University of Puerto Rico
Río Piedras Campus
Faculty of Natural Sciences
Department of Mathematics

Some New Absolutely Irreducibility Testing Criteria and Their Applications to the Proof of a Conjecture on Exceptional Almost Perfect Nonlinear (E-APN) Function

By

Carlos Agrinsoni Santiago

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF MASTER
OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY
OF PUERTO RICO, RÍO PIEDRAS CAMPUS

July 20, 2021

APPROVED BY THE MASTER DISSERTATION
COMMITTEE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF PHILOSOPHY IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

ADVISOR:

Heeralal Janwa, Ph.D.
University of Puerto Rico, Río Piedras

READERS:

Puhua Guan, Ph.D.
University of Puerto Rico, Río Piedras

Moises Delgado, Ph.D.
University of Puerto Rico, Cayey

Abstract of M.S. Thesis Presented to the Graduate School
of the University of Puerto Rico, Río Piedras Campus in Partial Fulfillment of the
Requirements for the Degree of Master of Philosophy in Mathematics

Some New Absolutely Irreducibility Testing Criteria and Their Applications to the Proof of A Conjecture on Exceptional Almost Perfect Nonlinear (E-APN) Function

By

Carlos A. Agrinsoni Santiago

July 2021

A MASTER THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF MASTER
OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY
OF PUERTO RICO, RÍO PIEDRAS CAMPUS

Abstract

Our research work is on the construction of new absolute irreducible testing criteria and the creation of criteria that guarantee the existence of an absolute irreducible factor defined over $\mathbb{F}_q$ and its applications towards the exceptional almost perfect nonlinear (APN) conjecture.

Our results have direct implications and applications to algebraic geometry, algebraic number theory, coding theory, cryptography, sequence design, exceptional polynomials, finite geometry and combinatorics, where absolute irreducibility is critical.
We use these new criteria and previous well establish results to solve many pending cases of the exceptional APN conjecture. We resolved the conjecture completely when the polynomial degree is Gold, and the second term is an odd degree term. We do this by generalizing a previous result by Delgado and Janwa. When the degree is Gold, and the second term is an even degree term, we use a method designed by Delgado and Janwa to prove the conjecture of all the possible cases with three exceptions. In these three cases, we gave a series of conditions the polynomials left need to fulfill.

For the Kasami-Welch degree case, first, we extend the criteria for factorization into absolutely irreducible factors for the monomial case. When the degree of the polynomial is a Kasami-Welch exponent, and the degree of the second term is $1 \pmod 4$, we generalize a result by Delgado and Janwa in two different ways. First, we give a bound on the degree of the second term that allows us to cover more cases than the one of degree $5 \pmod 8$. Second, we gave a condition on the Kasami exponent, which allows us to guarantee the existence of an absolutely irreducible factor defined over $\mathbb{F}_q$. Using a technique similar to the Gold, we manage to provide an upper bound on the multiplicity of the point $\{(1, 1, 1)\}$ for the second term. If this bound is not met, then we can guarantee the existence of an absolutely irreducible factor defined over $\mathbb{F}_q$. Using this bound, we can partially prove the conjecture when the second term has an even degree. For the even degree case, we provide a characterization of the factorization for an infinite family of cases. We also give a conditional proof for the general case. Using this characterization and the results of Caullery and Rodier, for the case, when the degree of the polynomial is $4e$, when e is a Gold or Kasami-Welch exponent, we prove that under a certain condition in the second term, the polynomial is not exceptional APN.

ACKNOWLEDGMENTS

First, I would like to thank my advisor Prof. Heeralal Janwa for his tremendous support for my research. I valued all the work done and the advice given in improving my communication and oral skills. His patient and guidance have been key to all the presentations, reports and articles submitted through these four years. He also provides many ideas and improvement to this thesis. His push for excellence has been crucial in the discovery in many results as well as many conjectures for the future. I really admire his dedication, enthusiasm, and work ethic. I cannot ask for a better advisor.

Second, I would like to thank my co-advisor Prof Moises Delgado for all his support, dedication, and availability. He introduces me to the topic of APN function back when I was an undergraduate student, something I am grateful. He gave me the opportunity to do research and get experience in the field of mathematics. I am also thankful for all his availability for discussing about research, without his advice and suggestions this thesis would not be possible. As the first student of Prof Delgado, I will always remember that the learning process in the world of research do not finish when you graduated from a Ph.D. I also will always remember that we can continue growing and improving even after finishing our studies.

Third, I acknowledge Dr. Errol Montes for teaching me most of the core courses in mathematics. Almost all my foundation in pure mathematics is thanks to him. He also encouraged me to apply for my first internship in mathematics. He also gave me many advice and guidance through my undergraduate studies. He constantly encourages me to improve and do more than the requirements, this helps me in graduate school. I always will remember his great, enthusiasm toward learning and his passion for the history of this beautiful subject.

I would like to thank Dr. Puhua Guan for agreeing in being part of my thesis committee. Having an algebraic expert like him as part of my committee is very valuable to me. His comments will help me improving the quality of this thesis.

I would like to thank also to all the professor which teach me along the years. Without their valuable lessons this will not be possible. All the experience lived throughout all this year has help me improve and get a better perspective of different areas of investigation and perspective in the world. Without these experiences I will not be here.

I would also like to thanks to all the opportunities I have been given through the years to participate in conferences, seminars, and research summer programs. These wonderful experiences help me to grow as a student as well as a person. I extend my thanks for all my friends during my academic career that made my life cheerful. It is impossible to enumerate all of them. All the wonderful memories made this journey a more pleasant experience.

I am really thankful to NASA for all the funding and the experiences given during these years. My work is supported by the NASA Training Grant No. NNX15AI11H, and 80NSSC20M0052. Opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NASA.

Finally, I would like to thanks to my family. My parents have been very encouraging, understanding, and supportive. I am very thankful to my dad for teaching me the value of working and the importance of responsibility. Without all your lessons will be impossible for

me to be here in the first place. I am very thankful to my mom for all the attention, support and the education invest in me. I am very thankful to my three brothers that have taught me many lessons through my entire life and have help me when I need the most.

Contents

LIST OF SYMBOLS

$\mathbb{N}$ set of natural numbers

$\mathbb{Z}$ set of integer numbers

$\mathbb{F}_{p^n}$, $GF(p^n)$ field of order p^n

$\mathbb{F}_{p^n}^*$ multiplicative group (without the zero element)

$R[X]$ a ring of polynomials in the variable X with coefficients in a ring R

$R[X_1, \ldots, X_n]$ a ring of multivariate polynomials in the variables $X_1, \ldots, X_n$ with coefficients in a ring R

$\nu_p(G)$ multiplicity of a p[oint p of a Multivariate polynomial G

$Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$, the Galois group of $\mathbb{F}_{q^r}$ associated with $\mathbb{F}_q$

$m(G)$, the minimal extension in which G factors into absolutely irreducible components

APN almost prefect nonlinear function

$EAPN$ exceptional almost prefect nonlinear

(a,b) greatest common divisor of a and b

T_G the tangent cone of G at 0

t_G the first cone of G

$DG(F)$ the degree-gap of $F(\mathbf{X})$

$\mathbf{X}$ represent the variables $X_1, \ldots, X_n$
$\lfloor a \rfloor$ the floor of a

$\phi_f(X, Y, Z)$ the polynomial $\phi(X, Y, Z) = \dfrac{f(X) + f(Y) + f(Z) + f(X + Y + Z)}{(X + Y)(Y + Z)(X + Z)}$

1. Introduction

Finite Fields were discovered by Evariste Galois and are usually referred to as Galois fields. During this thesis, every field we consider will be a finite field except is stated otherwise. Let $\mathbb{F}$ be any finite field, then $\mathbb{F}[X]$ is the polynomial ring in X with coefficients in $\mathbb{F}$. Let $p(X) \in \mathbb{F}[X]$ be an irreducible polynomial over $\mathbb{F}_q$, then it is well known that the ideal $< p(X) >$ is an irreducible ideal and hence a maximal ideal in this principal ideal domain. Therefore, the resulting quotient ring $\mathbb{F}[X]/ < p(X) >$ is a finite field of degree extension $\deg(p(X))$. Specifically, if $p(X)$ is an irreducible polynomial of degree n in $\mathbb{F}[X]$ and the order of $\mathbb{F}$ is q, then $ff[X]/ < p(X) >$ is a finite field of order q^n. The resulting field is the field of polynomials modulo $p(X)$ of degree less than n with coefficients in $\mathbb{F}$. This field is also represented as $\mathbb{F}[\alpha]$, where α is any root of $p(X)$. It is well known that every finite field has order p^n, where p is a prime number and it is the characteristic of the field. We denote the finite field of q elements by $\mathbb{F}_q$ or $GF(q)$. By Galois Theory, finite fields are unique up to isomorphisms, namely the splitting fields of separable polynomial $X^{q^n} - x$ over the finite field $\mathbb{F}_q$.

The order of an element α in the multiplicative group of nonzero elements of $\mathbb{F}_q$, is the smallest positive integer l such that $\alpha^l = 1$. $\mathbb{F}_q$ always contains at least one element of order $q - 1$, any such element is called a primitive element. Given a finite field $\mathbb{F}_q$, and an integer $n > 1$, we can always find a finite field $(\mathbb{F}_{q^n})$ with q^n elements, this field is known as the extension of $\mathbb{F}_q$ of degree n. We can define a map $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ by $\sigma(x) = x^q$, with the property that for every element $a \in \mathbb{F}_q$, we have that $\sigma(a) = a$ (that is, it fixes $\mathbb{F}_q$ pointwise), and is also a linear map. This map is known as the Frobenius automorphism. We can show that the Galois group $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is the group of automorphism of $\mathbb{F}_{q^n}$ such that $\mathbb{F}_q$ is fixed. It turns out this group is generated by the Frobenius automorphism i.e. the group is cyclic of order n.

Example 1. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ is the group of order 4 of characteristic 2. Then the map $\sigma : \mathbb{F}_4 \to \mathbb{F}_4$ defined by $\sigma(x) = x^2$ is the Frobenius automorphism and the generator of the group $Gal(\mathbb{F}_4/\mathbb{F}_2) =< \sigma >$.

1.1. **Algebraic Geometry.**

We present a background on the algebraic geometry results that is used in this thesis. For a more comprehensive and detail study of the subject we refer to Fulton [27], Shafarevich [49], and Hartshorne [30].

Definition 1. Let $G \in \mathbb{F}_q[X_1, \ldots, X_n]$, and $P \in \mathbb{F}_q^n$. Then we called P a *rational point* if $G(P) = 0$. If G is a not a constant, the set of rational points of G is called the *hypersurface* defined by G. A hypersurface in $\mathbb{F}_q^2$ is called an *affine plane curve.*

Every irreducible factor of G is called a *component.* We can classify the rational points of a hypersurface and assign them a multiplicity. Later in chapter 2, we will use the multiplicity of rational points to create absolutely irreducible criteria.

Definition 2 (Fulton [27])**.** Let $f(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$. A point $\mathbf{a} = (a_1, \dots, a_n)$ on f is *singular* if $\frac{\delta f}{\delta x_1}(\mathbf{a}) = \cdots = \frac{\delta f}{\delta x_n}(\mathbf{a}) = 0$. The *multiplicity* of $\mathbf{a}$ on f, denoted $\nu_{\mathbf{a}}(f)$, is the smallest degree term with nonzero coefficients in $F(\mathbf{X}) = f(\mathbf{X} - \mathbf{a})$. Any point o a curve will have multiplicity at least 1, while a singular point has multiplicity at least 2. Define $T(F)$ to be the homogeneous polynomial composed of the terms of degree $\nu_{\mathbf{a}}(f)$ in F. Then $T(F)$ is called the *tangent cone* of F at $\mathbf{a}$ and the tangent lines to f at $\mathbf{a}$ are the factors of $T(F)$.

Let $G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$ and $a \in \mathbb{F}_q^n$ we will denote by $\nu_a(G)$ be the multiplicity of a. We can establish the following properties.

Lemma 1. Let $G(X), F(X) \in \mathbb{F}_q[X_1, \dots, X_n]$ and $a \in \mathbb{F}_q^n$. Then the we have the following

(1) $\nu_a(FG) = \nu_a(F) + \nu_a(G)$,
(2) $\nu_a(F + G) \geq \min(\nu_a(F), \nu_a(G))$.

Definition 3. Let $G(\mathbf{X}) \in \overline{\mathbb{F}}_q[X_1, \dots, X_n]$, such that every rational point of the hypersurface obtained by G has multiplicity 1. Then $G(\mathbf{X})$ is called a *non-singular polynomial*, otherwise we called $G(\mathbf{X})$ a *singular polynomial*.

Proposition 1 (Fulton [27])**.** Let H be a hypersurface and let P be a singular point of H, then $\nu_P(H) > 1$.

Proposition 2 (Fulton [27])**.** Let H be a hypersurface and let P be a simple point of H, then $\nu_P(H) = 1$.

Definition 4. Let $G(\mathbf{X}) \in \mathbb{F}_q[X_1, \dots, X_n]$ be a polynomial in which every term has the same degree d. We called $G(\mathbf{X})$ a *homogeneous polynomial* or *form* of degree d.

The following definition will be important in chapter 2. We will put conditions sufficient conditions on the tangent cone to guarantee that a polynomial has an absolutely irreducible factor defined over $\mathbb{F}_q$.

Definition 5. Let $G(\mathbf{X}) \in \mathbb{F}_q[X_1, \dots, X_n]$ and let $P \in \mathbb{F}_q^n$. Let $G(\mathbf{X} - P) = G_d(\mathbf{X}) + \cdots + G_e(\mathbf{X})$, be the degree-decreasing order, where $G_i(\mathbf{X})$ is either a homogeneous polynomial of degree i or 0. We called $G_e(\mathbf{X})$ the *tangent cone* of $G(\mathbf{X})$ at P. If P is not specified is assumed to be the point 0.

We will denote the tangent cone of a polynomial G at P by $T_P(G)$. If no point P is specified we will assume is 0.

Example 2. Let $G(X, Y) = X^2 + Y^2 \in \mathbb{F}_4[X, Y]$. Then the hypersurface obtain by G is given by $\{(0, 0), (1, 1), (\alpha, \alpha), (\alpha + 1, \alpha + 1)\}$.

Example 3. Let $G(x) = x^2 + y^3 \in \mathbb{F}_2[X, Y]$. Then $\nu_{(0,0)}(G) = 2$, that is $(0, 0)$ is a singular point. the point $(1, 1)$ is a simple point since $\nu_{(1,1)}(G) = 1$.

Example 4. The polynomial from Example 2 is nonsingular, while the polynomial from Example 3 is singular.

Example 5. Let $G(X, Y) = X^2+Y^2 \in \mathbb{F}_q[X, Y]$, then $G(X, Y)$ is a homogeneous polynomial of degree 2.

Let $\overline{\mathbb{F}}_q$ is an algebraically closed field. Let F, G be plane curves and let $P \in \mathbb{F}_q^2$. We will denote the intersection number of F and G at P by $I(P, F \cap G)$. We say that F and G intersect properly at P if F and G have no common components that pass through P. Two curves F and G intersect transversally at P if P is a simple point on both F and G with different tangent lines from F and G. We require the intersection number to have the following properties.

(1) $I(P, F \cap G)$ is a nonnegative integer for any F, G and P given that F and G intersect properly at P. Otherwise if they do not intersect properly at P we have $I(P, F \cap G) = \infty$.
(2) $I(P, F \cap G) = 0$ if and only if $P \notin F \cap G$. $I(P, F \cap G)$ depends only on the components of F and G that pass through P. Moreover $I(P, F \cap G) = 0$ if either F or G is a nonzero constant.
(3) The intersection number is invariant under affine change of coordinate in the following sense. If T is an affine change of coordinates on $\mathbb{A}^2$, and $T(Q) = P$, then $I(P, F \cap G) = I(Q, F^T \cap G^T)$.
(4) $I(P, F \cap G) = I(P, G \cap F)$ (symmetric).
(5) $I(P, F \cap G) \geq m_p(F)m_p(G)$ with equality occurring if and only if F and G have no tangent lines in common at P.
(6) If $F = \prod F_i^{r_i}$ and $G = \prod G_j^{s_j}$, then $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.
(7) If F is irreducible, $I(P, F \cap G)$ should depend only on the image of G in $\Gamma(F)$. Which is equivalent to $I(P, F \cap G) = I(P, F \cap (G + AF))$ for any $A \in k[X, Y]$.

The following theorem defines the intersection number.

Theorem 1. There is a unique intersection number $I(P, F \cap G)$ defined for all plane curves F, G, and all points $P \in \mathbb{A}^2$, satisfying the previous seven properties. Moreover, this number is given by the formula

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)).$$

One can also prove teo more properties about the intersection number.

(8) If P is a simple point then $I(P, F \cap G) = ord_p^F(G)$.
(9) If F, G have no common components then

$$\textstyle\sum_P I(P, F \cap G) = \dim_k(k[x, y]/(F, G)).$$

Remark: This properties can be extended to include projective plane curves.
The following theorem has great importance in analysing singularities and points in common between two projective plane curves. Janwa, Wilson, and McGuire [35] used the following theorem to give an algorithm to test absolute irreducibility.

Theorem 2 (Bezout's Theorem [27])**.** Let F and G be absolutely irreducible projective plane curves of degree m and n respectively. Assume F and G have no common component. Then

$$\textstyle\sum_P I(P, F \cap G) = mn.$$

1.2. **Absolutely Irreducible Criteria.**

Definition 6. Let $G(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a non-constant multivariate polynomial. We say $G(\mathbf{X})$ is *absolutely irreducible* if $G(\mathbf{X})$ is irreducible over $\overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

Finding Criteria to test whether or not a polynomial is an absolutely irreducible is a very complex problem in mathematics. There only exists a few criteria in the literature that can be applied to any polynomial. Many times we only need that the polynomial $g(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$. There exist many criteria that guarantee the existence of an absolutely irreducible factor defined over $\mathbb{F}_q$. Later in chapter 2, we will present new criteria to guarantee the existence of absolutely irreducible factors defined over $\mathbb{F}_q$. Absolute irreducibility have applications in many areas of mathematics; for example, finite geometry [32, 33], combinatorics [53], algebraic-geometric codes [52], permutation polynomials [42], function field sieve [1], coding theory [34], cryptography [34] and algebraic geometry [30].

For polynomials in 1 variable, we have a well-known test for irreducibility given by Eisenstein [22].

Theorem 3 (Eisenstein's Criterion 1850)**.** Let R be a unique factorization domain and let $f = f_0 + f_1x + \cdots + f_nx^n \in R[x]$, where $f_0, f_n \neq 0$. If there is a prime $p \in R$ such that all the coefficients except f_n of f are divisible by p but f_0 is not divisible by p^2 then f is irreducible over the fraction field of R.

This theorem can be generalized to multiple variables. The following two theorem are generalizations due to Dumas [20] and Wan [54].

Theorem 4 (Eisenstein-Dumas Criterion)**.** Let R be a unique factorization domain and let $f = f_0 + f_1x + \cdots + f_nx^n \in R[x]$, where $f_0, f_n \neq 0$. Assume that f is primitive; i.e. $f_0, \ldots, f_n$ have no common factor in R. If the Newton polygon of f with respect to some prime $p \in R$ consists of the only line segment from $(0, m)$ to $(n, 0)$ and $(n, m) = 1$ then f is irreducible in $R[X]$

This theorem can be generalized into another context such as local fields or fields with valuations [7, 38, 43].

Theorem 5 (Special Case of Eisenstein-Dumas Criterion)**.** Let $\mathbb{F}$ be any field and let $f = f_0(y) + f_1(y)x + \cdots + f_n(y)x^n \in \mathbb{F}[x, y]$. Assume that $f_0(y) \neq 0$ and $f_n(y)$ is a nonzero constant in $\mathbb{F}$. If the Newton polygon of f has only one line segment from $(0, m)$ to $(n, 0)$ and $(n, m) = 1$ then f is absolutely irreducible over $\mathbb{F}$.

The following criterion to test absolute irreducibility is due to Stepanov and Schmidt [48, 50, 51].

Theorem 6 (Stepanov-Schmidt Criterion)**.** Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x, y]$ with degree n in X. If the upper Netwon polygon of f with respect to y has only one line segment from $(0, m)$ to $(n, 0)$ and $(n, m) = 1$, then f is absolutely irreducible over $\mathbb{F}$.

These methods using the Newton polygon has been generalized to Newton Polytopes by Gao in [28] obtaining the following two absolute irreducibility criterion.

Theorem 7 (Gao 2001 [28])**.** Let $f = g(X) + h(X_1, \ldots, X_n)$, where $g \in \mathbb{F}[X]$ of degree r and $h \in \mathbb{F}[X_1, \ldots, X_n]$ of total degree m. If $(r, m) = 1$, then f is absolutely irreducible over $\mathbb{F}$.

Theorem 8 (Gao 2001 [28])**.** Let $f = aX^m + by^n + \sum c_{ij}X^iY^j \in \mathbb{F}[X, Y]$ with $a, b \neq 0$ and (i, j) different from $(m, 0)$, $(0, n)$. Suppose that the Newton polytope of f is contained in the triangle with vertices $(m, 0)$, $(0, n)$ and (u, v) for some point $(u, v) \in \mathbb{R}^2$. If $(m, n) = 1$, then f is absolutely irreducible over $\mathbb{F}$.

One can use algebraic geometry to create many absolute irreducibility testing criteria. The following two criteria are well-known results.

Theorem 9. Let $F(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$ be a non constant polynomial. If $F(\mathbf{X})$ is non singular then $F(\mathbf{X})$ is absolutely irreducible.

Theorem 10. Let $F(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$ be a non constant polynomial and $F(\mathbf{X}) = F_d(\mathbf{X}) + \cdots + F_0(\mathbf{X})$, where $F_i(\mathbf{X})$ is a form of degree i or 0. If $F_d(\mathbf{X})$ is absolutely irreducible then $F(\mathbf{X})$ is absolutely irreducible.

The following lemma is proven in [14]. Later in Chapter 2 in Lemma 18 we generalize Lemma 2 by lower the condition of relatively primeness of the highest degree two nonzero homogeneous polynomials to the relative primeness of all the nonzero homogeneous polynomials. We also generalized for polynomials in several variables. This generalization will then prove all the exceptions left in the Gold degree case when the second-highest degree is congruent with 1 (mod 4).

Lemma 2. [Delgado and Janwa [14]] Let K be a field. Let $G(X, Y, Z) \in K[X, Y, Z]$ be a polynomial whose graded homogeneous representation is: $G = G_b + G_a + \cdots + G_0$, where G_i is 0 or homogeneous of degree $i \in \{0, \ldots, b\}$. We also assume that $b > 2a$ and that G_b factors into distinct irreducible factors over $\overline{K}$ and $(G_a, G_b) = 1$. Then, G is absolutely irreducible.

One can also test absolute irreducibility by using Noether irreducibility forms [37].

Janwa and Wilson [34] and Janwa, McGuire and Wilson [35] introduce the algorithm 1. This is one of the most powerful tools to test the absolute irreducibility of polynomials of several variables. This algorithm is quite powerful and valuable since it is one of the few criteria that can be used for arbitrary polynomials. The algorithm is based on intersection theory, singularity analysis by using Bezout's Theorem. The main problem with this algorithm is that finding all the singularities for many polynomials is quite difficult and computationally exhaustive.

Algorithm 1. [Janwa and Wilson [34], Janwa, McGuire and Wilson [35]] Let $F(X, Y, Z) \in K[X, Y, Z]$, where K is an arbitrary field.

1. Assume $F(X, Y, Z)$ factors as $P(X, Y, Z)Q(X, Y, Z)$.
2. Compute and classify multiplicities of each singular point.
3. Find intersection multiplicities.
4. If the sum of intersection multiplicities exceeds that predicted by Bezout's theorem, then factorization can not occur.

For many applications we do not need to prove the whole polynomial is absolutely irreducible, instead it is enough to show the existence of an absolutely irreducible factor defined over the same field as the polynomial. For example, in the Segre Bartocci conjecture regarding exceptional hyperovals, Hernando and McGuire show that if a specific polynomial contains an absolutely irreducible factor, its corresponding hyperoval can not be exceptional hyperoval [32]. Using Algorithm 1 Hernando and Mcguire show that apart from the exceptions every polynomial associate with the hyperoval has an absolutely irreducible factor, and thus, they prove the conjecture [32]. Similarly, Jedlicka [36], and Hernando and McGuire [31] use Algorithm 1 to prove the Exceptional APN conjecture for monomials.

In 2010 Aubry, McGuire, and Rodier [2] using intersection analysis gave the following criteria to determine the existence of an absolutely irreducible factor.
Let X be a hypersurface in three variables and let $\overline{X}$ be its projective closure.

Lemma 3. [2] Let H be a projective hypersurface in $\mathbb{P}^3$. If $\overline{X} \cap H$ is a reduced absolutely irreducible curve, then $\overline{X}$ is absolutely irreducible.

The following lemma gave conditions to guarantee the existence of an absolutely irreducible factor.

Lemma 4. [2] Let H be a projective hypersurface. If $\overline{X} \cap H$ has a reduced absolutely irreducible factor defined over $\mathbb{F}_q$ then $\overline{X}$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Recently Bartoli and Schmidt [3] have proved the lemma below. In chapter 2 we generalized this lemma in two different ways. We generalize to several variables and for reduced absolutely irreducible factors rather than linear factors. Moreover, we create new criteria by changing the conditions of Lemma 5 to obtain many new criteria, including absolute irreducibility criteria. Furthermore, we gave a construction we will call the first cone, which has similar properties to the ones of the tangent cone. We present analog theorems to the tangent cone criteria by using the first cone.

Lemma 5. [3] Let $H \in \mathbb{F}_q[x, y]$ and suppose that the tangent cone of H contains a reduced linear factor over $\mathbb{F}_q$. Then H has an absolutely irreducible factor defined over $\mathbb{F}_q$.

The following results regarding the factorization of a polynomial are important. In Chapter 2, we present an improvement of this result. The following lemma will play an important role in chapters 3 and 4.

Lemma 6. [39] Suppose $p(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ is of degree d and is irreducible in $\mathbb{F}_q[X_1, \ldots, X_n]$. Then there exists r with $r \mid d$ and an absolutely irreducible polynomial $h(X) \in \mathbb{F}_{q^r}[X_1, \ldots, X_n]$ of degree d/r 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 homogeneous, then so is $h(X)$.

For a computational approach to factor into absolutely irreducible factors, we refer to the Lenstra algorithm [41].

1.3. **Almost Perfect Nonlinear Conjecture.** One can obtain the definition of almost perfect nonlinear functions by different areas of mathematics. The following construction is obtained by cryptography. The differential cryptanalysis is an attack invented by Biham and Shamir in 1991 [4] which exploit the symmetries of the difference and the fact that some difference occurs with high probability. Precisely, differential cryptanalysis is an iterative process that can summarize as follows. Let consider an r-round, symmetric block cipher. We can summarize the differential cryptanalysis as follows [40] :

(1) Find a differential (α, β) such that $P(\Delta X = \alpha | \Delta X(r-1) = \beta)$ with high probability.
(2) Choose a random plaintext x and compute $x*$ such that $\Delta X = \alpha$ Now encrypt x, $x*$ (under the secret key) and obtain the outputs y and y*. Now using the expected difference in the $(r-1)$-round and partially decrypting predict some of the key values.
(3) Repeat this process until some key values occur with a great frequency. Take these values as the values of the key.

A natural way to make a cryptographic system that is resistant to this type of attack is to make sure every difference occurs with low probability. This motivates the definition of a δ-uniform function. For the rest of the document let $L = \mathbb{F}_{2^k}$.

Definition 7. A function $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ is *δ-uniform* if for every $a \in \mathbb{F}_{2^k}$, $a \neq 0$, then the equation $f(x+a) + f(x) = b$ has at most δ solutions for every $b \in \mathbb{F}_{2^k}$.

If a function is 2-uniform then it is called an almost perfect nonlinear (APN). More formally:

Definition 8. Let $f : \mathbb{F}_q \to \mathbb{F}_q$. We say that f is an *Almost Perfect Nonlinear Function* if for every $a, b \in \mathbb{F}_q$, $a \neq 0$ the equation

$$f(x+a) - f(X) = b$$

has at most 2 solutions.

Example 6. Consider the function $f : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$ define by $f(x) = x^3$. Then $f(x)$ is APN.

Notice that if x is a solution of the equation $f(x+a) + f(x) = b$, then $x + a$ is also a solution, so the solutions come in pairs. In this sense, APN functions minimize the probability of success of the differential cryptanalysis.

We can also derive the concept of APN function using code theory. Lets start by recalling the Hamming codes are $[2^m, 2^m - 1 - m, 3]$ codes. Let $H_m := [h_1, h_2, \ldots, h_{2^m-1}]$ where $h_i \in \mathbb{F}_2^n - \{0\}$ where $n = 2^m$. Now we can think $\mathbb{F}_2^n$ as a vector space over $\mathbb{F}_2$ with dimension m. Also we can think on it as the extension field $\mathbb{F}_2$ given by the following quotient $\mathbb{F}_2[x]\ x^n - x$ give us an extension of $\mathbb{F}_2$ in which the polynomial $x^n - x = x(x^{n-1} - 1)$ split completely (i.e. every root of this polynomial is an element of the field). The following theorem is a classical theorem in algebra that state a relation between every nonzero element.

Theorem 11. Let K be a finite field then $(K^\times, *, 1)$ is a cyclic group.

By using this theorem we can express $\mathbb{F}_2^m - \{0\}$ as $< \alpha >$ where $\alpha \in \mathbb{F}_2^m$ and α is a generator of $ff_2^m - \{0\}$.

Let $H = [\alpha^0, \alpha, \alpha^2, \ldots \alpha^{2^m-2}]$, $\alpha^{2^m-1} = 1 = \alpha^0$. Now we can define the hamming code:

$$CH_m := \{x | H_m x = 0\}$$

i.e. $x \in CH_m$ if $\sum_{i=0}^{2^m-2} x_i \alpha^i = 0$. Let $f(x) = sum_{i=0}^{2^m-2} x_i x^i$. So $f(\alpha) = 0$. Notice that $0 = f(\alpha) = sum_{i=0}^{2^m-2} x_i \alpha^i$. Now if we multiply by α we obtain

$$0 = 0 \cdot \alpha = \alpha \cdot f(\alpha) = \sum_{i=0}^{2^m-2} x_i \alpha^{i+1}$$
$$= x_0\alpha + x_1\alpha^2 + \cdots + x_{2^m-3}\alpha^{2^m-2} + x_{2^m-2}\alpha^{2^m-1}$$

Therefore, $(x_{2^m-2}), x_0, x_1, \ldots, x_{2^m-2}) \in CH_m$. A code with this property that if x is a solution then all the solutions are shift of this element is called a cyclic code. Now given a cyclic code C we can try to obtain a new code by adding more rows to increase the minimum distance and hence it can correct more errors. Consider the matrix analyze previously H_m and add extended as follows: Let

$$H = \begin{pmatrix} \alpha^0 & \alpha & \alpha^2 & \ldots & \alpha^{2^m-2} \\ \alpha^{0t} & \alpha^t & \alpha^{2t} & \ldots & \alpha^{(2^m-2)t} \end{pmatrix}.$$

Now consider the code $CH = \{x | Hx^t = 0\}$ and let $x = [0, 0, \ldots, 1, 0, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 0]$ be the vector with nonzero coordinates in the $0 \leq i, j, k, l \leq 2^m - 2$ position. Now Hx^t give us the following system of equations:

$$\begin{bmatrix} \alpha^i + \alpha^j + \alpha^k + \alpha^l = 0 \\ \alpha^{it} + \alpha^{jt} + \alpha^{kt} + \alpha^{lt} = 0 \end{bmatrix}$$

If 4 columns are linearly independent then the code CH has minimum distance $d_{min}(CH) \geq 5$. Lets see an example,

Example 7. Let $t = 3$ and $(m, t) = 1$ then we obtain the following matrix:

$$H = \begin{pmatrix} \alpha^0 & \alpha & \alpha^2 & \ldots & \alpha^{2^m-2} \\ \alpha^0 & \alpha^3 & \alpha^6 & \ldots & \alpha^{(2^m-2)3} \end{pmatrix}.$$

Let x be the mentioned vector and denote $x_i = \alpha^i$, $x_j = \alpha^j$, $x_k = \alpha^k$, and $x_l = \alpha^l$. So we obtained the following system of equation:

$$\begin{bmatrix} x_i + x_j + x_k + x_l = 0 \\ x_i^3 + x_j^3 + x_k^3 + x_l^3 = 0 \end{bmatrix}$$

We can extend this system and create the following system of equation. Let first

$$V_m = \begin{bmatrix} x_i & x_j & x_k & x_l \\ x_i^2 & x_j^2 & x_K^2 & x_l^2 \\ x_i^3 & x_j^3 & x_k^3 & x_l^3 \\ x_i^4 & x_J^4 & x_k^4 & x_l^4 \end{bmatrix}$$

then the system can be express as $V_m * 1 = 0$ where 1 is the vector with all entries equal to 1. Now notice that V_m is a Vandermonde matrix so is invertible if $x_i \neq x_j$ for $i \neq j$. Therefore, the columns V_m are linearly independent and 4 columns of H are linearly independent. This implies that distance of $CH \geq 5$.

