+\zeta_p^j(p-1)p^{m-1} \\ &\quad -(p-2)(-p^{m-1})-(p-1)p^{m-1} \qquad (2.4) \\ &= \zeta_p^j p^m. \end{aligned}$$

Equation (2.4) holds because

$$\chi(D_a)=\begin{cases} -p^{m-1} & \text{if } a\neq j \\ (p-1)p^{m-1} & \text{if } a=j \end{cases}$$

and $1+\zeta_p+\cdots+\zeta_p^{p-1}=0$. Similarly, $\chi(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b)=\zeta_p^{-j}p^m$. □

Lemma 2.3.7. *Assume the notations and conditions in Theorem 2.3.1. Then*

$$\chi_0\left(\left(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a\right)\left(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b\right)\right)=p^{2m}(p^m-1)^2.$$

Proof. We know that for the trivial character $\chi_0(D_j)=p^{m-1}(p^m-1)$, for all $j\in\mathbb{F}_p^*$. So $\chi_0(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a)=(-1-(p-1))p^{m-1}(p^m-1)=-p^m(p^m-1)$ by the fact that $\sum_{a=1}^{p-1}\zeta_p^a=-1$. Thus the result follows. □

Lemma 2.3.8. *Assume the notations and conditions in Theorem 2.3.1. For all nontrivial characters χ of G,*

$$\chi\left(\left(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a\right)\left(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b\right)\right)=p^{2m}.$$

Proof. We have

$$\begin{aligned} &\chi\left((\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a)(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b)\right) \\ &=\chi(\sum_{a=1}^{p-1}(\zeta_p^a-1)D_a)\chi(\sum_{b=1}^{p-1}(\zeta_p^{-b}-1)D_b) \end{aligned}$$

Then by Lemma 2.3.6, for for all i and j, we get $p^mp^m=p^{2m}$ if $\chi\notin\widetilde{S}_{ji}$ and $\zeta_p^jp^m\zeta_p^{-j}p^m=p^{2m}$ if $\chi\in\widetilde{S}_{ji}$. □

Now we give the proof of Theorem 2.3.1.

Proof. For ease of notation, we let $G = \mathbb{F}_p^{2m}$.

Let I be the $p^{2m} \times p^{2m}$ identity matrix. Let

$$A = (\sum_{a=1}^{p-1} (\zeta_p^a - 1) D_a)(\sum_{b=1}^{p-1} (\zeta_p^{-b} - 1) D_b).$$

Let J be the $p^{2m} \times p^{2m}$ matrix with all entries 1. By Theorem 1.6.6, Lemma 2.3.8 and Lemma 2.3.7, for any nontrivial character χ,

$$\begin{aligned} A &= p^{2m} + (\chi_0(A) - \chi(A))/vG \\ &= p^{2m} + (p^{2m}(p^m - 1)^2 - p^{2m})/p^{2m} G \\ &= p^{2m} + ((p^m - 1)^2 - 1)G. \end{aligned}$$

Hence, after recalling Definition 1.6.7 we get

$$(\sum_{a=1}^{p-1} (\zeta_p^a - 1)[D_a])(\sum_{b=1}^{p-1} (\zeta_p^{-b} - 1)[D_b]) = p^{2m} I + ((p^m - 1)^2 - 1)J. \tag{2.5}$$

We have

$$\sum_{a=1}^{p-1} (\zeta_p^a - 1)[D_a]J = \sum_{a=1}^{p-1} (\zeta_p^a - 1) p^{m-1}(p^m - 1)J, \tag{2.6}$$

because each entry of $[D_a]J$ is $\#D_a$. Similarly,

$$\sum_{b=1}^{p-1} (\zeta_p^{-b} - 1)[D_b]J = \sum_{b=1}^{p-1} (\zeta_p^{-b} - 1) p^{m-1}(p^m - 1)J. \tag{2.7}$$

We also have $[D_0] = J - \sum_{a=1}^{p-1} [D_a]$. By Lemma 2.3.4 (for equation (2.8)),

$$\begin{aligned} [f][f]^* &= (\sum_{a=0}^{p-1} \zeta_p^a [D_a])(\sum_{b=0}^{p-1} \zeta_p^{-b} [D_b])^T \\ &= (J + \sum_{a=1}^{p-1} (\zeta_p^a - 1)[D_a])(J + \sum_{b=1}^{p-1} (\zeta_p^{-b} - 1)[D_b]) \end{aligned} \tag{2.8}$$

$$\begin{aligned}
&= p^{2m}J + \sum_{a=1}^{p-1}(\zeta_p^a - 1)p^{m-1}(p^m-1)J \qquad (2.9)\\
&\quad + \sum_{b=1}^{p-1}(\zeta_p^{-b} - 1)p^{m-1}(p^m-1)J\\
&\quad + p^{2m}I + ((p^m-1)^2-1)J\\
&= p^{2m}J - 2p^m(p^m-1)J + p^{2m}I + ((p^m-1)^2-1)J \qquad (2.10)\\
&= p^{2m}I.
\end{aligned}$$

Equation (2.9) follows from Equation (2.5), Equation (2.6), Equation (2.7) and $J^2 = p^{2m}J$. Equation (2.10) follows from the property that $1+\zeta_p+\ldots+\zeta_p^{p-1}=0$.

Therefore, by Theorem 2.2.10, f is bent. □

Next we will prove the converse of Theorem 2.3.1 that will be used in Chapter 3 as follows.

Theorem 2.3.9. *Let $m>1$. Suppose that S is a partial m-spread of $\mathbb{F}_p^{2m}$ and $f:\mathbb{F}_p^{2m}\to\mathbb{F}_p$ is constant on T^* for each $T\in S$ and $f(0)=0$. Note: $T^*=T\setminus\{0\}$. For all $j\in\mathbb{F}_p$, let N_j be the number of T such that $T^*\subset f^{-1}(j)$. Suppose $\bigcup_{T\in S}T^*=\bigcup_{j\in\mathbb{F}_p^*}f^{-1}(j)$. If f is bent then $N_j=p^{m-1}$ for all $j\in\mathbb{F}_p^*$.*

Proof. Assume f is bent. Let b_j be the cardinality of $f^{-1}(j)$, for $j=0,\ldots,p-1$. Then $\widehat{f}(0)=\sum_{x\in\mathbb{F}_p^{2m}}\zeta_p^{f(x)}=\sum_{j=0}^{p-1}b_j\zeta_p^j$. By Property 7 and Property 8 in [14], for all $a\in\mathbb{F}_p^{2m}$, there exists some integer k such that $\widehat{f}(a)=\pm p^m\zeta_p^k$. Hence $\widehat{f}(0)=\pm p^m\zeta_p^k$ for some integer k. We know that the polynomial $h(x)=x^{p-1}+\cdots+x^2+x+1$ is irreducible over the rational number field and $h(\zeta_p)=0$. Thus $h(x)$ is the minimal polynomial of ζ_p over the rational numbers. Let $h'(x)=b_0+b_1x+\cdots+b_{p-1}x^{p-1}$. Then $h'(x)$ is a polynomial of degree at most $p-1$ and $h'(\zeta_p)=0$. So $h'(x)$ is a constant multiple of $h(x)$. We have

$$\sum_{j=0}^{p-1}b_j\zeta_p^j \mp p^m\zeta_p^k = 0.$$

So b_j are equal except for b_k that differs from the rest by $\pm p^m$. By assumption, $p^m>2$. The cardinality of each T^* is p^m-1. We have $s(p^m-1)=t(p^m-1)+1$ where s,t are positive integers if and only if $(s-t)(p^m-1)=1$. But $p^m-1>1$, thus $s(p^m-1)\neq t(p^m-1)+1$.

For each $j \in \mathbb{F}_p$, we have b_j is multiple of $p^m - 1$ except at b_0 we need to add 0 (because $f(0) = 0$). In order for all b_j to be equal (for each $j \in \mathbb{F}_p$), except for b_k, and $f(0) = 0$, k has to be 0.

Case I: $\sum_{j=0}^{p-1} b_j \zeta_p^j - p^m = 0$ which implies $b_0 = b_j + p^m$ for $j \neq 0$. For all $j \in \mathbb{F}_p^*$, let $b_j = B$. We have $(p-1)B + B + p^m = p^{2m}$. Thus $b_j = (p^{2m} - p^m)/p = p^{m-1}(p^m - 1)$ for $j \in \mathbb{F}_p^*$. Hence $N_j = p^{m-1}$ for all $j \in \mathbb{F}_p^*$.

Case II: $\sum_{j=0}^{p-1} b_j \zeta_p^j + p^m \zeta_p^k = 0$ which implies $b_0 = b_j - p^m$ for $j \neq 0$. For all $j \in \mathbb{F}_p^*$, let $b_j = B$. We have $(p-1)B + B - p^m = p^{2m}$. We have $|T^*| = p^m - 1$. Hence $b_j = (p^{2m} + p^m)/p = N_j(p^m - 1)$, for $j \in \mathbb{F}_p^*$. For all $j \in \mathbb{F}_p^*$, observe that $N_j = (p^{2m} + p^m)/(p(p^m - 1)) = p^{m-1}(p^m + 1)/(p^m - 1)$ is not an integer except for $m = 1$ and $p = 3$ where $N_1 = N_2 = 2$ or $m = 1$ and $p = 2$ where $N_1 = 3$, because $p^{m-1}(p^m + 1) \equiv 2p^{m-1} \pmod{p^m - 1}$, $\gcd(p^{m-1}, p^m - 1) = 1$ and hence $(p^m - 1) | 2$.

So for $m > 1$ and $j \in \mathbb{F}_p^*$, we have $N_j = p^{m-1}$. □

We will give an example for the exceptional case where Theorem 2.3.9 does not hold, that is, the $m = 1$ case:

Example 2.3.10. We can find this example in Appendix A.2. Let $m = 1$ and $p = 3$. Let $f : \mathbb{F}_{3^2} \to \mathbb{F}_3$ be defined as $f(x) = T_1^2(x^4)$. As we will see in the next chapter, f satisfies all assumptions of Theorem 2.3.9 (except for the assumption $m > 1$). The function f is bent, but $N_1 = N_2 = 2 \neq 3^{1-1} = 1$. For the special case where $m = 1$ and $p = 2$, we get a similar example.

In Figure 2.1 we see an illustration of a 2-spread of $\mathbb{F}_3^4$. Each slice represents a subspace of dimension 2. The corresponding function f is constant on each slice with value notated in the figure. (e.g. $0, 1, 2$). There are three slices with function value 1 and three slices with function value 2. By Theorem 2.3.1, f is bent.

2.4 Difference Sets and Relative Difference Sets

In this section, we will discuss the relation between bent functions in our construction and difference sets. Since we only deal with abelian groups in this thesis, we use additive notation for all groups.

