LOW DIFFERENTIAL UNIFORM FUNCTIONS FROM ALGEBRAIC AND COMBINATORIC STRUCTURES

by

Emily Bergman

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Summer 2020

LOW DIFFERENTIAL UNIFORM FUNCTIONS

FROM ALGEBRAIC AND COMBINATORIC STRUCTURES

by

Emily Bergman

Approved: _____

Louis Rossi, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: _____

John Pelesko, Ph.D.
Dean of the College of Arts and Sciences

Approved: _____

Douglas J. Doren, Ph.D.
Interim Vice Provost for Graduate and Professional Education and
Dean of the Graduate College

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Robert Coulter, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Qing Xiang, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Sebastian Cioaba, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Pamela Kosick, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

I have grown in many ways during my graduate studies at the University of Delaware. There are many people that have taught and supported me throughout this journey; without them, none of this would have been possible.

My advisor, Dr. Robert S. Coulter, has taught me countless things about mathematics, teaching, and European cultures. I'm grateful for your guidance and patience during this process. Special thanks to my committee, Dr. Qing Xiang, Dr. Sebastian Cioaba, and Dr. Pamela Kosick, for your time and support. To the staff in the Mathematics Department, who provided administrative support without which my success would not be possible, thank you.

There are many great teachers that have facilitated my love of mathematics. I am thankful for my high school mathematics teachers that made mathematics fun; for my undergraduate professors that saw my potential and encouraged me to continue my education; and for the professors at UD who pushed me to be a better mathematician.

I would like to acknowledge my family and friends. To my family, thank you for your unconditional love that has kept me grounded and focused during this experience. A huge thank you to my Ewing family who supported me with teaching advice, AWM events, and mathematical collaboration. Finally, thank you to my friends. You have been a constant source of encouragement, joy, and compassion.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

This dissertation splits into two major parts. First, given a function, f, over $\mathbb{F}_q$ and nonzero $a \in \mathbb{F}_q$ we define the difference function as $\Delta_f(x,a) := f(x+a) - f(x) - f(a)$. The differential uniformity (DU) of f is $\delta := \max_{b \in \mathbb{F}_q} \#\{c : c \in \mathbb{F}_q \mid \Delta_f(c,a) = b\}$. Functions with lower differential uniformity are more resistant to differential cryptanalysis and as such are more desirable for use in substitution boxes. Inspired by the work in [23], we investigate the differential uniformity of functions of the form $f(x) = x * x$ using multiplication from algebraic objects with the objective of constructing functions with low differential uniformity. The second major part concerns the classification of planar monomials over fields of size $\mathbb{F}_{p^3}$. Previous work on this problem has been completed for fields of size p, p^2, and p^4 with p odd [48], [21], [26] and the problem has been reduced considerably for fields of size p^{2k} with $p \geq 5$ and $k \geq 2$ through the work in [26]. We make significant progress on the p^3 case.

The thesis can be broken down as follows. In Chapter 1, we give the preliminary material that we will need throughout this work including: background on finite fields and polynomials over those fields; the framework for algebraic objects like S-sets, (pre)semifields, and nearfields; and the background of differential uniformity. The main result for Chapter 2, Theorem 2.1.1, explores the notion of creating a new function with low DU by replacing the coordinate functions of known functions. We use mutually orthogonal systems to create bounds for the differential uniformity of these new functions and we discuss known results in terms of this new methodology. The results of our investigation for low DU functions from algebraic objects are included in Chapter 3. We find functions corresponding to specific Kantor presemifields that are at most 4 DU in Theorem 3.3.2 and give a bound for the differential uniformity of functions from other Kantor presemifields in Theorem 3.3.3. In Theorem 3.4.3, we give a lower bound for the differential uniformity for the function $f(x) = x * x$ where the multiplication is from the regular planar nearfield $N(2, q^2)$ with q

odd. This constitutes the first major part. The second major part of the thesis is contained in Chapter 4. The classification of planar monomials for fields of size p^3 falls in three parts. Proposition 4.2.1 and Proposition 4.2.2 fully resolve two of those cases while Section 4.3 outlines the current status of case three. Finally, in Chapter 5 we give discuss open problems that have come from this work.

Chapter 1

PRELIMINARIES

1.1 Motivation

Cryptography is the science of secure communication between individuals through the threat of interference from a third party. Encryption is the process of encoding a piece of information, called the plaintext, into a new form, called the ciphertext, such that an unintended recipient cannot gain access to it. Decryption is the process of returning the ciphertext to its plaintext form. A cipher is the algorithm for the encryption and decryption processes. A common example of such a process is the Caesar Cipher or a shift cipher. In this work we will be focused on substition boxes or S-boxes. S-boxes take some number of bits of the plaintext and transform them into some number of output bits. We will focus on S-boxes whose input and output sizes are the same, though you can have S-boxes with different input and output bits. These S-boxes can be thought of as functions over a finite field, which is how we study them in this thesis.

An eavesdropper can perform types of attacks on the cipher to attain the key to decrypt the ciphertext. Differential cryptanalysis is the study of how differences in the input bits in a S-box affect the differences of the output bits in a S-box. Considering the S-box as a function $f(x)$ and a fixed non-zero element of the field a, differential cryptanalysis observes how $f(x + a)$ and $f(x)$ are related for every input value of x. If the behavior of these differences does not appear random, then an attacker can exploit these properties to help decode the ciphertext and gain access to the information. Therefore, for a fixed nonzero a in the field and b an arbitrary element of the field, we will be interested in the number of solutions of $f(x + a) - f(x) = b$ (equivalently $f(x + a) - f(x) - f(a) = b$). We want this to have as even a distribution as possible for all nonzero a. This would be we have the lowest possible and

thus, optimal differential uniformity. A major aim of this thesis is to construct near optimal, or low, differentially uniform functions.

1.2 Finite Fields

Throughout this work we let p be a prime, n be a natural number, and q be a power of p. The finite field with q elements will be denoted as $\mathbb{F}_q$ and $\mathbb{F}_q^n$ denotes the n dimensional vector space over $\mathbb{F}_q$. In general, if we have a set S with a binary operation and an identity element e corresponding to the binary relation we will denote the set $S \setminus \{e\}$ as S^*. For example, let 0 be the additive identity of $\mathbb{F}_q$, then the set of non-zero elements of $\mathbb{F}_q$ is $\mathbb{F}_q^*$. Since the multiplicative group of a finite field is cyclic, it can be generated by a primitive element $a \in \mathbb{F}_q^*$; in general we denote the group generated by a as $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Given a fixed basis, $\{b_i\}_{i=1}^n$, for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ we can view $x \in \mathbb{F}_{q^n}$ as the element $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ where $x = x_1 b_1 + \ldots x_n b_n$. This is an isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$ (when viewed as vector spaces over $\mathbb{F}_q$); therefore, we will use these interchangeably depending on what is more useful. Any function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ can be represented uniquely as a polynomial of degree less than q which we call the *reduced form*. We will let $\mathbb{F}_q[X]$ denote the polynomial ring over $\mathbb{F}_q$ in indeterminate X. The following theorem from [19] is an example of the relationship between functions and polynomials. An indicator function for a subset $S \subseteq \mathbb{F}_q$ is a function $i_S : \mathbb{F}_q \to \mathbb{F}_q$ satisfying:

$$i_S(x) = \begin{cases} 0, & x \notin S \\ 1, & x \in S. \end{cases}$$

Theorem 1.2.1. *(Castillo, [19]) Let m be a divsor of $q-1$. The polynomial representation of the indicator function for the multiplicative coset $c^a\langle c^{(q-1)/m}\rangle \subseteq \mathbb{F}_q^*$ is given by*

$$i_{c^a\langle c^{(q-1)/m}\rangle}(X) = -m(h_{q-1/m}((c^{-a}X)^m) - 1)$$

where $h_k(X) = 1 + X + X^2 + \ldots X^k \in \mathbb{F}_q[X]$ and c is a primitive element of $\mathbb{F}_q$.

Given the isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$ fix a basis, $\{b_1, \ldots, b_n\}$, for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. We can view f as a function in n variables, called F, where

$$F(x_1, \ldots, x_n) = f(x_1 b_1 + \ldots + x_n b_n).$$

We may also view f as a *vectorial function* $(f_1(x), \ldots, f_n(x))$ each $f_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined as $f_i(x) = c_i$ where $f(x) = c_1 b_1 + \ldots + c_n b_n$. We call the f_i's *coordinate functions*. We can also view the coordinate functions as multivariate functions given as $(F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots x_n))$ with $F_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$. The version of the function we will look at will depend on how we will use the function.

1.2.1 S-sets

Every degree 2 polynomial over $\mathbb{F}_q$ splits completely in $\mathbb{F}_{q^2}$. That is, for every $a, b \in \mathbb{F}_q$ there exists some $u_1, u_2 \in \mathbb{F}_{q^2}$ such that

$$X^2 + bX + a = (X + u_1)(X + u_2).$$

Therefore, u_1 and u_2 satisfy the equations

$$u_1 u_2 = a, \text{ and}$$
$$u_1 + u_2 = b.$$

Without loss of generality if $u_1 = 0$, then $a = 0$ and $u_2 = b$. Assuming that $a \neq 0$ and rearranging these equations we find that $u_1 + a u_1^{-1} = b$. It follows that, given a fixed $a \in \mathbb{F}_q$, every $b \in \mathbb{F}_q$ can be written as $u + au^{-1}$ for some $u \in \mathbb{F}_{q^2}$.

Let q is odd and a is a square in $\mathbb{F}_q$; in other words $a = \alpha^2$ for some $\alpha \in \mathbb{F}_q$. We can partition the elements in $\mathbb{F}_q$ into the following sets:

$$S_0^a(q) = \{\pm 2\alpha\},$$
$$S_1^a(q) = \{u + au^{-1} \mid u \in \mathbb{F}_{q^2} \text{ and } u^{q-1} = 1 \text{ and } u \neq \pm\sqrt{a}\}, \text{ and}$$
$$S_2^a(q) = \{u + au^{-1} \mid u \in \mathbb{F}_{q^2} \text{ and } u^{q+1} = a \text{ and } u \neq \pm\sqrt{a}\}.$$

If $b = \pm 2\alpha$, then the equation is $x^2 \pm 2\alpha x + a = 0$. This is the same as $(x \pm \alpha)^2 = 0$. Which implies that $u = \pm\alpha$. When a is not a square $\pm 2\sqrt{a}$ is not an element of $\mathbb{F}_{q^2}$. Thus, $S_0^a(q) = \emptyset$ and we can partition the elements of $\mathbb{F}_q$ into the sets:

$$S_1^a(q) = \{u + au^{-1} \mid u \in \mathbb{F}_{q^2} \text{ and } u^{q-1} = 1 \text{ and } u \neq \pm\sqrt{a}\} \text{ and}$$
$$S_2^a(q) = \{u + au^{-1} \mid u \in \mathbb{F}_{q^2} \text{ and } u^{q+1} = a \text{ and } u \neq \pm\sqrt{a}\}.$$

The above S-sets can be a useful representation of $\mathbb{F}_q$. They arise, for example, in the study of Dickson polynomials of the first and second kind see [27], [44], and [53] Chapter 7 for more information.

1.2.2 Distribution of Squares and Non-squares in $\mathbb{F}_{p^n}$

Fix a non-zero $a \in \mathbb{F}_{p^n}$. One can partition the elements of $\mathbb{F}_q$ in the following way:

$$K_1(a) = \{b : b \in \mathbb{F}_{p^n} \mid b \text{ and } a+b \text{ are non-squares in } \mathbb{F}_{p^n}\},$$

$$K_2(a) = \{b : b \in \mathbb{F}_{p^n} \mid b \text{ and } a+b \text{ are squares in } \mathbb{F}_{p^n}\},$$

$$K_3(a) = \{b : b \in \mathbb{F}_{p^n} \mid b \text{ is a square and } a+b \text{ is a non-square in } \mathbb{F}_{p^n}\},$$

$$K_4(a) = \{b : b \in \mathbb{F}_{p^n} \mid b \text{ is a non-square and } a+b \text{ is a square in } \mathbb{F}_{p^n}\}.$$

The cardinalities of these sets were considered by Raber [62], who showed that

$$\#K_i(a) = \frac{p^n - 1}{4} + t_i$$

where t_i is either 0 or 1 for $i = 1, 2, 3, 4$.

We will be interested in these sets in Section 3.4.2. We will also use the quadratic character $\eta_q : \mathbb{F}_q \to \mathbb{C}$ known as the quadratic character, see [53] Chapter 5. If the domain is clear from context we may drop the subscript q. If $a \in \mathbb{F}_q$, then

$$\eta_q(a) = \begin{cases} 0 & a = 0, \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square}, \\ -1 & \text{if } a \text{ is not a square.} \end{cases}$$

1.3 Some Classes of Polynomials

A polynomial is called *linearized* if it is of the form $\sum_i a_i X^{p^i}$ with $a_i \in \mathbb{F}_{p^n}$. Any linearized polynomial acts as linear transformation; in other words, $L(ax) = aL(x)$ and $L(x+y) = L(x) + L(y)$ for all $a \in \mathbb{F}_p$ and $x, y \in \mathbb{F}_{p^n}$. The *trace function* maps $\mathbb{F}_{q^n}$ to a subfield $\mathbb{F}_{q^m}$ and is given by

$$\mathrm{Tr}_{n/m}(\alpha) = \alpha + \alpha^{q^m} + \alpha^{q^{2m}} + \ldots + \alpha^{q^{m(\frac{n}{m}-1)}}.$$

When q is a prime and $m = 1$, this is called *the absolute trace function* and maps into the prime subfield. All of the linear transformations from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ can be written in terms of the trace function as $\mathrm{Tr}_{n/m}(bx)$ for some $b \in \mathbb{F}_{q^n}$ ([53], Theorem 2.24). We will denote the polynomial representation of the trace function as $\mathrm{Tr}_{n/m}(X)$ later in this thesis.

Given a basis $B = \{b_i\}_{i=1}^n$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ the *dual basis* corresponding to B is the basis, $\{\beta_i\}_{i=1}^n$, for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfying

$$\mathrm{Tr}(b_i\beta_j) = \begin{cases} 0 & i \neq j, \\ 1 & i = j. \end{cases}$$

If $\{b_i\}_{i=1}^n$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\{\beta_i\}_{i=1}^n$ is the corresponding dual basis, then it can be verified that the coordinate functions for $f(x)$ is $\{\mathrm{Tr}(\beta_i f(x))\}_{i=1}^n$.

In addition to linearized polynomials, we will refer to many special types of functions over $\mathbb{F}_q$ throughout this work. A polynomial is called a *permutation polynomial* if the polynomial induces a bijection on $\mathbb{F}_q$. In Section 3.5 and Chapter 4, we will use Hermite's criterion for permutation polynomials.

Theorem 1.3.1. *[Hermite, [45]; Dickson, [33]] Let $q = p^n$. A polynomial $f \in \mathbb{F}_q[X]$ is a permutation polynomial over $\mathbb{F}_q$ if and only if*

i. f has exactly one root in $\mathbb{F}_q$, and

ii. the reduction of f^t mod $(X^q - X)$,with $0 < t < q-1$ and $t \not\equiv 0 \mod p$, has degree less than $q-1$.

A polynomial is called *affine* if it is a sum of a linearized polynomial and a constant. The kernel of a linearized polynomial, $L(X)$, is the set $Ker(L(x)) = \{x : x \in \mathbb{F}_q \mid L(x) = 0\}$ A polynomial is called a *Dembowski-Ostrom (DO) polynomial* if it is of the form $\sum_{k,j} a_{kj} X^{p^k+p^j}$ for $a_{kj} \in \mathbb{F}_q$. Finally, a polynomial is called *quadratic* if it is the sum of a DO polynomial and an affine polynomial.

There are also a number of relevant equivalence relations on functions. Let F_1 and F_2 map $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then F_1 and F_2 are

- *affine (linearized) equivalent* if $F_2 = A_1 \circ F_1 \circ A_2$ where A_1 and A_2 are affine (linearized) permutations of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ respectively;

- *extended affine equivalent (EA equivalent)* if $F_2 = A_1 \circ F_1 \circ A_2 + A$ where A_1 and A_2 are affine (linearized) permutations of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ respectively and A is an affine map from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$;

- *CCZ equivalent* if for some permutation L of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ the image of the graph of F_1 is the graph of F_2. In other words $L(G_{F_1}) = G_{F_2}$ where $G_{F_i} = \{(x, F_i(x)) | x \in \mathbb{F}_{p^n}\}$.

1.4 Semifields

A finite set S with a binary operation $*$ is a *quasigroup* if for every $a, b \in S$ there exists unique $x, y \in S$ such that $a * x = b$ and $y * a = b$.

Definition 1.4.1. *A finite set S with two operations, $+$ (addition) and $*$ (multiplication), is called a **presemifield** if*

- $(S, +)$ *is an abelian group with identity* 0*,*

- $(S^*, *)$ *is a quasigroup,*

- *there are no zero divisors, and*

- *left and right distributive properties hold.*

*If a presemifield has a multiplicative identity, then we call it a **semifield**.*

The additive structure of a presemifield is necessarily elementary abelian so presemifields can be viewed as $S = (\mathbb{F}_q, +, *)$, where $(\mathbb{F}_q, +)$ is the additive group of $\mathbb{F}_q$ and $x * y = \phi(x, y)$ for some function $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q$. Since finite fields are semifields, we call a semifield which is not a finite field a *proper semifield*. Note that presemifields and semifields do not have to be associative nor commutative with respect to multiplication.

Definition 1.4.2. *Let $S_1 = (\mathbb{F}_q, +, *)$ and $S_2 = (\mathbb{F}_q, +, \circ)$ be two presemifields. Then S_1 and S_2 are **isotopic** if and only if there exists three linearized permutation polynomials $L, M, N \in \mathbb{F}_q[x]$ such that for all $x, y \in \mathbb{F}_q$ $M(x) * N(y) = L(x \circ y)$. We say that (L, M, N) is an **isotopism** between S_1 and S_2. If $M = N$, then it is called a **strong isotopism**.*

One can always extend a presemifield to a semifield in the following way. Let $S = (\mathbb{F}_q, +, *)$ be a presemifield which does not contain an identity. To create a semifield from S choose any $a \in \mathbb{F}_q^*$ and define a new multiplication $\circ$ by $(x * a) \circ (a * y) = x * y$ for all $x, y \in \mathbb{F}_q$. Then $S' = (\mathbb{F}_q, +, \circ)$ is a semifield isotopic to S with identity $a * a$ and isotopism $(x * a, a * x, x)$. We say S' is a semifield corresponding to the presemifield S. If the original presemifield is commutative, then the semifield constructed is commutative and strongly isotopic to the original presemifield [23].

Lemma 1.4.3. *A non commutative presemifield cannot be strongly isotopic to a commutative presemifield.*

Proof. Suppose that there is a presemifield $R = (\mathbb{F}_q, +, *)$, a commutative presemifield $S = (\mathbb{F}_q, +, \circ)$, and linearized permutation polynomials $L, M \in \mathbb{F}_q[x]$ where

$$M(x) \circ M(y) = L(x * y) \ \forall x, y \in \mathbb{F}_q.$$

Since S is commutative, for all $x, y \in \mathbb{F}_q$ $M(x) \circ M(y) = M(y) \circ M(x)$. Since $M(x) \circ M(y) = L(x * y)$ we have that $L(x * y) = L(y * x)$. We have that $x * y = y * x$ since L is a permutation polynomial. So, R is commutative. Hence, our lemma is proven. □

1.4.1 Nuclei

To investigate a proper semifield's "distance" from multiplicative associativity we look at the following subsets.

Definition 1.4.4. *Let S be a semifield. Then*

- *the **left nucleus** is the set $N_l(S) = \{\alpha \in S | (\alpha * x) * y = \alpha * (x * y)\}$;*
- *the **middle nucleus** is the set $N_m(S) = \{\alpha \in S | (x * \alpha) * y = x * (\alpha * y)\}$;*

- *the **right nucleus** is the set* $N_r(S) = \{\alpha \in S | (x * y) * \alpha = x * (y * \alpha)\}$*; and*
- *the **nucleus** is the set* $N = N_l(S) \cap N_m(S) \cap N_r(S)$.

