Finite Fields and Their Applications 25 (2014) 26–36

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On a class of quadratic polynomials with no zeros and its application to APN functions

Carl Bracken [a], Chik How Tan [b,1], Yin Tan [b,*,1]

[a] Department of Mathematics, School of Physical & Mathematical Sciences, Nanyang Technology University, Singapore
[b] Temasek Laboratories, 5A, Engineering Drive 1, ♯ 09-02, National University of Singapore, 117411 Singapore, Singapore

ARTICLE INFO

Article history:
Received 24 April 2012
Received in revised form 21 August 2013
Accepted 29 August 2013
Available online 14 September 2013
Communicated by Gary McGuire

MSC:
11T06
11T71

Keywords:
APN functions
Zeros of polynomials
Irreducible polynomials

ABSTRACT

In [6], Lilya Budaghyan and Claude Carlet introduced a family of APN functions on $\mathbb{F}_{2^{2k}}$ of the form $F(x) = x(x^{2^i} + x^{2^k} + cx^{2^{k+i}}) + x^{2^i}(c^{2^k}x^{2^k} + \delta x^{2^{k+i}}) + x^{2^{k+i}+2^k}$. They showed that this infinite family exists provided the existence of the quadratic polynomial $G(y) = y^{2^i+1} + cy^{2^i} + c^{2^k}y + 1$, which has no zeros such that $y^{2^k+1} = 1$, or in particular has no zeros in $\mathbb{F}_{2^{2k}}$. However, up to now, no construction of such polynomials is known. In this paper, we show that, when k is an odd integer, the APN function F is CCZ-equivalent to the one in [2, Theorem 1]; and when k is even with $3 \nmid k$, we explicitly construct the polynomial G, and hence demonstrate the existence of F. More generally, it is well known that G relates to the polynomial $P_a(x) = x^{2^i+1} + x + a \in \mathbb{F}_{2^n}[x]$ and P_a has applications in many other contexts. We determine all coefficients a such that P_a has no zeros on $\mathbb{F}_{2^n}$ when $\gcd(i, n) = 1$ and n is even.

1. Introduction

Let $\mathbb{F}_{2^n}$ be a finite field. The number of zeros of the polynomial

$$P_a(x) = x^{2^i+1} + x + a, \quad a \in \mathbb{F}_{2^n}^* \tag{1}$$

* Corresponding author.
E-mail addresses: carlbracken@ntu.edu.sg (C. Bracken), tsltch@nus.edu.sg (C.H. Tan), itanyinmath@gmail.com (Y. Tan).

[1] The work was funded by DSO National Laboratories, Singapore.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.08.006

has been studied in [17,18] as it has applications in several different contexts. For example, constructing difference sets with Singer parameters [10,11], finding crosscorrelation between m-sequences [13,16] and more recently in constructing error correcting codes [3]. Also, a similar problem concerning the polynomial $x^{p^i+1}+ax+b$ over $\mathbb{F}_{p^n}$ has been considered by Bluher in [1] for any prime p.

The following result from [15, Lemma 9] (for n odd), and [1, Theorem 5.6] (for any n and without the condition $\gcd(i,n)=1$) shows that, when $\gcd(i,n)=1$, the polynomial P_a can only have none, one or three zeros.

Result 1.1. For any $a\in\mathbb{F}_{2^n}^*$ and a positive integer i with $\gcd(i,n)=1$, the polynomial $P_a(x)=x^{2^i+1}+x+a$ has either none, one, or three zeros in $\mathbb{F}_{2^n}$. Further, let M_j denote the number of a such that $P_a(x)$ has j zeros, then

(1) If n is odd,

$$M_0=\frac{2^n+1}{3},\qquad M_1=2^{n-1}-1,\qquad M_3=\frac{2^{n-1}-1}{3},$$

(2) If n is even,

$$M_0=\frac{2^n-1}{3},\qquad M_1=2^{n-1},\qquad M_3=\frac{2^{n-1}-2}{3}.$$

Furthermore, it was studied in [17, Theorem 1] that, for which a, $P_a(x)$ has exactly one zero. But it is still unclear that for which a, $P_a(x)$ has no zeros. In Theorem 2.1, when n is even, we solve the following problem.

Problem 1.2. For which $a\in\mathbb{F}_{2^n}^*$, does $P_a(x)$ have no zeros.

It is well known that $P_a(x)$ are related to other polynomials. More precisely, for a polynomial of the form $G(x)=x^{2^i+1}+\alpha x^{2^i}+\beta x+\gamma$ over $\mathbb{F}_{2^n}$, by substituting x with $x+\alpha$, $G(x)$ can be reduced to the form $H(x)=x^{2^i+1}+\alpha x+\beta$. Moreover, by a simple substitution $x=sx$ with $s^{2^i}=\alpha$, $H(x)$ can be transformed into the form $P_a(x)=x^{2^i+1}+x+a$. Through the above transformations and the polynomials obtained in Theorem 2.1, we may get the polynomials with the forms G and H which has no zeros on $\mathbb{F}_{2^n}$. These polynomials of the form G and H, especially those with no zeros, are of interest in other contexts, which is another reason for us to consider Problem 1.2. We will explain its applications to APN functions below.

