Deficiency and Ambiguity of Low Degree Permutation Polynomials

by

Ommkaltoum Omar

A Thesis Submitted to the faculty of Garaduate Student and Research in partial fulfilment of the requirements for the degree of Master of Science

School of Mathematics and Statistics
Ottawa-Carleton Institution for Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada
2015

Abstract

In this thesis, we study the concepts of deficiency and ambiguity for a bijection on a finite Abelian group, in particular, for permutation polynomials over finite fields. Our focus is on all normalized permutation polynomials of degree less than or equal to 5. We obtain explicit numbers for deficiency and ambiguity of eleven classes of polynomials in Table A.0.1. We verified them by using SAGE. However, we could not find a formula for the last class of remaining two cases, except one observation on a relation between ambiguity and deficiency in a special case for one of the remaining unsolved classes.

Acknowledgement

Foremost, I would like to express my sincere gratitude to my supervisor Prof. Steven Wang for the continuous support of my master's degree, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better supervisor and mentor for my master's degree.

Last but not the least, I would like to thank my family: my parents, (Altoumiyah Omar and Abduallah Musa Omar), my brothers (Wesam, Hosam, Sami and Basim) and sisters (Assmaa, Zynab and Fatimaa) for their pray and support throughout my life. In particular, my sincere thanks to my husband, Mohamed Ali for his full support and help during my study, and also present this work for my children.

Contents

List of Tables

Chapter 1

Introduction

In this thesis, we study mappings between two finite Abelian groups of the same cardinality, in particular, over two finite fields of the same cardinality. A permutation polynomial over a finite field $\mathbb{F}_q$ that introduces a bijective map from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a good example for this concept. Our main focus is on normalized permutation polynomials of degree smaller than or equal to 5 over finite field $\mathbb{F}_q$, which essentially give all permutation polynomials with degree smaller than or equal to 5; see [37]. In particular, we are interested in two cryptographic measures, ambiguity and dificiency, of these permutation polynomials.

Let $F : G_1 \to G_2$ be any map, or partial map, between two Abelian groups of the same sizes. The difference maps of F are given by $\Delta_{F,a} = F(x + a) - F(x)$, where $a \in G_1^* = G \setminus \{0\}$. Difference maps bring a lot of attention when cryptographers design good substitution boxes (S-boxes) in substitution-permutation networks. In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext. Mathematically, they can be implemented as permutation polynomial over finite fields. Differential cryptanalysis and linear cryptanalysis are two common attacks on ciphers. Differential cryptanalysis is an attack which exploits pairs of differences of inputs and outputs $(\Delta g, \Delta h)$ occur with high probability. More specifically, if F is the function induced by an S-box, then

for a fixed input difference $\Delta g = a$, differential cryptanalysis requires pairs $(x + a, x)$ such that $((x + a) - x, F(x + a) - F(x))$ occur with significant probability. Another common attack is linear cryptanalysis. 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.

One of the most famous example is the Advanced Encryption Stardard (AES) cipher [22], which uses the inverse polynomial $f(x) = x^{-1}$ over the finite field of size 2^8. Namely, $f : x \to x^{2^8-2}$ over $\mathbb{F}_{2^8}$ such that $f(0) = 0$ and $f(x) = x^{-1}$, if $x \neq 0$. It is well known that the inverse polynomial over $\mathbb{F}_{2^8}$ has high nonlinearity and close to optimal differential properties.

A measure to study the differential property of polynomials over finite fields is so called differential uniformity. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a polynomial over finite field $\mathbb{F}_q$. We define $N_f(a, b) = |\{x \in \mathbb{F}_q : \Delta_{f,a} = f(x+a)-f(x) = b\}|$ and $\delta_f = max\{N_f(a, b) : a, b \in \mathbb{F}_q\}$. Then F is differentially k-uniform if $\delta_f = k$. A polynomial has a better resistence to differential attack if k is smaller. The optimal values are $k = 1$ for polynomials over finite fields with odd characterics and $k = 2$ for polynomials over finite fields with even characteristic, respectively. In the former case, these polynomials are called perfect nonlinear functions and the latter polynomials are called almost perfect nonlinear (APN) functions. In fact, $f : x \to x^{2^8-2}$ over $\mathbb{F}_{2^8}$ is a differentially 4-uniform function. An open question is to search for APN permutation over $\mathbb{F}_{2^8}$.

The goal of any cryptosystem allows the secure transmission of data between two parties. Since, we are not only interested in the cardinalities of the value sets of the $\Delta_{F,a}$, but in the number of repetitions of elements in the value multi-sets of the $\Delta_{F,a}$. Deficiency and Ambiguity were first introduced in [50] to measure the surjectivity and injectivity of these difference maps. Bound on permutations over finite cyclic groups are given. An extended journal version of these results and proofs appeared in [48]. In these papers, several optimal functions achieving these lower bounds over cyclic groups are studied. Moreover, they proved that optimum ambiguity is essentially the same as APN for permutations over finite fields with even characteristics. However, for

polynomials over finite fields with odd characteristics, APN does not necessarily implies the optimum ambiguity and it turns out that optimum ambiguity is a finer measure. Later on, deficiencies and ambiguities of several special classes of polynomials, such as APN monomials over finite fields with odd characterics, Linearized polynomials, Dembowski-Ostrom (DO) polynomials are studied in [47], which can also be found in [59].

Despite of recent progress in studying deficiency and ambiguity of several classes of polynomials over finite fields, there is no study on these measures for permutation polynomials with low degrees. In [37], a list of thirteen classes of normalized permutation polynomials of degree smaller than or equal to 5 over finite field $\mathbb{F}_q$ is given. Essentially they give all permutation polynomials with degree smaller than or equal to 5. One can also find a list of PPs of degree 6 over finite fields with odd characteristic in [17] and a list of PPs of degree 6 and 7 over finite fields with characteristic two in [36]. Moreover, all monic PPs of degree 6 in the normalized form are tabulated in [58]. In this thesis, we take an initiative to study deficiency and ambiguity of all these normalized permutation polynomials of degree less than or equal to 5. We have done some computer experiments in SAGE and obtained some preliminary partial results.

This thesis organized as following. In Chapter 2, we present the background on finite fields, and permutation polynomials over finite fields The reader might find that [37, Ch. 7] and [44, Sec. 8.1] are useful references. In addition, we define Almost Perfect Nonlinear Functions (APN). Lastly, we cover some results of two equivalence relations which is needed in this thesis.

In Chapter 3, we review the definition of deficiency and ambiguity of a given bijection F on a finite Abelian group G, which measure the surjectivity and injectivity of the difference map

$$\Delta_{F,a}(x) = F(x+a) - F(x)$$

where $a \in G$ [47], [48], [49], [50]. In [47], they are defined for a general map between finite Abelian groups. Moreover, a general lower bound on the deficiency and ambiguity

can be found in [47]. For the maps between finite fields of even characteristic, attaining the minimum ambiguity implies that F is almost perfect non-linear (APN). That means each difference map for $a \neq 0$ is at worst 2-to-1. However, not every APN function attains the minimum deficiency and ambiguity. In particular, the lower bound of deficiency and ambiguity of a bijection between two Abelian groups first obtained in [48] and reformulated in [47] by removing the restriction on the co-domain. We review these results in Section 3.2. Then in Section 3.3, we review several special functions over the multiplicative group of a finite field achieving these optimal lower bounds. These functions include twisted permutation monomials and Mobiüs functions. In Section 3.4, we review several classes of polynomials over finite fields. Theses results of permutations over finite fields and their deficiencies and ambiguities are obtained in [47, 48]. In first subsection, we give the deficiencies and ambiguities of linearized polynomials. After that, we review the inverse function over $\mathbb{F}_{2^m}$. Next subsection, APN monomials over a finite field $\mathbb{F}_{p^e}$ of characteristic $p > 2$ are addressed. In Subsection 3.4.4, we show how the authors of [48] derive a formula for the deficiencies and ambiguities of DO-polynomials in terms of ranks of matrices and survey these matrices for some specific DO permutations. Specifically, Permutations based on trace functions are also considered.

In Chapter 4, we study deficiency and ambiguity of all normalized permutation polynomials of degree less than or equal to 5. The list of these polynomials can be found in Table 4.0.1. We are able to obtain the explicit numbers of deficiency and ambiguity for eleven items in this table. We also verified these formulas using SAGE program over finite fields of small sizes. However, for the remaining two classes (more interesting classes), we can only obtain some preliminary computer results over finite fields of small sizes and we do not know how to obtain general formulae for these classes. Some computer experiments can be found in the Appendix.

It would be interesting to completely determine deficiency and ambiguity of normalized permutation polynomials of low degree. More generally, the problem of classifying all deficiency and ambiguity is wide open. Even the case of classifying all the power

functions is still unresolved.

Chapter 2

Preliminaries

In this chapter, we line out the background and results needed in this thesis. In Section 2.1, we start with basic facts related to finite fields theory. In Section 2.2, we cover permutation polynomials and basic properties, and results. In Section 2.3, we define almost perfect nonlinear functions (APN functions). In the last section, we present an equivalence for permutations. More details and proofs can be found in references [37], [44] and references therein.

2.1 Finite Fields

In this section, we give a quick overview of finite field theory. We only state some basic facts, definition and results. All the proofs can be found in the excellent comprehensive reference [37].

Definition 2.1.1. *A group $(G, *)$ is a set G, together with a binary operation $*$ on G which satisfies the following conditions:*

(i) *For any $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.*

(ii) *There exists $e \in G$ such that $a * e = e * a = a$ and e is the identity element of G.*

(iii) *For any $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$, the inverse of a.*

Definition 2.1.2. *A group $(G, *)$ commutative if for any $a, b \in G$ we have $a*b = b*a$.*

Definition 2.1.3. *A field $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$, together with two binary operations $+$ and $\cdot$, such that*

(i) *$(\mathbb{F}, +)$ is an abelian group with the identity element "0".*

(ii) *$(\mathbb{F}^*, \cdot)$ is an abelian group, where $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$.*

(iii) *For all $a, b, c \in \mathbb{F}$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Definition 2.1.4. *A finite field is a field that has a finite number of elements.*

Definition 2.1.5. *A multiplicative group G cyclic if there is an element $a \in G$ such that for any $b \in G$ there is some integer j with $b = a^i$. Such an element a is a generator of the cyclic group, and we write $G =< a >$.*

Definition 2.1.6. *Let $\mathbb{F}$ be a field. For all $a \in \mathbb{F}$ the characteristic of $\mathbb{F}$ is the least positive integer m such that $ma = 0$. Moreover, the order of a which is denoted by $|a|$, is the least positive integer m such that $a^m = 1$.*

Proposition 2.1.1. *The characteristic of a finite field $\mathbb{F}$ is a prime number p.*

Theorem 2.1.1. *For every prime p and every positive integer n there exists a finite field with p^n elements. Conversely, any finite field has p^n elements for a prime number p and a positive integer $n \geq 1$.*

From now, we use p to denote a prime number, $\mathbb{F}_{p^n}$ to denote the finite field of size p^n, and $\mathbb{F}_{p^n}^*$ to denote $\mathbb{F}_{p^n}\backslash\{0\}$.

Proposition 2.1.2. *For every finite field $\mathbb{F}_{p^n}$, we have the following:*

(i) *For all $a \in \mathbb{F}_{p^n}^*$, we have $a^{p^n-1} = 1$, and $|a|$ divides $p^n - 1$.*

(ii) *For every integer $i \geq 0$ and $a, b \in \mathbb{F}_{p^n}$, we have $(a + b)^{p^i} = a^{p^i} + b^{p^i}$.*

Proposition 2.1.3. *Let q be a prime power and $\mathbb{F}_q$ be a finite field of size q. The multiplicative group $\mathbb{F}_q^*$ of all nonzero elements of $\mathbb{F}_q$ is cyclic. Any generator of $\mathbb{F}_q^*$ is a primitive element of $\mathbb{F}_q$.*

Definition 2.1.7. *Let $\mathbb{F}$ is a subset of a field $\mathbb{E}$ such that $\mathbb{F}$ is also a field under the same operation associated with $\mathbb{E}$. Then $\mathbb{F}$ is a subfield of $\mathbb{E}$ and $\mathbb{E}$ is a field extension of $\mathbb{F}$.*

Definition 2.1.8. *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements up to isomorphism.*

Definition 2.1.9. *A field containing no proper subfield $\mathbb{F}_{p^n}$ is a prime field. The intersection of all subfield of $\mathbb{F}_{p^n}$ is prime subfield, and is a prime field itself. In case of $\mathbb{F}_{p^n}$, the prime subfield is isomorphic to $\mathbb{F}_p$.*

Next we review some results on polynomials over finite fields.

Definition 2.1.10. ***(Lagrange Interpolation Formula)*** *Let $n \geq 0$ be an integer and q be a prime power. Let $a_0, \ldots, a_n$ be distinct elements of $\mathbb{F}_q$, and let $b_0, \ldots, b_n$ be any elements of $\mathbb{F}_q$. Then there exists a unique polynomial polynomial $f \in \mathbb{F}_q[x]$ of degree at most n such that $f(a_i) = b_i$, for $0 \leq i \leq n$. This polynomial is given by*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k\neq i}^{n} (a_i - a_k)^{-1}(x - a_k).$$

Corollary 2.1.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be any function. When we apply the formula of Langrange Interpolation, f has a unique representation as a polynomial in $\mathbb{F}_{p^n}[x]$ of degree at most $p^n - 1$.*

Definition 2.1.11. *Let q be a prime power and let L be a polynomial over $\mathbb{F}_{q^m}$. if L is the form*

$$L(x) = \sum_{j=0}^{n} l_j x^{q^j} = l_0 x + l_1 x^q + \cdots + l_n x^{q^n} \in \mathbb{F}_{q^m}[x],$$

*then L is a **q-polynomial** over $\mathbb{F}_{q^m}$; these polynomials are also known as **linearized polynomials** because of these properties:*

(i) $L(\beta + \gamma) = L(\beta) + L(\gamma) \quad$ *for all* $\beta, \gamma \in \mathbb{F}_{q^m}$,

(ii) $L(c\beta) = cL(\beta)$ *for all* $c \in \mathbb{F}_q, \beta \in \mathbb{F}_{q^m}$.

