A note on exceptional APN functions of Gold and Kasami-Welch type*

Nurdagül Anbar[1][0000−0003−4600−5088], Tekgül Kalaycı[1][0000−0002−8472−9792], and Nihal Yurdakul[2][0000−0003−2374−6908]

[1] Sabancı University,
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
nurdagulanbar2@gmail.com tekgulkalayci@sabanciuniv.edu
[2] Carleton University, 1125 Colonel By Dr, Ottawa, ON K1S 5B6, Canada
nihalyurdakul@cmail.carleton.ca

Abstract. An almost perfect non-linear (APN) function over $\mathbb{F}_{2^n}$ is called exceptional APN if it remains APN over infinitely many extensions of $\mathbb{F}_{2^n}$. Exceptional APN functions have attracted attention from many researchers in the last decades. Although the classification of exceptional APN monomials was completed in 2011 by Hernando and McGuire, there are only partial results on the classification of exceptional APN polynomials. In this note, we present new results on the exceptional APN-ness of the polynomials of Gold and Kasami-Welch type (i.e., polynomials of type $f(X) = X^{2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{k_j}+1}$ and $f(X) = X^{2^{2k}-2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{2k_j}-2^{k_j}+1}$, respectively) by using techniques from curves and their function fields.

Keywords Exceptional APN functions, Gold and Kasami-Welch functions, Eisenstein's irreducibility criterion, Kummer's theorem

Mathematics Subject Classification 06E30 05B10 94C10

1 Introduction

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n. *Almost perfect non-linear* (APN) functions are of particular interest due to their good resistance to differential attacks, see [10]. A function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is called APN over $\mathbb{F}_{2^n}$ if

$$D_a f(X) := f(X + a) + f(X) = b \tag{1}$$

has at most 2 solutions for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Note that if x_0 is a solution of $D_a f(X) = b$ then so $x_0 + a$ is, as the characteristic of $\mathbb{F}_{2^n}$ is 2. Hence, f is APN over $\mathbb{F}_{2^n}$ if and only if Equation (1) has either 0 or 2 solutions for all

* Nurdagül Anbar and Tekgül Kalaycı are supported by TÜBİTAK Project under Grant 120F309

$a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Equivalently, f is APN over $\mathbb{F}_{2^n}$ if and only if for any non-zero $a \in \mathbb{F}_{2^n}$ the set $\{D_a f(x) : x \in \mathbb{F}_{2^n}\}$ has cardinality 2^{n-1}.

Another characterization for APN-ness is given by the Janwa-Wilson-Rodier condition. It states that a function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is APN over $\mathbb{F}_{2^n}$ if and only if all the elements $(x, y, z) \in \mathbb{F}_{2^n}^3$ satisfying

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

belong to the variety defined by $(X + Y)(X + Z)(Y + Z) = 0$.

Well-known examples of APN functions are the Gold function, i.e., $f(X) = X^{2^k+1}$, and the Kasami-Welch function, i.e., $f(X) = X^{2^{2k}-2^k+1}$. More precisely, $f(X)$ is APN over $\mathbb{F}_{2^n}$ if and only if $\gcd(n, k) = 1$. Therefore, the Gold and the Kasami-Welch functions are APN over infinitely many extensions of $\mathbb{F}_{2^n}$, and are called *exceptional APN* over $\mathbb{F}_{2^n}$. The following conjecture is due to Aubry, McGuire and Rodier, see [1].

Conjecture 1. Up to CCZ equivalence (see [2]), the Gold and the Kasami-Welch functions are the only exceptional APN functions. That is, if $f(X) \in \mathbb{F}_{2^n}[X]$ is exceptional APN then $f(X)$ is CCZ equivalent to the Gold or the Kasami-Welch function.

Let $f(X) = \sum_{j=0}^{d} c_j X^j \in \mathbb{F}_{2^n}[X]$ be a polynomial of degree d. Set

$$F(X, Y, Z) := \frac{f(X) + f(Y) + f(Z) + f(X + Y + Z)}{(X + Y)(X + Z)(Y + Z)} \in \mathbb{F}_{2^n}[X, Y, Z]. \tag{2}$$

Note that F is a polynomial of degree $d - 3$. Let $\mathcal{F}$ be the variety over $\mathbb{F}_{2^n}$ defined by F. Then by the Janwa-Wilson-Rodier condition we conclude that f is not APN over $\mathbb{F}_{2^n}$ if and only if there exits a rational point $(x, y, z) \in \mathcal{F}$ with pairwise distinct coordinates. In particular, if $\mathcal{F}$ has an absolutely irreducible component defined over $\mathbb{F}_{2^n}$ other than $X + Y$, $X + Z$ and $Y + Z$ then f can not be exceptional APN over $\mathbb{F}_{2^n}$, see [9]. Therefore, the main aim is to find an absolutely irreducible factor over $\mathbb{F}_{2^n}$ of F (other than $X+Y$, $X+Z$ and $Y+Z$) in Equation (2) in order to show that f is not exceptional APN over $\mathbb{F}_{2^n}$.

