International Journal of Algebra, Vol. 18, 2024, no. 1, 15 - 30
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2024.91851

Construction of the First Nonmonomial Exceptional APN and Solution of a Conjecture Plus the Core Cases of a Second

Roberto C. Reyes Carranza

Department of Mathematics
Long Island University, Brooklyn Campus
1 University Plaza
Brooklyn, NY 11201 USA

Mathematics Department
Manhattan College
4513 Manhattan College Parkway
Riverdale, NY 10471 USA

Abstract

Discovering a key (function) especially resistant to differential attacks, required by cryptographic systems as investigated by Nyberg, encompasses the race for security with the discovery of Almost Perfect Non-linear (APN) functions being a priority. Here we build for the first time an Exceptional APN function (APN over infinite field extensions) not belonging to the Gold or Kasami-Welch class, $J : \bigcup_{l=1}^{\infty} \mathbb{F}_{p^{\Pi_{k=0}^{l} n_k}} \rightarrow \bigcup_{l=1}^{\infty} \mathbb{F}_{p^{\Pi_{k=0}^{l} n_k}}$. The other leading conjecture (stated by Budaghyan, Carlet, and Leander) deals with CCZ-inequivalence, we solve it by encompassing the main map—Kasami—along with all known APN power functions regardless of whether the field degree is even or odd. Inside the process we provide a fairly general method.

Mathematics Subject Classification: 11T06, 12E20, 11T71

Keywords: Almost Perfect Nonlinear, CCZ-equivalence, S-Box, Field

1 Introduction

Almost Perfect Non-linear (APN) functions are enormously interesting functions having the highest possible non linearity in the sense of violating the additivity property (part of the definition of a linear function) over as many subsets of the field $\mathbb{F}_{2^n}$ as possible. Nyberg [9, 17] proved that APN functions have the property of being highly resistant against differential cryptanalytic attacks when they are used as S-Boxes in block ciphers. Among the experts involved in this topic it is worth mentioning Janwa, Delgado, Dillon, McGuire, Aubry, Wilson, Frard, Oyono, Canteaut, Jedlika, Hernando, Caullery, Rodier, Anbar, Kalayc, and Yurdakul [1, 2, 6, 8, 12, 14, 16]. All these years the business has focused on identifying that more classes of functions do not qualify to be Exceptional APN (refer to Definition 1.1), which has become a real challenge for worldwide laboratories facing the investigation of the security and privacy. The complementary direction (our approach) consists in finding the existence of an Exceptional APN function not equivalent to the two known exceptional APN functions, achieving a double goal of classifying highly non-linear functions and the research of the non-linearity phenomena in science. Regarding non exceptional APN functions, Delgado [7] provides an overview of the methods used for the resolved cases and covers a new Gold degree member. Let $i \in [0, 2^n - 1]$ be an integer, then its 2-weight ($w_2(i) = \sum_{s=0}^{n-1} i_s$) is the number of ones in its binary representation ($i = \sum_{s=0}^{n-1} i_s 2^s$, where $i_s \in \{0, 1\}$). Let f be a univariate polynomial on $\mathbb{F}_{2^n}$, then its *algebraic degree* is calculated as follows: $d^0(f) = \max\{w_2(i); i \text{ is the exponent of a term in } f\}$. If f has algebraic degree 1, 2, or 3, it is called affine (linear if $f(0) = 0$), quadratic, or cubic, respectively.

Definition 1.1 *[2, 3, 17] Let G_1 and G_2 be finite Abelian groups. A function $f : G_1 \to G_2$ is differentially δ-uniform if $\forall a \in G_1 - \{0\}$ and $b \in G_2$, the equation $\Delta_a f(x) = b$ admits at most δ solutions, where $\Delta_a f(x) := f(x + a) - f(x)$. The set $\{\delta_f(a, b); a \in G_1 - \{0\}, b \in G_2\}$ is called the differential spectrum of f, where $\delta_f(a, b) =\mid \{x \in G_1; \Delta_a f(x) = b\} \mid$. For (the optimal δ-value) $\delta = 2$, $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called APN (almost perfect nonlinear). Moreover, if it is APN on infinitely many extensions of $\mathbb{F}_{2^n}$, f is called exceptional APN.*

Table 1: Current Monomial APN functions over $\mathbb{F}_{2^n}$ [11, 13, 17]

$f(x) = x^t$	Exponent t	Constraints	Nonlinearity
Gold	$2^r + 1$	$\gcd(r, n) = 1$	$2^{n-1} - 2^{(n-1)/2}$, n odd
			$2^{n-1} - 2^{n/2}$, n even
Kasami-Welch	$2^{2r} - 2^r + 1$	$\gcd(r, n) = 1$	$2^{n-1} - 2^{(n-1)/2}$, n odd
			$2^{n-1} - 2^{n/2}$, n even
Welch	$2^\omega + 3$	$n = 2\omega + 1$	$2^{n-1} - 2^{(n-1)/2}$
Niho	$2^\omega + 2^{\omega/2} - 1$	$n = 2\omega + 1$, ω even	
	$2^\omega + 2^{(3\omega+1)/2} - 1$	$n = 2\omega + 1$, ω odd	
Inverse	$2^{2\omega} - 1$	$n = 2\omega + 1$	
Dobbertin	$2^{4s} + 2^{3s} + 2^{2s} + 2^s - 1$	$n = 5s$	

1.1 The Exceptional APN Conjecture

Historically, Janwa, McGuire, and Wilson [14, 16] gave the first version of the exceptional APN conjecture as follows, **Conjecture 1** *The only exceptional values for t are the Gold and KasamiWelch numbers.* Later, Dillon [10, 14] from the NSA stated an equivalent version of Conjecture 1. This conjecture corresponds to when a monomial function $f(x) = x^t$ is exceptional APN. Hernando and McGuire [14] established that this conjecture is veridical—becoming an important theorem. Lately in 2010, Aubry, McGuire and Rodier [2] scaled up the conjecture to cover more general Exceptional APN functions. **Conjecture 2** (current version) Up to equivalence, the Gold and Kasami-Welch functions are the only exceptional APN functions. Below we list few relevant results in regard to the exceptional APN conjecture:

Theorem 1.2 *(Frard, Oyono and Rodier [12]) Suppose that* $f(x) = x^{2^{2k}-2^k+1} + g(x) \in \mathbb{F}_{2^n}[x]$. *Then:*

a). If $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$ *and there exist a nonzero coefficient* a_j *of* g *such that* $\phi_j(x, y, z)$ *is absolutely irreducible. Then* f *is not exceptional APN.*

b). If $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 2$, *where* $k \geq 3$ *is odd and relatively prime to* n. *If* $g(x)$ *does not have the form* $ax^{2^{2k-1}-2^{k-1}+2} + a^2x^3$ *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 1.3 *(Delgado, Janwa [7, 8]) For* $k \geq 2$, *let* $f(x) = x^{2^k+1} + h(x) \in \mathbb{F}_{2^n}[x]$, *where any of the following is true:*

a). $\deg(h) \equiv 3 \mod (4) < 2^k + 1$.

b). $\deg(h) \equiv 1 \mod (4) < 2^k + 1$. *If* ϕ_{2^k+1} *and* ϕ_d *are relatively prime, or* $\deg(h)$ *is not a Gold number.*

c). $\deg(h) = 2^s + 1 < 2^k + 1$. *If* $(k, s) \neq 1$ *and* h *contains a term of degree* m *such that* $(\phi_{2^k+1}, \phi_m) = 1$, *or* $(k, s) = 1$.

Then f *is not exceptional APN.*

Caullery [6] investigated the case of not exceptional APN polynomials of degree $4e$ with $e > 3$. Anbar et al. [1] have added new not exceptional APN functions of Gold and Kasami-Welch type. Since the appearance of Conjecture 2, every effort has been made to show that most functions belonging to the class of polynomials cannot be APN on an infinite sequence of field extensions. In this article, we investigate the complementary direction centered on demonstrating the existence of an new Exceptional APN function.

1.2 Conjecture about CCZ-Equivalence

Definition 1.4 *[3, 18] Let the functions* $F, F', A_1, A_2, A_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, *where* A_3 *is affine,* A_1 *and* A_2 *are affine permutations, and* $G_F = \{(x, F(x)); x \in \mathbb{F}_{2^n}\}$ *denotes the graph of the function* F. *Then:*

1). F and $A_1 o F o A_2$ are called affine equivalent (A-Equivalent).