Each of these sets are fields and semifields are vector spaces over their corresponding nuclei. The larger these sets are the closer the semifield is to having multiplicative associativity. These sets are useful in the classification of semifields.

Next, we introduce two classes of presemifields. Our list is not intended to be exhaustive.

1.4.2 Albert's Generalized Twisted Fields

Twisted fields and generalized twisted field were introduced by Albert in [1, 2, 3, 4]. Let $\mathbb{F}_{p^n}$ be a finite field of odd characteristic p and $n > 2$. Consider the nontrivial automorphisms θ and α defined by $x^\theta = x^{p^i}$ and $x^\alpha = x^{p^j}$ for some $i, j \in [1, \ldots, n-1]$. Fix an element $c \in \mathbb{F}_{p^n}$ satisfying $c \neq \frac{x}{x^\theta}\frac{y}{y^\alpha}$ for any $x, y, y \in \mathbb{F}_q^*$ and define a new multiplication $x * y = xy - cx^\theta y^\alpha$ for $x, y \in \mathbb{F}_q$. Then $A = (\mathbb{F}_{p^n}, +, *)$ is a semifield where $+$ is field addition. Albert showed in [2] that A is commutative if and only if $(x^\theta)^\alpha = x$ and $c = -1$.

1.4.3 Kantor's Characteristic Two Presemifields

Consider the field $\mathbb{F}_{q^n}$ with q a power of 2 and n odd. Given a chain of fields

$$K = \mathbb{F}_q \subseteq F_k \subsetneq \ldots \subsetneq F_1 \subsetneq F = \mathbb{F}_{q^n}$$

with the corresponding trace functions $T_i : F \to F_i$ defined as in Section 1.2 and a sequence $(a_1, \ldots a_n)$ where $a_i \in F^*$, define a new multiplication as

$$x * y = xy^2 + \sum_{i=1}^{n} (T_i(a_i x)y + a_i T_i(xy)).$$

Then Kantor [49] showed $(\mathbb{F}_{q^m}, +, *)$, is a presemifield.

1.4.4 A few Classification Results for Commutative Semifields

There have been a few classification results for commutative semifields. Knuth in 1965 showed that any semifield of order p^2 is a finite field [51]. In 1977, Menichetti showed

that a commutative presemifield which is three dimensional over its middle nucleus is necessarily isotopic to Albert's commutative twisted field [57].

1.5 Quasifields and Nearfields

Definition 1.5.1. *A set S with binary operations $+$ and $*$ is a **left quasifield** if it satisfies:*

- $(S, +)$ *is a group,*
- *for every $a, b \in S$ there exists $x, y \in S$ such that $a * x = b$ and $y * a = b$.*
- *there exists a multiplicative identity element,*
- *the left distributive law holds, and*
- *$a * x = b * x + c$ has exactly one solution for all $a, b, c \in S$ with $a \neq b$.*

You can make a similar definition for the right quaifield where the right distributive law holds and the last property is $x * a = x * b + c$ has exactly one solution for all $a, b, c \in S$ with $a \neq b$. As with semifields, the additive structure of a quasifield is elementary abelian.

Definition 1.5.2. *A finite set S with two operations, $+$ (addition) and $*$ (multiplication), is called a **nearfield** if*

- $(S, +)$ *is an abelian group with identity* 0*,*
- *multiplication is associative,*
- *there is a multiplicative identity,*
- *for all non-zero $a \in S$ there is a multiplicative inverse a^{-1}, and*
- *one of the distributive properties hold.*

*If $(S, +, *)$ is also a left quasifield, then it is a **planar nearfield**.*

Dickson discovered two types of planar nearfields: regular and irregular nearfields [34]. Zassenhaus proved that every finite nearfield is either a regular nearfield or one of the irregular nearfields [65]. We will describe the nearfields below. For more about nearfields see [31], [34], and [65].

1.5.1 The Regular Planar Nearfields

Let q be a prime power and n a natural number such that the prime divisors of n also divide $q-1$. Additionally, if $q \equiv 3 \pmod 4$, then $n \not\equiv 0 \pmod 4$. Let c be a primitive element of $\mathbb{F}_{q^n}$ and let C be the group generated by c^n. The coset representatives of C are $c_i = c^{q^i-1/q-1}$ with $i = 0, \ldots, n-1$. We define the function $\alpha(y)$ $x \mapsto x^{q^i}$ if and only if $y \in c_i C$. Define a new multiplication on $\mathbb{F}_{q^n}$ by $x * y = x^{\alpha(y)}y$ for $y \neq 0$ and $x * 0 = 0$. Then $N(n,q) = (\mathbb{F}_{q^n}, +, *)$, where $+$ is the field addition, can be shown to be a nearfield, see [34]. These are called the *regular nearfields*.

1.5.2 The Irregular Nearfields

Though we have only computational results regarding them, and so don't need a theoretical description, for completeness we outline a description of the irregular nearfields in the remainder of this section. To describe them, we need to give a description of both the addition and multiplication of each. For the addition, we have the following theorem which holds for all nearfields.

Theorem 1.5.3. *Let N be a nearfield of finite dimension n over its prime field $\mathbb{F}_p$. Then (n,p) has a fixed point free subgroup $S^\star$ such that if $S = S^\star \cup \{\mathbf{0}\}$, where $\mathbf{0}$ denotes the $n \times n$ zero matrix, then an addition can be defined on S in such a way that, under this addition and matrix multiplication, S is a nearfield isomorphic to N.*

Though this does not give an explicit description of the addition, it does allow for a description of the irregular nearfields in terms of just the generators of the subgroup $S^\star$ of the theorem. This is given in the following classification statement due to Zassenhaus [65].

Theorem 1.5.4. *Let N be a finite irregular nearfield. Then N has order p^2 and is isomorphic to one of the following nearfields S_i, where $S_i^\star$ is the subgroup of $(2,p)$ generated by the matrices given below and where addition is defined as in Theorem 1.5.3.*

I. $|S_1| = 5^2$ *and* $S_1^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}.$$

II. $|S_2| = 11^2$ *and* $S_2^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

III. $|S_3| = 7^2$ *and* $S_3^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & 4 \\ -1 & -2 \end{pmatrix}.$$

IV. $|S_4| = 23^2$ *and* $S_4^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

V. $|S_5| = 11^2$ *and* $S_5^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}.$$

VI. $|S_6| = 29^2$ *and* $S_6^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}.$$

VII. $|S_7| = 59^2$ *and* $S_7^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

While there are several standard treatments of the irregular nearfields, the description just given comes from S.D. Groves in [43].

1.6 Orthogonal Systems

Definition 1.6.1. *A system of functions $f_1, \ldots, f_m$ over $\mathbb{F}_q^n$ with $1 \leq m \leq n$ is said to be orthogonal in $\mathbb{F}_q$ if the system*

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= y_1 \\ f_2(x_1, \ldots, x_n) &= y_2 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= y_m \end{aligned}$$

has exactly q^{n-m} solutions in $\mathbb{F}_q^n$ for each $(y_1, \ldots, y_m) \in \mathbb{F}_q^m$. If $m = n$, then an orthogonal system is said to be maximal.

Orthogonal systems were introduced implicitly by Carlitz in [17, 18], and again by Nöbauer in [59]. Orthogonal systems with $n = 2$ and q a prime were studied by Kurvbatov and Starkov in [52]. The following theorems will prove useful.

Theorem 1.6.2. *(Carlitz, [18]; Niederreiter, [58]) Every orthogonal system can be extended to a maximal orthogonal system.*

Theorem 1.6.3. *(Niederreiter, [58]) Fix natural numbers n and m with $m \leq n$. A system of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ is orthogonal if and only if for all non-zero $(b_1, \ldots, b_m) \in \mathbb{F}_q^m$ the polynomial $b_1 f_1 + \ldots b_m f_m$ is a permutation polynomial.*

1.7 Differential Uniformity

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. We call $\Delta_f(x, a) = f(x+a) - f(x) - f(a)$ *the difference function* of f; if f is in its polynomial representation, then $\Delta_f(X, a)$ is called the *difference polynomial*. We call $D_f(x, a)$ the *derivative of* f in the direction of a.

The following definition is central to this thesis.

Definition 1.7.1. *A function, $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is said to be δ* differentially uniform *(δ - DU) if for all non-zero $a \in \mathbb{F}_{p^n}$ and for all $b \in \mathbb{F}_{p^m}$ $\Delta_f(x, a) = b$ has at most δ solutions.*

This definition is equivalent if we use $D_f(x,a)$ in place of $\Delta_f(x,a)$; later in this work it will be advantageous for us to use $D_f(x,a)$ instead of $\Delta_f(x,a)$. For a DO polynomial, $f(X) = \sum a_{ij}X^{p^i+p^j}$, the difference polynomial is the linearized polynomial $\Delta_f(X,a) = \sum a_{ij}(X^{p^i}a^{p^j} + a^{p^i}X^{p^j})$. The differential uniformity of a DO polynomial is $\max_{a\in\mathbb{F}_q^*} \#Ker(\Delta_f(X,a))$. The worst possible differential uniformity that a function $f : \mathbb{F}_q \to \mathbb{F}_q$ can have is q. This is only attained when the difference function is constant for some $a \in \mathbb{F}_q^*$. We will use these facts in future proofs.

There are some special cases of differential uniformity. We outline them in the next definition.

Definition 1.7.2. *A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is called **perfect nonlinear** if it is p^{n-m} - DU. When $n = m$, a function that is differentially 1 uniform is called a **planar function**. A function is called **almost perfect nonlinear (APN)** if it is differentially 2 uniform.*

Planar functions were introduced in a more general context by Dembowski and Ostrom in [32], while studying projective planes with a collineation group acting transitively on the affine points. An example of a planar function is x^2 over any field with odd characteristic. Another important example is given by the following lemma.

Lemma 1.7.3 (Coulter and Matthews, [29])**.** *Let p be an odd prime. The function $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^n}$ if and only if $\dfrac{n}{(n,\alpha)}$ is odd.*

Planar functions do not exist over characteristic two fields. In characteristic two, the difference function of $f(x)$ is $\Delta_{f,a}(x) = f(x+a) + f(x) + f(a)$. Suppose x_0 is a solution of $\Delta_f(x,a) = b$. Then

$$f(x_0 + a + a) + f(x_0 + a) + f(a) = b.$$

So, $x_0 + a$ is also a solution and there are at least two solutions to $\Delta_{f,a}(x) = b$. A family of APN functions over $\mathbb{F}_{2^n}$ is the set of Gold functions. A Gold function is of the form x^{2^i+1} where $\gcd(i,n) = 1$ [42, 56, 60].

For all nonzero $a \in \mathbb{F}_{p^n}$ and $b \in \mathbb{F}_{p^m}$, if $\Delta_{f,a}(x) = b$ has either λ or 0 solutions, then $f(x)$ is a *semiplanar function of index* λ. The following theorem describes a family of semiplanar functions.

Theorem 1.7.4 (Coulter and Fain, [22]). *If* $\dfrac{n}{(i,n)}$ *is even, then* x^{p^i+1} *is semiplanar of index* $p^{(i,n)}$.

In 2008, Budaghyan and Helleseth showed that a DO polynomial is CCZ-inequivalent to the planar function x^2 if $a_{jj} = 0$ for all j and is CCZ-inequivalent to the planar function x^{p^t+1} with $\frac{n}{(t,n)}$ odd if $a_{kj} = 0$ for all k and $j = k \pm t \pmod{n}$ [15].

All of the equivalences in Section 1.3 preserve differential δ uniformity.

The *Walsh transform* of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the integer valued function

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ab)} \text{ for } a, b \in \mathbb{F}_{2^n}.$$

The *Walsh coefficients* of F are the values $W_F(a,b)$ and the multiset $\{W_F(a,b) : a, b \in \mathbb{F}_{2^n}\}$ is the *Walsh spectrum of* F. The *extended Walsh spectrum* is the multiset $\{|W_F(a,b)| : a, b \in \mathbb{F}_{2^n}\}$. These too are invariants under the equivalences of Section 1.3.

1.7.1 Planar Functions and Orthogonal Systems

There is a natural relationship between planar functions and orthogonal systems that stems from the relationship between orthogonal systems and permutation polynomials in Theorem 1.6.3.

Theorem 1.7.5 (Coulter and Matthews, [28]). *Let* $f \in \mathbb{F}_{q^n}[X]$ *be planar,* $\{b_1, \ldots, b_n\}$ *a fixed basis for* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*, and* $f_1, \ldots, f_n \in \mathbb{F}_q[X]$ *be the corresponding coordinate functions for* f *as polynomials. The system of polynomials* $\{\Delta_{f_i}(X,a) \mid i = 1, \ldots, n\}$ *forms a maximal orthogonal system in* $\mathbb{F}_q$ *for each non-zero* $a \in \mathbb{F}_{q^n}$.

1.7.2 Correspondence Between Commutative Presemifields and Planar Functions

In 2008 Coulter and Henderson showed that there is a correspondence between commutative semifields and planar DO polynomials.

Theorem 1.7.6 (Coulter and Henderson, [23]). *Let q be an odd prime power. If $f \in \mathbb{F}_q[X]$ is a planar DO polynomial, then $(\mathbb{F}_q, +, *)$ is a commutative presemifield, where $x * y = f(x + y) - f(x) - f(y)$. Conversely, if $(\mathbb{F}_q, +, *)$ is a commutative presemifield, then $f(X) = \frac{1}{2}(X * X)$ is a planar DO polynomial.*

This connection between algebraic objects and functions with low differential uniformity form the core motivation for the majority of the work of this thesis.

1.8 The Dembowski-Ostrom Conjecture

In [32], Dembowski and Ostrom questioned whether, ignoring constants and linearized terms the only planar polynomial over finite fields are Dembowski-Ostrom polynomials.

This query is nowadays called the Dembowski-Ostrom conjecture.

Conjecture 1.8.1 (Dembowski and Ostrom, 1968). *A planar polynomial is necessarily a Dembowski-Ostrom polynomial.*

This conjecture was proven for prime fields in 1989-1990 [41], [46], and [63]. In 1997, Coulter and Matthews showed the conjecture was false in [29] with the smallest counterexample being X^{14} over $\mathbb{F}_{3^4}$.

Theorem 1.8.2 (Coulter and Matthews, [29]). *Let $q = 3^e$ and α a natural number. Then $X^{(3^\alpha+1)/2}$ is planar over $\mathbb{F}_q$ is and only if $(\alpha, e) = 1$ and α is odd.*

Up to EA equivalence, these are the only known counterexamples; thus, the conjecture is open for characteristic larger than 3.

1.8.1 Classification of Planar Monomials.

More is known when we restrict the problem to planar monomials

Proposition 1.8.3 (Coulter and Matthews [29]). *The following statments hold.*

(i) If $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $\frac{e}{(\alpha,e)}$ is odd.

(ii) *If X^n is planar over $\mathbb{F}_q$, then X^n is planar over every subfield of $\mathbb{F}_q$.*

(iii) *If X^n is planar over $\mathbb{F}_q$, then $(n, q-1) = 2$.*

(iv) *The monomial X^n is planar over $\mathbb{F}_q$ if and only if X^{np^i} is planar over $\mathbb{F}_q$ for any non-negative integer i.*

Some progress has been made on the DO conjecture for monomials. The next proposition outlines that progress.

Proposition 1.8.4. *The current status on the Dembowski-Ostrom Conjecture is as follows.*

(i) *The polynomial X^n is planar over $\mathbb{F}_p$ if and only if $n \equiv 2 \mod (p-1)$ (Johnson, [48]).*

(ii) *Let p be an odd prime. The polynomial X^n is planar over $\mathbb{F}_{p^2}$ if and only if $n \equiv 2 \mod (p^2-1)$ or $n \equiv 2p \mod (p^2-1)$ (Coulter, [21]).*

(iii) *The polynomial X^n is planar over $\mathbb{F}_{p^4}$, with $p \geq 5$ an odd prime, if and only if $n \equiv 2p^j \mod (p^4-1)$ for some integer $0 \leq j < 4$ (Coulter and Lazebnik, [26]).*

Coulter and Lazebnik in 2012 give a classification of planar monomials for p^4 and made additional progress on Conjecture 1.8.1. They resolved case one and case two of the following theorem.

Theorem 1.8.5 (Coulter and Lazebnik, [26])**.** *Let $q = p^e$ with p an odd prime and $e = 2w$ with $w \geq 2$. Suppose X^n is planar over $\mathbb{F}_q$, $n < q$, and there exists an integer j, $0 \leq j < w$, for which $n \equiv 2p^j \mod (p^w - 1)$. If $n = (a_{e-1} \cdots a_0)_p$, then some cyclic shift of the w-tuple*

$$(a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1})$$

must be one of the following:

$$(0, 0, \ldots, 0, 2),$$

$$(p-1, p-1, \ldots, p-1, p+1), \quad \text{or}$$

$$(\underbrace{0, 0, \ldots, 0}_{m \geq 0 \text{ times}}, p, \underbrace{p-1, p-1, \ldots, p-1}_{w-2-m \text{ times}}, 1).$$

1.9 APN Functions and the switching technique

A function f that maps into $\mathbb{F}_2$ is called a *boolean function*. Given an APN function F and $u \in \mathbb{F}_{2^n}^*$, Edel and Pott [39] gave the following conditions on a boolean function f so that $F(x) + uf(x)$ is APN. They called this the *Dillon Switching Technique*.

Theorem 1.9.1 (Edel and Pott, [39]). *Assume that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an APN function. Let $u \in \mathbb{F}_{2^n}$ with $u \neq 0$ and let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Then $F(x) + uf(x)$ is an APN function if and only if for all $x, y, a \in \mathbb{F}_{2^n}$ such that $F(x) + F(x + a) + F(y) + F(y + a) = u$,*

$$f(x) + f(x + a) + f(y) + f(y + a) = 0.$$

Similarly, Budaghyan, Carlet, and Leander gave conditions on an APN DO polynomial $F(x)$ and a DO polynomial $f(x)$ such that $F(x) + f(x)$ is APN.

Theorem 1.9.2 (Budaghyan, Carlet, and Leander, [14]). *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a DO APN function and f be a DO function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ where m is a divisor of n. If for every nonzero $a \in \mathbb{F}_{2^n}$ there exists a linear function l_a from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ satisfying:*

1. *$\Delta_{f,a}(x) = l_a(\Delta_{F,a}(x))$, and*
2. *if there exists $x \in \mathbb{F}_{2^n}$ such that $\Delta_{F,a}(x) = y \in \mathbb{F}_{2^m}$ with $y \neq 0$, then $l_a(y) \neq y$,*

then the function $F(x) + f(x)$ is APN.

The methods in these two theorems prove to be very useful in showing that a function has low differential uniformity. We will generalize these theorems in Chapter 2 and use them in Chapter 3.

1.10 Further Results

In this section we give some more results that are needed in this thesis.

We are interested in algebraic objects; all of which have a set and a multiplication $*$. Given a set S and a binary operation $*$ the center is the set

$$Z(S) = \{c : c \in S \mid c * a = a * c \ \forall a \in S\}.$$

As shall be seen, depending on the properties of the algebriac object and the function, f, the center can help us determine a bound for the differential uniformity of f.

1.10.1 Number Theory Results

The following theorem of Lucas was instrumental in the proofs of Proposition 1.8.4 and will be used in Section 3.5 and Chapter 4.

Lemma 1.10.1 (Lucas, [54])**.** *Let p be a prime and $\alpha \geq \beta$ be positive integers with base p expansion $\alpha = \sum_i \alpha_i p^i$ and $\beta = \sum_j \beta_j p^j$. Then,*

$$\binom{\alpha}{\beta} = \prod_i \binom{\alpha_i}{\beta_i} \mod p,$$

where $\binom{n}{k} = 0$ if $n < k$.

Lucas' Theorem is particularly relevant when considering the differential uniformity of monomials, see Proposition 1.8.3 (iv) for example.

