The Exceptional Almost Perfect Nonlinear Function Conjecture

Carlos Agrinsoni[1]
(joint work Heeralal Janwa[2] and Moises Delgado[3])

[1]Purdue University

[2]University of Puerto Rico at Rio Piedras

[3]University of Puerto Rico at Cayey

February 5, 2024

Outline

Background

Definition

$f(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$ is *absolutely irreducible* if $f(\boldsymbol{X})$ is irreducible in $\overline{\mathbb{F}}[\boldsymbol{X}]$.

Background

Definition

$f(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$ is *absolutely irreducible* if $f(\boldsymbol{X})$ is irreducible in $\overline{\mathbb{F}}[\boldsymbol{X}]$.

Example

$f(X, Y) = Y^{q+1} - (X^q + X) \in \mathbb{F}_{q^2}[X, Y]$ is absolutely irreducible.
$f(X, Y, Z) = X^5 + Y^5 + Z^5 \in \mathbb{F}_3[X, Y, Z]$ is absolute irreducible.

Background

For background, we refer to Fulton [18], Shafarevich [29], and Hartshorne [20].

Background

For background, we refer to Fulton [18], Shafarevich [29], and Hartshorne [20].

Definition

Let $P \in \mathbb{F}^n$ is called a simple point of F if $F(P) = 0$ and $\frac{\partial F}{\partial X_i}(P) \neq 0$ for some $i \in \{1, \ldots, n\}$. If $G(F) = 0$ and is not simple, then it is called a singular point.

Background

For background, we refer to Fulton [18], Shafarevich [29], and Hartshorne [20].

Definition

Let $P \in \mathbb{F}^n$ is called a simple point of F if $F(P) = 0$ and $\frac{\partial F}{\partial X_i}(P) \neq 0$ for some $i \in \{1, \ldots, n\}$. If $G(F) = 0$ and is not simple, then it is called a singular point.

Definition

Let $F(X - p_1, \ldots, X_n - p_n) = F_m(\mathbf{X}) + F_{m+1}(\mathbf{X}) + \ldots$. Then $F_m = t_{F,P}$ is the *tangent cone* of F at P and $\deg(F_m) = \nu_P(F)$ is the multiplicity of F at P.

Example

Example

Consider $F(X, Y, Z) = X^2 + XY + Y^2 + XZ + YZ + Z^2 \in \mathbb{F}_4[X, Y, Z]$.

1. $F(X, Y, Z)$ is a homogeneous polynomial of degree 2.
2. $F(X, Y, Z) = (X + \alpha Y + (\alpha + 1)Z)(X + \alpha^2 Y + (\alpha^2 + 1)Z)$, then $1 = (1, 1, 1) \in \mathbb{F}_4^3$ is a singular point of F.
3. $F(X + 1, Y + 1, Z + 1) = F(X, Y, Z)$, therefore $t_{F,1}(X, Y, Z) = F(X, Y, Z)$ and $\nu_{(1,1,1)}(F) = 2$.

Lemma 1

Let $F(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $a \in \mathbb{F}_q^n$. Suppose that $F(X) = G(X)H(X)$, then

$$t_{F,a}(X) = t_{G,a}(X)t_{H,a}(X).$$

APN functions

Definition

A function $f : \mathbb{F}_q \to \mathbb{F}_q$, (necessarily a polynomial) is almost perfect nonlinear (APN) on $\mathbb{F}_q$ if for all $a, b \in \mathbb{F}_q$, $a \neq 0$,

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

has at most 2 solutions.

APN functions

Definition

A function $f : \mathbb{F}_q \to \mathbb{F}_q$, (necessarily a polynomial) is almost perfect nonlinear (APN) on $\mathbb{F}_q$ if for all $a, b \in \mathbb{F}_q$, $a \neq 0$,

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

has at most 2 solutions.

Definition

$f : \mathbb{F}_q \to \mathbb{F}_q$, is an exceptional APN if f is APN over $\mathbb{F}_q$ and over infinitely many extensions of $\mathbb{F}_q$.

Equivalent Definition of APN Functions

Definition (Janwa & Wilson 1993 [22])

Let $\mathbb{F}_{2^m}^* = \langle \alpha \rangle$. A function $f(X) \in \mathbb{F}_{2^m}[X]$ is APN if the code $C_s^{(t)}$ with parity check matrix

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

is a 2-error correcting code.

Equivalent Definition of APN Functions

Definition (Janwa & Wilson 1993 [22])

Let $\mathbb{F}_{2^m}^* = \langle\alpha\rangle$. A function $f(X) \in \mathbb{F}_{2^m}[X]$ is APN if the code $C_s^{(t)}$ with parity check matrix

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

is a 2-error correcting code.