2). F and $A_1 o F o A_2 + A_3$ are called extended affine equivalent (EA-Equivalent)

3). F and F' are called Carlet-Charpin-Zinoviev equivalent (CCZ-Equivalent) if there exists an affine permutation L of $(\mathbb{F}_2^n)^2$ between their graphs, i.e. $L(G_F) = G_{F'}$.

Theorem 1.5 *[5] The algebraic degree is preserved by EA-equivalence, but the differential spectrum is a CCZ-invariant.*

Theorem 1.6 *[4, 18] Let $Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$ the trace function from $\mathbb{F}_{2^n}$ onto its subfield $\mathbb{F}_{2^m}$. Then the function $F_n(x) = x^3 + Tr_n^1(x^9)$ is:*

a). APN on $\mathbb{F}_2^n$ for each dimension n.

b). CCZ-inequivalent to the Gold, inverse and Dobbertin APN functions on $\mathbb{F}_{2^n}$ when $n \geq 7$.

c). EA-inequivalent to power functions on $\mathbb{F}_{2^n}$ when $n \geq 7$.

d). CCZ-inequivalent to power functions on $\mathbb{F}_{2^7}$.

EA-equivalence implies CCZ-equivalence, but not vice versa. In [3], Budaghyan and Carlet present a collection of known classes of quadratic APN polynomials CCZ-inequivalent to power functions, but none of those functions can be Exceptional APN, because their formulas are directly tied to the degree of the finite field. The next important conjecture was stated by Budaghyan, Carlet, and Leander, and is solved in Section 2. **Conjecture 3** [4] For $n \geq 7$, $F_n(x) = x^3 + Tr_n^1(x^9)$ is CCZ-inequivalent to any power function ($F'(x) = x^t$).

2 Taking both Conjectures by the horns

The switching neighbors $F_n(x) = x^3 + Tr_n^1(x^9)$ are not necessarily Exceptional APN. The theorem below provides us with initial evidence in this regard based on the domain dependency.

Theorem 2.1 *Let $n = 10k$, $k \geq 1$, and $U_{n+j}(x) = x^3 + Tr_{10k+j}^1(x^9)$, where $j \geq 0$. Then $\Delta(U_{n+0}) = 2$, but $\Delta(U_{n+j}) \geq 4$ on each field extension (of $\mathbb{F}_{2^{10}}$) $\mathbb{F}_{2^n}$, for $j : 1, 2$. In particular, for an infinite number of field extensions $\mathbb{F}_{2^n}$, U_{n+j} are not APN on $\mathbb{F}_{2^n}$, for $j : 1, 2$.*

Proof. We rewrite the functions U_{n+j} as $U_{n+1}(x) = \Phi_1(x) + Tr_{10k}^1(x^9)$ and $U_{n+2}(x) = \Phi_2(x) + Tr_{10k}^1(x^9)$, both functions are on $\mathbb{F}_{2^{10k}}$, where $\Phi_1(x) = x^3 + x^9$ and $\Phi_2(x) = \Phi_1(x) + x^{18}$. It can be shown that $\Phi_1(x)$ and $\Phi_2(x)$ are differentially 8-uniform on $\mathbb{F}_{2^{10}}$ ($\Delta(\Phi_j) = 8$). Let $a \neq 0$ and b both in $\mathbb{F}_{2^{10}}$, such that $\Delta_a(\Phi_j(x)) = b$ has at least the 8 solutions on $\mathbb{F}_{2^{10}}$, $X = \{s_i, s_i + a\}_{i=1}^4$. Let's define $\delta_\epsilon = \Delta_a Tr_{10k}^1(x_\epsilon^9) \in \mathbb{F}_2$, where $x_\epsilon \in X$, $\epsilon : 1, \cdots, 8$. Due to the cardinality of $\mathbb{F}_2$, at least four of the δ_ϵ are repeated, say $\delta_{\epsilon_1} = \cdots = \delta_{\epsilon_4}$. Then $\Delta_a U_{n+j}(x_{\epsilon_1}) = \cdots = \Delta_a U_{n+j}(x_{\epsilon_4})$. Using the same parameters we used at the beginning, a and b, let's state the equation for the function U_{n+j} below: $\Delta_a U_{n+j}(x) = b + \delta_{\epsilon_1}$ on $\mathbb{F}_{2^{10k}}$. We have that this equation has at least the four solutions x_{ϵ_t}, where $t : 1, 4$. Meaning that, $\Delta(U_{n+j}) \geq 4$. ■

Let us consider $n_0 \in \mathbb{N}$ and $(n_k)_{k=1}^{\infty}$ a sequence of odd numbers other than 1. Let M denote the domain $\mathbb{F}_{2^{n_0}}$ or any of its field extensions of the form $\mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}}$ (for some l), even the union of all its extensions in consideration $\Omega = \bigcup_{l=1}^{\infty} \mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}}$. J_1 and J_2 are functions defined on Ω. Let's define the correspondence below, $J : M \to M$, such that for each input x in M an output is assigned as follows: set $\xi = \sum_{i=0}^{-1+n_0} J_2^{2^i}(x)$. If $\xi \in \mathbb{F}_2$, then define $J(x) = J_1(x) + \xi$, otherwise set $\xi = \sum_{i=0}^{-1+\prod_{k=0}^{1} n_k} J_2^{2^i}(x)$. If $\xi \in \mathbb{F}_2$, then define $J(x) = J_1(x) + \xi$, otherwise set $\xi = \sum_{i=0}^{-1+\prod_{k=0}^{2} n_k} J_2^{2^i}(x)$. If $\xi \in \mathbb{F}_2$, then define $J(x) = J_1(x)+\xi$, otherwise continue this process until ξ belongs to $\mathbb{F}_2$, then set $J(x) = J_1(x)+\xi$. Let $x \in M$, thus x belongs to some field $\mathbb{F}_{2^n}$ ($\geq \mathbb{F}_{2^{n_0}}$). In the scenario that there exists a subfield, $\mathbb{F}_{2^m}$ ($\leq \mathbb{F}_{2^n}$), such that $\Gamma_m = \sum_{i=0}^{m-1} J_2^{2^i}(x)$ belongs to the prime field $\mathbb{F}_2$. Then $z = Tr_n^1(J_2(x))$ accepts a decomposition of the following form, $z = (\Gamma_m)^{2^m} + (\Gamma_m)^{2^{2m}} + \cdots + (\Gamma_m)^{2^{m(\frac{n}{m}-1)}} + \Gamma_m = \Gamma_m$, where the number of terms in this sum is odd. So, the value $J(x)$ exist in $\mathbb{F}_{2^n} (\leq M)$ and is unique. It is, each correspondence (using the same correspondence rule J) $J : M \to M$ is well defined. A function J on M (denoted as $J_{(n_i)_{i=0}^{\infty}}$ or J) can also be seen as a piecewise-defined function. In Section 2.1 we will focus on the mapping J when $J_1(x) = x^{2^\sigma+1}$ (with $\sigma \geq 1$) and $J_2(x) = x^9$. As an example, we can refer to those J that satisfy that $n_{k-1} = m_0$ ($\neq 1$), for some odd m_0, $\forall\ k \in \mathbb{N}$.

2.1 A Universal Method for CCZ-Inequivalence

As can be reviewed in the literature, proving that two functions are or are not CCZ-equivalent could be a headache, both algebraically and through computer software. In the body of Theorem 2.2, we establish a novel way that can be used to prove CCZ-inequivalence between a wide range of classes of functions. The Gold, Dobbertin and Inverse cases were covered by Theorem 1.6. In this section we will cover the Kasami class—well known in this area of research for being so challenging—and all pending cases listed in Table 1. We will focus on the following equation as it plays the central role in the research about the CCZ-equivalence between functions of Conjecture 3.