For X^k, consider k in its p-ary expansion

$$k = (a_{n-1}\ a_{n-2}\ \ldots\ a_1\ a_0)_p,$$

where $k = a_{n-1}p^{n-1} + a_{n-2}p^{n-2} + \ldots a_1 p + a_0$. Calculating $X^{k\alpha} \bmod (X^q - X)$ is the same as calculating $k\alpha \bmod (q-1)$, and $kp \bmod (q-1)$ results in simply a cyclic shift of the base p coefficients. That is, $kp \bmod (q-1) = (a_{n-2}\ a_{n-3}\ \ldots\ a_1\ a_0\ a_{n-1})_p$. Additionally, if a b_i in $k\alpha = \sum_{i=0}^{n-1} b_i p^i$ is at least p, say b_{n-1}, then determining the base p description of $k\alpha$ results in a subtraction of p from the 1st coordinate, and an adding of 1 to the last coordinate. That is $\sum_{i=0}^{n-1} b_i p^i \bmod (q-1) = (b_{n-1} - p)p^{n-1} + b_{n-2} + \cdots + b_1 p + (b_0 + 1)$. We will refer to such an occurrence as a carry.

1.10.2 Projective Planes

Given a system of points and lines with an incidence structure we say that two or more points are *collinear* if they lie on the same line.

Definition 1.10.2. *An **affine plane** is an incidence structure that satisfies the following properties:*

- *any two points line on a unique line;*

- *every line has at least two points;*
- *given any line and any point not on that line there is a unique line which contains the point and does not meet the given line; and*
- *there exists three non-collinear points.*

In an affine plane, two lines are parallel if they are either the same line or there is no point that is incident to both lines. The relation defined by parallel lines is an equivalence relation and we can partition the set of lines into sets of parallel lines, called the parallel classes.

For a finite affine plane there exists a natural number n, called the *order* of the affine plane, such that

- each line contains n points;
- each point is on $n + 1$ lines;
- there are n^2 points; and
- there are $n^2 + n$ lines.

Give a set of n elements R and two binary relations on R, $+$ and $*$, we can define an incidence structure using $(R, +, *)$ by:

- the points are $R \times R$,
- one of the parallel class is the set of lines of the form $[v] := \{(v, y) : y \in R\}$ - these are called the vertical lines,
- the other parallel classes are the the lines with the same slope $[m, k] : \{(x, m * x + k) : x \in R\}$ - these are called the slope lines.

Given a semifield, nearfield, or quasifield the incidence structure defined above is an affine plane of order n.

Definition 1.10.3. *A **projective plane** is an incidence structure that satisfies the following properties:*

- *every two distinct points line are incident to a unique line;*
- *every two distinct lines are incident to a unique point; and*
- *there exists four points no three of which are non-collinear.*

For a finite projective plane plane there exists a natural number n, called the *order* of the projective plane, such that

- each line contains $n + 1$ points;
- each point is on $n + 1$ lines; and
- there are $n^2 + n + 1$ points and there are $n^2 + n + 1$ lines.

There is a standard technique for extending an affine plane to a projective plane. For each class of parallel lines we add a new point, also adding that point to each line in the parallel class. A new line consisting of all the new points is also created. To obtain an affine plane from a projective plane you simply delete any one line of the projective plane along with all the points on it.

Chapter 2

COORDINATE FUNCTIONS

In this chapter, we will generalize Dillon's Switching Technique in Theorem 2.1.1. We then apply this technique in Theorem 2.3.1 to get bounds on the differential uniformity for functions that are a sum of a planar function and an arbitrary function.

2.1 Extended Switching Technique

As was outlined in Section 1.2, by fixing a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ that includes u, call it $\{u = b_1, b_2, \ldots, b_n\}$, we can represent the $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ by the coordinate functions $(f_1, \ldots, f_n)$. Given any boolean function $f : \mathbb{F}_q \to \mathbb{F}_2$ Then the coordinate functions of $F(X) + uf(X)$ are $(f_1 + f, f_2, \ldots, f_n)$.

We can think of the Dillon switching technique as a condition on how to change one coordinate of an APN function and obtain an APN function, see Theorem 1.9.1. Our first theorem generalizes Theorem 1.9.1 to multiple coordinates. We will refer to this as Extended Switching Technique.

Theorem 2.1.1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function and $f : \mathbb{F}_{2^n} \to B$ where B is a k dimensional subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then $F(X) + f(X)$ is an APN function if and only if for all x, y, a in $\mathbb{F}_{2^n}$, $a \neq 0$, such that $f(x) + f(x + a) + f(y) + f(y + a) = b \in B$,*

$$F(x) + F(x + a) + F(y) + F(y + a) \neq b.$$

Proof. As was stated in Section 1.7, if x is a solution to $\Delta_f(x, a) = b$ in characteristic 2 then $x + a$ is also a solution. Let $z \in \mathbb{F}_{2^n}$ and suppose to the contrary there are four solutions to

$F(x) + F(x+a) + f(x) + f(x+a) = z$ for some nonzero $a \in \mathbb{F}_{2^n}$. We can call our solutions $x,\ x+a,\ y,\ y+a$. So, we have the following system of equations:

$$F(x) + F(x+a) + f(x) + f(x+a) = z,$$
$$F(y) + F(y+a) + f(y) + f(y+a) = z.$$

Then we have

$$F(x) + F(x+a) + F(y) + F(y+a) + f(x) + f(x+a) + f(y) + f(y+a) = 0,$$

or equivalently,

$$F(x) + F(x+a) + F(y) + F(y+a) = f(x) + f(x+a) + f(y) + f(y+a).$$

These can only be equal when $F(x) + F(x+a) + F(y) + F(y+a) = b$ for some $b \in B$. So, $F(x)+f(x)$ is APN if and only if $F(x)+F(x+a)+F(y)+F(y+a) \neq b$ for all x, y, a in $\mathbb{F}_{2^n}$ with $a \neq 0$ such that $f(x)+f(x+a)+f(y)+f(y+a) = b \in B$, $F(x)+F(x+a)+F(y)+F(y+a) \neq b$. □

Let $\{u_1, u_2, \ldots, u_k\}$ be a basis for B and consider a basis for $\mathbb{F}_{p^n}$, $\{u_1 = b_1, u_2 = b_2, \ldots, u_k = b_k, b_{k+1}, \ldots, b_n\}$. If we represent $F(x)$ and $f(x)$ in their coordinate function form with respect to their bases as $F(x) = (f_1(x), \ldots, f_n(x))$ and $f(x) = (g_1(x), \ldots g_k(x))$, then the coordinate function form of $F(x) + f(x)$ is

$$(f_1(x) + g_1(x), f_2(x) + g_2(x), \ldots, f_k(x) + g_k(x), f_{k+1}(x), \ldots, f_n(x)).$$

So, we can consider the extended switching technique as a condition on how to change multiple coordinates of an APN function to obtain another APN function. Thus Theorem 1.9.2 is a consequence of our Theorem 2.1.1. We can, in fact, obtain the following generalization of Theorem 1.9.2.

Theorem 2.1.2. *Let $F \in \mathbb{F}_{2^n}[X]$ be a DO APN polynomial and $f \in \mathbb{F}_{2^n}[X]$ be a DO polynomial from $\mathbb{F}_{2^n}$ to B where B is a k dimensional subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. The polynomial $F + f$ is APN if for every $a \in \mathbb{F}_{2^n}^*$ there exists a linear function $l_a : \mathbb{F}_{2^n} \to B$ satisfying*

i. $\Delta_{f,a}(x) = l_a(\Delta_{F,a}(x))$, *and*

ii. if there exists $x \in \mathbb{F}_{2^n}$ such that $\Delta_{F,a}(x) = y \in B$ with $y \neq 0$, then $l_a(y) \neq y$.

Proof. Since $F(x) + f(x)$ is a DO polynomial, then we only need to determine the roots of $\Delta_{F+f}(x, a)$ for all nonzero $a \in \mathbb{F}_{2^n}^*$. If there are at most two solutions, then the function is APN. By (i), we have

$$\begin{aligned} 0 &= \Delta_{F+f}(x, a) \\ &= \Delta_F(x, a) + \Delta_f(x, a) \\ &= \Delta_F(x, a) + l_a(\Delta_F(x, a)). \end{aligned}$$

By (ii), this only occurs when $\Delta_F(x, a) = 0$. Since $F(x)$ is APN we know there are only 2 solutions, namely $x = 0$ and $x = a$. Hence, $F(x) + f(x)$ is APN. □

2.2 Coordinate Functions and Orthogonal Systems

Motivated by the correspondence between planar functions and maximal orthogonal systems, we now investigate what happens to planar functions when we consider them as orthogonal systems and alter the coordinate functions.

Theorem 2.2.1. *Changing any k coordinate functions of a planar function $f(x)$ over $\mathbb{F}_{p^n}$ gives us a function that is at most p^k-DU.*

Proof. Consider $f(x) = (f_1(x), \ldots, f_n(x))$ as a planar function over $\mathbb{F}_{p^n}$ in coordinate function form. Without loss of generality, suppose we replace the last k coordinate functions in the following way:

$$g(x) = (f_1(x), \ldots, f_{n-k}(x), g_{n-k+1}(x), \ldots, g_n(x)).$$

Then, the difference polynomial of g is

$$\Delta_g(x, a) = (\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a), \Delta_{g_{n-k+1}}(x, a), \ldots, \Delta_{g_n}(x, a)).$$

The set $\{\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a)\}$ still forms a mutually orthogonal system but it is no longer maximal. This means that for $\alpha_1, \ldots \alpha_{n-k} \in \mathbb{F}_p$ there exists p^k solutions to

$$\Delta_{f_1}(x, s) = \alpha_1, \ldots, \Delta_{f_{n-k}}(x, a) = \alpha_{n-k}.$$

So when $(\alpha_1, \dots \alpha_n) \in \mathbb{F}_{p^n}$, the maximum number of solutions to

$$(\Delta_{f_1}(x,a), \dots, \Delta_{f_{n-k}}(x,a), \Delta_{g_{n-k+1}}(x,a), \dots, \Delta_{g_n}(x,a)) = (\alpha_1, \dots, \alpha_n)$$

is p^k. Specifically the elements satisfying

$$(\Delta_{f_1}(x,a), \dots, \Delta_{f_{n-k}}(x,a)) = (\alpha_1, \dots, \alpha_{n-k})$$

all also satisfy $\Delta_{g_{n-k+1}}(x,a) = \alpha_{n-k+1}, \dots, \Delta_{g_n}(x,a) = \alpha_n$. Hence, the new function g is at most p^k differential uniform. □

Corollary 2.2.2. *Let $f \in \mathbb{F}_q[X_1, \dots X_n]$ be a planar polynomial and consider its coordinate polynomials, $f_1, \dots, f_n \in \mathbb{F}_q[X_1, \dots, X_n]$. Fix i, j with $1 \leq i, j, \leq n$ and let $F_j \in \mathbb{F}_q[X_1, \dots, X_n]$ be the polynomial we obtain from removing all the terms involving X_i from coordinate function f_j. The function $F \in \mathbb{F}_q[X_1, \dots X_n]$ defined by $(f_1, \dots, f_{j-1}, F_j, f_{j+1}, \dots f_n)$ is p - DU.*

Proof. From Theorem 2.2.1, we know that this new function is at most differential p uniform. Without loss of generality, suppose we remove all terms involving x_n from f_n. Then when we consider $a = (0, \dots, 0, 1)$, the difference polynomials of the coordinate functions $f_i(x)$ are $f_1(x_1, \dots, x_{n-1}, x_n + 1) - f_1(x_1, \dots, x_n)$ for $i \in [1, \dots, n-1]$ and for f_n the difference polynomial is $f_n(x_1, \dots x_{n-1}) - f_n(x_1, \dots, x_{n-1}) = 0$. We know by properties of orthogonal systems that for any $(\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{F}_p^n$ there are p elements satisfying

$$\begin{aligned} f_1(x_1, \dots, x_{n-1}, x_n + 1) - f_1(x_1, \dots, x_n) &= b_1, \\ &\vdots \\ f_{n-1}(x_1, \dots, x_{n-1}, x_n + 1) - f_{n-1}(x_1, \dots x_n) &= b_{n-1}. \end{aligned}$$

So, the new function is p differentially uniform. □

2.3 Applications of Extended Switching Technique

We can also use the extended switching technique to get bounds on the differential uniformity of functions.

Theorem 2.3.1. *Let p be odd, $D : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a planar function, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Let $\Delta Max(F) := \max_{a \in \mathbb{F}_q^*} \#Im(\Delta_F(x, a))$. Then $f(X) = D(X) + F(X)$ is at most $\Delta Max(F)$-DU.*

Proof. The derivative of $f(x)$ in direction of a is

$$\Delta_f(x, a) = \Delta_D(x, a) + \Delta_F(x, a).$$

For a fixed $b \in \mathbb{F}_{p^n}$, we need to know the number of solutions to $\Delta_f(x, a) = b$. By the extended switching technique, we need to know when $\Delta_D(x, a) + b = \Delta_F(x, a)$. Since $D(x)$ is planar $\Delta_D(x, a) + b$ is a permutation. Therefore, we can bound the differential uniformity of $D(x) + F(x)$ by the maximum image size of $\Delta_F(x, a)$ which by definition is $\Delta Max(F)$. Thus, $f(x)$ is at most $\Delta Max(F)$-DU. □

From this last theorem we see that we can create a low differentially uniform function from a known planar function by adding a function whose difference function has a small image size.

It seems reasonable that we could use the Extended Switching Technique to obtain new APN functions. We have completed the following computational searches in search of APN functions that were inequivalent to known examples and that required the use of the extended switching technique; in other words, we tested to be sure that these functions did not use Dillon's switching technique inductively.

Recall that Gold functions are APN functions over $\mathbb{F}_{2^n}$ of the form x^{2^i+1} with $(i, n) = 1$. We have run code for small extensions to see how adding coordinate functions of a Gold function with coordinate functions from other Gold functions affects the differential uniformity.

First, fix a basis. We choose the basis $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{2^n-2}\}$. We started by deconstructing a Gold function, $f(x)$, into its coordinate functions $\{f_1(x), \ldots, f_n(x)\}$. Then we took two other Gold functions, $g(x)$ and $h(x)$, and wrote them in their coordinate function form $\{g_1(x), \ldots, g_n(x)\}$ and $\{h_1(x), \ldots, h_n(x)\}$ respectively. Note that $g(x)$ and $h(x)$ could be the same Gold function. We test the differential uniformity of the function that has coordinate functions $\{f_1(x) + g_1(x), f_2(x) + h_2(x), f_3(x), \ldots, f_n(x)\}$. For n from 3 to 12, we do not obtain

any new APN functions using this method. Similarly, we have computational data for adding three coordinate functions to a Gold function in a similar manner as above. For n from 4 to 9, we do not obtain any new APN functions.

We extended this computational search by adding coordinate functions of APN functions to the coordinate functions of another APN functions. We focused on the following known APN functions which you can find in Appendix B: Gold, Kasami, Welch, Niho, Inverse, Dobbertin, and the function from [14].

The computer search included the following:

- replace 2 coordinate function of any of the functions listed above with the corresponding 2 coordinate functions of any other function listed above with n from 4 to 8;
- replace 3 coordinate function of any of the functions listed above with the corresponding 3 coordinate functions of any other function listed above with n from 4 to 5;
- add 2 coordinate functions of Gold functions to a different Gold function for n from 3 to 10;
- add 2 coordinate functions of Kasami functions to a different Kasami function for n from 3 to 8;

These additional computational searches did not yield any new APN functions that are inequivalent to known examples. There are more known APN functions that you can see in Appendix B that could also be used in the search method above.

Chapter 3

LOW DIFFERENTIAL UNIFORM FUNCTIONS FROM ALGEBRAIC STRUCTURES

Let $S = (\mathbb{F}_q, +, *)$ be a commutative presemifield of odd order. Theorem 1.7.6 shows the polynomial $F(X) = X * X$ must be planar. Thus, commutative semifields give rise to low DU functions. Motivated by this connection, in this chapter, we replace commutative semifields with other well-structured algebraic objects and examine the DU of the function $x * x$. As shall be seen, though we do not find APN or planar function, we still obtain functions with low DU. Theorem 3.3.2 gives conditions on some of the Kantor presemifields to create functions that are 4 differentially uniform. In Theorem 3.4.3, we give a lower bound for the differential uniformity for the function $f(x) = x * x$ where the multiplication is from the regular planar nearfield $N(2, q^2)$ with q odd and we conjecture that this lower bound is the differential uniformity of these functions.

3.1 Albert's Generalized Twisted Fields

In Section 1.4.2 we defined Albert's Generalized Twisted fields. We want to investigate the differential uniformity of the function $f(x) = x * x$ using the twisted field multiplication. We note that the planar functions that we obtain computationally for order 3^5 were found by Weng, see Coulter and Kosick, [25]. In addition, all of the planar functions that we obtain computationally for order 7^3 are known as all must correspond to either a finite field or Albert's twisted field.

Table 3.4 gives the differential uniformities for specific primes p and extension n. Since c runs through the elements of $\mathbb{F}_{p^n}$ that satisfy the properties in Section 1.4.2, the frequency column notes the number of c's that yield functions that correspond to that specific differential uniformity.

Table 3.1: Differential Uniformity of $f(x) = x * x$ with multiplication from Albert's Generalized Twisted Fields.

p	n	δ	frequency
3	3	3	13
3	4	3	120
3	5	1 3 9	11 473 242
3	6	3 9	1768 2145
3	7	3 9	6558 9837
3	8	3 9	19760 56500
5	3	5 25	62 31
5	4	5	1404
5	5	1 5 25	71 6621 7384
7	3	1 7 49	38 228 19
7	4	7 49	5520 480
11	3	11 121	1064 133

Let p be an odd prime and $n > 2$. Given automorphisms $x \rightarrowtail x^{p^i}$ and $x \rightarrowtail x^{p^j}$ and a $c \in \mathbb{F}_{p^n}$ satisfying the conditions in Section 1.4.2, then $f(X) = X^2 - cX^{p^i+p^j}$. Therefore, the difference polynomial is $\Delta_f(X, a) = 2aX - c[X^{p^i}a^{p^j} + X^{p^j}a^{p^i}]$. Since $f(X)$ is a DO polynomial then we want to know how many solutions to $\Delta_f(x, a) = 0$; equivalently, the number of solutions to

$$2ax = c[x^{p^i}a^{p^j} + x^{p^j}a^{p^i}].$$

For every $b \in \mathbb{F}_{p^n}$ there exists an $x \in \mathbb{F}_{p^n}$ such that $2ax = b$, specifically $x = 2^{-1}a^{-1}b$. We want to know the number of elements in $\mathbb{F}_{p^n}$ such that

$$-b = c[(2^{-1}a^{-1}b)^{p^j}a^{p^i} + (2^{-1}a^{-1}b)^{p^i}a^{p^j}]. \tag{3.1}$$

When we rearrange Equation 3.1 we get $-2c^{-1} = a^{p^i-p^j}b^{p^j-1} + a^{p^j-p^i}b^{p^i-1}$. For a fixed $a, c \in \mathbb{F}_q$ with $a \neq 0$, we want the number of solutions in $\mathbb{F}_q$ of

$$-2c^{-1} = a^{p^i-p^j}x^{p^j-1} + a^{p^j-p^i}x^{p^i-1}. \tag{3.2}$$

From our discussion above, we get the following theorem.

Theorem 3.1.1. *Given a non-commutative generalized twisted field $A = (\mathbb{F}_{p^n}, +, *)$, the differential uniformity of $f(x) = x * x$ is*

$$\max_{a \in \mathbb{F}^*_{q^n}} \#\{\gamma : \gamma \in \mathbb{F}_{q^n} | -2c^{-1} = a^{p^i-p^j}\gamma^{p^j-1} + a^{p^j-p^i}\gamma^{p^i-1}\},$$

where $x * y = xy + cx^{p^i}y^{p^j}$.

