Vectorial Bent Functions in Characteristic Two

by

Lucien Lapierre

B.Sc., Thompson Rivers University, 2013

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Spring 2016

Approval

Name:	**Lucien Lapierre**
Degree:	**Master of Science (Mathematics)**
Title:	***Vectorial Bent Functions in Characteristic Two***
Examining Committee:	**Chair:** Dr. Marni Mishna Associate Professor

Dr. Petr Lisonek
Senior Supervisor
Professor _____

Dr. Jonathan Jedwab
Supervisor
Professor _____

Dr. Nathan Ilten
Internal Examiner
Assistant Professor _____

Date Defended: February 2, 2016

Abstract

We study Dillon-type vectorial bent functions of the monomial and multinomial varieties. We also study Kloosterman sums, which relate to the construction of Dillon-type monomial bent functions.

For Dillon-type monomial functions we give sufficient conditions for vectorial bentness, leading to the construction of several new examples. We give useful necessary conditions for functions from $GF(2^{4m})$ to $GF(4)$. We give new restrictions on the maximum output dimension of Dillon-type monomial bent functions on $GF(2^{4m})$. We subsequently show that certain Dillon-type multinomial bent functions do not meet the Nyberg bound. We give computational results regarding Dillon-type functions from $GF(2^{4m})$ to $GF(4)$, suggesting that while bent monomials of this type appear to be rare, their binomial counterparts seem to be relatively abundant. Finally, we give divisibility results on Kloosterman sums valued on cosets of certain subfields of $GF(2^m)$, leading to explicit constructions of Kloosterman zeros and Dillon-type monomial bent functions.

Keywords: Cryptography, Bent function, Boolean function, Dillon, Kloosterman sum, Vectorial bent function.

Acknowledgements

I thank the Department of Mathematics at Simon Fraser University for giving me the opportunity to study and grow in such a compelling environment. I also thank them for their support via the Graduate Fellowship and numerous teaching appointments. I thank NSERC for making possible my Research Assistantships through Dr. Petr Lisonek's grant.

I thank my supervisor Dr. Petr Lisonek for guiding me through an engaging research experience, for thorough and constructive critique of my work, and for the wealth of advice he has provided to me during my time at SFU.

I thank the members of the Examining Committee for their diligent review of my work and helpful suggestions for its improvement.

I thank the members of CECM for providing a positive working environment, and my fellow graduate students for camaraderie and interesting discussions on various topics. I thank Stefan Trandafir for numerous mathematical "jam sessions", some of which led to important breakthroughs. I thank Dr. Renée Lapierre for her careful proofreading of my writing.

Finally, I thank Queenie Liaw for her continual love and support throughout the 2 1/2 year project that was my pursuit of a Master's degree.

Table of Contents

List of Tables

List of Figures

Chapter 1

Background

In this chapter we motivate the study of bent functions and give some necessary background.

1.1 Introduction

In 1966, O.S. Rothaus introduced what he called "bent functions" in an unpublished technical report, where he defined them as Boolean functions that achieve maximum non-linearity. This was the first work in English on the subject (V.A. Eliseev and O.P. Stepchenkov had introduced a similar notion into the Soviet mathematical literature in the early 1960's, though their work apparently remains classified to this day [65]). Rothaus' work would not be made public until 1976 [61]. In the meantime, a seminal work on the subject had appeared as a part of the 1972 Ph.D. thesis of J.F. Dillon [21]. In 1985, the notion of a bent function was extended to characteristics other than two by Kumar, Scholtz, and Welch [37]. Nyberg subsequently defined what it meant for a vector-valued function to be bent in 1991 [56].

In the modern sense, a bent function is a vector-valued function on a finite vector space that is as different as possible from any affine mapping with the same domain and range. There are numerous equivalent ways to characterize the bent property depending on context (see e.g. [12, Section 8.6], [21, Section 6.1], and especially [65, Chapter 6]). Bent functions exist for finite vector spaces of any positive characteristic [37]. In this thesis, however, we will only consider the case of characteristic two.

Academic study of the cryptographic properties and applications of Boolean bent functions began in earnest in 1989, when Meier and Staffelbach studied linear approximations of Boolean functions used in *stream ciphers* [65, Foreword], [50]. The application of a stream cipher involves generating a pseudorandom sequence of equal length to the plaintext, and then combining this sequence with the plaintext via bit-wise addition to produce the ciphertext.

One could argue that vectorial extensions of the Boolean bent functions have had the greater impact on modern cryptology, where multiple-output functions resistant to *linear cryptanalysis* and *differential cryptanalysis* hold great interest. Linear cryptanalysis, introduced by Matsui in 1993 [49], refers to cryptanalytic attacks that involve the construction of affine approximations to the actions of a cipher. Among all vectorial functions, bent functions are by definition the most difficult to approximate via affine functions, and therefore lend resistance to these attacks. Differential cryptanalysis refers to attacks that seek to infer secret information by studying how differences in the input of a given cipher affect differences in the output. The first published work on differential cryptanalysis is the 1990 paper of Biham and Shamir [6], though it has since been revealed that the technique was known to the developers of the Data Encryption Standard (DES) at least 16 years prior. Vectorial bent functions are also resistant to differential cryptanalysis, as they have the property that the addition of any non-zero vector to the input induces a change in exactly half of the outputs [16].

Specific attacks of the kinds described above have been developed for both stream ciphers and *block ciphers*. A block cipher may be viewed as a permutation of a finite field (or a finite ring) that is the composition of multiple permutations in a subfield (or subring). An important class of block ciphers are the *substitution-permutation network* (SPN) ciphers, which employ *substitution boxes* (S-boxes) as non-linear components. An S-box is a function that maps an n-bit input to an m-bit output in such a way so as to obscure the relationship between the ciphertext and the method used to generate it. S-boxes having the property that every linear combination of the outputs corresponds to a Boolean bent function of the inputs are called "perfect S-boxes", and these correspond exactly with vectorial bent functions [56]. SPN ciphers that use S-boxes based on bent functions are immune to the differential cryptanalysis of Biham and Shamir [2].

The development of the S-boxes used in the ubiquitous Advanced Encryption Standard (AES) benefited greatly from early advances in the study of vectorial bent functions [65, Foreword]. Another prominent example lies in the design of the S-boxes used in the CAST-128 block cipher of Adams and Tavares [3]. First published in 1996, the CAST-128 cipher is used as the default cipher in many notable cryptographic software packages, and has also been approved for Canadian government use by the Communications Security Establishment (CSE) [1]. CAST-128 contains four distinct 8-bit to 32-bit S-boxes, each of which can be represented by a collection of Boolean functions $f_i^{(j)}$, $i = 1, \ldots, 32$, $j = 1, \ldots, 4$. The CAST-128 S-boxes have the property that all such functions $f_i^{(j)}$ are bent; furthermore, for each j, all linear combinations of the functions $f_i^{(j)}$ are themselves highly non-linear functions (they are not quite bent, due to other considerations in the selection of the S-boxes [1]).

Interest in bent functions is not limited to cryptography: they have also found applications in coding, for the construction of maximum-length sequences with good autocorrelation and cross-correlation properties [27], in combinatorial design, for the construc-

tion of difference sets and Hadamard matrices [21], and in graph theory, for the construction of distance-regular graphs [5]. The reader is referred to [65, Chapter 4] for a comprehensive overview of the applications of bent functions.

A complete classification of all bent functions currently appears to be an insurmountable task [42]. Nevertheless, there exist multiple constructions of various types and subtypes. There are two main approaches to the construction and study of bent functions: combinatorial and algebraic [65, Chapters 8 and 9]. In this thesis we take only the algebraic perspective.

Certainly one of the most heavily researched classes of bent functions is the class of monomial bent functions, which admit a representation of the form $x \mapsto Tr(ax^d)$ (this notation will be explained shortly). There are five known classes of monomial bent functions, each named for its discoverer(s): Gold, Dillon, Kasami, Leander, and Canteaut-Charpin-Kyureghyan (denoted as CCK below). The Boolean functions in these classes are described in Table 1.1 below, which is transcribed from [70]. Exhaustive computer searches have shown that every Boolean monomial bent function of dimension 24 or less belongs to one of these five classes [40], with consideration given up to the appropriate level of equivalence.

A short note on the notation used in Table 1.1: the notation $\mathbb{F}_{2^n}$ denotes the Galois field $GF(2^n)$ containing 2^n elements. The notation $Tr_1^n(x)$ denotes the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The notation $N_{n/2}^n(x)$ denotes the *norm function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{n/2}}$ (where n is assumed to be even). Both the trace and the norm will be formally introduced in Section 1.3. Finally, $\mathcal{K}_{2^{n/2}}(x)$ denotes the *Kloosterman sum* over $\mathbb{F}_{2^{n/2}}$ at the point x. This will be formally introduced in subsection 2.2.2.

Table 1.1: Boolean Monomial Bent Functions of the Form $Tr_1^n(ax^d)$

Class	Exponent d	Condition on d	Condition on a	Section/ reference
Gold	2^s+1	$s \in \mathbb{N}$	$a \notin \{x^d : x \in \mathbb{F}_{2^n}\}$	2.2.1/ [27], [42]
Dillon	$l(2^{n/2}-1)$	$\gcd(l, 2^{n/2}+1) = 1$	$\mathcal{K}_{2^{n/2}}(N_{n/2}^n(a)) = 0$	2.2.2/ [21], [42]
Kasami	$2^{2s}-2^s+1$	$\gcd(3,n) = \gcd(s,n) = 1$	$a \notin \{x^3 : x \in \mathbb{F}_{2^n}\}$	–/ [22], [42]
Leander	$(2^s+1)^2$	$n = 4s$, s odd	$a \in (\mathbb{F}_4 \backslash \mathbb{F}_2) \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$	–/ [42]
CCK	$2^{2s}+2^s+1$	$n = 6s$, $s \geq 2$	$a \in \{x^d : x \in \mathbb{F}_{2^n}^*\}$ $\cdot\{\rho : Tr_s^{3s}(\rho) = 0, \rho \in \mathbb{F}_{2^{3s}}^*\}$	–/ [11]

Though not as heavily studied as their monomial counterparts, multinomial bent functions have also enjoyed a fair amount of recent attention (see e.g. [17], [47], [51], [54], [55], and [60]). Two classes of such functions are presented in Table 1.2 below. The first is a multinomial generalization of the monomial Dillon functions, characterized by Charpin and Gong in [17]. The second is a class of binomial functions discovered quite recently by Pott, Pasalic, Muratović-Ribić, and Bajrić (PPMB), described in [60].

Table 1.2: Two Classes of Boolean Multinomial Bent Functions

Class	Description	Conditions	Section/ reference
Charpin-Gong	$Tr_1^{2m}\left(\sum_{r\in\mathbb{Z}}\beta_r x^{r(2^m-1)}\right)$, $\beta_r\in\mathbb{F}_{2^m}$	see Theorem 2.2.40	2.2.3/ [17]
PPMB	$Tr_1^{2m}(\lambda x^{2^i+1}+\lambda x^{2^m+2^i})$, $\lambda\in\mathbb{F}_{2^{2m}}$	$\lambda\notin\mathbb{F}_{2^m}$, $i\in\{0,1,\ldots,m-1\}$	4.4.3/ [60]

The goal of this thesis is to communicate several new results on *vectorial* bent functions, that is, bent functions that are valued in vector spaces over $\mathbb{F}_2$. This communication is aimed at the general mathematical audience. At this point we wish to alert the reader that our main results are presented in a much more succinct manner in the forthcoming publication [41].

The thesis is divided into four chapters: two introductory chapters, and two chapters concerning original work. The main purpose of the first two chapters is to provide context for the second two.

The first chapter provides a brief introduction to the study of bent functions (which the reader has already seen), as well as some preliminary material on finite fields of characteristic two (which follows in the next section). The start of the second chapter deals with the fundamentals of bent functions as studied in the context of these fields. The chapter then transitions to providing a more specific context for the original material presented in the third and fourth chapters.

In the third chapter we present our original work. All of our results are related to vectorial generalizations of the Dillon functions described in Table 1.1, and of the Charpin-Gong functions described in Table 1.2. Parallel to our investigation of these functions, we present several new results on a class of exponential sums, the famous *Kloosterman sums*.

The fourth and final chapter is an open-ended discussion of future research, where we discuss the prospects of extending our results, methods for doing so, and computational results. We conclude the chapter with a list of conjectures, each of which is supported by computational evidence that is provided in the appendices.

1.2 The Study of Bent Functions on Finite Fields

Throughout this thesis (with the exception of section headings) we will denote by $\mathbb{F}_{2^n}$ the finite Galois field $GF(2^n)$ consisting of 2^n elements. This is not to be confused with the notation $\mathbb{F}_2^n$, which we will use to denote the n-dimensional vector space over $GF(2)$.

Bent functions are formally defined as mappings on finite vector spaces [56]. However, the discussion and study of bent functions can be re-cast in the setting of finite fields by virtue of the isomorphism that exists between $\mathbb{F}_2^n$ and the additive group of $\mathbb{F}_{2^n}$ [44, Exercise 2.36]. This is often done in the literature, particularly when one wishes to consider algebraic constructions of bent functions [12, Section 8.2]. Therefore we will hereby identify the vector space $\mathbb{F}_2^n$ with the additive group of $\mathbb{F}_{2^n}$. Among the advantages that this affords us is not only ease of expression and simplification of formulae, but also the use of the properties of the trace function (see Theorem 1.3.9). Additionally, this approach allows us to take advantage of the multiplicative structure of $\mathbb{F}_{2^n}$, where we may easily consider such objects as multiplicative cosets of subfields and the like.

Nevertheless, we stress that the full structure of a finite field is not necessary for the study of bent functions. Indeed, generalizations of bent functions sharing many of the key properties of the original formulation have been defined over algebraic structures more general than finite vector spaces (see e.g. [14]).

The main reference for the following comments is [44, Chapter 10, Section 1].

In practice we achieve an explicit construction of $\mathbb{F}_{2^n}$ by using polynomials over $\mathbb{F}_2$. To construct the field $\mathbb{F}_{2^n}$, one finds an irreducible polynomial $P(x) \in \mathbb{F}_2[x]$ having degree n (this may be done in a variety of ways, see e.g. [44, Chapter 3, Section 3]). One then considers the ring of polynomials over $\mathbb{F}_2$ modulo $P(x)$, where the summation and multiplication of polynomials is defined in the usual way (the product of two polynomials is always taken modulo $P(x)$, of course). This ring, denoted $\mathbb{F}_2[x]/\langle P(x)\rangle$, has the structure of the finite field of order 2^n. Each polynomial $a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n \in \mathbb{F}_2[x]/\langle P(x)\rangle$, $a_i \in \mathbb{F}_2$ corresponds naturally with the vector $(a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{F}_2^n$.

1.3 Results on Finite Fields of Characteristic Two

In this section we review some basic definitions and theorems necessary to study vectorial bent functions in characteristic two. Namely, we establish some important properties of finite fields of characteristic two, and of functions defined on such fields. Almost all of the material pertaining to the former can be found in the text [44] by Lidl and Niederreiter, which provides an excellent in-depth treatment of finite fields. A comprehensive quick reference is provided by the handbook [53], edited by Mullen and Panario. For material pertaining more specifically to functions we have used [12] and [28] as the primary references.

The theorem below is an amalgamation of statements given in [44]. It gives a collection of fundamental properties of the field $\mathbb{F}_{2^n}$. Throughout this thesis we will make extensive use of these properties, often without explicit reference.

Theorem 1.3.1 ([44])**.** *The finite field $\mathbb{F}_{2^n}$ exhibits the following properties:*

i. [44, Corollary 1.45] For any $\alpha \in \mathbb{F}_{2^n}$ we have $\alpha + \alpha = 0$.

ii. [44, Lemma 2.4] In $\mathbb{F}_{2^n}[x]$ we have

$$x^{2^n} - x = \prod_{\alpha \in \mathbb{F}_{2^n}} (x - \alpha).$$

Consequently, for any α residing in an extension field of $\mathbb{F}_{2^n}$ we have $\alpha \in \mathbb{F}_{2^n}$ if and only if $\alpha^{2^n} = \alpha$. A secondary consequence is that for all non-zero $\alpha \in \mathbb{F}_{2^n}$ we have $\alpha^{2^n-1} = 1$ and $\alpha^{-1} = \alpha^{2^n-2}$.

iii. [44, Theorem 1.46] For any $\alpha, \beta \in \mathbb{F}_{2^n}$ we have $(\alpha + \beta)^2 = \alpha^2 + \beta^2$.

iv. [44, Theorem 2.6] For every positive integer m that divides n, $\mathbb{F}_{2^n}$ contains a unique subfield of order 2^m. In this case $\mathbb{F}_{2^n}$ is called the extension of $\mathbb{F}_{2^m}$ of degree n/m*. Conversely, every subfield of $\mathbb{F}_{2^n}$ has order 2^m for some m dividing n.*

v. [44, Theorem 2.14 & following remarks] Let $m|n$. For $\alpha \in \mathbb{F}_{2^n}$, let $\phi(x) \in \mathbb{F}_{2^m}[x]$ be the non-zero polynomial of lowest degree d such that $\phi(\alpha) = 0$ (the minimal polynomial of α over $\mathbb{F}_{2^m}$*). Then*

$$\{x \in \mathbb{F}_{2^n} : \phi(x) = 0\} = \{\alpha^{2^{im}} : 0 \leq i \leq n/m - 1\}.$$

The elements $\alpha, \alpha^{2^m}, \ldots, \alpha^{2^{n-m}}$ are called the conjugates of α over $\mathbb{F}_{2^m}$*. If $d = n/m$ then these elements are distinct, otherwise each conjugate is repeated $\frac{n/m}{d}$ times.*

vi. [44, remarks following Definition 2.22] Let $m|n$. For $\alpha \in \mathbb{F}_{2^n}$, the polynomial

$$\prod_{i=0}^{n/m-1} \left(x - \alpha^{2^{im}}\right),$$

called the characteristic polynomial of α over $\mathbb{F}_{2^m}$*, is a power of the minimal polynomial of α over $\mathbb{F}_{2^m}$. The two polynomials are equal if and only if $\mathbb{F}_{2^n}$ is the smallest extension of $\mathbb{F}_{2^m}$ that contains α.*

vii. [44, Theorem 2.8] There exists a primitive element $\gamma \in \mathbb{F}_{2^n}$ *such that*

$$\{x \in \mathbb{F}_{2^n} : x \neq 0\} = \{\gamma^i : 0 \leq i \leq 2^n - 2\}.$$

The minimal polynomial over $\mathbb{F}_2$ of such an element is said to be primitive. *The set of all primitive elements in $\mathbb{F}_{2^n}$ is $\{\gamma^t : \gcd(t, 2^n - 1) = 1\}$.*

Throughout the thesis, we will most often denote the cardinality of a set A by $\#A$. We will only use the notation $|A|$ for this purpose when A is the pre-image of a function: for example, if b is an element in the range of a function f then the cardinality of the pre-image $f^{-1}(b)$ will be denoted by $|f^{-1}(b)|$.

We denote by $\mathbb{F}_{2^n}^*$ the *multiplicative group of* $\mathbb{F}_{2^n}$, which consists of all the non-zero elements of $\mathbb{F}_{2^n}$. By property (*vii*) above, this group is cyclic. Additionally, for $n > 1$ we obtain from property (*ii*) and Vieta's Rule that $\sum_{x \in \mathbb{F}_{2^n}^*} x = 0$ (this can also be seen via property (*vii*) by computing the sum $1 + \gamma + \ldots + \gamma^{2^n-2}$).

The following proposition describes the action of a monomial on the elements of $\mathbb{F}_{2^n}^*$. This is important since many of the functions we study in this thesis are described by monomials.

Proposition 1.3.2. *Let $t \in \mathbb{Z}$. The image of $\mathbb{F}_{2^n}^*$ under the mapping $x \mapsto x^t$ is the set $\{x^{\gcd(t,2^n-1)} : x \in \mathbb{F}_{2^n}^*\}$. Furthermore, this set has size $\frac{2^n-1}{\gcd(t,2^n-1)}$.*

Proof. Let $d = \gcd(t, 2^n - 1)$. Then there exist $a, b \in \mathbb{Z}$ such that $d = at + b(2^n - 1)$. Let $\gamma \in \mathbb{F}_{2^n}^*$ be primitive. Since every element of $\mathbb{F}_{2^n}^*$ is a power of γ, to show that $\{x^t : x \in \mathbb{F}_{2^n}^*\} = \{x^d : x \in \mathbb{F}_{2^n}^*\}$ it is enough to show that γ^t is a d-th power, and conversely that γ^d is a t-th power.

Since $d \mid t$, it is clear that γ^t is a d-th power. In the other direction we have $\gamma^d = \gamma^{at+b(2^n-1)} = (\gamma^a)^t(\gamma^b)^{2^n-1} = (\gamma^a)^t$, yielding the desired conclusion.

The elements of $\{x^d : x \in \mathbb{F}_{2^n}^*\}$ are $1, \gamma^d, \gamma^{2d}, \ldots, \gamma^{(2^n-1)-d}$, hence the set has size $\frac{2^n-1}{d}$. □

Definition 1.3.3 ((n, m)–function, Boolean function, Vectorial function)**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called an* (n, m)–function. *When $m = 1$, we call f a* Boolean function. *When $m > 1$, we call f a* vectorial function.

Remark 1.3.4. Note that when m divides n, any (n, m)-function may be viewed as a function from $\mathbb{F}_{2^n}$ to itself, since $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$ [12, Section 9.2.2.2].

Generally speaking, vector-valued functions on $\mathbb{F}_{2^n}$ are called *vectorial Boolean functions*, to emphasize that the domain and range have characteristic two. However, since it is understood that we are dealing strictly with characteristic two in this thesis, we omit the second adjective.

We have the following terminology regarding (n, m)-functions:

Definition 1.3.5 (Hamming Distance)**.** *Let $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_2$. The* Hamming distance *between f and g is defined as*

$$d(f, g) := \#\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}.$$

Thus the Hamming distance between two Boolean functions on the same domain is equal to the number of points in the domain where the two functions differ. Note that we may equivalently express the Hamming distance $d(f,g)$ between the functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ as $d(f,g) = 2^n - \#\{x \in \mathbb{F}_{2^n} : f(x) = g(x)\}$.

The *Hamming weight* of a Boolean function f defined as the Hamming distance between f and the null function, which maps every point in the domain to the zero element. The Hamming weight of f is therefore equal to the number of points in the domain where f takes a non-zero value.

Definition 1.3.6 (Hamming Weight)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. The* Hamming weight *of f is defined as*

$$\mathrm{wt}(f) := d(f, 0).$$

The set of points where an (n,m)-function takes a non-zero value is called its *support*. Thus for Boolean functions the cardinality of the support is equal to the Hamming weight.

Definition 1.3.7 (Support of an (n,m)-function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The* support of f *is defined as*

$$\mathrm{supp}(f) := \{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}.$$

The function we define next is of central importance to the study of (n,m)-functions, as it allows for ease of expression and manipulation due to its amicable properties.

Definition 1.3.8 (Trace Function)**.** *Let m and n be positive integers such that m divides n. For $x \in \mathbb{F}_{2^n}$, define the* trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ *by*

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{n-m}}.$$

The function $Tr_1^n(x)$ is called the *absolute trace*. When the domain is clear from context, the absolute trace will simply be denoted by "$Tr(x)$". When $m > 1$ the function $Tr_m^n(x)$ is called the *trace relative to* $\mathbb{F}_{2^m}$, or simply the *relative trace* when the context is clear. Note that if $a \in \mathbb{F}_{2^n}$ and

$$\prod_{i=0}^{n/m-1} \left(x - a^{2^{im}}\right) = x^{n/m} + e_1 x^{n/m-1} + \ldots + e_{n/m-1}x + e_{n/m}$$

is the characteristic polynomial of a over $\mathbb{F}_{2^m}$ then we have $Tr_m^n(a) = e_1$.

Theorem 1.3.9 ([44])**.** *The trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ has the following properties:*

i. [44, remarks preceding Theorem 2.23] For any $\alpha \in \mathbb{F}_{2^n}$ we have $Tr_m^n(\alpha) \in \mathbb{F}_{2^m}$.

ii. [44, Theorem 2.23] For any $\alpha, \beta \in \mathbb{F}_{2^n}$ we have $Tr_m^n(\alpha + \beta) = Tr_m^n(\alpha) + Tr_m^n(\beta)$.

iii. [44, Theorem 2.23] For any $\alpha \in \mathbb{F}_{2^n}$ and for any $c \in \mathbb{F}_{2^m}$ we have $Tr_m^n(c\alpha) = cTr_m^n(\alpha)$.

iv. [44, Theorem 2.23] The trace is a $\mathbb{F}_{2^m}$-linear map from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^m}$.

v. [44, Theorem 2.23] For $\alpha \in \mathbb{F}_{2^m}$ we have $Tr_m^n(\alpha) = \frac{n}{m}\alpha$.

vi. [44, Theorem 2.23] For $\alpha \in \mathbb{F}_{2^n}$ we have $Tr_m^n(\alpha^{2^m}) = Tr_m^n(\alpha)$.

vii. [44, Theorem 2.26] For any $k \in \mathbb{N}$ and $\alpha \in \mathbb{F}_{2^{kn}}$ we have $Tr_m^{kn}(\alpha) = Tr_m^n(Tr_n^{kn}(\alpha))$.

The following is a well-known characterization of elements having trace zero:

Theorem 1.3.10 (Additive Hilbert 90)**.** [44, Theorem 2.25] *Let m and n be positive integers such that m divides n. For any $a \in \mathbb{F}_{2^n}$, the equation $a = t^{2^m} + t$ has exactly 2^m solutions in $\mathbb{F}_{2^n}$ if and only if $Tr_m^n(a) = 0$, otherwise it has no solutions.*

Proof. First note that since $t^{2^m} + t + a$ is a polynomial in t having degree 2^m, it can have at most 2^m roots in any extension field of $\mathbb{F}_{2^n}$. If this polynomial has a root $t \in \mathbb{F}_{2^n}$, then $Tr_m^n(a) = Tr_m^n(t^{2^m} + t) = Tr_m^n(t^{2^m}) + Tr_m^n(t) = 0$. Conversely, suppose that $Tr_m^n(a) = 0$. For any t residing in some extension field of $\mathbb{F}_{2^n}$ satisfying $a = t^{2^m} + t$, we have

$$\begin{aligned} 0 = Tr_m^n(a) &= a + a^{2^m} + a^{2^{2m}} + \cdots + a^{2^{n-m}} \\ &= (t^{2^m} + t) + (t^{2^m} + t)^{2^m} + (t^{2^m} + t)^{2^{2m}} + \cdots + (t^{2^m} + t)^{2^{n-m}} \\ &= t + (t^{2^m} + t^{2^m}) + (t^{2^{2m}} + t^{2^{2m}}) + \cdots + (t^{2^{n-m}} + t^{2^{n-m}}) + t^{2^n} \\ &= t + t^{2^n}. \end{aligned}$$

Therefore any root of $t^{2^m} + t + a$ is an element of $\mathbb{F}_{2^n}$. Additionally, if t is a root, then for any $b \in \mathbb{F}_{2^m}$ we have

$$(t+b)^{2^m} + (t+b) = t^{2^m} + t + b^{2^m} + b = t^{2^m} + t = a.$$

Therefore the equation $a = t^{2^m} + t$ has at least 2^m solutions in $\mathbb{F}_{2^n}$, therefore it has exactly this many solutions. □

Definition 1.3.11 (Balanced Function)**.** *Let A, B, and C be finite sets such that $B \subseteq A$ and that $\#C$ divides $\#B$. A function $f : A \to C$ is said to be* balanced on B *if for each $y \in C$ we have*

$$\#\{x \in B : f(x) = y\} = \frac{\#B}{\#C}.$$

In the case that $A = B$ then we simply say that f is balanced*.*

Remark 1.3.12. Note that a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is balanced if and only if

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = 0. \tag{1.1}$$

This fact will be used throughout the thesis.

In the next section and beyond we will see how the property of being balanced plays an integral role in characterizing bent functions. In addition, we will often use the fact that the trace function is balanced:

Proposition 1.3.13. *Let n and m be positive integers such that m divides n. Then for each $b \in \mathbb{F}_{2^m}$ we have*

$$\#\{a \in \mathbb{F}_{2^n} : Tr_m^n(a) = b\} = 2^{n-m}.$$

Proof. Let $S = \{x \in \mathbb{F}_{2^n} : Tr_m^n(x) = 0\}$. One can easily check that S forms a subspace of $\mathbb{F}_{2^n}$ when the latter is viewed as an n-dimensional vector space over $\mathbb{F}_2$. Furthermore, if $a \in \mathbb{F}_{2^n}$ is such that $Tr_m^n(a) = b$ for some $b \in \mathbb{F}_{2^m}^*$, then for any $x \in S$ we have $Tr_m^n(x + a) = Tr_m^n(x) + Tr_m^n(a) = 0 + b = b$. Since $x \mapsto Tr_m^n(x)$ maps $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^m}$, for any $b \in \mathbb{F}_{2^m}^*$ the set $\{x \in \mathbb{F}_{2^n} : Tr_m^n(x) = b\}$ is non-empty and thus forms a coset of S.

By Theorem 1.3.10, each $x \in S$ corresponds to 2^m unique elements of $\mathbb{F}_{2^n}$. Therefore $\#S = 2^{n-m}$, and every coset of S also has this size. □

Thus the trace function is balanced. Our next proposition is a direct consequence of this fact.

Proposition 1.3.14. *Let $a \in \mathbb{F}_{2^n}$. Then*

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax)} = \begin{cases} 2^n \text{ if } a = 0 \\ 0 \text{ otherwise.} \end{cases}$$

Proof. If $a = 0$ then $Tr(ax) = Tr(0) = 0$ for all $x \in \mathbb{F}_{2^n}$ and therefore $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax)} = \sum_{x \in \mathbb{F}_{2^n}} 1 = 2^n$. If $a \neq 0$ then $x \mapsto ax$ is a permutation on $\mathbb{F}_{2^n}$ and therefore

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x)} = \sum_{\substack{x \in \mathbb{F}_{2^n} \\ Tr(x)=0}} 1 + \sum_{\substack{x \in \mathbb{F}_{2^n} \\ Tr(x)=1}} (-1) = 2^{n-1} - 2^{n-1} = 0.$$

□

When considering Boolean functions, Theorem 1.3.9 part (*vi*) allows us in many instances to consider exponents as being equivalent up to multiplication modulo $2^n - 1$ by a power of 2. That is, we consider exponents belonging to the same cyclotomic coset modulo $2^n - 1$ to be equivalent. We formally define cyclotomic cosets modulo a positive integer:

Definition 1.3.15 (Cyclotomic Coset Modulo n, Set of Representatives Modulo n)**.** *Let n be an odd positive integer and let $i \in \mathbb{Z}_n$. Define the* cyclotomic coset modulo n containing i *as*

$$C(i, n) := \{2^j i \mod n : j \geq 0\}.$$

Given some collection of pairwise distinct cosets $C(i,n)$, a set consisting of one element from each coset is called a set of representatives modulo n. *A set of representatives modulo n containing an element from every coset is called* complete.

Proposition 1.3.16. *Let $n = 2^m - 1$ and let $i \in \mathbb{Z}_n$. Then $\#C(i,n)$ divides m.*

Proof. Let $s_i = \#C(i,n)$. Clearly s_i is the smallest positive integer such that $i \equiv 2^{s_i} i \pmod{n}$, therefore $i \not\equiv 2^j i \pmod{n}$ for $1 \leq j < s_i$. Therefore for any $t \in \mathbb{N}$ we have $2^t i \equiv i \pmod{n}$ if and only if s_i divides t. Since $2^m \equiv 1 \pmod{n}$ we have $2^m i \equiv i \pmod{n}$, and therefore s_i divides m. □

The following theorem is vital to our work, as it allows us to take advantage of the properties of the trace function when studying bent functions in the setting of finite fields.

Theorem 1.3.17. [28, Theorem 6.5] *Any function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ can be uniquely represented in the form*

$$f(x) = \sum_{i \in \Gamma_2(n)} Tr_1^{n_i}(a_i x^i) + \epsilon(1 + x^{2^n - 1}),\ a_i \in \mathbb{F}_{2^{n_i}},\ \epsilon \in \mathbb{F}_2, \tag{1.2}$$

where $\Gamma_2(n)$ is a complete set of representatives modulo $2^n - 1$, n_i is the size of the coset $C(i, 2^n - 1)$, and $\epsilon = \mathrm{wt}(f) \mod 2$.

In particular, we have the following:

Corollary 1.3.18. *Any function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ may be represented in the form*

$$f(x) = Tr_1^n\left(\sum_{i \in \Gamma_2(n)} \beta_i x^i\right),\ \beta_i \in \mathbb{F}_{2^n}, \tag{1.3}$$

where $\Gamma_2(n)$ is a complete set of representatives modulo $2^n - 1$.

Proof. By Theorem 1.3.17, f admits a (unique) representation of the form

$$f(x) = \sum_{i \in \Gamma_2(n)} Tr_1^{n_i}(a_i x^i) + \epsilon(1 + x^{2^n - 1}),\ a_i \in \mathbb{F}_{2^{n_i}},\ \epsilon \in \mathbb{F}_2,$$

where n_i is the size of the coset $C(i, 2^n - 1)$, and $\epsilon = \mathrm{wt}(f) \mod 2$. Let $j, k \in \Gamma_2(n)$, and let $\lambda_j, \lambda_k \in \mathbb{F}_{2^n}$ be such that $Tr_{n_j}^n(\lambda_j) = Tr_{n_k}^n(\lambda_k) = 1$. Then we have

$$\begin{aligned}
Tr_1^{n_j}(a_j x^j) + Tr_1^{n_k}(a_k x^k) &= Tr_1^{n_j}(Tr_{n_j}^n(\lambda_j) a_j x^j) + Tr_1^{n_k}(Tr_{n_k}^n(\lambda_k) a_k x^k) \\
&= Tr_1^{n_j}(Tr_{n_j}^n(\lambda_j a_j x^j)) + Tr_1^{n_k}(Tr_{n_k}^n(\lambda_k a_k x^k)) \\
&= Tr_1^n(\lambda_j a_j x^j) + Tr_1^n(\lambda_k a_k x^k) \\
&= Tr_1^n(\lambda_j a_j x^j + \lambda_k a_k x^k).
\end{aligned}$$

Since $\epsilon(1+x^{2^n-1}) = Tr_1^n(\lambda\epsilon(1+x^{2^n-1}))$ for any $\lambda \in \mathbb{F}_{2^n}$ such that $Tr_1^n(\lambda) = 1$, this completes the proof. □

Every Boolean function admits a unique expression of the form (1.2), while expressions of the form (1.3) are not unique [28], [12]. Indeed, the last claim can be verified by observing that for each $i \in \Gamma_2(n)$ there are 2^{n-n_i} elements $\lambda_i \in \mathbb{F}_{2^n}$ with $Tr_{n_i}^n(\lambda_i) = 1$.

Definition 1.3.19 (Unique Trace Representation of a Boolean Function, Absolute Trace Representation of a Boolean Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. The expression* (1.2) *is called the* unique trace representation of f*. An expression of f having the form* (1.3) *is called an* absolute trace representation of f*. Expressions of the form* (1.2) *and* (1.3) *are called globally* trace representations.

Definition 1.3.20 (Algebraic Degree of a Boolean Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ have a unique trace representation*

$$f(x) = \sum_{i \in \Gamma_2(n)} Tr_1^{n_i}(a_i x^i) + \epsilon(1+x^{2^n-1}),\ a_i \in \mathbb{F}_{2^{n_i}},\ \epsilon \in \mathbb{F}_2$$

as defined in the statement of Theorem 1.3.17. The algebraic degree *of f, denoted* $\deg(f)$*, is defined as*

$$\deg(f) = \begin{cases} \max\{\mathrm{wt}_2(i) : i \in \Gamma_2(n),\ a_i \neq 0\} \text{ if } \epsilon = 0 \\ n \text{ if } \epsilon = 1, \end{cases}$$

where $\mathrm{wt}_2(i)$ *denotes the number of non-zero symbols in the base 2 representation of the integer i (this is called the* 2-weight of i*).*

The definition above is derived from the usual definition of the algebraic degree of a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, which is in turn defined in terms of the *algebraic normal form*:

Definition 1.3.21 (Algebraic Normal Form)**.** *The* algebraic normal form *(ANF) of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the unique expression given by*

$$f(x_0, \ldots, x_{n-1}) = \sum_{I \subseteq \{0,1,\ldots,n-1\}} a_I \left(\prod_{i \in I} x_i \right),\ a_I \in \mathbb{F}_2. \tag{1.4}$$

The algebraic degree *of f is the cardinality of the largest set $I \subseteq \{0, 1, \ldots, n-1\}$ such that the corresponding coefficient a_I is non-zero.*

Proposition 1.3.22. [16, p. 8] *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, and let*

$$(x_0, \ldots, x_{n-1}) \mapsto \sum_{I \subseteq \{0,1,\ldots,n-1\}} a_I \left(\prod_{i \in I} x_i \right),\ a_I \in \mathbb{F}_2 \tag{1.5}$$

be the ANF of f when viewed as a mapping on $\mathbb{F}_2^n$. Then $\deg(f)$ *is equal to the cardinality of the largest set* $I \subseteq \{0, 1, \ldots, n-1\}$ *such that the corresponding coefficient* a_I *is non-zero.*

We note that Definition 1.3.20 and Proposition 1.3.22 are reversed with respect to the conventional presentation – one typically defines the algebraic degree in the context of mappings on vector spaces and then derives the corresponding characteristic of mappings on finite fields. We have chosen to take the latter as the definition since we are studying bent functions in the context of finite fields.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and let $c_1, \ldots, c_k \in \mathbb{F}_2^n$ be the elements of $\mathrm{supp}(f)$, where $k = \mathrm{wt}(f) = \#\,\mathrm{supp}(f)$. Then the ANF of f is the sum of the ANFs of the k functions $f_1, \ldots, f_k : \mathbb{F}_2^n \to \mathbb{F}_2$, which are defined by

$$f_i(x) = \begin{cases} 1 \text{ if } x = c_i \\ 0 \text{ otherwise} \end{cases} \qquad \text{for } i = 1, \ldots, k.$$

The functions $f_1, \ldots, f_k$ are called the *atomic functions* of f. Let $c_i = \left(c_0^{(i)}, c_1^{(i)}, \ldots, c_{n-1}^{(i)}\right)$, where $c_j^{(i)} \in \mathbb{F}_2$ for each j. Then, denoting by x the vector $(x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, the ANF of f_i is given by

$$f_i(x) = \left(x_0 + c_0^{(i)} + 1\right)\left(x_1 + c_1^{(i)} + 1\right) \cdots \left(x_{n-1} + c_{n-1}^{(i)} + 1\right).$$

Remark 1.3.23. As in [12, Section 8.2.1], we note that every atomic function of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ has algebraic degree equal to n, and therefore that $\deg(f) = n$ if and only if $\mathrm{wt}(f)$ is odd. The consequences for bent functions will be explained in Chapter 2.

