On difference maps and their cryptographic applications

by

David Thomson

A thesis submitted to
the Faculty of Graduate and Postgraduate Affairs
in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

in

Mathematics

School of Mathematics and Statistics
Ottawa-Carleton Institute for Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada

Abstract

The focus of this thesis is on the difference maps of functions over finite groups. Let $f\colon G_1 \to G_2$, its difference map with parameter $a \in G_1^*$ is $\Delta_{f,a}(x) = f(x+a) - f(x)$, where G_1 and G_2 are written additively. Two new measures, ambiguity and deficiency, are introduced. The ambiguity of f measures the number of pairs of elements x_1 and x_2 such that $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$ for some $a \in G_1^*$. The deficiency of f measures the number of elements $b \in G_2$ such that $\Delta_{f,a}^{-1}(b) = \emptyset$, for some $a \in G_1^*$. As such, the ambiguity is a collective measure of the injectivity of the $\Delta_{f,a}$ and the deficiency is a collective measure of the surjectivity of the $\Delta_{f,a}$.

We present theoretical results on the ambiguity and deficiency of permutation functions. In particular, we give lower bounds for both ambiguity and deficiency of permutations. We show that permutations that achieve optimal ambiguity and deficiency are also highly non-linear. We prove that ambiguity and deficiency (as well as other differential properties of functions) are invariant under extended-affine and Carlet-Charpin-Zinoviev equivalences. Finally, the ambiguity and deficiency of some commonly considered functions are also computed.

Dembowski-Ostrom polynomials over finite fields are characterized as those polynomials whose difference maps are linearized polynomials. We give a formula for the ambiguity and deficiency of any Dembowski-Ostrom polynomial in terms of the ranks of matrices having a specific shape. We compute the ambiguity and deficiency of the Dembowski-Ostrom monomial, also called the Gold polynomial, and recover its well-known differential properties using our new method. We also compute the ambiguity and deficiency of Dembowski-Ostrom polynomials which are known to be permutation polynomials. These include permutation binomials and trinomials, polynomials with two and three non-zero terms, respectively, and polynomials arising as trace functions.

We give a partial solution to a conjecture of Golomb and Moreno on a multiplicative analogue of planar functions over prime fields. If $f \in \mathbb{F}_p[x]$ has degree $s > 0$, the Golomb-Moreno conjecture states that if $f(0) = 0$ and $\Delta_{f,a}(x) = f(xa) - f(x)$ is a permutation for all $a \neq 1$ (hence, f is also a permutation), then $f(x) = x^s$. We show that the number of non-zero terms of f is at most $s/4$ and give a new conjecture, which is implied by the Golomb-Moreno conjecture, based on the number of moved elements of f. We also outline a possible method of completing the proof.

We also discuss some first steps on future research. We give a criterion for a specific type of linearized polynomial to be a permutation and give an infinite class of linearized permutation trinomials. We give a proof of the ambiguity and deficiency of a reversed Dickson polynomial, based on a conjecture on the shape of the terms of the polynomial. Proving the conjecture requires a technical analysis of the 2-divisibility of binomial coefficients. Finally, we present a construction of an imperfect design which uses ambiguity and deficiency of permutation functions.

Acknowledgements

First and foremost, I would like to acknowledge the support, mentorship and friendship of my advisor, Daniel Panario. I would also like to thank Evangelos Kranakis, Gary McGuire and Mike Newman for their thoughtful comments and questions during my thesis defense. Special mention is due for Brett Stevens and Steven Wang for their help and oversight throughout the course of this research, and to Amin Sakzad for his helpful collaboration.

Thanks to Ben Seamone for reading a portion of this thesis and providing insightful comments, and to Gary Bazdell for years of support and office talks. My most grateful thanks to Kseniya Garaschuk for providing crutches on this and an immeasurable amount of things over the years.

All of the members of the School of Mathematics and Statistics at Carleton University have had some part in guiding my studies over the past ten years. The faculty and staff alike have always maintained a warm and welcoming environment for me to grow both personally and professionally.

This PhD was supported in large part by NSERC of Canada. A portion of the research was done while I was visiting the Claude Shannon Institute in Dublin, IR. Most of the writing and polishing was done at The Pennsylvania State Unversity. These opportunities would not have been possible without the supervision and kindness of Gary L. Mullen.

Finally, to all my friends and family. Too numerous to mention individually and impossible to forget, you've all had a hand in guiding me throughout.

Contents

Notation

p	a prime
q	$q = p^e$, for some positive integer e
$\mathbb{F}_q$	the finite field with q elements
$\mathbb{F}_q^*$	the multiplicative group of $\mathbb{F}_q$
$(\mathbb{F}_q, +)$	the additive group of $\mathbb{F}_q$
$\mathbb{F}_q^e$	the vector space of dimension e over $\mathbb{F}_q$
$\mathbb{F}_{q^e}$	the field extension of degree e over $\mathbb{F}_q$ isomorphic to $\mathbb{F}_q^e$
$\mathbb{F}_q[x]$	polynomials over $\mathbb{F}_q$ in the single variable x
$\mathbb{Z}_n$	the finite ring of integers modulo n
G_1, G_2	finite groups
$\widehat{G_1}$	the group of characters (the dual) of G_1
f	a map $G_1 \to G_2$
$\widehat{f}$	the Fourier transform of f
$\Delta_{f,a}(x)$	the difference map with parameter $a \in G_1^*$: $$\Delta_{f,a}(x) = f(x+a) - f(x) \in G_2.$$
$\mathbb{L}(f)$	the linearity of a function f
$\mathbb{NL}(f)$	the non-linearity of a function f
$\mathbb{NB}(\mho)$	the non-balancedness of a function f
ϵ_L	the probability bias of a linear expression L representing a cipher

List of Acronyms

AES	the Advanced Encryption Standard
APN	almost perfect non-linear
DO	Dembowski-Ostrom
PN	perfect non-linear
SAFER	the Secure and Fast Encryption Routine
SPN	substition-permutation network

List of Tables

List of Figures

Chapter 1

Introduction

The main goal of this thesis is to study the new measures of *ambiguity* and *deficiency* of a function f between finite groups G_1 and G_2. The *difference maps* of f are given by $\Delta_{f,a}(x) = f(x+a) - f(x)$, where $a \in G_1^*$, and here both G_1 and G_2 are written additively. Informally, the ambiguity of a function counts the number of distinct pairs of elements $x_1, x_2 \in G_1$ such that $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$. Hence, the ambiguity of a function is a collective measure of the injectivity of its difference maps. The deficiency of a function is the sum of the number of elements of G_2 which do not arise as an image of $\Delta_{f,a}$, $a \in G_1^*$. Similarly, the deficiency of a function is a collective measure of the surjectivity of its difference maps.

We are chiefly concerned with functions over the additive and multiplicative groups of finite fields. We also consider the additive and multiplicative groups of the finite ring $\mathbb{Z}_n$. We are mainly interested when $G_1 = G_2$ and the function is a permutation, however in most cases we maintain generality until we require some special property of either the group or the function.

Any mapping from a finite field to itself can be defined as a polynomial by the Lagrange Interpolation Formula (Theorem 2.1.1). A *permutation polynomial* is the induced polynomial due to a permutation of the field elements. The *value set* of a function is the set of all its images. When a function is a permutation (hence, its domain is equal to its co-domain), its value set is the entire co-domain. Since the ambiguity and deficiency are measures of injectivity and surjectivity, respec-

tively, of the difference maps of functions, in particular we are concerned with the multi-set of their values. Thus, we are interested not only in the cardinalities of the value sets of the $\Delta_{f,a}$, but also in the number of repetitions of elements in the value multi-sets of the $\Delta_{f,a}$.

Though we do not claim that this is a thesis devoted to cryptography, we cannot ignore the cryptographic motivations and implications of this work. In order to make this thesis self-contained, we present the basics of many relevant cryptographic notions. Difference maps arise quite naturally in studying candidates for good *substitution boxes* (S-boxes) in *substitution-permutation networks*. *Differential cryptanalysis* is an attack on ciphers which exploits pairs of differences of inputs and outputs, say $(\Delta X, \Delta Y)$, that occur with high probability. More specifically, if S is the function induced by an S-box, then for a fixed input difference $\Delta X = a$, differential cryptanalysis requires pairs $(x+a, x)$ such that $((x+a)-x, S(x+a)-S(x))$ occur with significant probability. In the above terminology, functions which have low ambiguity are desirable due to their resistance against these differential attacks. Another common attack on symmetric-key cryptosystems is *linear cryptanalysis*. Linear cryptanalysis exploits the presence of linear or affine relations in a cipher that occur with a high probability *bias*, that is a probability differing significantly from $1/2$. Since in most modern ciphers the only non-linear portion of the cipher is in its S-boxes, it is critical to design S-boxes with not only good differential characteristics, but also high non-linearity.

Without question, the most important modern cipher is the *Advanced Encryption Standard* (AES). The main non-linear component of AES is the function $f\colon x \to x^{2^8-2}$ over $\mathbb{F}_{2^8}$. This "power function" is simply described as the function $f(0) = 0$ and $f(x) = x^{-1}$, if $x \neq 0$. The inverse function is known to be highly non-linear and also has nearly optimal differential characteristics. One of the motivations of studying ambiguity is the small distance AES has from optimal differential characteristics. This closeness to optimality is not captured in the currently accepted measures of differential strength.

The measures of ambiguity and deficiency were first introduced in the proceedings paper [56]. In that paper, the authors consider only the ambiguity and deficiency over finite groups of the same size. They give bounds on the ambiguity and deficiency of permutations over $\mathbb{Z}_n$. Constructions of

permutations of $\mathbb{Z}_n$ which achieve these bounds also appear. An extended journal version of these results, including proofs, appears in [55]. In particular, a modified version of the discussion of the bounds presented in [55] also appears in Section 5.2 of this work. The functions with optimal or near-optimal ambiguity and deficiency constructed in [55] are presented in Section 5.4.

New results on the ambiguity and deficiency of specific polynomials appear in the proceedings paper [54]. In this paper, the authors consider *monomials* (or *power functions*), *Linearized polynomials*, *Dickson polynomials* and *Dembowski-Ostrom* polynomials. Specifically, the authors give experimental results on the ambiguities and deficiencies of Dickson (and reversed Dickson) polynomials and state the ambiguity and deficiency of the reversed Dickson polynomial of degree $2^n + 5$. Also stated in [54] are the ambiguity and deficiency of the Dembowski-Ostrom monomial and one Dembowski-Ostrom polynomial due to a trace function.

Main contributions

Now, we give an outline of this thesis and highlight our main contributions.

In Part I, we develop many of the foundations necessary to motivate and understand the remainder of the thesis. In Chapter 2, we present some necessary mathematical background. Therein, we describe some special mappings over finite fields, namely trace functions, characters and the discrete Fourier transform. Canonical results on permutation polynomials are given in Section 2.2 and some related combinatorial objects are presented in Section 2.3.

Special functions of interest, particularly over finite fields, are given in Chapter 3. We introduce classes of functions with known differential characteristics, namely *planar functions* and *almost perfect non-linear* functions. We also introduce particular polynomials over finite fields whose ambiguity and deficiency we study in Part II. These functions include monomials, linearized polynomials and Dickson polynomials. In order to study functions which are not permutations, we introduce their value sets in Section 3.6. The value sets of linearized polynomials given in Section 3.6.2 will play a special role in Chapter 6 and also in Sections 5.4 and 8.1. We give some introductory results on a special type of value set, the *subfield value set*, in Section 3.7. Results from Sections 3.6.2 and 3.7

appear in [16].

We formally state the cryptographic motivations mentioned above in Chapter 4. We introduce substitution-permutation networks in Section 4.1. These networks are both simple to describe and important in practice; for instance, AES is a substitution-permutation network. We give a very brief outline of differential and linear cryptanalysis, due to [35], in Section 4.2. In Section 4.3, we state some criteria for strong S-box design due to [46]. We end the chapter with an in-depth look at two ciphers, AES and SAFER. We describe AES in detail in Section 4.4.1, where we show not only its design and structure but also its differential characteristics. Similar results are given for the SAFER cipher in Section 4.4.2. We note that SAFER provides particular motivation for abstracting ambiguity and deficiency away from finite fields of characteristic two, since SAFER uses both the vector space $\mathbb{F}_2^8$ and the multiplicative group of the ring $\mathbb{Z}_{257}$ in its design.

Our main contributions on ambiguity and deficiency appear in Part II. In particular, our focus is on the ambiguity and deficiency of permutation functions. We formally and rigorously give some of the essential properties of ambiguity and deficiency of permutations in Chapter 5. A preliminary discussion of many of these properties originally appears in [55]. Our new contributions to the theory of ambiguity and deficiency of permutations include a connection between functions which have optimal ambiguity and deficiency to functions having good linearity properties in Section 5.3.1 and Section 5.3.2. The results of Section 5.3.1 appear in [53] and those of Section 5.3.2 are found in [61]. In Section 5.3.3, also appearing in [53], we show that the properties of ambiguity and deficiency are invariant under well-known equivalence classes of functions, namely the *extended-affine* and *Carlet-Charpin-Zinoviev* equivalences. Section 5.4 is devoted to calculating the ambiguity and deficiency of commonly considered functions. These include the inverse function of AES, APN and other functions with prescribed differential characteristics and linearized polynomials.

Chapter 6 is concerned with the ambiguity and deficiency of *Dembowski-Ostrom* (DO) permutation polynomials. DO polynomials are characterized as those polynomials over finite fields whose difference maps are linearized polynomials. In Section 6.1, we give a formula for the ambiguity and deficiency of any DO polynomial in terms of the ranks of matrices of a specific shape. We use this

formula to compute the ambiguity and deficiency of known DO permutation monomials, binomials (containing two non-zero terms) and trinomials (containing three non-zero terms). We recover known results such as when the DO monomial, called the Gold polynomial, is planar or APN. The results of the binomial and trinomial cases are new and depend on analyzing the ranks of matrices whose non-zero terms are contained in three diagonals. We also derive the ambiguity and deficiency of various forms of DO permutation polynomials which are constructed using trace functions. Since the images of trace functions are well-understood, the results on DO polynomials due to trace functions are obtained using elementary methods. All of the results in Chapter 6, except for those on the Gold polynomial in Section 6.2, appear in [53].

In Chapter 7, we give a partial solution to a conjecture of Golomb and Moreno [33]. The Golomb-Moreno conjecture states that if a permutation polynomial $f \in \mathbb{F}_p[x]$ has the added property that $\Delta_{f,d}(x) = f(xd) - f(x)$ is a permutation for all $d \neq 1$, then $f(x) = x^s$ for some positive s. If additionally $f(0) = 0$, we call these polynomials *Costas polynomials*, since Golomb and Moreno's motivation was on periodicity properties of *circular Costas sequences*. Thus, proving the Golomb-Moreno conjecture requires showing that Costas polynomials (which are essentially planar permutation polynomials over $\mathbb{F}_p^*$) are monomials. We use the method of Hiramine [36], who shows that planar functions over $\mathbb{F}_p$ must be defined by quadratic polynomials, to show that Costas polynomials contain at most $s/4$ terms. We also state a new conjecture which is implied by the Golomb-Moreno conjecture in terms of the number of *moved* elements of f. A brief version of these results can be found in [62].

In Chapter 8, we outline some areas for future research. In Section 8.1, we give a simple condition to determine if a linearized polynomial $L \in \mathbb{F}_{q^e}[x]$ is a permutation when e is a power of the characteristic of $\mathbb{F}_{q^e}$ and the coefficients of L are elements of $\mathbb{F}_q$. Informally, the polynomial L is a permutation under these conditions if the sum of its coefficients is non-zero. As a corollary, we give an infinite class of linearized permutation trinomials.

Dickson polynomials are defined as the (unique) bi-variate polynomial D_n such that $D_n(x_1 + x_2, x_1x_2) = x_1^n + x_2^n$. The univariate Dickson polynomial is denoted $D_n(x, a) \in \mathbb{F}_q[x]$, where $a \in \mathbb{F}_q[x]$.

If $a = 0$, then $D_n(x, 0)$ is a monomial. For $a \neq 0$, it is well-known that the Dickson polynomial $D_n(x, a)$ defines a permutation of $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$. A *reversed Dickson* polynomial is obtained by reversing the role of the variable and parameter of the univariate D_n, thus considering instead $D_n(a, x)$. In the reversed Dickson case, only some sufficient conditions are known under which $D_n(a, x)$ defines a permutation of $\mathbb{F}_q$. The coefficients of Dickson polynomials involve expressions of the form $\frac{n}{n-i}\binom{n-i}{i}$, due to Waring's formula ([43, Theorem 1.76]). Studying the ambiguity and deficiency of Dickson polynomials first requires studying the divisibility of binomial coefficients. We give some preliminary results in this direction in Section 8.2.

Finally, in Section 8.3, we formalize an application of ambiguity and deficiency to a construction of an imperfect design, which was originally presented in [1]. We state the three constructions for a tournament schedule given there, the final of which is based on ambiguity and deficiency. We also discuss further how measuring ambiguity and deficiency may lead to other design-like structures.

We end with some concluding remarks in Part III.

Part I

Foundations

Chapter 2

Mathematical background

The intention of this chapter is to develop the concepts and give the mathematical background necessary to understand all of the subsequent chapters. We assume a basic knowledge of algebra and number theory and, in particular, some basic knowledge of finite fields. In Section 2.1, we remind the reader of the most relevant concepts in finite fields. Permutation polynomials play a special role in this work, so we give them a brief introduction in Section 2.2. In addition, many of the concepts we will deal with have a particular combinatorial flavour, and we discuss some related combinatorial objects in Section 2.3.

2.1 Basic concepts

In this section, we recall some basic concepts in finite fields. The essential reference on finite fields is the book [43] and a handbook containing the state-of-the-art of many of the topics in finite fields and their numerous applications is to appear [49].

Let p be a prime and denote by $\mathbb{F}_q$ the finite field of $q = p^n$ elements. Suppose $\mathbb{F}_{q^e}$ is the degree $e \geq 1$ extension of $\mathbb{F}_q$, then $\mathbb{F}_{q^e} \cong \mathbb{F}_q[x]/(f)$, where $f \in \mathbb{F}_q[x]$ is an irreducible polynomial of degree e. The multiplicative group of $\mathbb{F}_{q^e}$, denoted $\mathbb{F}_{q^e}^*$, is cyclic and if $\mathbb{F}_{q^e}^* = \langle g \rangle$, then g is a *primitive element* of $\mathbb{F}_{q^e}$. A *primitive polynomial* $f \in \mathbb{F}_q[x]$ of degree e is a polynomial whose roots are primitive elements of $\mathbb{F}_{q^e}$. The automorphisms of $\mathbb{F}_{q^e}$ that fix $\mathbb{F}_q$ are generated by the

Frobenius q-automorphism ϕ_q, where $\phi_q(\alpha) = \alpha^q$ for all $\alpha \in \mathbb{F}_{q^e}$. The Galois group of $\mathbb{F}_{q^e}$ over $\mathbb{F}_q$ is given by $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q) = \langle \phi_q \rangle$. Finally, for any $\alpha \in \mathbb{F}_{q^e}$, the *(Galois) conjugates* of α are given by $\{\alpha, \phi_q(\alpha), \ldots, \phi_q^{e-1}(\alpha)\} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{e-1}}\}$.

This work is concerned with properties of maps between finite Abelian groups. The following theorem states that there is an induced polynomial for every map from a field to itself.

Theorem 2.1.1. [43, Theorem 1.71] **(Lagrange Interpolation Formula)**. *For $n \geq 0$, let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of $\mathbb{F}$ and let $b_0, b_1, \ldots, b_n$ be $n+1$ arbitrary elements of $\mathbb{F}$. Then there exists exactly one polynomial $f \in \mathbb{F}[x]$ of degree at most n such that $f(a_i) = b_i$ for $i = 0, 1, \ldots, n$. This polynomial is given by the formula*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{0 \leq k \leq n, k \neq i} \frac{x - a_k}{a_i - a_k}. \tag{2.1}$$

The Lagrange Interpolation Formula allows us to use the notions of functions over a finite field and the corresponding polynomial interchangeably.

2.1.1 The difference map

The difference map is paramount throughout this entire thesis. We highlight its definition here. Properties of the difference maps of commonly considered functions are given in Chapter 3. Part II of this thesis deals with two measures of a function based on their difference maps.

Definition 2.1.2. *Let G_1 and G_2 be finite groups, and let $f\colon G_1 \to G_2$. The* difference map of f at $a \in G_1^*$, *also called the* derivative of f in direction a, *is given by the map*

$$\begin{aligned} \Delta_{f,a}\colon G_1 &\to G_2 \\ x &\to f(x+a) - f(x), \end{aligned}$$

where G_1 and G_2 are written additively.

2.1.2 Traces over finite fields

Informally, the trace of any element in $\mathbb{F}_{q^e}$ is the sum of its Galois conjugates. The values of the trace function, and the number of times the trace takes on each value, has particular importance in Chapter 6.

Definition 2.1.3. *Let $\alpha \in \mathbb{F}_{q^e}$ and denote by $\mathrm{Tr}\colon \mathbb{F}_{q^e} \to \mathbb{F}_q$ the* trace *map given by*

$$\mathrm{Tr}_{q^e/q}(\alpha) = \sum_{i=0}^{e-1} \alpha^{q^i}.$$

It is easy to see that $\mathrm{Tr}_{q^e/q}(\alpha)^q = \mathrm{Tr}_{q^e/q}(\alpha)$, so the trace is a projection map $\mathbb{F}_{q^e} \to \mathbb{F}_q$. When the extension and ground fields are understood, we drop the subscript.

Proposition 2.1.4. *Let $\mathbb{F}_{q^e}$ be an extension of $\mathbb{F}_q$ and let $\alpha, \beta \in \mathbb{F}_{q^e}$. Then $\mathrm{Tr}_{q^e/q}$ is a linear projection from $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$. In addition,*

1. *$\mathrm{Tr}_{q^e/q}(a) = ea$ for all $a \in \mathbb{F}_q$;*
2. *$\mathrm{Tr}_{q^e/q}(\alpha^q) = \mathrm{Tr}_{q^e/q}(\alpha)$ for all $\alpha \in \mathbb{F}_{q^e}$.*

We now discuss the values of the trace function.

Theorem 2.1.5. *Let $\alpha \in \mathbb{F}_{q^e}$. Then $\mathrm{Tr}_{q^e/q}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$, for some $\beta \in \mathbb{F}_{q^e}$.*

Theorem 2.1.6. *There are q^{e-1} elements $\alpha \in \mathbb{F}_{q^e}$ with $\mathrm{Tr}(\alpha) \neq 0$ and for any $b_1, b_2 \in \mathbb{F}_q^*$, the number of elements $\alpha, \gamma \in \mathbb{F}_{q^e}$ with $\mathrm{Tr}_{q^e/q}(\alpha) = b_1$ and $\mathrm{Tr}_{q^e/q}(\gamma) = b_2$ are equal.*

The trace function is especially important as it serves as a representation of all linear transformation from $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$, independently of the chosen basis.

Theorem 2.1.7. *Consider $\mathbb{F}_{q^e}$ as a vector space over $\mathbb{F}_q$. The linear projections from $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$ are precisely the mappings L_β, where $\beta \in \mathbb{F}_{q^e}$, such that $L_\beta(\alpha) = \mathrm{Tr}(\beta\alpha)$ for all $\alpha \in \mathbb{F}_{q^e}$. Furthermore, $L_\beta \neq L_\gamma$ whenever $\beta \neq \gamma$.*

2.1.3 Characters over finite fields

Characters play a fundamental role in the non-linearity of functions, see Section 2.1.4. We present the basics of characters over finite groups. These results can be found [43, Chapter 5]. The proofs are omitted for brevity.

Definition 2.1.8. *Let G be a finite Abelian group (written multiplicatively) of order $|G|$ with identity element 1_G. A* character *χ of G is a homomorphism $\chi : G \to U$ where U is the multiplicative group of complex numbers of length 1.*

In particular, for any $g_1, g_2 \in G$, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$.

Definition 2.1.9. *Let G be a finite Abelian group. The* trivial character*, χ_0, on G is defined by $\chi_0(g) = 1$ for all $g \in G$.*

Definition 2.1.10. *Let G be a finite Abelian group and suppose χ is a character of G. The* conjugate character *of χ, $\overline{\chi}$, is given by $\overline{\chi}(g) = \overline{\chi(g)}$.*

Proposition 2.1.11. *Let G be a finite Abelian group and let χ be a character of G. Then,*

(1) $\chi(1_G) = 1$;

(2) $\chi(g)^{|G|} = \chi\left(g^{|G|}\right) = \chi(1_G) = 1$, hence $\chi(g)$ is a $|G|$th root of unity;

(3) $\chi(g)\chi\left(g^{-1}\right) = \chi\left(gg^{-1}\right) = \chi(1_G) = 1$, hence $\chi\left(g^{-1}\right) = \chi(g)^{-1} = \overline{\chi(g)}$;

(4) The set $\widehat{G}$ of characters of G forms an Abelian group, the dual *of G, under the operation $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. Furthermore, $|\widehat{G}| = |G|$.*

Proposition 2.1.12. *Let G be a finite cyclic group of order n with $G = \langle g \rangle$ for some g. Define $\chi_j \colon G \to U$ such that $\chi_j : g^k \to \left(e^{2\pi i k/n}\right)^j$. Then, the dual of G is the cyclic group $\widehat{G} = \langle \chi_1 \rangle$.*

Theorem 2.1.13. *1. If χ is a nontrivial character of the finite Abelian group G, then*

$$\sum_{g \in G} \chi(g) = 0. \tag{2.2}$$

2. For any $g \in G$ with $g \neq 1_G$,

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0. \tag{2.3}$$

Theorem 2.1.14. (Orthogonal relations for characters).

1. Let χ and ψ be characters of G,

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0 & \text{for } \chi \neq \psi \\ 1 & \text{for } \chi = \psi. \end{cases} \tag{2.4}$$

2. Let g, h be elements of G, then

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{for } g \neq h \\ 1 & \text{for } g = h. \end{cases} \tag{2.5}$$

Characters of the multiplicative group of a finite field are given in Proposition 2.1.12, since the multiplicative group of a finite field is cyclic of order $q - 1$. We now consider characters over the additive group of $\mathbb{F}_q$.

Definition 2.1.15. *Let p be a prime and let $\mathbb{F}_q$ be the finite field with $q = p^n$. The* canonical additive character*, χ_1, is given by $\chi_1(c) = e^{2\pi i \mathrm{Tr}(c)/p}$.*

Theorem 2.1.16. *For every $\beta \in \mathbb{F}_q$ define the function $\chi_\beta(c) = \chi_1(\beta c)$. Then, χ_β is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ is obtained in this way.*

2.1.4 Discrete Fourier transform for measuring non-linearity

In this section, we begin by showing the usefulness of various transforms restricted to Boolean (or vectorial Boolean) functions. Using this as motivation, we then describe the more general case of mappings between any finite Abelian groups.

Boolean functions

In this section, we identify the finite field $\mathbb{F}_{2^e}$ with the finite vector space $\mathbb{F}_2^e$. For any $a \in \mathbb{F}_{2^e}$, there is a corresponding representation $(a_1, a_2, \ldots, a_e)$ under some basis in the vector space $\mathbb{F}_2^e$. Addition in the vector space is performed component-wise, $(a_1, a_2, \ldots, a_e)+(b_1, b_2, \ldots, b_e) = (a_1+b_1 \pmod 2, a_2 + b_2 \pmod 2, \ldots, a_e + b_e \pmod 2)$. This modulo-2 vector addition is simply the XOR of the bits, which we denote by the symbol $\oplus$.

A function $f\colon \mathbb{F}_2^e \to \mathbb{F}_2$ is a *Boolean* function and a function $g\colon \mathbb{F}_2^e \to \mathbb{F}_2^d$ is a *vectorial Boolean* function. More information on Boolean and vectorial Boolean functions can be found [8] and [9], respectively.

Suppose $f\colon \mathbb{F}_2^e \to \mathbb{F}_2^d$ is a vectorial Boolean function. Then, $f(x_1, x_2, \ldots, x_e) = (y_1, y_2, \ldots, y_d)$, where $x_i, y_j \in \mathbb{F}_2$, $1 \le i \le e$, $1 \le j \le d$. Denote by $f_1, f_2 \ldots, f_d$ the *component Boolean* functions

$$f(x_1, x_2, \ldots, x_e) = (f_1(x_1, x_2, \ldots, x_e), f_2(x_1, x_2, \ldots, x_e), \ldots, f_d(x_1, x_2, \ldots, x_e)).$$

The non-trivial character of $\mathbb{F}_2$ is given by $\chi(x) = (-1)^x$. The discrete Fourier transform in the binary case (also called the Hadamard transform) is defined as follows.

Definition 2.1.17. *The discrete Fourier transform $\widehat{f}\colon \mathbb{F}_2^e \to \mathbb{C}$ of a Boolean function $f\colon \mathbb{F}_2^e \to \mathbb{F}_2$ is given by*

$$\widehat{f}(u) = \sum_{x \in \mathbb{F}_2^e} f(x)(-1)^{x \cdot u},$$

where $x \cdot u$ denotes the usual inner product.

Setting $u = 0$ gives $\widehat{f}(0) = \sum_{x \in \mathbb{F}_2^e} f(x)$, which is the size of the support of f. For two Boolean functions f and g, $\widehat{f \oplus g}(0) = \sum_{x \in \mathbb{F}_2^e} f \oplus g(x)$ which again is the size of the support of $f \oplus g$. In other words, $\widehat{f \oplus g}(0)$ is the number of $x \in \mathbb{F}_2^e$ such that $f(x) \neq g(x)$.

Definition 2.1.18. *Let f and g be Boolean functions.*

1. *The* Hamming weight *of f, denoted $w_H(f)$ is the size of the support of f and is given by $w_H(f) = \widehat{f}(0)$.*

2. *The* Hamming distance *of f and g, denoted $d_H(f,g)$, is the size of the support of $f \oplus g$, and is given by $\widehat{f \oplus g}(0)$.*

Now, denote by $f_\chi(x) = (-1)^{f(x)}$, the real-valued *sign* function of f.

Definition 2.1.19. *The* Walsh transform *of a Boolean function $f\colon \mathbb{F}_2^e \to \mathbb{F}_2$ is the Fourier transform of f_χ,*

$$\widehat{f_\chi}(u) = \sum_{x \in \mathbb{F}_2^e} (-1)^{f(x) \oplus x \cdot u}.$$

Since $f_\chi = 1 - 2f$, $\widehat{f_\chi} = 2^e\delta_0 - 2\widehat{f}$, where δ_0 is the Dirac delta function. Re-arranging and evaluating at zero gives the following proposition.

Proposition 2.1.20. *Let f be a Boolean function. Then,*

$$w_H(f) = 2^{e-1} - \frac{\widehat{f_\chi}(0)}{2}. \tag{2.6}$$

Let $\ell_a(x) = a \cdot x = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_ex_e$. An expression of this form is a *linear form.* Applying Equation (2.6) to $f \oplus \ell_a$ yields the identity

$$d_H(f, \ell_a) = w_H(f \oplus \ell_a) = 2^{e-1} - \frac{\widehat{f_\chi}(a)}{2}.$$

Since any linear form ℓ_a is determined by the element a, a notion of the distance of a function from all linear forms is given by

$$\min_{a \in \mathbb{F}_2^e} \left(2^{e-1} - \frac{\widehat{f_\chi}(a)}{2} \right) = \min_{a \in \mathbb{F}_2^e} \left(2^{e-1} - \frac{\sum_{x \in \mathbb{F}_2^e} (-1)^{f(x) \oplus x \cdot a}}{2} \right).$$

Definition 2.1.21. *Let $f\colon \mathbb{F}_2^e \to \mathbb{F}_2$ and denote by $\mathbb{L}(f)$ the (Boolean)* linearity *of f, given by the expression*

$$\mathbb{L}(f) = \max_{a \in \mathbb{F}_2^e} \widehat{f_\chi}(a) = \max_{a \in \mathbb{F}_2^e} \sum_{x \in \mathbb{F}_2^e} (-1)^{f(x) \oplus x \cdot a}.$$

We also present the more common measure stated in the literature.

Definition 2.1.22. *Let $f\colon \mathbb{F}_2^e \to \mathbb{F}_2$ and denote by $\mathbb{NL}(f)$ the (Boolean)* non-linearity *of f, given by the expression*

$$\mathbb{NL}(f) = 2^{e-1} - \max_{a \in \mathbb{F}_2^e} \left(\frac{\widehat{f_\chi}(a)}{2} \right).$$

In Section 4.2.1, we show that constructing a linear expression modeling a cryptosystem requires only a subset of the inputs and outputs of each function. As a result, we require that each component function of a vectorial Boolean function is highly non-linear. This is captured in the definition of the non-linearity of a vectorial Boolean function.

Definition 2.1.23. *Let $f\colon \mathbb{F}_2^e \to \mathbb{F}_2^d$ be a vectorial Boolean function with component Boolean functions $(f_1, f_2, \ldots, f_d)$. The non-linearity of f is given by*

$$\mathbb{NL}(f) = \min_{1 \leq i \leq d} \mathbb{NL}(f_i).$$

The discrete Fourier transform over finite Abelian groups

In the non-Boolean case, we require a more general form of the Fourier transform. The general form of the non-linearity of a mapping between any two finite groups is given in [25]. In [25] the authors also state that these definitions accurately portray the linearity as it pertains to its resistance against linear cryptanalysis. We now follow the general definition given there.

Definition 2.1.24. *Let $(G, +)$ be a finite Abelian group. The Fourier transform of any complex-valued function Φ on G is given by*

$$\widehat{\Phi}(\chi) = \sum_{x \in G} \Phi(x)\chi(x),$$

where χ is a character of G.

Since the group of characters of G, denoted by $\widehat{G}$, is in bijective correspondence to G, let χ_α to the image of α under some bijection of G to $\widehat{G}$. Then we write

$$\widehat{\Phi}(\alpha) = \sum_{x \in G} \Phi(x)\chi_\alpha(x).$$

We can therefore consider $\widehat{\Phi}$ to be defined on the group G.

Definition 2.1.25. *If f is a function between finite Abelian groups G_1 and G_2, then identifying ψ_β as the image of $\beta \in G_2$ under any bijection from $G_2 \to \widehat{G_2}$, the Fourier transform of f at $\alpha \in G_1$ and $\beta \in G_2$ is given by*

$$\widehat{f}(\alpha, \beta) = \sum_{x \in G_1} (\psi_\beta \circ f)(x)\chi_\alpha(x).$$

We now define the (general) linearity and non-linearity using the discrete Fourier transform.

Definition 2.1.26. *If $f \colon G_1 \to G_2$, the* linearity *of F is given by*

$$\mathbb{L}(f) = \max_{\alpha \in G_1, \beta \in G_2^*} |\widehat{f}(\alpha, \beta)|.$$

The non-linearity of a function is finally given by the following normalized measure.

Definition 2.1.27. *Let G_1, G_2 be finite Abelian groups, and $f \colon G_1 \to G_2$. The* non-linearity *of f is given by*

$$\mathbb{NL}(F) = \frac{|G_1| - \mathbb{L}(F)}{|G_2|}.$$

When either of the groups G_1 or G_2 are non-Abelian, the notion of Fourier transform must change, since there are no longer characters. Poinsot [57] defines Fourier-like transforms for functions between G_1 and G_2 where G_1 or G_2 is a Abelian. We briefly discuss this as an avenue for future research in the conclusions.

2.2 Permutation polynomials

By Theorem 2.1.1, any map defined from a finite field to itself can be defined by a polynomial. A natural question to ask is when does a polynomial define a permutation from the field to itself. We begin with a general definition.

