Solving X q+1 + X + a = 0 over finite fields

Kwang Ho Kim, Junyop Choe, Sihem Mesnager

▶ **To cite this version:**

Kwang Ho Kim, Junyop Choe, Sihem Mesnager. Solving X q+1 + X + a = 0 over finite fields. Finite Fields and Their Applications, 2021, 70, pp.101797 -. 10.1016/j.ffa.2020.101797 . hal-03493884

HAL Id: hal-03493884
https://hal.science/hal-03493884

Submitted on 2 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Version of Record: https://www.sciencedirect.com/science/article/pii/S1071579720301660
Manuscript_16fcf1532d5c5e2aff055667ca1745c9

Solving $X^{q+1} + X + a = 0$ over Finite Fields

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

[1] Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People's Republic of Korea
khk.cryptech@gmail.com; jyc.cryptech@outlook.com
[2] PGItech Corp., Pyongyang, Democratic People's Republic of Korea
[3] Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, LAGA UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, 93430 Villetaneuse, France and Telecom ParisTech, 91120 Palaiseau, France
smesnager@univ-paris8.fr

Abstract. Solving 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 [2], the construction of difference sets with Singer parameters [8], determining cross-correlation between m-sequences [9, 15] and the construction of error-correcting codes [5], as well as speeding up the index calculus method for computing discrete logarithms on finite fields [11, 12] and on algebraic curves [18].
Subsequently, in [3, 13, 14, 6, 4, 16, 7, 19], the $\mathbb{F}_Q$-zeros of $P_a(X)$ have been studied. It was shown in [3] that their number 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 [13, 14, 6, 16, 19]. However, while the ultimate goal is to identify all the $\mathbb{F}_Q$-zeros, even in the case $p = 2$, it was solved only under the condition $\gcd(n, k) = 1$ [16].
We discuss this equation without any restriction on p and $\gcd(n, k)$. Criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(x)$ are proved by a new methodology. For the cases of one or two $\mathbb{F}_Q$-zeros, we provide explicit expressions for these rational zeros in terms of a. For the case of $p^{\gcd(n,k)}+1$ rational zeros, we provide a parametrization of such a's and express the $p^{\gcd(n,k)} + 1$ rational zeros by using that parametrization.

Keywords: Equation · Finite fields · Zeros of a polynomial · Projective polynomial.

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

1 Introduction

Let k and n 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

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

© 2020 published by Elsevier. This manuscript is made available under the CC BY NC user license
https://creativecommons.org/licenses/by-nc/4.0/

where $\mathbb{F}_Q^* := \mathbb{F}_Q \setminus \{0\}$. Note that the more general polynomials

$$X^{q+1} + rX^q + sX + t,$$

with $s \neq r^q$ and $t \neq rs$ can be transformed into this shape by the substitution

$$X = (s - r^q)^{\frac{1}{q}} X_1 - r.$$

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

Polynomials of the form

$$\sum_{i=0}^{t} a_i X^{\frac{q^i-1}{q-1}}, \quad a_i \in \mathbb{F}_{q^m},$$

are called projective polynomials. Projective polynomials were introduced by Abhyankar [1]. His original motivation was to find polynomials with a given Galois group. $P_a(X)$ is a particular projective polynomial where $t = 2$, $a_1 = a_2 = 1$, $a_0 = a$ and $m = \frac{n}{\gcd(n,k)}$.

Projective polynomials have arisen in several different contexts including finite geometry, the inverse Galois problem [2], the construction of difference sets with Singer parameters [8], determining cross-correlation between m-sequences [9, 15], the construction of error-correcting codes [5] and the calculation of composition collisions [10]. These polynomials are also exploited to speed up (the relation generation phase in) the index calculus method for the computation of discrete logarithms on finite fields [11, 12] and on algebraic curves [18].

Let N_a denote the number of zeros in $\mathbb{F}_Q$ of the 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 [3] proved that N_a equals 0, 1, 2 or $p^d + 1$ 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 number of roots of any projective polynomial was determined implicitly in [10] and explicitly in [19] from its coefficients. In particular, new criteria for which $P_a(X)$ has 0, 1, 2 or $p^d + 1$ roots were proved in [19] for any characteristic.

The ultimate goal in this direction of research is to identify all the $\mathbb{F}_Q$-zeros of $P_a(X)$. Really many efforts were made by several researchers toward this goal, specifically for a particular instance of the problem over binary fields i.e. $p = 2$. In 2008 and 2010, Helleseth and Kholosha [13, 14] 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 [14]. They also showed in [13] that if $d = 1$ then N_a equals 0, 1 or 3. In 2014, Bracken, Tan and Tan [6] presented a criterion for $N_a = 0$ in $\mathbb{F}_{2^n}$ when $d = 1$ and n is even. Very recently, Kim and Mesnager [16] completely solved the 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 $P_a(X)$ can be divided into two problems with odd k : to find the unique preimage of an element in $\mathbb{F}_{2^n}$ under a MCM 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 3 as a by-product.

We 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 defining a sequence of polynomials and considering its properties in Section 2, it is shown in Section 3 that if $N_a \leq 2$ then there exists a quadratic equation that the rational zeros must satisfy. In Section 4, we state some useful properties of the polynomials which appear as the coefficients of that quadratic equation. In Section 5, criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(x)$ are proved. For the cases of one or two $\mathbb{F}_Q$-zeros, we provide explicit expressions for these rational zeros in terms of a. We also provide a parametrization of the a's for which $P_a(X)$ has $p^{\gcd(n,k)}+1$ rational zeros. Based on that parametrization, all the $p^{\gcd(n,k)}+1$ rational zeros are expressed. For the case of $p^{\gcd(n,k)}+1$ rational zeros, some results to explicitly express these rational zeros in terms of a are presented in Section 6. Finally, we conclude in Section 7.

