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

[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 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 [8], determining cross-correlation between m-sequences [11, 14] and to construct error-correcting codes [4], as well as to speed up the index calculus method for computing discrete logarithms on finite fields [12, 13] and on algebraic curves [21].

Subsequently, in [2, 16, 17, 5, 3, 15, 7, 22], 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 [16, 17, 5, 15, 22]. 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 $\gcd(n, k) = 1$ [15].

We discuss this equation without any restriction on p and $\gcd(n, k)$. New 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. 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 · Müller-Cohen-Matthews (MCM) polynomial · Dickson polynomial · Zeros of a polynomial · Irreducible polynomial.

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

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

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 [8], determining cross-correlation between m-sequences [11, 14] and to construct error-correcting codes [4]. 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 [12, 13] and on algebraic curves [21].

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 $p^d + 1$ 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 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 [16, 17] 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 [17]. 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. Very recently, Kim and Mesnager [15] 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 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 $p^d + 1$ 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 [22] for any characteristic.

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, new 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 that parametrization, all the $p^{\gcd(n,k)}+1$ rational zeros are also 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 further presented in Section 6. Finally, we conclude in Section 7.

2 Preliminaries

Given positive integers k and l, define a 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 $Tr_1^l(x)$ of x. The zeros of this polynomial are studied in [?]. In particular, we need the following.

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} can not have a kernel of greater cardinality than its degree $p^{k(r-1)}$. $\square$

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

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

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 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

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

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 $u \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2}$. $\square$

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

Letting $m = n/d$, define 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 4. *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 $r \geq 1$. Raising $q-$th power to both sides of (6) and substituting (5), we have

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

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. $\square$

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 5. *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

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

By the way, since

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

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:

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

□

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

Proposition 6. *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 $H = Tr_1^d\left(\frac{Nr_d^n(a)}{G^2(a)}\right)$. The followings hold.*

1.

$$Tr_1^n(E) = mH. \tag{10}$$

2.

$$T_k(E) = \frac{G(a) + F(a)^q}{G(a)} + \frac{k}{d}H. \tag{11}$$

Proof. Regarding the fact that $Nr_k^{mk}(a) = Nr_d^n(a)$ as $a \in \mathbb{F}_Q$, we have

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

Hence, immediately (10) follows from the facts $Nr_d^n(a) \in \mathbb{F}_{p^d}$ and $G(a) \in \mathbb{F}_{p^{md}} \cap \mathbb{F}_{p^k} = \mathbb{F}_{p^d}$ (which follows from (13) as $a \in \mathbb{F}_{p^{md}}$). And also

$$\begin{aligned}
T_k(E) &= \frac{A_{m+1}(a)}{G(a)} + \left(\frac{A_{m+1}(a)}{G(a)}\right)^q + \frac{k}{d}H \overset{(13)}{=} \frac{A_{m+1}(a) + A_{m+1}(a)^q}{G(a)} + \frac{k}{d}H \\
&= \frac{G(a) + aA_{m-1}(a)^q + A_{m+1}(a)^q}{G(a)} + \frac{k}{d}H \\
&\overset{(2)}{=} \frac{G(a) + aA_{m-1}(a)^q + \left(A_m(a) + a^{q^{m-1}} A_{m-1}(a)\right)^q}{G(a)} + \frac{k}{d}H \\
&= \frac{G(a) + F(a)^q}{G(a)} + \frac{k}{d}H.
\end{aligned}$$

□

5 Rational zeros of $P_a(X)$

By exploiting the results of previous sections, now we can completely solve the equation $P_a(X) = 0$ in arbitrary finite fields.

5.1 $N_a = p^d + 1$

Lemma 7. *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 $\Longleftrightarrow$ 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

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

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

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

Thus $P_a(X)$ splits in $\mathbb{F}_{q^m}$. Corollary 7.2 of [2] states that $P_a(X)$ splits in $\mathbb{F}_{q^m}$ if and only if $P_a(X)$ has exactly $p^d + 1$ zeros in $\mathbb{F}_Q$.

(Item 1 $\iff$ Item 3)

To begin with, define $S_0 = \mathbb{F}_Q \setminus \mathbb{F}_{q^2}$, $S_1 = \{v \in \mathbb{F}_Q \setminus \mathbb{F}_q \mid Tr^n_d(v) = 0\}$, $S_2 = \{v^{q-1} \mid v \in S_1\}$ 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 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 $\varphi_1 : u \in S_0 \longmapsto u - u^q \in S_1$, $\varphi_2 : v \in S_1 \longmapsto v^{q-1} \in S_2$, $\varphi_3 : w \in S_2 \longmapsto \frac{w^q}{(1+w)^{q+1}} \in S$.

