Further Results on Exceptional APN Functions

Heeralal Janwa
(Joint work with Moises Delgado)

AGCT- India, Mumbai, India
December 6, 2013

Definition 1

Let $L = \mathbb{F}_q$, with $q = p^n$. $f : L \to L$ is **almost perfect nonlinear** *(APN) on L if for all $a, b \in L$, $a \neq 0$*

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

has at most 2 solutions.

Equivalently, for $p = 2$, the cardinality of $\{f(x+a)-f(x) : x \in L\}$ is at least 2^{n-1} for each $a \in L^*$. APN functions are important in applications to cryptography, coding theory, combinatorics, finite geometries, and other related areas.

The best known examples of APN functions are

x^d	Exponent d	Constraints
Gold	2^r+1	$(r,n)=1$
Kasami-Welch	$2^{2r}-2^r+1$	$(r,n)=1$,n odd
Welch	2^r+3	$n=2r+1$
Niho	$2^r+2^{r/2}-1$ $2^r+2^{(3r+1)/2}-1$	$n=2r+1$, r even $n=2r+1$, r odd
Inverse	$2^{2r}-1$	$n=2r+1$
Dobbertin	$2^{4r}+2^{3r}+2^{2r}+2^r-1$	$n=5r$

Table: Monomial APN Functions

Until 2006, the list of known APN functions on $L = GF(2^n)$ was rather short.
Y. Edel, G. Kyureghyan and A. Pott established (by an exhaustive search) the first example of an APN function not equivalent to any monomial APN functions. Their example is

$$x^3 + ux^{36} \in GF(2^{10})[x],$$

where $u \in wGF(2^5)^* \cup w^2GF(2^5)^*$ and w has order 3, is APN on $GF(2^{10})$. Since then, several new infinite families of polynomial APN functions have been discovered.

Definition 2

Let $L = \mathbb{F}_q$, $q = p^n$. 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 made the following conjecture:
Up to equivalence, the Gold and Kasami-Welch functions are the only exceptional APN functions.

Proposition 1 (J and Wilson 93, Rodier 2009)

Let $L = \mathbb{F}_q$, with $q = 2^n$. A function $f : L \to L$ is APN if and only if the affine surface X with equation

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

has all its rational points contained in the surface

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

Theorem 1 (J and Wilson 93, Rodier 2009)

Let f be a polynomial from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$, d its degree. Suppose that the surface X with affine equation

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)}=0 \qquad (2)$$

is absolutely irreducible. Then, if $d < 0.45q^{1/4}+0.5$ and $d \geq 9$, f is not APN.

Proposition 2 (J and Wilson 93, Rodier 2009)

Let f be a polynomial of $\mathbb{F}_{2^m}$ to itself, d its degree. Let us suppose that d is not a power of 2 and that the curve X_∞ with equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible. Then the surface X of equation (2) is absolutely irreducible.

Theorem 2 (J and Wilson 93, Rodier 2009)

Let f be a polynomial from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$, d its degree. Let us suppose that d is not a power of 2 and that the surface X

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)}=0$$

is regular in codimension one. Then if $d \geq 10$ and $d < q^{1/4}+4$, f is not APN.

PROOF: From an improvement of a theorem of Deligne on Weil's conjectures by Ghorpade-Lachaud,

$$|X(k)-q^2-q-1| \leq (d-4)(d-5)q^{3/2}+(-82+57d-13d^2+d^3)q$$

If $q > 183 - 230d + 94d^2 - 16d^3 + d^4$ and $d \geq 6$, then $X(k) > 3((d-3)q+1)$ and so f is not APN. Q.E.D.

Absolute irreducibility testing (J and Wilson 91, J 92, J, McGuire and Wilson 95)

The main ingredient in all the proofs on APN functions (by perhaps everyone) is the following absolute irreducibility testing. Algorithm:

- Assume $f(x, y, z)$ factors as $P(x, y, z)Q(x, y, z)$.
- Compute and classify multiplicities of each singular point.
- Find intersection multiplicities.
- If the sum of intersection multiplicies exceeds that predicted by Bezout's theorem, then factorization can not occur.