The trace function is an important type of linear operator.

Definition 2.1.12. *For* $\alpha \in \mathbb{F} = \mathbb{F}_{q^m}$ *and* $\mathbb{K} = \mathbb{F}_q$ *the trace* $Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$ *of* α *over* $\mathbb{K}$ *is defined by*

$$Tr_{\mathbb{F}/\mathbb{K}}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

If $\mathbb{K}$ *is the prime subfield of* $\mathbb{F}$, *then* $Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$ *is the absolute trace of a and is simply denoted by* $Tr_{\mathbb{F}}(\alpha)$.

Proposition 2.1.4. *Let* $\mathbb{K} = \mathbb{F}_q$ *and* $\mathbb{F} = \mathbb{F}_{q^m}$. *Then the trace function* $Tr_{\mathbb{F}/\mathbb{K}}$ *satisfies the following properties:*

(i) $Tr_{\mathbb{F}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{F}/\mathbb{K}}(\alpha) + Tr_{\mathbb{F}/\mathbb{K}}(\beta)$, *for all* $\alpha, \beta \in \mathbb{F}$;

(ii) $Tr_{\mathbb{F}/\mathbb{K}}(c\alpha) = cTr_{\mathbb{F}/\mathbb{K}}(\alpha)$, *for all* $c \in \mathbb{K}$, $\alpha \in \mathbb{F}$;

(iii) $Tr_{\mathbb{F}/\mathbb{K}}$ *is a linear transformation from* $\mathbb{F}$ *onto* $\mathbb{K}$, *where both* $\mathbb{F}$ *and* $\mathbb{K}$ *are viewed as vector spaces over* $\mathbb{K}$;

(iv) $Tr_{\mathbb{F}/\mathbb{K}}(a) = ma$, *for all* $a \in \mathbb{K}$;

(v) $Tr_{\mathbb{F}/\mathbb{K}}(\alpha^q) = Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$, *for all* $\alpha \in \mathbb{F}$.

Proposition 2.1.5. *Let* $\langle \cdot, \cdot \rangle$ *be a map from* $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ *to* $\mathbb{F}_p$. *The map* $\langle \cdot, \cdot \rangle$ *is an inner product on* $\mathbb{F}_{p^n}$ *if it satisfies the following:*

(i) $\langle a + b, c \rangle = \langle a, c \rangle + \langle b, c \rangle$, *for all* $a, b, c \in \mathbb{F}_p^n$;

(ii) $\langle ua, b \rangle = u\langle a, b \rangle$, *for all* $a, b \in \mathbb{F}_p^n$, $u \in \mathbb{F}_p$;

(iii) $\langle a, b \rangle = \langle b, a \rangle$, *for all* $a, b \in \mathbb{F}_p^n$.

The absolute trace function of ab, $Tr(ab)$, *defines an inner product on* $\mathbb{F}_{p^n}$.

Corollary 2.1.2. (i) *For any* $a \in \mathbb{F}_q$ *thw number of elements* $\alpha \in \mathbb{F}_{p^n}$ *such that* $Tr(\alpha) = a$ *is* q^{n-1}.

(ii) *For any $a \in \mathbb{F}_q^*$ thw number of elements $\alpha \in \mathbb{F}_{p^n}^*$ such that $N(\alpha) = a$ is $(q^{n-1} - 1)/(q-1)$.*

Let us consider quadratic equations over the finite field $\mathbb{F}_{2^n}$.

Lemma 2.1.1. *[62] Let $\alpha, \theta \in \mathbb{F}_{2^n}$ be such that $Tr(\alpha) = 0$ and $Tr(\theta) = 1$. Then the quadratic equation $x^2 + x + \alpha = 0$ has a solution $\beta = \alpha\theta^2 + (\alpha + \alpha^2)\theta^{2^2} + \cdots + (\alpha + \alpha^2 + \cdots + \alpha^{2^{n-2}})\theta^{2^2}$ and $\beta + 1$.*

In general, we have the following theorem.

Theorem 2.1.2. *[62, P.157] Let*

$$ax^2 + bx + c = 0 \tag{2.1.1}$$

be a quadratic equation over $\mathbb{F}_{q^n}$, where $a, b, c \in \mathbb{F}_{q^n}$ and $a \neq 0$. When $b = 0$, Equation (2.1.1) has a unique solution $x = (c/a)^{2^{n-1}}$. When $b \neq 0$, Equation (2.1.1) has

$$\begin{cases} \textit{no solution}, & \textit{if } Tr(ac/b^2) = 1, \\ \textit{two solution}, & \textit{if } Tr(ac/b^2) = 0. \end{cases}$$

2.1.1 Vectorial Function

For every finite field $\mathbb{F}_{p^n}$, there exists a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_{p^n}$ such that any $x \in \mathbb{F}_{p^n}$ can be expressed as a linear combination of $\alpha_1, \alpha_2, \ldots, \alpha_n$. We denote an n-dimensional vector space over $\mathbb{F}_p$ by $\mathbb{F}_p^n$, where p is prime. For vector $u = (u_1, \ldots, u_n) \in \mathbb{F}_p^n$, we let u_i denote the i-th coordinate of u. Hence, the n-dimensional vector space of $\mathbb{F}_p^n$ over $\mathbb{F}_p$ can be endowed with the structure of the finite field $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ via the bijection from $\mathbb{F}_p^n$ to $\mathbb{F}_{p^n}$ as follows:

$$(x_1, \ldots, x_n) \mapsto x_1\alpha_1 + \cdots + x_n\alpha_n. \tag{2.1.2}$$

A common basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is a polynomial basis, which is $\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}\}$, where α is primitive of $\mathbb{F}_{p^n}$. We show that functions over finite vector space, can be

represented uniquely in algebraic normal form by using the bijection between vector spaces and finite fields.

Proposition 2.1.6. ***(Carlet et al. [10])*** *Let n be a positive integer and $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be any function. Then F can be uniquely represented as a polynomial in n variables $x_1, \ldots, x_n$, with coefficient in $\mathbb{F}_p^n$ such that $deg(x_i) < p$ for $1 \leq i \leq n$:*

$$F(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_p^n} c(u) \left(\prod_{i=1}^{n} x_i^{u_i} \right), c(u) \in \mathbb{F}_p^n.$$

This polynomial representation of F is the algebraic normal form (ANF) of F.

The way to obtain algebraic normal form $F(x_1, \ldots, x_n)$ from the polynomial representation F is the following: let α be a primitive element of $\mathbb{F}_{p^n}$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ be a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Write x as the expression $\sum_{j=1}^{n} x_j \alpha^{j-1}$. Then we have

$$\begin{aligned} F(x_1, \ldots, x_n) &= f\left(\sum_{j=1}^{n} x_j \alpha^{j-1} \right) \\ &= \sum_{i=0}^{p^n-1} c_i \left(\sum_{j=1}^{n} x_j \alpha^{j-1} \right)^i \\ &= \sum_{i=0}^{p^n-1} c_i \left(\sum_{j=1}^{n} x_j \alpha^{j-1} \right)^{\sum_{k=1}^{n} i_k p^{k-1}} \\ &= \sum_{u \in \mathbb{F}_p^n} c(u) \left(\prod_{j=1}^{n} x_j^{u_j} \right). \end{aligned}$$

We now define the algebraic degree of a vectorial function.

Definition 2.1.13. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a function with ANF*

$$F(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_p^n} c(u) \left(\prod_{i=1}^{n} x_i^{u_i} \right), c(u) \in \mathbb{F}_p^n.$$

The algebraic degree of F is denoted $d^\circ(F)$ is define as

$$max \left\{ \sum_{i=1}^{n} u_i : c(u) \neq 0 \right\}.$$

Definition 2.1.14. *Let i be any integer such that $0 \leq i \leq p^n - 1$, and the p-adic expansion of i be*

$$i = \sum_{k=0}^{n-1} i_k p^k, 0 \leq i_k \leq p - 1.$$

The weight of i, denoted $w_p(i)$ is

$$w_p(i) = \sum_{k=0}^{n-1} i_k.$$

Definition 2.1.15. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ have polynomial representation $f = \sum_{i=0}^{p^n-1} c_i x^i$ in $\mathbb{F}_{p^n}[x]$. Then, the p-degree of f is define as maximum p-weight of exponents:*

$$max\{w_p(i) : 0 \leq i \leq p^n - 1, c_i \neq 0\}.$$

Proposition 2.1.7. ***(Carlet et al. [10])*** *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be any function. Then, algebraic degree of f is given by the p-degree of f:*

$$d^\circ(f) = max\{w_p(i) : 0 \leq i \leq p^n - 1, c_i \neq 0\}.$$

Definition 2.1.16. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function and let $\mathbb{K}$ be a subfield of both $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$. Then L is $\mathbb{K}$-linear if the following holds*

$$L(x + y) = L(x) + L(y), \forall x, y \in \mathbb{F}_{p^n},$$

$$L(cx) = cL(x), \forall c \in \mathbb{K}.$$

A function $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is $\mathbb{K}$-affine if $A(x) = L(x) + c$, where L is $\mathbb{K}$-linear and $c \in \mathbb{F}_{p^m}$ is constant. When $\mathbb{K} = \mathbb{F}_p$, the prime subfield of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, L and A are also linear and affine, respectively.

Remark 2.1.1. *A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is linear if and only if the polynomial representation in $\mathbb{F}_{p^n}[x]$ obtained from the ANF of F is a linearized polynomial.*

2.2 Permutation Polynomials

This section introduce the definitions of permutation polynomials and some fundamental results. More details and proofs can be found in [37].

2.2.1 Criteria for Permutation Polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is a Permutation Polynomial(PP) of $\mathbb{F}_q$ if the associated polynomial function $f : c \mapsto f(c)$ is a permutation of $\mathbb{F}_q$. It is obvious that by the finiteness of $\mathbb{F}_q$ we can express this definition in various other ways.

Lemma 2.2.1. *The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions hold:*

(i) *the function $f : c \mapsto f(c)$ is one-to-one,*

(ii) *the function $f : c \mapsto f(c)$ is onto,*

(iii) *$f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.*

Definition 2.2.1. *Permutation polynomials of $\mathbb{F}_q$ may be characterised as polynomial functions $f \in \mathbb{F}_q[x]$ satisfying the property $\{f(c) : c \in \mathbb{F}_q\} = \mathbb{F}_q$. The set $\{f(c) : c \in \mathbb{F}_q\}$ is known as the value set of f, denoted V_f.*

Lemma 2.2.2. *[37, P.348] For $f, g \in \mathbb{F}_q[x]$ we have $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \bmod (x^q - x)$.*

Lemma 2.2.3. *[37, p.349] Let $a_0, ..., a_{q-1}$ be elements of $\mathbb{F}_q$. Then the following two conditions are equivalent:*

(i) *$a_0, ..., a_{q-1}$ are distinct;*

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

The following criterion for permutation polynomials is known as Hermite's criterion.

Theorem 2.2.1. ***(Hermite's criterion. [37, Theorem.7.4])*** *Let $q = p^r$, where p is a prime and r is a positive integer. Then a polynomial $f \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(i) *f has exactly one root in $\mathbb{F}_q$;*

(ii) *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \bmod (x^q - x)$ has degree $\leq q-2$.*

Corollary 2.2.1. *If $d > 1$ is divisor of $q-1$, then there is no permutation polynomial of $\mathbb{F}_q$ of degree d.*

The following theorem is a consequence of Theorem 2.2.1.

Theorem 2.2.2. *Let $\mathbb{F}_q$ be of characteristic p. Then $f \in \mathbb{F}_p[x]$ is a PP of $\mathbb{F}_q$ if and only if the following conditions hold:*

(i) *the reduction of $f(x)^{q-1} \bmod (x^q - x)$ has degree $q-1$;*

(ii) *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \bmod (x^q - x)$ has degree $\leq q-2$.*

2.2.2 Special Classes of Permutation Polynomials

In this subsection, we give some classes of permutation polynomials. The following are elementary results of PPs.

Theorem 2.2.3. *Suppose that $\mathbb{F}_q$ is a finite field with q element.*

(i) *Every linear polynomial over $\mathbb{F}_q$ is a PP of $\mathbb{F}_q$.*

(ii) *The monomial x^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.*

Proof. (i) Trivial. (ii) Since $0^n = 0$, the monomial x^n is onto if and only if the function $f : \mathbb{F}_q^* \to \mathbb{F}_q^*$, $x \mapsto x^n$ is onto. Let g be a primitive element of the cyclic group $\mathbb{F}_q^*$. Then the image is the cyclic subgroup generated by g^n, which equals $\mathbb{F}_q^*$ if and only if g^n is a primitive element. This is equivalent to the condition $\gcd(n, q-1) = 1$. □

We now present a class of polynomials known as q-polynomials from previous section.