$$\Big(\sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_i x^{2^i} + \sum_{j\in\mathbb{Z}/n\mathbb{Z}} b_j x^{t2^j} + C\Big)^{2^\sigma+1} - \sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_i' x^{2^i} - \sum_{j\in\mathbb{Z}/n\mathbb{Z}} b_j' x^{t2^j} - C' = -Tr_n^1\Big(\Big(\sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_i x^{2^i} + \sum_{j\in\mathbb{Z}/n\mathbb{Z}} b_j x^{t2^j} + C\Big)^9\Big) \text{(Eq. (I))}$$

where $\sigma \geq 1$. Assuming that F' and F_n are CCZ-equivalent leads us to Eq. (I) (see Theorem 2.2). The coefficient corresponding to any term in Eq. (I) must be equal to zero. Following is the coefficient (equaled to zero)

corresponding to the linear term of degree 2^k:

$$C^{2^\sigma}a_k + a_{k-\sigma}^{2^\sigma}C + a_{k-\sigma-1}^{2^\sigma}a_{k-1} + \boldsymbol{\epsilon}_{r,\frac{n}{3}}\left(b_{k-1+r-\sigma}^{2^\sigma}b_{k-1} + b_{k-1-\sigma}^{2^\sigma}b_{k-1+r}\right) + \boldsymbol{\epsilon}_{r,\frac{n}{2}}\left(a_{k-1+r-\sigma}^{2^\sigma}b_{k-1} + b_{k-1-\sigma}^{2^\sigma}a_{k-1+r}\right) - a_k' + \sum_{\gamma\in\mathbb{Z}/n\mathbb{Z}}\Bigg(C^8a_{k-\gamma} + a_{k-\gamma-3}^8C + a_{k-\gamma-4}^8a_{k-\gamma-1} + \boldsymbol{\epsilon}_{r,\frac{n}{3}}\left(b_{r+k-\gamma-4}^8b_{k-\gamma-1} + b_{k-\gamma-4}^8b_{r+k-\gamma-1}\right) + \boldsymbol{\epsilon}_{r,\frac{n}{2}}\left(a_{r+k-\gamma-4}^8b_{k-\gamma-1} + b_{k-\gamma-4}^8a_{r+k-\gamma-1}\right)\Bigg)^{2^\gamma} = 0.$$

Where $\boldsymbol{\epsilon}_{i,j} \in \mathbb{F}_2$ is the delta of Kronecker. Following is the coefficient (equaled to zero) of the term of degree $t2^k$:

$$b_{k-\sigma}^{2^\sigma}C + C^{2^\sigma}b_k + b_{k-\sigma-1}^{2^\sigma}b_{k-1} + T' - b_k' = 0$$

Where T' brings together all the coefficients of like terms that come from $Tr_n^1\big(\big(\sum_{i=0}^{n-1}a_ix^{2^i} + \sum_{j=0}^{n-1}b_jx^{t2^j} + C\big)^9\big)$. The coefficient of the cubic term with literal part of the form $x^{2^k+2^{r+k}+2^{2r+k}}$ (for large enough values of $r(\neq \frac{n}{2})$) is given by $a_{r+k+1-\sigma}^{2^\sigma}b_k + b_{k-\sigma}^{2^\sigma}a_{r+k+1} + T'' = 0$, this equation connects terms a_l with terms b_k, and T'' gather all the coefficients of like terms coming from $Tr_n^1\big(\big(\sum_{i=0}^{n-1}a_ix^{2^i} + \sum_{j=0}^{n-1}b_jx^{t2^j} + C\big)^9\big)$ (T''' is defined in the same way as T' and T''). Alternatively to $x^{2^k+2^{r+k}+2^{2r+k}}$ (depending on the size of r compared to n, we can focus on one type of term) we can always consider the term $x^{2^{2r+k}+\cdots+2^{r+k}+2^k}$, such that $(n+3)/2 \geq r+2 = d^0(x^{2^{2r+k}+\cdots+2^{r+k}+2^k})$. Other supporting relationships to connect equations can come from $\left(a_{k-\sigma}^{2^\sigma}a_l + a_{l-\sigma}^{2^\sigma}a_k\right)x^{2^k+2^l}$, provided that $\frac{|l-k|}{r} \neq i$, for $i : 0, 3$.

Theorem 2.2 *The function $F_n(x) = x^3 + Tr_n^1(x^9)$ and the Kasami-Welch family of functions $K_r(x) = x^{4^r-2^r+1}$ are CCZ-inequivalent on $\mathbb{F}_{2^n}$, where $n > 7$ and $\gcd(r,n) = 1$. Moreover, F_n is CCZ-inequivalent to both functions, Welch $W(x) = x^{2^\omega+3}$ and Niho $N_\gamma(x) = x^{2^\omega+2^\gamma-1}$, where $n = 2\omega+1$, $\gamma = \frac{3\omega+1}{2}$ if ω is odd, and $\gamma = \frac{\omega}{2}$ if ω is even.*

Proof. We assume that there exists an affine permutation L of $\mathbb{F}_{2^n}^2$ such that $L(G_F) = G_{F'}$, $L'(G_{F'}) = G_F$, $L'(x,y) = \big(\sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_ix^{2^i} + \sum_{j\in\mathbb{Z}/n\mathbb{Z}}b_jy^{2^j} + C, \sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_i'x^{2^i} + \sum_{j\in\mathbb{Z}/n\mathbb{Z}}b_j'y^{2^j} + C'\big)$ (of course the coefficients a_i, a_i', b_j, b_j', C, and C' are in $\mathbb{F}_{2^n}$), and $L' = L^{-1}$. This involves considering the equation $F\big(\sum_{i=0}^{n-1}a_ix^{2^i} + \sum_{j=0}^{n-1}b_jF'^{2^j}(x) + C\big) = \sum_{i=0}^{n-1}a_i'x^{2^i} + \sum_{j=0}^{n-1}b_j'F'^{2^j}(x) + C', \forall x \in \mathbb{F}_{2^n}$, along with a restriction over the a_i, b_j, and F' so that $\tilde{L}_1(x) = \sum_{i=0}^{n-1}a_ix^{2^i} + \sum_{j=0}^{n-1}b_jF'^{2^j}(x) + C$ is a permutation of $\mathbb{F}_{2^n}$. That is, we consider Equation (I) for $F = F_n$ and $\gcd(r,n) = 1$ (to keep the Kasami's APN property, for $F' = K_r$). The parameter r satisfies $1 \leq r \leq n-1$. By applying the permutation $A_r(x) = x^{2^{2r}}$ we observe that the Kasamis K_{n-r} and K_r are EA-E (so CCZ-E): $(K_{n-r} \circ A_r)(x) = \big(A_{\frac{r}{2}}(x)\big)^{2^n\left(2^{n-r}-1\right)+2^r} = K_r(x)$. Then it is enough to consider

the Kasami sub-list for r running into $1 \leq r \leq \frac{n-1}{2}$. Since K_1 matches a Gold member and F_n is CCZ-inequivalent to Golds, we will consider $r > 1$, namely, $2 \leq r \leq \frac{n-1}{2}$. That is, $\frac{n+1}{2} \geq d^0(K_r) \geq 3$, so K_r is at least a cubic function.

Let (k,l), $(i,j) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2$ such that $\left(\{k,l\} \cap \{i,j\}\right) \cup \left(\{k,j\} \cap \{l,i\}\right) = \varnothing$. Let $C_{t(2^k+2^l)}x^{t(2^k+2^l)}$ denote the term of degree $t(2^k+2^l)$ in Equation (I). Regarding the term $C_{t(2^k+2^l)}x^{t(2^k+2^l)}$ below we will show the property for $t = t_{K_r}$: $t_{K_r}(2^k+2^l) \neq t_{K_r}(2^i+2^j)$, where $t_{K_r} = 2^{2r-1} + \cdots + 2^r + 1$ is the Kasami APN exponent. Let's define $A_v := \{2^{2r+v-1}, \cdots, 2^{r+v}, 2^v\}$. We can see A_v as the result of a translation of A_0 determined by 2^v inside the set $\{2^z; z \in \mathbb{Z}/n\mathbb{Z}\}$ (and $t_{K_r}2^v$ the sum of its points). It can be observed that two different subsets ($A \neq B$) from $\{2^z; z \in \mathbb{Z}/n\mathbb{Z}\}$ cannot have the same sum of their points, namely $\sum_{x\in A} x \neq \sum_{x\in B} x$. The following are all the possible cases that may occur: **Case** $A_k \cap A_l = \varnothing$ and $A_i \cap A_j = \varnothing$: both sets $A_l \cup A_k$ and $A_i \cup A_j$ (both of cardinality equal to $2r+2$) consist of different points, i.e. $A_l \cup A_k \neq A_i \cup A_j$, because $A_i \cup A_j \not\supseteq A_l$. Then they have different sums, $t_{K_r}(2^k+2^l) = \sum_{x\in A_l\cup A_k} x \neq \sum_{x\in A_i\cup A_j} x = t_{K_r}(2^i+2^j)$. **Case** $A_k \cap A_l \neq \varnothing$ and $A_i \cap A_j \neq \varnothing$. The following subcases may occur:

Subcase $2^{r+l} \in \{2^{2r+k-1}, \cdots, 2^{r+k+1}\}$ and $2^{r+j} \in \{2^{2r+i-1}, \cdots, 2^{r+i+1}\}$: obtaining the following result consisting of $r+2$ summands: $t_{K_r}(2^k+2^l) = 2^{2r+l}+2^{2r+k-1}+\cdots+2^{r+k}+2^l+2^k$ (2^{r+l} is absent). Where two noteworthy parts are: the exactly $r-1$ consecutive terms $2^{2r+k-1}+\cdots+2^{r+k}$ and the binomial $2^{2r+l}+2^l$. **If** $2^{2r+l} = 2^k$ and $2^{2r+j} = 2^i$: the result is reduced to $r+1$ summands: $t_{K_r}(2^k+2^l) = 2^{2r+k-1}+\cdots+2^{r+k}+2^l+2^{k+1}$ (2^{r+l} is absent). **If** $2^{2r+l} = 2^k = 2^{l-1}$ and $2^{2r+j} = 2^i = 2^{j-1}$: the result is reduced to r summands: $t_{K_r}(2^k+2^l) = 2^{2r+k-1} + \cdots + 2^{r+k} + 2^{k+2}$ (2^{r+l} is absent). Whether $t_{K_r}(2^k+2^l)$ of these instances is made up of $r+2$, $r+1$, or r terms, the set of terms in $t_{K_r}(2^k+2^l) \not\supseteq \{2^{2r+i-1}, \cdots, 2^{r+i}\}$ (2^{r+j} is absent). Then Set of terms in $t_{K_r}(2^k+2^l) \neq$ Set of terms in $t_{K_r}(2^i+2^j)$. Then $t_{K_r}(2^k+2^l) = \sum_{x \in \text{ Set of terms in } t_{K_r}(2^k+2^l)} x \neq \sum_{x \in \text{ Set of terms in } t_{K_r}(2^i+2^j)} x = t_{K_r}(2^i+2^j)$. The only possible degenerate subcase would occur when simultaneously $2^{r+l} = 2^{r+k+1}$, $2^{r+j} = 2^{r+i+1}$, and $2r = n$. Obtaining the following result of $r+1$ summands: $t_{K_r}(2^k+2^l) = 2^{2r+k-1}+\cdots+2^{r+k}+2^{l+1}+2^k$ (2^{r+l} is absent), such that the set of terms in $t_{K_r}(2^k+2^l) \not\supseteq \{2^{2r+i-1}, \cdots, 2^{r+i}\}$ (2^{r+j} is absent). We can disregard this degenerate subcase because the Kasami class will require that $2 < 2r < n$.

Subcase $2^l \in \{2^{2r+k-1}, \cdots, 2^{r+k}\}$ and $2^j \in \{2^{2r+i-1}, \cdots, 2^{r+i}\}$:

If $2^l = 2^{r+k}$ and $2^j = 2^{r+i}$. We get: $t_{K_r}(2^k+2^l) = 2^{2r+l} + 2^k$, whose terms form a set of cardinality 2. But **if** $3r = n$, the power $x^{(2^k+2^l)t_{K_r}}$ becomes linear with $(2^k+2^l)t_{K_r} = 2^{k+1}$.

If $2^l \in \{2^{2r+k-1}, \cdots, 2^{r+k+1}\}$ and $2^j \in \{2^{2r+i-1}, \cdots, 2^{r+i+1}\}$: the following possible subcases take place:

Subcase $2^k \notin \{2^{2r+l-1}, \cdots, 2^{r+l}\}$ and $2^i \notin \{2^{2r+j-1}, \cdots, 2^{r+j}\}$:

$t_{K_r}(2^k + 2^l) = 2^{2r+l-1} + \cdots + 2^{r+l} + 2^{2r+k} + 2^{l-1} + \cdots + 2^{r+k} + 2^k$, where $r+3 \leq$ number of terms in $t_{K_r}(2^k+2^l) \leq 2r+1 \leq n$. A feature of $t_{K_r}(2^k+2^l)$ that distinguishes it is that it contains r consecutive terms: $2^{2r+l-1}+\cdots+2^{r+l}$. The set of terms in $t_{K_r}(2^k + 2^l) \not\supseteq \{2^{2r+j-1}, \cdots, 2^{r+j}\}$, then $t_{K_r}(2^k + 2^l) = \sum_{x \in \text{ Set of terms in } t_{K_r}(2^k+2^l)} x \neq \sum_{x \in \text{ Set of terms in } t_{K_r}(2^i+2^j)} x = t_{K_r}(2^i + 2^j)$.

Subcase $2^k \in \{2^{2r+l-1}, \cdots, 2^{r+l}\}$ and $2^i \in \{2^{2r+j-1}, \cdots, 2^{r+j}\}$. We get the following expression: $t_{K_r}(2^k + 2^l) = 2^{2r+l} + 2^{k-1} + \cdots + 2^{r+l} + 2^{2r+k} + 2^{l-1} + \cdots + 2^{r+k}$ (of at most $2r$ terms and at least 4 terms, if $2^k \neq 2^{r+l}$), where each part $2^{k-1} + \cdots + 2^{r+l}$ and $2^{l-1} + \cdots + 2^{r+k}$ contains at most $r-1$ terms. Set of terms in $t_{K_r}(2^k + 2^l) \not\supseteq \{2^{2r+j}, 2^{r+j}, 2^{2r+i}, 2^{r+i}\}$ (provided that $r \neq n/2$ and $2^k \neq 2^{r+l}$), then Set of terms in $t_{K_r}(2^k+2^l) \neq$ Set of terms in $t_{K_r}(2^i+2^j)$. Thus $t_{K_r}(2^k + 2^l) \neq t_{K_r}(2^i + 2^j)$. In particular, **if** occurs that $2^k = 2^{r+l}$ and $2^i = 2^{r+j}$, then we get the degenerate case $t_{K_r}(2^k+2^l) = 2^{2r+k}+2^l$. **If** $3r = n$, then $(2^k + 2^l)t_{K_r} = 2^{l+1}$. On the other hand, if we perform the comparison with respect to the cases at the beginning of $r+2$, $r+1$, and r terms, we highlight that: the common subset $\{2^{2r+i-1}, \cdots, 2^{r+i}\}$ (2^{r+j} is absent) present in those subcases is not contained by the set of terms in $t_{K_r}(2^k + 2^l) = \{2^{2r+l}, 2^{k-1}, \cdots, 2^{r+l}, 2^{2r+k}, 2^{l-1}, \cdots, 2^{r+k}\}$. Hence $t_{K_r}(2^k + 2^l) \neq t_{K_r}(2^i + 2^j)$.

These cases suggest us adding certain conditions to consider only $C_{t(2^k+2^l)}x^{t(2^k+2^l)}$ (for $t = t_{K_r}$) such that $d^0(x^{t(2^k+2^l)}) > 2$, in this way we avoid adding coefficients of like terms—quadratic or linear—that might not come from $C_{t_{K_r}(2^k+2^l)}x^{t_{K_r}(2^k+2^l)}$. In general we can talk about K_r that are differentially $\delta(\geq 4)$-uniform or those that are APN ($\gcd(r, n) = 1$). The APN property of our K_r frees us from the linear cases (since $\gcd(r, 3r) \neq 1$). In the scenario that (k, l) and (i, j) belong to different cases or subcases, the set of terms in $t_{K_r}(2^k + 2^l)$ cannot be the same as that of $t_{K_r}(2^i + 2^j)$, due to their cardinalities are different or due to a particular difference, accordingly $t_{K_r}(2^k + 2^l) \neq t_{K_r}(2^i + 2^j)$.

Next, let us prove the inequality $t_W(2^k + 2^l) \neq t_W(2^i + 2^j)$ for the Welch exponent, $t_W = 2^{\frac{n-1}{2}} + 2 + 1$, whenever $n = 2\omega + 1$. Let's define $A'_v := \{2^{\frac{n-1}{2}+v}, 2^{v+1}, 2^v\}$. **Case** $A'_k \cap A'_l = \varnothing$ and $A'_i \cap A'_j = \varnothing$: since k, l, i, and j are all different parameters on $\mathbb{Z}/n\mathbb{Z}$, we have that $A'_l \cup A'_k$ and $A'_i \cup A'_j$ (each union of cardinality 6) satisfy $A'_l \cup A'_k \not\supseteq \{2^{i+1}, 2^i, 2^{j+1}, 2^j\}$, i.e. $A'_l \cup A'_k \neq A'_i \cup A'_j$. Then $t_W(2^k+2^l) \neq t_W(2^i+2^j)$. **Case** $A'_k \cap A'_l \neq \varnothing$ (and $A'_i \cap A'_j \neq \varnothing$): without loss of generality, the only possibilities that can happen are of the three types below:

If $2^{\frac{n-1}{2}+l} = 2^k$ and $2^{\frac{n-1}{2}+j} = 2^i$, then $t_W(2^k+2^l) = 2^{l+1}+2^l+2^{\frac{n-1}{2}+k}+2^{k+2}$ (contains 4 terms whenever $n > 5$, and size 1 for $n = 5$). Based on the shape of the sets, it can be seen that $\{2^{l+1}, 2^l, 2^{\frac{n-1}{2}+k}, 2^{k+2}\} = \{2^{\frac{n+3}{2}+l}, 2^{l+1}, 2^l, 2^{l-1}\} \neq \{2^{\frac{n+3}{2}+i}, 2^{i+1}, 2^i, 2^{i-1}\}$ (remains valid if j is used instead of i), for $n \geq 5$.