We note here that if we loosen our restrictions and allow one of the automorphisms to be the identity, say $j = 0$, then Equation 3.2 can be simplified to $[-2c^{-1} - a^{p^i-1}]a^{p^i-1} = b^{p^i-1}$. In this case, we want to determine the number of solutions in $\mathbb{F}_q$ of the equation

$$[-2c^{-1} - a^{p^i-1}]a^{1-p^i} = x^{p^i-1}$$

for any natural number $i < n$. For a fixed element of $\mathbb{F}_q = \mathbb{F}_{p^n}$ there is either 0 or $p^{\gcd(n,i)} - 1$ solutions. For example, if n is even, $j = 0$, and $i = \frac{n}{2}$, then the differential uniformity of f is $p^{\frac{n}{2}}$.

We also note that if $i = j$ then $f(X) = X^2 + cX^{2p^i}$. So, $f(X) = l(X^2)$ where $l(X) = X + cX^{p^i}$. Since $l(X)$ is a linearized polynomial, the differential uniformity of $f(X)$ is exactly the number of roots of $l(X)$. If $l(X)$ is a permutation polynomial, then $f(X)$ is linearly equivalent to X^2.

We can use Theorem 2.3.1 to bound the differentially uniformity of $f(X)$ obtained from specific generalized twisted fields. The bound is nontrivial only if n is even, $j \neq i$, and $\frac{n}{(j-i,n)}$ is even.

Theorem 3.1.2. *Suppose $(\mathbb{F}_{p^n}, +, *)$ is a generalized twisted field described in Section 1.4.2 where n is even, $j \neq i$, and $\frac{n}{(j-i,n)}$ is even. Then the differential uniformity of $f(x) = x * x$ is bounded above by $p^{n-(j-i,n)}$.*

Proof. The function is

$$\begin{aligned} f(x) &= x^2 - cx^{p^j+p^i} \\ &= x^2 - c(x^{p^{j-i}+1})^{p^i}. \end{aligned}$$

We have that $D(x) = x^2$ and $F(x) = L(G(x))$ where $L(x) = -cx^{p^i}$, and $G(x) = x^{p^{j-i}+1}$. Since $\frac{n}{(j-i,n)}$ is even, $G(x)$ is semiplanar of index $p^{(j-i,n)}$ from Theorem 1.7.4. Therefore, the image size of $F(x)$ is $p^{n-(j,i)}$ and by Theorem 2.3.1 the differential uniformity of $f(x)$ is at most $p^{n-(j-i,n)}$. □

You can see a comparison between the bound in Theorem 3.1.2 and the actual differential uniformity for characteristic 3 and $3 \leq n \leq 8$ in Table 3.2. These are very loose bounds that we have obtained from Theorem 2.3.1. Note that the dimension of the bounds is the same regardless of the characteristic.

3.2 Arbitrary Semifields of Characteristic Two

Suppose q is a power of two we have a semifield of the form $S = (\mathbb{F}_q, +, *)$ and consider $f(x) = x * x$ over $\mathbb{F}_q$. The difference function of f is $\Delta_f(x, a) = x * a + a * x$. If $a = 1$ then $\Delta_f(x, 1) = 0$. So, $f(x)$ is q differential. More generally, for all elements $a \in Z(S)$, $\Delta_f(x, a) = 0$.For $a \in \mathbb{F}_q \setminus Z(G)$, the number of solutions to $\Delta_f(x, a) = 0$ is the size of the

Table 3.2: Comparison of the bound in Theorem 3.1.2 and corresponding differential uniformity of functions from Albert's Generalized Twisted Fields for characteristic 3 for $3 \leq n \leq 8$.

p	n	i	j	$j-i$	$\frac{n}{(j-i,n)}$	bound $= p^{n-(j-i,n)}$	δ(s)
3	4	1	2	1	$\frac{4}{(1,4)} = 4$	$3^{4-1} = 3^3$	3
3	4	1	3	2	$\frac{4}{(2,4)} = 2$	$3^{4-2} = 3^2$	3
3	4	2	3	1	$\frac{4}{(1,4)} = 4$	$3^{4-1} = 3^3$	3
3	6	1	2	1	$\frac{6}{(1,6)} = 6$	$3^{6-1} = 3^5$	3
3	6	1	4	3	$\frac{6}{(3,6)} = 2$	$3^{6-3} = 3^3$	3
3	6	2	3	1	$\frac{6}{(1,6)} = 6$	$3^{6-1} = 3^5$	9
3	6	2	5	3	$\frac{6}{(3,6)} = 2$	$3^{6-3} = 3^3$	3
3	6	3	4	1	$\frac{6}{(1,6)} = 6$	$3^{6-1} = 3^5$	9
3	6	3	5	2	$\frac{6}{(2,6)} = 3$	$3^{6-2} = 3^3$	9
3	6	4	5	1	$\frac{6}{(1,6)} = 6$	$3^{6-1} = 3^6$	3
3	8	1	2	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	3
3	8	1	3	2	$\frac{8}{(2,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	1	4	3	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	3, 9
3	8	1	5	4	$\frac{8}{(4,8)} = 4$	$3^{8-4} = 3^4$	3
3	8	1	6	5	$\frac{8}{(5,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	1	7	6	$\frac{8}{(6,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	2	3	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	2	4	2	$\frac{8}{(2,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	2	5	3	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	3
3	8	2	6	4	$\frac{8}{(4,8)} = 2$	$3^{8-4} = 3^4$	9
3	8	2	7	5	$\frac{8}{(5,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	3	4	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	3	5	2	$\frac{8}{(2,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	3	6	3	$\frac{8}{(3,8)} = 8$	$3^{8-1} = 3^7$	3
3	8	3	7	4	$\frac{8}{(4,8)} = 2$	$3^{8-4} = 3^4$	3
3	8	4	5	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	4	6	2	$\frac{8}{(2,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	4	7	3	$\frac{8}{(3,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	5	6	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	9
3	8	5	7	2	$\frac{8}{(2,8)} = 4$	$3^{8-2} = 3^6$	9
3	8	6	7	1	$\frac{8}{(1,8)} = 8$	$3^{8-1} = 3^7$	3

Table 3.3: Differential Uniformity of $f(x) = x * x$ where $*$ is Kantor's presemifield multiplication defined in Section 1.4.3.

Size of the field	Chain of Subfields	Sequence of elements in $\mathbb{F}_{2^n}$	Differential Uniform
2^3	$\mathbb{F}_2 \subset \mathbb{F}_{2^3}$	1	2
2^3	$\mathbb{F}_2 \subset \mathbb{F}_{2^3}$	$g, g^2, g^3, g^4, g^5, g^6$	4
2^5	$\mathbb{F}_2 \subset \mathbb{F}_{2^5}$	every element of $\mathbb{F}_{2^5}^*$	4
2^7	$\mathbb{F}_2 \subset \mathbb{F}_{2^7}$	every element of $\mathbb{F}_{2^7}^*$	4
2^9	$\mathbb{F}_2 \subset \mathbb{F}_{2^9}$	every element of $\mathbb{F}_{2^9}^*$	4
2^9	$\mathbb{F}_2 \subset \mathbb{F}_{2^3} \subset \mathbb{F}_{2^9}$	see the appendix	4
		see the appendix	8
		see the appendix	16

centralizer of a. For $a \neq 1$ in $\mathbb{F}_q$, the number of solutions to $\Delta_f(x, a) = 0$ is bounded below by 4 for all $a \in \mathbb{F}_q$, because $\Delta_f(1, a) = 1 * a + a * 1 = a + a = 0$. So even if we restrict to $\mathbb{F}_q \setminus \mathbb{F}_2$, we sill get a function which is at least 4-DU.

3.3 Kantor's Presemifields of Characteristic Two

In Section 1.4.3 we defined the Kantor presemifield. We want to investigate the function $f(x) = x * x$ using the multiplication defined in Section 1.4.3. In Table 3.3 we give computational results that we have obtained using MAGMA.

Theorem 3.3.1. *Consider the presemifield $(\mathbb{F}_{2^3}, +, *)$ defined by Section 1.4.3 with $F_0 = \mathbb{F}_2$, $F_1 = \mathbb{F}_{2^3}$, and $a_1 = 1$. The function $f(x) = x * x$ is APN and linearly equivalent to x^5.*

Proof. The function $f(x)$ is

$$\begin{aligned} x^3 + Tr(x)x + Tr(x) &= x^3 + x^2 + x^3 + x^5 + \mathrm{Tr}(x) \\ &= x^5 + x^2 + \mathrm{Tr}(x) \end{aligned}$$

Since $f(x)$ is affine equivalent to x^5, which is a Gold function, $f(x)$ is APN. □

Theorem 3.3.2. *Consider the presemifield $(\mathbb{F}_{2^n}, +, *)$ defined by Section 1.4.3 where $n > 3$ is odd and the chain of fields is $F_0 = \mathbb{F}_2$ and $\mathbb{F}_{2^n} = F_1$ with $a_1 \in \mathbb{F}_{2^n}^*$. The function $f(x) = x * x$ is at most 4-DU . Furthermore, if $a_1 \neq 1$, then f is 4-DU.*

Proof. We note that $f(X) = X^3 + \mathrm{Tr}(a_1X)X + a_1\,\mathrm{Tr}(X)$ is affine equivalent to $g(X) = X^3 + X\,\mathrm{Tr}(a_1X)$; therefore, we need only investigate the differential uniformity of $g(X)$. We have $\Delta_g(X, a) = X^2a + a^2X + a\,\mathrm{Tr}(a_1X) + x\,\mathrm{Tr}(a_1a)$. We will use the extended switching technique (Theorem 2.1.1) to determine the differential uniformity. Since $g(X)$ is a DO polynomial we want to determine the number of solutions to

$$x^2a + a^2x = a\,\mathrm{Tr}(a_1x) + x\,\mathrm{Tr}(a_1a).$$

Set $b = x^2a + a^2x$. Clearly, $x = 0$ and $x = a$ are always solutions and they correspond to $x^2a + a^2x = 0$. For the remainder we assume $b \neq 0$ and $x \in \mathbb{F}_{2^n} \setminus \{0, a\}$. Regardless of the value of $\mathrm{Tr}(a_1a)$, $x = b$ or $x = b + a$ and replacing b with ether of these results in a quadratic equation in x. Thus, there are at most 2 more solutions for a total of at most 4 solutions to $x^2a + a^2x = a\,\mathrm{Tr}(a_1x) + x\,\mathrm{Tr}(a_1a)$. Thus the differential uniformity of $f(X)$ is at most 4.

To prove that f is 4-DU when $a_1 \neq 1$ we need only produce an element $a \in \mathbb{F}_{2^n}^*$ such that

$$x^2a + a^2x = a\,\mathrm{Tr}(a_1x) + x\,\mathrm{Tr}(a_1a) \tag{3.3}$$

has 4 solutions. There are two cases when $\mathrm{Tr}(a_1) = 1$ or $\mathrm{Tr}(a_1) = 0$.

Case 1**:** When $\mathrm{Tr}(a_1) = 1$ set $a = a_1^{-1}$. Then Equation (3.3) reduces to

$$0 = x^2 + (a_1 + a_1^{-1})x + \mathrm{Tr}(a_1x).$$

It is easily verified that $x = 0, a_1, a_1^{-1}, a_1 + a_1^{-1}$ are solutions. If $a_1 \neq 1$, then these are four distinct solutions and thus f is 4-DU.

Case 2**:** Suppose $\mathrm{Tr}(a_1) = 0$. If $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_2$ satisfies $\mathrm{Tr}(a_1\alpha) = \mathrm{Tr}(a_1\alpha^{-1}) = 1$, set $a = \alpha^+\alpha^{-1}$. Note $\mathrm{Tr}(a_1a) = 0$. We may again verify that $x = 0, \alpha, \alpha^{-1}, a$ are solutions to Equation (3.3). If α exists, f is 4-DU.

Let $T_i(a_1) = \{\alpha \in \mathbb{F}_q : \mathrm{Tr}(a_1\alpha) = i\}$ for $i = 0, 1$. Now $|T_i(a_1)| = 2^{n-1}$ and $0, 1 \in T_0(a_1)$. Furthermore, the only element in $\mathbb{F}_q$ which is its own multiplicative inverse is 1. Thus, if there were no pairs α, α^{-1} contained in $T_1(a_1)$, then we would have $|\{\alpha^{-1} : \alpha \in T_1(a_1)\}| = 2^{n-1} < 2^{n-1} - 2$, a clear contradiction. Hence there must exist an $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_2$ for which $\mathrm{Tr}(a_1\alpha) = \mathrm{Tr}(a_1\alpha^{-1}) = 1$, and the theorem is proved.

□

Theorem 3.3.3. *Consider the presemifield $(\mathbb{F}_{2^n}, +, *)$ defined by Section 1.4.3 where n is odd and the chain of fields is $K = \mathbb{F}_2 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots \subsetneq F_k = \mathbb{F}_{2^m} \subsetneq F = \mathbb{F}_{2^n}$ with m odd and $a_1, a_2, \ldots, a_k \in \mathbb{F}_{2^n}^*$. The function $f(x) = x * x$ has differential uniformity at most 2^{m+1}.*

Proof. The polynomial we are considering is $f(X) = X^3 + X\sum_{i=1}^{k} \mathrm{Tr}_i(a_i X) + \sum_{i=1}^{k} a_i \mathrm{Tr}(X^2)$. The difference polynomial is $\Delta_f(x, a) = x^2a + a^2x + a\sum_{i=1}^{k} \mathrm{Tr}(a_i x) + x\sum_{i=1}^{k} \mathrm{Tr}(a_i a)$. We already know that 0 and a are roots of this difference polynomial. Set $b = x^2a + a^2x$ with $x \in \mathbb{F}_{2^n}$.If x satisfies $\Delta_g(x, a) = 0$, then $a\sum_{i=1}^{k} \mathrm{Tr}(a_i x) + x\sum_{i=1}^{k} \mathrm{Tr}(a_i a) = b$.

We have two cases, either $\sum_{i=1}^{k} \mathrm{Tr}(a_i x) = 0$ or not.

Case 1: If $\sum_{i=1}^{k} \mathrm{Tr}(a_i x) = 0$. then $b = \alpha x$ for some $\alpha \in \mathbb{F}_{2^m}^*$. Solving for x we get $\alpha a^{-1} + a = x$. Hence, in this case there are at most 2 more roots of $\Delta_g(x, a)$ namely, $\alpha a^{-1} + a$ and αa^{-1}. So, in this case there are at most 4 roots to $\Delta_f(x, a)$.

Case 2: If $\sum_{i=1}^{k} \mathrm{Tr}(a_i x) = \beta \in \mathbb{F}_{2^m}^*$, then $b = \alpha x + \beta a$ where $\alpha \in \mathbb{F}_{2^m}$. Rearranging the equation $b = ax^2 + a^2x$ we find that the roots of $\Delta_g(x, a)$ are the roots of $x^2 + (a + \alpha a^{-1})x + \beta$. There are at most two solutions for each $\beta \in \mathbb{F}_{2^m}^*$ to add to the solution set. Hence the differential uniformity is at most 2^{m+1}. □

This result means that we can create relatively low differentially uniform functions with respect to the field size using this method. Given a large extension n and a small divisor, m, of n with arbitrary choice of $(a_1, \ldots, a_k) \in (\mathbb{F}_{2^n}^*)^k$, we can create a function that is at most 2^{m+1} differentially uniform.

3.4 Nearfields

In this section we consider the function $f(x) = x * x$ where we use nearfield multiplication, see Section 1.5. Using Theorem 1.2.1 we can write f as s polynomial.

Theorem 3.4.1. *Consider a regular nearfield $N(n, q)$. The polynomial representation of the function $f(x) = x * x$ is*

$$f(X) = \frac{-q^n + 1}{n} \sum_{j=0}^{n-1} \sum_{i=1}^{n} (c^{\frac{-q^j+1}{q-1}} X)^{\frac{q^n-1}{n} i} X^{q^j+1}.$$

Proof. Let the indicator function for the multiplicative co-set c_iC be denoted as $I_{c_i}(x)$. We can write $f(x)$ terms of the indicator functions as

$$f(x) = \sum_{j=0}^{n-1} I_{c_j}(x) x^{q^j+1}. \tag{3.4}$$

Since $m = \frac{q^n-1}{n}$, $I_{c_j}(x) = \frac{-q^n-1}{n}(h_n(c_j^{-1}x)^{\frac{q^n-1}{n}} - 1)$ from Theorem 1.2.1. Replacing $h_n(x)$ with $1 + x + x^2 + \ldots x^n$, the indicator function can be represented by the polynomial

$$\frac{-q^n - 1}{n} \sum_{i=0}^{n} (c_j^{-1}X)^{\frac{q^n-1}{n} i}. \tag{3.5}$$

When we substitute Equation 3.5 into Equation 3.4, we obtain the desired result. □

The Table 3.4 gives computational results for the differential uniformity of $f(x)$ for a given regular nearfield.

3.4.1 The Exceptional Nearfield

The exceptional nearfield is $N(2, 3)$. Using MAGMA we find that

$$f(X) = X^8 + 2X^6 + 2X^4 + 2X^2 = X^8 + 2\,\mathrm{Tr}(X^2) + \mathrm{Tr}(X^4)(\mod X^q - X)$$

over $\mathbb{F}_{3^2}$. We now show that f is 7-DU.

Proof. The polynomial f can be written as a pieciewise function in the following way

$$f(x) = \begin{cases} 0 & x = 0 \\ 1 & x \in \mathbb{F}_3^* \\ 2 & x \in \mathbb{F}_9 \setminus \mathbb{F}_3 \end{cases}.$$

Let $a \in \mathbb{F}_3^*$, then

$$\Delta_f(x, a) = \begin{cases} 0 & x \in \mathbb{F}_3 \setminus \{a\} \\ -1 & x \in \mathbb{F}_9 \setminus \mathbb{F}_3 \cup \{a\} \end{cases}.$$

Table 3.4: Differential Uniformity of $f(x) = x * x$ with multiplication from the regular nearfield $N(n, q)$.

q	n	δ
q	2	$\frac{q+1}{2}$ *
3	2	7 **
5	2	4
5	4	4
7	2	9
7	3	6
11	2	11
13	2	8
13	3	8
13	4	8
17	2	9
17	4	9
19	2	5
19	3	9
23	2	17
25	3	12
27	2	19
29	2	15
31	2	21
37	2	19
81	2	41

* See Conjecture 3.4.2.

** This is the exceptional nearfield. See Section 3.4.1.

So, when $a \in \mathbb{F}_3^*$ and $b = -1$ there are 7 solutions to $\Delta_f(x, a) = b$. When $b \neq -1$ then there are fewer than 7 solutions. On the other hand, when $a \in \mathbb{F}_9 \setminus \mathbb{F}_3$, then

$$\Delta_f(x,a) = \begin{cases} 0 & x \in \{0, 1-a, 2-a\} \\ -1 & x \in \mathbb{F}_3^* \\ -2 & x \in \mathbb{F}_9 \setminus (\mathbb{F}_3 \cup \{1-a, 2-a\}) \end{cases}.$$

Therefore, when $a \in \mathbb{F}_9 \setminus \mathbb{F}_3$ and $b \in \mathbb{F}_9$ there are less than 7 solutions. Hence, f is 7-DU. □

3.4.2 Nearfields of the Form $N(2s, p^{2t})$

We next consider the regular nearfields $N(2s, q)$ where $q = p^{2t}$ for some odd prime p and integers $t, s \geq 1$. Consider the function $f(x) = x * x$ where $*$ is the multiplication on this nearfield. We make the following conjecture.

Conjecture 3.4.2. *The function $f(x)$ defined above is $\frac{q+1}{2}$ differentially uniform.*

In support of our conjecture, we prove that the DU of f can be no smaller than $\frac{q+1}{2}$.

Theorem 3.4.3. *When $s = 1$ $f(x)$ defined above is at least $\frac{q+1}{2}$ differentially uniform.*

This proof will require the following obvious lemma and corollary.

Lemma 3.4.4. *Let q be odd then, $4k \not\equiv 4j+r \pmod{q^2-1}$ for any integers k, j and $0 < r < 4$.*

We immediately get the following corollary which is a necessary condition for Conjecture 3.4.2.

Corollary 3.4.5. *Consider h to be the generator of the multiplicative group of $\mathbb{F}_{q^2}$. Then, for any integers k and j, $h^{4k} \neq h^{4j+2}$.*

The following lemmas are joint work with Fain during our dissertation studies.

