ON EXCEPTIONAL ALMOST PERFECT NON-LINEAR FUNCTIONS

by
NİHAL YURDAKUL

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Spring 2021

ON EXCEPTIONAL ALMOST PERFECT NON-LINEAR FUNCTIONS

APPROVED BY

DATE OF APPROVAL:

"In a hole in the ground there lived a hobbit. "

J.R.R. Tolkien

ON EXCEPTIONAL ALMOST PERFECT NON-LINEAR FUNCTIONS

Nihal Yurdakul

Mathematics, Master Thesis, 2021

Thesis Supervisor: Asst. Prof. Dr. Nurdagül Anbar Meidl

Keywords: Absolutely irreduciblity, APN functions, EA and CCZ equivalences, exceptional APN functions, finite fields

Abstract

In this master thesis, we study exceptional APN functions. We first give a detailed survey on exceptional APN monomials using the methods from algebraic geometry, especially algebraic curves over finite fields. We also collect recent results on exceptional APN polynomials, and we introduce a result for polynomials of Gold and Kasami-Welch types.

İstisnai APN Fonksiyonlar

Nihal Yurdakul

Matematik, Master Tezi, 2021

Tez Danışmanı: Dr. Öğr. Üyesi Nurdagül Anbar Meidl

Anahtar Kelimeler: APN fonksiyonlar, CCZ ve EA denklikleri, istisnai APN fonksiyonlar, mutlak indirgenemezlik, sonlu cisimler

Özet

Bu yüksek lisans tezinde, istisnai APN fonksiyonlarını çalıştık. Önce, isnisnai APN tek terimlileri üzerine ayrıntılı bir inceleme verdik, bu incelemeyi yaparken cebirsel geometriden, özellikle sonlu cisimler üzerine cebirsel eğrilerden yöntemler kullandık. Son olarak, istisnai APN polinomları hakkında sonu cları sunduk. Buna ek olarak Gold ve Kasami-Welch tipindeki polinomların hakkında bulduğumuz bir sonucu sunduk.

Acknowledgments

I would like to first say a huge thank you to my supervisor Asst. Prof. Dr. Nurdagul Anbar Meidl for all the support she gave me. My deep appreciation goes out to all my friends and professors at Sabanci University for their support and help. I would also like to say a heartfelt thank you to my family for their constant beliefs in me. At the last moment, my deepest thank you goes to my fiancé Murat, without his encouragement and his support this master thesis would not have been achievable.

Contents

Introduction

An interesting class of functions defined over $\mathbb{F}_{2^n}$ are Almost Perfect Non-Linear (APN) functions. They are of central interest in many mathematical areas such as coding theory and cryptography. In particular, having optimal differential properties, they provide good resistance against differential attacks in cryptography, see [3].

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n. Consider the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. To define an APN function, we need to define the derivative of a function over $\mathbb{F}_{2^n}$. For a non-zero $a \in \mathbb{F}_{2^n}$, the derivative of F with respect to a is $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by

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

Now, we are allowed to define APN function. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called APN, if $D_aF(x) = b$ has at most 2 solutions for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$. That is, $F(x + a) + F(x) = b$ has either 0 or 2 solutions for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$. Equivalently, a function F on $\mathbb{F}_{2^n}$ is APN if and only if for any nonzero $a \in \mathbb{F}_{2^n}$ the set $\{D_aF(x) \mid x \in \mathbb{F}_{2^n}\}$ has cardinality 2^{n-1}.

An APN function F over $\mathbb{F}_{2^n}$ is called exceptional APN if F is also APN over infinitely many extensions of $\mathbb{F}$. This thesis is about the conjecture on exceptional APN functions over $\mathbb{F}_{2^n}$, see [14] where the proof of the conjecture is completed for the monomial case. The conjecture states that the only exceptional APN functions are the Gold and Kasami-Welch monomial functions which are x^{2^i+1} and $x^{4^i-2^i+1}$, respectively.

The method from algebraic geometry, especially algebraic curves over finite fields are used to show the monomials other than Gold and Kasami-Welch are not exceptional APN. For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we define a Fermat surface $\mathcal{C}$ over $\mathbb{F}_{2^n}$ by $F(x) + F(y) + F(z) + F(x + y + z)$ [15]. We use the fact which states F is APN if and only if the affine surface $F(x) + F(y) + F(z) + F(x + y + z) = 0$ has all rational points on the surface defined by $(x + y)(y + z)(x + z)$, to decide whether F is APN. If the surface $\mathcal{C}$ has a rational point $P = (x, y, z)$ such that P does not lie on $x = y$, $y = z$ and $x = z$, then F is not APN. To have such a rational point, we determine whether $\mathcal{C}$ has a hyperplane section containing an absolutely irreducible curve $\mathcal{X}$ defined over $\mathbb{F}_{2^n}$.

Suppose that $\mathcal{C}$ has such a hyperplane section then by the Hasse-Weil bound [15], we have

$$N(\mathcal{X}) \geq 2^n - \frac{(deg(\mathcal{X}) - 1)(deg(\mathcal{X}) - 2)}{2}\sqrt{2^n}.$$

Note that $N(\mathcal{X})$ is large enough, for all sufficiently large n. Since the planes $x = y$, $y = z$ and $x = z$ intersect with $\mathcal{X}$ at most $deg(\mathcal{X})$ points by Bezout's theorem [11], $N(\mathcal{X}) - 3deg(\mathcal{X}) > 0$ for all sufficiently large n. In other words, there exists a rational point $P = (x, y, z) \in \mathcal{X}$ such that $x \neq y$, $y \neq z$ and $x \neq z$. Therefore, F is not APN.

After preliminary chapter, we introduced APN functions and their properties. We explained the difference between an APN function and exceptional APN function giving two examples. In Chapter 3, we were interested in CCZ(Carlet-Charpin-Zinoviev) and EA(Extended Affine) equivalences which preserve APN property. In the consequent chapter, we introduced exceptional APN functions and we gave the complementary proof of the conjecture we stated above. For Chapter 5, we showed Gold and Kasami-Welch functions are exceptional APN functions using the method expanded in Chapter 4. In the last chapter, we exposed a survey on exceptional APN functions which are not monomials. In addition we introduced our contribution on exceptional APN polynomials of Gold and Kasami-Welch types.

Chapter 1

Preliminaries

1.1 Finite Fields

We begin this chapter giving the main definitions and properties of finite fields which will be needed in the rest of the thesis.

Definition 1.1.1. *A field is a set* $\mathbb{F}$ *with two operation* $+$ *and* $.$ *which satisfies following properties:*

- $\mathbb{F}$ *is an abelian group under* $+$ *with identity element* 0*.*
- $\mathbb{F} \setminus \{0\}$ *is an abelian group under* $.$ *with identity element* 1*.*
- x *distributes over* $+$*, i.e.,* $a_1.(a_2 + a_3) = a_1.a_2 + a_2.a_3$ *where* $a_1, a_2, a_3 \in \mathbb{F}$*.*

The *field* is *finite* means that the *field* contains finitely many elements.

Definition 1.1.2. *The characteristic of a field* $\mathbb{F}$*, denoted* $ch(\mathbb{F})$*, is defined to be the smallest positive integer* p *such that* $p.1_{\mathbb{F}} = 0$*, if such a* p *exists and is defined to be* 0 *otherwise.*

Definition 1.1.3. *The prime subfield of a field* $\mathbb{F}$ *is the subfield of* $\mathbb{F}$ *generated by the multiplicative identity* $1_{\mathbb{F}}$*, it is isomorphic to either* $\mathbb{Q}$ *or* $\mathbb{F}_p$*.*

Note that every field has a unique smallest subfield, called the prime subfield, which is the intersection of all its subfields.

Lemma 1.1.4. *[21, Lemma 1.2.1] Let* $\mathbb{F}$ *be a finite field and* K *be a subfield of* $\mathbb{F}$*. Suppose that* K *contains* q *elements. Then,* $\mathbb{F}$ *is a vector space over* K *and* $|\mathbb{F}| = q^n$ *where* n *is the dimension of* $\mathbb{F}$ *over* K*.*

Proof. First, we will show that $\mathbb{F}$ is a vector space over K. Since $\mathbb{F}$ is a field, $0 \in \mathbb{F}$. For $\alpha \in K$, it is also $\alpha \in \mathbb{F}$, then $\alpha a + b \in \mathbb{F}$ for any $a, b \in \mathbb{F}$ and $\alpha \in K$. Then, $\mathbb{F}$ is a vector space over K. Now, we will show that n is the dimension of $\mathbb{F}$ over K where $|\mathbb{F}| = q^n$ and $|K| = q$. Since $\mathbb{F}$ contains finitely many elements, we can choose a basis

$\mathcal{B} = \{\beta_1, \beta_2 \ldots, \beta_n\}$ for $\mathbb{F}$ over K. We write $a \in \mathbb{F}$ as a linear combination of the elements of $\mathcal{B}$, $a = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n$ where $a_i \in K$. Note that $(a_1, a_2, \ldots, a_n)$ is uniquely determined by a. Since $a_i \in K$, there are q choices for each a_i. Then, there are $q^n = |K|^n$ distinct sequences of coefficients. Hence, the dimension of $\mathbb{F}$ over K is n. □

Theorem 1.1.5. *[21, Theorem 1.2.2] Let $\mathbb{F}$ be a finite field. Then, $|\mathbb{F}| = p^n$ where p is the characteristic of $\mathbb{F}$ with $n \in \mathbb{Z}^+$.*

Corollary 1.1.6. *Let $\mathbb{F}$ be a finite field with q elements where $q = p^n$. Then, $\mathbb{F}$ is an extension of $\mathbb{F}_p$.*

Proof. Since $\mathbb{F}_q$ is finite, the characteristic of $\mathbb{F}$ is positive. That is, $\mathbb{F}$ contains a subfield K which is isomorphic to $\mathbb{F}_p$. Then, $\mathbb{F}$ is a finite extension of K of degree n, for some $n \in \mathbb{Z}^+$. By Lemma 1.1.4, we conclude that $|\mathbb{F}| = |K| = p^n$. □

Note that we can deduce from Theorem 1.1.5 that there is no finite field of order 6.

Lemma 1.1.7. *[21, Lemma 1.2.3] If $\mathbb{F}_q$ is the finite field of order q and $a \in \mathbb{F}_q$ with $a \neq 0$, then $a^{q-1} = 1$. Therefore, $a^q = a$ for all $a \in \mathbb{F}_q$.*

Proof. Let $a \in \mathbb{F}_q$ with $a \neq 0$. Since $a \neq 0$, a is a unit in $\mathbb{F}_q$ and there are $q - 1$ units in $\mathbb{F}_q$. Furthermore, the units in $\mathbb{F}_q$ form a multiplicative group of order $q - 1$. Note that any finite multiplicative subgroup of a field is cyclic. Then, the units in $\mathbb{F}_q$ form a cyclic group of order $q - 1$. By Lagrange's theorem, the multiplicative order of a divides $q - 1$. Thus, we have $a^{q-1} = 1$, and by multiplying both sides with a, we have $a^q = a$.

Lemma 1.1.8. *[21, Lemma 1.2.4] Let $\mathbb{F}_q$ be the finite field of order q. Then, $x^q - x$ splits into its linear factors in $\mathbb{F}_q[x]$ as*

$$\prod_{a \in \mathbb{F}_q} x - a.$$

Proof. Since $x^q - x$ has degree q, it can has at most q roots. By Lemma 1.1.7, we know that $a^q = a$ for all $a \in \mathbb{F}_q$. Then, a is a root of $x^q - x$, that is, $x - a$ is a factor of $x^q - x$ for all $a \in \mathbb{F}_q$. Hence, $x^q - x$ has q distinct roots and $x^q - x = \prod_{a \in \mathbb{F}_q} x - a$.

Theorem 1.1.9. *[21, Theorem 1.2.5](Existance and Uniqueness of a Finite Field) For any prime p and positive integer n, there exists a finite field of order p^n and any field of order $q = p^n$ is isomorphic to the splitting field of $x^q - x \in \mathbb{F}_p$.*

Proof. Let $q = p^n$, we consider $x^q - x \in \mathbb{F}_p[x]$. Let F be the splitting field of $x^q - x$ over $\mathbb{F}_p$. Since $x^q - x$ is separable polynomial, i.e., it has distinct roots, by Lemma 1.1.8, it has exactly q roots in the splitting field. Set $S = \{a \in F \mid a^q - a = 0\}$. S is a subfield of F containing all the roots of $x^q - x$. Then, $S = F$ by the definition of the splitting field. Hence, F is a field of order $q = p^n$. It gives us the uniqueness of this finite field, by the uniqueness of the splitting field of a polynomial. □

Theorem 1.1.10. *[21, Theorem 1.2.7] Let $\mathbb{F}_q$ be the finite field of order $q = p^n$. Then, every subfield of $\mathbb{F}_q$ has order p^m for some $m \in \mathbb{Z}^+$ with $m \mid n$. Conversely, if $m \in \mathbb{Z}^+$ with $m \mid n$, then there exists a unique subfield of $\mathbb{F}_q$ of order p^m.*

Proof. Let K be a subfield of $\mathbb{F}_q$ where $q = p^n$. K must contain p^m distinct elements for some $m \leq n$. Then, by Lemma 1.1.4, p^n must be a power of p^m. Thus m divides n.
Now, we will show that there exists a unique subfield of $\mathbb{F}_q$ of order p^m for $m \in \mathbb{Z}^+$ with $m|n$. Since $m|n$, the polynomial $x^{p^m} - x$ divides $x^{p^n} - x$. Then, we can write $x^{p^n} - x = (x^{p^m} - x)p(x)$ where $p(x) \in \mathbb{F}_q[x]$. That is, all roots of $x^{p^m} - x$ are roots of $x^{p^n} - x$. Thus, $\mathbb{F}_q$ should contain a splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$ which contains p^m distinct elements. By uniqueness of the splitting field of a polynomial, this subfield is unique. □

We can conclude from Theorem 1.1.10 that the finite field $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_{p^m}$ where $m|n$.

Lemma 1.1.11. *Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be the finite fields of orders p^n and p^m, respectively. Then,*

$$\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^r}$$

where $r = \gcd(n, m)$.

Proof. By Theorem 1.1.10, we know that $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$ is isomorphic to a finite field $\mathbb{F}_{p^s}$ where $s|m$ and $s|n$. Since r is the greatest common divisor of m and n, we have $s|r$. By the same theorem, $\mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^r}$, i.e., $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^r}$. Conversely, we know from Theorem 1.1.10 that $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^m}$ and $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^n}$, since $r|m$ and $r|n$. Then, $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$ □

Now, we will define *Trace* function and express the properties of Trace function.

Definition 1.1.12. *Let $\alpha \in \mathbb{F}_{q^n}$ where q is a prime power and $n \in \mathbb{Z}^+$. The Trace function of α, $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$, is defined as follows.*

$$Tr_n(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}}$$

Equivalently, $Tr_n(\alpha)$ is the sum of the conjugates of α.

Theorem 1.1.13. *[21, Theorem 1.4.4] The trace function, $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ satisfies the following properties.*

- $Tr_n(\alpha + \beta) = Tr_n(\alpha) + Tr_n(\beta)$ *where* $\alpha, \beta \in \mathbb{F}_{q^n}$.
- $Tr_n(c\alpha) = cTr_n(\alpha)$ *where* $\alpha \in \mathbb{F}_{q^n}$ *and c is a constant.*
- $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *is a linear function and it is onto.*
- $Tr_n(\alpha) = m\alpha$ *for* $\alpha \in \mathbb{F}_q$ *and* $m \in \mathbb{Z}_{\geq 0}$.
- $Tr_n(\alpha^q) = Tr_n(\alpha)$ *for any* $\alpha \in \mathbb{F}_{q^n}$

We will give a definition of a linear function on $\mathbb{F}_{2^n}$. It will be used in the following chapters.

Definition 1.1.14. *(Linear Function) Let L be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ where n is a positive integer. L is a linear function if*

$$L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$$

with $a_i \in \mathbb{F}_{2^n}$.

Note that

$$L(x+y) = L(x) + L(y)$$

for all $x, y \in \mathbb{F}_{2^n}$, since $(x+y)^{2^i} = x^{2^i} + y^{2^i}$.

Now, we can give the definition of an affine function on $\mathbb{F}_{2^n}$. A linear function L fixes 0, i.e., $L(0) = 0$ whereas an affine function need not do so. An affine function is the composition of a linear function with a translation, so while the linear part fixes 0 , the translation can map it somewhere else.

Definition 1.1.15. *(Affine Function) An affine function $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a function defined by*

$$A(x) = L(x) + d$$

where $d \in \mathbb{F}_{2^n}$ and L is a linear function on $\mathbb{F}_{2^n}$.

Theorem 1.1.16. *Lagrange's Interpolation Theorem Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function. Then, $F(x)$ can be written as follows.*

$$F(x) = \sum_{a \in \mathbb{F}_{p^n}} F(a)\Big(1 - (x-a)^{p^n-1}\Big)$$

Using Lagrange's interpolation formula, we can deduce that every function on the finite field $\mathbb{F}_q$ can be express as a unique polynomial of degree less than q.

One of the important theorem which will be used for some proofs in the thesis is Lucas' Theorem. It will be used in Chapter 4.

Theorem 1.1.17. *[Lucas' Theorem][20] Let a and b two integers and p be a prime. If $0 \leq a \leq b$ writing a and b in p-adic notation as $a = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n$ and $b = b_0 + b_1 p + b_2 p^2 + \ldots + b_n p^n$ where $0 \leq a_i, b_i < p$ with $b_n \neq 0$. Then,*

$$\binom{b}{a} \equiv \binom{b_r}{a_1}\binom{b_{r-1}}{a_{r-1}} \ldots \binom{b_1}{a_1}\binom{b_0}{a_0} \mod p$$

3

Chapter 2

Almost Perfect Non-Linear Functions

2.1 APN Functions

In this section, we will introduce almost perfect non-linear functions and some properties of these functions. Consider the finite field of characteristic 2, the field $\mathbb{F}_{2^n}$ where n is a positive integer. From now on, we will study on functions on $\mathbb{F}_{2^n}$. To define APN function on $\mathbb{F}_{2^n}$, we introduce a derivative of a function over a finite field of characteristic 2 as follows.

Definition 2.1.1. *Let $n \in \mathbb{Z}_{>0}$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For any $a \in \mathbb{F}_{2^n}$, the derivative of F at a, is $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by*

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

Before stateting the definition of APN function we will make some observations on the equation $D_aF(x) = b$ where $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$.

Observation 2.1.2. *Consider the derivative of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ at $a \in \mathbb{F}_{2^n}$. Let x_0 be a solution of $D_aF(x) = b$. Letting $y_0 = x_0 + a$, we have the following equalities.*

$$\begin{aligned} D_aF(y_0) &= F(y_0 + a) + F(y_0) \\ &= F(x_0 + a + a) + F(x_0 + a) = F(x_0) + F(x_0 + a) \\ &= D_aF(x_0) = b \end{aligned}$$

Thus, we observe that if $D_aF(x) = b$ has a solution, namely $x = x_0$, then $x = x_0 + a$ is also a solution.

Observation 2.1.3. *Let $\{x_0, x_1, x_2\}$ be the set of solutions of $D_aF(x) = b$ where x_0, x_1, x_2 are distinct and $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. We observed above that $x_0 + a$ is a solution whenever x_0 is a solution of $D_aF(x) = b$. Without loss of generality, say $x_1 = x_0 + a$. Then, the set of solutions became $\{x_0, x_0 + a, x_2\}$. But, we know also that $x_2 + a$ is a solution whenever x_2 is a solution. If $x_2 + a = x_0$, then $x_2 = x_0 + a = x_1$. Similarly, if $x_2 + a = x_0 + a$ then $x_2 = x_0$. Hence, it is a contradiction. Then,*

the equation $D_aF(x) = b$ cannot have three distinct solutions. The set of solutions of the equation $D_aF(x) = b$ is distinct union of the sets $\{x_i, x_i + a\}$.

We can observe that the image of D_aF has even number of elements, since it is distinct union of sets with two elements.

After making above observations on the derivative of a function F, we define APN function as follows.

Definition 2.1.4. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. If*

$$D_aF(x) = F(x + a) + F(x) = b$$

is 2- to- 1 for all $a \neq 0$ and $b \in \mathbb{F}_{2^n}$, then F is APN. That means $F(x+a)+F(x) = b$ has 0 or 2 solutions for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$.

To give an other description to be an APN function, we can look at the following proposition.