Now a function that extend the minimum distance of the code to 5 is APN.

Definition 9. A function $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ is APN if the cyclic codes $C_s^{(t)}$ generated by f has a minimum distance 5.

The definition of an almost perfect nonlinear function can be derived also from algebraic geometry. The following proposition gives another characterization of these functions.

Proposition 3 (Rodier [46])**.** A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is APN if and only if the rational points f_q of the affine surface

$$f(X) + f(y) + f(z) + f(x + y + z) = 0$$

are contained in the surface $(x + y)(x + z)(y + z) = 0$.

Almost perfect nonlinear property is invariant under certain transformations. This allows us to define equivalence classes. The following three are the equivalence transformation. The last transformation is the most general one and includes the other two.

Definition 10. A polynomial in $\mathbb{F}_{2^m}[x]$ of the form

$$L(x) = \sum_i c_i x^{2^i}$$

is called a *linearized* polynomial. The addition of a linearized polynomial and a constant term is called an *affine* polynomial. A linearized (resp. affine) polynomial which defines a permutation over $\mathbb{F}_{2^m}$ is called a linear (resp. affine) permutation.

Proposition 4. Let $A(x)$ be affine polynomial and $f(x)$ be a APN polynomial in $\mathbb{F}_{2^m}[x]$, then $f(x) + A(x)$ is APN over $\mathbb{F}_{2^m}[x]$.

Proposition 5. Let $A_1(x)$ and $A_2(x)$ be affine permutations, $A(x)$ be an affine polynomial and $f(x)$ be an APN polynomial in $\mathbb{F}_{2^m}[x]$. The polynomial

$$A_1 \circ f \circ A_2(x) + A(x)$$

is APN over $\mathbb{F}_{2^m}[x]$.

The last equivalence was introduced by Carlet, Charpin, and Zinoviev [6] and it includes the previous equivalences.

Proposition 6 (Carlet, Charpin and Zinoviev [6])**.** Let f and g be two polynomials in $\mathbb{F}_q[x]$. Suppose there exists a linear permutation $\mathcal{L} : \mathbb{F}_q \to \mathbb{F}_q$ between the sets $\{(x, f(x))|x \in \mathbb{F}_q\}$ and $\{x, g(x))|x \in \mathbb{F}_q\}$. Then f is APN if and only if g is APN.

Finding functions that are APN is not an easy task and is a good research problem the following table summarize the known APN monomial functions.

$f(x) = x^d$	Exponent d	Constraints	References
Gold	$2^r + 1$	$(r, n) = 1$	[45]
Kasami-Welch	$2^{2r} - 2^r + 1$	$(r, n) = 1$	[34]
Welch	$2^r + 3$	$n = 2r + 1$	[18]
Niho	$2^r + 2^{r/2} - 1$ $2^r + 2^{(3r+1)/2} - 1$	$n = 2r + 1$, r even $n = 2r + 1$, r odd	[17]
Inverse	$2^{2r} - 1$	$n = 2r + 1$	
Dobbertin	$2^{4r} + 2^{3r} + 2^{2r} + 2^r - 1$	$n = 5r$	[19]

Table 1. Monomial APN functions

It is conjectured that these are the only monomial up to equivalence that is APN functions. Until 2006 this was the only APN function that is known up to equivalence. In this year Y.Edel, G.Kyureghyan, and A.Pott discover the first APN polynomial function that is not equivalent to any APN monomial [21]. Since then, the researcher has found many APN polynomial functions. A similar list of known families of polynomials that are APN is given in [29] (see table 2). Now let's define what is an exceptional APN function. For a good survey on APN function see [29], and see [5] for a good survey on cryptography and APN functions.

$f(x)$	Constraints
$x^{2^s+1} + a^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 3t, (t, 3) = (s, 3t) = 1, t \geq 3$ $i \equiv st \pmod 3, r = 3 - i$, a is primitive in L
$x^{2^s+1} + a^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 4t, (t, 2) = (s, 2t) = 1, t \geq 3$ $i \equiv st \pmod 4, r = 4 - i$, a is primitive in L
$ax^{2^s+1} + a^{2^m}x^{2^{m+s}+2^m} + bx^{2^m+1} +$ $\sum_{j=1}^{m-1} c_j x^{2^{m+i}+2^i}$	$n = 2m$, m odd $c_j \in \mathbb{F}_{2^m}, (s, m) = 1$, s odd a, b are primitive in L
$ax^{2^{n-t}+2^{t+s}} + a^{2^t}x^{2^{s+1}} + bx^{2^{n-t}+1}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en L, $b \in \mathbb{F}_{2^t}$
$a^{2^t}x^{2^{n-t}+2^{t+s}} + ax^{2^{s+1}} + bx^{2^{n-t}+1}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en L, $b \in \mathbb{F}_{2^t}$
$a^{2^t}x^{2^{n-t}+2^{t+s}} + ax^{2^{s+1}} + bx^{2^{n-t}+1} +$ $ca^{2^t+1}x^{2^{t+s}+2^s}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en L, $b, c \in \mathbb{F}_{2^t}, bc \neq 1$
$x^{2^{2k}+2^k} + bx^{q+1} + cx^{q(2^{2k}+2^k)}$	$n = 2m$, m odd, c a power of $(q - s)$ but no a power of $(q - 1)(2^i + 1), cb^q + b \neq 0$
$x^3 + tr_1^n(x^9)$	
$x^{2^k+1} + tr_m^n(x)^{2^k+1}$	$n = 2m = 4t, (n, k) = 1$

Table 2. Nonmonomial APN functions

Definition 11. A polynomial function $f : L \to L$ is an *exceptional APN* if f is APN over L and on infinitely many extensions of L.

Notice that Gold and Kasami-Welch monomials are exceptional APN.

Example 8. Let $f(x) = x^13 \in \mathbb{F}_{2^3}$. Now we have $13 = 2^{2(2)} - 2^2 + 1$ and $(2,3) = 1$. Therefore, $f(x)$ is APN over $\mathbb{F}_{2^3}$. Moreover, $f(x)$ is also APN over any odd extension of $\mathbb{F}_{2^3}$, thus $f(x)$ is APN in infinitely many extension. Hence, $f(x)$ is exceptional APN.

Janwa and Wilson [34] characterize the exceptional almost perfect nonlinear monomials using algebraic geometry. Later in 2009 Rodier in [46] gave a characterization of APN and Exceptional APN functions. For any $f(x) \in \mathbb{F}_q[x]$, we define

$$\phi_f(X,Y,Z) = \frac{f(X) + f(y) + f(z) + f(x+y+z)}{(x+y)(x+z)(y+z)}.$$

If $\deg(f) = d$ and d is not a power of two then $\phi_f(X,Y,Z)$ has degree $d-3$. For convenience if $f(X) = X^t$ we will denote $\phi_f(X,Y,Z)$ by $\phi_t(X,Y,Z)$. Notice that if every $f(X) = a$ or $f(X) = a_iX^{2^i}$, $(a, a_i \in \mathbb{F}_q)$ then there corresponding $\phi_f(X,Y,Z) = 0$. Now for every $f(X) \in \mathbb{F}_q[x]$ of degree d we have

$$\phi_f(X,Y,Z) = \sum_{i=3}^{d} a_i \phi_i(X,Y,Z).$$

The following theorem characterizes the Exceptional APN functions.

Theorem 12. [46] Let $f : \mathbb{F}_q \to \mathbb{F}_q$ a polynomial function of degree d. Suppose that the surface X of affine equation

$$\frac{f(X) + f(y) + f(z) + f(x+y+z)}{(x+y)(x+z)(y+z)} = 0$$

is absolutely irreducible (or has an absolutely irreducible factor defined over L) and $d \geq 9$, $d < 0.45q^{1/4} + 0.5$, then f is not an APN function.

Using this theorem is easy to prove that it is enough to satisfy the following condition to not be an APN function.

Corollary 1. If $\phi_f(X,Y,Z)$ is absolutely irreducible or contain an absolutely irreducible factor different from $(x+y)$, $(x+z)$, $(y+z)$, then f is not exceptional APN.

In 2009 Hernando and Mcguire stated the next conjecture. In the next subsections, we will detail all the known results regarding the exceptional APN conjecture.

Exceptional APN conjecture [31]. *The only exceptional APN functions up to equivalence are the Kasami-Welch and Gold monomials.*

1.3.1. *Monomial Case.* Consider $f(x) = x^n$, if n is even then $f(x)$ is CCZ equivalent to a monomial $x^{n'}$, where n' is an odd number. To be precise, $n = 2^a n'$. So it is enough to work only with the monomials of odd degree. If $f(x)$ is linear then it is clear by the definition that $f(x)$ is not APN. It is well known that X^{2^n+1} (Gold) and $X^{4^n - 2^n + 1}$ (Kasami-Welch) are APN in $\mathbb{F}_{2^m}$ whenever $(n,m) = 1$. Therefore, both are exceptional APN over ff_2. Janwa and Wilson [34] prove the following factorization for their corresponding surfaces $\phi(X,Y,Z)$. For the Gold Case we have that

$$\phi_{2^n+1}(X,Y,Z) = \prod_{\alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2} (x + \alpha y + (\alpha+1)z) \tag{1}$$

while for the Kasami Welch case we have

$$\phi_{2^{2n}-2^{n}+1}(X,Y,Z)=\prod_{\alpha\in\mathbb{F}_{2^n}-\mathbb{F}_2} p_\alpha(X,Y,Z), \tag{2}$$

where $P_\alpha(X,Y,Z)$ is an absolutely irreducible polynomial of degree 2^k+1, defined over $\mathbb{F}_{2^k}$ and $P_\alpha(X,0,1)=(X+\alpha)^{2^k+1}$.

The next two results characterize the multiplicity of $(1,1,1)$ in the absolutely irreducible factors of the Gold and Kasami-Welch cases respectively. This will be important in Chapter 3 and Chapter 4 in the proofs of new cases of the exceptional APN conjecture.

Lemma 7. [Janwa and Wilson [34]] In the absolutely irreducible factorization of Equation 1, the component $(X+\alpha Y+(\alpha+1)Z)$, $\alpha\in\mathbb{F}_{2^k}-\mathbb{F}_2$, we have $\nu_{(1,1,1)}((X+\alpha Y+(\alpha+1)Z)=1$ for every $\alpha\in\mathbb{F}_{2^k}-\mathbb{F}_2$.

Lemma 8. [Delgado and Janwa, [12]] In the absolutely irreducible factorization of Equation 2, the components $P_\alpha(X,Y,Z)$, $\alpha\in\mathbb{F}_{2^k}-\mathbb{F}_2$, intercept transversally at $p=(1,1,1)$.

This lemma implies directly that $\nu_{(1,1,1)}(P_\alpha)=1$, for every $\alpha\in\mathbb{F}_{2^k}-\mathbb{F}_2$.
Aubry McGuire and Rodier prove the following result.

Lemma 9. If d is an odd integer, then $(X+Y)(Y+Z)(X+Z)\nmid\phi_d(X+Y+Z)$.

We also have the following characterization of the factorization when d is even. Suppose $d=2^m e$, where e is an odd number, then we have

$$\phi_{2^m e}(X,Y,Z)=\phi_6^{2^m-1}(X,Y,Z)\phi_e^{2^m}(X,Y,Z), \tag{3}$$

where $\phi_6(X,Y,Z)=(X+Y)(Y+Z)(X+Z)$. The following lemmas regarding the relatively prime between two different factor as well as the resulting polynomial obtained after intersect $\phi_d(X,Y,Z)$ with the hyperplane $Y=Z$ are important results.

Lemma 10 ([13])**.** For an integer $k>1$, let $l=2^k+1$, $m=2^{2k}-2^k+1$ and $n=2^k+3$ be Gold, Kasami-Welch and Welch numbers, respectively. Then $(\phi_l,\phi_m)=1$, $(\phi_l,\phi_n)=1$, and $(\phi_m,\phi_n)=1$. Also:

a) If $l_1=2^{k_1}+1$ and $l_2=2^{k_2}+1$ are two different Gold numbers such that $(k_1,k_2)=1$, then $(\phi_{l_1},\phi_{l_2})=1$.
b) $(\phi_{m_1},\phi_{m_2})=1$ for different Kasami-Welch numbers m_1 and m_2.
c) $(\phi_{n_1},\phi_{n_2})=1$ for different Welch numbers n_1 and n_2.

Later Delgado and Janwa using an affine transformation manage to prove that ϕ_{2^k+1} is relatively prime with ϕ_d, d odd whenever d is not a Gold or a Gold satisfying the previous lemma [13].

Theorem 13. [Delgado and Janwa [13]] If d is an odd integer, then ϕ_{2^k+1} and ϕ_d are relatively prime for all $k\geq 1$ except when $d=2^l+1$ and $(l,k)>1$.

The following Lemma characterizes the intersection of the surface $\phi(X,Y,Z)$ with the plane $Y=Z$.

Lemma 11. [Delgado and Janwa [15]] Let $\phi_n(X,Y,Z) \in \mathbb{F}_2[X,Y,Z]$. Then

a) For $n = 2^k + 1 > 3$, $\phi_n(X,Y,Y) = (X+Y)^{2^k-2}$.

b) For $n \equiv 3 \pmod 4 > 3$, $\phi_n(X,Y,Y) = R(X,Y)$ such that $X+Y$ does not divides $R(X,Y)$.

c) For $n \equiv 1 \pmod 4 > 5$, $\phi_n(X,Y,Y) = (X+Y)^{2^l-2}S(X,Y)$, such that $X+Y$ does not divides $S(X,Y)$, where $n = 1 + 2^l m$, and $m > 1$ is an odd number.

Janwa and Wilson [34] also show the following results:

Theorem 14 (Janwa and Wilson [34])**.** Suppose that $t \equiv 3 \pmod 4$, say $t = 2^l$, with l an odd integer. If the maximal cyclic code B_i of length l has no codewords of weight 4, in particular if the minimum distance of B_l is at least 5, then the curve defined by $\phi_t(X,Y,Z)$ is a nonsingular curve. Hence, $\phi_t(X,Y,Z)$ is absolutely irreducible.

The following two corollaries are a direct consequence of the previous theorem.

Corollary 2 (Janwa and Wilson [34])**.** The curve $\phi_t(X,Y,Z)$ is nonsingular for those values of $t = 2l + 1$, where l is an odd integer such that $2^r \equiv -1 \pmod l$ for some r.

Corollary 3 (Janwa and Wilson [34])**.** The curve $\phi_t(X,Y,Z)$ is nonsingular for those values of $t = 2l + 1$, where l is a prime ≥ 17 such that the order of 2 modulo l is $(l-1)/2$.

Janwa and Wilson also show the following key result.

Lemma 12. [Janwa and Wilson [34]] If $t \equiv 3 \pmod 4$, then $(1,1,1)$ is not a rational point of the curve given by $\phi_t(X,Y,Z)$.

This theorem implies that $\nu_{(1,1,1)}(\phi_t) = 0$ if $t \equiv 3 \pmod 4$. This will be important in Chapter 3, 4, and 5.

Later in 1995 Janwa, McGuire, and Wilson in [35] extend the results obtained by Janwa and Wilson in 1993.

Theorem 15 (Janwa, McGuire and Wilson [35])**.** If $t \equiv 3 \pmod 4$, $t > 3$, then $\phi_t(X,Y,Z)$ is absolutely irreducible.

Theorem 16 (Janwa, McGuire and Wilson [35])**.** Suppose that $t \equiv 5 \pmod 8$, $t > 13$ and that the maximal cyclic code B_l has no codewords of weight 4. Then $\phi_t(X,Y,Z)$ is absolutely irreducible.

Ferard in the next theorem provides other criteria for the case when $t \equiv 5 \pmod 8$ to guarantee that $\phi_t(X,Y,Z)$ is absolutely irreducible.

Theorem 17 (Ferard [24])**.** Let l be an odd integer, $l \geq 7$, $t = 4l + 1$ and $\phi_t(x,y,1)$ as in equation. We assume that there are no points $(x,y) \in (\overline{\mathbb{F}_2})^2$ which satisfy the following system

$$\begin{cases} x \neq 1, y \neq 1, x \neq y \\ x^l = 1, y^l = 1, (x+y+1)^l = 1 \\ \phi_{13}(x,y) = 0 \end{cases}$$

Then the polynomial ϕ_t is absolutely irreducible.

In the case when ϕ_t is not absolutely irreducible Ferard proved the following theorem.

Theorem 18 (Ferard [23, 9])**.** Suppose that $t \equiv 5 \pmod 8$, $t \geq 29$ and that ϕ_t is not absolutely irreducible. Then $\phi_1 3$ divides ϕ_t.

Theorem 19 (Janwa, McGuire and Wilson [35])**.** Suppose that the maximal cyclic code B_l has no codewords of weight 4, and that $\mathbb{F}_{2^i}$ does not contain a nontrivial lth root of unity i.e., $(l, 2^i - 1) = 1$. Then $\phi_t(X, Y, Z)$ is absolutely irreducible.

Using Algorithm 1 and the following characterization of APN functions Jedlicka proved Theorem 20 below. He also classifies the singularities and their corresponding multiplicities for many cases, see table 3 for the classification.

Definition 12. Define $q(x, y) = (x + 1)^m + x^m + (y + 1)^m + y^m$ and $h(x, y) = \frac{q(x,y)}{(x+y)(x+y+1)}$

Proposition 7. If $h(x, y)$ has an absolutely irreducible factor over $\mathbb{F}_2$, then $f(x) = x^m$ is not APN over $\mathbb{F}_{2^n}$ for large enough n.

Theorem 20. Let $f(x) = x^{2^i l+1} \in \mathbb{F}_2[x]$. If $(l, 2^i - 1) < l$, then $f(x)$ is not exceptional APN.

Type	description	$\nu_p(h)$	I_p bound	Max number of points
Ia	Affine, on a line, $x_0, y_0 \in \mathbb{F}^*_{2^l}$	2^l	$(2^{l-1})^2$	2(d-1)
Ib	Affine, on a line, $x_0, y_0 \notin \mathbb{F}^*_{2^l}$	$2^l - 1$	0	$m' - 3$
IIa	Affine, off both lines, $x_0, y_0 \in \mathbb{F}^*_{2^l}$	$2^l + 1$	$2^{l-1}(2^{l-1} + 1)$	$(d - 1)(d - 3)$
IIb	Affine, off both lines, exactly one of $x_0, y_0 \in \mathbb{F}^*_{2^l}$	2^l	0	Not important
IIc	Affine, off both lines, $x_0, y_0 \notin \mathbb{F}^*_{2^l}$	2^l	2^l if $l > 1$, 0 if $l = 1$	$(\frac{m'-3}{2})(m' - a - 3)-$ $(d - 1)(d - 3)$ and $(\frac{m'-3}{2})(2^l - 2)(2^l + 1)$
IIIa	$(1 : 1 : 0)$	$2^l - 2$	$(2^{l-1})^2$	$d - 1$
IIIb	$(\omega : 1 : 0)$, $\omega^d = 1$, $\omega \neq 1$	2^l	$(2^{l-1})^2$	$d - 1$
IIIc	$(\omega : 1 : 0)$, $\omega^d \neq 1$	$2^l - 1$	0	Not important

Table 3. All singularities of h [36]

The constants m, l, m', d are defined by the following definition.

Definition 13 (Jedlicka [36])**.** Let $f(x) = x^m$. Define l to be the largest integer such that 2^l divides $m - 1$. Also let $m' = \frac{m-1}{2^{l-1}} + 1$. Let $d = (m - 1, 2^l - 1) = (\frac{m'-1}{2}, 2^l - 1)$.

The remaining case was settled by Hernando and McGuire [31]. They also classified the singularities for $\phi_d(X, Y, Z)$ for the remaining case. Table 4.

Theorem 21 (Hernando and McGuire [31])**.** Let $f(x) = x^{2^i l+1} \in \mathbb{F}_2$, not a Kasami-Welch exponent. If $(l, 2^i - 1) = l$, then $\phi(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_2$. Therefore, $f(x)$ is not exceptional APN.

Type	Number of Points	$\nu_p(f_{2^il+1})$	$\nu_p(\phi_{2^il+1})$
I	1	2^i+1	2^i-2
II	$3(l-1)$	2^i+1	2^i
III	$\leq (l-1)(l-3)$	2^i+1	2^i+1

TABLE 4. Singularities of ϕ_{2^il+1} [31]

Where $f_{2^il+1}(X,Y,Z) = X^{2^il+1}+Y^{2^il+1}+Z^{2^il+1}+(X+Y+Z)^{2^il+1}$. The following are the three types of singular points (α,β,λ).

(I) $\alpha=\beta=\lambda=1$.

(II) Either $\alpha=1$ and $\beta\neq 1$, or $\beta=1$ and $\alpha\neq 1$, or $\alpha=\beta\neq 1$ and $\lambda=1$ We divide these singular points into two cases:

  (II.A) Where II holds and $\alpha,\beta\in\mathbb{F}_{2^i}$.

  (II.B) Where II holds and $\alpha\beta$ not both in $GF(2^i)$.

(III) $\alpha\neq 1$, $\beta\neq 1$ and $\alpha\neq\beta$. We divide these singular points into two cases:

  (III.A) Where III holds and $\alpha,\beta\in\mathbb{F}_{2^i}$.

  (III.B) Where III holds and α,β not both in $\mathbb{F}_{2^i}$.

This last theorem complete the case of all monomials. Now let take a look to the polynomial case. We will separate the polynomial case into the following 4 subcases.

1. Odd degree case, not Gold or Kasami-Welch.
2. Gold degree case.
3. Kasami-Welch degree case.
4. Even degree case.

1.3.2. *Odd degree case, not Gold or Kasami-Welch case.* This case was completely solved by Aubry, McGuire and Rodier [2] in the following theorem. Later in Chapter 2 we give an alternative proof of this theorem by using the new criteria develop in that chapter.

Theorem 22. If the degree of the polynomial function f is odd and not a Gold or a Kasami-Welch number, then f is not APN over $\mathbb{F}_q^n$ for all n sufficiently large.

1.3.3. *The degree of f is a Gold number.* Now we are going to explore the case of polynomials of degree 2^r+1. The following results summarize what is known in this case.

Theorem 23. [2] Suppose $f(X)=X^{2^r+1}+h(X)$ $h(X)$ have $\deg(h)\leq 2^{r-1}+1$. Let $h(X)=\sum_{j=0}^{2^{r-1}+1}a_jX^j$. If there exist a coefficient $a_j\neq 0$ in h such that $\phi_j(X,Y,Z)$ is absolutely irreducible, then $\phi(X,Y,Z)$ is also absolutely irreducible. Moreover f is not exceptional APN.

Theorem 24 ([2])**.** Suppose $f(X)=X^{2^r+1}+h(X)\in\mathbb{F}_{2^n}[x]$ and $\deg(h)=2^{r-1}+2$. Let r be odd and relatively prime to n. If $g(x)$ does not have the form $\alpha x^{2^{k-1}+2}+\alpha^2x^3$ then ϕ is absolutely irreducible, while if $g(x)$ does have this form, then either ϕ is absolutely irreducible or ϕ splits into two absolutely irreducible factors that are both defined over L.

Theorem 25 (DJ [15])**.** Let $k\geq 2$ and $\alpha\neq 0$. Take $h(x)=\sum_{j=0}^{2^{k-1}+1}a_jx^j\in\mathbb{F}_q[2^n]$ and suppose that a) or b) holds.

a) $a_5 = 0$
b) There is a nonzero $a_j\phi_j$ for some $j \neq 5$.

Set $f(x) = x^{2^k+1} + \alpha x^{2^{k-1}+3} + h(x) \in \mathbb{F}_{2^n}[x]$. Then $\phi(X,Y,Z)$ is absolutely irreducible.

Theorem 26. [15] If $f(X) = X^{2^r+1} + h(X)$, $\deg(h) \equiv 3 \pmod 4$, $\deg(h) < 2^r + 1$ and $r \geq 2$. then $f(X)$ is not exceptional APN.

Theorem 27. [15] For $k \geq 2$, let $f(X) = 2^k + 1 + h(X) \in L[x]$, where $\deg(h(X) \equiv 1 \pmod 4) < 2^k + 1$. If $(\phi_{2^k+1}, \phi_d) = 1$, then f is not exceptional APN.

Later Delgado and Janwa improve this theorem.

Theorem 28 ([15])**.** For $k \geq 2$, let $f(X) = 2^k + 1 + h(X) \in L[x]$, where $\deg(h(X) \equiv 1 \pmod 4) < 2^k + 1$. If $\deg(h)$ is not a Gold number, then f is not exceptional APN.

This last theorem left some exceptions which have been partially solved. In Chapter 3 we will prove the remaining cases.

Theorem 29. [11, 16] For $k \geq 2$, let $f(X) = X^{2^k+1} + h(X) \in \mathbb{F}_{2^{n}[x]}$ where $\deg(h) = 2^s + 1 < 2^k + 1$. Then:

a. If $(k,s) = 1$, then f is not exceptional APN.
b. If $(k,s) \neq 1$ and h contains a term of degree m such that $(\phi_{2^k+1}, \phi_m) = 1$, then ϕ_f is not exceptional APN.

Theorem 30. [44, 14] For $k_1 \geq 2$, let $f(x) = x^{2^{k_1}+1} + h(x) \in \mathbb{F}_{2^n}[x]$, where $\deg(h) = 2^{k_2+1} < 2^{k_1} + 1$. Then ϕ is absolutely irreducible when $h(x) = \sum_{j=2}^{t} a_j x^{2^{k_j}+1}$, is such that $a_j \neq 0$ for $2 \leq j \leq t$, and $(k_1, \ldots, k_t) = 1$ and f is not an exceptional APN function. Under the same conditions, if $(k_1, \ldots, k_t) = q > 1$, then ϕ is divisible by ϕ_{2^q+1} and ϕ is not absolutely irreducible.

Theorem 31 ([14])**.** Let $f(x) = x^{2^{k_1}+1} + h(x) \in \mathbb{F}_{2^n}[x]$, where $\deg(h) = 2^{k_2+1} < 2^{k_1} + 1$. If $h(x) = \sum_{j=2}^{t} a_j x^{2^{m_j}(2^{k_j}+1)}$ and $(k_1, \ldots, k_t) = (k_1, k_2) = q > 1$, then ϕ contains an absolutely irreducible factor and f is not exceptional APN.

In Chapter 3 we remove the condition $(k_1, \ldots, k_t) = (k_1, k_2)$ from the previous theorem and thus finish the conjecture in the odd degee case of the Gold case.

1.3.4. *Kasami-Welch Case.* From the odd cases, the Kasami-Welch turns out to be the most difficult. Only a few results have been obtained. Here we are just going to present the two main results that have been obtained so far. The first results in these cases whereby Ferard, Oyono, and Rodier in [26]. Apart from those results and the ones presented here, there is nothing much proved.

Theorem 32. [26] Suppose that $f(X) = X^{4^k-2^k+1} + g(X) \in \mathbb{F}_{2^n}[x]$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 2$. Let $k \geq 3$ be odd and relatively prime to n. If $g(X)$ does have the form $aX^{2k-1-2^{k-1}+2} + a^2X^3$ then ϕ is absolutely irreducible, while if $g(X)$ does have this form then either ϕ is irreducible or ϕ splits into two absolutely irreducible factors which are both defined over $\mathbb{F}_{2^n}$.

Theorem 33. [26] Let $f(x) = x^{2^{2k}-2^k+1} + g(x) \in L[x]$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Assume, there exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not exceptional APN.

Theorem 34. [12, 25] Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_{2^n}$, where $d = \deg(h) \equiv 3 \pmod 4$. Then $\phi(X, Y, Z)$ is absolutely irreducible.

Ferard in [25] obtains the same result by using different arguments.

Theorem 35. [12] Let $f(X) = X^{2^{2k}-2^k+1} + h(X)$, where $d = \deg(h) \equiv 5 \pmod 8$, $h < 2^{2k} - 3(2^k) - 1$. If $(\phi_{2^{2k}-2^k+1}, \phi_d) = 1$, then f is not exceptional APN.

In Chapter 4 we generalize this result in two different ways.

Theorem 36. [Ferard [25]] Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ a Kasami exponent, d and odd integer, $5 \leq d < k_r$ and $f(x) = x^{k_r} + h(x)$ where $h(x)$ is a polynomial of degree d. Assume that $d \equiv 1 \pmod 4$. We write $d = 12^j l$ with l an odd integer and j and integer ≥ 2. If $2^r - 1$ does not divide l, then $\phi_f(X, Y, Z)$ is absolutely irreducible.

1.3.5. *Even degree.* This case is the hardest case of all except when the degree is of the form $2e$, with e odd. Until now there not exists a clear path on how to proceed. We gave a new criterion that can potentially simplify these problems.

Theorem 37. [2] If the degree of the polynomial function f is $2e$ with e odd, and if f contains a term of odd degree, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

We will give in Chapter 2, an alternative proof of this theorem using our new techniques.

Theorem 38. [47] If the degree of the polynomial function f is even such that $\deg(f) = 4e$ with $e \equiv 3 \pmod 4$, and if the polynomials of the form

$$(x + y)(y + z)(x + z) + P,$$

with

$$P(X, Y, Z) = c_1(X^2 + y^2 + z^2) + c_4(xy + xz + zy) + b_1(x + y + z) + d$$

for $c_1, c_4, b_1, d \in \mathbb{F}_{q^3}$, do not divide ϕ then f is not APN over $\mathbb{F}_{q^n}$ for n large.

Theorem 39. [8] Let $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $\deg(f) = 4e$ with $e \equiv 3 \pmod 4$ and $e > 3$, then f cannot be APN over infinitely many extensions of $\mathbb{F}_q$.

Caullery also proves the following theorem. This theorem characterizes the exceptional APN polynomials of degree $4e$, e odd. We are going to use later this theorem together with some new techniques to prove that certain polynomials of degree $4e$ when $e \equiv 1 \pmod 4$ are not exceptional APN.

Theorem 40 ([10])**.** Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an exceptional APN function of degree $4e$ with e odd and let $\phi_f(X, Y, Z)$ be its associated polynomial. Let σ be a generator of the Galois group $Gal(\mathbb{F}_{2^{3n}}/\mathbb{F}_{2^n})$. One of the three conditions holds

(1) The polynomial ϕ_f is divisible by

$$(\phi_6 + P(X, Y, Z))(\phi_6 + \sigma(P(X, Y, Z)))(\phi_6 + \sigma^2(P(X, Y, Z))),$$

where $P(X, Y, Z)$ is a symmetric polynomial of degree 2 defined over $\mathbb{F}_{q^3}$.

(2) The polynomial ϕ_f is divisible by

$$(\Psi(X,Y,Z)+L(X,Y,Z))(\phi_6\Psi(X,Y,Z)+R(X,Y,Z))\sigma((\phi_6\Psi(X,Y,Z)+ R(X,Y,Z))\sigma^2((\phi_6\Psi(X,Y,Z)+R(X,Y,Z)),$$

where $\Psi(X,Y,Z)$ is a non absolutely irreducible symmetric factor of ϕ_e defined over $\mathbb{F}_{2^{3n}}$ but not over $\mathbb{F}_{2^n}$ and $R(X,Y,Z)$ annd $L(X,Y,Z)$ are symmetric polynomials of degree respectively less than $\deg(A\Psi)$ and $\deg(\Psi)$ defined over $\mathbb{F}_{2^{3n}}$ and $\mathbb{F}_{2^n}$.

(3) The polynomial ϕ_f is divisible by

$$(\phi_6\psi^3(X,Y,Z)+S(X,Y,Z))\sigma(\phi_6\psi^3(X,Y,Z)+S(X,Y,Z))\sigma^2(\phi_6\psi^3(X,Y,Z)+S(X,Y,Z)),$$

where $\psi(X,Y,Z)$ is a square-free non absolutely irreducible symmetric factor of ϕ_e defined over $\mathbb{F}_{2^{3n}}$ such that ψ, $\sigma(\psi)$ and $\sigma^2(\psi)$ are coprime.