Example 1.3.24. Denote by x the vector $(x_0, x_1, x_2) \in \mathbb{F}_2^3$. Consider the function $f : \mathbb{F}_2^3 \to \mathbb{F}_2$, defined in Table 1.3. We shall determine the algebraic normal form of f. The

Table 1.3: A Function from $\mathbb{F}_2^3$ to $\mathbb{F}_2$

x_0	x_1	x_2	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

ANF of f may be uniquely expressed as the sum of the ANFs of the four atomic functions $f_1, f_2, f_3, f_4 : \mathbb{F}_2^3 \to \mathbb{F}_2$. We have $\mathrm{supp}(f) = \{(0,0,1), (0,1,0), (0,1,1), (1,0,0)\}$, thus we

may write

$$\begin{aligned} f_1(x) &= (x_0+1)(x_1+1)x_2 \\ f_2(x) &= (x_0+1)x_1(x_2+1) \\ f_3(x) &= (x_0+1)x_1x_2 \\ f_4(x) &= x_0(x_1+1)(x_2+1). \end{aligned}$$

Thus we have

$$\begin{aligned} f(x) &= f_1(x) + f_2(x) + f_3(x) + f_4(x) \\ &= (x_0+1)(x_1+1)x_2 + (x_0+1)x_1(x_2+1) + (x_0+1)x_1x_2 + x_0(x_1+1)(x_2+1) \\ &= x_0 + x_1 + x_2 + x_1x_2. \end{aligned}$$

Example 1.3.25. In this example we will recover the ANF of a Boolean function from its trace representation.

Let $p(x) \in \mathbb{F}_2[x]$ be the primitive polynomial $x^3 + x + 1$, and let α be a root of $p(x)$ in $\mathbb{F}_{2^3}$. Then for any $x \in \mathbb{F}_{2^3}$ we may write $x = x_0 + x_1\alpha + x_2\alpha^2$, where $x_0, x_1, x_2 \in \mathbb{F}_2$. Note that due to the choice of $p(x)$ we have

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^4 = \alpha(1 + \alpha + \alpha^3) = 0.$$

Since $Tr(x) = Tr(x^2)$ for all x we infer that 0, α, α^2, and α^4 all have trace 0. Since the trace function is balanced we conclude that 1, α^3, α^5, and α^6 have trace 1.

Let $a = \alpha^2$, and let $f : \mathbb{F}_{2^3} \to \mathbb{F}_2$ be defined by $f(x) = Tr(ax^3)$. Then we have

$$\begin{aligned} f(x) &= Tr(ax^3) \\ &= Tr\left(\alpha^2(x_0 + x_1\alpha + x_2\alpha^2)^3\right) \\ &= Tr\left(x_1x_2 + x_2\alpha + x_0\alpha^2 + x_0x_1\alpha^3 + (x_0x_1 + x_0x_2)\alpha^4 + x_1\alpha^5 + (x_0x_2 + x_1x_2)\alpha^6\right) \\ &= Tr\left(x_1x_2\right) + Tr\left(x_2\alpha\right) + Tr(x_0\alpha^2) + Tr(x_0x_1\alpha^3) \\ &\qquad + Tr\left((x_0x_1 + x_0x_2)\alpha^4\right) + Tr(x_1\alpha^5) + Tr\left((x_0x_2 + x_1x_2)\alpha^6\right) \\ &= x_1x_2 + x_2Tr(\alpha) + x_0Tr(\alpha^2) + x_0x_1Tr(\alpha^3) \\ &\qquad + (x_0x_1 + x_0x_2)Tr(\alpha^4) + x_1Tr(\alpha^5) + (x_0x_2 + x_1x_2)Tr(\alpha^6) \\ &= x_1x_2 + x_0x_1 + x_1 + x_0x_2 + x_1x_2 \\ &= x_1 + x_0x_1 + x_0x_2. \end{aligned}$$

For ease of expression, we will use the absolute trace representation when discussing functions whose unique trace representations consist of multiple trace terms.

As we will be defining bent functions in terms of their distance to the set of all affine functions, it is of course necessary to give a formal definition of an affine function on a finite field.

Definition 1.3.26 (Linear Function, Affine Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. If f admits a representation of the form $f(x) = Tr_1^n(ax) + b$ for some $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$ then f is called* affine*. If $b = 0$ then f is called* linear*.*

Any function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ may be viewed as a collection of m Boolean functions, i.e. we may write

$$f(x) = (f_1(x), \ldots, f_m(x)) .$$

These are called the *coordinate functions of f*. Properties of an (n, m)-function f may be characterized by the $2^m - 1$ non-zero linear combinations of its coordinate functions. In the context of finite fields, these are the functions of the form $Tr_1^m(bf(x))$, $b \in \mathbb{F}_{2^m}^*$. These functions have a common name in the literature:

Definition 1.3.27 (Component Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The functions*

$$Tr_1^m (bf(x)) , \, b \in \mathbb{F}_{2^m}^*$$

are called the component functions of f*.*

The algebraic degree of an (n, m)-function may be defined in terms of the algebraic degrees of its Boolean component functions, as defined in Definition 1.3.20:

Definition 1.3.28 (Algebraic Degree of an (n, m)-Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The* algebraic degree *of f, denoted* $\deg(f)$*, is defined as*

$$\deg(f) = \max\{\deg(Tr_1^m(bf(x))) : b \in \mathbb{F}_{2^m}^*\}.$$

That is, the algebraic degree of f is equal to the maximum algebraic degree of its component functions.

In consideration of Definitions 1.3.20 and 1.3.28, we immediately see that the algebraic degree of an (n, m)-function of the form $x \mapsto Tr_m^n(ax^d)$ may be quickly ascertained:

Proposition 1.3.29. *Let $a \in \mathbb{F}_{2^n}^*$, let $d \in \mathbb{N}$, and let $f(x) = Tr_m^n(ax^d)$. Then*

$$\deg(f) = \mathrm{wt}_2(d).$$

Proof. The component functions of f have the form $Tr_1^m(bf(x))$, $b \in \mathbb{F}_{2^m}^*$. For any $b \in \mathbb{F}_{2^m}^*$ we have

$$Tr_1^m(bf(x)) = Tr_1^m(bTr_m^n(ax^d)) = Tr_1^n(abx^d).$$

Therefore each component function of f has degree $\mathrm{wt}_2(d)$, hence $\deg(f) = \mathrm{wt}_2(d)$. □

Remark 1.3.30. By the above proposition and the fact that $Tr(x) = Tr(x^2)$ for all $x \in \mathbb{F}_{2^n}$, the set of all $(n, 1)$-functions of degree at most one coincides exactly with the set of all affine functions on the same domain. Even though we have not yet formally defined the bent property, we may therefore infer that all bent functions must have algebraic degree two or greater.

Proposition 1.3.31. [12, Proposition 9.2] *An (n, m)-function f is balanced if and only if all of its component functions are balanced.*

Proof. If f is balanced then by definition f takes every value in $\mathbb{F}_{2^m}$ equally often. Therefore for each $v \in \mathbb{F}_{2^m}^*$ we have

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(vf(x))} &= 2^{n-m} \sum_{u \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(uv)} \\
&= 2^{n-m} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(y)} \qquad \text{since } u \mapsto uv \text{ permutes } \mathbb{F}_{2^m} \\
&= 2^{n-m} \cdot 0 \qquad \text{by Proposition 1.3.14} \\
&= 0.
\end{aligned}$$

This implies that each component function of f is balanced.

Now let us suppose that the function $x \mapsto Tr_1^m(vf(x))$ is balanced on $\mathbb{F}_{2^n}$ for all $v \in \mathbb{F}_{2^m}^*$. Define the function $\phi : \mathbb{F}_{2^m} \to \mathbb{Z}$ by

$$\phi(v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(vf(x))}.$$

Then for all non-zero v we have $\phi(v) = 0$. Now let us define the function $\psi : \mathbb{F}_{2^m} \to \mathbb{Z}$ by

$$\psi(u) = \sum_{v \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(uv)} \phi(v).$$

By Proposition 1.3.14, for any $x \in \mathbb{F}_{2^n}$ we have

$$\sum_{v \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(uv)} (-1)^{Tr_1^m(vf(x))} = \sum_{v \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(v(f(x)+u))} = \begin{cases} 2^m \text{ if } f(x) = u \\ 0 \text{ otherwise,} \end{cases}$$

therefore the image of $u \in \mathbb{F}_{2^m}$ under ψ is

$$\psi(u) = \sum_{\substack{v \in \mathbb{F}_{2^m} \\ x \in \mathbb{F}_{2^n}}} (-1)^{Tr_1^m(v(f(x)+u))} = 2^m |f^{-1}(u)|. \tag{1.6}$$

Since $\phi(v) = 0$ for all $v \in \mathbb{F}_{2^m}^*$, for any $u \in \mathbb{F}_{2^m}$ we have

$$\begin{aligned}\psi(u) &= \sum_{v \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(uv)} \phi(v) \\ &= \phi(0) = 2^n.\end{aligned}$$

By (1.6), this implies that $|f^{-1}(u)| = 2^{n-m}$ for all $u \in \mathbb{F}_{2^m}$. Therefore f is balanced. □

We now define a multiplicative analogue of the trace. Though it will not be used as extensively as the trace, it will play a central role in characterizing certain generalizations of the Dillon functions.

Definition 1.3.32 (Norm Function)**.** *Let m and n be positive integers such that m divides n. For $x \in \mathbb{F}_{2^n}$, define the* norm from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ *by*

$$N_m^n(x) = x \cdot x^{2^m} \cdot x^{2^{2m}} \cdots x^{2^{n-m}}.$$

Theorem 1.3.33 ([44])**.** *The norm from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ has the following properties:*

i. [44, remark preceding Theorem 2.28] For any $\alpha \in \mathbb{F}_{2^n}$ we have $N_m^n(\alpha) \in \mathbb{F}_{2^m}$.

ii. [44, Theorem 2.28] For any $\alpha, \beta \in \mathbb{F}_{2^n}$ we have $N_m^n(\alpha\beta) = N_m^n(\alpha)N_m^n(\beta)$.

iii. [44, Theorem 2.28] The norm maps $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}^*$ onto $\mathbb{F}_{2^m}^*$.

iv. [44, Theorem 2.28] For any $\alpha \in \mathbb{F}_{2^m}$ we have $N_m^n(\alpha) = \alpha^{n/m}$.

v. [44, Theorem 2.28] For any $\alpha \in \mathbb{F}_{2^n}$ we have $N_m^n(\alpha^{2^m}) = N_m^n(\alpha)$.

vi. [44, Theorem 2.29] For any $k \in \mathbb{N}$ and $\alpha \in \mathbb{F}_{2^{kn}}$ we have $N_m^{kn}(\alpha) = N_m^n(N_n^{kn}(\alpha))$.

The terminology used to describe the trace also applies to the norm: The function $N_1^n(x)$ is called the *absolute norm*. When the domain is clear from context, the absolute norm is simply denoted by "$N(x)$". When $m > 1$ the function $N_m^n(x)$ is called the *norm relative to* $\mathbb{F}_{2^m}$, or simply the *relative norm* when the context is clear. Similar to the observation that we made for the trace, note that if $a \in \mathbb{F}_{2^n}$ and

$$\prod_{i=0}^{n/m-1} \left(x - a^{2^{im}}\right) = x^{n/m} + e_1 x^{n/m-1} + \ldots + e_{n/m-1}x + e_{n/m}$$

is the characteristic polynomial of a over $\mathbb{F}_{2^m}$ then we have $N_m^n(a) = e_{n/m}$.

The notion of derivative exists for (n, m)-functions. Bent functions may be characterized by the behaviour of the derivative.

Definition 1.3.34 (Derivative of a Function)**.** *Let* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$*, and let* $a \in \mathbb{F}_{2^n}^*$*. The* derivative of f in the direction of a *is defined as*

$$D_a f(x) := f(x + a) - f(x).$$

The phrase "in the direction of" originates from the more general setting of functions on finite vector spaces. Note that in characteristic 2 there is no distinction between "-" and "+" (see Theorem 1.3.1); we have defined the derivative using the "-" symbol in order to draw a parallel with the familiar notion of the derivative from Calculus.

Note the similarity in the behaviour of the discrete derivative of an affine function on a finite field, and that of the derivative of an affine function on a field of characteristic zero (the reals, say), as it is defined in Calculus – namely, both are constant. In a finite field, the opposite of a constant function is a balanced function, which not only takes on every possible value, but does so as often as possible. We therefore require the derivative of a maximally non-linear function in the direction of a given point to be balanced. This will be formalized in the next section.

Chapter 2

Bent Functions

In this chapter we introduce bent functions and give a detailed overview of several specific classes of bent functions. Statements and proofs that are taken expressly from external sources are clearly indicated as such, though they may be modified for the convenience of the reader. Specifically, the proofs presented here will tend to be more detailed than the original versions. In the literature, many of the more fundamental and/or elementary results are often stated without proof and without a reference. As such, any proof that is given in this chapter without an explicit reference has been devised by the current author, though there is no guarantee that a similar proof does not appear elsewhere in the literature. The author wishes to emphasize that every statement in this chapter appears in the literature in some form, unless otherwise indicated. Non-original statements that are given without a reference are considered to be common knowledge in the field.

2.1 Preliminary Definitions and Results

In this section we formally introduce bent functions. In the spirit of the original formulation and historical development of bent functions, we will first introduce the concept of bentness in the setting of Boolean functions. We will give necessary definitions and fundamental results before extending the Boolean formulation to vector-valued functions.

Recall that a function $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called *affine* if it admits a representation of the form $g(x) = Tr(ax) + b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$. We define the *non-linearity* of a Boolean function f to be the smallest Hamming distance between f and an affine function.

Definition 2.1.1 (Non-linearity)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. For $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$, define the function $h_{a,b} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ by $h_{a,b}(x) = Tr(ax) + b$. The* non-linearity *of f is defined as*

$$nl(f) := \min_{a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_2} d(f, h_{a,b}).$$

We will see shortly that, for even n, the maximum attainable non-linearity of a Boolean function on $\mathbb{F}_{2^n}$ is $2^{n-1} - 2^{n/2-1}$, and that the functions that meet this bound are exactly the (Boolean) bent functions. Interestingly, the corresponding bound for odd n is only known for $n \leq 7$ [65, Section 2.3]. In general, for Boolean functions of odd dimension n we have the so-called *bent concatenation bound* of $2^{n-1} - 2^{\frac{n-1}{2}}$. It is known that this bound gives the maximum attainable non-linearity of Boolean functions on $\mathbb{F}_{2^n}$ for $n = 3, 5$, and 7 [59]. Functions meeting the bent concatenation bound are constructed by combining two Boolean bent functions of even dimension $n-1$. More precisely, given two Boolean bent functions f_0 and f_1 of even dimension $n-1$, construct the function $F : \mathbb{F}_2^n \to \mathbb{F}_2$ by

$$F(x) = F(x_0, \ldots, x_{n-1}) = (1 + x_{n-1}) \cdot f_0(x_0, \ldots, x_{n-2}) + x_{n-1} \cdot f_1(x_0, \ldots, x_{n-2}).$$

It can be checked that $nl(F)$ is indeed equal to $2^{n-1} - 2^{\frac{n-1}{2}}$. The 2^n bit-long truth table of F is concatenation of the two 2^{n-1} bit-long truth tables of f_0 and f_1, hence the term "concatenation" [35].

In [59], Patterson and Wiedemann constructed Boolean functions on $\mathbb{F}_{2^{15}}$ having non-linearity $2^{15-1} - 2^{\frac{15-1}{2}} + 20$. This work was especially notable in that it marked the first time that the bent concatenation bound had been beaten. More recently, it has been shown for $n = 9, 11$, and 13 one can construct Boolean functions on $\mathbb{F}_{2^n}$ having non-linearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2^{\frac{n-9}{2}+1}$ [36]. The most recent development in this direction is the work [35] of Kavut and Maitra, where Boolean functions on $\mathbb{F}_{2^{21}}$ having non-linearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61$ are demonstrated.

2.1.1 Boolean Bent Functions

We will see how the non-linearity of a Boolean function f can be characterized in a useful way by the values taken by its Walsh transform, which we define now:

Definition 2.1.2 (Walsh Transform)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, and let $a \in \mathbb{F}_{2^n}$. Define the* Walsh transform *of f at a by*

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

The values $W_f(a)$ are called the Walsh coefficients *of f, and the multi-set $\{W_f(a) : a \in \mathbb{F}_{2^n}\}$ is called the* Walsh spectrum *of f.*

Remark 2.1.3. Evaluating the Walsh spectrum of a Boolean function at a given point using the definition above is obviously inefficient, requiring $O(2^{2n})$ time. Fortunately, there exists an $O(n2^n)$ algorithm for computing transforms of this type, called the *fast Walsh transform*. This algorithm is described in [12, Section 8.2.2], along with an example that computes the Walsh spectrum of a given Boolean function using the algorithm. This algorithm will feature in several of the computations presented in Appendix B.

Proposition 2.1.4. *For any $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, we have $W_f(0) = 2^n - 2\,\mathrm{wt}(f)$.*

Proof. We have

$$\begin{aligned} W_f(0) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \\ &= \#\{x \in \mathbb{F}_{2^n} : f(x) = 0\} - \#\{x \in \mathbb{F}_{2^n} : f(x) = 1\} \\ &= (2^n - \#\{x \in \mathbb{F}_{2^n} : f(x) = 1\}) - \#\{x \in \mathbb{F}_{2^n} : f(x) = 1\} \\ &= 2^n - 2\,\mathrm{wt}(f). \end{aligned}$$

□

The following classic theorem will enable us to put tight upper and lower bounds on the maximum value attained by the absolute values of the Walsh coefficients of a Boolean function.

Theorem 2.1.5 (Parseval's Identity)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then*

$$\sum_{a \in \mathbb{F}_{2^n}} |W_f(a)|^2 = 2^{2n}.$$

Proof. We have

$$\begin{aligned} \sum_{a \in \mathbb{F}_{2^n}} |W_f(a)|^2 &= \sum_{a \in \mathbb{F}_{2^n}} \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)} \right|^2 \\ &= \sum_{a \in \mathbb{F}_{2^n}} \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)} (-1)^{f(y)+Tr(ay)} \\ &= \sum_{a \in \mathbb{F}_{2^n}} \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(y)+Tr(ax)+Tr(ay)} \\ &= \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{Tr(a(x+y))} \\ &= \sum_{\substack{x,y \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{Tr(a(x+y))} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{2f(x)} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{Tr(a(2x))} \\ &= 0 + \sum_{x \in \mathbb{F}_{2^n}} \sum_{a \in \mathbb{F}_{2^n}} 1 \qquad \text{(by Proposition 1.3.14)} \\ &= 2^{2n}. \end{aligned}$$

□

Corollary 2.1.6. *For any $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and for any $a \in \mathbb{F}_{2^n}$ we have*

$$2^{n/2} \leq \max_{a \in \mathbb{F}_{2^n}} |W_f(a)| \leq 2^n.$$

Proof. If $\max_{a\in\mathbb{F}_{2^n}} |W_f(a)| < 2^{n/2}$ then $\sum_{a\in\mathbb{F}_{2^n}} |W_f(a)|^2 < 2^{2n}$, contradicting Parseval's Identity. Therefore we must have $\max_{a\in\mathbb{F}_{2^n}} |W_f(a)| \geq 2^{n/2}$. On the other hand, given $\sum_{a\in\mathbb{F}_{2^n}} |W_f(a)|^2 = 2^{2n}$, it is clear that the maximum attainable value of $|W_f(a)|$ is 2^n. □

With this in mind, we will now see how the non-linearity of a Boolean function f is characterized by its Walsh spectrum:

Proposition 2.1.7. [12, Equation (8.35)] *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then*

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^n}} |W_f(a)|.$$

Proof. For $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$, let $h_{a,b}(x) = Tr(ax) + b$. Then we have

$$W_{f+h_{a,b}}(0) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)+b} = (-1)^b W_f(a).$$

Correspondingly, we have

$$\begin{aligned} d(f, h_{a,b}) &= wt(f + h_{a,b}) \\ &= 2^{n-1} - \frac{1}{2} W_{f+h_{a,b}}(0) \qquad \text{by Proposition 2.1.4} \\ &= 2^{n-1} - \frac{1}{2}(-1)^b W_f(a). \end{aligned}$$

Therefore

$$\begin{aligned} nl(f) &= \min_{a\in\mathbb{F}_{2^n},\, b\in\mathbb{F}_2} d(f, h_{a,b}) \\ &= \min_{a\in\mathbb{F}_{2^n},\, b\in\mathbb{F}_2} \left(2^{n-1} - \frac{1}{2}(-1)^b W_f(a)\right) \\ &= 2^{n-1} - \frac{1}{2} \max_{\substack{a\in\mathbb{F}_{2^n} \\ b\in\mathbb{F}_2}} (-1)^b W_f(a) \\ &= 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^n}} |W_f(a)|. \end{aligned}$$

□

We can now formulate an upper bound for the non-linearity of a Boolean function.

Proposition 2.1.8. [12, Equation (8.36)] *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then*

$$nl(f) \leq 2^{n-1} - 2^{n/2-1}.$$

Proof. From Proposition 2.1.7 we have

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^n}} |W_f(a)|$$

and from Corollary 2.1.6 we have

$$2^{n/2} \leq \max_{a \in \mathbb{F}_{2^n}} |W_f(a)|$$

therefore

$$nl(f) \leq 2^{n-1} - 2^{n/2-1}.$$

□

Proposition 2.1.7 makes simple the task of establishing the fundamental fact that the non-linearity of a Boolean function is invariant under linear transformations on the domain.

Proposition 2.1.9. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. For $a \in \mathbb{F}_{2^n}^*$, define $f_a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ by $f_a(x) = f(ax)$. Then*

$$nl(f) = nl(f_a).$$

Proof. By Proposition 2.1.7 we have $nl(f) = nl(f_a)$ if and only if $\max_{\alpha \in \mathbb{F}_{2^n}} |W_f(\alpha)| = \max_{\alpha \in \mathbb{F}_{2^n}} |W_{f_a}(\alpha)|$. For any $\alpha \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned} W_{f_a}(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(ax)+Tr(\alpha x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(\alpha a^{-1} x)} \\ &= W_f(\alpha a^{-1}). \end{aligned}$$

Since $x \mapsto a^{-1}x$ is a permutation on $\mathbb{F}_{2^n}$, the Walsh spectra of f and f_a are therefore identical. Therefore f and f_a have the same non-linearity. □

Proposition 2.1.7 also makes it clear that the non-linearity of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is maximized when $\max_{a \in \mathbb{F}_{2^n}} |W_f(a)|$ is minimized. We therefore define bent functions to be those Boolean functions whose Walsh coefficients meet the lower bound given in Corollary 2.1.6:

Definition 2.1.10 (Boolean Bent Function)**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called* bent *if for all $a \in \mathbb{F}_{2^n}$ we have*

$$|W_f(a)| = 2^{n/2}.$$

We immediately notice that the bent property restricts the parity of the dimension of the domain:

Proposition 2.1.11. *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent then n is even.*

Proof. This follows immediately from Definition 2.1.10 and the fact that $W_f(a)$ is always an integer. □

Propositions 2.1.7 and Proposition 2.1.8 together show that bent functions attain the maximum possible non-linearity among all Boolean functions.

It is known that Boolean bent functions exist in any even dimension:

Proposition 2.1.12. [12, Section 9.3.1.1] *For all positive even integers n there exists a bent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$.*

The following theorem shows that bent functions exhibit the maximum possible differential uniformity.

Theorem 2.1.13. [12, Theorem 8.28] *Let $f := \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then f is bent if and only if the derivative $D_a f(x) = f(x + a) - f(x)$ is balanced for all $a \in \mathbb{F}_{2^n}^*$.*

This property makes bent functions desirable for use in block ciphers that aim to be resistant to the *differential attack* of Biham and Shamir [6] (see also [12, Section 9.1]). However, the algebraic degree of a bent function is bounded:

Theorem 2.1.14. (Rothaus' bound [12, Proposition 8.31]) *Let $n \geq 4$ be even, and let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be bent. Then the algebraic degree of f is at most $n/2$.*

Remark 2.1.15. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Recall that $\deg(f) = n$ if and only if $\mathrm{wt}(f)$ is odd (Remark 1.3.23). Thus Theorem 2.1.14 implies that all bent functions have even weight.

Remark 2.1.16. Any Boolean or vectorial function used for cryptographic purposes should have high algebraic degree, as cryptosystems that use such functions for confusion are increasingly vulnerable to attack as the algebraic degrees of these functions decrease [12, Section 8.4.1]. In particular, high algebraic degree of Boolean functions used in block ciphers results in greater complexity in algebraic attacks designed to recover the key bits [65, Section 10.2]. In the next section we will see a class of bent functions that meet Rothaus' bound.

Remark 2.1.17. We have seen that bent functions exhibit the maximum possible non-linearity and the maximum possible differential uniformity. As we will see in the forthcoming sections, it is also possible to construct bent functions achieving relatively high algebraic degree. Of the desirable properties of a perfect cryptographic function (as described by Adams and Tavares in [3]), bent functions satisfy all but one: the property of being balanced. However, it is possible to modify bent functions to obtain balanced functions that retain a high degree of non-linearity and differential uniformity [12, Sections 8.6.8 and 8.7.5].

Proposition 2.1.18. *If a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is bent, then it is not balanced.*

Proof. Clearly a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is balanced if and only if $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = W_f(0) = 0$. It follows from Definition 2.1.10 that a bent function is not balanced. □

2.1.2 Vectorial Bent Functions

The bent property can be extended to a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ for values of m greater than one in several equivalent ways, with each characterization being useful in various contexts. In this section we present three characterizations of vectorial bentness.

The non-linearity of an (n, m)-function is characterized in terms of the non-linearities of its component functions:

Definition 2.1.19 (Non-linearity of an (n, m)-Function)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The* non-linearity *of f is defined as the minimum non-linearity among all the component functions of f.*

Analogous to Proposition 2.1.7, the non-linearity of an (n, m)-function may be characterized in terms of an extended version of the Walsh transform:

Definition 2.1.20 (Extended Walsh Transform)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, let $a \in \mathbb{F}_{2^n}$, and let $b \in \mathbb{F}_{2^m}^*$. Define the* extended Walsh transform *of f at (a, b) by*

$$W_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(bf(x)) + Tr_1^n(ax)}.$$

The values $W_f(a, b)$ are called the extended Walsh coefficients *of f, and the multi-set $\{W_f(a, b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*\}$ is called the* extended Walsh spectrum *of f.*

Proposition 2.1.21. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. Then*

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^m}^*} |W_f(a, b)|.$$

Proof. For $b \in \mathbb{F}_{2^m}^*$, let $g_b(x) = Tr_1^m(bf(x))$. Then we have

$$\begin{aligned}
nl(f) &= \min_{b \in \mathbb{F}_{2^m}^*} nl(g_b) && \text{by Definition 2.1.19} \\
&= \min_{b \in \mathbb{F}_{2^m}^*} \left(2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} |W_{g_b}(a)| \right) && \text{by Proposition 2.1.7} \\
&= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^m}^*} \Big| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(bf(x)) + Tr(ax)} \Big| \\
&= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^m}^*} |W_f(a, b)| && \text{by Definition 2.1.20.}
\end{aligned}$$

□

Since the non-linearity of an (n, m)-function is by definition equal to the non-linearity of a particular Boolean function, we see from Proposition 2.1.7 and Corollary 2.1.6 that

$\max_{a\in\mathbb{F}_{2^n},\, b\in\mathbb{F}_{2^m}^*} |W_f(a,b)|$ must satisfy the same bounds as $\max_{a\in\mathbb{F}_{2^n}} |W_f(a)|$, that is,

$$2^{n/2} \leq \max_{a\in\mathbb{F}_{2^n},\, b\in\mathbb{F}_{2^m}^*} |W_f(a,b)| \leq 2^n. \tag{2.1}$$

In conjunction with Proposition 2.1.21 above, this gives us a natural extension of Definition 2.1.10:

Definition 2.1.22 (Bent (n,m)-Function)**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called* bent *if for all $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}^*$ we have*

$$|W_f(a,b)| = 2^{n/2}.$$

There are three equivalent characterizations of bent (n,m)-functions that will be used interchangeably throughout this thesis:

Theorem 2.1.23. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The following statements are equivalent:*

i. For any $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^m}^*$ we have $|W_f(a,b)| = 2^{n/2}$.

ii. The function $x \mapsto Tr_1^m(bf(x))$ is bent for all $b \in \mathbb{F}_{2^m}^*$

iii. The function $D_a f(x) = f(x+a) - f(x)$ is balanced for all $a \in \mathbb{F}_{2^n}^*$.

Proof. We will show that (i) holds if and only if (ii) holds, and likewise that (ii) holds if and only if (iii) holds:

For $b \in \mathbb{F}_{2^m}^*$, let $g_b(x) = Tr_1^m(bf(x))$. Then the component functions of f are exactly the functions $g_b(x)$, and we have $W_{g_b}(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g_b(a)+Tr(ax)} = W_f(a,b)$ for any $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}^*$. Therefore (i) holds if and only if (ii) holds.

By Theorem 2.1.13, the function $g_b(x) = Tr_1^m(bf(x))$ is bent for all $b \in \mathbb{F}_{2^m}^*$ if and only if the function $x \mapsto g_b(x+a) - g_b(x)$ is balanced for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^m}^*$. As the function $x \mapsto g_b(x+a) - g_b(x)$ is equal to the function $x \mapsto Tr_1^m(bD_a f(x))$, we see by Proposition 1.3.31 that the function $D_a f(x)$ is balanced for all $a \in \mathbb{F}_{2^n}^*$ if and only if $Tr_1^m(bf(x))$ is bent for all $b \in \mathbb{F}_{2^m}^*$. Therefore (ii) holds if and only if (iii) holds. □

Remark 2.1.24. Property (ii) above immediately shows us that, for any polynomial $P(x) \in \mathbb{F}_{2^n}[x]$, it is necessary for $Tr_1^n(P(x))$ to be bent in order for $Tr_m^n(P(x))$ to be bent, since the former is a component function of the latter. Therefore every class of vectorial bent functions can be viewed as an extension of a class of Boolean bent functions. In particular, we have from [40] that every vectorial bent function of the form $Tr_m^n(ax^d)$ in dimension 24 or less is in (a vectorial extension of) one of the five classes described in Table 1.1 (see the remarks immediately preceding Table 1.1).

In [56], Nyberg showed that if $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is bent, then the dimension of the range $\mathbb{F}_{2^m}$ is bounded above by $n/2$: in particular, there are no bent functions that map $\mathbb{F}_{2^n}$ to itself.

Theorem 2.1.25 (Nyberg bound [56]). *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is bent then $m \leq n/2$.*

Proof. For each $y \in \mathbb{F}_{2^m}$, let

$$a_y = |f^{-1}(y)|.$$

We will show in particular that a_0 has the form

$$a_0 = 2^{n/2-m} b_0 \tag{2.2}$$

where b_0 is an odd integer. Since a_y is an integer for all y this will give the result.

For $c \in \mathbb{F}_{2^m}^*$, let $f_c(x) = Tr_1^m(cf(x))$ be the component function of f corresponding to c. Then

$$W_{f_c}(0) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_c(x)} = \sum_{y \in \mathbb{F}_{2^m}} a_y (-1)^{Tr_1^m(cy)}. \tag{2.3}$$

Taking the sum over all non-zero c gives

$$\begin{aligned}
\sum_{c \in \mathbb{F}_{2^m}^*} W_{f_c}(0) &= \sum_{y \in \mathbb{F}_{2^m}} a_y \sum_{c \in \mathbb{F}_{2^m}^*} (-1)^{Tr_1^m(cy)} \\
&= a_0 \sum_{c \in \mathbb{F}_{2^m}^*} (-1)^{Tr_1^m(c \cdot 0)} + \sum_{y \in \mathbb{F}_{2^m}^*} a_y \sum_{c \in \mathbb{F}_{2^m}^*} (-1)^{Tr_1^m(cy)} \\
&= a_0(2^m - 1) + \sum_{y \in \mathbb{F}_{2^m}^*} a_y \left(\sum_{c \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(cy)} - (-1)^{Tr_1^m(0 \cdot y)} \right) \\
&= a_0(2^m - 1) - \sum_{y \in \mathbb{F}_{2^m}^*} a_y. \qquad (2.4)
\end{aligned}$$

Since f is bent we have $W_{f_c}(0) = \pm 2^{n/2}$ for all $c \in \mathbb{F}_{2^m}^*$, therefore $\sum_{c \in \mathbb{F}_{2^m}^*} W_{f_c}(0)$ is a multiple of $2^{n/2}$. Let

$$S = 2^{-n/2} \sum_{c \in \mathbb{F}_{2^m}^*} W_{f_c}(0).$$

From (2.4) we have

$$\begin{aligned}
S &= 2^{-n/2} \left(a_0(2^m - 1) - \sum_{y \in \mathbb{F}_{2^m}^*} a_y \right) \\
&= 2^{-n/2} \left(a_0(2^m - 1) + a_0 - \sum_{y \in \mathbb{F}_{2^m}} a_y \right) \\
&= 2^{-n/2} \left(a_0 2^m - 2^n \right) \\
&= a_0 2^{m-n/2} - 2^{n/2}. \qquad (2.5)
\end{aligned}$$

If S is odd then $a_0 2^{m-n/2}$ must be odd and therefore a_0 must have the form (2.2), that is, $a_0 = 2^{n/2-m}b_0$ where b_0 is an odd integer. Therefore to prove the theorem it suffices to show that S is odd.

For $i \in \{0, 1\}$ let

$$r_i = \#\{c \in \mathbb{F}_{2^m}^* : W_{f_c}(0) = (-1)^i 2^{n/2}\}. \tag{2.6}$$

Then we have

$$\begin{aligned} r_0 + r_1 &= 2^m - 1 \\ \text{and } r_0 - r_1 &= S, \end{aligned}$$

from which it follows that $S = 2r_0 - 2^m + 1$ is odd. □

Given a bent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, the definition (2.6) suggests constructing a second Boolean function on $\mathbb{F}_{2^n}$ by considering the *signs* of the Walsh coefficients of f. This construction features heavily in the literature (see e.g. [12] and [42]) and is commonly called the *dual function*.

Definition 2.1.26. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be bent. The* dual *of f is the function $f^* : \mathbb{F}_{2^n} \to \mathbb{F}_2$ given by*

$$f^*(x) = \begin{cases} 0 \text{ if } W_f(x) = 2^{n/2} \\ 1 \text{ if } W_f(x) = -2^{n/2}. \end{cases}$$

Proposition 2.1.27. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be bent, and let $f^* : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be the dual of f. Then f^* is bent. Furthermore, the dual of f^* is f.*

Proof. For any $\alpha \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned} W_{f^*}(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f^*(x)+Tr(\alpha x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\alpha x)} (-1)^{f^*(x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\alpha x)} 2^{-n/2} W_f(x) \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\alpha x)} 2^{-n/2} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y)+Tr(xy)} \\ &= 2^{-n/2} \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y)+Tr(x(\alpha+y))} \\ &= 2^{-n/2} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x(\alpha+y))} \\ &= 2^{-n/2} (-1)^{f(\alpha)} 2^n \\ &= (-1)^{f(\alpha)} 2^{n/2}. \end{aligned}$$

Hence f^* is bent function. Additionally, by considering the definition of the dual and the fact that the equation $W_{f^*}(\alpha) = (-1)^{f(\alpha)}2^{n/2}$ is valid for all $\alpha \in \mathbb{F}_{2^n}$, one can see that $f^{**} = f$. □

Remark 2.1.28. In the known constructions of bent functions, we observe a trade-off between meeting the Nyberg bound and achieving high algebraic degree. In particular, there is currently no polynomial-time construction that achieves both the Nyberg bound and the Rothaus Bound. The importance of cryptographic functions having high algebraic degree was discussed in Remark 2.1.16. On the other hand, in applications one often desires a bent (n, m)-function to have high output dimension – in particular, this leads to a large number of *Boolean* bent functions as per Theorem 2.1.23 part (ii). In section 2.2.1 we will discuss a class of quadratic bent functions that meet the Nyberg bound, and in the following section 2.2.2 we will discuss a class of bent functions that achieve Rothaus' bound, but can never meet the Nyberg bound.

2.1.3 Hyperbent Functions

In [71], Youssef and Gong defined and studied a class of bent functions that satisfy a stronger condition than that of Definition 2.1.10:

Definition 2.1.29 (Boolean Hyperbent Function)**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called* hyperbent *if, for all $a \in \mathbb{F}_{2^n}$ and for all i coprime with $2^n - 1$, we have*

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

Clearly every hyperbent function is bent, since taking $i = 1$ in the definition above reduces it to Definition 2.1.10.

Proposition 2.1.30 ([12])**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is hyperbent if and only if $f(x^i)$ is bent for all i coprime with $2^n - 1$.*

Proof. Let $j \in \{0, 1, \ldots, 2^n - 2\}$ be such that j is coprime with $2^n - 1$. Since f is hyperbent we have

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax^j)} = \pm 2^{n/2}$$

for all $a \in \mathbb{F}_{2^n}$. Let i be the multiplicative inverse of j modulo $2^n - 1$. Then for any $a \in \mathbb{F}_{2^n}$ we have

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

As the expression on the right is the value of the Walsh transform at the point a of the function $x \mapsto f(x^i)$ this completes the proof. □

The extension to vectorial functions is natural:

Definition 2.1.31 (Vectorial Hyperbent Function)**.** *A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called* hyperbent *if the component function $Tr_1^m(bf(x))$ is hyperbent for all $b \in \mathbb{F}_{2^m}^*$.*

The primary motivation for the notion of a hyperbent function stems from work by Jakobsen and Knudsen [34, 33], and from subsequent work by Gong and Golomb [31]. Jakobsen and Knudsen introduced a new method of cryptanalysis for block ciphers that involved constructing polynomial approximations of the coordinate functions of S-boxes via interpolation. The success of the attack is contingent on the polynomial approximations having few terms and/or low algebraic degree. In a similar vein, Golomb and Gong introduced a new criteria for the design of S-boxes – namely, that it should not be possible to approximate the coordinate functions of an S-box by the trace of a bijective monomial. More precisely, Golomb and Gong proposed that in the design of block cipher algorithms, the Walsh spectrum of each component function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ should be the same as the multiset

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

for each i coprime with $2^n - 1$. Combined with the requirement that each f is highly nonlinear, one can easily see how this criteria leads naturally to the definition of hyperbentness as given by Youssef and Gong.