Proposition 2.1.5. *Let F be any function on $\mathbb{F}_{2^n}$. Then, F is APN if and only if for any nonzero $a \in \mathbb{F}_{2^n}$ the set $\{D_aF(x) \mid x \in \mathbb{F}_{2^n}\}$ has cardinality 2^{n-1}.*

Proof. By Observation 2.1.3, we know that the cardinality of the image of $D_aF(x)$ is an even number and it is distinct union of the sets with two elements. We know also that F is APN if and only if $D_aF(x) = b$ has none or two solutions for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Then, there is at most one set $\{x_i, x_i + a\}$ for every $b \in \mathbb{F}_{2^n}$ where $D_aF(x) = b$. Denote by $Im(D_aF(x))$ the image of $D_aF(x)$. Then, for every $b \in Im(D_aF(x))$, there are exactly two elements $x_i, x_i + a$ such that $D_aF(x_i) = D_aF(x_i + a) = b$. Hence, F is APN if and only if $|\{D_aF(x) \mid x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$. □

2.2 Exceptional APN Functions

We are going to introduce some functions which are APN under some conditions and we will make observations on these APN functions. One of these functions is *the Gold function*. The Gold function is a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F(x) = x^{2^i+1}$. We will show that it is APN if and only if $\gcd(i, n) = 1$. The other function is called *the inverse function*, it is defined by $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$. We will also show that the inverse function is also APN on $\mathbb{F}_{2^n}$ if and only if n is an odd integer. Now, we will prove a few facts which will be used in the proof.

Definition 2.2.1. *Let F be a function on $\mathbb{F}_{2^n}$ where n is a positive integer. F is a quadratic function if*

$$F(x) = \sum_{\substack{i,j \in \{0,\ldots,n-1\} \\ i<j}} a_{i,j} x^{2^i+2^j} + \sum_{k=0}^{n-1} b_k x^{2^k} + c.$$

Fact 2.2.2. *Let F be a function on $\mathbb{F}_{2^n}$. If F is a quadratic function then $D_aF(x)$ is an affine function where $a \in \mathbb{F}_{2^n}$, $a \neq 0$.*

Proof. Suppose that F is a quadratic function from $\mathbb{F}_{2^n}$ to itself. By definition of the quadratic function, we can write

$$F(x) = \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} + \sum_{k=0}^{n-1} b_k x^{2^k} + c.$$

We have following equalities.

$$\begin{aligned}
D_aF(x) &= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}(x+a)^{2^i+2^j} + \sum_{k=0}^{n-1} b_k(x+a)^{2^k} + c \\
&\quad + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} + \sum_{k=0}^{n-1} b_k x^{2^k} + c \\
&= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}(x+a)^{2^i}(x+a)^{2^j} + \sum_{k=0}^{n-1} b_k(x+a)^{2^k} \\
&\quad + \sum_{k=0}^{n-1} b_k x^{2^k} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j}.
\end{aligned}$$

Since $(x+a)^{2^i} = x^{2^i} + a^{2^i}$, we have the following equalities:

$$\begin{aligned}
D_aF(x) &= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}(x^{2^i} + a^{2^j})(x^{2^j} + a^{2^j}) + \sum_{k=0}^{n-1} b_k(x^{2^k} + a^{2^k}) \\
&\quad + \sum_{k=0}^{n-1} b_k x^{2^k} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} \\
&= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}(x^{2^i} + a^{2^i})(x^{2^j} + a^{2^j}) + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} \\
&\quad + \sum_{k=0}^{n-1} b_k a^{2^k} \\
&= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}(x^{2^i+2^j} + x^{2^i}a^{2^j} + x^{2^j}a^{2^i} + a^{2^i+2^j}) \\
&\quad + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i}a^{2^j} \\
&+ \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^j}a^{2^i} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}a^{2^i+2^j} \\
&+ \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k} \\
&= \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i}a^{2^j} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^j}a^{2^i} \\
&+ \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}a^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k}.
\end{aligned}
$$

Since $\sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i}a^{2^j}$ and $\sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^j}a^{2^i}$ are linear functions on $\mathbb{F}_{2^n}$ and $\sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}a^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k}$ is a constant, $D_aF(x)$ is the sum of two linear functions and a constant, which means $D_aF(x)$ is an affine function. □

Corollary 2.2.3. *Let F be a function on $\mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. If $F(x)$ is a quadratic function then $D_aF(x) = b$ has at most two solutions if and only if $D_aF(x) + F(a) + F(0) = 0$ has exactly two solutions.*

Proof. Let $F(x)$ be a quadratic function, i.e., $F(x) = \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i+2^j} \sum_{k=0}^{n-1} b_k x^{2^k} + c$. Then by Fact 2.2.2,

$$
\begin{aligned}
D_aF(x) + F(a) + F(0) = &\sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i}a^{2^j} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^j}a^{2^i} \\
&+ \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}a^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k} \\
&+ \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i\leq j}} a_{i,j}a^{2^i+2^j} + \sum_{k=0}^{n-1} b_k a^{2^k} + c + c.
\end{aligned}
$$

Since characteristic is 2, we have the following equality.

$$
D_aF(x) + F(a) + F(0) = \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^i}a^{2^j} + \sum_{\substack{i,j\in\{0,\ldots,n-1\}\\ i<j}} a_{i,j}x^{2^j}a^{2^i}
$$

Then, $D_aF(x) + F(a) + F(0)$ is a linear function. If $D_aF(x) + F(a) + F(0) = 0$ has exactly two solutions then they should be $x = 0$ and $x = a$. Since $D_aF(x) + b = 0$ is a translation of $D_aF(x) + F(a) + F(0)$ and is a linear function, the solutions of $D_aF(x) + b = 0$ should be a translation of $x = 0$ and $x = a$. Then, $D_aF(x) + b = 0$

has at most two solutions, since a translation of $x = 0$ and $x = a$ must not be a solution of $D_aF(x) = b$. Conversely, suppose that $D_aF(x) + b = 0$ has at most two solutions. Choosing $b = F(a) + F(0)$, we can observe that $D_aF(x) + F(a) + F(0) = F(x + a) + F(x) + F(a) + F(0) = 0$ has exactly two solutions, namely $x = a$ and $x = 0$. □

Fact 2.2.4. *Let n and k be positive integers. Then*

$$\gcd(2^n - 1, 2^k - 1) = 2^{\gcd(n,k)} - 1.$$

Proof. Let $s = \gcd(n, k)$ and $d = \gcd(2^n - 1, 2^k - 1)$ We know that $2^n \equiv 1 \bmod d$ and $2^k \equiv 1 \bmod d$, then $2^s = 2^{nt+kr}$ where $s = nt + kr$ for some integers t and r. We have $2^s = 2^{nt+kr} = (2^n)^t(2^k)^r \equiv 1 \bmod d$. Thus, $d \mid 2^s - 1$.
Conversely, we know that $s \mid n$ and $s \mid k$, then $2^n - 1 = 2^{sl} - 1$ and $2^k - 1 = 2^{sl'} - 1$ for some integer l and l'. We have

$$2^n - 1 = 2^{sl} - 1 = ((2^s)^l - 1) = (2^s - 1)(2^{s(l-1)} + \ldots + 1)$$

and

$$2^k - 1 = 2^{sl'} - 1 = ((2^s)^{l'} - 1) = (2^s - 1)(2^{s(l'-1)} + \ldots + 1).$$

Thus, $2^s - 1 \mid d$. Hence, we have the equality $\gcd(2^n - 1, 2^k - 1) = 2^{\gcd(n,k)} - 1$. □

Now, we are going to prove that the Gold function is APN under a necessary and sufficient condition.

Theorem 2.2.5. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^{2^i+1}$. Then, F is APN if and only if $\gcd(i, n) = 1$.*

Proof. Let a be a non-zero element from $\mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}$. Since $F(x)$ is a quadratic function, by Corollary 2.2.3, $D_aF(x) = b$ has at most two solutions if and only if $D_aF(x) + F(a) + F(0) = 0$ has exactly two solutions. It means that F is APN if and only if $D_aF(x) + F(a) + F(0) = 0$ has exactly two solutions. We have the following equalities.

$$\begin{aligned} D_aF(x) + F(a) + F(0) &= (x + a)^{2^i+1} + x^{2^i+1} + a^{2^i+1} \\ &= (x + a)^{2^i}(x + a) + x^{2^i+1} + a^{2^i+1} \\ &= (x^{2^i} + a^{2^i})(x + a) + x^{2^i+1} + a^{2^i+1} \\ &= x^{2^i+1} + ax^{2^i} + a^{2^i}x + a^{2^i+1} + x^{2^i+1} + a^{2^i+1} \\ &= ax^{2^i} + a^{2^i}x. \end{aligned}$$

We can observe that one of the solutions of $D_aF(x)+F(a)+F(0) = 0$ is $x = 0$. When $x \neq 0$ the equation $ax^{2^i} + a^{2^i}x = 0$ becomes $x^{2^i-1} = a^{2^i-1}$. That is, $\left(\frac{x}{a}\right)^{2^i-1} = 1$. Setting $y = \frac{x}{a}$, we have $y^{2^i-1} = 1$. Thus, $F(x)$ is APN on $\mathbb{F}_{2^n}$ if and only if $y^{2^i-1} = 1$ has a unique solution, namely $y = 1$. It is the case if and only if $\gcd(2^i-1, 2^n-1) = 1$, since $\mathbb{F}_{2^n}$ does not contain (2^i-1)-th root of unity if and only if $\gcd(2^i-1, 2^n-1) = 1$. By Fact 2.2.4, we know that $\gcd(2^i - 1, 2^n - 1) = 2^{\gcd(i,n)} - 1 = 1$. Hence, $F(x)$ is APN on $\mathbb{F}_{2^n}$ if and only if $\gcd(i, n) = 1$ for any $b \in \mathbb{F}_{2^n}$. □

At this moment, we are going to give the proof of APN property for inverse function after the following remark.

Remark 2.2.6. *Let $F(x) = x^t$ be a monomial function and $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Assume that $F(x+a) + F(x) = (x+a)^t + x^t = b$ has at most two solutions.*

$$(x+a)^t + x^t = a^t\left(\left(\frac{x}{a}+1\right)^t + \left(\frac{x}{a}\right)^t\right) = b \tag{2.2.1}$$

Setting $\tilde{x} = \dfrac{x}{a}$, we can say that Equation 2.2.1 has at most two solutions if and only if $a^t\Big((\tilde{x}+1)^t + \tilde{x}^t\Big) = b$ has at most two solutions. It is the case if and only if $(\tilde{x}+1)^t + \tilde{x}^t = \dfrac{b}{a^t}$ has at most two solutions. Hence, we can without loss of generality take $a = 1$ to check that $D_aF(x) = b$ has at most two solutions.

Theorem 2.2.7. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^{2^n-2}$ where n is an odd integer. Then F is APN.*

Proof. Let $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. We will show that $D_aF(x) = F(x+a) + F(x) = b$ has at most two solutions. Equivalently, we will show that $F(x+a)+F(x)+F(a) = b$ has at most two solutions.

$$F(x+a) + F(x) + F(a) = (x+a)^{2^n-2} + x^{2^n-2} + a^{2^n-2} = b$$

Note that $x = a$ and $x = 0$ are solutions if and only if $b = 0$. Hence, if $b \neq 0$, we can suppose that $x \neq a$ and $x \neq 0$.
Case 1: Consider $b = 0$. Since $x = a$ and $x = 0$ are solutions, suppose that $x \neq a$ and $x \neq 0$. Then, we have following equalities.

$$\begin{aligned} F(x+a) + F(x) + F(a) = \frac{1}{x+a} + \frac{1}{x} + \frac{1}{a} = 0 \\ \Leftrightarrow\ ax + a(x+a) + x(x+a) = 0 \\ \Leftrightarrow\ ax + ax + a^2 + x^2 + ax = 0 \\ \Leftrightarrow\ x^2 + ax + a^2 = 0. \end{aligned}$$

By remark above, we can without loss of generality take $a = 1$. Then we have the equation $x^2 + x + 1 = 0$.
Suppose that $\alpha \in \mathbb{F}_{2^n}$ is a root of $x^2 + x + 1$, i.e., $\alpha^2 + \alpha = 1$. We know that Tr_n is a linear function on $\mathbb{F}_{2^n}$. Then we have $Tr_n(\alpha^2 + \alpha) = Tr_n(\alpha^2) + Tr_n(\alpha)$. Observe that

$$\begin{aligned} Tr_n(\alpha^2) &= \alpha^2 + (\alpha^2)^2 + (\alpha^2)^{2^2} + \ldots + (\alpha^2)^{2^{n-1}} \\ &= \alpha^2 + \alpha^{2^2} + \alpha^{2^3} + \ldots + \alpha^{2^n} \\ &= \alpha + \alpha^2 + \alpha^{2^2} + \ldots + \alpha^{2^{n-1}} \\ &= Tr_n(\alpha). \end{aligned}$$

Thus, $Tr_n(\alpha^2+\alpha) = Tr_n(\alpha^2) + Tr_n(\alpha) = 0$. On the other hand, $Tr_n(\alpha^2+\alpha) = Tr_n(1)$ and $Tr_n(1) = n.1$. Since n is an odd integer, $Tr_n(1) = 1$ which is a contradiction. Hence, $F(x+a)+F(x)+F(a) = b$ has at most two solutions when $b = 0$.
Case 2: Consider $b \neq 0$. We know that $x = 0$ and $x = a$ are not solutions.

$$F(x+a)+F(x)+F(a) = \frac{1}{(x+a)} + \frac{1}{x} + \frac{1}{a} = b$$

$$\begin{aligned} &\Leftrightarrow\ ax + (x+a)a + ax(x+a) = bax(x+a) \\ &\Leftrightarrow\ a^2 + ax^2 + a^2x + abx^2 + a^2bx = 0 \\ &\Leftrightarrow\ (ba+a)x^2 + (a+ba^2)x + a^2 = 0. \end{aligned}$$

Since $a \neq 0$, we can cancel out a and we obtain

$$(b+1)x^2 + (1+ba)x + a = 0. \tag{2.2.2}$$

Since we have a degree two polynomial, it has at most two solutions. Hence, $F(x+a)+F(x)+F(a) = b$ has at most two solutions when $b \neq 0$. □

In the proof of Case 1, we have the polynomial x^2+x+1 and we have looked for a root α of this polynomial such that $\alpha^2+\alpha = 1$. We have obtained a contradiction by using the fact $Tr_n(1) = n.1 = 1$, since n is an odd integer. However, if n was an even integer, we couldn't obtain a contradiction, since $Tr_n(1) = 0$.

Fact 2.2.8. *Let $d \in \mathbb{F}_{2^n}$. $x^2+x+d = 0$ has a solution in $\mathbb{F}_{2^n}$ if and only if $Tr_n(d) = 0$.*

Proof. Suppose that $x^2+x+d = 0$ has a solution, namely $x = \alpha$. We have $\alpha^2+\alpha+d = 0$, i.e., $\alpha^2+\alpha = d$. In addition, we have $Tr_n(\alpha^2+\alpha) = Tr_n(d)$. Since Tr_n is a linear function, $Tr_n(\alpha^2+\alpha) = Tr_n(\alpha^2) + Tr_n(\alpha)$ and since $Tr_n(\alpha^2) = Tr_n(\alpha)$, we have $Tr_n(d) = 0$.

Conversely, suppose that $Tr_n(d) = 0$. We will show that there exists $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha^2+\alpha = d$. Consider the map $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $\phi(\alpha) = \alpha^2+\alpha$.

$$\phi(a+b) = (a+b)^2 + (a+b) = a^2+b^2+a+b = \phi(a)+\phi(b)$$

for $a, b \in \mathbb{F}_{2^n}$. That is, ϕ is a group homomorphism. Denote $Ker(\phi)$ is the kernel of ϕ.

$$\begin{aligned} Ker(\phi) &= \{x \in \mathbb{F}_{2^n} :\ \phi(x) = 0\} \\ &= \{x \in \mathbb{F}_{2^n} :\ x^2+x = 0\} \\ &= \{x \in \mathbb{F}_{2^n} :\ x^2 = x\} \\ &= \mathbb{F}_2 \end{aligned}$$

By the first isomorphism theorem $\mid Im(\phi) \mid = 2^{n-1}$. Note that $Im(\phi) \subseteq \{\beta \in \mathbb{F}_{2^n} :\ Tr_n(\beta) = 0\}$, since $Tr_n(\alpha^2+\alpha) = 0$. Now, we will show that $Im(\phi) = \{\beta \in \mathbb{F}_{2^n} :\ Tr_n(\beta) = 0\}$ using cardinality of these two sets, i.e., we will show that $\mid \{\beta \in \mathbb{F}_{2^n} :\ Tr_n(\beta) = 0\} \mid = 2^{n-1}$. Let N_0 and N_1 be the number of trace 0 elements

and trace 1 elements, respectively. Every elements in $\mathbb{F}_{2^n}$ satisfies

$$x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}} = 0$$

or

$$x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}} = 1$$

but not both. Since both of them have at most 2^{n-1} roots in $\mathbb{F}_{2^n}$, then $N_0 \leq 2^{n-1}$ and $N_1 \leq 2^{n-1}$. Since $Tr_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is an onto function, both 0 and 1 have preimages in $\mathbb{F}_{2^n}$. Therefore, $N_0 + N_1 = 2^n$. Hence, $N_0 = 2^{n-1}$ and $N_1 = 2^{n-1}$. Since $\mid \{\beta \in \mathbb{F}_{2^n} : Tr_n(\beta) = 0\} \mid = 2^{n-1}$, we have $Im(\phi) = \{\beta \in \mathbb{F}_{2^n} : Tr_n(\beta) = 0\}$. Hence, there exists an $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha^2 + \alpha = d$. □

Remark 2.2.9. *If n is an even integer then the inverse function $F(x) = x^{2^n-2}$ defined over $\mathbb{F}_{2^n}$ is not an APN function. The equation $F(x+a)+F(x)+F(a) = 0$ has exactly 4 solutions for a non-zero $a \in \mathbb{F}_{2^n}$. For example, for $a = 1$, $F(x+1)+F(x)+F(1) = 0$ has exactly 4 solutions, namely $x = 0$, $x = 1$, $x = \alpha$ and $x = \alpha+1$ where $\alpha^2 + \alpha = 1$ and $\alpha \in \mathbb{F}_{2^n}$ by Fact 2.2.8.*

Theorem 2.2.10. *$F(x) = x^{2^n-2}$ is APN over $\mathbb{F}_{2^n}$ if and only if n is odd.*

Here, we should observe that the Gold function $F(x) = x^{2^i+1}$ is APN over $\mathbb{F}_{2^n}$ for infinitely many n. Since it is APN if and only if $\gcd(i, n) = 1$ and there are infinitely many n which are relatively prime to i. On the other hand, the inverse function $F(x) = x^{2^n-2}$ is also APN on $\mathbb{F}_{2^n}$ when n is odd. But the function changes for each n , i.e., we have different function for each n defined on $\mathbb{F}_{2^n}$.

According to the observation above, we define exceptional APN function as follows.

Definition 2.2.11. *Let F be an APN function on $\mathbb{F}_{2^n}$. F is an exceptional APN function if it remains APN on $\mathbb{F}_{2^n}$ for infinitely many n.*

After this definition, we can say that the Gold function is an exceptional APN function, since it is APN on $\mathbb{F}_{2^n}$ for infinitely many n. But, we will see that the inverse function is not an exceptional APN function.

Another exceptional APN function is Kasami-Welch function defined by $F(x) = x^{4^i-2^i+1}$ on $\mathbb{F}_{2^n}$. It is an exceptional APN function has been proven in [8, Theorem 5] for n is even. For the odd case, they proved in [17] using coding theoretical methods. We will also prove that Kasami-Welch function is an exceptional APN function in Chapter 5 by using algebraic geometric methods as given in [13].

Chapter 3

CCZ(Carlet-Charpin-Zinoviev) Equivalence and Extended Affine Equivalence

3.1 CCZ Equivalence and EA Equivalence

In this chapter, we will show that Extended Affine (EA) equivalence and Carlet-Charpin- Zinoviev (CCZ) equivalence preserve APN property. First of all, we define CCZ equivalence and EA equivalence.

Definition 3.1.1. *(EA-equivalence) Two functions* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and* $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *are EA-equivalent if there exist two affine permutations* $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, *and* $B : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and an affine function* $C : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such that*

$$F(x) = B \circ G \circ A(x) + C(x).$$

The most general form of equivalence that known to preserve the differential uniformity is CCZ equivalence, of which EA-equivalence is a particular case. We will explain the reason after the proof of Proposition 3.2.6. Carlet, Charpin and Zinoviev presented an equivalence between Boolean functions using graphs of functions. The graph of $F(x)$ is $G_F = \{(F(x), x) : \ x \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Definition 3.1.2. *(CCZ-equivalence) Two functions* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and* $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *are CCZ-equivalent if there exists an affine permutation* $\mathcal{A}$ *of* $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ *such that*

$$\{(F(x), x) : \ x \in \mathbb{F}_{2^n}\} = \mathcal{A}(\{(G(x), x) : \ x \in \mathbb{F}_{2^n}\}).$$

3.2 APN Property Under CCZ and EA Equivalences

To show extended affine equivalence preserve APN property, we need to show some propositions and a claim which will be used in the proof.