Definition 2.2.1. *Let R be an integral domain and let $f \in R[x]$ be a polynomial with coefficients in R such that $f(R) = R$. Then f is a* permutation polynomial *(sometimes referred to as a PP).*

We most commonly take the ring R to be the finite field with q elements $\mathbb{F}_q$. Permutation polynomials over finite fields are well-studied but the problem of characterizing most classes of permutation polynomials remains open. An introduction to the canonical results on permutation polynomials is given in [43, Chapter 7]. The permutation behaviour of some special functions over finite fields is further studied in Chapter 3.

Theorem 2.2.2. *Let $f, g \in \mathbb{F}_q[x]$. Then $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{x^q - x}$.*

As a consequence of Theorem 2.2.2, we consider only permutation polynomials of degree less than q. The following are useful criteria for checking if a polynomial is a permutation.

Proposition 2.2.3. [43, Lemma 7.3] *Let $S = \{a_0, a_1, \ldots, a_{q-1}\}$ be a set of elements of $\mathbb{F}_q$. Then $S = \mathbb{F}_q$ if and only if*

$$\sum_{i=0}^{q-1} (a_i)^t = \begin{cases} 0 & \text{if } 1 \leq t \leq q-2, \\ -1 & \text{if } t = q-1. \end{cases}$$

Theorem 2.2.4. [43, Theorem 7.4] **(Hermite's Criterion)**. *Let $\mathbb{F}_q$ have characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if the following two conditions hold:*

1. *f has exactly one root in $\mathbb{F}_q$,*
2. *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{x^q - x}$ has degree at most $q-2$.*

In Chapter 7 we make extensive use of a consequence of Proposition 2.2.3 to determine the specific form of a special class of permutation polynomials. Hermite's Criterion is critical in the proof of many results on permutation polynomials. For example, we have the following simple corollary.

Corollary 2.2.5. *If $d > 1$ is a divisor of $q-1$, then there is no permutation polynomial of $\mathbb{F}_q$ of degree d.*

Determining if a polynomial defines a permutation can also be done by using additive characters over finite fields.

Theorem 2.2.6. *Let $\mathbb{F}_q$ be a finite field of q elements. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0, \text{ for all nontrivial } \chi \in \widehat{\mathbb{F}_q}.$$

Some classes of permutation polynomials can be obtained by simple elementary results.

Theorem 2.2.7. *The monomial $x^s \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if* $\gcd(s, q-1) = 1$.

Theorem 2.2.8. *Every degree-1 affine polynomial over $\mathbb{F}_q$ is a permutation polynomial over $\mathbb{F}_q$.*

Since composition of permutation polynomials again yields permutations, we immediate obtain classes of permutation polynomials.

Corollary 2.2.9. *Let $f \in \mathbb{F}_q[x]$ be a permutation polynomial. Then $af(cx + d) + b$ is also a permutation polynomial.*

As a consequence of Corollary 2.2.9, we often consider only monic polynomials. Further compositions can exploit Hermite's Criterion to give even broader classes of permutation polynomials.

Theorem 2.2.10. [43, Theorem 7.10] *Let $r \in \mathbb{N}$ with* $\gcd(r, q-1) = 1$ *and let s be a positive divisor of $q-1$. Let $g \in \mathbb{F}_q[x]$ be such that $g(x^s)$ has no nonzero root in $\mathbb{F}_q$. Then $f(x) = x^r g(x^s)^{(q-1)/s}$ is a permutation polynomial of $\mathbb{F}_q$.*

The permutation behaviour of special functions over finite fields is considered in Chapter 3. Information about the images of functions which do not define permutations is further studied in Section 3.6.

2.3 Costas arrays and related combinatorial objects

In this section we give many definitions of combinatorial objects which have similar properties to the functions we discuss in Chapter 3 and Part II of the thesis. In the following definitions, we follow the notation given in [24]. We introduce the notation $[n] = \{0, 1, \ldots, n-1\} \subset \mathbb{Z}$ and $\mathbb{Z}_m$ to denote the integers modulo m.

Definition 2.3.1.

1. *A permutation* $f\colon [n] \to [n]$ *is* Costas *if, for all* $i, j, k \in [n]$ *with* $(i+k), (j+k) \in [n]$, $f(i+k) - f(i) = f(j+k) - f(j)$ *implies* $k = 0$ *or* $i = j$.

2. *A permutation* f *is* domain-periodic Costas *modulo* m *if, for all* $i, j, k \in [n]$, $f(i+k \pmod m) - f(i) = f(j+k \pmod m) - f(j)$ *implies* $k = 0$ *or* $i = j$.

3. *A permutation* f *is* range-periodic Costas *modulo* m *if, for all* $i, j, k \in [n]$ *with* $(i+k), (j+k) \in [n]$, $f(i+k) - f(i) \pmod m = f(j+k) - f(j) \pmod m$ *implies* $k = 0$ *or* $i - j$.

Definition 2.3.2. *Let* f *be a bijection of* $[n]$ *and construct the* $n \times n$ *array such that there is a dot in the* (x, y) *position if* $f(y) = x$ *and a blank otherwise. If* f *is a Costas permutation, then* f *is a* Costas array.

Costas arrays are motivated by applications in RADAR and SONAR systems [32]. The Costas property implies that in any superimposed translation of the array there is at most one overlapping pair of dots. If one axis measures time-shift and the other frequency-shift, then the overlapping dot will correspond to the target's true position and velocity, respectively. We now give the two algebraic constructions of Costas arrays, both due to [31].

Theorem 2.3.3. *(Welch Construction of Costas arrays) Let* p *be a prime and let* a *be a primitive element of* $\mathbb{F}_p$. *The* $(p-1) \times (p-1)$ *array given by placing a dot at position* (x, y) *whenever* $a^y \equiv x \pmod p$ *is a Costas array of order* $p - 1$.

Theorem 2.3.4. *(Golomb construction of Costas arrays) Let* q *be a prime power and let* b *and* c *be primitive elements of* $\mathbb{F}_q$. *The* $(q-2) \times (q-2)$ *array given by placing a dot at position* (x, y) *whenever* $b^x + c^y = 1$ *is a Costas array*

We now present one doubly-periodic Costas permutation and one range-periodic Costas sequence, due to [24].

Definition 2.3.5. *Let* p *be a prime and let* g *be a primitive element of* $\mathbb{F}_p$. *The* exponential Welch-Costas *bijection* $f\colon \mathbb{Z}_{p-1} \to \mathbb{F}_p^*$ *is defined by* $f(i) = g^i$.

Theorem 2.3.6. [25] *Exponential Welch-Costas bijections are domain-periodic modulo* $p-1$ *and range-periodic modulo* p*.*

Definition 2.3.7. *Let* f *be an exponential Welch-Costas bijection. The* logarithmic Welch-Costas *bijection* $h\colon \mathbb{F}_p^* \to \mathbb{Z}_{p-1}$ *is the inverse permutation of* f *and is given by* $h(i) = \log_g(i)$*.*

Theorem 2.3.8. [25] *Logarithmic Welch-Costas bijections are range-periodic modulo* $p-1$*.*

We return to exponential and logarithmic Welch-Costas bijections in Section 3.4. We conclude by giving a definition of a special type of Costas sequence which we use in Chapter 7.

Definition 2.3.9. *Let* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ *be a permutation of the integers* $1, 2, \ldots, n$*. If, in addition, the differences* $\alpha_{i+k} - \alpha_i$*,* $i = 0, 1, \ldots, n-1$*, are distinct, where the elements are considered modulo* $n+1$ *and the subscripts are considered modulo* n*, the sequence* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ *is a* circular Costas sequence*.*

The work in Chapter 7 is motivated by the work in [33] on the following conjecture.

Conjecture 2.3.10. *Any circular Costas sequence is an exponential Welch-Costas bijection.*

Chapter 3

Special functions

In this chapter we consider functions having special properties over finite fields. Since we are interested in studying the difference maps (Definition 2.1.2) of functions between finite groups, functions over finite fields are natural candidates. Linearized polynomials play a prominent role throughout this work, and they are introduced in Section 3.1. We present some results on Dickson polynomials in Section 3.2. Dickson polynomials are well-studied and under certain conditions define either monomials or linearized polynomials. Planar functions and almost perfect non-linear functions are discussed in Sections 3.3 and 3.4. These functions have the optimal differential properties which make them desirable for use in symmetric-key cryptography. Results on Dembowski-Ostrom polynomials are given in Section 3.5. Dembowski-Ostrom polynomials have the remarkable property that their difference maps are linearized polynomials. The value set of a polynomial is given by its set of images in the co-domain. Some introductory works on value sets of polynomials are given in Section 3.6, including some new results on the value sets of linearized polynomials. In Section 3.7, we introduce a new kind of value set, the subfield value set, giving the number of images of a polynomial which exist in a subfield of the extension. In Section 3.7, we also compute the subfield value sets for monomials, linearized polynomials and Dickson polynomials.

3.1 Linearized polynomials over finite fields

Linearized polynomials play an important role in this thesis. Here, we give the definition and some basic results about linearized polynomials. In Section 3.6.2 and Section 3.7, we discuss further some properties about their value sets, which will be necessary in later chapters.

Definition 3.1.1. *A polynomial of the form*

$$L(x) = \sum_{i=0}^{n} a_i x^{q^i} \in \mathbb{F}_{q^e}[x]$$

is a linearized polynomial *over* $\mathbb{F}_{q^e}$.

Linearized polynomials are particularly useful because they define linear operators over finite fields; that is $L(\alpha + \beta) = L(\alpha) + L(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^e}$ and $L(c\alpha) = cL(\alpha)$ for all $c \in \mathbb{F}_q$ and all $\alpha \in \mathbb{F}_{q^e}$. We also introduce a strongly related class of polynomials, namely *affine* polynomials.

Definition 3.1.2. *A polynomial $A(x) = L(x) - \alpha$, where L is a linearized polynomial over $\mathbb{F}_{q^e}$ and $\alpha \in \mathbb{F}_{q^e}$, is an* affine *polynomial over $\mathbb{F}_{q^e}$.*

Often, affine polynomials are referred to as *affine q-polynomials* to distinguish them from degree-1 affine polynomials. Since linear polynomials define linear operators, we give a simple condition to determine when they define permutations of the finite field.

Theorem 3.1.3. *Let L be a linearized polynomial over $\mathbb{F}_q$. Then L is a permutation polynomial if and only if L has no non-zero roots in $\mathbb{F}_q$.*

We give an equivalent condition for when linearized polynomials define permutations in Section 3.6.2 which also provides the cardinality of the image of the linearized polynomial when it does not define a permutation.

3.2 Dickson polynomials

In this section, we define the *Dickson polynomials* and outline some of their useful properties for this work. For a treatise on Dickson polynomials, see [42]. For more general forms of Dickson

polynomials, see [49, Section 9.5].

The elementary symmetric polynomials x_1+x_2 and x_1x_2 form a $\mathbb{Z}$-basis of the ring of symmetric polynomials in $\mathbb{Z}[x_1, x_2]$. Thus, there exists a polynomial $F \in \mathbb{Z}[x_1, x_2]$ such that $x_1^n + x_2^n = F(x_1+x_2, x_1x_2)$. Waring's formula [43, Theorem 1.76] gives an explicit expression for the polynomial F:

$$x_1^n + x_2^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-x_1x_2)^i(x_1+x_2)^{n-2i}.$$

Definition 3.2.1. *Let n be a positive integer. The* Dickson polynomial of the first kind *of degree n and parameter a is given by*

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}. \tag{3.1}$$

Proposition 3.2.2. *The Dickson polynomial with parameter 0 is a monomial, that is $D_n(x, 0) = x^n$.*

Dickson polynomials satisfy the functional equation

$$x^n + \frac{a^n}{x^n} = D_n\left(x + \frac{a}{x}, a\right). \tag{3.2}$$

Dickson polynomials can also be defined recursively: let $D_0(x, a) = 2$, $D_1(x, a) = x$ and for $n \geq 2$

$$D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a).$$

Dickson originally studied these polynomials to determine their permutation properties over finite fields.

Theorem 3.2.3. [43, Theorem 7.16] *Suppose $a \neq 0$, then the Dickson polynomial $D_n(x, a)$ induces a permutation of $\mathbb{F}_q$ if and only if* $\gcd(n, q^2 - 1) = 1$.

3.2.1 Reversed Dickson polynomials

Interchanging the role of the parameter of Dickson polynomials and the indeterminate also yield interesting polynomials. We investigate the differential properties of reversed Dickson polynomials

n	condition
$2^k + 1$	$(k, 2e) = 1$ (Gold)
$2^{2k} - 2^k + 1$	$(k, 2e) = 1$ (Kasami)
$2^e + 2^k + 1$, $k > 0$	$(k - 1, e) = 1$, e even
$2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$	$e = 5k$ (Dobbertin)

Table 3.1: Reversed Dickson permutation polynomials, $D_n(1, x)$, over $\mathbb{F}_{2^e}$.

n	condition
$p^e + 2$	$p^e \equiv 1 \pmod 3$
$\frac{3^k+1}{2}$	$p = 3$, $(k, 2e) = 1$
$3^e + 5$	$p = 3$, e even
$\frac{5^k+1}{2}$	$p = 5$, $(k, 2e) = 1$

Table 3.2: Reversed Dickson permutation polynomials, $D_n(1, x)$, over $\mathbb{F}_{p^e}$, $p \neq 2$.

in Section 8.2.

Definition 3.2.4. *Let n be a positive integer. The* reversed Dickson polynomial *of degree n and parameter a is given by*

$$D_n(a, x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}. \tag{3.3}$$

The reversed Dickson polynomial $D_n(0, x)$ is a permutation of $\mathbb{F}_q$ if and only if $\gcd(n, q-1)$. In addition, for $a \neq 0$ it follows from Equation (3.1) that $D_n(a, x) = a^n D_n(1, xa^{-2})$ and hence $D_n(a, x)$ is a permutation of $\mathbb{F}_q$ if and only if $D_n(1, x)$ is a permutation on $\mathbb{F}_q$. The permutation property of reversed Dickson polynomials is studied in [39] and the authors note that reversed Dickson polynomials are closely related to almost perfect non-linear functions, see Section 3.4. Necessary conditions for reversed Dickson polynomials to be permutations are given in [38], and permutation polynomials related to reversed Dickson polynomials are given in [37]. A summary of cases for which reversed Dickson polynomials define permutations over $\mathbb{F}_{2^e}$ is given in Table 3.1. A similar table for reversed Dickson permutation polynomials over higher characteristic is given in Table 3.2.

3.3 Planar (perfect non-linear) functions

Planar functions were first studied by Dembowski and Ostrom [19] while investigating collineation groups of projective geometries. We cite an equivalent definition of planar functions.

Definition 3.3.1. *Let G_1 and G_2 be finite groups. A function $f\colon G_1 \to G_2$ is a* planar function *if both $\Delta_{f,a}(x) = f(x+a)-f(x)$ and $\nabla_{f,a}(x) = -f(x)+f(x+a)$ are bijections for all $a \in G_1^* = G_1\backslash\{0\}$.*

If the group G_2 is Abelian, it is clear that $\Delta_{f,a} = \nabla_{f,a}$, and if $G_1 = G_2$ and f is planar, then $\Delta_{f,a}$ and $\nabla_{f,a}$ are permutations. The function $\Delta_{f,a}$ is the difference map of f with parameter a and is introduced in Defintion 2.1.2. This function is the keystone upon which this thesis is built.

Definition 3.3.2. *Suppose $L : G_1 \to G_2$ is a mapping between finite groups G_1 and G_2. The function L is* additive *on G_1 if $L(x + y) = L(x) + L(y)$ for all $x, y \in G_1$ (that is, if L is a homomorphism).*

If $G_1 = G_2 = (\mathbb{F}_q, +)$, then any additive function is a $\mathbb{F}_p$-linear transformation over $\mathbb{F}_q$. Polynomials which induce these linear mappings are linearized polynomials, see Definition 3.1.1. The planar property is preserved under linear shift, that is, if f is planar than so is $f(ax + b) + c$, for $a, b, c \in \mathbb{F}_q$. More generally, planarity is preserved under composition of additive polynomials in the following way.

Theorem 3.3.3. [17] *Let $f \in \mathbb{F}_q[x]$ and let $L \in \mathbb{F}_q[x]$ be an linearized polynomial. The following are equivalent:*

(a) $f(L)$ is a planar polynomial;

(b) $L(f)$ is a planar polynomial;

(c) f is a planar polynomial and L is a linearized polynomial.

Johnson [40] first showed that a monomial $f(x) = x^j \in \mathbb{F}_p[x], p > 2$ is planar if and only if $j = 2$. The following theorem was independently and simultaneous obtained by Rónyai and Szőnyi [58] and Gluck [29] using Segre's theorem from finite geometries, and by Hiramine [36] using Hermite's Criterion, see Theorem 2.2.4.

Theorem 3.3.4. *Let p be an odd prime. Then $f \in \mathbb{F}_p[x]$ be a planar polynomial only if f is quadratic.*

Polynomial	Condition
$x^{p^\alpha+1}$	$e/\gcd(\alpha, e)$ is odd
$x^{10}+x^6-x^2$	$p=3$, $e=2$ or e is odd
$x^{(3^\alpha+1)/2}$	$\gcd(\alpha, e)=1$ and α is odd
$x^{(3^\alpha+q)/2}$	$\gcd(\alpha, e)=1$ and $\alpha-e$ is odd

Table 3.3: Planar functions over $\mathbb{F}_q$, $q=p^e$ [17].

We use Hiramine's method in Chapter 7 to give a partial solution to a conjecture on multiplicative analogue of planar functions.

In the broader extension field case, we do not have such tight restrictions on f. For monomial functions, we have $(x+a)^n - x^n$ is planar if and only if $a^n\left((x/a+1)^n-(x/a)^n\right)$ is planar, and thus we restrict our attention to $\Delta_{x^n,1}$.

Theorem 3.3.5. [17] *A monomial x^n over $\mathbb{F}_q$ is planar if and only if $(x+1)^n - x^n$ is a permutation polynomial over $\mathbb{F}_q$. Furthermore, if x^n is planar, then $n \equiv 2 \pmod{p-1}$ and $(n, q-1)=2$.*

A series of planar functions over non-prime finite fields is obtained in [17]. We give these in Table 3.3.

3.4 Almost perfect non-linear functions

A planar function f has the property that the difference maps $\Delta_{f,a}(x) = f(x+a) - f(x)$ and $\nabla_{f,a}(x) = -f(x) + f(x+a)$ are permutations. When f is a mapping between Abelian groups, of course we consider only the $\Delta_{f,a}$ maps.

Definition 3.4.1. *Let G_1 and G_2 be Abelian groups and let $f\colon G_1 \to G_2$. If $\Delta_{f,a}(x) = f(x+a)-f(x)$ is one-to-one for all $a \in G_1^*$, then f is* perfect non-linear *(PN).*

Perfect non-linear permutations do not exist since $\Delta_{f,a}(x) \neq 0$ and thus, by the Pigeon-Hole Principle, there must be a repeated element of the image set of $\Delta_{f,a}$. Furthermore, perfect non-linear functions cannot exist when G_1 is a 2-group because $\Delta_{f,a}(x) = \Delta_{f,a}(x+a)$. Since the additive groups of finite fields of characteristic 2 are the most important for implementations, we give an alternate definition for the best-possible differential structure of a function over a 2-group.

Functions	Exponent d	Conditions	Reference
Gold	2^k+1	$\gcd(k,e)=1$	[52]
Welch	2^k+3	$e=2k+1$	[22]
Inverse	$2^{2k}-1$	$e=2k+1$	[52]
Kasami	$2^{2k}-2^k+1$	$\gcd(k,e)=1$	[41]
Niho (even)	$2^k+2^{\frac{k}{2}}-1$, k even	$e=2k+1$	[21]
Niho (odd)	$2^k+2^{\frac{3k+1}{2}}-1$, k odd	$e=2k+1$	[21]
Dobbertin	$2^{4k}+2^{3k}+2^{2k}+2^k-1$	$e=5k$	[23]

Table 3.4: Known APN monomial functions x^d on $\mathbb{F}_{2^e}$.

Exponent	Condition
3	$p \neq 3$
p^e-3	$p=3$ and e odd
p^e-2	$p \equiv 2 \pmod 3$
$p^{e/2}+2$	$p>3$, e even and $p^{e/2} \equiv 1 \pmod 3$
$p^{(e+1)/2}-1$	$p=3$ and e odd
$\frac{2p^e-1}{3}$	$p^e \equiv 2 \pmod 3$
$\frac{p^k+1}{2}$	$p=5$ and $\gcd(2e,k)=1$

Table 3.5: Known APN monomial functions $x^d \in \mathbb{F}_{p^e}$, p odd [34].

Definition 3.4.2. *Let G_1 and G_2 be Abelian groups and let $f\colon G_1 \to G_2$. If $\Delta_{f,a}(x)=f(x+a)-f(x)$ is at most two-to-one for all $a \in G_1^*$, then f is* almost perfect non-linear *(APN).*

Almost perfect non-linear functions between finite fields of characteristic two are highly desired for their use in symmetric key cryptosystems due to their resistance to differential cryptanalysis, see Section 4.2. Even still, APN functions are not well understood and no non-trivial characterizations of APN functions are known. Furthermore, few classes of APN functions over finite fields are known; in Table 3.4 and Table 3.5 we present a list of known APN monomial functions over $\mathbb{F}_{2^e}$ and over $\mathbb{F}_{p^e}$, respectively.

In most applications, candidate functions for use in symmetric key cryptosystems must be permutations. Furthermore, for implementation purposes, functions over $\mathbb{F}_{2^e}$ with e even are preferred. Combining these criteria, the most desirable candidate functions are APN permutations over $\mathbb{F}_{2^e}$ where e is even.

Problem. Find APN permutations over $\mathbb{F}_{2^e}$, when e is even.

Currently, there is *only one* known APN permutation over $\mathbb{F}_{2^e}$, when e is even. This function was introduced by Dillon in [6]. We do not give the polynomial here, since it has more than 50

terms.

The definition of PN and APN functions appears to coincide with the the definition of the variants of Costas permutations from Definition 2.3.1. However, each variant involves addition in the (infinite) group $\mathbb{Z}$, and so does not fit our general framework directly. However, using the modular variants, namely exponential Welch-Costas bijections (Definition 2.3.5) and logarithmic Welch-Costas bijections (Definition 2.3.7), we find APN permutations over finite rings.

Theorem 3.4.3. [25]

1. *Let p be a prime. Let f be an exponential Welch-Costas bijection $\mathbb{Z}_{p-1} \to \mathbb{F}_p^*$. Let $g(i) = f(i) - 1$. Then g is an APN permutation over $\mathbb{Z}_{p-1}$.*

2. *Let f be a Costas permutation $\{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, n-1\}$. Then $h \colon \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $h(i+j) = f(i+j \pmod n)$ is an APN permutation.*

3. *Let h be the inverse permutation of g from Case 1. Then h is an APN permutation of $\mathbb{Z}_{p-1}$. Furthermore, $\Delta_{f,a}$ is a permutation for all $a \neq p-1, p-1-a$.*

There is an abuse of notation in Case 2. of Theorem 3.4.3. The co-domain of f is $\{0, 1, \ldots, n-1\}$, not $\mathbb{Z}_n$, and hence h is not defined over finite groups. However, identifying the images as the elements of $\mathbb{Z}_n$ gives the required inclusion.

The SAFER cryptosystem uses a special case of both exponential and logarithmic Welch-Costas permutations in its S-boxes, where $p = 257$. Thus, the functions used in SAFER are APN. See Section 4.4.2 for more information on SAFER.

The Advanced Encryption Standard (AES) is the most commonly used block-cipher. The S-boxes of AES use the inverse function over the finite field with $2^8 = 256$ elements. For more details on AES, see Section 4.4.1. For motivation, we state a result which will appear later.

Theorem 3.4.4. (Proposition 4.4.1) *The inverse function $f(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ is at most 4-to-1 when n is even and at most 2-to-1 when n is odd.*

The previous result motivates the following definition.

Definition 3.4.5. *Let G_1 and G_2 be finite groups and let $f\colon G_1 \to G_2$. Then f has* differential uniformity *equal to k if $\Delta_{f,a}(x) = f(x+a) - f(x)$ is at most k-to-one for all $a \in G_1^*$. We also say that f is differential-k-uniform.*

The Advanced Encryption Standard has been the NIST FIPS-197 [27] standard for symmetric key encryption since 2001, and the known exploits of AES are still impractical. Thus, AES is still considered secure, even though it uses a differential-4-uniform function in its S-boxes. In Section 4.4.1, we show that AES is somehow "minimally" differential-4-uniform. This indicates that, while differential uniformity is a practical measure for resistance against differential cryptanalysis, it may be too coarse. Conversely, we would like to have the entire differential spectrum of a function, but we do not even have characterizations of differential-k-uniformity in most cases.

In Part II of this thesis, we give a measure on functions between finite groups which is related to, but finer than, differential uniformity. We introduce our measure in Section 5.1.

3.5 Dembowski-Ostrom polynomials

The Dembowski-Ostrom polynomials were considered in [19], where the authors consider projective planes of order n which admit a collineation group of order n^2.

Definition 3.5.1. *The polynomials (in reduced form) of the shape*

$$f(x) = \sum_{i,j=0}^{n} a_{ij} x^{p^i+p^j} \in \mathbb{F}_q[x]$$

are Dembowski-Ostrom *(or DO) polynomials.*

We consider the slightly more general case when the polynomial is considered over any extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ and each exponent is of the form $q^i + q^j$. In [19], DO polynomials are given as an example of planar functions. In particular, the authors show the following.

Theorem 3.5.2. *[19] Suppose $f(x)$ is a DO polynomial with coefficients a_{ij} such that*

$$\sum_{i,j=0}^{n-1} a_{ij}\left(x^{p^i}y^{p^j} + x^{p^j}y^{p^i}\right) = 0 \text{ if and only if } x = 0 \text{ or } y = 0,$$

then f is planar.

In [19], the authors (weakly) conjecture that every planar polynomial over $\mathbb{F}_q$ is a DO polynomial, up to addition of a linearized polynomial. A counterexample to this conjecture is given in [17]. A characterization of DO polynomials in terms of their difference polynomials is also given in [17].

Theorem 3.5.3. [17] *Let $f \in \mathbb{F}_q[x]$ with $\deg(f) < q$. Then $f = D + L + c$, where D is a DO polynomial, L is a linearized polynomial and $c \in \mathbb{F}_q$ is a constant, if and only if for each $a \in \mathbb{F}_q^*$, $\Delta_{f,a} = L_a + c_a$, where L_a is a linearized polynomial and $c_a \in \mathbb{F}_q$ is a constant.*

The simplest non-trivial case of DO polynomials is when one of the q-exponents is 0. When the characteristic $p = 2$, these polynomials are the *Gold* polynomials and conditions for Gold polynomials to be planar are known. We recover many results on Gold polynomials (and their q-ary analogue) using a new technique in Section 6.1.

Theorem 3.5.4. [17] *Let $f(x) = x^{p^n+1} \in \mathbb{F}_q[x]$. Then f is planar over $\mathbb{F}_q$ if and only if $e/(n,e)$ is odd.*

There are few cases of DO polynomials where their permutation behaviour is known. In Theorems 3.5.5 and 3.5.6 we summarize many interesting cases in the literature. First, we observe that any DO polynomial F can be written as $F(x) = (xL(x)) \circ x^{p^i}$ for some i. Since raising to a pth power is an isomorphism, it does not affect the permutation behaviour of the polynomial, and so we consider only DO polynomials of the form $F(x) = xL(x)$.

Theorem 3.5.5. [3] *Let $q = 2^e$ and β be any primitive element of $\mathbb{F}_q$. Let k be any integer and set $d = (k, e)$. Suppose $F \in \mathbb{F}_q[X]$ is a DO polynomial satisfying $F(x) = xL(x)$ for some linearized polynomial L. Then F permutes $\mathbb{F}_q$ when any of the following conditions are satisfied:*

1. *$L(x) = x^{2^k}$ where e/d is odd;*

2. $L(x) = x^{2^k} + cx^{2^{e-k}}$ *where* e/d *is odd and* $c \neq \beta^{t(2^d-1)}$ *for any integer* t*;*

3. $L(x) = x^{2^{2k}} + c^{2^k+1}x^{2^k} + cx$ *where* $e = 3k$ *and* $c \neq \beta^{t(2^d-1)}$ *for any integer* t*.*

Theorem 3.5.5 gives direct constructions of DO polynomials with low weight (that is, having few non-zero terms). The next theorem is analogous and gives DO polynomials due to certain trace functions.

Theorem 3.5.6. [3, 14] *Let the p-weight of a number be the number of terms in its p-ary expansion. Then,*

1. *Let* q *be even and* e *be odd. The polynomial* $F \in \mathbb{F}_{q^e}[x]$ *defined by*

$$F(x) = x(\mathrm{Tr}(x) + sx), \tag{3.4}$$

is a permutation polynomial of $\mathbb{F}_{q^e}$ *for all* $s \in \mathbb{F}_q \setminus \{0, 1\}$*.*

2. *Let* $1 \leq k \leq e-1$ *and* $1 \leq s \leq 2^e - 2$*. The polynomial* $F \in \mathbb{F}_{2^e}[x]$ *defined by*

$$F(x) = x^{2^k} + x + \mathrm{Tr}\left(x^s\right) \tag{3.5}$$

is a permutation polynomial over $\mathbb{F}_{2^e}$ *if and only if*

   (a) e *is odd,*

   (b) $\gcd(k, e) = 1$

   (c) s *has* 2*-weight* 1 *or* 2*.*

3. *Let* $d \geq 1$ *and* $t \leq 2^e - 2$*. The polynomial* $F \in \mathbb{F}_{2^e}[x]$ *defined by*

$$F(x) = x^d + \mathrm{Tr}\left(x^t\right) \tag{3.6}$$

is a permutation polynomial over $\mathbb{F}_{2^e}$ *if and only if*

   (a) e *is even,*

(b) $\gcd(d, 2^e - 1) = 1$

(c) $t \equiv s \cdot d \pmod{2^e - 1}$ *for some* $1 \leq s \leq 2^e - 2$, s *has* 2*-weight* 1 *or* 2.

For each polynomial given in Theorem 3.5.6, if the 2-weight of s is 1, then the polynomials are linearized and if the 2-weight of s is 2, the polynomials are DO.

We show another family of DO binomials which define APN functions.

Theorem 3.5.7. [7] *Let* s *and* k *be positive integers with* $\gcd(s, 3k) = 1$ *and* $t \in \{1, 2\}, i = 3 - t$. *Furthermore, let*

$$d = 2^{ik} + 2^{tk+s} - (2^s - 1),$$

$$g_1 = \gcd(2^{3k} - 1, d/(2^k - 1)),$$

$$g_2 = \gcd(2^k - 1, d/(2^k - 1)),$$

and let α *be a primitive element of* $\mathbb{F}_{2^{3k}}$. *If* $g_1 \neq g_2$, *then the function*

$$F(x) = x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}}$$

is almost perfect non-linear on $\mathbb{F}_{2^{3k}}$.

Corollary 3.5.8. [7] *Let* s *and* k *be positive integers such that* $\gcd(k, 3) = \gcd(s, 3k) = 1$ *and let* $i \equiv sk \pmod 3, t \equiv 2i \pmod 3$, $n = 3k$ *and* α *be a primitive element of* $\mathbb{F}_{2^n}$. *Then the function*

$$F(x) = x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}}$$

is APN on $\mathbb{F}_{2^n}$. *Furthermore,*

1. *F is a permutation if and only if k is odd,*

2. *F is extended-affine inequivalent to any monomial (see Section 5.3.3).*

Extended-affine and Carlet-Charpin-Zinoviev equivalence are discussed in Section 5.3.3. Essentially, the conclusion of Item 2. of Corollary 3.5.8 is that F is genuinely a new class of APN

polynomials. Another class of polynomials with the same structure as those in Theorem 3.5.7, now with n a multiple of 4, are also given in [7].

3.6 Value sets of non-permutations

When a polynomial does not define a permutation, information about its images is still desirable. In particular, studying the number of distinct images of difference maps and the number of repetitions of each image is critical in this thesis. For example, a function is APN over $\mathbb{F}_{2^e}$ if each of its difference maps have exactly 2^{e-1} distinct images, each repeated twice.

Definition 3.6.1. *Let R be an integral domain and let $f \in R[x]$. The* value set *of f, denoted V_f is given by*

$$V_f = \{f(x) \colon x \in R\}.$$

If f is a permutation polynomial, then $V_f = R$.

Though we are principally concerned with polynomials over integral domains (more specifically, over finite fields or the ring $\mathbb{Z}_n$), the value set of any function between finite groups is given by the set of its images in the co-domain.

Consider $f \in \mathbb{F}_q[x]$ of degree d, then since f can take any image at most d times we have $|V_f| \geq q/d$, or alternatively $|V_f| \geq \lfloor (q-1)/d \rfloor + 1$. Polynomials which meet this lower bound have *minimal value sets*. The case where f is single or double-valued is treated in [13] as well as a complete characterization of all polynomials with minimal value sets when $q = p$. The proofs in [13] are shortened and extended to the case $q = p^2$ in [48].

We restrict our attention to value sets of polynomials which we consider later.

3.6.1 Value sets of monomials

The value sets of monomials over finite fields is well-known and is easy to derive.

Theorem 3.6.2. [16] *Let $x^n \in \mathbb{F}_{q^e}[x]$ and denote by V_{x^n} the value set of x^n. Then,*

$$V_{x^n} = \frac{q^e - 1}{(n, q^e - 1)} + 1.$$

3.6.2 Value sets of linearized polynomials

In this section, we study the value sets of linearized polynomials. Corollary 3.6.4 appears in [16].

Suppose L is a linearized polynomial. Since linearized polynomials define linear operators over finite fields, by the first isomorphism theorem we have $\mathbb{F}_{q^e}/\ker(L) \cong V_L$, where $\ker(L)$ denotes the kernel of L and V_L is the value set (or image space) of L. Thus, every image of L has an equal number of preimages, which is equal to $q^{\dim(\ker(L))}$.

Theorem 3.6.3. [43, Page 362] *For any linearized polynomial $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i} \in \mathbb{F}_{q^e}$, denote by A the matrix*

$$\begin{bmatrix} a_0 & a_{e-1}^q & \cdots & a_1^{q^{e-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ a_{e-1} & a_{e-2}^q & \cdots & a_0^{q^{e-1}} \end{bmatrix}. \tag{3.7}$$

Then L is a permutation polynomial over $\mathbb{F}_{q^e}$ if and only if $\det(A) \neq 0$.

Matrices of the form given in Equation (3.7) are sometimes called *auto-circulant*, where "auto" means that an automorphism of the Galois group is applied to a circulant matrix at each column. The same matrix also provides the cardinality of the value set of L.

Corollary 3.6.4. [16] *Let $L(x) = \sum_{i=0}^{e-1} \alpha_i x^{q^i} \in \mathbb{F}_{q^e}[x]$ be a linearized polynomial and let A be its corresponding matrix from Equation* (3.7)*. Then the value set of L, V_L, satisfies $|V_L| = q^{\mathrm{rk}(A)}$ and the number of preimages of each image is given by $q^{e-\mathrm{rk}(A)}$.*

Proof. Fix a basis $\{\beta_0, \beta_1, \ldots, \beta_{e-1}\}$ of $\mathbb{F}_{q^e}$ over $\mathbb{F}_q$ and let $\gamma_i = L(\beta_i)$, $i = 0, 1, \ldots, e-1$.