Recall that bent functions achieve the maximal minimum distance to the set of all affine functions, which are precisely the functions that may be expressed as the trace of a bijective monomial of algebraic degree no greater than one. However, it is possible for the distance from a bent function to the trace of a bijective monomial to be small. For example, Youssef and Gong performed computations showing that 120 of the 896 Boolean bent functions on $\mathbb{F}_{2^4}$ have distance 2 to the monomial function $x \mapsto Tr_1^4(x^7)$ [71]. Thus Youssef and Gong posed – and answered in the affirmative – the question of the existence of functions that have equal distance to all functions expressible as the trace of a bijective monomial [71].

In [15], Carlet and Gaborit showed that hyperbent functions meets Rothaus' bound:

Theorem 2.1.32 (Carlet, Gaborit [15])**.** *Every hyperbent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ can be represented as*

$$f(x) = \sum_{i=1}^{r} Tr(a_i x^{t_i}) + \epsilon, \tag{2.7}$$

where $a_i \in \mathbb{F}_{2^n}$, $\epsilon \in \mathbb{F}_2$, and $\mathrm{wt}_2(t_i) = n/2$. Consequently, all hyperbent functions have algebraic degree $n/2$.

Therefore hyperbent functions achieve the maximum possible algebraic degree among all bent functions on the same domain.

An example of a class of functions that are bent, but not hyperbent, is the class of bent Gold functions. This will be discussed further in subsection 2.2.1. A class of hyperbent functions will be discussed in subsection 2.2.2.

2.2 Results on Certain Classes of Bent Functions

In this section we discuss some known results in the study of Boolean bent functions, focusing on several specific classes of functions. We will then discuss current progress with regards to extending several known Boolean constructions to vectorial ones. Our chief goal will be to provide context for the new results that will be presented in the following section.

The class of bent functions that has been perhaps the most-studied in recent memory is the class of monomial bent functions, which we define now:

Definition 2.2.1 (Monomial Bent Function, Bent Exponent)**.** *A* monomial bent function *is a bent function that may be expressed in the form $Tr_m^n(ax^d)$ for some $a \in \mathbb{F}_{2^n}^*$ and some $d \in \mathbb{N}$. The exponent d (which is taken modulo $2^n - 1$) is called a* bent exponent *if there exists an element $a \in \mathbb{F}_{2^n}^*$ such that $Tr_m^n(ax^d)$ is bent.*

Proposition 2.2.2. *If $Tr_m^n(ax^d)$ is bent then $Tr_m^n(a^{2^{im}}x^{2^{im}d})$ is bent for $0 \leq i \leq n/m - 1$.*

Proof. This follows immediately from the fact that $Tr_m^n(x) = Tr_m^n(x^{2^m})$ for all $x \in \mathbb{F}_{2^n}$. □

In order for a Boolean function of the form $Tr_1^n(ax^d)$ to be bent, there are conditions that must be satisfied by the exponent d:

Lemma 2.2.3 ([42])**.** *Let d be a bent exponent for some Boolean monomial function. Then* $\gcd(d, 2^n - 1) > 1$. *Furthermore, if $f_a(x) = Tr_1^n(ax^d)$ is bent, then*

i. $W_{f_a}(0) = 2^{n/2}$ *if and only if* $\gcd(d, 2^{n/2} + 1) = 1$

ii. $W_{f_a}(0) = -2^{n/2}$ *if and only if* $\gcd(d, 2^{n/2} - 1) = 1$

Proof. If $\gcd(d, 2^n - 1) = 1$, then $x \mapsto x^d$ is a permutation on $\mathbb{F}_{2^n}$ and so for all $a \in \mathbb{F}_{2^n}^*$ we have $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(ax^d)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(ax)} = 0$. Hence $f_a(x) = Tr_1^n(ax^d)$ is balanced for all $a \in \mathbb{F}_{2^n}^*$, which contradicts the assumption that f_a is bent (and hence not balanced by Proposition 2.1.18) for at least one $a \in \mathbb{F}_{2^n}^*$.

Let $g = \gcd(d, 2^n - 1)$, and let $A = \{x \in \mathbb{F}_{2^n} : x^d = 1\}$ (hence by Proposition 1.3.2 we have $A = \{x \in \mathbb{F}_{2^n} : x^g = 1\}$). Let $\alpha \in \mathbb{F}_{2^n}^*$ be such that $f_\alpha(x) = Tr_1^n(\alpha x^d)$ is bent. Observe that f_α is constant on all multiplicative cosets of A. Thus we have

$$W_{f_\alpha}(0) = 1 + g \sum_{x\in\mathbb{F}_{2^n}^*/A} (-1)^{Tr(\alpha x^d)} \equiv 1 \pmod{g}.$$

Since f_α is bent we have $|W_{f_\alpha}(0)| = 2^{n/2}$. If $W_{f_\alpha}(0) = 2^{n/2}$ then g divides $2^{n/2} - 1$, and if $W_{f_\alpha}(0) = -2^{n/2}$ then g divides $2^{n/2} + 1$. Since $\gcd(2^{n/2} - 1, 2^{n/2} + 1) = 1$, this implies that g and hence d must be coprime to either $2^{n/2} - 1$ or $2^{n/2} + 1$. □

It is important to note that a function of the form $Tr_1^n(ax^d)$ cannot be bent for every choice of $a \in \mathbb{F}_{2^n}^*$.

Lemma 2.2.4. *There exists an element $a \in \mathbb{F}_{2^n}^*$ such that the function $Tr_1^n(ax^d)$ is not bent.*

Proof. Suppose to the contrary that the function $Tr_1^n(ax^d)$ is bent for all $a \in \mathbb{F}_{2^n}^*$. Let $\alpha \in \mathbb{F}_{2^n}^*$, and consider the function $F(x) = Tr_n^n(\alpha x^d) = \alpha x^d$. The component functions of F are exactly the functions of the form $Tr_1^n(ax^d)$, $a \in \mathbb{F}_{2^n}^*$. As these are all bent by our assumption, F is bent as per Theorem 2.1.23. However, this is impossible, as it contradicts the Nyberg bound (Theorem 2.1.25). □

In [60], Pott *et al.* stated and proved the following:

Theorem 2.2.5 (Pott *et al.* [60])**.** *Let $P(x) \in \mathbb{F}_{2^n}[x]$ and let $f(x) = Tr_1^n(\lambda P(x))$. The maximum number of coefficients λ such that f is bent is $2^n - 2^{n/2}$.*

Furthermore they showed that this bound is tight by demonstrating that is it met by at least two classes of quadratic bent functions.

Finally, the following is essentially a restatement of Theorem 2.1.23, part (ii):

Proposition 2.2.6 ([64])**.** *Let $C \subset \mathbb{F}_{2^n}$ denote the set of all coefficients c such that the function $f_c(x) = Tr_1^n(cx^d)$ is bent. Then the (n, m)-function $g(x) = Tr_m^n(ax^d)$ is bent if and only if $\{ax : x \in \mathbb{F}_{2^m}^*\} \subseteq C$.*

Proof. Theorem 2.1.23 tells us that g is bent if and only if $Tr_1^m(bg(x)) = Tr_1^m(bTr_m^n(ax^d)) = Tr_1^n(bax^d)$ is bent for all $b \in \mathbb{F}_{2^m}^*$. As b runs through all of $\mathbb{F}_{2^m}^*$, this is the same as requiring that f_c is bent for all $c \in \{ax : x \in \mathbb{F}_{2^m}^*\}$. □

As mentioned in the Introduction, there are five known classes of monomial bent functions. We will now introduce and characterize two of these classes: the Gold class and the Dillon class. For each class we begin with the Boolean characterizations, and then proceed to known extensions to the vectorial case.

2.2.1 Gold Functions and Their Vectorial Extensions

The Gold functions are Boolean monomial functions that were introduced in 1968 by Robert Gold in the context of maximal linear sequences [27].

Definition 2.2.7 (Gold Exponent, Gold Function)**.** *Let $f(x) = Tr_1^n(ax^d)$. The exponent d is called a* Gold exponent *if it is of the form $d = 2^l + 1$ for some $l \in \{1, \ldots, n-1\}$. In this case f is called a* Gold function*.*

Since $\mathrm{wt}_2(2^l + 1) = 2$ for all $l \in \{1, \ldots, n-1\}$, Proposition 1.3.29 implies that all Gold functions have algebraic degree two (i.e., they are quadratic functions). Therefore the bent Gold functions have the lowest possible algebraic degree among non-linear functions. Additionally, we deduce from Theorem 2.1.32 that Gold functions are never hyperbent.

On the other hand, it is possible to construct vectorial extensions of certain bent Gold functions that meet the Nyberg bound. Additionally, bent Gold functions are maximal among monomial bent functions $Tr_1^n(ax^d)$ in the sense that they are bent for the maximum possible number of choices of the coefficient $a \in \mathbb{F}_{2^n}^*$ (see Theorem 2.2.5). Certain vectorial extensions of Gold functions also have this property.

A good characterization of the bent functions that are vectorial extensions of the Gold functions was given by Xu and Wu in [70], which was published during the current author's research on the same topic. After introducing and characterizing the Boolean case, we will present and prove the theorem of Xu and Wu.

Proposition 2.2.8. *Let m and n be integers. Then* $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$.

Proof. Let $d = \gcd(2^n - 1, 2^m - 1)$. As $2^n \equiv 2^m \equiv 1 \pmod{d}$, we have that $2^{nx+my} \equiv 1 \pmod{d}$ for any $x, y \in \mathbb{Z}$. In particular, $2^{\gcd(m,n)} \equiv 1 \pmod{d}$. Therefore d divides $2^{\gcd(m,n)} - 1$, and thus $d \leq 2^{\gcd(m,n)} - 1$.

On the other hand, $2^{\gcd(m,n)} - 1$ divides both $2^n - 1$ and $2^m - 1$, and so $2^{\gcd(m,n)} - 1 \leq d$. Therefore $d = 2^{\gcd(m,n)} - 1$. □

Proposition 2.2.9. *Let m and n be integers. Then*

$$\gcd(2^n - 1, 2^m + 1) = \begin{cases} 1 & \text{if } n/\gcd(m,n) \text{ is odd} \\ 2^{\gcd(m,n)} + 1 & \text{if } n/\gcd(m,n) \text{ is even} \end{cases}.$$

Proof. We observe that $\gcd(2^n - 1, 2^m + 1)$ is a divisor of $\gcd(2^n - 1, 2^{2m} - 1)$ since $2^{2m} - 1 = (2^m - 1)(2^m + 1)$. By Proposition 2.2.8, $\gcd(2^n - 1, 2^m + 1)$ is therefore a divisor of $2^{\gcd(2m,n)} - 1$.

If $n/\gcd(m,n)$ is odd, then $\gcd(2m, n) = \gcd(m, n)$, and so $\gcd(2^n - 1, 2^m + 1)$ divides $2^{\gcd(m,n)} - 1$, which in turn divides $2^m - 1$. As $\gcd(2^m - 1, 2^m + 1) = 1$, we conclude that $\gcd(2^n - 1, 2^m + 1) = 1$.

On the other hand, if $n/\gcd(n,m)$ is even, then $\gcd(2m, n) = 2\gcd(m, n)$, which implies that $\gcd(2^n - 1, 2^m + 1)$ divides $2^{2\gcd(m,n)} - 1 = (2^{\gcd(m,n)} - 1)(2^{\gcd(m,n)} + 1)$. As $\gcd(2^m + 1, 2^{\gcd(m,n)} - 1) = 1$, it must be that $\gcd(2^m + 1, 2^n - 1)$ divides $2^{\gcd(m,n)} + 1$. Now observe that $2^{\gcd(m,n)} + 1$ divides both (i) $2^n - 1$ and (ii) $2^m + 1$.

Observation (i) follows from the fact that $2^{\gcd(m,n)} + 1$ divides $(2^{\gcd(m,n)} + 1)(2^{\gcd(m,n)} - 1) = 2^{2\gcd(m,n)} - 1 = 2^{\gcd(2m,n)} - 1$, which in turn divides $2^n - 1$. Observation (ii) follows from the fact that $(2^{\gcd(m,n)} + 1)(2^{\gcd(m,n)} - 1) = 2^{2\gcd(m,n)} - 1 = 2^{\gcd(2m,n)} - 1$ divides $2^{2m} - 1 = (2^m + 1)(2^m - 1)$, which in turn implies that $2^{\gcd(m,n)} + 1$ divides $2^m + 1$.

We therefore conclude that $\gcd(2^n - 1, 2^m + 1) = 2^{\gcd(m,n)} + 1$. □

Together with Lemma 2.2.3, Proposition 2.2.9 stipulates that if $x \mapsto Tr_1^n(ax^d)$ is a Gold function with $d = 2^l + 1$, then $n/\gcd(l, n)$ must be even.

Theorem 2.2.10 (Gold [27]). *Let $a \in \mathbb{F}_{2^n}$, let l be a positive integer such that $n/\gcd(l,n)$ is even, and let $d = 2^l + 1$. Then the function $f(x) = Tr_1^n(ax^d)$ is bent if and only if*

$$a \notin \{x^d : x \in \mathbb{F}_{2^n}\}.$$

Proof [42]. First, let us suppose that $a \notin \{x^d : x \in \mathbb{F}_{2^n}\}$. Observe that for any $x, y \in \mathbb{F}_{2^n}$ we have

$$(x+y)^d = (x+y)^{d-1}(x+y) = (x^{d-1} + y^{d-1})(x+y) = x^d + y^{d-1}x + yx^{d-1} + y^d.$$

Thus for any $\alpha \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned} W_f(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax^d) + Tr(\alpha x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(a((x+b)^d + b^{d-1}x + bx^{d-1} + b^d)) + Tr(\alpha x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(a(x+b)^d + ab^{d-1}x + abx^{d-1} + ab^d + \alpha x)}. \end{aligned}$$

Observe that if

$$Tr(ab^{d-1}x + abx^{d-1} + \alpha x) = 0 \text{ for all } x \in \mathbb{F}_{2^n} \tag{2.8}$$

then we would have

$$\begin{aligned} W_f(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(a(x+b)^d + ab^d)} \\ &= (-1)^{Tr(ab^d)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(a(x+b)^d)} \\ &= (-1)^{Tr(ab^d)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax^d)} \\ &= (-1)^{Tr(ab^d)} W_f(0). \end{aligned}$$

Thus the Walsh coefficients of f would have constant absolute value. By Theorem 2.1.5, the Walsh spectrum of f would therefore consist entirely of the values $\pm 2^{n/2}$, hence f would be bent. Therefore we consider the linear equation (2.8):

$$\begin{aligned} 0 &= Tr(ab^{d-1}x + abx^{d-1} + \alpha x) \\ &= Tr(a^{d-1}b^{(d-1)^2}x^{d-1} + abx^{d-1} + \alpha^{d-1}x^{d-1}) \\ &= Tr(x^{d-1}(a^{d-1}b^{(d-1)^2} + ab + \alpha^{d-1})). \end{aligned} \tag{2.9}$$

Therefore (2.8) holds for all $x \in \mathbb{F}_{2^n}$ if and only if $a^{d-1}b^{(d-1)^2} + ab + \alpha^{d-1} = 0$. In order to be able to choose such a $b \in \mathbb{F}_{2^n}$, the mapping $b \mapsto a^{d-1}b^{(d-1)^2} + ab$ must be a bijection.

As it is a linear mapping, we must therefore show that the kernel is trivial. To this end, suppose that $a^{d-1}b^{(d-1)^2} + ab = 0$ for some $b \neq 0$. Thus

$$\begin{aligned} & a^{d-1}b^{(d-1)^2} + ab = 0 \\ \Rightarrow\ & b^{(d-1)^2-1} = a^{2-d} \\ \Rightarrow\ & (b^d)^{d-2} = (a^{-1})^{d-2}. \end{aligned} \tag{2.10}$$

Clearly the left-hand side of (2.10) is a d-th power. However, since $\gcd(d, d-2) = 1$, the right-hand side of (2.10) is a d-th power if and only if a is a d-th power, contrary to our hypothesis. Therefore we conclude that f is bent whenever $a \notin \{x^d : x \in \mathbb{F}_{2^n}\}$.

Now let us suppose that $a \in \{x^d : x \in \mathbb{F}_{2^n}\}$, and, seeking a contradiction, suppose furthermore that f is bent. Clearly a must be non-zero, therefore we may write $a = c^d$ for some $c \in \mathbb{F}_{2^n}^*$. Then

$$\begin{aligned} f(x) &= Tr_1^n\left(ax^d\right) \\ &= Tr_1^n\left((cx)^d\right). \end{aligned} \tag{2.11}$$

By Proposition 2.1.9, the function $x \mapsto f(bx)$ is bent for any $b \in \mathbb{F}_{2^n}^*$. By (2.11), this implies that f is bent for *any* choice of $a \in \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Since we have already proven that f is bent whenever $a \notin \{x^d : x \in \mathbb{F}_{2^n}\}$, we therefore conclude that f is bent for all $a \in \mathbb{F}_{2^n}^*$. We have already seen that this is impossible in Lemma 2.2.4. □

The recently-found characterization of the vectorial extensions of the monomial Gold functions turned out to be very similar to the characterization of the Boolean case. We note that Dong *et al.* had earlier proven the sufficiency of the condition in the special case of monomial Gold functions mapping $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{n/2}}$ [24].

Theorem 2.2.11 (Xu, Wu [70])**.** *Let m be a proper divisor of n, and let $t = \frac{2^n-1}{2^m-1}$. Let l be an integer such that $n/\gcd(l,n)$ is even, and let $d = 2^l + 1$. Then the function $f(x) = Tr_m^n(ax^d)$ is bent if and only if*

$$a \notin \{x^{\gcd(d,t)} : x \in \mathbb{F}_{2^n}\}.$$

Proof. Let $D = \{x^d : x \in \mathbb{F}_{2^n}\}$. By Theorem 2.2.10, the set of coefficients b such that the function $x \mapsto Tr_1^n(bx^d)$ is bent is $C := \{b \in \mathbb{F}_{2^n} : b \notin D\}$. By Proposition 2.2.6, $f(x) = Tr_m^n(ax^d)$ is bent if and only if $\{ax : x \in \mathbb{F}_{2^m}^*\} \subseteq C$, i.e., if and only if $\{ax : x \in \mathbb{F}_{2^m}^*\} \cap D$ is empty. This in turn is true if and only if $a \notin \{xy : x \in \mathbb{F}_{2^m}^*,\ y \in D\}$.

Let $\gamma \in \mathbb{F}_{2^n}$ be primitive. Then γ^t is a primitive element of $\mathbb{F}_{2^m}^*$, and furthermore we have $D = \{x^d : x \in \mathbb{F}_{2^n}\} = \{\gamma^{i\cdot\gcd(d,2^n-1)} : i = 0, 1, \ldots, 2^n - 2\}$. Thus we have

$$\{xy : x \in \mathbb{F}_{2^m}^*,\ y \in D\} = \{\gamma^{i\cdot t}\gamma^{j\cdot\gcd(d,2^n-1)} : 0 \leq i, j \leq 2^n - 2\}$$

$$= \{\gamma^{i\cdot\gcd(t,\gcd(d,2^n-1))} : 0 \le i \le 2^n-2\}$$
$$= \{\gamma^{i\cdot\gcd(d,t)} : 0 \le i \le 2^n-2\}$$
$$= \{x^{\gcd(d,t)} : x \in \mathbb{F}_{2^n}\}\backslash\{0\}.$$

As it is clear that $Tr_m^n(ax^d)$ is not bent when $a = 0$, the result holds. □

Remark 2.2.12. Note that, according to the theorem above and Proposition 1.3.2, vectorial bent functions $x \mapsto Tr_m^n(ax^d)$ where d is a Gold exponent exist if and only if $\gcd(2^n - 1, \gcd(d,t)) > 1$, since this is the condition required for the set $\mathbb{F}_{2^n}\backslash\{x^{\gcd(d,t)} : x \in \mathbb{F}_{2^n}\}$ to be non-empty. This is achieved if we take $d = 2^m + 1$, for example.

In particular, we have by Theorem 2.2.11 that $f(x) = Tr_m^{2m}(ax^{2^m+1})$ is bent whenever $a \notin \{x^{2^m+1} : x \in \mathbb{F}_{2^{2m}}\}$. Since we have

$$\#\{x^{2^m+1} : x \in \mathbb{F}_{2^{2m}}\} = 1 + \frac{2^{2m}-1}{\gcd(2^m+1, 2^{2m}-1)} = 2^m$$

by Proposition 1.3.2, f is therefore bent for $2^{2m} - 2^m$ choices of a. This demonstrates that the Gold family produces vectorial bent functions that meet the Nyberg bound.

Recall that, for any polynomial $P(x) \in \mathbb{F}_{2^n}[x]$, the maximum number of coefficients $a \in \mathbb{F}_{2^n}$ such that the Boolean function $x \mapsto Tr_1^n(aP(x))$ is bent is $2^n - 2^{n/2}$ (see Theorem 2.2.5). Clearly this bound also applies to vectorial extensions $x \mapsto Tr_m^n(aP(x))$ (see Remark 2.1.24). Therefore the vectorial Gold functions described above are maximal in this sense as well.

2.2.2 Dillon Functions

In his Ph.D. thesis [21], J.F. Dillon introduced what he called *partial spread* (PS) functions, which are functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_2$ whose support consists of the union of $N \in \{2^{m-1}, 2^{m-1}+1\}$ m-dimensional subspaces of $\mathbb{F}_{2^{2m}}$ such that any two intersect only at the origin. The class having $N = 2^{m-1}$ is called PS^-, and the class having $N = 2^{m-1}+1$ is called PS^+. The following theorem characterizes the bent functions in the PS^- class.

Theorem 2.2.13 (Dillon [21])**.** *Let $S_1, \ldots, S_N$ be a collection of m-dimensional subspaces of $\mathbb{F}_{2^{2m}}$ such that $S_i \cap S_j = \{0\}$ whenever $i \neq j$. Suppose $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ is such that $\mathrm{supp}(f) = \bigcup_{i=1}^N S_i^*$. Then f is bent if and only if $N = 2^{m-1}$.*

Of particular interest to us is a subclass of PS^- called PS_{ap}, also introduced in [21] (here "ap" stands for "affine plane"). Recall that $\mathbb{F}_{2^{2m}}$ is isomorphic to $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. The constructions in the PS_{ap} class are based on the fact that $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ may be decomposed into a collection of $2^m + 1$ pairwise distinct lines that pass through the origin, with each line containing $2^m - 1$ non-zero points. Each of these lines through the origin constitutes an m-dimensional subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ (which is itself a $2m$-dimensional vector space over

$\mathbb{F}_2$). Indeed, these are exactly the subspaces where the function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^* \to \mathbb{F}_{2^m}$ defined by

$$(x, y) \mapsto \frac{x}{y} = xy^{2^m-2} \tag{2.12}$$

has constant value. A PS_{ap} function is any function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$ that is constant on each such subspace. By Theorem 2.2.13, constructing a bent function f in the PS_{ap} class therefore amounts to choosing 2^{m-1} such subspaces to be the support of f. Thus the class of bent PS_{ap} functions may be described as all functions of the form $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ with

$$f(x, y) = g(xy^{2^m-2}) \tag{2.13}$$

where $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is any balanced function with $g(0) = 0$.

These functions have the following notable property:

Theorem 2.2.14 (Dillon [21])**.** *Let $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a balanced function such that $g(0) = 0$, and let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined in terms of g by*

$$f(x, y) = g(xy^{2^m-2}).$$

Then f has algebraic degree equal to m.

Therefore every bent function in the PS_{ap} class meets Rothaus' bound (see Theorem 2.1.14).

The decomposition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ into lines through the origin can be viewed as a decomposition of $\mathbb{F}_{2^{2m}}$ into polar coordinates, since $\mathbb{F}_{2^{2m}}^*$ may be expressed as the Cartesian product of $\mathbb{F}_{2^m}^*$ with a *unit circle* of order $2^m + 1$, which consists of all the elements of norm 1 relative to $\mathbb{F}_{2^m}$. We formalize these ideas below:

Definition 2.2.15 (Cyclic Subgroup of Order $2^m + 1$)**.** *The set*

$$\mathcal{U} := \{x \in \mathbb{F}_{2^{2m}} : x^{2^m+1} = 1\}$$

is called the cyclic subgroup of order $2^m + 1$ *in* $\mathbb{F}_{2^{2m}}^*$.

Remark 2.2.16. Let $\omega \in \mathbb{F}_{2^{2m}}^*$ be primitive. The generators of $\mathcal{U}$ are the elements of the form $\omega^{t(2^m-1)}$, where $\gcd(t, 2^m + 1) = 1$. Hence $\mathcal{U}$ consists of all the $(2^m - 1)$-st powers in $\mathbb{F}_{2^{2m}}^*$. Additionally, note that for all $u \in \mathcal{U}$ we have $u^{2^m} = u^{-1}$.

Proposition 2.2.17. *For any $\alpha \in \mathbb{F}_{2^{2m}}^*$, we have $\alpha = \beta u$ for some $\beta \in \mathbb{F}_{2^m}^*$ and $u \in \mathcal{U}$. Furthermore, this decomposition is unique.*

Proof. Let $t = 2^{m-1}$, and note that $t(2^m + 1) - (t + 1)(2^m - 1) = 1$. For $\alpha \in \mathbb{F}_{2^{2m}}^*$, we have

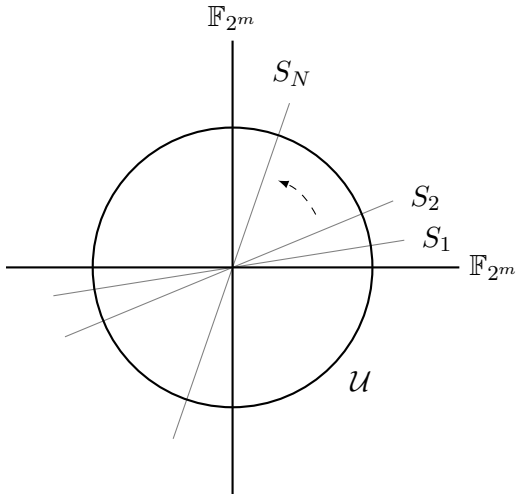
$$\alpha = \alpha^{t(2^m+1)-(t+1)(2^m-1)}$$

$$= \alpha^{t(2^m+1)}\alpha^{-(t+1)(2^m-1)}.$$

Clearly $\alpha^{t(2^m+1)} \in \mathbb{F}_{2^m}^*$ and $\alpha^{-(t+1)(2^m-1)} \in \mathcal{U}$.

To see uniqueness, note that we have $\#\mathcal{U} = 2^m + 1$, $\#\mathbb{F}_{2^m}^* = 2^m - 1$, and $\#\mathbb{F}_{2^{2m}}^* = 2^{2m} - 1 = (2^m + 1)(2^m - 1)$. Therefore it must be that each element of $\mathbb{F}_{2^{2m}}^*$ corresponds to a unique pair in $\mathbb{F}_{2^m}^* \times \mathcal{U}$. □

Figure 2.1: Decomposing $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} = \mathbb{F}_{2^{2m}}$



A partial decomposition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} = \mathbb{F}_{2^{2m}}$ into pairwise distinct lines $S_1, \ldots, S_N$ through the origin is depicted in Figure 2.1. Note that each line S_i, which is an m-dimensional subspace of $\mathbb{F}_{2^{2m}}$, is uniquely determined by a point in $\mathcal{U}$. Therefore in the context of $\mathbb{F}_{2^{2m}}^*$ as the Cartesian product $\mathbb{F}_{2^m}^* \times \mathcal{U}$, the m-dimensional subspaces where the function (2.12) takes constant value are uniquely determined by points in $\mathcal{U}$. Now note that $x \mapsto x^{2^m-1}$ maps $\mathbb{F}_{2^{2m}}^*$ onto $\mathcal{U}$. This may be seen by noting that for any $x \in \mathbb{F}_{2^{2m}}^*$ we have $x = yz$ for a unique pair $(y, z) \in \mathbb{F}_{2^m}^* \times \mathcal{U}$, as per Proposition 2.2.17 above. Thus we have $x^{2^m-1} = (yz)^{2^m-1} = y^{2^m-1}z^{2^m-1} = z^{2^m-1}$. Since the mapping $u \mapsto u^{2^m-1}$ is a permutation on $\mathcal{U}$, this determines a unique element of $\mathcal{U}$, and thus a unique m-dimensional subspace of $\mathbb{F}_{2^{2m}}$. Thus an instance the PS_{ap} functions may be expressed in a univariate representation as the functions $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ with

$$f(x) = Tr_1^{2m}(ax^{2^m-1}),\ a \in \mathbb{F}_{2^{2m}}^*. \tag{2.14}$$

We will call functions of the kind (2.14) *Dillon functions.*

Definition 2.2.18 (Dillon Exponent, Dillon Function)**.** *Let $f(x) = Tr_1^{2m}(ax^d)$. The exponent d is called a* Dillon exponent *if $d = 2^m - 1$. In this case f is called a* Dillon function*.*

By Theorem 2.2.13, a Dillon function of the form (2.14) is thus a bent function if and only if its support has the requisite cardinality of 2^{m-1}. This condition is contingent upon the choice of the coefficient a. Later on in this section we will show the derivation of the exact condition on the coefficient a that leads to a bent Dillon function of the form (2.14).

Recall Proposition 1.3.29, which states that the algebraic degree of a monomial function $x \mapsto Tr(ax^d)$ is equal to the 2-weight of the exponent d. Since $2^m-1 = 1+2+2^2+\ldots+2^{m-1}$, we observe that Dillon functions on $\mathbb{F}_{2^{2m}}$ have algebraic degree equal to m, in agreement with Theorem 2.2.14. This is in stark contrast to the Gold functions, which have exponents of the form $d = 2^l + 1$, and thus have algebraic degree equal to two (the lowest possible among non-linear functions).

When considering the non-linearity of a Dillon function $f(x) = Tr_1^{2m}(ax^{2^m-1})$, we may assume without loss of generality that $a \in \mathbb{F}_{2^m}^*$. The reason for this is provided by Propositions 2.2.19 and 2.2.20.

Proposition 2.2.19. *Let $\alpha \in \mathbb{F}_{2^{2m}}^*$, and write $\alpha = \beta u$ for $\beta \in \mathbb{F}_{2^m}^*$, $u \in \mathcal{U}$. Let k be a positive integer dividing $2m$, and define $f_\alpha : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ and $f_\beta : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ by*

$$f_\alpha(x) = Tr_k^{2m}(\alpha x^{2^m-1}),$$
$$f_\beta(x) = Tr_k^{2m}(\beta x^{2^m-1}).$$

Then there exists an element $v \in \mathbb{F}_{2^{2m}}^*$ such that $f_\alpha(x) = f_\beta(vx)$.

Proof. Since $u \in \mathcal{U}$, there exists an element $v \in \mathbb{F}_{2^{2m}}^*$ such that $u = v^{2^m-1}$. Thus we have

$$\begin{aligned} f_\alpha(x) &= Tr_k^{2m}(\alpha x^{2^m-1}) \\ &= Tr_k^{2m}(\beta u x^{2^m-1}) \\ &= Tr_k^{2m}(\beta (vx)^{2^m-1}) \\ &= f_\beta(vx). \end{aligned}$$

□

Proposition 2.2.20 ([17])**.** *Let $\alpha \in \mathbb{F}_{2^{2m}}^*$, and let $\beta \in \mathbb{F}_{2^m}^*$, $u \in \mathcal{U}$ be such that $\alpha = \beta u$. Then the functions $f_\alpha : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ and $f_\beta : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ defined as*

$$f_\alpha(x) = Tr_1^{2m}(\alpha x^{2^m-1}),$$
$$f_\beta(x) = Tr_1^{2m}(\beta x^{2^m-1})$$

have identical Walsh spectra.

Proof. By Proposition 2.2.19 there exists an element $v \in \mathbb{F}_{2^{2m}}^*$ such that $f_\alpha(x) = f_\beta(vx)$. Note that $x \mapsto xv$ is a permutation on $\mathbb{F}_{2^{2m}}$. Then for $a \in \mathbb{F}_{2^{2m}}$ we have

$$\begin{aligned} W_{f_\beta}(a) &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{f_\beta(x)+Tr(ax)} \\ &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{f_\beta(vx)+Tr(avx)} \\ &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{f_\alpha(x)+Tr(avx)} \\ &= W_{f_\alpha}(av). \end{aligned}$$

Since $x \mapsto xv$ is a permutation on $\mathbb{F}_{2^{2m}}$, it follows that the multisets $\{W_{f_\alpha}(a) : a \in \mathbb{F}_{2^{2m}}\}$ and $\{W_{f_\beta}(a) : a \in \mathbb{F}_{2^{2m}}\}$ are identical. □

We now define a special class of exponential sums, which completely determine the Walsh spectra of Dillon functions.

Definition 2.2.21 (Kloosterman Sum, Kloosterman Zero)**.** *Let $a \in \mathbb{F}_{2^n}^*$. The* Kloosterman sum over $\mathbb{F}_{2^n}$ at a *is defined as*

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

If $a \in \mathbb{F}_{2^n}^*$ is such that $\mathcal{K}_{2^n}(a) = 0$, then a is called a Kloosterman zero in $\mathbb{F}_{2^n}$*.*

Remark 2.2.22. Some authors choose to define the Kloosterman sum by taking the sum over $\mathbb{F}_{2^n}^*$ rather than over all of $\mathbb{F}_{2^n}$, though this is becoming less common. This version is denoted by $K_{2^n}(a)$, and we have

$$K_{2^n}(a) := \mathcal{K}_{2^n}(a) - 1.$$

We use Definition 2.2.21 instead of this version, mainly so as to avoid confusion in conjunction with the use of the phrase *Kloosterman zero*, which would otherwise be defined as an element $a \in \mathbb{F}_{2^n}^*$ such that $K_{2^n}(a) = -1$. Indeed, there is no $a \in \mathbb{F}_{2^n}^*$ such that $K_{2^n}(a) = 0$, as will be established by Theorem 2.2.23 below.

As we will soon see, constructing a bent Dillon function mapping $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_2$ is equivalent to finding a Kloosterman zero in $\mathbb{F}_{2^m}$. For this reason, it is important to establish that Kloosterman zeros do, in fact, exist. The following theorem was proven by Lachaud and Wolfmann using connections to the theory of elliptic curves (the interested reader is referred to Appendix A for more on this topic).

Theorem 2.2.23 (Lachaud, Wolfmann [38]). *The image of $\mathbb{F}_{2^n}^*$ in $\mathbb{Z}$ under the mapping $x \mapsto \mathcal{K}_{2^n}(x)$ consists of all integers in the interval $[1 - 2^{n/2+1}, 1 + 2^{n/2+1}]$ congruent to* 0 (mod 4).

In particular, we conclude the following:

Corollary 2.2.24. *For all $n > 1$ there exists an element $a \in \mathbb{F}_{2^n}^*$ such that $\mathcal{K}_{2^n}(a) = 0$ and an element $b \in \mathbb{F}_{2^n}^*$ such that $\mathcal{K}_{2^n}(b) \neq 0$.*

The following well-known fact will be used often:

Proposition 2.2.25. *For any $a \in \mathbb{F}_{2^n}$, we have $\mathcal{K}_{2^n}(a) = \mathcal{K}_{2^n}(a^2)$.*

Proof. By Theorem 1.3.9 and the fact that $x \mapsto x^2$ is a permutation on $\mathbb{F}_{2^n}$, we have

$$\begin{aligned}
\mathcal{K}_{2^n}(a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{2^n-2}+ax)} \\
&= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr((x^{2^n-2}+ax)^2)} \\
&= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{2(2^n-2)}+a^2x^2)} \\
&= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr(y^{2^n-2}+a^2y)} \\
&= \mathcal{K}_{2^n}(a^2).
\end{aligned}$$

□

Remark 2.2.26. Proposition 2.2.25 shows that if $a \in \mathbb{F}_{2^n}^*$ is a Kloosterman zero in $\mathbb{F}_{2^n}$, then we obtain the additional Kloosterman zeros $a^2, a^4, \ldots, a^{2^{n-1}} \in \mathbb{F}_{2^n}^*$ "for free". In other words, we may consider zeros of the Kloosterman sum over $\mathbb{F}_{2^n}$ as being distinct up to equivalence under the mapping $x \mapsto x^2$.

To characterize the Walsh spectra of Dillon functions in terms of Kloosterman sums, we will need the following proposition and lemma. The first statement establishes a 2-to-1 correspondence between the non-identity elements of $\mathcal{U}$ and the elements $x \in \mathbb{F}_{2^m}$ such that $Tr_1^m(x^{-1}) = 1$. The second statement gives the value of the Kloosterman sum at point $a \in \mathbb{F}_{2^m}^*$ in terms of a relatively simple exponential sum over $\mathcal{U}$.

Proposition 2.2.27 (Delsarte, Goethals [20]). *Let γ be a generator of $\mathcal{U}$. Then*

$$\{\gamma^i + \gamma^{-i} : 1 \leq i \leq 2^m\} = \{x \in \mathbb{F}_{2^m} : Tr_1^m(x^{-1}) = 1\}.$$

Proof [39]. Let $u \in \mathbb{F}_{2^m}^*$ be such that $Tr_1^m(u^{-1}) = 1$, and consider the equation

$$x^2 + ux + 1 = 0 \tag{2.15}$$

along with the equivalent equation

$$y^2 + y = u^{-2} \tag{2.16}$$

(with the latter being obtained from the former by setting $uy = x$). Since $Tr_1^m(u^{-1}) = Tr_1^m(u^{-2}) = 1$, (2.16) has no solutions in $\mathbb{F}_{2^m}$ by Theorem 1.3.10. The polynomial x^2+ux+1 is therefore irreducible over $\mathbb{F}_{2^m}$, and thus it has two roots z_1, z_2 in the quadratic extension $\mathbb{F}_{2^{2m}}$. These roots are conjugates over $\mathbb{F}_{2^m}$, and thus we have

$$z_1 + z_2 = u, \qquad z_1 z_2 = 1, \qquad z_2 = z_1^{2^m}.$$

Therefore

$$z_1^{2^m+1} = 1, \qquad u = z_1 + z_1^{-1}, \qquad z_1 \neq 1.$$

Therefore there exists $i \in \{1, \ldots, 2^m\}$ such that $u = \gamma^i + \gamma^{-i}$.