Proposition 1 (Rodier [28])

A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ 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 $(x+y)(x+z)(y+z) = 0$.

$\phi(X, Y, Z)$

Multivariate Polynomial $\phi(X, Y, Z)$

For the rest of this presentation, let $q = 2^m$ for $m \geq 1$. Let $f(X) \in \mathbb{F}_q[X]$, then we define

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

$\phi(X, Y, Z)$

Multivariate Polynomial $\phi(X, Y, Z)$

For the rest of this presentation, let $q = 2^m$ for $m \geq 1$. Let $f(X) \in \mathbb{F}_q[X]$, then we define

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

Notation and facts about $\phi_f(X, Y, Z)$

1. If $f(x) = x^d$ then we denoted $\phi_f(X, Y, Z) = \phi_d(X, Y, Z)$.
2. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0x^0$, then $\phi_f(X, Y, Z) = \phi_n(X, Y, Z) + a_{n-1}\phi_{n-1}(X, Y, Z) + \cdots + a_0\phi_0(X, Y, Z)$.
3. If $f(X)$ is affine then, $\phi_f(X, Y, Z) = 0$.
4. If $f(X) = X^d$ not affine, then $\deg(\phi_d) = d - 3$.

Relationship between Exceptional APN and absolutely irreducible polynomials

The problem was formulated as an algebraic assertion by Janwa and Wilson ([22] 1993) and later generalized by Rodier [28].

Theorem 1

Let $f : L \to L$ a polynomial function of degree d. Suppose that the surface X of affine equation

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

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

Corollary 1

If $\phi_f(x, y, z)$ contain an absolutely irreducible factor over $\mathbb{F}_q$ different from $(x + y), (x + z), (y + z)$, then $f(x)$ is not an exceptional APN.

Equivalence of APN functions

The APN property is invariant under some transformations.

Proposition 2

Let $A_1(X)$ and $A_2(X)$ be affine permutations, $A(X)$ be an affine polynomial and $f(X)$ be APN in $\mathbb{F}_q[X]$. Then the polynomial

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

is APN over $\mathbb{F}_q[X]$.

Proposition 3 (Carlet, Charpin and Zinoviev [6])

Let $f(X), g(X) \in \mathbb{F}_q[X]$. Suppose $\exists$ a linear permutation $\mathcal{L} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ 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.

Known Monomial APN Functions

$f(x) = x^d$	Exponent d	Constraints	References
Gold	$2^r + 1$	$(r, n) = 1$	[19, 22]
Kasami-Welch	$2^{2r} - 2^r + 1$	$(r, n) = 1$	[22]
Welch	$2^r + 3$	$n = 2r + 1$	[15]
Niho	$2^r + 2^{r/2} - 1$ $2^r + 2^{(3r+1)/2} - 1$	$n = 2r + 1$, r even $n = 2r + 1$, r odd	[14]
Inverse	-1	$n = 2r + 1$	[5, 27]
Dobbertin	$2^{4r} + 2^{3r} + 2^{2r} + 2^r - 1$	$n = 5r$	[16]

Table 1: Known Monomial APN functions on $\mathbb{F}_{2^n}$ up to CCZ equivalence

Exceptional APN Monomials up to CCZ Equivalence

Function	Exceptional	Constraints	References
x^{2^i+1}	**Yes**	APN $\iff (i,n)=1$	[22, 27]
$x^{4^i-2^i+1}$	**Yes**	APN $\iff (i,n)=1$	[22]
x^t	No	$t \equiv 3 \pmod 4,\ t>3$	[23]
$x^{2^i l+1}$	No	$(l, 2^i-1) < l$	[24]
$x^{2^i l+1}$	No	$(l, 2^i-1) = l$	[21]

Table 2: Exceptional APN Monomials on $\mathbb{F}_{2^n}$

Exceptional APN Conjecture

Theorem 2 (Janwa and Wilson [22], Janwa, Wilson and McGuire [23], Jedlicka [24], Hernando and McGuire [21] (2011))

The Gold and Kasami-Welch are the only exceptional APN monomials.

Exceptional APN Conjecture

Theorem 2 (Janwa and Wilson [22], Janwa, Wilson and McGuire [23], Jedlicka [24], Hernando and McGuire [21] (2011))

The Gold and Kasami-Welch are the only exceptional APN monomials.

Conjecture 1 (Aubry, McGuire and Rodier [4], (2010))

The only exceptional APN functions up to CCZ equivalence are the Kasami-Welch and Gold monomials.

