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

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

[1] Institute of Mathematics, State Academy of Sciences and PGItech Corp., Pyongyang, Democratic People's Republic of Korea
khk.cryptech@gmail.com

[2] LAGA, Department of Mathematics, Universities of Paris VIII and Paris XIII, CNRS, UMR 7539 and Telecom ParisTech, France
smesnager@univ-paris8.fr

March 16, 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 [11] have got criteria for $N_a = 1$ and an explicit expression of the unique solution when $\gcd(k, n) = 1$. In 2014, Bracken, Tan and Tan [5] presented a 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 condition $\gcd(n, k) = 1$. We explicitly calculate all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$. New criterion for which a, N_a is equal to 0, 1 or 3 is a by-product of our result.

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

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

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

has been studied in [2, 11, 12]. This polynomial has arisen in several different contexts including the inverse Galois problem [1], the construction of difference sets with Singer parameters [7], to find cross-correlation between m-sequences [9, 11] and to construct error correcting codes [4]. 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 $P_a(x)$ have 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, three or $2^{\gcd(k,n)} + 1$ zeros in $\mathbb{F}_{2^n}$.*

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 $\mathbb{F}_{2^n}$.

In 2008, Helleseth and Kholosha [11] have provided criteria for which a $P_a(x)$ has exactly one zero in $\mathbb{F}_{2^n}$ and an explicit expression of the unique zero when $\gcd(k, n) = 1$.

In 2014, Bracken, Tan and Tan [5] presented a criterion for which a $P_a(x)$ 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 criterion for which a, $P_a(x)$ has none, one or three zeros is a by-product 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 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. Other is to find an explicit solution formula for 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 expression of all possible zeros of P_a in $\mathbb{F}_{2^n}$ by 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.

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 polynomial 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 another classical polynomials defined as follows [6],

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

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 a 2-to-1 on $\mathbb{F}_{2^n}$.*

Proof. For odd k, see [6]. When k is even, $f_{k,2^k+1}$ is not a permutation of $\mathbb{F}_{2^n}$. Indeed, Theorem 10 of [7] 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 $\gcd(k,n)=1$. □

We will exploit a recent polynomial identity involving Dickson polynomials established 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 lead us to solving $P_a(x)=0$.

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 is to exploit Theorem 3 to the study of zeros in $\mathbb{F}_{2^n}$ of P_a. To this end, we observe firstly that

$$\begin{aligned}X^{q^2-1} &+ \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1} \\ &= X^{q^2-1} + Y^q T_k\left(\frac{1}{Y}\right)^2 X^{q-1} + Y^{q-1}.\end{aligned}$$

Substituting tx to X in the above identity with $t^{q^2-q} = Y^q T_k\left(\frac{1}{Y}\right)^2$, we get

$$\begin{aligned}X^{q^2-1} &+ \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1} \\ &= Y^q T_k\left(\frac{1}{Y}\right)^2 t^{q-1}\left(x^{q^2-1} + x^{q-1} + \frac{1}{YT_k\left(\frac{1}{Y}\right)^2 t^{q-1}}\right).\end{aligned}$$

Now, $t^{q^2-q} = Y^q T_k\left(\frac{1}{Y}\right)^2$ is equivalent to $t^{q-1} = YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}$. Therefore

$$YT_k\left(\frac{1}{Y}\right)^2 t^{q-1} = Y^2 T_k\left(\frac{1}{Y}\right)^{\frac{2(q+1)}{q}} = \left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}.$$

By all these calculations, we get

$$\begin{aligned}x^{q^2-1} &+ x^{q-1} + \frac{1}{\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}} \\ &= \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}}\left(X^{q^2-1} + \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1}\right).\end{aligned} \tag{3}$$

If k is odd, $f_{k,q+1}$ is a permutation polynomial of $\mathbb{F}_{2^n}$ by Theorem 2. Therefore, for any $a \in \mathbb{F}_{2^n}^*$, there exists a unique Y in $\mathbb{F}_{2^n}^*$ such that $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Hence, by Theorem 3 and equation (3), we have

$$P_a\left(x^{q-1}\right) = x^{q^2-1} + x^{q-1} + a = \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}} \prod_{w\in\mathbb{F}_q^*} \left(D_{q+1}(wtx) - Y\right) \tag{4}$$

where Y is the unique element of $\mathbb{F}_{2^n}^*$ such that $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$ and $t^{q-1} = YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}$. Now, since $\gcd(q-1, 2^n-1) = 1$, the zeros of $P_a(x)$ are the images of the zeros of $P_a(x^{q-1})$ by the map $x \mapsto x^{q-1}$. Therefore, when k is odd, equation (4) states that finding the zeros of $P_a(x^{q-1})$ amounts to determine 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 $x \in \mathbb{F}_{2^n}$,

