SOME NEW RESULTS ON THE CONJECTURE ON
EXCEPTIONAL APN FUNCTIONS AND ABSOLUTELY
IRREDUCIBLE POLYNOMIALS: THE GOLD CASE

MÓISES DELGADO  
Department of Mathematics  
UPR- Cayey, Puerto Rico (PR), 00736 USA

HEERALAL JANWA  
Department of Mathematics  
UPR-Rio Piedras, San Juan, PR 00931 USA

(Communicated by Andrew Tirkel)

Abstract. An almost perfect nonlinear (APN) function \( f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \) (necessarily polynomial) is called exceptional APN if it is APN on infinitely many extensions of \( \mathbb{F}_{2^n} \). Aubry, McGuire and Rodier conjectured that the only exceptional APN functions are the Gold and the Kasami-Welch monomial functions. They 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 \( (2^{2k} - 2^k + 1) \). When the degree of the polynomial function is a Gold number or a Kasami-Welch number, several partial results have been obtained by several authors including us. In this article we address these exceptions. We almost prove the exceptional APN conjecture in the Gold degree case when \( \deg (h(x)) \) is odd. We also show exactly when the corresponding multivariate polynomial \( \phi(x, y, z) \) is absolutely irreducible. Also, there is only one result known when \( f(x) = x^{2^k + 1} + h(x) \), and \( \deg (h(x)) \) is even. Here, we extend this result as well, thus making progress in this case that seems more difficult.

1. Introduction and background

In this section, we give the necessary background that we use in the article. For a deeper introduction to APN functions and exceptional APN functions, and their applications, we recommend the articles in the bibliography from [1] to [25] and the survey articles [4, 24] and references therein.

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

\[
(1) \quad f(x + a) - f(x) = b
\]

has at most 2 solutions. It is called exceptional APN if it is APN on infinitely many extensions of \( L \).

2010 Mathematics Subject Classification: Primary: 14G50, 11T71; Secondary: 13P10.  
Key words and phrases: Almost perfect nonlinear (APN), cyclic codes, Deligne estimate, Lang-Weil estimate, absolutely irreducible polynomial, CCZ-equivalence, EA-equivalence, Gold function, Kasami function.
Nyberg [23] proved that APN functions have the property of being highly resistant against differential cryptanalytic attacks when they are used as substitution components of block ciphers (S-Boxes).

Much earlier, the motivation for APN functions came by way of research in communication systems in the theory of sequence design and in the design of cyclic codes. Consider the cyclic code of length $2^n - 1$ generated by $C_{s(t)}^m = m_\omega(T)m_{\omega^t}(T)$ where $m_\omega(T)$ (resp. $m_{\omega^t}(T)$) is the minimal polynomial of $\omega$ (resp. $\omega^t$), where $\omega$ is a primitive element of $\mathbb{F}_{2^n}$. These codes had arisen in the context of Preparata and Goethals codes, see [2], and in sequence design [22]. By a result of van Lint and Wilson, these cyclic codes have minimum distance at most 5 when $s \geq 4$. When $t = 2^k + 1$ (a Gold exponent) or $t = 2^{2k} - 2^k + 1$ (a Kasami-Welch exponent), then there exist infinitely many values of $s$, for which the minimum distance of the code is 5 (see [21] for the references). Janwa and Wilson [21] studied this question for other families of exponents, and gave partial results. They formulated this problem as an algebraic geometric problem as follows. A word of weight 4 of $C_{s(t)}^m$ corresponds to $\omega^t + \omega^{-t} + \omega^k + \omega^{-k} = 0$ and $\omega^t + \omega^{-t} + \omega^k t + \omega^{-k} t = 0$. The equations $\omega^t + \omega^{-t} + \omega^k + \omega^{-k} = 0$ and $\omega^t + \omega^{-t} + \omega^k t + \omega^{-k} t = 0$ lead to the hyperplane section of the following Fermat variety $x^t + y^t + z^t + w^t = 0$ by the hyperplane $z + y + z + w = 0$ and the study of its nontrivial solutions. This led them [21] to study the number of rational points on the associated projective curve corresponding to the function (with $j = t$):

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

If this curve has a non-trivial solution then the corresponding cyclic code has minimum distance at most 4. If this curve is absolutely irreducible (i.e. irreducible over the algebraic closure) or has an absolutely irreducible component, then they use the Weil estimate to show that only finitely many codes can have minimum distance 5 (see [21]). The authors, in [21], conjectured that the exceptional exponents are precisely the Gold or the Kasami-Welch exponents. A firm foundation for a resolution of this conjecture was laid in Janwa, McGuire and Wilson [20] (they gave an algorithmic approach involving multiplicity analysis introduced in [21] in Bezout’s Theorem to prove absolute irreducibility, and settled most of the cases of the conjecture). After a series of results by several contributors, Hernando and McGuire [19] established that this conjecture is true. That conjecture corresponded to the monomial function $f(x) = x^t$, and whether they are exceptional APN functions.

