Complete solution over $\mathbb{F}_{p^n}$ of the equation

$$X^{p^k+1} + X + a = 0$$

Kwang Ho Kim$^{1,2}$, Jong Hyok Choe$^3$, and Sihem Mesnager$^3$

$^1$ Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People’s Republic of Korea
khk.cryptech@gmail.com
$^2$ PGItech Corp., Pyongyang, Democratic People’s Republic of Korea
$^3$ Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, University Sorbonne Paris Cité, LAGA, UMR 7539, CNRS, 93430 Villetaneuse and Télécom Paris, 91120 Palaiseau, France.
smesnager@univ-paris8.fr

Abstract. The problem of solving explicitly the equation $P_a(X) := X^{q+1} + X + a = 0$ over the finite field $\mathbb{F}_Q$, where $Q = p^n$, $q = p^k$ and $p$ is a prime, arises in many different contexts including finite geometry, the inverse Galois problem [1], the construction of difference sets with Singer parameters [9], determining cross-correlation between $m$-sequences [12] and to construct error correcting codes [4], cryptographic APN functions [5, 6], designs [26], as well as to speed up the index calculus method for computing discrete logarithms on finite fields [13, 14] and on algebraic curves [23].

Subsequently, in [2, 15, 16, 5, 3, 20, 8, 24, 19], the $\mathbb{F}_Q$-zeros of $P_a(X)$ have been studied. In [2], it was shown that the possible values of the number of the zeros that $P_a(X)$ has in $\mathbb{F}_Q$ is 0, 1, 2 or $p \gcd(n,k) + 1$. Some criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(x)$ were found in [15, 16, 5, 20, 24]. However, while the ultimate goal is to explicit all the $\mathbb{F}_Q$-zeros, even in the case $p = 2$, it was solved only under the condition gcd$(n,k) = 1$ [20].

In this article, we discuss this equation without any restriction on $p$ and gcd$(n,k)$. In [19], for the cases of one or two $\mathbb{F}_Q$-zeros, explicit expressions for these rational zeros in terms of $a$ were provided, but for the case of $p \gcd(n,k) + 1 \mathbb{F}_Q$-zeros it was remained open to explicitly compute the zeros. This paper solves the remained problem, thus now the equation $X^{p^k+1} + X + a = 0$ over $\mathbb{F}_{p^n}$ is completely solved for any prime $p$, any integers $n$ and $k$.

Keywords: Equation · Finite field · Zeros of a polynomial.

Mathematics Subject Classification. 12E05, 12E12, 12E10.
1 Introduction

Let $n$ and $k$ be any positive integers with $\gcd(n, k) = d$. Let $Q = p^n$ and $q = p^k$ where $p$ is a prime. We consider the polynomial

$$P_a(X) := X^{q+1} + X + a, \ a \in \mathbb{F}_Q^*.$$  

Notice the more general polynomial forms $X^{q+1} + rX^q + sX + t$ with $s \neq r^q$ and $t \neq rs$ can be transformed into this form by the substitution $X = (s-r^q)^{\frac{1}{q}}X_1 - r$.

It is clear that $P_a(X)$ have no multiple roots.

These polynomials have arisen in several different contexts including finite geometry, the inverse Galois problem [1], the construction of difference sets with Singer parameters [9], determining cross-correlation between $m$-sequences [12] and to construct error correcting codes [4], APN functions [5, 6], designs [26].

These polynomials are also exploited to speed up (the relation generation phase in) the index calculus method for computation of discrete logarithms on finite fields [13, 14] and on algebraic curves [23].

Let $N_a$ denote the number of zeros in $\mathbb{F}_Q$ of polynomial $P_a(X)$ and $M_i$ denote the number of $a \in \mathbb{F}_Q^*$ such that $P_a(X)$ has exactly $i$ zeros in $\mathbb{F}_Q$.

In 2004, Bluher [2] proved that $N_a$ takes either of 0, 1, 2 and $p\gcd(k,n) + 1$ where $d = \gcd(k, n)$ and computed $M_i$ for every $i$. She also stated some criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(X)$.

