On the Decomposition of Generalized Fermat Varieties in P^3 Corresponding to Kasami-Welch Functions

Moisés Delgado, H Janwa

Moisés Delgado

Department of Mathematics
University of Puerto Rico – Cayey Campus
Cayey, Puerto Rico, 00727 USA

Heeralal Janwa

Department of Mathematics, Faculty of Natural Sciences
University of Puerto Rico – Río Piedras Campus
San Juan, Puerto Rico, 00931 USA

Abstract

The study of the generalized Fermat variety $\phi_j = \frac{x^j+y^j+z^j+(x+y+z)^j}{(x+y)(x+z)(y+z)}$ defined over a finite field $L = \mathbb{F}_q$, $q = 2^n$ for some positive integer n, plays an important role in the study of APN functions and exceptional APN functions. This study arouse after a characterization by Rodier that relates these functions with the number of rational points of $\phi_j(x, y, z)$. The more studied cases are when $j = 2^k + 1$ and $j = 2^{2k} - 2^k + 1$, the Gold and Kasami-Welch numbers. In this article we make a claim about the decomposition of ϕ_j into absolutely irreducible components. We show that if these components intersect transversally at a particular point, then the corresponding Kasami-Welch polynomial is absolutely irreducible. Furthermore, this implies that the function is not exceptional APN, thus helping us make progress on the stated conjecture.

Keywords: APN functions, exceptional APN functions, absolutely irreducible polynomials, transversal intersection, exceptional APN conjecture.

2000 Mathematics Subject Classification: 94A60, 20C05, 05B10, 11T71

CONGRESSUS NUMERANTIUM 232 (2019), pp.101-112

1 Introduction

Definition 1. Let $L = \mathbb{F}_q$, with $q = 2^n$ for some positive integer n. A function $f : L \to L$ is said to be *almost perfect nonlinear* (APN) on L if for all $a, b \in L$, $a \neq 0$, the equation

$$f(x+a) - f(x) = b \tag{1}$$

have at most 2 solutions.

APN functions have direct implications in Coding Theory and Cryptography. For a coding approach see [4, 16, 17]. For a cryptographic approach see [18, 19]. The best known examples of APN functions are the Gold functions $f(x) = x^{2^k+1}$ and the Kasami-Welch functions $f(x) = x^{4^k-2^k+1}$, whose names are due to its exponents names, the Gold and Kasami-Welch numbers respectively. These functions are APN on any field $\mathbb{F}_{2^n}$ where k, n are relatively prime integers. A special class of APN functions are called exceptional APN functions.

Definition 2. Let $L = \mathbb{F}_q$, $q = 2^n$ for some positive integer n. A function $f : L \to L$ is called exceptional APN if f is APN on L and also on infinitely many extensions of L.

Aubry, McGuire and Rodier [1] conjectured that, up to equivalence, the Gold and Kasami-Welch functions are the only exceptional APN functions. Many articles have been published since then by many authors, among them [1, 20, 21, 5, 6, 7, 10, 15, 13, 14]. Rodier characterized APN functions as follows [20].

Proposition 1. A function $f : L \to L$ is APN if and only if the rational points of the affine surface

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

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

Given a polynomial function $f \in L[x, y, z]$, $\deg(f) = d$. We define:

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(x+z)(y+z)} \tag{2}$$

2 The Gold and the Kasami-Welch Generalized Fermat Varieties

Janwa and Wilson [16] studied the surface $\phi_j(x, y, z)$ related to the Gold and Kasami-Welch numbers.

For a Gold number $j = 2^k + 1$, the authors proved that ϕ_j decompose into a product of linear factors as:

$$\phi_j(x, y, z) = \prod_{\alpha \in F_{2^k} - F_2} (x + \alpha y + (\alpha + 1)z) \tag{5}$$

For a Kasami-Welch number $t = 2^{2k} - 2^k + 1$, they proved that ϕ_j decompose into a product of absolutely irreducible factors as:

$$\phi_t(x, y, z) = \prod_{\alpha \in \mathbf{F}_{2^k} - \mathbf{F}_2} P_\alpha(x, y, z) \tag{6}$$

where $P_\alpha(x, y, z)$ is absolutely irreducible of degree $2^k + 1$ over $\mathbb{F}_{2^k}$. Furthermore, P_α satisfies $P_\alpha(x, 0, 1) = (x + \alpha)^{2^k+1}$.

ttAs can be seen in (5), ϕ_j factors as a product of different linear factors. Using this fact, several results were found towards the resolution of the conjecture of exceptional APN functions (see [6, 8, 9]). On the other hand, for the factorization in (6), there is not much information about the factors P_α except degrees. We have made some experimentation using MAGMA for the first Kasami-Welch numbers and the following results were obtained.