$f(x) = x^d$	Exponent d	Constraints	References
Gold	$2^r + 1$	$(r, n) = 1$	[19, 22]
Kasami-Welch	$2^{2r} - 2^r + 1$	$(r, n) = 1$	[22]

Gold Degree Case

Theorem 3 (Delgado and Janwa [9] (2016), Delgado, Janwa and Agrinsoni [13] (2023))

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 $(l, k) > 1$.

Gold Degree Case

Theorem 3 (Delgado and Janwa [9] (2016), Delgado, Janwa and Agrinsoni [13] (2023))

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 $(l, k) > 1$.

Theorem 4 (Delgado and Janwa [11] (2017))

If $f(X) = X^{2^r+1} + h(X)$, where $\deg(h) \equiv 3 \pmod 4$, then $\phi_f(X, Y, Z)$ is absolutely irreducible and $f(X)$ is not EAPN.

Gold Degree Case

Theorem 5 (Delgado and Janwa [11] (2017))

For $k \geq 2$, *let* $f(X) = 2^k + 1 + h(X) \in L[X]$, *where* $\deg(h) \equiv 1 \pmod 4$. *If* $\deg(h)$ *is not a Gold exponent, then* f *is not EAPN.*

Gold Degree Case

Theorem 5 (Delgado and Janwa [11] (2017))

For $k \geq 2$, *let* $f(X) = 2^k + 1 + h(X) \in L[X]$, *where* $\deg(h) \equiv 1 \pmod 4$. *If* $\deg(h)$ *is not a Gold exponent, then* f *is not EAPN.*

Theorem 6 (Delgado and Janwa [10] (2018))

Let $f(X) = x^{2^{k_1}+1} + h(X) \in \mathbb{F}_{2^m}[X]$, *where* $\deg(h) = 2^{k_2+1}$. *If* $h(X) = \sum_{j=2}^{t} a_j x^{2^{c_j}(2^{k_j}+1)}$ *and* $(k_1, \ldots, k_t) = (k_1, k_2) = q$, *then* ϕ *contains an absolutely irreducible factor and* f *is not EAPN.*

Kasami-Welch Degree Case

Theorem 7 (Delgado and Janwa [8] (2017) and Ferard [17] (2017))

Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_{2^m}$, *where* $d = \deg(h) \equiv 3 \pmod 4$. *Then,* $\phi(X, Y, Z)$ *is absolutely irreducible and* $f(X)$ *is not EAPN.*

Kasami-Welch Degree Case

Theorem 7 (Delgado and Janwa [8] (2017) and Ferard [17] (2017))

Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_{2^m}$, *where* $d = \deg(h) \equiv 3 \pmod 4$. *Then,* $\phi(X, Y, Z)$ *is absolutely irreducible and* $f(X)$ *is not EAPN.*

Theorem 8 (Ferard [17] (2017))

Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_{2^m}$, *where* $k \geq 2$, $d = \deg(h) = 1 + 2^j\ell$, $j \geq 2$ *and* ℓ *odd. If* $(2^k - 1, \ell) \neq 2^k - 1$, *then* $\phi_f(X, Y, Z)$ *is absolutely irreducible and* $f(X)$ *is not EAPN.*

Theorem 9 (Delgado, Janwa and Agrinsoni [13] (2023))

Let $f(X) = X^{2^{2k}-2^k+1} + h(X) \in \mathbb{F}_{2^m}[X]$, $d = \deg(h)$, *and* $d \equiv 2^{n-1} + 1 \pmod{2^n}$. *If* $d < 2^{2k} - 2^k(2^n - 1) - 1$, $2 \leq n < k - 1$ *and* $(\phi_{2^{2k}-2^k+1}, \phi_d) = 1$, *then* $\phi(X, Y, Z)$ *is absolutely irreducible, and* $f(X)$ *is not EAPN.*

Even Degree Case

Theorem 10 (Aubry McGuire and Rodier [4] (2010))

Let $f(X) \in \mathbb{F}_{2^m}[X]$*, where* $\deg(f) = 2e$ *with* e *odd, and if* f *contains a term of odd degree, then* f *is not APN over* $\mathbb{F}_{2^{mn}}$ *for all* n *sufficiently large.*

Theorem 11 (Caullery [7] (2014))

Let $f(X) = X^{4e} + h(X)$*, where* $\deg(f) = 4e$*,* $e > 1$ *odd. If* e *is not Gold or Kasami then* $f(X)$ *is not an exceptional APN.*

Theorem 12 (Aubry, Issa and Herbaut [3] (2023))

Let $n = 2^r(2^\ell + 1)$*, where* $\gcd(r, \ell) \leq 2$*,* $r \geq 2$ *and* $\ell \geq 1$*. Let* $f(X) = X^n + h(X) \in \mathbb{F}_{2^m}[X]$*. If* $\deg(h) = n - 1$*, then* f *is not EAPN.*

Structure of $\phi_d(X, Y, Z)$

Structure of $\phi_d(X, Y, Z)$

Janwa and Wilson [22] show that If $e \equiv 3 \pmod 4$, then $\phi_e(X, Y, Z)$ is absolutely irreducible. For Gold and Kasami monomial, we have, then

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

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

where $P(X, Y, Z) \in \mathbb{F}_{2^n}(X, Y, Z)$, $\deg(P_\alpha) = 2^n + 1 \; \forall \; \alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2$.