2. New Absolute Irreducibility Testing Criteria

This chapter is divided into four sections. In the first section, we define the reverse polynomial for a certain class of polynomials and then prove there exists a relationship between the factorization of a polynomial and its reverse polynomial. Moreover, in definition 14 we introduce a new concept that we called the first cone of a polynomial. Then, we show there exists a relationship between the first cone of a polynomial and the tangent cone of its reverse polynomial.
In the second section, we use the tangent cone, the first cone, and the combination of both cones to create a new absolute irreducibility testing criterion as well as some criteria that guarantee the existence of absolutely irreducible factors. Moreover, we generalized lemma 5 for the case of more than two variables. In the third section, we introduce a new definition called the degree-gap of a polynomial. Using this definition, we can characterize the factorization of a large family of multivariate polynomials. Moreover, we generalize Lemma 2. In the last section of this chapter, we gave an alternative proof of some results of the exceptional APN conjecture.

2.1. **Reverse Mapping.**

Before proving some results, we first introduce some notation that is useful for stating the results. Let $G(X) = G(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ be a polynomial. Define d_i to be greatest integer such that $X_i^{d_i}$ divides at least one of the terms of the polynomial $G(X)$. Notice that if the polynomial is symmetric then $d_1 == \cdots = d_n = d$. Define the polynomial $\psi_G(X) = \psi_G(X_1, \dots, X_n) = X_1^{d_1} \cdots X_n^{d_n} f(\frac{1}{X_1}, \dots, \frac{1}{X_n})$. We called $\psi_G(X)$ the *reverse polynomial* of $G(X)$. When the context is clear we will denoted $\psi_G(X)$ by simply $\psi(X)$. Notice that if $G(X_1, \dots, X_n) = X_1^{d_1} \cdots X_n^{d_n}$ then $\psi(X) = 1$. For the rest of this article we will assume that X_i do not divide $G(X)$ for every $i \in \{1, \dots n\}$.

Lemma 13. Let $G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$, then $G(X)$ is reducible over $\mathbb{F}_q$ if and only if $\psi_G(X)$ is reducible over $\mathbb{F}_q$.

Proof: Suppose that $G(X) = P(X)Q(X)$. Define q_i to be the greatest integer such that $X_i^{q_i}$ divides at least one term of $Q(X)$ (respectively define p_i to be the greatest integer such that $X_i^{p_i}$ divides $P(X)$). Notice that $p_i + q_i = d_i$. Then

$$\psi_G(X) = X_1^{d_1} \cdots X_n^{d_n} G(\frac{1}{X_1}, \dots, \frac{1}{X_n}) =$$

$$X_1^{p_1} \cdots, X_n^{p_n} P(\frac{1}{X_1}, \dots, \frac{1}{X_n}) X_1^{q_1} \cdots X_n^{q_n} Q(\frac{1}{X_1}, \dots, \frac{1}{X_n})$$

Since X_i do not divide $G(X)$ for every $i \in \{1, \dots, n\}$, we have that X_i do not divide $P(X)$ and $Q(X)$ for every $i \in \{1, \dots, n\}$.
Notice that $X_1^{p_1} \cdots, X_n^{p_n} P(\frac{1}{X_1}, \dots, \frac{1}{X_n}) \in \mathbb{F}_q[X_1, \dots, X_n]$ and
$X_1^{q_1} \cdots X_n^{q_n} Q(\frac{1}{X_1}, \dots, \frac{1}{X_n}) \in \mathbb{F}_q[X_1, \dots, X_n]$. Since X_i do not divide any of the polynomials for every $i \in \{1, \dots, n\}$ is clear that the degree of both polynomial is ≥ 1. Therefore, $\psi_G(X)$ is reducible.

Now we will prove that the reverse of $\psi_G(X)$ is $G(X)$. For every $i \in \{1, \dots, n\}$, since X_i do not divide $G(X)$ this implies there exists a term (we will denote it by $g_i(X)$) in $G(X)$ such that X_i do not divide it. Now this implies that the term $X_1^{d_1} \cdots X_n^{d_n} g_i(\frac{1}{X_1}, \dots, \frac{1}{X_n})$ is a term of $\psi_f(X)$. Therefore, $X_i^{d_i}$ divide at least one term of $\psi_G(X)$. Now by the definition of $\psi_G(X)$ we know there not exists a $i \in \{1, \dots, n\}$ such that $X_i^{d_i}$ divide a term of $\psi_G(X)$. Therefore the reverse of $\psi_G(X)$ is given by

$$X_1^{d_1} \cdots X_n^{d_n} \psi_f(\frac{1}{X_1}, \dots, \frac{1}{X_n}) = X_1^{d_1} \cdots X_n^{d_n} \cdot \frac{1}{X_1^{d_1} \cdots X_n^{d_n}} f(X) = f(X).$$

Therefore, if $\psi_f(X)$ is reducible by the first part, $f(X)$ is also reducible. □

Definition 14. Let $G(X) = G_d(X) + \cdots + G_0(X) \in \mathbb{F}_q[X_1, \dots, X_n]$, where $G_i(X)$ is either a homogeneous polynomial of degree i or 0. We called $G_d(X)$ the **first cone** of $G(X)$.

Lets denote by $T_G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$ the tangent cone of $G(X)$ and $t_G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$ the first cone of $G(X)$. When the context is clear we will denoted $T_G(X)$ by $T(X)$ and $t_G(X)$ by $t(X)$.

Lemma 14. Suppose $G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$, then the tangent cone of $\psi_G(X)$ is given by

$$T_\psi(X) = X_1^{d_1} \cdots X_n^{d_n} t_G(\frac{1}{X_1}, \dots, \frac{1}{X_n}). \tag{4}$$

Moreover, if for every $i \in \{1, \dots, n\}$, s_i is the highest power of X_i such that $X_i^{s^i}$ divides at least one term of $t_G(X)$, then $T_\psi(X)$ can be written as follows

$$T_\psi(X) = X_1^{d_1 - s_1} \cdots X_n^{d_n - s_n} \psi_{G_s}(X_1, \dots, X_n) \tag{5}$$

Proof: Let $G(X) = G_s(X) + G_{s-1}(X) + \cdots + G_0(X_1, \dots, X_n)$, where $G_i(X_1, \dots, X_n)$ is a form of degree i or 0. Now taking the reverse on both sides we obtain that

$$\psi(X) = X_1^{d_1} \cdots X_n^{d_n} f(\frac{1}{X_1}, \dots, \frac{1}{X_n}) =$$

$$X_1^{d_1} \cdots X_n^{d_n} (G_s(\frac{1}{X_1}, \dots, \frac{1}{X_n}) + \cdots + G_0(\frac{1}{X_1}, \dots, \frac{1}{X_n}))$$

This implies that $X_1^{d_1} \cdots X_n^{d_n} G_i(\frac{1}{X_i}, \dots, \frac{1}{X_n})$ is either a form of degree $d_1 + d_2 + \cdots + d_n - i$ or 0. Since $\deg(G(X)) = s$ and $G_s(X_1, \dots, X_n) \neq 0$. We can conclude that equation 4 is the equation of the tangent cone. Equation 5 is obtained directly from equation 4 and the definition of s_i. □

The following two corollary are a direct consequence of lemma 13 and equation 5.

Corollary 4. Let $G(X) \in \mathbb{F}_q[X_1, \dots, X_n]$. If the $t_G(X)$ contains an irreducible factor (absolutely irreducible factor) of multiplicity n_1 defined over $\mathbb{F}_q$, then $T_\psi(X)$ contains an irreducible factor (absolutely irreducible factor) of multiplicity n_1 over $\mathbb{F}_q$.

Proof: Suppose that $t_G(X)$ contains an irreducible factor (absolutely irreducible factor) of multiplicity n_1 over $\mathbb{F}_q$. By lemma 13 and equation 5 we can conclude that $T_\psi(X)$ contains an irreducible factor (absolutely irreducible factor) of multiplicity n_1 defined over $\mathbb{F}_q$. □

Remark: Every result we obtain for the tangent cone of a polynomial will imply an analog result for the first cone of a polynomial since the first cone of $G(X)$ will correspond to the tangent cone of $\psi_G(X)$.

2.2. **New Absolute Irreducibility Testing Criteria.**

2.2.1. *Using the Tangent Cone to Create Criterion for Testing Absolute Irreducibility.* The following proposition extends lemma 6 to Theorem 41 which will be useful for the proof of Theorem 43.

Proposition 8. Suppose that $h(X_1,\dots,X_n) \in \mathbb{F}_{q^r}[X_1,\dots,X_n]$ is absolutely irreducible, then for every $\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$, $\sigma(h) = \sigma(h(X_1,\dots,X_n))$ is absolutely irreducible.

Proof: Assume that for some $\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ we have that $\sigma(h)$ is reducible, i.e. $\sigma(h) = ab$, where $a, b \in \mathbb{F}_{q^r}[X_1,\dots,X_n]$. Now apply σ^{-1} to both sides to obtain, $h = (\sigma^{-1} \circ \sigma)(h) = \sigma^{-1}(a)\sigma^{-1}(b)$. This implies that either $\sigma^{-1}(a)$ is constant or $\sigma^{-1}(b)$ is a constant. This lead to either a be constant or b be a constant, which is a contradiction with $\sigma(h)$ being reducible. Assume that for some $\beta \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ we have that $\beta(h)$ is not absolutely irreducible. By lemma 6 we know there exists a k, an absolutely irreducible polynomial $G \in \mathbb{F}_{q^{rk}}$ and $c \in \mathbb{F}_{q^r}$ such that:

$$\beta(h) = c \prod_{\sigma \in Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_{q^r})} \sigma(G).$$

Notice that $Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_{q^r})) \triangleleft Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_q)$ and $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q) \triangleleft Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_q)$. Therefore, every $\sigma \in Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_{q^r})$ and β, β^{-1} are element of $Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_q)$ so we can apply β^{-1} to both sides to obtain

$$h = c \prod_{\sigma \in Gal(\mathbb{F}_{q^{rk}}/\mathbb{F}_{q^r})} (\beta^{-1} \circ \sigma)(G)$$

Since h is absolutely irreducible we obtain the same contradiction as before. □

The following theorem generalizes lemma 6 in the sense that we show that each factor is absolutely irreducible.

Theorem 41. Suppose $p(X) \in \mathbb{F}_q[X_1,\dots,X_n]$ is of degree d and is irreducible in $\mathbb{F}_q[X_1,\dots,X_n]$. Then there exists a unique r with $r \mid d$ and an absolutely irreducible polynomial $h(X) \in \mathbb{F}_{q^r}[X_1,\dots,X_n]$ of degree d/r such that

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

where $G = Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ and $c \in \mathbb{F}_q$. For each $\sigma \in G$, $\sigma(h(X))$ is absolutely irreducible. Furthermore, if $p(X)$ is homogeneous, then so is $h(X)$.

Remark: Let $\mathbb{F}(G)$ be the splitting field of $G(X)$, where $G(X)$ split completely into absolutely irreducible factors. Let $m(G) = [\mathbb{F}_q(G)) : \mathbb{F}_q]$. Then $m(G)$ is an invariant of $G(X)$. It is clear that if $G(X)$ is irreducible then the r obtained in theorem 41 is equal to $m(G)$.

Let $G(X)$ be an irreducible polynomial. Then, there exist an absolutely irreducible polynomial $h(X) \in \mathbb{F}_q(G)[X_1, \ldots, X_n]$ and $c \in \mathbb{F}_q$

$$G(X) = \prod_{\sigma \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)} \sigma(h(X)). \tag{6}$$

Let $T(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the tangent cone of $G(X)$ and let $T_h(X) \in \mathbb{F}_{q^r}[X_1, \ldots, X_n]$ be the tangent cone of $h(X)$. Then we have that

$$T(X) = c \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(T_h(X)). \tag{7}$$

Let $t(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the tangent cone of $G(X)$ and let $t_h(X) \in \mathbb{F}_{q^r}[X_1, \ldots, X_n]$ be the tangent cone of $h(X)$. Then we have that

$$t(X) = c \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(t_h(X)). \tag{8}$$

The following theorem is a generalization of lemma 5 above. This is a generalized to multi-variable case and for absolutely irreducible component rather than a linear factor.

Theorem 42. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $T_G(X)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$ then $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Note that if $G(X)$ factors then the tangent cone of $G(X)$ is the product of the tangent cone of the factors. Therefore, without loss of generality we can assume that $G(X)$ is irreducible. So there exists $h(X) \in \mathbb{F}_q(G)[X_1, \ldots, X_n]$ such that $G(X)$ satisfy equation 6 and $T_G(X)$ satisfy equation 7.
Since $T_G(X)$ contains a reduce absolutely irreducible factor $t_1(X)$, there exists $\alpha \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $t_1(X) \mid \alpha(T_h(X))$. For every $\beta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ we have $\beta(t_1(X)) = t_1(X) \mid (\beta \circ \alpha)(T_h(X))$. Since $t_1(X)$ is reduced, this force $r = 1$. Therefore $G(X)$ be absolutely irreducible over $\mathbb{F}_q$. □

Corollary 5. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $t_G(X)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$ then $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Let $\psi_G(X)$ be the reverse polynomial of $G(X)$, then by theorem 42 $\psi_G(X)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. Therefore, by lemma 13 $G(X)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

Before stating and proving the new criterion for testing absolute irreducibility we will prove the following lemmas which will be useful during the proof.

Lemma 15. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $T_G(X)$ contain an absolutely irreducible factor $t_1(X)$ of multiplicity n_1, then $m(G) \mid n_1$.

Proof: Suppose $G(X)$ is irreducible, then there exists $h(X) \in \mathbb{F}_q(G)[X_1, \ldots, X_n]$, $c \in \mathbb{F}_q$ such that $G(X)$ satisfy equation 6 and $T_G(X)$ satisfy equation 7. Since $t_1(X)$ is absolutely irreducible there exist $\alpha \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $t_1(X) \mid \alpha(T_h(X))$. Take l to be the greatest integer such that $t_1(X)^l \mid \alpha(T_h(X))$. For every $\beta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ we have

$\beta(t_1(X)^l) = t_1(X)^l \mid (\beta \circ \alpha)(T_h(X))$. Since every element of $Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ can be written in the form $(\beta \circ \alpha)$ we can conclude that $t_1(X)^l \mid \gamma(T_h(X))$ for every $\gamma \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$. Notice that there not exists $\delta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $t_1^{l+1}(X) \mid \delta(T_h(X))$ because if there exist that would imply by the first part that $t_1^{l+1} \mid \alpha(T_h(X))$ which is a contradiction of the definition of l. Therefore, we can conclude that $|Gal(\mathbb{F}_q(G)/\mathbb{F}_q)| = m(G) \mid n_1$. □

Corollary 6. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $t_G(X)$ contain an absolutely irreducible factor $R_1(X)$ of multiplicity n_1, then $m(G) \mid n_1$.

Proof: Let $\psi_G(X)$ be the reverse polynomial of $G(X)$, then by lemma 13 we have that $m(G) = m(\psi_G)$. By lemma 4 the tangent cone of $\psi_G(X)$ contains an absolutely irreducible factor of multiplicity n_1. Therefore, by lemma 15 $m(G) \mid n_1$. □

Lemma 16. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $T_G(X)$ contains a reduced irreducible factor $R(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, then $m(G) \mid m(R)$.

Proof: Suppose $G(X)$ is irreducible, then there exists $h(X) \in \mathbb{F}_q(G)[X_1, \ldots, X_n]$, $c \in \mathbb{F}_q$ such that $G(X)$ satisfy equation 6 and $T_G(X)$ satisfy equation 7. Let $t_1(X) \in \mathbb{F}_q(R)[X_1, \ldots, X_n]$ be an absolutely irreducible factor of $R(X)$ and $t_1(X) \mid T_G(X)$. Notice that $t_1(X)$ is reduced otherwise it contradict the fact that $R(X)$ is reduced. By theorem 42 $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q(R)$. Since the factorization in equation 6 is the factorization into absolutely irreducible factors which is unique up to ordering and associates we have that either $m(G) \mid m(R)$ or $m(R) \mid m(G)$.
Assume that $m(R) \mid m(G)$ with $m(G) > m(R)$. Let $\alpha \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ be a generator of $Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$. Since $t_1(X)$ is absolutely irreducible there exists a $\beta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $t_1(X) \mid \beta(T_h(X))$. Then $\alpha^{m(R)}(t_1(X)) = t_1(X) \mid (\alpha^{m(R)} \circ \beta)(T_h(X)) \neq \beta(T_h(X))$ which contradicts the fact that $t_1(X)$ is a reduced factor. Therefore, $m(G) \mid m(R)$. □

Corollary 7. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $t_G(X)$ contains a reduced irreducible factor $R(X) \in \mathbb{F}_q[x_1, \ldots, X_n]$, then $m(G) \mid m(R)$.

Proof: Let $\psi_G(X)$ be the reverse polynomial of $G(X)$. Then by lemma 13 we have that $m(G) = m(\psi_G)$. By lemma 4 the tangent cone of $\psi_G(X)$ contains a reduced irreducible factor $\psi_f(X)$ with $m(R) = m(\psi_R(X))$. Therefore, by lemma 16 $m(G) \mid m(R)$. □

Lemma 17. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $T_G(X)$ contains an irreducible factor $R(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and $(m(R), m(G)) = 1$. Then $m(G) \mid n_1$.

Proof: Suppose $G(X)$ is irreducible, then there exists $h(X) \in \mathbb{F}_q(G)[X_1, \ldots, X_n]$, $c \in \mathbb{F}_q$ such that $G(X)$ satisfy equation 6 and $T_G(X)$ satisfy equation 7. Now $(m(R), m(G)) = 1$ this implies that $R(X)$ is irreducible over $\mathbb{F}_q(G)$. Then there exist $\alpha \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $R(X) \mid T_h(X)$.Take l to be the greatest integer such that $R(X)^l \mid \alpha(T_h(X))$. For every $\beta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ we have $\beta(R(X)^l) = R(X)^l \mid (\beta \circ \alpha)(T_h(X))$. Since every element of $Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ can be written in the form $(\beta \circ \alpha)$ we can conclude that $R(X)^l \mid \gamma(T_h(X))$ for every $\gamma \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$. Notice that there not exists $\delta \in Gal(\mathbb{F}_q(G)/\mathbb{F}_q)$ such that $R^{l+1}(X) \mid \delta(T_h(X))$ because if there exist that would imply by the first part that $R^{l+1} \mid \alpha(T_h(X))$ which is a contradiction of the definition of l. Therefore, we can conclude that $|Gal(\mathbb{F}_q(G)/\mathbb{F}_q)| = m(G) \mid n_1$. □

Corollary 8. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If $t_G(X)$ contains an irreducible factor $R(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and $(m(R), m(G)) = 1$. Then $m(G) \mid n_1$.

Proof: Let $\psi_G(X)$ be the reverse polynomial of $G(X)$. Then by lemma 13 we have that $m(G) = m(\psi_G)$. By lemma 4 the tangent cone of $\psi_G(X)$ contains a absolutely irreducible factor of multiplicity n_1. Therefore, by lemma 16 $m(G) \mid n_1$. □

Remark: Notice that $J(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ is irreducible if and only if for any $a \in \mathbb{F}_q^n$, $J(X - a)$ is irreducible. Therefore, $m(J)$ is invariant to translation of $J(X)$.

Theorem 43. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial and let $a, b \in \mathbb{F}_q^n$. If one of the following conditions is satisfied then $G(X)$ is absolutely irreducible.

(1) The tangent cone of $G(X - a)$ contain a absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and the tangent cone of $G(X - b)$ contain an absolutely irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$.

(2) The tangent cone of $G(X - a)$ contain an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and the tangent cone of $G(X - b)$ contain an irreducible polynomial $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$ and $(m(G), m(R_2)) = 1$.

(3) The tangent cone of $G(X - a)$ contain an irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and the tangent cone of $G(X - b)$ contain irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $(m(R_1), m(R_2)) = 1$.

Proof: Suppose $G(X)$ is irreducible. We prove that each of the conditions implies that $G(X)$ is absolutely irreducible.

(1) Suppose that the tangent cone of $G(X - a)$ contain a absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and the tangent cone of $G(X - b)$ contain a absolutely irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$. Then, by applying lemma 15 twice we obtain that $m(G)$ divides both n_1 and n_2. Therefore, $m(G) \mid (n_1, n_2)$. Thus $G(X)$ is absolutely irreducible.

(2) Suppose that the tangent cone of $G(X - a)$ contain an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and the tangent cone of $G(X - b)$ contain an irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$ and $(m(R_2), m(G)) = 1$. Then applying lemma 15 to the tangent cone of $G(X - a)$ we obtain that $m(G) \mid n_1$. Applying lemma 17 to the tangent cone of $G(X - b)$, we obtain that $m(G) \mid n_2$. Therefore, $m(G) \mid (n_1, n_2)$. Thus $G(X)$ is absolutely irreducible.

(3) Suppose The tangent cone of $G(X - a)$ contain an irreducible factor $R_1(X)$ and the tangent cone of $G(X - b)$ contain an irreducible factor $R_2(X)$, with $(m(R_1), m(R_2)) = 1$. By applying lemma 16 to the tangent cone of $G(X - a)$, we obtain that $m(G) \mid n_1$. Similarly, if we apply lemma 16 to the tangent cone of $G(X - b)$, we obtain that $m(G) \mid n_2$. Therefore, $m(G) \mid (n_1, n_2)$. Thus $G(X)$ is absolutely irreducible.

□

Corollary 9. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If one of the following conditions is satisfied, then $G(X)$ is absolutely irreducible.

(1) $T_G(X)$ contain two absolutely irreducible factors $R_1(X)$, $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicities n_1, n_2 (respectively) with $(n_1, n_2) = 1$.
(2) $T_G(X)$ contain an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and an irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$ and $(m(R), m(G)) = 1$.
(3) $T_G(X)$ contains two reduced absolutely irreducible factors $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $(m(R_1), m(R_2)) = 1$.

Proof: Take $a = b = 0$ and apply theorem 43 to conclude that $G(X)$ is absolutely irreducible. □

Corollary 10. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial and let $a, b \in \mathbb{F}_q^n$. If one of the following conditions is satisfied then $G(X)$ is absolutely irreducible.

(1) The first cone of $G(X-a)$ contain a absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicities n_1 and the first cone of $G(X - b)$ contain a absolutely irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicities n_2 with $(n_1, n_2) = 1$.
(2) The first cone of $G(X-a)$ contain a absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicities n_1 and the first cone of $G(X - b)$ contain an irreducible polynomial $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$ and $(m(R_2), m(G)) = 1$.
(3) The first cone of $G(X - a)$ contain an irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and the first cone of $G(X - b)$ contain an irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $(m(R_1), m(R_2)) = 1$.

Proof: Let $\psi_G(X)$ be the reverse polynomial of $G(X)$. By lemma 4 the tangent cone of $\psi_G(X)$ satisfy the same conditions as the first cone of $G(X)$. By theorem 43 $\psi_G(X)$ is absolutely irreducible. Therefore, by lemma 13 $G(X)$ is absolutely irreducible. □

Corollary 11. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible polynomial. If one of the following conditions is satisfied then $G(X)$ is absolutely irreducible.

(1) $t_G(X)$ contain two absolutely irreducible factors $R_1(X)$, $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicities n_1, n_2 (respectively) with $(n_1, n_2) = 1$.
(2) $t_G(X)$ contain an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1 and an irreducible polynomial $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$ and $(m(R_2), m(G)) = 1$.
(3) $t_G(X)$ contains two reduced irreducible factors $R_1(X), R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $(m(R_1), m(R_2)) = 1$.

Proof: Take $a = b = 0$ and apply corollary 10 to conclude that $G(X)$ is absolutely irreducible. □

Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $a \in \mathbb{F}_q^n$ we will denote by $\mathcal{M}_a(G)$ be the multiplicity of a.

Theorem 44. Let $F(X)$, $H(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If there exists $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that $1 \leq \mathcal{M}_a(F) < \mathcal{M}_a(H)$ and the tangent cone of $F(X - a)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$, then $G(X) = F(X) + H(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Take $G(X-a)$. Lets compute the tangent cone of this polynomial. Since $m_a(f) < m_a(h)$ we know the tangent cone is of $G(X-a)$ is the same as the tangent cone of $F(X-a)$. Then by assumption the tangent cone of $G(X-a)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$. By theorem 42, $G(X_1+a_1,\dots,X_n+a_n)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$. Thus, $G(X_1,\dots,X_n)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Corollary 12. Let $F(X)$, $H(X) \in \mathbb{F}_q[X_1,\dots,X_n]$. If there exists $a=(a_1,\dots,a_n)\in\mathbb{F}_q^n$ such that $\mathcal{M}_a(F)=1$, and $\mathcal{M}_a(H)>1$, then $G(X)=F(X)+H(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

2.2.2. *Using the Tangent and the First Cone to Create Absolute Irreducibility Testing Criteria.*

Theorem 45. Let $G(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ and $a,b\in\mathbb{F}_q^n$ be an irreducible polynomial. If one of the following condition is satisfied, then $G(X)$ is absolutely irreducible.

1. The first cone of $G(X-a)$ contains a reduced irreducible factor $R_1(X)\in\mathbb{F}_q[X_1,\dots,X_n]$, and the tangent cone of $G(X-b)$ contains a reduced irreducible factor $R_2(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ with $(m(R_1),m(R_2))=1$.
2. The first cone of $G(X-a)$ contains an absolutely irreducible factor $R_1(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ of multiplicity n_1 and the tangent cone of $G(X-b)$ contains a reduced irreducible factor $R_2(X)$ with $(n_1,m(R_2))=1$.
3. The first cone of $G(X-a)$ contains a reduced irreducible factor $R_1(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ and the tangent cone of $G(X-b)$ contains an irreducible factor $R_2(X)$ of multiplicity n_2 with $(m(R_1),n_2)=1$.
4. The first cone of $G(X-a)$ contains an absolutely irreducible factor $R_1(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ of multiplicity n_1, and the tangent cone of $G(X-b)$ contains an absolutely irreducible factor $R_2(X)$ defined over $\mathbb{F}_q$ of multiplicity n_2 with $(n_1,n_2)=1$.

Proof: Since $G(X)$ is irreducible we have that $G(X-a)$ and $G(X-b)$ are irreducible. Now we prove that each of the conditions implies that $G(X)$ is absolutely irreducible.

1. By corollary 7 $m(G)\mid m(R_1)$. Similarly by lemma 16 $m(G)\mid m(R_2)$. Therefore, $m(G)\mid(m(R_1),m(R_2))$. Thus, $G(X)$ is absolutely irreducible.
2. By corollary 6 $m(G)\mid n_1$ and by lemma 16 $m(G)\mid m(R_2)$. Therefore, $m(G)\mid(n_1,m(R_2))$. Thus, $G(X)$ is absolutely irreducible.
3. By corollary 7 $m(G)\mid m(R_1)$ and by lemma 15 $m(G)\mid n_2$. Therefore, $m(G)\mid(m(R_1),n_2)$. Thus, $G(X)$ is absolutely irreducible.
4. By corollary 6 $m(G)\mid n_1$. Similarly, by lemma 15 $m(G)\mid n_2$. Therefore, $m(G)\mid(n_1,n_2)$. Thus, $G(X)$ is absolutely irreducible.

□

Corollary 13. Let $G(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ be a irreducible polynomial. If one of the following condition is satisfied, then $G(X)$ is absolutely irreducible.

1. $t_G(X)$ contains a reduced irreducible factor $R_1(X)\in\mathbb{F}_q[X_1,\dots,X_n]$, and $T_G(X)$ contains a reduced irreducible factor $R_2(X)\in\mathbb{F}_q[X_1,\dots,X_n]$ with $(m(R_1),m(R_2))=1$.

(2) $t_G(X)$ contains an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1, and $T_G(X)$ contains a reduced irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $(n_1, m(R_2)) = 1$.
(3) $t_G(X)$ contains a reduced irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, and $T_G(X)$ contains an absolutely irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(m(R_1), n_2) = 1$.
(4) $t_G(X)$ contains an absolutely irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_1, and $T_G(X)$ contains an absolutely irreducible factor $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of multiplicity n_2 with $(n_1, n_2) = 1$.

Proof: Take $a = b = 0$ and apply theorem 45 to conclude that $G(X)$ is absolutely irreducible. □

Theorem 46. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $a, b \in \mathbb{F}_q^n$. If the tangent cone of $G(X - a)$ contains a reduced irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, the first cone of $G(X - b)$ is reduced, and every irreducible factor of the first cone of $G(X - b)$ over $\mathbb{F}_q$ are also irreducible over $\mathbb{F}_q(R_1)$, then $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Suppose that $G(X)$ is irreducible, then $G(X - a)$ and $G(X - b)$ are irreducible. Let $R_2(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an irreducible factor of the first cone of $G(X - b)$, then $(m(R_1), m(R_2)) = 1$. Therefore, by theorem 45 part 1, $G(X)$ is absolutely irreducible.
Suppose that $G(X)$ factors over $\mathbb{F}_q$, then $G(X - a)$ and $G(X - b)$ also factors over $\mathbb{F}_q$. Let $Q(X - a) = P(X)Q(X)$, where $P(X), Q(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $Q(X)$ is an irreducible polynomial such that the tangent cone of $Q(X)$ contains $R_1(X)$. Notice that $Q(X + a - b)$ is an irreducible factor of $G(X - b)$. Since the degree of the first cone of $Q(X + a - b)$ is greater than 1, it contains a reduced irreducible factor. Now $Q(X + a)$ is a factor of $G(X)$, and by the first part of this proof it is absolutely irreducible. Therefore, $G(X)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

Corollary 14. Let $G(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $T_G(X)$ contains a reduced irreducible factor $R_1(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, and every irreducible factor of the first cone of $G(X)$ over $\mathbb{F}_q$ are also irreducible over $\mathbb{F}_q(R_1)$, then $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Take $a = b = 0$, then by theorem 46 $G(X)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

2.3. **Characterization of Factorization of a Large Family of Polynomials of Several Variables.** In this section, we will define a new concept called the degree-gap of a polynomial. This definition will allow us to characterize the factorization of a large family of multivariate polynomials. In concrete, we can bound the number of factors the polynomial can have as well as give a lower bound on the degree of the factors.

Definition 15. Let $f(X_1, \ldots, X_n)$ be a polynomial of degree n with at least two terms. We defined the *degree-gap* $DG(f)$ as the difference between the two highest degree of the polynomial. If $f(X_1, \ldots, X_n)$ is a homogeneous polynomial then $DG(f)$ is defined to be infinity.

Notice that if $f(X) = f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ satisfy that $\deg(f(X)) < DG(f)$ then $f(X)$ is a homogeneous polynomial.

Theorem 47. Let $F(\mathbf{X}) = F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X})$. If $F_m(\mathbf{X})$ is square free, then every factor of $F(\mathbf{X})$ has degree-gap at least that of $F(\mathbf{X})$.

Proof: If $F(\mathbf{X})$ is a homogeneous polynomial, then this result is immediate since a homogeneous polynomial factors as the product of homogeneous polynomials. Without loss of generality we can assume that $F(\mathbf{X})$ is not a homogeneous polynomial. It is clear that every homogeneous factor of $F(\mathbf{X})$ satisfy the stated property.

We may assume that without loss of generality that $(F_m, H) = 1$ that is there are no homogeneous factors. If $DG(F) = 1$, then this is a trivial result. Suppose that $DG(F) = k > 1$, then assume that $F(\mathbf{X})$ factors as follows

$$F(\mathbf{X}) = (P_s(\mathbf{X}) + \cdots + P_0(\mathbf{X}))(Q_t(\mathbf{X}) + \cdots + Q_0(\mathbf{X})),$$

where P_i, (respectively Q_j) is homogeneous polynomials of degree i (respectively degree j) or zero, and $DG(Q) \geq DG(P)$. Assume that $DG(F) > DG(P)$. Let $j = DG(P)$, then we have the following equation

$$0 = F_{m-j} = \sum_{i=1}^{j} P_{s-i} Q_{t-j+i}. \tag{9}$$

By the degree-gap of $P(\mathbf{X})$ we have that $P_{s-1} = \ldots P_{s-j+1} = 0$ (respectively by the degree-gap of $Q(\mathbf{X})$ $Q_{t-1} = \cdots = Q_{t-j+1} = 0$). Substituting these in Equation 9 we obtain

$$0 = \sum_{i=1}^{j} P_{s-i} Q_{t-j+i} = P_s Q_{t-j} + P_{s-j} Q_t$$

implying that $P_s Q_{t-j} = Q_t P_{s-j}$. Since $(P_s, Q_t) = 1$ as $F_m(\mathbf{X})$ is square free, we obtain that $P_s \mid P_{s-j}$ that is $P_{s-j} = 0$. This is a contradiction with $DG(P) = j$. Therefore, $DG(F) \leq DG(P) \leq DG(Q)$. Since $P(\mathbf{X})$ and $Q(\mathbf{X})$ are arbitrary factor we can conclude that every factor of $F(\mathbf{X})$ has degree-gap at least that of $F(\mathbf{X})$.