Proposition 3.2.1. *Let* $C : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a function. If* $C(x)$ *is affine then* $C(x) + C(x + a)$ *is constant.*

Proof. Let $a \in \mathbb{F}_{2^n}$ and $a \neq 0$. Suppose that $C : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an affine function. By definition of affine function, there exists a linear function L such that $C(x) = L(x)+d$ where $d \in \mathbb{F}_{2^n}$.

$$C(x) + C(x + a) = L(x) + d + L(x + a) + d$$

Since L is a linear function, we have

$$C(x) + C(x + a) = L(x) + d + L(x) + L(a) + d = L(a).$$

Hence $C(x) + C(x + a)$ is constant. □

We observed in Proposition 3.2.1 that $C(x) + C(x + a) = C(a) + C(0)$ for a non-zero $a \in \mathbb{F}_{2^n}$.

Claim 3.2.2. *An affine map A is permutation of $\mathbb{F}_q$ if and only if $A(x) - A(0)$ has a unique zero in $\mathbb{F}_q$, namely $x = 0$.*

Proof. Let $A : \mathbb{F}_q \to \mathbb{F}_q$ be an affine map, i.e., $A(x) = L(x) + d$ for some liner map $L : \mathbb{F}_q \to \mathbb{F}_q$ and $d \in \mathbb{F}_q$. Suppose that A is a permutation, then by definition of a permutation $A(x) - A(0)$ has a unique zero, namely $x = 0$.
Now, suppose that $A(x) - A(0)$ has a unique zero, namely $x = 0$. We have $A(x) - A(0) = L(x)+d-L(0)-d = L(x)-L(0) = L(x)$, as $L(0) = 0$. Since L has a unique zero, namely $x = 0$, $Ker(L) = \{0\}$. Then L is an injective linear map. Thus, L is a permutation of $\mathbb{F}_q$, then A is a permutation of $\mathbb{F}_q$. □

Corollary 3.2.3. *A linear map L over $\mathbb{F}_q$ is a permutation if and only if $L(x)$ has a unique zero in $\mathbb{F}_q$, namely $x = 0$.*

Proof. Since any linear map is also an affine map, taking $d = 0$ where $A(x) = L(x) + d$, it is straightforward from Claim 3.2.2. □

Here, we are going to prove one of our main aims which is stated at the beginning.

Proposition 3.2.4. *EA-equivalence preserves APN property.*

Proof. Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function such that F and G are EA-equivalent. We will show that EA-equivalence preserves being APN function by showing F is an APN function. By definition of EA-equivalence, we know that there exist two affine permutations $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $B : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an affine function $C : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F(x) = B \circ G \circ A(x) + C(x)$.

Consider $A(x) = L_1(x) + c_1$ and $B(x) = L_2(x) + c_2$ where L_1 and L_2 are linear part of A and B, respectively, and $c_1, c_2 \in \mathbb{F}_{2^n}$. That is $L_1(x) = A(x) - A(0)$ and $L_2(x) = B(x) - B(0)$, it implies that $c_1 = A(0)$ and $c_2 = B(0)$. We want to show that

$$F(x) + F(x + a) = B \circ G \circ A(x) + B \circ G \circ A(x + a) + C(x) + C(x + a) = b$$

has at most two solutions for all $b \in \mathbb{F}_{2^n}$ and for all non-zero $a \in \mathbb{F}_{2^n}$. We know from Proposition 3.2.1 that $C(x) + C(x + a)$ is constant. Saying $C(x) + C(x + a) = d$ for

some $d \in \mathbb{F}_{2^n}$, we have

$$F(x) + F(x+a) = B \circ G(A(x)) + B \circ G(A(x+a)) + d = b. \tag{3.2.1}$$

By expanding the compositions on the right hand side and setting $b' = b + d$, we obtain

$$B \circ G(L_1(x) + c_1) + B \circ G(L_1(x+a) + c_1) = b'.$$

Since L_1 is a linear function,

$$B \circ G(L_1(x) + c_1) + B \circ G(L_1(x) + L_1(a) + c_1) = b'.$$

By applying the composition, we have

$$B(G(L_1(x) + c_1)) + B(G(L_1(x) + L_1(a) + c_1)) = b'.$$

Since $B(x) = L_2(x) + c_2$, we obtain

$$L_2(G(L_1(x) + c_1)) + c_2 + L_2(G(L_1(x) + L_1(a) + c_1)) + c_2 = b'.$$

Since we are in characteristic 2,

$$L_2(G(L_1(x) + c_1)) + L_2(G(L_1(x) + L_1(a) + c_1)) = b'.$$

And, since L_2 is a linear function, we have

$$L_2(G(L_1(x) + c_1) + G(L_1(x) + L_1(a) + c_1)) = b'.$$

Setting $L_1(x) + c_1 = x'$ and $L_1(a) = a'$, we obtain

$$L_2(G(x') + G(x' + a')) = b'. \tag{3.2.2}$$

Since B is an affine permutation, $B(x) - B(0)$ has a unique zero, namely $x = 0$, by Claim 3.2.2. Also, we know that $B(x) - B(0) = L_2(x)$, then $L_2(x)$ has unique zero in $\mathbb{F}_{2^n}$, namely $x = 0$. By Corollary 3.2.3, we can say that $L_2(x)$ is a permutation of $\mathbb{F}_{2^n}$. Since L_2 is a permutation, Equation 3.2.2 has at most two solutions, because G is APN. Thus, Equation 3.2.1 has at most two solutions if and only if Equation 3.2.2 has at most two solutions. Hence, it gives us the desired result, i.e., F is APN. □

We are going to prove a proposition which is needed to show CCZ-equivalence preserves APN property.

Proposition 3.2.5. *[2] Let F be an APN function on $\mathbb{F}_{2^n}$ and $L_1 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $L_2 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be two linear functions. Suppose that (L_1, L_2) is a permutation on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and the function $F_2(x) = L_2(F(x), x)$ is a permutation on $\mathbb{F}_{2^n}$. Then, the function $F_1 \circ {F_2}^{-1}$ where $F_1(x) = L_1(F(x), x)$ is APN.*

Proof. By definition of APN function, $F_1 \circ {F_2}^{-1}$ is APN if and only if for any pair (a, b) from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with $a \neq 0$,

$$\begin{aligned} F_1 \circ {F_2}^{-1}(x) + F_1 \circ {F_2}^{-1}(y) &= b \\ x + y &= a \end{aligned} \tag{3.2.3}$$

has at most two solutions (x, y).
Since F_2 is permutation, we replace x by $F_2(x)$ and y by $F_2(y)$. Then we can write Equation 3.2.3 as follows.

$$\begin{aligned} F_1(x) + F_1(y) &= b \\ F_2(x) + F_2(y) &= a \end{aligned} \tag{3.2.4}$$

Then, $F_1 \circ {F_2}^{-1}$ is APN if and only if Equation 3.2.4 has at most two solutions for any pair (a, b) where a is non-zero. Or equivalently we have the following system for Equation 3.2.4.

$$\begin{aligned} L_1(F(x), x) + L_1(F(y), y) &= b \\ L_2(F(x), x) + L_2(F(y), y) &= a \end{aligned} \tag{3.2.5}$$

Equivalently, we have

$$\begin{aligned} &\Big(L_1(F(x), x) + L_1(F(y), y), L_2(F(x), x) + L_2(F(y), y)\Big) = (b, a) \\ \Leftrightarrow\ &\Big(L_1(F(x), x) + L_2(F(x), x)\Big) + \Big(L_1(F(y), y) + L_2(F(y), y)\Big) = (b, a) \\ \Leftrightarrow\ &(L_1, L_2)(F(x), x) + (L_1, L_2)(F(y), y) = (b, a) \end{aligned}$$

Since (L_1, L_2) is a linear permutation, there exists (b', a') such that $(L_1, L_2)(b', a') = (b, a)$. Then, we have

$$(L_1, L_2)(F(x) + F(y), x + y) = (L_1, L_2)(b', a').$$

Hence, we have the following system.

$$\begin{aligned} F(x) + F(y) &= b' \\ x + y &= a' \end{aligned} \tag{3.2.6}$$

Since F is APN, Equation 3.2.6 has at most two solutions (x, y) for any pair (a', b') with $a' \neq 0$. □

Note that if we take affine functions instead of linear functions on Proposition 3.2.5 such that $(L_1(x) + c_1, L_2(x) + c_2)$ is a permutation, then Proposition 3.2.5 again holds. Because Equation 3.2.4 becomes as follows.

$$\begin{aligned} L_1(F(x), x) + c_1 + L_1(F(y), y) + c_1 &= b \\ L_2(F(x), x) + c_2 + L_2(F(y), y) + c_2 &= a. \end{aligned}$$

Since characteristic is 2, we will obtain Equation 3.2.4 itself.

$$\begin{aligned} L_1(F(x), x) + L_1(F(y), y) &= b \\ L_2(F(x), x) + L_2(F(y), y) &= a \end{aligned}$$

Hence, the proof will be the same for an affine permutation $(L_1(x) + c_1, L_2(x) + c_2)$ with the proof of Proposition 3.2.5.

Proposition 3.2.6. *CCZ-equivalence preserves APN property.*

Proof. Let F and G be two CCZ-equivalent function. Suppose that F is APN, we will show that G is also. Since F and G are CCZ-equivalent, we have

$$\{(G(x), x) : \ x \in \mathbb{F}_{2^n}\} = \mathcal{A}(\{(F(x), x) : \ x \in \mathbb{F}_{2^n}\})$$

where $\mathcal{A} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is an affine permutation.
Let L_1 and L_2 be two linear functions from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ where $\mathcal{A}(x, y) = (L_1(x, y) + c_1, L_2(x, y) + c_2)$ with $(c_1, c_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.
Consider $F_2(x) = L_2(F(x), x) + c_2$ and $G(x) = L_1(F(x), x) + c_1 = F_1(x)$ which are maps from $\mathbb{F}_{2^n}$ to itself. First, we will show that $F_2(x) = L_2(F(x), x) + c_2$ is a permutation. We have $\mathcal{A}(F(x), x) = (F_1(x), F_2(x))$, then

$$\{(F_1(x), F_2(x)) : \ x \in \mathbb{F}_{2^n}\} = \{(G(x), x) : \ x \in \mathbb{F}_{2^n}\}.$$

Since all $x \in \mathbb{F}_{2^n}$ will appear in the pair $(G(x), x)$ in the set $\{(G(x), x) : \ x \in \mathbb{F}_{2^n}\}$, we can say that $F_2(x)$ is onto. Hence $F_2(x)$ is permutation on $\mathbb{F}_{2^n}$. Since $(L_1(x, y)+c_1, L_2(x, y)+c_2)$ is a permutation on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and $F_2(x) = L_2(F(x), x)+c_2$ is permutation on $\mathbb{F}_{2^n}$, the function $F_1 \circ {F_2}^{-1}$ is APN where $F_1(x) = L_1(F(x), x)+c_1$ by Proposition 3.2.5. Therefore $F_1(x) = L_1(F(x), x) + c_1 = G(x)$ is APN, since $F_1 \circ {F_2}^{-1}$ is APN and F_2 is permutation. □

Remark 3.2.7. *EA-equivalence is a particular case of CCZ-equivalence.*

Proof. Let F and G be two APN functions on $\mathbb{F}_{2^n}$. Suppose that F and G are EA-equivalent, i.e., there exist two affine permutation A, B on $\mathbb{F}_{2^n}$ and an affine function C on $\mathbb{F}_{2^n}$ such that

$$F(x) = B \circ G \circ A(x) + C(x).$$

We want to show that F and G are also CCZ-equivalent.
Let $\mathcal{G}_F$ and $\mathcal{G}_G$ be the graphs of F and G, respectively, in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

$$\mathcal{G}_F = \{(F(y), y) : \ y \in \mathbb{F}_{2^n}\}$$

$$\mathcal{G}_G = \{(G(x), x) : \ x \in \mathbb{F}_{2^n}\}$$

We need to show that there is an affine permutation $\mathcal{A}$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\mathcal{A}(\mathcal{G}_G) = \mathcal{G}_F$.
Let $z, w \in \mathbb{F}_{2^n}$ and $\mathcal{A}(z, w) = (L_1(z, w), L_2(z, w))$ such that $L_1(z, w) = B(z) + C \circ A^{-1}(w)$ and $L_2(z, w) = A^{-1}(w)$. We have the following equality.

$$\begin{aligned} \mathcal{A}(G(x), x) &= (L_1, L_2)(G(x), x) \\ &= (B \circ G(x) + C \circ A^{-1}(x), \ A^{-1}(x)) \end{aligned}$$

Set $y = A^{-1}(x)$, since A is a permutation, it means $x = A(y)$, we have

$$(B \circ G(x) + C \circ A^{-1}(x), \ A^{-1}(x)) = (B \circ G \circ A(y) + C(y), \ y) = (F(y), y).$$

That is $\mathcal{A}$ maps $\mathcal{G}_G$ into $\mathcal{G}_F$. Now, we need to show that $(L_1, L_2)(z, w)$ is a permutation of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Let $(z_1, w_1), (z_2, w_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Suppose that $(L_1, L_2)(z_1, w_1) =$

$(L_1, L_2)(z_2, w_2)$. Then we have following two equality.

$$B(z_1) + C \circ A^{-1}(w_1) = B(z_2) + C \circ A^{-1}(w_2)$$

$$A^{-1}(w_1) = A^{-1}(w_2) \tag{3.2.7}$$

Since A is a permutation of $\mathbb{F}_{2^n}$,we have $w_1 = w_2$ by Equation 3.2.7. We know that if $w_1 = w_2$ then $C \circ A^{-1}(w_1) = C \circ A^{-1}(w_2)$. Thus, Equation 3.2 holds if and only if $B(z_1) = B(z_2)$. We know also that B is a permutation of $\mathbb{F}_{2^n}$ then $z_1 = z_2$. Hence, $(L_1, L_2) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is an injective map, (L_1, L_2) is a permutation of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. □

Hence, we showed that EA and CCZ equivalences preserve APN property and EA equivalence is a particular case of CCZ equivalence.

Chapter 4

Exceptional APN Monomials

4.1 Exceptional APN Monomials

As we mentioned in preliminary chapter, every function on a finite field can be express as a polynomial by Lagrange's interpolation formula, then we will study on polynomials to study exceptional APN functions. To investigate exceptional APN functions, we will start to investigate with monomials.

In this section, we will introduce exceptional APN monomials and the procedure to show a given function is not an exceptional APN monomials. We will work on APN monomials on $\mathbb{F}_{2^n}$ and we will inquiry that it remains an APN function on infinitely many extension of $\mathbb{F}_{2^n}$.

We are going to begin with a lemma for a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ which is not necessarily an APN function. However, if this function is an APN function then it turns out that this statement is an biconditional statement.

Lemma 4.1.1. *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and (x_0, y_0, z_0) be a point in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Define an affine surface by $F(x)+F(y)+F(z)+F(x+y+z) = 0$ over $\mathbb{F}_{2^n}$. If $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$ then (x_0, y_0, z_0) satisfies the equation $F(x) + F(y) + F(z) + F(x + y + z) = 0$.*

Proof. Let (x_0, y_0, z_0) be a point in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $x_0 = y_0$. We have

$$F(x_0) + F(y_0) + F(z_0) + F(x_0 + y_0 + z_0) = F(x_0) + F(x_0) + F(z_0) + F(x_0 + x_0 + z_0).$$

Since the characteristic is 2, we obtain

$$F(x_0) + F(x_0) + F(z_0) + F(x_0 + x_0 + z_0) = F(z_0) + F(z_0) = 0.$$

Thus, (x_0, y_0, z_0) satisfies the equation $F(x) + F(y) + F(z) + F(x + y + z) = 0$ in the case $x_0 = y_0$.

The proof of the cases $y_0 = z_0$ and $x_0 = z_0$ are similar. Hence, the points (x_0, y_0, z_0) where $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$ lie on the affine surface defined by $F(x) + F(y) + F(z) + F(x + y + z) = 0$ over $\mathbb{F}_{2^n}$. □

The question is taking a point (x_0, y_0, z_0) from this affine surface, do we have always the cases $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$? Or, under which condition this is the case? We will answer this question with following lemma.

Lemma 4.1.2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function. If $F(x) + F(y) + F(z) + F(x+y+z) = 0$ has a solution $(x_0, y_0, z_0) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, then $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$.*

Proof. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function and (x_0, y_0, z_0) be a solution for $F(x) + F(y) + F(z) + F(x + y + z) = 0$. Let $b \in \mathbb{F}_{2^n}$ such that $D_aF(x_0) = b$. Suppose on the contrary that $x_0 \neq y_0$, $y_0 \neq z_0$ and $x_0 \neq z_0$. By setting $x_0 = y_0 + a$ for a non-zero element $a \in \mathbb{F}_{2^n}$, we obtain

$$F(y_0 + a) + F(y_0) + F(z_0) + F(y_0 + a + y_0 + z_0) = 0.$$

Since characteristic is 2, we have

$$F(y_0) + F(y_0 + a) + F(z_0) + F(z_0 + a) = 0.$$

It gives us $D_aF(y_0) = D_aF(z_0)$. On the other hand, we have

$$D_aF(x_0) = F(x_0) + F(x_0 + a) = F(y_0 + a) + F(y_0) = D_aF(y_0).$$

Then, we have the equality

$$b = D_aF(x_0) = D_aF(y_0) = D_aF(z_0).$$

Thus, $D_aF(x) = b$ has the following solutions: x_0, $x_0 + a$, z_0. That is, x_0, y_0, z_0 are solutions of $D_aF(x) = b$. This is a contradiction, since F is APN if and only if $D_aF(x) = b$ has at most two solutions for all $b \in \mathbb{F}_{2^n}$ and for all non-zero $a \in \mathbb{F}_{2^n}$. Hence, $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$. □

Theorem 4.1.3. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. F is APN if and only if the points (x_0, y_0, z_0), with $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$, are the only solutions of the equation $F(x) + F(y) + F(z) + F(x + y + z) = 0$.*

Proof. By Lemma 4.1.1 and Lemma 4.1.2, it is straightforward. □

Now, we will look at what is the relation between the affine surface $\mathcal{C}$ defined by $F(x) + F(y) + F(z) + F(x + y + z)$ over $\mathbb{F}_{2^n}$ and being an APN function. Before that, we have to give the Hasse-Weil bound for algebraic curves over finite fields, the definition of absolutely irreducibility and the definition of a rational point.

Definition 4.1.4. *Let V_ϕ be an affine algebraic variety defined by $\phi \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ where ϕ is a non-zero polynomial in n indeterminates over $\mathbb{F}_q$, to be a subset of $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q \times \ldots \times \overline{\mathbb{F}}_q$ (the cartesian product of n copies of the algebraic closure of $\mathbb{F}_q$) of the form*

$$V_\phi = \{(a_1, a_2, \ldots, a_n) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q \times \ldots \times \overline{\mathbb{F}}_q : \ \phi(a_1, a_2, \ldots, a_n) = 0\}$$

A point $(a_1, a_2, \ldots, a_n)$ on V_ϕ is called a rational point if $a_1, a_2, \ldots, a_n$ belong to $\mathbb{F}_q$ for all n.

Definition 4.1.5. *A polynomial $\phi(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is an absolutely irreducible polynomial if $\phi(x_1, x_2, \ldots, x_n)$ is irreducible over $\mathbb{F}_q$ and is irreducible over $\overline{\mathbb{F}}_q$*

Theorem 4.1.6. *(Hasse-Weil Bound)[19, Chapter 6] Let $\mathcal{C}$ be an absolutely irreducible curve over the finite field $\mathbb{F}_q$. We denote by $N(\mathcal{C})$ the number of rational points on the curve $\mathcal{C}$. Then, we have the following inequality.*

$$N(\mathcal{C}) \geq q - \frac{(\deg(\mathcal{C}) - 1)(\deg(\mathcal{C}) - 2)}{2} q^{1/2}.$$

Theorem 4.1.7. *(Bezout's Theorem) [11, Theorem 5.3] Let g and h be two affine plane curves of degree d_1 and d_2 respectively. The intersection number of g and h at the point P is denoted by $I(P, g, h)$. Assume that f and g have no common component. Then,*

$$\sum_P I(P, g, h) \leq d_1 d_2.$$

Observation 4.1.8. *Let $\mathcal{C}$ be a curve over $\mathbb{F}_{2^n}$ having an absolutely irreducible factor $\mathcal{X}$ defined over $\mathbb{F}_{2^n}$. Suppose the defining equation is not $x = y$, $y = z$ and $x = z$. By the Hasse-Weil bound, we have the following inequality.*

$$N(\mathcal{C}) \geq N(\mathcal{X}) \geq 2^n - \frac{(\deg(\mathcal{X}) - 1)(\deg(\mathcal{X}) - 2)}{2} 2^{n/2}$$

Note that $N(\mathcal{X})$ is large enough for all sufficiently large n. Recall that the planes $x = y$, $y = z$ and $x = z$ has at most $\deg(\mathcal{X})$ intersection points with $\mathcal{X}$ by Bezout's theorem. Then, we observe that $N(\mathcal{X}) - 3\deg(\mathcal{X}) > 0$ for a sufficiently large n. It means that there exists a rational point $(x_0, y_0, z_0) \in \mathcal{X}$ such that $x_0 \neq y_0$, $y_0 \neq z_0$ and $x_0 \neq z_0$. Thus, there exists a rational point (x_0, y_0, z_0) on the curve $\mathcal{C}$ such that $x_0 \neq y_0$, $y_0 \neq z_0$ and $x_0 \neq z_0$.