2 Preliminaries

Given positive integers k and l, define the polynomial

$$T_k^{kl}(X) := X + X^{p^k} + \cdots + X^{p^{k(l-2)}} + X^{p^{k(l-1)}}.$$

Usually we will abbreviate $T_1^l(\cdot)$ as $T_l(\cdot)$. For $x \in \mathbb{F}_{p^l}$, $T_l(x)$ is the absolute trace $\mathrm{Tr}_1^l(x)$ of x. For $x \in \mathbb{F}_{p^{kl}}$, its norm $\mathrm{Nr}_k^{kl}(x)$ over $\mathbb{F}_{p^k}$ is defined by

$$\mathrm{Nr}_k^{kl}(x) := x^{1+p^k+\cdots+p^{k(l-2)}+p^{k(l-1)}}.$$

The preimages of $T_k^{kl}(X)$ are studied in [20]. Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. The following is, in essence, a restatement of Hilbert's Theorem 90 (cf. Theorem 2.25 in [17]).

Proposition 1. *For any positive integers k and r,*

$$\{x \in \overline{\mathbb{F}_p} \mid T_k^{kr}(x) = 0\} = \{u - u^{p^k} \mid u \in \mathbb{F}_{p^{kr}}\}.$$

Proof. Evidently, $\{u - u^{p^k} | u \in \mathbb{F}_{p^{kr}}\} \subset \mathbf{ker}(T_k^{kr})$. The linear mapping $u \mapsto u - u^{p^k}$ has the kernel $\mathbb{F}_{p^k}$ and so $\#\{u - u^{p^k} | u \in \mathbb{F}_{p^{kr}}\} = p^{k(r-1)}$. On the other hand, T_k^{kr} cannot have a kernel of greater cardinality than its degree $p^{k(r-1)}$. □

Define the sequence of polynomials $\{A_r(X)\}$ as follows:

$$\begin{aligned} &A_0(X) = 0, A_1(X) = 1, A_2(X) = -1, \\ &A_{r+2}(X) = -A_{r+1}(X)^q - X^q A_r(X)^{q^2} \text{ for } r \geq 0. \end{aligned} \tag{1}$$

This sequence of polynomials $\{A_r(X)\}$ have also appeared in [13, 14] for p even and in the independent study [19] for general p by a bit different form (see also

Remarks 12 and 13). However, our motivation is different from [13, 14, 19] (see Sec. 3).

Lemma 2 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 important later. Its proof also appear in [14] for p even and in [19] for general p. For completeness, we include here the proof.

Lemma 2. *For any $r \geq 1$, the following are true.*

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

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

Proof. We will prove these identities by induction on r. It is easy to check that they hold for $r = 1, 2$. Suppose that they hold for all indices less than $r(\geq 3)$. Then, we have

$$\begin{aligned}
A_{r+3}(X) &= -A_{r+2}(X)^q - X^q A_{r+1}(X)^{q^2} \\
&= \left(A_{r+1}(X) + X^{q^r} A_r(X)\right)^q + X^q \left(A_r(X) + X^{q^{r-1}} A_{r-1}(X)\right)^{q^2} \\
&= \left(A_{r+1}^q(X) + X^q A_r^{q^2}(X)\right) + X^{q^{r+1}} \left(A_r^q(X) + X^q A_{r-1}^{q^2}(X)\right) \\
&= -A_{r+2}(X) - X^{q^{r+1}} A_{r+1}(X),
\end{aligned}$$

which proves (2) for all r. Also, using the proved equality (2), we have

$$\begin{aligned}
&A_{r+2}(X)^{q+1} - A_{r+1}(X)^q A_{r+3}(X) \\
&= A_{r+2}(X)^{q+1} + A_{r+1}(X)^q \left(A_{r+2}(X) + X^{q^{r+1}} A_{r+1}(X)\right) \\
&= X^{q^{r+1}} \left(A_{r+1}(X)^{q+1} - A_r(X)^q A_{r+2}(X)\right) + A_{r+2}(X) \left(A_{r+2}(X)^q + A_{r+1}(X)^q + X^{q^{r+1}} A_r(X)^q\right) \\
&\overset{(2)}{=} X^{q^{r+1}} \left(A_{r+1}(X)^{q+1} - A_r(X)^q A_{r+2}(X)\right) \\
&= X^{q^{r+1}} X^{\frac{q(q^r-1)}{q-1}} = X^{\frac{q(q^{r+1}-1)}{q-1}},
\end{aligned}$$

which proves (3) for all r. □

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

Proposition 3. *For any $r \geq 3$,*

$$\{x \in \overline{\mathbb{F}_p} \mid A_r(x) = 0\} = \left\{ \frac{(u - u^q)^{q^2+1}}{(u - u^{q^2})^{q+1}}, \quad u \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2} \right\}.$$

Proof. Given any $x \in \overline{\mathbb{F}_p} \setminus \{0\}$, there exists at least one element $v \in \overline{\mathbb{F}_p}$ such that $x = \frac{v^{q^2+1}}{(v+v^q)^{q+1}}$ and $v + v^q \neq 0$. Then, for any $r \geq 2$, we have

$$A_r(x) = (-1)^{r+1} \frac{\sum_{j=1}^{r} v^{q^j}}{v^q + v^{q^2}} \prod_{j=2}^{r-1} \left(\frac{v}{v+v^q} \right)^{q^j},$$

where for $i = 2$ it is assumed that the product over the empty set is equal to 1. Indeed, this can be proved by induction on r as follows. For $r = 2$ and $r = 3$, we have

$$A_2(x) = -1 = (-1)^3 \frac{\sum_{j=1}^{2} v^{q^j}}{v^q + v^{q^2}}$$

and

$$A_3(x) = 1 - x^q = 1 - \frac{v^{q+q^3}}{(v+v^q)^{q+q^2}} = (-1)^4 \frac{\sum_{j=1}^{3} v^{q^j}}{v^q + v^{q^2}} \left(\frac{v}{v+v^q} \right)^{q^2}.$$