Definition 3

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

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

$$\phi(x,y,z) = \Sigma f_j \phi_j(x,y,z)$$

Theorem 3

If the degree of f is odd and not a Gold or a Kasami-Welch number, then f is not exceptional APN.

Theorem 4

If the degree of f is $2e$ with e odd, and if f contains an odd degree term, then f is not exceptional APN.

Theorem 5

If the degree of f is $4e$ with $e \geq 7$ and $e \equiv 3 \pmod 4$, then f is not exceptional APN.

Theorem 6

Suppose $f(x) = x^{2^k+1} + g(x)$, *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* f *is not exceptional APN.*

Theorem 7 (J and Wilson, 93)

If $f(x) = x^{2^k+1}$ is a Gold function, then

$$\phi(x, y, z) = \prod_{\alpha \in F_{2^k} - F_2} (x + \alpha y + (\alpha + 1)z). \tag{3}$$

Theorem 8 (J and Wilson, 93)

If $f(x) = x^{2^{2k}-2^k+1}$ is a Kasami Welch function, then

$$\phi(x, y, z) = \prod_{\alpha \in F_{2^k} - F_2} P_\alpha(x, y, z), \tag{4}$$

where $P_\alpha(x, y, z)$ is absolutely irreducible of degree $2^k + 1$ over $GF(2^k)$.

PROOF:
Hensel lifting, Bezout's theorem, Gauss' lemma and so on.

Lemma 1

For $k > 1$, 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

$$(\phi_l, \phi_m) = 1, (\phi_l, \phi_n) = 1, (\phi_m, \phi_n) = 1.$$

Also:

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

Theorem 9

For $k \geq 2$ and $\alpha \neq 0$, let $f(x) = x^{2^k+1} + \alpha x^{2^{k-1}+3} + h(x) \in L[x]$, where $h(x) = \sum_{j=0}^{2^{k-1}+1} a_j x^j$ and either $a_5 = 0$ or there is a non zero $a_j \phi_j$ for some $j \neq 5$.
Then $\phi(x, y, z)$ is absolutely irreducible.

Hyperplane sections

Lemma 2

Let $\phi_j(x, y, z)$ be as in (3). Then

- *For $n = 2^k + 1 > 3$; $\phi_n(x, y, y) = (x + y)^{2^k - 2}$*
- *For $n \equiv 3 \pmod 4 > 3$, $x + y$ does not divide $\phi_n(x, y, y)$*
- *For $n \equiv 1 \pmod 4 > 5$, The highest power of $(x + y)$ that divides $\phi_n(x, y, y)$ is $2^l - 2$, where $n = 1 + 2^l m$, $l \geq 2$ and $m > 1$ is an odd number.*

Main results: Gold case

Theorem 10

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

Theorem 11

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

Theorem 12

Let $f(x) = x^d + h(x) \in L[x]$, where $d = 2^{2k} - 2^k + 1$, $deg(h) \leq 2^{2k-1} - 2^{k-1} + 1$. Suppose that there exist $a_j \neq 0$ such that ϕ_j, ϕ_n are relatively primes. Then $\phi(x, y, z)$ is absolutely irreducible.

Kasami exponents

Lemma 3

Let $\phi_j(x, y, z)$ be as before.