Conversely, if $u = \gamma^i+\gamma^{-i}$ then (2.16) has no solution $y \in \mathbb{F}_{2^m}$, and therefore $Tr_1^m(u^{-2}) = Tr_1^m(u^{-1}) = 1$ by Theorem 1.3.10. □

Lemma 2.2.28. *Let $a \in \mathbb{F}_{2^m}^*$. Then*

$$\sum_{z \in \mathcal{U}} (-1)^{Tr(az)} = 1 - \mathcal{K}_{2^m}(a).$$

Proof [42]. Note that for all $u \in \mathcal{U}$ we have

$$Tr_m^{2m}(u) = u + u^{2^m} = u + u^{-1}. \tag{2.17}$$

Therefore $Tr(az) = Tr_1^m(aTr_m^{2m}(z)) = Tr_1^m(a(z + z^{-1}))$, and so

$$\begin{aligned}\sum_{z \in \mathcal{U}} (-1)^{Tr(az)} &= \sum_{z \in \mathcal{U}} (-1)^{Tr_1^m(a(z+z^{-1}))} \\ &= 1 + \sum_{\substack{z \in \mathcal{U} \\ z \neq 1}} (-1)^{Tr_1^m(a(z+z^{-1}))}.\end{aligned}$$

By Proposition 2.2.27, for every non-identity element $z \in \mathcal{U}$, the element $z + z^{-1}$ may be uniquely represented by an element of the form $1/b = b^{2^m-2}$ for some $b \in \mathbb{F}_{2^m}^*$ such that $Tr_1^m(b) = 1$. Conversely, each element of the form $1/b$ for some $b \in \mathbb{F}_{2^m}^*$ such that $Tr_1^m(b) = 1$ uniquely represents the set $\{z, z^{-1}\}$. Thus

$$\sum_{z \in \mathcal{U}} (-1)^{Tr(az)} = 1 + 2 \sum_{\substack{b \in \mathbb{F}_{2^m}^* \\ Tr_1^m(b)=1}} (-1)^{Tr_1^m(ab^{2^m-2})}$$

$$= 1 + 2\left(\sum_{b\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(ab^{2^m-2})} - \sum_{\substack{b\in\mathbb{F}_{2^m}\\ Tr_1^m(b)=0}} (-1)^{Tr_1^m(ab^{2^m-2})}\right)$$

$$= 1 + 2\left(\sum_{b\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(ab^{2^m-2})}\right) - 2\left(\sum_{\substack{b\in\mathbb{F}_{2^m}^*\\ Tr_1^m(b)=0}} (-1)^{Tr_1^m(ab^{2^m-2})}\right) - 2$$

$$= -1 - 2\left(\sum_{\substack{b\in\mathbb{F}_{2^m}^*\\ Tr_1^m(b)=0}} (-1)^{Tr_1^m(ab^{2^m-2})} - \sum_{b\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(ab^{2^m-2})}\right).$$

By Theorem 1.3.10, $Tr_1^m(b) = 0$ implies that $b = x^2 + x$ has exactly two solutions in $\mathbb{F}_{2^m}$. The solutions of $0 = x^2 + x$ are exactly the elements of $\mathbb{F}_2$. Therefore

$$\sum_{\substack{b\in\mathbb{F}_{2^m}^*\\ Tr_1^m(b)=0}} (-1)^{Tr_1^m(ab^{2^m-2})} = \frac{1}{2}\sum_{c\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m(a(c^2+c)^{2^m-2})}.$$

On the other hand, $\sum_{b\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(ab^{2^m-2})} = 0$ by Proposition 1.3.14. Thus we have

$$\begin{aligned}
\sum_{z\in\mathcal{U}} (-1)^{Tr(az)} &= -1 - 2\left(\frac{1}{2}\sum_{c\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m(a(c^2+c)^{2^m-2})} - 0\right)\\
&= -1 - \sum_{c\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m(a(c^2+c)^{2^m-2})}\\
&= -1 - \sum_{c\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m\left(\frac{a}{c^2+c}\right)}\\
&= -1 - \sum_{c\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m\left(a\left(\frac{1}{c}+\frac{1}{1+c}\right)\right)}\\
&= -1 - \sum_{d\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m\left(a\left(d+\frac{d}{1+d}\right)\right)}\\
&= -1 - \sum_{d\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m\left(a\left((d+1)+\frac{(d+1)}{1+(d+1)}\right)\right)}\\
&= -1 - \sum_{d\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2} (-1)^{Tr_1^m\left(a\left(d+\frac{1}{d}\right)\right)}\\
&= -1 - \sum_{d\in a^{-1}\mathbb{F}_{2^m}\setminus a^{-1}\mathbb{F}_2} (-1)^{Tr_1^m\left(a\left(ad+\frac{1}{ad}\right)\right)}\\
&= -1 - \sum_{d\in a^{-1}\mathbb{F}_{2^m}\setminus a^{-1}\mathbb{F}_2} (-1)^{Tr_1^m\left(a^2d+\frac{1}{d}\right)}
\end{aligned}$$

$$
\begin{aligned}
&= -1 - \sum_{d \in a^{-1/2}\mathbb{F}_{2^m} \setminus a^{-1/2}\mathbb{F}_2} (-1)^{Tr_1^m\left(ad + \frac{1}{d}\right)} \\
&= -1 - \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(ax + x^{2^m-2})} - \sum_{x \in \{0, a^{2^m-1}-1\}} (-1)^{Tr_1^m(ax + x^{2^m-2})} \right) \\
&= -1 - (\mathcal{K}_{2^m}(a) - 2) \\
&= 1 - \mathcal{K}_{2^m}(a).
\end{aligned}
$$

□

Finally, the following theorem reveals the connection between Kloosterman sums and the Walsh spectra of Dillon functions. Namely, it shows that the Walsh spectrum of a Dillon function consists of at most three distinct values, and is completely determined by the value of the Kloosterman sum at a particular point.

Theorem 2.2.29 (Dillon [21])**.** *Let $\alpha \in \mathbb{F}_{2^{2m}}$, let $a \in \mathbb{F}_{2^m}^*$, and let $f(x) = Tr_1^{2m}(ax^{2^m-1})$. Then*

$$
W_f(\alpha) = \begin{cases} 2^m + \mathcal{K}_{2^m}(a)(1 - 2^m) & \text{if } \alpha = 0 \\ 2^m(-1)^{Tr_1^{2m}(a\alpha^{2^m-1})} + \mathcal{K}_{2^m}(a) & \text{if } \alpha \neq 0. \end{cases}
$$

In [17], Charpin and Gong attributed the main argument of the following proof to Leander [42].

Proof [17]. For any $x \in \mathbb{F}_{2^{2m}}^*$ we have $x = yz$ for some $y \in \mathbb{F}_{2^m}^*$ and $z \in \mathcal{U}$. Then for $\alpha \in \mathbb{F}_{2^{2m}}^*$ we have

$$
\begin{aligned}
W_f(\alpha) &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{Tr(ax^{2^m-1} + \alpha x)} \\
&= 1 + \sum_{z \in \mathcal{U}} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{Tr(az^{2^m-1} + \alpha yz)} && \text{(by Proposition 2.2.17)} \\
&= 1 + \sum_{z \in \mathcal{U}} (-1)^{Tr(a/z^2)} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{Tr(\alpha yz)} \\
&= 1 + \sum_{z \in \mathcal{U}} (-1)^{Tr(a/z^2)} \left(-1 + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr(\alpha yz)} \right). && (2.18)
\end{aligned}
$$

Since

$$
Tr(\alpha yz) = Tr_1^m(Tr_m^{2m}(\alpha yz)) = Tr_1^m(yTr_m^{2m}(\alpha z)) = Tr_1^m(y(\alpha z + \alpha^{2^m} z^{-1})),
$$

we have $\sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr(\alpha yz)} \neq 0$ if and only if $\alpha z = \alpha^{2^m} z^{-1}$, or what is the same, $z^2 = \alpha^{2^m-1}$. In this case we must then have $\sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr(\alpha yz)} = 2^m$ by Proposition 1.3.14.

Therefore

$$W_f(\alpha) = 1 + 2^m \sum_{\substack{z \in \mathcal{U} \\ z^2 = \alpha^{2^m-1}}} (-1)^{Tr(a/z^2)} - \sum_{z \in \mathcal{U}} (-1)^{Tr(a/z^2)}$$
$$= 1 + 2^m (-1)^{Tr(a/\alpha^{2^m-1})} - \sum_{z \in \mathcal{U}} (-1)^{Tr(az)}. \tag{2.19}$$

The last equality follows from the fact that the mappings $z \mapsto z^2$ and $z \mapsto 1/z^2$ permute the elements of $\mathcal{U}$.

Finally, we have $Tr(a/\alpha^{2^m-1}) = Tr((a/\alpha^{2^m-1})^{2^m}) = Tr(a\alpha^{2^m-1})$, and by Lemma 2.2.28, we have $\sum_{z \in \mathcal{U}} (-1)^{Tr(az)} = 1 - \mathcal{K}_{2^m}(a)$, and thus

$$W_f(\alpha) = 2^m (-1)^{Tr(a\alpha^{2^m-1})} + \mathcal{K}_{2^m}(a).$$

Now suppose that $\alpha = 0$. By (2.18), we have

$$W_f(0) = 1 + \sum_{z \in \mathcal{U}} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{Tr(az^{2^m-1})}$$
$$= 1 + (2^m - 1) \sum_{z \in \mathcal{U}} (-1)^{Tr(az)}$$
$$= 1 + (2^m - 1)(1 - \mathcal{K}_{2^m}(a))$$
$$= 2^m + \mathcal{K}_{2^m}(a)(1 - 2^m). \tag{2.20}$$

□

Corollary 2.2.30 (Dillon [21])**.** *For $a \in \mathbb{F}_{2^m}^*$, the function $f(x) = Tr_1^{2m}(ax^{2^m-1})$ is bent if and only if $\mathcal{K}_{2^m}(a) = 0$.*

Proof. This is immediate from Theorem 2.2.29 and the observation that $|\mathcal{K}_{2^m}(a)| \leq 2^m$. □

In [71], Youssef and Gong credited Carlet with pointing out that the class of hyperbent functions constructed in [71] belong to Dillon's PS_{ap} class. This was formally proved shortly thereafter in [15]. Therefore if $Tr_1^{2m}(ax^{2^m-1})$ is bent, then $Tr_1^{2m}(ax^{r(2^m-1)})$ is bent for all r coprime with $2^{2m} - 1$. In fact, a slightly stronger statement holds:

Corollary 2.2.31 (Carlet, Gaborit [15])**.** *For $a \in \mathbb{F}_{2^m}^*$ and for r coprime with $2^m + 1$, the function $f(x) = Tr_1^{2m}(ax^{r(2^m-1)})$ is bent whenever $Tr_1^{2m}(ax^{2^m-1})$ is bent.*

Proof. Substituting x^r for x and running through the proofs of Theorem 2.2.29 and Corollary 2.2.30 gives the result. □

Previously, we gave justification as to why we can assume without loss of generality that $a \in \mathbb{F}_{2^m}^*$ when considering bent functions of the form $f(x) = Tr_1^{2m}(ax^{2^m-1})$. When

considering vectorial formulations of these functions however, we must be aware of the exact condition for the Boolean function f to be bent in the general case that $a \in \mathbb{F}_{2^{2m}}^*$. This is due to the fact that the non-linearity of an (n, m)-function is determined by the non-linearities of its component functions, which are Boolean functions. In particular, for $k \mid 2m$, the set of component functions of $Tr_k^{2m}(ax^{2^m-1})$ is $\{Tr_1^{2m}(bax^{2^m-1}) : b \in \mathbb{F}_{2^k}^*\}$. Since the condition $k \mid m$ is not required, $\mathbb{F}_{2^k}$ need not be a subfield of $\mathbb{F}_{2^m}$, hence some of the coefficients ba may reside in $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_{2^m}$.

Theorem 2.2.32 (Langevin, Leander [40]). *Let $a \in \mathbb{F}_{2^{2m}}^*$. The function $f(x) = Tr_1^{2m}(ax^{2^m-1})$ is bent if and only if $\mathcal{K}_{2^m}(N_m^{2m}(a)) = 0$.*

Proof. If $a \in \mathbb{F}_{2^m}^*$ then $N_m^{2m}(a) = a^{2^m+1} = a^2$ and thus the statement of the theorem reduces to that of Corollary 2.2.30 by virtue of Proposition 2.2.25.

Now suppose that $a \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_{2^m}$. Then $a = bu$ for some $b \in \mathbb{F}_{2^m}^*$, $u \in \mathcal{U}$, and we have $N_m^{2m}(a) = (bu)^{2^m+1} = b^2$. Define the function $f_b : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ by

$$f_b(x) = Tr_1^{2m}(bx^{2^m-1}).$$

By Proposition 2.2.20, f is bent if and only if f_b is bent. We compute

$$\begin{aligned} \sum_{z \in \mathcal{U}} (-1)^{Tr(bz)} &= 1 - \mathcal{K}_{2^m}(b) && \text{by Lemma 2.2.28} \\ &= 1 - \mathcal{K}_{2^m}(b^2) && \text{by Proposition 2.2.25} \\ &= 1 - \mathcal{K}_{2^m}(N_m^{2m}(a)). \end{aligned}$$

Then by (2.19), for any $\alpha \in \mathbb{F}_{2^{2m}}^*$ we have

$$W_{f_b}(\alpha) = 2^m (-1)^{Tr(b/\alpha^{2^m-1})} + \mathcal{K}_{2^m}(N_m^{2m}(a))$$

and by (2.20) and Proposition 2.2.25 we have

$$W_{f_b}(0) = 2^m + \mathcal{K}_{2^m}(N_m^{2m}(a))(1 - 2^m).$$

Therefore f_b is bent if and only if $\mathcal{K}_{2^m}(N_m^{2m}(a)) = 0$. □

2.2.3 Dillon-type Functions

So far our attention has been restricted to monomial bent functions. We will now expand our discussion to include functions having multiple terms in their trace representation, i.e. *multinomial functions*, of which monomial functions are clearly a proper subset. Part of the motivation in studying multinomial bent functions comes from cases where monomial constructions of bent functions are sparse. In these cases it may happen that many more

examples are produced when one allows for multinomial constructions. We will focus solely on multinomial functions that are generalizations of the monomial Dillon functions.

Definition 2.2.33 (Dillon-type Function)**.** *A function of the form*

$$f(x) = Tr_k^{2m}\left(\sum_{r\in\mathbb{Z}} \beta_r x^{r(2^m-1)}\right) \tag{2.21}$$

where only finitely many of the coefficients β_r are non-zero is called a Dillon-type function*.*

If $k = 1$ then a function of the form (2.21) *is called a* Dillon-type Boolean function*, otherwise it is called a* Dillon-type vectorial function*. A function of the form* (2.21) *with one or more trace terms is called a* Dillon-type multinomial function*. A Dillon-type multinomial function with exactly one/two/three/etc. trace terms is called a* Dillon-type monomial/binomial/trinomial/etc. function*.*

Remark 2.2.34. As an example of the terminology described above, a bent function of the form (2.21) with an unspecified number of non-zero trace terms and with $k > 1$ is called a *Dillon-type vectorial multinomial bent function.*

We reserve the phrase *Dillon function* for the Dillon-type Boolean monomial functions, as defined in Definition 2.2.18.

When considering a function of the form $x \mapsto Tr_1^{2m}\left(\sum_{r\in\mathbb{Z}} \beta_r x^{r(2^m-1)}\right)$, we need only consider those r that reside in distinct cyclotomic cosets modulo $2^m + 1$:

Proposition 2.2.35. *Let*

$$f(x) = Tr_1^{2m}\left(\sum_{r\in\mathbb{Z}} \beta_r x^{r(2^m-1)}\right),$$

where only finitely many of the coefficients β_r are non-zero. Then there exists a subset E of a set R of representatives of cyclotomic cosets modulo $2^m + 1$ and coefficients β'_r such that

$$f(x) = Tr_1^{2m}\left(\sum_{r\in E} \beta'_r x^{r(2^m-1)}\right).$$

Proof. If $r, s \in \mathbb{Z}$ belong to the same cyclotomic coset modulo $2^m + 1$ then we have $r \equiv 2^t s \pmod{2^m+1}$ for some $t \in \mathbb{Z}$. Therefore

$$\begin{aligned} Tr_1^{2m}\left(\beta_r x^{r(2^m-1)} + \beta_s x^{s(2^m-1)}\right) &= Tr_1^{2m}\left(\beta_r x^{r(2^m-1)} + (\beta_s x^{s(2^m-1)})^{2^t}\right) \\ &= Tr_1^{2m}\left((\beta_r + \beta_s^{2^t}) x^{r(2^m-1)}\right). \end{aligned} \tag{2.22}$$

Suppose $A \subset \mathbb{Z}$ consists solely of elements of a particular cyclotomic coset modulo $2^m + 1$. Then (2.22) shows that the terms corresponding to the elements of A in the polynomial

$\sum_{r\in\mathbb{Z}} \beta_r x^{r(2^m-1)}$ may be grouped into a single term in the expression $Tr_1^{2m}\left(\sum_{r\in\mathbb{Z}} \beta_r x^{r(2^m-1)}\right)$ (though it is important to note that the coefficients will be modified as in (2.22) above). The result follows. □

The next theorem, quoted from [17, Theorem 2], will be key to characterizing a specific class of Dillon-type Boolean multinomial bent functions.

Theorem 2.2.36 (Youssef, Gong [71])**.** *Let R be a non-empty set of representatives of cyclotomic cosets modulo 2^m+1, and let $E \subseteq R$. With each $r \in E$ associate an element $\beta_r \in \mathbb{F}_{2^m}^*$. Let*

$$f(x) = Tr_1^{2m}\left(\sum_{r\in E} \beta_r x^{r(2^m-1)}\right). \tag{2.23}$$

Let γ be a generator of $\mathcal{U}$. Then f is hyperbent if and only if $\#\{i : f(\gamma^i) = 1,\ 0 \le i \le 2^m\} = 2^{m-1}$.

Proof [17]. First note that for any $x \in \mathbb{F}_{2^{2m}}^*$ we have $x = yz$ for $y \in \mathbb{F}_{2^m}^*$, $z \in \mathcal{U}$ and thus

$$\begin{aligned} f(x) = f(yz) &= Tr_1^{2m}\left(\sum_{r\in E} \beta_r (yz)^{r(2^m-1)}\right) \\ &= Tr_1^{2m}\left(\sum_{r\in E} \beta_r z^{r(2^m-1)}\right) = f(z). \end{aligned}$$

For $i = 0, 1, \ldots, 2^m$, define $S_i := \gamma^i \mathbb{F}_{2^m}$. Then $f[S_i] = \{f(x) : x \in S_i\} = \{f(\gamma^i)\}$ for all i by the above. Let $I = \{i : f(\gamma^i) = 1,\ 0 \le i \le 2^m\}$, and note that $\mathrm{supp}(f) = \bigcup_{i\in I} S_i^*$. Applying Theorem 2.2.13 with $N = \#I$, we see that f is bent. We further conclude that f is hyperbent since the mapping $\gamma^i \mapsto \gamma^{ik}$ is a permutation on $\mathcal{U}$ for all k coprime with 2^m+1. □

Remark 2.2.37. By Theorem 2.1.32, the hyperbent functions of the form (2.23) on the domain $\mathbb{F}_{2^{2m}}$ have algebraic degree equal to m. We reiterate that this is the maximum possible algebraic degree among all bent functions on the same domain. Additionally, Carlet and Gaborit showed in [15] that the functions of the form (2.23) are exactly the functions of Dillon's PS_{ap} class, up to the linear transformations $x \mapsto ax$, $a \in \mathbb{F}_{2^{2m}}^*$.

It will turn out that the bentness of the functions (2.23) can be characterized in terms of the Hamming weights of certain related Boolean functions, which are in turn defined in terms of a special, well-studied class of polynomials over $\mathbb{F}_2$:

Definition 2.2.38 (Dickson Polynomial Over $\mathbb{F}_2$)**.** *The* Dickson polynomials *over $\mathbb{F}_2$ are defined recursively by*

$$D_0(x) = 0,$$

$$D_1(x) = x,$$
$$D_i(x) = xD_{i-1}(x) + D_{i-2}(x) \text{ for } i \geq 2.$$

We call $D_i(x) \in \mathbb{F}_2[x]$ *the* i-th Dickson polynomial over $\mathbb{F}_2$.

Our primary reference for Dickson polynomials is the monograph [43] by Lidl, Mullen, and Turnwald. We record some useful properties of the Dickson polynomials:

Proposition 2.2.39 ([43])**.** *For* $i, j > 0$*, the Dickson polynomials over* $\mathbb{F}_2$ *exhibit the following properties:*

i. $\deg D_i = i$

ii. $D_{2i}(x) = (D_i(x))^2$

iii. $D_i(x + x^{-1}) = x^i + x^{-i}$

iv. $D_{ij}(x) = D_i(D_j(x))$.

Proof.

i. This follows quickly from the definition and induction on i.

ii. By induction we have

$$\begin{aligned} D_{2i}(x) &= xD_{2i-1}(x) + D_{2i-2}(x) \\ &= x[xD_{2i-2}(x) + D_{2i-3}(x)] + [xD_{2i-3}(x) + D_{2i-4}(x)] \\ &= x^2 D_{2i-2}(x) + D_{2i-4}(x) \\ &= x^2 (D_{i-1}(x))^2 + (D_{i-2}(x))^2 \\ &= (D_i(x))^2. \end{aligned}$$

The base case is easy to verify.

iii. Using induction we have

$$\begin{aligned} D_i(x + x^{-1}) &= (x + x^{-1})D_{i-1}(x + x^{-1}) + D_{i-2}(x + x^{-1}) \\ &= (x + x^{-1})(x^{i-1} + x^{1-i}) + (x^{i-2} + x^{2-i}) \\ &= x^i + x^{-i} + 2(x^{i-2} + x^{2-i}) \\ &= x^i + x^{-i}. \end{aligned}$$

Once again, the base case may be verified quickly.

iv. Let $x \in \mathbb{F}_{2^n}$ and let $y \in \mathbb{F}_{2^{2m}}$ be such that $x = y + y^{-1}$. Then by property (*iii*) we have

$$\begin{aligned} D_i(D_j(x)) &= D_i(D_j(y + y^{-1})) \\ &= D_i(y^j + y^{-j}) \\ &= y^{ij} + y^{-ij} \\ &= D_{ij}(y + y^{-1}) \\ &= D_{ij}(x). \end{aligned}$$

□

Note that property (*ii*) is a special case of property (*iv*). We note this case separately so that we may quickly refer to it in the coming material.

We are now in a position to state and prove a characterization of a large class of Dillon-type Boolean multinomial bent functions, presented by Charpin and Gong in [17]. We ask the reader to recall the Walsh Transform as defined in Definition 2.1.2.

Theorem 2.2.40 (Charpin, Gong [17])**.** *Let R be a non-empty set of representatives of cyclotomic cosets modulo $2^m + 1$, and let $E \subseteq R$. With each $r \in E$ associate an element $\beta_r \in \mathbb{F}_{2^m}^*$. Let*

$$f(x) = Tr_1^{2m}\left(\sum_{r \in E} \beta_r x^{r(2^m-1)}\right)$$

and let

$$g(x) = Tr_1^m\left(\sum_{r \in E} \beta_r D_r(x)\right).$$

Let $h(x) = Tr_1^m(x^{-1})$. Then f is hyperbent if and only if

$$W_{h+g}(0) = W_g(0). \tag{2.24}$$

Proof. Let γ be a generator of $\mathcal{U}$. Then

$$\begin{aligned} f(\gamma^i) &= Tr_1^{2m}\left(\sum_{r \in E} \beta_r \gamma^{ir(2^m-1)}\right) \\ &= \sum_{r \in E} Tr_1^{2m}(\beta_r \gamma^{ir(2^m-1)}) \\ &= \sum_{r \in E} Tr_1^{2m}(\beta_r \gamma^{-2ir}) \\ &= \sum_{r \in E} Tr_1^{m}(\beta_r Tr_m^{2m}(\gamma^{-2ir})) \\ &= \sum_{r \in E} Tr_1^{m}(\beta_r (\gamma^{2ir} + \gamma^{-2ir})) \qquad \text{by (2.17)} \end{aligned}$$

$$= \sum_{r \in E} Tr_1^m(\beta_r(\gamma^{ir} + \gamma^{-ir}))$$
$$= \sum_{r \in E} Tr_1^m(\beta_r D_r(\gamma^i + \gamma^{-i})).$$

The last equality follows from Proposition 2.2.39, properties (iii) and (iv) – indeed, we have $\gamma^{ir} + \gamma^{-ir} = D_{ir}(\gamma + \gamma^{-1}) = D_r(D_i(\gamma + \gamma^{-1})) = D_r(\gamma^i + \gamma^{-i})$. By Theorem 2.2.36, f is hyperbent if and only if

$$N := \#\{i : f(\gamma^i) = 1\} = 2^{m-1}. \tag{2.25}$$

Let $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be as above, i.e. $g(x) = \sum_{r \in E} Tr_1^m(\beta_r D_r(x))$. By Proposition 2.2.27, every $\{\gamma^i, \gamma^{-i}\} \subset \mathcal{U}$ is uniquely represented by an $x \in \mathbb{F}_{2^m}^*$ with $Tr_1^m(x^{-1}) = h(x) = 1$. Thus we have

$$N = 2\#\{x \in \mathbb{F}_{2^m} : h(x) = 1 \text{ and } g(x) = 1\}. \tag{2.26}$$

Note that $\mathrm{wt}(hg) = N/2$ by (2.26). By Proposition 2.1.4 and Definition 1.3.6, we have

$$\begin{aligned} W_{h+g}(0) &= 2^m - 2\,\mathrm{wt}(h+g) \\ &= 2^m - 2(\mathrm{wt}(h) + \mathrm{wt}(g) - 2\,\mathrm{wt}(hg)) \\ &= 2^m - 2(2^{m-1} + \mathrm{wt}(g) - 2\,\mathrm{wt}(hg)) && \text{(since } h \text{ is balanced)} \\ &= 2(N - \mathrm{wt}(g)). \end{aligned}$$

Therefore by (2.25) and Proposition 2.1.4, f is hyperbent if and only if

$$\begin{aligned} W_{h+g}(0) &= 2^m - 2\,\mathrm{wt}(g) \\ &= W_g(0). \end{aligned}$$

□

We make several remarks regarding Theorem 2.2.40. The first remark is in regards to the connection between Theorem 2.2.40 and Corollary 2.2.30, which characterizes the bent Dillon functions. The second remark has to do with the original statement of Theorem 2.2.40 as it appears in [17]. The third remark makes note of a characterization of the hyperbent functions (2.23) that has a lower time complexity to check than the one given by Theorem 2.2.40. The final remark addresses the assumption in the statement of Theorem 2.2.40 that the coefficients of the multinomials reside in the largest proper subfield of the domain. Specifically, we discuss how this limits the application of this theorem to vectorial extensions of the functions of the type (2.23).

Remark 2.2.41. Let $\beta \in \mathbb{F}_{2^m}^*$, and let $f(x) = Tr_1^{2m}(\beta x^{2^m-1})$. In the notation of Theorem 2.2.40, we may take $E = \{1\}$ without loss of generality. Therefore we have $g(x) =$

$Tr_1^m(\beta D_1(x)) = Tr_1^m(\beta x)$, and so by Theorem 2.2.40, f is bent if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr(\beta x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr(x^{-1}) + Tr(\beta x)}. \tag{2.27}$$

The left-hand side of (2.27) is equal to zero by Proposition 1.3.14, while the right-hand side of (2.27) is equal to $\mathcal{K}_{2^m}(\beta)$ by Definition 2.2.21 (where we set $Tr(0^{-1}) = Tr(0^{2^m-2}) = 0$). Thus we see that Theorem 2.2.40 is indeed a valid generalization of Corollary 2.2.30.

Remark 2.2.42. In the original statement of Theorem 2.2.40, Charpin and Gong required that the set R consist only of representatives of those cyclotomic cosets modulo $2^m + 1$ having the full size $2m$. However, by examining the proof of the theorem we see that this assumption is not required for a function of the form (2.23) to be hyperbent, therefore we have removed it.

Remark 2.2.43. In [47], Lisoněk noted that for fixed E and variable m, checking the condition (2.24) requires time exponential in m. He subsequently showed that the bentness (and hence hyperbentness) of functions of the form (2.23) can be checked in polynomial time by counting rational points on certain hyperelliptic curves [47, Theorem 2].

Remark 2.2.44. In the previous subsection we remarked that when considering the non-linearity of Boolean monomial functions

$$Tr_1^{2m}(ax^{2^m-1}), \tag{2.28}$$

we may assume without loss of generality that $a \in \mathbb{F}_{2^m}$. This is reflected in the characterization of the bent functions of this kind provided by Corollary 2.2.30. On the other hand, when considering the non-linearity of *vectorial* monomial functions

$$Tr_k^{2m}(ax^{2^m-1}), \tag{2.29}$$

it behooves us to be aware of the exact condition that functions of the form (2.28) are bent in the general case that $a \in \mathbb{F}_{2^{2m}}$. This is due to the fact that the function (2.29) is bent if and only if each of the Boolean component functions

$$Tr_1^k(\lambda Tr_k^{2m}(ax^{2^m-1})) = Tr_1^{2m}(\lambda a x^{2^m-1}),\ \lambda \in \mathbb{F}_{2^k}^*, \tag{2.30}$$

are bent. Since $\mathbb{F}_{2^k}$ need not be a subfield of $\mathbb{F}_{2^m}$, not all of the coefficients λa need reside in $\mathbb{F}_{2^m}$. A characterization that allows us to deal with this situation was provided by Theorem 2.2.32.

In the case of the multinomial functions

$$Tr_1^{2m}\left(\sum_{r \in E} \beta_r x^{r(2^m-1)}\right),\ \beta_r \in \mathbb{F}_{2^m}, \tag{2.31}$$

Theorem 2.2.40 generalizes Corollary 2.2.30 by characterizing the bent functions of this kind in the case that all the coefficients β_r are elements of $\mathbb{F}_{2^m}$. However, there is currently no generalization of Theorem 2.2.32 in the literature for functions of the type (2.31). That is, there is no characterization of the Boolean bent functions (2.31) in the case that not all of the coefficients β_r are elements of $\mathbb{F}_{2^m}$.

Therefore, if we wish to consider the non-linearity of a vectorial multinomial function

$$Tr_k^{2m}\left(\sum_{r\in E}\beta_r x^{r(2^m-1)}\right),\ \beta_r\in\mathbb{F}_{2^m} \tag{2.32}$$

by considering the component functions

$$Tr_1^k\left(\lambda Tr_k^{2m}\left(\sum_{r\in E}\beta_r x^{r(2^m-1)}\right)\right)=Tr_1^{2m}\left(\sum_{r\in E}\lambda\beta_r x^{r(2^m-1)}\right),\ \lambda\in\mathbb{F}_{2^k}^*, \tag{2.33}$$

then we must restrict ourselves to cases where k divides m if we are to apply Theorem 2.2.40.

We note that Muratović-Ribić, Pasalic, and Bajrić constructed a family of Dillon-type vectorial multinomial bent functions having a specific output dimension [55]. These functions have the form

$$f(x)=Tr_m^{2m}\left(\sum_{i=0}^{2^m}a_i x^{i(2^m-1)}\right),\ a_i\in\mathbb{F}_{2^{2m}}. \tag{2.34}$$

Clearly the Boolean function $x\mapsto Tr_1^{2m}(\sum_{i=0}^{2^m}a_i x^{i(2^m-1)})$ is bent whenever the corresponding function (2.34) is bent, as per Remark 2.1.24. However, we reiterate that a good characterization of the Boolean bent functions of this kind is not yet available.

Chapter 3

New Results

Having sufficiently developed a background on bent functions, we now present our new results. In the first section of this chapter we will give our results on Dillon-type vectorial monomial functions, before moving on to new results for the multinomial case in the second section. The third and final section of this chapter is devoted to some new results on the divisibility of Kloosterman sums, which we will use to give explicit constructions of Kloosterman zeros, and hence Dillon-type bent functions. We will now give an overview of the material presented in this chapter:

The first section of this chapter deals with Dillon-type vectorial monomial functions. The first main result gives a condition sufficient for such a function to be bent in the general case. We also present our reasons for believing that this condition is very close to being necessary. We then use our result to construct three examples of bent functions of this kind that are not covered by any theorem currently known in the literature. We emphasize that, apart from these three examples, all other Dillon-type vectorial monomial bent functions that are covered by results currently appearing in the literature are relatively easy to construct, in the sense that they follow directly from their Boolean counterparts. In particular these are the Dillon-type vectorial monomial functions defined on $\mathbb{F}_{2^{2m}}$ for odd m and valued in $\mathbb{F}_4$.

The second main result of the first section gives necessary conditions for the existence of Dillon-type vectorial monomial functions defined on $\mathbb{F}_{2^{2m}}$ for *even* m and valued in $\mathbb{F}_4$. In contrast to the case where m is odd, these functions are not easily obtained from their Boolean formulations (in fact we show that they are very rare). Our result serves as an efficient filter, which we demonstrate by reproducing two of the three examples that were obtained via the sufficient condition discussed in the previous paragraph, in a comparable timeframe.

We conclude the first section of this chapter by providing a necessary and sufficient condition for a Dillon-type vectorial monomial function to be bent in the general case. Though this characterization is not yet in a "useful" form in the sense of providing a polynomial-time

decision procedure regarding the bentness of such a function, it does provide insight on the restrictions that exist for bent functions of this type. In particular, we will use this condition to provide a short proof of the recent result of Muratović-Ribić, Pasalic, and Bajrić , which states that Dillon-type vectorial monomial bent functions cannot meet the Nyberg bound. We will subsequently extend this result by showing that there are no Dillon-type vectorial monomial bent functions from $\mathbb{F}_{2^{4m}}$ to $\mathbb{F}_{2^m}$ for any m.

The second section of this chapter deals with Dillon-type vectorial multinomial functions. The main result of this section is an extension of the above-mentioned result of Muratović-Ribić, Pasalic, and Bajrić to the multinomial case. We will show how the necessary conditions governing the existence of Dillon-type vectorial multinomial bent functions are correspondingly more complex than the associated conditions in the monomial case. Additionally, we return to Dillon-type functions defined on $\mathbb{F}_{2^{2m}}$ for even m and valued in $\mathbb{F}_4$, this time considering binomial constructions. We give computational results showing that these functions are much more abundant than the aforementioned monomial functions.

The third and final section of this chapter deals with the divisibility of Kloosterman sums. The main achievement of this section is the synthesis of a set of Kloosterman zeros in $\mathbb{F}_{2^m}$ for $m = 6$. To the best of our knowledge, this has not been done before for any value of m. We arrive at this by successively connecting elliptic curves, Kloosterman sums, and characteristic polynomials over $\mathbb{F}_2$, via several known results. We then apply these results to a special collection of cosets of a maximal proper subfield of a field $\mathbb{F}_{2^n}$ exhibiting a certain subfield structure. From this collection of Kloosterman zeros we independently obtain, for the third time, two of the three previously-mentioned examples of Dillon-type vectorial monomial bent functions that are not currently known in the literature.

Results and material in this chapter that are quoted or paraphrased from external sources are clearly marked as such. All other results presented in this chapter are, to the best knowledge and effort of the author, original.

At this point we wish to remind the reader that our main results may also be found in the forthcoming publication [41].

3.1 Dillon-type Monomial Functions

In Section 2.1.2 we saw that an (n, m)-function is bent if and only if its (Boolean) component functions are bent (Theorem 2.1.23). In Section 2.2.2 we established a good characterization of the bent Dillon functions, which are monomial functions mapping to $\mathbb{F}_2$ (Theorem 2.2.32). Our first original result will combine these two theorems to provide a list of conditions sufficient for a function of the form $Tr_k^{2m}(ax^{2^m-1})$ to be bent. This result will be shown to properly subsume the best previously-known theorem of this nature, via the construction of several examples that cannot be obtained from results currently appearing in the literature.

3.1.1 Sufficient Conditions for Vectorial Bentness

The characterization of the bent Dillon functions $x \mapsto Tr_1^{2m}(ax^{2^m-1})$ is well-known. However, there has been little progress in extending these functions to the vectorial case. The following theorem was proved by Xu and Wu in their recent e-print [70].

Theorem 3.1.1 (Xu, Wu [70])**.** *Let m be odd. Then $Tr_2^{2m}(ax^{2^m-1})$ is bent if and only if $Tr_1^{2m}(ax^{2^m-1})$ is bent.*

Xu and Wu had originally attempted to provide a more general result, but it later turned out to simplify to the theorem above. Nonetheless, Theorem 3.1.1 is currently the best known result of this nature. We will show how this result follows from Theorem 3.1.3 below.

Remark 3.1.2. At this point we wish to emphasize the disparity in the degree of difficulty in constructing bent functions of the form

$$Tr_2^{2m}\left(ax^{2^m-1}\right) \tag{3.1}$$

when m is odd versus when m is even. As we have seen just now, when m is odd, bent functions of the form (3.1) are obtained "for free" from their Boolean counterparts, for which we have a good characterization (Corollary 2.2.30). However, in the case that m is even, bent functions of the form (3.1) seem to be rare, and as of yet there is no useful characterization of these functions in general. In the coming material we will use our new results to obtain two examples of bent functions of the form (3.1) when m is even: one for $m = 6$, and the other for $m = 12$.

Theorem 3.1.3. *Let $k \mid 2m$, let $t = \frac{2^{2m}-1}{2^k-1}$, and let $s = \frac{2^k-1}{\gcd(2^k-1,2^m+1)}$. Let α be a primitive element of $\mathbb{F}_{2^{2m}}$, and suppose that r is an integer in $\{0, 1, \ldots, 2^m - 2\}$ such that $a := \alpha^{r(2^m+1)} \in \mathbb{F}_{2^m}$ is a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$.*

If, for each $i \in \{0, 1, \ldots, s-1\}$, there exists an integer $u_i \in \{0, 1, \ldots, m-1\}$ satisfying

$$it - r(2^{u_i} - 2) \equiv 0 \pmod{2^m - 1} \tag{3.2}$$

then the function $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent.