Assuming this identity holds for all indices less than r, we have

$$\begin{aligned}
A_r(x) &\overset{(2)}{=} -A_{r-1}(x) - x^{q^{r-2}} A_{r-2}(x) \\
&= (-1)^{r+1} \frac{\sum_{j=1}^{r-1} v^{q^j}}{v^q + v^{q^2}} \prod_{j=2}^{r-2} \left(\frac{v}{v+v^q} \right)^{q^j} - (-1)^{r+1} \frac{v^{q^r} \sum_{j=1}^{r-2} v^{q^j}}{(v+v^q)^{q^{r-1}+q}} \prod_{j=2}^{r-2} \left(\frac{v}{v+v^q} \right)^{q^j} \\
&= (-1)^{r+1} \frac{(v+v^q)^{q^{r-1}} \sum_{j=1}^{r-1} v^{q^j} - v^{q^r} \sum_{j=1}^{r-2} v^{q^j}}{v^{q^{r-1}} (v+v^q)^q} \prod_{j=2}^{r-1} \left(\frac{v}{v+v^q} \right)^{q^j} \\
&= (-1)^{r+1} \frac{\sum_{j=1}^{r} v^{q^j}}{v^q + v^{q^2}} \prod_{j=2}^{r-1} \left(\frac{v}{v+v^q} \right)^{q^j}.
\end{aligned}$$

Thus $A_r(x) = 0$ if and only if $\sum_{j=1}^{r} v^{q^j} = (T_k^{kr}(v))^q = 0$ and $v + v^q \neq 0$, which by Proposition 1 is equivalent to $v = u - u^q$ for some $u \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2}$.

Therefore, $A_r(x) = 0$ if and only if $x = \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}}$ for some $u \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2}$. □

Later we will need the following lemma.

Lemma 4 ([3]).

1. *$N_a = p^d + 1$ if and only if $P_a(X)$ splits in $\mathbb{F}_{q^m}$.*
2. *The number of $a \in \mathbb{F}_Q^*$ such that $P_a(X)$ has exactly $p^d + 1$ zeros in $\mathbb{F}_Q$ is*

$$M_{p^d+1} = \frac{p^{(m-1)d} - p^{\epsilon d}}{p^{2d} - 1},$$

where $\epsilon = 0$ if m is odd and $\epsilon = 1$ otherwise.

Proof. The first item follows from Theorem 4.3 and Corollary 7.2 of [3] since $\mathbb{F}_{q^m}$ is the smallest field containing both $\mathbb{F}_q$ and $\mathbb{F}_Q$. The second item is from Theorem 5.6 of [3]. □

3 Quadratic equation satisfied by rational zeros of $P_a(X)$

Put $m = n/d$ and define the polynomials

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

We will show 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 5. *Let $a \in \mathbb{F}_Q^*$. If $P_a(x) = 0$ for $x \in \mathbb{F}_Q$ then*

$$F(a)x^2 + G(a)x + aF^q(a) = 0. \tag{4}$$

Proof. If $x^{q+1} + x + a = 0$ for $x \in \mathbb{F}_Q$, then $x \neq 0$ and thus we get

$$x^q = \frac{-x-a}{x}. \tag{5}$$

Now, we prove that for any $r \geq 1$

$$x^{q^r}\left(A_r(a)x - aA_{r-1}(a)^q\right) - A_{r+1}(a)x + aA_r(a)^q = 0 \tag{6}$$

with the assumption $A_0(x) = 0$. In fact, if $r = 1$ then the left side of (6) is $P_a(x)$ and so it holds for $r = 1$. Suppose that it holds for $r \geq 1$. Taking $q-$th powers of (6) and substituting (5), we have

$$\begin{gathered}
x^{q^{r+1}}\left(A_r(a)^q x^q - a^q A_{r-1}(a)^{q^2}\right) - A_{r+1}(a)^q x^q + a^q A_r(a)^{q^2} = 0 \Rightarrow \\
x^{q^{r+1}}\left(-A_r(a)^q \tfrac{x+a}{x} - a^q A_{r-1}(a)^{q^2}\right) + A_{r+1}(a)^q \tfrac{x+a}{x} + a^q A_r(a)^{q^2} = 0 \Rightarrow \\
x^{q^{r+1}}\left(\left(-A_r(a)^q - a^q A_{r-1}(a)^{q^2}\right)x - aA_r(a)^q\right) + \left(A_{r+1}(a)^q + a^q A_r(a)^{q^2}\right)x + \\
aA_{r+1}(a)^q = 0 \Rightarrow \\
x^{q^{r+1}}\left(A_{r+1}(a)x - aA_r(a)^q\right) - A_{r+2}(a)x + aA_{r+1}(a)^q = 0.
\end{gathered}$$

This shows that (6) holds for $r+1$ and so for all r.

Taking $r = m$ in (6) and using the fact that $x^{q^m} = x^{Q^{k/d}} = x$ when $x \in \mathbb{F}_Q$, we obtain the result of the lemma. □

4 Some equalities involving F and G

To determine the $\mathbb{F}_Q-$rational zeros of $P_a(X)$ when $N_a \leq 2$, we will need the following properties of the polynomials F and G which appear as coefficients of the quadratic equation (4).

Proposition 6. *For any $x \in \mathbb{F}_{q^m}$, the following are true.*

1.

$$(G(x) - 2F(x))^q = -G(x). \tag{7}$$

2.

$$G(x)^2 - 4xF(x)^{q+1} \in \mathbb{F}_q. \tag{8}$$

3.

$$G(x) = -x^q F^{q^2}(x) + F^q(x) + xF(x). \tag{9}$$

Proof. The first item follows from

$$\begin{aligned}(G(x) - 2F(x))^q &= G(x)^q - 2F(x)^q = -A_{m+1}(x)^q - x^q A_{m-1}(x)^{q^2} - 2A_m(x)^q \\ &\overset{(2)}{=} (A_m(x) + x^{q^{m-1}} A_{m-1}(x))^q - x^q A_{m-1}(x)^{q^2} - 2A_m(x)^q \\ &= xA_{m-1}(x)^q - x^q A_{m-1}(x)^{q^2} - A_m(x)^q \text{ (since } x^{q^m} = x) \\ &\overset{(1)}{=} xA_{m-1}(x)^q + A_{m+1}(x) = -G(x).\end{aligned}$$