The ultimate goal in this direction of research is to identify all the $\mathbb{F}_Q$-zeros of $P_a(X)$. Subsequently, there were much efforts for this goal, specifically for a particular instance of the problem over binary fields i.e. $p = 2$. In 2008 and 2010, Helleseth and Kholosha [15, 16] found new criteria for the number of $\mathbb{F}_{2^n}$-zeros of $P_a(X)$. In the cases when there is a unique zero or exactly two zeros and $d$ is odd, they provided explicit expressions of these zeros as polynomials of $a$ [16]. In 2014, Bracken, Tan, and Tan [5] presented a criterion for $N_a = 0$ in $\mathbb{F}_{2^n}$ when $d = 1$ and $n$ is even. In 2019, Kim and Mesnager [20] completely solved this equation $X^{2^k+1} + X + a = 0$ over $\mathbb{F}_{2^n}$ when $d = 1$. They 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 an Müller-Cohen-Matthews polynomial and to find preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial. By completely solving these two independent problems, they explicitly calculated all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(X)$, with new criteria for which $N_a$ is equal to 0, 1 or $p^d + 1$ as a by-product.

Very recently, new criteria for which $P_a(X)$ has 0, 1, 2 or $p^d + 1$ roots were stated by [19, 24] for any characteristic. In [19], for the cases of one or two $\mathbb{F}_Q$-zeros, explicit expressions for these rational zeros in terms of $a$ are provided. For the case of $p^\gcd(n,k) + 1$ rational zeros, [19] provides a parametrization of such $a$’s and expresses the $p^\gcd(n,k) + 1$ rational zeros by using that parametrization, but it was remained open to explicitly represent the zeros.

Following [19], this paper discuss the equation $X^{p^k+1} + X + a = 0, a \in \mathbb{F}_p^n$, without any restriction on $p$ and $\gcd(n, k)$. After introducing some prerequisites from [19] (Sec. 2), we solve the open problem remained in [19] to explicitly
represent the $F_Q$-zeros for the case of $p^{\gcd(n,k)} + 1$ rational zeros (Sec. 3). After all, it is concluded that the equation $X^{p^{k+1}} + X + a = 0$ over $\mathbb{F}_p$ is completely solved for any prime $p$, any integers $n$ and $k$.

2 Prerequisites

Throughout this paper, we maintain the following notations.
- $p$ is any prime.
- $n$ and $k$ are any positive integers.
- $d = \gcd(n,k)$.
- $m := n/d$.
- $q = p^k$.
- $Q = p^n$.
- $a$ is any element of the finite field $\mathbb{F}_Q^*$.

Given positive integers $L$ and $l$, define a polynomial
\[ T_{Ll}^T(X) := X + X^{p^L} + \cdots + X^{p^{L(l-2)}} + X^{p^{L(l-1)}}. \]

Usually we will abbreviate $T_{l1}^T(\cdot)$ as $T_l(\cdot)$. For $x \in \mathbb{F}_{p^l}$, $T_l(x)$ is the absolute trace $Tr_{l1}^T(x)$ of $x$.

In [19], the sequence of polynomials \{A_r(X)\} in $\mathbb{F}_p[X]$ is defined as follows:
\[
A_1(X) = 1, A_2(X) = -1,
A_{r+2}(X) = -A_{r+1}(X)^q - X^q A_r(X)^q \quad \text{for } r \geq 1.
\tag{1}
\]

The following lemma gives another identity which can be used as an alternative definition of \{A_r(X)\} and an interesting property of this polynomial sequence which will be importantly applied afterwards.

**Lemma 1 ([19]).** For any $r \geq 1$, the following are true.

1. \[ A_{r+2}(X) = -A_{r+1}(X) - X^q A_r(X). \tag{2} \]
2. \[ A_{r+1}(X)^q + 1 - A_r(X)^q A_{r+2}(X) = X^{q(r-1)q^{-1}}. \tag{3} \]

The zero set of $A_r(X)$ can be completely determined for all $r$:

**Proposition 2 ([19]).** For any $r \geq 3$,
\[
\{ x \in \overline{\mathbb{F}_p} \mid A_r(x) = 0 \} = \left\{ \frac{(u - u^q)^{q^2+1}}{(u - u^{q^2})^{q^2+1}}, \quad u \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2} \right\}.
\]
Further, define polynomials

\[ F(X) := A_m(X), \]
\[ G(X) := -A_{m+1}(X) - XA_{m-1}^q(X). \]

It can be shown that if \( F(a) \neq 0 \) then the \( \mathbb{F}_q \)-zeros of \( P_a(X) \) satisfy a quadratic equation and therefore necessarily \( N_a \leq 2. \)

**Lemma 3 ([19]).** Let \( a \in \mathbb{F}_q^* \). If \( P_a(x) = 0 \) for \( x \in \mathbb{F}_q \), then

\[ F(a)x^2 + G(a)x + aF^q(a) = 0. \]  \( (4) \)

By exploiting these definitions and facts, the following results have been got.