Theorem 2.2.4. *[37][19] A linearized polynomial*

$$L(x) = \sum_{j=0}^{e-1} l_j x^{p^j} \tag{2.2.1}$$

is a permutation polynomial over $\mathbb{F}_q$ if and only if L has no roots in $\mathbb{F}_q$ other than 0.

The following theorem gives another class of permutation polynomials.

Theorem 2.2.5. *[37, P.351] Let $r \in \mathbb{N}$ with $\gcd(r, q-1) = 1$ and let s be a positive divisor of $q-1$. Then $f(x) = x^r(g(x^s))^{(q-1)/s}$ is a permutation polynomial of $\mathbb{F}_q$.*

Now, we review some other well-known polynomials over the finite field $\mathbb{F}_q$. We require the following terminology. For any positive integer s and any prime number p.

Definition 2.2.2. *[26] A polynomial F in $\mathbb{F}_q[x]$ such that*

$$F(x) = \sum_{k,j=0}^{e-1} a_{k,j} x^{p^j+p^k}, \tag{2.2.2}$$

is a Dembowski-Ostrom (DO) polynomial.

Next, we give a list of DO permutation polynomials over $\mathbb{F}_q$.

Theorem 2.2.6. *[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:*

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

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

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

Proposition 2.2.1. *[3], [13]*

(i) *Let q be even and r be odd. Then the polynomial*

$$F(x) = x(Tr(x) + sx), \tag{2.2.3}$$

permutes $\mathbb{F}_{q^r}$ for all $s \in \mathbb{F}_q \backslash \{0, 1\}$.

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

$$F(x) = x^{2^k} + x + Tr(x^s) \tag{2.2.4}$$

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.*

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

$$F(x) = x^d + Tr(x^t) \tag{2.2.5}$$

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) *$t \equiv sd \pmod{2^e - 1}$ for some $1 \leq s \leq 2^e - 2$, where s has 2-weight 1 or 2.*

2.2.3 Normalized Permutation Polynomials

Let $F(x) = \sum_{i=0}^{n} a_i x^i$ be a PP of $\mathbb{F}_q$. The set of PPs of $\mathbb{F}_q$ is closed under composition; in particular the polynomial

$$g(x) = cf(x + b) + d$$

is a PP of $\mathbb{F}_q$ for all choices of $b, c, d \in \mathbb{F}_q, c \neq 0$.

Definition 2.2.3. *A PP $f \in \mathbb{F}_q[x]$ is in a normalized form if f is monic, $f(0) = 0$, and when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero.*

The following table obtains all normalized permutation polynomials of degree ≤ 5 given by [37, P.352].

Table 2.2.1: List of All Normalized Permutation Polynomials of degree ≤ 5 .

	Normalized PPs	*any q*
1	x^2	$q \equiv 0 \pmod 2$
2	x^3	$q \not\equiv 1 \pmod 3$
3	$x^3 - wx \quad w$ not square	$q \equiv 0 \pmod 3$
4	$x^4 \pm 3x$	$q = 7$
5	$x^4 + wx^2 + w^2x \quad$ if its only root in $\mathbb{F}_q$ is 0	$q \equiv 0 \pmod 2$
6	x^5	$q \not\equiv 1 \pmod 5$
7	$x^5 - wx \quad w$ not a forth root	$q \equiv 0 \pmod 5$
8	$x^5 + wx \quad$ where $w^2 = 2$	$q = 9$
9	$x^5 \pm 2x$	$q = 7$
10	$x^5 + wx^3 \pm x^2 + 3w^2x \quad w$ not square	$q = 7$
11	$x^5 + wx^3 + 3w^2x \quad w$ not square	$q = 13$
12	$x^5 - 2wx^3 + w^2x \quad w$ not square	$q \equiv 0 \pmod 5$
13	$x^5 + wx^3 + 5^{-1}w^2x \quad w$ arbitrary	$q \equiv 2, 3 \pmod 5$

2.3 Almost Perfect Nonlinear (APN)

Almost perfect nonlinear(APN) functions are defined for vectorial functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, where n and m may be distinct. In the case $n = m$ the definitions can be extended in an analogous manner to functions from the finite field $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, which are represented uniquely as polynomials of degree at most $p^n - 1$.

Definition 2.3.1. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a function and let $a \in \mathbb{F}_p^n$. The derivative of F with respect to a is the function $D_aF : \mathbb{F}_p^n \to \mathbb{F}_p^m$ defined by*

$$D_aF = F(x + a) - F(x).$$

If $D_aF = c$, is constant for every $x \in \mathbb{F}_p^n$, then a is a linear structure of F.

Definition 2.3.2. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be any mapping, $a \in \mathbb{F}_p^n, b \in \mathbb{F}_p^m$, and*

$$N_F(a,b) = |\{x \in \mathbb{F}_p^n : F(x+a) - F(x) = b\}|;$$

also let

$$\Delta_F = max\{N_F(a,b) : a \in \mathbb{F}_p^{n*}, b \in \mathbb{F}_p^m\}.$$

Then F is differentially k-uniform, if $\Delta_F = k$ [46]; F is perfect nonlinear(PN) or planar if $k = 1$, and almost perfect nonlinear(APN) if $k = 2$. Equivalently, $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is APN if for every nonzero $(a,b) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$ the following system

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

has at most two solutions $(x,y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$.

Remark 2.3.1. *There are no PN mappings over fields of characteristic 2. Indeed, let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be any mapping. If x is a solution to $F(x+a)-F(x) = b$, then $x+a$ is also a solution, since $F((x+a)+a)-F(x+a) = F(x)-F(x+a) = F(x+a)-F(x)$. Therefore, the number of solutions to $F(x+a)-F(x) = b$ is always even.*

Proposition 2.3.1. ***(Dobbertin et al. [21])*** *For any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ we have*

$$\sum_{a,b \in \mathbb{F}_{p^n}} N_F(a,b) = p^{2n}.$$

Corollary 2.3.1. *For any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ we have $\Delta_F \neq 0$ and*

$$\sum_{a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}} N_F(a,b) = (p^n)^2 - p^n.$$

If F is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, there is another equivalent definition for APN functions.

Proposition 2.3.2. ***(Berger et al. [2])*** *Let F be any function on $\mathbb{F}_{2^n}$. Then, F*

is Almost Perfect Nonlinear (APN) if and only if, for any nonzero $a \in \mathbb{F}_{2^n}$, *the set* $\{D_aF(x) : x \in \mathbb{F}_{2^n}\}$ *has cardinality* 2^{n-1}.

We know that PN functions are furthest away from linear functions in the sense that the number of solutions to $D_a(F) = b$ is the smallest possible for PN function, and is maximum for linear functions. PN functions in odd characteristic fields and APN functions in even characteristic fields are optimally resistant to differential cryptanalysis. On the other hand, we define next almost bent (AB) functions.

Definition 2.3.3. *Let* $F : F_2^n \to \mathbb{F}_2^n$ *be any function. The Walsh transform or (discrete) Fourier transform of* F *is function* $\lambda_F : \mathbb{F}_2^n \times \mathbb{F}_2^n$ *define by*

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)} \in \mathbb{Z},$$

where $x \cdot y = x_1y_1 + \cdots + x_ny_n$ *is standard inner product. The Walsh spectrum of* F *is the set*

$$\Lambda_F = \{\lambda_F(a, b) : a, b \in \mathbb{F}_{p^n}, b \neq 0\}.$$

The Walsh transform is independent of the choice of inner product. Hence, if $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a polynomial function, it is possible to define the Walsh transform of F analogously. We have

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(ax + bF(x))}.$$

Instead of using the standard inner product for vectors, we use absolute trace function. The Walsh transform gives us a quantitative measure of Hamming distance from F to all linear function. If $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is nonzero linear function, then there exists $a, b \neq 0$ in $\mathbb{F}_{2^n}$ such that $\mathrm{Tr}(ax + bF(x)) = 0$ for all x. Then $\lambda_F(a, b) = 2^n$, which is the maximum possible value for $\lambda_F(a', b')$ for all $a', b' \in \mathbb{F}_{2^n}$.

Theorem 2.3.1. ***(Chabaud and Vaudenay [12])*** *Let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be an AB function. Then* F *is also APN. Moreover,* F *is AB if and only if the Walsh spectrum of* F *is* $\Lambda_F = \{0, \pm 2^{\frac{n+1}{2}}\}$.

Theorem 2.3.2. *If F is APN permutation, then F^{-1} is APN.*

Proof. Since F is a permutation, F^{-1} is bijective and since F is APN, if $b \in D_aF$, then $F(x+a) - F(x) = b$ has exactly 2 solutions. Let $y = F(x)$ and $y^0 = F(x+a)$, then $y^0 = y+b$. So, for given a and b, $F(x+a)-F(x) = b$ has at most 0 or 2 solutions. But, $x + a = F^{-1}(y + b)$ and $x = F^{-1}(y)$, so $F^{-1}(y + b) - F^{-1}(y) = a$ which has exactly 0 or 2 solutions since $F(x + a) - F(x) = b$ has exactly 0 or 2 solutions. That means, F^{-1} is APN. □

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be any polynomial function, then one must show that the maximum number of solutions to $F(x + 1) - F(x) = b$ for all $a \neq 0, b \in \mathbb{F}_{p^n}$ is two . In both the even and odd characteristic case, the first APN functions found over $\mathbb{F}_{p^n}$ were power functions, x^d. We can prove the APN property of a power function easier than for multinomial functions. In that case where $F(x) = x^d$ is equivalent to show that $F(x + 1) - F(x) = b$ has at most two solutions for all $b \in \mathbb{F}_{p^n}$. The following proposition illustrates this.

Proposition 2.3.3. ***(Dobbertin et al. [21])*** *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be defined by $F(x) = x^d$ where $1 \leq d \leq p^n - 1$. Then,*

$$N_F(a, b) = N_F(1, a^{-d}b), \forall a \in \mathbb{F}^*_{p^n},$$

where $-d$ is taken modulo $p^n - 1$.

Proof. We recall that $N_F(a, b)$ is the number of solution $x \in \mathbb{F}_{p^n}$ to equation $F(x + a) - F(x) = b$. Let $y = a^{-1}x$ and we have

$$\begin{aligned} F(x+a) - F(x) = b &\Leftrightarrow (x+a)^d - x^d = b \\ &\Leftrightarrow a^d(y+1)^d - a^d y^d = b \\ &\Leftrightarrow (y+1)^d - y^d = a^{-d}b. \end{aligned}$$

The number of solutions to the last equation is $N_F(1, a^{-d}b)$. □

This proposition is useful when verifying that $F(x) = x^d$ is APN with the help of computer. We give the known classes of APN functions over $\mathbb{F}_{2^n}$ in Table 2.3.1. In some cases, these functions are also AB; they are summarized in Table 2.3.2.

Table 2.3.1: Known APN Power Functions x^d on $\mathbb{F}_{2^n}$.

	Exponents d	Condition	Proven in
Gold functions	$2^i + 1$	$\gcd(n, i) = 1$	[27], [46]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(n, i) = 1$	[34], [35]
Welch functions	$2^i + 3$	$n = 2t + 1$	[19]
Niho functions	$2^t + 2^{t/2} - 1$ $2^t + 2^{\frac{3t+1}{2}} - 1$	$n = 2t + 1$, t even $n = 2t + 1$, t odd	[18]
Inverse functions	$2^{2t} - 1$	$n = 2t + 1$	[7], [46]
Dobbertin functions	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	[20]

Table 2.3.2: Known AB Power Functions x^d on $\mathbb{F}_{2^n}$ is odd.

	Exponents d	Condition	Proven in
Gold functions	$2^i + 1$	$\gcd(n, i) = 1$	[27], [46]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(n, i) = 1$	[34], [35]
Welch functions	$2^i + 3$	$n = 2t + 1$	[8], [9]
Niho functions	$2^t + 2^{t/2} - 1$ $2^t + 2^{\frac{3t+1}{2}} - 1$	$n = 2t + 1$, t even $n = 2t + 1$, t odd	[32]

2.4 Equivalence of Permutations

In this section, we present two equivalence relation, extended affine equivalence (EA-equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence). If two functions are EA-equivalence, one can obtain one of them from the other via compositions with an affine permutation. Also, we have that two functions are CCZ-equivalent if the graph of one function can be obtained via an affine permutation from a graph of other function. We comment that CCZ-equivalence is a generalization of EA-equivalence in the sense that if f and g are EA-equivalence, then they are CCZ-equivalence but the converse is not necessarily true.

2.4.1 Extended Affine Equivalence

We know by Definition 2.3.2 that a function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is APN or PN if $\Delta_F = 2$ or 1. For $a, b \in \mathbb{F}_p^n$ and two functions F and G, consider the multiset of values $\{N_F(a,b) : a, b \in \mathbb{F}_p^n\}$ and $\{N_G(a,b) : a, b \in \mathbb{F}_p^n\}$, where

$$N_F(a,b) = \left|\{x \in \mathbb{F}_p^n : F(x+a) - F(x) = b\}\right|,$$

$$N_G(a,b) = \left|\{x \in \mathbb{F}_p^n : G(x+a) - G(x) = b\}\right|.$$

When the multisets are the same, F and G have the same difference properties [21] and they are equivalent in the same sense. It is clear that F is k-differentially uniform if and only G is also k-differentially uniform. This motivates our first definition of equivalence, namely affine equivalence and extended affine equivalence.

Definition 2.4.1. *A function $L : G_1 \to G_2$ is linear if $L(x+y) = L(x) + L(y)$ for all $x, y \in G_1$. A function $K : G_1 \to G_2$ 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 codomain.*

Definition 2.4.2. *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 $F_1 \sim F_2$, if there exist affine permutations $K_1 : G_2 \to G_2, K_2 : G_1 \to G_1$ and an affine function $K_3 : G_1 \to G_2$ 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.