The second item is proved as follows. Let $E = G(x)^2 - 4xF(x)^{q+1}$. Then

$$\begin{aligned}E^q - E = &\left(A_{m+1}(x)^q + x^q A_{m-1}(x)^{q^2}\right)^2 - 4x^q A_m(x)^{q(q+1)} \\ &- \left(A_{m+1}(x) + xA_{m-1}(x)^q\right)^2 + 4xA_m(x)^{q+1}.\end{aligned}$$

Consider $A_{m+1}(x)^q \overset{(2)}{=} (-A_m(x) - x^{q^{m-1}} A_{m-1}(x))^q = -A_m(x)^q - xA_{m-1}(x)^q$. By substituting this and using (1), we have

$$\begin{aligned}E^q - E &= \left(-A_m(x)^q - xA_{m-1}(x)^q + x^q A_{m-1}(x)^{q^2}\right)^2 - 4x^q A_m(x)^{q(q+1)} \\ &\quad - \left(-A_m(x)^q - x^q A_{m-1}(x)^{q^2} + xA_{m-1}(x)^q\right)^2 + 4xA_m(x)^{q+1} \\ &= 4A_m(x)^q \left(xA_{m-1}(x)^q - x^q A_{m-1}(x)^{q^2}\right) - 4x^q A_m(x)^{q(q+1)} + 4xA_m(x)^{q+1} \\ &= 4A_m(x)^q \left(xA_{m-1}(x)^q - x^q A_{m-1}(x)^{q^2} - x^q A_m(x)^{q^2} + xA_m(x)\right).\end{aligned}$$

If $m = 1$, then obviously $E^q - E = 0$. Now, assume $m \geq 2$. Then, by using

$$\begin{aligned}x^q A_{m-1}(x)^{q^2} + x^q A_m(x)^{q^2} &= x^q (A_{m-1}(x) + A_m(x))^{q^2} \\ &\overset{(2)}{=} -x^q (x^{q^{m-2}} A_{m-2}(x))^{q^2} = -x^{q+1} A_{m-2}(x)^{q^2},\end{aligned}$$

we get $E^q - E = 4xA_m(x)^q \left(A_{m-1}(x)^q + x^q A_{m-2}(x)^{q^2} + A_m(x)\right) \overset{(1)}{=} 0$, that is, $E = G(x)^2 - 4xF(x)^{q+1} \in \mathbb{F}_q$.

Finally, the third item is verified as follows:

$$\begin{aligned}G(x) &= -A_{m+1}(x) - xA_{m-1}(x)^q \overset{(1)}{=} A_m(x)^q + x^q A_{m-1}(x)^{q^2} - xA_{m-1}(x)^q \\ &\overset{(1)}{=} A_m(x)^q + x^q A_{m-1}(x)^{q^2} + x\left(x^q A_{m-2}(x)^{q^2} + A_m(x)\right) \\ &= x^q \left(A_{m-1}(x) + x^{q^{m-2}} A_{m-2}(x)\right)^{q^2} + A_m(x)^q + xA_m(x) \\ &\overset{(2)}{=} -x^q A_m(x)^{q^2} + A_m(x)^q + xA_m(x).\end{aligned}$$

□

When $p = 2$, Item 1 and 2 of Proposition 6 are reduced to

$$G(x) \in \mathbb{F}_q \text{ for any } x \in \mathbb{F}_{q^m}. \tag{10}$$

For p even, we will further need the following proposition.

Proposition 7. *Let $p = 2$. Let $a \in \mathbb{F}_Q$ with $G(a) \neq 0$. Let $E = \frac{aF(a)^{q+1}}{G^2(a)}$ and $H = \mathrm{Tr}_1^d\left(\frac{\mathrm{Nr}_d^n(a)}{G^2(a)}\right)$. The followings hold.*

1.
$$\mathrm{Tr}_1^n(E) = mH. \tag{11}$$

2.
$$T_k(E) = \frac{G(a) + F(a)^q}{G(a)} + \frac{k}{d}H. \tag{12}$$

Proof. From the fact that modulo n the sets $\{0, k, 2k, \ldots, (m-1)k\}$ and $\{0, d, 2d, \ldots, (m-1)d\}$ coincide, $\mathrm{Nr}_k^{mk}(a) = \mathrm{Nr}_d^n(a)$ follows and we have

$$\begin{aligned} E = \frac{aF(a)^{q+1}}{G(a)^2} &\overset{(3)}{=} \frac{aA_{m-1}(a)^q A_{m+1}(a) + \mathrm{Nr}_d^n(a)}{G(a)^2} \\ &= \frac{(A_{m+1}(a) + G(a))\, A_{m+1}(a) + \mathrm{Nr}_d^n(a)}{G(a)^2} \\ &= \frac{A_{m+1}(a)}{G(a)} + \left(\frac{A_{m+1}(a)}{G(a)}\right)^2 + \frac{\mathrm{Nr}_d^n(a)}{G(a)^2}. \end{aligned}$$

Hence, (11) immediately follows from the facts $\mathrm{Nr}_d^n(a) \in \mathbb{F}_{p^d}$ and $G(a) \in \mathbb{F}_{p^{md}} \cap \mathbb{F}_{p^k} = \mathbb{F}_{p^d}$ (which follows from (10) as $a \in \mathbb{F}_{p^{md}}$). And also

$$\begin{aligned} T_k(E) &= \frac{A_{m+1}(a)}{G(a)} + \left(\frac{A_{m+1}(a)}{G(a)}\right)^q + \frac{k}{d}H \overset{(10)}{=} \frac{A_{m+1}(a) + A_{m+1}(a)^q}{G(a)} + \frac{k}{d}H \\ &= \frac{G(a) + aA_{m-1}(a)^q + A_{m+1}(a)^q}{G(a)} + \frac{k}{d}H \\ &\overset{(2)}{=} \frac{G(a) + aA_{m-1}(a)^q + \left(A_m(a) + a^{q^{m-1}}A_{m-1}(a)\right)^q}{G(a)} + \frac{k}{d}H \\ &= \frac{G(a) + F(a)^q}{G(a)} + \frac{k}{d}H. \end{aligned}$$

□

5 Rational zeros of $P_a(X)$

By exploiting the results of the previous sections, now we represent the rational zeros of $P_a(X)$ in terms of a.