### 2.1 \( N_a \leq 2: \text{Odd } p \)

**Theorem 4 ([19]).** Let \( p \) be odd. Let \( a \in \mathbb{F}_q^* \) and \( E = G(a)^2 - 4aF(a)^{q+1} \).

1. \( N_a = 0 \) if and only if \( E \) is not a quadratic residue in \( \mathbb{F}_p \) (i.e. \( E^{d-1} \neq 0, 1 \)).
2. \( N_a = 1 \) if and only if \( F(a) \neq 0 \) and \( E = 0 \). In this case, the unique zero in \( \mathbb{F}_q \) of \( P_a(X) \) is \( -\frac{G(a)}{2F(a)}. \)
3. \( N_a = 2 \) if and only if \( E \) is a non-zero quadratic residue in \( \mathbb{F}_p \) (i.e. \( E^{d-1} = 1 \)). In this case, the two zeros in \( \mathbb{F}_q \) of \( P_a(X) \) are \( x_{1,2} = \pm \frac{E^{d/2} - G(a)}{2F(a)}, \) where \( E^{d/2} \) represents a quadratic root in \( \mathbb{F}_p \) of \( E. \)

### 2.2 \( N_a \leq 2: \text{p = 2} \)

When \( p = 2, \) in [19] it is proved that \( G(x) \in \mathbb{F}_q \) for any \( x \in \mathbb{F}_q^m \) and using it

**Theorem 5 ([19]).** Let \( p = 2 \) and \( a \in \mathbb{F}_q \). Let \( H = \text{Tr}_1^d \left( \frac{N_{r(a)}(a)}{G(a)} \right) \) and \( E = \frac{aF(a)^{q+1}}{G(a)}. \)

1. \( N_a = 0 \) if and only if \( G(a) \neq 0 \) and \( H \neq 0 \).
2. \( N_a = 1 \) if and only if \( F(a) \neq 0 \) and \( G(a) = 0 \). In this case, \( (aF(a)^{q-1})^{d/2} \) is the unique zero in \( \mathbb{F}_q \) of \( P_a(X). \)
3. \( N_a = 2 \) if and only if \( G(a) \neq 0 \) and \( H = 0 \). In this case the two zeros in \( \mathbb{F}_q \) are \( x_1 = \frac{G(a)}{F(a)} \cdot T_n \left( \frac{E}{\zeta^{q+1}} \right) \) and \( x_2 = x_1 \pm \frac{G(a)}{F(a)}, \) where \( \zeta \in \mu_{q+1} \setminus \{1\}. \)

### 2.3 \( N_a = p^d + 1: \text{Auxiliary results} \)

**Lemma 6 ([19]).** Let \( a \in \mathbb{F}_q^*. \) The following are equivalent.

1. \( N_a = p^d + 1 \) i.e. \( P_a(X) \) has exactly \( p^d + 1 \) zeros in \( \mathbb{F}_q. \)
2. \( F(a) = 0 \), or equivalently by Proposition 2, there exists \( u \in \mathbb{F}_{q^m} \setminus \mathbb{F}_{q^2} \) such that \( a = \frac{(u-u^q)^{q^2+1}}{(u-u^q)^{q+1}} \).

3. There exists \( u \in \mathbb{F}_Q \setminus \mathbb{F}_{p^d} \) such that \( a = \frac{(u-u^q)^{q^2+1}}{(u-u^q)^{q+1}} \). Then the \( p^d + 1 \) zeros in \( \mathbb{F}_Q \) of \( P_a(X) \) are \( x_0 = \frac{-1}{1+(u-u^q)^{q+1}} \) and \( x_\alpha = \frac{-(u+\alpha)^{q^{q+1}}}{1+(u-u^q)^{q+1}} \) for \( \alpha \in \mathbb{F}_{p^d} \).