□

Corollary 15. Let $F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$, $F_m(\mathbf{X})$ is square free, and $(F_m, H) = 1$. If $P(\mathbf{X})$ is a factor of $F(\mathbf{X})$, then $\deg(P) \geq DG(F)$.

This corollary follows directly from the proof of Theorem 47

The following corollary gave a bound on the number of factors a polynomial satisfying certain conditions can have.

Corollary 16. Let $F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $F_m(\mathbf{X})$ is square free and $(F_m, H) = 1$, then $F(\mathbf{X})$ have at most $\left\lfloor \frac{\deg(F)}{DG(F)} \right\rfloor$ factors.

Proof: By Theorem 47 and Corollary 15 we have $\deg(G) \geq DG(F)$. Then $F(\mathbf{X})$ can have at most $\left\lfloor \frac{\deg(F)}{DG(F)} \right\rfloor$ factors. □

Using this corollary we can prove a generalization of Lemma 2 for finite fields in two different ways. First, we generalize to any multivariate polynomial and second, we weaken the greatest common divisor condition.

Corollary 17. Let $F(\mathbf{X}) \in F_m(\mathbf{X}) + H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $F_m(\mathbf{X})$ is square free, $(F_m, H) = 1$, and $2DG(F) > \deg(F)$, then $F(\mathbf{X})$ is absolutely irreducible.

Proof: By Corollary 16, $F(X)$ can have at most one factor. □

The following corollary gives sufficient conditions to guarantee that the degree-gap is preserved through factorization.

Corollary 18. Let $F(\mathbf{X}) = F_m(\mathbf{X})+H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$. If $F_m(\mathbf{X})$ is square free,$(F_m, H_d) = 1$, and $P(\mathbf{X})$ is a factor of $F(\mathbf{X})$, then $DG(P) = DG(F)$.

Proof: Assume that $F(\mathbf{X}) = (P_s(\mathbf{X})+\cdots+P_0(\mathbf{X}))(Q_t(\mathbf{X})+\cdots+Q_0(\mathbf{X})$. Then by the proof of Theorem 47 we have the following system of equations.

$$F_m(\mathbf{X}) = P_s(\mathbf{X})Q_t(\mathbf{X})$$
$$H_d(\mathbf{X}) = P_s(\mathbf{X})Q_{t-e}(\mathbf{X}) + P_{s-e}(\mathbf{X})Q_t(\mathbf{X}). \tag{10}$$

Since $(F_m, H_d) = 1$, we have that $P_{s-e}(\mathbf{X}) \neq 0$, and $Q_{t-e}(\mathbf{X}) \neq 0$. Therefore, $DG(P) = DG(F)$. □

Using this theorem we can show that many polynomials are absolutely irreducible. The following corollary proves that a class of polynomials is absolutely irreducible. Let $T_F(\mathbf{X})$ denote the tangent cone of a polynomial i.e., the lowest degree form of the polynomial.

Corollary 19. Let $F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$, where $\deg(F) = m$ and $\deg(H) = d < m$. If $F_m(\mathbf{X})$ is square free, $(F_m, H) = 1$ and $\deg(T_F) > \deg(F) - 2DG(F)$, then $F(\mathbf{X})$ is absolutely irreducible.

Proof: Assume that $F(\mathbf{X}) = P(\mathbf{X})Q(\mathbf{X})$, then $DG(P) \geq DG(F)$ and $DG(Q) \geq DG(Q)$. Then $\deg(T_P) \leq \deg(P) - DG(P) \leq \deg(P) - DG(F)$ and $\deg(T_Q) \leq \deg(Q) - DG(Q) \leq \deg(Q) - DG(F)$. Therefore, $\deg(T_F) = \deg(T_P) + \deg(T_Q) \leq \deg(Q) - DG(F) + \deg(P) - DG(F) = \deg(F) - 2DG(F)$. □

One can characterize the factorization of all monomials in which the highest degree form is square free.

Corollary 20. Let $F(\mathbf{X}) = F_m(\mathbf{X})+F_d(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$, where $\deg(F) = m$. If $F_m(\mathbf{X})$ is square free and $(F_m, F_d) = 1$, then $F(\mathbf{X})$ is absolutely irreducible.

Proof: Assume that $F(\mathbf{X}) = P(\mathbf{X})Q(\mathbf{X})$. Then by Theorem 47 $DG(P) = DG(F)$ and $DG(Q) = DG(F)$. Therefore, $T_F(\mathbf{X}) = T_P(\mathbf{X})T_Q(\mathbf{X})$, and $\deg(T_F) = \deg(T_P) + \deg(T_Q) \leq m - 2DG(F) < m - DG(F) = d$. □

Remark: Every polynomial $F(\mathbf{X}) = F_m(\mathbf{X}) + F_d(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$, where $F_m(\mathbf{X})$ is square free can be written as follows

$$F(\mathbf{X}) = L(\mathbf{X})Q(\mathbf{X}),$$

where $L(\mathbf{X}) = (F_m, F_d)$ and $Q(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$ is absolutely irreducible.

Corollary 21. Let $F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$, where $\deg(F) = m$, $\deg(H) = d$, $F_m(\mathbf{X})$ is square free and $(F_m, H) = 1$. If $F(\mathbf{X})$ is irreducible in $\mathbb{F}_{q^i}$ for $i = 1, \ldots, \left\lfloor \frac{\deg(F)}{DG(F)} \right\rfloor$, then F is absolutely irreducible.

Proof: Assume $F(\mathbf{X})$ factors over $\mathbb{F}_{q^r}$, where $r > \left\lfloor \frac{\deg(F)}{DG(F)} \right\rfloor$. Then, by Lemma 6 $F(\mathbf{X})$ have r-factors, but this contradicts Corollary 16. □

From this corollary, one can derive the following algorithm to test absolute irreducibility.

Algorithm 1: Absolute irreducibility testing

```
Result: The polynomial is absolutely irreducible or not
$t \leftarrow 1$;
$F(\mathbf{X}) \leftarrow$ polynomial in $\mathbb{F}_q[\mathbf{X}]$ satisfying conditions in Theorem 47;
while $t * DG(F) \leq \deg(F)$ do
    if if $F(\boldsymbol{X})$ is irreducible in $\mathbb{F}_{q^t}(\boldsymbol{X})$ then
        $t \leftarrow t + 1$;
    else
        return(F($\mathbf{X}$) is not absolutely irreducible);
        exit;
    end
end
return(F($\mathbf{X}$) is absolutely irreducible)
```

The following lemma is a generalization of Lemma 2 in two ways. It mild the conditions as well as generalized for polynomials of n variables.

Lemma 18. Let K be a field. Let $G(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a polynomial whose graded homogeneous representation is: $G = G_b + G_a + G_{a-1} + \cdots + G_0$, where G_i is 0 or homogeneous of degree $i \in \{0, \ldots, b\}$. If $b > 2a$, G_b factors into distinct irreducible factors over $\overline{K}$ and $(G_b, G_a, G_{a-1}, \ldots, G_0) = 1$, then G is absolutely irreducible.

Proof: Suppose that $G(X) = P(X)Q(X)$. Notice that $(G_b, G_a, G_{a-1}, \ldots, G_0) = 1$ implies that neither $P(X)$ or $Q(X)$ is homogeneous polynomial. By Definition 15 and Theorem 47 we have $\deg(P) \geq DG(G) > \frac{\deg(G)}{2}$ and $\deg(Q) \geq DG(G) > \frac{\deg(G)}{2}$. This is a contradiction with the degree of G. Therefore, G is absolutely irreducible. □

2.4. **Alternative Proofs.** For the rest of this thesis, let $q = 2^\ell$. We will assume that every polynomial $f(X) \in \mathbb{F}_q[x]$ contains an odd degree term. We can make this assumption without losing generalization because every polynomial with every term that has an even degree is EA-equivalent to a polynomial that contains an odd degree term.

Theorems 48 and 49 were proved originally in [2]. Here we gave new proofs of these theorems using the techniques developed at the beginning of this chapter.

Theorem 48. If the degree of the polynomial function $f(X) \in \mathbb{F}_q$ is odd and not a Gold or a Kasami-Welch number then $f(X)$ is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

Proof: By Hernando and Mcguire [31] we know that if the degree of $\deg(f) = d$ is odd and not a Gold or a Kasami-Welch number then $\phi_d(X, Y, Z)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$. Therefore, by corollary 5 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Thus, $f(X)$ is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large. □

Theorem 49. If the degree of the polynomial function $f(X) \in \mathbb{F}_q[x]$ is $2e$ with e odd, and if f contains a term of odd degree, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

Proof: Notice that $\phi_{2e} = \phi_6(X, Y, Z)\phi_e^2$ and $\phi_6(X, Y, Z) \nmid \phi_e$. This implies that ϕ_{2e} contains a reduced linear factor. Therefore, by corollary 5 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Thus, $f(X)$ is not APN over $\mathbb{F}_q^n$ for all n sufficiently large. □

3. Completion of the Gold Degree Case with Even Degree-gap and Substantial Progress in the Odd Degree-gap Case

This chapter is divided into four sections. In the first section, we use the concept of degree gap to provide bounds to guarantee the existence of absolute irreducible factors. Later in the next two sections this bounds will be improve using the multiplicity of the point $(1,1,1)$ to give an upper bound in the number of factors $\phi_f(X,Y,Z)$ can have in the remaining open cases in the literature. In the second section we prove the case when the second term have odd degree. We use 17 develop in the previous chapter to proof the remaining cases in the literature.

In the third section we investigate the case when the second term have even degree $2^{n-j}e$, when $e \equiv 3 \pmod 4$. We gave a bound in the number of factors the polynomial could have and show that if $j \geq 4$ then $\phi_f(X,Y,Z)$ contains an absolute irreducible factor defined over $\mathbb{F}_q$ and therefore, $f(X)$ is not exceptional APN. In the last section we investigate the case when $e \equiv 1 \pmod 4$. Similarly to the previous case we show that if $j > 4$ and e is not a Gold exponent, then $\phi_f(X,Y,Z)$ contain an absolute irreducible factor defined over $\mathbb{F}_q$. Therefore, $f(X)$ is not exceptional APN. At the end of Sections 3 and 4 we state all the cases left to proof in the exceptional APN conjecture with Gold degree.

Lemma 19. Let $f(X) = X^e + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) < e$ and e is a Gold or Kasami-Welch number. If ϕ_e contains an absolutely irreducible factor defined over $\mathbb{F}_q$ then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Let $\phi_f(X,Y,Z) = \phi_e(X,Y,Z) + \phi_h(X,Y,Z)$ and suppose $\phi_e(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Therefore, by corollary 5 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Theorem 50. Let $f(X) = X^{2^{n_1 n_2}+1} + h(X) \in \mathbb{F}_q[X]$, where $(n_1, n_2) = 1$, $n_1, n_2 > 1$. If $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$ then, $\phi_f(X,Y,Z)$ is absolutely irreducible.

Proof: Suppose $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$ and $(n_1, n_2) = 1$, $n_1, n_2 > 1$, then by corollary 11 $\phi_f(X,Y,Z)$ is absolutely irreducible. □

Theorem 51. Let $f(X) = X^e + h(X) \in \mathbb{F}_q[x]$ where $\deg(h) < e$ and e is Gold or Kasami-Welch number. If $T_\phi(X,Y,Z)$ contains a reduce irreducible factor $R(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$, with $(m(\phi_e), m(R)) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Suppose that $\phi_f(X,Y,Z)$ is irreducible, then by corollary 13 $\phi_f(X,Y,Z)$ is absolutely irreducible. Suppose $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z)$ is irreducible and $T_P(X,Y,Z)$ contains $R(X,Y,Z)$. Notice that $m(P) \mid m(\phi_f)$. Therefore, by corollary 13 $P(X,Y,Z)$ is absolutely irreducible. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

3.1. **Using the degree-gap to prove most of the Gold exception cases.** Notice that if do not contain any linear term $f(X)$ and $\phi_f(X,Y,Z)$ have the same degree-gap. Now consider the polynomial $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q$, where $h(X) = \sum_{i=1}^{m} a_i X^{2^{j_i}(2^{n_i}+1)}$ with $a_i \in \mathbb{F}_q$ and $\deg(h(X)) < 2^n + 1$. Then the maximum degree of $h(X)$ is $2^{n-2}(2+1)$. This implies that the degree-gap in these cases is $\geq 2^n + 1 - (2^{n-1} + 2^{n-2}) = 2^{n-2} + 1$.

Proposition 9. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q$, where $h(X) = \sum_{i=1}^{m} a_i X^{2^{j_i}(2^{n_i}+1)}$ with $a_i \in \mathbb{F}_q$ and $\deg(h(X)) < 2^n + 1$. If $\phi_f(X, Y, Z)$ factors over $\mathbb{F}_q$ and $(\phi_{2^n+1}, \phi_h) = 1$ then, $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Suppose that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$, where $P(X, Y, Z)$ and $Q(X, Y, Z)$ are non constant polynomials. Now writing its factor as sum of homogeneous term we obtain:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0).$$

where P_i, Q_i are zero or homogeneous of degree i, $s+t = 2^n - 2$. Without loss of generality assume that $s \geq t$ then, $t \leq 2^{n-1} - 1$. Now the degree-gap of Q is $\geq 2^{n-2} + 1$. Now we claim that Q is absolutely irreducible. If $\deg(Q_{t-1}) < DG(G)$ then, Q is absolutely irreducible (where $DG(G)$ is the degree-gap of G). By theorem 47 degree-gap $\geq 2^{n-2} + 1$ then, $\deg(Q_{t-1}) \leq 2^{n-1} - 1 - (2^{n-2} + 1) = 2^{n-2} - 2 < DG(G)$.Therefore G is absolutely irreducible. □

Corollary 22. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q$, where $h(X) = \sum_{i=1}^{m} a_i X^{2^{j_i}(2^{n_i}+1)}$ with $a_i \in \mathbb{F}_q$ and $\deg(h(X)) < 2^n + 1$ and let $\phi_d = (\phi_{2^n+1}, \phi_h)$. If $\frac{\phi_f}{\phi_d}$ factors over $\mathbb{F}_q$ then, $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Let $\rho_f = \frac{\phi_f}{\phi_d}$ Suppose that $\rho_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$, where $P(X, Y, Z)$ and $Q(X, Y, Z)$ are non constant polynomials. Now writing its factor as sum of homogeneous term we obtain:

$$\rho_f = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_i, Q_i are zero or homogeneous of degree i, $s + t = 2^n - 2^d$. Without loss of generality assume that $s \geq t$ then, $t \leq 2^{n-1} - 2^{d-1}$. Now the degree-gap of Q is $\geq 2^{n-2} + 1$. Now we claim that Q is absolutely irreducible. If $\deg(Q_{t-1}) < DG(G)$ then, Q is absolutely irreducible (where $DG(G)$ is the degree-gap of G). By theorem 47 degree-gap $\geq 2^{n-2} + 1$ then, $\deg(Q_{t-1}) \leq 2^{n-1} - 2^{d-1} - (2^{n-2} + 1) = 2^{n-2} - 2^{d-1} - 1 < DG(G)$.Therefore G is absolutely irreducible. □

Theorem 52. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q$, where $\deg(h(X)) < 2^n + 1$. If there exists a prime number p, $p > 3$ such that $p_1 | n$ and $(\phi_{2^p+1}, \phi_h) = 1$ then, $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Without loss of generality assume that $(\phi_{2^n+1}, \phi_h) = 1$ (in case when it is $\neq 1$, we just divide the polynomial by (ϕ_{2^n+1}, ϕ_h) and proceed in the same way). If $\phi_f(X, Y, Z)$ is reducible over $\mathbb{F}_q$ then, by lemma 9 $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can suppose $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$. Now ϕ_{2^n+1} contains reduced absolutely irreducible factors over $\mathbb{F}_{q^p}$. By lemma 4 we have that the tangent cone of ψ_ϕ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_{q^p}$. By Bartoli (generalization of Bartoli) we obtain that ψ_ϕ contain an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$. By lemma 13

$\phi_f(X,Y,Z)$ contain an absolutely irreducible factor H_1 over $\mathbb{F}_{q^p}$. By lemma 6 there exists an r, $c \in \mathbb{F}_q$ and an absolutely irreducible polynomial $H \in \mathbb{F}_{q^r}$ such that

$$\phi_f(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(H).$$

Since H_1 is absolutely irreducible we have that there exists $\beta \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ such that $H_1 \mid \beta(H)$. Notice that by lemma 8 $\beta(H)$ is absolutely irreducible. Therefore, $p \mid r$.
By lemma 6 the degree of $\sigma(H)$ is $\deg(\phi_f)/r$ for every $\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$. Then $\deg(\sigma(H)) < \deg(\phi_f)/4$. Notice that $4DG(\phi_f) \geq 4(2^{n-2}+1) = 2^n + 4 > \deg(\phi_f)$. Therefore, $DG(\phi_f) > \deg(\sigma(H))$ which implies by theorem 47 that $\sigma(H)$ is a form which is a contradiction with $(\phi_{2^n+1}, \phi_h) = 1$. □

Theorem 53. Let $f(X) = X^{2^p+1} + h(X) \in \mathbb{F}_q[x]$, where $\deg(h) < 2^p+1$, p prime number. If $DG(\phi_f) > \deg(\phi_{2^p+1})/p$ then, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Notice that $(\phi_{2^p+1}, \phi_h) = 1$. Suppose that $\phi_f = PQ$, where P is irreducible over $\mathbb{F}_q$. We are going to show that P is absolutely irreducible. By theorem 47 we know that $DG(P) \geq DG(\phi_f) > \deg(\phi_{2^p+1})/p$. By Kopparty lemma 6 there exists a positive integer r, absolutely irreducible polynomial $g(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ and $c \in \mathbb{F}_q$ such that

$$P = c \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(g(X,Y,Z)).$$

Notice that $P = P_s + \cdots + P_0$, P_s contains a reduced linear factor over $\mathbb{F}_{q^p}$ which implies by lemma 13 and theorem 42 that P have an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$. The factorization by Kopparty lemma gave the factorization into absolutely irreducible factors which implies the factor that lies in $\mathbb{F}_{q^p}$ also lies in $\mathbb{F}_{q^r}$ which only gave leave us with two options either P is absolutely irreducible or $p \mid r$). If $r > 1$ by theorem 47 each factor satisfy $\sigma(g(X,Y,Z))$ have degree $DG(\sigma(g(X,Y,Z))) > \deg(\phi_{2^p+1})/p > \deg(\sigma(g(X,Y,Z)))$. This implies that every factor of P are forms and therefore P is a form. This is a contradiction to the fact that $(\phi_{2^p+1}, \phi_h) = 1$. Therefore $r = 1$. Thus we can suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$.

Similarly by Kopparty lemma 6 there exists a positive integer r_1, absolutely irreducible polynomial $g_1(X,Y,Z) \in \mathbb{F}_{q^{r_1}}[X,Y,Z]$ and $c_1 \in \mathbb{F}_q$ such that

$$\phi_f(X,Y,Z) = c_1 \prod_{\sigma \in Gal(\mathbb{F}_{q^{r_1}}/\mathbb{F}_q)} \sigma(g_1(X,Y,Z)).$$

Notice that ϕ_{2^p+1} contains an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$ which implies that $\phi_f(X,Y,Z)$ have an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$ by lemma 13 and theorem 42. The factorization by Kopparty lemma gave the factorization into absolutely irreducible factors which implies the factor that lies in $\mathbb{F}_{q^p}$ also lies in $\mathbb{F}_{q^{r_1}}$ which only gave leave us with two options either P is absolutely irreducible or $p \mid r_1$). If $r_1 > 1$ by theorem 47 each factor satisfy $DG(\sigma(g_1(X,Y,Z))) > \deg(\phi_{2^p+1})/p = \deg(\sigma(g_1(X,Y,Z)))$. This implies that every factor of $\phi_f(X,Y,Z)$ are forms and therefore $\phi_f(X,Y,Z)$ is a form. This is a contradiction to the fact that $(\phi_{2^p+1}, \phi_h) = 1$. Therefore $r = 1$. Thus $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

But we can even improve further this result.

Theorem 54. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[x]$, where $\deg(h) < 2^n + 1$. Let p' be the highest prime that divide n and $(\phi_{2^{p'}+1}, \phi_f) = 1$. If $DG(\phi_f) > \deg(\phi_{2^n+1})/p'$ then, $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Suppose $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$. Notice that ϕ_{2^n+1} contains a reduced linear term over $\mathbb{F}_{q^{p'}}$, by applying the reverse to $\phi_f(X, Y, Z)$ we obtain that the tangent cone of ψ_ϕ (by lemma 4) contains a reduced absolutely irreducible factor defined over $\mathbb{F}_{q^{p'}}$. By theorem 42 ψ_ϕ contains an absolutely irreducible factor defined over $\mathbb{F}_{q^{p'}}$. This implies by lemma 13 that $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_{q^{p'}}$. Since $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$ by lemma 6 there exists a positive integer r, an absolutely irreducible polynomial $g(X, Y, Z) \in \mathbb{F}_{q^r}$ and $c \in \mathbb{F}_q$ such that

$$\phi_f(X, Y, Z) = c \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(g(X, Y, Z)).$$

If $r > 1$, and the fact that every $\sigma(g(X, Y, Z))$ is absolutely irreducible, we can conclude that $p' \mid r$ (since we know one of the absolutely irreducible factor of $\phi_f(X, Y, Z)$ lie over $\mathbb{F}_{q^{p'}}$). By theorem 47 $DG(\sigma(g(X, Y, Z))) \geq DG(\phi_f) > \deg(\phi_{2^n+1})/p$. This implies that every $\sigma(g(X, Y, Z))$ is a form and thus $\phi_f(X, Y, Z)$ is a form which is a contradiction. Therefore $r = 1$. Similarly if $\phi_f(X, Y, Z) = PQ$, where P is an irreducible polynomial over $\mathbb{F}_q$ that contain an irreducible factor of ϕ_{2^p+1}. Apply the same argument over P to conclude P is absolutely irreducible since P is not a form $(\phi_{2^{p'}+1}, \phi_f) = 1$ (implies this, otherwise is a contradiction with being relatively prime). □

3.2. **Completion of the Gold Degree Case with Even Degree-gap of the Exceptional APN Conjecture.** The following theorem finishes the Gold case when the second term is of odd degree.

Theorem 55. Let $f(x) = x^{2^{k_1}+1} + h(x) \in L[x]$, where $\deg(h) = 2^{k_2}+1$ and $\deg(h) < 2^{k_1}+1$. If $h(x) = \sum_{j=2}^{t} a_j x^{2^{m_j}(2^{k_j}+1)}$, then ϕ contains an absolutely irreducible factor and f is not an exceptional APN polynomial.

Proof: Suppose that $(k_1, k_2 \ldots, k_t) = 1$, then by Lemma 18 ϕ is absolutely irreducible. Suppose that $(k_1, k_2 \ldots, k_t) = q$, by Theorem 13, we can conclude that ϕ_{2^q+1} divides $\phi(x, y, z)$. Consider the factor of ϕ of degree $2^{k_1} - 2^q$, defined by:

$$H(x, y, z) := \frac{\phi(x, y, z)}{\phi_{2^q+1}(x, y, z)}. \tag{11}$$

Then writing (11) as the sum of homogeneous terms, $H = H_{b_1} + H_{b_2} + H_{b_3} + \cdots + H_{b_t}$, where $H_{b_1} = \phi_{2^{k_1}+1}/\phi_{2^q+1}$ and $H_{b_i} = a_i(x^{2^m_j}(2^{k_j}+1))$, for $i \in \{2, \ldots, t\}$. Therefore, $(H_b, H_a, H_{a-1}, \ldots, H_0) = 1$ and by Lemma 18 H is absolutely irreducible. □

Theorem 56. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^n + 1$, and $e = \deg(h) < d$. If $e \equiv 1 \pmod 4$, then $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Theorem 57. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^n + 1$, and $e = \deg(h) < d$. If e is odd, then $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

3.3. **Case when** $\deg(h) = 2^{n-j}e$**, where** $e \equiv 3 \pmod 4$**.** Let $f(x) = x^{2^n+1} + h(x)$, with $\deg(h) = 2^{n-j}e$, where $j \geq 2$ and $e \equiv 3 \pmod 4$. Then we have the following results

Lemma 20. $\nu_{(1,1,1)}(\phi_{(2^{n-j}e)}) = (2^{n-j} - 1)(3)$.

Proof: This follows directly from Equation 3 and Lemma 12. □

Lemma 21. Let $R(X, Y, Z)$ be a factor of ϕ_{2^n+1}, then $\deg(R) = \nu_{(1,1,1)}(R)$

Proof: By Equation 1 we have that

$$\phi_{2^n+1}(X, Y, Z) = \prod_{\alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2} (X + \alpha Y + (\alpha + 1)Z).$$

Notice that $\nu_{(1,1,1)}(X + \beta Y + (\beta + 1)Z) = 1$ for all $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_2$ and hence $\nu_{(1,1,1)}(\phi_{2^n+1}) = 2^n - 2$. Since $R(X, Y, Z) \mid \phi_{2^n+1}(X, Y, Z)$, then there exist a subset $A \subset \mathbb{F}_{2^n} - \mathbb{F}_2$ such that $R(X, Y, Z) = \prod_{\gamma \in A}(X + \gamma Y + (\gamma + 1)Z)$. Therefore, by lemma 1 we have that $\deg(R) = \nu_{(1,1,1)}(R)$. □

Lemma 22. Let $f(x) = x^{2^n+1} + h(x)$, with $\deg(h) = 2^{n-j}e$, where $j \geq 2$ and $e \equiv 3 \pmod 4$. Then, $\mathrm{DG}(\phi_f) \geq 2^{n-j} + 1$.

Proof: The maximum degree term of the form $2^{n-j}e$, with $2^n + 1 > 2^{n-j}e$ is given by $2^{n-j}(2^j - 1) = 2^n - 2^{n-j}$. Therefore, $\mathrm{DG}(\phi_f) \geq 2^n + 1 - (2^n - 2^{n-j}) = 2^{n-j} + 1$. □

Proposition 10. Let $f(X) = X^{2^n+1} + h(X)$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. Then $(\phi_{2^n+1}, \phi_h) = 1$. Moreover, $\phi_f(X, Y, Z)$ is not divisible by any homogeneous polynomial.

Notice that if $j = 2$, then we obtain that $e = 3$ and we obtain in some cases some exception of the Gold sum Case. For the rest of the article assume that $j \geq 4$.

Proposition 11. Let $f(X) = X^{2^n+1} + h(X)$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. Then $\phi_f(X, Y, Z)$ can factor up to 5 factors.

Proof: Assume that $\phi_f(X, Y, Z) = \prod_{i=1}^{6} R_i(X, Y, Z))$ is the product of 6 factors. Notice that by lemma 22 and lemma 20 $3(DG(\phi_f)) \geq 3(2^{n-j} + 1) > 3(2^{n-j} - 1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. By theorem 47 and lemma 22 $\mathrm{DG}(R_i) \geq \mathrm{DG}(\phi_f) \geq 2^{n-j} + 1$. By proposition 10 then we can conclude that $\deg(R_i) \geq \mathrm{DG}(R_i) \geq 2^{n-j} + 1$. Now consider $P(X, Y, Z) = \prod_{i=1}^{3} R_i(X, Y, Z)$ and $Q(X, Y, Z) = \prod_{i=4}^{6} R_i(X, Y, Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

Since ϕ_{2^k+1} is equal to the product of different linear factors, $(P_s, Q_t) = 1$. Then, equating the terms of degree $s + t - 1$ gives $P_s Q_{t-1} + Ps - 1Q_t = 0$. Hence, we have $P_s \mid P_{s-1}Q_t$ and this implies that $P_s \mid P_{s-1}$. Therefore, $P_{s-1} = 0$ and $Q_{t-1} = 0$ as $P_s \neq 0$.

Similarly, equating the terms of degree $> 2^{n-j}e - 3$ we get:

$$P_{s-2} = Q_{t-2} = 0$$
$$\dots$$
$$P_{s-d+1} = Q_{t-d+1} = 0$$

and

$$\phi_{2^{n-j}e}(X, Y, Z) = P_s Q_{t-d} + P_{s-d} Q_t.$$

Notice that $\nu_{(1,1,1)}(P_s) = \deg(P_s) \geq 3\mathrm{DG}(\phi_f) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ and $\nu_{(1,1,1)}(Q_t) = \deg(Q_t) \geq 3\mathrm{DG}(\phi_f) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. By lemma 1 we get $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq \min(P_s Q_{t-d}, P_{s-d} Q_t) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $\phi_f(X, Y, Z)$ can not have more than 5 factors. □

Proposition 12. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If n is a prime greater than 6, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor define over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$. By factorization in Equation 1 ϕ_{2^n+1} contains an irreducible factor $P(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ with $m(P) = n$. By Corollary 7 $m(\phi_f) \mid n$ but n prime implies that either $m(\phi_f) = 1$ or $m(\phi_f) = n$. If $m(\phi_f) = n$, then $\phi_f(X, Y, Z)$ factor into n factors which is a contradiction of proposition 11. Therefore, $m(\phi_f) = 1$ and $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$, where $P(X, Y, Z)$ is irreducible and $P(X, Y, Z), Q(X, Y, Z)$ are non constant polynomials. Since $P(X, Y, Z)$ is non constant polynomial, then $t_P(X, Y, Z)$ contains an irreducible factor $P_1(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ with $m(P_1) = n$. By the first part of the proof $P_1(X, Y, Z)$ is absolutely irreducible. Therefore, $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Proposition 13. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If n is odd, $n > 6$ and n is not a prime power, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes p_1, p_2 $(p_1 \neq p_2)$ such that $p_1 p_2 \mid n$, then by Theorem 50 $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that $\phi_f(X, Y, Z)$ factors over $\mathbb{F}_q$ and let p_1, p_2 be prime numbers such that $p_1 p_2 \mid n$ with $p_1 \neq p_2$. Let

$$\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)R(X, Y, Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains an irreducible factor of $\phi_{2^{p_1}+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^{p_2}+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^{p_2}+1}(X,Y,Z)) = 1$. Now we can assume without loss of generality that $t_Q(X,Y,Z)$ contains an irreducible factor of $\phi_{2^{p_2}+1}(X,Y,Z)$. Now by Corollary 7 we have that $m(P) \mid p_1$ and $m(Q) \mid p_2$. If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Assume that $m(P) = p_1$ and $m(Q) = p_2$, then $\phi_f(X,Y,Z)$ have a factorization with at least $p_1 + p_2 > 5$ factors which is a contradiction with proposition 11. Therefore, either $m(P) = 1$ or $m(Q) = 1$ and thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Proposition 14. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If n is a power of 5, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X,Y,Z)$ defined over $\mathbb{F}_q$ with $m(R) = 5$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = 5$ or $m(\phi_f) = 1$. If $m(\phi_f) = 5$, i.e. $\phi_f(X,Y,Z) = \prod_{i=1}^{5} R_i(X,Y,Z)$, where $R_i(X,Y,Z) \in \mathbb{F}_{q^5}[X,Y,Z]$. Then by theorem 41 we have that $\deg(R_i) = (2^n-2)/5$ for $i = 1, \dots, 5$. Notice that $\phi_{2^n+1}(X,Y,Z) = \prod_{i=1}^{5} t_{R_i}(X,Y,Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_{R_i}) = \deg(t_{R_i}) = (2^n-2)/5$.

Notice that $5\nu_{1,1,1}(\phi_{2^{n-j}e} = 15(2^{n-j}-1) \leq 15(2^{n-4}-1) = 2^n - 2^{n-4} - 15 < 2^n - 2$. Therefore, $\nu_{(1,1,1)}(t_{R_i}) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. Now define $P(X,Y,Z) = R_1(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=2}^{5} R_i(X,Y,Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-d}), \nu_{(1,1,1)}(P_{s-d} Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$, $P(X,Y,Z)$ and $Q(X,Y,Z)$ are non constant polynomials and $P(X,Y,Z)$ is irreducible. Since $P(X,Y,Z)$ is non constant then there exists an irreducible polynomial $W(X,Y,Z)$ such that $W(X,Y,Z) \mid t_P(X,Y,Z)$. By Equation 1 $m(W) = 5^k$ where $k \geq 1$ and by Corollary 7 we have $m(P) \mid m(W)$. Therefore, $m(P)$ is either $m(P) = 1$ or $m(P) = 5^{k_1}$, where $1 \leq k_1 \leq k$. If $m(P) = 5^{k_1}$, then by theorem 41 $P(X,Y,Z)$ factors into 5^{k_1} factors and we obtain that $\phi_f(X,y,Z)$ has a factorization with at least $5^{k_1} + 1$ factors which is a contradiction with

Proposition 11. Therefore, $m(P) = 1$ and thus, $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

□

Proposition 15. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$ and $j \geq 4$. If n is a power of 3, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X, Y, Z)$ defined over $\mathbb{F}_q$ with $m(R) = 3$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = 3$ or $m(\phi_f) = 1$. If $m(\phi_f) = 3$, i.e. $\phi_f(X, Y, Z) = \prod_{i=1}^{3} R_i(X, Y, Z)$, where $R_i(X, Y, Z) \in \mathbb{F}_{q^3}[X, Y, Z]$. Then by theorem 41 we have that $\deg(R_i) = (2^n - 2)/3$ for $i = 1, 2, 3$. Notice that $\phi_{2^n+1}(X, Y, Z) = \prod_{i=1}^{3} t_{R_i}(X, Y, Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_{R_i}) = \deg(t_{R_i}) = (2^n - 2)/3$.