Proposition 2.4.1. *The algebraic degree is an affine invariant for all functions and an EA-invariant for non-affine functions. More precisely:*

(i) *Let $F_1, F_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be two affine equivalent functions. Then, F_1 and F_2 have the same algebraic degree, i.e. $d^o(F_1) = d^o(F_2)$.*

(ii) *Let F_1, F_2 be two EA-equivalent functions such that F_1 is not affine. Then, $d^o(F_1) = d^o(F_2)$.*

2.4.2 Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence)

We define next the Carlet-Charpin-Zinoviev equivalence, or CCZ-equivalence introduced in [10]. The notion of extended affine equivalence introduced previously in Section 2.4.1 as a special case of CCZ-equivalence.

Definition 2.4.3. *Let G_1 and G_2 be arbitrary groups. If $F : G_1 \to G_2$ be a function, then the graph of F is defined as*

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

Definition 2.4.4. *The relation $\sim$ defined on the set of functions $G_1 \to G_2$ such that $F_1 \sim F_2$ if and only if $K(G_{F_1}) = G_{F_2}$ for some affine permutation*

$$K : G_1 \times G_2 \to G_1 \times G_2$$

is an equivalence relation. Functions in the same equivalence class are Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent).

It is easy to see that EA-equivalence implies CCZ-equivalence. In other words, if two functions are EA-equivalent, then they are CCZ-equivalent. Since CCZ-equivalence classes are larger than EA-equivalence classes, showing CCZ-invariance of these parameters is a stronger result.

Corollary 2.4.1. *Let $F : G_1 \to G_2 \sim F_0 : G_1 \to G_2$. The properties of PN and APN are all invariant between F and F_0.*

Chapter 3

Deficiency and Ambiguity of Functions

In this Chapter 3, we are ready to define the notion of deficiency and ambiguity of a given bijection F on a finite Abelian group G. In the first section, we present the definitions of two generalized measures of $\Delta_{F,a}$, deficiency and ambiguity. In Section 3.2, we show lower bounds on these measures then we can define notions of optimality with respect to them. In Section 3.3, we aim to cover the deficiency and ambiguity of some permutations of the cyclic group Z_n, where $n = p^m - 1$. In Section 3.4, we review some results of deficiencies and ambiguities of known permutations over finite fields. All these result can be found in [47–50, 59].

3.1 Deficiency and Ambiguity

We study the injectivity and surjectivity of $\Delta_{F,a}$ when F is a bijection. Then we can understand how close a bijection F is to being an APN function. Moreover, we present two generalized measures of injectivity and surjectivity of $\Delta_{F,a}$;, respectively. By [47], we see that the definition does not require F to be a bijection.

Definition 3.1.1. *[47] Let G_1 and G_2 be finite Abelian groups of the same cardinality n and $F : G_1 \to G_2$. Let $G_1^* = G_1 \backslash 0$ and $G_2^* = G_2 \backslash 0$. For any $a \in G_1^*$ and $b \in G_2$, we*

denote

$$\Delta_{F,a}(x) = F(x+a) - F(x)$$

and

$$\gamma_{a,b}(F) = |\Delta_{F,a}^{-1}(b)|.$$

Let

$$\alpha_i(F) = |\{(a,b) \in G_1^* \times G_2 \mid \gamma_{a,b}(F) = i\}|$$

for $0 \leq i \leq n$. *Then* $\alpha_0(F)$ *is the deficiency of* F, *denoted by* $\mathfrak{D}(F)$ *and* $\mathfrak{A}(F)$ *is the (weighted) ambiguity of* F *defined as*

$$\mathfrak{A}(F) = \sum_{0 \leq i \leq n} \alpha_i(F) \binom{i}{2}.$$

Remark 3.1.1. *[47] Hence* $\mathfrak{D}(F) = \alpha_0(F)$ *measures the number of pairs* (a,b) *such that* $\Delta_{F,a}(x) = b$ *has no solutions. This is a measure of the surjectivity of* $\Delta_{F,a}$*; the lower the deficiency the closer the* $\Delta_{F,a}$ *are to surjective. Similarly, the weighted ambiguity of* F *measures the total replication of pairs of* x *and* x' *such that* $\Delta_{F,a}(x) = \Delta_{F,a}(x')$ *for some* $a \in G_1^*$. *This is a measure of the injectivity of the functions* $\Delta_{F,a}$*; the lower the ambiguity of* F *the closer the* $\Delta_{F,a}$ *are to injective.*

For a fixed a the values of $\Delta_{F,a}(x)$ are the entries in the a-th row of what is often referred to as the difference triangle of F, when the domain of F is $\mathbb{Z}$ [15], [23], or what we might call the difference array, when the domain of F is a finite group G. Thus for fixed a, we define the row a-ambiguity of F as

$$\mathfrak{A}_{r=a}(F) = \sum_b \binom{\gamma_{a,b}(F)}{2}.$$

These measure the injectivity of the individual $\Delta_{F,a}$. We also define the row a-deficiency as

$$\mathfrak{D}_{r=a}(F) = |\{b \mid \gamma_{a,b}(F) = 0, b \in G_2\}|,$$

which measures the number of b's such that $\Delta_{F,a}(x) = b$ has no solutions for a fixed

a. Likewise, we define the column b-ambiguity as

$$\mathfrak{A}_{c=b}(F) = \sum_{a} \binom{\gamma_{a,b}(F)}{2},$$

and the column b-deficiency as

$$\mathfrak{D}_{c=b}(F) = |\{a \mid \gamma_{a,b}(F) = 0, a \in G_1^*\}|,$$

which measures the number of a's such that $\Delta_{F,a}(x) = b$ has no solutions for a fixed b.

We reformulate the following results in [47] to remove the restriction on the co-domain.

Lemma 3.1.1. *[47] If $a \in G_1^*$, then we get*

$$\mathfrak{D}_{r=a}(F) = n - |\{\Delta_{F,a}(x) \mid x \in G_1\}|.$$

Lemma 3.1.2. *[47] Let $F : G_1 \to G_2$ be a bijection. If a row a-deficiency of F is equal to d, then row a-ambiguity of F satisfies*

$$d \leq \mathfrak{A}_{r=a}(F) \leq \binom{d+2}{2}.$$

Proof. Since $\mathfrak{D}_{r=a}(F) = n - |\{\Delta_{F,a}(x) \mid x \in G_1\}|$, the size of the value set

$$\{\Delta_{F,a}(x) \mid x \in G_1\}$$

is $n - d$ for a given row a-deficiency d. The maximum row a-ambiguity,

$$\mathfrak{A}_{r=a}(F) = \binom{d+2}{2}$$

occurs when the n images, $\Delta_{F,a}(x)$, are distributed with $n - 1 - d$ values of x giving distinct images and the remaining $d + 1$ values all agreeing to some values. The

minimum value,

$$\mathfrak{A}_{r=a}(F) = d,$$

occurs when the n images are distributed with d pairs of $\{x, x_0\}$ having $\Delta_{F,a}(x) = \Delta_{F,a}(x_0)$ and the remaining $n - 2d$ images are distinct. □

Lemma 3.1.3. *[47] Let F, $\bar{F} : G_1 \to G_2$ be bijections such that*

$$\bar{F} = A_1 \circ f \circ A_2 + A$$

where A_1, A_2, are bijective affine transformations and A is an affine transformation. Then for each pair (a, b) there exists a unique pair $(\bar{a}, \bar{b})$ such that

$$\gamma_{a,b}(F) = \gamma_{\bar{a},\bar{b}}(\bar{F}).$$

In particular, F and $\bar{F}$ have the same deficiency, ambiguity, and corresponding row deficiencies and row ambiguities.

Proof. It is clear that

$$\bar{F}(x + a) - \bar{F}(x) = b$$

is equivalent to

$$A_1 \circ (F \circ A_2(x + a) - F \circ A_2(x)) = b - A(a),$$

because A_1 and A are affine transformations. Using the bijectivity of A_1 and A_2, we obtain

$$\gamma_{a,b}(F) = \gamma_{\bar{a},\bar{b}}(\bar{F}),$$

where $\bar{a} = A_2(a)$ and $\bar{b} = A_1^{-1}(b - A(a))$. □

Definition 3.1.2. *Let G_1 and G_2 be finite Abelian groups of the same cardinality and $F : G_1 \to G_2$. Then, F is a perfect non-linear function if*

$$F(x + a) - F(x) = b,$$

has exactly one solution for all $a \neq 0 \in G_1$ and all $b \in G_2$. This corresponds again to zero ambiguity. This property is often too strong to require and particularly in the case of bijections F, it can never be satisfied. Thus a relaxed definition is frequently useful.

Definition 3.1.3. *[24] Let G_1 and G_2 be finite Abelian groups of the same cardinality and $F : G_1 \to G_2$. Then, F is an almost perfect non-linear function if*

$$F(x + a) - F(x) = b,$$

has at most two solutions for all $a \neq 0 \in G_1$ and all $b \in G_2$.

3.2 Bound for Deficiency and Ambiguity Between Two Abelian Groups

In this section, we present a lower bound on the deficiency and ambiguity of a bijection between two Abelian groups first obtained in [48] and reformulated in [47] by removing the restriction on the co-domain.

Theorem 3.2.1. *[47], [48] Let $F : G \to G$ be a permutation, where G is an Abelian group of order n. Let I be the set of elements of order 2 in G such that $\imath = |I|$. Then the deficiency and the ambiguity of F are bounded below by*

$$\begin{cases} 2(n-1) & n \equiv 1 \ (mod\ 2), \\ 2(n-2) & n \equiv 0 \ (mod\ 2) \text{ and } \imath_1 = \imath_2 = 1, \\ 2(n-1) - \frac{3\min\{\imath_1,\imath_2\}}{2} + \frac{\imath_1\imath_2}{2} & n \equiv 0 \ (mod\ 2) \text{ and } \imath_1\imath_2 > 1. \end{cases}$$

In the particular case $G_1 = G_2 = \mathbb{Z}_n$, we have the following corollary [50].

Corollary 3.2.1. *[47] Let $n \in \mathbb{N}$ and $F : \mathbb{Z}_n \to \mathbb{Z}_n$ be a bijection. The ambiguity of F is at least $2(n-1)$ when n is odd and $2(n-2)$ when n is even. The deficiency of F is at least $n-1$ if n is odd and at least $n-3$ when n is even.*

Functions that meet these bounds are of particular interest.

Definition 3.2.1. *If a permutation $F : G_1 \to G_2$ has an ambiguity equal to the lower bound from Theorem 3.2.1, then F has optimum ambiguity and similarly we define optimum deficiency for a permutation if it achieves the lower bound for the deficiency.*

Next we show that optimum ambiguity implies the APN property for bijections from G_1 and G_2. For the optimum ambiguity, all the sets $\Delta_{F,a}^{-1}(b)$ have cardinality at most two.

Corollary 3.2.2. *[47] Let G be a finite Abelian group. If a permutation $F : G \to G$ achieves the minimal ambiguity, then F is Almost Perfect Non-linear.*

Proof. Consideration of the forced equalities throughout the proof of Theorem 3.2.1 gives that the number of pairs of (a, b) such that $|\Delta_{F,a}^{-1}(b)| \geq 2$ is exactly the ambiguity and each inverse image has size zero, one or two. Thus F is APN [24]. □

Proposition 3.2.1. *[47] Let G_1, G_2 be finite Abelian groups of order n. If $F : G_1 \to G_2$ is any APN permutation such that $\Delta_{F,a}(x) = F(x + a) - F(x)$ is 2-to-1 mapping for all $x \in G_1$ with at most one exception and for any $a \in G_1^*$, then the deficiency of F is $(n-1)(\lfloor n/2 \rfloor - 1)$ and the ambiguity of F is $(n-1)\lfloor n/2 \rfloor$.*

Proof. Suppose $\Delta_{F,a}$ is 2-to-1 mapping for each $a \in G_1^*$, then n is even and the deficiency of F is $(n-1)(n/2-1)$ and the ambiguity of F is $(n-1)n/2$. However, if $\Delta_{F,a}$ is 2-to-1 mapping for all $x \in G_1$ with at most one exception and for each $a \in G_1^*$, then n is odd. In this case, the deficiency of F is $(n-1)((n-1)/2-1)$ and the ambiguity of F is $(n-1)(n-1)/2$. □

Corollary 3.2.3. *[47] Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a bijective APN, then it has optimum ambiguity and deficiency.*

Proof. Since we are working in finite fields of characteristic 2, the solutions of every equation come in pairs. It means that every equation such as $\Delta_{F,a}(x) = b$ has either exactly two solutions or no solution because F is an APN function. Based on the proof of Lemma 3.1.2 the minimum value, $\mathfrak{A}_{r=a}(F) = d+1$, happens only when the n images are distributed with $d+1$ pairs of $\{x, x_0\}$ having $\Delta_{F,a}(x) = \Delta_{F,a}(x_0)$ and the remaining

$n - 2(d+1)$ images are distinct. Hence, in this case we get $d = 2^{m-1} - 1$ and the sets $\Delta_{F,a}^{-1}(b)$ having cardinality zero and two are necessary when $\mathfrak{A}_{r=a}(F)$ achieves its minimum. Therefore, F has optimum ambiguity because every row has optimum row-a-ambiguity. Finally, since optimum ambiguity is stronger than optimum deficiency, F has optimum deficiency as well. □

Let $OA_F(G)$ and $OD_F(G)$ denote the optimum ambiguity and optimum deficiency of a permutation F on G, respectively. Let p be a prime number, $q = p^e$ and $\mathbb{F}_q$ denote the finite field of order q. If $G = (\mathbb{F}_q, +)$, then the deficiency and ambiguity depend on the characteristic p of $\mathbb{F}_q$. The following corollary is a simple consequence of the above theorem and the fact that every non-zero element of $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) = 2$, has order 2.