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

and so

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x)=0\} = \left\{x+1 \mid x^{2^{n-k}+1}+x+a^{2^{n-k}}=0,\, x \in \mathbb{F}_{2^n}\right\}. \qquad (5)$$

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 discussions 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,*

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

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,*

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

Proof. Suppose that k is odd. Equation (4) shows that the zeros of P_a in $\mathbb{F}_{2^n}$ are x^{q-1} for the elements $x \in \mathbb{F}_{2^n}^\star$ such that $D_{q+1}(wtx)=Y$ where $t^{q-1} = YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}$. Set $z=wtx$. Then, since $w \in \mathbb{F}_q^*$, $x^{q-1} = \left(\frac{z}{wt}\right)^{q-1} = \frac{z^{q-1}}{t^{q-1}} = \frac{z^{q-1}}{YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Item 2 follows from Item 1 and equality (5). □

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

$$a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}. \tag{6}$$

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

$$D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^\star \mid D_{q+1}(z) = Y\}. \tag{7}$$

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

Define

$$Q'_{k,k'}(x) = \frac{x^{q+1}}{\sum_{i=1}^{k'} x^{q^i}} \tag{8}$$

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 permutation on $\mathbb{F}_{2^{2n}}$ (see [7] or [8] where $Q_{k,k'} = 1/Q'_{k,k'}$ is instead considered). Indeed, due to [7], 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

$$R_{k,k'}(x) = \sum_{i=1}^{k'} A_i(x) + B_{k'}(x). \tag{9}$$

Directively from the definitions, it follow

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

and

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

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

$$f_{k,q+1}(x + x^2) = Q'_{k,k'}(x + x^q) \tag{10}$$

for any $x \in \mathbb{F}_{2^{2n}}$. Let x be an element of $\mathbb{F}_{2^{2n}}$ such that

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

By using (10) we can rewrite (6) as

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

Therefore, we have

Proposition 3. *Let $a \in \mathbb{F}_{2^n}^*$. Let $x \in \mathbb{F}_{2^{2n}}$ be a solution of*

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

Then, $Y = \frac{1}{x+x^2} = \left(1 + \frac{1}{x}\right) + \frac{1}{\left(1+\frac{1}{x}\right)}$ *is the unique solution in $\mathbb{F}_{2^n}$ of* $a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{-1}$.

Proposition 3 shows that solving Problem 1 amounts to find a solution of an affine equation $x + x^q = b$, which is done in the following.

Proposition 4. *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 $\mu^\star_{2^n+1}$.*

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 $x + x^q = b$. □

By Proposition 3 and Proposition 4, we can now explicit 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 (6) 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 $\mathbb{F}_{2^{2n}}^\star$ 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 (9). Furthermore, we have $Y = T + \frac{1}{T}$ for

$$T = 1 + \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)}.$$

3.3 On Problem 2

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

$$D_{q+1}(z) = c^{q+1} + \frac{1}{c^{q+1}}. \tag{11}$$

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

Proposition 1 says that the equation $T + \frac{1}{T} = Y$ 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 $Tr_1^n\left(\frac{1}{Y}\right) = 1$. In fact, Proposition 4 gives an explicit solution expression, that is,

$$T = Y S_{n,1}\left(\frac{1}{Y^2(\zeta+1)}\right) \text{ and } T = Y S_{n,1}\left(\frac{1}{Y^2(\zeta+1)}\right) + Y, \tag{12}$$

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

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

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

$$\gcd(q+1, 2^n-1) = \begin{cases} 1, & \text{if } n \text{ is odd} \\ 3, & \text{if } n \text{ is even} \end{cases} \tag{13}$$

and

$$\gcd(q+1, 2^n+1) = \begin{cases} 1, & \text{if } n \text{ is even} \\ 3, & \text{if } n \text{ is odd.} \end{cases} \tag{14}$$