Proposition 4.1.9. *Let F be a function from $\mathbb{F}_{2^n}$ to itself. F is APN if and only if the affine surface $F(x) + F(y) + F(z) + F(x + y + z) = 0$ has all rational points on the surface defined by $(x + y)(y + z)(x + z) = 0$.*

Proof. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function. We know from Theorem 4.1.3 that F is APN if and only if the points (x_0, y_0, z_0) with $x_0 = y_0$ or $y_0 = z_0$ or $x_0 = z_0$, are the only solutions of the equation $F(x) + F(y) + F(z) + F(x + y + z) = 0$. Then the affine surface $F(x) + F(y) + F(z) + F(x + y + z) = 0$ has all rational points on the surface defined by $(x + y)(y + z)(x + z) = 0$ if and only if F is APN. □

We observed that $\dfrac{F(x) + F(y) + F(z) + F(x + y + z)}{(x + y)(y + z)(x + z)}$ is homogenous of degree $t - 3$ when F is a monomial defined by $F(x) = x^t$. To use Hasse- Weil bound, we have consider an absolutely irreducible curve over a projective plane. If the projective curve defined by $\dfrac{F(x) + F(y) + F(z) + F(x + y + z)}{(x + y)(y + z)(x + z)}$ has an absolutely irreducible component over $\mathbb{F}_{2^n}$ then there exists a rational point (x_0, y_0, z_0) such that $x_0 \neq y_0$, $y_0 \neq z_0$ and $x_0 \neq z_0$ where $x_0, y_0, z_0 \in \mathbb{F}_{2^n}$ for a sufficiently large n. By Lemma 4.1.2, we know that if F is APN then all rational points on $F(x) +$

$F(y)+F(z)+F(x+y+z)=0$ have to satisfy at least one of the equalities $x_0=y_0$ or $y_0=z_0$ or $x_0=z_0$. Therefore, F could not be an APN function if the curve $\dfrac{F(x)+F(y)+F(z)+F(x+y+z)}{(x+y)(y+z)(x+z)}$ contains an absolutely irreducible factor over $\mathbb{F}_{2^n}$. That is, F could not be an exceptional APN function.

4.2 The Only Exceptional APN Monomials

In this section, we will be interested in the conjecture states that the only exceptional APN monomials are Gold and Kasami- Welch functions which are x^{2^i+1} and $x^{2^{2i}-2^i+1}$, respectively.

Definition 4.2.1. *Monomial functions $f(x)=x^t$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, the exponent t is called exceptional if $f(x)=x^t$ is APN on infinitely many extension fields of $\mathbb{F}_2$, i.e., $f(x)=x^t$ is an exceptional APN.*

The conjecture about exceptional APN monomials was established by H. Janwa, G. McGuire and R.M. Wilson in 1995 as follows [14]:

Conjecture 4.2.2. *Up to equivalence, the only exceptional exponents are the Gold and the Kasami-Welch numbers which are 2^i+1 and 4^i-2^i+1, respectively.*

Here, equivalence refers to CCZ-equivalence. The list of some known inequivalent APN monomial functions over $\mathbb{F}_{2^n}$ with their constraints as follows.

Known APN Monomials		
Name	**Function**	**Constraints**
Gold	x^{2^i+1}	$\gcd(i,n)=1$ [12]
Kasami-Welch	$x^{2^{2i}-2^i+1}$	$\gcd(i,n)=1$ [17]
Welch	x^{2^i+3}	$n=2^i+1$ [8]
Niho	$x^{2^i+2^{i/2}-1}$	$n=2^i+1$, i even [9]
Niho	$x^{2^i+2^{(3i+1)/2}-1}$	$n=2^i+1$, i odd [9]
Dobbertin	$x^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$	$n=5i$ [10]
Inverse	$x^{2^{2i}-1}$	$n=2i+1$ [22]

To show Conjecture 4.2.2 is true, researchers generalize the monomial x^t as $t=2^il+1$ where l is an odd integer. As it can be observed that t is an odd integer.

Remark 4.2.3. *Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function defined by $F(x)=x^t$ where t is even. Consider $t=2^jk$ where k is odd. Then, we have $x^t=x^{2^jk}=(x^k)^{2^j}$. We know that $B(x)=x^{2^j}$ is a linear permutation. Taking an affine permutation and an affine*

map $A(x)$ and $C(x)$, respectively, in the definition of EA-equivalence as $A(x) = x$ and $C(x) = 0$, we have

$$F(x) = B \circ G \circ A(x) + C(x)$$

where $G(x) = x^k$ and k is odd. Hence, we can say that the monomials $x^{2^j k}$ and x^k are EA-equivalent. Because of this reason, it is enough to examine the monomials x^k where k is odd, since $x^{2^j k}$ is APN if and only if x^k is APN.

From now on, we fixed t to be an odd integer. Our main aim is to show that the monomial x^t is not an APN function over $\mathbb{F}_{2^n}$ for infinitely many n, except for the cases $t = 2^i + 1$ and $t = 4^i - 2^i + 1$. Therefore, we are examining the exponents of the form $t = 2^i l + 1$ where $i \geq 1$ and $l \geq 3$ is odd, since it is enough to examine for odd t's by the previous remark. Note that for the case $l = 1$ and $l = 2^i - 1$, we obtain Gold and Kasami-Welch functions, respectively. We can not take $l = 2$, since l is odd. Then, we separate the situation into two cases: $\gcd(l, 2^i - 1) < l$ and $\gcd(l, 2^i - 1) = l$.

R. Gold has shown that x^{2^i+1} is an exceptional APN function if and only if $\gcd(i, n) = 1$, see [12]. It has been shown by J.H. van Lint, H. Janwa and R.M. Wilson that the Kasami-Welch monomial $x^{2^{2i}-2^i+1}$ is an exceptional APN function if and only if $\gcd(i, n) = 1$, see [15], [26]. When we consider the functions which are not exceptional APN, D. Jedlicka proved that $x^{2^i l+1}$ is not an exceptional APN function when $\gcd(l, 2^i - 1) < l$, see [16]. To show the only exceptional values for x^t where $t = 2^i + 1$, it has to been proven for $\gcd(l, 2^i + 1) = l$ for some positive integer $l > 1$. F. Hernando and G. McGuire proved that the monomial $x^{2^i l+1}$ is nor exceptional APN when $\gcd(l, 2^i + 1) = l$, except for the cases $t = 2^i + 1$ and $t = 2^{2i} - 2^i + 1$, i.e, $l = 1$ and $l = 2^i + 1$ [13]. Hence, the proof of Conjecture 4.2.2 has finished by F. Hernando and G. McGuire, by stating the following theorem in [13].

Theorem 4.2.4. *[13] The only exceptional exponents are the Gold and Kasami-Welch numbers which are $2^i + 1$ and $4^i - 2^i + 1$ respectively.*

In other words the theorem says that for a fixed odd $t \geq 3$, when $t \neq 2^i + 1$ or $t \neq 4^i - 2^i + 1$, $F(x) = x^t$ is APN on at most a finite number of fields $\mathbb{F}_{2^n}$.

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F(x) = x^t$. Using Proposition 4.1.9, we define a function as follows.

$$f_t(x, y, z) = x^t + y^t + z^t + (x + y + z)^t$$

It is the same as an affine surface defined in Theorem 4.1.3, $F(x) + F(y) + F(z) + F(x + y + z) = 0$. We know from Theorem 4.1.3 that $f_t(x, y, z)$ has rational points over $\mathbb{F}_{2^n}$ with the same coordinates $x = y$,$y = z$ or $x = z$ if and only if F is APN .

Remark 4.2.5. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^t$ where t is an positive integer. Then $(x + y)(y + z)(x + z)$ divides $f_t(x, y, z) = F(x) + F(y) + F(z) + F(x + y + z)$, by Lemma 4.1.1.*

Assuming F is APN, we can easily see that the only solutions for $f_t(x,y,z)=0$ are $x=y$, $y=z$, $x=z$ by Theorem 4.1.3. Thus, $(x+y)(y+z)(x+z)$ divides $f_t(x,y,z)$. We know from Proposition 4.1.9 that $f_t(x,y,z)=0$ has all rational points on the surface defined by $(x+y)(y+z)(x+z)=0$. Hence, we can restrict ourselves to rational points of the homogeneous polynomial $g_t(x,y,z)$ defined by

$$g_t(x,y,z)=\frac{f_t(x,y,z)}{(x+y)(y+z)(x+z)}$$

to say that $F(x)=x^t$ is an exceptional APN or not.

Therefore, we can give the following proposition by using observation on having absolutely irreducible component above.

Proposition 4.2.6. *If $g_t(x,y,z)$ has an absolutely irreducible component defined over $\mathbb{F}_2$ then $g_t(x,y,z)$ has rational points $(\alpha,\beta,\gamma)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ with distinct coordinates for all n sufficiently large by Observation 4.1.8.*

Here, we are looking for having an absolutely irreducible component rather than being entirely absolutely irreducible. Because the conjecture was proposed by Janwa-McGuire and Wilson stating "The polynomial $g_t(x,y,z)$ is absolutely irreducible for all t not of the form 2^i+1 or 4^i-2^i+1" is shown to be wrong. However, Hernando and McGuire gave a counterexample for $t=205$ using MAGMA, they observed that $g_t(x,y,1)$ factors into two factors over $\mathbb{F}_2$ [13]. One of the factor is as follows.

$$\begin{aligned}&x^{10}+x^9y+x^9+x^8y^2+x^8y+x^8+x^6y^3+x^6y^2+x^6y+x^6+x^5y^5\\&+x^5+x^4y+x^4y^4+x^4y^3+x^4y^2+x^4+x^3y^6+x^3y^4+x^3y^3+x^3y+x^3y^8\\&+x^2y^6+x^2y^4+x^2y^2+x^2+xy^9+xy^8+xy^6+xy^3+xy+y^{10}+y^9\\&+y^8+y^6+y^5+y^4+y^2+y+1\end{aligned}$$

On the other hand, they showed the following theorem.

Theorem 4.2.7. *[13, Theorem 15] If $g_t(x,y,1)$ is irreducible over $\mathbb{F}_2$ and $l\mid 2^i-1$ but $l\neq 2^i-1$ then $g_t(x,y,1)$ is absolutely irreducible.*

Therefore, we are looking for having an absolutely irreducible component of the affine part $g_t(x,y,1)$ of $g_t(x,y,z)$ to show that the only exceptional APN monomials are Gold and Kasami- Welch functions.

Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function defined by $F(x)=x^t$ where $t\geq 3$ and t is odd. We can observe that $g_t(x,y,z)=\dfrac{f_t(x,y,z)}{(x+y)(y+z)(x+z)}=\dfrac{x^t+y^t+z^t+(x+y+z)^t}{(x+y)(y+z)(x+z)}$ is a homogenous polynomial of degree $t-3$. Hence $g_t(x,y,z)=0$ defines a projective curve. That is, we are looking for rational points of a projective plane curve.

Definition 4.2.8. *Let $\phi(x,y)$ be a polynomial on an affine plane over a field K and $\phi(P)=0$ where $P=(\alpha,\beta)$. Consider $\phi^P=\phi(x+\alpha,y+\beta)=F_0+F_1+\ldots+F_m$*

where F_i are homogenous polynomials of degree i where $0 \leq i \leq m$, i.e., forms of ϕ at point P of degree i. The multiplicity at the point P is the degree of the non-zero form of the smallest degree. It is denoted by $m_P(\phi)$. P is called a simple point of ϕ if and only if $m_P(\phi) = 1$. P is called a singular point if and only if $m_P(\phi) > 1$.

Notation 4.2.9. *Let F be a function on a field K. The partial derivatives of F according to x, y and z evaluated at a point P are denoted as follows.*

$$\frac{\partial F}{\partial x}\Big|_P \qquad \frac{\partial F}{\partial y}\Big|_P \qquad \frac{\partial F}{\partial z}\Big|_P$$

Fact 4.2.10. *Let $\phi(x, y, z)$ be a curve in a projective plane over a field K. Consider a point $P = (\alpha, \beta, \gamma)$ where $\alpha, \beta, \gamma \in K$ such that $\phi(P) = 0$. P is a singular point of ϕ if and only if $\frac{\partial F}{\partial x}\Big|_P = \frac{\partial F}{\partial y}\Big|_P = \frac{\partial F}{\partial z}\Big|_P = 0$.*

Equivalently, to determine the singular points of a curve defined by a polynomial ϕ, we can look at partial derivatives of ϕ at a point P such that $\phi(P) = 0$. If all partial derivatives of ϕ are vanished on P, then we can say that P is a singular point of this curve.

Definition 4.2.8 is the definition of a singular point and its multiplicity on an affine plane. But, $f_t(x, y, z) = 0$ and $g_t(x, y, z) = 0$ are projective curve. To define a singular point of a projective curve, consider the point $P = (\alpha, \beta, \gamma)$ on a projective plane such that $f_t(P) = 0$. Without loss of generality say that $\gamma \neq 0$ and write $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}, 1)$. Then multiplicity of $f_t(x, y, z)$ at the point P is defined as multiplicity of $f_t(x, y, z)$ at the point $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}, 1)$.

Fact 4.2.11. *$P = (\alpha, \beta, \gamma)$ is a singular point of $f_t(x, y, z)$ if and only if $\frac{\partial f_t}{\partial x}\Big|_{\tilde{P}} = \frac{\partial f_t}{\partial y}\Big|_{\tilde{P}} = f_t(\tilde{P}) = 0$, where $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}, 1)$.*

Observation 4.2.12. *Let (α, β, γ) be a point where $\alpha, \beta, \gamma \in \mathbb{F}_{2^n}$ such that $g_t(\alpha, \beta, \gamma) = 0$. (α, β, γ) is not a singular point of $g_t(x, y, z)$ if $\gamma = 0$.*

Proof. To examine singular points of g_t, we look at partial derivatives of $f_t(x, y, z)$.

$$\begin{aligned}
\frac{\partial f_t}{\partial x} &= tx^{t-1} + t(x + y + z)^{t-1} \\
\frac{\partial f_t}{\partial y} &= ty^{t-1} + t(x + y + z)^{t-1} \\
\frac{\partial f_t}{\partial z} &= tz^{t-1} + t(x + y + z)^{t-1}
\end{aligned}$$

Say $P = (\alpha, \beta, 0)$ is a singular point of g_t at infinity where $\alpha, \beta \in \mathbb{F}_{2^n}$ and $\alpha \neq 0$ or $\beta \neq 0$.

$$\frac{\partial f_t}{\partial x}\Big|_P = t\alpha^{t-1} + t(\alpha + \beta)^{t-1} = 0 \tag{4.2.1}$$

$$\frac{\partial f_t}{\partial y}\Big|_P = t\beta^{t-1} + t(\alpha+\beta)^{t-1} = 0 \tag{4.2.2}$$

$$\frac{\partial f_t}{\partial z}\Big|_P = t(\alpha+\beta)^{t-1} = 0 \tag{4.2.3}$$

Since $t(\alpha+\beta)^{t-1} = 0$ and t is an odd integer, $\alpha+\beta = 0$, i.e., $\alpha = \beta$. On the other hand, $t\beta^{t-1} + t(\alpha+\beta)^{t-1} = 0$, t is an odd integer and we deduced that $\alpha = \beta$, it implies that $\beta = 0$. Similarly, by Equation 4.2.1, we obtain $\alpha = 0$. But, one of α or β cannot be 0, it is a contradiction. Thus, P is a simple point of f_t. We know that $f_t(x,y,z) = g_t(x,y,z)\Big((x+y)(y+z)(x+z)\Big)$, then we have the following equality.

$$m_P(f_t) = m_P(g_t) + m_P(x+y) + m_P(y+z) + m_P(x+z)$$

Since P is a simple point of f_t, we have $m_P(f_t) = 1$. This implies that $m_P(g_t) = 1$, i.e., P is a simple point of g_t. □

Accordingly, there is no singular point of g_t at $(x,y,0)$ where $x \neq 0$ or $y \neq 0$. To find a point of the form $(x,y,0)$ such that the partial derivatives according to x, y and z vanish simultaneously, the only possibility is $x = y = 0$. Hence, the only singular points of g_t, respectively f_t, are the projective points of the form $(x,y,1)$ where $x \neq 0$ or $y \neq 0$.

Now, we will investigate singular points of f_t of the form $(x,y,1)$. Let $P = (\alpha,\beta,1)$ where $\alpha,\beta \in \bar{\mathbb{F}}_{2^n}$ and $t = 2^i l + 1$ where $i \geq 1$ and $l \geq 3$ is odd. To examine the singular points, we look at vanishing set of following system.

$$\begin{aligned}
\frac{\partial f_t}{\partial x}\Big|_P &= t\alpha^{t-1} + t(\alpha+\beta+1)^{t-1} = 0\\
\frac{\partial f_t}{\partial y}\Big|_P &= t\beta^{t-1} + t(\alpha+\beta+1)^{t-1} = 0\\
\frac{\partial f_t}{\partial z}\Big|_P &= t + t(\alpha+\beta+1)^{t-1} = 0
\end{aligned}$$

By cancelling out t, we obtain

$$\begin{aligned}
\frac{\partial f_t}{\partial x}\Big|_P &= \alpha^{2^i l} + (\alpha+\beta+1)^{2^i l} = 0\\
\frac{\partial f_t}{\partial y}\Big|_P &= \beta^{2^i l} + (\alpha+\beta+1)^{2^i l} = 0\\
\frac{\partial f_t}{\partial z}\Big|_P &= 1 + (\alpha+\beta+1)^{2^i l} = 0.
\end{aligned}$$

Setting $\lambda = \alpha+\beta+1$, we can observe that $\frac{\partial f_t}{\partial z}\Big|_P = 0$ if and only if $\lambda^{2^i l} + 1 = (\lambda^l + 1)^{2^i} = 0$, i.e, $\lambda^l = 1$. Therefore, λ should be l-th root of unity. Since $\alpha^{2^i l} + \lambda^{2^i l} = 0$

and $\beta^{2^i l} + \lambda^{2^i l} = 0$ where λ is a l-th root of unity, α and β are also l-th root of unity. Then, singular projective points of $f_t(x, y, z)$ are of the form $(\alpha, \beta, 1)$ where α, β and λ are l-th root of unity.

Thus, we can distinguish singular points as follows.

Type 1: $\alpha = 1$, $\beta = 1$, $\lambda = 1$.

Type 2: $\alpha = 1$ and $\beta \neq 1$, or $\beta = 1$ and $\alpha \neq 1$, or $\alpha \neq 1$, $\beta \neq 1$ and $\lambda = 1$.

Type 2.1: $\alpha, \beta \in \mathbb{F}_{2^i}$.

Type 2.2: $\alpha \notin \mathbb{F}_{2^i}$ and $\beta \notin \mathbb{F}_{2^i}$.

Type 3: $\alpha \neq 1$, $\beta \neq 1$ and $\alpha \neq \beta$.

Type 3.1: $\alpha, \beta \in \mathbb{F}_{2^i}$.

Type 3.2: $\alpha \notin \mathbb{F}_{2^i}$ and $\beta \notin \mathbb{F}_{2^i}$

Furthermore, we can calculate the number of singular points and multiplicity of f_t and g_t at these points for each type of singularities above. To calculate them, we will express the forms of $f_t(x + \alpha, y + \beta, 1)$. By binomial theorem, we have the following equalities.

$$\begin{aligned} f_t(x+\alpha, y+\beta) &= (x+\alpha)^t + (y+\beta)^t + (x+y+\alpha+\beta+1)^t + 1 \\ &= \sum_{j=0}^{t} \binom{t}{j} \alpha^{t-j} x^j + \sum_{j=0}^{t} \binom{t}{j} \beta^{t-j} y^j \\ &+ \sum_{j=0}^{t} \binom{t}{j} (\alpha+\beta+1)^{t-j} (x+y)^j + 1 \\ &= \sum_{j=0}^{t} \binom{t}{j} \left(\alpha^{t-j} x^j + \beta^{t-j} y^j + (\alpha+\beta+1)^{t-j} (x+y)^j \right) + 1 \end{aligned}$$

As it can be seen that the form F_i which is homogenous polynomial of degree i is correspond to the polynomial $\binom{t}{j}\left(\alpha^{t-j} x^j + \beta^{t-j} y^j + (\alpha+\beta+1)^{t-j} (x+y)^j \right)$ when $j = i$. To calculate the forms of $f_t(x + \alpha, y + \beta, 1)$, we need the following remark.