Proof. Let $\omega := \alpha^t$. Then ω is a primitive element of $\mathbb{F}_{2^k}$. Let f_i denote the i-th component function of f. Thus we have

$$f_i(x) = Tr_1^k\left(\omega^i f(x)\right) = Tr_1^{2m}\left(\omega^i a x^{2^m-1}\right).$$

By Theorem 2.1.23, f is bent if and only if $f_i(x)$ is bent for $i = 0, 1, \ldots, 2^k - 2$. By Theorem 2.2.32, $f_i(x)$ is bent for a given i if and only if $N_m^{2m}(\omega^i a)$ is a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$.

Therefore we have that f is bent if and only if

$$\mathcal{K}_{2^m}\left(N_m^{2m}(\omega^i a)\right) = 0 \text{ for } i = 0, 1, \ldots, 2^k - 2. \tag{3.3}$$

Bearing in mind that all exponents are taken modulo $2^{2m} - 1$, we compute

$$\begin{aligned} N_m^{2m}(\omega^i a) &= (\omega^i a)^{2^m+1} \\ &= (\alpha^{it+r(2^m+1)})^{2^m+1} \\ &= \alpha^{it(2^m+1)+r(2^m+1)^2} \\ &= \alpha^{it(2^m+1)+2r(2^m+1)}. \end{aligned} \tag{3.4}$$

Note that we have

$$\begin{aligned} \#\{N_m^{2m}(\omega^i a) : 0 \le i \le 2^k - 2\} &= \#\{(ax)^{2^m+1} : x \in \mathbb{F}_{2^k}^*\} \\ &= \#\{x^{2^m+1} : x \in \mathbb{F}_{2^k}^*\} \\ &= \frac{2^k - 1}{\gcd(2^k - 1, 2^m + 1)} \qquad \text{(by Proposition 1.3.2)} \\ &= s. \end{aligned} \tag{3.5}$$

Since $\alpha^{r(2^m+1)}$ is a Kloosterman zero in $\mathbb{F}_{2^m}$ by assumption, we have by Proposition 2.2.25 that $(\alpha^{r(2^m+1)})^{2^j} = \alpha^{2^j r(2^m+1)}$ is also a Kloosterman zero in $\mathbb{F}_{2^m}$ for $j = 0, 1, \ldots, m-1$. Therefore (3.3) will hold if (but not necessarily "only if")

$$\{\alpha^{it(2^m+1)+2r(2^m+1)} : 0 \le i \le 2^k - 2\} \subseteq \{\alpha^{2^j r(2^m+1)} : 0 \le j \le m - 1\}. \tag{3.6}$$

That is, f is bent if the relative norms of the coefficients of its component functions are all conjugates of the coefficient a, which is assumed to be a Kloosterman zero in $\mathbb{F}_{2^m}$.

By (3.5), the set $\{\alpha^{it(2^m+1)+2r(2^m+1)} : 0 \le i \le 2^k - 2\}$ is in fact equal to the set $\{\alpha^{it(2^m+1)+2r(2^m+1)} : 0 \le i \le s - 1\}$, therefore (3.6) becomes

$$\{\alpha^{it(2^m+1)+2r(2^m+1)} : 0 \le i \le s - 1\} \subseteq \{\alpha^{2^j r(2^m+1)} : 0 \le j \le m - 1\}. \tag{3.7}$$

Equation (3.7) holds if and only if, for each $i \in \{0, 1, \ldots, s-1\}$, there exists an integer $u_i \in \{0, 1, \ldots, m-1\}$ such that

$$it(2^m + 1) + 2r(2^m + 1) \equiv 2^{u_i} r(2^m + 1) \pmod{2^{2m} - 1}. \tag{3.8}$$

We divide by $2^m + 1$ throughout and rearrange to obtain

$$it - r(2^{u_i} - 2) \equiv 0 \pmod{2^m - 1}. \tag{3.9}$$

The result now follows. □

Remark 3.1.4. We note that the condition given by Theorem 3.1.3 is "close" to being a necessary condition, in the sense that Dillon-type vectorial monomial bent functions that are not obtained via this condition likely do not exist. We give our reasoning below:

Let $a \in \mathbb{F}_{2^m}^*$ such that $\mathcal{K}_{2^m}(a) = 0$ and let

$$A = \{a^{2^i} : 0 \leq i \leq m-1\}.$$

Then by Proposition 2.2.25 we have $\mathcal{K}_{2^m}(x) = 0$ for all $x \in A$. Let $k \mid 2m$, $k > 1$, and let

$$B = \{ba : b \in \mathbb{F}_{2^k}^*\}.$$

Note that the coefficients of the component functions of $f(x) = Tr_k^{2m}(ax^{2^m-1})$ are exactly the elements of B. Then by Theorem 2.2.32, f is bent whenever

$$N_m^{2m}[B] \subseteq A. \tag{3.10}$$

Theorem 3.1.3 gives a necessary and sufficient condition for (3.10), which is therefore a sufficient condition for f to be bent.

Now, suppose that there exists a Kloosterman zero $a' \in \mathbb{F}_{2^m}^*$ such that, for the set $B' = \{ba' : b \in \mathbb{F}_{2^k}^*\}$, the set

$$N_m^{2m}[B'] = \{(a')^2 N_m^{2m}(b) : b \in \mathbb{F}_{2^k}^*\}$$

consists entirely of Kloosterman zeros in $\mathbb{F}_{2^m}$, but

$$N_m^{2m}[B'] \not\subseteq \{a', (a')^2, \ldots, (a')^{2^{m-1}}\}. \tag{3.11}$$

That is, suppose that $N_m^{2m}[B']$ consists entirely of Kloosterman zeros, but not every element of $N_m^{2m}[B']$ is equivalent under the mapping $x \mapsto x^2$. Then the function

$$f'(x) = Tr_k^{2m}\left(a'x^{2^m-1}\right) \tag{3.12}$$

is bent; furthermore f' is not covered by Theorem 3.1.3. However, we have reason to believe that functions of this type are extremely rare, if not non-existent altogether (hence our claim that the condition of Theorem 3.1.3 is "close to necessary").

The reason lies in the vanishing scarcity of Kloosterman zeros in $\mathbb{F}_{2^m}$. In [62], Shparlinski remarked that

$$\#\{a \in \mathbb{F}_{2^m}^* : \mathcal{K}_{2^m}(a) = 0\} = O(2^{3m/4}); \tag{3.13}$$

furthermore he suggested that it can be shown that in fact this number is $O\left(2^{m/2}m(\log m)^2\right)$. Note that [62] is not simply considering Kloosterman zeros up to equivalence under the mapping $x \mapsto x^2$, as we have been doing. In any case, it is known that the density of Kloosterman zeros in $\mathbb{F}_{2^m}$ decreases exponentially with m. Therefore the likelihood that bent functions of the type (3.12) exist becomes vanishingly small as m grows.

As promised, we now give a proof of Theorem 3.1.1:

Proof of Theorem 3.1.1. If $Tr_1^{2m}(ax^{2^m-1})$ is bent then a is a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$ by Corollary 2.2.30. Let $\alpha \in \mathbb{F}_{2^{2m}}$ be primitive, and write $a = \alpha^{r(2^m+1)}$ for the appropriate $r \in \{0, 1, \ldots, 2^m - 2\}$. Using the notation of Theorem 3.1.3, we have $s = \frac{3}{\gcd(3,2^m+1)} = \frac{3}{3} = 1$. Therefore according to Theorem 3.1.3, in order to establish the bentness of $Tr_2^{2m}(ax^{2^m-1})$ we need only find an integer u satisfying the congruence

$$r(2^u - 2) \equiv 0 \pmod{2^m - 1}.$$

Clearly, $u = 1$ suffices.

On the other hand, if $Tr_2^{2m}(ax^{2^m-1})$ is bent, then $Tr_1^{2m}(ax^{2^m-1})$ is bent as per Remark 2.1.24. □

To demonstrate that Theorem 3.1.3 properly subsumes Theorem 3.1.1, we will now construct explicit examples of Dillon-type vectorial monomial bent functions that are not covered by Theorem 3.1.1:

Example 3.1.5. We give three examples of previously unknown bent functions of the form $f(x) = Tr_k^{2m}(ax^{2^m-1})$ for even m. These examples are tabulated in Table 3.1 below. The first column gives a label to each example, for reference. The second column gives the irreducible polynomial $p(x)$ used in the construction of the domain $\mathbb{F}_{2^{2m}}$, thus $\mathbb{F}_{2^{2m}} = \mathbb{F}_2[x]/\langle p(x)\rangle$ [8]. The third and fourth columns give the domain $\mathbb{F}_{2^{2m}}$ and the range $\mathbb{F}_{2^k}$, respectively. Let $\alpha \in \mathbb{F}_{2^{2m}}$ be a root of $p(x)$. The fifth column gives an integer r such that

$$a := \alpha^{r(2^m+1)}$$

is a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$. The sixth column gives the value of

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

Finally, the seventh and last column gives a sequence $(u_0, u_1, \ldots, u_{s-1}) \in \mathbb{Z}_m^s$ such that u_i satisfies $it - r(2^{u_i} - 2) \equiv 0 \pmod{2^m - 1}$ for $i = 0, 1, \ldots, s-1$, where $t = \frac{2^{2m}-1}{2^k-1}$ as before.

These examples were obtained via an exhaustive search, which iterated through all proper subfields $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^{2m}}$ for $1 < k < m < 32$ via a program written in Magma [8].

Table 3.1: Three New Examples of Bent Functions of the Form $Tr_k^{2m}\left(ax^{2^m-1}\right)$.

Example #	$p(x)$	Domain	Range	r	s	$(u_0, u_1, \ldots, u_{s-1})$
i.	$x^{12}+x^7+x^6+x^5$ $+x^3+x+1$	$\mathbb{F}_{2^{12}}$	$\mathbb{F}_{2^2}$	7	3	$(1,3,5)$
ii.	$x^{12}+x^7+x^6+x^5$ $+x^3+x+1$	$\mathbb{F}_{2^{12}}$	$\mathbb{F}_{2^4}$	7	3	$(1,3,5)$
iii.	$x^{24}+x^{16}+x^{15}+x^{14}$ $+x^{13}+x^{10}+x^9+x^7$ $+x^5+x^3+1$	$\mathbb{F}_{2^{24}}$	$\mathbb{F}_{2^2}$	91	3	$(1,5,9)$

Checking the case of $k = m$ was unnecessary due to the result of Muratović-Ribić, Pasalic, and Bajrić [54], which was mentioned in the introduction of this chapter. When m was odd we were able to initialize with $k > 2$ due to Theorem 3.1.1. When considering each subfield $\mathbb{F}_{2^k}$, the program iterated through possible values of $r \in \{0, 1, \ldots, 2^m - 2\}$ until one was found such that the congruence (3.2) had a solution for $i = 0, 1, \ldots, s-1$. The last step checked whether a primitive element of $\mathbb{F}_{2^m}$ (cast as a (2^m+1)-st power of α) yielded a Kloosterman zero in $\mathbb{F}_{2^m}$ when raised to the r-th power. In a period of approximately one day we were able to check all $m \leq 31$. See Appendix B.1 for the details and output of the computations. Computations for $m > 31$ become very expensive due to the exponential growth in the domain of r, since $0 \leq r \leq 2^m - 2$. In particular, for $m = 32$ the program must iterate through three proper subfields of $\mathbb{F}_{2^{64}}$, which are the fields $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^8}$, and $\mathbb{F}_{2^{16}}$.

As a result of our computations, we are able to conclude that the functions described in examples (i) – (iii) constitute a complete list of all bent functions described by Theorem 3.1.3 for even $m \leq 30$ and $2 \leq k < m$. Whether more exist for even $m > 30$ is unknown at this point. As discussed previously, we believe that the set of Dillon-type vectorial monomial bent functions that are not covered by Theorem 3.1.3 is in fact empty.

3.1.2 Bent Functions from $GF(2^{4m})$ to $GF(4)$

In this section we provide results that serve as efficient testing procedures for determining whether a function of the form $Tr_2^{2m}(ax^{2^m-1})$ may be bent in the case that m is even (the case of m odd has a good characterization in Theorem 3.1.1).

Let $\omega \in \mathbb{F}_{2^m}^*$ be a primitive cube-root of unity. For $a \in \mathbb{F}_{2^m}^*$, the first original theorem of this section gives a list of conditions that must be satisfied by the minimal polynomials of a, ωa, and $\omega^2 a$ over $\mathbb{F}_2$ if the function $Tr_2^{2m}(ax^{2^m-1})$ is to be bent. Using these results, we are able to reiterate the constructions of all such functions that exist for even $m \leq 30$ (these were described in rows (i) and (iii) of Example 3.1.5).

Our primary tool will be the following theorem of Lisoněk and Moisio:

Theorem 3.1.6 (Lisoněk, Moisio [48])**.** *Let $a \in \mathbb{F}_{2^k}^*$. If $\mathcal{K}_{2^{kn}}(a) = 0$ for $n > 1$, then $kn = 4$ and $a = 1$.*

We will also require the following two results regarding the minimal polynomials over $\mathbb{F}_2$ of elements residing in cosets of $\mathbb{F}_4^*$:

Theorem 3.1.7. *Let m be even, let $a \in \mathbb{F}_{2^m}^*$, and let $\omega \in \mathbb{F}_{2^m}^*$ be a primitive cube-root of unity. For $i \in \mathbb{Z}_3$, denote by $m_{a,i}(x)$ the minimal polynomial of $a\omega^i$ over $\mathbb{F}_2$. Let $j \in \mathbb{Z}_3$ be non-zero. If $m_{a,0}(x) = m_{a,j}(x)$ but $m_{a,0}(x) \neq m_{a,2j}(x)$, then $\deg m_{a,2j}(x) < \deg m_{a,0}(x)$*

Proof. Write $m_{a,0}(x) = \sum_{i=0}^{k} e_i x^i$, where $k = \deg m_{a,0}(x)$.

We have

$$\begin{aligned}
0 &= \sum_{i=0}^{k} e_i a^i + \sum_{i=0}^{k} e_i (a\omega^j)^i \\
&= \sum_{i=0}^{k} e_i a^i + \left[\left(\sum_{\substack{i \equiv 0 \pmod 3 \\ i \leq k}} e_i a^i \right) + \left(\omega \sum_{\substack{i \equiv j \pmod 3 \\ i \leq k}} e_i a^i \right) + \left(\omega^2 \sum_{\substack{i \equiv 2j \pmod 3 \\ i \leq k}} e_i a^i \right) \right] \\
&= \left((1+\omega) \sum_{\substack{i \equiv j \pmod 3 \\ i \leq k}} e_i a^i \right) + \left((1+\omega^2) \sum_{\substack{i \equiv 2j \pmod 3 \\ i \leq k}} e_i a^i \right) \\
&= \left(\omega^2 \sum_{\substack{i \equiv j \pmod 3 \\ i \leq k}} e_i a^i \right) + \left(\omega \sum_{\substack{i \equiv 2j \pmod 3 \\ i \leq k}} e_i a^i \right) \\
&= \sum_{\substack{i \not\equiv 0 \pmod 3 \\ i \leq k}} e_i (a\omega^{2j})^i.
\end{aligned}$$

Let $\phi(x) = \sum_{\substack{i \not\equiv 0 \pmod 3 \\ i \leq k}} e_i x^i$. Then $\deg m_{a,2j}(x) \leq \deg \phi(x) \leq k$. Let t be the smallest integer such that x^t appears as a term in $\phi(x)$, and note that $t \geq 1$. Since $(a\omega^{2j})^t \neq 0$, it must be that $a\omega^{2j}$ is a root of $x^{-t}\phi(x)$, which has degree strictly less than k. Therefore $\deg m_{a,2j}(x) < k$. □

Theorem 3.1.8. *Let m be even, let $a \in \mathbb{F}_{2^m}^*$, and let $\omega \in \mathbb{F}_{2^m}$ be a primitive cube-root of unity. Let $m_{a,i}(x)$ be the minimal polynomial of $a\omega^i$ over $\mathbb{F}_2$. If $m_{a,0}(x) = m_{a,1}(x) = m_{a,2}(x)$, then the exponent of each non-zero term of $m_{a,0}(x)$ is divisible by 3.*

Proof. Write $m_{a,0}(x) = \sum_{i=0}^{k} e_i x^i$, where $k = \deg m_{a,0}(x)$. Then

$$0 = \sum_{i=0}^{k} e_i a^i + \sum_{i=0}^{k} e_i (\omega a)^i + \sum_{i=0}^{k} e_i (\omega^2 a)^i$$

$$= \left(\sum_{\substack{i \equiv 0 \pmod 3 \\ i \leq k}} e_i a^i \right) + \left((1+\omega+\omega^2) \sum_{\substack{i \equiv 1 \pmod 3 \\ i \leq k}} e_i a^i \right) + \left((1+\omega+\omega^2) \sum_{\substack{i \equiv 2 \pmod 3 \\ i \leq k}} e_i a^i \right)$$
$$= \sum_{\substack{i \equiv 0 \pmod 3 \\ i \leq k}} e_i a^i + 0 + 0$$
$$= \sum_{\substack{i \equiv 0 \pmod 3 \\ i \leq k}} e_i a^i.$$

Let $\phi(x) = \sum_{\substack{i \equiv 0 \pmod 3 \\ i \leq k}} e_i x^i$. Clearly $\deg \phi(x) \leq \deg m_{a,0}(x)$. Since a is a root of both, and since $m_{a,0}(x)$ is minimal, we must have that in fact $\deg \phi(x) = \deg m_{a,0}(x)$. Therefore $\phi(x) = m_{a,0}(x)$. □

At this point it becomes pertinent to establish a vectorial analogue of Proposition 2.2.20:

Proposition 3.1.9. *Let $\alpha \in \mathbb{F}_{2^{2m}}^*$, and let $\beta \in \mathbb{F}_{2^m}^*$, $u \in \mathcal{U}$ be such that $\alpha = \beta u$. Let k be a positive integer dividing $2m$, and define $f_\alpha : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ and $f_\beta : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ by*

$$f_\alpha(x) = Tr_k^{2m}\left(\alpha x^{2^m-1}\right),$$
$$f_\beta(x) = Tr_k^{2m}\left(\beta x^{2^m-1}\right).$$

Then the extended Walsh spectra of f_α and f_β are identical.

Proof. By Proposition 2.2.19 there exists an element $v \in \mathbb{F}_{2^{2m}}^*$ such that $f_\alpha(x) = f_\beta(vx)$. Note that $x \mapsto xv$ is a permutation on $\mathbb{F}_{2^{2m}}$. Then for $a \in \mathbb{F}_{2^{2m}}$ and $b \in \mathbb{F}_{2^k}^*$ we have

$$\begin{aligned} W_{f_\beta}(a,b) &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{Tr_1^k(bf_\beta(x)) + Tr_1^{2m}(ax)} \\ &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{Tr_1^k(bf_\beta(vx)) + Tr_1^{2m}(avx)} \\ &= \sum_{x \in \mathbb{F}_{2^{2m}}} (-1)^{Tr_1^k(bf_\alpha(x)) + Tr_1^{2m}(avx)} \\ &= W_{f_\alpha}(av,b). \end{aligned}$$

Since $x \mapsto xv$ is a permutation on $\mathbb{F}_{2^{2m}}$, it follows that the multisets $\{W_{f_\alpha}(a,b) : a \in \mathbb{F}_{2^{2m}}, b \in \mathbb{F}_{2^k}^*\}$ and $\{W_{f_\beta}(a,b) : a \in \mathbb{F}_{2^{2m}}, b \in \mathbb{F}_{2^k}^*\}$ are identical. □

Therefore if $x \mapsto Tr_k^{2m}(ax^{2^m-1})$ is a bent function, then we can assume without loss of generality that $a \in \mathbb{F}_{2^m}^*$.

We now state and prove our main result for this section, which provides several criteria for the coefficient of a Dillon-type monomial bent function mapping to $\mathbb{F}_4$.

Theorem 3.1.10. *Let m be even. If the function $f(x) = Tr_2^{2m}(ax^{2^m-1})$ is bent, then the minimal polynomials of $a, a\omega$, and $a\omega^2$ over $\mathbb{F}_2$ are either all the same, or all different. In the case that they are all the same, then that polynomial must have all exponents divisible by 3, and so m must be divisible by 6.*

Proof. By Proposition 3.1.9, we may assume without loss of generality that $a \in \mathbb{F}_{2^m}^*$. Since f is assumed to be bent, we have by Corollary 2.2.30 that a is a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$. Therefore $a\omega^i$ is a Kloosterman zero in $\mathbb{F}_{2^m}$ for each $i \in \mathbb{Z}_3$ by Theorem 2.1.23 and Corollary 2.2.30.

Since they are all Kloosterman zeros in $\mathbb{F}_{2^m}$, none of $a, a\omega, a\omega^2$ reside in a proper subfield of $\mathbb{F}_{2^m}$ by Theorem 3.1.6. Indeed, this is clear if $m \neq 4$, and if $m = 4$ and it happens that one of the elements $a\omega^i$ is equal to 1 (which is the unique Kloosterman zero in $\mathbb{F}_{16}$ residing in a proper subfield), then the other two elements are equal to ω and ω^2. As these are elements of a proper subfield of $\mathbb{F}_{16}$ that are different from 1, they cannot be Kloosterman zeros, contradicting the assumption.

By applying Theorem 3.1.7 with $\deg m_{a,0}(x) = m$, if $a\omega$ (resp. $a\omega^2$) is a conjugate of a but $a\omega^2$ (resp. $a\omega$) is not, then $a\omega^2$ (resp. $a\omega$) must have algebraic degree strictly less than m, and thus reside in a proper subfield of $\mathbb{F}_{2^m}$. The first conclusion follows.

The second conclusion, in the case that all three elements have the same minimal polynomial over $\mathbb{F}_2$, follows immediately from Theorem 3.1.8. □

Remark 3.1.11. The second conclusion of Theorem 3.1.10 provides a method for devising a good list of candidates for Dillon-type monomial functions mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_4$ for m even. The method is to search for those irreducible polynomials of degree $6k$ over $\mathbb{F}_2$ having all exponents divisible by 3 whose roots are Kloosterman zeros in $\mathbb{F}_{2^{6k}}$. It is well-known [26] that the number of irreducible monic polynomials of degree n over $\mathbb{F}_q$ is given by *Gauss' formula*

$$M_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

where $\mu : \mathbb{N} \to \mathbb{Z}$ is the *Möbius function* defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is square-free and has an even number of prime factors} \\ -1 & \text{if } n \text{ is square-free and has an odd number of prime factors} \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

Note that every irreducible polynomial of degree $6k$ over $\mathbb{F}_2$ having all exponents divisible by 3 is equal to $p(x^3)$ for some irreducible polynomial $p(x)$ of degree $2k$ over $\mathbb{F}_2$. Therefore the number of irreducible polynomials of degree $6k$ over $\mathbb{F}_2$ having all exponents divisible by 3 is no greater than number of irreducible polynomials of degree $2k$ over $\mathbb{F}_2$, which is

$$M_{2k}(2) = \frac{1}{2k}\sum_{d|2k}\mu(d)2^{2k/d}.$$

Asymptotically we have

$$M_{2k}(2) \approx \frac{3}{4^{2k}}M_{6k}(2),$$

therefore this method is substantially faster than simply searching over all irreducible polynomials of full degree.

For k in the range $1 \leq k \leq 10$, among all irreducible polynomials of degree $6k$ having all exponents divisible by 3 there are exactly two having Kloosterman zeros over $\mathbb{F}_{2^{6k}}$ as roots. These are $x^6 + x^3 + 1$, corresponding to the bent functions from Example 3.1.5 parts (i) and (ii), and $x^{12} + x^3 + 1$, corresponding to the bent function from Example 3.1.5 part (iii).

The details of the computations may be found in Appendix B.

3.1.3 Restrictions on the Maximum Output Dimension

In [54], Muratović-Ribić, Pasalic, and Bajrić showed that there are in fact no bent functions of the form $Tr_m^{2m}(ax^{2^m-1})$. In this section we combine several of the fundamental theorems presented in the previous chapter to give a more general result, from which the result of Muratović-Ribić, Pasalic, and Bajrić follows as a corollary.

Theorem 3.1.12 (Muratović-Ribić, Pasalic, Bajrić [54])**.** *Let $a \in \mathbb{F}_{2^m}^*$. If $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent then $k < m$.*

For context, we paraphrase the original proof appearing in [54]:

Original proof of Theorem 3.1.12 [54]. By Theorem 2.1.25 we have $k \leq m$, therefore suppose that $k = m$. By [54, Theorem 3], f is bent if and only if

$$\sum_{u\in\mathcal{U}}(-1)^{Tr_1^m(\lambda Tr_m^{2m}(au^{2^m-1}))} = 1 \text{ for all } \lambda \in \mathbb{F}_{2^m}^*. \tag{3.14}$$

Let $\lambda' = a\lambda$. Thus f is bent if and only if

$$\sum_{u\in\mathcal{U}}(-1)^{Tr_1^m(\lambda' Tr_m^{2m}(u^{2^m-1}))} = 1 \text{ for all } \lambda \in \mathbb{F}_{2^m}^*. \tag{3.15}$$

Since $u \mapsto u^{2^m-1}$ permutes the elements of $\mathcal{U}$, (3.15) further reduces to

$$\sum_{u\in\mathcal{U}}(-1)^{Tr_1^m(\lambda' Tr_m^{2m}(u))} = 1 \text{ for all } \lambda \in \mathbb{F}_{2^m}^*. \tag{3.16}$$

Let $u_0 \in \mathcal{U}\backslash\{1\}$ such that $Tr_m^{2m}(u_0) = u_0^2 + u_0^{-2} = 0$, and let $\mathcal{U}_0 = \mathcal{U}\backslash\{u_0\}$. Then (3.16) is equivalent to

$$\sum_{u\in\mathcal{U}_0} (-1)^{Tr_1^m(\lambda' Tr_m^{2m}(u))} = 0 \text{ for all } \lambda \in \mathbb{F}_{2^m}^*. \tag{3.17}$$

This implies that $Tr_m^{2m}(u^{2^m-1})$ is a bijection from $\mathcal{U}_0$ to $\mathbb{F}_{2^m}$ if f is bent. On the other hand, this implies that the function $Tr_1^{2m}(\lambda' x^{2^m-1})$ must be bent for any choice of $\lambda' \in \mathbb{F}_{2^m}^*$. This is impossible, since it was shown in [17, Theorem 6] that $Tr_1^{2m}(\lambda' x^{2^m-1})$ is not bent whenever λ' belongs to the set $\mathcal{T}_m$ given by

$$\mathcal{T}_m = \begin{cases} \{1\} & \text{if } m \text{ is odd} \\ \mathbb{F}_{2^t}^* & \text{if } m = 2t \text{ and } t > 2 \text{ is even} \\ \mathbb{F}_4\backslash\mathbb{F}_2 & \text{if } m = 4 \\ \mathbb{F}_{2^t}^* \cup \mathbb{F}_4^* & \text{if } m = 2t \text{ and } t \text{ is odd.} \end{cases}$$

□

Remark 3.1.13. The statement of [54, Theorem 3] is the following:

> *Let $f(x) = Tr_m^{2m}(P(x))$, where $P(x) = \sum_{i=0}^{2^m} a_i x^{r_i(2^m-1)}$, $a_i \in \mathbb{F}_{2^{2m}}$. Then f is bent if and only if*
>
> $$\sum_{u\in\mathcal{U}} (-1)^{Tr_1^m(\lambda Tr_m^{2m}(P(u)))} = 1$$
>
> *for all $\lambda \in \mathbb{F}_{2^m}^*$.*

Both the necessity and the sufficiency of the condition are shown by computing the extended Walsh transform of f at the point $(\lambda, \sigma) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^{2m}}$, and using the bijection that exists between $\mathbb{F}_{2^{2m}}^*$ and $\mathbb{F}_{2^m}^* \times \mathcal{U}$. The complexity of the proof is similar to that of Theorem 2.2.29.

Theorem 3.1.12 will be generalized for multinomial functions in the following section. Our next theorem gives conditions that are both necessary and sufficient for Dillon-type vectorial monomial functions to be bent.

Theorem 3.1.14. *Let $a \in \mathbb{F}_{2^m}^*$. Then $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent if and only if*

$$\mathcal{K}_{2^m}(a^2 b^{2^m+1}) = 0$$

for all $b \in \mathbb{F}_{2^k}^*$.

Proof. By Theorem 2.1.23, f is bent if and only if $Tr_1^k(bf(x)) = Tr_1^{2m}(bax^{2^m-1})$ is bent for all $b \in \mathbb{F}_{2^k}^*$. By Theorem 2.2.32, this is true if and only if

$$\mathcal{K}_{2^m}\left(N_m^{2m}(ba)\right) = 0 \text{ for all } b \in \mathbb{F}_{2^k}^*. \tag{3.18}$$

For any $b \in \mathbb{F}_{2^k}^*$ we have

$$\begin{aligned} N_m^{2m}(ba) &= (ba)^{2^m+1} \\ &= a^2 b^{2^m+1}. \end{aligned} \tag{3.19}$$

Therefore (3.18) holds if and only if $\mathcal{K}_{2^m}(a^2 b^{2^m+1}) = 0$ for all $b \in \mathbb{F}_{2^k}^*$. □

From this we obtain the result of Muratović-Ribić, Pasalic, and Bajrić as a corollary:

Corollary 3.1.15. *Let $a \in \mathbb{F}_{2^m}^*$. If $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent then $k < m$.*

Proof. By Theorem 2.1.25 we have $k \leq m$, therefore suppose that $k = m$. By Theorem 3.1.14, f is bent if and only if

$$\mathcal{K}_{2^m}(a^2 b^{2^m+1}) = 0 \text{ for all } b \in \mathbb{F}_{2^m}^*. \tag{3.20}$$

Since $b^{2^m+1} = b^2$ for all $b \in \mathbb{F}_{2^m}^*$, (3.20) holds if and only if $\mathcal{K}_{2^m}((ab)^2) = 0$ for all $b \in \mathbb{F}_{2^m}^*$. By Proposition 2.2.25 and the fact that $x \mapsto ax$ is a permutation on $\mathbb{F}_{2^m}^*$, this is the same as requiring that $\mathcal{K}_{2^m}(b) = 0$ for all $b \in \mathbb{F}_{2^m}^*$. By Corollary 2.2.24, this is impossible. □

Remark 3.1.16. In the second-to-last sentence of the proof above we conclude that the function $Tr_m^{2m}(ax^{2^m-1})$ is bent if and only if $\mathcal{K}_{2^m}(b) = 0$ for all $b \in \mathbb{F}_{2^m}^*$. Note that from here, we may obtain the result of Corollary 3.1.15 without reference to Corollary 2.2.24: if $\mathcal{K}_{2^m}(b) = 0$ for all $b \in \mathbb{F}_{2^m}^*$, then by Proposition 2.2.20 this allows for the function $Tr_1^{2m}(\lambda x^{2^m-1})$ to be bent for any choice of $\lambda \in \mathbb{F}_{2^{2m}}^*$. However, we know from Lemma 2.2.4 that this is impossible.

Remark 3.1.17. Theorem 3.1.14 provides us with a short alternative proof of Theorem 3.1.1:

Second proof of Theorem 3.1.1. If $Tr_1^{2m}(ax^{2^m-1})$ is bent, then $\mathcal{K}_{2^m}(a) = 0$ by Corollary 2.2.30. Since m is odd, $2^m + 1$ is divisible by 3, therefore for any $b \in \mathbb{F}_4^*$ we have

$$\begin{aligned} \mathcal{K}_{2^m}(a^2 b^{2^m+1}) &= \mathcal{K}_{2^m}(a^2) \\ &= \mathcal{K}_{2^m}(a) \\ &= 0. \end{aligned} \tag{3.21}$$

Therefore $Tr_2^{2m}(ax^{2^m-1})$ is bent by Theorem 3.1.14.

On the other hand, if $Tr_2^{2m}(ax^{2^m-1})$ is bent, then $Tr_1^{2m}(ax^{2^m-1})$ is bent as per Remark 2.1.24. □

Remark 3.1.18. Upon consideration of the previous remark, the reader may have noticed an apparent opportunity for generalization. Specifically, note that the result of the computation (3.21) was due precisely to the fact that $2^m + 1$ was divisible by the number of component functions of $Tr_2^{2m}(ax^{2^m-1})$.

Since the number of component functions of the vectorial function $Tr_k^{2m}(ax^{2^m-1})$ is $2^k - 1$, we may therefore generalize the argument presented in Remark 3.1.17 and conclude that $Tr_k^{2m}(ax^{2^m-1})$ is bent whenever $Tr_1^{2m}(ax^{2^m-1})$ is bent and $2^k - 1$ divides $2^m + 1$.

However, this attractive-looking result is in fact merely a restatement of Theorem 3.1.1 (indeed, this was the realization of Xu and Wu, reflected in revisions to the original version of [70]). The reason for this is the following:

Proposition 3.1.19. *Suppose that k and m are positive integers such that $2^k - 1$ divides $2^m + 1$. Then $k \leq 2$, and furthermore, if $k = 2$, then m must be odd.*

Proof. Let t be the greatest integer such that $tk \leq m$. We may write $2^m + 1 = 2^{m-tk}(2^{tk} - 1) + (2^{m-tk} + 1)$. Hence $2^k - 1$ must divide $2^{m-tk} + 1$. By the definition of t, we have $m - tk < k$. If $k > 2$, then for all integers $k' < k$ we have $2^{k'} + 1 < 2^k - 1$. Therefore $2^k - 1$ cannot possibly be a divisor of $2^{m-tk} + 1$, and so we must have $k \leq 2$.

Now suppose that $k = 2$. Then either $m - tk = 0$ or $m - tk = 1$. Since $2^2 - 1 \mid 2^1 + 1$ but $2^2 - 1 \nmid 2^0 + 1$, clearly we must have $m - tk = 1$, and therefore m must be odd. □

We already know from Theorem 2.2.23 that Kloosterman sums are always divisible by 4. The next theorem, due to van der Geer and van der Vlugt, characterizes Kloosterman sums modulo 8. This theorem will be useful in providing additional information regarding the restrictions governing the existence of Dillon-type vectorial monomial bent functions.

Theorem 3.1.20 (van der Geer, van der Vlugt [67])**.** *Let $n \geq 3$ and let $a \in \mathbb{F}_{2^n}$. Then*

$$\mathcal{K}_{2^n}(a) \equiv 4\,(Tr(a)) \pmod 8.$$

We have seen that the non-existence of bent functions of the form $Tr_m^{2m}(ax^{2^m-1})$ follows relatively easily from a handful of fundamental results. With a little more effort and with the aid of Theorem 3.1.20, we can show that there are no bent functions of the form $Tr_{m/2}^{2m}(ax^{2^m-1})$ for even $m \geq 4$.

First we have need of a lemma:

Lemma 3.1.21. *Let $a \in \mathbb{F}_{2^{2n}} \backslash \mathbb{F}_{2^n}$. Then the function $x \mapsto Tr_1^{2n}(ax)$ is balanced on $\mathbb{F}_{2^n}$.*

Proof. First we must show that $Tr_1^{2n}(ax)$ does not vanish on $\mathbb{F}_{2^n}$. To this end, note that the restriction of $Tr_1^{2n}(ax)$ to $\mathbb{F}_{2^n}$ is equal to the function $x \mapsto Tr_1^n(xTr_n^{2n}(a))$. By Theorem 1.3.9 part (v) and Theorem 1.3.10 we have $Tr_n^{2n}(x) = 0$ if and only if $x \in \mathbb{F}_{2^n}$. Therefore $Tr_n^{2n}(a) \neq 0$, hence $x \mapsto xTr_n^{2n}(a)$ permutes the elements of $\mathbb{F}_{2^n}$. Therefore $Tr_1^n(xTr_n^{2n}(a))$ does not vanish on $\mathbb{F}_{2^n}$.

Let $u \in \mathbb{F}_{2^n}$ be such that $Tr_1^{2n}(au) = 1$ (such an element exists by the argument above). For any $v \in \mathbb{F}_{2^n}$ we have $Tr_1^{2n}(a(v+u)) = Tr_1^{2n}(av) + Tr_1^{2n}(au) = Tr_1^{2n}(av) + 1$. Therefore the mapping $x \mapsto x + u$ is a bijection from $\{x \in \mathbb{F}_{2^n} : Tr_1^{2n}(ax) = 0\}$ to $\{x \in \mathbb{F}_{2^n} : Tr_1^{2n}(ax) = 1\}$. The result follows. □

Remark 3.1.22. Lemma 3.1.21 can also be established by counting:

Second proof of Lemma 3.1.21. Note that the multiplicative group $\mathbb{F}_{2^{2n}}^*$ contains 2^n cosets of $\mathbb{F}_{2^n}^*$ different from $\mathbb{F}_{2^n}^*$ itself. Let $u \in \mathbb{F}_{2^{2n}}$ be such that $Tr_1^{2n}(u) = 1$, and let C_u be the coset of $\mathbb{F}_{2^n}^*$ containing u. By noting that the mapping $x \mapsto x + u$ is a bijection from $\{x \in C_u \backslash \{u\} : Tr_1^{2n}(x) = 0\}$ to $\{x \in C_u \backslash \{u\} : Tr_1^{2n}(x) = 1\}$, we see that $Tr_1^{2n}(x)$ is balanced on $C_u \backslash \{u\}$. Therefore C_u contains 2^{n-1} elements x such that $Tr_1^{2n}(x) = 1$.

Since $\#\{x \in \mathbb{F}_{2^{2n}} : Tr_1^{2n}(x) = 1\} = 2^{2n-1}$ by Proposition 1.3.13, this argument may be applied iteratively to conclude that each of the 2^n cosets of $\mathbb{F}_{2^n}^*$ different from $\mathbb{F}_{2^n}^*$ in $\mathbb{F}_{2^{2n}}^*$ contains 2^{n-1} elements x such that $Tr_1^{2n}(x) = 1$. In particular, this is true for the coset C_a containing a. Therefore $Tr_1^{2n}(ax)$ is balanced on $\mathbb{F}_{2^n}$. □

We conclude our treatment of Dillon-type monomial functions by showing that a function of the form $Tr_{m/2}^{2m}(ax^{2^m-1})$ is not bent for any choice of $a \in \mathbb{F}_{2^{2m}}$.