Lemma 3.4.6. *Let $\mathrm{Tr}_{q^2/q}(X) = X^q + X$ be trace function of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ for odd prime power q. If $q \equiv 1 \pmod 4$, the kernel of $\mathrm{Tr}_{q^2/q}(X)$ is the set of $q-1$ non-square elements of $\mathbb{F}_{q^2}$ and 0 and if $q \equiv -1 \pmod 4$ the kernel of $\mathrm{Tr}_{q^2/q}(X)$ is a set of squares and 0.*

Proof. Suppose $\mathrm{Tr}_{q^2/q}(\beta) = 0$. Then $\beta^q + \beta = \beta(\beta^{q-1} + 1) = 0$. If $\beta \neq 0$, then $\beta^{q-1} = -1$. So,

$$\beta^{(q^2-1)/2} = (\beta^{q-1})^{(q+1)/2} = (-1)^{(q+1)/2}.$$

Thus β is a square if $q \equiv -1 \pmod 4$ and a non-square if $q \equiv 1 \pmod 4$. □

As a generalization we have the following lemma.

Lemma 3.4.7. *Let $L(x) = \mathrm{Tr}_{q^2/q}(a^q x) = ax^q + a^q x$ be a function over $\mathbb{F}_{q^2}$ for odd prime power q and non-zero a in $\mathbb{F}_{q^2}$. If $L(\beta) = 0$, then either $\beta = 0$ or $\eta_{q^2}(\beta) = -\eta_q(-1)\eta_{q^2}(a)$.*

Proof. Suppose $L(\beta) = 0$. Then $a\beta^q + a^q\beta = a\beta(\beta^{q-1} + a^{q-1}) = 0$. If $\beta \neq 0$, then $\beta^{q-1} = -a^{q-1}$. So,

$$\eta_{q^2}(\beta) = (\beta^{q-1})^{(q+1)/2} = (-a^{q-1})^{(q+1)/2} = (-1)^{(q+1)/2}\eta_{q^2}(a).$$

Thus $\eta_{q^2}(\beta) = \eta_{q^2}(a)$ if $q \equiv -1 \pmod 4$ and $\eta_{q^2}(\beta) = -\eta_{q^2}(a)$ if $q \equiv 1 \pmod 4$. □

Lemma 3.4.8. *Let q be an odd prime power. If $\mathrm{Tr}_{q^2/q}(\beta) = 0$ then $\eta_{q^2}(\beta + 1) = \eta_{q^2}(\beta - 1)$.*

Proof. Consider the following relationship:

$$\begin{aligned}(x+1)^{q+1} - (x-1)^{q+1} &= (x^q + 1)(x + 1) - (x^q - 1)(x - 1) \\ &= x^{q+1} + x^q + x + 1 - x^{q+1} + x^q + x - 1 \\ &= 2(x^q + x) \\ &= 2\,\mathrm{Tr}_{q^2/q}(x)\end{aligned}$$

Therefore, if $\mathrm{Tr}_{q^2/q}(\beta) = 0$ then $(\beta+1)^{q+1} - (\beta-1)^{q+1} = 0$. Thus, $(\beta+1)^{q+1} = (\beta-1)^{q+1}$. Raising both sides to the $\frac{q-1}{2}$ we get that $\eta_{q^2}(\beta + 1) = \eta_{q^2}(\beta - 1)$. □

Lemma 3.4.9. *The equation $\mathrm{Tr}_{q^2/q}(x) = 0$ has q solutions. When $q \equiv 1 \pmod 4$ the $q - 1$ nonzero solutions, α, are non-squares and $(q - 1)/2$ are such that $\alpha + 1$ are squares and $(q - 1)/2$ such that $\alpha + 1$ being a non-square. When $q \equiv -1 \pmod 4$ then the $q - 1$ nonzero solutions, α, are squares and $(q - 1)/2$ are such that $\alpha + 1$ are squares and $(q - 1)/2$ such that $\alpha + 1$ being a non-square.*

Proof. Since $q \equiv 1 \pmod 4$ we know that the non-zero elements of the kernel of $\mathrm{Tr}_{q^2/q}(x)$ are non-squares from Lemma 3.4.6. The kernel of $\mathrm{Tr}_{q^2/q}(x)$ is a on dimensional subspace of $\mathbb{F}_q$ and we can denote it as $\overline{\beta}$ where β is a nonzero element in the kernel. Then we want to investigate the quadratic character of $\alpha + 1 = k\beta + 1$. We can divide $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$ into q one dimensional subspaces, $\overline{\beta + \lambda}$ for $\lambda \in \mathbb{F}_q^*$. The members of the same subspace will have the same quadratic character; thus $(q-1)/2$ of them are sets of squares and $(q+1)/2$ are sets of non-squares. The set $\{k\beta + 1 \mid k \in \mathbb{F}_q^\star\}$ intersects each of these subspaces, other than the space $\overline{\beta}$, exactly once. Since $\overline{\beta}$ is a set of non-square then the number of solutions to $\mathrm{Tr}_{q^2/q}(\alpha) = 0$ remove zero divides evenly into $\frac{q-1}{2}$ elements such that $\alpha + 1$ is a non-square and $\frac{q-1}{2}$ elements such that $\alpha + 1$ is a square.

The proof for $q \equiv -1 \pmod 4$ is the same as above except the kernel of the elements of $\mathrm{Tr}_{q^2/q}$ are squares from Lemma 3.4.6. □

Now, we will prove Theorem 3.4.3.

Proof. We consider the derivative $D_f(x, a)$ in place of the difference function $\Delta_f(x, a)$.

Suppose a is a nonzero element in $\mathbb{F}_{p^{4t}}$. We have four cases, based on if x and $x + a$ are each squares or not. We outline the cases below.

1. If x and $x + a$ are squares, then, $D_f(x, a) = (x + a)^2 - x^2 = 2ax + a^2$.
2. If x is a square and $x + a$ is not a square, then, $D_f(x, a) = (x + a)^{q+1} - x^2 = x^{q+1} + x^q a + a^q x + a^{q+1} - x^2$.
3. If $x + a$ is a square and x is not a square, then, $D_f(x, a) = (x + a)^2 - x^{q+1} = x^2 + 2xa + a^2 - x^{q+1}$.
4. If x and $x + a$ is not squares, then, $D_f(x, a) = (x + a)^{q+1} - x^{q+1} = x^q a + a^q x + a^{q+1}$.

Each case corresponds to one of the S-sets which we know from Section 1.2.2 have sizes either $\frac{p^4-1}{4}$ or $\frac{p^4-1}{4} + 1$.

In Case 1, after we fix a $c \in \mathbb{F}_{q^2}$ we are solving $2xa + a^2 = c$. Solving this we obtain $x = 2^{-1}a^{-1}c - 2^{-1}a$. Case 1 only adds a solution if $2^{-1}a^{-1}c - 2^{-1}a$ and $2^{-1}a^{-1}c - 2^{-1}a + a$ are squares.

Similarly, Case 4 provides at most q solutions. In Case 4, $D_f(x, a) = a^q x + x^q a = D_{x^{q+1}}(x, a)$. Since $\frac{4t}{(4t,2t)} = \frac{4t}{2t} = 2$ is even x^{q+1} is semiplanar of index $p^{2t} = q$ by Theorem 1.7.4. So, there is at most q solutions. However, we need to determine how many of these solutions satisfy the conditions that x and $x + a$ must both be non-squares.

We will prove that the differential uniformity is at least $\frac{q+1}{2}$ by allowing $a = 1$ and $b = 0$. First, we have in Case 1 that $x = -2^{-1}$ and $x + 1 = 1 - 2^{-1}$; since both x and $x + 1$ are in $\mathbb{F}_q$ then they are squares in $\mathbb{F}_{q^2}$. So this will yield a solution.

Furthermore, we have that Case 2 and Case 3 yield no solutions. In Case 2 we get,

$$0 = (x + 1)^{q+1} - x^2, \text{or equivalently,}$$
$$x^2 = (x + 1)^{q+1}.$$

But, x is a square then $x = h^{2s}$ where h is the generator of the multiplicative group of $\mathbb{F}_q$ and s is an integer. On the other hand, $(x + 1)$ is a non-square then h^{2k+1} and k is an integer.

Since $q \equiv 1 \pmod 4$, the left hand side is

$$(h^{2s})^2 = h^{4s}$$

The right hand side is

$$\begin{aligned}(h^{2k+1})^{4j+1+1} &= h^{(2k+1)(4j+2)} \\ &= h^{8kj+4k+4j+2} \\ &= h^{4(2kj+k+j)+2}\end{aligned}$$

These cannot be the same by Corollary 3.4.5. So there are no solutions in this case.

Similarly, in Case 3 we get the following:

$$0 = (x+1)^2 - x^{p^2+1}$$
$$x^{q+1} = (x+1)^2$$

But, x is not a square then $x = h^{2s+1}$ where h is the generator of the multiplicative group of $\mathbb{F}_q$ and s is an integer. $(x+1)$ is a square then h^{2k} and k is an integer. Then the same argument above holds and there are no solutions in this case.

By Lemma 3.4.9, since $q = p^{2t} \equiv 1 \pmod 4$ there are $\frac{q-1}{2}$ solutions for Case 4. Therefore, there are a total of $\frac{q+1}{2}$ solutions to $D_f(x,1) = 0$. Hence, the differential uniformity of $f(x)$ is at least $\frac{q+1}{2}$. □

3.4.3 Computational Results for The Seven Irregular Nearfields

Using the MAGMA algebra package, we set up a correspondence between the elements of a given exceptional nearfield N_i of order p^2 and the finite field $\mathbb{F}_{p^2}$: this is done via the command `Element(N,a)`, where $a \in \mathbb{F}_{p^2}$. This then allows us to generate, through interpolation, a polynomial f_i that satisfies $f_i(x) = x * x$. The DU of that function is then computed.

Magma #	**Order**	$du(f)$
1	$25 = 5^2$	6
2	$121 = 11^2$	6
3	$49 = 7^2$	9
4	$529 = 23^2$	19
5	$121 = 11^2$	17
6	$841 = 29^2$	21
7	$3481 = 59^2$	25

So, in particular we see that for $i = 2$ and $i = 7$ we obtain functions with low DU. Indeed we obtain f with differential uniformity less than or equal to $\frac{p+1}{2}$ on fields of order p^2.

3.5 Permutation Property

Since low differentially uniform functions are desirable for designing substitution boxes, we are interested in the size of the set of pre-images of any fixed element in the field. Permutations are particularly desirable as the number of pre-images corresponds to the number of possible plaintext bits for the ciphertext output. Ideally, the function is a permutation so that decryption is considerably easier. However, there is usually a trade off between ease of decryption and security against differential cryptanalysis.

It is easy to see that the functions obtained from the nearfields and Albert's Twisted fields are even functions and thus not permutations. We know that the Kantor functions of the form $f(x) = x^3 + x\,\mathrm{Tr}(a_1 x) + a_1\,\mathrm{Tr}(x)$ are EA equivalent to $g(x) = x^3 + x\,\mathrm{Tr}(a_1 x)$ so we will investigate if either of these are permutations.

When $\mathrm{Tr}(a_1) = 1$ we know that $g(1) = 0 = g(0)$; thus, $g(x)$ is not a permutation if $\mathrm{Tr}(a_1) = 1$. It is not as easily seen for $g(x)$ when $\mathrm{Tr}(a_1) = 0$.

Theorem 3.5.1. *Consider the function $g(x) = x^3 + x\,\mathrm{Tr}(a_1 x)$ which is EA equivalent to the Kantor function seen in Theorem 3.3.2. Then $g(x)$ is not a permutation.*

Proof. We will consider $f(X)$ as the reduced polynomial of $g(X)$ and use Hermite's criterion (Theorem 1.3.1) to prove this theorem. Let $t = 2 + \sum_{i=0}^{\frac{n-3}{2}} 2^{2i}$. We will show that $f^t(X)$ has degree $q-1$ with leading coefficient $\alpha^{2^{n-1}}$.

First, we note that the absolute trace in characteristic 2 has the property that $\mathrm{Tr}(x)^k = \mathrm{Tr}(x)$ for any integer k. We also note that $f^t(X)$ has the form

$$\begin{aligned} f^t(X) &= (X^{2+1} + X\,\mathrm{Tr}(\alpha X))^t \\ &\equiv (X^{2+1} + X\,\mathrm{Tr}(\alpha X))(X^{4+2} + X^2\,\mathrm{Tr}(\alpha X)) \prod_{i=2}^{\frac{n-3}{2}} (X^{2^{2i+1}+2^{2i}} + X^{2^{2i}}\,\mathrm{Tr}(\alpha X)) \pmod{X^q - X}. \end{aligned}$$

Each term in the expanded form of $f^t(X)$ is constructed by choosing one of the two terms in each part of the product. We will let $A_0 = X^{2+1} + X\,\mathrm{Tr}(\alpha X)$, $A_1 = X^{4+2} + X^2\,\mathrm{Tr}(\alpha X)$, and $A_i = X^{2^{2i+1}+2^{2i}} + X^{2^{2i}}\,\mathrm{Tr}(\alpha X)$ for $i = 2, \ldots, \frac{n-3}{2}$. We want the degree of $f^t(X)$ to be $2^n - 1$ after reduction modulo $X^q - X$ which means that the coefficient of the X^{2^n-1} term is not zero.

Now $2^n - 1 = \sum_{i=0}^{n-1} 2^i$. The choices of terms from the A_is are powers of two which will yield an exponent that is a sum of powers of two. This restricts our choices.

Before taking into account the terms involving the trace function, the largest power of X you can choose to include in a particular term is $2^{n-2} + 2^{n-3}$ which is less than 2^{n-1}. So, the 2^{n-1} power must be obtained from the trace function. When we construct the terms for the expanded version of $f^t(X)$ the X^{2^n-1} term will be the result of a term that includes the absolute trace function. We also notice that each term in the absolute trace function will only add one power of two to the exponent. Therefore, we will only choose the term with the power 2^{n-1} from the trace function.

The A_1 term will always add at least 2 to the exponent of a particular term. Since the A_1 and A_0 terms offer the only way to choose a term that adds a 2 to the exponent. If we choose 2 in both of them then we get 4 instead and cannot construct the X^{2^n-1} term. This forces us to choose $X\,\mathrm{Tr}(\alpha X)$ from A_1. Similarly, we are also forced to choose $X^2\,\mathrm{Tr}(\alpha X)$ from A_1 as A_2 adds at least 4 to the power. When $i = 2, \cdots, \frac{n-3}{2}$ we are forced to choose $X^{2^{2i+1}+2^{2i}}$. Otherwise, we will miss an odd power of two for our exponent. Therefore, the coefficient of the X^{2^n-1} term in this polynomial is $\alpha^{2^{n-1}}$ from choosing $\alpha^{2^{n-1}} X^{2^{n-1}}$ from the $\mathrm{Tr}(\alpha X)$ term. Clearly, $\alpha^{2^{n-1}}$ is not zero; hence, $f(x)$ is not a permutation. □

When we consider the function $f(x) = x^3 + x\,\mathrm{Tr}(\alpha x) + \alpha\,\mathrm{Tr}(x)$ over $\mathbb{F}_{2^n}$ we find that there is an example of a permutation function. Computationally we found when $\alpha = 1$ and $n = 3$, f is a permutation.

Theorem 3.5.2. *The Kantor functions $f(x) = x^3 + x\,\mathrm{Tr}(\alpha x) + \alpha\,\mathrm{Tr}(x)$ over $\mathbb{F}_{2^n}$ with $n > 3$ and $\alpha \in \mathbb{F}_{2^n}^*$ are not permutations.*

Proof. We will use Hermite's criterion again; however, we must split the proof into two cases: $\alpha = 1$ and $\alpha \neq 1$.

Case 1: Let $\alpha \neq 1$ and $t = 1 + 4 + \sum_{i=0}^{\frac{n-5}{2}} 2^{2i+1}$. Then $f^t(X) \mod (X^q - X)$ is

$$(X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))(X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^4 \prod_{i=0}^{\frac{n-5}{2}} (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^{2^{2i+1}}.$$

Let $A_0 = (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))$, $A_1 = (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^4$ and for $i = 2 \cdots \frac{n-1}{2}$ let

$$A_i = (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^{2^{2(i-2)+1}} = (X^{2^{2(i-1)}+2^{2(i-2)+1}} + X^{2^{2(i-2)+1}}\,\mathrm{Tr}(\alpha X) + \alpha^{2^{2(i-2)+1}}\,\mathrm{Tr}(X)).$$

We want to determine the coefficient of the X^{2^n-1} term. Since the powers X in each part of the product of $f^t(X)$ are sums of powers of X, we will view n as $\sum_{i=0}^{n-1} 2^i$.

Before we consider the trace functions, the largest power of X that we can choose from any part of the product is $X^{2^{2(n-5/2+1)}} = X^{2^{n-3}}$. So, we will be forced to choose $X^{2^{n-2}}$ and $X^{2^{n-1}}$ from $\mathrm{Tr}(\alpha X)$ and $\mathrm{Tr}(X)$. In order to get terms of the form $X^{2^{2k}}$ for $k \geq 2$ we need to choose the term $X^{2^{2k}+2^{2(k-1)+1}}$ from A_{k+1}.

So, we have to make choices for A_0, A_1, and A_2 to get the X^{2^n-1} term. We are forced to choose either X^{2+1} or $X\,\mathrm{Tr}(\alpha X)$ from A_0 in order to get the 1 in the representation of $2^n - 1$ as a sum of powers of 2. From A_1 we are forced to choose $X^4\,\mathrm{Tr}(\alpha X)$ or $\alpha^4\,\mathrm{Tr}(X)$ to avoid getting $2(8)$ in the sum of powers of 2. The choice of A_2 is completely determined by the choices we make in A_0 and A_1.

Subcase 1: Suppose we choose the terms X^{2+1} and $X^4\,\mathrm{Tr}(\alpha x)$. Then we will choose $\alpha^2\,\mathrm{Tr}(X)$ from A_2. Then the coefficient on X^{2^n-1} is $\alpha^{2^{n-1}}\alpha^2 + \alpha^{2^{n-2}}\alpha^2 = \alpha^{2^{n-2}}\alpha^2(1+\alpha^2)$.

Subcase 2: Suppose we choose $X\,\mathrm{Tr}(\alpha X)$ and $\alpha^4\,\mathrm{Tr}(X)$ then we will choose X^{4+2} from A_2. So the coefficient of X^{2^n-1} is $\alpha^{2^{n-1}}\alpha^4 + \alpha^{2^{n-2}}\alpha^4 = \alpha^4\alpha^{2^{n-2}}(1+\alpha^2)$.

Then, the coefficient of X^{2^n-1} is

$$\alpha^{2^{n-2}}\alpha^2(1+\alpha^2) + \alpha^{2^{n-2}}\alpha^4(1+\alpha^2) = \alpha^{2^{n-2}}\alpha^2(1+\alpha^2)^2.$$

This is only zero if $\alpha = 0$ or $\alpha = 1$. Since, α is neither 0 nor 1 then the coefficient is non-zero. Therefore, the degree of $f^t(X)$ is $2^n - 1$ and $f(X)$ is not a permutation.

Case 2: Let $\alpha = 1$. When $n = 5$ then $t = 11$ and when $n > 5$, then $t = 11 + \sum_{i=2}^{\frac{n-3}{2}} 2^{2i}$.
Subcase 1: When $n = 5$ then $f^t(X) \pmod{X^q - X}$ is

$$(X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X))(X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X))(X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)).$$

Table 3.5: Choosing terms from A_0, A_1, and A_2 to obtain a X^{2^n-1} term.

