Solving x 2 k + 1 + x + a = 0 in F 2 n with gcd (n , k) = 1

Kwang Ho Kim, Sihem Mesnager

Version of Record: https://www.sciencedirect.com/science/article/pii/S1071579719301339
Manuscript_8310875435d366328c8363ef9d23e3e9

Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$

Kwang Ho Kim[1,2] and Sihem Mesnager[3]

[1] Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People's Republic of Korea
[2] PGItech Corp., Pyongyang, Democratic People's Republic of Korea
khk.cryptech@gmail.com
[3] LAGA, Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cite, 93430 Villetaneuse, France and Telecom ParisTech 75013 Paris, France.
smesnager@univ-paris8.fr

November 13, 2019

Abstract. Let N_a be the number of solutions to the equation $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ where $\gcd(k, n) = 1$. In 2004, by Bluher [2] it was known that possible values of N_a are only 0, 1 and 3. In 2008, Helleseth and Kholosha [13] found criteria for $N_a = 1$ and an explicit expression of the unique solution when $\gcd(k, n) = 1$. In 2010 [14], the extended version of [13], they also got criteria for $N_a = 0, 3$. In 2014, Bracken, Tan and Tan [5] presented another criterion for $N_a = 0$ when n is even and $\gcd(k, n) = 1$.

This paper completely solves this equation $x^{2^k+1} + x + a = 0$ with only the condition $\gcd(n, k) = 1$. We explicitly calculate all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$. New criteria for which a, N_a is equal to 0, 1 or 3 are by-products of our result.

Keywords Equation · Müller-Cohen-Matthews (MCM) polynomial · Dickson polynomial · Zeros of polynomial · Irreducible polynomial.

1 Introduction

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

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

have been studied in [2, 13, 14]. This polynomial has arisen in several different contexts including the inverse Galois problem [1], the construction of difference sets with Singer parameters [9], finding cross-correlation between m-sequences [11, 12], construction of error correcting codes [4], APN functions [5, 6], and designs [15]. More general polynomial forms $x^{2^k+1} + rx^{2^k} + sx + t$ are also transformed into this form by a simple substitution of variable x with $(r + s^{\frac{1}{2^k}})x + r$.

It is clear that $P_a(x)$ has no multiple roots. In 2004, Bluher [2] proved following result.

Theorem 1. *For any $a \in \mathbb{F}_{2^n}^*$ and a positive integer k, the polynomial $P_a(x)$ has either none, one, two or $2^{\gcd(k,n)}+1$ zeros in $\mathbb{F}_{2^n}$.*

It should be pointed out that, Bluher demonstrated in [3] that P_a has the same splitting field as some Müller-Cohen-Matthews polynomial by explicitly writing the roots of P_a, more precisely, a polynomial that is equivalent to P_a, in terms of the roots of this Müller-Cohen-Matthews polynomial and conversely. However, the question of which roots are rational, that is, which solutions are in a given finite field, was not considered. Therefore, the rationality question requires new arguments that are presented in this paper.

In this paper, we will consider a particular case with $\gcd(n,k)=1$. In this case, Theorem 1 says that $P_a(x)$ has none, one or three zeros in $\mathbb{F}_{2^n}$ [13].

In 2008, Helleseth and Kholosha [13] have provided criteria for which a the polynomial $P_a(X)$ has exactly one zero in $\mathbb{F}_{2^n}$ and an explicit expression of the unique zero when $\gcd(k,n)=1$. In 2010 [14], the extended version of [13], they also got criteria for which a, $P_a(x)$ has none or three zeros.

In 2014, Bracken, Tan and Tan [5] presented another criterion for which a the polynomial $P_a(x)$ has no zero in $\mathbb{F}_{2^n}$ when n is even and $\gcd(k,n)=1$.

In this paper, we explicitly calculate all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$ when $\gcd(n,k)=1$. New criteria for which a, N_a is equal to 0, 1 or 3 are by-products of this result.

We begin with showing that we can reduce the study to the case when k is odd. In the odd k case, one core of our approach is to exploit a recent polynomial identity special to characteristic 2, presented in [3] (Theorem 3). This polynomial identity enables us to divide the problem of finding zeros in $\mathbb{F}_{2^n}$ of P_a into two independent problems: Problem 1 to find the unique preimage of an element in $\mathbb{F}_{2^n}$ under a Müller-Cohen-Matthews (MCM) polynomial and Problem 2 to find the preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial (subsection 3.1). There are two key stages to solve Problem 1. One is to establish a relation of the MCM polynomial with the Dobbertin polynomial. The other is to find an explicit formula for the solutions of the affine equation $x^{2^k}+x=b, b\in\mathbb{F}_{2^n}$. These are done in subsection 3.2 and Problem 1 is solved by Theorem 5. Problem 2 is relatively easy which is answered by Theorem 6 and Theorem 7 in subsection 3.3. Finally, we collect together all these results to give explicit expressions for all possible zeros in $\mathbb{F}_{2^n}$ of P_a in Theorem 8, Theorem 9 and Theorem 10.

2 Preliminaries

In this section, we state some results on finite fields and introduce classical polynomials that we shall need in the sequel. We begin with the following result that will play an important role in our study [9].