Notice that $3\nu_{1,1,1}(\phi_{2^{n-j}e}) = 9(2^{n-j} - 1) \leq 9(2^{n-4} - 1) = 2^{n-1} + 2^{n-4} - 9 < 2^n - 2$. Therefore, $\nu_{(1,1,1)}(t_{R_i}) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. Now define $P(X, Y, Z) = R_1(X, Y, Z)$ and $Q(X, Y, Z) = \prod_{i=2}^{3} R_i(X, Y, Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-d}), \nu_{(1,1,1)}(P_{s-d} Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)\ R(X, Y, Z)$, where $P(X, Y, Z)$, $Q(X, Y, Z)$, $R(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$, $P(X, Y, Z)$ and $Q(X, Y, Z)$ are non constant irreducible polynomials. Since $P(X, Y, Z)$ is non constant then there exists an irreducible polynomial $W(X, Y, Z)$ such that $W(X, Y, Z) \mid t_P(X, Y, Z)$. By Equation 1 $m(W) = 3^k$ where $k \geq 1$ and by Corollary 7 we have $m(P) \mid m(W)$. Therefore, $m(P)$ is either $m(P) = 1$ or $m(P) = 3^{k_1}$, where $1 \leq k_1 \leq k$. Similarly, there exists an irreducible polynomial $V(X, Y, Z)$ such that $V(X, Y, Z) \mid t_Q(X, Y, Z)$. By equation 1, $m(V) = 3^a$, where $a \geq 1$ and by Corollary7 we have $m(Q) \mid m(V)$. Therefore, $m(Q) = 1$ or $m(Q) = 3^{a_1}$, where $1 \leq a_1 \leq a$. If either $m(P) = 1$ or $m(Q) = 1$, then you have an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $m(P), m(Q) > 1$, then by Theorem 41 $P(X, Y, Z)$ factors into at least 3 factors. Similarly, $Q(X, Y, Z)$ factors into at least 3 factors. Therefore, $\phi(X, Y, Z)$ have a factorization into at least 6 factors which is a contradiction with Proposition 11. □

Proposition 16. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$ and $j \geq 4$. If $n = p^m$, where p is a prime $p > 5$, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X,Y,Z)$ defined over $\mathbb{F}_q$ with $m(R) = p$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = p$ or $m(\phi_f) = 1$. If $m(\phi_f) = p$, then by Theorem 41 $\phi_f(X,Y,Z)$ factors into p absolutely irreducible factors. This is a contradiction with Proposition 11. Therefore, $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z), \in \mathbb{F}_q[X,Y,Z]$, $P(X,Y,Z)$ and $Q(X,Y,Z)$ are non constant polynomials and $P(X,Y,Z)$ is irreducible. Since $P(X,Y,Z)$ is non constant then there exists an irreducible polynomial $W(X,Y,Z)$ such that $W(X,Y,Z) \mid t_P(X,Y,Z)$. By Equation 1 $m(W) = p^k$ where $k \geq 1$ and by Corollary 7 we have $m(P) \mid m(W)$. Therefore, $m(P)$ is either $m(P) = 1$ or $m(P) = p^{k_1}$, where $1 \leq k_1 \leq k$. If $m(P) = p^{k_1}$, then by theorem 41 $P(X,Y,Z)$ factors into p^{k_1} factors and we obtain that $\phi_f(X,y,Z)$ has a factorization with at least $p^{k_1}+1$ factors which is a contradiction with Proposition 11. Therefore, $m(P) = 1$ and thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

□

Proposition 17. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If n is a power of 2, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X,Y,Z)$ defined over $\mathbb{F}_q$ with $m(R) = 2$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = 2$ or $m(\phi_f) = 1$. If $m(\phi_f) = 2$, i.e. $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z)Q(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$. Then by theorem 41 we have that $\deg(P) = \deg(Q) = 2^{n-1}-1$. Notice that $\phi_{2^n+1}(X,Y,Z) = t_P(X,Y,Z)t_Q(X,Y,Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) = \deg(t_P) = 2^{n-1}-1$.

Notice that $2\nu_{1,1,1}(\phi_{2^{n-j}e} = 6(2^{n-j}-1) \leq 9(2^{n-4}-1) = 2^{n-1}+2^{n-4}-9 < 2^n-2$. Therefore, $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t = 2^k-2$. Then

$$\phi_{2^n+1} = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-d}), \nu_{(1,1,1)}(P_{s-d}Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ with factorization

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z), \tag{12}$$

where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is irreducible non constant polynomial for $i = 1,\dots,k$. Notice that for each $t_{R_i}(X,Y,Z)$, there exists an irreducible polynomial $W_i(X,Y,Z)$ such that $m(W_i) = 2^{k_i}$, where $k_i \geq 1$ for each $i = 1,\dots,k$. By Corollary 7 we have that $m(R_i) \mid m(W_i)$ for each $i = 1,\dots,k$. Therefore, $m(R_i) = 2^{a_i}$, where $0 \leq a_i \leq k_i$ for every $i = 1,\dots,k$. If there exists a i_0 such that $m(R_{i_0}) = 1$, then we have an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $m(R_i) = 2^{a_i}$, where $1 \leq a_i \leq k_i$ for each $i = 1,\dots,k$. Now for every $i = 1,\dots,k$ by Theorem 41 there exist an absolutely irreducible factor $h_i(X,Y,Z) \in \mathbb{F}_{q^{2^{a_i}}}[X,Y,Z]$, $c_i \in \mathbb{F}_q$ such that

$$R_i(X,Y,Z) = c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)), \tag{13}$$

Combining Equations 12 and 13 we obtain the following equation:

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)). \tag{14}$$

Notice that $|Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)| = 2^{a_i}$ and that for every $\alpha,\beta \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)$ we have that $\deg(\alpha(h_i)) = \deg(\beta(h_i))$. Let γ_i be a generator of $Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)$, define $g_i(X,Y,Z) = \prod_{r=1}^{2^{a_1-1}} \gamma_i^r(h_i(X,Y,Z))$ and $f_i(X,Y,Z) = \prod_{r=2^{a_i-1}+1}^{2^{a_i}} \gamma_i^r(h_i(X,Y,Z))$. Then using this definitions we can rewrite Equation 14 as

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i g_i(X,Y,Z) f_i(X,Y,Z)$$

Notice that $\deg(f_i) = \deg(g_i)$. Define $P(X,Y,Z) = \prod_{i=1}^{k} g_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=1}^{k} c_i f_i(X,Y,Z)$, then $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, with $\deg(P) = \deg(Q) = 2^{n-1} - 1$. Notice that $\phi_{2^n+1}(X,Y,Z) = t_P(X,Y,Z)t_Q(X,Y,Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) = \deg(t_P) = 2^{n-1} - 1$.

Notice that $2\nu_{1,1,1}(\phi_{2^{n-j}e} = 6(2^{n-j}-1) \leq 9(2^{n-4}-1) = 2^{n-1}+2^{n-4}-9 < 2^n-2$. Therefore, $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)} > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-d}), \nu_{(1,1,1)}(P_{s-d}Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, there exist an $i_0 \in \{1, \ldots, k\}$ such that $m(R_{i_0}) = 1$. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

Proposition 18. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If n is even, and $p \mid n$ is a prime $p > 3$, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes $2, p$ ($p \neq 2$) such that $2p \mid n$, then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ and let

$$\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)R(X,Y,Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains $\phi_{2^2+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^p+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^p+1}(X,Y,Z)) = 1$. Without loss of generality we can assume that $t_Q(X,Y,Z)$ contains an irreducible factor of ϕ_{2^p+1}. By Corollary 7 we have that $m(P) \mid 2$ and $m(Q) \mid p$, then we have that either $m(P) = 1$ (respectively $m(Q) = 1$) or $m(P) = 2$ (respectively $m(Q) = p$). If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. We can assume that $m(P) = 2$ and $m(Q) = p$, then $\phi_f(X,Y,Z)$ have a factorization with at least $2 + p > 6$ factors which is a contradiction of Proposition 11.

□

Proposition 19. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If $6 \mid n$, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

If n is divisible by any prime p different than 2 and 3, then by Proposition 18 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that n is only divisible by 2 and 3, i.e. $n = 2^{n_1}3^{n_2}$, where $n_1, n_2 \geq 1$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes $2, 3$ such that $6 \mid n$, then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ and let

$$\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)R(X,Y,Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains $\phi_{2^2+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^3+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^3+1}(X,Y,Z)) = 1$. Without loss of generality we can assume that $t_Q(X,Y,Z)$ contains an irreducible factor of ϕ_{2^3+1}.By Corollary 7 we have that $m(P) \mid 2$ and $m(Q) \mid 3$, then we have that either $m(P) = 1$ (respectively $m(Q) = 1$) or $m(P) = 2$ (respectively $m(Q) = 3$). If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. We can assume that $m(P) = 2$ and $m(Q) = 3$. If $R(X,Y,Z)$ is a non constant polynomial then we get a contradiction with Proposition 11 (2 factors from P, 3 factors from Q and 1 factor from R). Therefore, we can assume that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$.

Suppose that $\deg(P) \geq \deg(Q)$, then $\deg(P) \geq 2^{n-1}-1$. Since $m(P) = 2$, then there exists $R_1(X,Y,Z), R_2(X,Y,Z) \in \mathbb{F}_{q^2}(X,Y,Z)$ such that $P(X,Y,Z) = R_1(X,Y,Z)R_2(X,Y,Z)$, with $\deg(R_1) = \deg(R_2)$. Notice that $\deg(R_1) \geq 2^{n-2} - 1$. By Lemma 21 we have that $\nu_{(1,1,1)}(t_{R_1}) = \nu_{(1,1,1)}(t_{R_2}) \geq 2^{n-2} - 1 > 4(2^{n-4} - 1) > 3(2^{n-j} - 1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$.

Define $A(X,Y,Z) = R_1(X,Y,Z)$ and $B = R_2(X,Y,Z)Q(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write $A(X,Y,Z)$ and $B(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = A_s B_t,$$

and

$$\phi_{2^{n-j}e} = A_s B_{t-d} + A_{s-d} B_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(A_s B_{t-d}), \nu_{(1,1,1)}(A_{s-d} B_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$.

Suppose that $\deg(Q) \geq 2^{n-1}-1$. Since $m(Q) = 3$, then there exists $R_1(X,Y,Z), R_2(X,Y,Z)$, $R_3(X,Y,Z) \in \mathbb{F}_{q^3}[X,Y,Z]$ such that $Q(X,Y,Z) = \prod_{i=1}^{3} R_i(X,Y,Z)$ and $\deg(R_1) = \deg(R_2) = \deg(R_3)$. Notice that $\deg(R_i) > 2^{n-3} - 1$ for $i = 1,2,3$. Similarly, since $m(P) = 2$, then there exists $W_1(X,Y,Z), W_2(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$ such that $P(X,Y,Z) = W_1(X,Y,Z)W_2(X,Y,Z)$ and $\deg(W_1) = \deg(W_2)$. By Theorem 47 and Lemma 22 $\mathrm{DG}(W_i) \geq \mathrm{DG}(\phi_f) \geq 2^{n-j} + 1$. By Proposition 10 $\deg(W_i) \geq \mathrm{DG}(W_i) \geq 2^{n-j} + 1$. Define $A(X,Y,Z) = R_1(X,Y,Z)W_1(X,Y,Z)$ and $B(X,Y,Z) = R_2(X,Y,Z)R_3(X,Y,Z)W_2(X,Y,Z)$. We write $A(X,Y,Z)$ and $B(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = A_s B_t,$$

and

$$\phi_{2^{n-j}e} = A_s B_{t-d} + A_{s-d} B_t.$$

By Lemma 21 and Lemma 1 we have that $\nu_{(1,1,1)}(A_s) = \nu_{(1,1,1)}(t_{R_1}) + \nu_{(1,1,1)}(t_{W_1}) \geq 2^{n-3} + 2^{n-j} > 3(2^{n-j}-1) = \nu(1,1,1)(\phi_{2^{n-j}e})$. Clearly, $\deg(B) > \deg(A)$. Therefore, by Lemma 21 $\nu_{(1,1,1)}(B_t) > \nu_{(1,1,1)}(A_s) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$.

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(A_sB_{t-d}), \nu_{(1,1,1)}(A_{s-d}B_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$.

□

Theorem 58. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If $j \geq 4$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Lemma 23. Let $f(X) = x^d + h(X)$, where $d = 2^n + 1$, $e = \deg(h)$ $\nu_{(1,1,1)}(\phi_e) < 2^{n-2} - 1$. Then every irreducible factor $R(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ of $\phi_f(X,Y,Z)$ is either absolutely irreducible or $\nu_{(1,1,1)}(t_R) < 2^{n-2}$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Let $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ non constant polynomials and $P(X,Y,Z)$ be irreducible. If $m(P) = 1$, then $P(X,Y,Z)$ is absolutely irreducible. Therefore, $m(P) > 1$. It is enough to show that for every $m(P) = p$, p prime the condition is satisfied. Assume that $2^{n-2} - 1 < \nu_{(1,1,1)}(t_P) < 2^{n-1} - 1$. We write $P(X,Y,Z)$ and $Q(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = P_sQ_t,$$

and

$$\phi_e = P_sQ_{t-a} + P_{s-a}Q_t.$$

Since $\nu_{(1,1,1)}(t_P) < 2^{n-1} - 1$, then $\nu_{(1,1,1)}(t_Q) = \nu_{(1,1,1)}(\phi_d) - \nu_{(1,1,1)}(t_P) \geq 2^{n-1} - 1$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2} - 1 \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}),\ \nu_{(1,1,1)}(P_{s-a}Q_t)) > 2^{n-2} - 1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \geq 2^{n-1} - 1$. Assume that $\nu_{(1,1,1)}(t_R) \geq 2^{n-1} - 1$.

If $p = 2$, then we have

$$P(X,Y,Z) = V_1(X,Y,Z)V_2(X,Y,Z)$$

where $V_1(X,Y,Z), V_2(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$ are conjugates. Define $A(X,Y,Z) = V_1(X,Y,Z)$ and $B(X,Y,Z) = V_2(X,Y,Z)Q(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = A_sB_t,$$

and

$$\phi_e = A_sB_{t-a} + A_{s-a}B_t.$$

Since V_1, V_2 are conjugates then $\deg(V_1) = \deg(V_2)$, thus by Lemma 21 $\nu_{(1,1,1)}(t_{V_1}) = \nu_{(1,1,1)}(t_{V_2}) \geq 2^{n-2}$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2}-1 \geq \min(\nu_{(1,1,1)}(A_sB_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) > 2^{n-2}-1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \leq 2^{n-2}-1$.

If $p > 3$, then we have

$$P(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^p}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$, thus by Lemma 21 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1}-1)/p$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$P(X,Y,Z) = \prod_{i=1}^{p} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = Q(X,Y,Z)\prod_{i=1}^{(p-1/2)} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = \prod_{i=(p-1)/2+1}^{p} \gamma^i(H(X,Y,Z))$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write $A(X,Y,Z)$ and $B(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t = d$. Then

$$\phi_d = A_sB_t,$$

and

$$\phi_e = A_sB_{t-a} + A_{s-a}B_t.$$

Notice that $\nu_{(1,1,1)}(B_t) \geq (2^{n-1}-1)/2 \geq 2^{n-2}$. Computing $\nu_{(1,1,1)}(A_s)$, we obtain $\nu_{(1,1,1)}(A_s) = \frac{p-1}{2p}(2^n - 2 - \nu_{(1,1,1)}(t_Q)) + \nu_{(1,1,1)}(t_Q) = \frac{(p-1)(2^{n-1}-1)}{p} + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) \geq \frac{4}{5}(2^{n-1}-1) + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) = \frac{2^{n+1}-4}{5} + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) \geq 2^{n-2}$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2}-1 \geq \min(\nu_{(1,1,1)}(A_sB_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) \geq 2^{n-2} > 2^{n-2}-1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \leq 2^{n-2}-1$.

If $p = 3$, then we have

$$P(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^3}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$ thus by Lemma 21 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1}-1)/3$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$P(X,Y,Z) = \prod_{i=1}^{3} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = \prod_{i=1}^{2} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = Q(X,Y,Z)H(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_e = A_s B_{t-a} + A_{s-a} B_t.$$

Notice that $\nu_{(1,1,1)}(A_s) \geq \frac{2}{3}(2^{n-1}-1) = (\frac{2^n-2}{3}) > 2^{n-2}-1$. Let $c = \nu_{(1,1,1)}(t_Q)$, then $\nu_{(1,1,1)}(B_t) = c + \frac{2^n-2-c}{3} = \frac{2^n-2}{3} + \frac{2c}{3} > (2^{n-4}-1)(3) \geq (2^{n-j}-1)(3)$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2}-1 \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) \geq 2^{n-2} > 2^{n-2}-1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \leq 2^{n-2}-1$. □

Theorem 59. Let $f(X) = X^d + h(X)$, where $d = 2^n+1$, $\deg(h) = e$ and $\nu_{(1,1,1)}(\phi_e) < 2^{n-j}-1$. Then every irreducible factor $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Assume that $\phi_f(X,Y,Z)$ is irreducible, then by lemma 23 $\phi_f(X,Y,Z)$ is absolutely irreducible. Suppose that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z)$$

where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is a non-constant irreducible polynomial for $i \in \{1,\ldots,k\}$. If one of the $R_i(X,Y,Z)$ is absolutely irreducible then we are done, so we can assume without loss of generality that every $R_i(X,Y,Z)$ is not absolutely irreducible for $i \in \{1,\ldots,k\}$. By Lemma 23 we have $\nu_{(1,1,1)}(t_{R_i}) < 2^{n-2}$ for every $i \in \{1,\ldots,k\}$. Define $P(X,Y,Z) = \prod_{i=1}^{w} R_i(X,Y,Z)$, where w is the minimum number such that $\nu_{(1,1,1)}(t_P) > 2^{n-2}$ (i.e. $\nu_{(1,1,1)}(\prod_{i=1}^{w-1}(t_{R_i})) < 2^{n-2}$). Define $Q(X,Y,Z) = \prod_{i=w+1}^{k} R_i(X,Y,Z)$. We write $P(X,Y,Z)$ and $Q(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_s Q_t,$$

and

$$\phi_e = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $\nu_{(1,1,1)}(P_s) < 2 * (2^{n-2}) = 2^{n-1}$ and $\nu_{(1,1,1)}(Q_t) = 2^n - 2 - \nu_{(1,1,1)}(P_s) \leq 2^n - 2 - (2^{n-1}-1) = 2^{n-1}-1 > 2^{n-2}$. Therefore, $\nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t) < 2^{n-2}$ which is a contradiction. Thus, there exists a $i_0 \in \{1,\ldots,k\}$ such that $R_{i_0}(X,Y,Z)$ is absolutely irreducible.

□

The following theorem extend Proposition 11 for any $j > 2$.

Theorem 60. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, $e \equiv 3 \pmod 4$, and $j \geq 2$. If $\phi_f(X,Y,Z)$ is not absolutely irreducible, then $\phi_f(X,Y,Z)$ has at most 5 factors.

Proof: Assume that $\phi_f(X,Y,Z) = \prod_{i=1}^{6} R_i(X,Y,Z))$ is the product of 6 factors. Notice that by lemma 22 and lemma 20 $3(DG(\phi_f)) \geq 3(2^{n-j}+1) > 3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. By theorem 47 and lemma 22 $\mathrm{DG}(R_i) \geq \mathrm{DG}(\phi_f) \geq 2^{n-j}+1$. By proposition 10 then we can conclude that $\deg(R_i) \geq \mathrm{DG}(R_i) \geq 2^{n-j}+1$. Now consider $P(X,Y,Z) = \prod_{i=1}^{3} R_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=4}^{6} R_i(X,Y,Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

Since ϕ_{2^k+1} is equal to the product of different linear factors, $(P_s, Q_t) = 1$. Then, equating the terms of degree $s+t-1$ gives $P_s Q_{t-1} + Ps - 1Q_t = 0$. Hence, we have $P_s \mid P_{s-1}Q_t$ and this implies that $P_s \mid P_{s-1}$. Therefore, $P_{s-1} = 0$ and $Q_{t-1} = 0$ as $P_s \neq 0$.

Similarly, equating the terms of degree $> 2^{n-j}e - 3$ we get:

$$P_{s-2} = Q_{t-2} = 0$$

$$\cdots$$

$$P_{s-d+1} = Q_{t-d+1} = 0$$

and

$$\phi_{2^{n-j}e}(X,Y,Z) = P_s Q_{t-d} + P_{s-d} Q_t.$$

Notice that $\nu_{(1,1,1)}(P_s) = \deg(P_s) \geq 3\mathrm{DG}(\phi_f) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ and $\nu_{(1,1,1)}(Q_t) = \deg(Q_t) \geq 3\mathrm{DG}(\phi_f) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. By lemma 1 we get $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq \min(P_s Q_{t-d}, P_{s-d} Q_t) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $\phi_f(X,Y,Z)$ can not have more than 5 factors. □

Theorem 61. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-3}e$, $e \equiv 3 \pmod 4$. If is not a power of 3 or $n = 2^{n_1}3^{n_2}$, with $n_1, n_2 \geq 1$ then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

We have two possible cases when n is a prime power and when n is not a prime power. Let assume that $n = p^m$ for $p \neq 3$ prime. We have two possible cases $n = 2^k$, where $k \geq 1$. Notice that $\phi_5(X,Y,Z) \mid \phi_{2^n+1}$. Suppose that $\phi_f(X,Y,Z)$ is irreducible, then by Corollary 7 $m(\phi_f) \mid m(\phi_5)$ i.e. $m(\phi_f) \mid 2$. Therefore, either $m(\phi_f) = 1$ or $m(\phi_f) = 2$. If $m(\phi_f) = 1$, then $\phi_f(X,Y,Z)$ is absolutely irreducible. Suppose $m(\phi_f) = 2$, then there exists an absolutely irreducible polynomial $H(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ such that

$$\phi_f(X,Y,Z) = \prod_{\gamma \in Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)} \gamma(H(X,Y,Z)).$$

Now we have $\deg(H) = \deg(\alpha(H))$, $\alpha \in Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$, α not the identity. Let $P(X,Y,Z) = H(X,Y,Z)$ and $Q(X,Y,Z) = \alpha(H(X,Y,Z))$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

and

$$\phi_{2^{n-3}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 21 we have $\nu_{(1,1,1)}(P_s) = \nu_{(1,1,1)}(Q_t) = (2^n - 2)/2 = 2^{n-1} - 1$. Computing $\nu_{(1,1,1)}(\phi_{2^{n-3}e}) = (2^{n-3} - 1)(3) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a})\nu_{(1,1,1)}(P_{s-a}Q_t)) \geq 2^{n-1} - 1 > (2^{n-3} - 1)(3)$ which is a contradiction. Suppose that $\phi_f(X,Y,Z) = \prod_{i=1}^k R_i(X,Y,Z)$, where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is an irreducible non-constant polynomial for $i = 1,\ldots,k$. Notice that since n is a power of two, then we have by Corollary 7, $m(R_i) = 2^{b_i}$ for $b_i \in \{1,\ldots,n\}$, $i = 1,\ldots,k$ and $b_i \geq 0$. If for some $i_0 \in \{1,\ldots,k\}$ we have $m(R_{i_0}) = 1$, then $R_{i_0}(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $m(R_i) > 1$ for every $i \in \{1,\ldots,k\}$. Then there exists polynomials $H_i(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$, $i = 1,\ldots,k$ such that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} \prod_{\gamma \in Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)} \gamma(H_i(X,Y,Z)).$$

Now we have $\deg(H_i) = \deg(\alpha(H_i))$, $\alpha \in Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$, α not the identity and $i = 1,2,\ldots,k$. Let $P(X,Y,Z) = \prod_{i=1}^k H_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=1}^k \alpha(H_i(X,Y,Z))$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

and

$$\phi_{2^{n-3}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 21 we have $\nu_{(1,1,1)}(P_s) = \nu_{(1,1,1)}(Q_t) = (2^n - 2)/2 = 2^{n-1} - 1$. Computing $\nu_{(1,1,1)}(\phi_{2^{n-3}e}) = (2^{n-3} - 1)(3) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a})\nu_{(1,1,1)}(P_{s-a}Q_t)) \geq 2^{n-1} - 1 > (2^{n-3} - 1)(3)$ which is a contradiction.

Suppose that $n = p^m$, where $p > 3$ is a prime number. Assume that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$, then there exist an absolutely irreducible polynomial $H(X,Y,Z) \in \mathbb{F}_{q^p}[X,Y,Z]$ such that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{p} \gamma^i(H(X,Y,Z)),$$

where $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ is a generator of $Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$. Notice that $\deg(\alpha(H)) = \deg(\beta(H))$ for every $\alpha, \beta \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$. Define $P(X,Y,Z) = \prod_{i=1}^{(p-1)/2} \gamma^i(H(X,Y,Z))$ and $Q(X,Y,Z) = \prod_{i=(p-1)/2+1}^{p} \gamma^i(H(X,Y,Z))$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

and

$$\phi_{2^{n-3}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 21 we have $\nu_{(1,1,1)}(P_s) = \frac{2^n-2}{p}(\frac{p-1}{2}) = (\frac{(p-1)}{p})(2^{n-1}-1) \geq \frac{4}{5}(2^{n-1}-1) = \frac{2^{n+1}-4}{5}$ and $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s)$. Computing $\nu_{(1,1,1)}(\phi_{2^{n-3}e}) = (2^{n-3}-1)(3) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a}),$ $\nu_{(1,1,1)}(P_{s-a} Q_t)) \geq \frac{2^{n+1}-4}{5} > (2^{n-3}-1)(3)$ which is a contradiction.

Suppose that $\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z)$, where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is an irreducible non-constant polynomial for $i = 1, \ldots, k$. Notice that since n is a power a prime power, then by Corollary 7, $m(R_i) = p^{b_i}$ for $b_i \in \{1, \ldots, n\}$, $i = 1, \ldots, k$ and $b_i \geq 0$. If for some $i_0 \in \{1, \ldots, k\}$ we have $m(R_{i_0}) = 1$, then $R_{i_0}(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $m(R_i) > 1$ for every $i \in \{1, \ldots, k\}$. Then there exists polynomials $H_i(X,Y,Z) \in \mathbb{F}_{q^p}[X,Y,Z]$, $i = 1, \ldots, k$ such that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} \prod_{\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)} \gamma(H_i(X,Y,Z)). \tag{15}$$

Now we rewrite Equation 15 as follows. Let $\sigma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Define $W_i(X,Y,Z) = \prod_{b=1}^{k} \gamma^i(H_b(X,Y,Z))$ for $i = 1, 2, \ldots, p$. Then we have $\deg(W_i) = \deg(W_1)$, for $i = 1, 2, \ldots, p$. Let $P(X,Y,Z) = \prod_{i=1}^{(p-1)/2} H_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=(p-1)/2+1}^{p} \alpha(H_i(X,Y,Z))$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

and

$$\phi_{2^{n-3}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 21 we have $\nu_{(1,1,1)}(P_s) = \frac{2^n-2}{p}(\frac{p-1}{2}) = (\frac{(p-1)}{p})(2^{n-1}-1) \geq \frac{4}{5}(2^{n-1}-1) = \frac{2^{n+1}-4}{5}$ and $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s)$. Computing $\nu_{(1,1,1)}(\phi_{2^{n-3}e}) = (2^{n-3}-1)(3) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a}),$ $\nu_{(1,1,1)}(P_{s-a} Q_t)) \geq \frac{2^{n+1}-4}{5} > (2^{n-3}-1)(3)$ which is a contradiction.

Suppose that n is not a prime power and $n \neq 2^{k_1}3^{k_2}$ for some $k_1, k_2 \geq 1$. Suppose that $\phi_f(X,Y,Z)$ is irreducible then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible. Suppose that $\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z)$, where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is an irreducible non-constant polynomial for $i = 1, \ldots, k$. If there is an $i_0 \in \{1, \ldots, k\}$ such that $m(R_{i_0}) = 1$, then we have an absolutely irreducible factor defined over $\mathbb{F}_q$. Since n is not a prime power there exists two primes p_1, p_2, $p_1 \neq p_2$ such that $p_1p_2 \mid n$ and $p_1 + p_2 > 5$. Then there exists two different factors $R_{i_1}(X,Y,Z), R_{i_2}(X,Y,Z)$, $i_1, i_2 \in \{1,\dots,k\}$ such that $m(R_{i_1}) = p_1^{b_1}$, $m(R_{i_2}) = p_2^{b_2}$, with $b_1, b_2 \geq 1$. Then there exist polynomials $H_1(X,Y,Z) \in \mathbb{F}_{q^{p_1}}[X,Y,Z]$, $H_2(X,Y,Z) \in \mathbb{F}_{q^{p_2}}[X,Y,Z]$ such that

$$R_{i_1}(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^{p_1}}/\mathbb{F}_q)} \sigma(H_1(X,Y,Z)),$$

and

$$R_{i_2}(X,Y,Z) = \prod_{\gamma \in Gal(\mathbb{F}_{q^{p_2}}/\mathbb{F}_q)} \gamma(H_2(X,Y,Z)).$$

Now we can write $\phi_f(X,Y,Z)$ as follows,

$$\phi_f(X,Y,Z) = R(X,Y,Z)\Big(\prod_{\sigma \in Gal(\mathbb{F}_{q^{p_1}}/\mathbb{F}_q)} \sigma(H_1(X,Y,Z))\Big)\Big(\prod_{\gamma \in Gal(\mathbb{F}_{q^{p_2}}/\mathbb{F}_q)} \gamma(H_2(X,Y,Z))\Big)$$

which is a contradiction with Theorem 60. Therefore, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Notice that in the case $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-3}e$, $e \equiv 3 \pmod 4$, we only have two cases either $e = 3$ or $e = 7$. If $e = 3$, then $\mathrm{DG}(\phi_f) = 2^n + 2 - 2^{n-3}(3) > 2^n + 2 - 2^{n-3}(4) = 2^{n-1} + 2$. Therefore, this case is already solved by Aubry McGuire and Rodier in [2].

3.4. **Case when** $\deg(h) = 2^{n-j}e$**, where** $e \equiv 1 \pmod 4$**.** Define $\rho_d(X,Y) = \phi_d(X,Y,Y)$.

Lemma 24. Let $d = 1 + 2^k m$, where $k \geq 2$ and $m > 1$ is odd. Then $\nu_{(1,1,1)}(\phi_d) \leq \nu_{(1,1)}(\rho_d)$.

Proof: Let $G(X,Y,Z) = \phi_d(X+1, Y+1, Z+1)$. Writing $G(X,Y,Z)$ in homogeneous terms we obtain

$$G(X,Y,Z) = G_d(X,Y,Z) + G_{d-1}(X,Y,Z) + \cdots + G_a(X,Y,Z) \tag{16}$$

where G_i is either 0 or a homogeneous polynomial of degree i. Now intersecting $G(X,Y,Z)$ with the plane $Y = Z$, we obtain

$$F(X,Y) = G(X,Y,Y) = G_d(X,Y,Y) + G_{d-1}(X,Y,Y) + \cdots + G_a(X,Y,Y). \tag{17}$$

It is clear by Equations 16 and 17 that $\deg(T_G) \leq \deg(T_F)$. Notice that $F(X,Y) = \rho_d(X+1, Y+1)$. Therefore, $\nu_{(1,1)}(\rho_d) \geq \nu_{(1,1,1)}(\phi_d)$.

□

Lemma 25. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $\deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. Then, $\mathrm{DG}(\phi_f) \geq 2^{n-j+k} - 2^{n-j} + 1$.

Proof: Notice that if $k \geq j$, then it is clear that $\deg(h) > 2^n + 1$ which is a contradiction with the degree of f. Therefore, we have that $k < j$. For fix $j \geq 4$, we have that the maximum possible value of e is given by $e = 2^k(2^{j-k} - 1)$. Therefore, $DG(\phi_f) \geq 2^n + 1 - 2^{n-j}(2^k(2^{j-k} - 1) + 1) = 2^n + 1 - (2^n - 2^{n-j+k} + 2^{n-j}) = 2^{n-j+k} - 2^{n-j} + 1$. □

Lemma 26. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. Then $\nu_{(1,1,1)}(\phi_d) \leq 3(2^{n-j} - 1) + 2^{n-j+k} - 2^{n-j+1}$.