- *For $j = 2^k + 1 > 3$, $\phi_j(x, 1, 1) = (x+1)^{2^k - 2}$.*
- *For $j \equiv 3 \pmod 4 > 3$, $\phi_j(x, 1, 1) = (x^{2m} + x^{2m-1} + \ldots + x + 1)^2$, where $j = 3 + 4m$ for $m \geq 1$.*
- *For $j \equiv 1 \pmod 4 > 5$, $\phi_j(x, 1, 1) = (x+1)^{2^l - 2}(x^{m-1} + x^{m-2} + \ldots + x + 1)^{2^l}$, where $j = 1 + 2^l m$, $l \geq 2$ and $m > 1$ is an odd number.*

Theorem 13

For $k \geq 2$, let $f(x) = x^{2^{2k}-2^k+1} + h(x) \in L[x]$ where $d = \deg(h) \equiv 3 \pmod 4 < 2^{2k} - 2^{k+1} + 3$. Then:

- *If $d \leq 2^{2k-1} - 2^{k-1} + 1$ or*
- *if $d > 2^{2k-1} - 2^{k-1} + 1$ and $(2^k - 1, \frac{d-1}{2}) = 1$,*

then $\phi(x, y, z)$ is absolutely irreducible.

PROOF: Suppose that ϕ factors as $\phi(x,y,z) = P(x,y,z)Q(x,y,z)$, where P and Q are polynomials defined on the algebraic closure of L. Then

$$\sum_{j=3}^{2^{2k}-2^k+1} a_j \phi_j(x,y,z) = (P_s + P_{s-1} + \ldots + P_0)(Q_t + Q_{t-1} + \ldots + Q_0) \tag{5}$$

where P_i, Q_i the homogeneous components of P and Q. Assume that $s \geq t$, then

$$2^{2k} - 2^k + 1 > s \geq 2^{2k-1} - 2^{k-1} - 1 \geq t > 0.$$

Let $e = 2^{2k} - 2^k + 1 - d > 2^k - 2$.

$$P_s Q_t = \prod P_\alpha(x, y, z) \tag{6}$$

where $\alpha \in \mathbb{F}_{2^k}, \alpha \neq 0, 1$. Since P_α are different absolutely irreducible factors, P_s and Q_t are relatively prime.
By the hypothesis on $h(x)$, the homogeneous terms of degree r, for $d-3 < r < s+t$, equal zero. Then the terms of degree $s+t-1$ are $P_s Q_{t-1} + P_{s-1} Q_t = 0$. Hence, P_s divides $P_{s-1} Q_t$ and this implies that P_s divides P_{s-1}. We conclude that $P_{s-1} = 0$ as the degree of P_{s-1} is less than the degree of P_s. In addition $Q_{t-1} = 0$ as $P_s \neq 0$. Similarly,

$$P_{s-2} = Q_{t-2} = 0, P_{s-3} = Q_{t-3} = 0, ..., P_{s-(e-1)} = Q_{t-(e-1)} = 0.$$

The term of degree $d-3$ is:

$$P_s Q_{t-e} + P_{s-e} Q_t = a_d \phi_d(x, y, z) \tag{7}$$

We show that $Q_{t-e} = 0$. Suppose $d \leq 2^{2k-1} - 2^{k-1} + 1$. Then $e = 2^{2k} - 2^k + 1 - d \geq 2^{2k-1} - 2^{k-1}$. Since $t \leq 2^{2k-1} - 2^{k-1} - 1$, then $t - e < 0$. Thus $Q_{t-e} = 0$.

We assume that $d > 2^{2k-1} - 2^{k-1} + 1$ and $(2^k - 1, \frac{d-1}{2}) = 1$. Now consider $y = z = 1$.

$$P_s Q_t = (x+1)^{2^k-2}(x^{2^k-2} + x^{2^k-3} + \ldots + 1)^{2^k} \tag{8}$$

$$P_s Q_{t-e} + P_{s-e} Q_t = a_d(x^{2m} + x^{2m-1} + \ldots + 1)^2 \tag{9}$$

where P_s, Q_t are functions of x of degree s, t respectively and $d = 3 + 4m$.

$x+1 \nmid x^{2m} + x^{2m-1} + \ldots + 1$. The roots of $x^{2^k-2} + x^{2^k-3} + \ldots + 1$, $x^{2m} + x^{2m-1} + \ldots + 1$ are also lth root of unity for $l = 2^k - 1$ or $l = \frac{d-1}{2}$. Then, by hypothesis, the left hand side of (8) and (9) are relatively prime, so $(P_s, Q_t) = 1$ which implies that $s = 2^k(2^k - 2)$ and $t = 2^k - 2$.