Proposition 1. *Let n be a positive integer. Then, every element z of $\mathbb{F}_{2^n}^* := \mathbb{F}_{2^n} \setminus \{0\}$ can be written (twice) $z = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star := \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ if $Tr_1^n(\frac{1}{z}) = 0$ and $c \in \mu_{2^n+1}^\star := \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\} \setminus \{1\}$ if $Tr_1^n(\frac{1}{z}) = 1$.*

Proof. For $z \in \mathbb{F}_{2^n}^*$, $z = c + \frac{1}{c}$ is equivalent to $\frac{1}{z^2} = \frac{c}{z} + \left(\frac{c}{z}\right)^2$, and thus this equation has a solution in $\mathbb{F}_{2^n}$ if and only if $Tr_1^n(\frac{1}{z}) = 0$. Hence, mapping $c \longmapsto c + \frac{1}{c}$ is 2-to-1 from $\mathbb{F}_{2^n}$ onto $\{z \in \mathbb{F}_{2^n} \mid Tr_1^n(\frac{1}{z}) = 0\}$ with convention $\frac{1}{0} := 0$. Also, since $\left(c + \frac{1}{c}\right)^{2^n} = c^{2^n} + \left(\frac{1}{c}\right)^{2^n} = \frac{1}{c} + c$ for $c \in \mu_{2^n+1}^\star$, the mapping $c \longmapsto c + \frac{1}{c}$ is 2-to-1 from $\mu_{2^n+1}^\star$ with cardinality 2^n onto $\{z \in \mathbb{F}_{2^n} \mid Tr_1^n(\frac{1}{z}) = 1\}$ with cardinality 2^{n-1}. □

We shall also need two classical families of polynomials, Dickson polynomials of the first kind and Müller-Cohen-Matthews polynomials.

The Dickson polynomial of the first kind of degree k in indeterminate x and with parameter $a \in \mathbb{F}_{2^n}^*$ is

$$D_k(x,a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} a^k x^{k-2i},$$

where $\lfloor k/2 \rfloor$ denotes the largest integer less than or equal to $k/2$. In this paper, we consider only Dickson polynomials of the first kind $D_k(x,1)$, that we shall denote $D_k(x)$ throughout the paper. A classical property of Dickson polynomials that we shall use extensively is

Proposition 2. *For any positive integer k and any $x \in \mathbb{F}_{2^n}$, we have*

$$D_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}. \tag{2}$$

Müller-Cohen-Matthews polynomials are defined as follows [7],

$$f_{k,d}(X) := \frac{T_k(X^c)^d}{X^{2^k}}$$

where

$$T_k(X) := \sum_{i=0}^{k-1} X^{2^i} \quad \text{and} \quad cd = 2^k + 1.$$

A basic property for such polynomials that we shall need in this paper is the following statement.

Theorem 2. *Let k and n be two positive integers with $\gcd(k,n) = 1$.*

1. *If k is odd, then $f_{k,2^k+1}$ is a permutation on $\mathbb{F}_{2^n}$.*
2. *If k is even, then $f_{k,2^k+1}$ is 2-to-1 on $\mathbb{F}_{2^n}$.*

Proof. For odd k, see [7]. When k is even, n is odd as $\gcd(n,k) = 1$. Theorem 10 of [9] states that $f_{k,1}$ is 2-to-1, and then the statement follows from the facts that $f_{k,2^k+1}(x^{2^k+1}) = f_{k,1}(x)^{2^k+1}$ and $\gcd(2^k+1, 2^n-1) = 1$ when $\gcd(k,n) = 1$ and n is odd. □

We will exploit a recent polynomial identity involving Dickson polynomials established by Bluher in [3, Theorem 2.2].

Theorem 3. *In the polynomial ring* $\mathbb{F}_{2^k}[X,Y]$*, we have the identity*

$$X^{2^{2k}-1}+\left(\sum_{i=1}^{k} Y^{2^k-2^i}\right)X^{2^k-1}+Y^{2^k-1}=\prod_{w\in\mathbb{F}_{2^k}^*}\left(D_{2^k+1}(wX)-Y\right).$$

Finally, we remark that the identity by Abhyankar, Cohen, and Zieve [1, Theorem 1.1] tantalizingly similar to this identity treats any characteristic, while this identity is special to characteristic 2 (this may happen because the Dickson polynomials are ramified at the prime 2). However, the Abhyankar-Cohen-Zieve identity has not led us to solve $P_a(x)=0$.

3 Solving $P_a(x)=0$

Throughout this section, k and n are coprime and we set $q=2^k$.