Remark 4.2.13. *Note that* $\binom{t}{j} = 0$ *when* $1 < j < 2^i$ *and* $\binom{t}{j} = 1$ *when* $j = 2^i, 2^i + 1$ *where* $t = 2^i l + 1$ *and* l *is odd.*

$$\binom{t}{j} = \frac{t!}{j!(t-j)!} = \frac{(2^i l + 1)(2^i l)}{j(j-1)} \ \frac{(t-2)!}{(j-2)!(t-j)!} = \frac{(2^i l + 1)(2^i l)}{j(j-1)} \binom{t-2}{j-2}$$

It is sufficient to observe that $\frac{(2^i l+1)(2^i l)}{j(j-1)}$ *is even. Note that the only one of* j *and* $j - 1$ *can be even. Since* j *and* $j - 1$ *are less than* 2^i, 2^k *divides* j *or* 2^k *divides* $(j - 1)$ *implies that* $k < i$. *Then,* $\binom{t}{j} = 0$.

We know that $t = 2^i l + 1$ where l is an odd integer. When we write t in base 2, we will obtain the following.

$$\begin{aligned} t = 2^i l + 1 &= 1 + (1 + 2 + 2^2 + \ldots + 2^{m-1})2^i \\ &= 1 + 2^i + 2^{i+1} + \ldots + 2^{m+i-1} \end{aligned}$$

By Lucas' Theorem 1.1.17, we observe the followings.

$$\binom{t}{2^i} = \binom{1}{0}\binom{1}{1}\ldots\binom{1}{0} \equiv 1 \mod 2$$

$$\binom{t}{2^i + 1} = \binom{1}{1}\binom{1}{1}\ldots\binom{1}{0} \equiv 1 \mod 2$$

Hence, $\binom{t}{j} = 1$ when $j = 2^i, 2^i + 1$ where $t = 2^i l + 1$ for an odd integer l.

By Remark 4.2.13, we define the forms of $f_t(x + \alpha, y + \beta, 1)$ as follows.

$$\begin{aligned} F_0 &= 1 + \alpha^t + \beta^t + (\alpha + \beta + 1)^t \\ F_1 &= (\alpha^{t-1} + \lambda^{t-1})x^{t-1} + (\beta^{t-1} + \lambda^{t-1})y \\ F_{2^i} &= \binom{t}{2^i}(\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i} \\ &= (\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i} \\ F_{2^i+1} &= \binom{t}{2^i + 1}(\alpha^{t-2^i-1} + \lambda^{t-2^i-1})x^{2^i+1} + (\beta^{t-2^i-1} + \lambda^{t-2^i-1})y^{2^i+1} + \lambda^{t-2^i-1}(x^{2^i}y + xy^{2^i}) \\ &= (\alpha^{t-2^i-1} + \lambda^{t-2^i-1})x^{2^i+1} + (\beta^{t-2^i-1} + \lambda^{t-2^i-1})y^{2^i+1} + \lambda^{t-2^i-1}(x^{2^i}y + xy^{2^i}) \end{aligned}$$

We will investigate number of singular points according to their types, their multiplicity $m_P(f_t)$ and $m_P(g_t)$.

For the singularities of Type 1, i.e., $\alpha = \beta = \lambda = 1$, there is only one singular point in this type which is $(1, 1, 1)$. Since, it is a singular point, $F_0 = F_1 = 0$. The multiplicity of this point can be 2^i or $2^i + 1$. Note that

$$F_{2^i} = (\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i} = 0.$$

Then, we have to check that $F_{2^i+1} \neq 0$.

$$\begin{aligned} F_{2^i+1} &= (\alpha^{t-2^i-1} + \lambda^{t-2^i-1})x^{2^i+1} + (\beta^{t-2^i-1} + \lambda^{t-2^i-1})y^{2^i+1} + \lambda^{t-2^i-1}(x^{2^i}y + xy^{2^i}) \\ &= x^{2^i}y + y^{2^i}x \end{aligned}$$

Hence, $m_P(f_t) = 2^i + 1$ where $P = (1, 1, 1)$, i.e., the multiplicity of f_t at the singular point of Type 1 is $2^i + 1$. We will calculate $m_P(g_t)$ at the point $P = (1, 1, 1)$. To

calculate this multiplicity, consider the following curve.

$$g_t(x+\alpha, y+\beta, 1) = \frac{f_t(x+\alpha, y+\beta, 1)}{(x+\alpha+1)(y+\beta+1)(x+y+\alpha+\beta)}$$

We know that $m_P(f_t) = m_P(g_t) + m_P(w)$ where $w(x, y, 1) = (x+\alpha+1)(y+\beta+1)(x+y+\alpha+\beta)$. Then, we can calculate $m_P(g_t)$ by calculating $m_P(w)$.

$$\begin{aligned} w(x,y,1) &= (x+\alpha+1)(y+\beta+1)(x+y+\alpha+\beta) \\ &= x^2y + xy^2 + (\beta+1)x^2 + (\alpha+1)y^2 + (\beta^2+1)x \\ &+ (\alpha^2+1)y + (\alpha^2\beta + \alpha\beta^2 + \alpha^2 + \beta^2 + \alpha + \beta) \end{aligned}$$

The forms of $w(x, y, 1)$ are as follows.

$$\begin{aligned} W_0 &= \alpha^2\beta + \alpha\beta^2 + \alpha^2 + \beta^2 + \alpha + \beta \\ W_1 &= (\beta^2+1)x + (\alpha^2+1)y \\ W_2 &= (\beta+1)x^2 + (\alpha+1)y^2 \\ W_3 &= x^2y + xy^2 \end{aligned}$$

For the singular point $P = (1, 1, 1)$ of f_t, it can be seen that $W_0 = 0$, $W_1 = 0$, $W_2 = 0$ and $W_3 = x^2y + xy^2$. Hence, $m_P(w) = 3$ and $m_P(g_t) = m_P(f_t) - m_P(w) = 2^i + 1 - 3 = 2^i - 2$.

Now, we will calculate the number of singular points of Type 2.2 and their multiplicities, when $\gcd(2^i - 1, l) = 1$. For the singular points of other types, calculations are similar whenever $\gcd(2^i - 1, l) < l$ and $\gcd(2^i - 1, l) = l$.

Let $P = (\alpha, \beta, 1)$ be a singular point of f_t of Type 2.2, i.e., $\alpha, \beta \notin \mathbb{F}_{2^i}$, and $\gcd(2^i - 1, l) = 1$. First, we will determine the number of the singular points of Type 2.2. There are $(l-1)$ points of type $(1, \beta)$, since α, β, λ are l-th root of unity and $\beta \neq 1$. There are also $(l-1)$ points of type $(\alpha, 1)$ for the same reason. For the type $\alpha \neq 1$, $\beta \neq 1$ and $\lambda \neq 1$, the points are of the form (α, α), since $\lambda = \alpha+\beta+1 = 1$ and α, β are different from 0, we see that $\alpha = \beta$. Thus, there are $(l-1)$ points of type (α, α). In total, there are $3(l-1)$ points of Type 2.2.

We will calculate $m_P(f_t)$ and $m_P(g_t)$ where $P = (\alpha, \beta, 1)$ and $\alpha, \beta \notin \mathbb{F}_{2^i}$. Since we are investigating singular points of Type 2.2. when $\gcd(2^i - 1, l) = 1$, we have three possibilities for α, β and λ :

- $\alpha = 1$ and $\beta \neq 1$.
- $\beta = 1$ and $\alpha \neq 1$.
- $\alpha \neq 1$, $\beta \neq 1$ and $\lambda = 1$, i.e., $\alpha = \beta$ but $\alpha, \beta \neq 1$.

Since they are singular points of f_t where $t = 2^i l + 1$, we know that $F_0 = F_1 = 0$. Thus, we will check F_{2^i} vanishes or not at the point $P = (\alpha, \beta, 1)$ to calculate $m_P(f_t)$

and we will also check W_1, W_2, W_3 to calculate $m_P(g_t)$.

$$\begin{aligned} F_{2^i} &= (\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i} \\ &= (\alpha^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})x^{2^i} + (\beta^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})y^{2^i} \end{aligned}$$

First, consider the point $P = (\alpha, \beta, 1)$ where $\alpha = 1$ and $\beta \neq 1$. We have the following equalities.

$$\begin{aligned} F_{2^i} &= (\alpha^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})x^{2^i} \\ &\quad + (\beta^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})y^{2^i} \\ &= (\beta^{2^i(l-1)+1} + 1)x^{2^i} \end{aligned}$$

$$\begin{aligned} W_0 &= \alpha^2\beta + \alpha\beta^2 + \alpha^2 + \beta^2 + \alpha + \beta \\ &= \beta + \beta^2 + 1 + \beta^2 + 1 + \beta \\ &= 0 \end{aligned}$$

$$\begin{aligned} W_1 &= (\beta^2 + 1)x + (\alpha^2 + 1)y \\ &= (\beta^2 + 1)x \end{aligned}$$

We have to be sure $\beta^{2^i(l-1)+1} \neq 1$, to say that $m_P(f_t) = 2^i$ at point $P = (\alpha, \beta, 1)$ where $\alpha = 1$ and $\beta \neq 1$. We can write $\beta^{2^i l - 2^i} + 1$ as

$$\beta^{2^i l - 2^i + 1} = \frac{\beta^{2^i l}}{\beta^{2^i}}\beta.$$

Since β is the l-th root of unity, we have

$$\beta^{2^i l - 2^i + 1} = \frac{\beta}{\beta^{2^i}} = \beta^{1-2^i} = \beta^{-(2^i-1)}.$$

Since $\gcd(2^i - 1, l) = 1$, we can deduce $\beta^{2^i(l-1)+1} \neq 1$. Thus, $\beta^{2^i(l-1)+1} \neq 1$, i.e., $m_P(f_t) = 2^i$. Note that $\beta^2 \neq 1$, since β is l-th root of unity and $\beta \neq 1$, . Thus, $W_1 \neq 0$, that is, $m_P(w) = 1$ and $m_P(g_t) = m_P(f_t) - 1 = 2^i - 1$ for the case $\alpha = 1$ and $\beta \neq 1$.

Secondly, consider singular points $P = (\alpha, \beta, 1)$ where $\alpha \neq 1$ and $\beta = 1$. The calculations for $m_P(f_t)$ and $m_P(g_t)$ are similar with the points $P = (\alpha, \beta, 1)$ with $\alpha = 1$ and $\beta \neq 1$. Similarly, we have the following equalities.

$$\begin{aligned} F_{2^i} &= (\alpha^{2^i(l-1)+1} + 1)y^{2^i} \\ W_1 &= (\alpha^2 + 1)y \end{aligned}$$

For the same reason above, we obtain $F_{2^i} \neq 0$ and $W_1 \neq 0$. Thus, $m_P(f_t) = 2^i$ and $m_P(g_t) = 2^i - 1$ for the singular points $P = (\alpha, \beta, 1)$ where $\beta = 1$ and $\alpha \neq 1$.

Thirdly, we will calculate $m_P(f_t)$ and $m_P(g_t)$ at the singular point $P = (\alpha, \beta, 1)$ where $\alpha \neq 1$, $\beta \neq 1$ and $\lambda = 1$, i.e., $\alpha = \beta$ but $\alpha, \beta \neq 1$. Since it is a singular point, $F_0 = F_1 = 0$ and we have to check F_{2^i} vanishes at P or not. We have the following equalities for F_{2^i}, W_0 and W_1.

$$\begin{aligned} F_{2^i} &= (\alpha^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})x^{2^i} \\ &\quad + (\beta^{2^i(l-1)+1} + \lambda^{2^i(l-1)+1})y^{2^i} \\ &= (\alpha^{2^i(l-1)+1} + 1)x^{2^i} + (\alpha^{2^i(l-1)+1} + 1)y^{2^i} \end{aligned}$$

$$\begin{aligned} W_0 &= 0 \\ W_1 &= (\beta^2 + 1)x + (\alpha^2 + 1)y \\ &= (\alpha^2 + 1)x + (\alpha^2 + 1)y \end{aligned}$$

Since $\alpha^{2^i(l-1)+1} \neq 1$, $F_{2^i} \neq 0$, that is $m_P(f_t) = 2^i$. Note that $\alpha^2 \neq 1$, then $m_P(w) = 1$ and $m_P(g_t) = 2^i - 1$.

The calculations for the number of the singular points and their multiplicities other than Type 2.2. are very similar. Therefore, the number of singular point according to their types and the multiplicities at these point of f_t and g_t are as follows.

$\gcd(l, 2^i - 1) = 1$			
Type	Number of Points	$m_P(f_t)$	$m_P(g_t)$
Type 1	1	$2^i + 1$	$2^i - 2$
Type 2	$3(l-1)$	2^i	$2^i - 1$
Type 3	$\leq (l-1)(l-3)$	2^i	2^i

For this case, the Type 2 points belong to the Type 2.2 and the Type 3 points belong to the Type 3.2.

$\gcd(l, 2^i - 1) = l$			
Type	Number of Points	$m_P(f_t)$	$m_P(g_t)$
Type 1	1	$2^i + 1$	$2^i - 2$
Type 2	$3(l-1)$	$2^i + 1$	2^i
Type 3	$\leq (l-1)(l-3)$	$2^i + 1$	$2^i + 1$

For this case, Type 2 points belong to Type 2.1 and Type 3 points belong to Type 3.1.

For the case $1 < \gcd(l, 2^i - 1) < l$, singular points of f_t are with multiplicity 2^i and $2^i + 1$, then the table for singular points for this case is quite similar with two tables above.

The essential work to show our main goal for monomial case uses Bezout's theorem. Because of this reason, we will state Bezout's theorem for projective curves.

Theorem 4.2.14. *(Bezout's Theorem) [11, Theorem 5.3] Let g and h be two projective curves of degree d_1 and d_2 respectively. The intersection number of g and h at the point P is denoted by $I(P, g, h)$. Assume that g and h have no common component. Then,*

$$\sum_P I(P, g, h) = d_1 d_2.$$

Here, we have to make some observations. The sum runs over all points P in $\bar{K} \times \bar{K}$ where K is a field, but if g or h does not go through P then $I(P, g, h) = 0$. Since the sum counts the multiplicity of intersection points, the sum runs over the singular points of the product gh. We know that $m_P(gh) = m_P(g) + m_P(h)$, that is $m_P(gh) \geq 2$ when P is an intersection point of g and h. The point P might be a singular points of gh where P is not an intersection point of g and h, but it gives $I(g, h, P) = 0$. It implies that we can take this sum over the singular points of gh.

Proposition 4.2.15. *[11, Section 3.3] Let g and h be two projective curves over a field K and $g = g_1 g_2$. Then,*

$$I(P, g, h) = I(P, g_1 g_2, h) = I(P, g_1, h) + I(P, g_2, h).$$

Observation 4.2.16. *Using the proposition above, we can generalize Bezout's theorem for more than two curves. Let $f_1, f_2, \ldots, f_n$ be projective curves, then we have*

$$\sum_P \sum_{1 \leq i < j \leq n} I(P, f_i, f_j) = \sum_{1 \leq i < j \leq n} deg(f_i) deg(f_j).$$

Proposition 4.2.17. *[11, Section 3.3] Let g and h be two projective curves over a field K. Then,*

$$I(P, g, h) \geq m_P(g) m_P(h).$$

The equality holds if and only if the tangent cones of g and h do not share any linear factor.

Therefore, we are able to use Bezout's theorem when we separate a curve into its components using Proposition 4.2.15 and Proposition 4.2.17.

The main theorem in [13] which states $g_t(x, y, 1)$ always has an absolutely irreducible factor over $\mathbb{F}_2$ when $\gcd(2^i - 1, l) = l$, is a complementary proof. As they showed for the case $\gcd(2^i - 1, l) = l$, we can ask for the case $\gcd(2^i - 1, l) < l$. D. Jedlicka proved in [16] that $g_t(x, y, 1)$ has an absolutely irreducible factor over

$\mathbb{F}_2$ whenever $\gcd(2^i - 1, l) < l$ and t is not a Gold or Kasami-Welch exponent. F. Hernando and G. McGuire proved that for the case $\gcd(2^i - 1, l) = l$ which finishes the proof of the conjecture which states the only exceptional APN monomials are Gold and Kasami-Welch functions.

Theorem 4.2.18. *[13, Theorem 16] If $l \mid 2^i - 1$ but $l \neq 2^i - 1$, then $g_t(x, y, 1)$ always has an absolutely irreducible factor over $\mathbb{F}_2$.*

To be able to prove this theorem, we have to state following lemmas which will be used in the proof.

Lemma 4.2.19. *[18, Lemma 3.1] Suppose that $p(x) \in \mathbb{F}_q[x_1, \ldots, x_n]$ is of degree d and it is irreducible in $\mathbb{F}_q[x_1, \ldots, x_n]$. There exists $r \in \mathbb{N}$ such that $r \mid d$ and an irreducible polynomial $h(x) \in \mathbb{F}_{q^r}[x_1, \ldots, x_n]$ of degree $\frac{r}{d}$ such that*

$$p(x) = c \prod_{\sigma \in G} \sigma(h(x))$$

where $G = Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ and $c \in \mathbb{F}_q$. Furthermore, if $p(x)$ is homogenous then $h(x)$ is also homogenous.

Lemma 4.2.20. *[13, Lemma 4] If $F_{2^i} \neq 0$ then $F_{2^i} = (Ax + By)^{2^i}$ where $A^{2^i} = \alpha^{1-2^i} + \lambda^{1-2^i}$ and $B^{2^i} = \beta^{1-2^i} + \lambda^{1-2^i}$.*

Lemma 4.2.21. *[13, Lemma 5] F_{2^i+1} has $2^i + 1$ distinct linear factors.*

Lemma 4.2.22. *[13, Lemma 14] If $l \mid 2^i - 1$ but $l \neq 2^i - 1$, then*

$$\deg(g_t)^2 > \sum_P m_P(g_t)^2$$

where P runs over singular points of g_t.

Lemma 4.2.23. *[13, Lemma 17] Suppose that $g_t(x, y, 1)$ splits into $\mathbb{F}_2$-irreducible factors, $g_t = f_1 f_2 \ldots f_r$ and each factor f_i where $1 \leq i \leq r$ splits irreducible factors, $f_i = f_{i,1} \ldots f_{i,n}$. Then all components satisfies the following inequalities.*

$$\deg(f_i)^2 \leq \sum_P m_P(f_i)^2$$

$$\sum_{1 \leq k < l \leq n} m_P(f_{i,k}) m_P(f_{i,l}) \leq m_P(f_i)^2 \frac{(n-1)}{2n}$$

where P runs over the singular points of g_t.

Now, we will prove Theorem 4.2.18.

Proof of Theorem 4.2.18. Suppose that $g_t(x, y, 1)$ splits into $\mathbb{F}_2$-irreducible components, $g_t = f_1 f_2 \ldots f_r$ and each factor f_i splits into absolutely irreducible components, $f_i = f_{i,1} f_{i,2} \ldots f_{i,n_i}$.

By Lemma 4.2.19, we know that each $f_{i,j}$ where $1 \leq j \leq n_i$ has degree $\frac{\deg(f_i)}{n_i}$. Applying Bezout's theorem to the product

$$g_t = f_1 f_2 \dots f_r = (f_{1,1} \dots f_{1,n_1}) \dots (f_{r,1} \dots f_{r,n_r}),$$

we obtain for the intersection multiplicities (left hand side of Bezout's theorem) by Proposition 4.2.15, as follows.

$$\sum_{i=1}^{r} \sum_{1 \leq k < l \leq n_i} \sum_{P} I(P, f_{i,k}, f_{i,l}) + \sum_{1 \leq i < j \leq r} \sum_{\substack{1 \leq k \leq n_i \\ 1 \leq l \leq n_j}} \sum_{P} I(P, f_{i,k}, f_{j,l}) \tag{4.2.4}$$

Here, the sums runs over the singular points P of g_t and when it writes a sum which runs over P, it refers to the singular points of g_t in the continuation of this proof.