For j=13, ϕ_j factors into 2 absolutely irreducible factors of degree 5, for j=57, ϕ_j factors into 6 absolutely irreducible factors of degree 9, for j=241, ϕ_j factors into 14 absolutely irreducible factors of degree 17, and for j=993, ϕ_j factors into 30 absolutely irreducible factors of degree 33. This results and some additional evidence we got make us to claim the P_α in (6) intersects transversally at a point and, in the case the claim is true, consequences on the conjecture of exceptional APN functions will be provided in section 4. The main result of this article (theorem 11) implies that this fact help us to establish absolute irreducibility criterion and thus leading to non-exceptional APN results.

3 On the conjecture of exceptional APN functions

The following results towards the conjecture of exceptional APN functions (stated in the introduction) are based mainly on proving that the surface X in (2) is absolutely irreducible, or it has an absolutely irreducible factor, as justified in theorem 1.

Aubry, McGuire and Rodier established that a polynomial function of odd degree is not exceptional APN provided the degree is not a Gold number $(2^k + 1)$ or a Kasami-Welch number $(2^{2k} - 2^k + 1)$. Then, the only open cases for odd degree polynomials are the Gold and Kasami-Welch degree polynomial functions. Next we will state the main results obtained on these two cases.

3.1 On the Gold case

Aubry, McGuire and Rodier proved [1]:

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

They extended the previous theorem with:

Theorem 3. *Suppose $f(x) = x^{2^k+1} + g(x) \in L[x]$ and $\deg(g) = 2^{k-1} + 2$. Let k be odd and relatively prime to n. If $g(x)$ does not have the form $ax^{2^{k-1}+2} + a^2x^3$ 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.*

In [6, 8] we extended these results with the following:

Theorem 4. *For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$, where $\deg(h) < 2^k + 1$, and $\deg(h) \equiv 3 \pmod 4$. Then, $\phi(x, y, z)$ is absolutely irreducible.*

For the case 1 (mod 4), in [6, 8] we also proved:

Theorem 5. *For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $d = \deg(h) \equiv 1 \pmod 4$ and $d < 2^k + 1$. If ϕ_{2^k+1}, ϕ_d are relatively prime, then $\phi(x, y, z)$ is absolutely irreducible.*

Additional complementary results were proven by us in [9, 11] that almost complete the proof of the conjecture for the Gold degree case with the following theorems.

Theorem 6. *For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $\deg(h) = 2^l + 1 < 2^k + 1$. Then, If $(k, l) \neq 1$ and h contains a term of degree m such that $(\phi_{2^k+1}, \phi_m) = 1$, then $\phi(x, y, z)$ is absolutely irreducible and f is not exceptional APN.*

Theorem 7. *For $k_1 \geq 2$, let $f(x) = x^{2^{k_1}+1} + h(x) \in L[x]$ 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 $(k_1, \cdots, k_t) = 1$ and f is not an exceptional APN function. Under the same conditions, if $(k_1, \cdots, k_t) = q > 1$, then ϕ is divisible by ϕ_{2^q+1} and ϕ is not absolutely irreducible.*

In this last theorem, we go further for the case when ϕ is divisible by ϕ_{2^q+1}, by showing that it could happen that ϕ contains an absolutely irreducible factor in this case, consequently f could not be exceptional APN.