3.1 Splitting the problem

One core of our approach relies on Theorem 3. To this end, we observe firstly that

$$\sum_{i=1}^{k} Y^{q-2^i}=Y^qT_k(1/Y)^2$$

and

$$f_{k,q+1}(1/Y)=Y^qT_k(1/Y)^{q+1}.$$

Introduce an indeterminate T, algebraic over $\mathbb{F}_{2^n}(Y)$, satisfying

$$T^{q^2-q}=\sum_{i=1}^{k} Y^{q-2^i}=Y^qT_k(1/Y)^2. \tag{3}$$

Then,

$$(T^{q^2-q})^{q+1}=Y^{q(q+1)}T_k(1/Y)^{2(q+1)}=Y^{q^2-q}f_{k,q+1}(1/Y)^2. \tag{4}$$

Substituting TZ for X in the identity of Theorem 3, the left side is

$$(TZ)^{q^2-1}+T^{q^2-q}(TZ)^{q-1}+Y^{q-1}=T^{q^2-1}(Z^{q^2-1}+Z^{q-1}+A),$$

where $A=Y^{q-1}/T^{q^2-1}$. By (4),

$$A^q=Y^{q^2-q}/T^{q^3-q}=f_{k,q+1}(1/Y)^{-2}. \tag{5}$$

Theorem 3 therefore implies that

$$Z^{q^2-1}+Z^{q-1}+A=T^{1-q^2}\prod_{w\in\mathbb{F}_{2^k}^*}(D_{q+1}(wTZ)-Y). \tag{6}$$

If we specialize to $A=a,T=t,Y=y$ in a manner so that the corresponding relations (3), (5) hold with a,t,y in place of A,T,Y, then (6) will hold as well. In particular, let $a\in\mathbb{F}_{2^n}^*$. Assuming k to be odd, then $f_{k,q+1}$ permutes $\mathbb{F}_{2^n}^*$, so that a unique $y\in\mathbb{F}_{2^n}^*$ can be found satisfying the specialization of (5):

$$a^q=f_{k,q+1}\left(\frac{1}{y}\right)^{-2}. \tag{7}$$

Since $\gcd(q-1,2^n-1)=1$, the function x^{q-1} permutes $\mathbb{F}_{2^n}^*$. Thus, there is a unique t satisfying the specialization of (3):

$$t^{q^2-q}=y^qT_k\left(\frac{1}{y}\right)^2. \tag{8}$$

We then have from (6):

$$P_a(Z^{q-1})=t^{1-q^2}\prod_{w\in\mathbb{F}_{2^k}^*}(D_{q+1}(wtZ)-y). \tag{9}$$

Therefore, when k is odd, equation (9) states that finding the zeros of $P_a(Z^{q-1})$ amounts to determining the preimages of y under the Dickson polynomial D_{q+1}.

When k is even, $f_{k,q+1}$ is no longer a permutation and we cannot repeat again the preceding argument (indeed, when k is even, $f_{k,q+1}$ is 2-to-1, see Theorem 2). Fortunately, we can go back to the odd case by rewriting the equation. Indeed, for $z\in\mathbb{F}_{2^n}$,

$$\begin{aligned}P_a(z)=z^{2^k+1}+z+a&=\left(z^{2^{n-k}+1}+z^{2^{n-k}}+a^{2^{n-k}}\right)^{2^k}\\&=\left((z+1)^{2^{n-k}+1}+(z+1)+a^{2^{n-k}}\right)^{2^k}\end{aligned}$$

and so

$$\{z\in\mathbb{F}_{2^n}\mid P_a(z)=0\}=\left\{z+1\mid z^{2^{n-k}+1}+z+a^{2^{n-k}}=0,\ z\in\mathbb{F}_{2^n}\right\}. \tag{10}$$

If k is even, then n is odd as $\gcd(k,n)=1$, and so $n-k$ is odd and we can reduce to the odd case.

We now summarize all the above discussion in the following theorem.

Theorem 4. *Let k and n be two positive integers such that $\gcd(k,n)=1$.*

1. *Let k be odd and $q=2^k$. Let $y\in\mathbb{F}_{2^n}^*$ be (uniquely) defined by $a=\frac{1}{f_{k,q+1}\left(\frac{1}{y}\right)^{\frac{2}{q}}}$. Then,*

$$\{z\in\mathbb{F}_{2^n}\mid P_a(z)=0\}=\left\{\frac{u^{q-1}}{yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}}\mid D_{q+1}(u)=y,\ u\in\mathbb{F}_{2^n}\right\}.$$

2. *Let k be even and $q' = 2^{n-k}$. Let $y' \in \mathbb{F}_{2^n}^*$ be (uniquely) defined by $a^{q'} = \frac{1}{f_{n-k,q'+1}\left(\frac{1}{y'}\right)^{\frac{2}{q'}}}$. Then,*

$$\{z \in \mathbb{F}_{2^n} \mid P_a(z) = 0\} = \left\{ 1 + \frac{u^{q'-1}}{y' T_{n-k}\left(\frac{1}{y'}\right)^{\frac{2}{q'}}} \mid D_{q'+1}(u) = y',\ u \in \mathbb{F}_{2^n} \right\}.$$

Proof. Suppose that k is odd. Let t be the unique element of $\mathbb{F}_{2^n}^*$ such that $t^{q-1} = yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}$.