Before discussing the application to APN functions, we would like to briefly introduce these functions. A function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN) if the number of solutions in $\mathbb{F}_{2^n}$ of the equation

$$F(x+a)+F(x)=b$$

is at most 2, for all $a,b\in\mathbb{F}_{2^n}, a\neq 0$. We also say it has differential uniformity of 2. APN functions were introduced by Nyberg in [20], who defined them as the mappings with highest resistance to differential cryptanalysis. In other words, APN functions are those for which the plaintext difference $x-y$ yields the ciphertext difference $f(x)-f(y)$ with probability $1/2^{n-1}$. Since Nyberg's characterization, many new APN functions have been constructed, see [6,2,5,7] and the references there. All the new infinite families (from 2005) have been quadratic (algebraic degree of 2) multinomials, as is the one F in this article. Note that, for a function $F(x)=\sum_{i=0}^{2^n-1}a_ix^i\in\mathbb{F}_{2^n}[x]$, its *algebraic degree*, denoted by $\deg F$, is defined to be the maximal 2-weight of the exponent i such that $a_i\neq 0$, where the 2-weight of an integer i is the number of ones in its binary expression.

Another application of APN functions is in the construction of error correcting codes. Each new APN function yields a new and inequivalent error correcting code with the parameters of the double error correcting BCH code. In fact, APN functions are said to be inequivalent if the extended BCH-like codes constructed from them are inequivalent codes, see [2] for details. We refer to inequivalent APN functions as CCZ-inequivalent (named after Carlet, Charpin and Zinoviev) [8]. This is a more general form of equivalence than the previously used affine and extended affine equivalences. It is well known that CCZ equivalence preserves the differential and extended Walsh spectrum of the function. Some other equivalent descriptions of CCZ-equivalence and its invariants may be found in [14].

In [6], the authors constructed a family of quadratic APN functions provided the existence of certain polynomials.

Result 1.3. Let n and i be any positive integers, $n = 2k$, $\gcd(i, k) = 1$, and $c, \delta \in \mathbb{F}_{2^n}$ be such that $\delta \notin \mathbb{F}_{2^k}$. If the equation

$$G(x) = x^{2^i+1} + cx^{2^i} + c^{2^k}x + 1 = 0$$

has no solution x such that $x^{2^k+1} = 1$, and in particular if the polynomial G has no zeros in $\mathbb{F}_{2^n}$, then the function

$$F(x) = x\left(x^{2^i} + x^{2^k} + cx^{2^{k+i}}\right) + x^{2^i}\left(c^{2^k}x^{2^k} + \delta x^{2^{k+i}}\right) + x^{2^{k+i}+2^k}$$

is an APN function.

It was verified by a computer in [6] that the aforementioned irreducible polynomial G exists on fields $\mathbb{F}_{2^{2k}}$ with $3 \leqslant k \leqslant 500$. But, up to now, there is no construction of an infinitive family of such polynomials. In Section 3, when $n = 2k$ with k even and $3 \nmid k$, we construct the polynomials with the form $G(x)$ without zeros on $\mathbb{F}_{2^{2k}}$ (Theorem 3.4) by applying the techniques used in Section 2.

We will conclude this section by giving some remarks on the APN function F in Result 1.3. One may check that, if $n = 2k$ with k odd, F is CCZ-equivalent to the multinomial APN function in [2, Theorem 1] by substituting x with $x + \gamma x^{2^k}$. Indeed, let $T(x) = bx^{2^i+1} + b^{2^k}x^{2^{k+i}+2^k} + cx^{2^k+1} + x^{2^{k+i}+2^i}$ be an APN function in [2, Theorem 1]. Substituting x with $x + \gamma x^{2^k}$ ($\gamma^{2^k+1} \neq 1$) into T, after expanding, simplifying and leaving the linear terms, we may get an APN function of the form F in Result 1.3. Therefore, to prove the existence of the APN function F in Result 1.3, it is sufficient to consider the case k is even and the existence of F.