Theorem 3.1.23. *Let $m \geq 4$ be even, and let $a \in \mathbb{F}_{2^m}^*$. If $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent then $k \neq m/2$.*

Proof. Let us first deal with the case where $m > 4$. Let us assume to the contrary that $f(x) = Tr_{m/2}^{2m}(ax^{2^m-1})$ is bent. Since f is bent, we have by Theorem 3.1.14

$$\mathcal{K}_{2^m}(a^2 b^{2^m+1}) = 0 \text{ for all } b \in \mathbb{F}_{2^{m/2}}^*. \tag{3.22}$$

Since $\mathbb{F}_{2^m}$ is a quadratic extension of $\mathbb{F}_{2^{m/2}}$ we have $a^2 b^{2^m+1} = (ab)^2$ for all $b \in \mathbb{F}_{2^{m/2}}^*$. Therefore by Proposition 2.2.25 and (3.22) we have

$$\mathcal{K}_{2^m}(ab) = 0 \text{ for all } b \in \mathbb{F}_{2^{m/2}}^*. \tag{3.23}$$

In particular, we have $\mathcal{K}_{2^m}(a) = 0$. Since $\mathcal{K}_{2^m}(a) = 0$, we have that $a \in \mathbb{F}_{2^m} \backslash \mathbb{F}_{2^{m/2}}$ by Theorem 3.1.6. By applying Lemma 3.1.21 with $n = m/2$, there exists an element $u \in \mathbb{F}_{2^{m/2}}^*$ such that $Tr_1^m(au) = 1$. By Theorem 3.1.20, we have $\mathcal{K}_{2^m}(au) \equiv 4 \pmod 8$, hence $\mathcal{K}_{2^m}(au) \neq 0$. Therefore there exists an element of $u \in \mathbb{F}_{2^{m/2}}^*$ such that au is not a Kloosterman zero in $\mathbb{F}_{2^m}$. As this contradicts (3.23), f cannot be bent.

For the case of $m = 4$, let us again assume that $f(x) = Tr_2^8(ax^{2^4-1})$ is bent. Then again we have

$$\mathcal{K}_{2^4}(ab) = 0 \text{ for all } b \in \mathbb{F}_4^*. \tag{3.24}$$

In particular, we have $\mathcal{K}_{2^4}(a) = 0$. If $a \in \mathbb{F}_{2^4} \backslash \mathbb{F}_4$, the result follows from the argument for the previous case. If $a \notin \mathbb{F}_{2^4} \backslash \mathbb{F}_4$, then $\mathcal{K}_{2^4}(a) = 0$ implies that $a = 1$ by Theorem 3.1.6. If $a = 1$, then by (3.24) we have $\mathcal{K}_{2^4}(b) = 0$ for all $b \in \mathbb{F}_4^*$, which is impossible. □

3.2 Dillon-type Multinomial Functions

In this section we consider vectorial extensions of multinomial functions of the type (2.23) that were characterized by Charpin and Gong in [17].

We begin by discussing binomial functions mapping $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_4$ in the case that m is even. Recall that this case is difficult to deal with for monomial functions (see Remark 3.1.2), and furthermore examples of bent functions of this kind are sparse. Therefore examining binomials of the type (2.23) is a logical next step in the search for quaternary bent functions of high algebraic degree that admit a relatively simple algebraic description.

After this we present a new result regarding conditions necessary for the existence of Dillon-type vectorial multinomial bent functions. Namely, we will use the characterization given by Charpin and Gong (Theorem 2.2.40) to extend Theorem 3.1.12 to vectorial extensions of multinomial functions of the type (2.23). This shows that functions of this kind cannot meet the Nyberg bound given by Theorem 2.1.25. We note that questions of this kind have received some very recent attention, most notably in [57], where it was claimed that a function of the form

$$Tr_m^{2m}\left(x^{2^m-1} + \lambda x^{r(2^m-1)}\right)$$

with m even is not bent for any choice of $r \in \{1, \ldots, 2^m\}$, $\lambda \in \mathbb{F}_{2^{2m}}$. However, this claim was later retracted in [58], due to an error in the proof, which in turn stemmed from a typographical error in [54, Open Problem 1]. A variation of this claim, where $\lambda \in \mathbb{F}_{2^m}$ and the parity of m is not restricted, follows from the main result of subsection 3.2.2.

3.2.1 Binomial Functions Mapping to $GF(4)$

In the previous section we discussed the existence of Dillon-type monomial bent functions mapping from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_4$. We saw that such functions exist in abundance when m is odd, and, conversely, are quite rare when m is even. Somewhat ironically, it is the even case that is more desirable for implementations, since software engineers will always desire bit lengths to have a minimal number and size of odd factors. Thus we examine Dillon-type *binomial* functions as the logical next step in producing bent functions of high algebraic degree mapping $\mathbb{F}_{2^{4m}}$ to $\mathbb{F}_4$. Happily, our computational results have shown that these functions are plentiful relative to their monomial counterparts. The full computations and their results are presented in Appendix B.3.

To get some sense of the density of these functions among all binomial functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_4$ we sampled random pairs $\beta_1, \beta_3 \in \mathbb{F}_{2^m}^*$ until the corresponding function

$$f(x) = Tr_2^{2m}\left(\beta_1 x^{2^m-1} + \beta_3 x^{3(2^m-1)}\right) \tag{3.25}$$

was bent, as determined by the criteria of Theorems 2.1.23 and 2.2.40. We recorded the average number of random samples required to achieve this in the course of a manageable number of trials (ten). We carried out the computations for each even m in the range $4 \leq m \leq 10$, where we found bent functions of the type (3.25) for each value of m.

3.2.2 Necessary Conditions for Vectorial Bentness

Prior to stating and proving the main theorem of this section, we establish a demonstrative proposition and a useful lemma. We will make use of the following terminology:

Definition 3.2.1 (Indicator Function)**.** *Let $A \subseteq \mathbb{F}_{2^m}$. The function $\phi_A : \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$\phi_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ otherwise} \end{cases}$$

is called the indicator function of A.

In particular, every Boolean function is the indicator function of its support.

Proposition 3.2.2. *Let S be a subset of $\mathbb{F}_{2^m}$ such that $\#S = 2^{m-1}$, and let $\phi_S : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be the indicator function of S. Then for $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ we have*

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{g(x)+\phi_S(x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{g(x)} \tag{3.26}$$

if and only if g is balanced on S.

Proof. By the definition of ϕ_S we have

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{g(x)+\phi_S(x)} = \sum_{x \in S} (-1)^{g(x)+1} + \sum_{x \in \mathbb{F}_{2^m} \setminus S} (-1)^{g(x)},$$

therefore (3.26) holds if and only if

$$\sum_{x \in S} (-1)^{g(x)+1} = \sum_{x \in S} (-1)^{g(x)}$$

which reduces to

$$\sum_{x \in S} (-1)^{g(x)} = 0.$$

□

Lemma 3.2.3. *Let S be a subset of $\mathbb{F}_{2^m}$ such that $\#S = 2^{m-1}$, and let $h : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. Then there exists an element $\alpha \in \mathbb{F}_{2^m}^*$ such that the function*

$$x \mapsto Tr(\alpha h(x))$$

is not balanced on S.

Proof. For $\alpha \in \mathbb{F}_{2^m}$ define

$$n(\alpha) := \#\{x \in S : Tr(\alpha h(x)) = 0\} - \#\{x \in S : Tr(\alpha h(x)) = 1\}.$$

We must show that there exists $\alpha \in \mathbb{F}_{2^m}^*$ such that $n(\alpha) \neq 0$. For a given $\alpha \in \mathbb{F}_{2^m}$ we have

$$n(\alpha) = \sum_{x \in S} (-1)^{Tr(\alpha h(x))}. \tag{3.27}$$

Squaring both sides of (3.27) and subsequently summing over all $\alpha \in \mathbb{F}_{2^m}$ yields

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_{2^m}} n(\alpha)^2 &= \sum_{\alpha \in \mathbb{F}_{2^m}} \sum_{x,y \in S} (-1)^{Tr(\alpha h(x))} (-1)^{Tr(\alpha h(y))} \\ &= \sum_{\alpha \in \mathbb{F}_{2^m}} \sum_{x,y \in S} (-1)^{Tr(\alpha (h(x)+h(y)))} \\ &= \sum_{x,y \in S} \sum_{\alpha \in \mathbb{F}_{2^m}} (-1)^{Tr(\alpha (h(x)+h(y)))}. \end{aligned} \tag{3.28}$$

By Proposition 1.3.14 we have

$$\sum_{\alpha \in \mathbb{F}_{2^m}} (-1)^{Tr(\alpha (h(x)+h(y)))} = \begin{cases} 2^m \text{ if } h(x) = h(y) \\ 0 \text{ otherwise} \end{cases}.$$

Therefore (3.28) becomes

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_{2^m}} n(\alpha)^2 &= \sum_{\substack{x,y \in S \\ h(x)=h(y)}} 2^m \\ &= 2^{m-1} \cdot 2^m + \sum_{\substack{x,y \in S \\ x \neq y \\ h(x)=h(y)}} 2^m = 2^{2m-1} + \sum_{\substack{x,y \in S \\ x \neq y \\ h(x)=h(y)}} 2^m. \end{aligned} \tag{3.29}$$

This implies that $\sum_{\alpha \in \mathbb{F}_{2^m}} n(\alpha)^2 \geq 2^{2m-1}$. For $\alpha = 0$, we have $n(\alpha) = n(0) = \#S = 2^{m-1}$, and thus $n(0)^2 = 2^{2m-2}$. Therefore

$$\sum_{\alpha \in \mathbb{F}_{2^m}^*} n(\alpha)^2 \geq 2^{2m-2} > 0$$

which implies that there exists at least one $\alpha \in \mathbb{F}_{2^m}^*$ such that $n(\alpha) \neq 0$. □

Remark 3.2.4. As we did with Lemma 3.1.21, we make note of an alternative proof of the preceding Lemma:

Second proof of Lemma 3.2.3. Let f be any bijection from $\mathbb{F}_{2^m} \backslash S$ to S. Define the function $H : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ by

$$H(x) = \begin{cases} h(x) \text{ if } x \in S \\ h(f(x)) \text{ if } x \in \mathbb{F}_{2^{2m}} \backslash S. \end{cases}$$

Then for each $x \in \mathbb{F}_{2^m}$, the pre-image $H^{-1}(x)$ has even size. Therefore H is not a bijection, and is therefore not balanced. By Proposition 1.3.31, this implies that there exists an element $a \in \mathbb{F}_{2^m}^*$ such that the function $x \mapsto Tr(aH(x))$ is not balanced on $\mathbb{F}_{2^m}$. Since $x \mapsto Tr(aH(x))$ is balanced on $\mathbb{F}_{2^m}$ exactly when the function $x \mapsto Tr(ah(x))$ is balanced on S, the result follows. □

We are now in a position to generalize Theorem 3.1.12 for functions of the type (2.23).

Theorem 3.2.5. *Let R be a non-empty set of representatives of cyclotomic cosets modulo 2^m+1, and let $E \subseteq R$. With each $r \in E$ associate an element $\beta_r \in \mathbb{F}_{2^m}^*$. For $k \mid 2m$, define $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ by*

$$f(x) = Tr_k^{2m}\left(\sum_{r \in E} \beta_r x^{r(2^m-1)}\right). \tag{3.30}$$

If f is bent, then $k < m$.

Proof. By Theorem 2.1.25 we have $k \leq m$, therefore suppose that $k = m$. Let $\omega \in \mathbb{F}_{2^m}$ be primitive, and for $i = 0, 1, \ldots, 2^m - 2$ let

$$g_i(x) = Tr_1^m\left(\sum_{r \in E} \omega^i \beta_r D_r(x)\right),$$

where $D_r(x)$ denotes the r-th Dickson polynomial over $\mathbb{F}_2$. By Theorem 2.1.23, f is bent if and only if the function $x \mapsto Tr_1^m(\omega^i f(x))$ is bent for $i = 0, 1, \ldots, 2^m - 2$. By noting that

$$\begin{aligned} Tr_1^m(\omega^i f(x)) &= Tr_1^m\left(\omega^i Tr_m^{2m}\left(\sum_{r \in E} \beta_r x^{r(2^m-1)}\right)\right) \\ &= Tr_1^{2m}\left(\sum_{r \in E} \omega^i \beta_r x^{r(2^m-1)}\right) \end{aligned}$$

and applying Theorem 2.2.40, we see that f is bent if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{g_i(x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr(x^{-1}) + g_i(x)} \text{ for } i = 0, 1, \ldots, 2^m - 2. \tag{3.31}$$

Let S denote the support of the function $x \mapsto Tr_1^m(x^{-1})$, and note that $\#S = 2^{m-1}$ since $x \mapsto x^{-1}$ is a permutation on $\mathbb{F}_{2^m}$ (where we take $0^{-1} = 0^{2^m-2} = 0$). By Proposition 3.2.2, (3.31) holds for a given i if and only if g_i is balanced on S. But by Lemma 3.2.3, there exists an i such that g_i is not balanced on S. Therefore (3.31) does not hold for all values of i, and so f is not bent. □

Once again, we obtain Theorem 3.1.12 as a corollary:

Corollary 3.2.6 (Muratović-Ribić, Pasalic, Bajrić [54])**.** *If $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent then $k < m$.*

Proof. By Proposition 2.2.20, it is sufficient to consider the case that $a \in \mathbb{F}_{2^m}^*$. Theorem 3.2.5 now gives the result. □

Remark 3.2.7. In [55], Muratović-Ribić, Pasalic, and Ribić gave an exact count of the number of vectorial bent functions of the form

$$f(x) = Tr_m^{2m}\left(\sum_{i=0}^{2^m} a_i x^{i(2^m-1)}\right),\ a_i \in \mathbb{F}_{2^{2m}}. \tag{3.32}$$

Note that these functions are not of the type (3.30), since a function of the latter type has all coefficients in the multinomial residing in the largest proper subfield of the domain, whereas the functions (3.32) have no such specification.

Additionally, the authors gave a method for computing those coefficients $a_i \in \mathbb{F}_{2^{2m}}$ that result in a bent function of the form (3.32) [55, Corollary 2]. However, we note that computing the a_i's using this method is of exponential complexity, in terms of both time and memory requirements [55, Equation (12)]. The authors proposed an optimization for the number of coefficients in [55, Section V], but this does not appear to reduce the overall time or space complexities of the computations by more than a constant factor. On the other hand, recall that the Dillon-type multinomial functions (2.23) are constructable in polynomial time (see Remark 2.2.43).

Remark 3.2.8. We compare the complexity of the conditions governing the bentness of Dillon-type multinomial functions to those for the simpler monomial case:

We saw in Theorem 3.1.14 that the function $Tr_k^{2m}(ax^{2^m-1})$ is bent if and only if

$$\mathcal{K}_{2^m}(a^2 b^{2^m+1}) = 0 \text{ for all } b \in \mathbb{F}_{2^k}^*. \tag{3.33}$$

If $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^m}$, that is, if k divides m, then (3.33) simplifies to

$$\mathcal{K}_{2^m}(b) = 0 \text{ for all } b \in a\mathbb{F}_{2^k}^*. \tag{3.34}$$

We compare this to the condition induced by Theorems 2.1.23 and 2.2.40 in the case that $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^m}$. Consider the function

$$f(x) = Tr_k^{2m}\left(\sum_{r\in E} \beta_r x^{r(2^m-1)}\right),$$

as defined in the statement of Theorem 3.2.5. By Theorem 2.1.23, f is bent if and only if the component function

$$\begin{aligned} f_\lambda(x) &= Tr_1^k(\lambda f(x)) \\ &= Tr_1^k\left(\lambda Tr_k^{2m}\left(\sum_{r\in E} \beta_r x^{r(2^m-1)}\right)\right) \\ &= Tr_1^{2m}\left(\sum_{r\in E} \lambda\beta_r x^{r(2^m-1)}\right) \end{aligned}$$

is bent for all $\lambda \in \mathbb{F}_{2^k}^*$. We may apply Theorem 2.2.40 to each of the component functions f_λ to conclude as in the proof of Theorem 3.2.5 that f is bent if and only if the function

$$g_\lambda(x) = Tr_1^m\left(\sum_{r\in E} \lambda\beta_r D_r(x)\right)$$

is balanced on the support of $x \mapsto Tr_1^m(x^{-1})$ for all $\lambda \in \mathbb{F}_{2^k}^*$.

On the other hand, if $\mathbb{F}_{2^k}$ is *not* a subfield of $\mathbb{F}_{2^m}$, then the coefficients $\lambda\beta_r$ are not all elements of $\mathbb{F}_{2^m}$, and so Theorem 2.2.40 does not apply to all of the component functions f_λ (see Remark 2.2.44 at the end of the previous chapter).

3.3 Divisibility of Kloosterman Sums

As we have seen, to construct a Dillon-type monomial bent function from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_2$ is to find a zero of the Kloosterman sum over $\mathbb{F}_{2^m}$, and to construct such a function from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^k}$ is to find a certain multiplicative coset consisting entirely of such elements. However, there exists no method for explicitly constructing these elements, and they are notoriously hard to locate. In [46], Lisoněk gave an algorithm that required approximately one day to find a Kloosterman zero in all fields of order 2^m for $m \leq 64$ using the computer algebra system Magma 2.14 running on an Intel Xeon CPU at 3.0 GHz. An algorithm that is estimated to be at most $2m$ times faster than the one given in [46] was presented in [4].

In this section we present some new results regarding the value of Kloosterman sums modulo 64 and 256 for field elements residing in the union of certain cosets of a maximal proper subfield. Our primary tools will be the recent results of Göloğlu *et al.* regarding the value of Kloosterman sums modulo 2^k for $k \in \{1, 2, \ldots, 8\}$. In a special case, we will be able to use our results in conjunction with Theorem 2.2.23 to give a set of Kloosterman

zeros in $\mathbb{F}_{64}$. Despite being a special case, this example will be notable in that it is the first time that a set of Kloosterman zeros has been synthesized explicitly (as opposed to being found algorithmically). The author hopes that the methods used here will inspire further constructions in the future.

3.3.1 Kloosterman Sums and the Characteristic Polynomial

Recall the characteristic polynomial over $\mathbb{F}_2$ of an element $a \in \mathbb{F}_{2^n}$,

$$\prod_{i=0}^{n-1} \left(x - a^{2^i}\right) = x^n + e_1 x^{n-1} + \ldots + e_{n-1}x + e_n. \tag{3.35}$$

Formally, the coefficients $e_1, \ldots, e_n$ are elements of $\mathbb{F}_2$. However, in this section and beyond we will view them simultaneously as integers in $\{0, 1\}$. The reason for this will become apparent shortly.

In [30], Göloğlu *et al.* gave several results relating the coefficients of the characteristic polynomial over $\mathbb{F}_2$ of an element $a \in \mathbb{F}_{2^n}$ to the value of $\mathcal{K}_{2^n}(a) \mod 2^k$ for $k = 5, 6, 7, 8$, with $n \geq k$ (characterizations corresponding to $k = 1, 2, 3, 4$ were already relatively well-known via [32], [46], and [67]). In our work we will only make use of the results corresponding to the cases $k = 6, 8$. In this section we quote only the result corresponding to $k = 6$ in its entirety. For the full statement of the result corresponding to $k = 8$ we refer the reader to Appendix C.1, and also to [52, Theorem 3.17]. We give an abridged version in Theorem 3.3.2 below, for the sake of giving the reader a sense of its character.

First, the result corresponding to the case $k = 6$. As was done in [30] we note that an equivalent version appears in [29].

Theorem 3.3.1 (Moloney [52])**.** *Let $n \geq 6$ and let $a \in \mathbb{F}_{2^n}^*$. Let $e_1, \ldots, e_8$ be the coefficients of the characteristic polynomial of a over $\mathbb{F}_2$ as described in* (3.35)*. Then*

$$\begin{aligned}\mathcal{K}_{2^n}(a) \equiv\ & 28e_1 + 40e_2 \\ & + 16(e_1e_2 + e_1e_3 + e_4) \\ & + 32(e_1e_4 + e_1e_5 + e_1e_6 + e_1e_7 \\ & + e_2e_3 + e_2e_4 + e_2e_6 + e_3e_5 \\ & + e_1e_2e_3 + e_1e_2e_4 + e_8) \pmod{64}.\end{aligned}$$

We now give an abridged version of the result corresponding to the case $k = 8$. The full statement of the result may be found in Appendix C.1.

Theorem 3.3.2 (Göloğlu *et al.* [30], [52])**.** *Let $n \geq 8$ and let $a \in \mathbb{F}_{2^n}^*$. Let $e_1, \ldots, e_{32}$ be the coefficients of the characteristic polynomial of a over $\mathbb{F}_2$ as described in* (3.35)*. Then*

$e_1, \ldots, e_{32}$ are related to $\mathcal{K}_{2^n}(a)$ via a congruence of the form

$$\begin{aligned}\mathcal{K}_{2^n}(a) \equiv\ & 16e_4 + 32(e_1e_7 + e_2e_6 + e_8) \\ & \cdots + 224(e_2e_3 + e_2e_4 + e_3e_5 + e_1e_2e_4) \pmod{256}.\end{aligned}$$

The proofs of the results corresponding to each of the cases $k = 1, \ldots, 8$ may be found in [52].

3.3.2 New Divisibility Results on Kloosterman Sums

Using the preceding material, we will now establish some new divisibility theorems for Kloosterman sums over fields of characteristic two. In conjunction with Theorem 2.2.23, these new theorems will allow us to explicitly synthesize a collection of Kloosterman zeros in $\mathbb{F}_{2^6}$. We will use these zeros to construct two new examples of Dillon-type vectorial monomial bent functions. These examples are not constructible via any other results currently known in the literature. In fact, we will see that these examples correspond to two of the three examples given previously in Section 3.1 (see Table 3.1).

Prior to discussing the central material of this section, we are compelled to establish an elementary divisibility fact:

Proposition 3.3.3. *Let p and k be positive integers, and suppose that $q = 2^p - 1$ is prime. Then $\frac{2^{qk}-1}{2^k-1}$ is divisible by q if and only if p divides k.*

Proof. First note that p must be prime since q is prime.

If p divides k then $2^p \equiv 1 \pmod{q}$ implies that $2^k \equiv 1 \pmod{q}$, and therefore

$$\begin{aligned}\frac{2^{qk}-1}{2^k-1} &= 1 + 2^k + 2^{2k} + \ldots + 2^{(q-1)k} \\ &\equiv \underbrace{1 + 1 + \ldots + 1}_{q \text{ terms}} \equiv 0 \pmod{q}.\end{aligned}$$

On the other hand, suppose that p does not divide k, but q divides $\frac{2^{qk}-1}{2^k-1}$. This implies that $q = 2^p - 1$ divides $2^{qk} - 1$, which in turn implies that p divides qk. Since $\gcd(k, p) = 1$, we conclude that p divides q, which is impossible. □

The proposition above ensures that we are not in fact discussing the empty set in the material that follows (see Remark 3.3.5 below). The next theorem pertains to elements residing in cosets of a certain subfield of a field with a specific subfield structure. In particular, we will see that the characteristic polynomials of these elements exhibit a fairly restricted structure, which is (happily) conducive to the application of the results of Göloğlu *et al.*.

Theorem 3.3.4. *Let p be a positive integer such that $q = 2^p - 1$ is prime, and let k be a positive integer divisible by p. Let $F = \mathbb{F}_{2^{qk}}$, let $L = \mathbb{F}_{2^k}$, and let $\beta \in F$ be such that β^q is a primitive element of L. If*

$$\phi(x) = x^{qk} + e_1 x^{qk-1} + ... + e_{qk-1}x + e_{qk}$$

is the characteristic polynomial over $\mathbb{F}_2$ of a non-zero element $a \in \bigcup_{i=0}^{p-1} \beta^{2^i} L$, then

$$e_i = 0 \quad \text{if } i \not\equiv 0 \pmod{q}.$$

Proof. Note that for $\alpha \in L$ and $i \in \{1, \ldots, p-1\}$, the element $\beta^{2^i}\alpha$ has a conjugate of the form $\beta\alpha'$ for some $\alpha' \in L$. In particular, $\beta^{2^i}\alpha$ and $\beta\alpha'$ have the same characteristic polynomial. Therefore it is sufficient to deal with the case that a is a non-zero element of βL.

Let $\psi(x)$ be the minimal polynomial of a over $\mathbb{F}_2$. Then $\phi(x)$ is a power of $\psi(x)$ by Theorem 1.3.1. Therefore it is sufficient to show that $\psi(x)$ has the property that the exponent of every non-zero term is a multiple of q.

Let $\psi_q(x)$ be the minimal polynomial of a^q over $\mathbb{F}_2$. Then a is a root of $\psi_q(x^q)$, and furthermore $\psi_q(x^q)$ has the desired property. We will show further that $\deg \psi_q(x^q) = \deg \psi(x)$, and therefore that $\psi_q(x^q) = \psi(x)$, yielding the result.

Let $n = \deg \psi(x)$, and let $m = \deg \psi_q(x)$. Since a^q is an element of L and of $\mathbb{F}_2(a)$, we have $m \mid k$ and $m \mid n$. Since $a \in F \backslash L$, we have $n \mid qk$, but $n \nmid k$. Clearly we have $m \leq n \leq qm$. Suppose that $n = jm$ for some $j \in \{1, ..., q-1\}$. Then $n \mid jk$ since $m \mid k$. But since $\gcd(j, q) = 1$ and $n \mid qk$, this implies that $n \mid k$, a contradiction. Therefore $n = qm$, and thus $\deg \psi_q(x^q) = q \deg \psi_q(x) = qm = n = \deg \psi(x)$. □

Remark 3.3.5. Prior to the statement and proof of Theorem 3.3.4 we claimed that Proposition 3.3.3 "ensures that we are not in fact discussing the empty set". We now clarify this statement:

The statement of Theorem 3.3.4 assume the existence of an element $\beta \in \mathbb{F}_{2^{qk}}$ such that $\beta^q \in \mathbb{F}_{2^k}$ is primitive. Since a primitive element of L has the form $\omega^{(2^{qk}-1)/(2^k-1)}$ for some primitive element $\omega \in F$, such a β exists if and only if $q = 2^p - 1$ divides $(2^{qk} - 1)/(2^k - 1) = 1 + 2^k + 2^{2k} + \ldots + 2^{(q-1)k}$. Proposition 3.3.3 establishes that this happens exactly when p divides k, therefore we include this latter condition as an assumption in all statements that require the existence of such a $\beta \in \mathbb{F}_{2^{qk}}$.

We now apply Theorem 3.3.4 with $p = 2$ to obtain our first new theorem pertaining to the divisibility of Kloosterman sums:

Theorem 3.3.6. *Let k be an even integer, let $F = \mathbb{F}_{2^{3k}}$, and let $L = \mathbb{F}_{2^k}$. Let $\beta \in F$ be such that β^3 is a primitive element of L. Then for any non-zero $a \in \beta L \cup \beta^2 L$ we have*

$$\mathcal{K}_{2^{3k}}(a) \equiv 0 \pmod{64}.$$

Proof. Let a be a non-zero element of $\beta L \cup \beta^2 L$, and let

$$\phi(x) = x^{3k} + e_1 x^{3k-1} + ... + e_{3k-1}x + e_{3k}$$

be the characteristic polynomial of a over $\mathbb{F}_2$. By Theorem 3.3.4, we have

$$e_i = 0 \text{ whenever } i \not\equiv 0 \pmod{3}. \tag{3.36}$$

From Theorem 3.3.1 we have

$$\begin{aligned}\mathcal{K}_{2^{3k}}(a) \equiv\ & 28e_1 + 40e_2 \\ & + 16(e_1e_2 + e_1e_3 + e_4) \\ & + 32(e_1e_4 + e_1e_5 + e_1e_6 + e_1e_7 \\ & + e_2e_3 + e_2e_4 + e_2e_6 + e_3e_5 \\ & + e_1e_2e_3 + e_1e_2e_4 + e_8) \pmod{64}.\end{aligned} \tag{3.37}$$

One may check that (3.36) and (3.37) combine to give the result. □

The following example is a demonstration of the above theorem. Details of the computations may be found in Appendix B.6.

Example 3.3.7. Let $p(x) \in \mathbb{F}_2[x]$ be the irreducible polynomial

$$x^{24} + x^{16} + x^{15} + x^{14} + x^{13} + x^{10} + x^9 + x^7 + x^5 + x^3 + 1,$$

and let $F = \mathbb{F}_2[x]/\langle p(x)\rangle$. Hence $F = \mathbb{F}_{2^{24}}$. Let $\alpha \in F$ be a root of $p(x)$, let $t = (2^{24} - 1)/(2^8 - 1)$ and let $\gamma = \alpha^t$. Then the set $\{0, \gamma\}$ generates the subfield L of order 2^8, i.e. $L = \mathbb{F}_{2^8}$. Let $\beta \in F$ be such that $\beta^3 = \gamma$. Then $a = \beta\gamma^3$ has characteristic polynomial

$$x^{24} + x^{21} + x^{18} + x^{15} + x^{12} + x^3 + 1$$

over $\mathbb{F}_2$, and $\mathcal{K}_{2^{24}}(a) = -3264$, which is divisible by 64 (but not by 128).

Recall Theorem 2.2.23, which states that $x \mapsto \mathcal{K}_{2^n}(x)$ maps $\mathbb{F}_{2^n}^*$ to the set $\{t : 1 - 2^{n/2+1} \leq t \leq 1 + 2^{n/2+1} \text{ and } t \equiv 0 \pmod 4\} \subset \mathbb{Z}$. In particular, we will make use of the fact that $\mathcal{K}_{2^n}(a)$ resides in the interval $[1 - 2^{n/2+1}, 1 + 2^{n/2+1}]$ for all $a \in \mathbb{F}_{2^n}^*$.

We will now use Theorems 2.2.23 and 3.3.6 to explicitly synthesize a collection of Kloosterman zeros in $\mathbb{F}_{64}$. We will subsequently use these elements to construct two examples of

Dillon-type vectorial monomial bent functions previously unknown in the literature: one mapping $\mathbb{F}_{2^{12}}$ to $\mathbb{F}_4$, and the other mapping $\mathbb{F}_{2^{12}}$ to $\mathbb{F}_{16}$. See Appendix B.6 for details of the computations.

Example 3.3.8. Let $p(x) \in \mathbb{F}_2[x]$ be the irreducible polynomial

$$x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1,$$

and let $E = \mathbb{F}_2[x]/\langle p(x)\rangle$. Hence $E = \mathbb{F}_{2^{12}}$. Let F denote the subfield of index 2 in E; $F = \mathbb{F}_{64}$. Let $\omega \in E$ be a root of $p(x)$, and let $\alpha = \omega^{65}$. Hence α is a primitive element of F.

Let $\beta = \alpha^7$, and let $\gamma = \alpha^{21}$. Then the set $\{0, \gamma\}$ generates the subfield L of order 4, i.e. $L = \mathbb{F}_4$. By Theorem 3.3.6, for any $a \in \beta L \cup \beta^2 L$ we have $\mathcal{K}_{2^6}(a) \equiv 0 \pmod{64}$. Let $\mathcal{E}(a)$ be the elliptic curve over $\mathbb{F}_{2^6}$ defined by

$$\mathcal{E}(a) := y^2 + xy = x^3 + a.$$

By Theorem 2.2.23, $\mathcal{K}_{2^6}(a)$ lies in the interval $[-15, 17]$. As 0 is the only integer in the interval $[-15, 17]$ that is divisible by 64, we must have $\mathcal{K}_{2^6}(a) = 0$.

Thus by Corollary 2.2.30, for any non-zero $a \in \beta L \cup \beta^2 L$, the function

$$Tr_1^{12}(ax^{63})$$

is bent. Additionally, it can be shown that

$$\{N_6^{12}(\gamma^i a) : i = 0, 1, 2\} \subseteq \beta L \cup \beta^2 L \text{ for all } a \in \beta L \cup \beta^2 L$$

(note that $\{N_6^{12}(\gamma^i a) : i = 0, 1, 2\} = \{N_6^{12}(a) : a \in \beta L \cup \beta^2 L\} \backslash \{0\}$, see Appendix B.6). Therefore the function

$$Tr_2^{12}(ax^{63})$$

is also bent for any non-zero $a \in \beta L \cup \beta^2 L$ by Theorem 2.1.23 and Theorem 2.2.32.

Finally, let $t = (2^{12} - 1)/(2^4 - 1)$, and let $\delta = \omega^t$. Then δ is a primitive element of $\mathbb{F}_{16}$, and we see that a similar situation occurs, that is,

$$\{N_6^{12}(\delta^i a) : 0 \leq i \leq 14\} \subseteq \beta L \cup \beta^2 L \text{ for all } a \in \beta L \cup \beta^2 L.$$

Therefore the function

$$Tr_4^{12}(ax^{63})$$

is also bent for any non-zero $a \in \beta L \cup \beta^2 L$.

Note that we have recovered the first two functions that were described in Example 3.1.5, which, as noted previously, constitute two of the three bent functions of the form $Tr_k^{2m}(ax^{2^m-1})$ for $2 \leq k < m \leq 30$, with m even.

We now apply Theorem 3.3.4 with $p = 3$ to obtain our second and last result regarding the divisibility of Kloosterman sums. Unfortunately, we will not be able to make use of Theorem 2.2.23 to explicitly identify Kloosterman zeros (and hence vectorial bent functions), as we did in the example above. The reasons for this will be made clear shortly in Example 3.3.11.

Theorem 3.3.9. *Let k be an positive integer divisible by three, let $F = \mathbb{F}_{2^{7k}}$, and let $L = \mathbb{F}_{2^k}$. Let $\beta \in F$ be such that β^7 is a primitive element of L. Then for any non-zero $a \in \beta L \cup \beta^2 L \cup \beta^4 L$ we have*

$$\mathcal{K}_{2^{7k}}(a) \equiv 0 \pmod{256}.$$

Proof. Let a be a non-zero element of $\beta L \cup \beta^2 L \cup \beta^4 L$, and let

$$\phi(x) = x^{7k} + e_1 x^{7k-1} + ... + e_{7k-1}x + e_{7k}$$

be the characteristic polynomial of a over $\mathbb{F}_2$. By Theorem 3.3.4, we have

$$e_i = 0 \text{ whenever } i \not\equiv 0 \pmod{7}. \tag{3.38}$$

By Theorem 3.3.2 we have

$$\begin{aligned} \mathcal{K}_{2^{7k}}(a) \equiv\ & 16e_4 + 32(e_1e_7 + e_2e_6 + e_8) \\ & \cdots + 224(e_2e_3 + e_2e_4 + e_3e_5 + e_1e_2e_4) \pmod{256} \end{aligned} \tag{3.39}$$

(see Appendix C.1 for the full statement of the congruence). One may check that (3.38) and (3.39) combine to give the result (see Appendix C.2 for more details). □

As before, we demonstrate the theorem with an example. Details of the computations may be found in Section B.6.

Example 3.3.10. Let $p(x) \in \mathbb{F}_2[x]$ be the irreducible polynomial

$$x^{42} + x^{30} + x^{26} + x^{25} + x^{24} + x^{20} + x^{18} + x^{12} + x^{11} + x^9 + x^6 + x^5 + x^2 + x + 1,$$

and let $F = \mathbb{F}_2[x]/\langle p(x)\rangle$. Hence $F = \mathbb{F}_{2^{42}}$. Let $\alpha \in F$ be a root of $p(x)$, let $t = (2^{42} - 1)/(2^6 - 1)$ and let $\gamma = \alpha^t$. Then the set $\{0, \gamma\}$ generates the subfield L of order 2^6; $L = \mathbb{F}_{2^6}$. Let $\beta \in F$ be such that $\beta^7 = \gamma$. Then $a = \beta\gamma^5$ has characteristic polynomial

$$x^{42} + x^{14} + 1,$$

and $\mathcal{K}_{2^{42}}(a) = -4096$, which is divisible by 256.

Here we see a divergence from the form of Example 3.3.7: note that -4096 is divisible by powers of 2 higher that $2^8 = 256$. In Example 3.3.7, we noted that 64 was the highest power of 2 dividing the value of the Kloosterman sum, hence demonstrating that the stated scope of Theorem 3.3.6 is in fact its true scope. Interestingly, in the case of Theorem 3.3.9, for all $a \in \beta L$ we observed for $k = 3, 6, 9, 12, 15$ that $\mathcal{K}_{2^{7k}}(a)$ was divisible by a power of 2 no less than 2^{11}.

Example 3.3.11. We will attempt to mimic Example 3.3.8:

Let $p(x) \in \mathbb{F}_2[x]$ be the irreducible polynomial

$$x^{21} + x^6 + x^5 + x^2 + 1,$$

and let $F = \mathbb{F}_2[x]/\langle p(x)\rangle$. Hence $F = \mathbb{F}_{2^{21}}$. Let $t = (2^{21} - 1)/(2^3 - 1)$. Let $\alpha \in F$ be be a root of $p(x)$, let $\beta = \alpha^{t/7} = \alpha^{42799}$, and let $\gamma = \alpha^t$. Then the set $\{0, \gamma\}$ generates the subfield L of order 7, and by Theorem 3.3.6, for any $a \in \beta L \cup \beta^2 L \cup \beta^4 L$ we have $\mathcal{K}_{2^{21}}(a) \equiv 0 \pmod{256}$. Let $\mathcal{E}(a)$ be the elliptic curve over $\mathbb{F}_{2^{21}}$ defined by

$$\mathcal{E}(a) := y^2 + xy = x^3 + a.$$

By Theorem 2.2.23, $\mathcal{K}_{2^{21}}(a)$ lies in the interval

$$[1 - 2^{21/2+1}, 1 + 2^{21/2+1}].$$

Since the interval has size $2^{21/2+2} \approx 5800$, clearly there are many integers in the interval that are divisible by 256 ($\lfloor 2^{21/2+2-8} \rfloor = 22$, to be exact). Therefore we cannot draw any conclusions about the exact value of $\mathcal{K}_{2^{21}}(a)$ similar to what we did in Example 3.3.8.

Remark 3.3.12. Primes of the form $q = 2^p - 1$ are called *Mersenne primes*. One can see that p must be prime in order for q to be prime via the identity

$$2^{mn} - 1 = (2^n - 1)(1 + 2^n + 2^{2n} + \ldots + 2^{(m-1)n}).$$

On the other hand we have $2^{11} - 1 = 23 \times 89$. The smallest prime p such that $2^p - 1$ is composite is in fact $p = 11$. It is not known whether or not the set of Mersenne primes is infinite (though it has been conjectured that this is indeed the case [68]). Currently there are 48 known Mersenne primes.