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

It remains to show in the case when there are three solutions c, they define three different elements $z \in \mathbb{F}_{2^n}^\star$. Denote w a primitive element of $\mathbb{F}_4$. Then these three solutions of $c^{q+1} = T$ 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 because it implies that $T = c^{q+1} = \left(\frac{1}{w_1^{\frac{1}{2}} w_2^{\frac{1}{2}}}\right)^{q+1} = 1$ 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 T be any element of $\mathbb{F}_{2^{2n}}$ such that $T + \frac{1}{T} = Y$ (this can be given by* (12)*).*

1. *If T is a non-cube in $\mathbb{F}_{2^n}^\star$, then*
$$D_{q+1}^{-1}(Y) = \emptyset.$$
2. *If T is a cube in $\mathbb{F}_{2^n}^\star$, then*
$$D_{q+1}^{-1}(Y) = \left\{ cw + \frac{1}{cw} \mid c^{q+1} = T,\ c \in \mathbb{F}_{2^n}^\star,\ w \in \mathbb{F}_4^* \right\}.$$
3. *If T is not in $\mathbb{F}_{2^n}$, then*
$$D_{q+1}^{-1}(Y) = \left\{ T^{(q+1)^{-1} \mod 2^n+1} + \frac{1}{T^{(q+1)^{-1} \mod 2^n+1}} \right\}.$$

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 $a^{-1} = f_{k,q+1}\left(\frac{1}{T+\frac{1}{T}}\right)^{\frac{2}{q}}$ for some non-cube T of $\mathbb{F}_{2^n}^\star$. 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 T be any element of $\mathbb{F}_{2^{2n}}$ such that $T + \frac{1}{T} = Y$ (this can be given by* (12)*).*

1. *If T is a non-cube in $\mu_{2^n+1}^\star$, then*
$$D_{q+1}^{-1}(Y) = \emptyset.$$

2. *If T is a cube in $\mu^\star_{2^n+1}$, then*

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

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

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

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 odd k. Let k' be the inverse of k modulo $2n$. Define

$$T = 1 + \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)},$$

where ζ is any element of $\mathbb{F}^\star_{2^{2n}}$ 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 (9).

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

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

1. *If T is a non-cube in $\mathbb{F}_{2^n}$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If T 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 $c^{q+1} = T$, $w \in \mathbb{F}_4^*$ and $Y = T + \frac{1}{T}$.*
3. *If T 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 $c = T^{(q+1)^{-1} \mod 2^n+1}$ and $Y = T + \frac{1}{T}$.*

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 odds with $\gcd(n,k) = 1$ and $a \in \mathbb{F}^*_{2^n}$.*

1. *If T is a non-cube in $\mu^\star_{2^n+1}$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If T 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 $c^{q+1} = T$, $w \in \mathbb{F}_4^*$ and $Y = T + \frac{1}{T}$.*
3. *If T 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 $c = T^{(q+1)^{-1} \mod 2^n-1}$ and $Y = T + \frac{1}{T}$.*

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

$$T' = 1 + \frac{1}{S_{n,l}\left(\frac{R_{l,l'}\left(a^{-\frac{(q')^2}{2}}\right)}{\zeta+1}\right)},$$

where ζ is any element of $\mathbb{F}_{2^{2n}}^\star$ 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 (9).

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

1. *If T' is a non-cube $\mu_{2^n+1}^\star$, then $P_a(x)$ has no zeros in $\mathbb{F}_{2^n}$.*
2. *If T' is a cube in $\mu_{2^n+1}^\star$, 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 $d^{q'+1}=T'$, $w\in\mathbb{F}_4^*$ and $Y'=T'+\frac{1}{T'}$.*
3. *If T' 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 $c=T'^{(q'+1)^{-1} \bmod 2^n-1}$ and $Y'=T'+\frac{1}{T'}$.*

Remark 3. When n is even, Theorem 8 shows that P_a has a unique solution if and only if T is not in $\mathbb{F}_{2^n}$. According to Proposition 3, 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 T (resp. T') is in $\mathbb{F}_{2^n}$. According to Proposition 3, 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 $T'\in\mathbb{F}_{2^n}$, 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 [11, 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, 11, 12], 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 expression of all possible roots 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 Müller-Cohen-Matthews (MCM) polynomial and to find 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 solution formula for the affine equation $x^{2^k}+x=b, b\in\mathbb{F}_{2^n}$.

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. S.D. Cohen, R.W. Matthews. A class of exceptional polynomials. *Transactions of the American Mathematical Society*, 345:897 – 909, 1994.
7. J.F. Dillon, H, Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342 – 389, 2004.
8. J.F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography*, 17:225 – 235, 1999.
9. 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.
10. 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.
11. 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.
12. 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.