Proof: By Equation 3 and Lemma 1 we have that $\nu_{(1,1,1)}(\phi_d) = (2^{n-j} - 1)\nu_{(1,1,1)}(\phi_6) + 2^{n-j}\nu_{(1,1,1)}(\phi_e)$ Then by lemma 24 $\nu_{(1,1,1)}(\phi_d) \leq 3(2^{n-j} - 1) + 2^{n-j}\nu_{(1,1)}(\rho_{2^k m+1})$. By Lemma 11 we can deduce that $\nu_{(1,1)}(\rho_{2^k m+1}) = 2^k - 2$. Therefore, $\nu_{(1,1,1)}(\phi_d) \leq 3(2^{n-j} - 1) + 2^{n-j+k} - 2^{n-j+1}$. □

Theorem 62. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. Then $\phi_f(X, Y, Z)$ can have up to 5 factors (non constant).

Proof: To show it can have up to 5 factors is enough to show that if $\phi_f(X, Y, Z)$ is the product of 6 factors then you have a contradiction. Assume on the contrary that $\phi_f(X, Y, Z)$ can be written as the product of 6 nonconstant factors, i.e.

$$\phi_f(X, Y, Z) = \prod_{i=1}^{6} R_i(X, Y, Z)$$

Notice that by Theorem 13 we have that $(\phi_{2^n+1}, \phi_e) = 1$, thus $(\phi_{2^n+1}, \phi_{2^{n-j}e}) = 1$. By Corollary 15 and Lemma 25 we have that $\deg(R_i) \geq DG(\phi_f) \geq 2^{n-j+k} - 2^{n-j} + 1$. Notice that, $2^{n-j+k} > 2(2^{n-j} - 1)$, $2^{n-j+k} - 2^{n-j} > 2^{n-j} - 1$. Therefore, $3DG(\phi_f) \geq 3(2^{n-j+k} - 2^{n-j} + 1) = 2^{n-j+k} + 2^{n-j+k} + 2^{n-j+k} - 2^{n-j+1} - 2^{n-j} + 1 > 2(2^{n-j} - 1) + 2^{n-j} - 1 + 2^{n-j+k} - 2^{n-j+1} + 1 = \nu_{(1,1,1)}(\phi_d) + 1$. Define $P(X, Y, Z) = \prod_{i=1}^{3} R_i(X, Y, Z)$ and $Q(X, Y, Z) = \prod_{i=4}^{6} R_i(X, Y, Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_i and Q_i are zero or homogeneous of degree i, $s + t = 2^n - 2$. Without loss of generality assume that $s \geq t$. Then,

$$P_s Q_t = \phi_{2^n+1},$$

and

$$\phi_d = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 21 and the previous discussion we have $\nu_{(1,1,1)}(P_s) \geq \nu_{(1,1,1)}(\phi_d) + 1$, $\nu_{(1,1,1)}(Q_t) \geq \nu_{(1,1,1)}(\phi_d) + 1$. Computing $\nu_{(1,1,1)}(\phi_d) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a})\nu_{(1,1,1)}(P_{s-a} Q_t)) \geq \nu_{(1,1,1)}(\phi_d) + 1$ which is a contradiction. □

Proposition 20. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If $n = 2^l$ $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X, Y, Z)$ defined over $\mathbb{F}_q$ with $m(R) = 2$. By Corollary 7 we have that $m(\phi_f)$ |

$m(R)$ so we have that either $m(\phi_f) = 2$ or $m(\phi_f) = 1$. If $m(\phi_f) = 2$, i.e. $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$, where $P(X, Y, Z)Q(X, Y, Z) \in \mathbb{F}_{q^2}[X, Y, Z]$. Then by theorem 41 we have that $\deg(P) = \deg(Q) = 2^{n-1} - 1$. Notice that $\phi_{2^n+1}(X, Y, Z) = t_P(X, Y, Z)t_Q(X, Y, Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) = \deg(t_P) = 2^{n-1} - 1$.

Notice that $2\nu_{1,1,1}(\phi_{2^{n-j}e} \leq 2(3(2^{n-j} - 1) + 2^{n-j+k} - 2^{n-j+1}) < 8(2^{n-j} - 1) + 2^{n-j} + k + 1) - 2^{n-j+2} = 2^{n-j} + 2^{n-j+k+1} - 8 < 2^n - 2$ (since $j > k + 1$ otherwise you get a contratiction with $\deg(f) > \deg(h)$). Therefore, $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-d}), \nu_{(1,1,1)}(P_{s-d}Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that $\phi_f(X, Y, Z)$ factors over $\mathbb{F}_q$ with factorization

$$\phi_f(X, Y, Z) = \prod_{i=1}^{k} R_i(X, Y, Z), \tag{18}$$

where $R_i(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ is irreducible non constant polynomial for $i = 1, \ldots, k$. Notice that for each $t_{R_i}(X, Y, Z)$, there exists an irreducible polynomial $W_i(X, Y, Z)$ such that $m(W_i) = 2^{k_i}$, where $k_i \geq 1$ for each $i = 1, \ldots, k$. By Corollary 7 we have that $m(R_i) \mid m(W_i)$ for each $i = 1, \ldots, k$. Therefore, $m(R_i) = 2^{a_i}$, where $0 \leq a_i \leq k_i$ for every $i = 1, \ldots, k$. If there exists a i_0 such that $m(R_{i_0}) = 1$, then we have an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $m(R_i) = 2^{a_i}$, where $1 \leq a_i \leq k_i$ for each $i = 1, \ldots, k$. Now for every $i = 1, \ldots, k$ by Theorem 41 there exist an absolutely irreducible factor $h_i(X, Y, Z) \in \mathbb{F}_{q^{2^{a_i}}}[X, Y, Z]$, $c_i \in \mathbb{F}_q$ such that

$$R_i(X, Y, Z) = c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)} \sigma(h_i(X, Y, Z)), \tag{19}$$

Combining Equations 18 and 19 we obtain the following equation:

$$\phi_f(X, Y, Z) = \prod_{i=1}^{k} c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)} \sigma(h_i(X, Y, Z)). \tag{20}$$

Notice that $|Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)| = 2^{a_i}$ and that for every $\alpha, \beta \in Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)$ we have that $\deg(\alpha(h_i)) = \deg(\beta(h_i))$. Let γ_i be a generator of $Gal(\mathbb{F}_{q^{2^{a_i}}})/\mathbb{F}_q)$, define $g_i(X, Y, Z) = \prod_{r=1}^{2^{a_1-1}} \gamma_i^r(h_i(X, Y, Z))$ and $f_i(X, Y, Z) = \prod_{r=2^{a_i-1}+1}^{2^{a_i}} \gamma_i^r(h_i(X, Y, Z))$. Then using this definitions we can rewrite Equation 20 as

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i g_i(X,Y,Z) f_i(X,Y,Z)$$

Notice that $\deg(f_i) = \deg(g_i)$. Define $P(X,Y,Z) = \prod_{i=1}^{k} g_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=1}^{k} c_i f_i(X,Y,Z)$, then $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, with $\deg(P) = \deg(Q) = 2^{n-1} - 1$. Notice that $\phi_{2^n+1}(X,Y,Z) = t_P(X,Y,Z)t_Q(X,Y,Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)}(t_Q) = \deg(t_P) = 2^{n-1} - 1$.

Notice that $2\nu_{1,1,1}(\phi_{2^{n-j}e} = 6(2^{n-j}-1) \leq 9(2^{n-4}-1) = 2^{n-1}+2^{n-4}-9 < 2^n-2$. Therefore, $\nu_{(1,1,1)}(t_P) = \nu_{(1,1,1)} > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-d}), \nu_{(1,1,1)}(P_{s-d} Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, there exist an $i_0 \in \{1, \ldots, k\}$ such that $m(R_{i_0}) = 1$. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

Proposition 21. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If $n = p^l$, where $p > 6$ is prime, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. By factorization in Equation 1 ϕ_{2^n+1} contains an irreducible factor $P(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ with $m(P) = p$. By Corollary 7 $m(\phi_f) \mid p$ but p prime implies that either $m(\phi_f) = 1$ or $m(\phi_f) = p$. If $m(\phi_f) = p$, then $\phi_f(X,Y,Z)$ factor into p factors which is a contradiction of Theorem 62. Therefore, $m(\phi_f) = 1$ and $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z)$ is irreducible and $P(X,Y,Z), Q(X,Y,Z)$ are non constant polynomials. Since $P(X,Y,Z)$ is non constant polynomial, then $t_P(X,Y,Z)$ contains an irreducible factor $P_1(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ with $m(P_1) = p^k$, for some $k \geq 1$. By Corollary 7 $m(\phi_f) \mid p^k$ but p prime implies that either $m(\phi_f) = 1$ or $m(\phi_f) = p^{k_1}$, where $1 \leq k_1 \leq k$. If $m(\phi_f) = p^{k_1}$, then $\phi_f(X,Y,Z)$ factor into p^{k_1} factors which is a contradiction of Theorem 62. Therefore, $m(P) = 1$ and $P(X,Y,Z)$ is absolutely irreducible. □

Proposition 22. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If n is odd, $n > 6$ and n is not a prime power, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes p_1,p_2 ($p_1 \neq p_2$) such that $p_1p_2 \mid n$, then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ and let p_1,p_2 be prime numbers such that $p_1p_2 \mid n$ with $p_1 \neq p_2$. Let

$$\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)R(X,Y,Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains an irreducible factor of $\phi_{2^{p_1}+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^{p_2}+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^{p_2}+1}(X,Y,Z)) = 1$. Now we can assume without loss of generality that $t_Q(X,Y,Z)$ contains an irreducible factor of $\phi_{2^{p_2}+1}(X,Y,Z)$. Now by Corollary 7 we have that $m(P) \mid p_1$ and $m(Q) \mid p_2$. If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Assume that $m(P) = p_1$ and $m(Q) = p_2$, then $\phi_f(X,Y,Z)$ have a factorization with at least $p_1 + p_2 > 5$ factors which is a contradiction with Theorem 62. Therefore, either $m(P) = 1$ or $m(Q) = 1$ and thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. □

Proposition 23. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If n is a power of 5, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X,Y,Z)$ defined over $\mathbb{F}_q$ with $m(R) = 5$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = 5$ or $m(\phi_f) = 1$. If $m(\phi_f) = 5$, i.e. $\phi_f(X,Y,Z) = \prod_{i=1}^{5} R_i(X,Y,Z)$, where $R_i(X,Y,Z) \in \mathbb{F}_{q^5}[X,Y,Z]$. Then by theorem 41 we have that $\deg(R_i) = (2^n - 2)/5$ for $i = 1,\ldots,5$. Notice that $\phi_{2^n+1}(X,Y,Z) = \prod_{i=1}^{5} t_{R_i}(X,Y,Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_{R_i}) = \deg(t_{R_i}) = (2^n - 2)/5$.

Define $P(X,Y,Z) = R_1(X,Y,Z)R_2(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=3}^{5} R_i(X,Y,Z)$.

We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $5\nu_{1,1,1}(\phi_{2^{n-j}e} = 5(3(2^{n-j}-1)+2^{n-j+k}-2^{n-j+1}) = 2^4(2^{n-j})-15-2^{n-j}+5(2^{n-j+k}-2^{n-j+1}) = 2^{n-j+4}-15-2^{n-j}+2^{n-j+k+2}-2^{n-j+3}+2^{n-j+k}-2^{n-j+1}$. The maximum multiplicity is attained when $k = j-2$ so we have $5\nu_{1,1,1}(\phi_{2^{n-j}e} = 5(3(2^{n-j}-1)+2^{n-j+k}-2^{n-j+1}) \leq 2^{n-j+4}-15-2^{n-j}+2^n-2^{n-j+3}+2^{n-2}-2^{n-j+1} = 2^n+2^{n-2}+2^{n-j+3}-2^{n-j+1}-2^{n-j}-15 < 2^{n+1}-15 < 4(2^{n-1}-1)$ that is $5\nu_{(1,1,1)}(\phi_d) < 2^{n+1}-4$. Now by Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-d}), \nu_{(1,1,1)}(P_{s-d}Q_t)) = \nu_{(1,1,1)}(P_s) = (\frac{2}{5}(2^n-2)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$, $P(X,Y,Z)$ and $Q(X,Y,Z)$ are non constant polynomials and $P(X,Y,Z)$ is irreducible. Since $P(X,Y,Z)$ is non constant then there exists an irreducible polynomial $W(X,Y,Z)$ such that $W(X,Y,Z) \mid t_P(X,Y,Z)$. By Equation 1 $m(W) = 5^k$ where $k \geq 1$ and by Corollary 7 we have $m(P) \mid m(W)$. Therefore, $m(P)$ is either $m(P) = 1$ or $m(P) = 5^{k_1}$, where $1 \leq k_1 \leq k$. If $m(P) = 5^{k_1}$, then by theorem 41 $P(X,Y,Z)$ factors into 5^{k_1} factors and we obtain that $\phi_f(X,y,Z)$ has a factorization with at least $5^{k_1}+1$ factors which is a contradiction with Proposition 11. Therefore, $m(P) = 1$ and thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

□

Proposition 24. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^km+1$, $k \geq 2$ and $m > 1$ odd. If n is even, and $p \mid n$ is a prime $p > 3$, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes $2, p$ $(p \neq 2)$ such that $2p \mid n$, then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ and let

$$\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)R(X,Y,Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains $\phi_{2^2+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^p+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^p+1}(X,Y,Z)) = 1$. Without loss of generality we can assume that $t_Q(X,Y,Z)$ contains an irreducible factor of ϕ_{2^p+1}. By Corollary 7 we have that $m(P) \mid 2$ and $m(Q) \mid p$, then we have that either $m(P) = 1$ (respectively $m(Q) = 1$) or $m(P) = 2$ (respectively $m(Q) = p$). If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. We can assume that $m(P) = 2$ and $m(Q) = p$, then $\phi_f(X,Y,Z)$ have a factorization with at least $2+p > 6$ factors which is a contradiction of Theorem 62.

□

Proposition 25. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If n is a power of 3, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible. Notice that ϕ_{2^n+1} contains an irreducible factor $R(X, Y, Z)$ defined over $\mathbb{F}_q$ with $m(R) = 3$. By Corollary 7 we have that $m(\phi_f) \mid m(R)$ so we have that either $m(\phi_f) = 3$ or $m(\phi_f) = 1$. If $m(\phi_f) = 3$, i.e. $\phi_f(X, Y, Z) = \prod_{i=1}^{3} R_i(X, Y, Z)$, where $R_i(X, Y, Z) \in \mathbb{F}_{q^3}[X, Y, Z]$. Then by theorem 41 we have that $\deg(R_i) = (2^n - 2)/3$ for $i = 1, 2, 3$. Notice that $\phi_{2^n+1}(X, Y, Z) = \prod_{i=1}^{3} t_{R_i}(X, Y, Z)$. Now by lemma 21 we have that $\nu_{(1,1,1)}(t_{R_i}) = \deg(t_{R_i}) = (2^n - 2)/3$.

Define $P(X, Y, Z) = R_1(X, Y, Z)$ and $Q(X, Y, Z) = \prod_{i=2}^{3} R_i(X, Y, Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $3\nu_{1,1,1}(\phi_{2^{n-j}e}) = 3(3(2^{n-j} - 1) + 2^{n-j+k} - 2^{n-j+1}) = 9(2^{n-j} - 1) + 3(2^{n-j+k}) - 3(2^{n-j+1}) = 2^{n-j+3} + 2^{n-j+k+1} + 2^{n-j+k} - 2^{n-j+2} - 2^{n-j+1} + 2^{n-j} - 9 < 2^n - 2$. Therefore, $\nu_{(1,1,1)}(t_{R_i}) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. Now by Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-d}), \nu_{(1,1,1)}(P_{s-d} Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)\, R(X, Y, Z)$, where $P(X, Y, Z)$, $Q(X, Y, Z)$, $R(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$, $P(X, Y, Z)$ and $Q(X, Y, Z)$ are non constant irreducible polynomials. Since $P(X, Y, Z)$ is non constant then there exists an irreducible polynomial $W(X, Y, Z)$ such that $W(X, Y, Z) \mid t_P(X, Y, Z)$. By Equation 1 $m(W) = 3^k$ where $k \geq 1$ and by Corollary 7 we have $m(P) \mid m(W)$. Therefore, $m(P)$ is either $m(P) = 1$ or $m(P) = 3^{k_1}$, where $1 \leq k_1 \leq k$. Similarly, there exists an irreducible polynomial $V(X, Y, Z)$ such that $V(X, Y, Z) \mid t_Q(X, Y, Z)$. By equation 1, $m(V) = 3^a$, where $a \geq 1$ and by Corollary7 we have $m(Q) \mid m(V)$. Therefore, $m(Q) = 1$ or $m(Q) = 3^{a_1}$, where $1 \leq a_1 \leq a$. If either $m(P) = 1$ or $m(Q) = 1$, then you have an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $m(P), m(Q) > 1$, then by Theorem 41 $P(X, Y, Z)$ factors into at least 3 factors. Similarly, $Q(X, Y, Z)$ factors into at least 3 factors. Therefore, $\phi(X, Y, Z)$ have a factorization into at least 6 factors which is a contradiction with Theorem 62. □

Proposition 26. Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, where $d = \deg(h) = 2^{n-j}e$, $j \geq 4$, $e = 2^k m + 1$, $k \geq 2$ and $m > 1$ odd. If $6 \mid n$, then $\phi_f(X, Y, Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^n+1}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_{2^n+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

If n is divisible by any prime p different than 2 and 3, then by Proposition 24 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that n is only divisible by 2 and 3, i.e. $n = 2^{n_1}3^{n_2}$, where $n_1, n_2 \geq 1$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Since n is not a prime power there exist at least two primes $2,3$ such that $6 \mid n$, then by Theorem 50 $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\phi_f(X,Y,Z)$ factors over $\mathbb{F}_q$ and let

$$\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)R(X,Y,Z),$$

where $P(X,Y,Z)$, $Q(X,Y,Z)$ are irreducible non constant polynomials and $t_P(X,Y,Z)$ contains $\phi_{2^2+1}(X,Y,Z)$. If $t_P(X,Y,Z)$ also contain an irreducible factor of $\phi_{2^3+1}(X,Y,Z)$, then by Corollary 11 $P(X,Y,Z)$ is absolutely irreducible. Therefore, we can assume without loss of generality that $(t_P(X,Y,Z), \phi_{2^3+1}(X,Y,Z)) = 1$. Without loss of generality we can assume that $t_Q(X,Y,Z)$ contains an irreducible factor of ϕ_{2^3+1}.By Corollary 7 we have that $m(P) \mid 2$ and $m(Q) \mid 3$, then we have that either $m(P) = 1$ (respectively $m(Q) = 1$) or $m(P) = 2$ (respectively $m(Q) = 3$). If either $m(P) = 1$ or $m(Q) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. We can assume that $m(P) = 2$ and $m(Q) = 3$. If $R(X,Y,Z)$ is a non constant polynomial then we get a contradiction with Theorem 62 (2 factors from P, 3 factors from Q and 1 factor from R). Therefore, we can assume that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$.

Suppose that $\deg(P) \geq \deg(Q)$, then $\deg(P) \geq 2^{n-1} - 1$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = 2^k - 2$. Then

$$\phi_{2^n+1} = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

Notice that by Lemmas 21, 25 and $m(Q) = 3$, we have $\nu_{(1,1,1)}(Q_t) = \deg(Q_t) \geq 3DG(\phi_f) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$. Similarly, by Lemma 21 we have that $\nu_{(1,1,1)}(P_s) > \nu_{(1,1,1)}(\phi_{2^{n-j}e}$. Now by Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-d}), \nu_{(1,1,1)}(P_{s-d}Q_t)) > \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, $m(\phi_f) = 1$ and $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that $\deg(Q) \geq 2^{n-1}-1$. Since $m(Q) = 3$, then there exists $R_1(X,Y,Z), R_2(X,Y,Z), R_3(X,Y,Z) \in \mathbb{F}_{q^3}[X,Y,Z]$ such that $Q(X,Y,Z) = \prod_{i=1}^{3} R_i(X,Y,Z)$ and $\deg(R_1) = \deg(R_2) = \deg(R_3) \geq \frac{2^{n-1}-1}{3}$. Define $A(X,Y,Z) = R_1(X,Y,Z)R_2(X,Y,Z)$ and $B(X,Y,Z) = R_3(X,Y,Z) \cdot P(X,Y,Z)$. We write $A(X,Y,Z)$ and $B(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=2^k-2$. Then

$$\phi_{2^n+1}=A_sB_t,$$

and

$$\phi_{2^{n-j}e}=A_sB_{t-a}+A_{s-a}B_t.$$

Notice that $3\nu_{(1,1,1)}(\phi_{2^{n-j}e})<2^n-2$, which implies by Lemma 21 that $\nu_{(1,1,1)}(\phi_{2^{n-j}e})<\nu_{(1,1,1)}(A_s)$. By Lemma 21 and Lemma 25 we have $\nu_{(1,1,1)}(B_t)=\deg(B_t)\geq 3DG(\phi_f)>\nu_{(1,1,1)}(\phi_{2^{n-j}e})$. By Lemma 1, $\nu_{(1,1,1)}(2^{n-j}e)\geq\min(\nu_{(1,1,1)}(A_sB_{t-d}),\nu_{(1,1,1)}(A_{s-d}B_t))>\nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Thus, $\phi_f(X,Y,Z)$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. □

Theorem 63. Let $f(X)=X^{2^n+1}+h(X)\in\mathbb{F}_q[X]$, where $d=\deg(h)=2^{n-j}e$, $j\geq 4$, $e=2^km+1$, $k\geq 2$ and $m>1$ odd. Then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

4. Completion of the Kasami-Welch Case with Even Degree-gap and Some Progress in the Odd Degree-gap Case

This chapter is divided into two sections. In the first section, we investigate the case when the second term has even degree. We show in Theorem 68 that if the second term of the polynomial with degree d and $\nu_{(1,1,1)}(\phi_d) < 2^{n-2}$ then ϕ_f contain an absolute irreducible factor defined over $\mathbb{F}_q$ and thus $f(X)$ is not exceptional APN. In the second section we proof an analogue of Theorem 68 (see Theorem 70). Using this theorem we show the remaining case of the exceptional APN conjecture with Kasami-Welch degree and the second term with odd degree (see Corollary 23).

The next theorem extends the knowledge we have from equation 2. In fact the next theorem prove that $\phi_d(X,Y,Z) \in \mathbb{F}_2[X,Y,Z]$, where $d = 2^{2k}-2^k+1$ contains an absolutely irreducible factor defined over every proper subfield of $\mathbb{F}_{2^k}$ except $\mathbb{F}_2$. This is an analogue of the Gold Case.

Theorem 64. Let $f(X) = X^d \in \mathbb{F}_2$, where $d = 2^{2k} - 2^k + 1$. If $k > 1$ then, $\phi_d(X,Y,Z)$ contains an absolutely irreducible factor defined over every proper subfield of $\mathbb{F}_{2^k}$ except from $\mathbb{F}_2$. Moreover, if $H(X,Y,Z) \in \mathbb{F}_{2^t}[X,Y,Z]$ is absolutely irreducible and divides $\phi_d(X,Y,Z)$ then, $\prod_{\sigma \in Gal(\mathbb{F}_{2^t}/\mathbb{F}_2)} \sigma(H(X,Y,Z))$ also divides $\phi_d(X,Y,Z)$.

Proof: If k is a prime number then, $\mathbb{F}_{2^k}$ only has $\mathbb{F}_2$ as a subfield and therefore the theorem do not apply to this case. Therefore, we can assume without loss of generality that k is not prime. Let β be a primitive element of $\mathbb{F}_{2^k}$ then, we can rewrite equation 2 as

$$\phi_d(X,Y,Z) = \prod_{i=1}^{2^k-2} P_{\beta^i}(X,Y,Z).$$

Let $t > 1$ be any divisor of k then, there exists $n > 1$ such that β^n is a primitive element of $\mathbb{F}_{2^t}$. Let σ_0 be the Frobenius automorphism of $\mathbb{F}_2$.
Claim: $Q(X,Y,Z) = \prod_{i=1}^{t} \sigma_0^i(P_{\beta^n}(X,Y,Z)) \in \mathbb{F}_2[X,Y,Z]$.

Notice that $\sigma_0(P_{\beta^j}(X,0,1) = \sigma_0((X+\beta^j)^{2^k+1}) = (X+\sigma_0(\beta^j))^{2^k+1} = P_{\sigma(\beta^j)}(X,0,1)$, for every $j \in \{1,\dots,2^k-2\}$. Since the Frobenius automorphism is a generator of the group $Gal(\mathbb{F}_{2^k}/\mathbb{F}_2)$, we only need to show that $\sigma_0(Q(X,Y,Z)) = Q(X,Y,Z)$. But $\sigma_0(Q(X,Y,Z)) = \sigma_0(\prod_{i=1}^{t} \sigma_0^i(P_{\beta^n}(X,Y,Z))) = \prod_{i=1}^{t} \sigma_0^{i+1}(P_{\beta^n}(X,Y,Z)) = \prod_{i=2}^{t+1} \sigma_0^i(P_{\beta^n}(X,Y,Z)) = \prod_{i=2}^{t+1} P_{\sigma_0^i(\beta^n)}(X,Y,Z)$. Since β^n is a primitive element of $\mathbb{F}_{2^t}$ we have that $\sigma_0^{t+1}(P_{\beta^n}) = \sigma_0(P_{\sigma_0^t(\beta^n)}(X,Y,Z)) = \sigma_0(P_{\beta^n}(X,Y,Z))$. Therefore,

$$\sigma_0(Q(X,Y,Z)) = \prod_{i=2}^{t+1} P_{\sigma_0^i(\beta^n)}(X,Y,Z) = \prod_{i=1}^{t} P_{\sigma_0^i(\beta^n)}(X,Y,Z) = Q(X,Y,Z)$$

Therefore the claim is true.

Now by lemma 6 we know there exists $r > 1$ and an absolutely irreducible polynomial $h(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ such that

$$Q(X,Y,Z) = \prod_{\alpha \in Gal(\mathbb{F}_{2^r}/\mathbb{F}_2)} \alpha(h(X,Y,Z)$$

where α act on the coefficients of $h(X,Y,Z)$. Since factorization into absolutely irreducible factors is unique up to associates and ordering we can conclude that $r = t$ (i.e. you must have the same number of absolutely irreducible factors). Therefore, $Q(X,Y,Z)$ (and thus $\phi_d(X,Y,Z)$) contains an absolutely irreducible factor defined over $\mathbb{F}_{2^t}$.

□

Theorem 65. Let $f(X) = X^{2^{2n_1n_2} - 2^{n_1n_2}+1} + h(X) \in \mathbb{F}_q[X]$, where $(n_1, n_2) = 1$, $n_1, n_2 > 1$. If $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$ then, $\phi_f(X,Y,Z)$ is absolutely irreducible.

Proof: Suppose $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$ and $(n_1,n_2) = 1$, $n_1, n_2 > 1$, then by corollary 11 $\phi_f(X,Y,Z)$ is absolutely irreducible. □

Theorem 66. Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_q[X]$, and $\deg(h) < 2^{2k} - 2^k + 1$. Let p be the greatest prime that divide k. If $DG(\phi_f) > (2^{2k} - 2^k - 2)/p$ then, $\phi_f(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_{2^{2k}-2^k+1}(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$ then, by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Therefore, we can assume that $\phi_{2^{2k}-2^k+1}(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$. Assume that $\phi_f(X,Y,Z)$ is irreducible defined over $\mathbb{F}_q$. Let $\psi_\phi(X,Y,Z)$ be the reverse polynomial of $\phi_f(X,Y,Z)$ then, by lemma 13 $\psi_\phi(X,Y,Z)$ is also irreducible over $\mathbb{F}_q$. By lemma 6 there exists an integer $r > 1$ and absolutely irreducible polynomial $h(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ and $c \in \mathbb{F}_q$ such that

$$\psi_\phi(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(h(X,Y,Z)). \tag{21}$$

Let $T(X,Y,Z)$ be the tangent cone of $\psi_\phi(y,y,z) \in \mathbb{F}_q[X,Y,Z]$ then, there exists $t(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ such that

$$T(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(t(X,Y,Z)).$$

By theorem 64, $\phi_{2^{2k}-2^k+1}(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$ (is the minimum extension of $\mathbb{F}_q$ that contain $\mathbb{F}_{2^p}$ as a subfield). By lemma 4 $T(X,Y,Z)$ contains a reduced absolutely irreducible polynomial defined over $\mathbb{F}_{q^p}$ and by theorem 42 $\psi_\phi(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$. Since the factorization in equation 21 is unique up to associates and ordering wee obtain that $p \mid r$.

By lemma 13 we obtain that there exists an absolutely irreducible polynomial $g(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ and $c \in \mathbb{F}_q$ such that

$$\phi_f(X,Y,Z) = \prod_{\beta \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)} \beta(g(X,Y,Z)).$$

Now each factor $\beta(g(X,Y,Z))$ have degree $(2^{2k} - 2^k - 2)/r$. Since $r = ps$, we have by theorem 47 that for each $\beta \in Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$, $DG(\beta(g(X,Y,Z))) \geq (2^{2k} - 2^k - 2)/p \geq$

$(2^{2k}-2^k-2)/r = \deg(\beta(g(X,Y,Z)))$. This implies that $\phi_f(X,Y,Z)$ is the product of homogeneous polynomials which is a contradiction. Therefore $r=1$. Thus, $\phi_f(X,Y,Z)$ is absolutely irreducible.

Similarly assume that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$, where $P(X,Y,Z)$ is an irreducible polynomial (not homogeneous) defined over $\mathbb{F}_q$ such that the highest homogeneous form of $P(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_{q^p}$. We can make a similar argument as with $\phi_f(X,Y,Z)$ to obtain that $P(X,Y,Z)$ is absolutely irreducible over $\mathbb{F}_q$.

□

4.1. **Kasami Welch Case when the second term is even degree.**

Lemma 27. Let $f(X) = X^d \in \mathbb{F}_q[X]$, where $d = 2^{2n}-2^n+1$. If $P(X,Y,Z)Q(X,Y,Z) \mid \phi_f(X,Y,Z)$ and $\deg(P) = \deg(Q)$, then $\nu_{(1,1,1)}(P) = \nu_{(1,1,1)}(Q)$.

Proof: This follows directly from the fact that every absolutely irreducible factor $R(X,Y,Z)$ of $\phi_f(X,Y,Z)$ have the same degree and $\nu_{(1,1,1)}(R) = 1$. □

Lemma 28. Let $f(X) = X^d + h(X)$, where $d = 2^{2n}-2^n+1$ $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. Then $(\phi_{2^n+1}, \phi_h) = 1$. Moreover, $\phi_f(X,Y,Z)$ is not divisible by any homogeneous polynomial.

For the rest of this section assume that $j \geq 4$.

Proposition 27. Let $f(X) = X^d + h(X)$, where $d = 2^{2n}-2^n+1$ $\deg(h) = 2^{n-j}e$, where $e \equiv 3 \pmod 4$. If $n = 2^m$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,Y,Z)$ is irreducible. By Theorem 64 $\phi_d(X,Y,Z)$ contains an irreducible factor $R(X,Y,Z)$ such that $m(R) = 2$. By Corollary 7 we obtain $m(\phi_f) \mid 2$ .i.e. $m(\phi_f) = 1$ or $m(\phi_f) = 2$. If $m(\phi_f) = 2$, then by theorem 41 we can write $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$ and $\deg(P) = \deg(Q)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

Notice that $\deg(P_s) = \deg(Q_t)$. By lemma 27 we have $\nu_{(1,1,1)}(P) = \nu_{(1,1,1)}(Q)$. By lemma 1 we have $2^n - 2 = \nu_{(1,1,1)}(\phi_d) = \nu_{(1,1,1)}(P) + \nu_{(1,1,1)}(Q) = 2\nu_{(1,1,1)}(P)$. Therefore we have that $\nu_{(1,1,1)}(P) = 2^{n-1}-1$. Similarly we have that $3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq$

$\min(P_sQ_{t-a}, P_{s-a}Q_t) \geq 2^{n-1} - 1 > 3(2^{n-3} - 1) > 3(2^{n-j} - 1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore $m(\phi_f) = 1$ and hence $\phi_f(X, Y, Z)$ is absolutely irreducible.