5.1 $N_a = p^d + 1$

Theorem 8. *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 3, there exists $u \in \mathbb{F}_{q^m} \setminus \mathbb{F}_{q^2}$ such that $a = \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}}$.*
3. *There exists $u \in \mathbb{F}_Q \setminus \mathbb{F}_{p^{2d}}$ such that $a = \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}}$. 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 $x_\alpha = \frac{-(u+\alpha)^{q^2-q}}{1+(u-u^q)^{q-1}}$ for $\alpha \in \mathbb{F}_{p^d}$.*

Proof. (Item 1 $\iff$ Item 2)

We already showed that if $F(a) \neq 0$, then $N_a \leq 2$, i.e. $N_a \neq p^d + 1$.

If $F(a) = 0$ i.e. there exists $u \in \mathbb{F}_{q^m} \setminus \mathbb{F}_{q^2}$ such that $a = \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}}$, then the set given by

$$\bigcup_{\alpha \in \mathbb{F}_q} \left\{ \frac{-(u+\alpha)^{q^2-q}}{1+(u-u^q)^{q-1}} \right\} \bigcup \left\{ \frac{-1}{1+(u-u^q)^{q-1}} \right\}$$

is the set of all $q+1$ zeros of $P_a(X)$. In fact, the cardinality of this set is exactly $q+1$ as u is not in $\mathbb{F}_q$. Also, we have

$$\begin{aligned} P_a\left(\frac{-1}{1+(u-u^q)^{q-1}}\right) &= \frac{-1}{1+(u-u^q)^{q-1}} \left(1 - \frac{1}{1+(u-u^q)^{q-1}}\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} \\ &= \frac{-(u-u^q)}{u-u^{q^2}} \left(\frac{(u-u^q)^q}{u-u^{q^2}}\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} = 0 \end{aligned}$$

and

$$\begin{aligned} &P_a\left(\frac{-(u+\alpha)^{q^2-q}}{1+(u-u^q)^{q-1}}\right) = \frac{-(u+\alpha)^{q^2-q}}{1+(u-u^q)^{q-1}} \left(1 + \frac{-(u+\alpha)^{q^2-q}}{1+(u-u^q)^{q-1}}\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} \\ &= \frac{-(u-u^q)}{(u-u^{q^2})^{q+1}(u+\alpha)^q} \left((u-u^{q^2})(u+\alpha)^q - (u-u^q)(u+\alpha)^{q^2}\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} \\ &= \frac{-(u-u^q)}{(u-u^{q^2})^{q+1}(u+\alpha)^q} \left((u-u^{q^2})(u^q+\alpha) - (u-u^q)(u^{q^2}+\alpha)\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} \\ &= \frac{-(u-u^q)}{(u-u^{q^2})^{q+1}(u+\alpha)^q} \left((u-u^q)^q(u+\alpha)\right)^q + \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} = 0. \end{aligned}$$

Lemma 4 concludes $N_a = p^d + 1$.

(Item 1 $\iff$ Item 3)

To begin with, define $S_0 = \mathbb{F}_Q \setminus \mathbb{F}_{q^2}$, $S_1 = \{u - u^q \mid u \in S_0\}$, $S_2 = \{v^{q-1} \mid v \in S_1\}$ and $S = \{a \in \mathbb{F}_Q \mid N_a = p^d + 1\}$.

Now, we will show that the mapping

$$\Psi : u \in S_0 \longmapsto \frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} \in S,$$

which is well-defined by Proposition 3 and by the equivalence between Item 1 and Item 2, is surjective.

Regarding $\frac{(u-u^q)^{q^2+1}}{(u-u^{q^2})^{q+1}} = \frac{((u-u^q)^{q-1})^q}{(1+(u-u^q)^{q-1})^{q+1}}$, we can write $\Psi = \varphi_3 \circ \varphi_2 \circ \varphi_1$ where $\varphi_1 : u \in S_0 \longmapsto u - u^q \in S_1$, $\varphi_2 : v \in S_1 \longmapsto v^{q-1} \in S_2$, $\varphi_3 : w \in S_2 \longmapsto \frac{w^q}{(1+w)^{q+1}} \in S$. Here, we note that $-1 \notin S_2$ (and hence φ_3 is well-defined) since $(u-u^q)^{q-1} = -1$ would yield $u = u^{q^2}$, i.e. $u \in \mathbb{F}_{q^2}$.

Consider $\varphi_1(u + \mathbb{F}_{p^d}) = \varphi_1(u)$ for any $u \in S_0$ and $\#S_1 = p^{(m-1)d} - (p^d - (p^d-1)\cdot(m \mod 2)) = (p^{md} - p^{(2-m \mod 2)d})/p^d = \#S_0/p^d$. Therefore φ_1 is p^d-to-one and surjective. Next, note that $\varphi_2(v_1) = \varphi_2(v_2)$ for $v_1, v_2 \in \mathbb{F}_Q$ if and only if $v_2 = \beta v_1$ for some $\beta \in \mathbb{F}_{p^d}^*$ and that if $v_1 \in S_1$ then $\beta v_1 \in S_1$ for any $\beta \in \mathbb{F}_{p^d}^*$ since $Tr_d^n(\beta v_1) = \beta Tr_d^n(v_1) = 0$. Hence φ_2 is (p^d-1)-to-one and surjective. On the other hand, if $a = \varphi_3(w)$ for $w \in S_2$, then $P_a(-\frac{1}{1+w}) = \left(-\frac{1}{1+w}\right)^{q+1} + \left(-\frac{1}{1+w}\right) + \frac{w^q}{(1+w)^{q+1}} = 0$. Since $a \in S$ and so $N_a = p^d + 1$, there are at most $p^d + 1$ such $w \in S_2$ that $\varphi_3(w) = a$. Therefore we get

$$\#\Psi(S_0) \geq \frac{\#S_2}{p^d+1} = \frac{p^{(m-1)d} - p^{(1-m \mod 2)d}}{p^{2d}-1}.$$