By setting

$$F_j(X, Y, Z) := \frac{X^j + Y^j + Z^j + (X + Y + Z)^j}{(X + Y)(X + Z)(Y + Z)} \in \mathbb{F}_{2^n}[X, Y, Z], \tag{3}$$

we can write $F(X, Y, Z) = \sum_{j=3}^{d} c_j F_j(X, Y, Z)$. With the notation mentioned above, we can summarize some known results on Conjecture 1 for "odd degree" polynomials f as follows. Throughout the paper, we mean the polynomial degree as the degree of a polynomial.

Lemma 1. *(i) If $f(X) = X^t$ is exceptional APN then f is either the Gold or the Kasami-Welch function, see [7] and references therein. That is, Conjecture 1 holds for monomial functions.*

(ii) *If the leading term of f is not the Gold or the Kasami-Welch then f is not exceptional APN, see [1].*

(iii) *Suppose that $f(X) = X^{2^k+1} + g(X) \in \mathbb{F}_{2^n}[X]$ for $k \geq 2$ and $d = \deg(g) < 2^k + 1$. Say, $g(X) = \sum_{j=0}^{d} c_j X^j$.*

- *(a) If $d \leq 2^{k-1} + 1$, and F_j is absolutely irreducible for a non-zero c_j then f is not exceptional APN, see [1].*
- *(b) If $d \equiv 3 \mod 4$ then f is not exceptional APN, see [5].*
- *(c) If $d \equiv 1 \mod 4$, and F_{2^k+1} and F_d are relatively prime then f is not exceptional APN, see [5].*
- *(d) If $d \equiv 5 \mod 8$ then f is not exceptional APN, see [5].*
- *(e) If d is an odd integer that is not of the form $2^\ell + 1$ or that is of the form $2^\ell + 1$ with $\gcd(k, \ell) = 1$ then f is not exceptional APN, see [3,4].*

(iv) *Suppose that $f(X) = X^{2^{2k}-2^k+1} + g(X) \in \mathbb{F}_{2^n}[X]$ for $k \geq 2$ and $d = \deg(g) < 2^{2k} - 2^k + 1$. Say, $g(X) = \sum_{j=0}^{d} c_j X^j$.*

- *(a) If $d \leq 2^{2k-1} - 2^{k-1} + 1$, and F_j is absolutely irreducible for a non-zero coefficient c_j of g then f is not exceptional APN, see [6].*
- *(b) Suppose that $d \equiv 3 \mod 4$. If $d \leq 2^{2k-1} - 2^{k-1} + 1$ or $d > 2^{2k-1} - 2^{k-1} + 1$ and $\gcd(2^k - 1, (d-1)/2)$ then f is not exceptional APN, see [3].*

Remark 1. Note that $\mathcal{F}$ defines a surface in an affine space in the cases $(ii) - (iv)$ whereas it defines a curve in a projective plane in the case (i). Moreover, in the cases (iii) and (iv), the polynomial $F(X, Y, Z)$ is absolutely irreducible over $\mathbb{F}_{2^n}$, and $F(X, Y, Z)$ is known to have an absolutely irreducible factor over $\mathbb{F}_{2^n}$ in (i) and (ii).

For further results including even degree polynomials, we refer to [4] and references therein.

This note is organized as follows. In Section 2, we describe the main method, used to show a polynomial is not exceptional APN. In Section 3, we first apply the method with Eisenstein's irreducibility criterion to obtain new classes of polynomials of Gold and Kasami-Welch type that are not exceptional APN, see remarks 2 and 3. Then in Section 4 we apply the method with Kummer's theorem to characterize the non-exceptional APN property of Gold and Kasami-Welch type polynomials f in terms of the existence of a root of the polynomial associated to given f. Similarly, we obtain new classes of polynomials of Gold and Kasami-Welch type that are not exceptional APN, see Corollary 2.

2 The main method

We can summarize the method used in the paper as follows.
Let $f(X) = \sum_{j=0}^{d} c_j X^j \in \mathbb{F}_{2^n}[X]$ be a polynomial of degree d and $\mathcal{F}$ be the affine surface defined by $F(X, Y, Z)$ given by Equation (2). Consider the homogenization of $F(X, Y, Z)$ by the variable T, i.e., $F(X, Y, Z, T) = \sum_{j=3}^{d} c_j F_j(X, Y, Z) T^{d-j}$, where F_j's are defined as in Equation (3). Let $\bar{\mathcal{F}}$ be the zero set of $F(X, Y, Z, T)$ in the projective space $\mathbb{P}^3$, i.e., $\bar{\mathcal{F}}$ is the projective closure of $\mathcal{F}$. The aim is to

find an absolutely irreducible curve defined over $\mathbb{F}_{2^n}$ lying in $\bar{\mathcal{F}}$ which does not lie in the hyperplane defined by T (i.e., the hyperplane at infinity), $X+Y$, $X+Z$ or $Y+Z$. Then the Hasse-Weil bound (see [8, Theorem 9.57]) implies that there exists a rational point $(x : y : z : t) \in \bar{\mathcal{F}}$ for all sufficiently large extensions of $\mathbb{F}_{2^n}$ such that $t \neq 0$, $x \neq y$, $x \neq z$ and $y \neq z$. This implies the existence of a rational point, namely $(x/t, y/t, z/t)$, of $\mathcal{F}$ with pairwise distinct coordinates over all sufficiently large extensions of $\mathbb{F}_{2^n}$. Therefore, we conclude that $f(X)$ is not APN over all sufficiently large extensions of $\mathbb{F}_{2^n}$, i.e., it is not exceptional APN over $\mathbb{F}_{2^n}$.