Suppose that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z), \tag{22}$$

where $R_i(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ is irreducible for $i = 1, \dots, k$. By Theorem 64 every factor $R(X, Y, Z)$ of $\phi_d(X, Y, Z)$ have the property $m(R)$ is a power of two. So we can conclude by Corollary 7 that $m(R_i) = 2^{k_i}$, where $k_i \geq 0$ with $i = 1, \dots, k$. If there exists an i_0 such that $m(R_{i_0}) = 1$, then $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $k_i \geq 1$ for $i = 1, \dots, k$. By Theorem 41 there exists an absolutely irreducible factor $h_i(X, Y, Z)$, $c_i \in \mathbb{F}_q$ such that

$$R_i(X,Y,Z) = c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{2^{k_i}}}/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)). \tag{23}$$

Combining Equations 22 and 23 we obtain:

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{\sigma \in Gal(\mathbb{F}_{q^{2^{k_i}}}/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)). \tag{24}$$

Now let γ_i be a generator of $Gal(\mathbb{F}_{q^{2^{k_i}}}/\mathbb{F}_q)$ for $i = 1, \dots, k$ and define $G_i = |Gal(\mathbb{F}_{q^{2^{k_i}}}/\mathbb{F}_q)|$. We can rewrite Equation 24 as

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{b=1}^{G_i} \gamma_i^b(h_i(X,Y,Z))$$

Notice that by Theorem 41 every factor of $R_i(X, Y, Z)$ have the same degree for $i = 1, \dots, k$. Define $P(X,Y,Z) = \prod_{i=1}^{k} \prod_{b=1}^{G_i/2} \gamma_i^b(h_i(X,Y,Z)$ and $Q(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{b=G_i/2+1}^{G_i} \gamma_i^b(H_i(X,Y,Z))$. It is clear that $\deg(P) = \deg(Q)$. That is $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

Notice that $\deg(P_s) = \deg(Q_t)$. By lemma 27 we have $\nu_{(1,1,1)}(P) = \nu_{(1,1,1)}(Q)$. By lemma 1 we have $2^n - 2 = \nu_{(1,1,1)}(\phi_d) = \nu_{(1,1,1)}(P) + \nu_{(1,1,1)}(Q) = 2\nu_{(1,1,1)}(P)$. Therefore we have that $\nu_{(1,1,1)}(P) = 2^{n-1} - 1$. Similarly we have that $3(2^{n-j} - 1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq \min(P_sQ_{t-a}, P_{s-a}Q_t) \geq 2^{n-1} - 1 > 3(2^{n-3} - 1) > 3(2^{n-j} - 1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore, there exists at least one i_0 such that $m(R_{i_0}) = 1$. □

Lemma 29. Let $n \geq 3$ and $j \geq 4$. Then,

$$\frac{n-1}{n}(2^{n-1}-1) > 3(2^{n-j}-1).$$

Proof: We will prove that the function $f(x) = \frac{x-1}{x}(2^{x-1}-1) - 3(2^{x-j}-1)$ satisfy $f(x) > 0$ for $x \geq 3$. Notice that $f(x) \geq \frac{x-1}{x}(2^{x-1}-1) - 3(2^{x-4}-1)$ for every $x \geq 3$. We just need to prove that $g(x) = \frac{x-1}{x}(2^{x-1}-1) - 3(2^{x-4}-1) > 0$ for $x \geq 3$. Taking the derivative we obtain

$$g'(X) = \frac{2^{x-4}(5x^2\ln(2) - 8x\ln(2)) + 2^{x-1} - 1}{x^2}$$

It is clear that $g'(x) > 0$ for $x \geq 3$ and $g(3) = 3.5$. So we can conclude that $\frac{n-1}{n}(2^{n-1}-1) > 3(2^{n-j}-1)$. □

Lemma 30. Let $n \geq 4$, $p \mid n$ be an odd prime and $j \geq 4$. Then,

$$\frac{p-1}{p}(2^{n-1}-1) > 3(2^{n-j}-1).$$

Proof: Notice that $\frac{p-1}{p}(2^{n-1}-1) > \frac{2}{3}(2^{n-1}-1)$. Hence, it is enough to show that $f(x) = \frac{2}{3}(2^{x-1}-1) - 3(2^{x-4}-1)$ is an increasing function for $x \geq 3$ and $f(3) > 0$.(f(x) being increasing and $f(3) > 0$ implies that $f(x) = \frac{2}{3}(2^{x-1}-1) > 3(2^{x-4}-1) \geq 3^{(}2^{x-j}-1))$ Now taking the derivative we obtain

$$f'(x) = \frac{7}{3} \cdot 2^{x-4}\ln(2) > 0.$$

Therefore, $\frac{p-1}{p}(2^{n-1}-1) > 3(2^{n-j}-1)$. □

Proposition 28. Let $f(X) = X^d + h(X)$, where $d = 2^{2n} - 2^n + 1$ $\deg(h) = 2^{n-j}e$, $e \equiv 3 \pmod 4$ and $j \geq 4$. If $n = p^m$, where p is an odd prime, then $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_d(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X, Y, Z]$, then by lemma 19 $\phi_f(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X, Y, Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X, Y, Z)$ is irreducible. By Theorem 64 $\phi_d(X, Y, Z)$ contains an irreducible factor $R(X, Y, Z)$ such that $m(R) = p$. By Corollary 7 we obtain $m(\phi_f) \mid p$ .i.e. $m(\phi_f) = 1$ or $m(\phi_f) = 2$. If $m(\phi_f) = p$, then by theorem 41 there exists $h(X, Y, Z) \in \mathbb{F}_{q^p}[X, Y, Z]$, $c \in \mathbb{F}_q$ such that

$$\phi_f(X, Y, Z) = \prod_{i=1}^{p} \sigma^i(h(X, Y, Z)),$$

where σ is a generator of $Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ and $\deg(\alpha(h)) = \deg(\beta(h))$ for every $\alpha, \beta \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$. Define $P(X, Y, Z) = \prod_{i=1}^{(p-1)/2} \sigma^i(h(X, Y, Z))$ and $Q(X, Y, Z) = \prod_{i=(p-1)/2+1}^{p} \sigma^i(h(X, Y, Z))$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $\deg(P_s) < \deg(Q_t)$. By lemma 1 we have $2^n - 2 = \nu_{(1,1,1)}(\phi_d) = p\nu_{(1,1,1)}(t_\sigma(h))$, then $\nu_{(1,1,1)}(t_{\sigma(h)}) = (2^n-2)/p$. Therefore $\nu_{(1,1,1)}(P_s) = ((2^n-2)/p)((p-1)/2) = (p-1)(2^{n-1}-1)/p$ and $\nu_{(1,1,1)}(Q_t) = \nu_{(1,1,1)}(P_s)+1$. Similarly, we have that $3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq \min(P_s Q_{t-a}, P_{s-a}Q_t) \geq (p-1)(2^{n-1}-1)/p$. By lemma 30 we have $(p-1)(2^{n-1}-1)/p > 3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction. Therefore $m(\phi_f) = 1$ and hence $\phi_f(X,Y,Z)$ is absolutely irreducible.

Suppose that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z), \tag{25}$$

where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is irreducible for $i=1,\ldots,k$. By Theorem 64 every factor $R(X,Y,Z)$ of $\phi_d(X,Y,Z)$ have the property $m(R)$ is a power of p. So we can conclude by Corollary 7 that $m(R_i) = p^{k_i}$, where $k_i \geq 0$ with $i = 1,\ldots,k$. If there exists an i_0 such that $m(R_{i_0}) = 1$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. So we can assume that $k_i \geq 1$ for $i=1,\ldots,k$. By Theorem 41 there exists an absolutely irreducible factor $h_i(X,Y,Z) \in \mathbb{F}_{q^{p^{k_i}}}$, $c_i \in \mathbb{F}_q$ such that

$$R_i(X,Y,Z) = c_i \prod_{\alpha \in Gal(\mathbb{F}_{q^{p^{k_i}}}/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)). \tag{26}$$

Combining Equations 25 and 26 we obtain:

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{\sigma \in Gal(\mathbb{F}_{q^{2^{k_i}}}/\mathbb{F}_q)} \sigma(h_i(X,Y,Z)). \tag{27}$$

Now let γ_i be a generator of $Gal(\mathbb{F}_{q^{p^{k_i}}}/\mathbb{F}_q)$ for $i=1,\ldots,k$ and define $G_i = |Gal(\mathbb{F}_{q^{p^{k_i}}}/\mathbb{F}_q)|$. We can rewrite Equation 27 as

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} c_i \prod_{b=1}^{G_i} \gamma_i^b(h_i(X,Y,Z)) \tag{28}$$

Define $W_a(X,Y,Z) = \prod_{i=1}^k c_i \prod_{b=(a-1)(p^{k_i-1})+1}^{ap^{k_i-1}} \gamma_i^b(h_i(X,Y,Z))$ for $a = 1,\ldots,p$. Notice that $\deg(W_{a_1}) = \deg(W_{a_2})$ for $a_1, a_2 \in \{1,\ldots,p\}$. Now we can rewrite Equation 28 as

$$\phi_f(X,Y,Z) = \prod_{a=1}^{p} W_a(X,Y,Z)$$

Define $P(X,Y,Z) = \prod_{i=1}^{(p-1)/2} W_i$ and $Q(X,Y,Z) = \prod_{i=(p-1)/2+1}^{p} W_i$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_sQ_t,$$

and

$$\phi_{2^{n-j}e} = P_sQ_{t-a} + P_{s-a}Q_t.$$

Notice that $\deg(P_s) < \deg(Q_t)$. By lemma 1 we have $2^n-2 = \nu_{(1,1,1)}(\phi_d) = p\nu_{(1,1,1)}(t_{V_a})$, then $\nu_{(1,1,1)}(t_{V_a}) = (2^n-2)/p$. Therefore $\nu_{(1,1,1)}(P_s) = ((2^n-2)/p)((p-1)/2) = (p-1)(2^{n-1}-1)/p$ and $\nu_{(1,1,1)}(Q_t) = \nu_{(1,1,1)}(P_s)+1$. Similarly, we have that $3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e}) \geq \min(P_sQ_{t-a}, P_{s-a}Q_t) \geq (p-1)(2^{n-1}-1)/p$. By lemma 30 we have $(p-1)(2^{n-1}-1)/p > 3(2^{n-j}-1) = \nu_{(1,1,1)}(\phi_{2^{n-j}e})$ which is a contradiction.

□

Lemma 31. Let $f(X) = x^d + h(X)$, where $d = 2^{2n}-2^n+1$ $\deg(h) = 2^{n-j}e$, $e \equiv 3 \pmod 4$ and $j \geq 4$. Then every irreducible factor $R(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ of $\phi_f(X,Y,Z)$ is either absolutely irreducible or $\nu_{(1,1,1)}(t_R) < 2^{n-2}$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Let $\phi_f(X,Y,Z) = R(X,Y,Z)Q(X,Y,Z)$. If $t_R(X,Y,Z)$ contains irreducible factors $W_1(X,Y,Z)$, $W_2(X,Y,Z)$ such that $m(W_1) = p_1$, $m(W_2) = p_2$, and $(p_1,p_2) = 1$, then $\phi_f(X,Y,Z)$ is absolutely irreducible by Theorem 65. Therefore, we can assume that $m(t_R) = w$. Thus, by Corollary 7 $m(R) \mid w$.

Let $p \mid w$ be a prime number. Assume that $\nu_{(1,1,1)}(t_R) > (2^{n-j}-1)(3)$. If $\nu_{(1,1,1)}(t_R) < 2^{n-1}-1$, then $\nu_{(1,1,1)}(t_Q) = \nu_{(1,1,1)}(\phi_d) - \nu_{(1,1,1)}(t_R) \geq 2^{n-1}-1$. We write R and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (R_s + R_{s-1} + \cdots + R_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where R_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = R_sQ_t,$$

and

$$\phi_{2^{n-j}e} = R_sQ_{t-a} + R_{s-a}Q_t.$$

Then we have $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = (2^{n-j}-1)(3) \geq \min(\nu_{(1,1,1)}(R_sQ_{t-a}),\ \nu_{(1,1,1)}(R_{s-a}Q_t)) > (2^{n-j}-1)(3)$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \geq 2^{n-1}-1$.

Assume that $\nu_{(1,1,1)}(t_R) \geq 2^{n-1}-1$. If $p=2$, then we have

$$R(X,Y,Z) = V_1(X,Y,Z)V_2(X,Y,Z)$$

where $V_1(X,Y,Z), V_2(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$ are conjugates. Therefore $\deg(V_1) = \deg(V_2)$, thus by Lemma 27 $\nu_{(1,1,1)}(t_{V_1}) = \nu_{(1,1,1)}(t_{V_2}) \geq 2^{n-2}-1$. Define $A(X,Y,Z) = V_1(X,Y,Z)$ and $B(X,Y,Z) = V_2(X,Y,Z)Q(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_{2^{n-j}e} = A_s B_{t-a} + A_{s-a} B_t.$$

Then we have $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = (2^{n-j}-1)(3) \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}),\ \nu_{(1,1,1)}(A_{s-a}B_t)) > 2^{n-2}-1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \leq (2^{n-j}-1)(3)$.

If $p > 3$, then we have

$$R(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^p}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ thus by Lemma 27 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1}-1)/p$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$R(X,Y,Z) = \prod_{i=1}^{p} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = \prod_{i=1}^{(p-1/2)} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = Q(X,Y,Z) \cdot \prod_{i=(p-1)/2+1}^{p} \gamma^i(H(X,Y,Z))$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_{2^{n-j}e} = A_s B_{t-a} + A_{s-a} B_t.$$

Notice that $\nu_{(1,1,1)}(A_s) \geq \frac{p-1}{2}(\frac{2^{n-1}-1}{p}) \geq \frac{p-1}{p}(2^{n-2}-1) \geq \frac{4}{5}(2^{n-2}-1) = \frac{2^n-4}{5} > (2^{n-4}-1)(3) \geq (2^{n-j}-1)(3)$. Moreover, $\nu_{(1,1,1)}(B_t) > \nu_{(1,1,1)}(A_s)$. Then we have $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = (2^{n-j}-1)(3) \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}),\ \nu_{(1,1,1)}(A_{s-a}B_t))$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \leq (2^{n-j}-1)(3)$.

If $p = 3$, then we have

$$R(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^3}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$ thus by Lemma 27 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1}-1)/3$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$R(X,Y,Z) = \prod_{i=1}^{3} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = \prod_{i=1}^{2} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = Q(X,Y,Z)\ \gamma^3(H(X,Y,Z))$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_{2^{n-j}e} = A_s B_{t-a} + A_{s-a} B_t.$$

Notice that $\nu_{(1,1,1)}(A_s) \geq (\frac{2^n-2}{3}) > (2^{n-4}-1)(3) \geq (2^{n-j}-1)(3)$. Let $c = \nu_{(1,1,1)}(t_Q)$, then $\nu_{(1,1,1)}(B_t) = c + \frac{2^n-2-c}{3} = \frac{2^n-2}{3} + \frac{2c}{3} > (2^{n-4}-1)(3) \geq (2^{n-j}-1)(3)$. Then we have $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = (2^{n-j}-1)(3) \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) > (2^{n-j}-1)(3)$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \leq (2^{n-j}-1)(3)$.

□

Proposition 29. Let $f(X) = x^d + h(X)$, where $d = 2^{2n} - 2^n + 1$ $\deg(h) = 2^{n-j}e$, $e \equiv 3 \pmod 4$ and $j \geq 4$. If n is not prime, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

If $\phi_f(X,Y,Z)$ is irreducible then by Theorem 65 $\phi_f(X,Y,Z)$ is absolutely irreducible. Let $\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z)$, where $R_a(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is irreducible for $a = 1,\ldots,k$. If for some $b \in \{1,\ldots,k\}$ $t_{R_b}(X,Y,Z)$ contains two irreducible factors $W_1(X,Y,Z)$, $W_2(X,Y,Z)$ such that $m(W_1) = p_1$, $m(W_2) = p_2$, and $(p_1,p_2) = 1$, then $\phi_f(X,Y,Z)$ is absolutely irreducible by Theorem 65. If one of the $R_a(X,Y,Z)$ is absolutely irreducible then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor. Therefore, we can assume that $m(t_{R_a}) > 1$ for all $a \in \{1,\ldots,k\}$. By lemma 31 $\nu_{(1,1,1)}(t_{R_a}) < (2^{n-j}-1)(3)$. Let k_1 be the least integer such that $\nu_{(1,1,1)}(\prod_{i=1}^{k_1} t_{R_i}) > (2^{n-j}-1)(3)$. By the definition of k_1 we have that $\nu_{(1,1,1)}(\prod_{i=1}^{k_1-1} t_{R_i}) < (2^{n-j}-1)(3)$ and by Lemma 31 $\nu_{(1,1,1)}(t_{R_{k_1}}) < (2^{n-j}-1)(3)$. Therefore, $\nu_{(1,1,1)}(\prod_{i=1}^{k_1} t_{R_i}) < (2^{n-j+1}-1)(3) < 2^{n-1}-1$. Similarly $\nu_{(1,1,1)}(\prod_{i=k_1+1}^{k} t_{R_i}) = 2^n - 2 - \nu_{(1,1,1)}(\prod_{i=1}^{k_1} t_{R_i}) \geq 2^n - 2 - 2^{n-1} + 1 = 2^{n-1} - 1$.

Define $P(X,Y,Z) = \prod_{i=1}^{k_1} R_i$ and $Q(X,Y,Z) = \prod_{i=K_1+1}^{k} R_i$. We write P and Q as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_s Q_t,$$

and

$$\phi_{2^{n-j}e} = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = (2^{n-j}-1)(3) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}),\ \nu_{(1,1,1)}(P_{s-a}Q_t)) > (2^{n-j}-1)(3)$ which is a contradiction.

□

Theorem 67. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^{2n} - 2^n + 1$ $\deg(h) = 2^{n-j}e$, $e \equiv 3 \pmod 4$ and $j \geq 4$. Then, $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Lemma 32. Let $f(X) = x^d + h(X)$, where $d = 2^{2n} - 2^n + 1$, $e = \deg(h)$ and $\nu_{(1,1,1)}(\phi_e) < 2^{n-2} - 1$. Then every irreducible factor $R(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ of $\phi_f(X,Y,Z)$ is either absolutely irreducible or $\nu_{(1,1,1)}(t_R) < 2^{n-2}$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Let $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z), Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ non constant polynomials and $P(X,Y,Z)$ be irreducible. If $m(P) = 1$, then $P(X,Y,Z)$ is absolutely irreducible. Therefore, $m(P) > 1$. It is enough to show that for every $m(P) = p$, p prime the condition is satisfied. Assume that $2^{n-2} - 1 < \nu_{(1,1,1)}(t_P) < 2^{n-1} - 1$. We write $P(X,Y,Z)$ and $Q(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = P_sQ_t,$$

and

$$\phi_e = P_sQ_{t-a} + P_{s-a}Q_t.$$

Since $\nu_{(1,1,1)}(t_P) < 2^{n-1} - 1$, then $\nu_{(1,1,1)}(t_Q) = \nu_{(1,1,1)}(\phi_d) - \nu_{(1,1,1)}(t_P) \geq 2^{n-1} - 1$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2} - 1 \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}),\ \nu_{(1,1,1)}(P_{s-a}Q_t)) > 2^{n-2} - 1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \geq 2^{n-1} - 1$. Assume that $\nu_{(1,1,1)}(t_R) \geq 2^{n-1} - 1$.

If $p = 2$, then we have

$$P(X,Y,Z) = V_1(X,Y,Z)V_2(X,Y,Z)$$

where $V_1(X,Y,Z), V_2(X,Y,Z) \in \mathbb{F}_{q^2}[X,Y,Z]$ are conjugates. Define $A(X,Y,Z) = V_1(X,Y,Z)$ and $B(X,Y,Z) = V_2(X,Y,Z)Q(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = A_sB_t,$$

and

$$\phi_e = A_sB_{t-a} + A_{s-a}B_t.$$

Since V_1, V_2 are conjugates then $\deg(V_1) = \deg(V_2)$, thus by Lemma 27 $\nu_{(1,1,1)}(t_{V_1}) = \nu_{(1,1,1)}(t_{V_2}) \geq 2^{n-2}$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2}-1 \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) > 2^{n-2} - 1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \leq 2^{n-2} - 1$.

If $p > 3$, then we have

$$P(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^p}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$, thus by Lemma 27 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1} - 1)/p$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$P(X,Y,Z) = \prod_{i=1}^{p} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = Q(X,Y,Z)\prod_{i=1}^{(p-1/2)} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = \prod_{i=(p-1)/2+1}^{p} \gamma^i(H(X,Y,Z))$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write $A(X,Y,Z)$ and $B(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s + t = d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_e = A_s B_{t-a} + A_{s-a} B_t.$$

Notice that $\nu_{(1,1,1)}(B_t) \geq (2^{n-1}-1)/2 \geq 2^{n-2}$. Computing $\nu_{(1,1,1)}(A_s)$, we obtain $\nu_{(1,1,1)}(A_s) = \frac{p-1}{2p}(2^n - 2 - \nu_{(1,1,1)}(t_Q)) + \nu_{(1,1,1)}(t_Q) = \frac{(p-1)(2^{n-1}-1)}{p} + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) \geq \frac{4}{5}(2^{n-1} - 1) + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) = \frac{2^{n+1}-4}{5} + \frac{p+1}{2p}\nu_{(1,1,1)}(t_Q) \geq 2^{n-2}$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2} - 1 \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}), \nu_{(1,1,1)}(A_{s-a}B_t)) \geq 2^{n-2} > 2^{n-2} - 1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_P) \leq 2^{n-2} - 1$.

If $p = 3$, then we have

$$P(X,Y,Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)} \sigma(H(X,Y,Z))$$

where $H(X,Y,Z) \in \mathbb{F}_{q^3}[X,Y,Z]$. Therefore $\deg(\alpha(H)) = \deg(\beta(H))$, for all $\alpha, \beta \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$ thus by Lemma 27 $\nu_{(1,1,1)}(t_{\alpha(H)}) = \nu_{(1,1,1)}(t_{\beta(H)}) \geq (2^{n-1} - 1)/3$. Let $\gamma \in Gal(\mathbb{F}_{q^p}/\mathbb{F}_q)$ be a generator. Then,

$$P(X,Y,Z) = \prod_{i=1}^{3} \gamma^i(H(X,Y,Z))$$

Define $A(X,Y,Z) = \prod_{i=1}^{2} \gamma^i(H(X,Y,Z))$ and $B(X,Y,Z) = Q(X,Y,Z)H(X,Y,Z)$, then $\phi_f(X,Y,Z) = A(X,Y,Z)B(X,Y,Z)$. We write A and B as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (A_s + A_{s-1} + \cdots + A_0)(B_t + B_{t-1} + \cdots + B_0),$$

where A_j and B_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = A_s B_t,$$

and

$$\phi_e = A_s B_{t-a} + A_{s-a} B_t.$$

Notice that $\nu_{(1,1,1)}(A_s) \geq \frac{2}{3}(2^{n-1}-1) = (\frac{2^n-2}{3}) > 2^{n-2}-1$. Let $c = \nu_{(1,1,1)}(t_Q)$, then $\nu_{(1,1,1)}(B_t) = c + \frac{2^n-2-c}{3} = \frac{2^n-2}{3} + \frac{2c}{3} > (2^{n-4}-1)(3) \geq (2^{n-j}-1)(3)$. Then we have $\nu_{(1,1,1)}(\phi_e) \leq 2^{n-2}-1 \geq \min(\nu_{(1,1,1)}(A_s B_{t-a}), \nu_{(1,1,1)}(A_{s-a} B_t)) \geq 2^{n-2} > 2^{n-2}-1$, which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_R) \leq 2^{n-2}-1$.

□

Theorem 68. Let $f(X) = x^d + h(X)$, where $d = 2^{2n} - 2^n + 1$, $e = \deg(h)$ and $\nu_{(1,1,1)}(\phi_e) < 2^{n-2}-1$. Then every irreducible factor $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Assume that $\phi_f(X,Y,Z)$ is irreducible, then by lemma 32 $\phi_f(X,Y,Z)$ is absolutely irreducible. Suppose that

$$\phi_f(X,Y,Z) = \prod_{i=1}^{k} R_i(X,Y,Z)$$

where $R_i(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is a non-constant irreducible polynomial for $i \in \{1,\ldots,k\}$. If one of the $R_i(X,Y,Z)$ is absolutely irreducible then we are done, so we can assume without loss of generality that every $R_i(X,Y,Z)$ is not absolutely irreducible for $i \in \{1,\ldots,k\}$. By Lemma 32 we have $\nu_{(1,1,1)}(t_{R_i}) < 2^{n-2}$ for every $i \in \{1,\ldots,k\}$. Define $P(X,Y,Z) = \prod_{i=1}^{w} R_i(X,Y,Z)$, where w is the minimum number such that $\nu_{(1,1,1)}(t_P) > 2^{n-2}$ (i.e. $\nu_{(1,1,1)}(\prod_{i=1}^{w-1}(t_{R_i})) < 2^{n-2}$). Define $Q(X,Y,Z) = \prod_{i=w+1}^{k} R_i(X,Y,Z)$. We write $P(X,Y,Z)$ and $Q(X,Y,Z)$ as sums of homogeneous terms:

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0),$$

where P_j and Q_j are zero or homogeneous of degree j, $s+t=d$. Then

$$\phi_d = P_s Q_t,$$

and

$$\phi_e = P_s Q_{t-a} + P_{s-a} Q_t.$$

Notice that $\nu_{(1,1,1)}(P_s) < 2 * (2^{n-2}) = 2^{n-1}$ and $\nu_{(1,1,1)}(Q_t) = 2^n - 2 - \nu_{(1,1,1)}(P_s) \leq 2^n - 2 - (2^{n-1}-1) = 2^{n-1}-1 > 2^{n-2}$. Therefore, $\nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_s Q_{t-a}), \nu_{(1,1,1)}(P_{s-a} Q_t) < 2^{n-2}$ which is a contradiction. Thus, there exists an $i_0 \in \{1,\ldots,k\}$ such that $R_{i_0}(X,Y,Z)$ is absolutely irreducible.

□

4.2. **A generalization of the case** 1 (mod 4).

Theorem 69. Let the Kasami-Welch degree polynomial $f(x) = x^{2^{2k}-2^k+1} + h(x) \in \mathbb{F}_q[x]$, where $d = \deg(h) \equiv 2^{m-1}+1(\pmod{2^m})$. If $d < 2^{2k} - (2^m-1)(2^k) - 1$, $2 \leq m < k-1$ and $(\phi_{2^{2k}-2^k+1}, \phi_d) = 1$, then $\phi(x,y)$ is absolutely irreducible, and $f(x)$ can not be exceptional APN.

Proof: Supposing that $\phi(x,y)$ factors as $P(x,y)Q(x,y)$ and using the same divisibility arguments as before, we get the system:

$$P_sQ_t = \prod P_\alpha(x,y), \quad \alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2, \tag{29}$$

$$P_sQ_{t-e} + P_{s-e}Q_t = a_d\phi_d(x,y) \tag{30}$$

where $s \geq t$ and $s+t = 2^{2k} - 2^k - 2$. Let $p = (1,1)$ and let us consider the following two cases to prove the theorem.
Let $t > (2^m-2)(2^k+1)$. Then using theorem 8 and the fact that P_α are absolutely irreducible polynomials of degree 2^k+1, from Equation 30 we have that $m_p(Q_t) > 2^m-2$, $m_p(P_s) > 2^m-2$. This implies also that $m_p(\phi_d(x,y)) = m_p(P_sQ_{t-e}+P_{s-e}Q_t) \geq \min(m_p(P_s), m_p(Q_t)) > 2^m-2$. Contradicting that $m_p(\phi_d) = 2^m-2$ (for $d \equiv 2^{m-1}(\pmod{2^m})$, $m_p(\phi_d) = 2^m-2$). On the other hand, let $t \leq (2^m-2)(2^k+1)$. Since $d < 2^{2k} - (2^m-1)(2^k) - 1$, then $e > 2^{2k} - 2^k + 1 - (2^{2k} - (2^m-1)(2^k) - 1) > (2^m-2)(2^k+1)$ and $t < e$.
The equation 30 becomes $P_{s-e}Q_t = a_d\phi_d(x,y)$, which contradicts the relatively prime hypothesis. □

Theorem 70. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^{2n} - 2^n + 1$ $e = \deg(h) < d$. If $\nu_{(1,1,1)}(\phi_e) < 2^{n-2}$, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor define over $\mathbb{F}_q$.

Proof: If $\phi_d(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ contains an absolutely irreducible factor defined over $\mathbb{F}_q[X,Y,Z]$, then by lemma 19 $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. Without loss of generality we can assume that $\phi_d(X,Y,Z)$ do not contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Suppose that $\phi_f(X,y,Z)$ is irreducible over $\mathbb{F}_q$. By Lemma 6, there exist an integer $r \geq 1$, $c \in \mathbb{F}_q$ and an absolutely irreducible polynomial $h(X,Y,Z) \in \mathbb{F}_{q^r}[X,Y,Z]$ such that

$$\phi_f(X,Y,Z) = c\prod_{i=1}^{r} \sigma(h(X,Y,Z), \tag{31}$$

where σ is a generator of $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$. If r is even then define $P(X,Y,Z) = \prod_{i=1}^{r/2} \sigma^i(h(X,Y,Z))$ and $Q(X,Y,Z) = \prod_{i=r/2+1}^{r} \sigma^i(h(X,Y,Z))$. Substituting $P(X,Y,Z)$ and $Q(X,Y,Z)$ in Equation 31 and writing $P(X,Y,Z)$, $Q(X,Y,Z)$ as the sum of homogeneous terms we obtain

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0), \tag{32}$$

where P_i is either a form of degree i or 0 (respectively Q_j is either a form of degree j or 0). By the factorization given in Equation 2 we have $(P_s, Q_t) = 1$. Equating the terms of degree $s+t-1$, we get $P_sQ_{t-1} + P_{s-1}Q_t = 0$, which implies that $P_{s-1} = Q_{t-1} = 0$ (since P_s, Q_t are relatively prime and $P_s \mid P_{s-1}Q_t$). In the same fashion, equating the terms of degree $s+t-2, s+t-3, ..., e-2$ we get $P_{s-1} = Q_{t-1} = 0, P_{s-2} = Q_{t-2} = 0, P_{s-3} = Q_{t-3} = 0, ..., P_{s-(a-1)} = Q_{t-(a-1)} = 0$. We obtain the following system of equations:

$$\phi_d(X,Y,Z) = P_sQ_t \tag{33}$$

and

$$\phi_e(X,Y,Z) = P_sQ_{t-a} + P_{s-a}Q_t \tag{34}$$

By Lemma 6 $\deg(\alpha(h)) = \deg(\beta(h))$, which implies that $\deg(P) = \deg(Q)$ (i.e $s = t$) and by Lemma 27 we have $\nu_{(1,1,1)}(P_s) = \nu_{(1,1,1)}(Q_t) = 2^{n-1} - 1$. We have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) \geq 2^{n-1} - 1$ which is a contradiction. Therefore, r can not be even.

Assume that r is odd. If $r = 1$, then $\phi_f(X, Y, Z)$ is absolutely irreducible. If $r = 3$, define $P(X, Y, Z) = \sigma(h(X, Y, Z)$ and $Q(X, Y, Z) = \sigma^2(h(X, Y, Z))\sigma^3(h(X, Y, Z))$. Using the same factorization as in Equations 32, 33 and 34. By Lemma 6 and Lemma 27 we have $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s) = (2^n-2)/3 \geq 2^{n-2}$. We have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) \geq (2^n - 2)/3$ which is a contradiction.

If $r > 3$, define $P(X, Y, Z) = \prod_{i=1}^{(r-1)/2} \sigma^i(h(X, Y, Z))$ and $Q(X, Y, Z) = \prod_{i=(r-1)/2+1}^{r} \sigma^i(h(X, Y, Z))$. Using the same factorization as in Equations 32, 33 and 34. By Lemma 6 and Lemma 27 we have $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s) = \frac{r-1}{2}\frac{2^n-2}{r} > \frac{2}{3}(2^{n-1} - 1) = \frac{2^n-2}{3}$. Therefore, we have the same contradiction as in the previous case. Hence, if $\phi_f(X, Y, Z)$ is irreducible then $\phi_f(X, Y, Z)$ is absolutely irreducible.