For $0 \leq i, j \leq e-1$ we have

$$\gamma_i^{q^j} = \sum_{s=0}^{e-1} \alpha_s^{q^j} \beta_i^{q^{s+j}},$$

and taking subscripts $\pmod e$, we have

$$\gamma_i^{q^j} = \sum_{s=0}^{e-1} \alpha_{s-j}^{q^j} \beta_i^{q^s}.$$

We therefore have a matrix equation relating the conjugates of the γ_i, β_i and α_{s-j} of the following form

$$\begin{bmatrix} \gamma_0 & \gamma_0^q & \cdots & \gamma_0^{q^{e-1}} \\ \gamma_1 & \gamma_1^q & \cdots & \gamma_1^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \gamma_{e-1} & \gamma_{e-1}^q & \cdots & \gamma_{e-1}^{q^{e1}} \end{bmatrix} = \begin{bmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{e-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{e-1} & \beta_{e-1}^q & \cdots & \beta_{e-1}^{q^{e-1}} \end{bmatrix} \begin{bmatrix} \alpha_0 & \alpha_{e-1}^q & \cdots & \alpha_1^{q^{e-1}} \\ \alpha_1 & \alpha_0^q & \cdots & \alpha_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_{e-1} & \alpha_{e-2}^q & \cdots & \alpha_0^{q^{e-1}} \end{bmatrix}.$$

Labeling the corresponding matrices Γ, B and A respectively, by [43, Corollary 2.38] the matrix B is non-singular and thus the rank of Γ is equal to the rank of A. Since the value set of the linearized polynomial L is equal to the image set of the linear operator, we have $|V_L| = q^{\mathrm{rk}(A)}$. □

3.6.3 Value sets of Dickson polynomials

Dickson polynomials were introduced in Section 3.2. The results from this section come from [15]. We note that further results on the *subfield value set* of Dickson polynomials, that is the set of images of a Dickson polynomial which fall within a subfield of the original field, are discussed in Section 3.7.

In this section we use the notation $\alpha^r || \beta$ to mean that r is the highest power of α dividing β. We also denote by η the quadratic character of $\mathbb{F}_q$, hence $\eta(\alpha) = 1$ if α is a quadratic residue in $\mathbb{F}_q$ (that is, $\alpha = \beta^2$ for some $\beta \in \mathbb{F}_q$), otherwise $\eta(\alpha) = -1$.

Theorem 3.6.5. [15] *For each $d \geq 1$ and for each $a \in \mathbb{F}_q^*$ denote the Dickson polynomial of the first kind with degree d and parameter a by $D_d(x, a)$. Then*

$$|V_{D_d(x,a)}| = \frac{q-1}{2\gcd(d, q-1)} + \frac{q+1}{2\gcd(d, q+1)} + \alpha,$$

where

$$\alpha = \begin{cases} 1 & \text{if } q \text{ is odd, } 2^{r-1}||d \text{ and } \eta(a) = -1, \\ 1/2 & \text{if } q \text{ is odd, } 2^t||d \text{ with } 1 \leq t \leq r-2, \\ 0 & \text{otherwise.} \end{cases}$$

3.7 Subfield value sets

This section concerns value sets of functions over finite fields, where the values lay in a subfield. The idea of studying function on extension fields whose imags lie in subfields is a natural one. For example, consider the trace function given in Definition 2.1.3. Suppose d divides e, then the trace function Tr_{q^e/q^d} is a projection map from $\mathbb{F}_{q^e}$ to its subfield $\mathbb{F}_{q^d}$. Moreover, Tr_{q^e/q^d} maps onto $\mathbb{F}_{q^d}$ uniformly in the sense that every image in the subfield $\mathbb{F}_{q^d}$ contains the same number of pre-images in $\mathbb{F}_{q^e}$.

From now on, let $V_f(q^e;q^d) = \{f(c) \in \mathbb{F}_{q^d} : c \in \mathbb{F}_{q^e}\}$ denote the subfield value set of f: the set of images of f in the subfield $\mathbb{F}_{q^d}$ as c ranges over the extension field $\mathbb{F}_{q^e}$. Further let $|V_f(q^e;q^d)|$ denote the cardinality of $V_f(q^e;q^d)$, that is, the number of distinct elements in the image of f that lie in $\mathbb{F}_{q^d}$ as c ranges over the extension field $\mathbb{F}_{q^e}$. As a special case, $V_f(q^e;q^e)$ denotes the usual value set $\{f(c) : c \in \mathbb{F}_{q^e}\}$ of a polynomial f over the field $\mathbb{F}_{q^e}$.

Further, let $N_f(q^e;q^d)$ denote the number of images $f(c)$ (counting multiplicities) of $f : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$ that lie in the subfield $\mathbb{F}_{q^d}$, as c ranges over the elements of the extension field $\mathbb{F}_{q^e}$. We clearly have $|V_f(q^e;q^d)| \leq N_f(q^e;q^d)$, and of course $N_f(q^e;q^e) = q^e$ for any polynomial f over the field $\mathbb{F}_{q^e}$.

In this section, we first present a related notion, namely the König-Rados theorem, which we extend to a subfield theorem. We further consider subfield value sets for several classes of polynomials, namely *linearized polynomials*, *monomials* and *Dickson polynomials*. All of the results in this section appear in [16]. We omit the proof of the subfield value set of Dickson polynomials, since it is lengthy and very technical, and they are not a particular focus of this thesis. We refer the reader to [16] for the proof.

3.7.1 König-Rados theorem for subfields

Let $n > 0$, let $f \in \mathbb{F}_q[x]$ and consider the equation $f(x) = 0$. The distinct roots of f can be found as the roots of $\gcd(f, x^q - x)$, which have multiplicity 1. Thus, the number of distinct solutions of $f(x) = 0$ is equal to the degree of $\gcd(f, x^q - x)$. It is trivial to determine if $f(0) = 0$ and so we consider only the solutions to $\gcd(f, x^{q-1} - 1)$. Furthermore, since $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q$, we may assume, without loss of generality, that $n \leq q-2$ when we consider the number of nonzero solutions of $f(x) = 0$.

The König-Rados Theorem expresses the number of nonzero roots of a polynomial in terms of the rank of a coefficient matrix.

Theorem 3.7.1. [43, Theorem 6.1] *Let q be a power of a prime, let*

$$f(x) = \sum_{s=0}^{q-2} a_s x^s \in \mathbb{F}_q[x]$$

and denote by C the left circulant matrix

$$C = \begin{bmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \cdots & a_{q-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3} \end{bmatrix}.$$

The number of nonzero solutions of the equation $f(x) = 0$ in $\mathbb{F}_q$ is equal to $q - 1 - \mathrm{rk}(C)$, where $\mathrm{rk}(C)$ is the rank of the matrix C.

We further extend the König-Rados Theorem to determine the number of roots of the polynomials occurring within a subfield.

Theorem 3.7.2. *Let q be a power of a prime, and let e, d be positive integers with d dividing e. Let*

$$f(x) = \sum_{s=0}^{q^e-2} a_s x^s \in \mathbb{F}_{q^e}[x],$$

and denote by C and B_d the matrices

$$C = \begin{bmatrix} a_0 & a_1 & \cdots & a_{q^e-3} & a_{q^e-2} \\ a_1 & a_2 & \cdots & a_{q^e-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q^e-2} & a_0 & \cdots & a_{q^e-4} & a_{q^e-3} \end{bmatrix}, \; B_d = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ c_1 & c_2 & \cdots & c_{q^d-1} \\ c_1^2 & c_2^2 & \cdots & c_{q^d-1}^2 \\ \vdots & \vdots & & \vdots \\ c_1^{q^e-2} & c_2^{q^e-2} & \cdots & c_{q^d-1}^{q^e-2} \end{bmatrix},$$

where $c_1, c_2, \ldots, c_{q^d-1}$ are the distinct elements of $\mathbb{F}_{q^d}^*$. Then, the number of non-zero solutions of the equation $f(x) = 0$ in $\mathbb{F}_{q^d}$ is equal to $q^d - 1 - \mathrm{rk}(CB_d)$.

Proof. Let N_d be the number of solutions of $f(x) = 0$ occurring within $\mathbb{F}_{q^d}^*$. Let $c_1, c_2, \ldots, c_{q^d-1}$ be ordered so that $f(c_i) \neq 0$ for $1 \leq i \leq q^d - 1 - N_d$ and $c_{q^d-N_d}, c_{q^d-N_d+1}, \ldots, c_{q^d-1} \in \mathbb{F}_{q^d}^*$. Let the columns of B_d be ordered in this way. Since the elements of $\mathbb{F}_{q^d}^*$ which are solutions of $f(x) = 0$ appear in the final columns of B_d, the final N_d columns of CB_d are equal to 0 and the rank of CB_d is at most $q^d - 1 - N_d$.

Now consider the submatrix E of CB_d

$$E = \begin{bmatrix} f(c_1) & f(c_2) & \cdots & f(c_{q^d-1-N_d}) \\ c_1^{-1}f(c_1) & c_2^{-1}f(c_2) & \cdots & c_{q^d-1-N_d}^{-1}f(c_{q^d-1-N_d}) \\ c_1^{-2}f(c_1) & c_2^{-2}f(c_2) & \cdots & c_{q^d-1-N_d}^{-2}f(c_{q^d-1-N_d}) \\ \vdots & \vdots & & \vdots \\ c_1^{-(q^d-2-N_d)}f(c_1) & c_2^{-(q^d-2-N_d)}f(c_2) & \cdots & c_{q^d-1-N_d}^{-(q^d-2-N_d)}f(c_{q^d-1-N_d}) \end{bmatrix}.$$

The matrix E is non-singular since $\det(E) = f(c_1)f(c_2)\cdots f(c_{q^d-1-N_d}) \cdot \det(E')$, where E' is Vandermonde with defining row $(c_1^{-1}, c_2^{-1}, \ldots, c_{q^d-1-N_d}^{-1})$. Thus, $\mathrm{rk}(CB_d) = q^d - 1 - N_d$. □

3.7.2 Subfield value sets of linearized polynomials

The cardinality of the value set of a linearized polynomial is given by Corollary 3.6.4. In this section, we give the cardinality of the value set of linearized polynomials which occur in subfields.

Lemma 3.7.3. *Let $L \in \mathbb{F}_{q^e}[x]$ be a linearized polynomial with value set of cardinality $q^{\mathrm{rk}(M)}$. Every image is repeated $q^{e-\mathrm{rk}(M)}$ times. Furthermore, $N_L(q^e;q^d) = |V_L(q^e;q^d)|q^{e-\mathrm{rk}(M)}$, where $N_L(q^e;q^d)$ denotes the total number of images of L in $\mathbb{F}_{q^d}$, including repetitions.*

Proof. Since L defines a linear operator $\mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$, we have, by the first isomorphism theorem, $\mathbb{F}_{q^e}/\ker(L) \cong V_L$. Since $\dim(\ker(L)) = e - \mathrm{rk}(M)$, the claim follows. □

The subfield value sets of affine polynomials are less clear. Suppose $L \in \mathbb{F}_{q^e}[x]$ is a linearized polynomial and let $A(x) = L(x) + \alpha$, for some $\alpha \in \mathbb{F}_{q^e}$. Consider the subfield value set of A, $V_A(q^e;q^d)$, for any d dividing e. We have trivially that $|V_A(q^e;q^e)| = |V_L(q^e;q^e)|$. If $\alpha \in \mathbb{F}_{q^d}$, then $|V_A(q^e;q^d)| = |V_L(q^e;q^d)|$.

Example 3.7.4. *Let $L(x) = \mathrm{Tr}_{q^e/q^d}(x)$. Then L is a linearized polynomial and L maps $\mathbb{F}_{q^e}$ onto $\mathbb{F}_{q^d}$. Let $\alpha \in \mathbb{F}_{q^e}$ with $\alpha \notin \mathbb{F}_{q^d}$ and let $A(x) = L(x) + \alpha$. Then $V_A(q^e;q^d) = \emptyset$.*

If $\alpha \in V_L(q^e;q^e)$, that is, if α is an image of L, then for all $\beta \in \mathbb{F}_{q^e}$, $A(\beta) = L(\beta) + \alpha = L(\beta + \gamma)$, where $\alpha = L(\gamma)$. Thus, running over all $\beta \in \mathbb{F}_{q^e}$, we have that $V_L(q^e;q^d) = V_A(q^e;q^d)$ for all d dividing e. If α is not an image of L, then the subfield value set of A depends on the additive cosets of the subfield value set of L. It can be easily verified using a computer algebra package such as SAGE [63], that the cardinalities of subfield value sets of affine polynomials most often vary from the subfield value sets of their corresponding linearized polynomials.

Lemma 3.7.5. *Let q be a power of a prime, and let e be a positive integer. Let $\mathbb{F}_{q^e}$ be the finite field with q^e elements and let L be a linearized polynomial over $\mathbb{F}_{q^e}$ defined by $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$. Then*

$$N_L(q^e;q^d) = \left| \left\{ \beta : \sum_{i=0}^{e-1} \left(a_{e-d+i}^{q^d} - a_i \right) \beta^{q^i} = 0 \right\} \right|$$

and

$$|V_L(q^e;q^d)| = N_L(q^e;q^d)/q^{e-\mathrm{rk}(M)},$$

where M is the matrix given in Equation (3.7).

Proof. Let

$$L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$$

and suppose that $L(\alpha)$ lies in $\mathbb{F}_{q^d}$. That is,

$$L(\alpha)^{q^d} = \sum_{i=0}^{e-1} a_i^{q^d} \alpha^{q^{i+d}} = L(\alpha) = \sum_{i=0}^{e-1} a_i \alpha^{q^i}.$$

Rearranging, we find

$$\sum_{i=0}^{e-1} a_i^{q^d} \alpha^{q^{i+d}} - \sum_{i=0}^{e-1} a_i \alpha^{q^i} = \sum_{i=0}^{e-1} (a_{e-d+i}^{q^d} - a_i)\alpha^{q^i} = 0,$$

where the subscripts are taken (mod e). Thus $L(\alpha)$ lies in the subfield $\mathbb{F}_{q^d}$ of $\mathbb{F}_{q^e}$ if and only if α is a root of the polynomial

$$b(x) = \sum_{i=0}^{e-1} (a_{e-d+i}^{q^d} - a_i) x^{q^i}. \tag{3.8}$$

The final expression for $|V_L(q^e; q^d)|$ is given by Lemma 3.7.3. □

Counting the number of zeroes of the polynomial b in Equation (3.8) can be done by the König-Rados theorem, see Theorem 3.7.1.

Theorem 3.7.6. *Let L be a linearized polynomial over $\mathbb{F}_{q^e}$ given by $L(x) = \sum_{i=0}^{q^e-1} a_i x^i$, that is $a_j = 0$ for $j \neq 1, q, q^2, \ldots, q^{e-1}$. Let C be the left-circulant matrix of size $q^e - 1$ with defining row*

$$\left[0\ b_0\ \underbrace{0 \cdots 0}_{q-2 \text{ times}}\ b_1\ \underbrace{0 \cdots 0}_{q^2-q-1 \text{ times}}\ b_2 \cdots b_{e-2}\ \underbrace{0 \cdots 0}_{q^{e-1}-q^{e-2}-1 \text{ times}}\ b_{e-1}\ \underbrace{0 \cdots 0}_{q^e-q^{e-1}-2 \text{ times}} \right],$$

where b_i are the coefficients of b in Equation (3.8). *Then,*

$$|V_L(q^e; q^d)| = \frac{q^e - \mathrm{rk}(C)}{q^{e-\mathrm{rk}(M)}},$$

where M is given by the matrix in Equation (3.7).

Proof. Theorem 3.7.1 gives the number of non-zero roots of b is $q^e - 1 - \mathrm{rk}(C)$. Since 0 is a root of

b, the claim follows. □

3.7.3 Subfield value sets of monomials and Dickson polynomials

We combine the results of monomials and Dickson polynomials into this section, since the Dickson polynomial with parameter 0 defines a monomial, that is $D_n(x,0) = x^n$. Here we state the subfield value sets of monomials and Dickson polynomials. We refer the reader to [16] for the proofs.

We first show the number of preimages of the subfield value set of a monomial.

Theorem 3.7.7. *Let d be a divisor of e. The number of preimages of the monomial x^n is given by $N_{x^n}(q^e;q^d) = (n(q^d-1), q^e-1)) + 1$.*

Proof. If $\alpha \in \mathbb{F}_{q^e}$, then $\alpha \in \mathbb{F}_{q^d}$ if and only if $\alpha^{q^d} = \alpha$. For $c \in \mathbb{F}_{q^e}^*$, if $(c^n)^{q^d} = c^n$, we have $c^{n(q^d-1)} = 1$. The number of solutions of this equation for $c \in \mathbb{F}_{q^e}^*$, is given by $(n(q^d-1), q^e-1)$, and the result follows. □

Theorem 3.7.8. *Let d be a divisor of e. The cardinality of the subfield value set of the monomial $x^n \in \mathbb{F}_{q^e}[x]$ is given by*

$$|V_{x^n}(q^e;q^d)| = \frac{(n(q^d-1), q^e-1)}{(n, q^e-1)} + 1.$$

Proof. Since the multiplicative group $\mathbb{F}_{q^e}^*$ is cyclic, we have in $\mathbb{F}_{q^e}^*$

$$|V_{x^n}(q^e;q^d)| = \frac{N_{x^n}(q^e;q^d)}{(n, q^e-1)} + 1 = \frac{(n(q^d-1), q^e-1)}{(n, q^e-1)} + 1.$$ □

If $(n, q^e-1) = 1$ and hence x^n is a permutation polynomial on $\mathbb{F}_{q^e}$, then $|V_{x^n}(q^e;q^d)| = N_{x^n}(q^e;q^d) = q^d$ since x^n must map $\mathbb{F}_{q^d}$ onto itself. In fact, if $(n, q^d-1) = 1$, then x^n is a permutation polynomial on $\mathbb{F}_{q^d}$ and so $|V_{x^n}(q^e;q^d)| = q^d$.

We now present the subfield value set of Dickson polynomials, first for q even and then for q odd. When q is odd, even the statement of the theorem is quite technical. We recall that the notation $p^n||m$ implies p^n divides m, but p^{n+1} does not divide m, hence n is the highest non-negative power of p dividing m.

Theorem 3.7.9. [16] *Let q be even and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. Then*

$$N_{D_n(x,a)}(q^e;q^d) = \frac{(q^e-1,n(q^d-1))+(q^e-1,n(q^d+1))-(q^e-1,n)}{2} + \frac{(q^e+1,n(q^d-1))+(q^e+1,n(q^d+1))-(q^e+1,n)}{2}.$$

Theorem 3.7.10. [16] *Let q be even and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. Then*

$$|V_{D_n(x,a)}(q^e;q^d)| = \frac{(q^e-1,n(q^d-1))+(q^e-1,n(q^d+1))}{2(q^e-1,n)} + \frac{(q^e+1,n(q^d-1))+(q^e+1,n(q^d+1))}{2(q^e+1,n)} - 1.$$

Theorem 3.7.11. [16] *Let q be odd and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. For integers m and k, let $\delta_{m<k} = 1$, if $m < k$, and $\delta_{m<k} = 0$, if $m \geq k$. Also, let $\delta_{m=k} = 1$, if $m = k$, and $\delta_{m=k} = 0$, if $m \neq k$. Suppose that $2^r || (q^{2e}-1)$.*

a. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = 1$, then $|V_{D_n(x,a)}(q^e;q^d)| =$*

$$\frac{(q^e-1,n(q^d-1))+(q^e-1,n(q^d+1))}{2(q^e-1,n)} + \frac{(q^e+1,n(q^d-1))+(q^e+1,n(q^d+1))}{2(q^e+1,n)} - \frac{3+(-1)^{n+1}}{2}.$$

b. *If $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = 1$, then $|V_{D_n(x,a)}(q^e;q^d)| =$*

$$-\delta_{r-1<r_n} + \frac{(q^e-1,n(q^d-1))+\delta_{r_{q^e-1}<r_{n(q^d+1)}}(q^e-1,n(q^d+1))}{2(q^e-1,n)} + \frac{\delta_{r_{q^e+1}<r_{n(q^d-1)}}(q^e+1,n(q^d-1))+\delta_{r_{q^e+1}<r_{n(q^d+1)}}(q^e+1,n(q^d+1))}{2(q^e+1,n)}.$$

c. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = -1$, then $|V_{D_n(x,a)}(q^e;q^d)| =$*

$$\frac{(q^e-1,n(q^d-1))+\delta_{r_{n(q^d+1)}<r_{q^e-1}}(q^e-1,n(q^d+1))}{2(q^e-1,n)} + \frac{\delta_{r_{n(q^d-1)}<r_{q^e+1}}(q^e+1,n(q^d-1))+\delta_{r_{n(q^d+1)}<r_{q^e+1}}(q^e+1,n(q^d+1))}{2(q^e+1,n)}.$$

d. *If* $\eta_{q^e}(a) = -1$ *and* $\eta_{q^d}(a^n) = -1$, *then* $|V_{D_n(x,a)}(q^e; q^d)| =$

$$\frac{(q^e - 1, n(q^d - 1)) + \delta_{r_{q^e-1}=r_{n(q^d+1)}}(q^e - 1, n(q^d + 1))}{2(q^e - 1, n)}$$
$$+ \frac{\delta_{r_{q^e+1}=r_{n(q^d-1)}}(q^e + 1, n(q^d - 1)) + \delta_{r_{q^e+1}=r_{n(q^d+1)}}(q^e + 1, n(q^d + 1))}{2(q^e + 1, n)}.$$

Chapter 4

Cryptographic notions

In this chapter, we present some of the cryptographic notions which motivate the definitions and results we present in the rest of the thesis. We begin with a brief introduction to two major attacks on block ciphers, namely linear and differential cryptanalysis. We also give a list of desirable traits for S-boxes used in cryptosystems. Finally, we introduce some real-world cryptosystems and discuss their properties as they pertain to the results appearing in this thesis.

The goal of any cryptosystem is allow the secure transmission of data between two parties. Here, security means that the two parties can communicate across a public channel and their messages cannot be recovered by a third party. In *symmetric-key* cryptosystems, a secret key is shared by the sender and receiver and the same key is used to both encrypt and decrypt the data. In contrast, in *public-key* cryptosystems each user has a private secret key which is encoded into a shared public key by a function which is computationally infeasible to invert. Our focus in this work is on symmetric-key cryptography.

We introduce the notions used in the remainder of this chapter. The *plaintext* is an unencrypted message to be transmitted and the *ciphertext* is a received encrypted message. The *secret key* (or simply key) is shared between both the sender and the receiver. A third-party, who does not possess the secret key, is the *attacker*. We interchangeably use the terms *system* or *cipher* to denote the encryption/decryption mechanism. The common assumption is that the structure of the cipher is

public, hence an attacker may exploit any component of the cipher. The only secret information is the shared key.

Many cryptographic systems are based on Claude Shannon's [59] notions of *confusion* and *diffusion*. In Shannon's terminology, confusion of a system is a complex relationship between the secret key and some computable statistics of the system. Diffusion means that characteristics of the original message do not propagate to the encrypted message in a computable way.

4.1 Substitution-permutation networks

Substitution-permutation networks were introduced by Feistel [26] (U.S. Patent 3,798,359 (IBM)) as cryptosystems which realize Shannon's confusion and diffusion concepts. A substitution-permutation network consists of R rounds and the secret key is broken into $R+1$ subkeys. At each round, the data stream is mixed with a subkey and fed into a series of *substitution boxes* (S-boxes), then the resulting output bits are mixed by a *permutation box* (P-box). S-boxes are functions which act on a subset of the input bits into a round; their primary purpose is to increase the confusion of the cipher. Although S-boxes may map and n-bit string to an m-bit string where $m \neq n$, in this work we consider only the simple model where S-boxes are transformations of bit strings of a fixed size. In Section 4.4.1, we will show that probably the most important substitution-permutation network in use today, the Advanced Encryption Standard, satisfies this simple model. P-boxes act as a shuffling of the bits between rounds; their purpose is to diffuse characteristics of the data stream. No permutation is applied before the first round or after the final round, since this would not add any cryptographic strength to the system. Finally, the output of the final round's S-boxes is mixed with a final round key to create the ciphertext. A diagram of a basic substitution-permutation network, taken verbatim from [35, Figure 1] is given in Figure 4.1 and appears on page 46. Key-mixing is done by the XOR operation of the key bits with the input bits of the round.

An S-box is a one-to-one look-up table which substitutes small blocks of bits for another block of the same size. In most cases, we consider S-boxes as maps from $\mathbb{F}_2^n \to \mathbb{F}_2^n$. Since permutations and adding round keys are all linear relations between bits, S-boxes are the only possibly non-linear

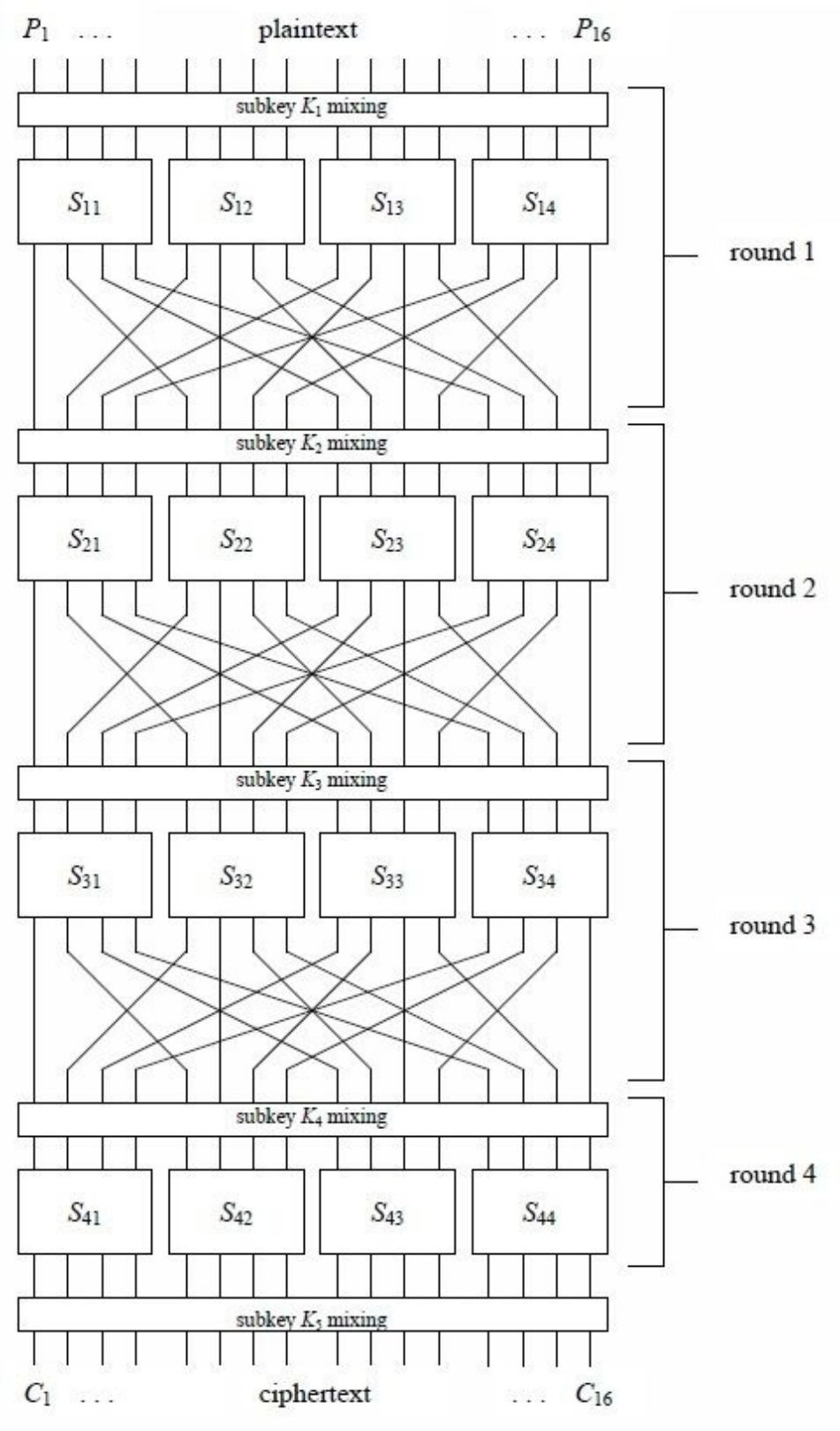

Figure 4.1: A basic 16-bit, 4-round substitution-permutation network [35].

component of the network. As the following section indicates, this non-linearity will be crucial to the security of the cipher.

The XOR operation is self-inverse, thus removing the round subkey is performed by re-mixing it with the data stream. Each S-box is a one-to-one function, and so can be inverted, and each P-box is a permutation, so decryption involves applying the inverse permutation. Since each component of the network is invertible, decryption is performed by running the ciphertext backwards through the cipher.

A substitution-permutation network achieves diffusion in that a small change in the plaintext will be transformed by an S-box and these changes will be permuted by a P-box to other S-boxes in subsequent rounds. In a secure cipher, the probability of any output bit changing due to a change in any input bit is indistinguishable from $1/2$. A substitution-permutation network achieves confusion since changing a bit of the key will change several bits of the round keys. These changes will then also be diffused in each subsequent round.

A variant of a substitution-permutation network, a *Feistel network*, achieves diffusion by only acting on a subset of the bits at every round. An introductory reference to both substitution-permutation networks as well as canonical examples of both Feistel networks and substitution-permutation networks can be found in [47, Chapter 7]. We focus our discussion on substitution-permutation networks, but the attacks outlined in the following section may also be analogously applied to Feistel networks. In more general settings, S-boxes may also accept inputs and outputs of different sizes. We omit this technicality here.

4.2 A brief discussion of linear and differential cryptanalysis

The information contained in this section is due to [35] and corresponding lecture slides for a course on the same topic, given at the SP-ASCrypto school in Atibaia, Brazil in November, 2011 [60]. Only a brief statement of the concepts of linear and differential cryptanalysis are presented here. We encourage interested readers to follow the examples of each attack given in [35].

Both of the attacks outlined in these section make use of the specific structure of the cipher,

since they require a partial decryption of ciphertexts across the final round's S-boxes.

4.2.1 Linear cryptanalysis

Linear cryptanalysis was first introduced by Matsui in 1993 [45] as an attack against the *Data Encryption Standard* (DES). DES is an example of a Feistel network and, although is now considered insecure, variants of DES served as the NIST standard for symmetric key cryptography from 1977 to 2002 [28]. A brute-force attack of DES requires testing 2^{55} keys. Linear cryptanalysis reduces the number of necessary keys to 2^{43}, an improvement by a factor of 4096. In this section, we give a brief outline of the process of linear cryptanalysis.

Linear cryptanalysis is a *known plaintext attack*: a (random) selection of plaintexts are known with their corresponding ciphertexts, but the attacker cannot choose which plaintexts to encrypt. In a real-world setting, this is analogous to having a key-logger saving messages and intercepting the encrypted packets, but the key being entered in some secure way.

Preparing the attack

Linear cryptanalysis is based on finding linear (or affine) relationships between input bits and output bits of S-boxes. A linear relationship between s input bits $[X_{i_1}, X_{i_2}, \ldots, X_{i_s}]$ and t output bits $[Y_{j_1}, Y_{j_2}, \ldots, Y_{j_t}]$ is an expression of the form

$$X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_s} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \cdots \oplus Y_{j_t} = 0 \tag{4.1}$$

which occurs with high probability. An affine relationship between the input bits and output bits is an expression as in Equation (4.1) which occurs with low probability. Thus, we define the *probability bias* of a linear expression L as $\epsilon_L = p_L - 1/2$, where p_L is the probability of the expression L occurring. If the $s + t$ bits in Equation (4.1) are randomly chosen, then the expression L will occur with a probability of exactly $1/2$.

Equation (4.1) could be reformulated to contain the sum of a number of subkey bits. Denote by $K_{i,j}$ the jth subkey bit of round i. Once the subkey bits are chosen, let $\Sigma_K = \bigoplus_{i,j} K_{i,j}$, where i

and j range over all of the subkey bits considered in all rounds. In particular, Σ_K is fixed as 0 or 1. Setting Equation (4.1) equal to Σ_K maintains equal probability bias (in magnitude), and so the subkey bits are omitted from the linear expression.

We then create a linear expression for the entire cipher by observing the linear expressions for each of the S-boxes contained within the cipher. In order to combine the probabilities from the various S-boxes in the cipher, we require an important lemma.

Lemma 4.2.1. (Piling-Up Lemma [45]) *Let $X_1, X_2, \ldots, X_n$ be independent, binary random variables with probability biases $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$, respectively. Then,*

$$\Pr(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \epsilon_i. \tag{4.2}$$

Equivalently, the probability bias of $X_1 \oplus X_2 \cdots \oplus X_n = 0$ is

$$\epsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \epsilon_i.$$

Proof. (Sketch) Consider two binary random variables X_1 and X_2 with probability distributions determined by $\Pr(X_i = 0) = p_i$, $i = 1, 2$. Assuming independence, we have $\Pr(X_1 \oplus X_2 = 0) = \Pr(X_1 = X_2 = 0) + \Pr(X_1 = X_2 = 1) = p_1 p_2 + (1 - p_1)(1 - p_2)$.

Considering now biases, that is $p_1 = 1/2 + \epsilon_1$ and $p_2 = 1/2 + \epsilon_2$, we have $\Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\epsilon_1\epsilon_2$, thus the bias $\epsilon_{1,2}$ of $X_1 \oplus X_2$ is $\epsilon_{1,2} = 2\epsilon_1\epsilon_2$. The lemma follows by induction under the assumption that the n random binary variables are independent. □

The independence assumption of the Piling-Up Lemma is certainly false, since changes in one S-box will diffuse to the other S-boxes. However, [35] shows that the independence assumption works in practice.

To analyze each S-box (with inputs $X_1, X_2, \ldots, X_s$ and outputs $Y_1, Y_2, \ldots, Y_t$), we examine the 2^s input combinations and their corresponding output combinations. We compute the $2^s \times 2^t$ linear expressions and pick an expression with high (or low) probability bias. The table of input sums against output sums is called the *linear approximation table* of the S-box.

The attack

The first step in the attack is to construct linear approximation tables for all of the S-boxes in the cipher. Denote by $X_{i,j}$ the input of round i at bit j and similarly denote by $Y_{i,j}$ the output of round i at bit j. We have $X_{i+1,P_i(j)} = Y_{i,j} + K_{i,P_i(j)}$, where $P_i(j)$ is the output the P-box of round i at bit j and $K_{i,j'}$ is the j'th bit of the ith round subkey.

Using the linear approximation tables, we construct a linear expression of the entire cipher as a concatenation of linear expressions for each round. This concatenation will involve a sum of round-key bits, however as noted above, these bits can be combined into the expression Σ_K and their exclusion does not affect the magnitude of the probability bias of the expression, given by Equation (4.2) of Lemma 4.2.1.

We require only a $R-1$ round linear approximation for a cipher of R rounds that occurs with large probability bias magnitude. Furthermore, the $R-1$ round linear expression should (for reasons we will see shortly) involve input bits to as few S-boxes as possible. The attack is to recover bits of the final round key K_R.

We consider the round R final subkey bits which correspond to the output bits of the S-boxes whose input bits are included in the linear expression of the cipher. For each possible target subkey (if there are m S-boxes $\mathbb{F}_2^n \to \mathbb{F}_2^n$ in the Rth round whose input bits are involved in the linear expression of the cipher, there will be 2^{mn} such subkeys) and for each plaintext/ciphertext pair, we partially decrypt the ciphertext by running the corresponding bits backwards through the final round of the cipher. If the partially decrypted ciphertext matches the linear expression in the plaintext bits, increment a counter for the target subkey. The target subkey corresponding to the linear approximation with the highest bias magnitude is assumed to be the correct key.

Suppose L is a linear expression for $R-1$ rounds of an R round cipher and denote by $\epsilon_L = p_L - 1/2$ the probability bias of L. Matsui shows that the number of known plaintext/ciphertext pairs required for a successful attack is proportional to $1/\epsilon_L^2$ [45].