The first sum is for factors of each f_i and the second sum is for cross factors between f_i and f_j. By Lemma 4.2.20 and Lemma 4.2.21, for every i and k the tangent cones of the $f_{i,k}$ contains different lines and the sum 4.2.4 becomes to the following by Proposition 4.2.17.

$$\sum_{P} \left[\sum_{i=1}^{r} \sum_{1 \leq k < l \leq n_i} m_P(f_{i,k}) m_P(f_{i,l}) + \sum_{1 \leq i < j \leq r} \sum_{\substack{1 \leq k \leq n_i \\ 1 \leq l \leq n_j}} m_P(f_{i,k}) m_P(f_{j,l}) \right] \tag{4.2.5}$$

Note that

$$\begin{aligned}
(m_P(g_t))^2 &= \Big(\sum_{i=1}^{r} m_P(f_i) \Big)^2 \\
&= \sum_{i=1}^{r} m_P(f_i)^2 + 2 \Big(\sum_{1 \leq i < j \leq r} m_P(f_i) m_P(f_j) \Big) \\
&= \sum_{i=1}^{r} m_P(f_i)^2 + 2 \sum_{1 \leq i < j \leq r} \left(\Big(\sum_{k=1}^{n_i} m_P(f_{i,k}) \Big) \Big(\sum_{l=1}^{n_j} m_P(f_{j,l}) \Big) \right) \\
&= \sum_{i=1}^{r} m_P(f_i)^2 + 2 \sum_{1 \leq i < j \leq r} \sum_{\substack{1 \leq k \leq n_i \\ 1 \leq l \leq n_j}} m_P(f_{i,k}) m_P(f_{j,l})
\end{aligned}$$

Substituting this equality, the sum in 4.2.5 becomes the following.

$$\sum_{P} \left[\sum_{i=1}^{r} \sum_{1 \leq k < l \leq n_i} m_P(f_{i,k}) m_P(f_{i,l}) + \frac{1}{2} \Big(m_P(g_t)^2 - \sum_{i=1}^{r} m_P(f_i)^2 \Big) \right] \tag{4.2.6}$$

Using the second inequality in Lemma 4.2.23, the sum 4.2.6 is less than or equal to the following.

$$\sum_{P}\left[\sum_{i=1}^{r} m_P(f_i)^2\frac{n_i-1}{2n_i}+\frac{1}{2}\Big(m_P(g_t)^2-\sum_{i=1}^{r} m_P(f_i)^2\Big)\right]$$
$$=\frac{1}{2}\sum_{P}\left[m_P(g_t)^2-\sum_{i=1}^{r}\frac{m_P(f_i)^2}{n_i}\right]$$

We will consider the right hand side of Bezout's theorem which is related to the degrees. By Observation 4.2.16, we have the following sum for the right hand side of the equality in Bezout's theorem.

$$\sum_{i=1}^{r}\sum_{1\le k<l\le n_i}\deg(f_{i,k})\deg(f_{i,l})+\sum_{1\le i<j\le r}\sum_{\substack{1\le k\le n_i\\1\le l\le n_j}}\deg(f_{i,k})\deg(f_{j,l}) \tag{4.2.7}$$

We know from Lemma 4.2.19, each $f_{i,k}$ has the same degree for all k, then the first sum in 4.2.7 becomes the following.

$$\sum_{i=1}^{r}\deg(f_i)^2\frac{(n_i-1)}{2n_i}=\frac{1}{2}\sum_{i=1}^{r}\deg(f_i)^2-\frac{1}{2}\sum_{i=1}^{r}\frac{\deg(f_i)^2}{n_i} \tag{4.2.8}$$

Note that

$$\begin{aligned}(\deg(g_t))^2&=\Big(\sum_{i=1}^{r}\deg(f_i)\Big)^2\\&=\sum_{i=1}^{r}\deg(f_i)^2+2\Big(\sum_{1\le i<j\le r}\deg(f_i)\deg(f_j)\Big)\\&=\sum_{i=1}^{r}\deg(f_i)^2+2\sum_{1\le i<j\le r}\left(\Big(\sum_{k=1}^{n_i}\deg(f_{i,k})\Big)\Big(\sum_{l=1}^{n_j}\deg(f_{j,l})\Big)\right)\\&=\sum_{i=1}^{r}\deg(f_i)^2+2\sum_{1\le i<j\le r}\sum_{\substack{1\le k\le n_i\\1\le l\le n_j}}\deg(f_{i,k})\deg(f_{j,l})\end{aligned}$$

Substituting Equation 4.2.8 and the note above into the sum in 4.2.7, it becomes the following.

$$\frac{1}{2}\Big(\deg(g_t)^2-\sum_{i=1}^{r}\frac{\deg(f_i)^2}{n_i}\Big) \tag{4.2.9}$$

To summarize the paragraphs above, we showed the followings.

$$\sum_{i=1}^{r} \sum_{1\le k<l\le n_i} \sum_{P} I(P, f_{i,k}, f_{i,l}) + \sum_{1\le i<j\le r} \sum_{\substack{1\le k\le n_i \\ 1\le l\le n_j}} \sum_{P} I(P, f_{i,k}, f_{j,l}) \le \frac{1}{2} \sum_{P} \left[m_P(g_t)^2 - \sum_{i=1}^{r} \frac{m_P(f_i)^2}{n_i} \right]$$

$$\sum_{i=1}^{r} \sum_{1\le k<l\le n_i} \deg(f_{i,k}) \deg(f_{i,l}) + \sum_{1\le i<j\le r} \sum_{\substack{1\le k\le n_i \\ 1\le l\le n_j}} \deg(f_{i,k}) \deg(f_{j,l}) = \frac{1}{2} \Big(\deg(g_t)^2 - \sum_{i=1}^{r} \frac{\deg(f_i)^2}{n_i} \Big)$$

Using Bezout's theorem, we have the following inequality.

$$\deg(g_t)^2 - \sum_{i=1}^{r} \frac{\deg(f_i)^2}{n_i} \le \sum_{P} \left[m_P(g_t)^2 - \sum_{i=1}^{r} \frac{m_P(f_i)^2}{n_i} \right]$$

By Lemma 4.2.22, we know that $\deg(g_t)^2 > \sum_P m_P(g_t)^2$. We also know by the first inequality in Lemma 4.2.23 that $\sum_{i=1}^{r} \frac{\deg(f_i)^2}{n_i} \le \sum_{i=1}^{r} \frac{m_P(f_i)^2}{n_i}$. It leads to a contradiction. Hence, at least one of the factors of g_t cannot splits into its factors, i.e., g_t has an absolutely irreducible factor. □

Chapter 5

The Gold and Kasami-Welch Functions

In previous section, we showed that the monomials different from Gold and Kasami-Welch functions cannot be an exceptional APN functions. In this chapter, we will show that Gold and Kasami- Welch functions are exceptional APN functions using the method which we mentioned in previous chapter.

5.1 The Gold Function

In this section, we will show that the Gold monomial, $F(x) = x^{2^i+1}$, is an exceptional APN function. Recall that $F(x)$ is APN if and only if the only solutions of $F(x) + F(y) + F(z) + F(x + y + z) = 0$ are $x = y$, $y = z$ or $x = z$. Hence, we consider the polynomial

$$g_t(x, y, z) = \frac{f_t(x, y, z)}{(x + y)(x + z)(y + z)} = \frac{x^t + y^t + z^t + (x + y + z)^t}{(x + y)(x + z)(y + z)}.$$

$g_t(x, y, z)$ is a homogenous of degree $t - 3$ and it defines a projective curve. We consider the affine part of this curve, i.e., $z = 1$.

$$g_t(x, y, 1) = \frac{f_t(x, y, 1)}{(x + y)(x + 1)(y + 1)} = \frac{x^t + y^t + 1 + (x + y + 1)^t}{(x + y)(x + 1)(y + 1)}.$$

Proposition 5.1.1. *$f_t(x, y, 1) = 0$ has no rational points over $\mathbb{F}_{2^n}$ besides with $x = y$, $x = 1$ and $y = 1$ if and only if x^t is APN over $\mathbb{F}_{2^n}$.*

Proof. By Theorem 4.1.3, we know that $F(x) = x^t$ is APN if and only if the affine curve $F(x)+F(y)+1+F(x+y+1) = x^t+y^t+1+(x+y+1)^t = 0$ has all rational points on the surface defined by $(x+y)(x+1)(y+1) = 0$. Hence, $F(x) = x^t$ is APN if and only if $f_t(x, y, 1) = 0$ has no rational points over $\mathbb{F}_{2^n}$ except $x = y$, $x = 1$ and $y = 1$. □

We will prove that $f_t(x, y, 1) = 0$ has no rational points except $x = y$, $x = 1$ and $y = 1$, when $t = 2^i + 1$ on $\mathbb{F}_{2^n}$ if and only if $\gcd(i, n) = 1$.

Theorem 5.1.2. *The Gold function, defined as $F(x) = x^{2^i+1}$, is exceptional APN.*

Proof. Using Proposition 5.1.1, we want to show that $f_t(x,y,1) = x^t + y^t + 1 + (x + y + 1)^t = 0$ has no rational points over $\mathbb{F}_{2^n}$ besides with $x = y$, $x = 1$ and $y = 1$, when $t = 2^i + 1$ and $\gcd(i,n) = 1$.

We replace x and y by $x + 1$ and $y + 1$, respectively. We have the following equalities.

$$\begin{aligned}
f_t(x+1,y+1,1) &= (x+1)^{2^i+1} + (y+1)^{2^i+1} + 1 + (x+y+1)^{2^i+1} \\
&= (x+1)(x+1)^{2^i} + (y+1)(y+1)^{2^i} + 1 + (x+y+1)(x+y+1)^{2^i} \\
&= x^{2^i+1} + x + x^{2^i} + 1 + y^{2^i+1} + y + y^{2^i} + 1 + 1 + x^{2^i+1} \\
&+ xy^{2^i} + x + yx^{2^i} + y^{2^i+1} + y + x^{2^i} + y^{2^i} + 1 \\
&= xy^{2^i} + yx^{2^i} \\
&= xy(x^{2^i-1} + y^{2^i-1}) \\
&= xy\Big(y^{2^i-1}(\frac{x}{y})^{2^i-1} + y^{2^i-1}\Big) \\
&= xy^{2^i}\Big((\frac{x}{y})^{2^i-1} + 1\Big)
\end{aligned}$$

Setting $z = \frac{x}{y}$, we obtain for the polynomial $\Big((\frac{x}{y})^{2^i-1} + 1\Big)$ that

$$z^{2^i-1} + 1 = \prod_{\substack{\alpha \in \mathbb{F}_{2^i} \\ \alpha \neq 0}} z + \alpha.$$

Then, we have the following equalities.

$$\begin{aligned}
f_t(x+1,y+1,1) &= xy^{2^i}\Big(\prod_{\substack{\alpha \in \mathbb{F}_{2^i} \\ \alpha \neq 0}} (\frac{x}{y} + \alpha)\Big) \\
&= xy^{2^i}\Big(\prod_{\substack{\alpha \in \mathbb{F}_{2^i} \\ \alpha \neq 0}} \frac{x + \alpha y}{y}\Big) \\
&= xy\Big(\prod_{\substack{\alpha \in \mathbb{F}_{2^i} \\ \alpha \neq 0}} (x + \alpha y)\Big) \\
&= y\Big(\prod_{\alpha \in \mathbb{F}_{2^i}} (x + \alpha y)\Big)
\end{aligned}$$

Now, we replace x and y by $x + 1$ and $y + 1$, respectively, and we will obtain again $f_t(x,y,1)$, since characteristic is 2.

$$f_t(x,y,1) = (y+1) \prod_{\alpha \in \mathbb{F}_{2^i}} (x + 1 + \alpha y + \alpha)$$

In what follows, we will show that the polynomial which we will find by dividing $f_t(x,y,1)$ by $(x+y)(x+1)(y+1)$ has no rational points over $\mathbb{F}_{2^n}$ when $\gcd(i,n) = 1$.

It can be seen that $(y+1)$ divides $f_t(x,y,1) = (y+1)\prod_{\alpha\in\mathbb{F}_{2^i}}(x+1+\alpha y+\alpha)$. When $\alpha = 0$ and $\alpha = 1$, we obtain factors $(x+1)$ and $(x+y)$, respectively. Then we have the following polynomial.

$$g_t(x,y,1) = \prod_{\substack{\alpha\in\mathbb{F}_{2^i}\\ \alpha\notin\{0,1\}}} (x+1+\alpha y+\alpha)$$

Suppose that $g_t(a,b,1) = 0$ for some $a,b \in \mathbb{F}_{2^n}$ with $a \neq b$, $a \neq 1$ and $b \neq 1$. By factorization of $g_t(x,y,1)$ above, we have $a+1+\alpha b+\alpha = 0$ where $\alpha \neq 0,1$ and $\alpha \in \mathbb{F}_{2^i}$. That is, $\alpha = \dfrac{a+1}{b+1}$. Since $a,b \in \mathbb{F}_{2^n}$ and $\alpha \in \mathbb{F}_{2^i}$, $\dfrac{a+1}{b+1}$ should lie in $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^i}$. Since $\gcd(i,n) = 1$, we have $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^i} = \{0,1\}$. Therefore, $\frac{a+1}{b+1} = 0$ or $\frac{a+1}{b+1} = 1$. Since $a \neq 1$ and $a \neq b$, it is a contradiction. Hence, $f_t(x,y,1) = 0$ has no rational points over $\mathbb{F}_{2^n}$ except $x = y$, $x = 1$ and $y = 1$ when $\gcd(i,n) = 1$. By Proposition 5.1.1, we conclude that $F(x) = x^{2^i+1}$ is APN over $\mathbb{F}_{2^n}$ when $\gcd(i,n) = 1$. Thus, $F(x) = x^{2^i+1}$ is exceptional APN, since there are infinitely many n where $\gcd(i,n) = 1$. □

Hence, we showed that the Gold function is an exceptional function, i.e., it is an APN function on $\mathbb{F}_{2^n}$ for infinitely many n where $\gcd(i,n) = 1$.

5.2 The Kasami-Welch Function

In this section, we will show that the Kasami-Welch monomial is an exceptional APN function using methods we mentioned in Chapter 4. To show that the Kasami-Welch function is an exceptional APN function, we need to prove the following claims and lemmas which will be used in the proof. From now on, we fix $t = 2^{2i}-2^i+1$ which is the Kasami-Welch exponent and we will write $f_t(x,y)$ and $g_t(x,y)$ for $f_t(x,y,1)$ and $g_t(x,y,1)$, respectively.

Claim 5.2.1. *If $f_t(x,y)$ has a multiple component then $\dfrac{\partial f_t}{\partial x}$ and $\dfrac{\partial f_t}{\partial y}$ has a common factor.*

Proof. Suppose that $f_t(x,y) = s(x,y)^2 r(x,y)$ for some $s,r \in \mathbb{F}_{2^n}[x,y]$. We have the following equalities.

$$\frac{\partial f_t}{\partial x} = 2s(x,y)\frac{\partial s(x,y)}{\partial x}r(x,y) + s(x,y)^2\frac{\partial r(x,y)}{\partial x}$$
$$\frac{\partial f_t}{\partial y} = 2s(x,y)\frac{\partial s(x,y)}{\partial y}r(x,y) + s(x,y)^2\frac{\partial s(x,y)}{\partial y}$$

Then, $\dfrac{\partial f_t}{\partial x}$ and $\dfrac{\partial f_t}{\partial y}$ have a common factor. □

Claim 5.2.2. *There exist $2^{2i} - 32^i + 3$ many (α,β) such that α, β and $\alpha+\beta+1$ are (2^i-1)-th root of unity.*

Proof. Note that α is 2^i-th root of unity if and only if $\alpha \in \mathbb{F}_{2^i} \setminus \{0\} = \mathbb{F}_{2^i}{}^*$. There are 2^i pairs of $(\alpha, \beta) \in \mathbb{F}_{2^i} \times \mathbb{F}_{2^i}$ such that $\alpha + \beta + 1 = 0$. Namely $(\alpha, \alpha + 1)$ for $\alpha \in \mathbb{F}_{2^i}$. However, the pairs $(0, 1)$ and $(1, 0)$ is not included in (α, β), since $\alpha, \beta \in \mathbb{F}_{2^i}{}^*$. Then, there are $(2^i - 1)^2 - (2^i - 2)$ pairs where $\alpha, \beta, \alpha + \beta + 1$ lie in $\mathbb{F}_{2^i}{}^*$. Hence, there are $2^{2^i} - 32^i + 3$ pairs (α, β) such that α, β and $\alpha + \beta + 1$ are $(2^i - 1)$-th root of unity. □

Now, we will investigate the multiplicities of singular points of $f_t(x, y)$ where $t = 2^{2i} - 2^i + 1$. Recall the forms of $f_t(x + \alpha, y + \beta)$ as follows.

$$F_0 = 1 + \alpha^t + \beta^t + (\alpha + \beta + 1)^t$$
$$F_1 = (\alpha^{t-1} + \lambda^{t-1})x^{t-1} + (\beta^{t-1} + \lambda^{t-1})y$$
$$F_{2^i} = (\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i}$$
$$F_{2^i+1} = (\alpha^{t-2^i-1} + \lambda^{t-2^i-1})x^{2^i+1} + (\beta^{t-2^i-1} + \lambda^{t-2^i-1})y^{2^i+1} + \lambda^{t-2^i-1}(x^{2^i}y + xy^{2^i})$$

Recall that $\lambda = \alpha + \beta + 1$.

Claim 5.2.3. *If $P = (\alpha, \beta)$ is a singular point of $f_t(x, y)$ then $m_P(f_t) = 2^i + 1$.*

Proof. Suppose that $P = (\alpha, \beta)$ is a singular point of $f_t(x, y)$. We know that if P is a singular point, then $\alpha, \beta, \alpha + \beta + 1 \in \mathbb{F}_{2^i}{}^*$ from Chapter 4. Since P is a singular point, $F_0 = F_1 = 0$. Then, we look at F_{2^i} and F_{2^i+1}.

$$F_{2^i} = (\alpha^{t-2^i} + \lambda^{t-2^i})x^{2^i} + (\beta^{t-2^i} + \lambda^{t-2^i})y^{2^i}$$

Since $t - 2^i = 2^{2i} - 2^i + 1 - 2^i = 2^i(2^i - 1) - (2^i - 1) = (2^i - 1)^2$, we obtain that $\alpha^{t-2^i} = \beta^{t-2^i} = (\alpha + \beta + 1)^{t-2^i} = 1$, because $\alpha, \beta, \lambda = \alpha + \beta + 1 \in \mathbb{F}_{2^i}{}^*$. Then, we have $F_{2^i} = \left(x^{2^i} + y^{2^i} + (x + y)^{2^i}\right) = 0$, since $(x + y)^{2^i} = x^{2^i} + y^{2^i}$. Now, we will check $F_{2^i+1} \neq 0$.

$$F_{2^i+1} = (\alpha^{t-2^i-1} + \lambda^{t-2^i-1})x^{2^i+1} + (\beta^{t-2^i-1} + \lambda^{t-2^i-1})y^{2^i+1} + \lambda^{t-2^i-1}(x^{2^i}y + xy^{2^i})$$

Note that the coefficient of $(x^{2^i}y + xy^{2^i})$ which is $\lambda^{2^i(2^i-2)}$ is not zero. Then, $F_{2^i+1} \neq 0$. Hence, $m_P(f_t) = 2^i + 1$. □

Proposition 5.2.4. *[15, Proposition A] Let $\mathcal{C}$ be a projective plane curve of degree d over an algebraically closed field. Suppose that $\mathcal{C}$ has no multiple components and has N simple components. Then, the following inequality holds.*

$$\sum_P \frac{m_P(m_P - 1)}{2} \leq \frac{(d - 1)(d - 2)}{2} + N - 1$$

where the sum runs over the singular points P of $\mathcal{C}$.

Suppose that $f_t(x, y)$ has a multiple factor where $t = 2^{2i} - 2^i + 1$. We know that if $f_t(x, y)$ has a multiple component then its partial derivatives will have a common

factor by Claim 5.2.1.

$$\begin{aligned}\frac{\partial f_t}{\partial x} &= tx^{t-1} + t(x+y+1)^{t-1} \\ &= (x^{2^i-1} + (x+y+1)^{2^i-1})^{2^i} \\ &= \Big(\prod_{a \in \mathbb{F}_{2^i}{}^*} (y + (1+a)x + 1) \Big)^{2^i}\end{aligned}$$

$$\begin{aligned}\frac{\partial f_t}{\partial y} &= ty^{t-1} + t(x+y+1)^{t-1} \\ &= (y^{2^i-1} + (x+y+1)^{2^i-1})^{2^i} \\ &= \Big(\prod_{a \in \mathbb{F}_{2^i}{}^*} (x + (1+a)y + 1) \Big)^{2^i}\end{aligned}$$

There is no factor $by + x + 1$ with $b \neq 0$ of $\frac{\partial f_t}{\partial y}$ is equal to a scalar multiple of any factor $y + cx + 1$ with $c \neq 0$ of $\frac{\partial f_t}{\partial x}$. Thus, $f_t(x, y)$ does not have a multiple component. Therefore, we can calculate the number of simple components of $f_t(x, y)$ using Proposition 5.2.4. Note that, it is the number of absolutely irreducible components of f_t.

We know that the number of the singular points of $f_t(x, y)$ is $2^{2i} - 32^i + 3$ by Claim 5.2.2 and we know that $f_t(x, y)$ has no singular point at infinity. Since the multiplicity of all singular points is $2^i + 1$ by Claim 5.2.3, we can give a lower bound for the number of absolutely irreducible components of f_t, namely N, using Proposition 5.2.4 as follows.

$$\begin{aligned}\sum_P \frac{m_P(m_P - 1)}{2} &\leq \frac{(n-1)(n-2)}{2} + N - 1 \\ (2^{2i} - 32^i + 3)\frac{(2^i+1)2^i}{2} &\leq \frac{(t-1)(t-2)}{2} + N - 1\end{aligned}$$

We obtain $N \geq 2^i + 1$ from the inequality above. Therefore, we can say that f_t has at least $2^i + 1$ many absolutely irreducible factors. Since $g_t(x, y) = \dfrac{f_t(x, y)}{(x+y)(x+1)(y+1)}$, $g_t(x, y)$ has at least $2^i - 2$ absolutely irreducible factor.

We will give the following proposition to show our main aim which will be stated after the proposition.