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, consider 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 $Tr^n_d(\beta v_1) = \beta Tr^n_d(v_1) = 0$. 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 Theorem 5.6 of [2], 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. $\square$

5.2 $N_a \leq 2$: Odd p

Theorem 8. *Let p be odd. Let $a \in \mathbb{F}_Q$ and $E = G(a)^2 - 4aF(a)^{q+1}$.*

1. *$N_a = 1$ 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 $-\frac{G(a)}{2F(a)}$.*
2. *$N_a = 0$ if and only if E is not a quadratic residue in $\mathbb{F}_{p^d}$ (i.e. $E^{\frac{p^d-1}{2}} \neq 0, 1$).*
3. *$N_a = 2$ if and only if E 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 $x_{1,2} = \frac{\pm E^{\frac{1}{2}} - G(a)}{2F(a)}$, where $E^{\frac{1}{2}}$ represents a quadratic root in $\mathbb{F}_{p^d}$ of E.*

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

Assume $F(a) \neq 0$. Then the equation (4) can be rewritten as

$$\left(x + \frac{G(a)}{2F(a)}\right)^2 = \frac{E}{4F(a)^2}. \tag{12}$$

Now, we will show that the solutions $x_{1,2} = \frac{\pm E^{\frac{1}{2}} - G(a)}{2F(a)}$ of (12) become the zeros of $P_a(X)$ if and only if E is a quadratic residue in $\mathbb{F}_q$. In fact, letting $\left(E^{\frac{1}{2}}\right)^q = E^{\frac{1}{2}} + \delta$, we have

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

and so $P_a(x_{1,2}) = 0$ if and only if $\delta = 0$, that is, $E^{\frac{1}{2}} \in \mathbb{F}_q$. On the other hand, $x_{1,2} \in \mathbb{F}_Q$ if and only if $E^{\frac{1}{2}} \in \mathbb{F}_Q$. Combining above discussion with Lemma 7 completes the proof. $\square$

Remark 9. In the last two cases of Theorem 8 (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 $E = 0$.

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

When $p = 2$, Item 1 and 2 of Proposition 5 are reduced to

$$G(x) \in \mathbb{F}_q \text{ for any } x \in \mathbb{F}_{q^m}. \tag{13}$$

Theorem 10. *Let $p = 2$ and $a \in \mathbb{F}_Q$. Let $H = Tr_1^d\left(\frac{Nr_d^n(a)}{G^2(a)}\right)$ and $E = \frac{aF(a)^{q+1}}{G^2(a)}$.*

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 $\zeta \in \mu_{Q+1} \setminus \{1\}$.*

Proof. Let assume $F(a) \neq 0$. If $G(a) = 0$, then the equation (4) has 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 $\left(\frac{F(a)}{G(a)}x\right)^2 + \frac{F(a)}{G(a)}x = E$ and so it has a solution in $\mathbb{F}_Q$ if and only if

$$Tr_1^n(E) = 0. \tag{14}$$

In case of existence of solution, (4) has exactly two solutions x_1 and x_2 in $\mathbb{F}_Q$. Indeed, $\left(\frac{F(a)}{G(a)}x_1\right)^2 + \frac{F(a)}{G(a)}x_1 = \left(\frac{F(a)}{G(a)}x_2\right)^2 + \frac{F(a)}{G(a)}x_2 = T_n\left(\frac{E}{\zeta+1}\right)^2 + T_n\left(\frac{E}{\zeta+1}\right) = \left(\frac{E}{\zeta+1}\right)^Q + \left(\frac{E}{\zeta+1}\right) = E(\frac{1}{\frac{1}{\zeta}+1} + \frac{1}{\zeta+1}) = E$, 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 $T_n\left(\frac{E}{\zeta+1}\right)^Q + T_n\left(\frac{E}{\zeta+1}\right) = T_n(E) = Tr_1^n(E) \overset{(14)}{=} 0$ i.e. $T_n\left(\frac{E}{\zeta+1}\right) \in \mathbb{F}_Q$.

Let x be a solution of (4). Then we have $T_k\left(\left(\frac{F(a)}{G(a)}x\right)^2 + \frac{F(a)}{G(a)}x\right) = T_k(E)$, i.e. $\left(\frac{F(a)}{G(a)}x\right)^q + \frac{F(a)}{G(a)}x = T_k(E)$, hence $x^q = \left(\frac{G(a)}{F(a)}\right)^q\left(\frac{F(a)}{G(a)}x + T_k(E)\right) \overset{(13)}{=} \frac{F(a)x+G(a)T_k(E)}{F(a)^q}$ and $P_a(x) = x(x^q+1) + a = \frac{x(F(a)x+G(a)T_k(E)+F(a)^q)}{F(a)^q} + a \overset{(4)}{=} \frac{x(G(a)T_k(E)+F(a)^q+G(a))}{F(a)^q}$.