In this section we applied Theorem 3.3.4 with $p = 2, 3$ to the results of Göloğlu *et al.* to obtain new results on the divisibility of Kloosterman sums modulo 64 and 256, respectively. One naturally wonders whether Theorem 3.3.4 could be applied with greater values of p to obtain similar results for greater moduli. However we are limited by the extent of the results

of Göloğlu *et al.*, which are in turn limited by the increasing complexity of the arguments as the modulus grows [30].

Chapter 4

Computational Results and Future Research

In this chapter we discuss avenues of future research on the topic of vectorial bent functions in characteristic two. Most of the topics for future research discussed here relate directly to extending the methods and results presented in the previous chapter. The first two sections of this chapter are of this nature, where we specifically discuss extending the methods of Sections 3.1 and 3.2 to obtain tighter necessary conditions for the existence of both monomial and mutlinomial bent functions of the Dillon type. In the third section of this chapter we discuss an open problem of Charpin and Gong relating to the construction of Dillon-type Boolean binomial bent functions. In the fourth and final section we give a list of original conjectures based on the research done for this thesis, and supported by computer experiments.

We alert the reader that the open problems discussed in the first two sections of this chapter constitute part of the subject matter of a second publication currently in preparation, intended in part to extend the work presented in our current publication [41].

4.1 Obtaining Stronger Necessary Conditions for Dillon-type Bent Functions

Theorem 3.1.14 states that the function $Tr_k^{2m}(ax^{2^m-1})$ is bent if and only if the set

$$\{a^2x^{2^m+1} : x \in \mathbb{F}_{2^k}^*\} \subseteq \mathbb{F}_{2^m}^*$$

consists entirely of Kloosterman zeros (recall that we may assume without loss of generality that $a \in \mathbb{F}_{2^m}^*$). Recall Theorem 3.1.6, which states that the multiplicative identity is a zero of the Kloosterman sum over $\mathbb{F}_{16}$, and, most importantly, that this is the *only* occurrence of a Kloosterman zero residing in a proper subfield. Thus a natural question arises:

For $k \mid 2m$ and for a fixed $a \in \mathbb{F}_{2^m}^*$, when does the set $\{a^2 x^{2^m+1} : x \in \mathbb{F}_{2^k}^*\}$ have a non-empty intersection with a proper subfield of $\mathbb{F}_{2^m}$?

There are two cases:

Case 1. If $k \mid m$, then $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^m}$. In this case we have $b^{2^m+1} = b^2$ for all $b \in \mathbb{F}_{2^k}$. Therefore by Theorem 3.1.14 and Proposition 2.2.25, the function $Tr_k^{2m}(ax^{2^m-1})$ is bent if and only if

$$\mathcal{K}_{2^m}(ab) = 0 \text{ for all } b \in \mathbb{F}_{2^k}^*. \tag{4.1}$$

which is equivalent to

$$\mathcal{K}_{2^m}(b) = 0 \text{ for all } b \in a\mathbb{F}_{2^k}^*. \tag{4.2}$$

Note that we may assume without loss of generality that $a \in \mathbb{F}_{2^m} \backslash \mathbb{F}_{2^k}$ by virtue of Theorem 3.1.6.

In Theorem 3.1.23 we saw that in the case that $k = m/2$, the coset $a\mathbb{F}_{2^k}^*$ always contains an element of absolute trace 1, which is therefore not a Kloosterman zero in $\mathbb{F}_{2^m}$ by Theorem 3.1.20. Hence (4.2) fails in this case due in part to the distribution of the function $Tr_1^m(x)$ on the cosets of $\mathbb{F}_{2^{m/2}}^*$ in $\mathbb{F}_{2^m}$.

When $m \geq 8$ is divisible by 4 and $k = m/4$, preliminary computational results suggest that the *subtrace* $\tau : \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$\tau(x) = \sum_{0 \leq i < j \leq m-1} x^{2^i + 2^j}$$

exhibits four possible distributions on cosets of the form $a\mathbb{F}_{2^k}^*$ for $a \in \mathbb{F}_{2^m} \backslash \mathbb{F}_{2^k}$. The following theorem appears in [52]. As was done in [30] we note that a result giving the condition for divisibility by 16 was stated in an equivalent form in [46].

Theorem 4.1.1 (Göloğlu, McGuire, Moloney [29])**.** *Let $m \geq 4$ and let $a \in \mathbb{F}_{2^m}^*$. Then*

$$\mathcal{K}_{2^m}(a) \equiv 12\,(Tr(a)) + 8\,(\tau(a)) \pmod{16}.$$

With further analysis of the distributions of the subtrace on the cosets of $\mathbb{F}_{2^k}^*$, it may be possible to use Theorem 4.1.1 to rule out the existence of bent functions of the form

$$Tr_{m/4}^{2m}\left(ax^{2^m-1}\right)$$

when $m \geq 8$ is divisible by 4.

Case 2. If $k \nmid m$, then there exists no subfield relation between $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$. In this case we may say that the function $f(x) = Tr_k^{2m}(ax^{2^m-1})$ is bent if and only if

$$\mathcal{K}_{2^m}(x) = 0 \text{ for all } x \in \{a^2 b^{2^m+1} : b \in \mathbb{F}_{2^k}^*\}. \tag{4.3}$$

Note that the set $\{b^{2^m+1} : b \in \mathbb{F}_{2^k}\}$ contains both 0 and 1 and is closed under multiplication. Furthermore, by Propositions 1.3.2 and 2.2.9, the image of $\mathbb{F}_{2^k}^*$ in $\mathbb{F}_{2^m}^*$ under the mapping $x \mapsto x^{2^m+1}$ has size

$$\frac{2^k-1}{\gcd(2^k-1, 2^m+1)} = \begin{cases} 2^k-1 & \text{if } k/\gcd(k,m) \text{ is odd} \\ \frac{2^k-1}{2^{\gcd(k,m)}+1} & \text{if } k/\gcd(k,m) \text{ is even.} \end{cases}$$

Since $k \mid 2m$ but $k \nmid m$, this implies that $k/\gcd(k,m)$ is even, therefore the image of $\mathbb{F}_{2^k}^*$ in $\mathbb{F}_{2^m}^*$ under the mapping $x \mapsto x^{2^m+1}$ has size

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

Therefore the set $\{b^{2^m+1} : b \in \mathbb{F}_{2^k}\}$ is exactly the subfield $\mathbb{F}_{2^{k/2}} \subset \mathbb{F}_{2^m}$, and we conclude that f is bent if and only if

$$\mathcal{K}_{2^m}(a^2 b) = 0 \text{ for all } b \in \mathbb{F}_{2^{k/2}}^*. \tag{4.4}$$

For any $b \in \mathbb{F}_{2^{k/2}}^*$, the element $a^2 b \in \mathbb{F}_{2^m}^*$ has a conjugate of the form ab' for some $b' \in \mathbb{F}_{2^{k/2}}^*$. Therefore (4.4) is equivalent to

$$\mathcal{K}_{2^m}(b) = 0 \text{ for all } b \in a\mathbb{F}_{2^{k/2}}^*. \tag{4.5}$$

Thus in both cases the most fruitful method for obtaining stronger necessary conditions for Dillon-type bent functions appears to be that of analyzing the distributions of the trace and subtrace on the multiplicative cosets of a certain subfield.

4.2 Obtaining a Tighter Bound on the Maximum Output Dimension for Dillon-type Multinomial Bent Functions

The following is an extension of Theorem 3.1.1 to multinomial functions:

Theorem 4.2.1 (Lisoněk [45])**.** *Let m be odd, let R be a non-empty set of representatives of cyclotomic cosets modulo 2^m+1, and let $E \subseteq R$ such that every $r \in E$ has the same non-zero remainder upon division by 3. With each $r \in E$ associate an element $\beta_r \in \mathbb{F}_{2^m}^*$. Define $P(x) \in \mathbb{F}_{2^m}[x]$ by*

$$P(x) = \sum_{r \in E} \beta_r x^{r(2^m-1)}.$$

Then $Tr_2^{2m}(P(x))$ is bent if and only if $Tr_1^{2m}(P(x))$ is bent.

Theorem 4.2.1 shows that Dillon-type multinomial bent functions mapping to $\mathbb{F}_4$ are comparably abundant to their Boolean counterparts, while Theorem 3.2.5 shows that any

Dillon-type vectorial multinomial bent function mapping $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^m}$ must have coefficients in $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_{2^m}$. In between these two extremes we have the Dillon-type monomial bent function constructed in Example 3.1.5, mapping $\mathbb{F}_{2^{12}}$ to $\mathbb{F}_{2^4}$. Computational results suggest that, at least for even m, vectorial functions of this kind are quite rare. However, we are restricted to computations in relatively low dimension, as the set of candidates on fields with more than 2^{60} elements is simply too large to search through in any reasonable amount of time. Therefore questions abound regarding the existence, abundance, and distribution of Dillon-type vectorial multinomial bent functions.

We discuss possible extensions of the results of Section 3.2. In particular, we discuss the limitations of the arguments used to prove Theorem 3.2.5, and determine what additional information is needed in order to extend these techniques to obtain tighter necessary conditions.

Let E be a non-empty set of representatives of cyclotomic cosets modulo $2^m + 1$, and to each $r \in E$ associate an element $\beta_r \in \mathbb{F}_{2^m}^*$. Let $k \mid 2m$, and define $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^k}$ by

$$f(x) = Tr_k^{2m}\left(\sum_{r \in E} \beta_r x^{r(2^m-1)}\right). \tag{4.6}$$

We seek to establish a tight upper bound on the dimension k of the range $\mathbb{F}_{2^k}$ if f is to be bent.

Let $\omega \in \mathbb{F}_{2^k}$ be primitive, and let $g_i(x) = Tr_1^m\left(\sum_{r \in E} \omega^i \beta_r D_r(x)\right)$. Similar to what was established in the proof of Theorem 3.2.5, f is bent if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{g_i(x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{g_i(x) + Tr(x^{-1})} \tag{4.7}$$

for $i = 0, 1, \ldots, 2^k - 2$.

Let S denote the support of $Tr(x^{-1})$. In order for Equation (4.7) to hold for all values of i, we have by Proposition 3.2.2 that g_i must be balanced on S for $i = 0, 1, \ldots, 2^k - 2$.

Thus a reasonable approach to establishing necessary conditions on k is to determine the conditions that cause g_i *not* to be balanced on S for a given value of i, and how those conditions relate to k. We have already seen that this occurs when $k = m$, via Lemma 3.2.3. Let us determine the obstructions to extending this particular method. We begin by re-iterating the setting of Lemma 3.2.3:

Let m and k be positive integers such that $k \mid m$. Let $h : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, and let $S \subset \mathbb{F}_{2^m}$ be such that $\#S = 2^{m-1}$. Finally, for $\alpha \in \mathbb{F}_{2^k}$ define $n(\alpha) := \#\{x \in S : Tr(\alpha h(x) = 0)\} - \#\{x \in S : Tr(\alpha h(x) = 0)\}$.

We wish to outline a set of conditions on the function h and on the integer k guaranteeing the existence of an $\alpha \in \mathbb{F}_{2^k}^*$ such that $n(\alpha) \neq 0$. Following the proof of Lemma 3.2.3, but

this time summing over $\mathbb{F}_{2^k}$ rather than over $\mathbb{F}_{2^m}$, we have

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_{2^k}} n(\alpha)^2 &= \sum_{\substack{x,y\in S\\ h(x)=h(y)}} 2^k \\ &= 2^{m+k-1} + \sum_{\substack{x,y\in S\\ x\neq y\\ h(x)=h(y)}} 2^k. \end{aligned} \tag{4.8}$$

Let $N = \#\{x, y \in S : x \neq y \text{ and } h(x) = h(y)\}$. As shown previously, $n(0)^2 = 2^{2m-2}$. Therefore in order to have $\sum_{a\in\mathbb{F}_{2^k}^*} n(\alpha)^2 > 0$ (and hence guarantee the existence of an $\alpha \in \mathbb{F}_{2^k}^*$ such that $n(\alpha) \neq 0$), we must have

$$\begin{aligned} & 2^{m+k-1} + 2^k N - 2^{2m-2} > 0 \\ \Rightarrow\ & N > 2^{m-1}(2^{m-k-1} - 1). \end{aligned} \tag{4.9}$$

At this point we can go no further without possessing meaningful information regarding the number N, which is dependent on the characteristics of the function h (namely, the degree of "non-injectivity" of the restriction of h to S). In our desired application of this argument, we set $h(x) = \sum_{r\in E} \beta_r D_r(x)$, where the set E and the coefficients β_r are as defined previously. The set S will be the support of the function $x \mapsto Tr_1^m(x^{-1})$. Obtaining estimates of the size of the set $\{x, y \in S : x \neq y \text{ and } h(x) = h(y)\}$ may therefore benefit from further study of the Dickson polynomials over $\mathbb{F}_2$.

In [18], Chou, Gomez-Calderon and Mullen provided an exact formula for the size of the image of $\mathbb{F}_{2^n}$ under the action of the i-th Dickson polynomial over $\mathbb{F}_2$.

Theorem 4.2.2 (Chou, Gomez-Calderon, Mullen [18])**.** *For all $i \geq 1$ we have*

$$\#\{D_i(x) : x \in \mathbb{F}_{2^n}\} = \frac{2^n - 1}{2\gcd(i, 2^n - 1)} + \frac{2^n + 1}{2\gcd(i, 2^n + 1)}. \tag{4.10}$$

If one were able to extend this result to a useful formula which calculates

$$\#\{\sum_{r\in E} \beta_r D_r(x) : x \in \mathbb{F}_{2^m}\} \tag{4.11}$$

for a given $E \subset \mathbb{Z}$, this could possibly be applied to (4.9) to obtain meaningful results (it would still be necessary to know how a polynomial of the form $\sum_{r\in E} \beta_r D_r(x)$ behaves on the support of the function $x \mapsto Tr_1^m(x^{-1})$). However, given the effort expended in [18] to obtain Theorem 4.2.2, the problem of finding a good formula for (4.11) may very well be more difficult than extending Theorem 3.2.5 via some other method.

4.3 Regarding an Open Problem of Charpin and Gong

In [17], Charpin and Gong posed the following Open Problem:

Open Problem 4.3.1 ([17], Open Problem 4)**.** *Let m, r be integers such that $m/\gcd(m,r)$ is odd. Describe the set of $\lambda \in \mathbb{F}_{2^m}^*$ such that the function $Tr_1^m(x^{2^m-2} + \lambda x^{2^r+1})$ is balanced on $\mathbb{F}_{2^m}$.*

This problem is motivated by a special case of the functions defined in Theorem 2.2.40. Namely, let $m/\gcd(m,r)$ be odd, and let

$$f(x) = Tr_1^m\left(\lambda(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)})\right). \tag{4.12}$$

Let $g(x) = Tr_1^m\left(\lambda(D_{2^r-1}(x) + D_{2^r+1}(x))\right)$. By Theorem 2.2.40, f is bent if and only if

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{g(x)+Tr_1^m(x^{2^m-2})} = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{g(x)}. \tag{4.13}$$

By Definition 2.2.38 and Proposition 2.2.39, we have

$$D_{2^r+1}(x) = xD_{2^r}(x) + D_{2^r-1}(x) = x(D_1(x))^{2^r} + D_{2^r-1}(x) = x^{2^r+1} + D_{2^r-1}(x),$$

therefore we have

$$\begin{aligned} g(x) &= Tr_1^m\left(\lambda(D_{2^r-1}(x) + x^{2^r+1} + D_{2^r-1}(x))\right) \\ &= Tr_1^m\left(\lambda x^{2^r+1}\right). \end{aligned}$$

Since $m/\gcd(m,r)$ is odd, $\gcd(2^r+1, 2^m-1) = 1$, and therefore $x \mapsto x^{2^r+1}$ is a permutation on $\mathbb{F}_{2^m}$. In particular, we have $\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(\lambda x^{2^r+1})} = 0$, and therefore (4.13) reduces to

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x^{2^m-2}+\lambda x^{2^r+1})} = 0 \tag{4.14}$$

thus motivating Open Problem 4.3.1.

Note that since $Tr_1^m(x^{2^m-2} + \lambda x^{2^r+1}) = Tr_1^m(x^{2^m-2}) + Tr_1^m(\lambda x^{2^r+1})$, the function $Tr_1^m(x^{2^m-2} + \lambda x^{2^r+1})$ is balanced on $\mathbb{F}_{2^m}$ if and only if the set $\{x \in \mathbb{F}_{2^m} : Tr_1^m(x^{2^m-2}) = Tr_1^m(\lambda x^{2^r+1})\}$ has size 2^{m-1}. In Appendix B.5 we give computational results showing that there are relatively many such $\lambda \in \mathbb{F}_{2^m}$ for m in the range $4 \le m \le 20$, and therefore relatively many binomial bent functions of the form (4.12). Recall that these functions meet Rothaus' bound, and that the associated monomial functions are never bent.

4.4 Conjectures

We conclude with a list of conjectures based on the work presented in Chapter 3. All but one of the conjectures relates directly to the work and methods presented in Chapter 3.

4.4.1 The Existence of Dillon-type Vectorial Monomial Bent Functions

The Nyberg bound shows that if $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is bent then $m \leq n/2$. In [54], Muratović-Ribić, Pasalic, and Bajrić showed that there are no bent functions of the form $Tr_m^{2m}(ax^{2^m-1})$. In Section 3.1 we extended this to show that there are no bent functions on the form $Tr_{m/2}^{2m}(ax^{2^m-1})$ (see Theorem 3.1.23). Given this trend, one is tempted to conjecture the following:

Conjecture 4.4.1. *Let r be a non-negative integer, let $k > 1$, and let $a \in \mathbb{F}_{2^{2^r k}}^*$. Then the function $Tr_k^{2^{r+1}k}\left(ax^{2^{2^r k}-1}\right)$ is never bent.*

As per the previous paragraph, this statement is now known to be true for $r = 0$ and $r = 1$. Considering the discussion in Section 4.1 along with some preliminary computational results, the statement seems quite likely to be true for $r = 2$ as well.

In subsection 3.1.1 we presented a condition sufficient for the existence of a bent function of the form

$$f(x) = Tr_k^{2m}\left(ax^{2^m-1}\right)$$

for $k \mid 2m$, $k > 1$ (see Theorem 3.1.3). In Remark 3.1.4, we gave our reasons for believing that this condition is in fact necessary. Here we formally state this belief as a conjecture:

Conjecture 4.4.2. *If $Tr_k^{2m}(ax^{2^m-1})$ is bent, then*

$$N_m^{2m}[\mathbb{F}_{2^k}^*] \subseteq \{a, a^2, \ldots, a^{2^{m-1}}\}.$$

In fact, given the results of our computations, we make the following much stronger conjecture:

Conjecture 4.4.3. *Let m be even. Bent functions of the form $Tr_k^{2m}(ax^{2^m-1})$ with $k > 1$ exist only for the following (m, k)-pairs: $(6, 2)$, $(6, 4)$, and $(12, 2)$.*

Note that Conjecture 4.4.2 can be re-stated as a conjecture on Kloosterman zeros:

Conjecture 4.4.4 (Re-statement of Conjecture 4.4.2)**.** *Let $A = \{a \in \mathbb{F}_{2^m}^* : \mathcal{K}_{2^m}(a) = 0\}$. For all $k \mid 2m$ and for all $a \in A$, if $a^2 N_m^{2m}[\mathbb{F}_{2^k}^*] \subseteq A$ then*

$$N_m^{2m}[\mathbb{F}_{2^k}^*] \subseteq \{a, a^2, \ldots, a^{2^{m-1}}\}.$$

4.4.2 Divisibility of Kloosterman Sums

In subsection 3.3.2 we gave new divisibility results on Kloosterman sums. In particular, for $k \in \mathbb{Z}^+$ we constructed subsets of $\mathbb{F}_{2^{6k}}$ (resp. $\mathbb{F}_{2^{21k}}$) wherein the Kloosterman sum at every element is divisible by 64 (resp. 256). The following material deals with the problem of constructing field elements whose Kloosterman sums are divisible by 128.

As before, we must establish a divisibility fact:

Proposition 4.4.5. *Let n and m be positive integers, and let k be a divisor of m. Then $(n^k-1)^2$ divides n^m-1 if and only if $m \equiv 0 \pmod{k(n^k-1)}$*

Proof. Clearly, $(n^k-1)^2$ divides n^m-1 if and only if n^k-1 divides $(n^m-1)/(n^k-1) = 1+n^k+...+n^{m-k}$. Since $n^k \equiv 1 \pmod{n^k-1}$, we have $1+n^k+...+n^{m-k} \equiv m/k \pmod{n^k-1}$. Therefore n^k-1 divides $1+n^k+...+n^{m-k}$ if and only if $m/k \equiv 0 \pmod{n^k-1}$, which is true if and only if $m \equiv 0 \pmod{k(n^k-1)}$. □

As in subsection 3.3.2, the divisibility fact above ensures the existence of a particular field element (see Conjecture 4.4.6 below).

The following conjecture is very similar to Theorem 3.3.4. Though the current author has not yet found a proof for it, the conjecture seems overwhelmingly likely to be true based on computational results.

Conjecture 4.4.6. *Let k be a positive integer, and let m be a multiple of $k(2^k-1)$. Let $F = \mathbb{F}_{2^m}$, let $L = \mathbb{F}_{2^k}$, let $\gamma \in L$ be primitive, and let $\beta \in F$ be such that $\beta^{2^k-1} = \gamma$. If $\phi_a(x) = e_0x^m + e_1x^{m-1} + ... + e_{m-1}x + e_m$ is the minimal polynomial over $\mathbb{F}_2$ of a non-zero element $a \in \bigcup_{i=0}^{k-1} \beta^{2^i}L$, then*

$$e_i = 0 \quad \text{if } i \not\equiv 0 \pmod{2^k-1}.$$

The preceding conjecture, along with extensive experiments performed using Magma, form the basis for the following two conjectures on the divisibility of Kloosterman sums.

Conjecture 4.4.7. *Let k be a positive integer, and let m be a multiple of $k(2^k-1)$. Let $L = \mathbb{F}_{2^k}$, let $F = \mathbb{F}_{2^m}$, let γ be a primitive element of L, and let $\beta \in F$ be such that $\beta^{2^k-1} = \gamma$. Let a be an element of $\bigcup_{i=0}^{k-1} \beta^{2^i}L$. Then*

$$\max\{t : 2^t \text{ divides } \mathcal{K}_{2^m}(a)\} \geq 3k, \text{ or } \mathcal{K}_{2^m}(a) = 0.$$

Conjecture 4.4.8. *Let n be a positive integer, and let m, k be divisors of n such that $\gcd(m,k) = 1$. Let $L = \mathbb{F}_{2^m}$, $F = \mathbb{F}_{2^n}$, let γ be a primitive element of L, and let $\beta \in F$ be such that $\beta^{2^k-1} = \gamma$. Let a be an element of $\bigcup_{i=0}^{k-1} \beta^{2^i}L$. Then*

$$\mathcal{K}_{2^n}(a) \equiv 0 \pmod{128}.$$

4.4.3 Function Families of Maximum Size

We give a necessary definition:

Definition 4.4.9 (Affine Equivalence)**.** *The functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ are called* affine-equivalent *if there exist affine permutations $h_n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $h_m : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that*

$$f(x) = h_m\left(g(h_n(x))\right).$$

If f and g are affine-equivalent, then $nl(f) = nl(g)$ [12, Section 8.6]. Proposition 2.1.9 is a special case of this.

Recall Theorem 2.2.5, which states that for any polynomial $P(x) \in \mathbb{F}_{2^n}[x]$, the maximum number of coefficients λ such that the function $f(x) = Tr_1^n(\lambda P(x))$ is bent is $2^n - 2^{n/2}$.

This bound was stated and proved by Pott *et al.* in [60]. It is met by functions that are linear-equivalent to the Gold monomials presented in subsection 2.2.1 [60]. Pott *et al.* also constructed a new class of binomial functions that meet this bound:

Theorem 4.4.10 (Pott *et al.* [60])**.** *For $i \in \{0, 1, \ldots, 2m-1\}$, the function $f(x) = Tr_1^{2m}\left(\lambda x^{2^i}(x + x^{2^m})\right)$ is bent if and only if $\lambda \notin \mathbb{F}_{2^m}$.*

We will refer to these function as *PPMB binomials* (after the surnames of the authors: Pott, Pasalic, Muratović-Ribić, Bajrić). Our conjecture is that, along with the Gold functions, this new class of functions is the only one to meet the bound given by Theorem 2.2.5.

Conjecture 4.4.11. *If $f(x) = Tr_1^n\left(\lambda(x^{d_1} + ax^{d_2})\right)$ is bent for $2^n - 2^{n/2}$ choices of λ, then either*

(i) f is affine-equivalent to a PPMB binomial,

or

(ii) f is affine-equivalent to a Gold function.

This conjecture is supported by exhaustive computer searches up to $n = 16$ (see Appendix B.7).

Bibliography

[1] Adams, C. *Constructing Symmetric Ciphers Using the CAST Design Procedure*. Des. Codes Cryptogr. 12 (1997), 283–316.

[2] Adams, C. *On immunity against Biham and Shamir's "differential cryptanalysis"*. Inf. Process Lett. (1992), no. 41, 77–80.

[3] Adams, C.; Tavares, S. *The structured design of cryptographically good S-boxes*. J. Cryptology 3 (1990), no. 1, 27–41.

[4] Ahmadi, O.; Granger, R. *An efficient deterministic test for Kloosterman sum zeros*. Math. Comp. 83 (2014), no. 285, 347–363.

[5] Bending, T. D.; Fon-Der-Flaass, D. *Crooked functions, bent functions, and distance regular graphs*. Electron. J. Combin. 5 (1998), Research Paper 34, 14 pp. (electronic). Available at: www.combinatorics.org/ojs/index.php/eljc/issue/view/Volume5

[6] Biham, E.; Shamir, A. *Differential cryptanalysis of DES-like cryptosystems*. Advances in Cryptology – CRYPTO '90. pp. 2–21. Springer–Verlag, 1990.

[7] Blake, I., Seroussi, G., Smart, N. *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[8] Bosma, W.; Steel, A. *Magma handbook: finite fields*. Computational Algebra Group, School of Mathematics and Statistics, University of Sydney.

[9] Budaghyan, L. *The simplest method for constructing APN polynomials EA-inequivalent to power functions*. Arithmetic of finite fields, 177 – 188, Lecture Notes in Comput. Sci., 4547, Springer, Berlin, 2007.

[10] Budaghyan, L.; Carlet, C. *CCZ-equivalence of bent vectorial functions and related constructions*. Des. Codes Cryptogr. 59 (2011), no. 1 – 3, 69 – 87.

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

[12] Carlet, C. *Boolean Functions for Error-Correcting Codes and Cryptography*, and *Vectorial Boolean Functions for Cryptography*, in: *Boolean models and methods in mathematics, computer science, and engineering*. Edited by Yves Crama and Peter L. Hammer. Encyclopedia of Mathematics and its Applications, 134. Cambridge University Press, Cambridge, 2010.

[13] Carlet, C.; Charpin, P.; Zinoviev, V. *Codes, bent functions and permutations suitable for DES-like cryptosystems*. Designs, Codes and Cryptography, 15 (2), pp. 125–156, 1998.

[14] Carlet, C.; Ding, C. *Highly Nonlinear Mappings*. J. Complexity 20 (2–3), 205–244 (2004).

[15] Carlet, C.; Gaborit, P. *Hyper-bent functions and cyclic codes*. J. Combin. Theory Ser. A 113 (2006), no. 3, 466–482.

[16] Carlet, C.; Mesnager, S. *Four decades of research on bent functions*. Des. Codes Cryptogr. 78 (2016), no. 1, 5–50.

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

[18] Chou, W. S.; Gomez-Calderon, J.; Mullen, G. L. *Value sets of Dickson polynomials over finite fields*. J. Number Theory 30 (1988), no. 3, 334–344.

[19] Cusick, T. W.; Stănică, P. *Cryptographic Boolean functions and applications*. Elsevier/Academic Press, Amsterdam, 2009.

[20] Delsarte, P.; Goethals, J.-M. *Irreducible binary cyclic codes of even dimension*. 1970 Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications (Univ. North Carolina, Chapel Hill, N.C., 1970) pp. 100–113 Univ. North Carolina, Chapel Hill, N.C.

[21] Dillon, J. F. *Elementary Hadamard Difference Sets*. Thesis (Ph.D.) – University of Maryland, College Park. 1974.

[22] Dillon, J. F.; Dobbertin, H. *New cyclic difference sets with singer parameters*. Finite Fields Applic., pp. 342–389, 2004.

[23] Dobbertin, H.; Leander, N. G. *A Survey of Some Recent Results on Bent Functions*.

[24] Dong, D.; Zhang, X.; Qu, L.; Fu, S. *A note on vectorial bent functions*. Inform. Process. Lett. 113 (2013), no. 22–24, 866–870.

[25] Edel, Y.; Pott, A. *On the equivalence of non-linear functions*. Enhancing cryptographic primitives with techniques from error correcting codes, 87 – 103, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 23, IOS, Amsterdam, 2009.

[26] Gauss, C. F. *Untersuchungen Uber Höhere Arithmetik*, second edition, reprinted, Chelsea publishing company, New York 1981.

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

[28] Golomb, S. W.; Gong, G. *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[29] Göloğlu, F.; McGuire, G.; Moloney, R. *Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula*. Acta Arith., vol. 148, no. 3, pp. 269–279, 2011.

[30] Göloğlu, F.; Lisoněk, P.; McGuire, G.; Moloney, R. *Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial*. IEEE Trans. Inform. Theory 58 (2012), no. 4, 2516 – 2523.

[31] Gong, G.; Golomb, S. W. *Transform Domain Analysis of DES*. IEEE transactions on Information Theory. Vol. 45. no. 6. pp. 2065–2073. September, 1999.

[32] Helleseth, T.; Zinoviev, V. *On Z4-linear Goethals codes and Kloosterman sums*. Des. Codes Cryptogr. 17 (1999), no. 1–3, 269–288.

[33] Jakobsen, T.; *Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low Degree*. Proceedings of Crypto '99. LNCS 1462. pp. 213–222. 1999.

[34] Jakobsen, T.; Knudsen, L. *The Interpolation Attack on Block Ciphers*. LNCS 1267, Fast Software Encryption. pp. 28–40. 1997.

[35] Kavut, S.; Maitra, S. *Patterson-Wiedemann type functions on* 21 *variables with Nonlinearity greater than Bent Concatenation bound*. Cryptology ePrint Archive: Report 2015/1036 (received 26 Oct 2015, last revised 28 Oct 2015). Available at: ia.cr/2015/1036

[36] Kavut, S.; Yücel, M. D. 9*–variable Boolean functions with nonlinearity* 242 *in the generalized rotation symmetric class*. Inform. and Comput. 208 (2010), no. 4, 341–350.

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

[38] Lachaud, G.; Wolfmann, J. *Sommes de Kloosterman, courbes elliptiques et codes cycliques en caracteristique* 2. C.R. Acad. Sci. Paris (I) 305 (1987) 881–883.

[39] Lachaud, G.; Wolfmann, J. *The weights of the orthogonals of the extended quadratic binary Goppa codes*. IEEE Trans. Inform. Theory 36 (1990), no. 3, 686–692.

[40] Langevin, P.; Leander, G. *Monomial bent functions and Stickelberger's theorem*. Finite Fields Appl. 14 (2008), no. 3, 727–742.

[41] Lapierre, L., Lisoněk, P. *On Vectorial Bent Functions with Dillon-type Exponents*. Accepted for presentation at the 2016 IEEE International Symposium on Information Theory (July 10 – 15, Barcelona, Spain), and for publication in the proceedings. Five pages.

[42] Leander, N. G. *Monomial bent functions*. IEEE Trans. Inform. Theory 52 (2006), no. 2, 738 – 743.

[43] Lidl, R.; Mullen, G. L.; Turnwald, G. (1993) *Dickson polynomials*. Pitman Monographs and Surveys in Pure and Applied Mathematics 65. Longman Scientific & Technical, Harlow; co-published in the United States with John Wiley & Sons, Inc., New York.

[44] Lidl, R.; Niederreiter, H. *Finite fields*. With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. xiv+755 pp. ISBN: 0–521–39231–4

[45] Lisoněk, P. *Highly nonlinear functions on finite fields.* The Fields–TIMC Workshop on Functions and Geometries over Finite Fields. July 8–10, 2015. Carleton University, Ottawa, Ontario.

[46] Lisoněk, P.; *On the connection between Kloosterman sums and elliptic curves.* Sequences and their applications–SETA 2008, 182–187, Lecture Notes in Comput. Sci., 5203, Springer, Berlin, 2008.

[47] Lisoněk, P.; *An efficient characterization of a family of hyperbent functions* IEEE Transactions on Information Theory 57 (2011), 6010–6014.

[48] Lisoněk, P.; Moisio, M. *On zeros of Kloosterman sums.* Designs, Codes and Cryptography 59 (2011), 223-230.

[49] Matsui, M. *Linear cryptanalysis method for DES cipher.* in Advances in Cryptology–EUROCRYPT (Lecture Notes in Computer Science), vol. 765. Berlin, Germany: Springer–Verlag, 1993, pp. 386–397.

[50] Meier, W.; Staffelbach, O. *Nonlinearity criteria for cryptographic functions.* Advances in cryptology–EUROCRYPT '89 (Houthalen, 1989), 549–562, Lecture Notes in Comput. Sci., 434, Springer, Berlin, 1990.

[51] Mesnager, S. *A new class of bent and hyperbent Boolean functions in polynomial forms.* Des. Codes Cryptogr. 59 (2011), no. 1–3, 265–279.

[52] Moloney, R. *Divisibility properties of Kloosterman sums and division polynomials for Edwards curves.* Ph.D. dissertation, University College, Dublin, Ireland, 2011.

[53] Mullen, G. L.; Panario, D. *Handbook of Finite Fields.* Discrete Mathematics and Its Applications. CRC Press, 2013.

[54] Muratović-Ribić, A.; Pasalic, E.; Bajrić, S. *Vectorial bent functions from multiple terms trace functions.* IEEE Trans. Inform. Theory 60 (2014), no. 2, 1337 – 1347.

[55] Muratović-Ribić, A.; Pasalic, E.; Ribić, S. *Vectorial hyperbent trace functions from the PS_{ap} class – their exact number and specification.* IEEE Trans. Inform. Theory 60 (2014), no. 7, 4408 – 4413.

[56] Nyberg, K.; *Perfect non-linear S-boxes.* Advances in Cryptology – EUROCRYPT'91, pages 378 – 386. Springer, 1991.

[57] Pasalic, E. *A note on nonexistence of vectorial bent functions with binomial trace representation in the PS^- class.* Inform. Process. Lett. 115 (2015), no. 2, 139 – 140.

[58] Pasalic, E. *Corrigendum to "A note on nonexistence of vectorial bent functions with binomial trace representation in the PS^- class".* [Information Processing Letters 115 (2) (2015) 139 – 140]. Inform. Process. Lett. 115 (2015), no. 4, 520.

[59] Patterson, N. J.; Wiedemann, D. H. *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.

[60] Pott, A.; Pasalic, E.; Muratović-Ribić, A.; Bajrić, S. *Vectorial quadratic bent functions as a product of two linearized polynomials*. Proceedings of the Encompassing Computer Science Workshop 2015, UP FAMNIT, Koper, Slovenia

[61] Rothaus, O. S. *On "bent" functions*. J. Combinatorial Theory Ser. A 20 (1976), no. 3, 300 – 305.

[62] Shparlinski, I. *On the values of Kloosterman sums*. IEEE Trans. Inform. Theory 55 (2009), no. 6, 2599–2601.

[63] Stinson, D. R. *Cryptography : Theory and Practice*. Boca Raton : Chapman & Hall/CRC, 2006. 3rd ed.

[64] Tang, C.; Qi, Y.; Xu, M.. *Multiple output bent functions characterized by families of bent functions*. Journal of Cryptologic Research, 1(4):321–326, 2014

[65] Tokareva, N. *Bent Functions: Results and Applications to Cryptography* (Foreword by Bart Preneel). Elsevier/Academic Press, Amsterdam, 2015.

[66] Stanley, R. P. *Enumerative combinatorics*. Volume 1. Second edition. Cambridge Studies in Advanced Mathematics, 49. Cambridge University Press, Cambridge, 2012.

[67] van der Geer, G.; van der Vlugt, M. *Kloosterman sums and the p-torsion of certain Jacobians*. Math. Ann., vol. 290, no. 3, pp. 549–563, 1991.

[68] Wagstaff, S. *Divisors of Mersenne numbers*. Math. Comp., 40:161 (January 1983) 385–397.

[69] Webster, A. F.; Tavares, Stafford E. *On the design of S-boxes*. Advances in Cryptology – Crypto '85. Lecture Notes in Computer Science 218. New York, NY: Springer–Verlag New York, Inc. pp. 523–534.

[70] Xu, Y.; Wu, C. *On the Existence and Constructions of Vectorial Boolean Bent Functions*. Cryptology ePrint Archive: Report 2015/077 (received 2 Feb 2015, last revised 23 Aug 2015). Available at: ia.cr/2015/077

[71] Youssef, A. M.; Gong, G. *Hyperbent functions*. Advances in cryptology–EUROCRYPT 2001 (Innsbruck), 406–419, Lecture Notes in Comput. Sci., 2045, Springer, Berlin, 2001.

Appendix A

Kloosterman Sums and Elliptic Curves

The evaluation of Kloosterman sums over $\mathbb{F}_{2^n}$ by definition is computationally expensive, requiring time exponential in n [4], [46]. Fortunately, Lachaud and Wolfmann showed that there is an intimate connection between the value of the Kloosterman sum over $\mathbb{F}_{2^n}$ and the number of $\mathbb{F}_{2^n}$–rational points on a special elliptic curve defined over $\mathbb{F}_{2^n}$ [38]. This allows us two things: first, that we may take advantage of the fast point-counting algorithms that exist for elliptic curves (this will be used extensively in Appendix B); second, that we may bound the value of Kloosterman sums using the famous *Hasse interval*.

A.1 Elliptic Curves Over $GF(2^n)$

We give a very brief introduction to ellitpic curves over $\mathbb{F}_{2^n}$. The primary reference for the following material is [7, Chapter III].

Definition A.1.1 (Elliptic Curve Over $\mathbb{F}_{2^n}$)**.** *An* elliptic curve over $\mathbb{F}_{2^n}$ *is defined by an equation of the form*

$$\mathcal{E} := y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with } a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_{2^n} \tag{A.1}$$

where the coefficients a_1, a_2, a_3, a_4, a_6 must satisfy

$$\Delta := a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3 \neq 0.$$

The quantity Δ is called the discriminant.