The design of practical substitution-permutation networks must include S-boxes which are highly non-linear, that is its S-boxes must have no known linear or affine relationships. They must also

have high diffusion properties so that any linear expression should activate an S-box in the final round (and thus require testing a higher number of target subkeys). Measures of linearity appear in Section 2.1.4 and are further discussed in Section 5.3.1.

4.2.2 Differential cryptanalysis

Differential cryptanalysis was introduced by Biham and Shamir in 1991 [2], also as an attack against DES. Differential cryptanalysis has been used to reduce the number of DES keys to be tested from 2^{55} (brute-force) to 2^{47}. Though less successful than linear cryptanalysis for DES, differential cryptanalysis scales very well to other ciphers.

Differential cryptanalysis is a *chosen plaintext attack*, where an attacker has access to the keyed cipher and is able to encrypt any plaintext. The main goal of differential cryptanalysis is to exploit highly probabilistic relationships between differences of plaintexts with the difference of inputs into the last round's cipher. As in linear cryptanalysis, differential cryptanalysis can be used to recover bits of the final round's key.

Suppose $X = [X_1, X_2, \ldots, X_n]$ is an input into the cipher and $Y = [Y_1, Y_2, \ldots, Y_n]$ is its corresponding output. Furthermore, let X' be a similarly defined input and Y' its corresponding output. The *input difference* between X and X' is denoted $\Delta X = X \oplus X'$, where the XOR operation is implemented bit-wise, that is $\Delta X_i = X_i \oplus X'_i$. The *output difference* is defined analogously.

If a cipher on n bits is chosen with uniform distribution of inputs and outputs, then given an input difference, each output difference would occur with probability $1/2^n$. The goal of differential cryptanalysis is to exploit $(\Delta X, \Delta Y)$ pairs that occur with "high" probability (meaning a constant factor of 2^{-n}).

The motivation for observing differences is as follows. Consider two input messages M_1 and M_2. When M_1 and M_2 enter a round, they are mixed with a round subkey K, forming $M'_1 = M_1 \oplus K$ and $M'_2 = M_2 \oplus K$. The resulting input difference into the S-box is

$$M'_1 \oplus M'_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2.$$

Since the keys cancel in the difference, we consider running the attack on an unkeyed cipher (equivalently, assume the key is the all-0 string).

Preparing the attack

The analysis of the cipher is similar to that of linear cryptanalysis. We note that for a fixed input difference ΔX and for a given X, the value of $X' = \Delta X \oplus X$ is uniquely determined. For an S-box with n input bits and m output bits, the probability of the m-bit difference ΔY given an input difference ΔX is tabulated in a *difference distribution table* by inputting all pairs of inputs with the given ΔX. A difference pair $(\Delta X, \Delta Y)$ occurring with high probability is called a *differential*.

A set of concatenated differentials of S-boxes for $R-1$ rounds of the cipher is called a *differential characteristic* of the cipher. The plaintext is then chosen to include pairs of messages which satisfy the differential input ΔX into the S-box of the first round. Since we are considering only permutation S-boxes, all other input differences are 0 and consequently their output differences are 0. S-boxes that admit non-zero difference inputs are called *active*. We will show that a well-constructed differential will contain few active S-boxes since, as in linear cryptanalysis, differential cryptanalysis requires running all possible target subkeys of active S-boxes backwards through the final round of the cipher.

The attack

The first step of the attack is to set up the $R-1$ round differential characteristic occurring with probability a multiple of 2^{-n}.

We attack the bits of the target subkey in each active S-box in the final round R. For each target subkey and for each pair of ciphertexts corresponding to a pair of plaintexts with chosen difference, we execute a partial decryption of the ciphertexts by feeding them backwards through the active S-boxes. If the input difference to the S-boxes (and hence the output after the keyed ciphertexts are run backwards) matches the difference expected by the characteristic, then we increment a counter for the subkey. Such pairs of plaintexts are called *right pairs*. The partial subkey with the highest count is assumed to be correct. It is not necessary to perform the partial decryption for every ciphertext pair. If the bits of the ciphertext difference corresponding to the *in*active S-boxes are

non-zero, then the ciphertexts cannot correspond to a right pair and they are discarded.

Suppose D is the differential characteristic of the first $R-1$ rounds of the cipher and suppose that D occurs with probability p_D. The number of chosen plaintext pairs needed to distinguish right pairs is a small constant multiple of $1/p_D$ [35].

The design of practical substitution-permutation networks must include S-boxes whose corresponding difference functions are injective. Proper diffusion of output differences by the P-boxes is also necessary to maximize the number of active S-boxes in any $R-1$ round differential characteristic.

We conclude this discussion by observing that a prescribed input difference can be denoted by $a \in \mathbb{F}_2^n \setminus \{0\}$, so for any $x \in \mathbb{F}_2^n$, the input difference can be seen instead as $a = (x \oplus a) \oplus x$. The output difference can therefore be taken as $S(x \oplus a) \oplus S(x)$, which corresponds precisely to $\Delta_{S,a}(x)$, where $\Delta_{S,a}$ is the difference map introduced in Definition 2.1.2 if S is considered as a permutation of $(\mathbb{F}_2^n, +)$.

4.3 Desirable traits for S-boxes

This section contains a list of traits considered in the design of S-boxes. This list is an annotated version of that given in [46]. We omit the entries from [46] with no known attacks. As noted in the reference, the precise combination of required properties for S-boxes depends on the application.

First, we introduce some notation. Since S-boxes are mappings $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (in most substitution permutation networks, $n = m$ and the S-box can be invertible), they can be represented as $2^n \times m$ matrices, where the rows are indexed by the elements of $\mathbb{F}_2^n$ and the columns correspond to the ith component Boolean function of S. That is, if $x \in \mathbb{F}_2^n$, the (x, S_i) entry of the matrix takes the value $S_i(x)$. This matrix is also called the *truth-table* of the S-box.

1. **Balanced.** An S-box is *balanced* if every column of its truth-table has an equal number of 0s and 1s. This is guaranteed to occur if the S-box is a bijection.

2. **k-Resilience.** A balanced Boolean function is *k-resilient* if when fixing k coordinates, the remaining $n-k$ coordinates remain balanced. Balanced functions are 0-resilient and for bijective

S-boxes, there are no k-resilient functions for $k > 0$.

3. **Non-linearity.** The *non-linearity* of an S-box should be high to provide resistance to linear cryptanalysis. For more properties of non-linearity, see Section 2.1.4, and Section 5.3.1.

4. **Difference table.** The *difference table* of a function f is the $(2^n - 1) \times 2^m$ array with (a, b) entry given by $|\Delta_{S,a}^{-1}(b)|$. The highest value of the difference table is the differential uniformity of the S-box; in particular, if the S-box is defined by an APN function, the entries of the difference table will be all 0s and 2s. A variant of the difference table will have special significance throughout the rest of this manuscript.

5. **k-th order Strict Avalanche Criterion.** Fixing a basis of $\mathbb{F}_2^n$, each element of $a \in \mathbb{F}_2^n$ is uniquely represented under the basis by a series of bits. The *weight* of an element $a \in \mathbb{F}_2^n$ is the number of non-zero bits in the coordinate vector of a. The *k-th order Strict Avalanche Criterion* states that $\Delta_{B,a}$ should be balanced for all a having weight at most k. That is, if k bits of the input are flipped, the output probability remains $1/2$.

6. **Degree k Propagation Criterion of order m.** Let B be a Boolean function. Similar to the k-th order Strict Avalanche Criterion, $\Delta_{B,a}$ should be balanced for all a of weight at most k when m input bits are fixed. S-boxes achieve the *degree k Propagation Criterion of order m* if $\Delta_{S,a}$ is balanced for all a of weight at most k.

7. **Bit Independence Criterion.** An S-box satisfies the *(i, j)-Bit Independence Criterion* if, for any i columns or fewer, their sum (which represents a Boolean function), satisfies the j-th order Strict Avalanche Criterion. Functions satisfying this criterion have the property that there is no correlation between up to i bits of the output, given a change of j bits of the input.

8. **Absence of linear structures.** Given a Boolean or vectorial Boolean function $B \in \mathbb{F}_{2^e}[x]$, a *linear structure* of B is an element $a \in \mathbb{F}_{2^e}$ such that $\Delta_{B,a}$ is a constant function.

9. **High algebraic degree.** The component Boolean functions of an S-box should all have high degree as (multi-variate) polynomials in the input bits.

10. **High polynomial complexity.** Any function over a finite field can be written as a polynomial due to the Lagrange Interpolation Formula (Theorem 2.1.1). The degree of the polynomial (mod $x^q - x$) should be high and it should be "complicated" to avoid attacks field-theoretically.

11. **Algebraic immunity.** Algebraic immunity has many definitions. In spirit, it is a measure of the resistance against algebraic attacks. Algebraic attacks represent part (or all) of a cipher as a system of non-linear multivariate polynomial equations, where the unknowns are the key bits. The algebraic attack is an efficient solution of the system.

4.4 Practical symmetric-key cryptosystems

4.4.1 The Advanced Encryption Standard (AES)

The *Advanced Encryption Standard* (AES) is the Federal Information Processing Standards Publication 197 (FIPS 197), named in 2001 as the standard for symmetric block ciphers [27].

AES is a minor variant of the cipher Rijndael, so named for its authors, Daemen and Rijmen. Rijndael and AES differ only in block and cipher key lengths: in Rijndael, the block length and the key length can be specified (independently) to any multiple of 32 bits between 128 bits and 256 bits. AES originally required the block length to be fixed at 128 bits, though Rijndael admits 192 and 256-bit variants. AES also allows key lengths of $128, 192$ or 256 bits. See [18], for the definitive reference on Rijndael. For a brief discussion of AES and Rijndael, see also [49, Section 16.2.6]. In what follows, we drop the distinction between AES and Rijndael.

AES is based on the substitution-permutation network framework described in Section 4.1. The S-boxes in AES are defined over $\mathbb{F}_{2^8} \cong \mathbb{F}_2[x]/(f)$, where $f(x) = x^8 + x^4 + x^3 + x + 1$ is a primitive pentanomial. Figure 4.2 shows a high-level figure of AES, taken verbatim from [49, Figure 16.2.8]. Now, we briefly summarize the design of AES.

At each round, the *state* of the cipher consists of a 4×4 matrix, where the (i, j) entry of the matrix is given by bit $4i + j$ of the data stream, $0 \leq i, j \leq 3$.

- There is one allowable block length, 128 bits, and three allowable key lengths, 128, 192 and

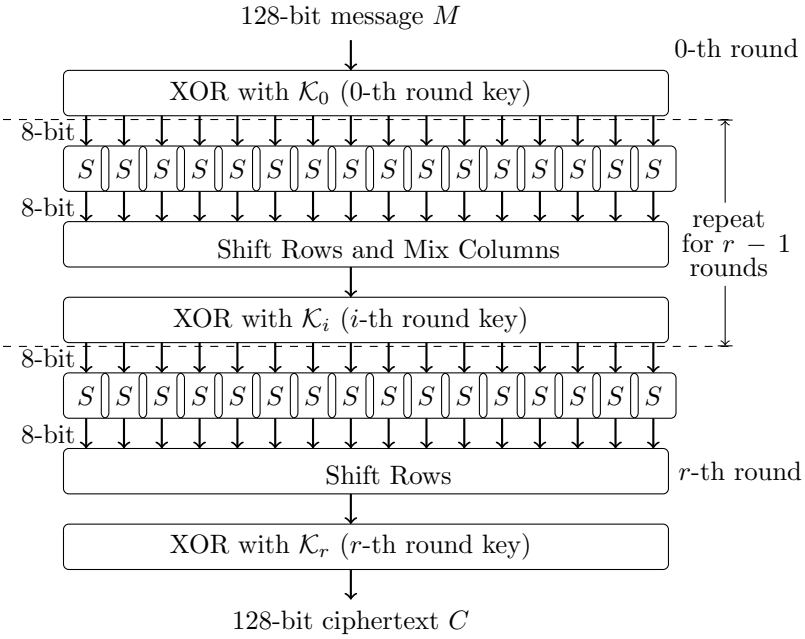

Figure 4.2: The basic structure of AES [49, Figure 16.2.8].

256 bits.

- There are 10, 12 or 14 rounds, corresponding to key lengths of 128, 192 or 256 bits, respectively.
- At each round, except for the last round, the following functions are applied in order

  1. An 8-bit substitution (called the *SubBytes()* transformation),
  2. a 128-bit permutation (called the *ShiftRows()* transformation),
  3. a 32-bit column mixing (called the *MixColumns()* transformation),
  4. addition of the round key (called the *AddRoundKey()* transformation).

The *ShiftRows()* transformation is performed by cyclically shifting row i of the matrix, $i = 0, 1, 2, 3$, to the left by $4i$ bytes. In *MixColumns()*, the columns of the state are treated as degree-4 polynomials over $\mathbb{F}_{2^8}$ and are multiplied by a fixed polynomial modulo $x^4 + 1$. Though $x^4 + 1$ is not irreducible in characteristic two, the polynomial chosen for AES has an inverse modulo $x^4 + 1$, so decryption is possible.

Characteristic	
Permutation	Yes
Balanced	Yes
Almost perfect non-linear	No
Differential uniformity	4
Non-linearity (Boolean)	112
Non-linearity (general)	0.875

Table 4.1: Cryptographic characteristics of the function $x \to x^{2^8-2}$ over $\mathbb{F}_{2^8}$.

SubBytes(): $x \to x^{2^8-2}$

Of particular interest for this work is the S-box defined by the *SubBytes()* transformation. The *SubBytes()* transformation is actually the composition of two (invertible) transformations:

1. Apply the multiplicative inverse function $x \to x^{2^8-2}$ over $\mathbb{F}_{2^8}$. Using this representation means that this mapping is well-defined even at 0.

2. Apply an invertible affine transformation (over $\mathbb{F}_2$) to further mix the output bits.

In implementation, every transformation is simply defined as a 16×16 lookup table. The only non-linear[1] portion of the cipher is the multiplicative inverse function. We present in Table 4.1 a brief summary of some of its cryptographic characteristics.

We now derive the differential properties of the function $f\colon x \to x^{2^n-2}$. We have stated in Section 3.4 that this function is APN if and only if n is odd (in the case of AES, $n = 8$). We include the proof here for completeness.

Proposition 4.4.1. *Let $f(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ and let $\Delta_{f,a}(x) = f(x+a) - f(x)$ for any $a \in \mathbb{F}_{2^n}^*$. The function f is APN if and only if n is odd. Furthermore, if n is even, then $\Delta_{f,a}$ is differential-4-uniform, and is optimally so (for monomials) in the sense that its difference table contains only one 4 in each row.*

Proof. Let $f(x) = x^{2^8-2} \in \mathbb{F}_{2^n}[x]$. We note that, since f is a monomial, for $a \neq 0$,

$$\begin{aligned}\frac{1}{a^{2^n-2}}\Delta_{f,a}(x) = \frac{f(x+a)-f(x)}{a^{2^n-2}} &= \frac{(x+a)^{2^n-2}}{a^{2^n-2}} - \frac{x^{2^n-2}}{a^{2^n-2}} \\ &= \left(\frac{x}{a}+1\right)^{2^n-2} - \left(\frac{x}{a}\right)^{2^n-2} = \Delta_{f,1}(x/a).\end{aligned}$$

[1] Although the affine transformation is non-linear, it is essentially linear when observing the security of the cipher. Its role is diffusion and to introduce resistance to algebraic attacks, though that is not the focus of this discussion.

Hence, we focus only on $\Delta_{f,1}$. Consider the equation $(x+1)^{2^n-2}+x^{2^n-2}=b$. Clearly, $b=0$ is never a solution since f is a permutation and $b=1$ is a solution for $x \in \mathbb{F}_2$. For $x \neq 0,1$ it is convenient to re-write the equation as

$$\frac{1}{x+1}+\frac{1}{x}=b,$$

which is equivalent to the equation $x^2+x=b^{-1}$. Thus, there are two such solutions x and $(x+1)$ if and only if $\mathrm{Tr}(b^{-1})=0$, where Tr is the absolute trace function. In this case, $\mathrm{Tr}(x)=\mathrm{Tr}(x+1)$ or $\mathrm{Tr}(1)=0$, which occurs if and only if n is even. Thus f is APN if and only if n is odd.

Suppose n is even, then $x^2+x=1$ if and only if $x^2+x+1=0$, which is satisfied for the elements of $\mathbb{F}_4 \setminus \mathbb{F}_2$. Thus, when n is even there are 4 solutions to $\Delta_{f,1}(x)=1$. For all other values of b, there are at most 2 solutions of $x^2+x=b$. Thus, when n is even, f is differential 4-uniform, and is optimally so in the sense that its difference table will contain 4s in the entries corresponding to $b=1$. □

We now state a corresponding result for inverse functions over odd characteristic which follows from the proof of Proposition 4.4.1 and the quadratic formula in finite fields of odd characteristic.

Proposition 4.4.2. *Let q be a power of an odd prime and let $f(x)=x^{q^n-2} \in \mathbb{F}_{q^n}[x]$. The function f is almost perfect non-linear.*

Again, since our focus is on the differential properties of functions, we simply quote the result on non-linearity of the inverse function.

Proposition 4.4.3. [9] *Let $f(x)=x^{2^n-2} \in \mathbb{F}_{2^n}[x]$. The (Boolean) non-linearity of the function $f(x)=x^{2^n-2}$ is equal to $2^{n-1}-2^{n/2}$ when n is even and is equal to the highest even number bounded above by $2^{n-1}-2^{n/2}$ when n is odd.*

4.4.2 The Secure and Fast Encryption Routine (SAFER)

The Secure And Fast Encryption Routine (SAFER) cryptosystem was introduced by Massey in 1994 [44]. A new characteristic of the SAFER cryptosystem is in its use of the *Pseudo-Hadamard Transform* to achieve diffusion and in *additive key biases* which are implemented in order to eliminate

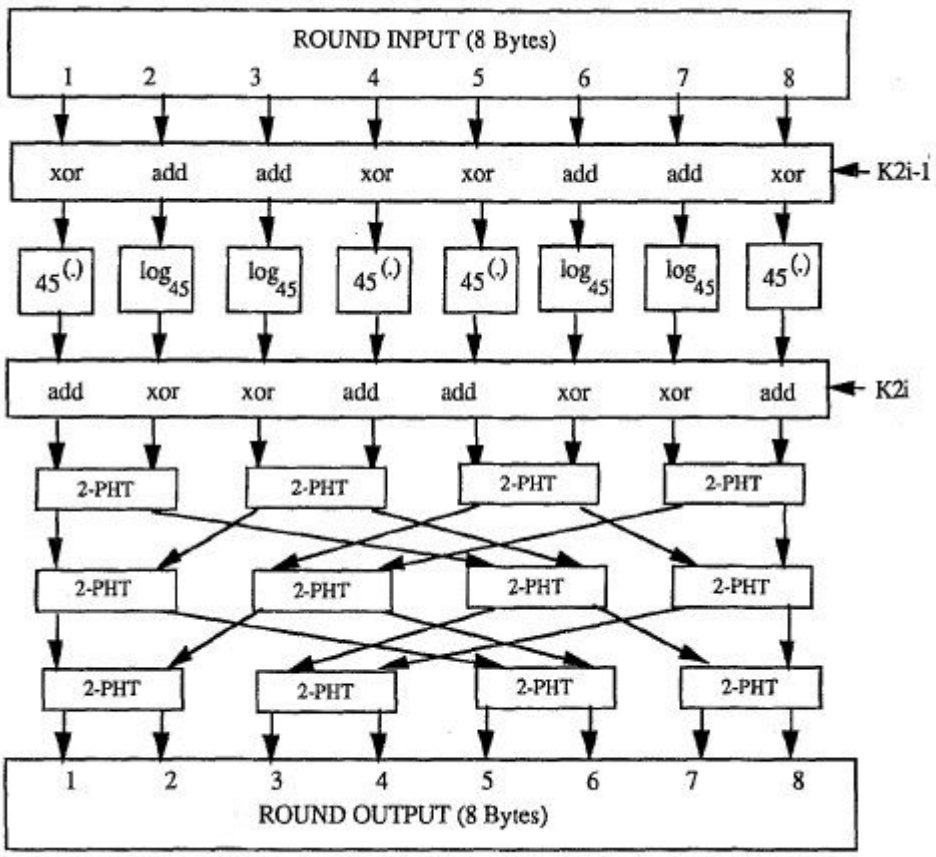

Figure 4.3: The encryption round of SAFER K-64.

the presence of weak keys (a notion that is not discussed in this work). SAFER can be implemented using only byte operations in encryption and decryption.

The original SAFER, SAFER K-64, uses 64-bit block length and also 64-bit key lengths and is run through a R-round substitution-permutation network, where $6 \leq R \leq 10$. At each round, 64-bits are input as a series of eight 8-byte words. As in AES, every encryption round of SAFER is identical. The encryption structure of SAFER is shown in Figure 4.3 and is taken verbatim from [44, Fig. 2].

A novel difference in the SAFER cryptosystem is in its mixing of arithmetic over $\mathbb{Z}_{257}$ and on byte-wise operations over $\mathbb{F}_2^8$. Bytes are interchangeably considered as elements in the vector space and as integers modulo 257.

Each round has a pair of key mixings. The round input uses the byte-wise XOR operation on bytes $1, 4, 5, 8$ and addition $\pmod{257}$ on bytes $2, 3, 6, 7$. Then, one of the non-linear functions f or

g, both described in the following paragraph, is applied and its output is either added (mod 257) on bytes $1, 4, 5, 8$ or XORed on bytes $2, 3, 6, 7$ (on each byte, the opposite operation than in the initial key mixing is applied).

The confusion in the S-box comes from the non-linear functions $f(x) = 45^x$ and

$$g(x) = \begin{cases} \log_{45}(x) & x \neq 0, \\ 128 & x = 0. \end{cases}$$

These functions are both considered over $\mathbb{Z}_{257}$. The base for the exponentiation in f and the base of the logarithm in g is chosen to be 45 since it is primitive modulo 257. The functions f and g restricted to $\mathbb{Z}_{257}^*$ are compositional inverses. Notions of equivalence of functions are given in Section 5.3.3; due to these equivalencies it is known that the APN property holds for inverse functions. We therefore consider only the function f. Table 4.2 gives a table of cryptographic statistics for the function f.

Diffusion of the system is performed using the Pseudo-Hadamard Transform (labeled "PHT" in Figure 4.3 on Page 59). Our focus is on the confusion aspects of the cryptosystem, so we refer the reader to [44] for the introduction of the PHT and to [5] for an analysis of the PHT layer of SAFER.

Characteristic	
Permutation	Yes
Balanced	Yes
Almost perfect non-linear	Yes
Differential uniformity	2
Non-linearity (Boolean)[†]	93
Non-linearity (general)	0.834

Table 4.2: Cryptographic characteristics of the function $f(x) = 45^x \in \mathbb{Z}_{257}$.

Differential properties of the SAFER cryptosystem have been considered as a special case of a class of APN functions over the finite ring $\mathbb{Z}_n$ which arise from Costas arrays in [24], see also Section 2.3. The non-linearity of these functions is also considered in [25].

[†]The Boolean definition of the non-linearity applies only when the function is considered as an element of $\mathbb{F}_2^8$. In the case of SAFER, the general non-linearity measures the non-linearity of a different function. This is in contrast to AES, where the Boolean non-linearity simply indicates a different normalization than the general non-linearity measure. For comparison to the general non-linearity, using the normalization factor of 256 instead of 2, the (re-normalized) Boolean non-linearity of the SAFER map is approximately 0.727.

Part II

Ambiguity and deficiency

Chapter 5

Theoretical aspects of ambiguity and deficiency

The measures of ambiguity and deficiency are introduced in [55]. In this chapter, we give the definitions of ambiguity and deficiency in Section 5.1. We discuss some theoretical aspects, leading up to lower bounds on the ambiguity and deficiency of a bijection in Section 5.2. We note that the lower bounds in Section 5.2 appear in [55], but the results therein are fundamental to understanding our measures. In addition, we give a slightly different more explicit treatment of the results here. We continue with some connections between ambiguity and deficiency and some cryptographic notions in Section 5.3. In particular, we give a connection between functions with optimal ambiguity and deficiency and their non-linear properties. We also show that ambiguities and deficiencies are invariant under some well-known notions of equivalence. Section 5.4 is devoted to giving the ambiguity and deficiency of various classes of functions.

5.1 The definition

Let G_1 and G_2 be Abelian groups and let $f\colon G_1 \to G_2$. Denote $G_1^* = G_1\backslash\{0\}$ and similarly $G_2^* = G_2\backslash\{0\}$. Recall the difference map of f with parameter $a \in G_1^*$ is given by $\Delta_{f,a}(x) = f(x+a) - f(x)$.

For $a \in G_1^*$, let $\lambda_{a,b}(f) = |\Delta_{f,a}^{-1}(b)|$; that is $\lambda_{a,b}(f)$ is the number of pre-images of b under $\Delta_{f,a}$. Define the *row-a-ambiguity* of f by

$$A_{r=a}(f) = \sum_{b \in G_2} \binom{\lambda_{a,b}}{2}. \tag{5.1}$$

Thus, $A_{r=a}(f)$ measures the number of distinct pairs x_1, x_2 such that $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$.

Now, define the *row-a-deficiency* of f by

$$D_{r=a}(f) = \sum_{b \in G_2} \left(1 - \delta_{\lambda_{a,b}}\right), \tag{5.2}$$

where $\delta_i = 0$ if $i = 0$ and $\delta_i = 1$ otherwise. Thus, the row-a-deficiency of f measures the number of elements of the co-domain which are not in the value set of $\Delta_{f,a}$.

By similarly defining the column ambiguity and deficiency, we have two $(n-1) \times n$ tables: the *ambiguity table* and the *deficiency table*. For $a \in G_1^*$ and $b \in G_2$, the (a, b) entry of the ambiguity table is given by $\binom{\lambda_{a,b}}{2}$ and these entries range from 0 to $\binom{|G_1|}{2}$. The (a, b) entry of the deficiency table are given by $1 - \delta_{\lambda_{a,b}}$ and is 1 or 0 depending if b is an image of $\Delta_{f,a}(x)$ or not, respectively. We note that an entry of 0 in the ambiguity table indicates that $\Delta_{f,a}(x) = b$ has 0 or 1 solution and an entry of 1 in the ambiguity table indicates that $\Delta_{f,a}(x) = b$ has exactly two solutions. Thus, PN functions (Section 3.3) have all-zero ambiguity table and APN functions (Section 3.4) have $0-1$ ambiguity tables.

We now give the overall measures of ambiguity and deficiency.

Definition 5.1.1. *The ambiguity of f, $A(f)$, is given by the sum of the row-ambiguities of f, that is*

$$A(f) = \sum_{a \in G_1^*} A_{r=a}(f).$$

Definition 5.1.2. *The deficiency of f, $D(f)$, is given by the sum of the row-deficiencies of f, that is*

$$D(f) = \sum_{a \in G_1^*} D_{r=a}(f).$$

Non-zero contributions to the ambiguity table of f involve *collisions* of images of $\Delta_{f,a}$. Thus, the ambiguity is a measure of the injectivity of the $\Delta_{f,a}$ considered collectively across all $a \in G_1^*$. Additionally, an all-0 deficiency table implies that $\Delta_{f,a}(x)$ is surjective for all $a \in G_1^*$ (equivalently, this implies that f is perfect non-linear). Thus, the deficiency of f is a measure of the surjectivity of the $\Delta_{f,a}$ considered collectively across all $a \in G_1^*$.

Our treatment of the definition of ambiguity and deficiency differs slightly from that of [55]. Here we briefly recap that definition. Denote by $\alpha_i(f)$ the number of pairs $(a, b) \in G_1^* \times G_2$ such that $|\Delta_{f,a}^{-1}(b)| = i$. The deficiency of f is therefore given by $\alpha_0(f)$. Furthermore, the ambiguity of f is given by $A(f) = \sum_{i=0}^{|G_1|} \alpha_i(f)\binom{i}{2}$.

We might also use the phrase *weighted ambiguity* for $A(f)$. We recall that the presence of the binomial coefficient gives the replication of pairs x_1, x_2 such that $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$, where the *unweighted ambiguity* (without the binomial coefficient) measures simply the presence of such pairs. We are concerned only with the weighted ambiguity in this work.

Some related measures are introduced in the literature; for example, the *differential spectrum* of f is the (multi-)set of $\alpha_i(f)$. In particular, the differential spectra of functions $f(x) = x^{2^t-1} \in \mathbb{F}_{2^e}[x]$ is considered in [4], generalizing known results on inverse functions, see Section 4.4.1.

5.2 Bounds for permutations

Bounds on the ambiguity and deficiency of a bijection between Abelian groups G_1 and G_2 are given in [55]. In that paper, the authors state the following paragraph.

> In this paper we restrict our attention to $f : G_1 \to G_2$ that are bijections. This has the implication that $\Delta_{f,a}(x) = b$ can never have solutions for $b = 0$, thus we use the corresponding form in all our definitions that restrict $b \in G_2^*$; this also includes summations and universal quantifiers. Another effect of this to note is that the domain and co-domain of $\Delta_{f,a}$ are now sizes n and $n-1$, respectively; this is particularly important to remember when reading the proofs otherwise our references to "$n-1$" will seem odd. The ambiguity and deficiency of a function and its compositional inverse are the same

since row-a-deficiency becomes column-a-deficiency, and reciprocally.

However, the ambiguity and deficiency of a function is defined for any function between finite groups: the function need not be a permutation. Similarly, since the difference maps are defined in terms of the original function, we are uncomfortable with considering it as having a different co-domain. We reformulate the results in [55] to remove this restriction on the co-domain, however we emphasize that placed in the appropriate setting the results from [55] are correct.

We fix some notation. Let G_1 and G_2 be arbitrary finite Abelian groups. Let $I_1 \subseteq G_1$ be the elements of order 2 in G_1, let $\iota_1 = |G_1|$ and let

$$\gamma_1 = \sum_{g \in I_1} g.$$

We similarly define I_2, ι_2 and γ_2 for G_2.

If f is a bijection, then $\Delta_{f,a}(x) \neq 0$ for all $x \in G_1$. Thus, $\Delta_{f,a}$ has at most $n-1$ distinct images.

Lemma 5.2.1. *Let $f\colon G_1 \to G_2$ be a bijection, then for any $a \in G_1^*$*

$$D_{r=a}(f) = D_{c=a}(f^{-1}) \tag{5.3}$$

$$A_{r=a}(f) = A_{c=a}(f^{-1}). \tag{5.4}$$

Proof. Let $f\colon G_1 \to G_2$ be a bijection. Let $y = f(x)$, then $f(x+a) - f(x) = b$ has a solution if and only if $a = f^{-1}(y+b) - f^{-1}(y)$. The result follows. □

Lemma 5.2.2. *Let $f\colon G_1 \to G_2$ be a bijection and let $a \in G_1^*$. If the row-a-deficiency of f is equal to d, then the row-a ambiguity of f satisfies*

$$d \leq A_{r=a}(f) \leq \binom{d+1}{2}.$$

Proof. Suppose the row-a-deficiency of f is $D_{r=a}(f) = n - |\{\Delta_{f,a}(x)\colon x \in G_1\}| = d$. The maximum row-$a$-ambiguity occurs when the n images of $\Delta_{f,a}$ are tightly compacted, that is, when $n-1-d$ images are distinct and the remaining $d+1$ images agree. The minimum value of $A_{r=a}(f)$ occurs

when the images are as close to equi-distributed as possible. That is, when the n images are distributed with d pairs $x, x' \in G_1$ satisfying $\Delta_{f,a}(x) = \Delta_{f,a}(x')$ and the remaining $n - 2d$ images are distinct. □

Now, suppose f is a bijection and let $I_1^0 \subseteq I_1$ be the elements of I_1 which have row-deficiency 1, that is $I_1^0 = \{a \in I_1 \colon D_{r=a}(f) = 1\}$ and let N_1^0 be the set of elements in $G_1 \backslash I_1$ which give row-deficiency 1. Again, we similarly define I_2^0 and N_2^0.

Lemma 5.2.3. *Let $f \colon G_1 \to G_2$ be a bijection. For all $a \in G_1^*$ the row deficiency of f $D_{r=a}(f)$ is at least 1, and if $D_{r=a}(f) = 1$ there is a single repeated value in the image set of $\Delta_{f,a}$ equal to γ_2. Moreover, $D_{r=a}(f) > 1$ if $\gamma_2 = 0$.*

Proof. The deficiency of f is the sum of its row-deficiencies. Thus, $D(f) = \sum_{a \in G_1^*} D_{r=a}(f) \geq (n-1) - |I_0^1 \cup N_1^0|$. If $a \in I_1^0 \cup N_1^0$, then $D_{r=a}(f) = 1$ and by the Pigeon-hole Principle there is a single repeated value r in the multiset $\{f(x+a) - f(x) \colon x \in G_1\} \subseteq G_2^*$. Thus,

$$\sum_{x \in G_1} \Delta_{f,a}(x) = \sum_{x \in G_1} f(x+a) - f(x),$$

so $r + \gamma_2 = \gamma_2 + \gamma_2$ and $\gamma_2 = r$. If $\gamma_2 = 0$, then $r = 0$ which is a contradiction since r is not an image of $\Delta_{f,a}$. □

Lemma 5.2.4. *Let f be a bijection and let $\gamma_2 \neq 0$, then*

$$n - 1 - |I_1^0 \cup N_1^0| \geq D_{c=\gamma_2}(f) \geq |I_1^0 \cup N_1^0| - 1.$$

Proof. Let f be a bijection$\colon G_1 \to G_2$. In the deficiency table, a non-zero entry in the γ_2 column corresponds to an element $a \in G_1^*$ such that $\Delta_{f,a}(\gamma_2)^{-1} = \emptyset$. That is, γ_2 is a "missed" element of $\Delta_{f,a}$. By Lemma 5.2.3, γ_2 is a repeated value of $\Delta_{f,a}$ for all $a \in I_1^0 \cup N_1^0$. Thus, $n - 1 - |I_1^0 \cup N_1^0| \geq D_{c=\gamma_2}(f)$.

There are $n-1$ entries in each column of the deficiency table, thus

$$n - 1 = D_{c=\gamma_2}(f) + n_1 + n_2, \tag{5.5}$$

where n_1 is the number of $a \in G_1^*$ for which there is a unique solution to $\Delta_{f,a}(x) = \gamma_2$ and n_2 is the number of $a \in G_1^*$ containing multiple solutions to $\Delta_{f,a}(x) = \gamma_2$.

Furthermore, if f is a permutation, given $x \in G_1$ and $b \in G_2$, there is an (unique) $a \in G_1^*$ such that $\Delta_{f,a}(x) = b$, namely $a = f^{-1}(f(x) + b) - x$. Thus,

$$n \geq 0 \cdot D_{c=\gamma_2}(f) + 1n_1 + 2n_2. \tag{5.6}$$

Combining Equations (5.6) and (5.5) gives $D_{c=\gamma_2} + 1 \geq n_2 \geq |I_1^0 \cup N_1^0|$, as required. □

Lemma 5.2.5. *Let G be an Abelian group, let $I \subseteq G$ be the elements of G of order 2 and set $\iota = |I|$ and $\gamma = \sum_{i \in I} i$. If $\iota \neq 1$, then $\gamma = 0$.*

Proof. If $\iota = 0$, the assertion is trivial. Suppose now that $\iota > 1$. Clearly, $I_0 = I \cup \{0\}$ is a subgroup of G; in particular, I_0 is a 2-group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. If $\iota > 1$, that is $|I_0| > 2$, then the sum of elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ is 0. □

Lemmas 5.2.3 and 5.2.5 can be combined into the following result.

Proposition 5.2.6. *Let $f\colon G_1 \to G_2$ be a bijection. If $\iota_2 > 1$, then $D_{r=a}(f) > 1$ for all $a \in G_1^*$.*

We now present a lower bound on the ambiguity and deficiency of bijections functions depending on their domain.