Lemma 7 ([19]). If \( A_m(a) = 0 \), then for any \( x \in \mathbb{F}_Q \) such that \( x^{q+1} + x + a = 0 \), it holds
\[
A_{m+1}(a) = N_{\mathbb{F}_{p^d}}(x) \in \mathbb{F}_{p^d}.
\]
Furthermore, for any \( t \geq 0 \)
\[
A_{m+t}(a) = A_{m+1}(a) \cdot A_t(a). \tag{5}
\]
In [19], it is remained as an open problem to explicitly compute the \( p^d + 1 \) rational zeros.

3 Completing the case \( N_a = p^d + 1 \)

Thanks to Lemma 6, throughout this section we assume \( F(a) = 0 \) i.e.
\[
A_m(a) = 0.
\]
Let
\[
L_a(X) := X^{q^2} + X^q + aX \in \mathbb{F}_Q[X].
\]
Define the sequence of polynomials \( \{B_r(X)\} \) as follows:
\[
B_1(X) = 0, B_{r+1}(X) = -a \cdot A_r(X)^q. \tag{6}
\]
From Lemma 7 and the definition (1) it follows
\[
B_m(a) = -a A_{m-1}(a)^q = A_{m+1}(a)^{\frac{1}{2}} \in \mathbb{F}_{p^d}. \tag{7}
\]
Using (5) and an induction on \( l \) it is easy to check:

**Proposition 8.**
\[
B_{l \cdot m}(a) = B_m(a)^l. \tag{8}
\]
for any integer \( l \geq 1 \).

The first step to solve the open problem is to induce

**Lemma 9.** For any integer \( r \geq 2 \), in the ring \( \mathbb{F}_Q[X] \) it holds
\[
X^{q^r} = \sum_{i=1}^{r-1} A_{r-i}(a)^{q^i} \cdot L_a(X)^{q^{i-1}} + A_r(a) \cdot X^q + B_r(a) \cdot X. \tag{9}
\]

5
Proof. The equality (9) for \( r = 2 \) is 
\[ X^q = L_a(X) - X^q - aX \]
which is valid by the definition of \( L_a(X) \). Suppose the equality (9) holds for \( r \geq 2 \). By raising \( q \)-th power to both sides of the equality (9), we get

\[
X^{q+1} = \sum_{i=1}^{r-1} A_{r-i}(a)^q \cdot L_a(X)^{q+i+1} + A_r(a)^q \cdot X^{q+1} + B_r(a)^q \cdot X^q
\]

This shows that the equality (9) holds also for \( r + 1 \) and so for all \( r \geq 2 \). \( \square \)

For \( r = m \), under the assumption \( A_m(a) = 0 \), Lemma 9 gives

\[
X^m = \sum_{i=1}^{m-1} A_{m-i}(a)^q \cdot L_a(X)^{q+i-1} + B_m(a) \cdot X.
\]

Now, we define

\[
F_1(X) := X^m - B_m(a) \cdot X = \sum_{i=1}^{m-1} A_{m-i}(a)^q \cdot L_a(X)^{q+i-1} \in \mathbb{F}_p[x]
\]  

(10)

and

\[
G_1(X) = \sum_{i=1}^{m-1} A_{m-i}(a)^q \cdot X^{q+i-1}.
\]

(11)

Then, evidently,

\[
F_1(X) = G_1 \circ L_a(X).
\]

(12)

Furthermore, we can show

**Proposition 10.**

\[
F_1(X) = L_a \circ G_1(X).
\]

Proof. When \( m = 3 \), \( A_3(a) = 0 \) is equivalent to \( a = 1 \). Therefore, one has

\[
F_1(X) = X^q - X = (X^q - X)^q + (X^q - X)^q + (X^q - X) = L_a \circ G_1(X).
\]
Now, suppose \( m \geq 4 \). Then, by using Definition (6)
\[
L_a \circ G_1(X) = \sum_{i=1}^{m-1} A_{m-i}(a)q^{i+2} \cdot X^{q^{i+1}} + \sum_{i=1}^{m-1} A_{m-i}(a)q^{i+1} \cdot X^{q^i} + \sum_{i=1}^{m-1} aA_{m-i}(a)q^i \cdot X^{q^{i-1}}
\]
\[
= \sum_{i=2}^{m} A_{m-i}(a)q^{i+1} \cdot X^{q^i} + \sum_{i=1}^{m-1} A_{m-i}(a)q^{i+1} \cdot X^{q^i} + \sum_{i=0}^{m-2} aA_{m-i-1}(a)q^{i+1} \cdot X^{q^i}
\]
\[
= X^{q^m} - B_m(a) \cdot X = F_1(X),
\]
where Equality (2) was exploited to deduce the last second equality. \( \square \)