Structure of $\phi_d(X, Y, Z)$

Janwa and Wilson [22] show that If $e \equiv 3 \pmod 4$, then $\phi_e(X, Y, Z)$ is absolutely irreducible. For Gold and Kasami monomial, we have, then

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

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

where $P(X, Y, Z) \in \mathbb{F}_{2^n}(X, Y, Z)$, $\deg(P_\alpha) = 2^n + 1 \ \forall \ \alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2$. Aubry, McGuire and Rodier [4] show that

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

where e is odd and $\phi_6(X, Y, Z) = (X + Y)(Y + Z)(X + Z)$.

Multiplicity of the point $(1,1,1)$ in the curve $\phi_d(X,Y,Z)$.

Janwa and Wilson [22]

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

$\nu_{(1,1,1)}(x + \alpha y + (\alpha+1)z) = 1 \ \forall \ \alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2.$

Multiplicity of the point $(1,1,1)$ in the curve $\phi_d(X,Y,Z)$.

Janwa and Wilson [22]

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

$\nu_{(1,1,1)}(x + \alpha y + (\alpha+1)z) = 1 \ \forall \ \alpha \in \mathbb{F}_{2^n} - \mathbb{F}_2$.

Lemma 2 (Janwa, Wilson and McGuire [23])

Let $\phi_n(X,Y,Z) \in \mathbb{F}_2[X,Y,Z]$. *Then*

a) *For* $n \equiv 3 \pmod 4$, $\nu_{(1,1,1)}(\phi_n) = 0$.

b) *For* $n = 1 + 2^l m$, *and* $m > 1$ *is odd.* $\nu_{(1,1,1)}(\phi_n) = 2^l - 2$.

Lemma 3 (Aubry, McGuire and Rodier [4])

c) *For* $n = 2^m e$, $\nu_{(1,1,1)}(\phi_n) = 3(2^m - 1) + 2^m \nu_{(1,1,1)}(\phi_e)$.

Factorization into absolutely irreducible factors

Lemma 4 (Kopparty and Yekhanin 2008, [25])

Suppose $p(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_n]$ *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 absolute irreducible polynomial* $h(\mathbf{X}) \in \mathbb{F}_{q^r}[X_1, \ldots, X_n]$ *of degree* d/r *such that*

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

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

Results: Degree-gap of a Polynomial

Formalization of techniques used by Aubry, McGuire, Rodier, Delgado, and Janwa.

Definition

$F(\mathbf{X}) = F_m(\boldsymbol{X}) + H(\boldsymbol{X})$. We defined the *degree-gap* $\gamma = \gamma(F) = \deg(F) - \deg(H)$. If F is homogenous, then $\gamma(F) = \infty$.

Results: Degree-gap of a Polynomial

Formalization of techniques used by Aubry, McGuire, Rodier, Delgado, and Janwa.

Definition

$F(\mathbf{X}) = F_m(\mathbf{X}) + H(\mathbf{X})$. We defined the *degree-gap* $\gamma = \gamma(F) = \deg(F) - \deg(H)$. If F is homogenous, then $\gamma(F) = \infty$.

Example

$F(X_1, X_2, X_3, X_4, X_5) = \prod_{\alpha \in \mathbb{F}_{2^4}} (X_1 + X_2 + X_3 + (\alpha + 1)X_4 + \alpha X_5) + X_1^{10} + X_2^{10} + X_3^{10} + X_1^5 X_4^5 + X_4^4 X_5^6 + X_2^3 X_3^7 + X_1^2 X_5^5 + X_1^8 + X_2^7 + X_1 X_2 X_3 X_4 X_5 + 1$ defined over $\mathbb{F}_2$. Then, $\gamma(F) = 6$.

An Important Property

Theorem 13 (Agrinsoni, Janwa and Delgado [1])

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. If* $P(\mathbf{X})$ *is a factor of* $F(\mathbf{X})$, *then* $\gamma(P) \geq \gamma(F)$.

Proof

WLOG let F is nonhonmogeneous, $(F_m, H) = 1, \gamma(F) > 1$. Let

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

where $\gamma(Q) \geq \gamma(P)$. Assume that $\gamma(F) > \gamma(P) = \gamma$. Then

$$0 = F_{m-\gamma} = \sum_{i=0}^{\gamma} P_{s-i} Q_{t-\gamma+i}. \quad (1)$$

New Result Degree-gap Property

Proof continuation.