The check matrix of the cyclic code with roots $\omega$ and $\omega^t$ can be replaced by those given by $\omega$ and $f(\omega)$, giving a code that is not necessarily cyclic. One can then ask, when the corresponding code has minimum distance 5. Rodier [25] then considered the functions $f(x)$, and framed the question of APN functions in terms of the corresponding affine hypersurface in $P^3$ associate with the multivariate polynomial:

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

He proved by using the theorem of Lang-Weil, or its improvement due to Ghorpade and Lachaud, that if the corresponding projective hypersurface is absolutely irreducible or has an absolutely irreducible component, then $f(x)$ can not be an exceptional APN function. The best known examples of APN functions are the families of Gold functions $f(x) = x^{2^n+1}$, and the family of Kasami-Welch functions $f(x) = x^{2^{2k} - 2^k + 1}$; which are APN on any field $\mathbb{F}_{2^n}$ where $k, n$ are relatively prime.
As another example, the family of Welch functions $f(x) = x^{2r} + 3$ are APN on $F_{2^n}$, where $n = 2r + 1$.

Notice that, as shown in the above examples, the APN property may depend on the extension degree of the finite field. For any $t = 2^r + 1$ there exist infinitely many values $n$ such that $(r, n) = 1$. That is, any fixed Gold function which is APN on $L$ is also APN on infinitely many extensions of $L$. Functions with this property are called exceptional APN functions. The situation is different for our second example, a Welch function that is APN over $L$ is not necessarily APN on an extension of $L$. One way to classify APN functions is to determine which of them has the property of being exceptional.

Aubry, McGuire and Rodier conjectured the following in [1].

CONJECTURE: Up to equivalence, the Gold and Kasami-Welch functions are the only exceptional APN functions.

After this conjecture was established, several researchers (including us) have obtained partial results in proving that any other polynomial function (not a Gold or a Kasami-Welch function) cannot be an exceptional APN polynomial (see Section 2 for a summary). In this article (see Section 3 and 4), we contribute to these efforts with some results for Gold degree polynomials.

2. Known results in the Gold degree case

For known results in the non-Gold degree case, we refer to [10, 16, 25]. Aubry, McGuire and Rodier [1] also found results for Gold degree polynomials.

Theorem 1. Suppose $f(x) = x^{2^k} + 1 + h(x) \in L[x]$ where $\deg(h) \leq 2^{k-1} + 1$. Let $h(x) = \sum_{j=0}^{2^{k-1}+1} a_j x^j$. Suppose that there exists a nonzero coefficient $a_j$ of $h$ 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.

In the case when $\deg(h)$ is even, they were able to obtain the following partial result.

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

In [11, 13], we extended these results for the Gold degree case and found new families of polynomials which are not exceptional APN.

Theorem 3. 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 $1 \pmod{4}$, we also proved in [11, 13].

Theorem 4. 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 $\phi_{2^k+1}, \phi_d$ are relatively prime, then $\phi(x, y, z)$ is absolutely irreducible.

The following result was conjectured in [13], and then proved in [14].

Theorem 5. If $d$ is an odd integer, then $\phi_{2^k+1}$ and $\phi_d$ are relatively prime for all $k \geq 1$ except when $d = 2^l + 1$ and $(l, k) > 1$.
Using this result, in [14], we generalized theorem 3 and 4 as follows:

**Theorem 6.** For \( k \geq 2 \), let \( f(x) = x^{2k+1} + h(x) \in L[x] \) where \( \deg(h) \) is an odd integer that is not a Gold number or that is a Gold number of the form \( 2^{l} + 1 \) with \( (l,k) = 1 \). Then \( \phi(x,y,z) \) is absolutely irreducible, and \( f(x) \) can not be exceptional APN.

For this article, we will need the following result (see Janwa and Wilson [21]): If \( f(x) = x^{2k+1} \) is a Gold function, then

\[
\phi(x,y,z) = \prod_{a \in F_{2k} - F_{2}} (x + ay + (a+1)z).
\]

Also, we will need an observation of [1] that if \( f \) is not a Gold number or that is a Gold number of the form \( 2^{l}, \) then \( \phi(x,y,z) = \Sigma f_{j} \phi_{j}(x,y,z) \).