By (5), from \( A_m(a) = 0 \) it follows \( A_{l \cdot m}(a) = 0 \) for any \( l \geq 1 \). Therefore, (8) and (9) for \( r = l \cdot m \) yield that for any \( l \geq 1 \)
\[
X^{q^{l \cdot m}} - B_m(a)^l \cdot X = \sum_{i=1}^{l-1} A_{l \cdot m-i}(a)q^{i} \cdot X^{q^{l \cdot m-i}}. \tag{13}
\]

**Proposition 11.** Relation (13) can be rewritten by using \( F_1(X) \) as follows:
\[
X^{q^{l \cdot m}} - B_m(a)^l \cdot X = \sum_{i=0}^{l-1} B_m(a)^{l-1-i} \cdot F_1(X)^{q^{m-i}}. \tag{14}
\]

**Proof.** If \( l = 1 \), the equality is equivalent to the definition of \( F_1(X) \). Suppose that it holds for \( l \geq 2 \). By raising \( q^{m} \)-th power to both sides of (14), we have
\[
X^{q^{(l+1) \cdot m}} - B_m(a)^l \cdot X^{q^{m}} = \sum_{i=0}^{l-1} B_m(a)^{l-1-i} \cdot F_1(X)^{q^{m \cdot (l+1)}}
\]
\[
= \sum_{i=1}^{(l+1)-1} B_m(a)^{(l+1)-1-i} \cdot F_1(X)^{q^{m-i}}.
\]

Since
\[
X^{q^{(l+1) \cdot m}} - B_m(a)^l \cdot X^{q^{m}} = X^{q^{(l+1) \cdot m}} - B_m(a)^l \cdot X^{q^{m}} - B_m(a)^l \cdot F_1(X),
\]
one has
\[
X^{q^{(l+1) \cdot m}} - B_m(a)^{l+1} \cdot X = \sum_{i=1}^{(l+1)-1} B_m(a)^{(l+1)-1-i} \cdot F_1(X)^{q^{m-i}} + B_m(a)^l \cdot F_1(X)
\]
\[
= \sum_{i=0}^{(l+1)-1} B_m(a)^{(l+1)-1-i} \cdot F_1(X)^{q^{m-i}}.
\]
This shows that Equality (14) holds for all \( l \geq 1 \). \( \square \)
Thus, regarding Equation (14) and Proposition 10, one has
\[ X^{q^N} - X = G_2 \circ F_1(X) = F_1 \circ G_2(X) = L_\alpha \circ G_1 \circ G_2(X) \quad (15) \]
and consequently
\[ \ker(F_1) = G_2(F_q), \]
\[ \ker(L_\alpha) = G_1 \circ G_2(F_q). \]
Since \( L_\alpha(X) = XP_a(X^{q-1}) \), here we can state:

**Proposition 12.** For \( a \in F_q^* \),
\[
\{x \in F_p : x^{q+1} + x + a = 0\} = \{x^{q-1} : x \in G_1 \circ G_2(F_q)\} \setminus \{0\}. \quad (18)
\]

Our goal is to determine \( S_\alpha = \{x \in F_q : P_a(x) = 0\} \), the set of all \( F_q \)-zeros to \( P_a(X) = X^{q+1} + X + a = 0, a \in F_q \).