By $\gamma(P)$ we have that $P_{s-1} = \cdots = P_{s-\gamma+1} = 0$ (respectively $Q_{t-1} = \cdots = Q_{t-\gamma+1} = 0$). Substituting these in (1),

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

New Result Degree-gap Property

Proof continuation.

By $\gamma(P)$ we have that $P_{s-1} = \cdots = P_{s-\gamma+1} = 0$ (respectively $Q_{t-1} = \cdots = Q_{t-\gamma+1} = 0$). Substituting these in (1),

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

$\implies P_s Q_{t-\gamma} = Q_t P_{s-\gamma}$. Since $(P_s, Q_t) = 1$ as $F_m(\boldsymbol{X})$ is square free, $P_s \mid P_{s-\gamma}$ that is $P_{s-\gamma} = 0$. A contradiction with $\gamma(P) = j$.
$\therefore \gamma(F) \leq \gamma(P) \leq \gamma(Q)$. □

A new Bound on the Number of Factors and a new Absolute Irreducibility Criterion: MAJOR RESULTS

Corollary 2 (Agrinsoni, Janwa and Delgado [1])

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

A new Bound on the Number of Factors and a new Absolute Irreducibility Criterion: MAJOR RESULTS

Corollary 2 (Agrinsoni, Janwa and Delgado [1])

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

Corollary 3 (Agrinsoni, Janwa and Delgado [1])

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* $2\gamma(F) > \deg(F)$, *then* $F(\boldsymbol{X})$ *is absolutely irreducible.*

Remaining Cases of the Gold Degree Case Of The Conjecture

Gold pending cases in the literature.

a. $f(X) = X^{2^{k_1}+1} + h(X)$, where $\deg(h) = 2^{k_2} + 1$,
$h(X) = \sum_{j=2}^{m} a_j X^{2^{m_j}(2^{k_j}+1)}$ and $1 < (k_1, \ldots, k_t) = q$, $q \neq (k_1, k_2)$.

b. $f(X) = X^{2^n+1} + h(X)$, where $\deg(h)$ is even and $\deg(h) \geq 2^{n-1} - 1$.

New Result: Completion of the Gold Degree Case of the Exceptional APN Conjecture with Even Degree-gap

Theorem 14 (Agrinsoni, Janwa and Delgado [2])

Let $f(X) = X^{2^{k_1}+1} + h(X) \in \mathbb{F}_{2^m}[X]$*, where* $\deg(h)$ *is odd, then* ϕ *contains an absolutely irreducible factor and* f *is not an exceptional APN polynomial.*

New Result: Completion of the Gold Degree Case of the Exceptional APN Conjecture with Even Degree-gap

Theorem 14 (Agrinsoni, Janwa and Delgado [2])

Let $f(X) = X^{2^{k_1}+1} + h(X) \in \mathbb{F}_{2^m}[X]$, *where* $\deg(h)$ *is odd, then* ϕ *contains an absolutely irreducible factor and* f *is not an exceptional APN polynomial.*

Proof.

We may assume from previous classifications, that if $h(x) \neq \sum_{j=2}^{t} a_j x^{2^{c_j}(2^{k_j}+1)}$ with $1 < (k_1, \ldots, k_t) = q \neq (k_1, k_2)$, then f is not exceptional APN from **Delgado and Janwa** [11, 12, 26]. If $h(x) = \sum_{j=2}^{t} a_j x^{2^{c_j}(2^{k_j}+1)}$, $(k_1, \ldots, k_t) = q$, and $q \neq (k_1, k_2)$. Let $\psi(X, Y, Z) = (\phi_{2^{k_1}+1}, \phi_h)(X, Y, Z)$. Then $\phi_f(X, Y, Z) = \psi(X, Y, Z)H(X, Y, Z)$. Then, by Corollary 3 (the degree-gap corollary), $H(X, Y, Z)$ is absolutely irreducible. □

Factorization of ϕ_f and Some Fundamental Identities

Let $f(X) = X^{2^n+1} + h(X)$, where $h(X) = \sum_{i=1}^{d} \alpha_i x^i$ and $\alpha_d \neq 0$. Assume $\phi_f(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0)$, where $s \geq t$, and $s + t = 2^n - 2$. Then

$$\phi_{2^n+1}(X,Y,Z) = P_s(X,Y,Z)Q_t(X,Y,Z). \tag{2}$$

Therefore, $\nu_{(1,1,1)}(Q_t) = t$ and $\nu_{(1,1,1)}(P_s) = s \geq 2^{k-1} - 1$.
By Theorem 13 we have

$$\alpha_d \phi_d(X,Y,Z) = P_s Q_{t-\gamma} + P_{s-\gamma} Q_t \tag{3}$$

Consider the term of degree $2^n - 2 - 2\gamma$, then we can derive the following equation:

$$\alpha_{2^n-2-2\gamma}\phi_{2^n-2-2\gamma}(X,Y,Z) = P_s Q_{t-2\gamma} + P_{s-\gamma} Q_{t-\gamma} + P_{s-2\gamma} Q_t. \tag{4}$$

Factorization of ϕ_f and Some of the Fundamental Identities (continued...)