Thus, $t - e < 0$ implying that $Q_{t-e} = 0$. Q.E.D.

Consider the particular subcase where $\deg(h)$ is a Gold number.

Theorem 14

For $k \geq 2$, let $f(x) = x^{2^{2k}-2^k+1} + h(x) \in L[x]$ where $d = \deg(h) = 2^m + 1 < 2^{2k} - 2^k + 1$. Then $\phi(x, y, z)$ is absolutely irreducible.

A new conjecture on ϕ_i

Based on overwhelming evidence, we believe that $(\phi_{2^k+1}, \phi_d) = 1$ is always the case, and therefore, theorem 11 is unconditionally true. From the evidence, we propose the following conjecture:

Conjecture 1

If $d \equiv 1 \pmod 4$ and d is not a Gold or Kasami exponent, then, ϕ_{2^k+1}, ϕ_d are relatively prime for all $k \geq 1$.

Evidence for the new conjecture

We define $\widetilde{\phi}_j(x,y) = \phi_j(x+1, y+1, 1)$. Then:
For a Gold number $j = 2^k + 1$ we have:

$$\widetilde{\phi}_j(x,y) = \prod_{\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2} (x + \alpha y) \tag{10}$$

For any number $j \equiv 5 \pmod 8$:

$$\widetilde{\phi}_j(x,y) = x^4 y + x y^4 + \sum_{r=6}^{1+4l} F_r(x,y) \tag{11}$$

where $j = 1 + 4l$, $l > 1$ is any odd number and F_r is zero or homogeneous of degree r.

Theorem 15

Given a Gold number n and a number $m \equiv 5 \pmod 8$, then $(\phi_n, \phi_m) = 1$.

PROOF: Since $(\phi_n, \phi_m) = 1 \Leftrightarrow (\widetilde{\phi}_n, \widetilde{\phi}_m) = 1$, we will work with the functions $\widetilde{\phi}$.
Let $n = 2^k + 1$, $\alpha \in \mathbb{F}_k$, $\alpha \neq 0, 1$ and $m = 4l + 1$, where $l > 1$ is an odd integer.
By eq. (10), $(\phi_n, \phi_m) = 1 \Leftrightarrow (x + \alpha y) \nmid \phi_m(x, y)$. We will prove that no factor of the form $(x + \alpha y)$ divides ϕ_m.
Suppose that $(x + \alpha y)$ divides $\widetilde{\phi}_m(x, y)$. Then $(x + \alpha y)$ divides $F(x, y) = \widetilde{\phi}_m(x, y)xy(x + y)$.
Writing $F(x, y)$ as a sum of homogeneous terms:

$$F(x, y) = F_5(x, y) + F_6(x, y) + ... + F_{1+4l}(x, y)$$

Then, $(x+\alpha y)|F(x,y)$ if and only if $(x+\alpha y)|F_r(x,y)$ for all r. By eq. (11), $(x-\alpha)|x^4y+xy^4$ implies $\alpha^3+1=0$, then α is a 3rd-root of unity.

Consider the following three cases to prove the theorem:

- $l \equiv 0 \pmod 3$
- $l \equiv 1 \pmod 3$
- $l \equiv 2 \pmod 3$

Case $l \equiv 0 \pmod 3$

Let $l \equiv 0 \pmod 3$, then $l = 3q$, $m = 4(3q) + 1$.
If $(x + \alpha y)$ divides $\widetilde{\phi}_m$, by the Remainder theorem $\widetilde{\phi}_m(\alpha y, y) = 0$.
However,

$$\widetilde{\phi}_m(\alpha y, y) = (\alpha y + 1)^m + (y + 1)^m + 1 + (\alpha^2 y + 1)^m$$

the term F_{m-1} of degree $m - 1$ is:
$F_{m-1} = \binom{m}{1} [\alpha^{m-1} + 1 + (\alpha^2)^{m-1}] y^{m-1} = y^{m-1}$, contradicting that $\widetilde{\phi}_m(\alpha y, y) = 0$.