For the aim mentioned above, we consider the affine part $\tilde{\mathcal{F}}$ of $\bar{\mathcal{F}}$ corresponding to variable Z. That is, we consider the zero set of

$$\tilde{F}(X,Y,T) := F(X,Y,1,T) = \sum_{j=3}^{d} c_j F_j(X,Y,1)T^{d-j}.$$

Let $\mathcal{Y}$ be the hyperplane defined by Y. Then the intersection $\tilde{\mathcal{F}} \cap \mathcal{Y}$ is defined as the zero set of the following polynomial.

$$G(X,T) := \tilde{F}(X,0,T) = \sum_{j=3}^{d} c_j F_j(X,0,1)T^{d-j} = \sum_{j=3}^{d} c_j \frac{X^j+1+(X+1)^j}{X(X+1)} T^{d-j} \tag{4}$$

Proposition 1. *If $G(X,T)$ in Equation (4) has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ that has a term containing T then $f(X)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. Let $H(X,T)$ be an absolutely irreducible factor of $G(X,T)$ defined over $\mathbb{F}_{2^n}$ that has a term containing T. Note that $H(X,T) \neq T$ since $G(X,0) = c_d \frac{X^d+1+(X+1)^d}{X(X+1)} \neq 0$. Moreover, $H(X,T)$ can not be X or $X+1$ as it has a term containing T. Let $\mathcal{H}$ be the curve defined by $H(X,T)$. Since $H(X,T)$ is absolutely irreducible over $\mathbb{F}_{2^n}$, by the Hasse-Weil bound, $\mathcal{H}$ has sufficiently large number of rational points for all sufficiently large extensions of $\mathbb{F}_{2^n}$. Hence, over all sufficiently large extensions of $\mathbb{F}_{2^n}$, there exists a rational point $(\alpha, \beta) \in \mathcal{H}$ such that $\alpha\beta \neq 0$ and $\alpha \neq 1$ since by Bezout's Theorem $\mathcal{X} \cap \{XT = 0\}$ and $\mathcal{X} \cap \{X = 1\}$ have cardinality at most $2\deg(H)$ and $\deg(H)$, respectively. Then $(x,y,z) := (\alpha/\beta, 1/\beta, 0)$ is a zero of $F(X,Y,Z)$, given in Equation (2), such that $x \neq y$, $x \neq z$ and $y \neq z$, which gives the desired result by the Janwa-Wilson-Rodier condition. ∎

3 An approach by Eisenstein's irreducibility criterion

In this section, we apply a special case of Eisenstein's irreducibility criterion to investigate the Gold and the Kasami-Welch type polynomials. Hence, we first state the criterion in the following lemma. For details, we refer to [11, Proposition 3.1.15].

Lemma 2. *Let $\mathbb{F}$ be a field and $G(X,T) \in \mathbb{F}[X,T]$. Write*

$$G(X,T) = G_d(X)T^d + G_{d-1}(X)T^{d-1} + \cdots + G_1(X)T + G_0(X)$$

for some $G_i(X) \in \mathbb{F}[X]$ for $i = 0, \ldots, d$. Set $C(X) = \gcd(G_d(X), \ldots, G_0(X))$. For an irreducible polynomial $P(X) \in \mathbb{F}[X]$, we denote the multiplicity of $P(X)$ in $G_i(X)$ by m_i. Suppose that the following holds.

(i) $m_0 > 0$ *and* $\gcd(m_0, d) = 1$,
(ii) $m_i \geq m_0$ *for all* $i = 1, \ldots, d-1$, *and*
(iii) $m_d = 0$.

Then $G(X,T)/C(X)$ is absolutely irreducible over $\mathbb{F}$.

3.1 Polynomials of Gold type

In this subsection, we apply Proposition 1 to the polynomials of the form $f(X) = X^{2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$, which are Gold type polynomials. In [9], it is shown that $F_{2^k+1}(X,Y,1)$ can be factorized as follows:

$$F_{2^k+1}(X,Y,1) = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (X + (\alpha+1)Y + \alpha)\,. \tag{5}$$