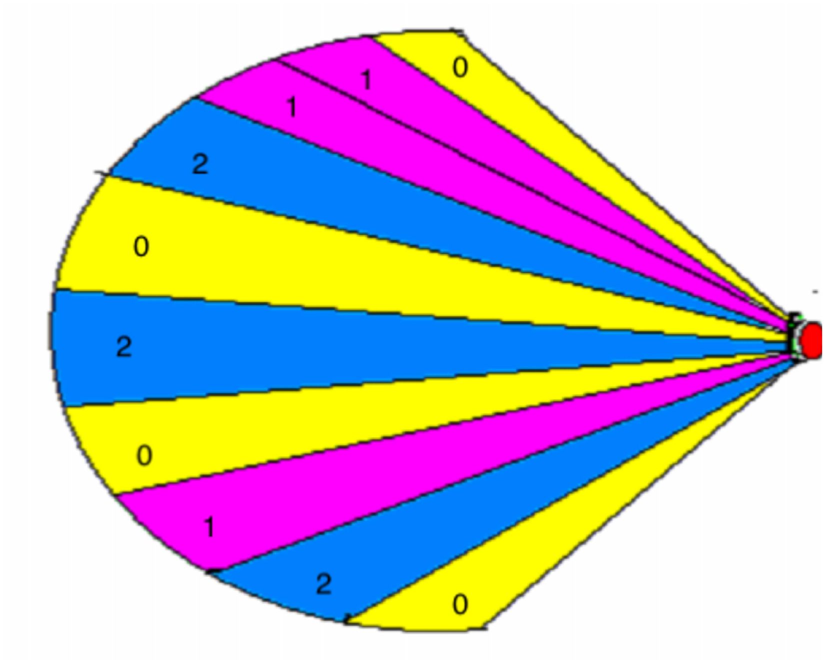


Figure 2.1: A bent function on $\mathbb{F}_3^4$

Definition 2.4.1. *Recall p is a prime. An* elementary abelian group *is an abelian group every nontrivial element of which has order p.*

Note: All elementary abelian groups with every nontrivial element of order p are of the form $\mathbb{F}_p^n$.

2.4.1 General Binary Case

In Dillon's thesis [4], he characterized bent functions in the binary case using difference sets defined as follows.

Definition 2.4.2. *A k-subset D of the group G of order v is called* a (v,k,λ)-difference set *if every non-identity element of G is represented in exactly λ ways as the difference of two elements of D.*

From Theorem 2.4.3, we can get another characterization of bent functions.

Theorem 2.4.3. *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent if and only if for all $j \in \mathbb{F}_2$ and all $a \in \mathbb{F}_2^n \setminus \{0\}$, $f(u+a) - f(u) = j$ has exactly 2^{n-1} solutions for u running through $\mathbb{F}_2^n$.*

Proof. By Theorem 2.2.10, f is bent if and only if $[f][f]^* = 2^n I_{2^n}$. This is used in our proof.

($\Rightarrow$): Assume $[f][f]^* = 2^n I_{2^n}$. Let $x, z \in \mathbb{F}_2^n$. We have

$$\sum_{y \in \mathbb{F}_2^n} (-1)^{f(x-y)-f(y-z)} = [f][f]^*(x,z).$$

By the fact that in the binary case $x - y = y - x$ we have

$$\sum_{y \in \mathbb{F}_2^n} (-1)^{f(x-y)-f(y-z)} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y-x)-f(y-z)}.$$

Let $y - z = u$ and $z - x = a$. We get that

$$\sum_{y \in \mathbb{F}_2^n} (-1)^{f(y-x)-f(y-z)} = \sum_{a \in \mathbb{F}_2^n} (-1)^{f(u+a)-f(u)}.$$

For $j \in \{0,1\}$ and a nonzero, let h_j be the number of u such that $f(u+a) - f(u) = j$. If $f(u+a) - f(u) = 0$, then we have $(-1)^{f(u+a)-f(u)} = (-1)^0 = 1$. Similarly, if $f(u+a) - f(u) = 1$, then we have $(-1)^{f(u+a)-f(u)} = (-1)^1 = -1$. Thus we have $h_0 + h_1(-1) = 0$. Hence $h_0 = h_1$. We have $h_0 + h_1 = 2^n$. So $h_0 = h_1 = 2^{n-1}$. Then for all $j \in \mathbb{F}_2$ and all $a \neq 0$, $f(u+a) - f(u) = j$ has exactly 2^{n-1} solutions for u running through $\mathbb{F}_2^n$.

($\Leftarrow$): Assume for all $j \in \mathbb{F}_2$ and all $a \in \mathbb{F}_2^n \setminus \{0\}$, $f(u+a) - f(u) = j$ has exactly 2^{n-1} solutions for u running through $\mathbb{F}_2^n$. For $x, z \in \mathbb{F}_2^n$ such that $z \neq x$, let $u = y - z$ and $a = z - x$. Then for all $j \in \{0,1\}$ and $x, z \in \mathbb{F}_2^n$ such that $z \neq x$, $f(y-x) - f(y-z) = j$ has exactly 2^{n-1} solutions for u running through $\mathbb{F}_2^n$. Thus

$$\begin{aligned}
[f][f]^*(x,z) &= \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y-x)-f(y-z)} \\
&= \sum_{y \in \mathbb{F}_2^n} (-1)^{f(x-y)-f(y-z)} \\
&= \begin{cases} 0 & \text{if } x \neq z \\ 2^n & \text{otherwise.} \end{cases}
\end{aligned}$$

Hence $[f][f]^* = 2^n I_{2^n}$. □

In accordance with Chapter 1, for $D \subset G$, let $[D]$ be the matrix defined by

$$[D](g,h) = \begin{cases} 1 & \text{if } g-h \in D \\ 0 & \text{otherwise.} \end{cases}$$

Let J denote any matrix with all entries equal to 1. For a (v,k,λ)-difference set, let $x = k-\lambda$. Usually $k-\lambda$ is denoted by n, but we already use n for other purposes in this chapter.

Theorem 2.4.4. *The subset D of a group G is a (v,k,λ)-difference set in G if and only if $[D]$ satisfies $[D][D]^T = xI + \lambda J$.*

Proof. $[D][D]^T(g,l) = \sum_{h \in G}[D](g,h)[D](l,h)$ is the number of h such that $g-h \in D$ and $l-h \in D$.
Case I: $g = l$. For h running through G, there are exactly $\#D$ h's such that $g-h \in D$. So $[D][D]^T(g,g) = k = x+\lambda$.
Case II: $g \neq l$. When h runs through G, the number of representations of $g-l$ as $g-l = (g-h)-(l-h)$ with $g-h \in D$ and $l-h \in D$ is λ. Hence $[D][D]^T(g,l) = \lambda$.

Therefore, $[D][D]^T = (x+\lambda)I + \lambda(J-I) = xI + \lambda J$ if and only if for each nonzero element in G there are exactly λ representations as a difference of two elements of D. □

Now let us discuss the relation between the difference sets and bent functions.

Theorem 2.4.5. *[4] Let m be a positive integer. Let $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$. Let $G = \mathbb{F}_2^{2m}$. Then one of $f^{-1}(1)$, $f^{-1}(0)$ is a $(2^{2m}, 2^{2m-1}-2^{m-1}, 2^{2m-2}-2^{m-1})$-difference set in G if and only if f is bent.*

Proof. $(\Rightarrow)$: Case I: Assume $f^{-1}(1)$ is a $(2^{2m}, 2^{2m-1}-2^{m-1}, 2^{2m-2}-2^{m-1})$-difference set. Let $D = f^{-1}(1)$. Recall that the matrix $[f]$ is defined by $[f](g,h) = (-1)^{f(g-h)}$. Then $[f] = J - 2[D]$. As before, let $x = k-\lambda$. We have D is a (v,k,λ)-difference set with order v of G ($v = 2^{2m}$), order k of D ($k = 2^{2m-1}-2^{m-1}$), $\lambda = 2^{2m-2}-2^{m-1}$ and $x = 2^{2m-2}$. The equation $[D]J = kJ$ holds because each entry of $[D]J$ is the cardinality of D. We have $[f][f]^T = (J-2[D])(J-2[D]^T) = J^2 - 2[D]J - 2J[D]^T + 4[D][D]^T = vJ - 4kJ + 4(xI + \lambda J) = 4xI + (v-4k+4\lambda)J = 4xI + (v-4x)J = 4xI = 2^{2m}I$. By Theorem 2.2.10, f is bent.

Case II: Assume $f^{-1}(0)$ is a $(2^{2m}, 2^{2m-1}-2^{m-1}, 2^{2m-2}-2^{m-1})$-difference set. Let $D = f^{-1}(0)$. Then $[f][f]^T = (2[D]-J)(2[D]^T-J) = (J-2[D])(J-2[D]^T)$. So same proof as in case I applies. We get f is bent.

($\Leftarrow$): Assume f is bent. Then $\widehat{f}(0) = \sum_{x\in\mathbb{F}_2^{2m}}(-1)^{f(x)} = \pm 2^m$. Let $b_j = \#f^{-1}(j)$ for $j \in \{0,1\}$. We have $b_0 + b_1(-1) = \pm 2^m$ and $b_0 + b_1 = 2^{2m}$.

Case I: $b_0 + b_1(-1) = -2^m$. Then $b_0 = 2^{2m-1} + 2^{m-1}$ and $b_1 = 2^{2m-1} - 2^{m-1}$. Let $a \in \mathbb{F}_2^n$. Let

$$n_{00} = \#\{v : f(v) = 0 \text{ and } f(v+a) = 0\},$$

$$n_{11} = \#\{v : f(v) = 1 \text{ and } f(v+a) = 1\}$$

and

$$n_{10} = \#\{v : f(v) = 1 \text{ and } f(v+a) = 0\}.$$

Then by Theorem 2.4.3, $n_{00} + n_{11} = 2^{2m-1}$. Since the cardinality of D is $2^{2m-1} - 2^{m-1}$, we have $n_{11} + n_{10} = 2^{2m-1} - 2^{m-1}$. Since the cardinality of $f^{-1}(0)$ is $2^{2m-1} + 2^{m-1}$, we have $n_{00} + n_{10} = 2^{2m-1} + 2^{m-1}$. Thus we get $n_{11} = 2^{2m-2} - 2^{m-1}$. The number of representations of $g \in G$ as a difference of elements in D is

$$\#\{v : v \in D \text{ and } v + a \in D\} = n_{11}.$$

So D is a $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$-difference set.

Case II: $b_0 + b_1(-1) = 2^m$. Then $b_0 = 2^{2m-1} - 2^{m-1}$ and $b_1 = 2^{2m-1} + 2^{m-1}$. By Theorem 1.7.7, the Boolean function $f(x)$ is bent if and only if $f(x) + 1$ is bent. We replace $f(x)$ by $F(x) = f(x) + 1$. Then $b_0 + b_1(-1) = -2^m$. By the same proof as in case I, we get $D = f^{-1}(0)$ is a $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$-difference set.

Therefore, the result follows. □

2.4.2 Specific Binary Case

The following theorem about difference sets is introduced by Dillon in [4].