It should be mentioned that we know the family of APN functions we are demonstrating the existence is inequivalent to other families, as computer evidence has verified that it is not equivalent to any power mapping when $n = 2k = 8$ [6]. Also for $n = 8$ we have checked by computer that F in not equivalent to $x^3 + \mathrm{Tr}(x^9)$. This is because F has Γ-rank 13 200 (see the definition in [14]), while $x^3 + \mathrm{Tr}(x^9)$ has Γ-rank 13 800. Furthermore, it must be different from the other recently discovered non-power APN functions as they are defined on fields with different degrees. In fact, it is a distinguishing factor of the family under consideration here that it can be defined on fields with degrees that are powers of 2. This property is seen as desirable for some (and necessary by others) cryptographic applications. The only other APN functions with this property are the Gold mapping x^{2^i+1}, Kasami mapping $x^{2^{2i}-2^i+1}$, as well as the mapping $x^3 + \mathrm{Tr}(x^9)$. These three mappings are defined on fields with any degree. Finally, by a computer, when $n = 8$, the function F in Result 1.3 is CCZ-equivalent to the No. 4 function in Dillon's slides [12].

2. A type of quadratic polynomial with no zeros

In this section, we will study for which $a \in \mathbb{F}_{2^n}^*$, the polynomial $P_a(x) = x^{2^i+1} + x + a$ has no zeros, where $n = 2k$ and $\gcd(n, i) = 1$. For the convenience of the expression, throughout the rest of the paper, we denote $q = 2^k$, $q' = 2^i$ and $Q = q^2$.

Theorem 2.1. *Let $P_a(x) = x^{q'+1} + x + a \in \mathbb{F}_Q[x]$, with $(n, i) = 1$. Let C be set of non-cubes in $\mathbb{F}_Q$ and A be a function from C to $\mathbb{F}_Q$ defined by*

$$A(b) \triangleq \frac{b(b+1)^{q'+q'^{-1}}}{(b+b^{q'^{-1}})^{q'+1}}, \tag{2}$$

where $x^{q'^{-1}}$ denotes $x^{1/q'}$. Then P_a has no zeros in $\mathbb{F}_Q$ if and only if $a \in \mathrm{Im}(A)$.

Proof. We start with the following polynomial,

$$K(x) = b\left(x + \frac{b^{q'^{-1}} + 1}{b + b^{q'^{-1}}}\right)^{q'+1} + \left(x + \frac{b^{q'^{-1}+1} + b}{b + b^{q'^{-1}}}\right)^{q'+1}.$$

Note that $b + b^{q'^{-1}}$ is always not zero as b is neither 1 nor 0 (as b is a non-cube). We will demonstrate that K has no zeros by setting $K(x) = 0$, which gives

$$b\left(x + \frac{b^{q'^{-1}} + 1}{b + b^{q'^{-1}}}\right)^{q'+1} = \left(x + \frac{b^{q'^{-1}+1} + b}{b + b^{q'^{-1}}}\right)^{q'+1}.$$

As one side of this expression is a cube, while the other is not, the only possible solutions are when it is identically zero. This implies

$$x = \frac{b^{q'^{-1}} + 1}{b + b^{q'^{-1}}} = \frac{b^{q'^{-1}+1} + b}{b + b^{q'^{-1}}},$$

which in turn implies that $b = 1$, a contradiction.

Next, we expand $K(x) = 0$ and gather terms to obtain,

$$(b+1)x^{q'+1} + \left(b \cdot \frac{b^{q'^{-1}} + 1}{b + b^{q'^{-1}}} + \frac{b^{q'^{-1}+1} + b}{b + b^{q'^{-1}}}\right)x^{q'} + \left(b \cdot \frac{b+1}{b + b^{q'}} + \frac{b^{q'+1} + b^{q'}}{b + b^{q'}}\right)x$$
$$+ b\left(\frac{b^{q'^{-1}} + 1}{b + b^{q'^{-1}}}\right)^{q'+1} + \left(\frac{b^{q'^{-1}+1} + b}{b + b^{q'^{-1}}}\right)^{q'+1} = 0.$$

This becomes

$$(b+1)x^{q'+1} + (b+1)x + \frac{b(b+1)^{q'+q'^{-1}+1}}{(b+b^{q'^{-1}})^{q'+1}} = 0.$$

Now, dividing by $b+1$ and with a few simplifications we obtain,

$$P_a(x) = x^{q'+1} + x + \frac{b(b+1)^{q'+q'^{-1}}}{(b+b^{q'^{-1}})^{q'+1}} = 0,$$

where $a = \frac{b(b+1)^{q'+q'^{-1}}}{(b+b^{q'^{-1}})^{q'+1}}$. So $P_a(x) = 0$ cannot have solutions in $\mathbb{F}_Q$ and hence $P_a(x)$ has no zeros when a has the required form.