Equation (9) shows that the zeros of P_a in $\mathbb{F}_{2^n}$ are z^{q-1} for the elements $z \in \mathbb{F}_{2^n}^\star$ such that $D_{q+1}(wtz) = y$ for some $w \in \mathbb{F}_{2^k}^*$. Now, we will prove that indeed it must be $w = 1$ for such z's if any. Remember $D_{q+1}(X) = X^{q+1}(1+T_k(1/X))^2$ (Lemma 2.1 of [8]). Hence, $y = D_{q+1}(wtz) = (tz)^{q-1}(wtz + wtzT_k(1/wtz))^2$. Setting $v = \frac{1}{wtz}$, we have $\frac{1+T_k(v)}{v} = \left(\frac{y}{(tz)^{q-1}}\right)^{1/2}$. For simplicity, let us introduce new denotation $c = \left(\frac{y}{(tz)^{q-1}}\right)^{1/2} \in \mathbb{F}_{2^n}^*$. Then, we have

$$1 + T_k(v) = cv.$$

Squaring both sides of this equality yields $1 + T_k(v) + v + v^q = c^2v^2$, and since $v^q = \frac{1}{(tz)^{q-1}}v$, we have

$$1 + T_k(v) + v(1 + \frac{1}{(tz)^{q-1}}) = c^2v^2.$$

From these two equalities, we get

$$v(1 + c + \frac{1}{(tz)^{q-1}}) = c^2v^2.$$

As $cv \neq 0$, from this equality it follows

$$v = \frac{1 + c + \frac{1}{(tz)^{q-1}}}{c^2} \in \mathbb{F}_{2^n}$$

and so $w = \frac{1}{vtz} \in \mathbb{F}_{2^k}^* \cap \mathbb{F}_{2^n}^* = \{1\}$, that is,

$$w = 1.$$

Thus, Item 1 is proved. Item 2 follows from Item 1 and equality (10). □

Theorem 4 shows that we can split the problem of finding the zeros in $\mathbb{F}_{2^n}$ of P_a into two independent problems with odd k.

Problem 1. For $a \in \mathbb{F}_{2^n}^*$, find the unique element y in $\mathbb{F}_{2^n}^*$ such that

$$a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{y}\right)}. \tag{11}$$

Problem 2. For $y \in \mathbb{F}_{2^n}^*$, find the preimages in $\mathbb{F}_{2^n}$ of y under the Dickson polynomial D_{q+1}, that is, find the elements of the set

$$D_{q+1}^{-1}(y) = \{u \in \mathbb{F}_{2^n} \mid D_{q+1}(u) = y\}. \tag{12}$$

In the following two subsections, we shall study those two problems only when k is odd since, if k is even, it suffices to replace k by $n-k$, q by $q'=2^{n-k}$, and a by $a^{q'}$ in all the results of the odd case.

3.2 On problem 1

In this subsection, we show that solving Problem 1 amounts to finding a solution in $\mathbb{F}_{2^{2n}}$ of an affine equation $x+x^q=b$, for which we prove

Proposition 3. *Let k be odd and $\gcd(n,k)=1$. Then, for any $b \in \mathbb{F}_{2^n}$,*

$$\{x \in \mathbb{F}_{2^{2n}} \mid x+x^q=b\} = S_{n,k}\left(\frac{b}{\zeta+1}\right) + \mathbb{F}_2,$$

where $S_{n,k}(x)=\sum_{i=0}^{n-1} x^{q^i}$ and ζ is an element of $\mu_{2^n+1}^\star$.

Proof. As it was assumed that k is odd and $\gcd(n,k)=1$, it holds $\gcd(2n,k)=1$ and so the linear mapping $x \in \mathbb{F}_{2^{2n}} \longmapsto x+x^q$ has kernel of dimension 1, i.e. the equation $x+x^q=b$ has at most 2 solutions in $\mathbb{F}_{2^{2n}}$. Since $S_{n,k}(x)+(S_{n,k}(x))^q = x+x^{q^n}$, we have

$$\begin{aligned} S_{n,k}\left(\frac{b}{\zeta+1}\right) + \left(S_{n,k}\left(\frac{b}{\zeta+1}\right)\right)^q + b &= \frac{b}{\zeta+1} + \left(\frac{b}{\zeta+1}\right)^{q^n} + b \\ &= \frac{b}{\zeta+1} + \frac{b}{\zeta^{q^n}+1} + b \\ &= \frac{b}{\zeta+1} + \frac{b}{1/\zeta+1} + b \\ &= 0 \end{aligned}$$

and thus really $S_{n,k}\left(\frac{b}{\zeta+1}\right), S_{n,k}\left(\frac{b}{\zeta+1}\right)+1 \in \mathbb{F}_{2^{2n}}$ are the $\mathbb{F}_{2^{2n}}-$solutions of the equation $x+x^q=b$. □

For any $x \in \mathbb{F}_{2^{2n}}$, define

$$Q'_{k,k'}(x) = \frac{x^{q+1}}{\sum_{i=1}^{k'} x^{q^i}} \tag{13}$$

where $k' < 2n$ is the inverse of k modulo $2n$, that is, s.t. $kk' = 1 \mod 2n$. Note that k' is odd since $\gcd(k',2n)=1$. It is known that if $\gcd(2n,k)=1$ and k' is odd, then $Q'_{k,k'}$ is a permutation on $\mathbb{F}_{2^{2n}}$ (see [9] or [10] where $Q_{k,k'}=1/Q'_{k,k'}$ is instead considered). Indeed, due to [9], defining the following sequences of polynomials

$$A_1(X)=X,\ A_2(X)=X^{q+1},\ A_{i+2}(X)=X^{q^{i+1}}A_{i+1}(X)+X^{q^{i+1}-q^i}A_i(X), \quad i \geq 1,$$