Since $\#S = \frac{p^{(m-1)d} - p^{(1-m \mod 2)d}}{p^{2d}-1}$ by the second item of Lemma 4, we have a sequence of inequalities $\#S \leq \#\Psi(S_0) \leq \#S$ which concludes that $\Psi(S_0) = S$, i.e. Ψ is surjective (note that it also follows that φ_3 is (p^d+1)-to-one and Ψ is $p^d(p^{2d}-1)$-to-one). This means that Item 1 and Item 3 are equivalent. □

5.2 $N_a \leq 2$: Odd p

Theorem 9. *Let p be odd. Let $a \in \mathbb{F}_Q^*$ and $E(a) = G(a)^2 - 4aF(a)^{q+1}$.*

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

Proof. To begin with, note $E(a) \in \mathbb{F}_q$ by (8) and so $E(a) \in \mathbb{F}_q \cap \mathbb{F}_Q = \mathbb{F}_{p^d}$.

Theorem 8 shows that $N_a \leq 2$ if and only if $F(a) \neq 0$. Now, assume $F(a) \neq 0$. Then Equation (4) can be rewritten as

$$\left(x + \frac{G(a)}{2F(a)}\right)^2 = \frac{E(a)}{4F(a)^2}. \tag{13}$$

Now, we will show that the solutions $x_{1,2} = \frac{\pm E^{\frac{1}{2}} - G(a)}{2F(a)}$ of (13) become the zeros of $P_a(X)$ if and only if $E(a)$ is a quadratic residue in $\mathbb{F}_q$. In fact, $\left(E(a)^{\frac{1}{2}}\right)^q = E(a)^{\frac{1}{2}} + \delta$ for some δ and then we have

$$\begin{aligned} P_a(x_{1,2}) = x_{1,2}(x_{1,2}+1)^q + a &= \frac{\pm E(a)^{\frac{1}{2}} - G(a)}{2F(a)} \left(1 + \frac{\pm E(a)^{\frac{1}{2}} - G(a)}{2F(a)}\right)^q + a \\ &= \frac{(\pm E(a)^{\frac{1}{2}} - G(a)) \left(\pm E(a)^{\frac{1}{2}} + \delta + (2F(a) - G(a))^q\right) + 4aF(a)^{q+1}}{4F(a)^{q+1}} \\ &\overset{(7)}{=} \frac{(\pm E(a)^{\frac{1}{2}} - G(a)) \left(\pm E(a)^{\frac{1}{2}} + \delta + G(a)\right) + 4aF(a)^{q+1}}{4F(a)^{q+1}} = \frac{(\pm E(a)^{\frac{1}{2}} - G(a))\delta}{4F(a)^{q+1}}, \end{aligned}$$

and so $P_a(x_{1,2}) = 0$ if and only if $\delta = 0$, that is, $E(a)^{\frac{1}{2}} \in \mathbb{F}_q$. On the other hand, $x_{1,2} \in \mathbb{F}_Q$ if and only if $E(a)^{\frac{1}{2}} \in \mathbb{F}_Q$. □

Remark 10. In the last two cases of Theorem 9 (i.e. the cases of $N_a = 0$ or 2), the condition $F(a) \neq 0$ is implied because $E \neq 0$ implies $F(a) \neq 0$. Indeed, if $F(a) = 0$, then from Equality (9) $G(a) = 0$ follows and so $E(a) = 0$.

5.3 $N_a \leq 2$: $p = 2$

Theorem 11. *Let $p = 2$ and $a \in \mathbb{F}_Q^*$. Let $H = \mathrm{Tr}_1^d\left(\frac{\mathrm{Nr}_d^n(a)}{G^2(a)}\right)$ and $E(a) = \frac{aF(a)^{q+1}}{G^2(a)}$.*

1. *$N_a = 1$ if and only if $F(a) \neq 0$ and $G(a) = 0$. In this case, $(aF(a)^{q-1})^{\frac{1}{2}}$ is the unique zero in $\mathbb{F}_Q$ of $P_a(X)$.*
2. *$N_a = 0$ if and only if $G(a) \neq 0$ and $H \neq 0$.*
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 $x_1 = \frac{G(a)}{F(a)} \cdot T_n\left(\frac{E}{\zeta+1}\right)$ and $x_2 = x_1 + \frac{G(a)}{F(a)}$, where $\zeta \in \mu_{Q+1}^* := \{z \in \mathbb{F}_{Q^2} \mid z^{Q+1} = 1\} \setminus \{1\}$.*

Proof. By Theorem 8 we may assume $F(a) \neq 0$ since this is equivalent to $N_a \in \{0, 1, 2\}$.

If $G(a) = 0$, then the Equation (4) has a unique solution $x_0 = (aF(a)^{q-1})^{1/2}$. Then $P_a^2(x_0) = \frac{a}{F(a)}\left(a^q F^{q^2}(a) + F^q(a) + aF(a)\right) \overset{(9)}{=} \frac{a}{F(a)} G(a) = 0$ and thus it follows that $P_a(X)$ has exactly one zero $(aF(a)^{q-1})^{1/2}$ in $\mathbb{F}_Q$ when $G(a) = 0$.