**Remark 13.** In order to find the \( F_q \)-zeros of \( P_a(X) \) it is not enough to consider the \( F_q \)-zeros of \( L_\alpha(X) \). In fact, one can see that \( B_m(a) \neq 1 \) in general. However, it holds:

**Proposition 14.** \( L_\alpha(X) = 0 \) has a solution in \( F_q^* \) if and only if \( B_m(a) = 1 \).

**Proof.** If \( L_\alpha(x) = 0 \) for \( x \in F_q^* \), then by (12) \( F_1(x) = 0 \) i.e. \( x^{q^m} - B_m(a) \cdot x = (1 - B_m(a)) \cdot x = 0 \) and consequently \( B_m(a) = 1 \). Conversely, assume \( B_m(a) = 1 \). Then \( F_1(X) = X^{q^m} - X = L_\alpha \circ G_1(X) \) and \( \ker(L_\alpha) = G_1(F_q) \). Assume \( G_1(F_q) = \{0\} \). Then, since \( G_1 \) is \( q \)-linearized, it holds \( G_1(F_q) \subseteq G_1(F_q) = \{0\} \) which contradicts to \( \deg(G_1) < q^m \). Thus there exists such a \( x_0 \) in \( F_q^* \) that \( G_1(x_0) \neq 0 \). Then \( G_1(x_0) \in \ker(L_\alpha) \cap F_q^* \).

To achieve the goal, we will further need the following lemmas.

**Lemma 15.** Let \( L(X) \) be any \( q \)-linearized polynomial over \( F_q \). If \( x^{q-1}_0 \in F_q \), then \( L(x_0^{q-1}) \in F_q \).

**Proof.** If \( x_0^{q-1} \in F_q \) i.e. \( x_0^{q-1} = \lambda \) for some \( \lambda \in F_q \), then \( x_0^q = \lambda x_0 \) and subsequently \( x_0^q = \prod_{i=0}^{q-1} \lambda^i x_0 \) for every \( i \geq 1 \). Therefore, when \( L(X) \) is a \( q \)-linearized polynomial over \( F_q \), one can write \( L(x_0) = \lambda x_0 \) for some \( \lambda \in F_q \). Thus, \( L(x_0^{q-1}) = \lambda^{q-1} \lambda \in F_q \).

**Lemma 16.** Let \( s = \frac{(q^m-1)(p^q-1)}{(q-1)(q^m-1)} \). If \( A_m(a) = 0 \) and \( x_0 \in \ker(F_1) \), then \( x_0^s \in \ker(F_1) \) and \( (x_0^s)^{q-1} \in F_q \).
Proof. For $x_0 = 0$, the statement is trivial. Therefore, we can assume $x_0 \neq 0$. Then, $x_0 \in \ker(F_1)$ implies

$$B_m(a) = x_0^{q^m-1} = (x_0^s)^{(q-1) \frac{q^m-1}{q-1}}.$$  

(19)

Since $B_m(a) \in \mathbb{F}_{p^m}$, therefore $(x_0^s)^{q^m-1} \in \mathbb{F}_Q$.

Now, we will show

$$B_m(a) = B_m(a)^s.$$  

Since $P_a(X)$ has $p^d + 1$ rational solutions when $A_m(a) = 0$, there exists such a non-zero $x_1$ that

$$L_a(x_1) = 0, x_1^{q^m-1} \in \mathbb{F}_Q.$$  

Then (12) gives $F_1(x_1) = 0$ i.e.

$$x_1^{q^m-1} = B_m(a),$$  

and on the other hand

$$x_1^{q^m-1} = (N_{\mathbb{F}_Q|\mathbb{F}_{p^m}}(x_1^{q^m-1}))^s = (N_{\mathbb{F}_{q^m} | \mathbb{F}_q}(x_1^{q^m-1}))^s = (x_1^{q^m-1})^s = B_m(a)^s,$$

where the second equality followed from the fact that $N_{\mathbb{F}_Q|\mathbb{F}_{p^m}}(y) = N_{\mathbb{F}_{q^m} | \mathbb{F}_q}(y)$ for any $y \in \mathbb{F}_Q$. Thus, $B_m(a) = B_m(a)^s$.