Theorem 2.4.6. *[4] Let G be a group of order M^2. Let $\{S_1, S_2, ..., S_r\}$ be pairwise disjoint (except for 0) subgroups of order M for G. Then*

(1) $D = (\cup S_i) \setminus \{0\}$ is a difference set if and only if G has order $4N^2$ and $r = N$. This is a difference set with parameters $(4N^2, 2N^2 - N, N^2 - N)$.

(2) $D = \cup S_i$ is a difference set if and only if G has order $4N^2$ and $r = N + 1$. This is a difference set with parameters $(4N^2, 2N^2 + N, N^2 + N)$.

In this section, we only consider Theorem 2.4.6 with $G = \mathbb{F}_2^{2m}$.

The following definitions are introduced by Dillon in [4]:

Definition 2.4.7. *The difference sets described in Theorem 2.4.6 (1) with cardinality $2N^2 - N$ are called type $\mathcal{PS}^{(-)}$. The difference sets described in Theorem 2.4.6 (2) with cardinality $2N^2 + N$ are called type $\mathcal{PS}^{(+)}$.*

In this definition, the abbreviation $\mathcal{PS}$ denotes "partial spread."

Another definition introduced by Dillon that relates difference sets to binary bent functions is:

The nonzero points lying on any 2^{m-1} lines through the origin constitute a difference set of $\mathbb{F}_2^{2m}$ in the affine plane $L+L = \mathbb{F}_2^{2m}$, $L = \mathbb{F}_{2^m}$ where $L+L$ is a direct sum. The set of bent functions corresponding to these difference sets are called $\mathcal{PS}_{ap}^{-}$ class. Such construction is a partial m-spread of G and $\{S_1, S_2, \dots, S_r\}$ in Theorem 2.4.6 can be viewed as a set of subspaces of $\mathbb{F}_2^{2m}$. This is a special case ($p = 2$) of Theorem 2.3.1.

2.4.3 p-ary Case

We extend the definition of $\mathcal{PS}_{ap}^{-}$ functions from binary to p-ary, where the p-ary bent functions f are those introduced in our Theorem 2.3.1. The reason why in Theorem 2.3.1 we extend the set of $\mathcal{PS}_{ap}^{-}$ functions which is a subset of $\mathcal{PS}^{(-)}$ but not some subset of the set of $\mathcal{PS}^{(+)}$ functions is that some of the $\mathcal{PS}^{(+)}$ functions may be polynomials of degree 2. From the point of view of cryptography, these kinds of functions are easily broken. The A5/1 stream cipher discussed in Chapter 1 is a good example. Let $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$. We can replace x_1x_2, x_1x_3 and x_2x_3 by u_1, u_2 and u_3 respectively. Then $u_1 + u_2 + u_3$ is linear and $x_1x_2 = u_1$, $x_1x_3 = u_2$ and $x_2x_3 = u_3$ have degree two. With known plaintext and ciphertext, we can solve for the keystream in polynomial time. (In fact, most bent functions in the literature are polynomials of degree 2. We will return to this at the beginning of Chapter 3.) But $\mathcal{PS}_{ap}^{-}$ functions have sufficiently high degrees, e.g., $\deg(f) = m$, where $\mathbb{F}_p^{2m}$ is the domain of f. That is why partial spread bent functions are so important in Cryptography.

Let $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ be a function. In Dillon's thesis, he used $D_1 = f^{-1}(1)$ as a (v, k, λ)-difference set with $v = 2^{2m}$, k being the cardinality of D_1 and $\lambda = k - v/4$ to prove the special case of Theorem 2.3.1 with $p = 2$. For general p, [22] is one of the most recent references on the connection between bent functions and difference sets.

Definition 2.4.8. *Let G be a finite group of order mn, and let N be a subgroup of G of order n. A k-subset R of G is called an* (m,n,k,λ)-relative difference set (RDS) *in G relative to N if every element $g \in G \setminus N$ has exactly λ representations $g = r_1 - r_2$ with $r_1, r_2 \in R$, and no non-identity element of N has such a representation.*

Let R be a $(p^{2m}, p, p^{2m}, p^{2m-1})$-relative difference set of $G = \mathbb{F}_p^{2m} \times \mathbb{F}_p$ with $N = \{0\} \times \mathbb{F}_p$. Since non-identity elements in N do not have representation as a difference of two elements in R, for each $h \in \mathbb{F}_p^{2m}$, there exists exactly one n_h such that $(h, n_h) \in R$. Otherwise, if there exist (h, n_{h_1}) and (h, n_{h_2}) such that $n_{h_1} \neq n_{h_2}$, then there is a representation $(h, n_{h_1}) - (h, n_{h_2})$ for the non-identity element $(0, n_{h_1} - n_{h_2})$ in N, which is a contradiction. We can define the function $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ such that $f(h) = n_h$. Also, $\#R = p^{2m}$, so all elements in $\mathbb{F}_p^{2m}$ are in the domain of f. Conversely, any function $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ defines the set $R_f = \{(h, f(h)) | h \in \mathbb{F}_p^{2m}\}$. This is the correspondence between bent functions and relative difference sets. It is stated, for example, as Proposition 2 in [22]:

Proposition 2.4.9. *The set R is a relative (p^n, p, p^n, p^{n-1})-difference set in $\mathbb{F}_p^{2m} \times \mathbb{F}_p$ if and only if the corresponding function is p-ary bent.*

Now let us explore the side of relative difference sets and see if there exists the partial spread construction described in Theorem 2.3.1. We read some related papers. For example, [12], [6]. We focus on the relative difference sets with parameters $(p^{2m}, p, p^{2m}, p^{2m-1})$. We find in Section 2 in [3], J. A. Davis described the construction of $(p^{i+j}, p^i, p^{i+j}, p^j)$-relative difference sets with j odd and $i = 1$. We choose $j = 2m - 1$. Then we get the parameters of difference set that we are interested in. Similar to our construction (Theorem 2.3.1 of this thesis), the construction in Section 2 in [3] defines the bent function by decomposing its domain into subsets, and dealing with each subset separately. However, in our Theorem 2.3.1 the bent function is *constant* on each subset (subspace in the partial spread), whereas in Section 2 in [3] the function in general takes different values on each subset. Hence we conclude that the constructions are not the same.

We also found a similar construction in [17]. But the number of subsets in that construction is a power of p, whereas in our construction it is $p^m + 1$. So the construction in [17] is not the same as ours.

Also, after a wide search, we did not find a reference that would give the construction of Theorem 2.3.1 in the context of relative difference sets for characteristic p, odd prime. So the construction described in Section 2.3 appears to be unknown in the literature.

Chapter 3

Monomial and Multinomial Bent Functions

Multinomial bent functions are functions with several terms (e.g. $T_1^n(x+x^2)$). We have discussed the combinatorial construction of bent functions in Chapter 2. In this chapter, we will give the algebraic construction of bent functions. The reason why we care about algebraic construction is that we can have an explicit formula for bent functions that will be easily computed by computers.

For reasons illustrated near the end of Chapter 2, quadratic bent functions are viewed as weak in Cryptography. T. Helleseth and A. Kholosha in Table I of [10] summarized all currently known non-quadratic p-ary monomial bent functions. There are four classes of them, one of which contains just one function, and $p = 3$ for all classes. One of the three infinite categories occurs for the Dillon type exponent (Theorem 3.3.8 in this chapter). Hence our algebraic construction covers one third of the known constructions of non-quadratic monomial bent functions. This is one of the reasons why we gave the combinatorial construction in Chapter 2, which appears unknown presently, yet it is connected with an important class of bent functions.

Throughout this entire chapter, we assume that p is an odd prime.

In this chapter, we are motivated by Theorem 7 in paper [2] by P. Charpin and G. Gong. This theorem gave conditions for multinomial binary functions with the Dillon type exponents to be bent. We extend this theorem from the binary case to the p-ary case.

Most theorems in this chapter are new.

3.1 Short Descriptions of Some Spreads

Let m be a positive integer. Let α be a generator of $\mathbb{F}_{p^{2m}}^*$. Let $\gamma = \alpha^{(p^m-1)/2^k}$, where $2^k b = p^m - 1$ for b odd and k a positive integer. We will construct a specific partial spread that is related to trace functions. With this spread we will reduce the running time for testing bentness.

As γ plays a main role in the whole chapter, let us prove some properties about γ:

Proposition 3.1.1. *For $i \in \{1,2,\dots,p^m+1\}$, the following statements hold:*
(1) $\gamma^{(p^m-1)i} = 1$ if and only if $i = p^m+1$.
(2) $\gamma^{(p^m-1)i} = -1$ if and only if $i = (p^m+1)/2$.

Proof. (1)($\Leftarrow$) For any element $\beta \in \mathbb{F}_{p^{2m}}$, we have $\beta^{(p^m-1)(p^m+1)} = 1$, hence if $i = p^m+1$, then $\gamma^{(p^m-1)i} = 1$. ($\Rightarrow$) Assume $\gamma^{(p^m-1)i} = 1$. We have $\gamma^{(p^m-1)i} = \alpha^{(p^m-1)^2 i/2^k} = \alpha^{(p^m-1)bi} = 1$. Thus the order $p^{2m}-1$ of α divides $(p^m-1)bi$, hence $(p^m+1)|(bi)$. Since $\gcd(p^m-1, p^m+1) = 2$, by definition, b is an odd factor of p^m-1 and $\gcd(b, p^m+1) = 1$. Therefore, $p^m+1|i$ and since $i \in \{1,2,\dots,p^m+1\}$, we have $i = p^m+1$.

(2)($\Leftarrow$) For any element $\beta \in \mathbb{F}_{p^{2m}}$, we have $\beta^{(p^m-1)(p^m+1)/2} = -1$, hence if $i = (p^m+1)/2$, then $\gamma^{(p^m-1)i} = -1$.($\Rightarrow$) Assume $\gamma^{(p^m-1)i} = -1$. We have $\gamma^{(p^m-1)2i} = 1$. By (1), we have $(p^m+1)|2i$. So $i = p^m+1$ or $i = (p^m+1)/2$. But $\gamma^{(p^m-1)i} = -1$, hence $i = (p^m+1)/2$. □

Theorem 3.1.2. *Let $p^m - 1 = 2^k b$, where b is odd and k is a positive integer. Let α be a generator of $\mathbb{F}_{p^{2m}}^*$. Let $\gamma = \alpha^{(p^m-1)/2^k}$. Then $\gamma^i \notin \mathbb{F}_{p^m}$, for each i that is not divisible by p^m+1.*

Proof. Let H be the group generated by γ. Assume $\gamma^i \in \mathbb{F}_{p^m}$, where i is not divisible by p^m+1. Also, note that $\gamma^i \neq 0$ and $|H| = 2^k(p^m+1)$. Then the order a of γ^i divides both the order of H and the order of $\mathbb{F}_{p^m}^*$ hence a divides 2^k, because

$$\begin{aligned}\gcd(|H|, |\mathbb{F}_{p^m}^*|) &= \gcd(2^k(p^m+1), p^m-1)\\ &= \gcd(2^k(2^k b+2), 2^k b) = 2^k.\end{aligned}$$

Also $(\gamma^i)^a = 1$ which is equivalent to $\alpha^{(ia(p^m-1))/2^k} = 1$. So $(p^{2m}-1)|(ia(p^m-1))/2^k$ which is equivalent to $(p^m+1)|(ia/2^k)$. Then $(p^m+1)|i$ because $a|2^k$ so $\frac{ia}{2^k}|i$, which is a contradiction. □

The m-spread defined by the following theorem is used quite often in our construction.