Corollary 3.2.4. *[48] The optimum deficiency and ambiguity of a permutation F over a finite field $\mathbb{F}_q$ is given in Table 3.2.1.*

Table 3.2.1: The Optimum Deficiency and Ambiguity of Permutations over $\mathbb{F}_q$ where $q = p$

	$OD_F(G)$	$OA_F(G)$
q odd	$2(q-1)$	$2(q-1)$
q even	$(q-1)(\frac{q}{2})$	$(q-1)(\frac{q}{2})$

Optimal functions with respect to ambiguity have the APN property. In other words, if a permutation $F : G \to G$ achieves the minimal ambiguity, then F is APN.

Theorem 3.2.2. *[48] Let $F : G \to G$ be a function with differential uniformity k. Suppose further that*

$$|G| = n = rk + s,$$

for some r, s with $0 \leq s < n$. Then the ambiguity of F satisfies

$$\binom{k}{2} \leq \mathfrak{A}(F) \leq (n-1)\left(r\binom{k}{2} + \binom{s}{2}\right),$$

and the deficiency of F satisfies

$$k - 1 \leq \mathfrak{D}(F) \leq (n-1)(n - r + \delta_s),$$

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

3.3 Ambiguity and Deficiency for Functions over the Multiplicative Group of $\mathbb{F}_q$

In this section, we review the ambiguities and deficiencies of functions given in [47]. These functions are defined over the multiplicative group of $\mathbb{F}_q$ and achieve the optimum bounds in the previous section. The idea is to obtain a permutation polynomial of fixed point 0 over a finite field $\mathbb{F}_q$ from another permutation polynomial of $\mathbb{F}_q$ which does not fix 0. Namely, let h be a permutation polynomial of $\mathbb{F}_q$ such that $h(0) = a \neq 0$ and $h(b) = 0$. Then we define g as

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

It is obvious that g is again a permutation polynomial of $\mathbb{F}_q$ which fixes 0. Then, twist of permutation polynomials can be used in constructing permutations of $\mathbb{Z}_n$ with optimum deficiency and ambiguity.

3.3.1 Functions Derived from Permutation Monomials

Theorem 3.3.1. *[47] 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

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

If $q \not\equiv 0 \pmod 3$ then $F : Z_n \to Z_n$ defined by $F(i) = log_\alpha(g(\alpha_i))$ has optimum deficiency. If additionally, $q \equiv 2 \pmod 3$ (i.e., q is an odd power of a prime p where $p \equiv 2 \pmod 3$), then F has optimum ambiguity as well.

If $q \equiv 1 \pmod 3$ then the ambiguity is $2(n-1)$ or $2n$ depending on whether q is odd or even, respectively. In these cases F is not APN. Also, if $q \equiv 0 \pmod 3$ then F has deficiency $n-2$ and ambiguity $2n-3$, both exactly one more than optimal. In this case, F is APN.

3.3.2 Möbius Function

Theorem 3.3.2. *[47] 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 $\beta, \gamma, \eta \neq 0$. If $q \not\equiv 0 \pmod 3$ then $F(i) = log_\alpha(g(\alpha_i))$ has optimum deficiency. Moreover, if $q \equiv 2 \pmod 3$ then F has optimum ambiguity. If $q \equiv 1 \pmod 3$ then the ambiguity is $2(n-1)$ or $2n$ depending on whether q is odd or even, respectively. Finally, if $q \equiv 0 \pmod 3$ then F has deficiency $n-2$ and ambiguity $2n-3$, both exactly one more than optimal.

3.4 Deficiency and Ambiguity of Known Polynomials over Finite Fields

In this section, we present some known results of permutations over finite fields and their deficiencies and ambiguities obtained in [47, 48]. In Subsection 3.4.1, we give the deficiencies and ambiguities of linearized polynomials. In Subsection 3.4.2, the inverse function over $\mathbb{F}_{2^m}$ are considered. In Subsection 3.4.3, APN monomials over a finite field $\mathbb{F}_{p^e}$ of characteristic $p > 2$ are addressed. In Subsection 3.4.4, we show how the authors of [48] derive a formula for the deficiencies and ambiguities of DO-polynomials in terms of ranks of matrices and survey these matrices for some specific DO permutations.

3.4.1 Linearized Polynomials

The deficiency and ambiguity of linearized polynomials is treated.

Lemma 3.4.1. *Let*

$$L(x) = \sum_{j=0}^{e-1} l_j x^{p^j}$$

be a linearized polynomial over $\mathbb{F}_q, q = p^e$. *Then*

$$\mathfrak{D}(L) = (q-1)^2$$

and

$$\mathfrak{A}(L) = (q-1)\binom{q}{2}.$$

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

$$\Delta_{L,a}(x) = L(x+a) - L(x) = \sum_{j=0}^{e-1} l(x+a)^{p^j} - \sum_{j=0}^{e-1} l_j x^{p^j}$$

$$= \sum_{j=0}^{e-1} l(x^{p^j} + a^{p^j}) - \sum_{j=0}^{e-1} l_j x^{p^j} = \sum_{j=0}^{e-1} l_j a^{p^j}.$$

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

$$b = \sum_{j=0}^{e-1} l_j a^{p^j},$$

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 $\mathbb{F}_q$, $n_0 = \mathfrak{D}(L) = (q-1)^2$ and $n_q = q-1$. Hence we get

$$\mathfrak{A}(L) = n_q \binom{q}{2} = (q-1)\binom{q}{2}.$$

□

3.4.2 Inverse Function Over Finite Fields of Even Characteristic

Let $q = 2^m$ and $F : \mathbb{F}_q \to \mathbb{F}_q$ be the inverse function defined as follows

$$F(x) = \begin{cases} x^{-1}, & x \neq 0; \\ 0, & x = 0. \end{cases}$$

It is easy to see that F is permutation function over $\mathbb{F}_q$ and $F(0) = 0$. We observe that the inverse function over finite field $\mathbb{F}_{2^8}$ is used in the S-box of AES.

Theorem 3.4.1. *[47] Let $q = 2^m$ and m odd. The inverse function $F(x) = x^{-1}$ over $\mathbb{F}_q^*$ has optimum deficiency and ambiguity. For even m, the deficiency and ambiguity are*

$$\mathfrak{A}(F) = (2^m - 1)(2^{m-1} + 4),$$

and

$$\mathfrak{D}(F) = (2^m - 1)2^{m-1}.$$

Remark 3.4.1. *[47] By Theorem 3.4.1, for $a \neq 0$, the equation $x^2 + ax + a^2 = 0$ has solutions in $\mathbb{F}_{2^m}$ if and only if m is even. Now, we distinguish between two cases.*

(i) For even m, we have two distinct solutions to $x^2 + ax + a^2 = 0$ for every $a \neq 0$. Therefore, all the elements in $\mathbb{F}_{2^m}$ are 2 to 1 except one of them which is 4 to 1.

(ii) For odd m this function is APN and Corollary 3.2.3 applies.

3.4.3 APN Monomials Over Finite Fields of Odd Characteristic

We present the ambiguity and deficiency results for a list of APN monomials functions over a finite field $\mathbb{F}_{p^e}$ of characteristic $p > 2$ that was obtained in [47].

Theorem 3.4.2. *[47] Let F be one of the APN permutations in Table 3.4.1 over $\mathbb{F}_q$ where $q = p^e$. Then the deficiency of F is $(q-1)\frac{q-3}{2}$ and the ambiguity of F is $(q-1)\frac{q-1}{2}$.*

Table 3.4.1: Four APN Functions x^d Over Finite Fields $\mathbb{F}_{p^e}$ of Odd Characteristic.

d	condition
3	$p \neq 3$
$p^e - 2$	$p > 2$ and $p^e \equiv 2 \pmod 3$
$\frac{2p^e-1}{3}$	$p^e \equiv 2 \pmod 3$
$\frac{p^k+1}{2}$	$p = 5$ and $(2e, k) = 1$

3.4.4 DO Polynomials

In this subsection, we study some known DO permutation polynomials.

Theorem 3.4.3. *[16] Let $F \in \mathbb{F}_q[x]$ with $deg(F) < q$. Then the following conditions are equivalent:*

(i) *$F = D + L + c$ where D is a DO polynomial, L is a linearized polynomial and $c \in \mathbb{F}_q$ is a constant;*

(ii) *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 (both depending on a).*

The main fact on the relation between linearized polynomials and DO polynomials shows how to compute the ambiguity and deficiency of some DO permutation polynomials.

Theorem 3.4.4. *[37][p.362] For any linearized polynomial*

$$L(x) = \sum_{j=0}^{r-1} l_j x^{q^j} \in \mathbb{F}_{q^r},$$

denote by L the matrix

$$\begin{pmatrix} l_0 & l_{r-1}^q & \dots & l_1^{q^{r-1}} \\ l_1 & l_0^q & \dots & l_2^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ l_{r-1} & l_{r-2}^q & \dots & l_0^{q^{r-1}} \end{pmatrix}. \tag{3.4.1}$$

Then L is a permutation polynomial over $\mathbb{F}_{q^r}$ if and only if $det(L) \neq 0$. The rank of the same matrix in Equation (3.4.1) also provides the cardinality of the value set of L.

Corollary 3.4.1. *[14], [30] Let*

$$L(x) = \sum_{j=0}^{r-1} l_j x^{q^j} \in \mathbb{F}_{q^r},$$

be a linearized polynomial and let L be the matrix in Equation (3.4.1). Then the value set of L, V_L, satisfies

$$|V_L| = q^{rk(L)},$$

where $rk(L)$ denotes the rank of the matrix L, and the number of preimages of each image is given by $q^{r-rk(L)}$.

Theorem 3.4.5. *[48] Let F be a DO polynomial and let $\Delta_{F,a} = L_a + c_a$, for any $a \in \mathbb{F}_{q^r}^*$, as in Theorem 3.4.3. Furthermore, let L_a be the matrix corresponding to L_a given in Equation (3.4.1). The ambiguity and deficiency of F are respectively given by*

$$\mathfrak{A}(F) = \sum_{a \in \mathbb{F}_{q^r}^*} q^{rk(L_a)} \binom{q^{r-rk(L_a)}}{2},$$

$$\mathfrak{D}(F) = \sum_{a \in \mathbb{F}_{q^r}^*} \left(q^r - q^{rk(L_a)}\right).$$

We now present the ambiguity and deficiency of DO permutation polynomials coming from Theorem 2.2.6.

Theorem 3.4.6. *[48] Let k be any integer and set $d = (k, e)$. Suppose $F \in \mathbb{F}_{2^e}[x]$ is a DO polynomial satisfying $F(x) = xL(x) = x^{2^k+1}$. Then*

$$\mathfrak{D}(F) = (2^e - 1)(2^e - 2^{e-d}),$$

and

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

If $d = 1$, then F is the APN Gold function over $\mathbb{F}_{2^e}$ which has optimal deficiency and ambiguity .

The pervious theorems involve analyzing the ranks of various forms of matrices which is similar to the following theorem.

Theorem 3.4.7. *[48] Let β be any primitive element of $\mathbb{F}_{2^e}$. Let either $e = 3k$ or $2e = 3k$ with $d = gcd(e, k) = e/3$. Also, let $F(x) = xL(x) \in \mathbb{F}_{2^e}[x]$ be a DO permutation polynomial, where $L(x) = x^{2^k} + cx^{2^{e-k}}$ and $c \neq \beta^{t(2^d-1)}$ for any integer t. Then, the deficiency of F is*

$$\mathfrak{D}(F) = 2^e(2^e - 1) - (2^e - 1)2^{2d},$$

and the ambiguity of F is

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

Theorem 3.4.8. *[48] Let β be any primitive element of $\mathbb{F}_{2^e}$ and 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

$$\mathfrak{D}(F) = 2^e(2^e - 1) - (2^e - 1)2^{2k}$$

and the ambiguity of F is

$$\mathfrak{A}(F) = (2^e - 1)2^{2k}\binom{2^k}{2}.$$

The matrix of Threorem 3.4.5 was used in [48] to give the deficiency and ambiguity of DO permutation polynomials coming from trace function given in Equation (2.2.3).