$B_1(X) = 0$, $B_2(X) = X^{q-1}$, $B_{i+2}(X) = X^{q^{i+1}} B_{i+1}(X) + X^{q^{i+1}-q^i} B_i(X), \quad i \geq 1,$

then the polynomial expression of the inverse $R_{k,k'}$ of the mapping induced by $Q'_{k,k'}$ on $\mathbb{F}_{2^{2n}}$ is

$$R_{k,k'}(x) = \sum_{i=1}^{k'} A_i(x) + B_{k'}(x). \tag{14}$$

Directly from the definitions, it follows that, for any $x \in \mathbb{F}_{2^{2n}}$,

$$f_{k,q+1}(x + x^2) = \frac{(x + x^q)^{q+1}}{x^q + x^{2q}}$$

and

$$Q'_{k,k'}(x + x^q) = \frac{(x + x^q)^{q+1}}{x^q + x^{q^{k'+1}}}.$$

Since $x^{2q} = x^{q^{k'+1}} \iff x = x^{2^{kk'-1}}$, it holds that

$$f_{k,q+1}(x + x^2) = Q'_{k,k'}(x + x^q). \tag{15}$$

Define an element x of $\mathbb{F}_{2^{2n}}$ by

$$\frac{1}{y} = x + x^2.$$

By using (15), we can rewrite (11) as

$$a^{-\frac{q}{2}} = Q'_{k,k'}(x + x^q).$$

Therefore, we have

Proposition 4. *Let $a \in \mathbb{F}_{2^n}^*$. Let $x \in \mathbb{F}_{2^{2n}}$ be a solution of*

$$R_{k,k'}\left(a^{-\frac{q}{2}}\right) = x + x^q. \tag{16}$$

Then, $y = \frac{1}{x+x^2} = \left(1 + \frac{1}{x}\right) + \frac{1}{\left(1+\frac{1}{x}\right)}$ is the unique element of $\mathbb{F}_{2^n}$ such that $a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{y}\right)\right)^{-1}$.

Proof. Let y be the unique element of $\mathbb{F}_{2^n}$ such that $a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{y}\right)\right)^{-1}$. Write $\frac{1}{y} = x + x^2$ with $x \in \mathbb{F}_{2^{2n}}$. Then, $a^{-\frac{q}{2}} = f_{k,q+1}\left(x + x^2\right) = Q'_{k,k'}(x + x^q)$ proving that x is a solution of (16). □

By Proposition 4 and Proposition 3, we can now explicitly write the solutions of Problem 1.

Theorem 5. *Let $a \in \mathbb{F}_{2^n}^*$. Let k be odd with $\gcd(n,k)=1$ and k' be the inverse of k modulo $2n$. Then, the unique solution of (11) in $\mathbb{F}_{2^n}^*$ is*

$$y = \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right) + \left(S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)\right)^2}$$

where ζ denotes any element of $\mathbb{F}_{2^{2n}} \setminus \mathbb{F}_2$ such that $\zeta^{2^n+1}=1$, $S_{n,k}(X) = \sum_{i=0}^{n-1} X^{q^i}$ and $R_{k,k'}$ is defined by (14). Furthermore, we have $y = v + \frac{1}{v}$ for

$$v = 1 + \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)}.$$

3.3 On Problem 2

To begin with, remind that Problem 2 is to find all solutions $u \in \mathbb{F}_{2^n}$ to $D_{q+1}(u) = y$ for given $y \in \mathbb{F}_{2^n}^*$.

By Proposition 1, one can write $u = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star$ or $c \in \mu_{2^n+1}^\star$. Equation (2) applied to u leads then to

$$D_{q+1}(u) = c^{q+1} + \frac{1}{c^{q+1}}. \tag{17}$$

Thus, we can be reduced to solve firstly equation $v + \frac{1}{v} = y$, then equation $c^{q+1} = v$ in $\mathbb{F}_{2^n}^\star \cup \mu_{2^n+1}^\star$, and set $u = c + \frac{1}{c}$. Here, let us point out that $c^{q+1} = v$ is equivalent to $\left(\frac{1}{c}\right)^{q+1} = \frac{1}{v}$ and that c and $\frac{1}{c}$ define the same element $u = c + \frac{1}{c}$ of $\mathbb{F}_{2^n}$.

Proposition 1 says that the equation $v + \frac{1}{v} = y$ has two solutions in $\mathbb{F}_{2^n}^\star$ if $Tr_1^n\left(\frac{1}{y}\right) = 0$ and in $\mu_{2^n+1}^\star$ if $Tr_1^n\left(\frac{1}{y}\right) = 1$ (Proposition 3 gives an explicit expression for these solutions).

Now, let us consider solutions of $c^{q+1} = v$ in $\mathbb{F}_{2^n}^\star \cup \mu_{2^n+1}^\star$. First, note that if $v \in \mathbb{F}_{2^n}^\star$, then necessarily $c \in \mathbb{F}_{2^n}^\star$ (indeed, if $c \in \mu_{2^n+1}^\star$, we get $v^2 = v \cdot v = v^{2^n} \cdot v = v^{2^n+1} = (c^{2^n+1})^{q+1} = 1$ contradicting $v \notin \mathbb{F}_2$).