Conversely, it is easy to verify that $A(b) = A(b^{-1})$ for any $b \in C$. Since $|C| = \frac{2(Q-1)}{3}$ and by Result 1.1(2) there are $\frac{Q-1}{3}$ elements a such that P_a has no zeros, it will be sufficient to prove that A is a 2-to-1 mapping. Writing $b = c^{2q'}$ and substituting it into (2) we have

$$\begin{aligned} A(b) &= \frac{c^{2q'}(c^{2q'}+1)^{q'+q'^{-1}}}{(c^{2q'}+c^2)^{q'+1}} = \frac{c^{2q'}(c^{2q'^2}+1)(c^2+1)}{(c^{2q'}+c^2)^{q'+1}} \\ &= \frac{c^{q'^2+2q'+1}(c^{q'^2}+c^{-q'^2})(c+c^{-1})}{(c^{2q'}+c^2)^{q'+1}} \\ &= \frac{c^{(q'+1)^2}(c+c^{-1})^{q'^2+1}}{c^{(1+q')^2}(c^{q'-1}+c^{1-q'})^{q'+1}} \\ &= \frac{(c+c^{-1})^{q'^2+1}}{(c^{q'-1}+c^{1-q'})^{q'+1}}. \end{aligned}$$

Note that as b is a non-cube we have $c \neq 0, 1$ and letting $e = \frac{1}{1+c}$, the following hold:

$$c + \frac{1}{c} = \frac{1}{e+e^2},$$

$$c^{q'-1} + c^{1-q'} = \left(\frac{1+e}{e}\right)^{q'-1} + \left(\frac{e}{1+e}\right)^{q'-1} = \frac{e^2+e^{2q'}}{(e+e^2)^{q'+1}}.$$

Substituting these two equations into $A(b)$ above we obtain

$$\begin{aligned} A(b) &= \left(\frac{1}{e+e^2}\right)^{q'^2+1} \cdot \left(\frac{(e+e^2)^{q'+1}}{e^2+e^{2q'}}\right)^{q'+1} \\ &= \frac{(e+e^2)^{2q'}}{(e+e^{q'})^{2q'+2}} \\ &= \frac{1}{(e+e^2)^2} \cdot \left(\frac{e+e^2}{e+e^{q'}}\right)^{2q'+2}. \end{aligned}$$

Now, we consider $\frac{1}{A(b)}$ and by the fact that $e + e^{q'} = (e+e^2) + (e^2+e^4) + \cdots + (e^{q'/2} + e^{q'})$, we get

$$\begin{aligned} \frac{1}{A(b)} &= \left(e+e^2\right)^2 \cdot \left(\frac{e+e^{q'}}{e+e^2}\right)^{2q'+2} \\ &= \left(\left(e^2+e\right) \cdot \left(1 + \left(e+e^2\right) + \cdots + \left(e+e^2\right)^{q'/2-1}\right)^{q'+1}\right)^2 \\ &= C_{q'}\left(e^2+e\right)^2 = C_{q'}\left(\frac{c}{1+c^2}\right), \end{aligned}$$

where $C_{q'}(z) = z(\sum_{j=0}^{\lg(q')-1} z^{2^j-1})^{q'+1}$ is the Muller–Cohen–Matthews polynomial, and $\lg(q')$ denotes the integer i such that $q' = 2^i$. By [9, Theorem 1.2], $C_{q'}$ is a permutation polynomial on $\mathbb{F}_Q$ if $\mathbb{F}_{q'} \cap \mathbb{F}_Q = \mathbb{F}_2$, which is the case here as $\gcd(i, 2k) = 1$.

Now, to prove that $A(b)$ is a 2-to-1 mapping, it is equivalent to showing that $\frac{1}{A(b)}$ is so. This is clear as one can check easily $\frac{c}{1+c^2}$ is a 2-to-1 mapping from C to $\mathbb{F}_Q$ and from above $C_{q'}(z)$ is a permutation on $\mathbb{F}_Q$. We finish the proof. □

Particularly, when $i = 1$, we may show that $P_a(x)$ is irreducible if and only if a has the form described in Theorem 2.1. We may claim the polynomial is irreducible as it has degree 3.

Corollary 2.2. *The polynomial $P_a(x) = x^3 + x + a$ is irreducible over $\mathbb{F}_Q$ if and only if $a = d + d^{-1}$ for some non-cube d.*

Proof. As $i = 1$ we have $q' = 2^i = 2$ in $A(b)$. Now

$$A(b) = \frac{b(b+1)^{2+2^{-1}}}{(b+b^{2^{-1}})^{2+1}} = \frac{b(b^{2^{-1}}+1)^{2\cdot(2+2^{-1})}}{b^{3\cdot 2^{-1}}(b^{2^{-1}}+1)^3} = \frac{b+1}{b^{2^{-1}}}.$$

By Theorem 2.1, $P_a(x)$ has no zeros if and only if $a = A(b) = \frac{b+1}{b^{2^{-1}}}$ for some $b \in C$. For a simpler form we let $b = d^2$ and a has the form $d + d^{-1}$ for a non-cube d. The proof is finished. □

By Theorem 2.1 and the relationship between the polynomials of the form $G(x) = x^{q'+1} + \alpha x^{q'} + \beta x + \gamma$ and $P_a(x) = x^{q'+1} + x + a$ mentioned in Section 1, we may obtain polynomials of the form G which has no zeros in $\mathbb{F}_Q$. In the next section, when $n \equiv 0 \bmod 4$ and $3 \nmid n$, we will use a variation of the method used in Theorem 2.1 to find the polynomial with the form $x^{q'+1} + cx^{q'} + c^q x + 1 \in \mathbb{F}_Q[x]$ and with no zeros in $\mathbb{F}_Q$ for some $c \in \mathbb{F}_Q$. It is the existence of this polynomial that guarantees the existence of the infinite family of APN functions in Result 1.3. We will show that for all relevant fields a coefficient c exists such that the polynomial has no zeros.