Theorem 3.4.9. *[48] Let $s \in \mathbb{F}_q \backslash \{0, 1\}$ and $F(x) = x(Tr(x) + sx)$ be the DO permutation polynomial over $\mathbb{F}_{q^r}$ for even q and odd r. Then the deficiency of F is*

$$\mathfrak{D}(F) = q^r(q^r - 1) - (q^r - q^{r-1})q^{r-1} - (q^r - q)$$

and the ambiguity of F is

$$A(F) = \left(q^r - q^{r-1}\right) q^{r-1}\binom{q}{2} + (q^r - q)\binom{q^{r-1}}{2}.$$

Theorem 3.4.10. *[48] Let $1 \leq k \leq e - 1$ and $1 \leq s \leq 2^e - 2$. Let*

$$F(x) = x^{2^k} + x + Tr(x^s) \in \mathbb{F}_{2^e}[x],$$

where e is odd, $gcd(k, e) = 1$ and s has 2-weight 1 or 2. If s has 2-weight 1, then the deficiency and ambiguity are respectively given by

$$\mathfrak{A}(F) = (2^e - 1)\binom{2^e}{2},$$

$$\mathfrak{D}(F) = 2^e(2^e - 1) - (2^e - 1) = (2^e - 1)^2.$$

If s has 2-weight 2, then the deficiency and ambiguity are respectively given by

$$\mathfrak{A}(F) = (2^{e+1} - 2^2)\binom{2^{e-1}}{2} + \binom{2^e}{2},$$

$$\mathfrak{D}(F) = 2^e(2^e - 1) - (2^{e+1} - 2^2) - 1.$$

Theorem 3.4.11. *[48] Let $F(x) = x + Tr(x^s) \in \mathbb{F}_{2^e}[x]$, where e is even and s has 2-weight 1 or 2. The deficiency and ambiguity of F are respectively given when s has 2-weight 1 .*

$$\mathfrak{A}(F) = (2^e - 1)\binom{2^e}{2},$$

$$\mathfrak{D}(F) = (2^e - 1)^2,$$

and when s has 2-weight 2 as following

$$\mathfrak{A}(F) = \left(2^{e+1} - 2^3\right)\binom{2^{e-1}}{2} + 3\binom{2^e}{2},$$

$$\mathfrak{D}(F) = 2^e(2^e - 1) - \left(2^{e+1} - 2^3\right) - 3.$$

Chapter 4

Deficiency and Ambiguity of Low Degree Permutation Polynomials

In Chapter 3.4, we presented the deficiency and ambiguity of several permutation polynomials of some special forms. The list of all normalized permutation polynomials of degree less than or equal to 5 is given in Table 2.2.1. However, the deficiency and ambiguity of these low degree permutation polynomials are not even formally studied. In this chapter we aim to study their deficiency and ambiguity. In particular, we use SAGE to compute these values when the field sizes are small and we formulate some conjectures based on the observation of our data.

Table 4.0.1: List of Normalized Permutation Polynomials of Low Degree.

	Permutation Polynomials	*any* q
1	x^2	$q \equiv 0 \pmod 2$
2	x^3	$q \not\equiv 1 \pmod 3$
3	$x^3 - wx \quad w$ not square	$q \equiv 0 \pmod 3$
4	$x^4 \pm 3x$	$q = 7$
5	$x^4 + wx^2 + w^2x \quad$ if its only root in $\mathbb{F}_q$ is 0	$q \equiv 0 \pmod 2$
6	x^5	$q \not\equiv 1 \pmod 5$
7	$x^5 - wx \quad w$ not a forth root	$q \equiv 0 \pmod 5$
8	$x^5 + wx \quad$ where $w^2 = 2$	$q = 9$
9	$x^5 \pm 2x$	$q = 7$
10	$x^5 + wx^3 \pm x^2 + 3w^2x \quad w$ not square	$q = 7$
11	$x^5 + wx^3 + 3w^2x \quad w$ not square	$q = 13$
12	$x^5 - 2wx^3 + w^2x \quad w$ not square	$q \equiv 0 \pmod 5$
13	$x^5 + wx^3 + 5^{-1}w^2x \quad w$ arbitrary	$q \equiv 2, 3 \pmod 5$

In the following we study deficiency and ambiguity of the above classes of PPs.

(1) $F(x) = x^2 \in \mathbb{F}_q[x]$ **such that** $q \equiv 0$ **(mod** 2**):**

It is clear that $F(x) = x^2$ is a linearized PP and by Lemma 3.4.1, the deficiency and ambiguity of x^2 are $\mathfrak{D} = (q-1)^2$ and $\mathfrak{A} = (q-1)\binom{q}{2}$ respectively. We verified the formulas through SAGE for small q's up to 2^9; see Table A.0.2.

(2) $F(x) = x^3 \in \mathbb{F}_q[x]$ **such that** $q \not\equiv 1$ **(mod** 3**):**

Let us consider three cases:

(i) $q \equiv 0 \pmod 3$,

(ii) $q = 2^m$ and m is odd,

(iii) q is odd and $q \equiv 2 \pmod 3$.

Case (i): $F(x)$ is a linearized PP and thus its deficiency and ambiguity are $\mathfrak{D} = (q-1)^2$ and $\mathfrak{A} = (q-1)\binom{q}{2}$, respectively; see Table A.0.3 for a few examples.
Case (ii): $F(x) = x^3$ is an APN permutation over $\mathbb{F}_{2^m}$ where m is odd, thus it has an optimum deficiency and ambiguity, where the result can be found by Theorem 2.1.2 and Corollary 2.1.2; see Table A.0.4 for a few examples. However, we give a direct proof as follows. Consider

$$\Delta_{F,a}(x) = F(x+a) - F(x) = (x+a)^3 - x^3 = ax^2 + a^2x + a^3 = b.$$

That is,

$$ax^2 + a^2x + a^3 - b = 0 \tag{4.0.1}$$

We have $\mathrm{Tr}\left(\frac{(a^3-b)}{(a^3)}\right) = \mathrm{Tr}(1-ab) = 1 - \mathrm{Tr}(ab)$. For each fixed $a \neq 0$, there are $\frac{q}{2}$ b's such that $Tr(ab) = 1$ and there are $\frac{q}{2}$ b's such that $Tr(ab) = 0$. Hence by Theorem 2.1.2, for each fixed $a \neq 0$ there $\frac{q}{2}$ b's such that Equation (4.0.1) has two solutions and

no solutions respectively. Therefore, by Definition 3.1.1, the deficiency and ambiguity of $F(x)$ are both $\frac{q(q-1)}{2}$.

Case (iii): We need to find how many solutions to $\Delta_{F,a}(x) = b$ if q is odd and $q \equiv 2 \pmod 3$. We note that $\Delta_{F,a}(x) = F(x+a) - F(x) = (x+a)^3 - x^3 = 3ax^2 + 3a^2x + a^3 = b$. In this case, the discriminant of this quadratic equation is $(3a^2)^2 - 4(3a)(a^3 - b) = 9a^4 - 12a^4 + 12ab = -3a^4 + 12ab$.

Let $a \neq 0$ be fixed. There is a unique b such that $4b = a^3$ and $\Delta_{F,a}(x) = b$ has a unique solution. There are $\frac{q-1}{2}$ b's such that $-3a^4 + 12ab$ is square and thus $\Delta_{F,a}x = b$ has two solutions. Similarly, there are $\frac{q-1}{2}$ b's such that $\Delta_{F,a}x = b$ has no solution. Therefore, by Definition 3.1.1, the deficiency and ambiguity of $F(x)$ are both $\frac{(q-1)^2}{2}$; see Table A.0.5.

(3) $F(x) = x^3 - wx \in \mathbb{F}_q[x]$**,** w **not square such that** $q \equiv 0$ **(mod** 3**):**

It is clear that $F(x) = x^3 - wx$ is a linearized PP and thus by Lemma 3.4.1 their deficiency and ambiguity are $\mathfrak{D} = (q-1)^2$ and $\mathfrak{A} = (q-1)\binom{q}{2}$, respectively.

(4) $F(x) = x^4 \pm 3x \in \mathbb{F}_7$**:**

Because we deal with a finite field of size 7, it is easy to compute the deficiency by computers. Indeed, we obtain that the deficiency and the ambiguity are both equal to 12. Thus, $F(x)$ has an optimum deficiency and ambiguity of permutation over $\mathbb{F}_q$ according to Table 3.2.1.

(5) $F(x) = x^4 + wx^2 + w^2x \in \mathbb{F}_q[x]$ **if its only root in** $\mathbb{F}_q$ **is 0 such that** $q \equiv 0$ **(mod** 2**):**

Obviously, $F(x) = x^4 + wx^2 + w^2x$ is a linearized PP. Then, by Lemma 3.4.1, the deficiency and ambiguity of $x^4 + wx^2 + w^2x$ are $\mathfrak{D} = (q-1)^2$ and $\mathfrak{A} = (q-1)\binom{q}{2}$,

respectively.

(6) $F(x) = x^5 \in \mathbb{F}_q[x]$ **such that** $q \not\equiv 1$ (**mod** 5) :

Essentially we need to study the number of solutions for the following equation:

$$\begin{aligned}\Delta_{F,a}(x) &= F(x+a) - F(x)\\ &= (x+a)^5 - x^5\\ &= 5ax^4 + 10a^2x^3 + a^3 + 10a^3x^2 + 5a^4x + a^5 + 3awx^3 + 3a^2wx + a^3w\\ &= b.\end{aligned}$$

Let us consider three cases:

(i) $q = 2^m$, m is even,

(ii) $q = 2^m$, m is odd,

(iii) q is odd, where $q \not\equiv 1 \pmod 5$.

Case (i): $F(x)$ over $\mathbb{F}_{2^m}$, where m is even, is APN Gold function. Then the deficiency is $(2^m - 1)(2^m - 2^{m-2})$ and ambiguity is $(2^m - 1)(2^{m-2})\binom{4}{2}$, by Theorem 3.4.6. In this case, $\gcd(2, m) = 2$.

Case (ii): $F(x) = x^5$ over $\mathbb{F}_{2^m}$, where m is odd, is APN Gold function. However, in this case, $\gcd(2, m) = 1$. By Theorem 3.4.6, the deficiency is $(2^m - 1)(2^m - 2^{m-1}) = (2^m - 1)2^{m-1}$ and ambiguity is $(2^m - 1)2^{m-1}$, thus both are optimal; see Table 3.2.1. and Table A.0.9 for concrete examples.

Case (iii): $F(x) = x^5$ over $\mathbb{F}_q$ for q odd and $q \not\equiv 1 \pmod 5$. In this case, we have done some experiments in SAGE for all prime numbers up to 293. From the data that we obtained, if $q \equiv 5$ *or* $7 \pmod 8$ and q is prime, the ambiguity of $F(x) = x^5 \in \mathbb{F}_q[x]$ is twice of the deficiency of F; see Table A.0.10.

(7) $F(x) = x^5 - wx \in \mathbb{F}_q[x]$**,** w **not a forth root such that** $q \equiv 0$ **(mod** 5**):**

Again, $F(x) = x^5 - wx$ is a linearized permutation polynomial over $\mathbb{F}_{5^m}$ and thus the deficiency and ambiguity are known by Lemma 3.4.1. Then $\mathfrak{D}(L) = \frac{q-1}{2}$ and $\mathfrak{A}(L) = (q-1)\binom{q}{2}$; see Table A.0.11.

(8) $F(x) = x^5 + wx \in \mathbb{F}_9$**,** $w^2 = 2$**:**

By SAGE, We calculate the deficiency and ambiguity of $F(x) = x^5 + wx$ over $\mathbb{F}_9$, where $w^2 = 2$. Then, the deficiency is 40 and the ambiguity is 72.

(9) $F(x) = x^5 \pm 2x \in \mathbb{F}_7$**, where** w **not square:**

By using over SAGE program, we can compute the deficiency and ambiguity of $F(x) = x^5 \pm 2x$ over $\mathbb{F}_7$, where w is not square. The deficiency is 12 and the ambiguity is 18; hence, $F(x)$ only has optimum deficiency.

(10) $F(x) = x^5 + wx^3 \pm x^2 + 3w^2 \in \mathbb{F}_7$**, where** w **is not square:**

In this case, by SAGE, the deficiency and the ambiguity are both 12; hence, F has optimum deficiency and ambiguity; see Table 3.2.1.

(11) $F(x) = x^5 + wx^3 + 3w^2x \in \mathbb{F}_{13}$**, where** w **is not square:**

In this case, by SAGE, the deficiency of $F(x)$ is 90 and the ambiguity is 210. Therefore, F does not have optimum deficiency and ambiguity.

(12) $F(x) = x^5 - 2wx^3 + w^2x \in \mathbb{F}_q$, w **not square such that** $q \equiv 0$ **(mod** 5**):**

We show that $\mathfrak{D} = \frac{(q-1)^2}{2}$, and $\mathfrak{A} = \frac{(q-1)^2}{2}$ in this case. Indeed,

$$\begin{aligned} & \Delta_{F,a}(x) = F(x+a) - F(x) \\ = \; & (x+a)^5 - 2w(x+a)^3 + w^2(x+a) - (x^5 - 2wx^3 + w^2x) \\ = \; & a^5 - 2w((x+a)^3 - x^3) + w^2a \\ = \; & -2w(3ax^2 + 3a^2x + a^3) + a^5 + w^2a \\ = \; & -awx^2 - wa^2x - 2wa^3 + a^5 + w^2a. \end{aligned}$$

We need to find how many solutions to $\Delta_{F,a}(x) = b$ if q is odd and $q \equiv 0 \pmod 5$. Then

$$x^2 + ax + a^2 - w - \frac{4a}{w} = \frac{b}{-aw}. \tag{4.0.2}$$

In this case, the discriminant of the quadratic Equation 4.0.2 is equal to $a^2 - 4(a^2 - w - \frac{a^4}{w} + \frac{b}{aw})$. Since w is fixed, for each fixed $a \neq 0$, there is a unique b such that $a^2 - 4(a^2 - w - \frac{a^4}{w} + \frac{b}{aw}) = 0$ and $\Delta_{F,a}(x) = b$ has a unique solution. There are $\frac{q-1}{2}$ b's such that $a^2 - 4(a^2 - w - \frac{a^4}{w} + \frac{b}{aw})$ is a square and thus $\Delta_{F,a}x = b$ has two solutions. Similarly, there are $\frac{q-1}{2}$ b's such that $\Delta_{F,a}x = b$ has no solution. Therefore, the deficiency and ambiguity of F are both $\frac{(q-1)^2}{2}$, by Definition 3.1.1; see Table A.0.12 for concrete examples.