Theorem 3.1.3. *Let $p^m - 1 = 2^k b$, where b is odd and k is a positive integer. Let α be a generator of $\mathbb{F}^*_{p^{2m}}$. Let $\gamma = \alpha^{(p^m-1)/2^k}$. Then $\gamma^i \mathbb{F}_{p^m} \cap \gamma^j \mathbb{F}_{p^m} = \{0\}$, where i is not congruent to j modulo $p^m + 1$. Furthermore, the set $\{\gamma^i \mathbb{F}_{p^m} | i = 1, \ldots, p^m + 1\}$ is an m-spread of $(\mathbb{F}_{p^{2m}}, +)$.*

Proof. Assume there exists a nonzero element in $\gamma^i \mathbb{F}_{p^m} \cap \gamma^j \mathbb{F}_{p^m}$, where i is not congruent to j mod $p^m + 1$. Thus $\gamma^i x = \gamma^j y$ for some $x, y \in \mathbb{F}_{p^m}$. Then $\gamma^{i-j} = yx^{-1} \in \mathbb{F}_{p^m}$. But by Theorem 3.1.2, $\gamma^{i-j} \notin \mathbb{F}_{p^m}$, which is a contradiction. Therefore, $\gamma^i \mathbb{F}_{p^m} \cap \gamma^j \mathbb{F}_{p^m} = \{0\}$, where i is not congruent to j modulo $p^m + 1$.

The cardinality of $\cup_{i=1}^{p^m+1} \gamma^i \mathbb{F}_{p^m}$ is p^{2m} and $\cup_{i=1}^{p^m+1} \gamma^i \mathbb{F}_{p^m}$ is a subset of $\mathbb{F}_{p^{2m}}$. Hence

$$\cup_{i=1}^{p^m+1} \gamma^i \mathbb{F}_{p^m} = \mathbb{F}_{p^{2m}}.$$

By Theorem 2.1.3, $\gamma^i \mathbb{F}_{p^m}$ is a subspace of $(\mathbb{F}_{p^{2m}}, +)$ for each $i \in \{1, \ldots, p^m + 1\}$. Thus by Definition 2.1.1, $\{\gamma^i \mathbb{F}_{p^m} | i \in \{1, \ldots, p^m + 1\}\}$ is an m-spread of $(\mathbb{F}_{p^{2m}}, +)$. □

3.2 Functions with Identical Walsh Spectra

In this section, we will prove that in the binary and the p-ary case, finding monomial bent functions (e.g. with only one term $T_1^n(\lambda_r x^{p^m-1})$) with coefficients in $\mathbb{F}_{p^{2m}}$ can be constrained to finding monomial bent functions with coefficients in $\mathbb{F}_{p^m}$.

Now let us prove lemmas that will be used in the next two subsections.

Theorem 3.2.1. *Let p be a prime. Let r be a positive integer such that $\gcd(r, p^{2m} - 1) = 1$. Let $f_\lambda : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ be defined as $f_\lambda(x) = T_1^{2m}(\lambda x^{r(p^m-1)})$, where $\lambda \in \mathbb{F}_{p^{2m}}$. Let G be the cyclic subgroup of $\mathbb{F}_{p^{2m}}$ with order $p^m + 1$. If $\lambda = uv$ for some $u \in \mathbb{F}_{p^m}$ and $v \in G$, then $f_\lambda(x) = f_u(\alpha^d x)$ for some non-negative integer d.*

Proof. Assume $\lambda = uv$ as in the statement of the lemma. Since $\gcd(r, p^{2m} - 1) = 1$, α^r is a generator of $\mathbb{F}_{p^{2m}}$. Thus $G = \langle \alpha^{r(p^m-1)} \rangle$. Since $G = \langle \alpha^{r(p^m-1)} \rangle$ and $v \in G$, we have

$v = \alpha^{rd(p^m-1)}$ for some non-negative integer d. Since $\alpha^{r(p^m-1)}$ is a generator of G, we have

$$\begin{aligned} f_\lambda(x) = T_1^{2m}(\lambda x^{r(p^m-1)}) &= T_1^{2m}(uvx^{r(p^m-1)}) \\ &= T_1^{2m}(u\alpha^{dr(p^m-1)}x^{r(p^m-1)}) \\ &= T_1^{2m}(u(\alpha^d x)^{r(p^m-1)}) \\ &= f_u(\alpha^d x). \end{aligned}$$

□

Recall Walsh spectrum is defined in Definition 1.7.2.

Theorem 3.2.2. *Let p be a prime. Let r be a positive integer such that $\gcd(r, p^{2m}-1) = 1$. Let $f_\lambda : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ be defined as $f_\lambda(x) = T_1^{2m}(\lambda x^{r(p^m-1)})$, where $\lambda \in \mathbb{F}_{p^{2m}}$. If $f_\lambda(x) = f_u(\alpha^d x)$ for some non-negative integer d and $u \in \mathbb{F}_p^m$, then f_λ and f_u have the same Walsh spectrum.*

Proof. Since the map $x \mapsto \alpha^d x$ is a bijection, for $a \in \mathbb{F}_{p^{2m}}$, the Walsh coefficient

$$\begin{aligned} \widehat{f_u}(a) &= \sum_{x\in\mathbb{F}_{p^{2m}}} \zeta_p^{f_u(x)-T_1^{2m}(ax)} \\ &= \sum_{x\in\mathbb{F}_{p^{2m}}} \zeta_p^{f_u(\alpha^d x)-T_1^{2m}(a\alpha^d x)} \\ &= \widehat{f_\lambda}(a\alpha^d). \end{aligned}$$

So the result follows. □

3.2.1 Binary Case

For the binary case, the following theorems have been proved in [2].

Proposition 3.2.3. *We have $\{uv : u \in \mathbb{F}_{2^m}^* \text{ and } v \in G\} = \mathbb{F}_{2^{2m}}^*$, where G is the cyclic subgroup of $\mathbb{F}_{2^{2m}}^*$ with order 2^m+1.*

Proof. Let $D = \{uv : u \in \mathbb{F}_{2^m}^* \text{ and } v \in G\}$. Clearly, $D \subset \mathbb{F}_{2^{2m}}^*$. Let $x \in \mathbb{F}_{2^{2m}}^*$. Since $\gcd(2^m-1, 2^m+1) = 1$, by Extended Euclidean Algorithm there exist $c, d \in \mathbb{Z}$ such that $(2^m-1)c + (2^m+1)d = 1$. So $x = x^{(2^m-1)c+(2^m+1)d} = x^{(2^m-1)c}x^{(2^m+1)d}$ where $v = x^{(2^m-1)c}$ and $u = x^{(2^m+1)d}$. Hence $x \in D$ and $\mathbb{F}_{2^{2m}}^* \subset D$. Therefore, $D = \mathbb{F}_{2^{2m}}^*$. □

Theorem 3.2.4. *Let G be the cyclic subgroup of $\mathbb{F}_{2^{2m}}$ with order 2^m+1. For $\lambda \in \mathbb{F}^*_{2^{2m}}$, there exists $u \in \mathbb{F}^*_{2^m}$ with $\lambda = uv$ and $v \in G$, such that the Boolean function $f_\lambda : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ defined as $f_\lambda(x) = T_1^{2m}(\lambda x^{2^m-1})$ has the same Walsh spectrum as $f_u : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ defined as $f_u(x) = T_1^{2m}(ux^{2^m-1})$.*

Proof. By Proposition 3.2.3, $\lambda = uv$. Let α be a generator of $\mathbb{F}_{p^{2m}}$. Thus by Theorem 3.2.1, $f_\lambda(x) = f_u(\alpha^d x)$. Hence by Theorem 3.2.2, f_λ and f_u have the same Walsh spectrum. □

3.2.2 p-ary Case

For the p-ary case, the following theorems are new and they are extensions of results in Section 3.2.1.

Theorem 3.2.5. *Let p be an odd prime. We have $\{uv : u \in \mathbb{F}^*_{p^m}$ and $v \in G\} = \{z^2 : z \in \mathbb{F}^*_{p^{2m}}\}$, where G is the cyclic subgroup of $\mathbb{F}^*_{p^{2m}}$ of order p^m+1.*

Proof. Let α be a generator of $\mathbb{F}^*_{p^{2m}}$. Let $D_1 = \{uv : u \in \mathbb{F}^*_{p^m}$ *and* $v \in G\}$ and let $D_2 = \{z^2 : z \in \mathbb{F}^*_{p^{2m}}\}$. First, let $x \in D_1$. Then $x = uv = \alpha^{(p^m+1)l}\alpha^{(p^m-1)l'}$, for some $l,\ l' \in \mathbb{Z}$. Since p^m+1 and p^m-1 are even, $x = z^2$ for some $z \in \mathbb{F}^*_{p^{2m}}$. So $x \in D_2$. We get $D_1 \subseteq D_2$.

On the other hand, let $x \in D_2$. Then $x = z^2$ for some $z \in \mathbb{F}^*_{p^{2m}}$. We have $x = \alpha^{2l}$, for some $l \in \mathbb{Z}$. We know that $\gcd(p^m+1, p^m-1) = 2$, so by Extended Euclidean Algorithm, there exist $c \in \mathbb{Z}$ and $d \in \mathbb{Z}$ such that $c(p^m+1)+d(p^m-1) = 2$. Then $x = (\alpha^2)^l = (\alpha^{(p^m+1)c}\alpha^{(p^m-1)d})^l = uv$, for some $u \in \mathbb{F}^*_{p^m}$ *and* $v \in G$. Hence, $D_2 \subseteq D_1$. Therefore, $D_1 = D_2$. □

Theorem 3.2.6. *Let p be an odd prime. Let G be the cyclic subgroup of $\mathbb{F}^*_{p^{2m}}$ of order p^m+1. Let $f_\lambda : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ be defined as $f_\lambda(x) = T_1^{2m}(\lambda x^{r(p^m-1)})$, where $\gcd(r, p^{2m}-1) = 1$. If f_λ is bent for some $\lambda \in \mathbb{F}^*_{p^{2m}}$, then there exists $u \in \mathbb{F}^*_{p^m}$ such that $\lambda = uv$ with $v \in G$ and f_λ, f_u and f_{-u} have the same Walsh spectrum.*

Proof. Case I $p > 3$: Recall Definition 1.5.7 of Kloosterman sum. By Theorem 2 [9], f_λ is bent if and only if $K_{p^m}(\lambda^{p^m+1}) = 0$, where $K_{p^m}(\cdot)$ is the Kloosterman sum on $\mathbb{F}_{p^m}$. Note: $\lambda^{p^m+1} \in \mathbb{F}^*_{p^m}$. By Corollary 2 in [13], we have that Kloosterman sum is never 0 if $p > 3$. Then there is no bent function f_λ.