Recall that if k is odd and $\gcd(n,k)=1$, then

$$\gcd(q+1, 2^n-1) = \begin{cases} 1, & \text{if } n \text{ is odd} \\ 3, & \text{if } n \text{ is even} \end{cases} \tag{18}$$

and

$$\gcd(q+1, 2^n+1) = \begin{cases} 1, & \text{if } n \text{ is even} \\ 3, & \text{if } n \text{ is odd.} \end{cases} \tag{19}$$

Therefore, if $v \in \mathbb{F}_{2^n}^\star$, then there are 0 (if v is a non-cube in $\mathbb{F}_{2^n}^\star$) or 3 (if v is a cube in $\mathbb{F}_{2^n}^\star$) elements c in $\mathbb{F}_{2^n}^\star$ such that $c^{q+1} = v$ when n is even while

there is a unique c (i.e. $v^{(q+1)^{-1} \mod 2^n-1}$) when n is odd. And, if $v \in \mu^{\star}_{2^n+1}$, then there are 0 (if v is a non-cube in $\mu^{\star}_{2^n+1}$) or 3 (if v is a cube in $\mu^{\star}_{2^n+1}$) elements c in $\mu^{\star}_{2^n+1}$ such that $c^{q+1} = v$ when n is odd while there is a unique c (i.e. $v^{(q+1)^{-1} \mod 2^n+1}$) when n is even.

It remains to show in the case when there are three solutions c, they define three different elements $u = c + \frac{1}{c}$ in $\mathbb{F}^{\star}_{2^n}$. Denote w a primitive element of $\mathbb{F}_4$. Then these three solutions of $c^{q+1} = v$ are of form c, cw and cw^2. Now, $cw_1 + \frac{1}{cw_1} = cw_2 + \frac{1}{cw_2}$ implies that $cw_1 = cw_2$ or $cw_1 = \frac{1}{cw_2}$ (because $A + \frac{1}{A} = B + \frac{1}{B}$ is equivalent to $(A + B)(AB + 1) = 0$). The second case is impossible since it implies that $v = c^{q+1} = \left(\frac{1}{w_1^{\frac{1}{2}} w_2^{\frac{1}{2}}}\right)^{q+1} = 1$ because 3 divides $q + 1$ when k is odd.

We can thus state the following answer to Problem 2.

Theorem 6. *Let k be odd and n be even. Let $y \in \mathbb{F}^*_{2^n}$. Let v be any element of $\mathbb{F}_{2^{2n}}$ such that $v + \frac{1}{v} = y$ (this can be given by Proposition 3).*

1. *If v is a non-cube in $\mathbb{F}^{\star}_{2^n}$, then*

$$D^{-1}_{q+1}(y) = \emptyset.$$

2. *If v is a cube in $\mathbb{F}^{\star}_{2^n}$, then*

$$D^{-1}_{q+1}(y) = \left\{ cw + \frac{1}{cw} \mid c^{q+1} = v,\, c \in \mathbb{F}^{\star}_{2^n},\, w \in \mathbb{F}^*_4 \right\}.$$

3. *If v is not in $\mathbb{F}_{2^n}$, then*

$$D^{-1}_{q+1}(y) = \left\{ v^{(q+1)^{-1} \mod 2^n+1} + \frac{1}{v^{(q+1)^{-1} \mod 2^n+1}} \right\}.$$

Remark 1. Item 1 of Theorem 6 recovers [5, Theorem 2.1] which states: when n is even and $\gcd(n, k) = 1$ (so k is odd), P_a has no zeros in $\mathbb{F}_{2^n}$ if and only if $a^{-1} = f_{k,q+1}\left(\frac{1}{v+\frac{1}{v}}\right)^{\frac{2}{q}}$ for some non-cube v of $\mathbb{F}^{\star}_{2^n}$. Indeed, the statement of Theorem 2.1 in [5] is not exactly what we write but it is worth noticing that the quantity that is denoted $A(b)$ in [5] satisfies $A(b)^{-1} = f_{k,q+1}\left(\frac{1}{b^{\frac{1}{4}} + \frac{1}{b^{\frac{1}{4}}}}\right)^{\frac{2}{q}}$.

Theorem 7. *Let k be odd and n be odd. Let $y \in \mathbb{F}^*_{2^n}$. Let v be any element of $\mathbb{F}_{2^{2n}}$ such that $v + \frac{1}{v} = y$ (this can be given by Proposition 3) :*

1. *If v is a non-cube in $\mu^{\star}_{2^n+1}$, then*

$$D^{-1}_{q+1}(y) = \emptyset.$$

2. *If v is a cube in $\mu^{\star}_{2^n+1}$, then*

$$D^{-1}_{q+1}(y) = \left\{ cw + \frac{1}{cw} \mid c^{q+1} = v,\, c \in \mu^{\star}_{2^n+1},\, w \in \mathbb{F}^*_4 \right\}.$$

3. *If v is in $\mathbb{F}_{2^n}$, then*

$$D_{q+1}^{-1}(y)=\left\{v^{(q+1)^{-1} \mod 2^n-1}+\frac{1}{v^{(q+1)^{-1} \mod 2^n-1}}\right\}.$$

3.4 On the roots in $\mathbb{F}_{2^n}$ of $P_a(x)$

We sum up the results of previous subsections to give an explicit expression of the roots in $\mathbb{F}_{2^n}$ of $P_a(x)$.