If $2^{\frac{n-1}{2}+l} = 2^{k+1}$ and $2^{\frac{n-1}{2}+j} = 2^{i+1}$, then $t_W(2^k+2^l) = 2^{l+1}+2^l+2^{\frac{n-1}{2}+k}+$

$2^{k+2}+2^k$ (has 5 terms if $n>5$, but contains 3 terms for $n=5$), where $\{2^{l+1},2^l,2^{\frac{n-1}{2}+k},2^{k+2},2^k\} = \{2^{\frac{n+1}{2}+l},2^{\frac{n-3}{2}+l},2^{l+1},2^l,2^{l-2}\} \not\supseteq \{2^{i+1},2^i,2^{i-2}\}$, for $n>5$. For $n=5$, $t_W(2^k+2^l)=2^{l+2}+2^l+2^{l-1}$ is such that $\{2^{l+2},2^l,2^{l-1}\} \neq \{2^{i+2},2^i,2^{i-1}\}$ (both facts remains valid if j is used instead of i).

If $2^l=2^{k+1}$ and $2^j=2^{i+1}$, then $t_W(2^k+2^l)=2^{\frac{n+1}{2}+k}+2^{\frac{n-1}{2}+k}+2^{k+3}+2^k$ (has 4, 2, 3, and 1 terms, granted that $n>7$, $n=7$, $n=5$, and $n=3$, respectively). Since $k\neq i$ on $\mathbb{Z}/n\mathbb{Z}$, it is true that $\{2^{\frac{n+1}{2}+k},2^{\frac{n-1}{2}+k},2^{k+3},2^k\} \neq \{2^{\frac{n+1}{2}+i},2^{\frac{n-1}{2}+i},2^{i+3},2^i\}$, except for $n=5$. Let us note that $t_W(2^k+2^l)$ does not contain 3 consecutive addends as occurs with the previous case of the same cardinality (4, for values $n>7$). No matter which of the four previous Welch's cases it is, we have: $t_W(2^k+2^l)\neq t_W(2^i+2^j)$. If (k,l) and (i,j) belong to different cases, $t_W(2^k+2^l)$ cannot coincide with $t_W(2^i+2^j)$, because their number of terms differ or due to a peculiar feature as happens between the two cases of 4 terms—where $t_W(2^k+2^l)$ contains 3 consecutive addends in one case but 2 in the other— so $t_W(2^k+2^l)\neq t_W(2^i+2^j)$.

Concerning the Niho function: $F'=N_\gamma$, provided $n=2\omega+1$. Its exponent can be rewritten as: $t_{N_\gamma}=2^{\frac{3\omega+1}{2}}+2^{\omega-1}+\cdots+2+1$ with $1+\omega$ addends, or $t_{N_\gamma}=2^\omega+2^{\frac{\omega}{2}-1}+\cdots+2+1$ with $\frac{\omega}{2}+1$ addends. Next we will prove that $t_{N_\gamma}(2^k+2^l)\neq t_{N_\gamma}(2^i+2^j)$ using Reductio ad Absurdum. We will do the proof for $\gamma=\frac{3\omega+1}{2}$, the case $\gamma=\frac{\omega}{2}$ can be demonstrated analogously. Let's assume that $t_{N_\gamma}(2^k+2^l)=t_{N_\gamma}(2^i+2^j)$. Equivalently we have: $2^{\omega+l}+2^{\frac{3\omega+1}{2}+l}+2^i+2^{\omega+k}+2^{\frac{3\omega+1}{2}+k}+2^j=2^{\omega+i}+2^{\frac{3\omega+1}{2}+i}+2^l+2^{\omega+j}+2^{\frac{3\omega+1}{2}+j}+2^k$. Since $i\neq l$ and $i\neq k$, and due to neither ω nor $\frac{3\omega+1}{2}$ is a multiple of n, it follows that $2^i\notin\{2^{\frac{3\omega+1}{2}+i},2^{\omega+i},2^l,2^k\}$. Since the right side of the previous equation is supposed to be equal to the left side, and since 2^i belongs to the left side, then the only possibilities left for 2^i are the following.

Case $2^i=2^{\omega+j}$: analogously, 2^j fulfills $2^j\notin\{2^{\frac{3\omega+1}{2}+j},2^{\omega+j},2^l,2^k\}$. Then only two possibilities can happen: **If** $2^j=2^{\omega+i}$: then n is a factor of 2ω, but this contradicts the fact that $2\omega=n-1$. **If** $2^j=2^{\frac{3\omega+1}{2}+i}$: then n is a factor of $\frac{5\omega+1}{2}=n+\frac{n-3}{4}$, which contradicts $n<n+\frac{n-3}{4}<2n$.

Case $2^i=2^{\frac{3\omega+1}{2}+j}$. Two subcases are possible: **If** $2^j=2^{\omega+i}$: then n is a factor of $n+\frac{n-3}{4}$ (a contradiction). **If** $2^j=2^{\frac{3\omega+1}{2}+i}$: then n is a factor of $3\omega+1=n+\frac{n-1}{2}$ (a contradiction). Then $2^i\notin\{2^{\frac{3\omega+1}{2}+i},2^{\omega+i},2^l,2^k,2^{\omega+j},2^{\frac{3\omega+1}{2}+j}\}$ which contradicts the fact that the summand 2^i should be one of the six summands on the right side of the equation. Consequently, $t_{N_\gamma}(2^k+2^l)\neq t_{N_\gamma}(2^i+2^j)$.

Let $\hat{C}_{t(2^k+2^l)}$ be the part of the coefficient $C_{t(2^k+2^l)}$ that comes from the expansion of $\big(\sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_ix^{2^i}+\sum_{j\in\mathbb{Z}/n\mathbb{Z}}b_jx^{t2^j}+C\big)^{2^\sigma+1}-\sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_i'x^{2^i}-\sum_{j\in\mathbb{Z}/n\mathbb{Z}}b_j'x^{t2^j}-C'$. Based on the inequality discussed above, the function $e_t(k,l)=t(2^k+2^l)$ is injective except for the fact that $e_t(k,l)=e_t(l,k)$ (almost injective), regardless of whether t is either, t_{K_r}, t_W, or t_{N_γ}. Hence $C_{t(2^k+2^l)}=b_{l-\sigma}^{2^\sigma}b_k+b_{k-\sigma}^{2^\sigma}b_l+$

$\sum_{\gamma\in\mathbb{Z}/n\mathbb{Z}}\left(b_{k-3-\gamma}^8 b_{l-\gamma}+b_{l-3-\gamma}^8 b_{k-\gamma}\right)^{2^\gamma}$ and $\hat{C}_{t(2^k+2^l)}=b_{l-\sigma}^{2^\sigma}b_k+b_{k-\sigma}^{2^\sigma}b_l$, if $k\neq l$, regarding Kasami case it is also requested that $2^{l+r}\neq 2^k$ and $2^{k+r}\neq 2^l$. In Eq. (I), the part $Tr_n^1\big(\big(\sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_i x^{2^i}+\sum_{j\in\mathbb{Z}/n\mathbb{Z}}b_j x^{t2^j}+C\big)^9\big)$ is the composition of the trace with a non-linear function, so the square of $\hat{C}_{t(2^k+2^l)}$ result in its successor $\hat{C}_{t(2^{k+1}+2^{l+1})}$. So we obtain recursive relationships of the form:

$$b_{l+1-\sigma}^{2^\sigma}b_{k+1}+b_{k+1-\sigma}^{2^\sigma}b_{l+1}=b_{l-\sigma}^{2^{\sigma+1}}b_k^2+b_{k-\sigma}^{2^{\sigma+1}}b_l^2,\ \text{for any } k\neq l,\ \text{regarding Kasami case the constraints } 2^{l+r}\neq 2^k \text{ and } 2^{k+r}\neq 2^l \text{ are added}\ \ \text{(System (1))}$$