Lemma 3. *For $k \geq 2$, let $f(X) = X^{2^k+1} + g(X)$, where $g(X) = \sum_{j=\ell}^{2^k} c_j X^j \in \mathbb{F}_{2^n}[X]$ with $c_\ell \neq 0$. Suppose that there exists $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$ such that $F_j(\alpha,0,1) = 0$ for all $j > \ell$ and $F_\ell(\alpha,0,1) \neq 0$. Then $f(X)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. For $f(X) = X^{2^k+1} + \sum_{j=\ell}^{2^k} c_j X^j$, by Equation (4) we have

$$G(X,T) = \sum_{j=\ell}^{2^k+1} c_j F_j(X,0,1) T^{2^k+1-j}.$$

That is, the coefficient of T^i in $G(X,T)$ is $G_i(X) = F_{2^k+1-i}(X,0,1)$ for $i = 0, \ldots, 2^k+1-\ell$. Note that by Equation (5), we have $F_{2^k+1}(X,0,1) = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (X+\alpha)$. That is, the minimal polynomial $P(X)$ of α over $\mathbb{F}_{2^n}$ is a simple factor of $F_{2^k+1}(X,0,1)$. The assumption $F_j(\alpha,0,1) = 0$ implies that $P(X)$ is also a factor of $F_j(X,0,1)$ for all $j > \ell$, but it is not a factor of $F_\ell(X,0,1)$. In other words, we have the following.

(i) $P(X)$ is a simple factor of $G_0(X)$, i.e., $m_0 = 1$.
(ii) $P(X)$ is a factor of $G_i(X)$, i.e., $m_i \geq m_0$, for all $i = 1, \ldots, 2^k - \ell$.
(iii) $P(X)$ is not a factor of $G_{2^k+1-\ell}(X)$, i.e., $m_{2^k+1-\ell} = 0$.

Hence by Lemma 2, $G(X,T)/C(X)$ is absolutely irreducible over $\mathbb{F}_{2^n}$. In particular, $G(X,T)$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ that has a term containing T, and hence we obtain the desired conclusion by Proposition 1. ■

Corollary 1. *There are no exceptional APN binomials of Gold type. That is, if $f(X) = X^{2^k+1} + cX^{2^l+1}$ for a non-zero $c \in \mathbb{F}_{2^n}$ then $f(X)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. Let $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^t} (\neq \emptyset)$, where $\mathbb{F}_{2^t} = \mathbb{F}_{2^k} \cap \mathbb{F}_{2^l}$. Then α satisfies the conditions in Lemma 3, and hence the result follows from Lemma 3. ■

We can extend the previous result for Gold type polynomials that are not binomials.

Theorem 1. *For $k \geq 2$, let $f(X) = X^{2^k+1} + g(X)$, where $g(X) = \sum_{j=1}^{\eta} c_j X^{2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$ for some positive integers $k_1 < k_2 < \cdots < k_\eta < k$ and $c_j \neq 0$ for $j = 1, 2, \ldots \eta$. If $\gcd(k_1, \ldots, k_\eta, k) < \gcd(k_2, \ldots, k_\eta, k)$ then $f(X)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. Let $\gcd(k_1, \ldots, k_\eta, k) = s$ and $\gcd(k_2, \ldots, k_\eta, k) = st$ for some integers $s \geq 1$, $t > 1$. Then $\mathbb{F}_{2^{st}} \subseteq \mathbb{F}_{2^{k_j}}$ for all $j = 2, \ldots, \eta$, $\mathbb{F}_{2^{st}} \subseteq \mathbb{F}_{2^k}$ and $\mathbb{F}_{2^{st}} \cap \mathbb{F}_{2^{k_1}} = \mathbb{F}_{2^s}$. By Equations (4) and (5), we have the following equalities.

$$\begin{aligned} G(X,T) &= \sum_{j=1}^{\eta} c_j F_{2^{k_j}+1}(X,0,1) T^{2^k - 2^{k_j}} + F_{2^k+1}(X,0,1) \\ &= \sum_{j=1}^{\eta} c_j \left(\prod_{\alpha \in \mathbb{F}_{2^{k_j}} \setminus \mathbb{F}_2} (X+\alpha) \right) T^{2^k - 2^{k_j}} + \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (X+\alpha) \end{aligned} \tag{6}$$

Let $\alpha \in \mathbb{F}_{2^{st}} \setminus \mathbb{F}_{2^s}$, i.e., $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$. By Equation (6), we have $F_j(\alpha, 0, 1) = 0$ for all $j > 2^{k_1} + 1$ and $F_{2^{k_1}+1}(\alpha, 0, 1) \neq 0$. Then we obtain the desired result by Lemma 3. ■

Remark 2. Set $d = \deg(g(x)) = 2^{k_\eta} + 1$. We observe that for a sufficiently integer k_η, we have $d \equiv 1 \mod 4$ and $d \not\equiv 5 \mod 8$. Also, $\gcd(k, \eta) > 1$ implies that $\gcd(2^k + 1, d) > 1$, and hence we observe that F_{2^k+1} and F_d are not relatively prime. In particular, Theorem 1 gives new classes of non-exceptional Gold type polynomials, which can not be obtained from previously known characterization, see Lemma 3.