Hence, $(x_0^s)^{q^m-1} = (x_0^s)^{(q^m-1)^s} = B_m(a)^s = B_m(a)^s$ i.e. $F_1(x_0^s) = 0$. \hfill \Box

Now, take any $x_0 \in \ker(F_1)$. The definition (10) and Lemma 16 shows

$$x_0^s \cdot \mathbb{F}_Q^s := \{x_0^s \cdot \alpha \mid \alpha \in \mathbb{F}_Q^s\} \subset \ker(F_1) = G_2(\mathbb{F}_{p^n})$$

and

$$(x_0^s \cdot \mathbb{F}_Q^s)^{q^m-1} \subset \mathbb{F}_Q.$$  

Subsequently, Lemma 15 and Equality (18) prove

$$G_1(x_0^s \cdot \mathbb{F}_Q^s)^{q^m-1} \subset S_a.$$

In order to avoid the trivial zero solution, we need

$$G_1(x_0^s \cdot \mathbb{F}_Q^s) \neq \{0\}. $$

In fact, this is the case. Really, if we assume $G_1(x_0^s \cdot \mathbb{F}_Q^s) = \{0\}$, then $G_1(x_0^s \cdot \mathbb{F}_{q^m}) = \{0\}$ (because $G_1$ is $\mathbb{F}_q$-linear, and $\mathbb{F}_{q^m}$ is generated by $\mathbb{F}_q$ and $\mathbb{F}_Q$) which contradicts to deg($G_1$) $< q^m$.

Next, in order to explicit all $p^d + 1$ elements in $S_a$, we need to deduce the following lemma.

**Lemma 17.** Let $A_m(a) = 0$ and $x_0$ be a $\mathbb{F}_Q$-solution to $P_a(X) = 0$. Then, $x_0^s \cdot \alpha$ is a $(q-1)$-th power in $\mathbb{F}_Q$. For $\beta \in \mathbb{F}_Q$ with $\beta^{q^m-1} = \frac{x_0^s}{\alpha}$,

$$w^q - w + \frac{1}{\beta x_0} = 0$$  

(20)
has exactly $p^d$ solutions in $\mathbb{F}_Q$. Let $w_0 \in \mathbb{F}_Q$ be a $\mathbb{F}_Q$-solution to Equation (20). Then, the $p^d + 1$ solutions in $\mathbb{F}_Q$ to $P_a(x) = 0$ are $x_0, (w_0 + \alpha)^{q-1} \cdot x_0$ where $\alpha$ runs over $\mathbb{F}_p^d$.

Proof. We substitute $x$ in $P_a(x)$ with $x_0 - x$ to get

$$(x_0 - x)^{q+1} + (x_0 - x) + a = 0$$

or

$$x^{q+1} - x_0x^q - x_0^q x - x + x_0^{q+1} + x_0 + a = 0$$

which implies

$$x^{q+1} - x_0x^q - (x_0^q + 1)x = 0,$$

or equivalently,

$$x^{q+1} - x_0x^q + \frac{a}{x_0}x = 0.$$ 

Since $x = 0$ corresponds to $x_0$ being a zero of $P_a(X)$, we can replace the latter equation by $x^{q+1}$ to get

$$\frac{a}{x_0} y^q - x_0 y + 1 = 0 \quad (21)$$

where $y = \frac{1}{x_0}$. Now, let $y = tw$ where

$$t^{q-1} = \frac{x_0^2}{a} \quad (22)$$

Then, Equation (21) is equivalent to

$$w^q - w + \frac{1}{tx_0} = 0. \quad (23)$$

If $t_0$ is a solution to Equation (22), then the set of all $q - 1$ solutions can be represented as $t_0 \cdot \mathbb{F}_q^*$. For every $\lambda \in \mathbb{F}_q^*$, when $w_0$ is a solution to Equation (23) for $t = t_0, \lambda w_0$ is a solution to Equation (23) for $t = t_0/\lambda$. By the way, $(t_0, w_0)$ and $(t_0/\lambda, \lambda w_0)$ give the same $w_0 = t_0 \cdot w_0 = t_0/\lambda \cdot \lambda w_0$. Therefore, to find all $\mathbb{F}_Q$-solutions to Equation (21) one can consider Equation (23) for any fixed solution $t_0$ of Equation (22).

Now, we will show that any solution $t_0$ to Equation (22) lies in $\mathbb{F}_q \cdot \mathbb{F}_Q := \{\alpha \cdot \beta \mid \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_Q\}$. In fact, we know that Equation (23) has $p^d$ solutions $w$ with $y = wt_0 \in \mathbb{F}_Q$. Let’s fix a solution $w_0$ with $y_0 = w_0 t_0 \in \mathbb{F}_Q$ of Equation (23). Then, the set of all solutions to Equation (23) can be written as $w_0 + \mathbb{F}_q$. Therefore, it follows that there exist $p^d + 2$ elements $\lambda \in \mathbb{F}_q$ with $(w_0 + \lambda)t_0 \in \mathbb{F}_Q$. As $w_0 t_0 \in \mathbb{F}_Q$ and $(w_0 + \lambda)t_0 \in \mathbb{F}_Q$, we have $\lambda t_0 \in \mathbb{F}_Q$ i.e. $t_0 \in \frac{1}{\lambda} \mathbb{F}_Q \subset \mathbb{F}_q \cdot \mathbb{F}_Q$.