(13) $F(x) = x^5 + wx^3 + 5^{-1}w^2x \in \mathbb{F}_q[x]$, w **arbitrary such that** $q \equiv 2, 3$ **(mod** 5**):**

We consider two cases:

(i) $q = 2^m$, m is odd,

(ii) q is odd, where $q \equiv 2, 3 \pmod 5$.

Case (i): $F(x) = x^5 + wx^3 + 5^{-1}w^2x$ over $\mathbb{F}_{2^m}$, where m is odd. We use SAGE to compute the deficiency and ambiguity of F for q's up to 2^9, but the values that we

got do not divide $q-1$. In addition, we could not find a pattern from our data; see Table A.0.13.

Case (ii): We compute the deficiency and ambiguity of $F(x) \in \mathbb{F}_q$ only for prime numbers q's up to 197. Moreover, we do not have any idea on how to find the explicit formula for the deficiency and ambiguity; see Table A.0.14.

Chapter 5

Conclusion

The main purpose of this thesis is to study the deficiency and ambiguity of all normalized permutation polynomials of degree smaller than or equal to 5. In Chapter 2, we review some basic facts of finite fields and permutation polynomials, as well as the definitions of almost perfect nonlinear functions, non-linearity, and equivalence of permutations. In Chapter 3, we present the definitions of deficiency and ambiguity of functions over finite abelian group and a general lower bound on the deficiency and ambiguity. We also review several special functions over multiplicative group of a finite field achieving these optimal lower bounds. Moreover, we review different methods of computing the deficiency and ambiguity of polynomials over finite fields. In particular, we review the method of calculating the deficiency and ambiguity of Dembowski-Ostrom polynomials based on analyzing matrices of a specific shape. In Chapter 4, we study ambiguity and deficiency of normalized permutation polynomials of degree smaller than or equal to 5. We are able to obtain the explicit numbers of ambiguity and deficiency for eleven classes of permutation polynomials in Table 4.0.1. We verified these formulas using SAGE program over finite fields of small sizes. For the remaining two classes, we can only obtain some preliminary computer results over finite fields of small sizes. However, we do not know how to obtain general formulae for these classes. It would be interesting to completely determine ambiguity and deficiency of normalized permutation polynomials of low degree. More generally, the problem of

classifying all deficiency and ambiguity is wide open. Even the case of classifying all the power functions is still unresolved.

Appendix A

Results of Deficiency and Ambiguity on Low Degree Permutation Polynomials

In Table A.0.1, we present the deficiencies and ambiguities of all the normalized PPs of low degree less or equal to 5 over finite fields. Moreover, we highlight all the optimum deficiencies and ambiguities. Then, by using SAGE, we compute all the normalized PPs of low degree one by one in different tables as concrete examples. Now, we present the code to compute the deficiency and ambiguity by SAGE as following:

$m =$

$p =$

$q = p^m$

$K. < w >= GF(p^(m))$

$P. < x >= K[x]$

def $f(x)$:

return

p^m

Def = 0

Amb = 0

for a in K :

if $a! = 0$:

val = []

for x in K :

val.append($f(x + a) - f(x)$)

#val

rowD = $q-$ Set(val).cardinality()

#print "row deficiency is", rowD

Def = Def + rowD

mult = []

for b in K :

mult.append(val.count(b))

#mult

rAmb = 0

S = set(mult)

for k in S :

alpha = mult.count(k)

#alpha

rAmb = rAmb + alpha$*$binomial($k, 2$)

#print "row ambiguity is", rAmb

Amb = Amb+rAmb

print "Deficiency is ", Def

print "Ambiguity is ", Amb

print Def/($q - 1$)

print Amb/($q - 1$)

f.close().

Table A.0.1: Examples of Deficiency and Ambiguity of Low Degree Normalised PPs

	Permutation Polynomials	*any* q	Deficiency	Ambiguity
1	x^2	$q \equiv 0 \pmod 2$	$(q-1)^2$	$(q-1)\binom{q}{2}$
2	x^3	$q \not\equiv 1 \pmod 3$		
		$q \equiv 0 \pmod 3$	$(q-1)^2$	$(q-1)\binom{q}{2}$
	when $p=2$, m is odd	$q \equiv 2 \pmod 3$	$\frac{\mathbf{q(q-1)}}{\mathbf{2}}$	$\frac{\mathbf{q(q-1)}}{\mathbf{2}}$
	when q is odd	$q \equiv 2 \pmod 3$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{2}$
3	$x^3 - wx$	$q \equiv 0 \pmod 3$	$(q-1)^2$	$(q-1)\binom{q}{2}$
	w not square			
4	$x^4 \pm 3x$	$q = 7$	**12**	**12**
5	$x^4 + wx^2 + w^2x$	$q \equiv 0 \pmod 2$	$(q-1)^2$	$(q-1)\binom{q}{2}$
	if its only root in $\mathbb{F}_q$ is 0			
6	x^5	$q \not\equiv 1 \pmod 5$		
	when $p=2$, m is even		$(q^m-1)q^{m-1}$	$(q^m-1)(q^{m-1})$
	when $p=2$, m is odd		$\frac{\mathbf{q(q-1)}}{\mathbf{2}}$	$\frac{\mathbf{q(q-1)}}{\mathbf{2}}$
	when $p>2$		?	?
7	$x^5 - wx$	$q \equiv 0 \pmod 5$	$(q-1)^2$	$(q-1)\binom{q}{2}$
	w not a forth root			
8	$x^5 + wx$	$q = 9$	40	72
	$w^2 = 2$			
9	$x^5 \pm 2x$	$q = 7$	**12**	18
10	$x^5 + wx^3 \pm x^2 + 3w^2x$	$q = 7$	**12**	**12**
	w not square			
11	$x^5 + wx^3 + 3w^2x$	$q = 13$	90	210
	w not square			
12	$x^5 - 2wx^3 + w^2x$	$q \equiv 0 \pmod 5$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{2}$
	w not square			
13	$x^5 + wx^3 + 5^{-1}w^2x$	$q \equiv 2, 3 \pmod 5$	?	?
	w arbitrary			

Table A.0.2: $x^2 \in \mathbb{F}_{2^m}$

$F(x) = x^2$				$q \equiv 0 \pmod 2$	
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^1}$	1	1	1	1	1
$\mathbb{F}_{2^2}$	3	9	18	3	6
$\mathbb{F}_{2^3}$	7	49	169	7	28
$\mathbb{F}_{2^4}$	15	225	1800	15	120
$\mathbb{F}_{2^5}$	31	961	15376	31	496
$\mathbb{F}_{2^6}$	63	3969	127008	63	2016
$\mathbb{F}_{2^7}$	127	16129	1032256	127	8128
$\mathbb{F}_{2^8}$	255	65025	8323200	255	32640
$\mathbb{F}_{2^9}$	511	261121	66846976	511	130816

Table A.0.3: $x^3 \in \mathbb{F}_{3^m}$ when $q \equiv 0 \pmod 3$

$F(x) = x^3$					$q \not\equiv 1 \pmod 3$
$\mathbb{F}_{3^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{3^1}$	2	4	6	2	3
$\mathbb{F}_{3^2}$	8	64	288	8	36
$\mathbb{F}_{3^3}$	26	676	9126	26	351
$\mathbb{F}_{3^4}$	80	6400	259200	80	3240
$\mathbb{F}_{3^5}$	242	58564	7115526	242	29403
$\mathbb{F}_{3^6}$	728	529984	193179168	728	265356

Table A.0.4: $x^3 \in \mathbb{F}_{2^m}$, where m is odd, when $q \equiv 2 \pmod 3$

$F(x) = x^3$					$q \not\equiv 1 \pmod 3$
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^1}$	1	1	1	1	1
$\mathbb{F}_{2^3}$	7	28	28	4	4
$\mathbb{F}_{2^5}$	31	496	496	16	16
$\mathbb{F}_{2^7}$	127	8128	8128	64	64
$\mathbb{F}_{2^9}$	511	130816	130816	256	256

Table A.0.5: $x^3 \in \mathbb{F}_q$, where q is odd, when $q \equiv 2 \pmod 3$

$F(x) = x^3$					$q \not\equiv 1 \pmod 3$
$\mathbb{F}_p$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_5$	4	8	8	2	2
$\mathbb{F}_{11}$	10	50	50	5	5
$\mathbb{F}_{17}$	16	128	128	8	8
$\mathbb{F}_{23}$	22	242	242	11	11
$\mathbb{F}_{29}$	28	392	392	14	14
$\mathbb{F}_{47}$	46	1058	1058	23	23
$\mathbb{F}_{53}$	52	1352	1352	26	26

Table A.0.6: $x^3 - wx \in \mathbb{F}_{3^m}$

$F(x) = x^3 - wx$, where w not square					$q \equiv 0 \pmod 3$
$\mathbb{F}_{3^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{3^1}$	2	4	6	2	3
$\mathbb{F}_{3^2}$	8	64	288	8	36
$\mathbb{F}_{3^3}$	26	676	9126	26	351
$\mathbb{F}_{3^4}$	80	6400	259200	80	3240
$\mathbb{F}_{3^5}$	242	8564	7115526	242	29403
$\mathbb{F}_{3^6}$	728	529984	193179168	728	265356

Table A.0.7: $x^4 + wx^2 + w^2x \in \mathbb{F}_{2^m}$

$F(x) = x^4 + wx^2 + w^2x$, if its only root in $\mathbb{F}_q$ is 0					$q \equiv 0 (\text{mod } 2)$
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^1}$	1	1	1	1	1
$\mathbb{F}_{2^2}$	3	9	18	3	6
$\mathbb{F}_{2^3}$	7	49	169	7	28
$\mathbb{F}_{2^4}$	15	225	1920	15	128
$\mathbb{F}_{2^5}$	31	961	15872	31	512
$\mathbb{F}_{2^6}$	63	3969	129024	63	2048
$\mathbb{F}_{2^7}$	127	16129	1056640	127	8320
$\mathbb{F}_{2^8}$	255	65025	8323200	255	32640
$\mathbb{F}_{2^9}$	511	261121	66977792	511	131072

Table A.0.8: $x^5 \in \mathbb{F}_{2^m}$ where m is even

$F(x) = x^5$				$q \not\equiv 1 \text{ (mod } 5)$	
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^2}$	3	9	18	3	6
$\mathbb{F}_{2^6}$	63	3024	6048	48	96
$\mathbb{F}_{2^{10}}$	1023	785664	1071328	768	1536

Table A.0.9: $x^5 \in \mathbb{F}_{2^m}$ where m is odd

$F(x) = x^5$				$q \not\equiv 1 \text{ (mod } 5)$	
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^1}$	1	1	1	1	1
$\mathbb{F}_{2^3}$	7	28	28	4	4
$\mathbb{F}_{2^5}$	31	496	496	16	16
$\mathbb{F}_{2^7}$	127	8128	8128	64	64
$\mathbb{F}_{2^9}$	511	130816	130816	256	256

Table A.0.10: $x^5 \in \mathbb{F}_q$ where q is odd

$F(x) = x^5$					$q \not\equiv 1 \pmod 5$
$\mathbb{F}_p$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_3$	2	4	6	2	3
$\mathbb{F}_7$	6	24	48	4	8
$\mathbb{F}_{13}$	12	84	168	7	14
$\mathbb{F}_{17}$	16	160	432	10	27
$\mathbb{F}_{19}$	18	216	540	12	30
$\mathbb{F}_{23}$	22	308	616	14	28
$\mathbb{F}_{29}$	28	476	952	17	34
$\mathbb{F}_{31}$	30	570	1140	19	38
$\mathbb{F}_{37}$	36	792	1584	22	44
$\mathbb{F}_{43}$	42	1134	2772	27	66
$\mathbb{F}_{47}$	46	1334	2668	29	58
$\mathbb{F}_{53}$	52	1664	3328	32	64
$\mathbb{F}_{59}$	58	2146	5220	37	90
$\mathbb{F}_{67}$	66	2772	6732	42	102
$\mathbb{F}_{73}$	72	3240	7992	45	111
$\mathbb{F}_{79}$	78	3822	7644	49	98
$\mathbb{F}_{83}$	82	4264	10332	52	126
$\mathbb{F}_{89}$	88	4840	11880	55	135
$\mathbb{F}_{97}$	96	5760	14112	60	147
$\mathbb{F}_{103}$	102	6528	13056	64	128
$\mathbb{F}_{107}$	106	7102	17172	67	162
$\mathbb{F}_{109}$	108	7236	14472	67	134
$\mathbb{F}_{113}$	112	7840	19152	70	171
$\mathbb{F}_{127}$	126	9954	19908	79	158
$\mathbb{F}_{137}$	136	11560	28152	85	207
$\mathbb{F}_{139}$	138	12006	28980	87	210
$\mathbb{F}_{149}$	148	13616	27232	92	184
$\mathbb{F}_{157}$	156	15132	30264	97	194
$\mathbb{F}_{163}$	162	16524	39852	102	246
$\mathbb{F}_{167}$	166	17264	34528	104	208
$\mathbb{F}_{173}$	172	18404	36808	107	214
$\mathbb{F}_{179}$	178	19936	48060	112	270
$\mathbb{F}_{193}$	192	23040	55872	120	291
$\mathbb{F}_{197}$	196	23912	47824	122	244
$\mathbb{F}_{199}$	198	24552	49104	124	248
$\mathbb{F}_{223}$	222	30858	61716	139	278
$\mathbb{F}_{227}$	226	32092	77292	142	342
$\mathbb{F}_{229}$	228	32376	64752	142	284
$\mathbb{F}_{233}$	232	33640	81432	145	351
$\mathbb{F}_{239}$	238	35462	70924	149	298
$\mathbb{F}_{257}$	256	40960	99072	160	387
$\mathbb{F}_{263}$	262	42968	85936	164	328
$\mathbb{F}_{269}$	268	44756	89512	167	334