3.2 On the Kasami-Welch case

For this case, Rodier proved the following [21]:

Theorem 8. *Suppose that $f(x) = x^{2^{2k}-2^k+1} + g(x) \in L[x]$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exist a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then $\phi(x, y, z)$ is absolutely irreducible.*

Rodier also studied the case when $\deg(g) = 2^{2k-1} - 2^{k-1} + 2$. Very recently, Ferard [14] and Delgado and Janwa [10] simultaneously, independently and using very different methods, improved these Kasami-Welch results. Both articles proved the following:

Theorem 9. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent, d be an integer, $1 \leq d < k_r$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d. If $d \equiv 3(\mod 4)$, then $\phi_f(x, y, z)$ is absolutely irreducible.*

Theorem 10. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent, d an odd integer, $5 \leq d < k_r$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d. Assume that $d \equiv 1(\mod 4)$. We write $d = 1 + 2^j l$ with l an odd integer and j an integer ≥ 2. If $2^r - 1$ does not divide l, then $\phi_f(x, y, z)$ is absolutely irreducible.*

Ferard also studied the case when $d = 2^i t$ with $t \equiv 1(\mod 4)$. Our results will be discussed in the next section.

4 Transversal intersection on the Kasami-Welch variety

The next theorem provides an infinite family of absolutely irreducible polynomials of Kasami-Welch degree k_r provided a especial decomposition exists of ϕ_{k_r} in equation (6). To state the result we recall that two or more curves f_i are said to intersect transversally at a point p if p is a simple point of each f_i and if the tangent lines to f_i at p are pairwise distinct.

Theorem 11. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent, and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d, $1 \leq d < k_r$. If ϕ_{k_r} intersects transversally at a point p that is not in ϕ_d, then $\phi(x, y, z)$ is absolutely irreducible.*

Proof. Supposing, by the way of contradiction (we follow the argument as in [6, 8]), that $\phi(x, y, z)$ factor as $P(x, y, z)Q(x, y, z)$, where P and Q are non constant polynomials. As sums of homogeneous terms, $P = P_s + P_{s-1} + ... + P_0$, $Q = Q_t + Q_{t-1} + ... + Q_0$. Then, we have

$$\sum_{j=3}^{2^{2r}-2^r+1} a_j \phi_j = (P_s + P_{s-1} + ... + P_0)(Q_t + Q_{t-1} + ... + Q_0) \quad (7)$$

where $s + t = 2^{2r} - 2^r - 2$. We can assume that $s \geq t$. Then $2^{2r} - 2^r - 2 > s \geq \frac{2^{2r}-2^r-2}{2} \geq t > 0$. Let $e = 2^{2r} - 2^r + 1 - d$.

From equations (6) and (7):

$$P_sQ_t = \prod P_\alpha(x,y,z), \quad \alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2 \tag{8}$$

Because P_s and Q_t are different absolutely irreducible factors, P_s and Q_t are relatively prime.

By the assumed degree of $g(x)$, the homogeneous terms of degree l, for $d-3 < l < 2^{2r} - 2^r - 2$, are equal to zero. 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 $P_s | P_{s-1}Q_t$). In the same fashion, equating the terms of degree $s+t-2, s+t-3, ..., d-2$ we get $P_{s-1} = Q_{t-1} = 0, P_{s-2} = Q_{t-2} = 0, P_{s-3} = Q_{t-3} = 0, ..., P_{s-(e-1)} = Q_{t-(e-1)} = 0$.

The equation of degree $d-3$ is:

$$P_sQ_{t-e} + P_{s-e}Q_t = a_d\phi_d(x,y,z) \tag{9}$$

By hypothesis on transversal intersection at p, $p \in P_\alpha(x,y,z)$ for all $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$. Then, by the absolute irreducible factorization in (8), $p \in P_s, p \in Q_t$. Then $p \in \phi_d(x,y,z)$ by equation (8). Which is a contradiction. □

As commented at the end of section 2, by using MAGMA, we proved that the components of ϕ_{k_r} in equation (6) intersects transversally at $p = (1,1,1)$ for the cases $k_r = 13, 57, 241, 993$. Using these results and previous results on rational points of $\phi_d(x,y,z)$, we conclude:

Corollary 2. For $k = 993, 241, 57, 13$, let $f(x) = x^k + g(x)$ where $g(x)$ is a polynomial of degree d, $1 \leq d < k$, $d \equiv 3(\mod 4)$. Then ϕ is absolutely irreducible.