Case II $p=3$: By Theorem 2 [9], f_λ is bent if and only if $K_{p^m}(\lambda^{p^m+1})=0$, where $K_{p^m}(\cdot)$ is the Kloosterman sum on $\mathbb{F}_{p^m}$. By Theorem 1.4 [7], if $K_{p^m}(\lambda^{p^m+1})=0$ and $\lambda^{p^m+1}\neq 0$, then λ^{p^m+1} is a square in $\mathbb{F}^*_{p^m}$. Let α be a generator for $\mathbb{F}^*_{p^{2m}}$, hence α^{p^m+1} is a generator for $\mathbb{F}^*_{p^m}$. Let $\lambda^{p^m+1}=z^2$ where $z\in\mathbb{F}^*_{p^m}$. Then $z=(\alpha^{p^m+1})^d$, for some $d\in\mathbb{Z}$. Hence,

$$\lambda^{p^m+1}=(\alpha^{2d})^{p^m+1}. \tag{3.1}$$

Claim: $\lambda=\alpha^{2s}$ for some $s\in\mathbb{Z}$. Assume not. Then $\lambda=\alpha^{2s+1}$. Substitute it into Equation (3.1) and we get an equation for the exponent of α, which is

$$\begin{aligned}(2s+1)(p^m+1)&\equiv 2d(p^m+1) \pmod{p^{2m}-1}\\ 2s+1&\equiv 2d \pmod{p^m-1}.\end{aligned}$$

So $(p^m-1)|(2s+1-2d)$. But p^m-1 is even and $2s+1-2d$ is odd, which is a contradiction. Hence $\lambda=\alpha^{2s}$ for some $s\in\mathbb{Z}$. Then by Theorem 3.2.5, there exist $u\in\mathbb{F}^*_{p^m}$ and $v\in G$ such that $\lambda=uv$. By Theorem 3.2.1, $f_\lambda(x)=f_u(\alpha^d x)$, for some non-negative integer d. Hence by Theorem 3.2.2, f_λ and f_u have the same Walsh spectrum.

For $u\in\mathbb{F}^*_{p^m}$ and $v\in G$, $-u\in\mathbb{F}^*_{p^m}$ and since $-1\in G$, we have $-v\in G$. For any λ, we have $\lambda=uv=(-u)(-v)$. By Theorem 3.2.1, we get $f_\lambda(x)=f_{-u}(\alpha^d x)$ for some non-negative integer d. Hence by Theorem 3.2.2 f_{-u} has the same Walsh spectrum as f_λ and f_u. □

3.3 Bent Functions and Partial Spreads

In this section, our purpose is to characterize bent functions with coefficients in $\mathbb{F}_{p^m}$.

Definition 3.3.1. *Let $a\in\mathbb{Z}_{p^m+1}$. The set $\{ap^k \pmod{p^m+1} : k=1,\ldots,2m\}$ is called the* cyclotomic coset of a modulo p^m+1.

Note: A cyclotomic coset modulo p^m+1 has cardinality at most $2m$, because $p^{2m}\equiv 1 \pmod{p^m+1}$ hence $ap^{2m}\equiv a \pmod{p^m+1}$. A cyclotomic coset modulo p^m+1 may have cardinality less than $2m$. For example: When $p=3$ and $m=2$, the cyclotomic cosets modulo 3^2+1 are: $\{0\},\{1,3,7,9\},\{2,4,6,8\},\{5\}$. We can see that $\{5\}$ has cardinality less than 4.

Definition 3.3.2. *We define L_m to be any set of representatives of cyclotomic cosets modulo p^m+1, where p is an odd prime and m is a positive integer.*

The following theorem shows that using elements in L_m is enough for a trace function of the form which we use.

Theorem 3.3.3. *Let p be any prime. Let the function $f_\lambda : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ be defined as $f(x) = \sum_{r\in\mathbb{Z}} T_1^{2m}(\lambda_r x^{r(p^m-1)})$, where $\lambda_r \in \mathbb{F}_{p^{2m}}$ and only finitely many λ_r are nonzero. Then without loss of generality we can write $f(x) = \sum_{r\in L_m} T_1^{2m}(\lambda_r x^{r(p^m-1)})$.*

Proof. Assume $r_2 \in L_m$. If r_1 and r_2 are in the same cyclotomic coset modulo p^m+1, then $r_2 \equiv r_1 p^k \pmod{p^m+1}$ for some integer k. Thus

$$\begin{aligned}&T_1^{2m}(\lambda_{r_1}x^{r_1(p^m-1)}+\lambda_{r_2}x^{r_2(p^m-1)})\\&=T_1^{2m}((\lambda_{r_1}x^{r_1(p^m-1)})^{p^k}+\lambda_{r_2}x^{r_2(p^m-1)})\\&=T_1^{2m}((\lambda_{r_1}^{p^k}+\lambda_{r_2})x^{r_2(p^m-1)}).\end{aligned}$$

So if r_1 and r_2 are in the same cyclotomic coset modulo p^m+1, then $T_1^{2m}(\lambda_{r_1}x^{r_1(p^m-1)}+\lambda_{r_2}x^{r_2(p^m-1)})$ can be written as $T_1^{2m}(\lambda_{r_o}x^{r_2(p^m-1)})$ for some $\lambda_{r_o} \in \mathbb{F}_{p^{2m}}$. Thus r_1 is redundant. By repeating this argument, we can prove the theorem. □

Theorem 3.3.4. *Let α be a generator of $\mathbb{F}_{p^{2m}}^*$. Let $\gamma = \alpha^{(p^m-1)/2^k}$, where $2^k b = p^m-1$ for b odd and k positive integer. Let $S_i = \gamma^i \mathbb{F}_{p^m}$, for all i, $1 \le i \le p^m+1$. Let $S_i^* = S_i \setminus \{0\}$ for all i, $1 \le i \le p^m+1$. For $\lambda_r \in \mathbb{F}_{p^m}$, define the function $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ by $f(x) = \sum_{r\in L_m} T_1^{2m}(\lambda_r x^{r(p^m-1)})$. Then f is constant on each S_i^*, equal to*

$$\sum_{r\in L_m} T_1^{2m}(\lambda_r \gamma^{ri(p^m-1)}),$$

which can be also expressed as

$$\sum_{r\in L_m} T_1^{m}(\lambda_r(\gamma^{ri(p^m-1)}+\gamma^{-ri(p^m-1)})).$$

Proof. Let $x \in S_i^*$ for some $i \in \{1,\dots,p^m+1\}$. Thus $x = \gamma^i u$ where $u \in \mathbb{F}_{p^m}$. Then

$$f(x) = \sum_{r\in L_m} T_1^{2m}(\lambda_r x^{r(p^m-1)}) =$$

$$\begin{aligned}
&= \sum_{r\in L_m} T_1^{2m}(\lambda_r(\gamma^j u)^{r(p^m-1)}) \\
&= \sum_{r\in L_m} T_1^{m}(T_m^{2m}(\lambda_r(\gamma^j)^{r(p^m-1)})) && (3.2)\\
&= \sum_{r\in L_m} T_1^{m}(\lambda_r((\gamma^j)^{r(p^m-1)}+(\gamma^j)^{r(p^m-1)p^m})) && (3.3)\\
&= \sum_{r\in L_m} T_1^{m}(\lambda_r((\gamma^j)^{r(p^m-1)}+(\gamma^j)^{r(p^m-1)(p^m+1)}\gamma^{-(p^m-1)ri})) \\
&= \sum_{r\in L_m} T_1^{m}(\lambda_r(\gamma^{ri(p^m-1)}+\gamma^{-(p^m-1)ri})).
\end{aligned}$$

Equation (3.2) holds by $u^{p^m-1}=1$ and Equation (3.3) holds by Proposition 1.3.4. □

The following theorems before Theorem 3.3.8 are new and they serve for the proof of Theorem 3.3.8, which is our second main result.

Theorem 3.3.5. *Let p be an odd prime. Let α be a generator of $\mathbb{F}_{p^{2m}}^*$. Let $\gamma=\alpha^{(p^m-1)/2^k}$, where $2^k b = p^m-1$ for b odd and k positive integer. Then $\{u+u^{-1}: u\in\mathbb{F}_{p^m}^*\}\cap\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}: i\in\{1,\dots,p^m+1\}\}=\{2,-2\}$.*

Proof. Let $v\in\{u+u^{-1}: u\in\mathbb{F}_{p^m}^*\}\cap\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}: i\in\{1,\dots,p^m+1\}\}$. We have $u+u^{-1}=v=\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}$, for some u and some i. As $\{u,u^{-1}\}$ and $\{\gamma^{(p^m-1)i}, \gamma^{-(p^m-1)i}\}$ are two pairs of solutions of $x^2-vx+1=0$, we have $u=\gamma^{(p^m-1)i}$ or $u^{-1}=\gamma^{(p^m-1)i}$. Without loss of generality, assume $u=\gamma^{(p^m-1)i}$.

We have that $u\in\mathbb{F}_{p^m}^*$, hence $u=\alpha^{(p^m+1)j}$ for some $j\in\{1,\dots,p^m-1\}$. Also, $\gamma^{(p^m-1)i}=\alpha^{(p^m-1)^2 i/2^k}$. Now we want to find possible values of j to prove $v\in\{2,-2\}$. We have $\alpha^{(p^m+1)j}=\alpha^{(p^m-1)^2 i/2^k}$. Then

$$(p^m+1)j-(p^m-1)^2 i/2^k=(p^{2m}-1)l$$

for some integer l. Since $(p^m-1)|((p^m-1)^2 i)/2^k$ and $(p^m-1)|(p^{2m}-1)l$, we have $(p^m-1)|(p^m+1)j$ hence $(p^m-1)/2|((p^m+1)/2)j$. With $\gcd((p^m-1)/2,(p^m+1)/2)=1$, we conclude that $(p^m-1)/2|j$. Hence $j=((p^m-1)/2)c$ for $c=1$ or $c=2$. Recalling $u=\alpha^{(p^m+1)j}$, we have $u=-1$ or $u=1$ hence $u+u^{-1}=-2$ or $u+u^{-1}=2$, so $\{u+u^{-1}: u\in\mathbb{F}_{p^m}^*\}\cap\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}: i\in\{1,\dots,p^m+1\}\}\subset\{2,-2\}$.

Conversely, let $u=1$ or $u=-1$. We get $u+u^{-1}=2$ or $u+u^{-1}=-2$. Let $i=(p^m+1)/2$ or $i=p^m+1$. By Proposition 3.1.1, we get $\gamma^{(p^m-1)i}=-1$ or $\gamma^{(p^m-1)i}=1$. So

$\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}=-2$ or 2. Thus $\{2,-2\}\subset\{u+u^{-1}:u\in\mathbb{F}^*_{p^m}\}\cap\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}:i\in\{1,\dots,p^m+1\}\}$.