Now consider the case of $G(a) \neq 0$. Note that (9) shows that $G(a) \neq 0$ implies $F(a) \neq 0$. The equation (4) can be rewritten as $\left(\frac{F(a)}{G(a)}x\right)^2 + \frac{F(a)}{G(a)}x = E(a)$ and so it has a solution in $\mathbb{F}_Q$ if and only if

$$\mathrm{Tr}_1^n\left(E(a)\right) = 0. \tag{14}$$

If Equation (4) has a solution then it has exactly two solutions x_1 and x_2 in $\mathbb{F}_Q$. Indeed, $\left(\frac{F(a)}{G(a)}x_1\right)^2 + \frac{F(a)}{G(a)}x_1 = \left(\frac{F(a)}{G(a)}x_2\right)^2 + \frac{F(a)}{G(a)}x_2 = T_n\left(\frac{E(a)}{\zeta+1}\right)^2 + T_n\left(\frac{E(a)}{\zeta+1}\right) = \left(\frac{E(a)}{\zeta+1}\right)^Q + \left(\frac{E(a)}{\zeta+1}\right) = E(\frac{1}{\frac{1}{\zeta}+1} + \frac{1}{\zeta+1}) = E(a)$, and so x_1 and x_2 are two solutions of (4). And, both x_1 and x_2 are in $\mathbb{F}_Q$ since $T_n\left(\frac{E(a)}{\zeta+1}\right)^Q + T_n\left(\frac{E(a)}{\zeta+1}\right) = T_n(E(a)) = \mathrm{Tr}_1^n\left(E(a)\right) \overset{(14)}{=} 0$ i.e. $T_n\left(\frac{E(a)}{\zeta+1}\right) \in \mathbb{F}_Q$.

Let x be a solution of (4). Then we have $T_k\left(\left(\frac{F(a)}{G(a)}x\right)^2 + \frac{F(a)}{G(a)}x\right) = T_k(E(a))$, i.e. $\left(\frac{F(a)}{G(a)}x\right)^q + \frac{F(a)}{G(a)}x = T_k(E(a))$, hence $x^q = \left(\frac{G(a)}{F(a)}\right)^q\left(\frac{F(a)}{G(a)}x + T_k(E(a))\right) \overset{(10)}{=} \frac{F(a)x+G(a)T_k(E(a))}{F(a)^q}$ and $P_a(x) = x(x^q+1)+a = \frac{x(F(a)x+G(a)T_k(E(a))+F(a)^q)}{F(a)^q} + a \overset{(4)}{=} \frac{x(G(a)T_k(E(a))+F(a)^q+G(a))}{F(a)^q}$.

Thus, it follows that the solution x of (4) is a zero of $P_a(X)$ if and only if

$$T_k\left(E(a)\right) = \frac{G(a)+F(a)^q}{G(a)}. \tag{15}$$

Equalities (11), (12), (14) and (15) together leads us to conclude that when $G(a) \neq 0$, $P_a(X)$ has a zero (equivalently, exactly two zeros) in $\mathbb{F}_Q$ if and only if $mH = 0$ and $\frac{k}{d}H = 0$ which is equivalent to $H = 0$ since at least one of m and k/d must be odd as $\gcd(m, k/d) = 1$.

Combining the discussion above with Theorem 8 completes the proof. □

Remark 12. When $p = 2$, $A_r(X)$ defined in this paper coincides with $C_r(X)$ introduced in [14]. Many of our results for $p = 2$ appears also in [14] with relatively longer and more complicated proofs.

Remark 13. On the other hand, very recently, the number of roots of linearized and projective polynomials was studied in [7, 19]. In particular, criteria for which $P_a(X)$ has $0, 1, 2$ or p^d+1 roots were stated by Theorem 8 of [19] using some polynomial sequence $G_r(X)$ which are related by $A_r(X) = G_{r-1}(X)^q$ with $A_r(X)$ defined in this paper. Using the notation of our paper, Theorem 8 of [19] states that $N_a = p^d + 1$ if and only if $A_m(a) = 0$ and $A_{m+1}(a) \in \mathbb{F}_{p^d}$. Firstly, here, the condition $A_{m+1}(a) \in \mathbb{F}_{p^d}$ is surplus because this follows from the condition $A_m(a) = 0$. In fact, if $F(a) = A_m(a) = 0$ then by (1) $A_{m+1}(a) = (-aA_{m-1}(a)^q)^q$ and by (9) $G(a) = 0$ i.e. $A_{m+1}(a) = -aA_{m-1}(a)^q$, so $A_{m+1}(a) = A_{m+1}(a)^q$ that is $A_{m+1}(a) \in \mathbb{F}_q \cap \mathbb{F}_Q = \mathbb{F}_{p^d}$.

Secondly, when $p = 2$, the criteria for $N_a = 0, 1, 2$ in [19] are false. In the criteria for $N_a = 0, 1, 2$ of Theorem 8 of [19], $G_n \in \mathbb{F}_q$ or $G_n \notin \mathbb{F}_q$ must be fixed

by $G_n + {G_n}^{\sigma} + {G_{n-1}}^{\sigma} = 0$ or $G_n + {G_n}^{\sigma} + {G_{n-1}}^{\sigma} \neq 0$ respectively. Note that the quantity $G_n + {G_n}^{\sigma} + {G_{n-1}}^{\sigma}$ (Δ_L for p odd, resp.) therein equals $G(a)^{\frac{1}{q}}$ ($E(a)^{\frac{1}{q}}$ for p odd, resp.) with the notation of our paper.

6 More for the case $N_a = p^d + 1$

Let $S_a = \{x \in \mathbb{F}_{p^{md}} = \mathbb{F}_Q \mid P_a(x) = 0\}$. The following problem remained : when $N_a = p^d + 1$ i.e. $A_m(a) = 0$, express S_a explicitly in terms of a.
For this problem, the following facts are the only things we know at the moment.

1. When $m = 3$ and $A_3(a) = 1 - a^q = 0$ i.e. $a = 1$, we have
$$S_a = \{(b - b^q)^{q-1}, b \in \mathbb{F}_{p^{3d}} \setminus \mathbb{F}_{p^d}\}.$$
2. When $p = 2$, $m = 4$ and $A_4(a) = 1 + a^q + a^{q^2} = 0$, we have
$$\sqrt{a} \in S_a.$$
3. When $p = 2$, $m = 5$ and $A_5(a) = 1 + a^q + a^{q^2} + a^{q^3}(1 + a^q) = 0$, we have
$$\frac{a(a + a^q)}{1 + a^q + a^{q+1}} \in S_a.$$
4. When $p = 2$, $m = 6$ and $A_6(a) = 1+a^q+a^{q^2}+a^{q^3}(1+a^q)+a^{q^4}(1+a^q+a^{q^2}) = 0$, we have
$$\sqrt{\frac{a^2(1 + a + a^q + a^{q^2+1}) + a^{q^2+q+1}(1 + a + a^q)^q}{a^{2q^2+q} + (1 + a + a^q)(1 + a^2 + a^q)^q}} \in S_a.$$

All these can be checked by direct substitutions to $P_a(X)$.