Proposition 5.2.5. *[15, Proposition B] Let $p(x, y)$ be a polynomial over a field K. Supposse that $p(x, 0)$ can be written as*

$$p(x, 0) = g_0(x)h_0(x)$$

with the property $\deg(p(x)) = \deg(p(x, 0)) = \deg(g_0(x)) + \deg(h_0(x))$ where $g_0(x)$ and $h_0(x)$ are relatively prime polynomials in $K[x]$. Then, there exists at most one

pair of polynomials $G(x,y)$, $H(x,y)$ in any extension of K such that

$$p(x,y) = G(x,y)H(x,y)$$

and $G(x,0) = g_0(x)$, $H(x,0) = h_0(x)$. In addition, if the polynomials $G(x,y)$ and $H(x,y)$ exist then all coefficients of $G(x,y)$ and $H(x,y)$ are in K.

Aim: $g_t(x,y)$ has exactly $2^i - 2$ absolutely irreducible factors. In particular,

$$g_t(x,y) = \prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} p_a(x,y)$$

such that $p_a(x,y)$ is absolutely irreducible of degree 2^i+1 with $p_a(x,0) = (x+a)^{2^i+1}$.

Proof of the Aim. Let $c_0(x) = g_t(x,0) = \dfrac{f_t(x,0)}{x(x+1)} = \dfrac{x^t + 1 + (x+1)^t}{x(x+1)}$ where $t = 2^{2i} - 2^i + 1$. We have the following equalities for $f_t(x,0)$.

$$\begin{aligned}
f_t(x,0) &= x^{2^{2i}-2^i+1} + 1 + (x+1)^{2^{2i}-2^i+1} = \frac{x^{2^{2i}+1}}{x^{2^i}} + 1 + \frac{(x+1)^{2^{2i}+1}}{(x+1)^{2^i}} \\
&= \frac{x^{2^{2i}+1}(x+1)^{2^i} + x^{2^i}(x+1)^{2^i} + (x+1)^{2^{2i}+1}x^{2^i}}{(x(x+1))^{2^i}} \\
&= \frac{x^{2^{2i}+1}(x^{2^i}+1) + x^{2^i}(x^{2^i}+1) + (x^{2^{2i}+1} + x^{2^{2i}} + x + 1)x^{2^i}}{(x(x+1))^{2^i}} \\
&= \frac{x^{2^i(2^i+1)} + x^{2^{2i}+1} + x^{2^{i+1}} + x^{2^i+1}}{(x(x+1))^{2^i}} \\
&= \frac{(x^{2^i})^{2^i+1} + (x^{2^i})^{2^i}x + x^{2^i}x^{2^i} + x^{2^i+1}}{(x(x+1))^{2^i}} \\
&= \frac{(x^{2^i}+x)^{2^i+1}}{(x(x+1))^{2^i}}
\end{aligned}$$

Then, we obtain $c_0(x)$ as follows.

$$\begin{aligned}
c_0(x) = g_t(x,0) &= \frac{(x^{2^i}+x)^{2^i+1}}{(x(x+1))^{2^i}}\Big(\frac{1}{x(x+1)}\Big) \\
&= \Big(\frac{x^{2^i}+x}{x(x+1)}\Big)^{2^i+1}
\end{aligned}$$

Since $x^{2^i} + x = \prod_{a \in \mathbb{F}_{2^i}} x + a$, we have

$$c_0(x) = g_t(x,0) = \Big(\prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} x + a\Big)^{2^i+1} = \prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} (x+a)^{2^i+1}.$$

Write $g_t(x,y) = c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3}$.

Claim 5.2.6. $(x+1)^2c_0(x) + (x^2+x)c_1(x) = (x+1)^{t-1}$ *where* $t = 2^{2i} - 2^i + 1$.

Proof. Note that $g_t(x,y)(x+y)(x+1)(y+1) = f_t(x,y) = x^t + y^t + 1 + (x+y+1)^t$. Substituting $g_t(x,y) = c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3}$ to this equation, we obtain the following equalities.

$$\begin{aligned}
&(c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3})\Big((x+y)(x+1)(y+1)\Big) \\
&= (c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3})(x^y + xy^2 + x^2 + y^2 + x + y) \\
&= x^t + y^t + 1 + (x+y+1)^t
\end{aligned}$$

We check the coefficients of y in the equality above. The coefficient of y in $(c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3})(x^y + xy^2 + x^2 + y^2 + x + y)$ is $c_0(x)(x^2+1) + c_1(x)(x^2+x)$. The coefficient of y in $x^t + y^t + 1 + (x+y+1)^t$ is $t(x+1)^{t-1} = (x+1)^{t-1}$. Hence, we have

$$c_0(x)(x^2+1) + c_1(x)(x^2+x) = (x+1)^{t-1}.$$

□

Claim 5.2.7. *Suppose that* $g_t(x,y) = G(x,y)H(x,y)$ *in* $\bar{\mathbb{F}}_2[x,y]$. *If* $\gcd(c_0(x), c_1(x)) = 1$ *then* $\gcd(G(x,0), H(x,0)) = 1$.

Proof. Suppose on the contrary that $\gcd(c_0(x), c_1(x)) = 1$ and $\gcd(G(x,0), H(x,0)) \neq 1$.

$$G(x,0) = g_0(x) = p_0(x)\tilde{g_0}(x)$$
$$H(x,0) = h_0(x) = p_0(x)\tilde{h_0}(x)$$

We wrote $g_t(x,y) = c_0(x) + c_1(x)y + \ldots + c_{t-3}(x)y^{t-3}$. We know also that $g_t(x,y) = G(x,y)H(x,y)$. Then, we have the following equalities.

$$\begin{aligned}
g_t(x,y) &= G(x,y)H(x,y) \\
&= (g_0(x) + g_1(x)y + \ldots)(h_0(x) + h_1(x)y + \ldots) \\
&= (p_0(x)\tilde{g_0}(x) + g_1(x)y + \ldots)(p_0(x)\tilde{h_0}(x) + h_1(x)y + \ldots) \\
&= p_0(x)^2\tilde{g_0}(x)\tilde{h_0}(x) + \Big(p_0(x)\tilde{g_0}(x)h_1(x) + p_0(x)\tilde{h_0}(x)g_1(x)\Big)y + \ldots
\end{aligned}$$

Thus, we can conclude that

$$c_0(x) = p_0(x)^2\tilde{g_0}(x)\tilde{h_0}(x)$$

and

$$c_1(x) = p_0(x)\tilde{g_0}(x)h_1(x) + p_0(x)\tilde{h_0}(x)g_1(x).$$

It gives us a contradiction with $\gcd(c_0(x), c_1(x)) = 1$, since $c_0(x)$ and $c_1(x)$ has common factor $p_0(x)$.

Continuation of Proof of the Aim. Recall that

$$c_0(x) = \prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} (x+a)^{2^i+1} \tag{5.2.1}$$

Suppose that $\gcd(c_0(x), c_1(x)) \neq 1$. Then, by Equation 5.2.1, there exists an $a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2$ such that $x+a$ divides both $c_0(x)$ and $c_1(x)$. Then, $x+a$ divides $c_0(x)(x^2+1) + c_1(x)(x^2+x)$. By Claim 5.2.6, we know that $c_0(x)(x^2+1) + c_1(x)(x^2+x) = (x+1)^{t-1}$. Then, $x+a$ divides $(x+1)^{t-1}$ which is a contradiction. Therefore, $\gcd(c_0(x), c_1(x)) = 1$. Hence, we have $g_t(x,0) = G(x,0)H(x,0) = g_0(x)h_0(x)$ with $\gcd(g_0(x), h_0(x)) = 1$ and

$$c_0(x) = g_0(x)h_0(x) = \prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} (x+a)^{2^i+1}.$$

We observe that

$$\deg(g_t(x,0)) = \deg_x(g_t(x,y)) = \deg(g_t(x,y)).$$

Then, for any factor $p(x,y)$ of $g_t(x,y)$, we have

$$\deg(p(x,0)) = \deg_x(p(x,y)).$$

Hence, for an absolutely irreducible factor $p(x,y)$ of $g_t(x,y)$, we have $\deg(p(x,0)) > 0$. If $x+a$ divides $p(x,0)$, then $(x+a)^{2^i+1}$ divides $p(x,0)$. Thus, $g_t(x,y)$ cannot have more than 2^i-2 factors. That is, $g_t(x,y)$ has exactly 2^i-2 factors $p_a(x,y)$ for $a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2$ and $p_a(x,0) = (x+a)^{2^i+1}$. Then, by Proposition 5.2.5, $p_a(x,y) \in \mathbb{F}_{2^i}[x,y]$. □

Finally, we are going to prove that the Kasami-Welch exponent is an exceptional APN function.

Corollary 5.2.8. *The Kasami-Welch function, defined by $F(x) = x^{2^{2i}-2^i+1}$, is exceptional APN.*

Proof. It is enough to show that $F(x)$ is APN over $\mathbb{F}_{2^n}$ with $\gcd(i,n) = 1$, since there are infinitely many n which is relatively prime with i.

This holds if and only if $g_t(x,y)$ has no rational points over $\mathbb{F}_{2^n}$ different from $x=y$ or $x=1$ or $y=1$. Suppose that $g_t(x,y) = 0$. We know from the previous aim that

$$g_t(x,y) = \prod_{a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2} p_a(x,y).$$

Then, there exists a factor $p_a(x,y)$ such that $p_a(x,y) = 0$ for some $a \in \mathbb{F}_{2^i} \setminus \mathbb{F}_2$. Since $\gcd(i,n) = 1$, by Chinese Remainder theorem, there exists $m \in \mathbb{Z}^+$ such that $m \equiv 0 \mod n$ and $m \equiv 1 \mod i$. Consider the automorphism σ of $\bar{\mathbb{F}}_2$ defined by

$$\sigma(z) = z^{2^m}.$$

Since $m \equiv 0 \mod n$, we have $\sigma(z) = z^{2^m} = z$. Beside that, for any $z \in \mathbb{F}_{2^i}$, we have $\sigma(z) = z^{2^m} = z^2$, since $m \equiv 1 \mod i$.

From the previous aim, we know that $p_a(x,y) \in \mathbb{F}_{2^i}[x,y]$. Say $p_a(x,y) = \sum c_{i,j} x^i y^j$. We observe that $\sigma(p_a(x,y)) \neq p_a(x,y)$, since $\sigma(p_a(x,y)) = \sum \sigma(c_{i,j}) x^i y^j = \sum {c_{i,j}}^2 x^i y^j \neq$

$p_a(x, y)$. But $\sigma(p_a(x, y))$ also vanishes at (x, y). Therefore, the multiplicity of $g_t(x, y)$ is greater than 1 at this point (x, y), it means (x, y) is a singular point of $g_t(x, y)$. Then, x and y should lie in $\mathbb{F}_{2^i} \setminus \{0\}$. Thus, we conclude that $x, y \in {\mathbb{F}_{2^n}}^* \cap {\mathbb{F}_{2^i}}^*$. Note that ${\mathbb{F}_{2^n}}^* \cap {\mathbb{F}_{2^i}}^* = \{1\}$, since $\gcd(i, n) = 1$. That is $x = y = 1$. Hence, $g_t(x, y)$ has no $\mathbb{F}_{2^n}$ rational points other than $x = y$ or $x = 1$ or $y = 1$. □

Hence, we showed that the Kasami- Welch function is an exceptional APN function.

Chapter 6

Exceptional APN Polynomials

6.1 On Exceptional APN Polynomials

In this section, we will investigate non-monomial exceptional APN functions. We will use similar way with monomial case to determine exceptional APN functions.

Theorem 6.1.1. *[23, Theorem 4.1] Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a polynomial function. Suppose that surface $\mathcal{X}$ defined by $\dfrac{F(x)+F(y)+F(z)+F(x+y+z)}{(x+y)(y+z)(x+z)} = 0$ is absolutely irreducible (or has an absolutely irreducible component of $\mathbb{F}_2$). Then f is not an exceptional APN function.*

The approach to show that a function which is non-monomial is not an exceptional APN function is very close to the method for monomials. We are looking for being absolutely irreducible or having an absolutely irreducible component for a function F on $\mathbb{F}_{2^n}$. In this section, we will use the function $\phi(x, y, z) = \dfrac{F(x)+F(y)+F(z)+F(x+y+z)}{(x+y)(y+z)(x+z)}$ (as the same function for monomial case) and absolutely irreducibility to show a polynomial is not exceptional APN.

Aubry, McGuire and Rodier made the following conjecture in 2010 in [1].

Conjecture 6.1.2. *Up to equivalence, the Gold and Kasami-Welch functions are the only exceptional APN functions.*

Here, equivalence refers to CCZ-equivalence.

This conjecture was proved for monomial functions as we showed in previous section. Now, we will investigate APN property for non-monomial functions. We are going to investigate the polynomials in three cases. The natural way is separate polynomial according to their degree, they can be an even degree polynomial or an odd degree polynomial. First, we will look at the polynomials of odd degree which are not Gold or Kasami-Welch degree polynomials, i.e., the polynomials of odd degree but degree is not equal to $2^i + 1$ or $4^i - 2^i + 1$ for some positive integer i. After, we will examine even degree polynomials and, Gold and Kasami-Welch degree polynomials, i.e., the polynomials of degree $2^i + 1$ or $4^i - 2^i + 1$ for some positive integer i.

For the odd degree polynomials, Aubry, Mcguire and Rodier have showed in 2010 that functions of odd degree which are not Gold and Kasami-Welch number are not exceptional APN.

Theorem 6.1.3. *[1, Theorem 2.3] If the degree of F is odd and not a Gold or a Kasami-Welch number, then F is not APN for all sufficiently large extensions of $\mathbb{F}_{2^n}$.*

With this theorem, it has been shown that a big part of polynomials are not exceptional APN. There were only even degree functions and the functions of degree $2^i + 1$ and $4^i - 2^i + 1$ to show they are exceptional APN or not.

For even degree functions, Aubry, McGuire and Rodier have showed following theorem in the same article [1].

Theorem 6.1.4. *[1, Theorem 2.4] If the degree of F is $2e$ with an odd integer e, and if F contains an odd degree term, then F is not APN for all sufficiently large extensions of $\mathbb{F}_{2^n}$.*

As it can be seen in Theorem 6.1.4, they have showed for a special case of even degree function under a condition. However, Caullery has showed in 2014 the following theorem in [4].

Theorem 6.1.5. *[4, Theorem 9] If the degree of F is $4e$ with $e \geq 7$ and $e \equiv 3 \bmod 4$, then F is not APN for all sufficiently large extensions of $\mathbb{F}_{2^n}$.*

Although a big amount of even degree functions has still left, it has been shown a part of functions of even degree are not APN on $\mathbb{F}_{2^n}$ for a sufficiently large n.

We will examine the functions of degree $2^i + 1$, i.e., the Gold degree functions. To investigate these type of functions, we consider $F(x) = x^{2^i+1} + h(x)$ on $\mathbb{F}_{2^n}$ where $\deg(h(x)) < 2^i + 1$. Delgado and Janwa have showed for any odd degree $h(x)$,with a mild condition in few cases, are not exceptional APN. To show this result, they have used absolutely irreducibility of $\phi(x, y, z)$ and $\phi_t(x, y, z)$ where $\phi_t(x, y, z) = \dfrac{x^t + y^t + z^t + (x + y + z)^t}{(x + y)(y + z)(x + z)}$. As it can be observed that $\phi_t(x, y, z)$ is the same as the function $g_t(x, y, z)$ in previous section. They showed $\phi(x, y, z)$ is absolutely irreducible which implies under a condition that the function $F(x) = x^{2^i+1} + h(x)$ where $\deg(h(x))$ is odd and less than $2^i + 1$ is not exceptional APN.

Theorem 6.1.6. *[6, Theorem 7] For $i \geq 2$, let $F(x) = x^{2^i+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $\deg(h(x)) < 2^i + 1$ and $\deg(h(x)) \equiv 3 \bmod 4$, then $\phi(x, y, z)$ is absolutely irreducible.*

Theorem 6.1.7. *[6, Theorem 8] For $i \geq 2$, let $F(x) = x^{2^i+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $d = \deg(h(x)) < 2^i + 1$ and $d = \deg(h(x)) \equiv 1 \bmod 4$. If ϕ_{2^i+1} and ϕ_d are relatively prime, then $\phi(x, y, z)$ is absolutely irreducible.*

Since all odd positive integers are congruent to 1 or 3 mod 4, then they showed absolutely irreducibility of $\phi(x, y, z)$ for odd degree $h(x)$ under an additional condition. We know from previous section and Theorem 6.1.1, if

$$\frac{F(x) + F(y) + F(z) + F(x + y + z)}{(x + y)(y + z)(x + z)}$$

has an absolutely irreducible factor then F is not an exceptional APN function. By showing $\phi(x, y, z)$ is absolutely irreducible rather than it has an absolutely irreducible component, we can conclude that F is not an exceptional function.

In 2017, Delgado and Janwa have managed to show following result.

Theorem 6.1.8. *[5, Theorem 10] If d is an odd integer, then ϕ_{2^i+1} and ϕ_d are relatively prime for all $i \geq 1$, except $d = 2^l + 1$ and $\gcd(l, i) > 1$.*

After giving this result, they have alleviated the condition on the odd degree of $h(x)$ and they have given the following theorem in the same article [5].

Theorem 6.1.9. *[5, Theorem 11] For $i \geq 2$, let $F(x) = x^{2^i+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $\deg(h(x)) < 2^i + 1$ and $\deg(h(x))$ is an odd integer (not a Gold number $2^l + 1$ with $\gcd(l, i) > 1$). Then $\phi(x, y, z)$ is absolutely irreducible, and $F(x)$ can not be exceptional APN.*

The missing case for Gold degree polynomials $F(x) = x^{2^i+1} + h(x)$ with $\deg(h(x))$ is an odd integer is when $\deg(h(x))$ is any Gold number $2^l + 1$ where $\gcd(l, i) > 1$. In the next section, we will introduce our contribution in this case, $\deg(h(x))$ is Gold number and $\gcd(l, i) > 1$.

However, Delgado and Janwa have proved under a condition that the Gold degree polynomials where degree of $h(x)$ is a Gold number $2^l + 1$ with $\gcd(l, i) \neq 1$ is neither exceptional APN.

Theorem 6.1.10. *[7, Theorem 7] For $i \geq 2$, let $f(x) = x^{2^i+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $\deg(h(x)) = 2^l + 1 < 2^i + 1$. If $\gcd(l, i) \neq 1$ and $h(x)$ contains a term of degree m such that $\gcd(\phi_{2^i+1}, \phi_m) = 1$, then $\phi(x, y, z)$ is absolutely irreducible and F is not exceptional APN.*

Until now, we know that the function $F(x) = x^{2^i+1} + h(x)$ is not an exceptional APN function when $\deg(h(x))$ is odd but not a Gold number. To finish the case for the Gold degree polynomial, we have to ask what if the degree of $h(x)$ is an even integer?

Delgado and Janwa have showed a result when $\deg(h(x))$ is an even integer in [7] for a special case under several conditions.

Theorem 6.1.11. *[1, Theorem3.2] Suppose that $F(x) = x^{2^i+1} + h(x) \in \mathbb{F}_{2^n}[x]$ and $\deg(h) = 2^{i-1} + 2$. Let i be an odd integer and relatively prime to n. If $h(x)$ does*

not have the form $ax^{2^{ki1}+2} + a^2x^3$ *then* ϕ *is absolutely irreducible, while if* $h(x)$ *does have this form, then either* ϕ *is absolutely irreducible or* ϕ *splits into two absolutely irreducible factors that are both defined over* $\mathbb{F}_{2^n}$*.*

As it can be seen that it has been shown for a small number of functions of the form $x^{2^i+1} + h(x)$ where degree of $h(x)$ is an even integer, are not an exceptional APN. However, it has been proven that a big infinite family of Gold degree polynomials can not be exceptional APN.

We will investigate the functions of the form $x^{4^i-2^i+1} + h(x)$, namely Kasami-Welch degree polynomials. Rodier was proved the following theorem for this type of functions in [24].

Theorem 6.1.12. *[24, Theorem 4.1] Suppose that* $F(x) = x^{2^{2i}-2^i+1} + g(x) \in \mathbb{F}_{2^n}[x]$ *where* $\deg(x) \leq 2^{2^i-1} - 2^{i-1} + 1$*. Let* $g(x) = \sum_{j=0}^{2^{2i-1}-2^i+1} a_j x^j$*. Suppose moreover that there exist a non-zero coefficient* a_j *of* g *such that* $\phi_j(x, y, z)$ *is absolutely irreducible. Then* $\phi(x, y, z)$ *is absolutely irreducible.*

Thus, there are still some cases for Gold and Kasami-Welch degree functions which are not proven.

6.2 A Proof For Gold and Kasami-Welch Degree Polynomials

In this section, we will give our main result on a type of Gold and Kasami-Welch degree polynomials using a similar method with monomial APN functions.