Theorem 5.2.7. *Let G_1 and G_2 be Abelian groups of order n with ι_1 and ι_2 elements of order 2, respectively. Let $f\colon G_1 \to G_2$ be a bijection. Then both the ambiguity and the deficiency of f are at*

least

$$\begin{cases} 2(n-1) & \text{if } n \equiv 1 \pmod 2, \\ 2(n-2) & \text{if } n \equiv 0 \pmod 2 \text{ and } \iota_1 = \iota_2 = 1, \\ 2(n-1) - \frac{3}{2}\min\{\iota_1, \iota_2\} + \frac{\iota_1\iota_2}{2} & \text{if } n \equiv 0 \pmod 2 \text{ and } \iota_1\iota_2 > 1. \end{cases}$$

Proof. After determining the deficiency, the bounds on the ambiguity are guaranteed by Lemma 5.2.2. When n is odd, there are no order-2 elements of G_2 and by Lemma 5.2.3, $D_{r=a}(f) > 1$ for all $a \in G_1^*$.

Suppose n is even and $\iota_1 = \iota_2 = 1$, that is $I_1 = \{\gamma_1\}$ and $I_2 = \{\gamma_2\}$. The deficiency can be computed as the sum of the row deficiencies or as the sum of the column deficiencies, thus

$$\sum_{a \in G_1^*} D_{r=a}(f) = \sum_{b \in G_2} D_{c=b}(f).$$

Let $D^*_{r=a}(f) = D_{r=a}(f) - 1$, that is $D^*_{r=a}$ denotes the row-a-deficiency of f not counting the entry from the 0-column. We apply Lemma 5.2.4 to both f (for column deficiencies) and f^{-1} (for row-deficiencies) to obtain

$$\begin{aligned} D(f) &= n - 1 + \frac{1}{2}\left(\sum_{a \in G_1^*} D^*_{r=a}(f) + \sum_{b \in G_2^*} D_{c=b}(f)\right) \\ &= n - 1 + \frac{1}{2}\left(\sum_{a \neq 0, \gamma_1} D^*_{r=a}(f) + \sum_{b \neq 0, \gamma_2} D_{c=b}(f) + D_{c=\gamma_2}(f) + D^*_{r=\gamma_1}(f)\right) \\ &\geq n - 1 + \frac{1}{2}\left((n - 2 - |I_1^0 \cup N_1^0|) + (n - 2 - |I_2^0 \cup N_2^0|) + |I_1^0 \cup N_1^0| - 1 + |I_2^0 \cup N_2^0| - 1\right) \\ &= n - 1 + n - 3 = 2(n-2). \end{aligned}$$

When $\iota_2 > 1$, the bound of $2(n-1)$ is trivial by Proposition 5.2.6. If $\iota_1 > 1$, we consider instead the deficiency table of f^{-1}; removing the $b = 0$ column, Lemma 5.2.1 gives that the $(n-1) \times (n-1)$ deficiency sub-array of f^{-1} is the transpose of that of f. Thus, reversing the role of G_1 and G_2 (and thus ι_1 and ι_2), we apply Proposition 5.2.6 again to obtain the lower bound of $2(n-1)$. In what follows, we improve this bound when $\iota_1\iota_2 > 1$.

Let $\alpha_{i,a} = |\{b \in G_2 \colon |\Delta_{f,a}^{-1}(b)| = i\}|$. A simple counting argument gives that $|G_2| = \sum_{i=0}^{n} \alpha_{i,a} =$

$\sum_{i=0}^{n} i\alpha_{i,a} = |G_1|$. Furthermore, suppose $a \in I_1$ and $b \in I_2$, then $\Delta_{f,a}(x) = b$ if and only if $\Delta_{f,a}(x+a) = b$ and so $\alpha_{1,a} \leq n-1-\iota_2$ (the extra -1 coming from $\Delta_{f,a}(x) \neq 0$) and $n/2 \geq \alpha_{2,a} \geq \iota_2$.

We have, $2\sum_{i=2}^{n} \alpha_{i,a} \leq \sum_{i=2}^{n} i\alpha_{i,a} = n - \alpha_{1,a}$. The left-hand side can be similarly expanded, giving $2(n - \alpha_{1,a} - \alpha_{0,a}) \leq n - \alpha_{1,a}$. Re-arranging and identifying $\alpha_{0,a} = D_{r=a}(f)$ gives

$$D_{r=a}(f) \geq \frac{n - \alpha_{1,n}}{2} \geq \frac{\iota_2 + 1}{2}.$$

Since the deficiency is the sum of the row-deficiencies, we find

$$\begin{aligned} D(f) &= \sum_{a \in I_1} D_{r=a}(f) + \sum_{a \in N_1} D_{r=a}(f) \geq \iota_1 \frac{\iota_2 + 1}{2} + 2(n - 1 - \iota_1) \\ &= 2(n-1) + \frac{\iota_1 \iota_2}{2} - \frac{3\iota_1}{2}. \end{aligned}$$

Repeating the same argument with f^{-1}, interchanging the roles of G_1 and G_2 (and thus $\iota_1 = |I_1|$ and $\iota_2 = |I_2|$), we bound the deficiency by

$$D(f) \geq 2(n-1) + \frac{\iota_1 \iota_2}{2} - \frac{3}{2}\min\{\iota_1, \iota_2\}. \qquad \square$$

Definition 5.2.8. *Let $f\colon G_1 \to G_2$ be a bijection achieving the lower bound of ambiguity or deficiency in Theorem 5.2.7, then f has* optimal ambiguity *or* optimal deficiency*, respectively.*

We observe that in the case of permutations on 2-groups, $\iota_1 = \iota_2 = n-1$ and the bounds converge to $(n-1)n/2$, which is optimal. In fact, APN functions are precisely those which achieve this lower bound, see Section 3.4.

Suppose $\iota_1 \iota_2 > 1$, we can present different formulations of the bound using a finer expansion of the identities. Let $a \in I_1$ so that $\alpha_{1,a} \geq n-1-\iota_2$. We find $3\sum_{i=3}^{n} \alpha_{i,a} \leq \sum_{i=3}^{n} i\alpha_{i,a} = n - \alpha_{1,a} - 2\alpha_{2,a}$. Further expanding the left-hand side gives $3(n - \alpha_{0,a} - \alpha_{1,a} - \alpha_{2,a}) \leq n - \alpha_{1,a} - 2\alpha_{2,a}$. We identify $\alpha_{0,a}$ with $D_{r=a}(f)$ and re-arrange to get

$$D_{r=a}(f) \geq \frac{2n - 2\alpha_{1,a} - \alpha_{2,a}}{3} \geq \frac{2\iota_2 + 2 - \alpha_{2,a}}{3} \geq \frac{2\iota_2 + 2 - n/2}{3}.$$

We observe that, for $\iota_2 > 1$, this bound is only meaningful when $D_{r=a}(f) \geq 2$, that is when $\iota_2 \geq n/4 + 2$.

The deficiency is the sum of the row-deficiencies and so

$$\begin{aligned} D(f) &= \sum_{a \in I_1} D_{r=a}(f) + \sum_{a \in N_1} D_{r=a}(f) \geq 2(n-1-\iota_1) + \iota_1 \left(\frac{2\iota_2 + 2 - n/2}{3} \right) \\ &= 2(n-1) + \frac{2\iota_1\iota_2}{3} - \iota_1 \left(\frac{4}{3} + \frac{n}{6} \right). \end{aligned}$$

Repeating the same argument with f^{-1}, interchanging the roles of G_1 and G_2 (and thus $\iota_1 = |I_1|$ and $\iota_2 = |I_2|$), we bound the deficiency by

$$D(f) \geq 2(n-1) + \frac{2\iota_1\iota_2}{3} - \min\{\iota_1, \iota_2\} \left(\frac{4}{3} + \frac{n}{6} \right).$$

This bound is an improvement on the one presented in Theorem 5.2.7 when $\iota_1\iota_2$ is larger than n but $\min\{\iota_1, \iota_2\}$ is small. If $\iota_1 = \iota_2 = n - 1$, then this bound is equivalent to the one presented in Theorem 5.2.7. We further remark that we could proceed incrementally, bounding $\alpha_{i,a}$ by n/i for $i = 3, 4, \ldots, n/2$, but the bounds improve only slightly and the conditions on ι_1, ι_2 become stronger.

5.3 Connections to other cryptographic notions

In this section, we link ambiguity and deficiency to other cryptographic notions. In Section 5.3.1, we show that in many cases functions with optimal ambiguity and deficiency have high non-linearity. We give a similar link between functions with optimal ambiguity and the lesser-known measure of non-balancedness in Section 5.3.2. We also show in Section 5.3.3 that ambiguity and deficiency are invariant for the most commonly considered types of equivalent functions, namely the EA and CCZ equivalence.

5.3.1 Non-linearity

The resistance of an S-box to linear cryptanalysis can be measured by the *non-linearity* of the function used in that S-box, with highly non-linear functions preferred. For more information about linear cryptanalysis, see Section 4.2.1. First, we recall the definitions of the general forms of linearity and non-linearity, Definition 2.1.26 and 2.1.27, respectively.

If $F\colon G_1 \to G_2$, the *linearity* of F is given by

$$\mathbb{L}(F) = \max_{\alpha \in G_1, \beta \in G_2^*} |\widehat{F}(\alpha, \beta)|,$$

where $\widehat{F}$ is the Fourier transform of F, that is

$$\widehat{F}(\alpha, \beta) = \sum_{x \in G_1} (\psi_\beta \circ F)(x) \chi_\alpha(x).$$

The *non-linearity* of F is given by

$$\mathbb{NL}(F) = \frac{|G_1| - \mathbb{L}(F)}{|G_2|}.$$

The non-linearity of F is 0 if and only if F is an affine function. In the remainder of this section, we derive a lower bound on the non-linearity of a permutation function which achieves the minimum ambiguity and deficiency over the additive group of a finite field (of both odd and even characteristic) and over a finite cyclic group. We recall that such a permutation function is APN.

The additive group of a finite field

In what follows, we assume $G_1 = G_2 = (\mathbb{F}_q, +)$, for some prime power q. Lower bounds on the optimum ambiguity and deficiency of F in terms of its domain and co-domain are given in Theorem 5.2.7. When q is even, functions which meet the bound in Theorem 5.2.7 are precisely the APN functions [55]. We give bounds on the non-linearity of F depending on whether q is odd or even.

Let $\lambda_F(a, b) = \sum_{x \in G_1} \chi(aF(x) + bx)$, where χ is an additive character $G_1 \to \mathbb{C}$, that is $\lambda_F(a, b) =$

$\widehat{F}(b,a)$. Thus,

$$\begin{aligned}|\lambda_F(a,b)|^2 &= \sum_{x\in G_1}\chi(aF(x)+bx)\overline{\sum_{y\in G_1}\chi(aF(y)+by)}\\ &= \sum_{x\in G_1}\chi\left(aF(x)+bx\right)\sum_{y\in G_1}\chi\left(-aF(y)-by\right)\\ &= \sum_{x,y\in G_1}\chi\left(a(F(x)-F(y))+b(x-y)\right),\end{aligned}$$

and letting $z=x-y$, we get

$$\begin{aligned}|\lambda_F(a,b)|^2 &= \left|\sum_{z,y\in G_1}\chi\left(a(F(y+z)-F(y))+bz\right)\right|\\ &= \left|\sum_{z\in G_1}\chi(bz)\sum_{y\in G_1}\chi(a\Delta_{F,z}(y))\right|\\ &= \left|n+\sum_{z\in G_1,z\neq 0}\chi(bz)\sum_{y\in G_1}\chi(a\Delta_{F,z}(y))\right|. \qquad (5.7)\end{aligned}$$

Since F is a permutation, for any $z\in G_1, z\neq 0$ we have $\Delta_{F,z}(y)=F(y+z)-F(y)\neq 0$. Thus, by the Pigeon-Hole Principle, there is a repeated image of $\Delta_{F,z}$, call this image $\widetilde{r_{0,z}} := r_{0,z}/a$.

Case 1: Odd characteristic Since F has optimum deficiency, for each $z\in G_1, z\neq 0$, there is exactly one $c\in G_1\backslash\{0\}$ such that $\Delta_{F,z}(x)=c$ has no solution. Thus, by the Pigeon-Hole Principle there is one omitted value of $\Delta_{F,z}$, call this $\widetilde{o_z} := o_z/a$ and a corresponding repeated image of $\Delta_{F,z}$ denoted $\widetilde{r_z} := r_z/a$.

We must separate the case $b=0$. If $b=0$, then with $z\neq 0$ we have

$$|\lambda(a,0)|^2 = \left|n+\sum_{z\in G_1,z\neq 0,y\in G_1}\chi(a\Delta_{F,z}(y))\right|.$$

We know that $\sum_{x\in G_1}\chi(x)=0$ and for each $z\neq 0$ we have that the image multiset of $\Delta_{F,z}$ is given by $\Delta_{F,z}(G_1)=G_1\backslash\{0,\widetilde{o_z}\}\cup\{\widetilde{r_{0,z}},\widetilde{r_z}\}$. We note that $\widetilde{r_{0,z}}\neq\widetilde{r_z}$ due to the minimality condition on

the ambiguity. Thus,

$$\sum_{y \in G_1} \chi(a\Delta_{F,z}(y)) = 0 - \chi(0) - \chi(o_z) + \chi(r_{0,z}) + \chi(r_z),$$

and $|\lambda(a,0)|^2 \leq n + 4(n-1) = 5n - 4$.

If $b \neq 0$, a similar derivation gives

$$\begin{aligned}
|\lambda(a,b)|^2 &= \left| n + \sum_{z \in G_1, z \neq 0} \chi(bz)\left(0 - \chi(0) - \chi(o_z) + \chi(r_{0,z}) + \chi(r_z)\right) \right| \\
&= \left| n - \sum_{z \in G_1, z \neq 0} \chi(bz) - \sum_{z \in G_1, z \neq 0} \chi(bz + o_z) + \sum_{z \in G_1, z \neq 0} \chi(bz + r_{0,z}) + \sum_{z \in G_1, z \neq 0} \chi(bz + r_z) \right| \\
&\leq n + 4.
\end{aligned}$$

Hence we have the following theorem.

Theorem 5.3.1. *Let $G = (\mathbb{F}_q, +)$ with q odd and let F be a permutation of G with optimum ambiguity and deficiency. The non-linearity of F satisfies*

$$\mathbb{NL}(F) \geq \frac{q - \sqrt{5q-4}}{q}.$$

Case 2: Even characteristic When q is even, $(\mathbb{F}_q, +)$ is a 2-group, so the number of order 2 elements is $q - 1$. Thus, we fit in the third case of Theorem 5.2.7. We note that functions which achieve the lower bound of Theorem 5.2.7 are APN functions, that is $\Delta_{F,a}$ is 2-to-1 for all $a \in \mathbb{F}_q^*$.

The balanced property of APN functions is somehow the worst possible for the analysis and the Fourier transform does not simplify beyond Equation (5.7); the multiset $\{a\Delta_{F,z}(G)\}$ contains $n/2$ elements, each repeated twice. Thus,

$$|\lambda(a,b)|^2 \leq \left| n + 2 \sum_{z,y \in G_1, z \neq 0} \chi(y_{1,z}) + \chi(y_{2,z}) + \cdots + \chi(y_{n/2,z}) \right| \leq n.$$

The bound on the linearity in this case using the coarse bounding of the triangle inequality is

equal to the highest possible which is attained from Parseval's identity. We note that expanding the sum across all z has potential to vastly improve this bound: if the $\Delta_{f,z}(y)$ are evenly distributed across all $z \neq 0$ and all y, then $|\lambda(a,b)| = \sqrt{n}$, which is the smallest allowable using Parseval's identity [25].

Indeed, there is only one known APN permutation (up to equivalence) over finite fields of even characteristic. Its polynomial form is complicated and so we refer the reader to [6]. Using SAGE [63], we calculate the non-linearity of this APN permutation to be 3/4.

Finite cyclic groups

In what follows, suppose $G_1 = G_2$ is the finite cyclic group of order n (isomorphic to $\mathbb{Z}_n$). The characters of G_1 are given by $\psi_j \colon G_1 \to \mathbb{C}$ with $\psi_j(g^k) = e^{2\pi ijk/n}$, where g is a generator of G_1 and $i = \sqrt{-1}$. In particular, every character is a power of ψ_1.

Let $\alpha \in G_1$ and let $\beta \in G_1^*$ (written multiplicatively so that $\beta \neq 1$). We have $\widehat{F}(\alpha,\beta) = \sum_{x \in G_1} (\phi_\beta \circ F)(x)\chi_\alpha(x)$, where χ_α and ϕ_β are the characters obtained as the image of some bijection $G_1 \to \widehat{G_1}$. We note that χ_1 is the trivial character (in what follows, we think of $\alpha' = 0$) and for $\alpha \neq 1$, we set $\chi_\alpha = \psi_1^{\alpha'}$ and $\phi_\beta = \psi_1^{\beta'}$. Then

$$\begin{aligned}
\widehat{F}(\alpha,\beta) &= \sum_{x \in G_1} \left(\psi_1^{\beta'} \circ F\right)(x)\psi_1^{\alpha'}(x) \\
&= \sum_{x \in G_1} \exp(2\pi i\beta' \log_g(F(x))/n) \exp(2\pi i\alpha' \log_g(x)/n) \\
&= \sum_{x \in G_1} \exp\left(2\pi i/n \left(\beta' \log_g(F(x)) + \alpha' \log_g(x)\right)\right) \\
&= \sum_{x \in G_1} \exp\left(2\pi i/n \left(\log_g(F(x)^{\beta'} x^{\alpha'})\right)\right) \\
&= \sum_{x \in G_1} \psi_1\left(F(x)^{\beta'} x^{\alpha'}\right).
\end{aligned}$$

Thus,

$$|\widehat{F}(\alpha,\beta)|^2 = \left|\sum_{x\in G_1}\psi_1\left(F(x)^{\beta'}x^{\alpha'}\right)\overline{\sum_{y\in G_1}\psi_1\left(F(y)^{\beta'}y^{\alpha'}\right)}\right|$$
$$= \left|\sum_{x,y\in G_1}\psi_1\left(\left(\frac{F(x)}{F(y)}\right)^{\beta'}\left(\frac{x}{y}\right)^{\alpha'}\right)\right|.$$

Set $z = x/y$ to obtain

$$|\widehat{F}(\alpha,\beta)|^2 = \left|\sum_{y,z\in G_1}\psi_1\left(\left(\frac{F(zy)}{F(y)}\right)^{\beta'}z^{\alpha'}\right)\right|$$
$$= \left|\sum_{y,z\in G_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}z^{\alpha'}\right)\right|$$
$$= \left|\sum_{z\in G_1}\psi_1\left(z^{\alpha'}\right)\sum_{y\in G_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}\right)\right|.$$

We remark that if $z = 1$, $\log_g(z) = \log_g(\Delta_{F,z}) = 0$ and so the sum splits as

$$|\widehat{F}(\alpha,\beta)|^2 \leq n + \left|\sum_{z\in G_1, z\neq 1}\psi_1\left(z^{\alpha'}\right)\sum_{y\in G_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}\right)\right|. \tag{5.8}$$

First, we note that in any cyclic group of order $n \equiv 0 \pmod 2$, there is only one element of order 2 (isomorphic to $n/2$ in $\mathbb{Z}_n$), and so we need to consider only the first two cases of Theorem 5.2.7.

Case 1: $n \equiv 1 \pmod 2$ Identical to the odd characteristic case ((Case a) above), the image multiset of $\Delta_{F,z}$, for each $z \neq 1$, is given by $G_1 \setminus \{1, o_z\} \cup \{r_{0,z}, r_z\}$. We note that $r_{0,z} \neq r_z$ due to the minimality condition on the ambiguity.

We recall that $\alpha = 1$ maps to the trivial character (equivalently, consider $\alpha' = 0$), so that $\psi_1(z^{\alpha'}) = 1$ for all z. Therefore, for any $z \neq 1$ we have that

$$\sum_{y\in G_1}\psi_1(\Delta_{F,z}(y)^{\beta'}) = \left(0 - \psi_1(1) - \psi_{\beta'}(o_z) + \psi_{\beta'}(r_{0,z}) + \psi_{\beta'}(r_z)\right),$$

and so Equation (5.8) gives $|\widehat{F}(1,\beta)|^2 \leq 5n - 4$.

If $\alpha \neq 1$, the precise value of $|\widehat{F}(\alpha,\beta)|^2$ depends on the number of values that $z^{\alpha'}$ takes over the finite cyclic group of order n. It is easy to see that the number of images is $n/\gcd(n,\alpha') - 1$. We note that in the worst case, this cannot exceed $n-1$. Thus, Equation (5.8) gives $|\widehat{F}(\alpha,\beta)|^2 \leq 5n-4$, as in the $\alpha = 1$ case.

Case 2: $n \equiv 0 \pmod 2$ **and** $\iota_1 = \iota_2 = 1$ The difference in the derivation when $n \equiv 0 \pmod 2$ is only in the row corresponding to the order-2 element γ. For the $z = \gamma$ row, the row-deficiency is 1 and the image multiset of $\Delta_{F,\gamma}$ is $G_1 \setminus \{1\} \cup \{r\}$, where r is some repeated value. Every other row appears exactly as in the $n \equiv 1 \pmod 2$ case.

Both cases where $\alpha = 1$ and when $\alpha \neq 1$ provide identical upper bounds by the same reasoning as the $n \equiv 1 \pmod 2$ case. So consider $\alpha = 1$. Equation (5.8) becomes

$$\begin{aligned} |\widehat{F}(1,\beta)|^2 &\leq n + \left| \sum_{y \in G_1} \psi_1\left(\Delta_{F,\gamma}(y)^{\beta'}\right) \right| + \left| \sum_{\substack{z \in G_1 \\ z \neq 1, z \neq \gamma}} \sum_{y \in G_1} \psi_1\left(\Delta_{F,z}(y)^{\beta'}\right) \right| \\ &\leq 5n - 6. \end{aligned}$$

Theorem 5.3.2. *Let G be a finite cyclic group of order n and let F be a permutation of G with optimum ambiguity and deficiency. The non-linearity of F satisfies*

$$\mathbb{NL}(F) \geq \begin{cases} \frac{n-\sqrt{5n-4}}{n} & \text{if } n \text{ is odd,} \\ \frac{n-\sqrt{5n-6}}{n} & \text{if } n \text{ is even.} \end{cases}$$

APN permutations over $\mathbb{Z}_n$ are considered in [24] and their non-linearity is studied in [25]. A consequence of Parseval's identity gives that the linearity of an APN permutation F on $\mathbb{Z}_n$ satisfies $\sqrt{n} \leq \mathbb{L}(F) \leq n$. In [25], the authors show that the linearity of their APN permutations over $\mathbb{Z}_p$ appears to be asymptotically $2p^{0.55}$. In particular, the APN permutation used in the SAFER cryptosystem for $p = 257$ has linearity exactly 42.484. Our upper bound on the linearity for the case of permutations with optimal ambiguity and deficiency for this parameter is ≈ 35.791. We conclude that permutations with optimal ambiguity and deficiency are good candidates for S-box design due

G	Property	Non-linearity lower bound
$(\mathbb{F}_q, +)$	$\text{char}(\mathbb{F}_q) = p \neq 2$	$(q - \sqrt{5q-4})/q$
$(\mathbb{Z}_n, \cdot)$	n odd	$(n - \sqrt{5n-4})/n$
	n even	$(n - \sqrt{5n-6})/n$

Table 5.1: Lower bounds on the non-linearity of functions with optimal ambiguity and deficiency.

to *both* their strong linearity properties as well as their resistance to differential attacks.

We summarize the connection of ambiguity and deficiency of this function to its non-linearity in Table 5.1.

5.3.2 Non-balancedness

The non-linearity is the most common measure of the resistance of a function to linear cryptanalysis. However, other measures of "non-linearity" exist in the literature. For example, the measure

$$P_f = \max_{a \in G_1^*} \max_{b \in G_2} \frac{|\Delta_{f,a}^{-1}(b)|}{|G_1|}$$

is the maximum probability that $\Delta_{f,a}(x) = b$. This measure was introduced by Nyberg [52] and further studied in [11]. The same authors as [11] introduce a new measure in [12], which is our focus in this section.

Let G_1 and G_2 be finite Abelian groups and let $f \colon G_1 \to G_2$. The mean of the random variable $|f^{-1}(b)|$ is $|G_1|/|G_2|$ and f is balanced if and only if the random variable is a constant function. The variance of this random variable is

$$\frac{1}{|G_2|}\varepsilon_f = \frac{1}{|G_2|} \sum_{b \in G_2} \left(|f^{-1}(b)| - \frac{|G_1|}{|G_2|} \right)^2.$$

The scale-factor of $|G_2|^{-1}$ is given to ensure that ε_f is an integer.

Definition 5.3.3. *The* non-balancedness *of a function $f \colon G_1 \to G_2$ is given by*

$$\mathbb{NB}(f) = \sum_{a \in G_1^*} \varepsilon_{\Delta_{f,a}}.$$

The non-balancedness is always non-negative and is equal to 0 if and only if f is perfect non-linear [12]. We calculate the non-balancedness of permutations achieving the minimum ambiguity and deficiency, given in Theorem 5.2.7. We consider the non-balancedness of APN functions over 2-groups rather than the third case of Theorem 5.2.7, since the proof of that case does not give a row-by-row account of the ambiguity table. The non-balancedness of APN functions is given in [12], however we include this result in Proposition 5.3.4 for both comparison and completeness.

Proposition 5.3.4. *Let G_1 be a finite Abelian group of order n and let f be a permutation of G_1 having minimal ambiguity and deficiency. Then*

$$\mathbb{NB}(f) = \begin{cases} 4(n-1) & \text{if } n \equiv 1 \pmod 2, \\ 4(n-1)-2 & \text{if } n \equiv 0 \pmod 2 \text{ and } G_1 \text{ has one element of order } 2, \\ n(n-1) & \text{if } G_1 \text{ is a 2-group } (f \text{ is necessarily APN}). \end{cases}$$

Proof. Let $|G_1| = n$ and let f be a permutation of G_1. Since the domain and co-domain of f are the same, the mean of the random variable $|f^{-1}(b)|$ is equal to 1. The non-balancedness of f is given by

$$\mathbb{NB}(f) = \sum_{a \in G_1^*} \sum_{b \in G_2} \left(|\Delta_{f,a}^{-1}(b)|^2 - 2|\Delta_{f,a}^{-1}(b)| + 1 \right). \tag{5.9}$$

We focus on each term of the sum individually. The final term of Equation (5.9) is clearly equal to $n(n-1)$.

For the middle term of Equation (5.9), we have $\sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)| = n$ and summing over all $a \in G_1^*$ gives $\sum_{a,b} |\Delta_{f,a}^{-1}(b)| = n(n-1)$.

Consider now the first term of Equation (5.9),

$$\sum_{aG_1^*} \sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)|^2.$$

We split into cases as in Theorem 5.2.7 and follow the terminology used there.

Case 1: $n \equiv 1 \pmod 2$

Suppose f has minimum ambiguity and deficiency. By Theorem 5.2.7, the image multiset of $\Delta_{f,a}(G_1)$ is given by $G_1 \setminus \{0, o_a\} \cup \{r_{1,a}, r_{2,a}\}$, where $r_{1,a} \neq r_{2,a}$ by the minimality of the ambiguity. Thus,

$$\sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)|^2 = n - 4 + 2 \cdot 2^2 = n + 4.$$

Summing over all $a \in G_1^*$ gives

$$\sum_{a \in G_1^*} \sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)|^2 = (n-1)(n+4)$$

and the non-balancedness of f is

$$\mathbb{NB}(f) = (n-1)(n+4) - n(n-1) = 4(n-1).$$

Case 2: $n \equiv 0 \pmod 2$ **and** $\iota_1 = \iota_2 = 1$

In this case, each row is identical to that in **Case 1** except for the row corresponding to the order-2 element γ. For the row $a = \gamma$, the image multiset of $\Delta_{f,\gamma}(G_1) = G_2 \setminus \{0\} \cup \{o_\gamma\}$ and thus

$$\sum_{b \in G_2} |\Delta_{f,\gamma}^{-1}(b)|^2 = n - 2 + 2^2 = n + 2.$$

The contribution from the first term is therefore

$$\sum_{a \in G_1^*} \sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)|^2 = n + 2 + (n-2)(n+4)$$

and the non-balancedness of f is

$$\mathbb{NB}(f) = n + 2 + (n-2)(n+4) - n(n-1) = 4(n-1) - 2.$$

Case 3: f is APN over a 2-group

Suppose f is APN over a 2-group, then $\Delta_{f,a}$ is exactly 2-to-1 for all $a \in G_1^*$. Thus,

$$\sum_{a \in G_1^*} \sum_{b \in G_2} |\Delta_{f,a}^{-1}(b)|^2 = (n-1)\left(\frac{n}{2} \cdot 2^2\right) = 2n(n-1)$$

and the non-balancedness of f is

$$\mathbb{NB}(f) = n(n-1). \qquad \square$$

APN functions over groups which are not 2-groups may have a range of non-balancedness. In particular, bijections which achieve the optimal ambiguity and deficiency are APN due to the inequality of the repeated elements of the images of their difference maps. Thus, Proposition 5.3.4 gives that certain APN permutations achieve a non-balancedness of less than $4n$, whereas in the worst case, when the difference maps are always 2-to-1 their non-balancedness is $n(n-1)$. This represents a range of non-balancedness in APN functions from linear to quadratic in n.

5.3.3 EA and CCZ-Equivalences

In Section 5.2 we show that a permutation and its compositional inverse have the same ambiguity and deficiency. In this section, we determine that ambiguity and deficiency of a function are invariant parameters under some other transformations. For example, adding a fixed element or applying a group automorphism to the left or right of the function does not affect the ambiguity or deficiency [55]. We extend this to common equivalence classes on cryptographic functions.

Definition 5.3.5. *A function $L\colon G_1 \to G_2$ is* linear *if $L(x+y) = L(x) + L(y)$ for all $x, y \in G_1$. A function $K\colon G_1 \to G_2$ is* affine *if $K(x+y) = K(x) + K(y) + c$ for a fixed constant $c \in G_2$ and every $x, y \in G_1$.*

In the classical definition of EA-equivalence, $G_1 = G_2 = (\mathbb{F}_{2^e}, +)$. While this is the most common practical case, our scope is more general and so we relax the restrictions on the domain and co-domain.

Definition 5.3.6. *Let G_1 and G_2 be arbitrary groups. Two functions F_1 and $F_2 : G_1 \to G_2$ are* Extended-Affine equivalent *(EA-equivalent), denoted $F_1 \overset{\text{EA}}{\sim} F_2$, if there exist affine permutations $K_1 \colon G_2 \to G_2, K_2 \colon G_1 \to G_1$ and an affine function $K_3 \colon G_1 \to G_2$ such that*

$$F_2 = K_1 \circ F_1 \circ K_2 + K_3.$$

If $K_3 = 0$, then F_1 and F_2 are affine equivalent*.*

We note that the nomenclature is well-defined, that is EA-equivalence is an equivalence relation on functions. EA-invariance of ambiguity and deficiency is shown in [55]. We present another standard definition of equivalence, originally given in [10]. As in EA-equivalence, we extend the usual definition to arbitrary groups. First, we introduce some necessary notation.

Definition 5.3.7. *Let G_1 and G_2 be arbitrary groups. If $F \colon G_1 \to G_2$ is a function, then the* graph *of F is defined as*

$$\mathcal{G}_F = \{(x, F(x)) : x \in G_1\} \subseteq G_1 \times G_2.$$

Definition 5.3.8. *The relation $\overset{\text{CCZ}}{\sim}$ defined on the set of functions $G_1 \to G_2$ such that $F_1 \overset{\text{CCZ}}{\sim} F_2$ if and only if*

$$K(\mathcal{G}_{F_1}) = \mathcal{G}_{F_2},$$

for some affine permutation $K \colon G_1 \times G_2 \to G_1 \times G_2$ is an equivalence relation. Functions in the same equivalence class are said to be Carlet-Charpin-Zinoviev equivalent *(CCZ-equivalent).*

It is easy to see that EA-equivalence is contained within CCZ-equivalence. In other words, if two functions are EA-equivalent, then they are CCZ-equivalent. It is well-known that the property of a function being APN is invariant under CCZ-equivalence, see [10]. Since CCZ-equivalence classes are larger than EA-equivalence classes, showing CCZ-invariance of these parameters is a stronger result. We note that the proof is similar to that of the APN case, but we include it in its entirety for completeness.

Theorem 5.3.9. *If F and F' are CCZ equivalent functions, then the entries of the ambiguity and*

deficiency tables of F' are a permutation of the entries of the ambiguity and deficiency tables of F, respectively.

Proof. Suppose $F\colon G_1 \to G_2$ and denote by $\mathcal{G}_F$ the graph of F. For an affine permutation $K\colon G_1 \times G_2 \to G_1 \times G_2$, we denote by $\mathcal{K}$ the restriction of K to graphs of functions. The function $\mathcal{K}$ remains a permutation on graphs of functions, so $\mathcal{K}^{-1}$ is well-defined. Such an affine function can be considered as a pair of affine functions $K_1\colon G_1 \times G_2 \to G_1$ and $K_2\colon G_1 \times G_2 \to G_2$ such that $\mathcal{K}(x, F(x)) = (F_1(x), F_2(x))$, where

$$F_1(x) = K_1(x, F(x)),$$
$$F_2(x) = K_2(x, F(x)).$$

We claim that the image $\mathcal{K}(\mathcal{G}_F)$ is the graph of a function if and only if F_1 is a permutation. Clearly, if the image $\mathcal{K}(\mathcal{G}_F)$ is the graph of a function, then F_1 must be a permutation. Suppose the converse, that F_1 is a permutation, and let $F' = F_2 \circ F_1^{-1}$. Then $\mathcal{K}(x, F(x)) = (F_1(x), F_2(x)) = (y, F'(y))$, where y ranges over all of G_1 as x ranges over G_1. Thus, $\mathcal{K}(\mathcal{G}_F) = \mathcal{G}_{F'}$.

Suppose F, F' are CCZ-equivalent functions, that is $\mathcal{K}(\mathcal{G}_F) = \mathcal{G}_{F'}$ for some linear map $\mathcal{K} = (K_1, K_2)$ and define F_1 and F_2 as before. Consider solutions of the equations

$$\begin{aligned} y - x &= a, \\ F'(y) - F'(x) &= b, \end{aligned} \tag{5.10}$$

with $F' = F_2 \circ F_1^{-1}$. Set $x = F_1(x')$ and $y = F_1(y')$ for some $x', y' \in G_1$ (this is well-defined because F_1 is a permutation) to get

$$F_1(y') - F_1(x') = a,$$
$$F_2(y') - F_2(x') = b.$$

We apply the affine inverse permutation $\mathcal{K}^{-1}$, where $(x, F(x)) \overset{\mathcal{K}^{-1}}{\leftarrow} (F_1(x), F_2(x))$ and $(a', b') \overset{\mathcal{K}^{-1}}{\leftarrow}$

(a, b), to obtain the system

$$y' - x' = a',$$
$$F(y') - F(x') = b'.$$

Since every map applied was invertible, the number of solutions to the system is the same as the number of solutions of Equation (5.10). □

Corollary 5.3.10. *Let* $F\colon G_1 \to G_2 \overset{\text{CCZ}}{\sim} F'\colon G_1 \to G_2$. *The properties of PN, APN, ambiguity and deficiency are all invariant between* F *and* F'.

5.4 Ambiguity and deficiency of common functions

In this section we give the ambiguity and deficiency of some known permutation functions. In Section 5.4.1, we present some functions with optimal or near-optimal ambiguity and deficiency which appear in [55]. In Section 5.4.2, we give the ambiguity and deficiency of functions with known differential uniformity. We end in Section 5.4.3 with a discussion of the ambiguity and deficiency of maps between both the additive and multiplicative groups of finite fields which are induced by linearized polynomials.