Let k denote any positive integer coprime with n and $a\in\mathbb{F}_{2^n}^*$.

First, let us consider the case of the odd k. Let k' be the inverse of k modulo $2n$. Define

$$v=1+\frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)},$$

where ζ is any element of $\mathbb{F}_{2^{2n}}\setminus\mathbb{F}_2$ such that $\zeta^{2^n+1}=1$, $S_{n,k}(x)=\sum_{i=0}^{n-1}x^{q^i}$ and $R_{k,k'}$ is defined by (14).

According to Theorem 5, Theorem 6 and Theorem 7, we have following.

Theorem 8. *Let n be even, $\gcd(n,k)=1$ and $a\in\mathbb{F}_{2^n}^*$.*

1. *If v is a non-cube in $\mathbb{F}_{2^n}$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If v is a cube in $\mathbb{F}_{2^n}$, then $P_a(x)$ has three distinct zeros $\frac{\left(cw+\frac{1}{cw}\right)^{q-1}}{yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}}$ in $\mathbb{F}_{2^n}$, where $c^{q+1}=v$, $w\in\mathbb{F}_4^*$ and $y=v+\frac{1}{v}$.*
3. *If v is not in $\mathbb{F}_{2^n}$, then $P_a(x)$ has a unique zero $\frac{\left(c+\frac{1}{c}\right)^{q-1}}{yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}}$ in $\mathbb{F}_{2^n}$, where $c=v^{(q+1)^{-1} \mod 2^n+1}$ and $y=v+\frac{1}{v}$.*

Remark 2. When $k=1$, that is, $P_a(x)=x^3+x+a$, Item (1) of Theorem 8 is exactly Corollary 2.2 of [5] which states that, when n is even, P_a is irreducible over $\mathbb{F}_{2^n}$ if and only if $a=c+\frac{1}{c}$ for some non-cube c of $\mathbb{F}_{2^n}$.

Theorem 9. *Let n and k be odd with $\gcd(n,k)=1$ and $a\in\mathbb{F}_{2^n}^*$.*

1. *If v is a non-cube in $\mu^\star_{2^n+1}$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If v is a cube in $\mu^\star_{2^n+1}$, then $P_a(x)$ has three distinct zeros $\frac{\left(cw+\frac{1}{cw}\right)^{q-1}}{yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}}$ in $\mathbb{F}_{2^n}$, where $c^{q+1}=v$, $w\in\mathbb{F}_4^*$ and $y=v+\frac{1}{v}$.*
3. *If v is in $\mathbb{F}_{2^n}$, then $P_a(x)$ has a unique zero $\frac{\left(c+\frac{1}{c}\right)^{q-1}}{yT_k\left(\frac{1}{y}\right)^{\frac{2}{q}}}$ in $\mathbb{F}_{2^n}$, where $c=v^{(q+1)^{-1} \mod 2^n-1}$ and $y=v+\frac{1}{v}$.*

When k is even, following Item (2) of Theorem 4, we introduce $l=n-k$, $q'=2^l$ and l' the inverse of l modulo $2n$. Define

$$v'=1+\frac{1}{S_{n,l}\left(\frac{R_{l,l'}\left(a^{-\frac{(q')^2}{2}}\right)}{\zeta+1}\right)},$$

where ζ is any element of $\mathbb{F}_{2^{2n}} \setminus \mathbb{F}_2$ such that $\zeta^{2^n+1} = 1$, $S_{n,l}(x) = \sum_{i=0}^{n-1} x^{q'^i}$ and $R_{l,l'}$ is defined by (14).

Theorem 10. *Let n be odd and k be even with $\gcd(n,k) = 1$. Let $a \in \mathbb{F}_{2^n}^*$.*

1. *If v' is a non-cube in $\mu^\star_{2^n+1}$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If v' is a cube in $\mu^\star_{2^n+1}$, then $P_a(x)$ has three distinct zeros $1 + \frac{\left(dw+\frac{1}{dw}\right)^{q'-1}}{y' T_l\left(\frac{1}{y'}\right)^{\frac{2}{q'}}}$ in $\mathbb{F}_{2^n}$, where $d^{q'+1} = v'$, $w \in \mathbb{F}_4^*$ and $y' = v' + \frac{1}{v'}$.*
3. *If v' is in $\mathbb{F}_{2^n}$, then $P_a(x)$ has a unique zero $1 + \frac{\left(c+\frac{1}{c}\right)^{q'-1}}{y' T_l\left(\frac{1}{y'}\right)^{\frac{2}{q'}}}$ in $\mathbb{F}_{2^n}$, where $c = v'^{(q'+1)^{-1} \bmod 2^n-1}$ and $y' = v' + \frac{1}{v'}$.*