Term from A_0	Term from A_1	Term from A_2	Choice from $\mathrm{Tr}(X)$	Coefficient
X^{2+1}	$X^2\,\mathrm{Tr}(X)$	X^{16+8}	X^2	1
X^{2+1}	$\mathrm{Tr}(X)$	X^{16+8}	X^4	1
$X\,\mathrm{Tr}(X)$	X^{4+2}	X^8	X^{16}	1
$X\,\mathrm{Tr}(X)$	$X^2\,\mathrm{Tr}(X)$	X^{16+8}	X^4	1
$\mathrm{Tr}(X)$	X^{4+2}	X^{16+8}	X	1

We will let

$$A_0 = (X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_1 = (X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)), \text{ and}$$
$$A_2 = (X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X))$$

There are 5 ways to choose terms to multiply to a term with exponent X^{2^n-1}; they are in the Table 3.5.

Summing we find the coefficient is 1. Hence, the degree of $f^t(X)$ is $2^n - 1$ and therefore, $f(X)$ is not a permutation.

Subcase 2: When $n > 5$ and $t = 11 + \sum_{i=2}^{\frac{n-3}{2}} 2^{2i}$. Then $f^t(X)$ is $(X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X))(X^{4+2}+X^2\,\mathrm{Tr}(X)+\mathrm{Tr}(X))(X^{8+16}+X^8\,\mathrm{Tr}(X)+\mathrm{Tr}(X))\prod_{i=2}^{\frac{n-3}{2}}\left(X^{2^{2i+1}+2^{2i}} + X^{2^{2i}}\,\mathrm{Tr}(X) + \mathrm{Tr}(X)\right)$.

We let

$$A_0 = (X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_1 = (X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_2 = (X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)), \text{ and}$$
$$A_i = (X^{2^{2(i-1)+1}+2^{2(i-1)}} + X^{2^{2(i-1)}}\,\mathrm{Tr}(X) + \mathrm{Tr}(X)) \text{ for } i \geq 3.$$

The largest exponent on X that we can choose from one of these terms before taking into account $\mathrm{Tr}(X)$ is $2(\frac{n-3}{2}) + 1 = n - 2$. We need a 2^{n-1} exponent on X. Therefore, we must choose the $X^{2^{n-1}}$ term from the trace function.

To obtain the odd powers of 2 (the terms of the form $2^{2(i-1)+1}$) we must choose the $X^{2^{2(i-1)+1+2(i-1)}}$ term from A_i for $1 \leq i \leq \frac{n-1}{2}$. This will give us the term $X^{2+4+\ldots+2^{n-2}}$. This forces us to choose $X\,\mathrm{Tr}(X)$ from A_0. Therefore, there is only one way to choose terms to get the term X^{2^n-1} and the coefficient on the term is 1. Hence, $f(X)$ is not a permutation.

□

3.6 Equivalences

As we are looking for low differential uniform functions, we want to make sure that they are not equivalent to each other or other known examples. From Section 1.7, we know that in addition to the differential uniformity, the extended Walsh spectrum is invariant under the CCZ equivalence. We computed the extended Walsh spectrum for some of the low differential uniform which are given in Appendix C Table C.1. Comparing the extended Walsh spectrum allows us to determine which functions are not CCZ equivalent to each other and which we need to investigate further.

Chapter 4

CLASSIFICATION OF PLANAR MONOMIALS OVER $\mathbb{F}_{p^3}$

In this chapter we present our work on the Dembowski-Ostrom conjecture for monomials over fields of order p^3.

Our work falls into three cases, with one of the cases much more complicated than the other two. In the next section we show how the problem can be broken into these three cases. In Section 4.2, we resolve the two easier cases. The remainder of the chapter considers the more difficult remaining case. In Section 4.3 we outline how the remaining case is broken down and partially resolved; there are 3 main and 11 minor subcases we must contend with. Some of these are unresolved. This is joint work with my advisor and I. Villa from the University of Bergen.

4.1 The basic principles of our approach

We wish to consider the planarity of X^n over $\mathbb{F}_q$. This involves examining the permutation behaviour of the polynomial $f_n(X) = (X+1)^n - X^n$. As planarity is a property of functions, we need only consider $n < q$. In fact, we may insist on $n \leq q-3$ as it is a necessary condition of planarity that $\gcd(n, q-1) = 2$ from Proposition 1.8.3. We assume this throughout the chapter.

There are several points about Hermite's criteria, Theorem 1.3.1, and our specific problem which we now expand on.

For arbitrary $0 < t < q-1$, we may write $f_n(X)^t \bmod (X^q - X)$ as

$$f_n^t \bmod (X^q - X) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} \left[(X+1)^{ni} \bmod (X^q - X)\right] \left[X^{n(t-i)} \bmod (X^q - X)\right], \quad (4.1)$$

and first reduce each of the terms $(X+1)^{ni}$ and $X^{n(t-i)}$ independently. Subsequently, unless both terms have degree $q-1$, the only way in which we can obtain X^{q-1} terms in the reduced

form of $f_n(X)^t$ is via the actual X^{q-1} term generated. This allows for much simplication in our arguments, and in what follows we shall rely on it consistently without further explanation.

The value of binomial coefficients, whether it be in (4.1) or in the expansion of $(X+1)^{ni}$, is clearly something we will need to handle. Fortunately, we have the classical result of Lucas, see Lemma 1.10.1, and the notion of a carry, see Section 1.10, at our disposal. So we will consider our exponent n in its base p expansion form. Set $n = (a_{e-1} \cdots a_0)_p$, with $0 \leq a_i < p$ for all i. There are several advantages in considering the base p expansion of n, over and above the possibility of applying Lucas' Theorem.

Firstly, X^{np} is planar over $\mathbb{F}_q$ if and only if X^n is planar over $\mathbb{F}_q$, and the reduction of X^{np} modulo $X^q - X$ is X^m, where $m = (a_{e-2} \cdots a_0 a_{e-1})_p$. Thus, we may cycle the base p digits of n around and could, for instance, choose to place the largest a_i in the most significant bit.

Secondly, if X^n is planar over $\mathbb{F}_q$, then it is necessarily planar over $\mathbb{F}_p$. This follows at once from observing $f_n \in \mathbb{F}_p[X]$. The classification of planar monomials over $\mathbb{F}_p$ now forces $n \equiv 2 \bmod (p-1)$. This provides the necessary condition

$$a_0 + a_1 + \cdots + a_{e-1} = S \equiv 2 \bmod (p-1).$$

Since $a_i < p$ for all $0 \leq i < e$, we have $S = 2 + k(p-1)$ for some $0 \leq k < e$.

4.1.1 Fixing our setup and the three main cases

For the rest of the chapter we fix $q = p^3$, where p is an odd prime, and consider the planarity of the monomial X^n over $\mathbb{F}_q$. In order to avoid certain degenerate situations later, we further assume $p \geq 11$. The cases $p \in \{3, 5, 7\}$ can easily be checked computationally. We write the base p expansion of the integer n with $0 \leq n < q$ by $n = (a_2 a_1 a_0)_p$. Based on our above discussion, there are three possible cases we must deal with:

Case 1. $S = 2$.

Case 2. $S = 2p$.

Case 3. $S = p + 1$.

The first case will be shown to be the only positive case that we have confirmed while the second case will prove to be empty of planar examples. The remainder of the chapter will be taken up with dealing with Case 3, which breaks into multiple subcases - some of which we resolve while others are still open. However, we conjecture that the remaining cases do not yield any planar functions.

4.2 Resolution of Cases 1 and 2

Coulter and Matthews showed $X^{p^i+p^j}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/\gcd(j-i,e)$ is odd, see [29], Theorem 3.3. This completely resolves Case 1.

Proposition 4.2.1. *If $S = 2$, then $n = p^i + p^j$ with $0 \le i \le j < 3$, and X^n is always planar over $\mathbb{F}_q$.*

The case $S = 2p$ is also relatively straightforward, the proof following very similarly to the classification of planar monomials over $\mathbb{F}_{p^2}$, even down to the exponent used in [21].

Proposition 4.2.2. *If $S = 2p$, then X^n is never planar over $\mathbb{F}_q$.*

Proof. For this case we must have $a_i \ge 2$ for all i and $a_i + a_j > p$ whenever $i \ne j$. We prove Hermite's criteria fails with power $t = p + 1$. We have

$$((X+1)^n - X^n)^t = (X+1)^{n(p+1)} - (X+1)^{np}X^n - (X+1)^n X^{np} + X^{n(p+1)}.$$

We determine the coefficient of X^{q-1} for each of these terms modulo $X^q - X$. Raising a term X^k to the p and reducing modulo $X^q - X$ results in a term with degree a cyclic shift of the base p expansion of k. Thus, for example, we can calculate X^{np} modulo $X^q - X$ easily as an interim step in determining $X^{n(p+1)}$ mod $(X^q - X)$. Proceeding as described we see

$$X^{n(p+1)} = X^{np}X^n \equiv X^{a_2+a_0p+a_1p^2}X^{a_0+a_1p+a_2p^2} \bmod (X^q - X).$$

Set $k = (a_2 + a_0) + (a_0 + a_1)p + (a_1 + a_2)p^2$. Now $n < q - 1$, so that $k < 2(q-1)$. On the other hand, we also know $a_1 + a_2 > p$, so that $k > q$. Consequently, X^k mod $(X^q - X)$ reduces to a term of degree not equal to $q - 1$.

We move to consider the remaining three terms. We note that, as a consequence of Lemma 1.10.1, we may write

$$(X+1)^n = \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \sum_{\alpha_2=0}^{a_2} \left(\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \right) X^{\alpha_0+\alpha_1 p+\alpha_2 p^2}.$$

Following a similar method as above, we see that the coefficient of the term of degree $q-1$ in $(X+1)^n X^{np} \bmod (X^q - X)$ is

$$\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \bmod p,$$

where $\alpha_0 + a_2 = \alpha_1 + a_0 = \alpha_2 + a_1 = p-1$. Since $a_i \leq p-1$, it is clear this coefficient is non-zero. The same argument shows the coefficient of the term of degree $q-1$ in $(X+1)^{np} X^n \bmod (X^q - X)$ is

$$\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \bmod p,$$

where $a_0 + \alpha_2 = a_1 + \alpha_0 = a_2 + \alpha_1 = p-1$, and that this too is nonzero. We note that the two coefficients for X^{q-1} so far determined are, in fact, equal, so that there sum is nonzero modulo p.

The situation for $(X+1)^{n(p+1)}$ is slightly more complicated but still relatively straightforward. Expanding in much the same way as above, it can be seen that the coefficients of resulting terms of degree X^{q-1} in $(X+1)^{n(p+1)} \bmod (X^q - X)$ are given by

$$\prod_i \prod_j \binom{a_i}{\alpha_i} \binom{a_j}{\beta_j}$$

where $\alpha_0 + \beta_2 = \alpha_1 + \beta_0 = \alpha_2 + \beta_1 = p-1$. Along with these equations, the bounds on α_i, β_j reduce the resulting coefficient of X^{q-1} in $(X+1)^{n(p+1)} \bmod (X^q - X)$ to

$$\sum_{\alpha_0=p-1-a_2}^{a_0} \sum_{\alpha_1=p-1-a_0}^{a_1} \sum_{\alpha_2=p-1-a_1}^{a_2} \left(\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \right) \binom{a_0}{p-1-\alpha_1} \binom{a_1}{p-1-\alpha_2} \binom{a_2}{p-1-\alpha_0}.$$

We may rearrange this:

$$\left(\sum_{\alpha_0=p-1-a_2}^{a_0} \binom{a_0}{\alpha_0} \binom{a_2}{p-1-\alpha_0} \right) \left(\sum_{\alpha_1=p-1-a_0}^{a_1} \binom{a_1}{\alpha_1} \binom{a_2}{p-1-\alpha_1} \right) \left(\sum_{\alpha_2=p-1-a_1}^{a_2} \binom{a_2}{\alpha_2} \binom{a_2}{p-1-\alpha_2} \right).$$

Recalling $a_0 + a_2 > p$ and $a_i \leq p-1$ for all i, we have

$$\begin{aligned}\sum_{\alpha_0=p-1-a_2}^{a_0} \binom{a_0}{\alpha_0}\binom{a_2}{p-1-\alpha_0} &= \sum_{j=p-1}^{a_0+a_2} \binom{a_0}{j-a_2}\binom{a_2}{p-1-(j-a_2)} \\ &= \binom{a_0+a_2}{p-1} \\ &\equiv 0 \bmod p.\end{aligned}$$

Thus the coefficient of X^{q-1} in $(X+1)^{n(p+1)} \bmod (X^q - X)$ is zero.

From the above calculations we see the coefficient of X^{q-1} in $((X+1)^n - X^n)^t \bmod (X_q - X)$ is

$$-2\binom{a_0}{p-1-a_2}\binom{a_1}{p-1-a_0}\binom{a_2}{p-1-a_1} \not\equiv 0 \bmod p.$$

By Hermite's criteria, $(X+1)^n - X^n$ is not a permutation polynomial. Thus X^n is not planar in this case. □

4.3 Outline of Case 3 resolution

The remainder of the chapter will solely be aimed at presenting our contribution to the remaining case.

Conjecture 4.3.1. *If $S = p+1$, then X^n is never planar over $\mathbb{F}_q$.*

To establish this statement, we will have to resort to dealing with a number of subcases involving a number of Hermite exponents. A synthesis of our approach to Conjecture 4.3.1 is as follows. We assume $S = a_0 + a_1 + a_2 = p+1$ with $a_2 \geq a_0, a_1$. We then proceed through a sequence of Hermite's exponents:

(i) We determine the coefficient of X^{q-1} in (4.1) for the exponent $t = (1\,1\,2)_p$ when $2 \leq a_0, a_1 \leq a_2$. The situation splits into two subcases based on whether $a_2 > (p-1)/2$ or $a_2 \leq (p-1)/2$. In the former subcase, the coefficient is clearly non-zero, and so there are no planar monomials in this subcase.

(ii) We determine the coefficient of X^{q-1} in (4.1) for the exponent $t = (0\,2\,2)_p$ when $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$.

(iii) We then show that the coefficient of X^{q-1} for $t = (0\,2\,2)_p$ and for $t = (1\,1\,2)_p$ cannot be zero simultaneously, thereby showing that this subcase contains no planar monomials. This concludes the situation where all of the a_i are at least 2.

(iv) We determine the coefficient of X^{q-1} in (4.1) for the exponent $t = (2\,2\,2)_p$ when at least one of a_0 and a_1 is less than 2. This eliminates many situations, but leaves us with 11 explicit subcases to deal with.

(v) We eliminate some of the remaining explicit 11 subcases using various Hermite's exponents.

Steps (4) and (5) remain incomplete and are therefore omitted from this thesis. The following subsections correspond to the solution of the first 3 steps outlined above.

For the ease of notaion, we will refer to the Hermite exponent $t = (1\,1\,2)_p$ as $(1, 1, 2)$ and so forth in what follows.

4.3.1 The Hermite exponent $t = (1, 1, 2)$

In this section, we assume $2 \leq a_0, a_1 \leq a_2$. This forces $a_2 \leq p - 3$.

Via Lucas' Theorem, the non-zero binomial coefficients in (4.1) correspond to the terms $(X + 1)^{n\alpha} X^{n\beta}$ and $(X + 1)^{n\beta} X^{n\alpha}$ in the following table:

α	β
$(1, 1, 2)$	$(0, 0, 0)$
$(1, 1, 1)$	$(0, 0, 1)$
$(1, 1, 0)$	$(0, 0, 2)$
$(1, 0, 2)$	$(0, 1, 0)$
$(1, 0, 1)$	$(0, 1, 1)$
$(1, 0, 0)$	$(0, 1, 2)$

We proceed to work through these six scenarios. Recall that the only way we can obtaing an X^{q-1} term in the reduced form of $f_n(X)^t$ having already reduced $(X + 1)^{n\alpha}$ and $X^{n\beta}$, is from the X^{q-1} term in the product of $(X + 1)^{n\alpha}$ and $X^{n\beta}$. We note that to obtain such a term, the sum of the corresponding coordinates of $n\alpha$ and $n\beta$ must be at least $p - 1$ in each case.

4.3.1.1 $\alpha = (1, 1, 2)$ and $\beta = (0, 0, 0)$

We have

$$\begin{aligned} n\alpha &= (a_2, a_1, a_0) \times (1, 1, 2) \\ &= (a_2 + a_1 + 2a_0, a_1 + a_0 + 2a_2, a_0 + a_2 + 2a_1) \\ &= (p + 1 + a_0, p + 1 + a_2, p + 1 + a_1) \\ &= (2 + a_0, 2 + a_2, 2 + a_1). \end{aligned}$$

To have an X^{q-1} term from $(X + 1)^{n\alpha}$ or $X^{n\alpha}$, we would need $2 + a_i = p - 1$ for $i = 0, 1, 2$. But this impossible under the restriction $a_0 + a_1 + a_2 = p + 1$ and $p \geq 11$. So we obtain no X^{q-1} term from this scenario.

4.3.1.2 $\alpha = (1, 1, 1)$ and $\beta = (0, 0, 1)$

We have

$$\begin{aligned} n\alpha &= (a_2 + a_1 + a_0, a_1 + a_0 + a_2, a_0 + a_2 + a_1) \\ &= (2, 2, 2), \text{ and} \\ n\beta &= (a_2, a_1, a_0). \end{aligned}$$

Since $n\alpha + n\beta = (a_2 + 2, a_1 + 2, a_0 + 2) < (p - 1, p - 1, p - 1)$, it is clear we cannot obtain an X^{q-1} term from this scenario.

4.3.1.3 $\alpha = (1, 1, 0)$ and $\beta = (0, 0, 2)$

We have

$$\begin{aligned} n\alpha &= (a_1 + a_0, a_0 + a_2, a_2 + a_1), \text{ and} \\ n\beta &= (2a_2, 2a_1, 2a_0). \end{aligned}$$

If $a_2 > (p - 1)/2$. then there is a carry in the first coordinate of $n\beta$ and $a_i < (p - 1)/2$ for $i = 0, 1$. Thus $n\beta = (2a_2 - p, 2a_1, 2a_0 + 1)$. However, now the sum of the first coordinates is $a_0 + a_1 + 2a_2 - p = a_2 + 1 < p - 1$. Hence we cannot obtain an X^{q-1} term if $a_2 > (p - 1)/2$.

Now suppose $a_2 \leq (p-1)/2$. Then there is no carry in either $n\alpha$ and $n\beta$, and the sum of each coordinate is $a_i + p + 1 > p - 1$. So we must get an X^{q-1} term. For $(X+1)^{n\alpha}X^{n\beta}$, the coefficient of the X^{q-1} term is

$$\begin{aligned} C_1 &= \binom{a_1 + a_0}{p-1-2a_2}\binom{a_0 + a_2}{p-1-2a_1}\binom{a_2 + a_1}{p-1-2a_0} \\ &= \binom{a_1 + a_0}{a_2 + 2}\binom{a_0 + a_2}{a_1 + 2}\binom{a_2 + a_1}{a_0 + 2}. \end{aligned} \tag{4.2}$$

For $(X+1)^{n\beta}X^{n\alpha}$, the coefficient of the X^{q-1} term is

$$\begin{aligned} C_2 &= \binom{2a_2}{p-1-(a_1 + a_0)}\binom{2a_1}{p-1-(a_0 + a_2)}\binom{2a_0}{p-1-(a_2 + a_1)} \\ &= \binom{2a_2}{a_2 + 2}\binom{2a_1}{a_1 + 2}\binom{2a_0}{a_0 + 2}. \end{aligned} \tag{4.3}$$

4.3.1.4 $\alpha = (1, 0, 2)$ and $\beta = (0, 1, 0)$

We have

$$\begin{aligned} n\alpha &= (2a_2 + a_0, 2a_1 + a_2, 2a_0 + a_1), \text{ and} \\ n\beta &= (a_1, a_0, a_2). \end{aligned}$$

Now $2a_2 + a_0 = a_2 - a_1 + p + 1 > p$, so $n\alpha$ must have a carry. Hence

$$n\alpha = (a_2 - a_1 + 1, 2a_1 + a_2, 2a_0 + a_1 + 1).$$

If there is no carry in the 2nd coordinate of $n\alpha$, then the sum of the first coordinates of $n\alpha$ and $n\beta$ is $a_2 + 1 \leq p - 2 < p - 1$, so we could not get an X^{q-1} term if there was no carry in the 2nd coordinate.