3. The existence of a family of hexanomial APN functions

In this section, we will demonstrate the existence of the hexanomial APN function F proposed in Result 1.3. Throughout this section, we assume $n = 2k$ with k is an even integer and $3 \nmid k$. In this section, we will show that the function

$$F(x) = x\left(x^{q'} + x^q + cx^{qq'}\right) + x^{q'}\left(c^q x^q + \delta x^{qq'}\right) + x^{qq'+q}$$

is an APN function over $\mathbb{F}_Q$ by choosing a particular type of $c, \delta \in \mathbb{F}_Q$. The nature of the coefficients was difficult to find and we require the following lemma to show that they exist. First we give the following results appeared in [21, Lemmas 1, 2, Main Theorem].

Result 3.1.

(1) Any element of the finite field $\mathbb{F}_{p^n}$, except $\mathbb{F}_4$ and $\mathbb{F}_7$, can be decomposed into the sum of two cubes.
(2) Let $\mathbb{F}_{2^n}$ be the finite field with n even, ω be a generator of $\mathbb{F}_4$ and C be the set of cubes in $\mathbb{F}_{2^n}$. Then an element in ωC is the sum of two cubes α, β if and only if $t = \alpha\beta^{-1} \in C$ and $t + 1 \in \omega C$. An element in $\omega^2 C$ is the sum of two cubes α, β if and only if $t = \alpha\beta^{-1} \in C$ and $t + 1 \in \omega^2 C$.

Now we give the following two lemmas which will be used later. Recall that $q = 2^k$, $q' = 2^i$ and $Q = q^2$.

Lemma 3.2. *Let $\mathbb{L} = \mathbb{F}_Q$ and k, i be integers such that $(i, 2k) = 1$ with k is even and $3 \nmid k$. Let $\mathbb{L}^3$ be the set of all cubes in $\mathbb{F}_Q$, ω be the generator of $\mathbb{F}_4$ and $D = \mathbb{F}_Q \setminus \mathbb{F}_q$. Then, there exist $a \in D \cap \mathbb{L}^3$, $b \in \mathbb{F}_q \cap \mathbb{L}^3$ and $c \in \mathbb{L}^3$ such that*

$$a + b = \omega c. \tag{3}$$

Proof. First, notice that, when n is even and $3 \nmid n$, all non-cubes in $\mathbb{L}$ can be written as ωc, $\omega^2 c$ for some $c \in \mathbb{L}^3$. To prove the result, it suffices to show that there exist $a \in D \cap \mathbb{L}^3$ and $c \in \mathbb{L}^3$ such that

$$a + 1 = \omega c \tag{4}$$

holds. Now, (i) if $a \in D \cap \mathbb{L}^3$ and $a + 1 \in \omega\mathbb{L}^3$, Eq. (4) clearly holds for some $c \in \mathbb{L}^3$; (ii) if $a \in D \cap \mathbb{L}^3$ and $a + 1 \in \omega^2\mathbb{L}^3$, we may then have an element $c \in \mathbb{L}^3$ such that $a + 1 = \omega^2 c$ and then $a^2 + 1 = \omega c^2$, thus we have Eq. (4) by replacing a, c with a^2, c^2 respectively. Therefore, we only need to exclude the case that $a + 1 \in \mathbb{L}^3$ for all $a \in D \cap \mathbb{L}^3$.

Assume this is true. Choosing one element $\beta \in \mathbb{F}_q \cap \mathbb{L}^3$, $\beta \neq 0, 1$, such that $\beta + 1 \in \mathbb{F}_q \cap \omega\mathbb{L}^3$. The existence of such β is guaranteed by Result 3.1(1) as the element in $\mathbb{F}_q \cap \omega\mathbb{L}^3 = \omega\mathbb{F}_q^3$ can be decomposed into the sum of two cubes of $\mathbb{F}_q$, and by Result 3.1(2) this holds if and only if such β exists. Now, given any $a \in D \cap \mathbb{L}^3$ (and then $a + 1 \in \mathbb{L}^3$ by the assumption), we claim that $a' = a\beta + a + \beta \in D \cap \mathbb{L}^3$ but $a' + 1 = (a\beta + a + \beta) + 1 \notin \mathbb{L}^3$, which gives the contradiction. We split the arguments into three steps:

(i) $a\beta + a + \beta = a(\beta + 1) + \beta \in D$, this is clear as $\beta \in \mathbb{F}_q$ and $a \in D$.
(ii) $a\beta + a + \beta \in \mathbb{L}^3$. Let $\eta = \frac{a\beta}{a+\beta}$, then η belongs to D as otherwise, if $\eta \in \mathbb{F}_q$, we have $a = \frac{\eta\beta}{\eta+\beta} \in \mathbb{F}_q$, which contradicts to $a \in D$ (note that $\eta \neq \beta$ since otherwise we will have $\eta\beta = 0$ from $\eta = a\beta/(a + \beta)$ and then $\eta = \beta = 0$, which contradicts to the choice of β above). Furthermore, $\eta \in \mathbb{L}^3$ since clearly $a\beta \in \mathbb{L}^3$, and $a + \beta = \beta(a\beta^{-1} + 1) \in \mathbb{L}^3$ by the fact that $a\beta^{-1} \in D \cap \mathbb{L}^3$ and then $a\beta^{-1} + 1 \in \mathbb{L}^3$ by the assumption above. It then follows from $\eta \in D \cap \mathbb{L}^3$ that $\eta + 1 = \frac{a\beta+a+\beta}{a+\beta} \in \mathbb{L}^3$, and then $a' = a\beta + a + \beta \in \mathbb{L}^3$.
(iii) $(a\beta + a + \beta) + 1 \notin \mathbb{L}^3$. This is because $(a\beta + a + \beta) + 1 = (a + 1)(\beta + 1)$, and by the assumption $a + 1 \in \mathbb{L}^3$ and $\beta + 1 \notin \mathbb{L}^3$.

We complete the proof. □

Lemma 3.3. *Let $\mathbb{L} = \mathbb{F}_Q$ and k, i be integers such that $(i, 2k) = 1$ with k is even and $3 \nmid k$. Let the other notations are the same as Lemma 3.2. Then there exist $\beta, \gamma \in \mathbb{L}^*(\triangleq \mathbb{L} \setminus \{0\})$ such that*

$$\gamma^{q'+1} + \omega\beta^{q'+1} + 1 = 0, \tag{5}$$

where ω has order 3 in $\mathbb{L}$ and $\gamma^{q-1} \neq \beta^{q-1}$.

Proof. By Lemma 3.2, there exist $a \in D \cap \mathbb{L}^3$, $b \in \mathbb{F}_q \cap \mathbb{L}^3$ and $c \in \mathbb{L}^3$ such that $a + b = \omega c$ holds. We divide $a + b = \omega c$ by a to obtain,

$$1 + \frac{b}{a} + \omega\frac{c}{a} = 0.$$

Letting α be primitive in $\mathbb{L}$ and assuming that $b/a = \alpha^t$, $\omega c/a = \alpha^r$ for some integers r, t, we rewrite the above equation as,

$$1 + \alpha^t + \alpha^r = 0. \tag{6}$$

All we can say about t and r is that $3 \mid t$ while $3 \nmid r$ and that at least one of α^t and α^r is not in $\mathbb{F}_q$.

From (6) we will give the construction of the required equation

$$\gamma^{q'+1} + \omega\beta^{q'+1} + 1 = 0,$$

and show that the condition $\gamma^{q-1} \neq \beta^{q-1}$ is satisfied.

We start with (6). Dividing by α^t to obtain

$$\alpha^{-t} + 1 + \alpha^{r-t} = 0.$$

Now, we let $\alpha^{-t} = \gamma^{q'+1}$ and $\alpha^{r-t} = \omega\beta^{q'+1}$ and then get the required Eq. (5). The existence of β, γ is guaranteed by the fact that $(i, 2k) = 1$ and then $(q'+1, Q-1) = 3$, so all cubes can be represented as $(q'+1)$-th powers. Now assume that

$$\gamma^{q-1} = \beta^{q-1},$$

which implies,

$$\gamma^{(q'+1)(q-1)} = \beta^{(q'+1)(q-1)}.$$

We write this in terms of α and get

$$\alpha^{-t(q-1)} = \left(\omega^2\alpha^{r-t}\right)^{q-1}.$$

This yields

$$\alpha^{r(q-1)} = 1.$$

In this case $\alpha^r \in \mathbb{F}_q$. However, this will not happen as otherwise by (6), $\alpha^r \in \mathbb{F}_q$ will yield $\alpha^t \in \mathbb{F}_q$, which contradicts to the assumption that one of α^t and α^r is not in $\mathbb{F}_q$. The proof is complete. □

Next we will use β and γ in Lemma 3.3 and a modification of the techniques in Theorem 2.1 to prove the existence of the following family of APN functions.