5.4.1 Twists and Möbius functions

In this section, we briefly cite the ambiguities and deficiencies of functions given in [55]. We give these without proof, since these constructions appear before the commencement of this thesis.

We first introduce a way to obtain a permutation polynomial with fixed point 0 over a finite field $\mathbb{F}_q$ from another permutation polynomial of $\mathbb{F}_q$ which does not fix 0. Let h be a permutation

polynomial of $\mathbb{F}_q$ such that $h(0) = a \neq 0$ and $h(b) = 0$. Then we define another polynomial g by

$$g(x) = \begin{cases} h(b) = 0, & x = 0, \\ h(0) = a, & x = b, \\ h(x), & x \neq 0, b. \end{cases}$$

It is obvious that g is again a permutation polynomial of $\mathbb{F}_q$ which fixes 0.

Such a *twist* of permutation polynomials can be used to construct permutations of $\mathbb{Z}_n$ with optimum deficiency and optimum ambiguity.

Theorem 5.4.1. *Let q be a prime power, $n = q-1$ and α a primitive element in $\mathbb{F}_q$. For $\gcd(e, n) = 1$ and $m, a \neq 0 \in \mathbb{F}_q$, let $h : \mathbb{F}_q \to \mathbb{F}_q$ be defined by $h(x) = mx^e + a$ and let b be the unique (non-zero) field element such that $h(b) = 0$. Let*

$$g(x) = \begin{cases} h(b) = 0, & x = 0, \\ h(0) = a, & x = b, \\ h(x) = mx^e + a, & x \neq 0, b. \end{cases}$$

Finally, define $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f(i) = \log_\alpha(g(\alpha^i))$. When q is odd, the ambiguity of f is given by

$$A(f) = \begin{cases} 2n - 3 & \text{if } q \equiv 0 \pmod 3, \\ 2(n-1) & \text{if } q \equiv 1 \pmod 3, \\ 2(n-2) & \text{if } q \equiv 2 \pmod 3, \end{cases}$$

and the deficiency of f is given by

$$D(f) = \begin{cases} 2n - 3 & \text{if } q \equiv 0 \pmod 3, \\ 2(n-2) & \text{if } q \equiv 1 \pmod 3, \\ 2(n-2) & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

If q is even, the ambiguity of f is given by

$$A(f) = \begin{cases} 2n & \text{if } q \text{ is an even power of } 2, \\ 2(n-1) & \text{if } q \text{ is an odd power of } 2, \end{cases}$$

and the deficiency of f is given by

$$D(f) = 2(n-1),$$

for all powers of 2.

We now give the ambiguity and deficiency of the *Möbius transformation* over a finite field, which is similar in shape to the classical Möbius transformation over the complex plane.

Theorem 5.4.2. *Let $q = p^m$, $n = q-1$ and α a primitive element in $\mathbb{F}_q$. Let $g : \mathbb{F}_q \to \mathbb{F}_q$ be defined as follows*

$$g(x) = \begin{cases} \frac{\beta x}{\gamma x + \eta} & x \neq \frac{-\eta}{\gamma}, \\ \frac{\beta}{\gamma} & x = \frac{-\eta}{\gamma}, \end{cases}$$

where $\beta, \gamma, \eta \neq 0$. Finally, define $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f(i) = \log_\alpha(g(\alpha^i))$. Then ambiguity and deficiency of f is identical to that of Theorem 5.4.1.

5.4.2 Ambiguity and deficiency of differential-k-uniform functions

In this section, we focus on functions which are known to be used in cryptographic settings. We begin with deriving the ambiguity and deficiency of APN functions.

APN functions

Proposition 5.4.3. *Suppose f defines an APN function over $\mathbb{F}_q$, q even. Then, the ambiguity and deficiency of f are given by*

$$A(f) = (q-1)\frac{q}{2},$$
$$D(f) = (q-1)\frac{q}{2},$$

respectively.

Proof. Since f is APN over a finite field $\mathbb{F}_q$ of even characteristic (hence, a 2-group), $\Delta_{f,a}$ is exactly 2-to-1 for all a. A simple counting gives that the ambiguity and deficiency of f are

$$A(f) = (q-1)\binom{2}{2}\frac{q}{2},$$
$$D(f) = (q-1)\frac{q}{2},$$

respectively. □

We state the ambiguity and deficiency of some APN monomial functions over finite fields of odd characteristic. We omit the proof since it appears in [55].

Proposition 5.4.4. *Let $q = p^e$ and let $f(x) = x^d$, where the exponent d admits an APN monomial, as in Table 3.5. Then both the ambiguity and deficiency of f are equal to $(q-1)\frac{q-1}{2}$.*

Inverse function

By Proposition 4.4.1, the inverse function used in AES is known to be APN over $\mathbb{F}_{2^n}$ when n is odd and is differential-4-uniform when n is even. We rephrase Proposition 4.4.1 in terms of ambiguity and deficiency.

Proposition 5.4.5. *Let $f(x) = x^{2^n-2} \in \mathbb{F}_{2^n}[x]$. Then the ambiguity and deficiency of f are given by*

$$A(f) = \begin{cases} (2^n-1)\frac{2^n}{2} & \text{if } n \text{ is odd,} \\ (2^n-1)\left(\frac{2^n+8}{2}\right) & \text{if } n \text{ is even;} \end{cases} \tag{5.11}$$

$$D(f) = \begin{cases} (2^n-1)\frac{2^n}{2} & \text{if } n \text{ is odd,} \\ (2^n-1)\frac{2^n-2}{2} & \text{if } n \text{ is even,} \end{cases} \tag{5.12}$$

respectively.

Proof. If n is odd, then f is APN and the result follows from Proposition 5.4.3.

If n is even, then by Proposition 4.4.1, for every $a \in \mathbb{F}_{2^n}^*$ there is one b such that $\Delta_{f,a}(x) = b$ has 4 solutions and for every other b, $\Delta_{f,a}(x) = b$ has either 0 or 2 solutions. Thus,

$$A(f) = (2^n - 1)\left(\binom{4}{2} + \binom{2}{2}\frac{2^n - 4}{2}\right),$$
$$D(f) = (2^n - 1)\left(\frac{2^n - 2}{2}\right).$$ □

Differential-k-uniform functions

Here we give bounds on the ambiguity and deficiency of functions with any differential uniformity, motivated by the small difference between the ambiguity of the inverse function of AES and that of an APN function over a 2-group. The bounds become further apart as the differential uniformity grows.

Proposition 5.4.6. *Let $f\colon G_1 \to G_1$ be a function with differential uniformity k. Suppose further that $|G_1| = n = rk + s$, for some r, s with $0 \le s < n$. Then the ambiguity of f satisfies*

$$\binom{k}{2} \le A(f) \le (n-1)\left(r\binom{k}{2} + \binom{s}{2}\right),$$

and the deficiency of f satisfies

$$k - 1 \le D(f) \le (n-1)\left(n - r + \delta_s\right),$$

where $\delta_s = 0$ if $s = 0$ and $\delta_s = 1$ otherwise.

Proof. Let $f\colon G_1 \to G_1$ be a function having differential uniformity k. Thus, $\Delta_{f,a}$ is at most k-to-1 for all $a \in G_1^*$. As in the hypothesis, suppose $|G_1| = n = rk + s$ for some r, s with $0 \le s < n$.

For the lower bound, suppose $\Delta_{f,a}(x) = b$ has k solutions for a single pair (a, b), and has either a unique solution or no solution for all other pairs $(a', b') \neq (a, b)$. Contributions to the ambiguity come only from the pair (a, b). The lower bound on the deficiency occurs in the same scenario. In this case, $|\Delta_{f,a}(G_1)| = n - k + 1$ and $\Delta_{f,a'}(G_1) = G_1$ for $a' \neq a$.

The upper bound is attained when $\Delta_{f,a}(x) = b$ has either k solutions or no solution for all pairs (a, b). Additionally, if k does not divide n, the maximum ambiguity and the maximum deficiency are both attained when, for each a, the images of the remaining s elements of $\Delta_{f,a}$ coincide. □

Perhaps the most striking observation is that the lower bounds of the ambiguity and deficiency of differential-k-uniform functions are both linear in k (which is at most n, and is in practice much smaller than n) and the upper bounds are quadratic in n.

5.4.3 Linearized polynomials

The ambiguity and deficiency of linearized polynomials are treated next.

Proposition 5.4.7. *Let $L(x) = \sum_{j=0}^{e-1} \ell_j x^{p^j}$ be a linearized polynomial over $\mathbb{F}_q$, $q = p^e$. Then $D(L) = (q-1)^2$ and $A(L) = (q-1)\binom{q}{2}$.*

Proof. Let us consider $\Delta_{L,a}$ for an arbitrary $a \in \mathbb{F}_q^*$:

$$\begin{aligned}\Delta_{L,a}(x) = L(x+a) - L(x) &= \sum_{j=0}^{e-1} \ell_j (x+a)^{p^j} - \sum_{j=0}^{e-1} \ell_j x^{p^j} \\ &= \sum_{j=0}^{e-1} \ell_j \left(x^{p^j} + a^{p^j}\right) - \sum_{j=0}^{e-1} \ell_j x^{p^j} = \sum_{j=0}^{e-1} \ell_j a^{p^j}.\end{aligned}$$

Thus, $\Delta_{L,a}$ is a constant function for every $a \in \mathbb{F}_q^*$. In other words, for every $a \in \mathbb{F}_q^*$ there exists a unique $b = \sum_{j=0}^{e-1} \ell_j a^{p^j}$ such that $\Delta_{L,a}(x) = b$ has exactly q solutions and there are $q-1$ choices for $b \in \mathbb{F}_q$ where $\Delta_{L,a}(x) = b$ has no solution. Since there are $q-1$ elements like $a \in \mathbb{F}_q^*$, $D(L) = (q-1)^2$ and $A(L) = (q-1)\binom{q}{2}$. □

If we consider $L\colon \mathbb{F}_q^* \to \mathbb{F}_q$, then for $a \neq 0, 1$, we have $\Delta_{L,a}(x) = L(xa) - L(x) = L(x(a-1))$, which is again a linearized polynomial. The cardinality of the value set of a linearized polynomial is given by Corollary 3.6.4 and depends on the form of the linearized polynomial.

Proposition 5.4.8. *Let $L\colon \mathbb{F}_q^* \to \mathbb{F}_q$ be the induced map from a linearized polynomial K over $\mathbb{F}_q$*

and denote by V_L the value set of L. Then the ambiguity and deficiency of L satisfy

$$A(L) = \begin{cases} (q-2)(|V_L|)\binom{\frac{q}{|V_L|+1}}{2} & \text{if } K \text{ is a permutation polynomial,} \\ (q-2)\left((|V_L|-1)\binom{\frac{q}{|V_L|}}{2} + \binom{\frac{q}{|V_L|}-1}{2}\right) & \text{otherwise,} \end{cases}$$

and $D(L) = (q-2)(q-1-|V_L|)$.

Proof. Let $q = p^e$ and let $L\colon \mathbb{F}_q^* \to \mathbb{F}_q$ be the map induced by $K(x) = \sum_{i=0}^{e-1} \ell_i x^{p^i} \in \mathbb{F}_q[x]$, $x \neq 0$. Then for $a \neq 1$, $\Delta_{K,a}(x) = K(x(a-1)) = K \circ ((a-1)x)$. The cardinality of the value set of K, $|V_K|$, is unchanged under an invertible composition. Furthermore, the cardinality of the value set of L is given by

$$|V_L| = \begin{cases} |V_K| - 1 & \text{if } K \text{ contains no roots but 0,} \\ |V_K| & \text{otherwise.} \end{cases}$$

If K contains no non-zero roots, then K is a permutation polynomial over $\mathbb{F}_q$ by Theorem 3.1.3.

Since K defines a linear operator on $\mathbb{F}_q$, the equal cardinalities of the value sets of K and $\Delta_{K,a}$ are a divisor of q (equivalently, a power of p). Furthermore, the number of repetitions of each non-zero element in the value set is given by $q/|V_K|$. If K contains non-zero roots, the number of (non-zero) repetitions of the 0 element in the value set is $(q/|V_K|) - 1$. The calculation of the ambiguity and deficiency is now immediate from the definition. □

We cannot properly define the ambiguity and deficiency of linearized polynomials $L\colon \mathbb{F}_q \to \mathbb{F}_q^*$, since $\Delta_{L,a}(x) = L(x+a)/L(x)$ and $L(0) = 0$ is a valid pre-image. One case of linearized polynomials remains. If $L\colon \mathbb{F}_q^* \to \mathbb{F}_q^*$ is the map induced by a linearized polynomial $K(x) = \sum_{i=0}^{e-1} \ell_i x^{q^i} \in \mathbb{F}_{q^e}[x]$, then for $x \neq 0$, $\Delta_{L,a}(x) = K(ax)/K(x)$. Indeed, we note that in order to avoid division by zero, we require the rational functions $\Delta_{L,a}$ to be *total*, that is that K must contain no non-zero roots. Equivalently, by Theorem 3.1.3, K must be a permutation polynomial. Even under this condition the value sets of rational functions is likely a hard problem, and we leave this case for future work.

The ambiguity and deficiency of Dembowski-Ostrom polynomials, namely those polynomials over a finite field whose difference maps yield linearized polynomials, are treated in detail in Chapter 6.

Chapter 6

Ambiguity and deficiency of DO Polynomials

This chapter deals with finding the ambiguity and deficiency of Dembowski-Ostrom (DO) polynomials; see Section 3.5 for more information on DO polynomials. In Section 6.1, we use the characterization of DO polynomials from Theorem 3.5.3, namely that DO polynomials have linearized difference maps, to give a formula for their ambiguities and deficiencies in terms of matrices described in Section 3.6.2. We analyze various cases of DO polynomials; specifically the DOs which define permutation polynomials given in Section 3.5.

The results from Sections 6.1, 6.3 and 6.4 appear in [53]. Section 6.2 does not appear in that paper since it is possible to obtain the result by elementary means. We include our derivation here for completeness and for proof-of-concept. In addition, we note that we do not use the permutation property of the DO polynomials in any of the following sections, only the conditions which describe the DO polynomials as permutations.

6.1 A formula for ambiguity and deficiency

Here, we derive a formula for the ambiguity and deficiency of DO functions in terms of ranks of matrices.

We briefly recall Corollary 3.6.4, which states that the cardinality of the value set of a linearized polynomial $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i} \in \mathbb{F}_{q^e}[x]$ is given by $q^{\mathrm{rk}(\mathbf{M}_a)}$, where $\mathbf{M}_a$ is the matrix given in Equation (3.7) and re-stated below

$$\mathbf{M}_a = \begin{bmatrix} a_0 & a_{e-1}^q & \cdots & a_1^{q^{e-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ a_{e-1} & a_{e-2}^q & \cdots & a_0^{q^{e-1}} \end{bmatrix}.$$

In addition, the number of pre-images of each element of the value set is given by $q^{e-\mathrm{rk}(\mathbf{M}_a)}$. We combine this with Theorem 3.5.3, which states that if f is the sum of a DO polynomial, a linearized polynomial and a constant polynomial, then $\Delta_{f,a}(x)$ is the sum of a linearized polynomial and a constant. Since the addition of a constant does not affect the cardinality of the value set, we obtain the following theorem as a consequence.

Theorem 6.1.1. *Let $f = D + L + c$, where D is a DO polynomial, L is a linearized polynomial and c is a constant. Furthermore, let $\Delta_{f,a} = L_a + c_a$, for any $a \in \mathbb{F}_q^*$, as in Theorem 3.5.3. Furthermore, let $\mathbf{M}_a$ be the matrix corresponding to L_a given in Equation* (3.7)*. The ambiguity and deficiency of f are given by*

$$A(f) = \sum_{a \in \mathbb{F}_{q^e}^*} q^{\mathrm{rk}(\mathbf{M}_a)} \binom{q^{e-\mathrm{rk}(\mathbf{M}_a)}}{2}, \text{ and} \tag{6.1}$$

$$D(f) = \sum_{a \in \mathbb{F}_{q^e}^*} (q^e - q^{\mathrm{rk}(\mathbf{M}_a)}), \tag{6.2}$$

respectively.

Proof. Define L_a as in the hypothesis and denote by V_{L_a} the value set of L_a. Since L_a is a linearized

polynomial, we have $|V_{L_a}| = q^{\mathrm{rk}(\mathbf{M}_a)}$ and every $b \in V_{L_a}$ contains the same number of preimages, $q^{e-\mathrm{rk}(\mathbf{M}_a)}$. Thus, the ambiguity and deficiency of f are respectively given by

$$A(f) = \sum_{a \in \mathbb{F}_{q^e}^*} q^{\mathrm{rk}(\mathbf{M}_a)} \binom{q^{e-\mathrm{rk}(\mathbf{M}_a)}}{2}$$

$$D(f) = \sum_{a \in \mathbb{F}_{q^e}^*} (q^e - q^{\mathrm{rk}(\mathbf{M}_a)}). \qquad \square$$

6.2 The Gold function

Let q be a power of a prime p and let e be a positive integer. Also, let $f(x) = x^{q^i+q^j} = x^{q^j\left(q^{i-j}+1\right)} \in \mathbb{F}_{q^e}[x]$ be a DO monomial. Since $(q^j, q^e - 1) = 1$ for all j, f is the composition of a permutation, say $f_1(x) = x^{q^j}$ and a q-ary Gold polynomial $f_2(x) = x^{q^{i-j}+1}$. Since f_1 is a permutation, we restrict our attention to the Gold polynomial f_2.

We give the precise form of $\Delta_{f,a}$ when f is a Gold polynomial. The proof is immediate from the definition of f.

Lemma 6.2.1. *Let $f(x) = x^{q^k+1}$ be a Gold polynomial over $\mathbb{F}_{q^e}$. Then $\Delta_{f,a} = ax^{q^k} + a^{q^k}x + c_a$, for some constant c_a.*

We now apply Theorem 6.1.1 to obtain the ambiguity and deficiency of the q-ary Gold polynomial.

Lemma 6.2.2. *For any positive integer $k < e$, let $d = \gcd(k, e)$ and let $L(x) = ax^{q^k} + a^{q^k}x \in \mathbb{F}_{q^e}[x]$. Then the value set of L, V_L, satisfies $|V_L| = q^{e-d}$.*

Proof. Let $L(x) = ax^{q^k} + a^{q^k}x \in \mathbb{F}_{q^e}[x]$, as given in Lemma 6.2.1. The matrix $\mathbf{M}_a$, as in Equa-

tion (3.7), has two diagonals and is given by

$$\mathbf{M}_a = \begin{bmatrix} a^{q^k} & 0 & \cdots & a^{q^{e-k}} & 0 & \cdots & 0 \\ 0 & a^{q^{k+1}} & \cdots & 0 & a^{q^{e-k+1}} & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \\ a & & & & & & \\ & \ddots & & & & \ddots & \\ 0 & \cdots & a^{q^{e-k-1}} & 0 & \cdots & & a^{q^{k+e-1}} \end{bmatrix}. \tag{6.3}$$

If $e = 2k$, then clearly the bottom k rows each have 2 identical nonzero entries which align with the first k rows. Thus, $\mathbf{M}_a$ has rank k.

Now, we assume that $e > 2k$ without loss of generality by considering instead the transpose of $\mathbf{M}_a$, if necessary. Also, let $d = \gcd(e, k)$ and let $e_0 = e/d$. The matrix $\mathbf{M}_a$ contains two non-zero transversals: on the main diagonal and another shifted exactly $e - k$ spaces to the right of the main diagonal.

Since there are exactly 2 non-zero entries per row and column, we term the *row-mate* and *column-mate* of a non-zero entry to be the other non-zero in its row and column, respectively. We perform the following algorithm to reduce the matrix. Beginning at the $(0, 0)$-position, we exchange Row 1 and Row k (note that Row k contains the column-mate for a_{00}), followed by exchanging Column 1 and Column k (again, noting that Column k contains the Row-mate of the new a_{10}). We perform the same operation, preserving the two transversals on the diagonal and sub-diagonal at each step beginning from position (i, i), $i = 0, 1, \ldots, e_0 - 2$.

It is clear that every entry below position $(i + 1, i)$ is 0 for $i = 0, 1, \ldots, e_0 - 2$. Now, consider Column $e_0 - 1$. By the algorithm, position $(e_0 - 1, e_0 - 1)$ is non-zero. Furthermore, the final column swap is Column $e_0 - 1$ with Column $e - k$, completing the sub-diagonal transversal with an entry in the $(0, e_0 - 1)$ position. More precisely, the column-mate below the diagonal is the q^{e-k}th power of the entry on the diagonal, and the row-mate to the right of the sub-diagonal on Row i is the $q^{(i+1)k}$th power of the entry on the sub-diagonal, $i = 1, 2, \ldots, e_0 - 1$. Thus, the entries in the main

diagonal of the block will be of the form $a^{q^{k+jk}}$, $j = 0, 1, \ldots, e_0 - 1$.

To complete the reduction of the matrix, begin at the (ie_0, ie_0), $i = 0, 1, \ldots, d-1$, entry of the reduced matrix, and repeat the above process.

After completion of the algorithm, what remains is a block matrix of the form

$$\begin{bmatrix} D_0 & 0_{e_0} & \cdots & 0_{e_0} \\ 0_{e_0} & D_1 & \cdots & 0_{e_0} \\ \vdots & \vdots & & \vdots \\ 0_{e_0} & 0_{e_0} & \cdots & D_{d-1} \end{bmatrix},$$

where 0_k is the $k \times k$ all-zero matrix.

The matrix D_0, is of the form

$$\begin{bmatrix} a^{q^k} & 0 & 0 & 0 & \cdots & a^{q^{e-k}} \\ a & a^{q^{2k}} & 0 & 0 & \cdots & 0 \\ 0 & a^{q^k} & a^{q^{3k}} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a^{q^{e_0 k}} \end{bmatrix}.$$

Moreover, the set of entries along each transversal of D_0 are identical: both are equal to the set of all $a^{q^{jk}}, j = 0, 1, 2, \ldots, e_0 - 1$. Furthermore, the elements of the block D_j, $j = 0, \ldots, d-1$, are precisely q^{je_0}th powers of the elements of D_0. Thus, $\det(\mathbf{M}_a) = 0$ if and only if $\det(D_0) = 0$. Furthermore, the rank of $\mathbf{M}_a$ is precisely $d \cdot \mathrm{rk}(D_0)$.

The determinant of D_0 is

$$\prod_{j=1}^{e_0} a^{q^{jk}} + (-1)^{e_0 - 1} a^{q^{e-k}} \prod_{j=0}^{e_0 - 1} a^{q^{jk}},$$

where again we note that the left and right products are identical. Thus, the determinant of D_0 is 0 if and only if either q is even, or if e_0 is even (for all q). Finally, we observe that any $(e_0 - 1) \times (e_0 - 1)$

minor of D_0 has full rank, since upon deletion of a row, or column, there is a corresponding column, respectively a row, which has a single non-zero term. □

A similar argument gives the rank of such a matrix over any integral domain. We leave the details to an interested reader. We give a series of corollaries summarizing the results of Lemma 6.2.2.

Corollary 6.2.3. *Let q be an odd prime power and let $0 \leq k < e$ be a positive integer with $d = \gcd(k, e)$. Finally, let $e_0 = e/d$. If e_0 is odd, then $f(x) = x^{q^k+1}$ is planar.*

We note that Corollary 6.2.3 is shown for the case where q is a prime using elementary methods in [17]. We do not actually improve upon that method: [17] could be re-written nearly identically with q a prime power.

Corollary 6.2.4. *Let $f = x^{q^k+1} \in \mathbb{F}_{q^e}[x]$ be a Gold polynomial and let $d = \gcd(e, k)$. The deficiency of f is given by*

$$D(f) = (q^e - 1)(q^e - q^{e-d}).$$

Proof. Let $d = \gcd(e, k)$. For fixed $a \in \mathbb{F}_{q^e}^*$, by Lemma 6.2.2 we have the number of images of $\Delta_{f,a}$ is q^{e-d}. Thus, the row-deficiency corresponding to a is $q^e - q^{e-d}$. Since every $a \in \mathbb{F}_{q^e}^*$ yields the same row-deficiency, the deficiency of f is $(q^e - 1)(q^e - q^{e-d})$. □

Corollary 6.2.5. *Let f be a Gold permutation, that is $f = x^{q^k+1} \in \mathbb{F}_{q^e}[x]$ with $\gcd(e, 2k) = 1$. Then the deficiency of f is given by $D(f) = (q^e - 1)(q^e - q^{e-1})$.*

Corollary 6.2.6. *Let $f = x^{q^k+1} \in \mathbb{F}_{q^e}[x]$ be a Gold polynomial and let $d = \gcd(e, k)$. The ambiguity of f, $A(f)$, is given by*

$$A(f) = (q^e - 1)q^{e-d}\binom{q^d}{2}.$$

In particular, if $q = 2^e$ Gold functions are APN when $\gcd(e, k) = 1$. Furthermore, x^3 is APN for all dimensions e.

Proof. By Lemma 6.2.2, for each $a \in \mathbb{F}_{q^e}^*$, there are at most two non-zero values contributing to the ambiguity: the $i = 0$ value (that is, corresponding to values in the co-domain which are not images of f) and the $i = q^d$ value. Therefore, the ambiguity $A(f) = (q^e - 1)q^{e-d}\binom{q^d}{2}$. □

The final assertion is well-known and can also be found in Table 3.4.

Corollary 6.2.7. *Let f be a Gold permutation, that is $f = x^{q^k+1} \in \mathbb{F}_{q^e}[x]$ with $\gcd(e, 2k) = 1$. Then the ambiguity of f is given by $A(f) = (q^e - 1)q^{e-1}\binom{q}{2}$.*

6.3 DO binomials and trinomials

In this section, we give the ambiguity and deficiency of the DO permutation binomials and trinomials from Theorem 3.5.5. The proof method is similar in both cases and uses the matrix formulation given in Section 6.1.

Theorem 6.3.1. *Let either $e = 3k$ or $2e = 3k$ and let $f(x) = xL(x) \in \mathbb{F}_{2^e}[x]$ be the DO permutation polynomial with $L(x) = x^{2^k} + cx^{2^{e-k}}$ and $c \neq \beta^{t(2^d-1)}$ for any integer t. Then, for $d = \gcd(e, k) = e/3$, the deficiency of f is*

$$D(f) = (2^e - 1)\left(2^e - 2^{2d}\right),$$

and the ambiguity of f is

$$A(f) = (2^e - 1)\, 2^{2d} \binom{2^{e-2d}}{2}.$$

Proof. Assume that $2e = 3k$, as the proof when $e = 3k$ is analogous. Suppose f is given as in the hypothesis, then

$$\begin{aligned}\Delta_{f,a}(x) &= (x + a)\left((x + a)^{2^k} + c(x + a)^{2^{e-k}}\right) - x\left(x^{2^k} + cx^{2^{e-k}}\right) \\ &= ax^{2^k} + cax^{2^{e-k}} + \left(a^{2^k} + ca^{2^{e-k}}\right)x + c_a,\end{aligned}$$

where $c_a \in \mathbb{F}_{2^e}$.

Let $L_a = \Delta_{f,a} - c_a$ and let $d = \gcd(e, k)$. Since $2e = 3k$, we have $d = e - k$, $e = 3d$ and $k = 2d$. The $e \times e$ matrix, denoted $\mathbf{M}_a$, in Equation (3.7) can be broken into diagonal blocks of size $d \times d$, where the jth entry along the diagonal is given in the following expression for $\mathbf{M}_a$ and every other

entry is equal to 0

$$\mathbf{M}_a = \begin{bmatrix} \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^j} & a^{2^{(e-k)+j}} & (ca)^{2^{k+j}} \\ (ca)^{2^j} & \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^{(e-k)+j}} & a^{2^{k+j}} \\ a^{2^j} & (ca)^{2^{(e-k)+j}} & \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^{k+j}} \end{bmatrix}, \quad j = 0, 1, \ldots, e-k-1.$$

We substitute $d = e - k$ and $2d = k$ for clarity and perform the following row operations:

1. $\text{Row}_j \leftarrow \text{Row}_j + \left(\dfrac{a^{2^{2d}} + ca^{2^d}}{a}\right)^{2^j} \text{Row}_{2d+j}, \quad j = 0, 1, \ldots, d-1;$
2. $\text{Row}_{d+j} \leftarrow \text{Row}_{d+j} + c^{2^j}\text{Row}_{2d+j}, \quad j = 0, 1, \ldots, d-1,$

to get a new block matrix of the form

$$\mathbf{M}_a \sim \begin{bmatrix} 0 & \Phi_j & \Phi_j^{2^{2d}} \\ 0 & \frac{a^{2^j}}{a^{2^{d+j}}}\Phi_j & \frac{a^{2^j}}{a^{2^{d+j}}}\Phi_j^{2^{2d}} \\ a^{2^j} & (ca)^{2^{d+j}} & \left(a^{2^{2d}} + ca^{2^d}\right)^{2^{2d+j}} \end{bmatrix},$$

where

$$\Phi_j = \left(a^{2^d} + \frac{\left(a^{2^{2d}} + ca^{2^d}\right) c^{2^d} a^{2^d}}{a}\right)^{2^j}.$$

It is clear that $\text{rk}(\mathbf{M}_a) \leq 2d$. To show equality, we determine that $\Phi_j \neq 0$ for any j, $0 \leq j \leq d-1$ and for any $a \in \mathbb{F}_{2^e}$.

Suppose that $\Phi_0 = 0$, then re-arranging gives

$$a = c^{2^d} a^{2^{2d}} + c^{2^d+1} a^{2^d}. \tag{6.4}$$

Raise to the power of 2^{2d} and multiply by c^{2^d} to obtain

$$c^{2^d} a^{2^{2d}} = c^{2^d+1}\left(a^{2^d} + c^{2^{2d}} a\right).$$

Substituting for the left-hand side using Equation (6.4) gives

$$a + c^{2^d+1}a^{2^d} = c^{2^d+1}a^{2^d} + c^{2^{2d}+2^d+1}a,$$

thus

$$1 = c^{2^{2d}+2^d+1} = c^{\left(2^{3d}-1\right)/\left(2^d-1\right)},$$

contradicting that $c \neq \beta^{t\left(2^d-1\right)}$ for a primitive element β.

□

Theorem 6.3.2. *Let $f(x) = xL(x)$ be the DO permutation polynomial over $\mathbb{F}_{2^e}$ where $L(x) = x^{2^{2k}} + c^{2^k+1}x^{2^k} + cx$ for which $e = 3k$ and $c \neq \beta^{t(2^d-1)}$ for any integer t. Then the deficiency of F is*

$$D(f) = \left(2^e - 1\right)\left(2^e - 2^{2k}\right)$$

and the ambiguity of F is

$$A(F) = \left(2^e - 1\right) 2^{2k} \binom{2^k}{2}.$$

Proof. Suppose f is given in the hypothesis, then

$$\begin{aligned}\Delta_{f,a}(x) &= (x+a)\left((x+a)^{2^{2k}} + c^{2^k+1}(x+a)^{2^k} + c(x+a)\right) - x\left(x^{2^{2k}} + c^{2^k+1}x^{2^k} + cx\right)\\ &= ax^{2^{2k}} + ac^{2^k+1}x^{2^k} + (c^{2^k+1}a^{2^k} + a^{2^{2k}})x + c_a,\end{aligned}$$

where c_a is a constant depending on a. Again, considering the value set of the polynomial $\Delta_{f,a} - c_a$, the $e \times e$ matrix in Equation (3.7), denoted $\mathbf{M}_a$, can be broken into $k \times k$ diagonal blocks, with the jth entry along the diagonal given in the following expression for $\mathbf{M}_a$ and every other entry is equal

to 0,

$$\begin{bmatrix} \mathbf{M}_a = \left(c^{2^k+1}a^{2^k} + a^{2^{2k}}\right)^{2^j} & a^{2^{k+j}} & (ac^{2^k+1})^{2^{2k+j}} \\ (ac^{2^k+1})^{2^j} & \left(c^{2^k+1}a^{2^k} + a^{2^{2k}}\right)^{2^{k+j}} & a^{2^{2k+j}} \\ a^{2^j} & (ac^{2^k+1})^{2^{k+j}} & \left(c^{2^k+1}a^{2^k} + a^{2^{2k}}\right)^{2^{2k+j}} \end{bmatrix}, j = 0, 1, \ldots, k-1.$$

Perform the following row operations:

1. $\text{Row}_j \leftarrow \text{Row}_j + \left(\dfrac{c^{2^k+1}a^{2^k} + a^{2^{2k}}}{a}\right)^{2^j} \text{Row}_{2k+j},\ j = 0, 1, \ldots, k-1$
2. $\text{Row}_{k+j} \leftarrow \text{Row}_{k+j} + \left(c^{2^k+1}\right)^{2^j} \text{Row}_{2k+j}, j = 0, 1, \ldots, k-1,$

to get a new block matrix of the form

$$\mathbf{M}_a \sim \begin{bmatrix} 0 & \Phi_j & \widetilde{\Phi_j} \\ 0 & \Psi_j & \Psi_j^{2^{2k}} \\ a^{2^j} & (ac^{2^k+1})^{2^{k+j}} & \left(c^{2^k+1}a^{2^k} + a^{2^{2k}}\right)^{2^{2k+j}} \end{bmatrix},$$

where

$$\begin{aligned} \Phi_j &= \left(a^{2^k} + c^{2^{2k}+2^{k+1}+1}a^{2^{k+1}-1} + a^{2^{2k}+2^k-1}c^{2^{2k}+2^k}\right)^{2^j}, \\ \widetilde{\Phi_j} &= \left(a^{2^{2k}+2^k-1} + a^{2^{k+1}-1}c^{2^k+1} + a^{2^k}c^{2^{2k}+2^k+2}\right)^{2^j}, \\ \Psi_j &= \left(a + a^{2^k}c^{2^{2k}+2^{k+1}+1} + a^{2^{2k}}c^{2^{2k}+2^k}\right)^{2^j}. \end{aligned}$$

We find that $\Psi_j = \frac{a^{2^j}}{a^{2^{k+j}}}\Phi_j$ and $\Psi_j^{2^{2k}} = \frac{a^{2^j}}{a^{2^{k+j}}}\widetilde{\Phi_j}$ and so our block matrix reduces to the form

$$\mathbf{M}_a \sim \begin{bmatrix} 0 & 0 & 0 \\ 0 & \Psi_j & \Psi_j^{2^{2k}} \\ a^{2^j} & (ac^{2^k+1})^{2^{k+j}} & \left(c^{2^k+1}a^{2^k} + a^{2^{2k}}\right)^{2^{2k+j}} \end{bmatrix}.$$

We have $\text{rk}(\mathbf{M}_a) = 2k$ if $\Psi_0 \neq 0$ and $\text{rk}(\mathbf{M}_a) = k$ otherwise. We see that $\Psi_0 = 0$ if and only if

$$a = a^{2^k}c^{2^{2k}+2^{k+1}+1} + a^{2^{2k}}c^{2^{2k}+2^k}. \tag{6.5}$$

Raise both sides of the last equation to the power 2^k and multiply with $c^{2^{2k}+2^{k+1}+1}$ to get

$$c^{2^{2k}+2^{k+1}+1}a^{2^k} = a^{2^{2k}}c^{3\cdot 2^{2k}+3\cdot 2^k+2} + ac^{2^{2k+1}+2^{k+1}+2}.$$

Replacing this with the first term in the right hand side of Equation (6.5), we obtain

$$\begin{aligned} a\left(1+c^{2^{2k+1}+2^{k+1}+2}\right) &= a^{2^{2k}}\left(c^{2^{2k}+2^k}+c^{3\cdot 2^{2k}+3\cdot 2^k+2}\right) \\ &= a^{2^{2k}}c^{2^{2k}+2^k}\left(1+c^{2^{2k+1}+2^{k+1}+2}\right). \end{aligned}$$

We can cancel out $1+c^{2^{2k+1}+2^{k+1}+2}$ from both sides because otherwise $\left(c^{2^{2k}+2^k+1}\right)^2 = 1$, and this implies a contradiction by the choice of c (the proof is similar to the last lines of Proposition 6.3.1). Hence $a = a^{2^{2k}}c^{2^{2k}+2^k}$. If we raise again both sides to the power 2^k, we have $a^{2^k} = ac^{2^{2k}+1}$ which is equivalent to $a^{2^k-1} = c^{2^{2k}+1}$. It follows that

$$\left(a^{2^k-1}\right)^{2^k\left(2^{2k}-2^k+1\right)} = \left(c^{2^{2k}+1}\right)^{2^k\left(2^{2k}-2^k+1\right)} = c^{2^{3k}+1} = c^2.$$

Therefore, $a^{2^{k-1}\left(2^k-1\right)\left(2^{2k}-2^k+1\right)} = c$, which contradicts the selection of c. □

6.4 Ambiguity and deficiency of DO permutations due to traces

This section is devoted to the calculation of three types of DO permutation polynomials which arise as images of trace functions. These polynomials are given in Theorem 3.5.6. We use an elementary proof method in this case, since the values of the trace function equi-partitions the extension field, see Section 2.1.2, and so the counting arguments follow readily. We observe that the matrix formulation given in Section 6.1 is also likely viable, since the trace functions will give dense matrices.