3. Completion of the exceptional APN conjecture in the Gold degree case when \( \deg(h) \) is odd

From Theorem 6, the conjecture is completely finished for Gold degree polynomials of the form \( f(x) = x^{2k+1} + h(x), \) where \( d = \deg(h) \) is any odd integer that is not a Gold number or a Gold number with \( d = 2^{l} + 1 \) and \( (l,k) = 1 \).

For non relatively prime numbers \( k, l \):

Let us suppose that \( \phi \) (related to \( f \) in Theorem 6) is not absolutely irreducible. Then,

\[
\phi(x,y,z) = (P_{s} + P_{s-1} + \ldots + P_{0})(Q_{t} + Q_{t-1} + \ldots + Q_{0})
\]

where \( P_{i}, Q_{i} \) are zero or forms of degree \( i, s + t = 2^{k} - 2 \). Assuming that \( s \geq t, 2^{k} - 2 > s \geq \frac{2^{k} - 2}{2} \geq t > 0 \). Let \( e = 2^{k} + 1 - d \). From the last equation:

\[
P_{s}Q_{t} = \phi_{2^{k}+1}
\]

since \( \phi_{2^{k}+1} \) is equal to the product of different linear factors [21], \( P_{s} \) and \( Q_{t} \) are relatively prime. By the assumed degree of \( h(x) \), the homogeneous terms of degree \( r, \) for \( d - 3 < r < 2^{k} - 2, \) are equal to zero. Equating the homogeneous terms of degree \( s + t - 1, s + t - 2, ..., d - 2, \) as in the proof of Theorem 3; we get

\[
P_{s-1} = Q_{t-1} = 0, \\
\ldots = \ldots = 0, \\
P_{s-(e-1)} = Q_{t-(e-1)} = 0.
\]

Since for \( k > l, 2^{k-1} > 2^{l-1} \); then \( s > d \). Therefore, as in the proof of theorem 4 (First case) we obtain that: \( Q_{t-1} = Q_{t-2} = \ldots = Q_{0} = 0 \). (Observe in the proof of Theorem 4 that \( t < e, \) where \( e = 2^{k} + 1 - d \).

Then, the surface \( \phi \) factor as:

\[
\sum_{j=3}^{2k+1} a_{j}\phi_{j}(x,y,z) = (P_{s} + P_{s-1} + \ldots + P_{0})(Q_{t})
\]

Therefore \( Q_{1} \) divides each \( \phi_{j}(x,y,z) \). This implies that \( \phi(x,y,z) \) would be absolutely irreducible if \( h \) contains a non zero term \( a_{m}x^{m} \) such that \( \phi_{2^{k}+1} \) and \( \phi_{m} \) are relatively primes.

We can summarize the above discussion in the following theorem.
Theorem 7. For $k \geq 2$, let $f(x) = x^{2k+1} + h(x) \in L[x]$ where $\deg(h) = 2^t + 1 < 2^k + 1$. Then: If $(k,l) \neq 1$ and $h$ contains a term of degree $m$ such that $(\phi_{2k+1}, \phi_m) = 1$, then $\phi(x, y, z)$ is absolutely irreducible and $f$ is not exceptional APN.

The following theorem almost completes the classification of absolute irreducibility of Gold degree polynomials when $h(x)$ has odd degree. However, if the Aubry, McGuire and Rodier conjecture is true, then if $f(x)$ has Gold degree and is not a monomial then, $\phi(x, y, z)$ does have an absolutely irreducible factor defined over an extension of $L$, and therefore, $f(x)$ is not exceptional APN in that case as well. The proof of this theorem and further results will appear in a subsequent article.

Theorem 8. For $k_1 \geq 2$, let $f(x) = x^{2k_1+1} + h(x) \in L[x]$ where $\deg(h) = 2^{k_2} + 1 < 2^{k_1} + 1$. Then $\phi$ is absolutely irreducible when $h(x) = \sum_{j=2}^t a_j x^{2^j + 1}$, 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 $\phi$ is divisible by $\phi_{2k+1}$ and $\phi$ is not absolutely irreducible.

Theorem 9 leave out the case of the exceptional APN conjecture when $f(x)$ is a sum of Gold degree terms when $(k_1, \ldots, k_t) = q > 1$. Because then $\phi$ is divisible by $\phi_{2k+1}$, and therefore it is not absolutely irreducible. However, Berguer, Canteaut, Charpin, and Laigle-Chapuy proved that a polynomial of the form

$$f(x) = \sum_{j \in J} f_j x^{2^j + 1} \in L[x],$$

where $J$ is a finite set of integers of size at least two is not APN on $L$ (and therefore not an APN on any extension of $L$). And therefore, $f(x)$ is not an exceptional APN polynomial. This result was proved in the context of permutation polynomials (see the discussions in [3] and [7], where it is also discussed that this result was proven earlier by Payne in the context of the classification of hyperovals.)