3.2 Polynomials of Kasami-Welch type

In this subsection, we similarly apply Proposition 1 to the polynomials of the form $f(X) = X^{2^{2k}-2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{2k_j}-2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$, which are Kasami-Welch type polynomials. In [9], it is shown that $F_{2^{2k}-2^k+1}(X, Y, 1)$ can be factorized as follows:

$$F_{2^{2k}-2^k+1}(X,Y,1) = \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} P_\alpha(X,Y),$$

where $P_\alpha(X,Y)$ is an absolutely irreducible polynomial over $\mathbb{F}_{2^k}$ of degree 2^k+1 such that for each $\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$

$$P_\alpha(X,0) = (X+\alpha)^{2^k+1}. \tag{7}$$

By using above factorization, we have the following result.

Theorem 2. *For $k \geq 2$, let $f(X) = X^{2^{2k}-2^k+1} + g(X)$, where $g(X) = \sum_{j=1}^{\eta} c_j X^{2^{2k_j}-2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$ for some positive integers $k_1 < \cdots < k_\eta < k$ and $c_j \neq 0$ for $j = 1, \ldots, \eta$. Suppose that k is an even integer with $\gcd(k_1, k) = 1$ and $\gcd(k_1, \ldots, k_\eta) > 1$. Then $f(X)$ is not exceptional APN over $\mathbb{F}_{2^n}$.*

Proof. It is sufficient to show that $G(X,T)$ given in Equation (4) is absolutely irreducible over $\mathbb{F}_{2^n}$ since the desired result then follows from Lemma 1. By Equation (7), we can write $G(X,T)$ as follows.

$$\begin{aligned} G(X,T) &= \sum_{j=1}^{\eta} c_j F_{2^{2k_j}-2^{k_j}+1}(X,0,1) T^{2^{2k}-2^k-2^{2k_j}+2^{k_j}} + F_{2^{2k}-2^k+1}(X,0,1) \\ &= \sum_{j=1}^{\eta} c_j \left(\prod_{\alpha \in \mathbb{F}_{2^{k_j}} \setminus \mathbb{F}_2} (X+\alpha)^{2^{k_j}+1} \right) T^{2^{2k}-2^k-2^{2k_j}+2^{k_j}} + \prod_{\alpha \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2} (X+\alpha)^{2^k+1} \end{aligned}$$

Note that $G(X,T)$ is absolutely irreducible if and only if

$$H(X,T) = T^{2^{2k}-2^k-2^{2k_1}+2^{k_1}} G(X, 1/T) \in \mathbb{F}_{2^n}[X,T]$$

is absolutely irreducible. Set $A_\ell(X) = \prod_{\alpha \in \mathbb{F}_{2^\ell} \setminus \mathbb{F}_2} (X+\alpha)^{2^\ell+1}$. Then

$$H(X,T) = A_k(X) T^{2^{2k}-2^k-2^{2k_1}+2^{k_1}} + \sum_{j=1}^{\eta} c_j A_{k_j}(X) T^{2^{2k_j}-2^{k_j}-2^{2k_1}+2^{k_1}}.$$

Let $\gcd(k_1, \ldots, k_\eta) = s$ for some integer $s > 1$, i.e., $\mathbb{F}_{2^s} \subseteq \mathbb{F}_{2^{k_i}}$ for all $i = 1, \ldots, \eta$. We have $\mathbb{F}_{2^{k_1}} \cap \mathbb{F}_{2^k} = \mathbb{F}_2$, since $\gcd(k_1, k) = 1$, . Then $\alpha \in \mathbb{F}_{2^s} \setminus \mathbb{F}_2$ is a root of $A_{k_i}(X)$ of multiplicity $2^{k_i}+1$ for all $i = 1, \ldots, \eta$ and $A_k(\alpha) \neq 0$. That is, the multiplicity of the minimal polynomial $P(X)$ of α over $\mathbb{F}_{2^n}$ is 0 in $A_k(X)$, and it is $2^{k_i}+1$ in $A_{k_i}(X)$, where $2^{k_i}+1 \geq 2^{k_1}+1$ for all $i = 1, \ldots, \eta$. Set

$$m = \gcd(2^{2k} - 2^k - 2^{2k_1} + 2^{k_1}, 2^{k_1} + 1).$$

We will show that $m = 1$ under the assumptions $k \equiv 0 \mod 2$ and $\gcd(k_1, k) = 1$. Since $2^{2k_1} - 2^{k_1} \equiv 2 \mod (2^{k_1}+1)$, we have the following equalities.

$$\begin{aligned} m &= \gcd(2^{2k} - 2^k - 2, 2^{k_1} + 1) = \gcd(2^{2k-1} - 2^{k-1} - 1, 2^{k_1} + 1) \\ &= \gcd(2^{k-1} - 1, 2^{k_1} + 1) \gcd(2^k + 1, 2^{k_1} + 1) = \gcd(2^k + 1, 2^{k_1} + 1). \end{aligned}$$