If there is a carry in the 2nd coordinate, then the sum of the 2nd coordinates of $n\alpha$ and $n\beta$ could be no larger than

$$2a_1 + a_2 - p + 1 + a_0 = a_1 + 2 < p - 1,$$

as $a_1 \leq a_2$. Hence we cannot obtain an X^{q-1} term in this situation either.

4.3.1.5 $\alpha = (1,0,1)$ and $\beta = (0,1,1)$

We have

$$n\alpha = (a_2 + a_0, a_1 + a_2, a_0 + a_1), \text{ and}$$
$$n\beta = (a_2 + a_1, a_1 + a_0, a_0 + a_2).$$

There are no carries in either $n\alpha$ or $n\beta$, while the sum of the corresponding coordinates is $a_i + p + 1 > p - 1$. So we must obtain an X^{q-1} term. For $(X+1)^{n\alpha}X^{n\beta}$, the coefficient of the X^{q-1} term is

$$\begin{aligned} C_3 &= \binom{a_2 + a_0}{p - 1 - (a_2 + a_1)}\binom{a_1 + a_2}{p - 1 - (a_1 + a_0)}\binom{a_0 + a_1}{p - 1 - (a_0 + a_2)} \\ &= \binom{a_2 + a_0}{a_2 + 2}\binom{a_1 + a_2}{a_1 + 2}\binom{a_0 + a_1}{a_0 + 2}. \end{aligned} \tag{4.4}$$

For $(X+1)^{n\beta}X^{n\alpha}$, the coefficient of the X^{q-1} term is

$$\begin{aligned} C_4 &= \binom{a_2 + a_1}{p - 1 - (a_2 + a_0)}\binom{a_1 + a_0}{p - 1 - (a_1 + a_2)}\binom{a_0 + a_2}{p - 1 - (a_0 + a_1)} \\ &= \binom{a_2 + a_1}{a_2 + 2}\binom{a_1 + a_0}{a_1 + 2}\binom{a_0 + a_2}{a_0 + 2}. \end{aligned} \tag{4.5}$$

It is now a simple matter to show $C_3 = C_4$. Indeed, it is enough to expand each of the binomial coefficients in C_3 and C_4 and observe that all numerator and denominator terms pair off.

4.3.1.6 $\alpha = (1,0,0)$ and $\beta = (0,1,2)$

This scenario can be dealt with using an argument very similar to that of the $\alpha = (1,0,2)$ and $\beta = (0,1,0)$ scenario. The conclusion will be the same, there is no X^{q-1} term obtained.

4.3.1.7 Summary of the $t = (1,1,2)$ exponent

From our analysis of the above scenarios, we see that we have two situations.

- ⊡ If $a_2 > (p-1)/2$, then we only get an X^{q-1} term from the case $\alpha = (1,0,1), \beta = (0,1,1)$. In this case, the coefficient of X^{q-1} in $f_n(X)^t \bmod (X^q - X)$ is
$$\binom{2}{1}C_3 + \binom{2}{1}C_4 = 4C_3 \neq 0.$$

Thus X^n is not planar if $a_2 > (p-1)/2$.

⊡ If $a_2 \leq (p-1)/2$, then the coefficient of X^{q-1} in $f_n(X)^t \bmod (X^q - X)$ is

$$4C_3 + C_1 + C_2. \tag{4.6}$$

4.3.2 The Hermite exponent $t = (0, 2, 2)$

In this section, we assume $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$.

Via Lucas' Theorem, the non-zero binomial coefficients in (4.1) correspond to the terms $(X+1)^{n\alpha}X^{n\beta}$ and whenever $\alpha \neq \beta$, $(X+1)^{n\beta}X^{n\alpha}$ in the following table:

α	β
$(0, 2, 2)$	$(0, 0, 0)$
$(0, 2, 1)$	$(0, 0, 1)$
$(0, 2, 0)$	$(0, 0, 2)$
$(0, 1, 2)$	$(0, 1, 0)$
$(0, 1, 1)$	$(0, 1, 1)$

4.3.2.1 $\alpha = (0, 2, 2)$ and $\beta = (0, 0, 0)$

We have

$$\begin{aligned} n\alpha &= (2a_2 + 2a_1, 2a_1 + 2a_0, 2a_0 + 2a_2) \\ &= (2p + 2 - 2a_0, 2p + 2 - 2a_2, 2p + 2 - 2a_1) \\ &= (p + 3 - 2a_0, p + 3 - 2a_2, p + 3 - 2a_1). \end{aligned}$$

To obtain an X^{q-1} term in this scenario, we need $p + 3 - 2a_i = p - 1$, so that $a_i = 2$ for $i = 0, 1, 2$, implying $p = 5$. For $p \geq 11$ (as is assumed), we get no X^{q-1} term in this scenario.

4.3.2.2 $\alpha = (0, 2, 1)$ and $\beta = (0, 0, 1)$

We have

$$\begin{aligned} n\alpha &= (a_2 + 2a_1, a_1 + 2a_0, a_0 + 2a_2), \text{ and} \\ n\beta &= (a_2, a_1, a_0). \end{aligned}$$

Now $n\alpha$ must have at least one carry, as the sum of its coordinates is $3(a_0 + a_1 + a_2) = 3(p+1) > 3(p-1)$. If there are 2 or more carries, then the sum of the coordinates of $n\alpha + n\beta$ will be at most

$$3(p+1) - 2(p-1) + a_2 + a_1 + a_0 = 2p + 5 < 3(p-1) \text{ for } p \geq 11,$$

and so we cannot possibly obtain an X^{q-1} term in that situation.

Suppose, then, there is exactly one carry in $n\alpha$. It can either occur in the 1st or 3rd coordinate of $n\alpha$. If it is in the 1st coordinate, then

$$n\alpha = (a_2 + 2a_1 - p, a_1 + 2a_0, a_0 + 2a_2 + 1).$$

Now the sum of the 1st coordinates of $n\alpha$ and $n\beta$ is

$$2a_2 + 2a_1 - p \leq 2(p-1) - p = p - 2 < p - 1,$$

so we cannot obtain an X^{q-1} term in this scenario. A similar argument shows that a 3rd coordinate carry in $n\alpha$ cannot generate an X^{q-1} term also. Thus we do not obtain an X^{q-1} term in this scenario.

4.3.2.3 $\alpha = (0, 2, 0)$ and $\beta = (0, 0, 2)$

We have

$$n\alpha = (2a_1, 2a_0, 2a_2), \text{ and}$$
$$n\beta = (2a_2, 2a_1, 2a_0).$$

There are no carries as $a_i \leq (p-1)/2$. Additionally,

$$2a_i + 2a_j = 2(p+1) - 2a_k \geq 2(p+1) - (p-1) = p + 3 > p - 1,$$

and so we must obtain X^{q-1} terms here. For $(X+1)^{n\alpha}X^{n\beta}$, the coefficient of the X^{q-1} term is

$$C_5 = \binom{2a_2}{p-1-2a_1)}\binom{2a_1}{p-1-2a_0)}\binom{2a_0}{p-1-2a_2)}. \tag{4.7}$$

For $(X+1)^{n\beta}X^{n\alpha}$, the coefficient of the X^{q-1} term is

$$C_6 = \binom{2a_1}{p-1-2a_2)}\binom{2a_0}{p-1-2a_1)}\binom{2a_2}{p-1-2a_0)}. \tag{4.8}$$

It is not difficult to show $C_5 = C_6$.

4.3.2.4 $\alpha = (0, 1, 2)$ and $\beta = (0, 1, 0)$

The argument for this scenario is almost a replica of the argument for $\alpha = (0, 2, 1)$ and $\beta = (0, 1, 0)$. The conclusion will be the same, there is no X^{q-1} term obtained.

4.3.2.5 $\alpha = (0, 1, 1)$ and $\beta = (0, 1, 1)$

We have

$$n\alpha = (a_2 + a_1, a_1 + a_0, a_0 + a_2).$$

As $a_i \leq (p-1)/2$, there are no carries. In this scenario, we must get an X^{q-1} term. $(X+1)^{n\alpha}X^{n\beta}$, the coefficient of the X^{q-1} term is

$$\begin{aligned} C_7 &= \binom{a_2 + a_1}{p - 1 - (a_2 + a_1)}\binom{a_1 + a_0}{p - 1 - (a_1 + a_0)}\binom{a_0 + a_2}{p - 1 - (a_0 + a_1)} \\ &= \binom{a_2 + a_1}{a_0 - 2}\binom{a_1 + a_0}{a_2 - 2}\binom{a_0 + a_2}{a_1 - 2}. \end{aligned} \tag{4.9}$$

4.3.2.6 Summary of the $t = (0, 2, 2)$ exponent

From our analysis of the above scenarios, we see that the coefficient of X^{q-1} in $f_n(X)^t$ mod $(X^q - X)$ is

$$\binom{2}{1}\binom{2}{1}C_7 + C_5 + C_6 = 4C_7 + 2C_5. \tag{4.10}$$

4.3.3 Playing the two Hermite exponents $(1, 1, 2)$ and $(0, 2, 2)$ against each other

In this section we assume $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$. We shall show that for such n, with $a_0 + a_1 + a_2 = p + 1$, that it is impossible for both Hermite exponents $t = (1, 1, 2)$ and $t = (0, 2, 2)$ to fail to generate an X^{q-1} term, and consequently X^n is cannot be planar over $\mathbb{F}_q$. The following identity will prove useful. For odd prime p and arbitrary $0 \leq k < p$ we have

$$(p - 1 - k)! \equiv \frac{(-1)^{k+1}}{k!} \bmod p.$$

The lemma can be established by first proving

$$\binom{p-1}{k} \equiv (-1)^k \bmod p.$$

using an inductive argument and the identity $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$. The result then follows from observing $(p-1)! \equiv -1 \bmod p$.

For convenience, we preemptively set

$$\begin{aligned} U &= (a_0 + a_2)!\,(a_1 + a_0)!\,(a_2 + a_1)!, \\ V &= (a_0 - 2)!\,(a_1 - 2)!\,(a_2 - 2)!, \\ W &= (2a_0)!\,(2a_1)!\,(2a_2)!, \end{aligned}$$

and view U, V and W as elements of $\mathbb{F}_p$. We first derive a relation between U and V. In fact, we prove $UV = -1$ if $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$.

Proof. From Lemma 4.3.3 we find

$$\begin{aligned} (a_0 - 2)! &= \frac{(-1)^{a_0 - 1}}{(p + 1 - a_0)!} \\ &= \frac{(-1)^{a_0 - 1}}{(a_1 + a_2)!}. \end{aligned}$$

A similar identity can be derived for $(a_1 - 2)!$ and $(a_2 - 2)!$. It now follows that

$$\begin{aligned} V &= \frac{(-1)^{a_0 + a_1 + a_2 - 3}}{U} \\ &= \frac{-1}{U}, \end{aligned}$$

as claimed. □

Now assume that both the coefficients of X^{q-1}, given in (4.6) and (4.10), are zero. We next simplify (4.6). Taking the equation $4C_3 + C_1 + C_2 = 0$ and multiplying through by $\prod(a_i + 2)!$, we have

$$\begin{aligned} 0 &= 4\frac{U}{V} + \frac{U}{(a_1 + a_2 - a_0 - 2)!\,(a_2 + a_0 - a_1 - 2)!\,(a_0 + a_1 - a_2 - 2)!} + \frac{W}{V} \\ &= 4\frac{U}{V} - UW + \frac{W}{V}, \end{aligned}$$

where we have again used Lemma 4.3.3. We therefore find

$$2U + W = 0. \tag{4.11}$$

Next we shall simplify (4.10). Taking the equation $2C_7 + C_5 = 0$ and multiplying through by $\prod(p + 3 - 2a_i)!$, we have

$$\begin{aligned} 0 &= 2\frac{U}{V} + + \frac{W}{(p-1-2a_0)!\,(p-1-2a_1)!\,(p-1-2a_2)!} \\ &= -2U^2 + (-1)^3 W^2, \end{aligned}$$

again using Lemma 4.3.3. From (4.11) we have $W^2 = 4U^2$, and so $6U^2 = 0$ must hold. However, this is a contradiction as $U \neq 0$ and $p \geq 11$. This means that it is impossible for the Hermite exponents $t = (1, 1, 2)$ and $t = (0, 2, 2)$ to simultaneously generate a zero coefficient for X^{q-1} in $f_n(X)^t$ mod $(X^q - X)$. Hence, X^n cannot be planar when $n = (a_2 a_1 a_0)_p$, $a_0 + a_1 + a_2 = p + 1$ and $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$.

The final two steps of our outline are still open problems. We will discuss these in Chapter 5 with other open problems.

Chapter 5

OPEN PROBLEMS

In this chapter, we will discuss interesting open problems that resulted from this work. We include conjectures that follow from computational and theoretical evidence that we have collected along with our intuition for each of these problems.

5.1 Coordinate Replacement

In Chapter 2, we give the framework behind the extended switching technique. It seems reasonable to expect a new construction of low differentially uniform functions from this technique. As we saw in Section 2.3, we did not obtain new APN functions from adding coordinate functions of APN functions together. While we did not test these functions for their actual differential uniformity we know that the differential uniformity is bounded by 2^k where k is the number of coordinate functions that we alter. This leads us to our first set of open problems.

Open Problems One:

1. Can we find new APN functions that are inequivalent to any known examples using the extended switching technique? If we can, how do we classify these?

2. When do we obtain a function that is 2^k-DU when we alter k coordinate functions of an APN functions?

3. Can we alter k coordinate functions of an APN function and obtain a new function that is δ-DU with $\delta < 2^k$?

5.2 Mutually Orthogonal systems

Given the relationship between planar functions and orthogonal systems that we presented in Section 1.7.1, we can consider the coordinate functions of the difference polynomial of a planar function as a maximal orthogonal system. When we remove a coordinate function we have an orthogonal system that is no longer maximal. We noted in Theorem 1.6.2 that we can always extend an orthogonal system to a maximal orthogonal system. However, arbitrarily extending this orthogonal system and obtaining a another APN function seems hard. In [30], Coulter and Matthews give an algorithm to determine if for a fixed bivariate function, ϕ, over a finite field there exists a univariate function, f, such that $f(x+y) - f(x) - f(y) = \phi(x,y)$. However, this uses the algebraic form of ϕ rather than the functional description of ϕ. Therefore, to use this algorithm we would need to extend the orthogonal system into a maximal orthogonal system, then interpolate to get the coordinate functions before we could use the algebraic form. This leads us to our next set of open questions.

Open Questions Two:

1. What restrictions can we put on Theorem 1.6.2 to extend an orthogonal system to a maximal orthogonal system to ensure that the functions that we add to the system are difference polynomials?

2. Is the extension unique? How many coordinate functions do we need to remove before we can obtain a new planar function through Theorem 1.6.2?

3. Can we classify these planar functions?

5.3 Kantor Functions

In Section 3.3, we focused on creating relatively low differential uniform functions from Kantor's presemifields. When n is odd and the chain of fields is $\mathbb{F}_2 \subsetneq \mathbb{F}_{2^n}$ we have shown that the differential uniformity of a Kantor function, $f(x) = x^3 + x\,\mathrm{Tr}(a_1 x) + a_1\,\mathrm{Tr}(x)$ is at most 4. We showed that when $a_1 \neq 1$ $f(x)$ is differentially 4 uniform. However, computationally we find that when $n > 3$ and $a_1 = 1$, $f(x)$ is also 4-DU; so we have the following conjecture.

Conjecture 5.3.1. *For $n > 3$ and n odd $f(x) = x^3 + \mathrm{Tr}(a_1 x) + a_1 \mathrm{Tr}(x)$ is differentially 4 uniform for all $a_1 \in \mathbb{F}_{2^n}^*$.*

When the chain of fields is $\mathbb{F}_2 \subsetneq F_k \subsetneq \ldots \subsetneq F_1 = \mathbb{F}_{2^m} \subsetneq \mathbb{F}_{2^n}$, we have shown in Theorem 3.3.3 that $f(x) = x^3 + \sum_{i=1}^{k} x\,\mathrm{Tr}_i(\alpha_i x) + \alpha_x \mathrm{Tr}_i(x^2)$ is at most 2^{m+1} differentially uniform. To see if we can get more information on when the function obtains the bounds we investigate what the solutions of $x^2 + (a + \alpha a^{-1})x + \beta$ look like. There are two roots of $x^2 + (a + \alpha a^{-1})x + \beta$, call them γ_1 and γ_2, if and only if $\gamma_1\gamma_2 = \beta$ and $\gamma_1 + \gamma_2 = a + \alpha a^{-1}$. Rearranging we find that $\gamma_2 = \beta\gamma_1^{-1}$ and we need $\gamma_1 + \beta\gamma_1^{-1} = a + \alpha a^{-1}$. So, the number of roots of $\Delta_g(x, a)$ equals the number of $\beta \in \mathbb{F}_{2^m}^*$ such that $\gamma_1 + \beta\gamma_1^{-1} = a + \alpha a^{-1}$ for some $\gamma_1 \in \mathbb{F}_{2^n}$ where $\sum_{i=1}^{k} \mathrm{Tr}(a_i\gamma_1) = \beta$.

We would like to classify $\{\alpha_i\}_{i=1}^k$ by the differential uniformity that their corresponding $f(x)$ yields. In other words which $\{\alpha_i\}_{i=1}^k$ yield a function that is 2^{m+1}-DU; which yield functions that are 4-DU; and to determine if there are any that are APN.

Open Problems 3:

1. For what set of $\{\alpha_i\}_{i=1}^k$, does $f(x) = x^3 + \sum_{i=1}^{k} x\,\mathrm{Tr}_i(\alpha_i x) + \alpha_i\,\mathrm{Tr}_i(x^2)$ obtain the maximal differential uniformity of 2^{m+1}?

2. For what set of $\{\alpha_i\}_{i=1}^k$ is $f(x) = x^3 + \sum_{i=1}^{k} x\,\mathrm{Tr}_i(\alpha_i x) + \alpha_x\,\mathrm{Tr}_i(x^2)$ 4-DU?

We also showed in Section 3.3 that the Kantor functions of the form $f(x) = x^3 + x\,\mathrm{Tr}(\alpha x)$ were almost always not permutations. The smaller the number of the pre-images for each $b \in \mathbb{F}_{2^n}$ the more efficient the decryption process is. Therefore, we are interested in determining "how close" Kantor functions in general are to permutations. We will let $\gamma(f) = \max_{b\in\mathbb{F}_{2^n}} \#\{x : f(x) = b\}$. If $\gamma(f) = 1$, then clearly $f(X)$ is a permutation. The larger $\gamma(f)$ is, the further f is from being a permutation.

Open Problem 4:

1. Are there any other Kantor functions that are permutations?

2. For each Kantor function, f, that is not a permutation can we determine $\gamma(f)$?

5.4 Planar Nearfields

Recall the functions, $f(x)$, from the planar nearfields that we described in Conjecture 3.4.2. We proved in Theorem 3.4.3, that the differential uniformity of $f(x)$ is at least $\frac{q+1}{2}$. This leads us to the following open problems.

Open Problems 5:

1. Can we prove Conjecture 3.4.2?

2. Can we determine the differential uniformity of $f(x) = x*x$ for arbitrary regular planar nearfield, $N(n, q)$?

5.5 Equivalence of Low Differentially Uniform Functions.

In Table C.1 we found the extended Walsh spectrum for some of the low differentially uniform functions that we constructed from algebraic objects. Some of these functions have the same differential uniformity and extended Walsh spectrum; thus, they may be CCZ equivalent. We want to investigate such functions and classify these low differential uniform functions into their equivalence classes.

5.6 Low Differentially Uniform Functions and Affine Planes

Planar functions give rise to specific affine planes. The geometry gives insight into properties about these functions. In Section 1.10.2 we discussed the relationship between algebraic structures and affine planes. The low differentially uniform functions that we have discussed are associated with affine planes; however, at no point in this thesis has the geometry been used to study the DU of these functions. We would like to use information about the affine plane to help determine the differential uniformity of $f(x) = x * x$.