Therefore using Theorem 7 and Theorem 8, combined with the result just stated, we have almost established that the exceptional APN conjecture in the Gold degree case when $\deg(h)$ is odd is true. In the next section we will discuss the case when $\deg(h(x))$ is an even number.

4. The complement case of Theorem 2

Next we will discuss the case when $\deg(h)$ is an even number (the hardly discussed case, see the Remark at the end). The following theorem is the version of Theorem 2 when $k'$ is an even number.

Theorem 9. For $k \geq 2$, let $f(x) = x^{2k+1} + h(x) \in L[x]$ where $\deg(h) = 2^{2k-1} + 2$. Let $h(x) = \sum_{j=0}^{2^k-1+2} a_j x^j$. If there is a nonzero coefficient $a_j$ such that $(\phi_{2k+1}, \phi_j) = 1$. Then $\phi$ is absolutely irreducible, and $f(x)$ is not an exceptional APN function.

Proof. Suppose by way of contradiction that $\phi$ is not absolutely irreducible. Then, $\phi(x, y, z) = P(x, y, z)Q(x, y, z)$. Writing $P, Q$ as a sum of homogeneous terms:

$$\sum_{j=0}^{2^k+1} a_j \phi_j(x, y, z) = (P_0 + P_{s-1} + \ldots + P_0)(Q_0 + Q_{t-1} + \ldots + Q_0)$$
where \( P_t, Q_t \) are zero or homogeneous of degree \( i \) and \( s + t = 2^{2k} - 2 \). Assuming that \( s \geq t \), then \( 2^{2k} - 2 > s \geq \frac{2^{2k} - 2}{2} > t > 0 \). From the equation (2) we have that:

\[
(3) \quad P_s Q_t = \phi_{2^{2k}+1}.
\]

Since \( \phi_{2^{2k}+1} \) is equal to the product of different linear factors \([21]\), then \( P_s \) and \( Q_t \) are relatively primes. Since \( h(x) \) is assumed to have degree \( 2^{2k-1} + 2 \), the homogeneous terms of degree \( r \), for \( 2^{2k-1} - 1 < r < 2^{2k} - 2 \), are equal to zero. Then equating the terms of degree \( s + t - 1 \) gives \( P_s Q_{t-1} + P_{s-1} Q_t = 0 \). Hence we have that \( P_s \) divides \( P_{s-1} Q_t \) and this implies that \( P_s \) divides \( P_{s-1} \), since \( P_s \) and \( Q_t \) are relatively primes. We conclude that \( P_{s-1} = 0 \) and this is a contradiction by the hypothesis of the theorem.

Similarly, the equation of degree \( s + t - 2 \), \( s + t - 3 \), \ldots, \( s + 1 \) we get:

\[
P_{s-2} = Q_{t-2} = 0, \quad P_{s-3} = Q_{t-3} = 0, \ldots, \quad P_{s-(t-2)} = Q_1 = 0
\]

The equation of degree \( s \) is:

\[
(4) \quad P_s Q_0 + P_{s-t} Q_t = a_{s+3} \phi_{s+3}
\]

Let’s consider two cases to prove the absolute irreducibility of \( \phi(x, y, z) \).

**Case** \( s > t \). Then \( s > 2^{2k-1} - 1 \) and \( \phi_{s+3} = 0 \). Then the equation (4) becomes:

\[
P_s Q_0 + P_{s-t} Q_t = 0.
\]

Then, using the previous argument, \( P_{s-t} = Q_0 = 0 \). It means that \( Q = Q_t \) is homogeneous.

By the equation (3) and the factorization of \( \phi_{2^{2k}+1} \) in linear factors (see [7] for this factorization) we have that for all \( j \), \( \phi_j(x, y, z) \) is divisible by \( x + \alpha y + (\alpha + 1)z \) for some \( \alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2 \), which is a contradiction by the hypothesis of the theorem.