System (1) for $\sigma=1$ constitutes a system of quadratic equations in the variables b_j. Two facts about the b_j's: (**a**). If all b_j's are zero, then due to the form of Eq. (I) and $d^0(x^t)\geq 3$, each b_j' is equal to zero, which is a contradiction to the fact that the quadratic and dependent variable, $F(x)$, can be described as the affine expression $\sum_{i\in\mathbb{Z}/n\mathbb{Z}}a_i' x^{2^i}+C'$. So not every b_j can be zero. (**b**). If $\exists j$ such that $b_j=b_{j+1}=0$: parameters k, l can differ by 1 without violating any of the conditions ($2^{l+r}\neq 2^k$, $2^{k+r}\neq 2^l$) since $r>1$. Hence the equation of System (1), $b_{j+1}^2(b_{j+3}+b_{j+1}^4)=b_{j+2}^2(b_j^4+b_{j+2})$, implies $b_{j+2}=0$. In this way, any b_j is zero (contradicting item (**a**)). Consequently, there cannot be two consecutive b_j's both equal to zero. Let $b_{l''}$ be a non-zero coefficient. From System (1), we have:

$$b_l^2\left(\frac{b_{l''+1}+b_{l''-1}^4}{b_{l''}^2}\right)=b_{l-1}^4+b_{l+1},\text{for any } l\neq l'', l\neq l''\pm r\ \ \text{(Eq. (2))}$$

But we still need to find out if we can arrive at a similar formula for $l=l''$ and $l=l''\pm r$. **Case** $r\neq 1,2$: applying item (**b**) to the consecutive coefficients $b_{l''+1}$ and $b_{l''+2}$ we obtain the following instances.

Subcase $b_{l''+1}\neq 0$: from System (1), we have:

$$b_l^2\left(\frac{b_{l''+2}+b_{l''}^4}{b_{l''+1}^2}\right)=b_{l-1}^4+b_{l+1},\text{for any } l\neq l''+1, l\neq l''+1\pm r\ \ \text{(Eq. (3))}$$

If $2r<n-1$: since $\{l''+1,l''+1\pm r\}\cap\{l'',l''\pm r\}=\varnothing$, Eq. (2) is true for $l=l''+1$. Hence $\frac{b_{l''+1}+b_{l''-1}^4}{b_{l''}^2}=\frac{b_{l''+2}+b_{l''}^4}{b_{l''+1}^2}$. Equation (3) works over $\{l'',l''\pm r\}$, then Eq. (2) is true for any $l\in\mathbb{Z}/n\mathbb{Z}$. Let's define $\chi_j:=\frac{b_{j+1}+b_{j-1}^4}{b_j^2}$, provided $b_j\neq 0$, and $\tilde{\chi}_j:=\frac{a_{j+1}+a_{j-1}^4}{a_j^2}$, if $a_j\neq 0$.

If $2r=n-1$: Eq. (3) is true for $l=l''$ and $l=l''+r$ except for $l=l''-r$. Again $\chi_{l''}=\chi_{l''+1}$. That is, Eq. (2) also becomes true for $l=l'',l''+r$. Let $b_{l'''}\neq 0$ where l''' is one of the consecutives, $l''-2$ or $l''-1$. From System (1), $b_l^2\chi_{l'''}=b_{l-1}^4+b_{l+1}$ for all $l\neq l'''$, $l\neq l'''\pm r$ (then it holds for $l=l''-r$). Since

$l'' \neq l'''$ and $l'' \neq l''' \pm r$, thus $\chi_{l'''} = \chi_{l''}$. Then Eq. (2) holds for ($l'' - r$ and) each $l \in \mathbb{Z}/n\mathbb{Z}$.

Subcase $b_{l''+2} \neq 0$: from System (1), we have:

$$b_l^2 \left(\frac{b_{l''+3} + b_{l''+1}^4}{b_{l''+2}^2} \right) = b_{l-1}^4 + b_{l+1}, \text{for any } l \neq l'' + 2, l \neq l'' + 2 \pm r \quad \text{(Eq. (4))}$$

If $2r + 2 \neq n$: $\{l'' + 2, l'' + 2 \pm r\} \cap \{l'', l'' \pm r\} = \varnothing$ implies Eq. (4) for $l = l''$ (so $\chi_{l''} = \chi_{l''+2}$) and Eq. (2) for $l \in \{l'', l'' \pm r\}$. So Eq. (2) works for all $l \in \mathbb{Z}/n\mathbb{Z}$.

If $2r+2 = n$: $\{l'' + 2, l'' + 2 \pm r\} \cap \{l'', l'' \pm r\} = \{l''-r\}$ (because $l''+2+r = l'' - r$ on $l \in \mathbb{Z}/n\mathbb{Z}$) implies that Eq. (4) is true for $l = l''$ (i.e. $\chi_{l''+2} = \chi_{l''}$) and $l = l'' + r$. Then Eq. (2) also holds for $l = l'', l'' + r$. Let's see what arise for $l = l'' - r$. Let l''' be $l'' - 2$ or $l'' - 1$ so that $b_{l'''} \neq 0$. From System (1), $b_l^2 \chi_{l'''} = b_{l-1}^4 + b_{l+1}$ for all $l \neq l'''$, $l \neq l''' \pm r$ (then l can be l'' or also $l'' - r$). Then $\chi_{l'''} = \chi_{l''}$ and Eq. (2) is true for every $l \in \mathbb{Z}/n\mathbb{Z}$.

Case $r = 2$: using item (**b**) in consecutives $b_{l''+3}$ and $b_{l''+4}$, we split this case into two.

Subcase $b_{l''+3} \neq 0$: from System (1): $b_l^2 \left(\frac{b_{l''+4} + b_{l''+2}^4}{b_{l''+3}^2} \right) = b_{l-1}^4 + b_{l+1}, \text{for any } l \neq l''+3, l \neq l''+3 \pm r$ (Eq. (5)). Being that $\{l'' + 3, l'' + 3 \pm r\} \cap \{l'', l'' \pm r\} = \varnothing$, Eq. (5) is true for $l = l''$, $l = l'' \pm r$. Then $\chi_{l''+3} = \chi_{l''}$, and Eq. (2) is true for any $l \in \mathbb{Z}/n\mathbb{Z}$.

Subcase $b_{l''+4} \neq 0$: from System (1): $b_l^2 \left(\frac{b_{l''+5} + b_{l''+3}^4}{b_{l''+4}^2} \right) = b_{l-1}^4 + b_{l+1}, \text{for any } l \neq l'' + 4, l \neq l'' + 4 \pm r$. The cases $l = l'' + r$ (if $n \geq 8$) and $l = l'' - r$ (only if $n = 8$) still need to be covered. When applying item (**b**) to the pair $b_{l''+1}$, $b_{l''+2}$ the only worrying event occurs when $b_{l''+2} \neq 0$, since the value $l = l'' + r$ still needs to be covered. To solve this issue it is enough to consider the pair $b_{l''-1}$, $b_{l''-2}$. In any of the above cases, whether $r = 2$ or not, we get $b_{l+1} = \chi_{l''} b_l^2 + b_{l-1}^4$, $\forall l \in \mathbb{Z}/n\mathbb{Z}$, referred to any $t \in \{t_{K_r}, t_W, t_{N_\gamma}\}$.

The term of a particular shape (based on the set of powers of two corresponding to its exponent), $x^{2^i + t_{K_r} 2^j}$ for $2 < 2r \leq n$ and $\forall (i, j)$ that satisfies $2^i \notin \{2^{j+r}, 2^{j+r+1}\}$ (to ensure that $d^0(x^{2^i + t_{K_r} 2^j}) \not\leftarrow 3$), owns the following coefficient: $a_{i-\sigma}^{2^\sigma} b_j + b_{j-\sigma}^{2^\sigma} a_i + T''' = 0$. As before, this type of term is the square of its predecessor, resulting in, $a_{i+1-\sigma}^{2^\sigma} b_{j+1} + b_{j+1-\sigma}^{2^\sigma} a_{i+1} = a_{i-\sigma}^{2^{\sigma+1}} b_j^2 + b_{j-\sigma}^{2^{\sigma+1}} a_i^2$, then:

$$a_i^2 (b_{j+1} + b_{j-1}^4) = b_j^2 (a_{i-1}^4 + a_{i+1}) \text{ whenever } \sigma = 1,\ 2^i \notin \{2^{j+r}, 2^{j+r+1}\} \quad \text{(System (2))}$$