First, we show the ambiguity and deficiency of the DO permutation polynomial coming from the trace function given in Equation (3.4).

Theorem 6.4.1. *Let $s \in \mathbb{F}_q \setminus \{0,1\}$ and $f(x) = x(\mathrm{Tr}(x) + sx)$ be the DO permutation polynomial over $\mathbb{F}_{q^e}$ for even q and odd e. Then the deficiency of f is*

$$D(f) = q^e(q^e - 1) - (q^e - q^{e-1})q^{e-1} - (q^e - q)$$

and the ambiguity of f is

$$A(f) = \left(q^e - q^{e-1}\right) q^{e-1} \binom{q}{2} + (q^e - q) \binom{q^{e-1}}{2}.$$

Proof. Let us consider $\Delta_{F,a}(x)$ for $a \in \mathbb{F}_{q^e}^*$; we have

$$\begin{aligned} \Delta_{F,a}(x) &= (x+a)(\mathrm{Tr}(x+a) + s(x+a)) - x(\mathrm{Tr}(x) + sx) \\ &= x\mathrm{Tr}(a) + a\mathrm{Tr}(x) + a\mathrm{Tr}(a) + sa^2. \end{aligned}$$

If $\mathrm{Tr}(a) = 0$, then $\Delta_{F,a}(x) = a\mathrm{Tr}(x) + sa^2$. There are $q^{e-1} - 1$ pairs (a,b) such that $a \neq 0$, $b = at + sa^2$, $\mathrm{Tr}(x) = t$ and $\Delta_{F,a}(x) = b$ has exactly q^{e-1} solutions. Since $t \in \mathbb{F}_q$, there are q choices for t. Therefore, $q\left(q^{e-1} - 1\right) = (q^e - q)$ is the number of distinct pairs of (a,b) for which $\Delta_{F,a}(x) = b$ has exactly q^{e-1} solutions.

There exist $\left(q^e - q^{e-1}\right)$ elements a such that $\mathrm{Tr}(a) \neq 0$. On the other hand if $x\mathrm{Tr}(a) + a\mathrm{Tr}(x) + a\mathrm{Tr}(a) + sa^2 = b$, then applying $\mathrm{Tr}(\cdot)$ to both sides implies that

$$\begin{aligned} \mathrm{Tr}(b) &= \mathrm{Tr}\left(x\mathrm{Tr}(a) + a\mathrm{Tr}(x) + a\mathrm{Tr}(a) + sa^2\right) \\ &= \mathrm{Tr}(a)\mathrm{Tr}(x) + \mathrm{Tr}(x)\mathrm{Tr}(a) + \mathrm{Tr}(a)\mathrm{Tr}(a) + \mathrm{Tr}\left(sa^2\right) \\ &= \mathrm{Tr}(a)^2 + s\mathrm{Tr}(a)^2 = t_0^2(1+s). \end{aligned}$$

Since $\mathrm{Tr}(b) = t_0^2(1+s)$ is a constant, there are exactly q^{e-1} choices for b. Also the equation $\Delta_{f,a}(x) = x\mathrm{Tr}(a) + a\mathrm{Tr}(x) + a\mathrm{Tr}(a) + sa^2 = b$ has at least one solution for every pair (a,b) satisfying $\mathrm{Tr}(a) \neq 0$ and $\mathrm{Tr}(b) = t_0^2(1+s)$, since $x_0 = bt_0^{-1} + sa^2t_0^{-1} + a$ is one such solution. Now, since x_0 is

a solution for $\Delta_{F,a}(x) = b$, the element $x_0 + \beta_q a$, $\beta_q \in \mathbb{F}_q$ is another solution because

$$\begin{aligned}
\Delta_{f,a}(x_0 + \beta_q a) &= (x_0 + \beta_q a)\mathrm{Tr}(a) + a\mathrm{Tr}(x_0 + \beta_q a) + a\mathrm{Tr}(a) + sa^2 \\
&= x_0\mathrm{Tr}(a) + \beta_q a\mathrm{Tr}(a) + a\mathrm{Tr}(x_0) + a\mathrm{Tr}(\beta_q a) + a\mathrm{Tr}(a) + sa^2 \\
&= x_0\mathrm{Tr}(a) + \beta_q a\mathrm{Tr}(a) + a\mathrm{Tr}(x_0) + \beta_q a\mathrm{Tr}(a) + a\mathrm{Tr}(a) + sa^2 \\
&= x_0\mathrm{Tr}(a) + a\mathrm{Tr}(x_0) + a\mathrm{Tr}(a) + sa^2 = b.
\end{aligned}$$

Now suppose that y is a solution for $\Delta_{f,a}(x) = b$. Then $\Delta_{f,a}(y) = b = \Delta_{f,a}(x_0)$ implies that $y\mathrm{Tr}(a) + a\mathrm{Tr}(y) = x_0\mathrm{Tr}(a) + a\mathrm{Tr}(x_0)$ which is equivalent to $(y - x_0)\mathrm{Tr}(a) = a\mathrm{Tr}(y - x_0)$ or $y = x_0 + t_0^{-1}\mathrm{Tr}(y - x_0)a \in x_0 + a\mathbb{F}_q$. Therefore every other solution y for $\Delta_{F,a}(x) = b$ has to be in the form $x_0 + \gamma_q a$ for some $\gamma_q \in \mathbb{F}_q$. Hence under these assumptions $\Delta_{f,a}(x) = b$ has exactly q solutions, and the contribution to the ambiguity is $\left(q^e - q^{e-1}\right) q^{e-1}$. Overall the ambiguity of f is

$$\left(q^e - q^{e-1}\right) q^{e-1} \binom{q}{2} + (q^e - q) \binom{q^{e-1}}{2}.$$

Thus, there are $q^e(q^e - 1)$ possible pairs (a, b), we get

$$D(F) = q^e(q^e - 1) - (q^e - q^{e-1})q^{e-1} - (q^e - q).$$

□

Now, we treat the permutation polynomials due to traces introduced in Equations (3.5) and (3.6), see also [14].

Theorem 6.4.2. *Let $1 \leq k \leq e - 1$ and $1 \leq s \leq 2^e - 2$. Let $F(x) = x^{2^k} + x + Tr(x^s) \in \mathbb{F}_{2^e}$, where e is odd, $\gcd(k, e) = 1$ and s has 2-weight 1 or 2. If s has 2-weight 1, then the ambiguity and*

deficiency are respectively given by

$$A(f) = (2^e - 1)\binom{2^e}{2},$$
$$D(f) = (2^e - 1)^2.$$

If s has 2-weight 2, then the ambiguity and deficiency are respectively given by

$$A(f) = \left(2^{e+1} - 2^2\right)\binom{2^{e-1}}{2} + \binom{2^e}{2}$$
$$D(f) = 2^e(2^e - 1) - 2(2^e - 2) - 1.$$

Proof. If s has 2-weight 1, then f is linearized and the result follows from Proposition 5.4.7.

Suppose now that s has 2-weight 2, that is $s = 2^w + 2^j$ for some $0 \leq w < j$. Then,

$$\begin{aligned}\Delta_{f,a}(x) &= a^{2^k} + a + \mathrm{Tr}\left((x+a)^{2^w+2^j}\right) + \mathrm{Tr}\left(x^{2^w+2^j}\right) \\ &= a^{2^k} + a + \mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right).\end{aligned}$$

Since e is odd, $\mathrm{Tr}(1) = 1$ and it follows that $(a, b) = (1, 1)$ is the only pair with exactly 2^e solutions for $\Delta_{f,a}(x) = b$

There are 2^{e-1} elements $x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}$ satisfying

$$\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) = t_0 \in \mathbb{F}_2,$$

so we only need to enumerate the number of pairs

$$(a, b) = (a, a^{2^k} + a + t_0)$$

such that $a \in \mathbb{F}_{2^e} \setminus \{0, 1\}$. For all $a \in \mathbb{F}_{q^e}$, $a \neq 0, 1$, there are 2 solutions corresponding to $t_0 = 0, 1$, respectively. Thus the number of pairs is $2(2^e - 2)$. This completes the proof. □

We observe that the linearized portion of Equation (3.5) (that is, $x^{2^k} + x = f(x) - \mathrm{Tr}(x^s)$) does not affect the ambiguity or deficiency of f, since its difference map is constant. Thus, the ambiguity and deficiency of f would remain unchanged by replacing $x^{2^k} + x$ with any linearized polynomial. However, such a change may affect the permutation properties of f.

The polynomial given in Equation (3.6) can be decomposed as $f(x) = (x + \mathrm{Tr}(x^s)) \circ x^d$, where the monomial x^d defines a permutation polynomial. Here, we treat only the initial case $d = 1$.

Theorem 6.4.3. *Let $f(x) = x + \mathrm{Tr}(x^s) \in \mathbb{F}_{2^e}$, where e is even and s has 2-weight 1 or 2. The ambiguity and deficiency of f are respectively given by*

$$A(f) = (2^e - 1)\binom{2^e}{2},$$
$$D(f) = (2^e - 1)^2,$$

when s has 2-weight 1 and

$$A(f) = (2^e - 4) \cdot 2\binom{2^{e-1}}{2} + 3\binom{2^e}{2},$$
$$D(f) = 2^e(2^e - 1) - (2^{e+1} - 2^3) - 3,$$

when s has 2-weight 2.

Proof. If s has weight 1, then F is linearized and the result follows from Proposition 5.4.7. Suppose now that s has 2-weight 2, that is $s = 2^w + 2^j$ for some $0 \leq w < j$. Then,

$$\begin{aligned}\Delta_{f,a}(x) &= a + \mathrm{Tr}\left((x+a)^{2^w+2^j}\right) + \mathrm{Tr}\left(x^{2^w+2^j}\right) \\ &= a + \mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right).\end{aligned}$$

Since e is even, $\mathrm{Tr}(1) = 0$ and $\mathbb{F}_4 \subseteq \mathbb{F}_{2^e}$. We claim that the only pairs (a, b) with exactly 2^e solutions for $\Delta_{F,a}(x) = b$ are non-zero elements of $\mathbb{F}_4$. Let β be a primitive element of $\mathbb{F}_{2^e}$ and $\mathbb{F}_4^* = \{1, \eta, \eta + 1\}$ with $\eta = \beta^{(2^e-1)/3}$. For a non-unit $a \in \mathbb{F}_4^*$, it is clear that $a^{2^k} = a$ when k is even

and $a^{2^k} = a + 1$ otherwise. If the parity of i and j is the same, then

$$\begin{aligned}\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) &= \mathrm{Tr}\left(x^{2^w}a^{2^w} + a^{2^j}x^{2^j} + a^{2^{w+1}}\right)\\ &= \mathrm{Tr}\,(xa)^{2^w} + \mathrm{Tr}\,(xa)^{2^j} + \mathrm{Tr}\left(a^{2^{w+1}}\right) = \mathrm{Tr}(a).\end{aligned}$$

A similar derivation holds when $a = 1$. On the other hand, without loss of generality we can assume that w is even and j is odd and we have

$$\begin{aligned}\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) &= \mathrm{Tr}\left(x^{2^w}a + (a+1)x^{2^j} + a(a+1)\right)\\ &= \mathrm{Tr}\left(x^2a^2\right)^{2^{w-1}} + \mathrm{Tr}\left(x^2a^2\right)^{2^{j-1}} + \mathrm{Tr}\,(1) = 0.\end{aligned}$$

It is clear that there are 2^{e-1} elements satisfying

$$\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) = t_0,$$

for each choice of $t_0 \in \mathbb{F}_2$. So the number of pairs with

$$(a, b) = (a, a + t_0)$$

such that $a \in \mathbb{F}_{2^e} \setminus \{0, 1\}$ is of interest. A simple enumeration implies that the number of pairs is $2(2^e - 4)$. This completes the proof. □

Chapter 7

On a conjecture of Golomb and Moreno

In this chapter, we give a partial solution to a conjecture of Golomb and Moreno [33] on a multiplicative analogue of planar functions. Planar functions are discussed in Section 3.3; a function $f \in \mathbb{F}_q[x]$ is planar if $f(x+d)-f(x)$ is a permutation polynomial for all $d \neq 0$. The Golomb-Moreno conjecture is on the shape of polynomials such that $f(xd) - f(x)$ is a permutation polynomial for all $d \neq 1$. This is nearly the same scenario as we have considered in Chapters 5 and 6, where we are interested in the difference maps of functions between finite Abelian groups. The Golomb-Moreno conjecture therefore deals with the difference map of a function from the multiplicative group of the finite field to the additive group. In order to match our general framework, since $0 \notin \mathbb{F}_q^*$, we suppose further that $f(0) = 0$ and observe that $\Delta_{f,0} = -f$ is a permutation polynomial if and only if f is a permutation polynomial.

We introduce the Golomb-Moreno conjecture and give a partial solution in Section 7.1. In Section 7.2, we state a new conjecture which is implied by the Golomb-Moreno conjecture in terms of the number of *moved elements* of f. We also outline some first steps towards completing the proof. The results of this section appear in [62].

7.1 A partial solution using a method of Hiramine

In this section, we give a partial solution of a conjecture of Golomb and Moreno [33] on the multiplicative analogue of planar functions. Our solution follows the method of Hiramine [36] to determine that all planar polynomials over $\mathbb{F}_p[x]$ are quadratic. Since Golomb and Moreno's initial interest was on periodicity properties in Costas arrays, see Section 2.3, we define a *Costas* polynomial as follows.

Definition 7.1.1. *Let q be a power of an odd prime p. A polynomial $f \in \mathbb{F}_q[x]$ is* Costas *if $f(0) = 0$ and $\Delta_{f,d}(x) = f(xd) - f(x)$ is a permutation polynomial of $\mathbb{F}_q$ for all $d \in \mathbb{F}_q, d \neq 1$.*

A Costas polynomial f must be a permutation polynomial, since $\Delta_{f,0} = f(0) - f(x)$ is a permutation polynomial. By Corollary 2.2.9, f is a permutation polynomial if and only if $af + b$ is a permutation polynomial for any constants $a \neq 0$ and b. Thus, without loss of generality, we assume f is monic.

The polynomial $\Delta_{f,d}(x) = f(xd) - f(x)$ has domain equal to $\mathbb{F}_q$ rather than the expected $\mathbb{F}_q^*$ if $\Delta_{f,d}$ is considered as a difference map between from $\mathbb{F}_q^*$ to $\mathbb{F}_q$. However, with $f(0) = \Delta_{f,d}(0) = 0$ and the requirement that f is a permutation (hence, $\Delta_{f,0}$ is a permutation), the Golomb-Moreno conjecture fits into our previous framework.

We now state the conjecture of Golomb and Moreno in this language.

Conjecture 7.1.2. *Let $f \in \mathbb{F}_p[x]$ be a Costas polynomial. Then f is a monomial.*

Throughout this discussion, since f is permutation polynomial of $\mathbb{F}_q$ if and only if $g \equiv f \pmod{x^q - x}$ is a permutation polynomial of $\mathbb{F}_q$, we restrict our attention to polynomials of degree less than q.

Conjecture 7.1.2 is surely false if f is taken over a non-trivial extension of $\mathbb{F}_p$. For example, if L is a linearized polynomial, then $\Delta_{L,d}(x) = L(xd) - L(x) = L((d-1)x)$. Thus, $\Delta_{L,d}$ is a permutation polynomial for all $d \neq 1$ if L is a linearized permutation polynomial. Over $\mathbb{F}_p$, however, the only monic linearized polynomial is $f(x) = x$.

Proposition 7.1.3. *If $f(x) = x^s \in \mathbb{F}_q[x]$ then $\Delta_{f,d}$ is a permutation polynomial of $\mathbb{F}_q$ for all $d \in \mathbb{F}_q, d \neq 1$ if and only if $\gcd(q-1, s) = 1$.*

Proof. Suppose $d \in \mathbb{F}_q^*$, $d \neq 1$ and let $f(x) = x^s \in \mathbb{F}_q[x]$, $s \geq 1$ with $\gcd(q-1, s) = 1$. Then $f(xd) - f(x) = (d^s - 1)x^s$. Since $\gcd(q-1, s) = 1$ we know $d^s - 1 \neq 0$ for all $d \in \mathbb{F}_q$, $d \neq 1$. Thus $f(xd) - f(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if x^s is a permutation polynomial of $\mathbb{F}_q$, equivalently $\gcd(s, q-1) = 1$. □

Lemma 7.1.4. *Let f be a Costas polynomial. Then $f(-x) = -f(x)$ and all of its terms have odd degree.*

Proof. Let $y_1, y_2, \ldots, y_{p-1}$ be a circular Costas sequence, that is for any $i = 1, 2, \ldots, p-1$, the difference $y_{i+k} - y_i$ is distinct for all $k = 1, 2, \ldots, n-1$ (Definition 2.3.9). Let α be a primitive element of $\mathbb{F}_p$ and define $f(\alpha^i) = y_i$. Clearly, f permutes the elements of $\mathbb{F}_p^*$. Let $d \in \mathbb{F}_p^*$, that is $d = \alpha^k$ for some k, then for $x = \alpha^i \in \mathbb{F}_p^*$, we have $f(xd) - f(x) = f(\alpha^{i+k}) - f(\alpha^i) = y_{i+k} - y_i$ also permutes of $\mathbb{F}_p^*$ since $y_1, y_2, \ldots, y_{p-1}$ is a circular Costas sequence. We can consider f as a polynomial over $\mathbb{F}_p$ of degree at most $p-1$ by the Lagrange Interpolation Formula by specifying a constant term. Hence, f is a permutation polynomial of $\mathbb{F}_p[x]$ if $f(0) = 0$.

Similarly, let f be a Costas polynomial with $f(0) = 0$. Fix a primitive element α of $\mathbb{F}_p$ and let $y_i = f(\alpha^i)$. The y_i are distinct, since f is a permutation polynomial, and the differences $y_{i+k} - y_i$ are distinct and non-zero for $k = 1, 2, \ldots, p-1$, since $\Delta_{f,d}(x) = f(xd) - f(x)$ is also a permutation polynomial for all $d \neq 1$. Thus, we have shown that a circular Costas sequence is equivalent to a Costas polynomial.

We follow [33] to show that a circular Costas sequence has the property that $y_{i+(p-1)/2} = -y_i$ for any i. In [33], the authors prove that a circular Costas sequence is the inverse permutation of a permutation $x_1, x_2, \ldots, x_n$ which gives the polygonal path of a $n \times (n+1)$ circular Tuscan n-array. Furthermore, they state that such a path satisfies $x_{-t} = (p-1)/2 + x_t$. Indeed, if $(p-1)/2 + x_t = j_t$, we have $y_{j_t} = -t$. However, $-t$ is the image of x_{-t}, and since f is a permutation, we have $x_{-t} = (p-1)/2 + x_t$ for all t.

Since $\alpha^{(p-1)/2} = -1$, we have $y_{i+(p-1)/2} = f(-\alpha^i) = -y_i = -f(\alpha^i)$. Thus $f(-x) = -f(x)$ for all x. If $f(x) = o(x) + e(x)$, where o and e denote the terms of odd and even degree, respectively, we have $f(-x) = o(-x) + e(-x) = -o(x) + e(x) = -o(x) - e(x) = -f(x)$. Subtracting both sides

gives $0 = 2e(x)$ or $e(x) = 0$ for all x, completing the proof. □

We give a condition for a polynomial f to be Costas over $\mathbb{F}_p$ which follows immediately from Proposition 2.2.3.

Lemma 7.1.5. *Let $f \in \mathbb{F}_q[x]$. Then f is Costas if and only if*

$$\sum_{x\in\mathbb{F}_q} (f(xd) - f(x))^n = \begin{cases} 0 & \text{if } 1 \le n \le q-2, \\ -1 & \text{if } n = q-1, \end{cases}$$

for all $d \in \mathbb{F}_q$, $d \neq 1$.

Suppose f is Costas over $\mathbb{F}_p$, where $f(x) = \sum_{m=1}^{s} c_m x^m$. Then

$$\begin{aligned} \sum_{x\in\mathbb{F}_p} (f(xd) - f(x))^n &= \sum_{x\in\mathbb{F}_p} \sum_{r=0}^{n} \binom{n}{r} (-1)^r f(xd)^r f(x)^{n-r} \\ &= \sum_{r=0}^{n} \binom{n}{r} (-1)^r \sum_{x\in\mathbb{F}_p} f(xd)^r f(x)^{n-r}. \end{aligned}$$

For $n < p$, the binomial coefficients never give zero divisors over $\mathbb{F}_p$. Consider the inner sum

$$\begin{aligned} \sum_{x\in\mathbb{F}_p} f(xd)^r f(x)^{n-r} &= \sum_{x\in\mathbb{F}_p} \left(\sum_{m=1}^{s} c_m (xd)^m \right)^r \left(\sum_{m=1}^{s} c_m x^m \right)^{n-r} \\ &= \sum_{x\in\mathbb{F}_p} \prod_{w=1}^{r} \left(\sum_{m=1}^{s} c_m x^m d^m \right) \prod_{u=r+1}^{n} \left(\sum_{m=1}^{s} c_m x^m \right). \end{aligned} \tag{7.1}$$

Let $\Psi = \{k(p-1), k \in \mathbb{N}\}$ and

$$\delta(m_1, m_2, \ldots m_n) = \begin{cases} -1 & \text{if } m_1 + m_2 + \cdots + m_n \in \Psi, \\ 0 & \text{otherwise.} \end{cases}$$

Equation (7.1) becomes

$$\sum_{x\in\mathbb{F}_p} \sum_{m_j} c_{m_1} c_{m_2} \cdots c_{m_r} \cdot c_{m_{r+1}} \cdots c_{m_n} d^{\sum_{i=1}^{r} m_i} x^{\sum_{i=1}^{n}}, \tag{7.2}$$

where the second sum is taken over all possible terms $0 \leq m_j \leq s$, $j = 0, 1, \ldots, n$. By interchanging sums, Equation (7.2) becomes

$$\sum_{m_j} \delta(m_1, m_2, \ldots, m_n) c_{m_1} c_{m_2} \cdots c_{m_n} d^{m_1+m_2+\cdots+m_r}. \tag{7.3}$$

We analyze Equation (7.3) for specific values of n which provide us with necessary information on the coefficients of f.

Case 1: $n = 1$

We illustrate the basic method with the $n = 1$ case. Let f be a Costas polynomial. By Proposition 2.2.3, $\sum_{x \in \mathbb{F}_p} \Delta_{f,d}(x) = 0$ for all $d \neq 1$. Similarly, $d = 1$ trivially gives $\sum_{x \in \mathbb{F}_p} \Delta_{f,1}(x) = 0$. Viewing $\sum_{x \in \mathbb{F}_p} \Delta_{f,d}(x)$ as a polynomial in d, $\Delta_{f,d}(x)$ has exactly exactly p zeroes. However,

$$\sum_{x \in \mathbb{F}_p} \Delta_{f,d}(x) = \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{s} c_i (xd)^i - \sum_{i=0}^{s} c_i x^i,$$

where $s \leq p - 1$ by assumption. Thus, the polynomial $\Delta_{f,d}$ is identically 0 and each coefficient of the terms in d vanishes.

Consider the coefficient of d^s: $0 = \sum_{x \in \mathbb{F}_p} x^s$. By Proposition 2.2.3, $s \neq p-1$. This is well-known: indeed by Theorem 2.2.4, s cannot be a divisor of $p - 1$.

Case 2: $n = 2$

The following lemma yields our main contribution.

Lemma 7.1.6. *Let c_{m_1} be a nonzero coefficient of a Costas polynomial $f(x)$ over $\mathbb{F}_p$, $p > 3$. Then $c_{p-1-m_1} = 0$.*

Proof. Let $n = 2$ in the evaluation of Equation (7.1). That is,

$$\sum_{x \in \mathbb{F}_p} (f(xd) - f(x))^2 = \sum_{x \in \mathbb{F}_p} \left(f(xd)^2 - 2f(xd)f(x) + f(x)^2 \right),$$

where the first and third term vanish by Proposition 2.2.3. For the second term, using the notation as in Equation (7.3), we have

$$\sum_{1\leq m_i\leq s} c_{m_1}c_{m_2}\delta(m_1,m_2)d^{m_1}=0.$$

We view this expression as a polynomial in d. Since this is true for all $d\in\mathbb{F}_p, d\neq 1$ and the degree of the polynomial in d is $m_1\leq s<p-1$, every coefficient in d is equal to 0. That is,

$$c_{m_1}c_{m_2}\delta(m_1,m_2)=0.$$

When $\delta(m_1,m_2)\neq 0$, that is when $m_1+m_2\in\Psi$, $c_{m_1}c_{m_2}=0$ implies either $c_{m_1}=0$ or $c_{m_2}=0$. Since $m_1,m_2\leq s\leq p-2$, we have that $\delta(m_1,m_2)\neq 0$ if and only if $m_1+m_2=p-1$, proving the result. □

The only monic permutation polynomial of $\mathbb{F}_3$ with $f(0)=0$ is $f(x)=x$, so the restriction on p in Lemma 7.1.6 does not introduce any genuine exceptions.

Case 3: $n>2$

For larger n, we require additional restrictions in order to use our method. For $n=3$ we have

$$\begin{aligned}0=\sum_{x\in\mathbb{F}_p}(f(xd)-f(x))^3 =& -3c_{m_1}c_{m_2}c_{m_3}\delta(m_1,m_2,m_3)d^{m_1}\\ &+3c_{m_1'}c_{m_2'}c_{m_3'}\delta(m_1',m_2',m_3')d^{m_1'+m_2'}.\end{aligned}$$

If $s>\frac{p-1}{2}$, then $m_1'+m_2'$ could be larger than $p-1$ and we would be unable to say that the coefficients of d are identically 0.

Suppose that $s<\frac{p-1}{2}$. For $s<m_1'+m_2'<2s$ we have $c_{m_1'}c_{m_2'}c_{m_3'}\delta(m_1',m_2',m_3')=0$. We consider $\delta(m_1',m_2',m_3')\neq 0$, then $m_3'=p-1-m_1'-m_2'$ and $c_{m_1'}c_{m_2'}c_{p-1-m_1'-m_2'}=0$. The meaningful cases are when m_1' and m_2' are both odd, however $p-1-m_1'-m_2'$ is even, and so $c_{m_3'}=0$.

Similarly, for any n if $s<\frac{p-1}{n-1}$ we find the relation $c_{m_1'}c_{m_2'}\cdots c_{m_{n-1}'}c_{m_{p-1-m_1'-m_2'-\cdots-m_{n-1}'}}=0$,

which is only meaningful if all of $m'_1, m'_2, \ldots, m'_{n-1}$ are odd. If n is even, then $p-1-m'_1-m'_2-\cdots-m'_{n-1}$ is odd and we have a non-trivial relationship on the coefficients of f. However, we lose the generality due to the restriction imposed on s.

We summarize our results as follows.

Proposition 7.1.7. *Let $f(x)=\sum_{i=0}^{p-1} c_i x^i$ be a Costas permutation, then*

1. *$f(-x)=-f(x)$ for all $x\in\mathbb{F}_p$; equivalently, f is an odd function; moreover $c_{2j}=0$ for all j;*
2. *if $c_i\neq 0$, then $c_{p-1-i}=0$.*

Thus, if $s=\deg(f)$, then f contains at most $s/4$ non-zero terms.

7.2 A new conjecture based on moved elements

Suppose f is a Costas permutation. Denote by T the set of *moved* elements of f, that is $T=\{x\in \mathbb{F}_p*\colon f(x)\neq x\}$ and let $m=|T|$. If $x\notin T$, then x is a *fixed* point of f. We view f both as a mapping $\mathbb{F}_p^*\to\mathbb{F}_p^*$ and also as a permutation polynomial of $\mathbb{F}_p$, since $f(0)=0$.

With this notation, we have the following result.

Theorem 7.2.1. [51] *Let f be a polynomial over $\mathbb{F}_q$ of degree at most $q-1$, also representing a map which moves $m>1$ elements of $\mathbb{F}_q$. Suppose further that $f(0)=0$. Then there is no k, $1\leq k\leq q-1-m$ such that the successive m coefficients $a_{k+1}, a_{k+2}, \ldots, a_{k+m}$ of the (induced) polynomial f are all equal to zero. Moreover, there are at least $(q-1)/m-1$ non-zero coefficients in f if m divides $q-1$ and at least $(q-1)/m$ non-zero coefficients of f otherwise.*

From Theorem 7.2.1, we have immediately, for any polynomial of degree $s\leq q-1$, that $m>q-1-s$, since $a_{s+1}=a_{s+2}=\cdots=a_{s+(q-1-s)}=0$.

The identity map $f(x)=x$ defines a Costas polynomial and any non-identity permutation moves at least 2 elements, since a non-identity permutation must contain at least one cycle. From now on, suppose $f(x)\neq x$ (and thus, $m>1$).

Conjecture 7.2.2. *Let $f\in\mathbb{F}_p[x]$ be a non-identity Costas polynomial which moved m elements. Then $m\geq(p-1)/2$.*

Proposition 7.2.3. *Conjecture 7.1.2 implies Conjecture 7.2.2.*

Proof. Suppose f is a Costas polynomial and denote by m_f the number of moved elements of f. Suppose that $m_f < (p-1)/2$. By Theorem 7.2.1, f has at least 2 non-zero elements, contradicting Conjecture 7.1.2. □

As evidence supporting Conjecture 7.2.2, suppose $x \in \mathbb{F}_p^*$ is a fixed point of f, that is $f(x) = x$. Then $\Delta_{f,-1}(x) = f(-x) - f(x) = -f(x) - f(x) = -2x$, since f is an odd function. Thus, if x is a fixed point of f, it is a moved point of $\Delta_{f,-1}$. Similarly, if x is a fixed point of $\Delta_{f,-1}$, then it is a moved element of f. Furthermore, $\Delta_{f,-1}(x) = -2f(x)$ and so the number of non-zero coefficients of f is equal to the number of non-zero coefficients of $\Delta_{f,-1}$.

Suppose further that $\Delta_{f,a}(x) = \Delta_{f,b}(x)$ for non-unity $a, b \in \mathbb{F}_p$. Then $f(ax) = f(bx)$, showing that $x = 0$ or $a = b$, since f is a permutation. Thus, for $x \neq 0$, the set $S_x = \{\Delta_{f,a}(x) \colon a = 0, 2, \ldots, p-1\}$ has size $p-1$. Thus, given $x \neq 0$, it is a fixed point of $\Delta_{f,a}(x)$ for exactly one value of a.

Coefficients of the inverse polynomial

Suppose $f(x) = \sum_{i=0}^{q-1} a_i x^i$ is a permutation polynomial and let $f^{-1}(x) = \sum_{i=0}^{q-2} b_i x^i$ be its (compositional) inverse polynomial. Since $x^{q-1} = 1$ for all non-zero x, we consider the inverse polynomial as having degree strictly less than $q-1$. We obtain the following consequences, due to [50].

Proposition 7.2.4. [50] *Suppose $n = \deg(f)$, then $\deg(f^{-1}) \leq q - 1 - \frac{q-2}{n}$.*

Proposition 7.2.5. [50] *Let f be a permutation polynomial and let $f^{-1}(x) = \sum_{i=0}^{q-2} b_i x^i$ be its compositional inverse. The coefficient b_j, for $j = 0, 1, \ldots, q-2$ satisfies the formula*

$$b_j = \sum \frac{(q-1-j)!}{t_0! t_1! \cdots t_{q-2}!} a_0^{t_0} a_1^{t_1} \cdots a_{q-2}^{t_{q-2}},$$

under the convention $0^0 = 1$ and where the sum runs over the non-negative integers such that $\sum_{i=0}^{q-2} t_i = q-1-j$ and $\sum_{i=1}^{q-2} i t_i \equiv q-2 \pmod{q-1}$.

Proposition 7.2.5 is most useful when there are few non-zero coefficients of the polynomial f. For example, suppose $f(x) = x^s$ with $\gcd(s, q-1) = 1$. Then contributions to b_j come only from the terms $t_s \neq 0$ and $t_i = 0$ for $i \neq s$. That is, $t_s = q - 1 - j$ and $st_s \equiv q - 2 \pmod{q-1}$. Since $\gcd(s, q-1) = 1$, s is invertible $\pmod{q-1}$ and thus $t_s = \frac{q-2}{s} \pmod{q-1}$. Thus, j is uniquely determined and so $f^{-1}(x)$ is also a monomial. Indeed, this is well-known since $\gcd(s, q-1) = 1$ implies that $1 = as + b(q-1)$, for some a, b and thus $f^{-1}(x) = x^a$.

If f is Costas, then $\Delta_{f,d}$ are permutation polynomials for all $d \neq 1$. Since $\Delta_{f,d}$ has at most the same number of non-zero coefficients as f, concurrently studying bounds on the number of moved elements and the resulting formulas for the inverse polynomials of the $\Delta_{f,d}$ is a promising avenue for completing the proof.

Chapter 8

First steps on future directions

In this chapter, we discuss some future research on related topics for which we already have some preliminary steps. In Section 8.1, we give a class of linearized permutation polynomials over finite fields. Our proof relies on properties of circulant matrices. A partial solution to a problem of Kyureghyan on linearized permutation trinomials is also given in Section 8.1. In Section 8.2, we conjecture the ambiguity and deficiency of a class of reversed Dickson permutation polynomials. A proof of our conjecture is given supposing the truth of another conjecture on the 2-divisibility of certain binomial coefficients. Finally, in Section 8.3 we give a solution to a particular type of tournament schedule (alternatively, an imperfect design) which is based on ambiguity and deficiency of functions over finite fields.

8.1 A class of linearized permutation polynomials

This section was developed in private correspondence with Dr. John Sheekey. At the *2012 RICAM Workshop on Finite Fields: Character Sums and Polynomials* (Strobl, Austria), Kyureghyan posed the following problem.

Problem. Let $L(x) = x^{2^r} + x^{2^s} + x^{2^t} \in \mathbb{F}_{2^e}[x]$, where $r > s > t$, be a linearized polynomial. Give necessary and sufficient conditions for L to be a permutation.