Hence, we can write $t_0 = \alpha \cdot \beta$, where $\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_Q$, and it follows that the set of all solutions to Equation (22) are $\mathbb{F}_q^* \cdot \beta$. This means that Equation (22) has $p^d - 1$ solutions (i.e. $\mathbb{F}_q^* \cdot \beta$) in $\mathbb{F}_Q$, i.e., $\frac{\alpha}{a}$ is a $(q - 1)$-th power in $\mathbb{F}_Q$. Moreover, Equation (20) has exactly $p^d$ solutions in $\mathbb{F}_Q$ (because Equation (21) has exactly
\( p^d \) solutions \( y = w\beta \) in \( \mathbb{F}_Q \). When \( w_0 \in \mathbb{F}_Q \) is such a solution, the set of all \( p^d \) solutions in \( \mathbb{F}_Q \) is \( w_0 + \mathbb{F}_p^d \). Since Equation (23) yields \( y = wt = \frac{1}{1-w^{q-1}}x_0 \), we have \( x_0 - x = x_0 - \frac{1}{w} = x_0 - (1-w^{q-1})x_0 = w^{q-1}x_0 \). The proof is over. \( \Box \)

Finally, all discussion of this section are summed up in the following theorem.

**Theorem 18.** Assume \( A_m(a) = 0 \). Let \( N = m(p^d - 1) \), \( s = \frac{(q^m-1)(p^d-1)}{(q-1)(q^m-1)} \), \( G_1(X) = \sum_{i=0}^{m-2} A_{m-1-i}(a)q^{i+1}\cdot X^q \) and \( G_2(X) = \sum_{i=0}^{p^d-2} B_m(a)p^{i+2}\cdot X^q \). It holds \( G_1(G_2(\mathbb{F}_p^s))\cdot \mathbb{F}_p^s \cdot \mathbb{F}_Q^{q-1} \neq \{0\} \). Take a \( x_0 \in G_1(G_2(\mathbb{F}_p^s))\cdot \mathbb{F}_p^s \cdot \mathbb{F}_Q^{q-1} \setminus \{0\} \).

\[ \frac{x_0^2}{a} \] is a \((q-1)\)-th power in \( \mathbb{F}_Q \). For \( \beta \in \mathbb{F}_Q \) with \( \beta^{q-1} = \frac{x_0^2}{a} \),

\[ w^q - w + \frac{1}{\beta x_0} = 0 \]

has exactly \( p^d \) solutions in \( \mathbb{F}_Q \). Let \( w_0 \in \mathbb{F}_Q \) be a \( \mathbb{F}_Q \)-solution to Equation (20). Then, the \( p^d + 1 \) solutions in \( \mathbb{F}_Q \) of \( P_a(X) \) are \( x_0, (w_0 + \alpha)^{q-1}\cdot x_0 \) where \( \alpha \) runs over \( \mathbb{F}_{p^d} \).

Note that one can also explicit \( w_0 \) by an immediate corollary of Theorem 4 and Theorem 5 in [25].

## 4 Conclusion

In [2, 15, 16, 5, 3, 20, 8, 24, 19], partial results about the zeros of \( P_a(X) = X^{p^k+1} + X + a \) over \( \mathbb{F}_{p^d} \) have been obtained. In this paper, we provided explicit expressions for all possible zeros in \( \mathbb{F}_{p^d} \) of \( P_a(X) \) in terms of \( a \) and thus finalize the study initiated in these papers.

## Acknowledgement

The authors deeply thank Professor Dok Nam Lee for his many helpful suggestions and careful checking.

## References

23. M. Massierer. Some experiments investigating a possible $L(1/4)$ algorithm for the discrete logarithm problem in algebraic curves. *Cryptology ePrint Archive 2014/996*