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

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

Equalities (10), (11), (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 $mH = \frac{k}{d}H = 0$ 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 above discussion with Lemma 7 completes the proof. □

Remark 11. When $p = 2$, $A_r(X)$ defined in this paper coincides with $C_r(X)$ introduced in [17]. Many of our results specific to $p = 2$ also appears in [17] with relatively longer and complicate proof.

Remark 12. On the other hand, very recently, the number of roots of linearized and projective polynomials was studied in [7, 22]. In particular, criteria for which $P_a(X)$ has 0, 1, 2 or $p^d + 1$ roots were stated by Theorem 8 of [22] 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 notations of our paper, Theorem 8 of [22] states that $N_a = p^d + 1$ if and only if $A_m(a) = 0$ and $A_{m+1}(a) \in \mathbb{F}_{p^d}$. As the first note, 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 $A_{m+1}(a) \in \mathbb{F}_q \cap \mathbb{F}_Q = \mathbb{F}_{p^d}$.

As the second note, when $p = 2$, the criteria for $N_a = 0, 1, 2$ in [22] are false. In the criteria for $N_a = 0, 1, 2$ of Theorem 8 of [22], $G_n \in \mathbb{F}_q$ 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 $G(a)^{\frac{1}{q}}$ ($E^{\frac{1}{q}}$ for p odd, resp.) in 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 is 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 13. *If $x^{q+1} + x + a = 0$ for $a \in \mathbb{F}_Q^*$, then for any $r \geq 0$*
$$x^{q^r} = \frac{A_{r+1}(a)x - aA_r(a)^q}{A_r(a)x - aA_{r-1}(a)^q}, \tag{16}$$
where the denominator never equal zero.

Proof. This is an alternation of (6). Only thing to be verified is the fact that the denominator never equal 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 $a(A_r(a)^{q+1} - A_{r-1}(a)^q A_{r+1}(a)) = 0$. But (3) shows $a(A_r(a)^{q+1} - A_{r-1}(a)^q A_{r+1}(a)) = a^{\frac{q^r-1}{q-1}} \neq 0$ i.e. a contradiction. □

Lemma 14. *If $A_m(a) = 0$, then for any $x \in \mathbb{F}_Q$ such that $x^{q+1} + x + a = 0$, it holds*
$$Nr_k^{km}(x) = A_{m+1}(a).$$
Furthermore, for any $t \geq 0$
$$A_{m+t}(a) = A_{m+1}(a) \cdot A_t(a).$$

Proof. By 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. $A_{m+1}(a) = Nr_k^{km}(x)^q = Nr_k^{km}(x) \in \mathbb{F}_q$. 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 $P_a(x)$. For the cases of one or two $\mathbb{F}_{p^n}$-zeros, we provided explicit expressions for these rational 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 remaining problem is whether for any given p, n, k, in the case of $p^{\gcd(n,k)}+1$ rational zeros, it is always possible to explicitly express these $p^{\gcd(n,k)}+1$ rational zeros in terms of a.

References

1. 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.
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. *ArXiv:1610.05853 [math.NT]*, 2016.
4. C. Bracken, T. Helleseth. Triple-error-correcting BCH-like codes. in: *IEEE Int. Symp. Inf. Theory*, 2009, pp. 1723 – 1725.
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 and R. W. Matthews. A class of exceptional polynomials. *Transactions of the American Mathematical Society*, 345(2):897 – 909, 1994.
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. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45:1271 – 1275, 1999.
10. H. Dobbertin. Kasami power functions, permutation polynomials and cyclic difference sets. in: A. Pott, P.V. Kumar, T. Helleseth, D. Jungnickel (Eds.), Difference Sets, Sequences and their Correlation Properties, Proceedings of the NATO Advanced Study Institute on Difference Sets, Sequences and their Correlation Properties, Bad Windsheim, 2-14 August 1998, Kluwer, Dordrecht, 1999, pp. 133– 158.
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. 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.
13. F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel. Solving a 6120-bit DLP on a desktop computer. *Cryptology ePrint Archive 2013/306*
14. 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.
15. K.H. Kim, S. Mesnager. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$. *Cryptology ePrint Archive 2019/307* (Accepted for publication in the Journal 'Finite Fields and Their Applications").
16. 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.
17. 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.
18. 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.
19. T. Helleseth and V. Zinoviev. Codes with the same coset weight distributions as the Z_4-linear Goethals codes. *IEEE Trans. Inform. Theory*, 47(4): 1589 – 1595, 2001.
20. R. Lidl, G.L. Mullen and G. Turnwald. *Dickson Polynomials*, Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Addison-Wesley, Reading, MA 1993.
21. M. Massierer. Some experiments investigating a possible $L(1/4)$ algorithm for the discrete logarithm problem in algebraic curves. *Cryptology ePrint Archive 2014/996*
22. 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.