**Case** \( s = t = 2^{2k-1} - 1 \). For this case the equation (4) becomes:

\[
(5) \quad P_s Q_0 + P_t Q_t = a_{s+3} \phi_{2^{2k-1}+2}.
\]

If \( P_0 = 0 \) or \( Q_0 = 0 \), then we have that \( Q = Q_t \) or \( P = P_t \). Then by similar arguments of the first case we have a contradiction. If both \( P_0, Q_0 \) are different from zero, let us consider the intersection of \( \phi \) with the line \( z = 0, y = 1 \). Then the equation (3) and (4) become:

\[
(6) \quad P_s Q_t = \prod_{\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_2} (x + \alpha)
\]

\[
(7) \quad P_s Q_0 + P_0 Q_t = a_{s+3}(x + 1)(x) \prod_{\alpha \in \mathbb{F}_{2^{2k-2}} \setminus \mathbb{F}_2} (x + \alpha)^2
\]

This last equation is derived from a result in [1] that states:

\[
\phi_{2^{2k-1}+2} = (x + y)(x + z)(y + z)\phi_{2^{2k-2}+1}.
\]

It is easy to show that \( \mathbb{F}_{2^k} \cap \mathbb{F}_{2^{2k-2}} = \mathbb{F}_{2^2} \). Let \( x = \alpha_0 \in \mathbb{F}_4 \), \( \alpha_0 \neq 0, 1 \). Then, from \( (6) \), we have that \( P_s(\alpha_0) = 0 \) and \( Q_t(\alpha_0) = 0 \). If \( P_s(\alpha_0) = 0 \), then \( Q_t(\alpha_0) \neq 0 \) (since \( P_s Q_t \) is a product of different linear factors and from equation (7) we have \( P_0 Q_t(\alpha_0) = 0 \), a contradiction since both \( P_0, Q_t(\alpha_0) \) are different from zero. The case \( Q_t(\alpha_0) = 0 \) is analogous. Therefore \( \phi(x, y, z) \) is absolutely irreducible.
Remark. In Theorem 7, if the conditions are not satisfied, then \( f \) is reducible. In theorem 9, in the case when \( \deg(h) \) is even, becomes difficult because for this case, there is an example where \( f \) is reducible (see subsection 5.5.2 in [11] for such an example).

ACKNOWLEDGMENTS

The authors would like to thank Domingo Gomez, and the reviewers for helpful suggestions.

REFERENCES

[1] Y. Aubry, G. McGuire and F. Rodier, A few more functions that are not APN infinitely often in Finite Fields: Theory and Applications, 2010, 23–31.
[2] R. D. Baker, J. H. Van Lint and R. M. Wilson, On the preparata and goethals codes IEEE Trans. Inf. Theory, 29 (1983), 342–345.
[3] T. P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, On almost perfect nonlinear functions over \( \mathbb{F}_{2^n} \), IEEE Trans. Inf. Theory, 52 (2006), 4160–4170.
[4] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
[5] C. Blondeau and K. Nyberg, Perfect nonlinear functions and cryptography Finite Fields Appl., 32 (2015), 120–147.
[6] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN functions from known ones Finite Fields Appl., 15 (2009), 150–159.
[7] E. Byrne and G. McGuire, Quadratic binomial APN functions and absolutely irreducible polynomials, preprint, arXiv:0810.4523
[8] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for des-like cryptosystems Des. Codes Crypt., 15 (1998), 125–156.
[9] F. Caullery, Polynomial functions of degree 20 which are APN infinitely often, preprint, arXiv:1212.4638
[10] F. Caullery, A new large class of functions not APN infinitely often Des. Codes Crypt., 73 (2014), 601–614.
[11] M. Delgado and H. Janwa, On the conjecture on APN functions, preprint, arXiv:1207.5526
[12] M. Delgado and H. Janwa, Further results on exceptional APN functions, 2013.
[13] M. Delgado and H. Janwa, On the conjecture on APN functions and absolute irreducibility of polynomials Des. Codes Crypt., 2016, 1–11.
[14] M. Delgado and H. Janwa, Progress towards the conjecture on APN functions and absolutely irreducible polynomials, preprint, arXiv:1602.02576
[15] Y. Niho, Multi-Valued Cross-Correlation Functions between Two Maximal Linear Recursive Sequences, Ph.D thesis, Univ. Southern California, 1972.
[16] A. Pott, Almost perfect and planar functions Des. Codes Crypt., 78 (2016), 141–195.
[25] F. Rodier, Borne sur le degré des polynômes presque parfaitement non-linéaires. *Contemp. Math.*, **14** (2009), 169.

[26] F. Rodier, Some more functions that are not APN infinitely often. the case of Kasami exponents, preprint, [arXiv:1101.6033](https://arxiv.org/abs/1101.6033)

Received February 2016; revised March 2016.

E-mail address: moises.delgado@upr.edu
E-mail address: heeralal.janwa@upr.edu