We still need to connect the two missing cases, 2^{j+r} and 2^{j+r+1} (alternatively, we could cover them by means of the relationship for the aforementioned cubic term). If $\forall i \in \mathbb{Z}/n\mathbb{Z}$, $a_i = 0$, then $\chi_{l''} a_i^2 = a_{i-1}^4 + a_{i+1}$, $\forall i \in \mathbb{Z}/n\mathbb{Z}$ (next we will obtain this formula when $\exists$ an $a_i \neq 0$). From System (2), we have: $b_j^2 \tilde{\chi}_i = b_{j-1}^4 + b_{j+1}$, for all $j \neq i - r, i - r - 1$. Let l''' be $i - r - 2$ or $i - r - 3$

such that $b_{l'''} \neq 0$ (based on item (**b**)), so $\tilde{\chi}_i = \chi_{l'''}$. From System (2): for all $i \neq l''' + r, l''' + r + 1$ in $\mathbb{Z}/n\mathbb{Z}$, a_{i+1} has the form below:

$$a_{i+1} = a_i^2 \chi_{l'''} + a_{i-1}^4 \quad \text{(Eq. (6))}$$

Let $b_{l'''+3+\epsilon}$ be non-zero, for some $\epsilon \in \{0, 1\}$. From System (2): for any $i \neq l''' + 3 + \epsilon + r$, $l''' + 4 + \epsilon + r$ in $\mathbb{Z}/n\mathbb{Z}$, a_{i+1} has the form below:

$$a_{i+1} = a_i^2 \chi_{l'''+3+\epsilon} + a_{i-1}^4 \quad \text{(Eq. (7))}$$

Eq. (7) is true for $i = l''' + r$ and $i = l''' + r + 1$. So Eq. (6) is too. Then we get Eq. (6), $\forall i \in \mathbb{Z}/n\mathbb{Z}$. Regarding the Niho (in its two versions) and Welch cases, System (2) does not provide information when $i = j$, however Eq. (6) can be obtained analogously to the Kasami's.

We have obtained that $b_k = \chi_{l''} b_{k-1}^2 + b_{k-2}^4$ and $a_k = \chi_{l''} a_{k-1}^2 + a_{k-2}^4$. Let's divide $(\eta + \zeta)$ into two sums, $(\eta + \zeta)(x) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} \chi_{l''} \left(a_{j-1} x^{2^{j-1}} + b_{j-1} x^{t2^{j-1}}\right)^2 + \sum_{j \in \mathbb{Z}/n\mathbb{Z}} \left(a_{j-2} x^{2^{j-2}} + b_{j-2} x^{t2^{j-2}}\right)^4 = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} \chi_{l''} \left(a_i x^{2^i} + b_i x^{t2^i}\right)^2 + \sum_{l \in \mathbb{Z}/n\mathbb{Z}} \left(a_l x^{2^l} + b_l x^{t2^l}\right)^4$ on $\mathbb{F}_{2^n}$, where $\zeta(x) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} b_j x^{t2^j}$, $\eta(x) = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} a_i x^{2^i}$, and $\Lambda = \text{Range}\,(\eta + \zeta) \supseteq \left(\sum_{l \in \mathbb{Z}/n\mathbb{Z}} a_l + b_l\right) \mathbb{F}_2$. In order for $(\eta + \zeta)(x)$ to satisfy the conditions of the quadratic system of equations on the finite field of degree n, this sum must satisfy the following equation: $\eta + \zeta = \chi_{l''} (\eta + \zeta)^2 + (\eta + \zeta)^4$. Hence, the function $\tilde{L}_1(x) = (\eta + \zeta)(x) + C$ cannot be a permutation (contradicting its property of being a permutation) so long as $n \geq 3$. It is enough to choose $n > 7$ so that we do not worry about the fulfillment of any requirements in this theorem. Therefore F_n cannot be CCZ-E to any of the known families: Kasami K_r, Welch $x^{2^{\frac{n-1}{2}}+3}$, and Niho $x^{2^{\frac{n-1}{2}}+2^\gamma-1}$ (all on $\mathbb{F}_{2^n}$). ■

Remark 1 Theorem 2.2 also provides us with another way to prove that F_n is CCZ-inequivalent to the Dobbertin function. The entire method that we have introduced in Theorem 2.2 is general enough in the sense that it can also be applied to polynomials over the finite field as well as to functions that contain a nonlinear Boolean part. This extends the case for $\mathbb{F}_{2^7}$ and solves Conjecture 3 (of Budaghyan et al. in [4]) to all known APN power functions (see Table 1). **Remark 2** The function J agrees with the Budaghyan-Carlet-Leander function $F_n(x) = x^3 + Tr_n^1(x^9)$ —this kind of function is known as a *switching neighbor*, details about it can be found in the PhD Dissertation [18]— over the appropriate field extension $\mathbb{F}_{2^n}$ ($\geq \mathbb{F}_{2^{n_0}}$). Then J is APN on each field extension $\mathbb{F}_{2^{\Pi_{k=0}^l n_k}}$, for each l in $\mathbb{N}$. The CCZ-inequivalence between J and both classes, Gold and Kasami-Welch, guarantees that J is new, namely the first non-monomial Exceptional-APN function. It is interesting to note that J and the Gold x^3 differ by just a Boolean function piecewise-defined throughout the union of the field extensions. This crucial fact, as well as a point of clarification, suggests extending the protagonist functions in Conjecture 2, by

adding to the Gold family (as well as to the Kasami family) a Boolean function piecewise-defined along the field extensions. **Note** Conjecture 2 has been a great motivation for us to do this work. It is crucial that the research continues in both directions with the common aim of determining which functions are Exceptional APN and which are not. **Open problem 1** Discuss the existence of a new form of Exceptional APN function. **Open problem 2** Study the analogous question to the Exceptional APN Conjecture, for differentially δ (≤ 6)-uniform functions. In the next section we establish a practical way to build differentially δ-uniform trinomials over field extensions.

3 Differential δ-Uniformity Across Field Extensions

Theorem 3.1 *If the monomial $X^p : \mathbb{F}_{2^{\mu t}} \to \mathbb{F}_{2^{\mu t}}$ is APN, where $\mu = 3$ (respectively, $\mu = 11$) and $t \geq 1$, then the trinomial $\psi_1(x) = X^p + X^{2p} + X^{4p}$ is differentially 8-uniform over $\mathbb{F}_{2^{\mu t}}$ (respectively, $\mu = 11$). If X^s is differentially δ-uniform over $\mathbb{F}_{2^{r2^m}}$, where $m \geq 0$ and $r : 2, 5, 7, 13$. The trinomial $\psi_2(x) = X^s + X^{2s} + X^{4s}$ is differentially δ-uniform (A-E to X^s).*

Proof. We proceed to prove the case for $\mu = 3$. For $b_0 = 1 \in \mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, the equation $X + X^2 + X^4 = b_0$ has the four solutions $\{X_i\}_{i=1}^4 = \{1, \alpha+1, \alpha^2+1, \alpha^2+\alpha+1\}$. All restrictions of X^p to the subfield $\mathbb{F}_{2^3}$, $X^p|_{\mathbb{F}_{2^3}}$ are the APN monomials over $\mathbb{F}_{2^3}$: Gold X^3 and X^5. Then an equation of the form, $(X + a_0)^p - X^p = X_i$ becomes either $(X + a_0)^3 - X^3 = X_i$ or $(X + a_0)^5 - X^5 = X_i$. Thus, at the direction $a_0 = 1$ and each X_i, the numbers $\delta_{X^p|_{\mathbb{F}_{2^3}}}(1, X_i)$ satisfy: $\delta_{X^3}(1, X_i) = \delta_{X^5}(1, X_i) = 2$. Then at point $(a_0 = 1, b_0 = 1)$: $\delta_{\psi_1}(1, 1) = 4(2) = 8$ solutions. Then the differential uniformity of ψ_1 is lower bounded: $8 = \delta_{\psi_1}(a_0, b_0) \leq \delta_{\psi_1}(a, b)$. On the other hand, since X^p is APN the differential uniformity of ψ_1 is upper bounded by the same previous bound: $\max_{a \in \mathbb{F}_{2^{3t}}, a \neq 0, b \in \mathbb{F}_{2^{3t}}} \delta_{\psi_1}(a, b) \leq 8$. The case for $\mu = 11$ can be demonstrated analogously.