Theorem 3.4. *Let i and k be integers, with k even, such that $(i, 2k) = 1$ and $3 \nmid k$. Denoting by $q' = 2^i$, $q = 2^k$ and $Q = q^2$. We choose $\delta \notin \mathbb{F}_q$, ω to have order 3 and β and γ such that $\gamma^{q'+1} + \omega\beta^{q'+1} + 1 = 0$ with $\gamma^{q-1} \neq \beta^{q-1}$. Then the function*

$$F(x) = x\left(x^{q'} + x^q + cx^{qq'}\right) + x^{q'}\left(c^q x^q + \delta x^{qq'}\right) + x^{qq'+q}$$

is an APN function on $\mathbb{F}_Q$, where $c = \omega\beta^{q+q'} + \gamma^{q+q'}$.

Proof. The existence of β and γ is guaranteed from Lemma 3.3. By Result 1.3, to prove F is an APN function, it suffices to show that

$$G(y) = y^{q'+1} + \left(\omega\beta^{q+q'} + \gamma^{q+q'}\right)y^{q'} + \left(\omega\beta^{qq'+1} + \gamma^{qq'+1}\right)y + 1$$

has no zeros in $\mathbb{F}_Q$. In the following, we set $G(y) = 0$ and then use the techniques in Theorem 2.1 to produce a factorization which allows no solutions. The β and γ were chosen very carefully to allow the usage of this technique.

From $\omega^2\beta^{-q'-1}G(y)=0$, we obtain

$$\omega^2\beta^{-q'-1}y^{q'+1}+\left(\beta^{q-1}+\omega^2\gamma^{q'+q}\beta^{-q'-1}\right)y^{q'}+\left(\beta^{qq'-q'}+\omega^2\gamma^{qq'+1}\beta^{-q'-1}\right)y+\omega^2\beta^{-q'-1}=0.$$

A simple rearrangement of $\gamma^{q'+1}+\omega\beta^{q'+1}+1=0$ will allow us to write the coefficient of $y^{q'+1}$ as $\omega^2(\frac{\gamma}{\beta})^{q'+1}+1$. The coefficient of $y^{q'}$ can be rewritten as

$$\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{q-1}+\beta^{q-1},$$

while the coefficient of y can be written as

$$\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{qq'-q'}+\beta^{qq'-q'}.$$

Now, using the fact that,

$$\gamma^{q(q'+1)}+\omega\beta^{q(q'+1)}=1,$$

we can alter the last term, $\omega^2\beta^{-q'-1}$, as follows,

$$\begin{aligned}\omega^2\beta^{-q'-1}&=\omega^2\beta^{-q'-1}\left(\gamma^{q(q'+1)}+\omega\beta^{q(q'+1)}\right)\\&=\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{(q'+1)(q-1)}+\beta^{(q'+1)(q-1)}.\end{aligned}$$

Placing these alternate forms of the coefficients into $\omega^2\beta^{-q'-1}G(y)=0$ yields,

$$\left(\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}+1\right)y^{q'+1}+\left(\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{q-1}+\beta^{q-1}\right)y^{q'}+\left(\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{qq'-q'}+\beta^{qq'-q'}\right)y$$
$$+\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\gamma^{(q'+1)(q-1)}+\beta^{(q'+1)(q-1)}=0.$$

This implies

$$\begin{aligned}&\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\left(y^{q'+1}+\gamma^{q-1}y^{q'}+\gamma^{q'(q-1)}y+\gamma^{(q'+1)(q-1)}\right)\\&\quad=y^{q'+1}+\beta^{q-1}y^{q'}+\beta^{q'(q-1)}y+\beta^{(q'+1)(q-1)}.\end{aligned}$$

Next we factor each side to obtain,

$$\omega^2\left(\frac{\gamma}{\beta}\right)^{q'+1}\left(y+\gamma^{q-1}\right)^{q'+1}=\left(y+\beta^{q-1}\right)^{q'+1}.$$

Clearly the right hand side of this expression is a cube while the left hand side is not. So the only possible solutions occur when $y=\gamma^{q-1}=\beta^{q-1}$, but as we have chosen γ and β such that $\gamma^{q-1}\neq\beta^{q-1}$, we can now say that $G(y)$ has no zeros and the proof is complete. □

We cannot determine the Fourier (Walsh) spectrum of the APN function F in Theorem 3.4 and we leave this as an open problem. By a computer (with $n = 8$), the Fourier spectrum of F is the same as the Gold APN functions, i.e., the spectrum takes the values $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$.

All other known APN functions have had their Fourier spectra computed, see [4] and references therein. This is done for two reasons. The first is a cryptographic application. Knowing a function's spectrum can allow us to compute its nonlinearity, which measures the function's resistance to Matsui's linear attack [19]. Secondly, the weight distribution of the codewords in the BCH-like code constructed from the function is also determined by the functions spectrum. All codes derived from an APN function will have a minimum distance of 5, but the weight distributions differ among some of the six power mapping APN functions. The infinite families of multi-term quadratic APN functions discovered since 2005 all have the same spectrum as the Gold function and we expect the function in this article to be no different.