So the result follows. □

Theorem 3.3.6. *Let α be a generator of $\mathbb{F}^*_{p^{2m}}$. Let $\gamma=\alpha^{(p^m-1)/2^k}$, where $2^kb=p^m-1$ for b odd and k positive integer. Then γ^{p^m-1} generates the cyclic subgroup of $(\mathbb{F}^*_{p^{2m}},\cdot)$ of order p^m+1.*

Proof. Let a be the order of γ^{p^m-1}. Since $\gamma^{(p^m-1)(p^m+1)}=1$, $a\le p^m+1$. We also have $\gamma^{(p^m-1)a}=\alpha^{(p^m-1)^2a/2^k}=1$. Thus $(p^{2m}-1)|((p^m-1)^2a/2^k)$. Hence $(p^m+1)|(p^m-1)a/2^k$. And $\gcd(p^m+1,\,(p^m-1)/2^k)=1$ implies that $(p^m+1)|a$. We have $a\le p^m+1$. Therefore, $a=p^m+1$ and γ^{p^m-1} generates the cyclic group of $\mathbb{F}_{p^{2m}}$ of order p^m+1. □

Theorem 3.3.7. *Let α be a generator of $\mathbb{F}^*_{p^{2m}}$. Let $\gamma=\alpha^{(p^m-1)/2^k}$, where $2^kb=p^m-1$ for b odd and k positive integer. Then $\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}\in\mathbb{F}_{p^m}$ for all $i\in\{1,\dots,p^m+1\}$ and $\{u+u^{-1}:u\in\mathbb{F}^*_{p^m}\}\cup\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}:i\in\{1,\dots,p^m+1\}\}=\mathbb{F}_{p^m}$.*

Proof. For u running through $\mathbb{F}^*_{p^m}$, when $u=u^{-1}$, $u=\pm1$ and $u+u^{-1}=-2$ or $u+u^{-1}=2$. There is exactly one $u\in\mathbb{F}^*_{p^m}$ such that $u+u^{-1}=2$ and there is exactly one $u\in\mathbb{F}^*_{p^m}$ such that $u+u^{-1}=-2$. On the other hand, $u\neq u^{-1}$ implies that for each $v\in\{u+u^{-1}:u\in\mathbb{F}^*_{p^m}\}\setminus\{2,-2\}$, there exist two distinct u such that $v=u+u^{-1}$. Hence $\#\{u+u^{-1}:u\in\mathbb{F}^*_{p^m}\}=(p^m-1-2)/2+2=(p^m+1)/2$.

If $\gamma^{(p^m-1)i}=\gamma^{-(p^m-1)i}$, then by $z=z^{-1}\Rightarrow z=\pm1$, $\gamma^{(p^m-1)i}=\pm1$ and

$$\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}=\pm2.$$

On the other hand, by Theorem 3.3.6, for distinct i, $\gamma^{(p^m-1)i}$ are distinct. For each $v\in\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}:i\in\{1,\dots,p^m+1\}\}\setminus\{2,-2\}$, there exist two distinct i such that $v=\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}$. So $\#\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}:i\in\{1,\dots,p^m+1\}\}=(p^m+1-2)/2+2=(p^m+3)/2$.

Now we want to prove $\{\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i}:i\in\{1,\dots,p^m+1\}\}$ is a subset of $\mathbb{F}_{p^m}$. For i in $\{1,\dots,p^m+1\}$,

$$\begin{aligned}&(\gamma^{(p^m-1)i}+\gamma^{-(p^m-1)i})^{p^m}\\&=\gamma^{(p^m-1)p^mi}+\gamma^{-(p^m-1)p^mi}\end{aligned}$$

$$
\begin{aligned}
&= \gamma^{(p^m-1)(p^m+1)i}\gamma^{-(p^m-1)i} + \gamma^{-(p^m-1)(p^m+1)i}\gamma^{(p^m-1)i} \\
&= \gamma^{-(p^m-1)i} + \gamma^{(p^m-1)i}.
\end{aligned}
$$

So by Theorem 1.3.1, $\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} \in \mathbb{F}_{p^m}$. Then $\{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in \{1, \ldots, p^m+1\}\}$ is a subset of $\mathbb{F}_{p^m}$.

Furthermore, $\{u + u^{-1} : u \in \mathbb{F}_{p^m}^*\} \cup \{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in \{1, \ldots, p^m+1\}\}$ is a subset of $\mathbb{F}_{p^m}$. By Theorem 3.3.5, $\#(\{u + u^{-1} : u \in \mathbb{F}_{p^m}^*\} \cup \{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in \{1, \ldots, p^m+1\}\}) = \#\{u + u^{-1} : u \in \mathbb{F}_{p^m}^*\} + \#\{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in \{1, \ldots, p^m+1\}\} - 2 = (p^m+1)/2 + (p^m+3)/2 - 2 = p^m$. So $\{u + u^{-1} : u \in \mathbb{F}_{p^m}^*\} \cup \{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in \{1, \ldots, p^m+1\}\} = \mathbb{F}_{p^m}$. □

Remark: The proof of the next theorem uses Theorem 2.3.1. We can do that because we can view $(\mathbb{F}_{p^{2m}}, +)$ as the vector space $\mathbb{F}_p^{2m}$ by Theorem 1.3.2 and function f defined in the following theorem satisfies the conditions of function defined in Theorem 2.3.1.

Charpin and Gong proved theorems about bent functions in the binary case. We prove an analogue of Theorem 7 [2] for the p-ary case.

It is not straightforward to generalize Theorem 7 [2] from binary to p-ary. Let α be a generator of $\mathbb{F}_{p^{2m}}$. In the binary case [2] uses $\gamma = \alpha^{2^m-1}$ to prove the statements. But in the p-ary case, we let $\gamma = \alpha^{(p^m-1)/2^k}$, where $p > 2$ and $p^m - 1 = 2^k b$ for positive integer k and odd integer b. We need 2^k for the p-ary case, because if we let $\gamma = \alpha^{p^m-1}$ for the p-ary case, then by Theorem 3.2.5, $\bigcup_{i=1}^{p^m+1} \gamma^i \mathbb{F}_{p^m}$ is a set of squares of elements in $\mathbb{F}_{p^{2m}}$, hence $\bigcup_{i=1}^{p^m+1} \gamma^i \mathbb{F}_{p^m} \neq \mathbb{F}_{p^{2m}}$.

Recall Section 1.4 for definition and properties of Dickson polynomials.

Theorem 3.3.8. *We assume $m > 1$. Let $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ be defined by*

$$f(x) = \sum_{r \in L_m} T_1^{2m}(\lambda_r x^{r(p^m-1)}),$$

where $\lambda_r \in \mathbb{F}_{p^m}$. Define the function $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ as

$$g(u) = \sum_{r \in L_m} T_1^m(\lambda_r D_r(u)), \tag{3.4}$$

where $D_r(u)$ is the Dickson polynomial over $\mathbb{F}_p$.

(a) When $p = 3$, f is hyperbent if and only if $\#\{u \in \mathbb{F}_{3^m} : g(u) = j\} - \#\{u + u^{-1} : u \in \mathbb{F}_{3^m}^* | g(u + u^{-1}) = j\} = (3^{m-1} - 1)/2$ for all $j \in \{1, 2\}$ and $g(1) = -g(2) \neq 0$.

(b) When $p > 3$, f is never bent.

Proof. Let α be a generator of $\mathbb{F}_{p^{2m}}^*$. Let $\gamma = \alpha^{(p^m-1)/2^k}$, where $2^k b = p^m - 1$ for b odd and k positive integer. For $j \in \mathbb{F}_p^*$, let

$$V_j = \{i \in \{1, \dots, p^m+1\} : g(\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i}) = j\},$$

let

$$A_j = \{\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i} : i \in V_j\},$$

and let

$$B_j = \{u + u^{-1} : u \in \mathbb{F}_{p^m}^* | g(u+u^{-1}) = j\}$$

and

$$C_j = \{z \in \mathbb{F}_{p^m} | g(z) = j\}.$$

At first, we will give outline of the proof. Step I: Prove f is hyperbent if and only if $\#V_j = p^{m-1}$ for all $j \in \mathbb{F}_p^*$. Step II Case I $p = 3$: we prove f is hyperbent if and only if $g(1) = -g(2) \neq 0$ and $\#C_j - \#B_j = (3^{m-1}-1)/2$ for all $j \in \{1, 2\}$. Step II Case II $p > 3$: f is never bent.

Step I: By Theorem 3.1.3, $\{\gamma^l \mathbb{F}_{p^m} : l = 1, 2, \dots, p^m+1\}$ is an m-spread of $(\mathbb{F}_{p^{2m}}, +)$. By Theorem 3.3.4, f is constant on $\gamma^l \mathbb{F}_{p^m}$ for $l = 1, 2, \dots, p^m+1$. By Theorem 2.3.9, Theorem 2.3.1 and Theorem 3.3.4, f is bent if and only if $\#\{i \in \{1, \dots, p^m+1\} : f(\gamma^i) = j\} = p^{m-1}$, for all $j \in \{1, 2, \dots, p-1\}$, where

$$f(\gamma^i) = \sum_{r \in L_m} T_1^m(\lambda_r(\gamma^{(p^m-1)ri} + \gamma^{-(p^m-1)ri})). \tag{3.5}$$

Let k be coprime to $p^{2m}-1$, hence k is coprime to p^m+1. Then the map $\gamma^i \to \gamma^{ik}$ is a permutation on the subgroup of $(\mathbb{F}_{p^{2m}}^*, \cdot)$ generated by γ. By Definition 1.7.3, Theorem 2.3.9 and Theorem 2.3.1, f is hyperbent if and only if $\#\{i \in \{1, \dots, p^m+1\} : f(\gamma^{ki}) = j\} = p^{m-1}$ for all $j \in \{1, 2, \dots, p-1\}$ and all k coprime to $p^{2m}-1$. This happens if and only if $\#\{i \in \{1, \dots, p^m+1\} : f(\gamma^i) = j\} = p^{m-1}$ for all $j \in \{1, 2, \dots, p-1\}$.

By Proposition 1.4.1, $f(\gamma^i) = g(\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i})$.

Hence $\#\{i \in \{1, \dots, p^m+1\} : f(\gamma^i) = j\} = p^{m-1}$ for all $j \in \{1, 2, \dots, p-1\}$ if and only if $\#\{i \in \{1, \dots, p^m+1\} : g(\gamma^{(p^m-1)i} + \gamma^{-(p^m-1)i}) = j\} = p^{m-1}$ for all $j \in \{1, 2, \dots, p-1\}$.

So far, we have proved that f is hyperbent if and only if $\#V_j = p^{m-1}$, for all $j \in \mathbb{F}_p^*$.