Factorization of ϕ_f and Some Fundamental Identities

If $\nu_{(1,1,1)}(P_s) > \nu_{(1,1,1)}(\phi_d)$, then we have that $\nu_{(1,1,1)}(\phi_d) = \nu_{(1,1,1)}(P_{s-\gamma}Q_t)$. Furthermore, by Equation 3 we have

$$\alpha_d t_{\phi_d,1}(X,Y,Z) = t_{P_{s-\gamma},1}(X,Y,Z)t_{Q_t,1}(X,Y,Z). \tag{5}$$

We can classify the translation of ϕ_n by the point $(1,1,1)$:

1. $\phi_{2^n+1}(X+1,Y+1,Z+1) = \prod_{\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(X+1+\alpha(Y+1)+(\alpha+1)(Z+1)) = \prod_{\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(X+\alpha Y+(\alpha+1)Z) = \phi_{2^n+1}(X,Y,Z)$. Moreover, $X+1+\alpha(Y+1)+(\alpha+1)(Z+1) = X+\alpha Y+(\alpha+1)Z$. Therefore, $t_{Q_t,1}(X,Y,Z) = Q_t(X,Y,Z)$.
2. $\phi_6(X+1,Y+1,Z+1) = \phi_6(X,Y,Z) = (X+Y)(Y+Z)(X+Z)$. Thus $t_{\phi_6,1} = \phi_6(X,Y,Z)$.

Gold Even Case 3 (mod 4)

Proposition 4 (Agrinsoni, Janwa and Delgado [2])

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* $j \geq 3$*, then* $\phi_f(X, Y, Z)$ *is absolutely irreducible.*

Proof.

Assume that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$. Then

$$\alpha_{2^{n-j}e}\phi_{2^{n-j}e}(X, Y, Z) = P_s Q_{t-\gamma} + P_{s-\gamma} Q_t \tag{6}$$

Now $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = \nu_{(1,1,1)}(\phi_6^{2^{n-j}-1}) + \nu_{(1,1,1)}(\phi_e^{2^{n-j}}) = 3(2^{n-j} - 1) < 2^{n-1} - 1 \leq s$. Therefore,

$$\alpha_{2^{n-j}e} t_{\phi_{2^{n-j}e},1}(X, Y, Z) = t_{P_{s-\gamma},1}(X, Y, Z)Q_t(X, Y, Z).$$

Now, since $\nu_{(1,1,1)}(\phi_e) = 0$, we have $\deg(t_{\phi_e^{2^{n-j}},1}) = 0$. Therefore, $t_{\phi_{2^{n-j}e},1} = \beta t_{\phi_6^{2^{n-j}-1},1} = \beta\phi_6^{2^{n-j}-1}$. This is a contradiction. □

Gold Even Case 3 (mod 4) (The Really Hard Case)

Proposition 5 (Agrinsoni, Janwa and Delgado [2])

Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$*, where* $\deg(h) = 2^{n-2}(3)$*, and then* $\phi_f(X, Y, Z)$ *contains an absolutely irreducible factor defined over* $\mathbb{F}_q$*.*

Proof Outline.

Let $\gamma = \gamma(\phi_f) = 2^{n-2} + 1$. By Corollary 2 $\phi_f(X, Y, Z)$ have at most 3 factors. WLOG assume $\phi_f(X, Y, Z)$ is irreducible. **Two Factors:** By Lemma 4 assume that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$, where $Q(X, Y, Z) = \sigma(P(X, Y, Z))$, and $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Then we have

$$\alpha_{2^n - j_e}\phi_{2^n - j_e}(X, Y, Z) = P_s Q_{t-\gamma} + P_{s-\gamma} Q_t,$$

$$\alpha_{2^n-2-2\gamma}\phi_{2^n-2-2\gamma}(X, Y, Z) = P_{s-\gamma} Q_{t-\gamma}.$$

This is a contradiction.

The product, of three conjugates, gates several pages long.