Definition A.1.2 ($\mathbb{F}_{2^n}$-Rational Points)**.** *Let $\mathcal{E}$ be an elliptic curve of the form* (A.1)*. The* $\mathbb{F}_{2^n}$–rational points *on $\mathcal{E}$ are the points $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying* (A.1)*, along with a point "at infinity", denoted by $\mathcal{O}$.*

Theorem A.1.3 (Hasse interval)**.** [7, Theorem III.3] *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{F}_{2^n}$. Then the number of $\mathbb{F}_{2^n}$–rational points on $\mathcal{E}$ lies in the interval*

$$[2^n + 1 - 2^{n/2+1}, 2^n + 1 + 2^{n/2+1}].$$

Definition A.1.4 (Isomorphism of Elliptic Curves)**.** *Let $\mathcal{E}$ and $\mathcal{E}'$ be elliptic curves of the form* (A.1) *in the variables x, y and x', y', respectively. The two curves are said to be* isomorphic over $\mathbb{F}_{2^n}$ *if there exist constants $r, s, t \in \mathbb{F}_{2^n}$ and $u \in \mathbb{F}_{2^n}^*$ such that the change of variables*

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t \tag{A.2}$$

transforms $\mathcal{E}$ into $\mathcal{E}'$.

A.2 The Relationship Between Kloosterman Sums Over $GF(2^n)$ and Certain Elliptic Curves

We present the work of Lachaud and Wolfmann [39], connecting the value of the Kloosterman sum at the point $a \in \mathbb{F}_{2^n}$ to the number of $\mathbb{F}_{2^n}$-rational points on a certain elliptic curve parametrized by a.

Lemma A.2.1 (Lachaud, Wolfmann [39])**.** *Let $a \in \mathbb{F}_{2^n}^*$, and let $\mathcal{E}(a)$ be the elliptic curve over $\mathbb{F}_{2^n}$ defined by*

$$\mathcal{E}(a) := y^2 + xy = x^3 + a.$$

Then $\mathcal{E}(a)$ is isomorphic over $\mathbb{F}_{2^n}$ to the curve

$$\mathcal{E}'(a) := y^2 + y = \frac{1}{x} + ax.$$

In particular, the two curves contain the same number of $\mathbb{F}_{2^n}$-rational points.

Proof. First we apply the substitutions $x = \frac{x'}{z'}$, $y = \frac{y'}{z'}$ to $\mathcal{E}(a)$:

$$y^2 + xy = x^3 + a \to \left(\frac{y'}{z'}\right)^2 + \left(\frac{x'}{z'}\right)\left(\frac{y'}{z'}\right) = \left(\frac{x'}{z'}\right)^3 + a. \tag{A.3}$$

Deleting the prime figure and re-arranging yields

$$y^2z + xyz = x^3 + az^3. \tag{A.4}$$

Let $a' \in \mathbb{F}_{2^n}$ be such that $(a')^2 = a$. We successively apply the substitutions $y = y' + a'z$, $x = 1$, and $z = x'$ to (A.4) to obtain

$$(y' + a'x')^2x' + (y' + a'x')x' = 1 + a(x')^3. \tag{A.5}$$

Upon simplification and subsequent deletion of the prime figure we obtain

$$xy^2 + xy + ax^2 = 1. \tag{A.6}$$

Adding ax^2 to both sides of (A.6) and dividing through by x gives the result (note that $x = 0$ does not yield solutions to (A.6)). □

Theorem A.2.2 (Lachaud, Wolfmann [39])**.** *Let $a \in \mathbb{F}_{2^n}^*$, and let $\mathcal{E}(a)$ be the elliptic curve over $\mathbb{F}_{2^n}$ defined by*

$$\mathcal{E}(a) := y^2 + xy = x^3 + a.$$

Let $\#\mathcal{E}(a)$ denote the number of $\mathbb{F}_{2^n}$–rational points on $\mathcal{E}(a)$. Then

$$\#\mathcal{E}(a) = \mathcal{K}_{2^n}(a) + 2^n.$$

Proof. By Lemma A.2.1, we may transform $\mathcal{E}(a)$ into the curve

$$\mathcal{E}'(a) := y^2 + y = \frac{1}{x} + ax$$

for which we have $\#\mathcal{E}'(a) = \#\mathcal{E}(a)$.

For $i \in \mathbb{F}_2$, let $N_i(a)$ denote the number of solutions in $\mathbb{F}_{2^n}$ to the equation $Tr(x^{-1}+ax) = i$. Setting $Tr(0^{-1}) = Tr(0^{2^n-2}) = 0$, we have the following relations:

$$N_0(a) + N_1(a) = 2^n \tag{A.7}$$
$$N_0(a) - N_1(a) = \mathcal{K}_{2^n}(a). \tag{A.8}$$

Adding (A.7) and (A.8) yields

$$2N_0(a) = \mathcal{K}_{2^n}(a) + 2^n. \tag{A.9}$$

We complete the proof by recalling the additive Hilbert 90 (Theorem 1.3.10), which states that the elements having absolute trace equal to zero are precisely the elements of the form $t^2 + t$, $t \in \mathbb{F}_{2^n}$, and furthermore that the correspondence is (respectively) 1-to-2. □

Appendix B

Computer Programs

All computations were carried out on an Intel Core i7 six core CPU 3930K at 4.2 GHz, with 64 GB RAM.

B.1 Finding New Dillon-type Vectorial Monomial Bent Functions

Magma code pertaining to Theorem 3.1.3.

```
Z := Integers();

val2:=function(r)
   if r eq 0 then
      return -1;
   end if;
   res:=0;
   rr:=r;
   while (rr mod 2) eq 0 do
      res:=res+1;
      rr:=Z!(rr/2);
   end while;
   return res;
end function;

for m := 6 to 42 do

   printf"\n\n";
   printf"m = %o", m;

   F := GF(2^m);
   al := PrimitiveElement(F);

   K := function(a) //Kloosterman sum
      if a eq 0 then
         return 0;
```

```
   end if;
   return #EllipticCurve([ 1, 0, 0, 0, a ]) - 2^m;
end function;

k := 1;

repeat

   k := k+1;
   while 0 ne (2*m) mod k do k := k+1; end while;

   s := Z!((2^k-1)/GreatestCommonDivisor(2^k-1,2^m+1));
   t := Z!((2^(2*m)-1)/(2^k-1));

   r := -1;

   repeat

      r := r+1;

      U := {1}; //set of solutions, 1 is always a solution corresponding to
          i = 0

      for i := 1 to s-1 do

      u := 0;

      repeat

      u := u+1;
      C := i*t-r*(2^u-2);

      until (0 eq C mod (2^m-1)) or (u eq m-1); //find a solution for the
          i-th congruence, or exhaust possible exponents u

      if (0 eq C mod (2^m-1)) then
         U := Include(U,u);
      elif (u eq m-1) then
         break; //break i if i-th congruence does not have a solution
      end if;

      end for;

      if #U eq s and K(al^r) eq 0 then

         printf"\n\n";
         printf"2m = %o \n k = %o \n r = %o \n K(al^r) = %o \n val2(K(al^r))
             = %o \n U = %o",
         2*m, k, r, K(al^r), val2(K(al^r)), U;

         if 0 eq m mod 2 then
            printf"\n NEW BENT FUNCTION";
         elif 1 eq m mod 2 then
```

```
            printf"\n BENT FUNCTION";
          end if;

        end if;

      until r eq 2^m-2; //r

   until k eq m; //k

end for; //m
```

B.2 Computations Pertaining to Theorem 4.2.1

```
Pseudocode:

for even k in [2,30] do
   for P in AllIrreduciblePolynomials(GF(2),k) do
      Q := P(x^3);
      a := root of Q;
      if Ke(a) eq 0 then return Q ; end if;
   end for;
end for;
```

B.3 Dillon-type Binomial Bent Functions from $GF(2^{4m})$ to $GF(4)$

Magma code pertaining to subsection 3.2.1.

```
Z := Integers();
R := RealField(4);

Trials := 10;

for m := 4 to 100 by 2 do

   printf"\n\n m = %o \n",m;

   F := GF(2^m);
   F4 := sub<F|2>;
   al := PrimitiveElement(F);
   w := PrimitiveElement(F4);
   assert w^2+w+1 eq 0;

   RR<x> := PolynomialRing(F);

   TotalSamples := 0;
   TotalCG19time := 0;
   TotalPL10time := 0;
```

```
    for t := 1 to Trials do

       F4Bent := false;

       Samples := 0;

       repeat

          Samples := Samples + 1;

          b1 := Random(F); while b1 eq 0 do b1 := Random(F); end while;
          b3 := Random(F); while b3 eq 0 do b3 := Random(F); end while;

          i := -1;

          repeat

             i := i + 1;

             GS := {*Trace(w^i*((b1+b3)*a+b3*a^3)): a in F | a ne 0*};
             Gsum := 2^m-1 - 2*Multiplicity(GS,1);
             HS := {*Trace(1/a + w^i*((b1+b3)*a+b3*a^3)): a in F | a ne 0*};
             Hsum := 2^m-1 - 2*Multiplicity(HS,1);

          until i eq 2 or Gsum ne Hsum;

          F4Bent := i eq 2 and Gsum eq Hsum;


       until F4Bent;

       TotalSamples := TotalSamples + Samples;

       print b1, b3;

    end for;

    printf"avg. # of samples required over over %o trials: %o \n",
    Trials,R!(TotalSamples/Trials);

 end for;
```

Sample output:

```
m = 4
F.1^4 F.1^2
F.1^2 F.1^4
F.1^8 F.1
F.1^12 F.1^14
F.1^6 F.1^13
F.1^13 F.1^6
F.1^2 F.1^4
F.1^8 F.1
```

```
F.1 F.1^8
F.1^4 F.1^8
avg. # of samples required over over 10 trials: 17.40


m = 6
F.1^54 F.1^2
F.1^36 F.1^18
F.1^36 F.1^18
F.1^27 F.1^8
F.1^33 F.1^42
F.1^54 F.1^2
F.1^27 1
F.1^6 F.1^42
F.1^12 F.1^23
F.1^12 F.1^21
avg. # of samples required over over 10 trials: 78.50


m = 8
F.1^78 F.1^190
F.1^134 F.1^141
F.1^90 F.1^62
F.1^227 F.1^165
F.1^35 F.1^150
F.1^248 F.1^105
F.1^67 F.1^198
F.1^26 F.1^54
F.1^124 F.1^180
F.1^240 F.1^215
avg. # of samples required over over 10 trials: 445.9


m = 10
F.1^106 F.1^369
F.1^27 F.1^912
F.1^864 F.1^39
F.1^728 F.1^497
F.1^432 F.1^531
F.1^395 F.1^119
F.1^525 F.1^139
F.1^387 F.1^156
F.1^525 F.1^624
F.1^387 F.1^802
avg. # of samples required over over 10 trials: 5060.
```

B.4 In Support of a Conjecture On the Divisibility of Kloosterman Sums

Magma code pertaining to Conjecture 4.4.7.

```
Z := Integers();

val2:=function(r)
   if r eq 0 then
      return -1;
   end if;
   res:=0;
   rr:=r;
   while (rr mod 2) eq 0 do
      res:=res+1;
      rr:=Z!(rr/2);
   end while;
   return res;
end function;

for k := 2 to 10 do

   printf"\n\n k = %o",k;

   m := k*(2^k-1);

   F := GF(2^m);
   al := PrimitiveElement(F);

   Ke := function(a)
      assert a in F;
      if a eq 0 then return 0; end if;
      return #EllipticCurve([ 1, 0, 0, 0, a ]) - 2^m;
   end function;

   t := Z!((2^m-1)/(2^k-1));
   s := Z!(t/(2^k-1));

   ga := al^t;
   be := al^s;

   TIMES := 5;
   TRIAL := 0;

   while TRIAL lt TIMES do

      TRIAL := TRIAL + 1;

      I := {0 .. 2^k-2};
      i := Random(I);

      c := ga^i;
      a := c*be;

      MPa := MinimalPolynomial(a);

      printf"\n TRIAL # %o \n MPa = %o \n val2(Ke(a)) = %o", TRIAL, MPa,
          val2(Ke(a));
```

```
   end while;

end for;
```

B.5 Computations Relating to an Open Problem of Charpin and Gong

Code pertaining to Open Problem 4.3.1:

```
for m := 4 to 100 do

   printf"\n\n";
   printf"m = %o",m;
   printf"\n";

   count := 0;
   F := GF(2^m);
   al := PrimitiveElement(F);
   Ff := {x: x in F | x ne 0};
   r := 1;

   repeat
      r := r+1;
   until GCD(2^r+1, 2^m-1) eq 1;

   S := [];
   i := -1;

   repeat
      i := i+1;
      j := -1;
      InS := false;

      repeat
         j := j+1;
         InS := (2^j)*i mod (2^m-1) in S;
      until InS or j eq m-1;

      if InS eq false and j eq m-1 then S := Include(S,i); end if;

   until i eq 2^(m-1)-1;

   for i := 1 to #S do
      lam :=al^S[i];
      A := {x : x in Ff | Trace(1/x) eq Trace(lam*x^(2^r+1))};
      if #A eq 2^(m-1)-1 then
         count := count + 1;
      end if;
   end for;
```

```
    print count;

end for;
```

Output (up to $m = 17$ only):

```
m = 4
2

m = 5
3

m = 6
5

m = 7
5

m = 8
2

m = 9
9

m = 10
15

m = 11
13

m = 12
20

m = 13
14

m = 14
44

m = 15
35

m = 16
16

m = 17
72
```

This counts the elements $\lambda \in \mathbb{F}_{2^m}$ such that the function (4.12) is bent, and the count is taken up to equivalence under the mapping $x \mapsto x^2$.

B.6 Computations Relating to New Results on the Divisibility of Kloosterman Sums

B.6.1 A Demonstration of Theorem 3.3.6

```
> F := GF(2^24);
> alpha := PrimitiveElement(F);
> CharacteristicPolynomial(alpha);
$.1^24 + $.1^16 + $.1^15 + $.1^14 + $.1^13 + $.1^10 + $.1^9 + $.1^7 + $.1^5 +
$.1^3 + 1 //irreducible polynomial used in this construction of GF(2^24)
>
> Z := Integers();
> t := Z!((2^24-1)/(2^8-1));
>
> gamma := alpha^t;
> Order(gamma) eq 2^8-1; //gamma is a primitive element of GF(2^8)
true
>
> beta := alpha^(Z!(t/3));
> beta^3 eq gamma;
true
>
> a := beta*gamma^3;
> CharacteristicPolynomial(a);
$.1^24 + $.1^21 + $.1^18 + $.1^15 + $.1^12 + $.1^3 + 1 //all exponents are
    divisible by 3
>
> Ke := function(x) //Kloosterman sum over GF(2^24)
function>     assert x in F;
function>     if x eq 0 then return 0; end if;
function>     return #EllipticCurve([ 1, 0, 0, 0, x ]) - 2^24;
function> end function;
>
> Ke(a);
-3264 //the Kloosterman sum at a is divisible by 64, but not by 128
```

B.6.2 A Demonstration of Theorem 3.3.9

```
> F := GF(2^42);
> alpha := PrimitiveElement(F);
> CharacteristicPolynomial(alpha);
$.1^42 + $.1^30 + $.1^26 + $.1^25 + $.1^24 + $.1^20 + $.1^18 + $.1^12 + $.1^11
    +
$.1^9 + $.1^6 + $.1^5 + $.1^2 + $.1 + 1 //irreducible polynomial used in this
    construction of GF(2^42)
>
> Z := Integers();
> t := Z!((2^42-1)/(2^6-1));
>
> gamma := alpha^t;
> Order(gamma) eq 2^6-1; //gamma is a primitive element of GF(2^6)
```

```
true
>
> beta := alpha^(Z!(t/7));
> beta^7 eq gamma;
true
>
> a := beta*gamma^5;
> CharacteristicPolynomial(a);
$.1^42 + $.1^14 + 1 //all exponents are divisible by 7
>
> Ke := function(x) //Kloosterman sum over GF(2^42)
function>    assert x in F;
function>    if x eq 0 then return 0; end if;
function>    return #EllipticCurve([ 1, 0, 0, 0, x ]) - 2^42;
function> end function;
>
> Ke(a);
-4096 //the Kloosterman sum is divisible by 256
```

Code pertaining to the remarks at the end of Example 3.3.10:

```
Z := Integers();

val2:=function(r)
   if r eq 0 then
      return -1;
   end if;
   res:=0;
   rr:=r;
   while (rr mod 2) eq 0 do
      res:=res+1;
      rr:=Z!(rr/2);
   end while;
   return res;
end function;

for n := 1 to 10 do

   k := 3*n;

   printf"\n\n";
   printf"k = %o \n",k;

   F := GF(2^(7*k));
   alpha := PrimitiveElement(F);
   //CharacteristicPolynomial(alpha);

   t := Z!((2^(7*k)-1)/(2^k-1));

   gamma := alpha^t;
   //Order(gamma) eq 2^k-1; //gamma is a primitive element of GF(2^k)

   beta := alpha^(Z!(t/7));
```

```
   //beta^7 eq gamma;

   Ke := function(x) //Kloosterman sum over GF(2^(7*k))
      assert x in F;
      if x eq 0 then return 0; end if;
      return #EllipticCurve([ 1, 0, 0, 0, x ]) - 2^(7*k);
   end function;

   max := 7;

   for i := 1 to 2^k-2 do
      a := beta*gamma^i;
      if val2(Ke(a)) gt max then max := val2(Ke(a)); end if;
   end for;

   max;

end for;

//OUTPUT:

k = 3
11


k = 6
12


k = 9
13


k = 12
18


k = 15
24
```

B.6.3 Constructing New Examples of Dillon-type Vectorial Monomial Bent Functions

```
> Z := Integers();
> E := GF(2^12);
> omega := PrimitiveElement(E);
> CharacteristicPolynomial(omega);
$.1^12 + $.1^7 + $.1^6 + $.1^5 + $.1^3 + $.1 + 1 //irreducible polynomial used
    in this construction of GF(2^12)
>
> F := sub<E|6>;
> F;
```

```
Finite field of size 2^6
>
> alpha := PrimitiveElement(F);
> alpha eq omega^65;
true
>
> beta := alpha^7;
> gamma := alpha^21;
> Order(gamma) eq 3;
true //gamma is a primitive element of GF(4)
>
> L := {0,1,gamma,gamma^2}; //the elements of GF(4)
> A := {beta*x : x in L} join {beta^2*x : x in L}; //the union of special
    cosets
>
> Ke := function(x) //Kloosterman sum over GF(2^6)
function>     assert x in F;
function>     if a eq 0 then return 0; end if;
function>     return #EllipticCurve([ 1, 0, 0, 0, x ]) - 2^6;
function> end function;
>
> {Ke(a): a in A diff {0}};
{ 0 } //every element of A is a Kloosterman zero in GF(2^6), hence
    Tr^{12}_1(ax^{63}) is bent for all non-zero a in A
>
> {x^65 : x in A diff {0}} subset A;
true //the norm from GF(2^12) to GF(2^6) maps A into itself, hence
    Tr^{12}_2(ax^{63}) is bent for all non-zero a in A
>
> t := Z!((2^12-1)/(2^4-1));
> delta := omega^t;
> Order(delta) eq 15;
true //delta is a primitive element of GF(16)
>
> B := {delta^i*a : i in [0 .. 14] | a in A};
> {x^65: x in B diff {0}} subset A;
true //the norm from GF(2^12) to GF(2^6) maps B into A, hence
    Tr^{12}_4(ax^{63}) is bent for all non-zero a in A
```

B.7 In Support of a Conjecture on Function Families of Maximum Size

```
Z:= Integers();

for n:= 4 to 16 do

   m:= Z!(n/2);

   q:= 2^n;
   F:= GF(q);
```

```
F2:= sub<F | 1>;
assert #F2 eq 2;
Fm:= sub<F | m>;
assert #Fm eq 2^m;


FL:= {x : x in F};
FK:= {x : x in Fm};
FP:= {x: x in FL | not(x in FK)};
assert #FP eq 2^n - 2^m;


//Fast Walsh Transform

W:=function(f)

   al:=PrimitiveElement(F);

   c := [ 0 : j in [ 1 .. n ] ];
   L := [ 0 : j in [ 1 .. q ] ];

   for i := 1 to q do
      x:=&+[ c[j+1]*al^j : j in [ 0 .. n-1 ] ];
      L[i]:=(-1)^(Z!(f(x)));

      if i lt q then
         j:=1;
         while c[j] eq 1 do j:=j+1; end while;
         c[j]:=1;
         for jj:=1 to j-1 do
            c[jj]:=0;
         end for;
      end if;

   end for;


   for i := 0 to n-1 do
      tmi:=2^(n-i-1);

      for b := 0 to 2^i-1 do
         bo:=b*2^(n-i); // block offset

         for j := 0 to tmi-1 do

            // print bo+j + 1 , bo+j+tmi + 1 ;

            pl := L[ bo+j + 1 ] + L[ bo+j+tmi + 1 ] ;
            mi := L[ bo+j + 1 ] - L[ bo+j+tmi + 1 ] ;
            L[ bo+j + 1 ] := pl;
            L[ bo+j+tmi + 1 ] := mi;
         end for;
```

```
        end for;

      end for;

      return {* L[t] : t in [ 1 .. q ] *};
   end function;

   //Fast Walsh Transform

   //Bentness Test

   for i:= 0 to m-1 do

      BentCount:= 0;

      for lam in FP do

         f := function(x)
            return Trace(lam*(x^(2^i+1)+x^(2^(i+m)+1)));
         end function;

         if { Abs(z) : z in W(f) } eq { 2^m } then
            BentCount := BentCount + 1;
         end if;

      end for;

      if BentCount eq 2^n - 2^m then print 2^i+1, 2^(i+m)+1, i, i+m;
      end if;

   end for;

   //Bentness Test Complete

end for;
```

Appendix C

Kloosterman Sums Modulo 256

Due to its length, the full statement of Theorem 3.3.2 has been deferred to this appendix. Once we have given the full statement of the theorem we will use it as a reference for a slightly more detailed proof of Theorem 3.3.9.

C.1 The Full Statement of the Congruence Modulo 256

Let $n \geq 8$ and let $a \in \mathbb{F}_{2^n}^*$. The following result gives the value of $\mathcal{K}_{2^n}(a) \mod 256$ in terms of the coefficients of the characteristic polynomial of a over $\mathbb{F}_2$

$$\prod_{i=0}^{n-1} \left(x - a^{2^i}\right) = x^n + e_1 x^{n-1} + \ldots + e_{n-1}x + e_n. \tag{C.1}$$

Theorem C.1.1 (Göloğlu *et al.* [30], [52])**.** *Let $n \geq 8$ and let $a \in \mathbb{F}_{2^n}^*$. Let $e_1, \ldots, e_{32}$ be the coefficients of the characteristic polynomial of a over $\mathbb{F}_2$ as described in* (C.1)*. Then $e_1, \ldots, e_{32}$ are related to $\mathcal{K}_{2^n}(a)$ via the congruence*

$$\begin{aligned}
&\mathcal{K}_{2^n}(a) \equiv \\
&16e_4 + 32(e_1e_7 + e_2e_6 + e_8) + 64(e_3e_4 + e_1e_{11} + e_1e_2e_6 + e_{16} \\
&+ e_1e_4e_6 + e_5e_6 + e_1e_6e_8 + e_2e_{14} + e_2e_3e_9 + e_1e_{13} + e_2e_4e_6 \\
&+ e_2e_8 + e_1e_{15} + e_4e_{12} + e_1e_2e_3e_5 + e_2e_4e_5 + e_3e_{10} + e_1e_4e_7 \\
&+ e_1e_2e_5 + e_1e_2e_{12}) + 92e_1 + 96(e_1e_5 + e_1e_4 + e_1e_6) \\
&+ 128(e_1e_2e_5e_{19} + e_1e_2e_6e_7 + e_1e_2e_6e_8 + e_1e_2e_6e_{11} + e_1e_2e_6e_{16} + e_1e_2e_6e_{18} \\
&+ e_1e_2e_7e_9 + e_1e_2e_7e_{12} + e_1e_2e_7e_{13} + e_1e_2e_7e_{15} + e_1e_2e_7e_{17} + e_1e_2e_8e_9 \\
&+ e_1e_2e_8e_{10} + e_1e_2e_8e_{12} + e_1e_2e_8e_{14} + e_1e_2e_8e_{16} + e_1e_2e_9e_{11} + e_1e_2e_9e_{13} \\
&+ e_1e_2e_9e_{15} + e_1e_2e_{10}e_{12} + e_1e_2e_{10}e_{14} + e_{14}e_{18} + e_1e_2e_{11}e_{13} + e_{13}e_{19} \\
&+ e_1e_2e_{14} + e_1e_2e_{15} + e_1e_2e_{16} + e_1e_2e_{20} + e_1e_2e_{21} + e_1e_2e_{22} \\
&+ e_1e_2e_{26} + e_1e_2e_{27} + e_1e_2e_{28} + e_{12}e_{20} + e_1e_3e_4e_6 + e_1e_3e_4e_{10} \\
&+ e_1e_3e_4e_{13} + e_1e_3e_4e_{17} + e_1e_3e_4e_{18} + e_1e_3e_4 + e_1e_3e_5e_6 + e_1e_3e_5e_7
\end{aligned}$$

$$+ e_1e_3e_5e_8 + e_1e_3e_5e_{10} + e_1e_3e_5e_{11} + e_1e_3e_5e_{15} + e_1e_3e_5e_{17} + e_1e_3e_6e_7$$
$$+ e_1e_3e_6e_8 + e_1e_3e_6e_9 + e_1e_3e_6e_{13} + e_1e_3e_6e_{16} + e_1e_3e_7e_9 + e_1e_3e_7e_{11}$$
$$+ e_1e_3e_7e_{15} + e_{11}e_{21} + e_1e_3e_8e_9 + e_1e_3e_8e_{14} + e_1e_3e_9e_{13} + e_1e_3e_{10}e_{12}$$
$$+ e_1e_3e_{10} + e_{10}e_{22} + e_1e_3e_{12} + e_1e_3e_{13} + e_1e_3e_{15} + e_1e_3e_{17}$$
$$+ e_1e_3e_{19} + e_1e_3e_{22} + e_1e_3e_{23} + e_1e_3e_{27} + e_{10}e_{12} + e_1e_4e_5e_6$$
$$+ e_1e_4e_5e_7 + e_1e_4e_5e_9 + e_1e_4e_5e_{10} + e_1e_4e_5e_{11} + e_1e_4e_5e_{14} + e_1e_4e_5e_{15}$$
$$+ e_1e_4e_5 + e_1e_4e_6e_7 + e_1e_4e_6e_9 + e_1e_4e_6e_{10} + e_1e_4e_6e_{12} + e_1e_4e_6e_{14}$$
$$+ e_1e_4e_7e_9 + e_1e_4e_7e_{10} + e_1e_4e_7e_{13} + e_1e_4e_8e_{12} + e_{10}e_{11} + e_1e_4e_9e_{11}$$
$$+ e_9e_{23} + e_1e_4e_{13} + e_1e_4e_{16} + e_1e_4e_{18} + e_1e_4e_{19} + e_1e_4e_{22}$$
$$+ e_1e_4e_{23} + e_1e_4e_{24} + e_1e_4e_{26} + e_1e_5e_6e_7 + e_1e_5e_6e_8 + e_1e_5e_6e_{11}$$
$$+ e_1e_5e_6e_{12} + e_1e_5e_6 + e_1e_5e_7e_8 + e_1e_5e_7e_9 + e_1e_5e_7e_{11} + e_9e_{14}$$
$$+ e_1e_5e_8e_{10} + e_1e_5e_{10} + e_1e_5e_{11} + e_1e_5e_{14} + e_1e_5e_{15} + e_1e_5e_{18}$$
$$+ e_1e_5e_{19} + e_1e_5e_{23} + e_1e_5e_{25} + e_1e_6e_7e_8 + e_1e_6e_7e_9 + e_1e_6e_7$$
$$+ e_1e_6e_{14} + e_1e_6e_{15} + e_1e_6e_{18} + e_1e_6e_{19} + e_1e_6e_{20} + e_1e_6e_{22}$$
$$+ e_1e_6e_{24} + e_1e_7e_{11} + e_1e_7e_{12} + e_1e_7e_{14} + e_1e_7e_{15} + e_1e_7e_{19}$$
$$+ e_1e_7e_{21} + e_1e_7e_{23} + e_1e_8e_{11} + e_1e_8e_{14} + e_1e_8e_{15} + e_1e_8e_{16}$$
$$+ e_1e_8e_{18} + e_1e_8e_{20} + e_1e_8e_{22} + e_8e_{24} + e_1e_9e_{10} + e_1e_9e_{15}$$
$$+ e_1e_9e_{17} + e_1e_9e_{19} + e_1e_9e_{21} + e_8e_{16} + e_1e_{10}e_{11} + e_1e_{10}e_{12}$$
$$+ e_1e_{10}e_{14} + e_1e_{10}e_{16} + e_1e_{10}e_{18} + e_1e_{10}e_{20} + e_8e_{12} + e_1e_{11}e_{13}$$
$$+ e_1e_{11}e_{15} + e_1e_{11}e_{17} + e_1e_{11}e_{19} + e_1e_{12}e_{14} + e_1e_{12}e_{16} + e_1e_{12}e_{18}$$
$$+ e_7e_{25} + e_1e_{13}e_{15} + e_1e_{13}e_{17} + e_1e_{14}e_{16} + e_7e_{18} + e_1e_{16}$$
$$+ e_1e_{17} + e_1e_{18} + e_1e_{19} + e_1e_{20} + e_1e_{21} + e_1e_{22}$$
$$+ e_1e_{23} + e_1e_{24} + e_1e_{25} + e_1e_{26} + e_1e_{27} + e_1e_{28}$$
$$+ e_1e_{29} + e_1e_{30} + e_1e_{31} + e_2e_3e_4e_6 + e_1e_2e_3e_4e_5 + e_2e_3e_4e_9$$
$$+ e_2e_3e_4e_{10} + e_2e_3e_4e_{12} + e_2e_3e_4e_{13} + e_2e_3e_4e_{14} + e_2e_3e_5e_6 + e_2e_3e_5e_{13}$$
$$+ e_7e_{11} + e_2e_3e_6e_9 + e_2e_3e_6e_{10} + e_2e_3e_6e_{12} + e_2e_3e_7e_9 + e_2e_3e_7e_{11}$$
$$+ e_2e_3e_8e_{10} + e_7e_8e_{10} + e_2e_3e_{10} + e_2e_3e_{11} + e_2e_3e_{12} + e_2e_3e_{14}$$
$$+ e_2e_3e_{15} + e_2e_3e_{17} + e_2e_3e_{21} + e_2e_3e_{24} + e_2e_3e_{25} + e_7e_8e_9$$
$$+ e_2e_4e_5e_7 + e_2e_4e_5e_{10} + e_2e_4e_5e_{11} + e_2e_4e_6e_7 + e_2e_4e_6e_8 + e_2e_4e_6e_{10}$$
$$+ e_2e_4e_7e_9 + e_2e_4e_7 + e_6 + e_2e_4e_9 + e_2e_4e_{10} + e_2e_4e_{12}$$
$$+ e_2e_4e_{13} + e_2e_4e_{20} + e_2e_4e_{22} + e_2e_4e_{24} + e_6e_{26} + e_2e_5e_6e_7$$
$$+ e_2e_5e_6e_8 + e_6e_{20} + e_2e_5e_8 + e_2e_5e_{10} + e_2e_5e_{11} + e_2e_5e_{12}$$
$$+ e_2e_5e_{14} + e_2e_5e_{15} + e_2e_5e_{19} + e_2e_5e_{20} + e_2e_5e_{23} + e_2e_6e_9 + e_2e_6e_{14}$$
$$+ e_2e_6e_{22} + e_2e_7e_8 + e_2e_7e_9 + e_2e_7e_{10} + e_2e_7e_{13} + e_2e_7e_{16} + e_2e_7e_{17}$$
$$+ e_2e_7e_{21} + e_6e_{14} + e_2e_8e_{11} + e_2e_8e_{12} + e_2e_8e_{14} + e_2e_8e_{16} + e_2e_8e_{20} + e_2e_9e_{11}$$
$$+ e_2e_9e_{12} + e_2e_9e_{15} + e_2e_9e_{19} + e_2e_{10}e_{14} + e_2e_{10}e_{18} + e_6e_{13} + e_2e_{11}e_{13} + e_2e_{11}e_{17}$$
$$+ e_2e_{11} + e_2e_{12}e_{16} + e_6e_9e_{11} + e_2e_{13}e_{15} + e_2e_{15} + e_2e_{16} + e_2e_{18} + e_2e_{20}$$
$$+ e_2e_{22} + e_2e_{24} + e_2e_{26} + e_2e_{28} + e_2e_{30} + e_6e_8 + e_3e_4e_5e_6 + e_3e_4e_5e_7$$
$$+ e_6e_8e_{12} + e_6e_8e_{10} + e_3e_4e_7 + e_3e_4e_{12} + e_3e_4e_{13} + e_3e_4e_{16} + e_3e_4e_{21} + e_3e_4e_{22}$$

$$
\begin{aligned}
&+ e_3e_5e_6 + e_3e_5e_7 + e_3e_5e_8 + e_3e_5e_{10} + e_3e_5e_{12} + e_3e_5e_{15} + e_3e_5e_{19} + e_3e_5e_{21}\\
&+ e_6e_8e_9 + e_3e_6e_{14} + e_3e_6e_{17} + e_3e_6e_{20} + e_3e_7e_{11} + e_3e_7e_{13} + e_3e_7e_{15} + e_3e_7e_{19}\\
&+ e_6e_7e_{13} + e_3e_8e_{12} + e_3e_8e_{13} + e_3e_8e_{18} + e_3e_8 + e_3e_9e_{10} + e_3e_9e_{17} + e_3e_{10}e_{16}\\
&+ e_3e_{11}e_{15} + e_3e_{11} + e_3e_{12}e_{14} + e_6e_7e_{12} + e_3e_{14} + e_3e_{17} + e_3e_{20} + e_3e_{23}\\
&+ e_3e_{26} + e_3e_{29} + e_5 + e_4e_5e_6 + e_4e_5e_7 + e_4e_5e_8\\
&+ e_4e_5e_{11} + e_4e_5e_{18} + e_4e_5e_{19} + e_4e_5 + e_4e_6e_{10} + e_4e_6e_{11}\\
&+ e_4e_6e_{16} + e_4e_6e_{18} + e_5e_{27} + e_4e_7e_9 + e_4e_7e_{14} + e_4e_7e_{17}\\
&+ e_4e_7 + e_4e_8e_{10} + e_4e_8e_{12} + e_4e_8e_{16} + e_5e_{22} + e_4e_9e_{10}\\
&+ e_4e_9e_{15} + e_4e_{10}e_{14} + e_4e_{11}e_{13} + e_4e_{14} + e_4e_{16} + e_4e_{20}\\
&+ e_4e_{24} + e_4e_{28} + e_1e_2e_3e_4e_6 + e_5e_6e_{15} + e_5e_6e_{16} + e_5e_7e_{10}\\
&+ e_5e_7e_{13} + e_5e_7e_{15} + e_5e_7 + e_5e_8e_{11} + e_5e_8e_{14} + e_2e_3e_4e_8\\
&+ e_5e_9e_{13} + e_5e_9 + e_5e_{10}e_{12} + e_5e_{17} + e_5e_{12} + e_1e_2e_5e_{17}\\
&+ e_1e_2e_5e_{16} + e_1e_2e_5e_{15} + e_1e_2e_5e_{13} + e_1e_2e_5e_{12} + e_1e_2e_5e_9 + e_1e_2e_5e_8\\
&+ e_1e_2e_5e_6 + e_{15}e_{17} + e_1e_2e_4e_{20} + e_1e_2e_4e_{16} + e_1e_2e_4e_{15} + e_1e_2e_4e_{14}\\
&+ e_1e_2e_4e_{12} + e_1e_2e_4e_{10} + e_1e_2e_4e_7 + e_1e_2e_4e_5 + e_1e_2e_3e_{21} + e_1e_2e_3e_{20}\\
&+ e_1e_2e_3e_{19} + e_1e_2e_3e_{15} + e_1e_2e_3e_{12} + e_1e_2e_3e_9 + e_1e_2e_3e_7 + e_1e_2e_3e_6 + e_{32})\\
&+ 144e_1e_2 + 160e_1e_2e_3 + 168e_2 + 192(e_3 + e_3e_{13} + e_3e_7\\
&+ e_1e_2e_3e_4 + e_3e_4e_6 + e_3e_4e_5 + e_2e_{12} + e_6e_{10} + e_2e_{10}\\
&+ e_2e_7 + e_2e_5e_7 + e_2e_4e_8 + e_1e_2e_{10} + e_2e_3e_8 + e_5e_{11}\\
&+ e_2e_3e_5 + e_1e_{14} + e_1e_{12} + e_1e_{10} + e_1e_9 + e_1e_8\\
&+ e_1e_5e_9 + e_1e_5e_7 + e_1e_4e_{10} + e_1e_4e_8 + e_1e_2e_{11} + e_1e_3e_{11}\\
&+ e_1e_3e_7 + e_4e_6 + e_4e_8 + e_7e_9)\\
&+ 208e_1e_3 + 224(e_2e_3 + e_2e_4 + e_3e_5 + e_1e_2e_4) \pmod{256}.
\end{aligned} \tag{C.2}
$$

C.2 The Proof of Our Result Regarding Kloosterman Sums Divisible by 256

We now give a more detailed proof of Theorem 3.3.9.

Explicit Proof of Theorem 3.3.9. Let a be a non-zero element of $\beta L \cup \beta^2 L \cup \beta^4 L$, and let

$$\phi(x) = x^{7k} + e_1 x^{7k-1} + ... + e_{7k-1}x + e_{7k}$$

be the characteristic polynomial of a over $\mathbb{F}_2$. By Theorem 3.3.4, we have

$$e_i = 0 \text{ whenever } i \not\equiv 0 \pmod 7. \tag{C.3}$$

We confirm the result by checking that (C.3) forces every term of (C.2) to be zero. To accomplish this, it is sufficient to check that no product of the form

$$\prod_{i \in I} e_i,\ I \subseteq \{1, \ldots, 32\} \tag{C.4}$$

appearing as a term in (C.2) has every index i divisible by 7. One may check by hand (surprisingly quickly) that this is the case. $\square$