Note that in the last equality we used the fact that

$$\gcd(2^{k-1}-1, 2^{k_1}+1) = \frac{2^{\gcd(k-1,2k_1)}-1}{2^{\gcd(k-1,k_1)}-1} = 1$$

since $\gcd(k-1, 2k_1) = \gcd(k-1, k_1)$, which follows from the assumption that k is even. Moreover, we have

$$\gcd(2^k+1, 2^{2k_1}-1) = \frac{\gcd(2^{2k}-1, 2^{2k_1}-1)}{\gcd(2^k-1, 2^{2k_1}-1)} = \frac{2^{\gcd(2k,2k_1)}-1}{2^{\gcd(k,2k_1)}-1} = 1$$

since $\gcd(2k, 2k_1) = \gcd(k, 2k_1) = 2$, which follows from the assumptions that $\gcd(k_1, k) = 1$ and k is even. Note that $\gcd(2^k+1, 2^{k_1}+1)$ is a divisor of $\gcd(2^k+1, 2^{2k_1}-1)$, and hence we conclude that $\gcd(2^k+1, 2^{k_1}+1) = 1$, which implies that $m = 1$. Then we conclude that $H(X, T)$ is absolutely irreducible by Lemma 2, which gives the desired conclusion. ■

Remark 3. Set $d = \deg(g) = 2^{2k_\eta} - 2^{k_\eta} + 1$. Then $d \leq 2^{2k} - 2^k + 1$ and $d \equiv 1 \mod 4$ for a sufficiently large integer k_η. Moreover, by [9], we know that $F_{2^{2k_j}-2^{k_j}+1}$ is not absolutely irreducible for all $j = 1, \ldots \eta$. In particular, Theorem 2 gives new classes of non-exceptional Kasami-Welch type polynomials, which can not be obtained from previously known characterization, see Lemma 3.

4 An approach by Kummer's theorem

In this section we use the theory of function fields to obtain more classes of polynomials of Gold or Kasami-Welch type that are not exceptional APN. We need a special case of Kummer's theorem, see [11, Corollary 3.3.8] which we summarize as follows:
Let $\mathbb{F}(x)$ be a rational function field over the constant field $\mathbb{F}$ and $H_{(x)}(Y) = Y^n + h_{n-1}(x)Y^{n-1} + \cdots + h_0(x) \in \mathbb{F}(x)[Y]$ be an irreducible polynomial over $\mathbb{F}(x)$. Let $F = \mathbb{F}(x, y)$ be the function field defined by $H_{(x)}(y) = 0$. We consider the function field extension $\mathbb{F}(x, y)/\mathbb{F}(x)$. Let $\gamma \in \mathbb{F}$ such that $h_j(\gamma) \neq \infty$, i.e., γ is not a pole of $h_j(x)$, for all $j = 0, \ldots, n-1$. Denote by P_γ the rational place of $\mathbb{F}(x)$ corresponding to $x - \gamma$. Suppose that

$$H_{(\gamma)}(Y) := Y^n + h_{n-1}(\gamma)Y^{n-1} + \cdots + h_0(\gamma) \in \mathbb{F}[Y]$$

has the following factorization in $\mathbb{F}[T]$:

$$H_{(\gamma)}(Y) = \prod_{i=1}^{r} \psi_i(Y),$$

where $\psi_i(Y)$'s are irreducible, monic, pairwise distinct polynomials. Then there are exactly r places P_i of F lying over P_γ such that the relative degree of P_i over P_γ is the degree of ψ_i. In particular, if one of the ψ_i has degree 1, the residue

field of P_i and P_γ are the same, namely $\mathbb{F}$. That is, $\mathbb{F}$ is the full constant field F. Then by [11, Corollary 3.6.8] we conclude that $H_{(x)}(Y)$ is absolutely irreducible over $\mathbb{F}(x)$.

Write $h_i(X) = k_i(X)/\ell_i(X)$ for some relatively prime polynomials $k_i(X), \ell_i(X) \in \mathbb{F}[X]$. Set $\ell(X) = \mathrm{lcm}(\ell_{n-1}(X), \ldots, \ell_0(X))$ and $k(X) = \gcd(k_{n-1}(X), \ldots, k_0(X))$ in $\mathbb{F}[X]$, where lcm and gcd are the least common multiple and greatest common divisor, respectively. Then the absolutely irreducibility of $h_{(x)}(Y)$ over $\mathbb{F}(x)$ implies that $H(X,Y) := \ell(X)h_{(X)}(Y)/k(X) \in \mathbb{F}[X,Y]$ is absolutely irreducible over $\mathbb{F}$.

Now we apply the approach explained above to the following type of Kasami-Welch polynomials.

Theorem 3. *Let* $f(X) = X^{2^{2k}-2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{2k_j}-2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$ *with* $c_j \neq 0$ *for* $j = 1, \ldots, \eta$. *If the polynomial* $F(T) = \sum_{j=1}^{\eta} c_j T^{2^{2k}-2^k-2^{2k_j}+2^{k_j}} + 1$ *has a root* $\alpha \in \mathbb{F}_{2^n}$ *then* $f(X)$ *is not exceptional APN over* $\mathbb{F}_{2^n}$.