□

Gold Even Case 1 (mod 4)

Proposition 6

Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$, *where* $\deg(h) = 2^{n-j}e$, $e = 2^\ell m + 1$, $\ell \geq 2$ *and* $m > 1$ *odd. Then* $\phi_f(X, Y, Z)$ *is absolutely irreducible.*

Proof.

Assume that $\phi_f(X, Y, Z) = P(X, Y, Z)Q(X, Y, Z)$. Then

$$\alpha_{2^{n-j}e}\phi_{2^{n-j}e}(X, Y, Z) = P_s Q_{t-\gamma} + P_{s-\gamma} Q_t \tag{7}$$

$\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = \nu_{(1,1,1)}(\phi_6^{2^{n-j}-1}) + \nu_{(1,1,1)}(\phi_e^{2^{n-j}}) =$
$(2^{n-j} - 1)\nu_{(1,1,1)}(\phi_6) + 2^{n-j}\nu_{(1,1,1)}(\phi_e) = 2^{n-j}(2^\ell + 1) - 3 < 2^{n-1} - 1.$
Therefore, $\nu_{(1,1,1)}(\phi_{2^{n-j}e}) = \nu_{(1,1,1)}(P_{s-\gamma}Q_t)$ and

$$\alpha_{2^{n-j}e} t_{\phi_{2^{n-j}e},1}(X, Y, Z) = t_{P_{s-\gamma},1}(X, Y, Z)Q_t(X, Y, Z).$$

$t_{\phi_{2^{n-j}e},1} = \phi_6^{2^{n-j}-1} t_{\phi_e,1}^{2^{n-j}}$, $\deg(Q_t) \geq 2^{n-j+\ell} - 2^{n-j} + 1 > \nu_{(1,1,1)}(\phi_e)$. □

Gold Even Case 1 (mod 4) (continued...)

Proposition 7

Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$*, where* $\deg(h) = 2^{n-j}(2^\ell + 1)$*, and* $\ell \geq 2$*. Suppose that* $\ell \neq j-1$*, then* $\phi_f(X, Y, Z)$ *contains an absolutely irreducible factor defined over* $\mathbb{F}_q$*.*

Proof.

We have $\gamma(\phi_f) > 2^{n-1} - 1$. Let $\psi = (\phi_{2^n+1}, \phi_h)$, then by Corollary 3 we have

$$H(X, Y, Z) = \frac{\phi_f(X, Y, Z)}{\psi(X, Y, Z)},$$

is absolutely irreducible. □

Gold Even Case 1 (mod 4) (continued...)

Proposition 8

Let $f(X) = X^{2^n+1} + h(X) \in \mathbb{F}_q[X]$*, where* $\deg(h) = 2^{n-j}(2^{j-1}+1)$*, and* $j \geq 3$*. Then* $\phi_f(X,Y,Z)$ *contains an absolutely irreducible factor.*

Proof Outline.

$\gamma(\phi_f) = 2^n + 1 - 2^{n-j}(2^{j-1}+1) = 2^{n-1} - 2^{n-j} + 1 > 2^{n-2} + 1$. Let $\psi(X,Y,Z) = (\phi_{2^n+1}, \phi_h)$. Define

$$H(X,Y,Z) = \frac{\phi_f(X,Y,Z)}{\psi(X,Y,Z)},$$

Therefore, by Corollary 2, we have H have at most 3 factors. WLOG assume $\phi_f(X,Y,Z)$ is irreducible. By Lemma 4 assume that $H(X,Y,Z) = P(X,Y,Z)Q(X,Y,Z)$, where $Q(X,Y,Z) = \sigma(P(X,Y,Z))$, and $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. □

Gold Even Case 1 (mod 4) (continued...)

Proof Outline Continuation.

Now we have the following system of equations

$$\phi_{2^n+1}(X,Y,Z) = P_s Q_s \psi,$$

$$\alpha_{2^{n-j}(2^{j-1}+1)}\phi_{2^{n-j}(2^{j-1}+1)}(X,Y,Z) = (P_s Q_{s-\gamma} + P_{s-\gamma} Q_s)\psi,$$

$$\alpha_{2^n-2^{n-j+1}-1}\phi_{2^n-2^{n-j+1}-1}(X,Y,Z) = P_{s-\gamma} Q_{s-\gamma}\psi.$$

If $\alpha_{2^n-2^{n-j+1}-1} \neq 0$, then we get a contradiction as $\phi_{2^n-2^{n-j+1}-1}$ is absolutely irreducible.