In this section, we give an infinite class of linearized polynomials over finite fields which de-

fine permutation polynomials. Let $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$ be a linearized polynomial over $\mathbb{F}_{q^e}$ with coefficients in $\mathbb{F}_q$. Theorem 3.6.3 states that L is a permutation polynomial if the matrix

$$\begin{bmatrix} a_0 & a_{e-1}^q & \cdots & a_1^{q^{e-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ a_{e-1} & a_{e-2}^q & \cdots & a_0^{q^{e-1}} \end{bmatrix},$$

also given in Equation (3.7), is invertible. If the coefficients $a_0, a_1, \ldots, a_{e-1}$ are elements of $\mathbb{F}_q$, then this matrix is *circulant* (see [43]).

Let $A = (a_{ij})$ be an $e \times e$ circulant matrix with first row $(x_0, x_1, \ldots, x_{e-1})$, that is $a_{ij} = x_{i-j \pmod e}$. Denote by S_e the symmetric group on e letters. The determinant of A is given by

$$\det(A) = \sum_{\sigma \in S_e} \prod_{0 \le i \le e-1} a_{i\sigma(i)} = \sum_{\sigma \in S_e} \prod_{0 \le i \le e-1} x_{i-\sigma(i)}.$$

Furthermore, let $\pi = (1\ 2 \cdots e-1)$ and let $C_e = \langle \pi \rangle$. We give two short lemmas which allow us calculate the determinant of a circulant matrix A.

Lemma 8.1.1. *Let* $m(\sigma) = \prod_{0 \le i \le e-1} x_{i-\sigma(i)}$. *Then* $m(\sigma) = m(\rho^{-1}\sigma\rho)$ *for all* $\rho \in C_e$.

Proof. Clearly $\pi^k(i) = i + k \pmod e$, and

$$\begin{aligned} m(\sigma) &= \prod_{0 \le i \le e-1} x_{i-\sigma(i)} = \prod_{0 \le i \le e-1} x_{(i+k)-\sigma(i+k)} \\ &= \prod_{0 \le i \le e-1} x_{i-(\sigma(i+k)-k)} = \prod_{0 \le i \le e-1} x_{i-\pi^{-k}\sigma\pi^k(i)} \\ &= m(\pi^{-k}\sigma\pi^k), \end{aligned}$$

as claimed. □

Lemma 8.1.2. *Let* S *be a set of representatives for the orbits of* S_e *under the group action of*

conjugation by C_e. For any $\sigma \in S$, denote by $O(\sigma)$ the orbit of σ. Then

$$\det(A) = \sum_{\sigma \in S} |O(\sigma)| m(\sigma).$$

Furthermore, $|O(\sigma)|$ divides e, and $|O(\sigma)| = 1$ if and only if $\sigma \in C_e$.

We now give the determinant of a $e \times e$ circulant matrix when the characteristic of the field divides e.

Proposition 8.1.3. *Let $e = p^m$, and let A be an $e \times e$ circulant matrix over some field $\mathbb{F}$ of characteristic p. In $\mathbb{F}[x_0, x_1, \cdots, x_{e-1}]$, we have* $\det(A) = (x_0 + x_1 + \ldots x_{e-1})^e$.

Proof. By Lemma 8.1.2, $|O(\sigma)| \equiv 0 \pmod{p}$ unless $\sigma \in C_e$. It is clear that

$$m(\pi^{-k}) = x_k^e,$$

and hence

$$\det(A) = x_0^e + x_1^e + \cdots + x_{e-1}^e. \qquad \square$$

We use Proposition 8.1.3 to construct an infinite class of linearized permutation polynomials, giving a partial solution to Kyureghyan's question.

Corollary 8.1.4. *Let p be a prime, let q be a power of p and let $e = p^\ell$, for some $\ell > 0$. Let $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i} \in \mathbb{F}_{q^e}[x]$ such that $a_i \in \mathbb{F}_q$ for all $0 \leq i \leq e-1$. Then L is a permutation polynomial of $\mathbb{F}_{q^e}$ if and only if $a_0 + a_1 + \cdots + a_{e-1} \neq 0$.*

Corollary 8.1.5. *Let q be a power of a prime p and let $e = p^\ell$ for some positive integer $\ell > 3$. Then $L(x) = x^{q^r} + x^{q^s} - x^{q^t} \in \mathbb{F}_{q^e}[x]$ is a permutation polynomial for all $0 \leq r < s < t \leq e-1$.*

8.2 Reversed Dickson polynomials

This section gives the opening steps to calculate the ambiguity and deficiency of reversed Dickson permutation polynomials over finite fields. The ambiguity and deficiency of two reversed Dickson

polynomials appears in the proceedings [54].

Dickson and reversed Dickson polynomials are introduced in Section 3.2. By Definition 3.2.1, Dickson polynomials (of the first kind) are given by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}.$$

The reversed Dickson polynomials are obtained by interchanging the roles of the variable x and the parameter a. Theorem 3.2.3 gives necessary and sufficient conditions for a Dickson polynomial to be a permutation polynomial of $\mathbb{F}_q$. The permutation structure of reversed Dicksons is lesser known. Reversed Dickson polynomials which are known to be permutation polynomials of $\mathbb{F}_{2^e}$ are given in Table 3.1. An an analogous table for reversed Dickson permutation polynomials defined over odd characteristics appears in Table 3.2.

Due to their complicated expression, in order to calculate the difference maps of Dickson polynomials, we examine when their coefficients are non-zero. For this, we require the prime divisibility of binomial coefficients.

Definition 8.2.1. *Let $n \geq k \geq 0$ be integers and let p be a prime. Denote by $E_p\binom{n}{k}$ the largest exponent e such that p^e divides $\binom{n}{k}$ and p^{e+1} does not divide $\binom{n}{k}$.*

Lemma 8.2.2. [30] *Define $E_p\binom{n}{k}$ as in Definition 8.2.1 with*

$$n = \sum_{i=0}^{e} a_i p^i,\ k = \sum_{i=0}^{e} b_i p^i,\ n-k = \sum_{i=0}^{e} c_i p^i.$$

Then, the following hold

$$\begin{aligned} E_p\binom{n}{k} &= \frac{\sum_{i=0}^{e} b_i + c_i - a_i}{p-1}, \\ &= \#\ \textit{of borrows in the subtraction of } n-k \textit{ in base } p, \\ &= \#\ \textit{of carries in the addition } (n-k)+k \textit{ base } p. \end{aligned}$$

In Proposition 8.2.5, we state the ambiguity and deficiency of the reversed Dickson polynomials

over $\mathbb{F}_{2^e}$ that appear in [54]. The coefficients of the reversed Dickson polynomial are given first in Lemma 8.2.3. We omit the proofs, since they will be superceded by our general method.

Lemma 8.2.3.

1. *Let $n = 2^k + 1$ and $j \leq n$; then*

$$\begin{cases} 2 \nmid \frac{n}{n-j}\binom{n-j}{j} & j = 2^i \text{ for some } i, \\ 2 \mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise.} \end{cases}$$

2. *Let $n = 2^e + 2^2 + 1$ and $8 \leq j \leq n$. Then*

$$\begin{cases} 2 \nmid \frac{n}{n-j}\binom{n-j}{j} & j = 2^i \text{ or } 2^i + 1 \text{ or } 2^i + 2 \text{ for some } i, \\ 2 \mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise.} \end{cases}$$

Proposition 8.2.4. *Let $f(x) = D_n(1, x) \in \mathbb{F}_{2^e}[x]$, where $n = 2^k + 1$ for some non-negative integer k. Then $D_n(1, x)$ is a linearized polynomial and its ambiguity and deficiency are given by Proposition 5.4.7.*

Proposition 8.2.5. *The ambiguity and deficiency of the reversed Dickson polynomial $f(x) = D_n(1, x) \in \mathbb{F}_{2^e}[x]$, where $n = 2^e + 2^2 + 1$ and e is even, are respectively given by*

$$A(f) = 2^{e-1}(2^{e-1} + 1)^2,$$
$$D(f) = 2^e(2^e - 1) - (2^{e-1})2^{e-2} - (2^e - 4) - 1.$$

We now present a conjecture on the 2-divisibility of the coefficients of $D_n(1, x)$ when $n = 2^e + 2^{2t} + 1$ and e is even. This conjecture is a generalization of Case 2. of Lemma 8.2.3 and has been verified with a SAGE [63] program for small values of e and t.

Conjecture 8.2.6. *Let e be even and let $n = 2^e + 2^{2t} + 1$ for some integer $t \neq e, e/2$. The reversed*

Dickson polynomial $D_n(1,x)$ is given by the following expression

$$\begin{aligned} D_n(1,x) &= \sum_{j=0}^{2^{e-1}+2^{2t-1}} \frac{n}{n-j}\binom{n-j}{j}(-x)^j \\ &= 1 + x^2 + \cdots + x^{2^{2t-1}} + \sum_{j=0}^{e-1}\sum_{s=0}^{2t-1} x^{2^j+2^s}, \\ &= 1 + x^2 + \cdots + x^{2^{2t-1}} + \left(1 + \sum_{s=0}^{2t-1} x^{2^s}\right)\mathrm{Tr}(x). \end{aligned}$$

Conjecture 8.2.7. *Let e be even and let $n = 2^e + 2^{2t} + 1$, for some integer $t \neq e, e/2$. The ambiguity and deficiency of the reversed Dickson polynomial $f(x) = D_n(1,x) \in \mathbb{F}_{2^e}[x]$, are respectively given by*

$$\begin{aligned} A(f) &= 2^{e-1}(2^{e-1}+1)^2, \\ D(f) &= 2^e(2^e-1) - (2^{e-1})2^{e-2} - (2^e-4) - 1. \end{aligned}$$

Proof. To prove this conjecture, we assume the truth of Conjecture 8.2.6. Thus, proving Conjecture 8.2.6 also proves this conjecture.

Assuming Conjecture 8.2.6, we have the following expression for the reversed Dickson polynomial $D_n(1,x) \in \mathbb{F}_{2^e}[x]$, where $n = 2^e + 2^{2t} + 1$ for some integer $t \neq e, e/2$

$$D_n(1,x) = 1 + x^2 + \cdots + x^{2^{2t-1}} + \left(1 + \sum_{s=0}^{2t-1} x^{2^s}\right)\mathrm{Tr}(x),$$

where $\mathrm{Tr}(x)$ is the trace function from $\mathbb{F}_{2^e}$ to $\mathbb{F}_2$ Thus, we have

$$\begin{aligned} \Delta_{f,a}(x) &= 1 + (x+a)^2 + \cdots + (x+a)^{2^{2t-1}} + \left(1 + \sum_{s=0}^{2t-1}(x+a)^{2^s}\right)\mathrm{Tr}(x+a) \\ &\quad + 1 + x^2 + \cdots + x^{2^{2t-1}} + \left(1 + \sum_{s=0}^{2t-1} x^{2^s}\right)\mathrm{Tr}(x) \\ &= \sum_{s=1}^{2t-1} a^{2^s} + \left(1 + \sum_{s=0}^{2t-1} a^{2^s}\right)\mathrm{Tr}(a) + \left(\sum_{s=0}^{2t-1} x^{2^s}\right)\mathrm{Tr}(a) + \left(\sum_{s=0}^{2t-1} a^{2^s}\right)\mathrm{Tr}(x). \end{aligned}$$

Clearly, $(a,b) = (1,1)$ satisfies $\Delta_{f,a}(x) = b$ for every $x \in \mathbb{F}_{2^e}$.

If $\mathrm{Tr}(a) = 0$, then there are $2^{e-1} - 2$ pairs (a, b) with $a \neq 0, 1$ and

$$\Delta_{f,a}(x) = b = \sum_{s=1}^{2t-1} a^{2^s} + \left(\sum_{s=0}^{2t-1} a^{2^s} \right) \mathrm{Tr}(x).$$

Let $\mathrm{Tr}(x) = t_0$, then $\Delta_{f,a}(x) = b$ has exactly 2^{e-1} solutions for each $t_0 \in \mathbb{F}_2$. Therefore, the number of distinct pairs (a, b) for which $\Delta_{f,a}(x) = b$ has exactly 2^{e-1} solutions is $2\left(2^{e-1} - 2\right) = (2^e - 4)$.

Now suppose that $\mathrm{Tr}(a) = 1$ and so

$$\begin{aligned} b &= \sum_{s=1}^{2t-1} a^{2^s} + \left(1 + \sum_{s=0}^{2t-1} a^{2^s} \right) + \left(\sum_{s=0}^{2t-1} x^{2^s} \right) + \left(\sum_{s=0}^{2t-1} a^{2^s} \right) \mathrm{Tr}(x) \\ &= 1 + a + \sum_{s=0}^{2t-1} x^{2^s} + \left(\sum_{s=0}^{2t-1} a^{2^s} \right) \mathrm{Tr}(x). \end{aligned} \tag{8.1}$$

Since $2t - 1$ is odd and e is even, a simple linear algebra argument combined with Corollary 3.6.4 gives that the cardinality of the value set of $L(x) = \sum_{s=0}^{2t-1} x^{2^s}$ is 2^{e-1} and that each value of L is repeated twice. Moreover, if $\mathrm{Tr}(x_1) = \mathrm{Tr}(x_2)$, then $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$ implies that $L(x_1) = L(x_2)$. If $\mathrm{Tr}(x_1) \neq \mathrm{Tr}(x_2)$, then $\Delta_{f,a}(x_1) = \Delta_{f,a}(x_2)$ implies $L(x_1) = L(x_2 + a)$. Thus, for each a with $\mathrm{Tr}(a) = 1$, there are 2^{e-2} values of b for which $\Delta_{f,a}(x) = b$ has 4 solutions.

All of the pairs listed are the only pairs (a, b) which have solutions to $\Delta_{f,a}(x) = b$. Overall the ambiguity of f is

$$\left(2^{e-1}\right) 2^{e-2} \binom{4}{2} + (2^e - 4) \binom{2^{e-1}}{2} + \binom{2^e}{2} = 2^{e-1} \left(2^{e-1} + 1\right)^2.$$

Since there are $2^e(2^e - 1)$ possible pairs (a, b), we find

$$D(f) = 2^e(2^e - 1) - (2^{e-1})2^{e-2} - (2^e - 4) - 1. \qquad \square$$

A subset of the proof of Conjecture 8.2.6 which illustrates the general method follows. The proof on the 2-divisibility of binomial coefficients, given by Lemma 8.2.2.

Lemma 8.2.8. *Let $n = 2^e + 2^d + 1$. Suppose that $j = 2^r + 2^d$, where $e - 1 > r > d > 0$. Then,*

$$2 \mid \frac{n}{n-j}\binom{n-j}{j}.$$

Proof. Let $n = 2^e + 2^d + 1$ and let $j = 2^r + 2^d + 1$ for some $r > d$. By Lemma 8.2.2, we must compute the 2-ary expansion of $n - j$ and $n - 2j$ to determine the 2-divisbility of $\binom{n-j}{j}$.

Let $j = \sum_{i=0}^{e} j_i 2^i$. We use a table of the following form to find the 2-ary expansion of $n - j$. We input the specific form of j into the table.

	e				r		d				0
n	1	0		$\cdots$	0	$\cdots$	1	0	$\cdots$	0	1
j	0	0		$\cdots$	1	$\cdots$	1	0	$\cdots$	0	0
$n-j$	0	$_{e-1}$complement$_{r+1}$			1	$\cdots$	0	0	$\cdots$	0	1

By "complement" we mean the complement of all of each j_i in the specified range; the complement of j_i is $(1 - j_i)$. The 2-ary expansion of $n - j$ is given by $1 + \sum_{i=r}^{e-1} 2^i$. Hence, $n - j$ has $e - r - 2$ non-zero 2-ary coefficients.

The 2-ary expansion of $2j$ is the 2-ary expansion of j shifted to the left by one entry.

	e			r			d				0
n	1	0	$\cdots$		$\cdots$	0	1	0	$\cdots$	0	1
$2j$	0	0	$\cdots$	1	$\cdots$	1	0	0	$\cdots$	0	0
$n-2j$	0	$_{e-2}$complement$_{d+1}$				1	1	0	$\cdots$	0	1

Thus, the 2-ary expansion of $n - 2j$ is $1 + \sum_{i=d}^{e-2} 2^i - 2^r$ and there are $e - d - 4$ non-zero coefficients in the 2-ary expansion of $n - 2j$.

By Lemma 8.2.2, the 2-divisibility of $\binom{n-j}{j}$ is given by

$$E_2\binom{n}{k} = 2 + (e - d - 4) - (e - r - 2) = (r - d) > 0,$$

and the 2-divisibility of $\frac{n}{n-j}$is 0 since both n and $n-j$ are odd. □

The completion of the proof of Conjecture 8.2.6 requires considering all possible 2-ary expansions of j (and hence $n-j$ and $n-2j$). There are some patterns that arise in analyzing these expansions. For instance, the most important 2-ary coefficients of $j = \sum_{i=0}^{e-2} j_i 2^i$ are j_0, j_b, j_{d-1} and j_r, where $0 < b < d-1 < r$, and j_b, j_r are the first non-zero 2-ary expansions in their appropriate ranges (if they exist). Thus, there are approximately 16 general cases to analyze.

This method extends to other values of n. However, the number of general cases to consider grows with the number of gaps between non-zero coefficients of n. Thus, those n with high 2-weight or alternatively those n with low 2-weight are likely feasible to study.

8.3 A tournament scheduler

In this section, we formalize a tournament scheduling problem presented by Stevens at [1]. A solution to the problem, also due to [1], is given in terms of ambiguity and deficiency. We conclude with some remarks on possible areas of expanding ambiguities and deficiencies of functions to construct further imperfect designs.

Let X be a set of n^2 people and let $\mathcal{B} = \{B_{ij} : 0 \leq i, j < n\}$ be a set of n^2 matches (on n people) indexed by Room i and Round j. The problem is to create an adequate tournament schedule, where each person meets each other person a prescribed number of times. In particular, we want to find solutions to the schedule which minimizes both the number of missed pairs and the number of repeated pairs.

For each pair of players $x, y \in X$, define $\lambda_{xy} = |\{B \in \mathcal{B} : x, y \in B\}|$, that is λ_{xy} is the number of matches in which x and y meet. Furthermore, let $n_i = |\{\{x, y\}, x \neq y \subset X : \lambda_{xy} = i\}|$, that is n_i is the number of pairs of people that meet exactly i times. Note that $\lambda_{xy} = \lambda_{yx}$ so that each pair is counted twice.

We calculate some simple bounds to help analyze the problem. Consider the number of (ordered) (x, y) pairs of X.

Proposition 8.3.1. *Let X, $\mathcal{B}$ and n_i be defined as above. Then,*

1. $\sum_{i=0}^{n} n_i = \binom{n^2}{2}$;
2. $\sum_{i=0}^{n} i n_i = n^2 \binom{n}{2}$.

Proof. We prove the cases in order.

1. The sum $\sum_{i=0}^{n} n_i$ gives the number of pairs of people that meet any number of times, that is $\sum_{i=0}^{n} n_i = \binom{n^2}{2}$.

2. The sum $\sum_{i=0}^{n} i n_i$ gives the total number of meetings. Since there are n^2 total matches, there are $n^2\binom{n}{2}$ meetings. □

In any construction, we need to state our constraints and identify the set of people, and the matches (also identifying the room and the round). Two solutions based on finite geometries appear in [1]. The first construction is a solution with no constraints on the scheduler, where the second solution requires that no pair of people meet more than twice. In this work, we present only the solution focusing on ambiguity and deficiency.

Assumption: The λ_{xy} are equal and there is an automorphism of the system.

In this construction, each pair of people meet exactly the same number of times and there is an automorphism of the $n \times n$ system which transitively maps each person's schedule. Consider a single schedule as an ordered n-tuple $(x_0, x_1, \ldots, x_{n-1})$, where $1 \leq x_i \leq n-1$ denotes the room of person x in round i. Two people x and y meet in round j when $x_j = y_j$ and a (transitive) automorphism of the system can be thought as a bijection on this class of n-tuples with entries in $\mathbb{Z}_n$. The entire system can then be determined from a single person's tournament schedule.

Suppose that x and y have an interaction at round $j = i + a$, then $x_j = y_j$ if and only if $x_{j-a} + b = x_j$ for some a and b. Re-arranging gives $x_{j-a} - x_j = -b$. Letting $x_j = f(j)$ for some function f, we get $f(j + (-a)) - f(j) = -b$.

Let G_1 and G_2 be finite groups (of size $n + 1$) and let $f \colon G_1 \to G_2$ be a bijection. Define $\Delta_{f,a}(x) = f(x + a) - f(x)$ as usual. For any $a \in G_1^*$ and $b \in G_2$, let $\lambda_{a,b}(f) = |\Delta_{f,a}^{-1}(b)|$ and let

$\alpha_i(f) = |\{(a,b) \in G_1^* \times G_2 \colon \lambda_{a,b}(f) = i\}|$. An interaction between two players is given by a solution to $\Delta_{f,-a}(j) = -b$. As before, the deficiency of f, $D(f) = \alpha_0(f)$, is the number of missed interactions and the ambiguity of f, $A(f) = \sum_{i=0}^{n} \alpha_i(f)\binom{i}{2}$, is the total number of repeated encounters.

In this language, the goal of the tournament is to pick functions with minimal ambiguity and deficiency. The most natural functions to pick are permutations of $\mathbb{Z}_{n+1}$, however since G_1 and G_2 are finite groups, their elements have some numbering $0, 1, 2, \ldots, n$, so (with some care taken) any finite groups should suffice.

Permutations with optimum or near-optimum ambiguity and deficiency over $\mathbb{Z}_n$ are given in Section 5.4.1. The requirement that f be a permutation ensures only that each player encounters every room. Of course, a tournament scheduler may not care in which room the participants play (it stands to reason that omitting a room is less significant than missing a player interaction). Moreover, the requirement that $G_1 = G_2$, or even that $|G_1| = |G_2|$ is a function of the precise setup of this type of tournament. Further tournament types include those with more rooms than rounds (or vice versa), and tournaments where participants may sit out a certain number of rounds. The key requirement in order to analyze these cases by ambiguities and deficiencies is the existence of a (transitive) automorphism of the system.

This chapter outlines some first steps and partial solutions to problems related to work in this thesis. This is by no means an exhaustive list of problems related to ambiguity and deficiency. More directions for future research are discussed in the concluding remarks in Part III.

Part III

Concluding remarks

Conclusions

In this thesis, we study properties of the difference maps of functions between finite groups. We introduce and study the measures of the *ambiguity* and *deficiency* of a function between finite groups, which are collective measures of the injectivity and surjectivity, respectively, of the difference maps of the function.

We introduce some necessary background in Part I of the thesis. In Section 3.7, we also introduce the subfield value set of a function. The subfield value set of a functions is the set of images of the function which lay in a subfield of the extension field. We begin the discussion of ambiguity and deficiency in Chapter 5. In particular, we give lower bounds on the ambiguity and deficiency of permutations, and relate functions attaining these bounds to commonly considered notions of non-linearity. We further show that ambiguities and deficiencies are invariant within the extended affine and Carlet-Charpin-Zinoviev equivalence classes of functions. In Chapter 6, we give a formula for the ambiguity and deficiency of Dembowski-Ostrom (DO) polynomials in terms of a specific form of matrix. We then compute the ambiguities and deficiencies for known classes of DO permutation polynomials. In Chapter 7, we give a partial solution to a conjecture of Golomb-Moreno on a multiplicative analogue of planar functions. We also present a new conjecture, which is implied by the Golomb-Moreno conjecture, and indicate a possible avenue for the proof. We conclude with some first steps on future research in Chapter 8. These directions include determining classes of linearized permutation polynomials, computing the ambiguity and deficiency of reversed Dickson polynomials and translating ambiguity and deficiency to other forms of combinatorial structures.

Future areas for research on difference maps and, in particular, on computing the ambiguity and deficiency of functions may involve three main paths: changing the functions, changing the groups and changing the setting. For the first path, some first steps on the ambiguity and deficiency of reversed Dickson polynomials appear in Section 8.2. Any function over a finite field whose algebraic structure is understood is a candidate for further study. In this work, we focus on permutation functions. However, when a function is not a permutation, the (possibly unknown) value set of a function may complicate calculating its ambiguity and deficiency. Additionally, *zero-difference*

balanced functions are functions f for which the equation $\Delta_{f,a}(x) = 0$ has the same number of solutions for all a. Zero-difference balanced functions have applications to partitioned difference families, frequency hopping sequences, difference systems of sets and so on [20]. Since the difference maps of permutations never have 0 as an image, we have effectively ignored the presence of the 0 in the co-domain of $\Delta_{f,a}$ for permutations. Zero-difference balanced functions are the precise opposite and are a promising area for continued research.

Dembowski-Ostrom polynomials can also be easily generalized. If $f \in \mathbb{F}_{q^e}[x]$ is a polynomial such that the exponents of all of its non-zero terms have q-weight at most k, then $\Delta_{f,a}(x)$ is a polynomial with the exponents of all of its non-zero terms having q-weight at most $k-1$. This is a natural extension of one direction of Theorem 3.5.3. However, the DO polynomials are special since their difference maps are linearized (plus a constant). With $k = 3$, a polynomial f described above will have difference maps being the sum of a DO polynomial, a linearized polynomial and a constant. Studying the sums of images of multiple polynomials is naturally a hard problem. A first step in this direction would be to precisely determine the value set of a DO polynomial. Finally, DO polynomials arise in *Hidden-Field-Equations* for multi-variate public-key cryptography, see [49, Chapter 16.3]. In Chapter 6, we give some previously unknown properties of known DO permutations. Understanding the desired properties for these polynomials in the multi-variate public-key cryptography setting may yield new fruitful research.

This thesis focuses mainly on maps from a group to itself. Another natural question to ask is what happens when the map is from one group to a new group. Some initial steps are considered in Section 5.4.3, viewing linearized polynomials as mappings between either the additive or multiplicative groups of finite fields. A similar scenario occurs in Chapter 7, where a map from the multiplicative group to the additive group of a prime field is extended to define a polynomial and its difference maps over the entire field. Studying functions from large groups to small groups, or vice versa, may have applications to other structures, such as hash functions. In particular, if G_1 is large and G_2 is a (relatively) small subgroup of G_1, a hash function may be defined from G_1 to G_2. Differential attacks can also be defined on hash functions [2], so strong hash functions should

have low ambiguities. Finally, planar functions, defined in Section 3.3, have the property that both the difference maps $\Delta_{f,a} = f(x+a) - f(x)$ and $\nabla_{f,a} = -f(x) + f(x+a)$ are permutations. These difference maps coincide when the group is Abelian, so a future direction is to look at the ambiguity and deficiency of functions defined over non-Abelian groups. An optimally non-linear function is a *bent* function. It is well-known that a function (defined over an Abelian group) is bent if and only if it is perfect non-linear [57]. The measure of non-linearity given in Section 2.1.4 requires the evaluation of characters over finite Abelian groups. Corresponding notions of non-linearity and bent-ness for functions over non-Abelian groups are given in [57]. The author uses linear representations as a substitute for characters in the non-Abelian cases. Using these definitions of bent-ness, the duality between bent-ness and perfect non-linearity is also shown in [57]. Thus, our connections to non-linearity given in Section 5.3 will likely also translate to the non-Abelian case. Constructing functions with low-ambiguity and deficiency in the non-Abelian case is another interesting area of further study.

Changing the setting is, of course, wide-open. In Section 2.3, we give a solution, due to [1], to a tournament scheduling problem using the language of ambiguity and deficiency. Studying ambiguity and deficiency of functions also involves counting pairs of elements of $G_1^* \times G_2$ coming from functions whose difference maps have specific properties. Functions for which these pairs have balanced properties may translate to similar combinatorial objects. Furthermore, the conjecture which forms the basis of Chapter 7 has roots in the constructions of certain forms of circular Costas sequences. Studying the properties of the sequences given by the images of difference maps is another interesting area of further study.

Bibliography

[1] T. Alderson, K. Meagher, and B. Stevens. Finite field constructions of an imperfect design. Presented at the 2011 Canadian Discrete and Algorithmic Mathematics minisymposium *Finite Fields in Combinatorics*, 2011.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4:3–72, 1991.

[3] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe. Permutations amongst the Dembowski-Ostrom polynomials. In *Proc. 5th Int'l Conf. Finite Fields Appl.*, pages 37–42. Springer, 1999.

[4] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of $x \mapsto x^{2^t-1}$. *IEEE Trans. Inf. Theory*, 57:8127–8137, 2011.

[5] K. Brincat and A. Meijer. On the SAFER cryptosystem. In *Cryptography and Coding*, volume 1355 of *Lecture Notes Comput. Sci.*, pages 59–68, 1997.

[6] K. Browning, J. Dillon, M. McQuistan, and A. Wolfe. An APN permutation in dimension six. In *Proc. 9th Int'l Conf. on Finite Fields Appl.*, volume 518 of *Contemporary Math.*, pages 33–42. Amer. Math. Soc., 2010.

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

[8] C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Boolean functions for cryptography and error-correcting codes, pages 257–397. Yves Crama and Peter L. Hammer (eds.), Cambridge University Press, 2010.

[9] C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Vectorial Boolean functions for cryptography, pages 398–469. Yves Crama and Peter L. Hammer (eds.), Cambridge University Press, 2010.

[10] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15:125–156, 1998.

[11] C. Carlet and C. Ding. Highly nonlinear mappings. *J. Complexity*, 20:205–244, 2004.

[12] C. Carlet and C. Ding. Nonlinearities of S-boxes. *Finite Fields Appl.*, 13:121–135, 2007.

[13] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus. Polynomials over finite fields with minimal value sets. *Mathematika*, 8:121–130, 1961.

[14] P. Charpin and G. Kyureghyan. On a class of permutation polynomials over $\mathbb{F}_{2^n}$. In *Proc. 5th Int'l Conf. Sequences and Their Applications—SETA '08*, volume 5203 of *Lecture Notes Comput. Sci*, pages 368–376, 2008.

[15] W. S. Chou, J. Gomez-Calderon, and G. L. Mullen. Value sets of Dickson polynomials over finite fields. *J. Number Theory*, 30:334–344, 1988.

[16] W.-S. Chou, J. Gomez-Calderon, G. L. Mullen, D. Panario, and D. Thomson. Subfield value sets of polynomials over finite fields. *Funct. Approx. Comment. Math.*, In press, 21 pages, 2012.

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

[18] J. Daemen and V. Rijmen. *The design of Rijndael: AES — the Advanced Encryption Standard.* Springer-Verlag, 2002.

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

[20] C. Ding. Zero-difference balanced functions with applications. *J. Statistical Theory and Practice*, 6:3–19, 2012.

[21] H. Dobbertin. Almost perfect nonlinear power functions over GF(2^n): the Niho case. *Inform. and Comput.*, 151:57–72, 1999.

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

[23] H. Dobbertin. Almost perfect nonlinear power functions over GF(2^n): a new case for n divisible by 5. In *Proc. 5th Int'l Conf. Finite Fields Appl.*, pages 113–121, Augsburg, Germany, 2000. Springer.

[24] K. Drakakis, R. Gow, and G. McGuire. APN permutations on $\mathbb{Z}_n$ and Costas arrays. *Discrete Appl. Math.*, 157:3320–3326, 2009.

[25] K. Drakakis, V. Requena, and G. McGuire. On the nonlinearity of exponential Welch Costas functions. *IEEE Trans. Inform. Theory*, 56:1230–1238, 2010.

[26] H. Feistel. Block cipher cryptographic system, 1971. US Patent 3,798,359 (IBM).

[27] FIPS PUB 197. Advanced Encryption Standard (AES). Technical report, National Institute of Standards and Technology, U.S. Department of Commerce, 2001. available online, `http://csrc.nist.gov/publications/fips197/fips-197.pdf`.

[28] FIPS PUB 46-3. Data Encryption Standard. Technical report, National Institute of Standards and Technology, U.S. Department of Commerce, 1999. available online `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[29] D. Gluck. A note on permutation polynomials and finite geometries. *Discrete Math.*, 80:97–100, 1990.

[30] P. Goetgheluck. Computing binomial coefficients. *Amer. Math Monthly*, 94:360–365, 1987.

[31] S. Golomb and H. Taylor. Construction and properties of Costas arrays. *Proc. IEEE*, 72:1143–1163, 1984.

[32] S. W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, Cambridge, 2005.

[33] S. W. Golomb and O. Moreno. On periodicity properties of Costas arrays and a conjecture on permutation polynomials. *IEEE Trans. Inform. Theory*, 42:2252–2253, 1996.

[34] T. Helleseth, C. Rong, and D. Sandberg. New families of almost perfect nonlinear mappings. *IEEE Trans. Inf. Theory*, 45:475–485, 1999.

[35] H. M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, XXVI:189–221, 2002.

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

[37] X.-d. Hou. Two classes of permutation polynomials over finite fields. *J. Combin. Theory Ser. A*, 118:448–454, 2011.

[38] X.-d. Hou and T. Ly. Necessary conditions for reversed Dickson polynomials to be permutational. *Finite Fields Appl.*, 16:436–448, 2010.

[39] X.-d. Hou, G. L. Mullen, J. A. Sellers, and J. L. Yucas. Reversed Dickson polynomials over finite fields. *Finite Fields Appl.*, 15:748 – 773, 2009.

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

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

[42] R. Lidl, G. L. Mullen, and G. Turnwald. *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[43] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[44] J. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. In *Fast Software Encryption*, volume 809 of *Lecture Notes Comput. Sci.*, pages 1–17, 1994.

[45] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT '93*, volume 765 of *Lecture Notes Comput. Sci.*, pages 386–397, 1994.

[46] G. McGuire and R. Alvarez. S-boxes, APN functions and related codes. In B. Preneel, S. Dodunekov, V. Rijmen, and S. Nikova, editors, *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, volume 23 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 49–62, 2009.

[47] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.

[48] W. H. Mills. Polynomials with minimal value sets. *Pacific J. Math.*, 14:225–241, 1964.

[49] G. L. Mullen and D. Panario. *Handbook of Finite Fields.* CRC Press, forthcoming.

[50] A. Muratović-Ribić. A note on the coefficients of inverse polynomials. *Finite Fields Appl.*, 13:977–980, 2007.

[51] A. Muratović-Ribić and Q. Wang. On coefficients of polynomials over finite fields. *Finite Fields Appl.*, 17:575–599, 2011.

[52] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology—EUROCRYPT '91*, volume 547 of *Lecture Notes Comput. Sci.*, pages 378–386. Springer, Berlin, 1991.

[53] D. Panario, A. Sakzad, B. Stevens, D. Thomson, and Q. Wang. Ambiguity and deficiency of permutations over finite fields with linearized difference map. Submitted to *IEEE Trans. Inf. Theory*, 2012.

[54] D. Panario, A. Sakzad, B. Stevens, and Q. Wang. Ambiguity and deficiency of permutations from finite fields. In *Proc. Information Theory Workshop*, pages 165–169. IEEE, 2011.

[55] D. Panario, A. Sakzad, B. Stevens, and Q. Wang. Two new measures for permutations: Ambiguity and deficiency. *IEEE Trans. Inf. Theory*, 57:7648–7657, 2011.

[56] D. Panario, B. Stevens, and Q. Wang. Ambiguity and deficiency in Costas arrays and APN permutations. In *Proc. LATIN 2010*, volume 6034 of *Lecture Notes Comput. Sci.*, pages 397–406, 2010.

[57] L. Poinsot. Non Abelian bent functions. *Cryptogr. Commun.*, 4:1–23, 2012.

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

[59] C. E. Shannon. Communnication theory and secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[60] R. Terada. SP-ASCrypto - Linear cryptanalysis and differential cryptanalysis: A brief course. slides available on request, 2011.

[61] D. Thomson. A note on non-balancedness of permutations with optimal ambiguity and deficiency. Submitted to *Finite Fields Appl.*, 2012.

[62] D. Thomson and Q. Wang. A conjecture of Golomb and Moreno on permutation polynomials. Submitted to *IEEE Trans. Inf. Theory*, 2012.

[63] W. Stein, et al. Sage: Open source mathematics software, as viewed in October, 2012. available online, `http://www.sagemath.org`.