Case $l \equiv 1 \pmod 3$

Let $l \equiv 1 \pmod 3$, then $l = 1 + 3q$,
$m = 4(1+3q) + 1 = 5 + 4(3q)$.
If $(x + \alpha y)$ divides $\widetilde{\phi}_m$, $\widetilde{\phi}_m(\alpha y, y) = 0$. However the term F_{m-5} of degree $m-5$ in $\widetilde{\phi}_m(\alpha y, y)$ is:
$F_{m-5} = \binom{m}{5} [\alpha^{m-5} + 1 + (\alpha^2)^{m-5}] y^{m-5} = y^{m-5}$. Contradiction.

Case $l \equiv 2 \pmod 3$

If $l \equiv 2 \pmod 3$, then $l = 2 + 3q$, $m = 4(2+3q) + 1 = 9 + 4(3q)$.
If $(x + \alpha y)$ divides $\widetilde{\phi}_m$, $\widetilde{\phi}_m(\alpha y, y) = 0$; but computing the term F_m of degree m in $\widetilde{\phi}_m(\alpha y, y)$:
$F_m = \binom{m}{0} [\alpha^m + 1 + (\alpha^2)^m] y^m = y^m$. Q.E.D.

Theorem 16

For $k \geq 2$, let $f(x) = x^{2^k+1} + h(x) \in L[x]$ where $d = \deg(h) \equiv 5 \pmod 8 < 2^k + 1$. Then $\phi(x, y, z)$ is absolutely irreducible.

Theorem 17

All polynomials of the form $f(x) = x^{65} + h(x)$ are not exceptional APN for all odd degree polynomials h.

In Theorem 11, $(\phi_{2^k+1}, \phi_d) = 1$ is a necessary condition for $f(x)$ not to be exceptional APN.
This observation allows us to apply several key results. Janwa, McGuire and Wilson proved the absolute irreducibility of ϕ_d, when $d \equiv 3 \pmod 4$.
They also established absolute irreducibility for several other infinite cases with $d \equiv 1 \pmod 4$. Moreover for $d \equiv 5 \pmod 8 > 13$, if the maximal cyclic code of odd length m, B_m (where $d = 2^l m + 1$, $l > 0$), has no codewords of weight 4 then, $\phi_d(x, y, z)$ is absolutely irreducible. For many values of m it is possible that B_l has no codewords of weight 4, for example, if m is a prime congruent to $\pm 3 \pmod 8$. For more details and infinite classes of examples, see [1].

1. Until recently, it was thought that $\phi_d(x, y, z)$ was absolutely irreducible for the values of $d \equiv 5 \pmod 8$. F. Hernando and G. McGuire [2], with the help of MAGMA, found that the polynomial $\phi_{205}(x, y, z)$ factors in $F_2[x, y, z]$.
2. Janwa and Wilson [3] proved, using different methods including Hensel's lemma implemented on a computer, that $\phi_d(x, y, z)$ is absolutely irreducible for $3 < d < 100$, provided that d is not a Gold or a Kasami-Welch number.
3. Subsequent results, (Férard, Oyono, and Rodier [4] and Delgado and Janwa [5]) supplement our results for the Kasami degree polynomials.

Thank you for your attention.

Heeralal Janwa, Gary M. McGuire, and Richard M. Wilson.
Double-error-correcting cyclic codes and absolutely irreducible polynomials over $\mathrm{GF}(2)$.
J. Algebra, 178(2):665–676, 1995.

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.

H. Janwa and R. M. Wilson.
Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in $\mathrm{char.}\,2$ 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.

Eric Férard, Roger Oyono, and Franccois 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.

H. Janwa M. Delgado.
On the conjecture on apn functions.
2012.