Proof. We recall that if $f(X) = X^{2^{2k}-2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{2k_j}-2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$ then the polynomial $G(X,T)$ in Equation (4) is given by

$$G(X,T) = \sum_{j=1}^{\eta} c_j A_{k_j}(X) T^{2^{2k}-2^k-2^{2k_j}+2^{k_j}} + A_k(X),$$

where $A_\ell(X) = \prod_{\alpha \in \mathbb{F}_{2^\ell} \setminus \mathbb{F}_2} (X+\alpha)^{2^\ell+1}$. Then by Proposition 1, it is sufficient to show that $G(X,T)$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ that has a term containing T. Set $Y := T^{2^{k_1}}$, then $\tilde{G}(X,Y) := G(X,T)$ is given by

$$\tilde{G}(X,Y) = \sum_{j=1}^{\eta} c_j A_{k_j}(X) Y^{2^{2k-k_1}-2^{k-k_1}-2^{2k_j-k_1}+2^{k_j-k_1}} + A_k(X).$$

Note that $A_\ell(1) = 1$ for any $\ell > 1$, i.e.,

$$L(Y) := \tilde{G}(1,Y) = \sum_{j=1}^{\eta} c_j Y^{2^{2k-k_1}-2^{k-k_1}-2^{2k_j-k_1}+2^{k_j-k_1}} + 1.$$

By our assumption, we have $G(1,\alpha) = 0$ for some $\alpha \in \mathbb{F}_{2^n}$. This implies that $L(\beta) = 0$, where $\beta = \alpha^{2^{k_1}}$. The fact that the derivative $L'(Y) = c_1 Y^{2^{2k-k_1}-2^{k-k_1}-2^{k_1}}$ implies that $L(Y)$ is a separable polynomial. That is, β is a simple root of $L(Y)$. Let $H(X,Y) = h_n(X)Y^n + h_{n-1}(X)Y^{n-1} + \cdots + h_0(X)$ be an irreducible factor of $\tilde{G}(X,Y)$ such that $H(1,Y)$ is divisible by $Y+\beta$. Note that $\deg \tilde{G}(X,Y) = \deg L(Y)$, and hence $\deg H(X,Y) = \deg H(1,Y)$. That is, $h_n(1) \neq 0$. Then for

$$h_{(x)}(Y) = Y^n + f_{n-1}(x)Y^{n-1} + \cdots + f_0(x),$$

where $f_i(x) = h_i(x)/h_n(x)$ for $i = 0, \ldots, n-1$, we have $f_i(1) \neq \infty$ for all $i = 0, \ldots, n-1$. Moreover, since $L(Y)$ is separable, $h_{(1)}(Y)$ factors into pairwise

distinct irreducible factors such that one of them is $Y + \beta$. That is, $h_{(x)}(Y)$ satisfies the properties given above. Hence, $h_n(X)h_{(X)}(Y) = H(X, Y)$ is an absolutely irreducible polynomial over $\mathbb{F}_{2^n}$.

We now show that the absolute irreducibility of $H(X, Y)$ implies the existence of an absolute irreducibility factor of $H(X, T^{2^{k_1}})$ over $\mathbb{F}_{2^n}$ which has a term containing T. Then we obtain the desired conclusion by Proposition 1.

Suppose that $H(X, T^{2^{k_1}}) = A(X, T)B(X, T)$ for some relatively prime polynomials $A, B \in \bar{F}(X)[T]$, where $\bar{F}$ is the algebraic closure of $\mathbb{F}_{2^n}$. We without loss of generality suppose that $B(X, T) = P(X, T)^{s2^\ell}$ for an absolutely irreducible polynomial $P \in \bar{F}[X, T]$, which has a term containing T, and positive odd integer s. Note that

$$\tilde{H}(X, T)^{2^{k_1}} = H(X^{2^{k_1}}, T^{2^{k_1}}) = A(X^{2^{k_1}}, T)B(X^{2^{k_1}}, T) \tag{8}$$

for some $\tilde{H} \in \mathbb{F}_{2^n}[X, T]$. Since $A(X, T)$, $B(X, T)$ are relatively prime over $\bar{F}(X)$, the polynomials $A(X^{2^{k_1}}, T)$, $B(X^{2^{k_1}}, T)$ are relatively prime over $\bar{F}(X)$. Then Equation (8) implies that $B(X^{2^{k_1}}, T) = (\tilde{B}(X, T))^{2^{k_1}}$ for some $\tilde{B} \in \bar{F}[X, T]$. This shows that the exponents of T in $B(X, T)$ is divisible by 2^{k_1}, i.e., $B(X, T) = \bar{B}(X, T^{2^k})$ for some $\bar{B} \in \bar{F}[X, Y]$. Similarly, $A(X, T) = \bar{A}(X, T^{2^k})$ for some $\bar{A} \in \bar{F}[X, Y]$. This implies that $H(X, Y) = \bar{A}(X, Y)\bar{B}(X, Y)$. Since $H(X, Y)$ is absolutely irreducible, $H(X, Y) = \bar{B}(X, Y)$, and hence $H(X, T^{2^{k_1}}) = B(X, T) = \tilde{P}(X, T)^s$, where $\tilde{P}(X, T) = P(X, T)^{2^\ell} = P(X^{2^\ell}, T^{2^\ell})$. Then it is enough to observe that $s = 1$ to show $P \in \mathbb{F}_{2^n}[X, Y]$. For this, we show that the exponents of T in $\tilde{P}(X, T)$ are divisible by 2^{k_1}, i.e., $\tilde{P}(X, T) = \bar{P}(X, T^{2^{k_1}})$ for some $\bar{P} \in \bar{F}[X, Y]$. This implies that $H(X, Y) = B(X, Y) = \bar{P}(X, Y)^s$, which gives the desired conclusion $s = 1$. Let