Table A.0.10: $x^5 \in \mathbb{F}_q$ where q is odd

$F(x) = x^5$					$q \not\equiv 1 \pmod 5$
$\mathbb{F}_p$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{277}$	276	47472	94944	172	344
$\mathbb{F}_{283}$	282	49914	120132	177	426
$\mathbb{F}_{293}$	292	53144	106288	182	364

Table A.0.11: $x^5 - wx \in \mathbb{F}_{5^m}$

$F(x) = x^5 - wx$, where w is not forth root					$q \equiv 0 \pmod 5$
$\mathbb{F}_{5^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{5^1}$	4	16	40	4	10
$\mathbb{F}_{5^2}$	24	576	7200	24	300
$\mathbb{F}_{5^3}$	124	15376	961000	124	7750
$\mathbb{F}_{5^4}$	624	389376	121680000	624	195000

Table A.0.12: $x^5 - 2wx^3 + w^2x \in \mathbb{F}_{5^m}$

$F(x) = x^5 - 2wx^3 + w^2x$, where w not square					$q \equiv 0 \pmod 5$
$\mathbb{F}_{5^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{5^1}$	4	8	8	2	2
$\mathbb{F}_{5^2}$	24	288	288	12	12
$\mathbb{F}_{5^3}$	124	7688	7688	62	62
$\mathbb{F}_{5^4}$	624	194688	194688	312	312

Table A.0.13: $x^5 + wx^3 + 5^{-1}w^2x \in \mathbb{F}_{2^m}$ where m is odd

$F(x) = x^5 + wx^3 + 5^{-1}w^2x$, where w arbitrary					$q \equiv 2, 3 \pmod 5$
$\mathbb{F}_{2^m}$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_{2^1}$	1	1	1	1	1
$\mathbb{F}_{2^3}$	7	34	52	34/7	52/7
$\mathbb{F}_{2^5}$	31	616	976	616/31	976/31
$\mathbb{F}_{2^7}$	127	10144	16192	10144/127	16192/127
$\mathbb{F}_{2^9}$	511	163456	261376	163456/511	261376/511

Table A.0.14: $x^5 + wx^3 + 5^{-1}w^2x \in \mathbb{F}_q$ where q is odd

$F(x) = x^5 + wx^3 + 5^{-1}w^2x$, where w arbitrary					$q \equiv 2, 3 \pmod 5$
$\mathbb{F}_q$	$q-1$	Def	Amb	Def/$q-1$	Amb/$q-1$
$\mathbb{F}_3$	2	4	6	2	3
$\mathbb{F}_7$	6	24	44	4	22/3
$\mathbb{F}_{13}$	12	94	218	47/6	109/6
$\mathbb{F}_{17}$	16	164	370	41/46	185/8
$\mathbb{F}_{23}$	22	302	662	51/11	331/11
$\mathbb{F}_{37}$	36	820	1838	205/9	919/18
$\mathbb{F}_{47}$	46	1322	2906	661/23	9453/23
$\mathbb{F}_{53}$	52	1690	3770	65/2	145/2
$\mathbb{F}_{67}$	66	2772	5954	1361/33	2977/33
$\mathbb{F}_{73}$	72	3240	7236	45	201/2
$\mathbb{F}_{83}$	82	4222	9324	2111/41	4662/41
$\mathbb{F}_{97}$	96	5760	12816	60	267/2
$\mathbb{F}_{103}$	102	6528	14512	64	77256/51
$\mathbb{F}_{107}$	106	7048	15552	3524/53	7776/53
$\mathbb{F}_{113}$	112	7868	17410	281/4	8705/56
$\mathbb{F}_{127}$	126	9954	22084	79	11042/63
$\mathbb{F}_{137}$	136	11594	25630	341/4	12815/68
$\mathbb{F}_{157}$	156	15250	33698	7625/78	16849/78
$\mathbb{F}_{163}$	162	16402	36002	8201/81	18001/81
$\mathbb{F}_{167}$	166	17222	37886	8611/83	18943/83
$\mathbb{F}_{173}$	172	18490	40850	215/2	475/2
$\mathbb{F}_{193}$	192	23040	50976	120	531/2
$\mathbb{F}_{197}$	196	24010	53018	245/2	541/2

Bibliography

[1] A. Akbary, D. Ghioca, and Q. Wang, "On constructing permutations of finite fields", *Finite Fields Appl.* **17** (2011), 51-67.

[2] T. P. Berger, A. Carnteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions over $\mathbb{F}_2^n$", *IEEE Trans. Inform. Theory* **52** (2006), no. 9, 4160-4170.

[3] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe, "Permutations amongst the Dembowski-Ostrom polynomials", *Proc. 5th Int'l Conf. Finite Fields Appl.* 2001, 37-42.

[4] C. Blondeau, A. Canteaut and P. Charpin, "Differential properties of $x \to x^{2^{t-1}}$", *IEEE Trans. Inform. Theory* **57** (2011), 8127-8137.

[5] Eli Biham, Eimear Byrne, Nadya Markin and Gary McGuire, An infinite family of quadratic quadrinomial APN functions, Preprint, 2007.

[6] K. A. Browning, J. F. Dillon, M. T. Mcquistan, and A. J. Wolfe, "An APN permutation in dimension six", *Finite Fields Appl.* **518** (2010), 33-42.

[7] T. Beth and C. Ding, "On almost perfect nonlinear permutations", Advance in Cryptology-EUROCRYPT '93 (Lofthus, 1993) Lecture Note in Comput, Springer, Berlin, 1994, 56-76.

[8] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequence with there-valued crosscorrelation: a proof of Welch's conjecture", *IEEE Trans. Inform. Theory* **46** (2000), no 1, 4-8.

[9] A. Canteaue, weight divisiblity of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and corosscorrelation of maximum-lenght sequence, *SIAM J. Discrete Math.* **13** (2000), no 1, 105-138.

[10] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems", *Des. Codes Cryptogr.* **15** (1998), 125-156.

[11] C. Carlet, *Vectorial Boolean Functions for Cryptography*, chapter of the monograph Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. L. Hammer (eds.), Cambridge University Press, 2010, 398-468.

[12] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", Advance in cryptology-EUROCRYPT' 94 (Perugia), Lecture Notes in Comput. Sci. Springer, Berlin, **195** (1995), 356-365.

[13] P. Charpin and G. Kyureghyan, "On a class of permutation polynomials over $\mathbb{F}_{2^n}$", *SETA '08 Proc. 5th Int'l Conf. Sequences and Their Applications*, 2008, 368-376.

[14] W. S. Chou, J. Gomez-Calderon, G. L. Mullen, D. Panario, and D. Thomson, Subfield value sets of polynomials over finite fields, ???, 2013.

[15] C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs, Discrete Mathematics and its Applications*, CRC, Boca Raton, FL, second edition, 2007.

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

[17] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Part II, Ann. Math. 11 (1896-1897) 65-120.

[18] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case, *Inform. and Comput.* **151** (1999), no. 4, 127-1275.

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

[20] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: a new case divisible by 5, *Finite Fields and Applications, Springer*, Berlin, 2001, 133-121.

[21] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, and W. Willems, "APN function in odd characteristic", *Discrete Math.* **267** (2003), no. 13, 95-112.

[22] J. Daemen, and V. Rijmen, "The Design of Rijndael: AES-The Advanced Encryption Standard", Springer, 2002.

[23] K. Drakakis, "A review of Costas arrays", *J. Appl. Math., Art. ID* (2006), 26385, 32.

[24] K. Drakakis, R. Gow, and G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays", *Discrete Applied Math.* **157** (2009), no. 15, 3320-3326.

[25] K. Drakakis, V. Requena, and G. McGuire, "On the non-linearity of exponential Welch Costas functions", *IEEE Trans. Inform. Theory* **56** (2010), 1230-1238.

[26] P. Dembowski and T. G. Ostrom,"Planes of order n with collineation groups of order n", *Math. Z.* **2** (1968), 239-258.

[27] R. Gold, "Maximal recursive sequence with 3-valued recursive crosscorrelation functions (corresp.)", *IEEE Trans. Inform. Theory* **14** (1968), no. 1, 154-156.

[28] X. D. Hou and T. Ly, "Necessary conditions for reversed Dickson polynomials to be permutational", *Finite Fields Appl.* **16** (2010), 436-448.

[29] X. D. Hou, G. L. Mullen, J. A. Sellers, and J. Yucas, "Reversed Dickson polynomials over finite fields", *Finite Fields Appl.* **15** (2009), 748-773.

[30] X. D. Hou, "Solution to a problem of S. Payne", *Proc. of the American Mathematical Society*, **132** (2003), 1-6.

[31] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings", *IEEE Trans. Inform. Theory* **45** (1999), 475-485.

[32] H. D. L. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cress-correlations of binary m-sequence", *Finite Fields Appl.* **7** (2001), no. 2, 253-286.

[33] H. Iwaniec, E. Kowalski, *Analytic number theory*, AMS Colloquium Publications, 2004.

[34] H. Janwa and Richard M. Wilson, Hyperplane sections of Fermat varieties in $\mathbf{P^3}$ in char.2 and some applications to cyclic cods, Applied algebra, algebraic algorithms and error-correcting cods, Lecture Notes in Comput. sci., Springer, **673** (1993), 180-194.

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

[36] J. Li, D.B. Chandler, Q. Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, Finite Fields Appl. 16 (2010) 406-419.

[37] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, second edition, 1997.

[38] R. Lidl and G. L. Mullen, Unsolved problems: when does a polynomial over a finite field permute the elements of the field?, Amer. Math. Monthly. **95** (1988), 243-246.

[39] R. Lidl and G. L. Mullen, Unsolved problems: when does a polynomial over a finite field permute the elements of the field? II, Amer. Math. Monthly. **100** (1993), 71-74.

[40] J. Massey, "SAFER K64: A byte-oriented block-ciphering algorithm", Fast Software Encryption, pp. 117, 1993

[41] M. Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology EUROCRYPT '93, Lecture Notes Comput. Sci. **765** (1994), 386-397.

[42] G. L. Mullen. Permutation polynomials over finite fields. In Finite Fields, Coding Theory and Advances in Communications and Computing, 1993, 131-151.

[43] G. L. Mullen and H. Stevens, Polynomial functions (*mod m*), Acta Mathematica Hungarica **44** (1984), 237-241.

[44] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, 2013.

[45] G. L. Mullen and Q. Wang, *Premutation polynomails of one variable, in Handbook of Finite Fields*, Section 8.1, CRC, Boca Raton, 2013.

[46] K. Nyberg, Differentially uniform mapping for crypograph, Advances in cryptology-EUROCRYPT'(Lofthus,1993), Lecture Notes in Comput. Sci., Springer, Berlin, **765** (1994), 55-64.

[47] D. Panario, A. Sakzad, B. Stevens, D. Thomson and Q. Wang, "Two Measure for permutation polynomials: Ambiguity and Deficiency", *IEEE Trans. Inf. Theory* **57** (2011), no. 11, 7648-7657.

[48] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, "Ambiguity and deficiency of permutations over finite fields with linearized difference map", *IEEE Trans. Inf. Theory* 2013, 0018-9448.

[49] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, "Ambiguity and deficiency of permutations from finite fields", *IEEE Proc. Information Theory Workshop (ITW)*, 2011, 165-169

[50] D. Panario, B. Stevens, and Q. Wang, Ambiguity and deficiency in Costas arrays and APN permutations, Lecture Notes Comput. Sci. **6034** (2010), 397-406.

[51] G. Raussnitz. Zur theorie der congruenzen höheren grades. Math. Naturwiss. Ber. Ungarn, 1883, 266278.

[52] L. Redei, Uber eindeuting umkehrbare polynome in endlichen kopern, Acta Scientarium Mathmematicarum, **11**, 85-92, 1946-48.

[53] R. L. Rivest, "Permutation polynomials modulo 2^w", *Finite Fields Appl.* **7** (2001), 287-292.

[54] A. Sakzad, M-R. Sadeghi, and D. Panario,"Cycle structure of permutation functions over finite fields and their applications", *Adv. Math. Comm.* **6** (2012), 347-361.

[55] A. Sakzad, D. Panario, M-R. Sadeghi, and N. Eshghi, "Self-inverse interleavers based on permutation functions for turbo codes", *IEEE Proc. 48th Ann. Allerton Conf. on Communication, Control, and Computing*, (Allerton, Monticello, IL, USA), 2010, 22-28.

[56] J. Sun and O. Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings", *IEEE Trans. on Inform. Theory* **51** (2005), 101-119.

[57] SAGE Mathematics Software, Version 4.3 [Online]. Available: http://www.sagemath.org/

[58] C. Shallue and I. M. Wanless, Permutation polynomials and orthomorphism polynomials of degree six. Finite Fields Appl. 20 (2013), 84-92.

[59] D. Thomson, On difference maps and their cryptographic applications, PhD.Thesis, Carleton University, 2012.

[60] G. Turnwald, "A new criterion for permutation polynomials", *Finite Fields Appl.* 1995, 1:64-82.

[61] J. von zur Gathen, Tests for permutation polynomials, SIAM J. Comput. 1991, 591-602.

[62] Z. Wan, *Finite Fields and Galois Rings*, World Scientific Bublishing Co. Rteltd, 2003.