Conjecture 3.5. *The Fourier spectrum of the APN function F in Theorem 3.4 is* $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$.

4. Conclusions

In this paper, we considered for which $a \in \mathbb{F}_{2^n}$, the polynomial $P_a(x) = x^{2^i+1} + x + a \in \mathbb{F}_{2^n}[x]$ has no zeros in $\mathbb{F}_{2^n}$, where $\gcd(n, i) = 1$ and $n = 2k$. It is shown that $P_a(x) = 0$ has no solutions in $\mathbb{F}_{2^n}$ if and only if

$$a = \frac{b(b+1)^{2^i+2^{-i}}}{(b+b^{2^{-i}})^{2^i+1}}$$

for some non-cube b. Particularly, we show that $x^3 + x + a \in \mathbb{F}_{2^n}[x]$ is irreducible if and only if $a = d + d^{-1}$, for some non-cube d. By applying the techniques used here, when $\gcd(2k, i) = 1$, $3 \nmid k$ and k even, we obtain an infinite family of polynomials of the form $x^{2^i+1} + cx^{2^i} + c^{2^k}x + 1 \in \mathbb{F}_{2^{2k}}[x]$ which has no zeros in $\mathbb{F}_{2^{2k}}$. This guarantees the existence of the infinite family of quadratic APN functions proposed by Budaghyan and Carlet in [6].

Acknowledgments

We would like to thank the reviewers for their careful reading of the earlier version of this paper and their detailed comments, which improve the quality and the presentation significantly. We especially wish to thank one of the reviewers for suggesting a proof for the converse of Theorem 2.1.

References

[1] A.W. Bluher, On $x^{q+1} + ax + b$, Finite Fields Appl. 10 (3) (2004) 285–305.
[2] C. Bracken, E. Byrne, N. Markin, G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl. 14 (3) (2008) 703–714.
[3] C. Bracken, T. Helleseth, Triple-error-correcting BCH-like codes, in: IEEE Int. Symp. Inf. Theory, 2009, pp. 1723–1725.
[4] C. Bracken, Zhengbang Zha, On the Fourier spectra of the infinite families of quadratic APN functions, Adv. Math. Commun. 3 (3) (2009) 219–226.
[5] C. Bracken, E. Byrne, N. Markin, G. McGuire, A few more quadratic APN functions, Cryptogr. Commun. 3 (1) (2011) 43–53.
[6] L. Budaghyan, C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inform. Theory 54 (5) (2008) 2354–2357.
[7] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inform. Theory 54 (9) (2008) 4218–4229.
[8] C. Carlet, P. Charpin, V. Zinoviev, Bent functions and permutations suitable for DES-like cryptosytems, Des. Codes Cryptogr. 15 (2) (1998) 125–156.
[9] S.D. Cohen, R.D. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 354 (2) (1994) 897–909.
[10] J.F. Dillon, Geometry, codes and difference sets: Exceptional connections, in: A. Seress, K.T. Arasu (Eds.), Codes and Designs, in: Ohio State Uni. Math. Res. Inst. Publ., vol. 10, de Gruyter, Berlin, 2002, pp. 73–85.
[11] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (3) (2004) 342–389.

[12] J.F. Dillon, Almost perfect nonlinear polynomials: An update, in: 9th International Conference on Finite Fields and Applications of Fq9, Dublin, Ireland, 2009.
[13] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans. Inform. Theory 52 (2) (2006) 613–627.
[14] Y. Edel, A. Pott, A new almost perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3 (1) (2009) 59–81.
[15] T. Helleseth, V. Zinoviev, Codes with the same coset weight distributions as the $\mathbb{Z}_r$-linear Goethals codes, IEEE Trans. Inform. Theory 47 (4) (2001) 1589–1595.
[16] T. Helleseth, A. Kholosha, G.J. Ness, Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued crosscorrelation, IEEE Trans. Inform. Theory 53 (6) (2007) 2236–2245.
[17] T. Helleseth, A. Kholosha, On the equation $x^{2^l+1}+x+a=0$ over $GF(2^k)$, Finite Fields Appl. 14 (1) (2008) 159–176.
[18] T. Helleseth, A. Kholosha, $x^{2^l+1}+x+a$ and related affine polynomials over $GF(2^k)$, Cryptogr. Commun. 2 (2010) 85–109.
[19] M. Matsui, Linear cryptanalysis method for DES cipher, in: EUROCRYPT 93, in: Lecture Notes in Comput. Sci., vol. 765, 1994, pp. 386–397.
[20] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology—EUROCRYPT 93, in: Lecture Notes in Comput. Sci., vol. 765, 1994, pp. 55–64.
[21] S. Singh, Analysis of each integer as sum of two cubes in a finite integral domain, Indian J. Pure Appl. Math. 6 (1975) 29–35.