Lemma 14. *If $x^{q+1} + x + a = 0$ for $a \in \mathbb{F}_Q^*$, then for any $r \geq 1$*
$$x^{q^r} = \frac{A_{r+1}(a)x - aA_r(a)^q}{A_r(a)x - aA_{r-1}(a)^q}, \tag{16}$$
where the denominator never equals zero.

Proof. This is an alternation of (6). The only thing to be verified is the fact that the denominator never equals zero. In fact, if $A_r(a)x - aA_{r-1}(a)^q = 0$ (and so also $A_{r+1}(a)x - aA_r(a)^q = 0$ by (6)), then $x = \frac{aA_{r-1}(a)^q}{A_r(a)} = \frac{aA_r(a)^q}{A_{r+1}(a)}$ and thus it follows that $a(A_r(a)^{q+1} - A_{r-1}(a)^q A_{r+1}(a)) = 0$. But (3) shows $a(A_r(a)^{q+1} - A_{r-1}(a)^q A_{r+1}(a)) = a^{\frac{q^r-1}{q-1}} \neq 0$, a contradiction. □

Lemma 15. *If $A_m(a) = 0$, then for any $x \in \mathbb{F}_Q$ such that $x^{q+1} + x + a = 0$, it holds*
$$\mathrm{Nr}_k^{km}(x) = A_{m+1}(a).$$
Furthermore, for any $t \geq 0$
$$A_{m+t}(a) = A_{m+1}(a) \cdot A_t(a).$$

Proof. By Proposition 3 and the premise $A_m(a) = 0$, we have $a \in \mathbb{F}_{q^m}$. By multiplying all equalities (16) for r ranging from 1 to $m-1$ side by side we get $x^{\frac{q^m-1}{q-1}} = -aA_{m-1}(a)^q = A_{m+1}(a)^{1/q}$, i.e. $A_{m+1}(a) = \mathrm{Nr}_k^{km}(x)^q = \mathrm{Nr}_k^{km}(x) \in \mathbb{F}_q$. Then, an induction on t leads to the conclusion of the lemma. □

7 Conclusions

We studied the equation $P_a(X) = X^{p^k+1} + X + a = 0, a \in \mathbb{F}_{p^n}$ and proved some new criteria for the number of the $\mathbb{F}_{p^n}$-zeros of $P_a(x)$. In case of one or two $\mathbb{F}_{p^n}$-zeros, we expressed these zeros in terms of a. For the case of $p^{\gcd(n,k)}+1$ rational zeros, we provided a parametrization of such a's and expressed all the $p^{\gcd(n,k)}+1$ rational zeros by using this parametrization. An important open problem is to explicitly express in terms of a the $\mathbb{F}_{p^n}$-zeros when there are $p^{\gcd(n,k)}+1$ zeros in $\mathbb{F}_{p^n}$.

Acknowledgement

The authors deeply thank the Assoc. Edit. and the anonymous reviewers for their valuable comments which have highly improved the quality and the presentation of the paper.

References

1. S.S. Abhyankar. Projective polynomials, *Proc. Am. Math. Soc.*, 125 : 1643–1650, 1997.
2. S.S. Abhyankar, S.D. Cohen, and M.E. Zieve. Bivariate factorizations connecting Dickson polynomials and Galois theory. *Transactions of the American Mathematical Society*, 352(6) : 2871 – 2887, 2000.
3. A.W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3) : 285 – 305, 2004.
4. A.W. Bluher. A New Identity of Dickson Polynomials. *ArXiv:1610.05853 [math.NT]*, 2016.
5. C. Bracken, T. Helleseth. Triple-error-correcting BCH-like codes. in: *IEEE Int. Symp. Inf. Theory*, 2009, pp. 1723 – 1725.
6. 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.
7. B. Csajbók, G. Marino, O. Polverino, and F. Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56 : 109 – 130, 2019.
8. J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields Appl.*, 10 : 342 – 389, 2004.
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. J. von zur Gathen, M. Giesbrecht, K. Ziegler. Composition collisions and projective polynomials, in: ISSAC, 2010, 123–130.
11. F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel. On the function field sieve and the impact of higher splitting probabilities : application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$. *R. Canetti and J.A. Garay (Eds.): CRYPTO 2013, Part II*, LNCS 8043, 109–128, 2013.
12. F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel. Solving a 6120-bit DLP on a desktop computer. *Cryptology ePrint Archive 2013/306*
13. T. Helleseth, and A. Kholosha. On the equation $x^{2^l+1}+x+a$ over $GF(2^k)$. *Finite Fields and Their Applications*, 14(1) : 159–176, 2008.
14. T. Helleseth, and A. Kholosha. $x^{2^l+1}+x+a$ and related affine polynomials over $GF(2^k)$. *Cryptogr. Commun.*, 2 : 85 – 109, 2010.
15. 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) : 2236 – 2245, 2007.
16. K.H. Kim, S. Mesnager. Solving $x^{2^k+1}+x+a=0$ in $\mathbb{F}_{2^n}$ with $\gcd(n,k)=1$. *Finite Fields and Their Applications*, 63 : ? – ?, 2020. https://doi.org/10.1016/j.ffa.2019.101630
17. R. Lidl, H. Niederreiter. Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
18. M. Massierer. Some experiments investigating a possible $L(1/4)$ algorithm for the discrete logarithm problem in algebraic curves. *Cryptology ePrint Archive 2014/996*
19. G. McGuire and J. Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57 : 68 – 91, 2019.
20. S. Mesnager, K.H. Kim, J.H. Choe, D.N. Lee and D.S. Go. Solving $x+x^{2^l}+\cdots+x^{2^{ml}}=a$ over $\mathbb{F}_{2^n}$. *Cryptogr. Commun.*, 12(4) : 809-817, 2020.