Assume that $\phi_f(X, Y, Z)$ is reducible over $\mathbb{F}_q$, then let

$$\phi_f(X, Y, Z) = \prod_{j=1}^{m} R_j(X, Y, Z), \tag{35}$$

where $R_i(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ is irreducible over $\mathbb{F}_q$ for $i = 1, \ldots, m$ and $\nu_{(1,1,1)}(t_{R_i}) \geq \nu_{(1,1,1)}(t_{R_k})$, whenever $i \leq k$. If $\nu_{(1,1,1)}(t_{R_1}) < 2^{n-2}$, then define $P(X, Y, Z) = \prod_{i=1}^{\ell} R_i(X, Y, Z)$, where ℓ is the least integer such that $\sum_{i=1}^{\ell} \nu_{(1,1,1)}(t_{R_i}) \geq 2^{n-2}$. Define $Q(X, Y, Z) = \prod_{i=\ell+1}^{m} R_i(X, Y, Z)$. Using the same factorization as in Equations 32, 33 and 34. By the definition of ℓ we have $\nu_{(1,1,1)}(P_s) = \sum_{i=1}^{\ell} \nu_{(1,1,1)}(t_{R_i}) \geq 2^{n-2}$. Similarly, by the definition of ℓ we also have $\nu_{(1,1,1)}Q_t > 2^{n-2}$. We have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) > 2^{n-2}$ which is a contradiction. Therefore, $\nu_{(1,1,1)}(t_{R_1}) \geq 2^{n-2}$.

If $\sum_{i=2}^{m} \nu_{(1,1,1)}(t_{R_i}) \geq 2^{n-2}$, then define $P(X, Y, Z) = R_1(X, Y, Z)$ and $Q(X, Y, Z) = \prod_{i=2}^{m} R_i(X, Y, Z)$. Using the same factorization as in Equations 32, 33 and 34 we obtain that $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) \geq 2^{n-2}$ which is a contradiction. Therefore, we can assume that $\sum_{i=2}^{m} \nu_{(1,1,1)}(t_{R_i}) < 2^{n-2}$.

By Lemma 6 there exists an integer $r \geq 1$, $c \in \mathbb{F}_q$ and an absolutely irreducible polynomial $h(X, Y, Z) \in \mathbb{F}_{q^r}[X, Y, Z]$ such that

$$R_1(X, Y, Z) = c \prod_{i=1}^{r} \sigma(h(X, Y, Z), \tag{36}$$

where σ is a generator of $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$. If r is even then define $P(X, Y, Z) = \prod_{i=1}^{r/2} \sigma^i(h(X, Y, Z))$ and $Q(X, Y, Z) = (\prod_{i=r/2+1}^{r} \sigma^i(h(X, Y, Z)))(\prod_{i=2}^{m} R_i(X, Y, Z))$. Using the same factorization as in Equations 32, 33 and 34. By Lemma 6 and Lemma 27 we have $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s) > \frac{1}{2}(2^{n-1} - 1) > 2^{n-2}$. We have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) > 2^{n-2}$ which is a contradiction. Therefore, we can assume r is odd.

If $r = 1$, then $R_1(X, Y, Z)$ is absolutely irreducible. Assume that $r > 3$. Define $P(X, Y, Z) = \prod_{i=1}^{(r-1)/2} \sigma^i(h(X, Y, Z))$ and

$Q(X,Y,Z) = (\prod_{i=(r-1)/2+1}^{r} \sigma^i(h(X,Y,Z)))(\prod_{i=2}^{m} R_i(X,Y,Z))$. Using the same factorization as in Equations 32, 33 and 34. By Lemma 6 and Lemma 27 we have $\nu_{(1,1,1)}(Q_t) > \nu_{(1,1,1)}(P_s) > \frac{r-1}{2}\frac{2^n-2^{n-2}-2}{r} > \frac{2^n-2^{n-2}-2}{3} > 2^{n-2}-1$. Therefore, we have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_s$ 2^{n-2} which is a contradiction.

If $r = 3$, define $P(X,Y,Z) = \prod_{i=1}^{2} \sigma^i(h(X,Y,Z))$ and $Q(X,Y,Z) = \sigma^3(h(X,Y,Z))(\prod_{i=2}^{m} R_i(X,Y,Z))$. Using the same factorization as in Equations 32, 33 and 34. By Lemma 6 and Lemma 27 we have $\nu_{(1,1,1)}(P_s) \geq \frac{2}{3}(2^n - 2^{n-2}) = 2^{n-1}$. Let $c = \nu_{(1,1,1)}(\prod_{i=2}^{m} t_{R_i})$, then $\nu_{(1,1,1)}(Q_t) = \frac{2^n-2-c}{3} + c = \frac{2^n-2}{3} + \frac{2c}{3} > 2^{n-2}$. Therefore, we have $2^{n-2} > \nu_{(1,1,1)}(\phi_e) \geq \min(\nu_{(1,1,1)}(P_sQ_{t-a}), \nu_{(1,1,1)}(P_{s-a}Q_t)) \geq 2^{n-2}$ which is a contradiction. Thus, $R_1(X,Y,Z)$ is absolutely irreducible. □

Corollary 23. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^{2n} - 2^n + 1$ $e = \deg(h) = 2^j\ell + 1 < d$. If $(\ell, 2^n - 1) = 2^n - 1$, then $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: Notice that $j \leq n-1$, otherwise $\deg(h) \geq \deg(f)$ which is a contradiction. If $j < n-1$, then $\nu_{(1,1,1)}(\phi_e) = 2^j - 2 \leq 2^{n-2} - 2$. By Theorem 70 $\phi_f(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$. If $j = n-1$, then $\ell = 2^n - 1$, i.e. $e = 2^{n-1}(2^n-1) + 1 = 2^{2n-1} - 2^{n-1} + 1$. Let $\psi(X,Y,Z) = (\phi_d, \phi_h)$ and $p = \deg(\psi)$. Define,

$$\rho(X,Y,Z) = \frac{\phi(X,Y,Z)}{\psi(X,Y,Z)},$$

then writing $\rho(X,Y,Z)$ as the sum of homogeneous terms we obtain,

$$\rho(X,Y,Z) = \frac{\phi_d}{\psi} + c_e\frac{\phi_e}{\psi} + c_{e-1}\frac{\phi_{e-1}}{\psi} \cdots + c_5.\frac{\phi_5}{\psi}$$

Notice that $\deg(\frac{\phi_e}{\psi}) = 2^{2n-1} - 2^{n-1} - 2 - p < \frac{2^{2n}-2^n-2-p}{2} = \deg(\rho)$. Therefore, by Lemma 18 $\rho(X,Y,Z)$ is absolutely irreducible. Therefore, $\phi(X,Y,Z)$ contain an absolutely irreducible factor defined over $\mathbb{F}_q$.

□

Theorem 71. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^{2n} - 2^n + 1$ $e = \deg(h) < d$. If $e \equiv 1 \pmod 4$, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof: This follows directly from Theorem 36 and Corollary 23 □

Theorem 72. Let $f(X) = x^d + h(X) \in \mathbb{F}_q[X]$, where $d = 2^{2n} - 2^n + 1$ $e = \deg(h) < d$. If e is odd, then $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

5. New Results in the Even Degree case of the Exceptional APN Conjecture

This chapter is divided into two sections. The first section, work in the case when the degree of the polynomial is on the form $2^n e$, where $n \geq 3$ and $e > 1$ odd. This section is divided again into two subsections. The first section address the case when e is either Gold or Kasami-Welch exponent. We gave a factorization characterization when $\deg(h) \equiv 3 \pmod 4$ (see Lemma 33). Then we gave a conditional proof of the general case when certain conditions are met (see). In the second section we proof that is the highest odd degree term is $\equiv 3 \pmod 4$ then $\phi_f(X, y, Z)$ contain an absolute irreducible factor defined over $\mathbb{F}_q$.

we use the concept of degree gap to provide bounds to guarantee the existence of absolute irreducible factors. Later in the next two sections this bounds will be improve using the multiplicity of the point $(1, 1, 1)$ to give an upper bound in the number of factors $\phi_f(X, Y, Z)$ can have in the remaining open cases in the literature. In the second section we prove the case when the second term have odd degree. We use 17 develop in the previous chapter to proof the remaining cases in the literature.

5.1. **Case $2^n e$.**

Theorem 73. Let $f(X) = X^{2^n e} + h(X) \in \mathbb{F}_q[x]$, where e is an odd number no Gold or Kasami-Welch. If $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$, then $\phi_f(X, Y, Z)$ it is absolutely irreducible.

Proof: Suppose $\phi_f(X, Y, Z)$ is irreducible, then by corollary 11 $\phi_f(X, Y, Z)$ is absolutely irreducible. □

5.1.1. *Factorization for some cases of the form $2^n e$ where e is a Gold or a Kasami-Welch number.*

Theorem 74. Let $f(X) = X^{2^n e} + h(X) \in \mathbb{F}_q[x]$ and $n > 2$. If $\deg(h(X)) = 2^n e - 1$ then $\phi_f(X, Y, Z)$ is absolutely irreducible.

Proof: Assume that $\phi_f(X, Y, Z) = PQ$ where P, Q are non-constant polynomials. We can write P, Q as the sum of homogeneous polynomials, let

$$\phi_f(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_r + Q_{r-1} + \cdots + Q_0)$$

where P_i is either a form of degree i or 0 (respectively Q_j is either a form of degree i or 0). Now we have that $\phi_{2^n e} = P_s Q_r$ and $\phi_{2^n e-1} = P_s Q_{r-1} + P_{s-1} Q_r$. Since $(1, 1, 1)$ is a rational point for every absolutely irreducible factor of $\phi_{2^n e}(X, Y, Z)$ ([34], [12]) we have that $(1, 1, 1)$ is a rational point for P_s and Q_r then it is also a rational point of $\phi_{2^n e-1}(X, Y, Z)$ but this is a contradiction to a result from [34] which implies that $(1, 1, 1)$ is not a rational point for $\phi_h(X, Y, Z)$, when $h \equiv 3 \pmod 4$ (In this case $\phi_h(X, Y, Z)$ correspond to the monomial X^h). Therefore, $\phi_f(X, Y, Z)$ is absolutely irreducible. □

Lemma 33. Let $f(X) = X^{2^n e} + h(X) \in \mathbb{F}_q[x]$, where $d = \deg(h) \equiv 3 \, mod \, 4$, $3 < e < 2^n e - 1$. If $\phi_f(X, Y, Z)$ factors then each highest degree form of each factor is divisible by ϕ_e and $\phi_6(X, Y, Z)$.

Proof: Suppose that $\phi_f(X,Y,Z) = PQ$ where P, Q are non-constant polynomials. We can write P, Q as the sum of homogeneous polynomials, let

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_r + Q_{r-1} + \cdots + Q_0)$$

where P_i is either a form of degree i or 0 (respectively Q_j is either a form of degree i or 0). We have that $\phi_{2^n e} = P_s Q_r$. Assume that there exists an absolutely irreducible factor L from $\phi_{2^m e}$ such that $L \mid Q_r$ and $L \nmid P_s$. First we will show that if

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

for every $k = \{1, 2, \dots, m\}$ then $L \mid Q_{r-m+i}$ for every $i \in \{0, 1, 2 \dots, m\}$. In order to prove this we will do strong induction over k.

Case $k = 1$**:** We have

$$\sum_{i=0}^{1} P_{s-i} Q_{r-k+i} = P_s Q_{r-1} + P_{s-1} Q_r = 0.$$

Then $P_s Q_{r-1} = P_{s-1} Q_r$ and $L \mid P_s Q_{r-1}$. Since $L \nmid P_s$ and L is absolutely irreducible we can conclude that $L \mid Q_{r-1}$.

Induction Hypothesis: Suppose that for every $k < m$ we have that

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

then $L \mid Q_{r-k}$ for every $k < m$.

Case $k = m$**:** We have that

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

for every $k \leq m$. For $k = m$ we have

$$\sum_{i=0}^{m} P_{s-i} Q_{r-k+i} = 0$$

so we obtain;

$$P_s Q_{r-m} = \sum_{i=1}^{m} P_{s-i} Q_{r-k+i}.$$

By induction hypothesis we have that $L \mid Q_{r-k}$ for every $k < m$. So we can rewrite it as

$$P_s Q_{r-m} = LR$$

where $R = \frac{\sum_{i=1}^{m} P_{s-i} Q_{r-k+i}.}{L}$. Since $L \nmid P_s$ and L is absolutely irreducible we can conclude that $L \mid Q_{r-m}$.

Now $\phi_d(X,Y,Z) = \sum_{i=0}^{t} P_{s-i} Q_{r-t+i}$. By the previous argument we have that $L \mid Q_{r-t+i}$ for every $1 < i \leq t$. So we can write $\phi_d(X,Y,Z) = P_s Q_{r-t} + \sum_{i=1}^{t} P_{s-i} Q_{r-t+i} = P_s Q_{r-t} + LR_0$. Since $(1,1,1)$ is a rational point for every absolutely irreducible factor of $\phi_{2^n e}(X,Y,Z)$ ([34], [12]) we have that $(1,1,1)$ is a rational point for P_s and L then it is also a rational point of

$\phi_d(X,Y,Z)$ but this is a contradiction to a result from [34] which implies that $(1,1,1)$ is not a rational point for $\phi_d(X,Y,Z)$, when $d \equiv 3 \pmod 4$. □

5.1.2. *Even-Gold and Even Kasami-Wech cases.*

Theorem 75. Let $f(X) = X^{2^m e} + h(X)$, where $e = 2^j + 1$ or $e = 2^{2j} - 2^j + 1$ with j containing a prime number p in his factorization such that $p \nmid 2^m - 1$. If $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$ then $\phi_f(X,Y,Z)$ is absolutely irreducible.

Proof: Suppose $\phi_f(X,Y,Z)$ is irreducible over $\mathbb{F}_q$. Notice that $\phi_e(X,Y,Z)$ contains a reduced irreducible factor $R(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ such that $(m(R), 2^m - 1) = 1$. Therefore, by corollary 11 $\phi_f(X,Y,Z)$ is absolutely irreducible. □

Theorem 76. Let $f(X) = X^{2^n e} + h(X) \in \mathbb{F}_q[X]$, where $e, d = \deg(h) \equiv 3 \pmod 4$ and $n \geq 2$. If $R(X,Y,Z)$ is a factor of $\phi_f(X,Y,Z)$, then either $R(X,Y,Z)$ is absolutely irreducible or $t_R(X,Y,Z)$ is divisible by $\phi_6(X,Y,Z) \cdot \phi_e(X,Y,Z)$.

Proof: Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $P(X,Y,Z)$, $Q(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$. If $t_p(X,Y,Z)$ (respectively $t_Q(X,Y,Z)$) contains a reduced absolutely irreducible term, then by Corollary 5 $P(X,Y,Z)$ contains an absolutely irreducible factor (respectively $Q(X,Y,Z)$). We can assume $t_p(X,Y,Z)$ and $t_Q(X,Y,Z)$ do not contains any reduced absolutely irreducible terms. Without loss of generality let $A = A(X,Y,Z)$ be an absolutely irreducible factor such that $A(X,Y,Z) \mid t_P(X,Y,Z)$ but $A \nmid t_Q(X,Y,Z)$. Writing $P(X,Y,Z)$ and $Q(X,Y,Z)$ as the sum of homogeneous terms we obtain

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0)$$

where P_i and Q_i are either homogeneous polynomials of degree i or 0. Then

$$\phi_{2^n e}(X,Y,Z) = P_s Q_t$$

and

$$\phi_d(X,Y,Z) = \sum_{i=0}^{r} P_{s-i} Q_{t-r+i} \tag{37}$$

Now equating the terms of degree $2^n e - 4$ we obtain $0 = P_s Q_{t-1} + P_{s-1} Q_t$, i.e. $P_s Q_{t-1} = P_{s-1} Q_t$. Notice that $A^2 \mid \phi_{2^n e}(X,Y,Z)$ and $(A, Q_t) = 1$ implies that $A^2 \mid P_s$. Also, $(A, Q_t) = 1$ and $A^2 \mid P_s$, implies that $A^2 \mid P_{s-1}$. Now we can continue this process to obtain that $A^2 \mid P_{s-j}$ for $j = 0, 1, \ldots, r-1$. So we can rewrite Equation 37 as

$$\phi_d(X,Y,Z) = A^2(W) + Q_t P_{s-r}$$

By Bezout's Theorem there exists at least one point $a \in \overline{\mathbb{F}_q}$ such that $\nu_a(A) \geq 1$ and $\nu_a(Q_t) \geq 1$. Since Q_t do not contain any reduced absolutely irreducible factor, then $\nu_a(Q_t) \geq 2$. Therefore, $\nu_a(\phi_d) \geq \min(\nu_a(A^2 W), \nu_a(Q_t P_{s-r})) \geq 2$ which is a contradiction with $\phi_d(X,Y,Z)$ being a nonsingular. Thus, we can conclude that either a factor $R(X,Y,Z)$ of $\phi_f(X,Y,Z)$ is absolutely irreducible or $t_R(X,Y,Z)$ is divisible by $\phi_e(X,Y,Z)\phi_6(X,Y,Z)$.

□

Lemma 34. Let $f(X) = X^{2^n e} + h(X) \in \mathbb{F}_q[X]$, where e is Gold or Kasami-Welch, the highest odd degree term of $h(x)$ is $\equiv 3 \pmod 4$ and $n \geq 2$. If $R(X,Y,Z)$ is a factor of $\phi_f(X,Y,Z)$, then $t_R(X,Y,Z)$ is divisible by $\phi_6(X,Y,Z)$.

Proof: Let b be the degree of the highest odd term of $h(x)$. If $\deg(h) \equiv 3 \pmod 4$, then by Lemma 33 the first cone of each factor is divisible by $\phi_e(X,Y,Z)$ and $\phi_6(X,Y,Z)$. Assume that $d = \deg(h) \not\equiv 3 \pmod 4$ i.e. $\deg(h) = 2^m a$, where $m \geq 1$ and a is odd. Suppose that $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$ where P, Q are non-constant polynomials. We can write P, Q as the sum of homogeneous polynomials, let

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_r + Q_{r-1} + \cdots + Q_0)$$

where P_i is either a form of degree i or 0 (respectively Q_j is either a form of degree i or 0). We have that $\phi_{2^n e} = P_s Q_r$. Assume that there exists an absolutely irreducible factor L from ϕ_6 such that $L \mid Q_r$ and $L \nmid P_s$. First we will show that if

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

for every $k = \{1, 2, \ldots, m\}$ then $L \mid Q_{r-m+i}$ for every $i \in \{0, 1, 2 \ldots, m\}$. In order to prove this we will do strong induction over k.

Case $k = 1$: We have

$$\sum_{i=0}^{1} P_{s-i} Q_{r-k+i} = P_s Q_{r-1} + P_{s-1} Q_r = 0.$$

Then $P_s Q_{r-1} = P_{s-1} Q_r$ and $L \mid P_s Q_{r-1}$. Since $L \nmid P_s$ and L is absolutely irreducible we can conclude that $L \mid Q_{r-1}$.

Induction Hypothesis: Suppose that for every $k < m$ we have that

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

then $L \mid Q_{r-k}$ for every $k < m$.

Case $k = m$: We have that

$$\sum_{i=0}^{k} P_{s-i} Q_{r-k+i} = 0$$

for every $k \leq m$. For $k = m$ we have

$$\sum_{i=0}^{m} P_{s-i} Q_{r-k+i} = 0$$

so we obtain;

$$P_s Q_{r-m} = \sum_{i=1}^{m} P_{s-i} Q_{r-k+i}.$$

By induction hypothesis we have that $L \mid Q_{r-k}$ for every $k < m$. So we can rewrite it as

$$P_s Q_{r-m} = LR$$

where $R = \frac{\sum_{i=1}^{m} P_{s-i}Q_{r-k+i}}{L}$. Since $L \nmid P_s$ and L is absolutely irreducible we can conclude that $L \mid Q_{r-m}$.
Now $\phi_d(X,Y,Z) = \sum_{i=0}^{t} P_{s-i}Q_{r-t+i}$. By the previous argument we have that $L \mid Q_{r-t+i}$ for every $1 < i \leq t$. So we can write $\phi_d(X,Y,Z) = P_sQ_{r-t} + \sum_{i=1}^{t} P_{s-i}Q_{r-t+i}$. Since $L \mid \phi_d(X,Y,Z)$ and $L \mid \sum_{i=1}^{t} P_{s-i}Q_{r-t+i}$, then $L \mid P_sQ_{r-t}$ that is $L \mid Q_{r-t}$.

We can continue doing this to obtain that $L \mid Q_{t-j}$ for $j = 1, \ldots, k-1$ and

$$\phi_b(X,Y,Z) = \sum_{i=0}^{k} P_{s-i}Q_{r-k+i}.$$

Now we can rewrite this equation as follows

$$\phi_b(X,Y,Z) = P_sQ_{r-k} + \sum_{i=1}^{k} P_{s-i}Q_{r-k+i}.$$

By our previous argument we have $L \mid \sum_{i=1}^{k} P_{s-i}Q_{r-k+i}$, therefore $\nu_{(1,1,1)}(\sum_{i=1}^{k} P_{s-i}Q_{r-k+i}) \geq 1$ and $\nu_{(1,1,1)}(P_sQ_{t-k}) \geq 1$. Thus, $\nu_{(1,1,1)}(\phi_b) \geq \min(\nu_{(1,1,1)}(\sum_{i=1}^{k} P_{s-i}Q_{r-k+i}), \nu_{(1,1,1)}(P_sQ_{t-k})) \geq 1$ which is a contradiction.

We can conclude that $L \mid P_s$. Therefore, $\phi_6(X,Y,Z)$ divides the first cone of every factor. □

5.2. Case $4e$, when e is a Gold or a Kasami-Welch number.

Theorem 77. Let $f(X) = X^{4e} + h(X) \in \mathbb{F}_q[x]$, where $e > 3$ is Gold or Kasami-Welch number. If $h = \deg(h(X)) \equiv 3 \pmod 4$, then $f(X)$ is not exceptionally APN.

Proof: Assume that $\phi_f(X,Y,Z)$ factor over $\mathbb{F}_q$. Then by lemma 33 we know that $\phi_6(X,Y,Z)\phi_e(X,Y,Z)$ divides the highest degree form of each factor. Since the multiplicity of $\phi_6(X,Y,Z)$ is three we only have two possible options $\phi_f(X,Y,Z)$ factor into three irreducible polynomials over $\mathbb{F}_q$ or ϕ_f factor into two absolutely irreducible polynomials. If ϕ_f factor into three irreducible polynomials. Applying the reverse $\phi_f(X,Y,Z)$ and the factors we obtain by lemma 4 that each factor of $\psi_\phi(X,Y,Z)$ contains an absolutely irreducible factor of multiplicity 1 coming from $\phi_6(X,Y,Z)$. By theorem 42 this factors are absolutely irreducible over $\mathbb{F}_q$. By lemma 13 this implies that $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$. So let assume that $\phi_f(X,Y,Z)$ factor into two different factors. Suppose that $\phi_f(X,Y,Z) = PQ$ where P, Q are non-constant polynomials. We can write P, Q as the sum of homogeneous polynomials, let

$$\phi_f(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_r + Q_{r-1} + \cdots + Q_0)$$

where P_i is either a form of degree i or 0 (respectively Q_j is either a form of degree i or 0). We have that $\phi_{2^ne} = P_sQ_r$. Moreover we have that $\phi_6(X,Y,Z)\phi_e \mid P_s$ and $\phi_6(X,Y,Z)\phi_e \mid Q_r$. Without loss of generality assume that $\phi_6(X,Y,Z)^2 \nmid P_s$, and that $(x+y)^2 \nmid P_s$. Taking the reverse to both sides we obtain that $\psi_\phi(X,Y,Z) = \psi_P\psi_Q$ and by lemma 4 the tangent cone of $\psi_P(X,Y,Z)$ contains an absolutely irreducible factor of multiplicity 1. By theorem 42 this factors are absolutely irreducible over $\mathbb{F}_q$. By lemma 13 this implies that $\phi_f(X,Y,Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

So we can assume that $\phi_f(X, Y, Z)$ is irreducible over $\mathbb{F}_q$. Our goal now is show that $\phi_f(X, Y, Z)$ do not satisfy theorem 40. Assume that there exists an extension such that $\phi_f(X, Y, Z)$ factors into absolutely irreducible factors. Consider the lower extension in which this happens. By lemma 13 $\psi_\phi(X, Y, Z)$ should also factor over this extension. By lemma 4 the tangent cone of $\psi_\phi(X, Y, Z)$ contain an absolutely irreducible factor of multiplicity 3. Using lemma 15 the order of the extension should divide 3 (i.e. the multiplicity of an absolutely irreducible factor). Since 3 is prime we obtain that the extension is of order 3 i.e. we have 3 factors. The first characterization of theorem 40 is not possible since that would contradict lemma 33. The second characterization of theorem 40 is not possible due to the number of factors. Finally, the third characterization of theorem 40 is not possible because each factor has the same first cone up to associates.

Theorem 78. Let $f(X) = X^{4e} + h(X) \in \mathbb{F}_q[X]$, where e is Gold or Kasami-Welch, the highest odd degree term of $h(x)$ is $\equiv 3 \pmod 4$ and $n \geq 2$. Then $\phi_f(X, Y, Z)$ is not exceptional APN.

Proof: Let $\phi_f(X, Y, Z)$ be reducible over $\mathbb{F}_q$, then $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$ $R(X, Y, Z)$, where $P(X, Y, Z), Q(X.Y, Z)$ are non-constant irreducible polynomials and $P(X, Y, Z)$, $Q(X, Y, Z), R(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$. By Lemma 34 $\phi_6(X, Y, Z) \mid t_P(X, Y, Z)$ and $\phi_6(X, Y, Z) \mid t_Q(X, Y, Z)$. Notice that either $\phi_6^2(X, Y, Z) \nmid t_P(X, Y, Z)$ or $\phi_6^2(X, Y, Z) \nmid t_q(X, Y, Z)$. Without loss of generality assume that $\phi_6^2(X, Y, Z) \nmid t_P(X, Y, Z)$, then $t_P(X, Y, Z)$ contains a reduced absolutely irreducible factor defined over $\mathbb{F}_q$. By Corollary 5 $P(X, Y, Z)$ is absolutely irreducible. Therefore, $\phi_f(X, Y, Z)$ is not exceptional APN.

Suppose that $\phi_f(X, Y, Z)$ is irreducible, then by Corollary 6 $3 \mid m(\phi_f)$, that is $m(\phi_f) = 1$ or $m(\phi_f) = 3$. If $m(\phi_f) = 3$, then

$$\phi_f(X, Y, Z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)} \sigma(H(X, Y, Z)), \tag{38}$$

where $H(X, Y, Z) \in \mathbb{F}_{q^3}[X, Y, Z]$ is absolutely irreducible. Now we are going to show that $\phi_f(X, Y, Z)$ do not satisfy neither of the conditions of theorem 40. Clearly by Equation 38 the first cone of every factor must be divisible by $\phi_6(X, Y, Z)\phi_e(X, Y, Z)$. Therefore, conditions 1 and 2 are not satisfied. Moreover, the first cone of every factor is not square free. Therefore, condition 3 is not satisfied. Therefore, $\phi_f(X, Y, Z)$ is not exceptional APN.

□

□

References

[1] Leonard M. Adleman. The function field sieve. In *Algorithmic number theory (Ithaca, NY, 1994)*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 108–121. Springer, Berlin, 1994.

[2] 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 of *Contemp. Math.*, pages 23–31. Amer. Math. Soc., Providence, RI, 2010.

[3] Daniele Bartoli and Kai-Uwe Schmidt. Low-degree planar polynomials over finite fields of characteristic two. *J. Algebra*, 535:541–555, 2019.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[5] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. *J. Cryptology*, 30(3):859–888, 2017.

[6] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[7] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[8] Florian Caullery. A new large class of functions not APN infinitely often. *Des. Codes Cryptogr.*, 73(2):601–614, 2014.

[9] Florian Caullery. Polynomials over finite fields for cryptography. 2014.

[10] Florian Caullery. A divisibility criterion for exceptional APN functions. In *Topics in finite fields*, volume 632 of *Contemp. Math.*, pages 71–82. Amer. Math. Soc., Providence, RI, 2015.

[11] Moisés Delgado. The state of the art on the conjecture of exceptional APN functions. *Note Mat.*, 37(1):41–51, 2017.

[12] Moises Delgado and Heeralal Janwa. On the absolute irreducibility of hyperplane sections of generalized fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional apn functions: the kasami-welch degree case. *arXiv preprint arXiv:1612.05997*, 2016.

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

[14] Moisés Delgado and Heeralal Janwa. On the completion of the exceptional APN conjecture in the Gold degree case and absolutely irreducible polynomials. *Congr. Numer.*, 229:135–142, 2017.

[15] Moises Delgado and Heeralal Janwa. On the conjecture on APN functions and absolute irreducibility of polynomials. *Des. Codes Cryptogr.*, 82(3):617–627, 2017.

[16] Moises Delgado and Heeralal Janwa. Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case. *Adv. Math. Commun.*, 11(2):389–396, 2017.

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

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

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

[20] Gustave Dumas. Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, 2:191–258, 1906.

[21] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, 52(2):744–747, 2006.

[22] G. Eisenstein. Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *J. Reine Angew. Math.*, 39:160–179, 1850.

[23] Eric Férard. On the irreducibility of ϕ_e. *Personal communication*, 2013.

[24] Eric Férard. On the irreducibility of the hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in characteristic 2. *Adv. Math. Commun.*, 8(4):497–509, 2014.

[25] Eric Férard. A infinite class of Kasami functions that are not APN infinitely often. In *Arithmetic, geometry, cryptography and coding theory*, volume 686 of *Contemp. Math.*, pages 45–63. Amer. Math. Soc., Providence, RI, 2017.

[26] Eric Férard, Roger Oyono, and François Rodier. Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 27–36. Amer. Math. Soc., Providence, RI, 2012.

[27] William Fulton. *Algebraic curves. An introduction to algebraic geometry.* W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[28] Shuhong Gao. Absolute irreducibility of polynomials via Newton polytopes. *J. Algebra*, 237(2):501–520, 2001.

[29] Faruk Göloğlu. Almost perfect nonlinear trinomials and hexanomials. *Finite Fields Appl.*, 33:258–282, 2015.

[30] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[31] Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *J. Algebra*, 343:78–92, 2011.

[32] Fernando Hernando and Gary McGuire. Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes. *Des. Codes Cryptogr.*, 65(3):275–289, 2012.

[33] J. W. P. Hirschfeld. *Projective geometries over finite fields.* The Clarendon Press, Oxford University Press, New York, 1979. Oxford Mathematical Monographs.

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

[35] Heeralal Janwa, Gary M. McGuire, and Richard M. Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2). *J. Algebra*, 178(2):665–676, 1995.

[36] David Jedlicka. APN monomials over GF(2^n) for infinitely many n. *Finite Fields Appl.*, 13(4):1006–1028, 2007.

[37] Erich Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput. System Sci.*, 50(2):274–295, 1995. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

[38] Sudesh K. Khanduja and Jayanti Saha. On a generalization of Eisenstein's irreducibility criterion. *Mathematika*, 44(1):37–41, 1997.

[39] Swastik Kopparty and Sergey Yekhanin. Detecting rational points on hypersurfaces over finite fields. In *Twenty-Third Annual IEEE Conference on Computational Complexity*, pages 311–320. IEEE Computer Soc., Los Alamitos, CA, 2008.

[40] Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In *Advances in cryptology—EUROCRYPT '91 (Brighton, 1991)*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 17–38. Springer, Berlin, 1991.

[41] A. K. Lenstra. Factoring multivariate polynomials over finite fields. *J. Comput. System Sci.*, 30(2):235–248, 1985.

[42] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[43] Saunders MacLane. The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals. *Trans. Amer. Math. Soc.*, 43(2):226–239, 1938.

[44] Delgado Moises and Heeralal Janwa. On the decomposition of generalized fermat varieties in p^3 corresponding to kasami-welch functions. *Congress Numerantium*, 2017.

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

[46] François Rodier. Borne sur le degré des polynômes presque parfaitement non-linéaires. In *Arithmetic, geometry, cryptography and coding theory*, volume 487 of *Contemp. Math.*, pages 169–181. Amer. Math. Soc., Providence, RI, 2009.

[47] François Rodier. Functions of degree $4e$ that are not APN infinitely often. *Cryptogr. Commun.*, 3(4):227–240, 2011.

[48] Wolfgang Schmidt. *Equations over finite fields: an elementary approach.* Kendrick Press, Heber City, UT, second edition, 2004.

[49] Igor R. Shafarevich. *Basic algebraic geometry. 2.* Springer-Verlag, Berlin, second edition, 1994. Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.

[50] S. A. Stepanov. Congruences with two unknowns. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:683–711, 1972.

[51] S. A. Stepanov. Rational points of algebraic curves over finite fields. In *Current problems of analytic number theory (Proc. Summer School, Minsk, 1972) (Russian)*, pages 223–243, 272, 1974.

[52] Henning Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

[53] T. Szőnyi. Some applications of algebraic curves in finite geometry and combinatorics. In *Surveys in combinatorics, 1997 (London)*, volume 241 of *London Math. Soc. Lecture Note Ser.*, pages 197–236. Cambridge Univ. Press, Cambridge, 1997.

[54] Da Qing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995. Special issue dedicated to Leonard Carlitz.