If $\alpha_{2^n-2^{n-j+1}-1} = 0$, then WLOG assume $Q_{s-\gamma} = 0$. Then, $\phi_{2^{n-j}(2^{j-1}+1)}(X,Y,Z) = Q_s P_{s-\gamma}\psi$, implies, $Q_s\psi \mid \phi_{2^{j-1}+1}$ which is a contradiction as $\deg(Q_s\psi) \geq 2^{n-1} - 1 > 2^{j-1} - 2$. □

Resolution of the Gold degree Case

Theorem (Agrinsoni, Janwa and Delgado [2] (submitted))

Let $f(X) = x^{2^n+1} + h(X) \in \mathbb{F}_{2^m}[X]$*, where* $\deg(h) < 2^n + 1$*. If* $h(X)$ *is not affine then* $\phi_f(X, Y, Z)$ *contains an absolutely irreducible factor, and* $f(X)$ *is not EAPN.*

1. Investigate the Kasami-Welch case when the second term is even and the multiplicity of the point $(1,1,1)$ in the second term is greater than 2^{n-2}.
3. Investigate the case $4e$ when e is Gold or Kasami and the highest odd degree term has degree $\equiv 1 \pmod 4$.
4. Investigate the case $f(x) = x^{2^n e} + h(x)$, when $n > 3$ and $e > 1$ is odd.

Open Problems and Future Directions

1. Investigate the Kasami-Welch case when the second term is even and the multiplicity of the point $(1, 1, 1)$ in the second term is greater than 2^{n-2}.
3. Investigate the case $4e$ when e is Gold or Kasami and the highest odd degree term has degree $\equiv 1 \pmod 4$.
4. Investigate the case $f(x) = x^{2^n e} + h(x)$, when $n > 3$ and $e > 1$ is odd.
5. Find good irreducibility testing criteria.
6. Find new absolute irreducibility testing criteria.

Acknowledgement

Carlos A. Agrinsoni Santiago's work is supported by the National Aeronautics and Space Administration (NASA) Training Grant No. NNX15AI11H and 80NSSC20M0052. The content is solely the responsibility of the authors and does not necessarily represent the official views of NASA.

References I

[1] Carlos Agrinsoni, Heeralal Janwa, and Moises Delgado.
New absolute irreducibility testing criteria and factorization of multivariate polynomials.
Proceedings in Mathematics and Statistics, 2023.

[2] Carlos Agrinsoni, Heeralal Janwa, and Moises Delgado.
Resolution of the exceptional apn conjecture in the gold degree case.
Designs, Codes and Cryptography. An International Journal, submitted.

[3] Yves Aubry, Ali Issa, and Fabien Herbaut.
Polynomials with maximal differential uniformity and the exceptional apn conjecture.
Journal of Algebra, 635:822–837, 2023.

[4] 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.

References II

[5] Thomas Beth and Cunsheng Ding.
On almost perfect nonlinear permutations.
In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[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] Florian Caullery.
Polynomials over finite fields for cryptography.
2014.

[8] 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.

References III

[9] Moises Delgado and Heeralal Janwa.

Progress towards the conjecture on apn functions and absolutely irreducible polynomials.

arXiv preprint arXiv:1602.02576, 2016.

[10] 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.

[11] Moises Delgado and Heeralal Janwa.

On the conjecture on APN functions and absolute irreducibility of polynomials.

Des. Codes Cryptogr., 82(3):617–627, 2017.

[12] 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.

References IV

[13] Moises Delgado, Heeralal Janwa, and Carlos Agrinsoni.
Some new techniques and progress towards the proof on the conjecture on exceptional apn functions and absolutely irreducible polynomials.
Designs, Codes and Cryptography. An International Journal, 2023.

[14] Hans Dobbertin.
Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Niho case.
Inform. and Comput., 151(1-2):57–72, 1999.

[15] Hans Dobbertin.
Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Welch case.
IEEE Trans. Inform. Theory, 45(4):1271–1275, 1999.

[16] Hans Dobbertin.
Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: a new case for n divisible by 5.
In *Finite fields and applications (Augsburg, 1999)*, pages 113–121. Springer, Berlin, 2001.

References V

[17] 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.

[18] 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.

[19] R. Gold.

Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.).

IEEE Transactions on Information Theory, 14(1):154–156, 1968.

References VI

[20] Robin Hartshorne.
Algebraic geometry.
Springer-Verlag, New York-Heidelberg, 1977.
Graduate Texts in Mathematics, No. 52.

[21] 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.

[22] 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.

References VII

[23] 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.

[24] David Jedlicka.
APN monomials over $\mathrm{GF}(2^n)$ for infinitely many n.
Finite Fields Appl., 13(4):1006–1028, 2007.

[25] 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.

[26] Delgado Moises and Heeralal Janwa.
On the decomposition of generalized fermat varieties in p^3 corresponding to kasami-welch functions.
Congress Numerantium, 2017.

References VIII

[27] 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.

[28] 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.

[29] 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.