Remark 3. When n is even, Theorem 8 shows that P_a has a unique solution if and only if v is not in $\mathbb{F}_{2^n}$. According to Proposition 4, this is equivalent to $Tr_1^n(R_{k,k'}(a^{-\frac{q}{2}})) = 1$, that is, $Tr_1^n(R_{k,k'}(a^{-1})) = 1$. When n is odd and k is odd (resp. even), Theorem 9 and Theorem 10 show that P_a has a unique zero in $\mathbb{F}_{2^n}$ if and only if v (resp. v') is in $\mathbb{F}_{2^n}$. According to Proposition 4, this is equivalent to $Tr_1^n(R_{k,k'}(a^{-1})) = 0$ or $Tr_1^n(R_{l,l'}(a^{-1})) = 0$ for odd k or even k, respectively. By the way, for $x \in \mathbb{F}_{2^n}$, $Q'_{l,l'}\left(x + x^{q'}\right) = \frac{(x+x^{q'})^{q'+1}}{x^{q'}+x^{2q'}} = \left(\frac{(x+x^q)^{q+1}}{x^q+x^{2q}}\right)^{2^{(n-k)^2}} = Q'_{k,k'}\left(x+x^q\right)^{2^{(n-k)^2}}$. Hence if $v' \in \mathbb{F}_{2^n}$, then $R_{l,l'}(a^{-1}) = R_{k,k'}(a^{-1})^{\frac{1}{2^{(n-k)^2}}}$, and so $Tr_1^n(R_{l,l'}(a^{-1})) = 0$ is equivalent to $Tr_1^n(R_{k,k'}(a^{-1})) = 0$. After all, we can recover [13, Theorem 1] which states that P_a has a unique zero in $\mathbb{F}_{2^n}$ if and only if $Tr_1^n(R_{k,k'}(a^{-1}) + 1) = 1$.

4 Conclusion

In [2, 3, 5, 13, 14], partial results about the zeros of $P_a(x) = x^{2^k+1} + x + a$ in $\mathbb{F}_{2^n}$ have been obtained. In this paper, we provided explicit expressions for all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$ in terms of a and thus finish the study initiated in these papers when $\gcd(n,k) = 1$. We showed that the problem of finding zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$, in fact, can be divided into two problems with odd k: to find the unique preimage of an element in $\mathbb{F}_{2^n}$ under a M*ü*ller-Cohen-Matthews (MCM) polynomial and to find the preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial. We completely solved these two independent problems. We also presented an explicit formula for solutions to the affine equation $x^{2^k} + x = b, b \in \mathbb{F}_{2^n}$.

Acknowledgement. The authors thank the Assoc. Edit. for the valuable comments on the manuscript. They are also very grateful to the anonymous reviewer for his/her precious comments which have highly improved the manuscript.

References

1. S.S. Abhyankar, S.D.Cohen, M.E. Zieve. Bivariate factorizations connecting Dickson polynomials and Galois theory, Transactions of the American Mathematical Society, 352(6):2871 – 2887, 2000.
2. A.W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3):285 – 305, 2004.
3. A.W. Bluher. A New Identity of Dickson polynomials. eprint arXiv:1610.05853v1, October 2016.
4. C. Bracken, T. Helleseth. Triple-error-correcting bch-like codes. In *IEEE International Symposium on Information Theory, ISIT 2009, June 28 - July 3, 2009, Seoul, Korea, Proceedings*, pages 1723–1725, 2009.
5. C. Bracken, C.H. Tan, Y. Tan. On a class of quadratic polynomials with no zeros and its application to APN functions. *Finite Fields and Their Applications*, 25:26 – 36, 2014.
6. L. Budaghyan, C. Carlet. Classes of quadratic APN trinomials and hexanomials and related structures, In *IEEE Trans. Inform. Theory* 54 (5), 2354–2357, 2008.
7. S.D. Cohen, R.W. Matthews. A class of exceptional polynomials. *Transactions of the American Mathematical Society*, 345:897 – 909, 1994.
8. S.D. Cohen, R.W. Matthews. Exceptional polynomials over finite fields. *Finite Fields and Their Applications*, 1:261 – 277, 1995.
9. J.F. Dillon, H, Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342 – 389, 2004.
10. J.F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography*, 17:225 – 235, 1999.
11. H. Dobbertin, P. Felke, T. Helleseth, P. Rosendhal. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Transactions on Information Theory*, 52(2): 613 – 627, 2006.
12. T. Helleseth, A. Kholosha, G.J. Ness. Characterization of m-sequences of lengths $2^{2^{2k}-1}$ and $2^k - 1$ with three-valued crosscorrelation. *IEEE Transactions on Information Theory*, 53(6): 2236 – 2245, 2007.
13. T. Helleseth, A. Kholosha. On the equation $x^{2^l+1} + x + a = 0$ over $GF(2k)$. *Finite Fields and Their Applications*, 14(1):159 – 176, 2008.
14. T. Helleseth, A. Kholosha. $x^{2^l+1}+x+a$ and related affine polynomials over $GF(2k)$. *Cryptography and Communications*, 2(1):85 – 109, 2010.
15. C. Tang. Infinite families of 3-designs from APN functions. arXiv preprint arXiv:1904.04071, 2019.