$$\tilde{P}(X, T) = p_m(X)T^m + p_{m-1}(X)T^{m-1} + \cdots + p_1(X)T + p_0(X).$$

First note that $p_0(X) \neq 0$ as T is not a factor of $G(X, T)$. Denote the coefficient of T^μ in $\tilde{P}(X, T)^s$ by c_μ. Since $B(X, T^{2^{k_1}}) = \bar{P}(X, T)^s$, we conclude that $c_\mu \neq 0$ only if μ is divisible by 2^{k_1}. We proceed by induction on $p_\mu(X)$. Note that $c_1 = p_1(X)p_0(X)^{s-1} = 0$ implies that $p_1(X) = 0$. Then $p_1(X) = 0$ implies that $c_2 = p_2(X)p_0(X)^{s-1}$, and hence $p_2(X) = 0$ if $k_1 > 1$. Then we conclude that $p_\ell(X) = 0$ for all $\ell = 1, \ldots, 2^{k_1} - 1$ by induction. Suppose that for some $t \geq 1$ we have that $p_\mu(X) = 0$ for all $\mu \leq t2^{k_1}$ if μ is not divisible by 2^{k_1}. Then $0 = c_{t2^{k_1}+\ell} = p_{t2^{k_1}+\ell}(X)p_0(X)^{s-1}$, and hence $p_{t2^{k_1}+\ell}(X) = 0$, which gives the desired conclusion. ■

We apply the same approach to the polynomials of Gold type and obtain the following result.

Theorem 4. *Let* $f(X) = X^{2^k+1} + \sum_{j=1}^{\eta} c_j X^{2^{k_j}+1} \in \mathbb{F}_{2^n}[X]$ *with* $c_j \neq 0$ *for* $j = 1, \ldots, \eta$. *If the polynomial* $F(T) = \sum_{j=1}^{\eta} c_j T^{2^k - 2^{k_j}} + 1 \in \mathbb{F}_{2^n}[T]$ *has a root* $\alpha \in \mathbb{F}_{2^n}$ *then* $f(X)$ *is not exceptional APN over* $\mathbb{F}_{2^n}$.

Corollary 2. *If* $f(X) = X^{2^{2k}-2^k+1} + \sum_{j=1}^{2s-1} X^{2^{2kj}-2^{kj}+1}$ *or* $f(X) = X^{2^k+1} + \sum_{j=1}^{2s-1} X^{2^{kj}+1}$ *then* $f(X)$ *is not exceptional APN over* $\mathbb{F}_2$*. In particular, by Theorems 3 and 4 we obtain classes of non-exceptional Gold and Kasami-Welch type polynomials for sufficiently large* k*, which can not be obtained from previously known characterization given in Lemma 3, Theorems 1 and 2.*

References

1. Aubry, Y., McGuire, G., Rodier, F.: A few more functions that are not APN infinitely often. Finite fields: theory and applications, Contemp. Math., vol. 518, 23–31, Amer. Math. Soc., Providence, RI, (2010) 2, 3
2. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998) 2
3. Delgado M., Janwa H.: Further results on exceptional APN functions. AGCT-India (2013) http://www. math.iitb.ac.in/ srg/AGCT-India-2013/Slides/. 3
4. Delgado, M., Janwa, H.: Progress towards the conjecture on APN functions and absolutely irreducible polynomials. (2016). arXiv:1602.02576 3
5. Delgado, M., Janwa, H.: On the conjecture on APN functions and absolute irreducibility of polynomials. Des. Codes Cryptogr. **82**(3), 617–627 (2017) 3
6. Férard, E., Oyono, R., Rodier, F.: Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents. Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, 27–36, Amer. Math. Soc., Providence, RI, (2012) 3
7. Hernando, F., McGuire, G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. J. Algebra **343**, 78–92 (2011) 2
8. Hirschfeld, J.W.P., Korchmáros, G., Torres F.: Algebraic curves over a finite field. Princeton University Press, (2013) 4
9. Janwa, H., Wilson, R. M.: Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes. Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, 180–194, Springer, Berlin, (1993) 2, 5, 6, 8
10. Nyberg, K.: Differentially uniform mappings for cryptography. Advances in cryptology-Eurocrypt'93 (Lofthus,1993),Lecture Notes in Comput. Sci., vol. 765, 55–64, Springer, Berlin, (1994) 1
11. Stichtenoth, H.: Algebraic function fields and codes. 2nd edition. Graduate Texts in Mathematics, vol. 254 Springer-Verlag (2009). 4, 8, 9