Proof. p does not belong to $\phi_d(x,y,z)$ for $d \equiv 3(\mod 4)$, as demonstrated by Janwa and Wilson in [16]. □

Using theoretical arguments on transversal intersection, and analysis of intersection multiplicities, we prove in a future Designs, Codes and Cryptography article (submission in process) the following general result [12]:

Theorem 12. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent, and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d, $1 \leq d < k_r$. If $d \equiv 3(\mod 4)$, then $\phi(x, y, z)$ is absolutely irreducible.*

We also include in [12] an analogous result for $d \equiv 5(\mod 8)$. An important remark is that these results on the Kasami-Welch case were obtained independently by us in [10] and independently and simultaneously, and using completely different methods from Ferard's results in [14]. For more details about this see [10].

References

[1] I. Aubry, G. McGuire, F. Rodier, *A Few More Functions That Are Not APN Infinitely Often*, Finite Fields: Theory and Applications. Contemporary Mathematics.**518** (2010), 23-31.

[2] T. P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, *On almost perfect nonlinear functions over F_{2n}*, IEEE Trans. Inf. Theory **52** (2006), 4160 -4170.

[3] E. Byrne and G. McGuire, *Quadratic binomial APN functions and absolutely irreducible polynomials*, arXiv:0810.4523.

[4] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography,* **15(2)** (1998), 125-156.

[5] F. Caullery, *Polynomial functions of degree 20 which are APN infinitely often*, arXiv:1212.4638v2[cs.IT] (2013).

[6] M. Delgado, H. Janwa, *On The Conjecture on APN Functions*, arXiv:1207.5528v1[cs.IT]. (2012).

[7] M. Delgado, H. Janwa, *Progress Towards the Conjecture on APN Functions and Absolutely Irreducible Polynomials*, arXiv:1602.02576 [math.NT]. (2016).

[8] M. Delgado, H. Janwa, *On the conjecture on APN functions and absolute irreducibility of polynomials*, Designs, Codes and Cryptography. (2016), 1-11.

[9] M. Delgado, H. Janwa, *Some new results on the conjecture on APN functions and absolutely irreducible polynomials. The Gold case*, Advances in mathematics of communications. (2017), 389-395.

[10] M. Delgado, H. Janwa, *On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in P3 and the conjecture on exceptional APN functions: the Kasami-Welch degree case*, arXiv:1612.05997 [math.AG]. (2016).

[11] M. Delgado, H. Janwa, *On the Completion of the Exceptional APN Conjecture in the Gold degree case andon APN Absolutely Irreducible Polynomials* , Congressus Numerantium, **229** (2017), 135-142.

[12] M. Delgado, H. Janwa, *Some new techniques and progress towards the proof of the conjecture on exceptional APN functions and absolute irreducibility of polynomials*, Designs, Codes and Cryptography (May 07, 2019 (in the process of submission)).

[13] E. Ferard, *On the irreducibility of the hyperplane sections of Fermat varieties in P^3 in characteristic 2,* Advances in Mathematics of Communications, **8(4)** (2014).

[14] E. Ferard, *A infinite class of Kasami functions that are not APN infinitely often*, Arithmetic, Geometry, Cryptography and Coding Theory, (2017), 686, 45.

[15] F. Hernando, G. McGuire, *Proof of a Conjecture on Sequence of Excepcional Numbers, classifying cyclic codes and APN functions*, Journal of algebra, **343(1)** 2011, 78-92.

[16] H. Janwa, M. Wilson, *Hyperplane Sections of Fermat Varieties in P^3 in Char. 2 and Some Applications to Cyclic Codes*, In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. (1993), 180-194.

[17] H. Janwa, G. McGuire, M. Wilson, *Double Error-correcting Cyclic Codes and Absolutely Irreducible Polynomials over $GF(2)$*, Journal of Algebra. **178** (1995), 665-676.

[18] K. NYBERG, L. R. KNUDSEN, *Provable security against differential attacks,* Journal of Cryptology. **8** (1995), 27-37.

[19] K. NYBERG, *Differentially uniform mappings for Cryptography,* In Workshop on the Theory and Application of Cryptographic Techniques. (1993), 55-64.

[20] F. RODIER, *Borne sur le degré des polynômes presque parfaitement non-linéaires,* Contemporary Mathematics. **487** (2009), 169-181.

[21] E. FÉRARD, R. OYONO, F. RODIER, *Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents,* Arithmetic, Geometry, Cryptography and Coding Theory. Contemporary Mathematics. **574** (2012), 27-36.