Consider the polynomial $F(x) = \sum_{j=0}^{d} c_j x^j \in \mathbb{F}_{2^n}[x]$ and the polynomial

$$\phi(x, y, z) = \frac{F(x) + F(y) + F(z) + F(x + y + z)}{(x + y)(y + z)(x + z)} \in \mathbb{F}_{2^n}[x, y, z].$$

By setting

$$\phi_j(x, y, z) = \frac{x^j + y^j + z^j + (x + y + z)^j}{(x + y)(y + z)(x + z)},$$

we can write $\phi(x, y, z)$ as the following.

$$\phi(x, y, z) = \sum_{j=3}^{d} c_j \phi_j(x, y, z)$$

The sum is starts from $j = 3$, since $\phi_0(x, y, z) = \phi_1(x, y, z) = \phi_2(x, y, z) = 0$. In addition, we know from the proof of Theorem 5.1.2 that we have the following polynomial for $j = 2^k + 1$.

$$\phi_{2^k+1} = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (x + (\alpha + 1)y + \alpha z) \tag{6.2.1}$$

Moreover, for $j = 2^{2k} - 2^k + 1$, we have

$$\phi_{2^{2k}-2^k+1}(x, y, z) = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} p_\alpha(x, y), \tag{6.2.2}$$

where $p_\alpha(x, y)$ is absolutely irreducible polynomial over $\mathbb{F}_{2^k}$ of degree $2^k + 1$ for each $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$ such that

$$p_\alpha(x, 0) = (x + \alpha)^{2^k+1} \tag{6.2.3}$$

We consider a Gold degree polynomial, $F(x) = x^{2^k+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $h(x)$ is a polynomial of degree less than $2^k + 1$. Theorem 6.1.9 was stating that for a polynomial $F(x) = x^{2^k+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $\deg(h(x)) < 2^k + 1$ and $\deg(h(x))$ is an odd integer, in addition, the degree of $h(x)$ is not a Gold number $2^i + 1$ with $\gcd(i, k) > 1$, the polynomial $\phi(x, y, z)$ is absolutely irreducible. Then, $F(x)$ is not an exceptional APN function. Therefore, we are interested in $F(x) = x^{2^k+1} + h(x) \in \mathbb{F}_{2^n}[x]$ such that the leading term of $h(x)$ is of the form x^{2^l+1} with $\gcd(k, l) > 1$.

We know from the section "Exceptional APN Monomials" that $F(x)$ is not an APN function over $\mathbb{F}_{2^n}$ if and only if $\phi(x, y, z)$ has a point $(x, y, z) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with distinct coordinates. Note that the zero set of $\phi(x, y, z)$ defines an affine surface. We consider the homogenization $\phi(x, y, z, t)$ of $\phi(x, y, z)$ defined by

$$\phi(x, y, z, t) = \sum_{j=3}^{d} c_j \phi_j(x, y, z) t^{d-j}.$$

Let $\bar{X}$ be the zero set of $\phi(x, y, z, t)$ in the projective space $\mathbb{P}^3$, i.e., $\bar{X}$ is the projective closure of X. Our main aim is finding an absolutely irreducible curve lying in $\bar{X}$ which does not lie in the hyperplane defined by t. Using the Hasse-Weil bound, we will conclude that $\phi(x, y, z, t)$ has a rational point $(x, y, z, t) \in {\mathbb{F}_{2^n}}^4$ on an extension of $\mathbb{F}_{2^n}$ for a sufficiently large n such that $t \neq 0$, $x \neq y$, $y \neq z$, $x \neq z$. It will give us that $F(x)$ is not an APN function on $\mathbb{F}_{2^n}$ for a sufficiently large n, i.e., $F(x)$ is not an exceptional APN function.

For this aim, we consider the affine part $\tilde{X}$ of $\bar{X}$ corresponding to variable z. That is, we consider the zero set of

$$\tilde{\phi}(x, y, t) = \phi(x, y, 1, t) = \sum_{j=3}^{d} c_j \phi_j(x, y, 1) t^{d-j}.$$

Let H be the hyperplane defined by y. Then, the intersection $\tilde{X} \cap H$ is defined as the zero set of the following.

$$g(x, t) := \tilde{\phi}(x, 0, t) = \sum_{j=3}^{d} c_j \phi_j(x, 0, 1) t^{d-j} = \sum_{j=3}^{d} c_j \frac{x^j + 1 + (x+1)^j}{x(x+1)} t^{d-j} \tag{6.2.4}$$

Lemma 6.2.1. *If $g(x,t)$ in Equation 6.2.4 has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ containing t, then $F(x)$ is not an exceptional APN polynomial over $\mathbb{F}_{2^n}$.*

Proof. Let $h(x,t)$ be an absolutely irreducible factor of $g(x,t)$ containing t. Note that $h(x,t) \neq t$, since $g(x,0) = c_d \frac{x^d+1+(x+1)^d}{x(x+1)} \neq 0$. Let $\mathcal{X}$ be the curve defined by $h(x,t)$. Then by the Hasse-Weil bound $\mathcal{X}$ has sufficiently large number of rational points for all sufficiently large extension of $\mathbb{F}_{2^n}$. Hence, for all sufficiently large extension of $\mathbb{F}_{2^n}$, there exists $(x,t) \in \mathcal{X}$ such that $xt \neq 0$ and $x \neq 1$, since $\mathcal{X} \cap \{xt = 0\}$ and $\mathcal{X} \cap \{x = 1\}$ has cardinality at most $2\deg(h)$ and $\deg(h)$, respectively, by Bezout's theorem. Then $(\alpha, \beta, \gamma) = (x/t, 1/t, 0)$ is a zero of $\phi(x,y,z)$ such that $\alpha \neq \gamma$, $\alpha \neq \beta$ and $\gamma \neq \beta$, which gives the desired result. □

We will state the following proposition from [25] which is a special case of Eisenstein's Irreducibility Criterion to prove following lemma.

Proposition 6.2.2. *[25, Proposition 3.1.15] Let $\mathbb{F}$ be a field and $g(x,t) \in \mathbb{F}[x,t]$. Write*

$$g(x,t) = g_d(x)t^d + g_{d-1}(x)t^{d-1} + \ldots + g_1(x)t + g_0(x)$$

for some $g_i(x) \in \mathbb{F}[x]$ for $0 \leq i \leq d$. Set $c(x) = \gcd(g_d(x), \ldots, g_0(x))$. We denote by m_i the multiplicity of $g_i(x)$. Suppose that the followings hold.

- *$m_d = 0$ and $m_0 > 1$.*
- *$m_i \geq m_0$ for all $1 \leq i \leq d-1$.*
- *$\gcd(m_0, d) = 1$.*

Then $g(x,t)/c(x)$ is absolutely irreducible over $\mathbb{F}$.

Lemma 6.2.3. *Let $F(x) = x^{2^k+1} + \sum_{j=l}^{2^k} c_j x^j \in \mathbb{F}_{2^n}[x]$ with $c_l \neq 0$. Suppose that there exits $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$ such that $\phi_j(\alpha, 0, 1) = 0$ for all $l < j$ and $\phi_l(\alpha, 0, 1) \neq 0$. Then $F(x)$ is not exceptional APN.*

Proof. Note that by Equation 6.2.1, the polynomial $\phi_{2^k+1}(x, 0, 1)$ can be factorized as

$$\phi_{2^k+1}(x, 0, 1) = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (x + \alpha).$$

That is, the minimal polynomial $p(x)$ of α is a simple factor of $\phi_{2^k+1}(x, 0, 1)$. Since $\phi_j(\alpha, 0, 1) = 0$ for all $l < j$ and $\phi_l(\alpha, 0, 1) \neq 0$, $x + \alpha$ is also factor of $\phi_j(x, 0, 1)$ for all $j = l \leq j \leq 2^k$ but not $\phi_l(x, 0, 1)$. Hence, $g(x,t)$ is absolutely irreducible Proposition 6.2.2, which gives the desired result by Lemma 6.2.1, $F(x)$ is not exceptional APN. □

Using Lemma 6.2.3, we obtain the following result.

Theorem 6.2.4. *Let $F(x) = x^{2^k+1} + \sum_{i=1}^{d} c_i x^{2^{k_i}+1} \in \mathbb{F}_{2^n}[x]$ for some integers $k_1 < \cdots < k_d < k$ and $c_1 \neq 0$. If $\gcd(k_1, \ldots, k_d, k) < \gcd(k_2, \ldots, k_d, k)$, then $F(x)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. Let $\gcd(k_1, \ldots, k_d, k) = s$ and $\gcd(k_2, \ldots, k_d, k) = st$ for some integers $s \geq 1$, $t > 1$. Then, $\mathbb{F}_{2^{st}} \subseteq \mathbb{F}_{2^k}$, $\mathbb{F}_{2^{st}} \subseteq \mathbb{F}_{2^{k_i}}$ for all $i = 2, \ldots, d$ and $\mathbb{F}_{2^{st}} \cap \mathbb{F}_{2^{k_1}} = \mathbb{F}_{2^s}$. By Equation 6.2.1, we have the following equalities.

$$g(x,t) = \tilde{\phi}(x,0,t) = \sum_{i=1}^{d} c_i \phi_{2^{k_i}+1}(x,0,1) t^{2^k - 2^{k_i}} + \phi_{2^k+1}(x,0,1)$$

$$= \sum_{i=1}^{d} c_i \left(\prod_{\alpha \in \mathbb{F}_{2^{k_i}} \setminus \mathbb{F}_2} (x+\alpha) \right) t^{2^k - 2^{k_i}} + \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (x+\alpha) \tag{6.2.5}$$

Let $\alpha \in \mathbb{F}_{2^{st}} \setminus \mathbb{F}_{2^s}$, i.e., $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$. By Equation 6.2.5, we have $\phi_j(\alpha, 0, 1) = 0$ for all $2^{k_1} + 1 < j \leq 2^k$ and $\phi_{2^{k_1}+1}(\alpha, 0, 1) \neq 0$. Then, we obtain the desired result by Lemma 6.2.3. □

Remark 6.2.5. *We observe that $\phi(x, y, z)$ is not absolutely irreducible in the case $s > 1$ unlike the case given in Theorem 6.1.9.*

By Theorem 6.1.9 and 6.2.4, we obtain the following result.

Corollary 6.2.6. *There is no exceptional APN binomial of Gold type. That is, if $f(x) = x^{2^k+1} + \alpha x^{2^l+1}$ for a nonzero $\alpha \in \mathbb{F}_{2^n}$, then $f(x)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

In [7], they showed the following theorem.

Theorem 6.2.7. *[7, Theorem 8] Let $F(x) = x^{2^{k_1}+1} + h(x) \in \mathbb{F}_{2^n}[x]$ where $\deg(h(x)) = 2^{k_2} + 1 < 2^{k_1} + 1$ and $k_1 \geq 2$. For the polynomial $h(x) = \sum_{i=2}^{d} a_i x^{2^{k_i}+1}$ where $a_i \neq 0$ for all $2 \leq i \leq d$, and $\gcd(k_1, k_2, \ldots, k_d) = 1$, $\phi(x, y, z)$ is absolutely irreducible. That is, $F(x)$ is not an exceptional APN function. Under the same conditions, if $\gcd(k_1, k_2 \ldots, k_d) = 2^n$ then $\phi(x, y, z)$ is divisible by $\phi_{2^{2^n}+1}$ and $\phi(x, y, z)$ is not absolutely irreducible.*

In Theorem 6.2.4, we showed absolutely irreducibility for a special type of the polynomial $h(x)$. We can observe that the condition $\gcd(k_1, k_2, \ldots, k_d) = 1$ can be removed, when we take $h(x) = \sum_{i=1}^{d} c_i x^{2^{k_i}+1}$.

However, we have to mention that Berger, Canteaut, Charpin and Laigle-Chapuy contributed a more general result for the function of the form $F(x) = \sum_{i \in I} c_i x^{2^i+1}$ over $\mathbb{F}_{2^n}$ where $c_i \in \mathbb{F}^{2^n}$ is not an APN function, see [2]. They showed that there is no APN function of the form

$$F(x) = \sum_{i \in I} c_i x^{2^i+1} \in \mathbb{F}_{2^n}[x]$$

where I is a finite set of integers of size at least two on $\mathbb{F}_{2^n}$. Therefore, it is not an exceptional APN function. However, they used a different approach related to permutation polynomials to show this result.

We applied a similar method to the Kasami-Welch type polynomials. We obtained the following result.

Theorem 6.2.8. *Let* $F(x) = x^{2^{2k}-2^k+1} + \sum_{i=1}^{d} c_i x^{2^{2k_i}-2^{k_i}+1} \in \mathbb{F}_{2^n}[x]$ *for some integers* $k_1 < \cdots < k_d < k$ *and* $c_1 \neq 0$. *Suppose that* $\gcd(k_1, k) = 1$, $k \not\equiv k_1 \bmod 2$ *and* $\gcd(k_1, \ldots, k_d) > 1$. *Then* $F(x)$ *is not exceptional APN over* $\mathbb{F}_{2^n}$.

Proof. We will show that $g(x,t)$ given in Equation 6.2.4 is absolutely irreducible over $\mathbb{F}_{2^n}$. Then, we obtain the desired result by Lemma 6.2.1. By Equation 6.2.2 and 6.2.3, we can write $g(x,t)$ as follows.

$$\begin{aligned} g(x,t) &= \sum_{i=1}^{d} c_i \phi_{2^{2k_i}-2^{k_i}+1}(x,0,1) t^{2^{2k}-2^k-2^{2k_i}+2^{k_i}} + \phi_{2^{2k}-2^k+1}(x,0,1) \\ &= \sum_{i=1}^{d} c_i \left(\prod_{\alpha \in \mathbb{F}_{2^{k_i}} \setminus \mathbb{F}_2} (x+\alpha)^{2^{k_i}+1} \right) t^{2^{2k}-2^k-2^{2k_i}+2^{k_i}} + \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (x+\alpha)^{2^k+1} \end{aligned} \tag{6.2.6}$$

Note that $g(x,t)$ is absolutely irreducible if and only if

$$h(x,t) = t^{2^{2k}-2^k-2^{2k_1}+2^{k_1}} g(x, 1/t) \in \mathbb{F}_{2^n}[x,t]$$

is absolutely irreducible. Set $a_l(x) = \prod_{\alpha \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2} (x+\alpha)^{2^l+1}$. Hence, we consider

$$h(x,t) = a_k(x) t^{2^{2k}-2^k-2^{2k_1}+2^{k_1}} + \sum_{i=1}^{d} c_i a_{k_i}(x) t^{2^{2k_i}-2^{k_i}-2^{2k_1}+2^{k_1}}. \tag{6.2.7}$$

Let $\gcd(k_1, \ldots, k_d) = s$ for some integers $s > 1$, i.e., $\mathbb{F}_{2^s} \subseteq \mathbb{F}_{2^{k_i}}$ for all $i = 1, \ldots, d$. Since $\gcd(k_1, k) = 1$, we have $\mathbb{F}_{2^{k_1}} \cap \mathbb{F}_{2^k} = \mathbb{F}_2$. Then $\alpha \in \mathbb{F}_{2^s} \setminus \mathbb{F}_2$ is a root of $a_{k_i}(x)$ of multiplicity $2^{k_i}+1$ for all $i = 1, \ldots, d$ and $a_k(\alpha) \neq 0$. That is, the minimal polynomial $p(x)$ of α over $\mathbb{F}_{2^n}$ has multiplicity 0 in $a_k(x)$ and multiplicity $2^{k_i}+1 \geq 2^{k_1}+1$ in $a_{k_i}(x)$ for all $i = 1, \ldots, d$. Set

$$m = \gcd(2^{2k} - 2^k - 2^{2k_1} + 2^{k_1}, 2^{k_1} + 1).$$

Now, we observe that $m = 1$ under our assumptions. Since $2^{2k_1} - 2^{k_1} \equiv 2 \bmod (2^{k_1}+1)$, we have

$$\begin{aligned} m &= \gcd(2^{2k} - 2^k - 2, 2^{k_1} + 1) \\ &= \gcd(2^{2k-1} - 1, 2^{k_1} + 1) \gcd(2^k + 1, 2^{k_1} + 1) \\ &= \gcd(2^k + 1, 2^{k_1} + 1). \end{aligned}$$

Note that in the last equality, we used the fact that

$$\gcd(2^{2k-1} - 1, 2^{k_1} + 1) = \frac{2^{\gcd(2k-1, 2k_1)} - 1}{2^{\gcd(2k-1, k_1)} - 1} = 1$$

since $\gcd(2k-1, 2k_1) = \gcd(2k-1, k_1)$. Suppose that k is even and k_1 is odd.

Hence, we have

$$\gcd(2^k+1, 2^{2k_1}-1) = \frac{\gcd(2^{2k}-1, 2^{2k_1}-1)}{\gcd(2^k-1, 2^{2k_1}-1)} = \frac{2^{\gcd(2k,2k_1)}-1}{2^{\gcd(k,2k_1)}-1} = 1$$

since $\gcd(2k, 2k_1) = \gcd(k, 2k_1) = 2$. Since $\gcd(2^k+1, 2^{k_1}+1)$ is a divisor of $\gcd(2^k+1, 2^{2k_1}-1)$, we conclude that $\gcd(2^k+1, 2^{k_1}+1) = 1$. Similarly, if k is odd and k_1 is even, we observe that $\gcd(2^k+1, 2^{k_1}+1) = 1$. Note that $\gcd(k, k_1) = 1$ implies that $\gcd(a_k(X), a_{k_1}(X)) = 1$. Hence by Lemma 6.2.2, we conclude that $h(x,t)$ is absolutely irreducible, which gives the desired conclusion. □

Corollary 6.2.9. *There is no exceptional APN function which is CCZ or EA equivalent to the function*

$$F(x) = x^{2^k+1} + \sum_{i=1}^{d} c_i x^{2^{k_i}+1}$$

under the conditions in Theorem 6.2.4 and the functions

$$F(x) = x^{2^{2k}-2^k+1} + \sum_{i=1}^{d} c_i x^{2^{2k_i}-2^{k_i}+1}$$

under the conditions in Theorem 6.2.8.

Bibliography

[1] Yves Aubry, Gary McGuire, and François Rodier. A few more functions that are not apn infinitely often. In *Finite fields: theory and applications*, volume 518, pages 23–31. Amer. Math. Soc. Providence, RI, 2010.

[2] Lilya Budaghyan and Claude Carlet. Ccz-equivalence and boolean functions. *IACR Cryptology ePrint Archive*, 2009:63, 01 2009.

[3] Anne Canteaut. Lecture notes on cryptographic boolean functions. *Inria, Paris, France*, 03 2016.

[4] Florian Caullery. A new large class of functions not apn infinitely often. *Designs, codes and cryptography*, 73(2):601–614, 2014.

[5] Moises Delgado and Heeralal Janwa. Progress towards the conjecture on apn functions and absolutely irreducible polynomials. *arXiv preprint arXiv:1602.02576*, 2016.

[6] Moises Delgado and Heeralal Janwa. On the conjecture on apn functions and absolute irreducibility of polynomials. *Designs, Codes and Cryptography*, 82(3):617–627, 2017.

[7] Moises Delgado and Heeralal Janwa. Some new results on the conjecture on exceptional apn functions and absolutely irreducible polynomials: The gold case. *Advances in Mathematics of Communications*, 11(2):389, 2017.

[8] H. Dobbertin. Almost perfect nonlinear power functions on gf(2n): The welch case. 45(4), 2006.

[9] Hans Dobbertin. Almost perfect nonlinear power functions on gf(2n): The niho case. *Information and Computation*, 151(1):57–72, 1999.

[10] Hans Dobbertin. Almost perfect nonlinear power functions on gf(2n): A new case for n divisible by 5. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications*, pages 113–121, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[11] William Fulton. Algebraic curves. 2008.

[12] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE transactions on Information Theory*, 14(1):154–156, 1968.

[13] Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *CoRR*, abs/0903.2016, 2009.

[14] Heeralal Janwa, Gary Mcguire, and Richard M Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over gf (2). *Journal of Algebra*, 178(2):665–676, 1995.

[15] Heeralal Janwa and Richard M Wilson. Hyperplane sections of fermat varieties in p 3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[16] David Jedlicka. Apn monomials over gf (2n) for infinitely many n. *Finite Fields and Their Applications*, 13(4):1006–1028, 2007.

[17] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information and Control*, 18(4):369–394, 1971.

[18] Swastik Kopparty and Sergey Yekhanin. Detecting rational points on hypersurfaces over finite fields. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 311–320, 2008.

[19] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Number 20. Cambridge university press, 1997.

[20] Edouard Lucas. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. *Bulletin de la Société Mathématique de France*, 6:49–54, 1878.

[21] Gary Mullen. Mummert, and carl," finite fields and applications,". *American Mathematical Society*, page 112, 2007.

[22] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 55–64, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[23] François Rodier. Borne sur le degré des polynômes presque parfaitement nonlinéaires. *Contemporary Mathematics*, 487:169, 2009.

[24] François Rodier. Some more functions that are not apn infinitely often. the case of kasami exponents. *arXiv preprint arXiv:1101.6033*, 2011.

[25] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[26] J Van Lint and R Wilson. On the minimum distance of cyclic codes. *IEEE Transactions on Information Theory*, 32(1):23–40, 1986.