Step II Case I: Now we prove part (a). Note: $p = 3$ in part (a). Claim:f is hyperbent if and only if $\#A_j = (3^{m-1}+1)/2$ for all $j \in \{1,2\}$ and $g(1) = -g(2) \neq 0$. Proof of Claim: ($\Rightarrow$) Assume f is hyperbent. By the previous paragraph, $\#V_j = 3^{m-1}$ for all $j \in \{1,2\}$. For each element $t \in \{\gamma^{(3^m-1)i} + \gamma^{-(3^m-1)i} | i \in \{1,\dots,3^m+1\}\} \setminus \{1,2\}$, there exist exactly two distinct $i \in \{1,\dots,3^m+1\} \setminus \{3^m+1,(3^m+1)/2\}$ namely $i = h$ and $i = 3^m+1-h$ such that $t = \gamma^{(3^m-1)i} + \gamma^{-(3^m-1)i}$. Then the correspondence between t and i is one-to-two except for $h = 3^m+1$ or $h = (3^m+1)/2$ by Proposition 3.1.1 there is one-to-one correspondence between h and $\gamma^{(3^m-1)h} + \gamma^{-(3^m-1)h}$. We know that $\#V_j = 3^{m-1}$ for all $j \in \{1,2\}$. So A_j has to contain 2 or 1 but not both for all $j \in \{1,2\}$. Therefore, $g(1) = -g(2) \neq 0$. We also have following computations:

$$\begin{aligned}\#A_j &= (\#V_j - 1)/2 + 1\\ &= (3^{m-1}-1)/2+1\\ &= (3^{m-1}+1)/2.\end{aligned}$$

Now we prove ($\Leftarrow$). Assume for all $j \in \{1,2\}$, we have $\#A_j = (3^{m-1}+1)/2$ and $g(1) = -g(2) \neq 0$. We have for all $j \in \{1,2\}$

$$\begin{aligned}\#V_j &= 2(\#A_j - 1) + 1\\ &= 2((3^{m-1}+1)/2 - 1) + 1\\ &= (3^{m-1}-1) + 1 = 3^{m-1}.\end{aligned}$$

This finishes the proof of the claim. At this point, we have proved that for all $j \in \{1,2\}$, $\#V_j = 3^{m-1}$ if and only if $\#A_j = (3^{m-1}+1)/2$ and $g(1) = -g(2) \neq 0$.

Let us finish the proof of Step II Case I (part (a) of the theorem). By Theorem 3.3.7 and Theorem 3.3.5, $A_j \cup B_j = C_j$ for all $j \in \{1,2\}$. By inclusion and exclusion principle, for all $j \in \{1,2\}$, we have $\#(A_j \cup B_j) - \#B = \#A_j - \#(A_j \cap B_j) = \#A_j - 1$, hence $\#C_j - \#B_j = \#A_j - 1$. Using $g(1) = -g(2) \neq 0$, $A_j \cap B_j = \{1\}$ or $\{2\}$. Hence $\#V_j = 3^{m-1}$ if and only if $g(1) = -g(2) \neq 0$ and $\#C_j - \#B_j = (3^{m-1}+1)/2 - 1 = (3^{m-1}-1)/2$ for all $j \in \{1,2\}$.

Therefore, the result follows.

(b) If $p > 3$, there always exists j such that $\#V_j$ is even, since by Theorem 3.3.5 and the discussion above one of $g(-2)$ and $g(2)$ have to be equal to j if $\#V_j$ is odd for all $j \in \{1,\dots,p-1\}$ and there are more than 2 $j's$. So f is never bent.

□

There exist p-ary multinomial bent functions with $p > 3$ when we allow $\lambda_r \in \mathbb{F}_{p^{2m}}$, the larger field. Examples are showed in Appendix A.3.

For Theorem 3.3.8 we need the condition $g(1) = -g(2) \neq 0$. See Appendix A.4.

Let $N = p^m$. By using the fast Walsh transform, the time complexity for computing all Walsh coefficients of a function on $\mathbb{F}_{p^{2m}}$ is about $O(N^2 \log N)$. But by using Theorem 3.3.8, the time complexity for testing bentness is only about $O(N \log N)$.

When f is monomial, Corollary 3.3.9 shows a different proof of Theorem 2 in [9]. Although Corollary 3.3.9 is proved with $\lambda \in \mathbb{F}^*_{3^m}$, by Section 3.2.2, it is true that finding ternary monomial bent functions in our construction can be constrained to $\mathbb{F}_{3^m}$. Recall $K_{p^m}(d)$ is a Kloosterman sum. For $p > 3$ there do not exist p-ary monomial bent functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(x) = T_1^{2m}(\lambda_r x^{r(p^m-1)})$, because $K_{p^m}(a) \neq 0$ for each $a \in \mathbb{F}_{p^t}$ by [13]. So it is enough that we only prove for $\lambda_r \in \mathbb{F}^*_{3^m}$. All conditions in Theorem 2 [9] are the same as ours except their assumption is $\gcd(r, 3^m + 1) = 1$ and we use $\gcd(r, 3^{2m} - 1) = 1$, a bit stronger assumption. However, our proof is quite different. It uses the combinatorial setting of partial spreads as introduced by Dillon in the binary case and generalized to the p-ary case in Chapter 2 of this thesis, and then connected with the algebraic representation through Theorem 3.3.8. This combinatorial context is not apparent in [9].

Corollary 3.3.9. *Let $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ defined to be $f(x) = T_1^{2m}(\lambda_r x^{r(3^m-1)})$, where $\lambda_r \in \mathbb{F}^*_{3^m}$ and $\gcd(r, 3^{2m} - 1) = 1$. Then $f(x)$ is hyperbent if and only if the Kloosterman sum*

$$K_{p^m}(\lambda^{3^m+1}) = 0.$$

Proof. The function g is defined as Equation (3.4). Note: Here f is monomial hence we let $g(u) = T_1^m(\lambda_r D_r(u))$. Recall that Proposition 1.4.3 states that if $\gcd(r, 3^{2m} - 1) = 1$, then the Dickson polynomial $D_r : \mathbb{F}_{3^m} \to \mathbb{F}_{3^m}$ is a permutation. So by Theorem 1.3.6 and the bijective map: $x \mapsto \lambda_r x$, $\#\{u \in \mathbb{F}_{3^m} | g(u) = j\} = 3^{m-1}$ for all $j \in \mathbb{F}_3$.

By Theorem 3.3.8, f is hyperbent if and only if

$$3^{m-1} - \#\{u + u^{-1} : u \in \mathbb{F}^*_{3^m} | g(u + u^{-1}) = j\} = (3^{m-1} - 1)/2$$

for all $j \in \{1, 2\}$ and $g(1) = -g(2) \neq 0$. This holds if and only if $\#\{u + u^{-1} : u \in \mathbb{F}^*_{3^m}, g(u + u^{-1}) = j\} = (3^{m-1} + 1)/2$ for all $j \in \{1, 2\}$ and $g(1) = -g(2) \neq 0$. By Proposition 1.4.1, this holds if and only if $\#\{u \in \mathbb{F}^*_{3^m} : T_1^m(\lambda_r(u^r + u^{-r})) = j\} = 3^{m-1}$ for all $j \in \{1, 2\}$ and

$g(1)=-g(2)\neq 0$. By the bijection $u\mapsto u^r$, this holds if and only if $\#\{u\in\mathbb{F}_{3^m}^*: T_1^m(\lambda_r(u+u^{-1}))=j\}=3^{m-1}$ for all $j\in\{1,2\}$ and $g(1)=-g(2)\neq 0$.

Note: By the bijection $u\mapsto\lambda_r u$, we have $\{u+u^{-1}: u\in\mathbb{F}_{3^m}^*\}=\{\lambda_r u+(\lambda_r u)^{-1}: u\in\mathbb{F}_{3^m}^*\}$ for $\lambda_r\in\mathbb{F}_{3^m}^*$. At this point, we proved that f is hyperbent if and only if $\#\{u\in\mathbb{F}_{3^m}^*: T_1^m(\lambda_r(\lambda_r u+(\lambda_r u)^{-1}))=j\}=3^{m-1}$ for all $j\in\{1,2\}$ and $g(1)=-g(2)\neq 0$.

We have $\lambda_r^{3^m+1}=\lambda_r^{3^m-1+2}=\lambda_r^2$.

Now let us finish the proof for $\lambda\in\mathbb{F}_{3^m}$ by proving both directions separately. Assume f is hyperbent. Let ζ_3 be the third root of unity. Then by the previous paragraph $\#\{u\in\mathbb{F}_{3^m}^*: T_1^m(u^{-1}+\lambda_r^2 u)=j\}=3^{m-1}$ for all $j\in\{1,2\}$ and $\#\{u\in\mathbb{F}_{3^m}^*: T_1^m(u^{-1}+\lambda_r^2 u)=0\}=3^m-1-2\cdot 3^{m-1}=3^{m-1}-1$. So $K_{p^m}(\lambda_r^{3^m+1})=\sum_{c\in\mathbb{F}_{3^m}}\zeta_3^{T_1^m(\lambda_r^{3^m+1}c+c^{-1})}=3^{m-1}-1+1+3^{m-1}\zeta_3+3^{m-1}\zeta_3^2=0$.

On the other hand, assume $K(\lambda_r^{3^m+1})=0$. We have $h_0+h_1\zeta_3+h_2\zeta_3^2=0$, where h_i is the number of $c\in\mathbb{F}_{3^m}^*$ such that $T_1^m(c^{-1}+\lambda_r^{3^m+1}c)=i$ for $i\in\{0,1,2\}$. It is well-known that the polynomial $h(x)=x^2+x+1$ is irreducible over the rational number field and $h(\zeta_3)=0$. Thus $h(x)$ is the minimal polynomial of ζ_3 over the rational numbers. Let $h'(x)=h_0+h_1x+h_2x^2$. Then $h'(x)$ is a polynomial of degree 2 and $h'(\zeta_3)=0$. So $h'(x)$ is a constant multiple of $h(x)$. Hence $h_0=h_1=h_2$. We have $h_0+h_1+h_2=3^m$. So $h_0=h_1=h_2=3^{m-1}$. Thus $\#\{u\in\mathbb{F}_{3^m}^*: T_1^m(u^{-1}+\lambda_r^2 u)=j\}=3^{m-1}$ for all $j\in\{1,2\}$. By Theorem 1.4 in [7], if $K(\lambda_r^2)=0$ then $\lambda_r^2=0$ or $T_1^m(\lambda_r)\neq 0$. We also have $1=2^r+2^{-r}$ and $2=1+1^{-1}$. So by Proposition 1.4.1 and r odd, $g(1)=g(2+2^{-1})=T_1^m(\lambda_r(2^r+2^{-r}))=T_1^m(\lambda_r)$ and $g(2)=g(1+1^{-1})=T_1^m(\lambda_r(1^r+1^{-r}))=-T_1^m(\lambda_r)$. Hence $g(1)=-g(2)\neq 0$.

Therefore, the result follows. □

3.4 Conclusion

We have generalized the combinatorial construction of binary bent functions that is proved by Dillon in [4] to the p-ary case. We have also generalized the algebraic construction of binary multinomial bent functions that is proved by Charpin and Gong in [2] to p-ary multinomial bent functions.