Unlike our previous procedure, we will prove the case for X^s by exploiting the principle of induction. Let's prove the case when $r = 5$. It can be verified that for all b in $\mathbb{F}_{2^5}$, the equation $X + X^2 + X^4 = b$ has at most one solution in $\mathbb{F}_{2^5}$. Let's consider $\mathbb{F}_{2^{10}} = \{a_0 + a_1\Theta;\ a_i \in \mathbb{F}_{2^5}\}$ as an extension of $\mathbb{F}_{2^5}$, where $\Theta^2 = c_0 + c_1\Theta$, $c_i \in \mathbb{F}_{2^5}$. Let's prove the theorem by induction on m. For $\mathbf{m = 1}$, the sentence of the theorem is true. Given any $b_0 + b_1\Theta \in \mathbb{F}_{2^{10}}$, we start by solving the equation, $X + X^2 + X^4 = b_0 + b_1\Theta$, in the variable $X = a_0 + a_1\Theta \in \mathbb{F}_{2^{10}}$. Then, $b_0 + b_1\Theta = a_0 + a_0^2 + a_0^4 + a_1^2c_0 + a_1^4c_0^2 + a_1^4c_1^2c_0 + (a_1 + a_1^2c_1 + a_1^4c_1^2c_1)\Theta$. Then we have the system of equations in the variables a_0, a_1 below:

(1) $a_1 + a_1^2c_1 + a_1^4c_1^3 = b_1$,

(2) $a_0 + a_0^2 + a_0^4 = b_0 + a_1^2c_0 + a_1^4c_0^2 + a_1^4c_1^2c_0$, where c_0 and c_1 are fixed values which define Θ^2. It can be verified that for every $b_1 \in \mathbb{F}_{2^5}$ and for the c_1 (for an arbitrary $c_1 \in \mathbb{F}_{2^5}$) the equation (1) has only one solution a_1. The equation (2) has the same form of equation (1) when $c_1 = 1$. Then for every b_0, the expression $b_0+a_1^2c_0+a_1^4c_0^2+a_1^4c_1^2c_0$ is in $\mathbb{F}_{2^5}$ and the equation (2) has one solution a_0. Then the equation over $\mathbb{F}_{2^{10}}$, $X+X^2+X^4 = b_0+b_1\Theta$, has only one solution $X = a_0+a_1\Theta$. Because of X^s is *differentially δ-uniform*, we have that $\delta_{X^s}(a,\, a_0+a_1\Theta) \leq \delta$, for every $a \in \mathbb{F}_{2^{10}}^*$. In consequence for every $a \in \mathbb{F}_{2^{10}}^*$, and $b_0 + b_1\Theta \in \mathbb{F}_{2^{10}}$, $\delta_{\psi_2}(a,\, b_0 + b_1\Theta) \leq \delta$, which means $\delta(\psi_2) \leq \delta$. Let's suppose that for $\mathbf{m = k}$, for all $c_1,\, b_1 \in \mathbb{F}_{2^{(5)2^k}}$, the equation $X + c_1X^2 + c_1^3X^4 = b_1$ has one solution $X \in \mathbb{F}_{2^{(5)2^k}}$. It only remains to prove the statement of the theorem for $\mathbf{m = k+1}$. Given any $b_0+b_1\Theta \in \mathbb{F}_{2^{(5)2^{k+1}}}$, let's solve the equation $X + X^2 + X^4 = b_0 + b_1\Theta$ for $X = a_0 + a_1\Theta \in \mathbb{F}_{2^{(5)2^{k+1}}}$, where $a_i,\, b_i \in \mathbb{F}_{2^{(5)2^k}}$. We obtain the following system in the variables a_0 and a_1:

(1) $a_1 + a_1^2c_1 + a_1^4c_1^3 = b_1$ (which has one solution $a_1 \in \mathbb{F}_{2^{(5)2^k}}$).

(2) $a_0 + a_0^2 + a_0^4 = b_0 + a_1^2c_0 + a_1^4c_0^2 + a_1^4c_1^2c_0$ (this equation also has a unique solution given by $a_0 \in \mathbb{F}_{2^{(5)2^k}}$). Thus, $X = a_0+a_1\Theta \in \mathbb{F}_{2^{(5)2^{k+1}}}$ is the only solution for the system. Then as happened for $\mathbb{F}_{2^{10}}$: $\delta(X^s) \leq \delta$ implies $\delta(\psi_2) \leq \delta$, over $\mathbb{F}_{2^{(5)2^{k+1}}}$, completing the proof by induction. To prove the remaining cases, it is enough to replace $\mathbb{F}_{2^{r2^m}}$ by $\mathbb{F}_{2^{(5)2^m}}$ in the proof for the case $r = 5$. ■

Acknowledgements. I thank the NSF for the funds received during my stay as a researcher at UPRM, which has been a key piece to subsidize costs in my research. My gratitude to my ex-advisor, Professor Heeralal Janwa, for his valuable guidance and with whom we are conducting research in various lines. I also want to express my gratitude to my ex-advisor in the research of Boundary Value Problems in the framework of Elasticity Theory, Professor Lev Steinberg. I wish to thank my former Professor of Differential Geometry, Jos Olivencia Quiones. I also thank my colleagues for their advice. Finally, thank Professors Pantelimon Stănică and Gary McGuire for their time in reading a previous research work related to this one.

References

[1] N. Anbar, T. Kalayc, and N. Yurdakul, A note on exceptional APN functions of Gold and Kasami-Welch type.

[2] Y. Aubry, G. McGuire and F. Rodier, A few more functions that are not APN infinitely often, *Finite Fields: Theory and Applications*, **518** (2010), 23-31. https://doi.org/10.1090/conm/518/10193

[3] L. Budaghyan, and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, *IEEE Transactions on Information Theory,* **54** (2008), no. 5, 2354-2357.
https://doi.org/10.1109/tit.2008.920246

[4] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN functions from known ones, *Finite Fields and Their Applications*, **15** (2009), no. 2, 150-159. https://doi.org/10.1016/j.ffa.2008.10.001

[5] L. Budaghyan, C. Carlet and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Transactions on Information Theory*, **52** (2006), no. 2, 1141-1152.
https://doi.org/10.1109/tit.2005.864481

[6] F. Caullery, A new large class of functions not APN infinitely often, *Designs, Codes and Cryptography*, **73** (2014), no. 2, 601-614.
https://doi.org/10.1007/s10623-014-9956-2

[7] M. es Delgado, The state of the art on the conjecture of exceptional APN functions, *Note di Matematica*, **37** (2017), no. 1, 41-52.

[8] M. Delgado and H. Janwa, Progress towards the conjecture on APN functions and absolutely irreducible polynomials (2016), arXiv preprint arXiv:1602.02576.

[9] M. Delgado, R. Reyes and C. Agrinsoni, DES-like Ciphers, Differential Attacks and APN Functions, *Journal of Mathematical Sciences: Advances and Applications*, **49** (2018), no. 1, 2950.
https://doi.org/10.18642/jmsaa_7100121860

[10] J. F. Dillon, *Geometry, Codes and Difference Sets: Exceptional Connections*, Codes and designs (Columbus, OH, 2000), Vol. 10, 2002, 73-85.
https://doi.org/10.1515/9783110198119.73

[11] H. Dobbertin, Almost perfect nonlinear power functions on GF (2 n): a new case for n divisible by 5, *In Finite Fields and Applications*, Proceedings of The Fifth International Conference on Finite Fields and Applications F q 5, held at the University of Augsburg, Germany, August 26, 1999, 113-121, 2001. Springer Berlin Heidelberg.
https://doi.org/10.1007/978-3-642-56755-1_11

[12] E. Frard, R. Oyono and F. Rodier, Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents, *Arithmetic, Geometry, Cryptography and Coding Theory,* 2012, 27-36.
https://doi.org/10.1090/conm/574/11423

[13] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.), *IEEE Transactions on Information Theory,* **14** (1968), no. 1, 154-156. https://doi.org/10.1109/tit.1968.1054106

[14] F. Hernando, and G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, *Journal of Algebra,* **343** (2011), no. 1, 78-92. https://doi.org/10.1016/j.jalgebra.2011.06.019

[15] H. Janwa, and R. M. Wilson, Hyperplane sections of Fermat varieties in P 3 in char. 2 and some applications to cyclic codes,*In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 10th International Symposium, AAECC-10 San Juan de Puerto Rico, Puerto Rico, May 1014, 1993 Proceedings 10 180-194, 1993, Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-56686-4

[16] H. Janwa, G. Mcguire and R. M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF (2), *Journal of Algebra,* **178** (1995), no. 2, 665-676. https://doi.org/10.1006/jabr.1995.1372

[17] K. Nyberg, Differentially uniform mappings for cryptography. In Workshop on the Theory and Application of Cryptographic Techniques, 55-64, (1993, May). Berlin, Heidelberg: Springer Berlin Heidelberg.

[18] R. C. R. Carranza, Construction of New Differentially δUniform Families, Ph.D. Dissertation, University of Puerto Rico, Rio Piedras, 2020.

Received: February 11, 2024; Published: March 8, 2024