5.7 Classification of Planar Monomials over p^3

In Chapter 4 there are still two major parts left to prove that Case 3 does not yield any more planar functions. Determining the coefficient of X^{q-1} in (4.1) for the exponent $t = (2\,2\,2)_p$ when at least one of a_0 and a_1 is less than 2 is still in progress. We also need to prove that the explicit 11 subcases that are not covered by this exponent do not yield

any planar functions. Based on computational evidence, we believe we have determined the correct exponents in all 11 subcases too and have even determined the coefficient for most of them. However, we have so far been unable to prove the coefficients are nonzero.

BIBLIOGRAPHY

[1] A. A. Albert. Finite division algebras and finite planes. In *Proc. Sympos. Appl. Math.*, pages 53–70. American Mathematical Society, Providence, R.I., 1960.

[2] A. A. Albert. Generalized twisted fields. *Pacific J. Math.*, 11:1–8, 1961.

[3] A. A. Albert. Isotopy for generalized twisted fields. *An. Acad. Brasil. Ciênc.*, 33:265–275, 1961.

[4] A. A. Albert. On associative division algebras. *Bull. Amer. Math. Soc.*, 74:438–454, 1968.

[5] N. At and S. D. Cohen. A new tool for assurance of perfect nonlinearity. In *Sequences and their applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 415–419. Springer, Berlin, 2008.

[6] T. Beth and C. Ding. On almost perfect nonlinear permutations. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 65–76. Springer, Berlin, 1994.

[7] J. Bierbrauer. New commutative semifields and their nuclei. In *Applied algebra, algebraic algorithms, and error-correcting codes*, volume 5527 of *Lecture Notes in Comput. Sci.*, pages 179–185. Springer, Berlin, 2009.

[8] J. Bierbrauer. New semifields, PN and APN functions. *Des. Codes Cryptogr.*, 54(3):189–200, 2010.

[9] C. Bracken, E. Byrne, N. Markin, and G. McGuire. A few more quadratic APN functions. *Cryptogr. Commun.*, 3(1):43–53, 2011.

[10] L. Budaghyan, M. Calderini, C. Carlet, R.S. Coulter, and I. Villa. On isotopic construction of apn functions. to appear in the Proceedings of SETA 2018.

[11] L. Budaghyan and C. Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Trans. Inform. Theory*, 54(5):2354–2357, 2008.

[12] L. Budaghyan, C. Carlet, and G. Leander. On a construction of quadratic apn functions. *IEEE Trans. Inform. Theory*.

[13] L. Budaghyan, C. Carlet, and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Inform. Theory*, 54(9):4218–4229, 2008.

[14] L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. *Finite Fields Appl.*, 15(2):150–159, 2009.

[15] L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. In *Sequences and their applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 403–414. Springer, Berlin, 2008.

[16] L. Budaghyan, T Helleseth, and N. Kaleyski. A new family of apn quadrinomials. Cryptology ePrint Archive, Report 2019/994.

[17] L. Carlitz. Invariantive theory of equations in a finite field. *Trans. Amer. Math. Soc.*, 75:405–427, 1953.

[18] L. Carlitz. Invariant theory of systems of equations in a finite field. *J. Anal. Math.*, 3:382–413, 1954.

[19] C. Castillo. *A method for constructing groups of permutation polynomials and its application to projective geometry*. Ph.D. thesis, University of Delaware, 2015.

[20] S.D. Cohen and M.J. Ganley. Commuatative semifields, two dimensional over their middle nuclei. *J. Algebra*, 75:373–385, 1982.

[21] R.S. Coulter. The classification of planar monomials over fields of prime square order. *Proc. Amer. Math. Soc.*, 134(11):3373–3378, 2006.

[22] R.S. Coulter and B. Fain. On semi-planar functions. in preparation.

[23] R.S. Coulter and M. Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008.

[24] R.S. Coulter, M. Henderson, and P. Kosick. Planar polynomials for commutative semifields with specified nuclei. *Des. Codes Cryptogr.*, 44(1-3):275–286, 2007.

[25] R.S. Coulter and P. Kosick. Commutative semifields of order 243 and 3125. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 129–136. Amer. Math. Soc., Providence, RI, 2010.

[26] R.S. Coulter and F. Lazebnik. On the classification of planar monomials over fields of square order. *Finite Fields Appl.*, 18(2):316–336, 2012.

[27] R.S. Coulter and R. Matthews. On the permutation behaviour of Dickson polynomials of the second kind. *Finite Fields Appl.*, 8(4):519–530, 2002.

[28] R.S. Coulter and R.W. Matthews. Bent polynomials over finite fields. *Bull. Aust. Math. Soc.*, 56(3):429–437, 1997.

[29] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

[30] R.S. Coulter and R.W. Matthews. On the number of distinct values of a class of functions over a finite field. *Finite Fields Appl.*, 17(3):220–224, 2011.

[31] P. Dembowski. *Finite geometries*. Ergeb. Math. Grenzgeb. Springer-Verlag, Berlin-New York, 1968.

[32] P. Dembowski and T.G. Ostrom. Planes of order n with collineation groups of order n^2. *Math.Z.*, 103(3):239–258, Jun 1968.

[33] L.E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11(1-6):161–183, 1896/97.

[34] L.E. Dickson. On finite algebras. *Nachr. kgl. Ges. Wiss. Gottingen*, pages 358–393, 1905.

[35] L.E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 7:514–522, 1906.

[36] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Niho case. *Inform. and Comput.*, 151(1-2):57–72, 1999.

[37] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Welch case. *IEEE Trans. Inform. Theory*, 45(4):1271–1275, 1999.

[38] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5. In *Finite fields and applications (Augsburg, 1999)*, pages 113–121. Springer, Berlin, 2001.

[39] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3:59–81, 2009.

[40] M. Ganley. Central weak nucleus semifields. *European J. Combin.*, 2(4):339 – 347, 1981.

[41] D. Gluck. Affine planes and permutation polynomials. In *Coding theory and design theory, Part II*, volume 21 of *IMA Vol. Math. Appl.*, pages 99–100. Springer, New York, 1990.

[42] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14:154–156, 1968.

[43] S.D. Groves. *Locally finite near-fields*. Ph.D. Thesis, Australian National University, 1974.

[44] M. Henderson and R. Matthews. Dickson polynomials of the second kind which are permutation polynomials over a finite field. *New Zealand J. Math.*, 27(2):227–244, 1998.

[45] C. Hermite. Sur les fonctions de sept lettres. *C. R. Acad. Sci. Paris*, 57:750–757, 1863.

[46] Y. Hiramine. A conjecture on affine planes of prime order. *J. Combin. Theory Ser. A*, 52(1):44–50, 1989.

[47] H. Janwa and R. M. Wilson. Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. In *International Symposium on Applied algebra, algebraic algorithms and error-correcting codes*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 180–194. Springer, Berlin, 1993.

[48] N. L. Johnson. Projective planes of prime order p that admit collineation groups of order p^2. *J. Geom.*, 30(1):49–68, 1987.

[49] W. M. Kantor and M. E. Williams. Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Trans. Amer. Math. Soc.*, 356(3):895–938, 2004.

[50] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[51] D. Knuth. Finite semifields and projective planes. *J. Algebra*, 2(2):182 – 217, 1965.

[52] V. A. Kurbatov and N. G. Starkov. The analytic representation of permutations. *Sverdlovsk. Gos. Ped. Inst. Učen. Zap.*, 31:151–158, 1965.

[53] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia Math. Appl.* Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[54] E. Lucas. Theorie des Fonctions Numeriques Simplement Periodiques. *Amer. J. Math.*, 1:184–240,289–321, 1878.

[55] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. Symplectic semifield spreads of PG$(5, q)$ and the Veronese surface. *Ric. Mat.*, 60(1):125–142, 2011.

[56] M. Matsui. Linear cryptanalysis method for des cipher. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 386–397. Springer, Berlin, 1994.

[57] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[58] H. Niederreiter. Orthogonal systems of polynomials in finite fields. *Proc. Amer. Math. Soc.*, 28:415–422, 1971.

[59] W. Nöbauer. Zur Theorie der Polynomtransformationen und Permutationspolynome. *Math. Ann.*, 157:332–342, 1964.

[60] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 55–64. Springer, Berlin, 1994.

[61] T. Penttila and B. Williams. Ovoids of parabolic spaces. *Geom. Dedicata*, 82(1-3):1–19, 2000.

[62] N.C. Raber. A geometric approach to counting distribution of squares in a finite field. *Geom. Dedicata*, 4(2, /3/4):297–303, 1975.

[63] L. Rónyai and T. Szőnyi. Planar functions over finite fields. *Combinatorica*, 9(3):315–320, 1989.

[64] H. Taniguchi. On some quadratic APN functions. *Des. Codes Cryptogr.*, 87(9):1973–1983, 2019.

[65] H. Zassenhaus. Uber endlicke fastoper. 11:187–220, 1935.

[66] Z. Zha, G. Kyureghyan, and X. Wang. Perfect nonlinear binomials and their semifields. *Finite Fields Appl.*, 15(2):125 – 133, 2009.

[67] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Adv. Math.*, 234:43–60, 2013.

Appendix A

KNOWN PLANAR FUNCTIONS

There is a one-to-one correspondence between planar DO functions and commutative semifields Theorem 1.7.6. The table below gives known planar functions and commutative semifields.

Table A.1: Known Planar Functions

Planar Function as a Polynomial	Conditions	Citation	Corresponding Semifields
X^2			The finite field of order p^n.
$L(t^2(X)) + \frac{1}{2}X^2$	p^{2en} with p odd and n, e natural numbers, $L(X) = (8)^{-1}(X^{p^e} - X)$, and $t(X) = X^{p^{en}} - X$	Dickson, [35]	Dickson semifields
X^{p^e+1}	over $\mathbb{F}_{p^n}$ with $\frac{n}{\gcd(n,e)}$ is odd p^n where p is odd	Albert, [2]	Albert's commutative twisted fields.

$X^{1+q'} - vX^{q^2+q'q}$	over $\mathbb{F}_{q^3}$ with p an odd prime, $q = p^s$, $q' = p^t$, $s' = \frac{s}{(s,t)}$, s' odd, $t' = \frac{t}{(s,t)}$, $ord(v) = q^2 + q + 1$, and at least one of the following holds: $s' + t' \equiv 0 \mod 3$ or $q \equiv q' \equiv 1 \mod 3$	Zha, Kyureghyan, Wang [66]	Zha-Kyureghyan-Wang (ZKW) semifields
$X^{1+q'} - vX^{q^3+q'q}$	over $\mathbb{F}_{q^4}$ with p an odd prime, $q = p^s$, $q' = p^t$, such that $\frac{2s}{(2s,t)}$ is odd, $q \equiv q' \equiv 1 \mod 4$, and $ord(v) = q^3 + q^2 + q + 1$	Bierbrauer [8]	Bierbrauer semifields
$\mathrm{Tr}(X^{q+1}) + \mathrm{Tr}(\beta X^{p^s+1})\omega$	over $\mathbb{F}_{q^2}$ with p an odd prime, $q = p^m$, and $Tr(x)$ is the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$, $\omega, \beta \in \mathbb{F}_{q^2}$, $\mathrm{Tr}(\omega) = 0$ and s is a positive integer such that β^{q-1} is not contained in the subgroup of order $\frac{q+1}{(q+1,p^s+1)}$ in $(\mathbb{F}_{q^2}, *)$ and there is no $0 \neq a \in \mathbb{F}_{q^2}$, such that $\mathrm{Tr}(a) = 0$ and $a^{p^s} = -a$.	Budaghyan and Helleseth [15] and Bierbrauer [7]	Budaghyan-Helleseth-Bierbrauer (BHB) semifields

$\mathrm{Tr}(X^2) + G(X^{q^2+1})$	over $\mathbb{F}_{q^{2m}}$ where q is a power of an odd prime p, $m = 2k+1$, $\mathrm{Tr}(x)$ is the trace function from $\mathbb{F}_{q^{2m}}$ to $\mathbb{F}_{q^m}$, and $G(x) = h(x - x^{q^m})$ where $h \in \mathbb{F}_{q^{2m}}[x]$ is defined as $h(x) = \sum_{i=0}^{k}(-1)^i x^{q^{2i}} + \sum_{j=0}^{k-1}(-1)^{k+j} x^{q^{2j+1}}$.	Bierbrauer [7, 55]	Lunardon-Marino-Polverino-Trombetti-Bierbrauer (LMPTB) semifields.
$L(t^2(X)+D(t(X))+\frac{1}{2}X^2$	over $\mathbb{F}_{3^8}$ with $L(X) = X^{243}-X^{81}+X^9+X^3-X$, $D(X) = X^{246}-X^{10}$, and $t(X) = X^9 - X$ [1]	Coulter, Henderson, Kosick [24]	Coulter-Henderson-Kosick semifields
$L(t^2(X)) + \frac{1}{2}X^2$	over $q = 3^{2en}$ with $t(X) = X^{3^{en}} - X$, $\alpha = t(\beta)$ for $\beta \in \mathbb{F}_q \setminus \mathbb{F}_{3^{en}}$ fixed, and $L(X) = X^9 - \alpha X^3 + (1-\alpha^2)X$	Cohen and Ganley [20]	Cohen-Ganley semifields
$L(t^2(X))+D(t(X))+\frac{1}{2}X^2$	over 3^{2en} where $en \geq 3$ is odd, $t(X) = X^{3^{en}} - X$, $\alpha = t(\beta)$ for a fixed $\beta \in \mathbb{F}_{3^{2en}} \setminus \mathbb{F}_{3^{en}}$, $L(X) = -\alpha^{-1}X^3 + X$, and $D(X) = \alpha^{-2}X^{10}$	Ganley [40]	Ganley semifields

[1] The authors of [24] acknowledge an error in the original publication regarding this example. The correction was found on Dr. Coulter's webpage.

$X^{10} \pm X^6 - X^2$	over 3^n with n odd or $n = 2$	Coulter and Matthews [29]	Coulter-Matthews and Ding-Yuan semifields
$L(t^2(X)) + \frac{1}{2}X^2$	over 3^{10} with $t(X) = X^{243} - X$, $\alpha = t(\beta)$ for some fixed $\beta \in \mathbb{F}_{3^{10}} \setminus \mathbb{F}_{3^5}$, and $L(X) = -(\alpha^{-53}X^{27} + \alpha^{-18}X^9 - X)$	Penttila and Williams [61]	Penttila-Williamss semifield
$X^{\frac{3^k+1}{2}}$	over $\mathbb{F}_{3^n}$ where k is odd and $(k, n) = 1$	Coulter and Matthews, [29]	
$X^2 + X^{90}$	over $\mathbb{F}_{3^5}$	found by Weng [25]	At-Cohen-Weng (ACW) semifield [5]

Appendix B

KNOWN APN FUNCTIONS

The table belows give the known APN monomials and quadratic functions over $\mathbb{F}_{2^n}$.

Table B.1: Known APN monomials and quadratic functions.

Function	Conditions	Name and Reference
x^{p^i+1}	$\gcd(i,n) = 1$	Gold [42], [60]
$x^{2^{2i}-2^i+1}$	$gcd(i,n) = 1$	Kasami [50], [47]
x^{2^t+3}	$n = 2t+1$	Welch [37]
$x^{2^t+2^{\frac{t}{2}}-1}$	t even and $n = 2t+1$	Niho [36]
$x^{2^t+2^{\frac{3t+1}{2}}-1}$	t odd and $n = 2t+1$	Niho [36]
$x^{2^{2t}-1}$	$n = 2t+1$	Inverse [6], [60]
$x^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$	$n = 5i$	Dobbertin [38]
$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,3) = \gcd(s,3k) = 1$, $p \in \{3,4\}$, $i = sk \pmod p$, $m = p-i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$, $i = sk \pmod p$, $m = p-i, n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[13]
$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m$, $n = 2m$, $gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x such that $x^{q+1} = 1$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x such that $x^{q+1} = 1$	[11]

$x^3 + a^{-1}\,\mathrm{Tr}_n(a^3x^9)$	$a \neq 0$	[14]
$x^3 + a^{-1}\,\mathrm{Tr}_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[12]
$x^3 + a^{-1}\,\mathrm{Tr}_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[12]
$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3) = \gcd(s,3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k+s)$, u primitive in $\mathbb{F}_{2^n}^*$	[9]
$(x + x^{2^m})^{2^k+1} + u'(ux + u^{2^m}x^{2^m})^{(2^k+1)2^i} + u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$n = 2m$, $m \geqslant 2$ even, $\gcd(k,m) = 1$ and $i \geqslant 2$, $ei \geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[67]
$L(x)^{2^i}x + L(x)x^{2^i}$	$n = km$, $\gcd(n,i) = 1$, $L(x) = \sum_{j=0}^{k-1} a_j x^{2^{jm}}$ satisfies the conditions in Theorem 6.3 of [10]	[10]
$ut(x)(x^q + x) + t(x)^{2^{2i}+2^{3i}} + at(x)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$n = 2m$, $q = 2^m$, $\gcd(m,i) = 1$, $t(x) = u^q x + x^q u$, $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[64]
$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2$, $m = 10$, $(a,b,c) = (\beta,1,0,0)$, $i = 3$, $k = 2$, β primitive in $\mathbb{F}_{2^2}$	[16]
$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m$, m odd, $3 \nmid m$, $(a,b,c) = (\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[16]

Appendix C

EXTENDED WALSH SPECTRUM OF LOW DU FUNCTIONS

The following table gives the extended Walsh spectrum that we calculated for a sample of the low DU functions that we constructed in Chapter 3. We note that functions that have the same differential uniformity and extended Walsh spectrum should be investigated to determine if they are CCZ equivalent.

Table C.1: Extended Walsh Transforms

	The Algebraic Object corresponding to the function	Differential Uniformity	The Extended Walsh Spectrum
i	Albert's Generlized Twisted Field with $p = 3$, $n = 3$, $i = 1$, $j = 2$, and $c \in \{2, g, g^3, g^9\}$	3	3
ii	Albert's Generlized Twisted Field with $p = 3$, $n = 3$, $i = 1$, $j = 2$, and $c \in S_1$[1]	3	1, 3

[1] $S_1 = \{g^5, g^7, g^{11}, g^{15}, g^{17}, g^{19}, g^{21}, g^{21}, g^{25}\}$

iii	Albert's Generlized Twisted Field with $p = 3$, $n = 4$, for any combination of i and j in Section 1.4.2 for 12 choices of c	3	3
iv	Albert's Generlized Twisted Field with $p = 3$, $n = 4$, and for any combination of i and j in Section 1.4.2 for 27 choices of c.	3	1,3
v	Kantor's presemifield with the chain of fields $\mathbb{F}_2 \subset \mathbb{F}_{2^3}$ and $c \neq 0, 1$	4	0,4,8
vi	Kantor's presemifield with the chain of fields $\mathbb{F}_2 \subset \mathbb{F}_{2^5}$ and $c \in \{15, 23, 27, 29, 30\}$	4	0, 8, 16, 32
vii	Kantor's presemifield with the chain of fields $\mathbb{F}_2 \subset \mathbb{F}_{2^5}$ and $c \notin \{0, 15, 23, 27, 29, 30\}$	4	0, 8, 32
viii	$N(9, 2)$	5	5, 7, 17, 25, 31, 33, 37, 47, 57, 71, 81
ix	$N(19, 2)$	5	1, 17, 19, 21, 23, 39, 41, 57, 59, 61, 79, 97, 201, 217, 361

x	$N(5, 2)$	4	1, 3, 5, 7, 9, 15, 17, 19, 25
xi	$N(5, 4)$	4	7, 9, 15, 17, 21, 25, 27, 31, 33, 41, 49, 51, 57, 63, 65, 69, 71, 73, 79, 81, 87, 89, 91, 97, 101, 105, 107, 109, 111, 113, 115, 117, 121, 129, 131, 133, 135, 137, 143, 145, 149, 153, 155, 163, 169, 171, 175, 183, 187, 191, 197, 201, 207, 209, 211, 217, 225, 233, 235, 243, 257, 273, 275, 287, 305, 327, 625
xii	$N(13, 2)$	8	1, 3, 5, 7, 13, 15, 17, 19, 23, 31, 33, 35, 39, 41, 43, 47, 49, 51, 67, 73, 81, 87, 89, 97, 105, 169