In the non-binary case, we extended the algebraic construction of Helleseth and Kholosha [9], which is now known to work only for $p\leq 3$ (see the previous section). For illustration, these references are summarized in Figure 3.1.

	monomial bent functions	multinomial bent functions
$p=2$	Dillon (1974) [4]	Charpin, Gong (2008) [2]
$p>2$	Helleseth, Kholosha (2006) [9]	this thesis

Figure 3.1: Literature on bent functions with Dillon type exponents

Appendix A

Magma code and Maple code

A.1 Simplified A5/1 Attack

```
# This is an attack on a simplified
# version of the A5/1 cipher for GSM.

# the length of the keystream
L:=10^3:

# output of the top LFSR
for i from 20 to L do
a[i]:=(a[i-14]+a[i-17]+a[i-18]+a[i-19]) mod 2:
od:

# output of the middle LFSR
for i from 23 to L do
b[i]:=(b[i-21]+b[i-22]) mod 2:
od:

# output of the bottom LFSR
for i from 24 to L do
```

```
c[i]:=(c[i-8]+a[i-21]+a[i-22]+a[i-23]) mod 2:
od:


# keystream generated for use by the A5/1 cipher
for i from 1 to L do
z[i]:=(a[i]+b[i]+c[i]) mod 2:
od:


# The shared secret between the communicating parties
# are the values of the bits in the three registers:
# a[1],...,a[19],b[1],..,b[22],c[1],...,c[23]


# Suppose that z[1],z[2],...,z[64] were obtained
# say by a plaintext attack.

random_bit:=rand(0..1):

# We could plant the shared secret and
# compute the z[i]'s from it to simulate what
# really happens.  Let us shorten the computation
# by trying to attack random data:

equations := { seq( z[i]=random_bit(), i=1..64 ) }:
sol:=msolve(equations,2);
```

The output of this Maple code is:

$a[1] = 1, a[2] = 0, a[3] = 1, a[4] = 0, a[5] = 0, a[6] = 0, a[7] = 0,$
$a[8] = 1, a[9] = 0, a[10] = 1, a[11] = 0, a[12] = 1, a[13] = 1, a[14] = 0, a[15] = 0,$

$a[16]=1,a[17]=0,a[18]=1,a[19]=1,b[1]=1,b[2]=1,b[3]=1,b[4]=0,$
$b[5]=1,b[6]=1,b[7]=0,b[8]=1,b[9]=0,b[10]=1,b[11]=0,b[12]=0,$
$b[13]=0,b[14]=1,b[15]=0,b[16]=1,b[17]=1,b[18]=1,b[19]=0,$
$b[20]=0,b[21]=1,b[22]=1,c[1]=0,c[2]=1,c[3]=0,c[4]=0,c[5]=0,$
$c[6]=0,c[7]=1,c[8]=0,c[9]=1,c[10]=1,c[11]=1,c[12]=1,c[13]=0,$
$c[14]=1,c[15]=0,c[16]=0,c[17]=1,c[18]=1,c[19]=0,c[20]=0,c[21]=0,$
$c[22]=0,c[23]=0$

A.2 A Special Case in Theorem 2.3.9

The following Magma code finds coefficients of binomial ternary bent functions of the type studied in Chapter 3, with $m=1$ and $L_m=\{1,2\}$ using the definition of bent function:

```
m:=1;
n:=2*m;
p:=3;
w:=RootOfUnity(3);
Fn<om>:=GF(p^n);
Fm<al>:=sub< Fn | m >;
F3:=sub< Fn | 1 >;
Fks:={ x : x in Fm | x ne 0};
Z:=Integers();
Walsh_transform_binomial:=function(a1,a2,b)
return &+[ w^( Z!(
Trace( a1*x^(p^m-1)+ a2*x^(2*(p^m-1))     )-Trace(b*x)
)
) : x in Fn ];
end function;
// square of the absolute value
SqAbs:=function(z)
return z*ComplexConjugate(z);
end function;
```

```
Is_bent_binomial:=function(a1,a2)
is_bent:=true;
for b in Fn do
if is_bent then
 is_bent := SqAbs( Walsh_transform_binomial(a1,a2,b) )
eq 3^n;
end if;
end for;
return is_bent;
end function;
Walsh_spectrum_binomial:=function(a1,a2)
return { Walsh_transform_binomial(a1,a2,b) : b in Fn };
end function;
bent_coeffs:={};
non_bent_coeffs:={};
for a1 in Fm do
for a2 in Fm do
if Is_bent_binomial(a1,a2)
then bent_coeffs := bent_coeffs join { [a1,a2] };
else
non_bent_coeffs := non_bent_coeffs join { [a1,a2] };
end if;
end for;
end for;
bent_coeffs;
```

This code produces $\{[1,0],[2,0],[0,2],[0,1]\}$, which is the set of coefficients of bent functions.

Let us take the last of these four examples, that is the bent function $f(x) = T_1^2(x^4)$ on $\mathbb{F}_9$. Since $x \mapsto x^4$ maps any element of $\mathbb{F}_9^*$ to 1 or -1, we see that $f(x) = 0$ exactly if $x = 0$, and hence this function can not be covered by Theorem 2.3.9.

A.3 Examples of Multinomial Bent Functions for $p = 5$

We give examples of binomial bent functions on $\mathbb{F}_{5^2}$, $\mathbb{F}_{5^4}$, $\mathbb{F}_{5^6}$ found using Theorem 2.3.1.

```
p:=5;

SqAbs:=function(z)
return z*ComplexConjugate(z);
end function;

w:=RootOfUnity(p);

for m:=1 to 3 do

n:=2*m;
Fp:=GF(p);
Fpm:=GF(p^m);
Fpn:=GF(p^n);

Fpns:=Set(Fpn) diff {0};
Fpms:=Set(Fpm) diff {0};
Fps:=Set(Fp) diff {0};

reps:={};
todo:=Fpns;

while todo ne {} do
rep:=Random(todo);
reps := reps join {rep};
todo := todo diff { rep*x : x in Fpms };
end while;

found:=false;
```

```
while not found do

b1:=Random(Fpn);
b2:=Random(Fpn);

f:=function(x)
return Trace( b1*x^(p^m-1) + b2*x^(2*(p^m-1)) );
end function;

if {* f(r) : r in reps *}
eq {* 0^^(p^(m-1)+1) *} join {* x^^(p^(m-1)) : x in Fps *}

then printf "p=%o n=%o b1=%o b2=%o\n",p,n,b1,b2;

found:=true;

end if;

end while;

end for;
```

The code produces:

```
p=5 n=2 b1=Fpn.1^10 b2=4
p=5 n=4 b1=Fpn.1^57 b2=Fpn.1^261
p=5 n=6 b1=Fpn.1^12137 b2=Fpn.1^12419
```

A.4 Example for Theorem 3.3.8

This code shows that the condition $g(1) = -g(2) \neq 0$ in Theorem 3.3.8 is necessary.

```
 m:=2;
 p:=3;
 Fn<om>:=GF(p^(2*m));
 Fm<al>:=sub<Fn|m>;
 Fms:=Set(Fm) diff {0};
 W:={u+u^(-1): u in Fms};
 a1:=1;a2:=al^5;

 g:=function(u)
function> return Trace(a1*u^3+a2*(u^2-2));
function> end function;

 C1:={u: u in W|g(u) eq 1};
 C2:={u: u in W|g(u) eq 2};
 B1:={u: u in Fms|g(u) eq 1};
 B2:={u: u in Fms|g(u) eq 2};
 #B1-#C1 eq (p^(m-1)-1)/2 and #B2-#C2 eq (p^(m-1)-1)/2;
true
>
> g(1);
0
> g(2);
2
```

This example satisfies the first condition of Theorem 3.3.8 but it does not satisfy the second condition of the theorem. Hence in general, the second condition is not implied by the first condition.

Bibliography

[1] T. Beth, D. Jungnickel, H. Lenz, Design Theory. University of Cambridge, 1986.

[2] P. Charpin, G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials. IEEE Trans. Inform. Theory 54 (2008), no. 9, 4230–4238.

[3] J. A. Davis, Construction of relative difference sets in p-groups. Discrete Math., 103 (1992), no. 1, 7–15.

[4] J. F. Dillon, Elementary Hadamard Difference Sets. PhD thesis, University of Maryland, 1974.

[5] J. Eisfeld, L. Storme, (Partial) t-spreads and minimal t-covers in finite projective spaces. Lecture notes for the Socrates Intensive Course on Finite Geometry and its Applications, University of Ghent, 3–14 April 2000.

[6] J. E. H. Elliot, A. T. Butson, Relative difference sets. Illinois J. Math. 10 (1966), 517–531.

[7] K. Garaschuk, P. Lisonek, On ternary Kloosterman sums modulo 12. Finite Fields and Their Applications 14 (2008), 1083–1090.

[8] G. Gong, S. W. Golomb, Transform domain analysis of DES. IEEE Trans. Inform. Theory 45 (1999) no. 6, 2065–2073.

[9] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory 52 (2006), no. 5, 2018–2032.

[10] T. Helleseth, A. Kholosha, On generalized bent functions. Information Theory and Applications Workshop, University of California, San Diego, February 2010.

[11] K. Hoffman, R. Kunze, Linear Algebra, second addition. Prentice Hall, 1971.

[12] D. Jungnickel, On automorphism groups of divisible designs. Canad. J. Math. 34 (1982) 257–297.

[13] K. Kononen, K. P. Rinta-aho, M. J. Vaananen, On integer values of Kloosterman sums. IEEE Trans. Inform. Theory 56 (2010), issue 8, 4011–4013.

[14] P. V. Kumar, R. A. Scholtz, L. R. Welch, Generalized bent functions and their properties. J. Combin. Theory Ser. A 40 (1985), no. 1, 90–107.

[15] R. Lidl, G. L. Mullen, G. Turnwald, Dickson polynomials. Longman Scientific & Technical, copublished in United States with John Wiley & Sons, 1993.

[16] R. Lidl, H. Niederreiter, Finite fields. Second edition. Encyclopedia of Mathematics 20. University of Cambridge, 2003.

[17] S. L. Ma, B. Schmidt, On (p^a, p, p^a, p^{a-1})-relative difference sets. Des. Codes Cryptogr. 6 (1995), no. 1, 57–71.

[18] K. Nohl, C. Paget, GSM: SRSLY 26th Chaos Communication Congress. http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html Retrieved 24 May 2011.

[19] N. J. Patterson, D. H. Wiedemann. The covering radius of the (2^{15}, 16) Reed-Muller code is at least 16276. IEEE Trans. Inform. Theory 29 (1983), no. 3, 354–356.

[20] O. S. Rothaus, On "bent" functions. J. Comb. Theory Ser. A vol. 20, no. 3, pp. 300–305, 1976.

[21] D. Stinson, Cryptography: Theory and Practice. Chapman & Hall/CRC, 2006.

[22] Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. J. Combin. Theory Ser. A 117 (2010), no. 6, 668–682.

[23] A. M. Youssef, G. Gong, Hyper-bent functions. EUROCRYPT 2001. Lecture Notes in Comput. Sci., Vol. 2045, pp. 406–419, Springer, Berlin, 2001.