Cryptography and Communications (2020) 12:809–817
https://doi.org/10.1007/s12095-020-00425-3

Solving $x + x^{2^l} + \cdots + x^{2^{ml}} = a$ over $\mathbb{F}_{2^n}$

Sihem Mesnager[1,2,3] · Kwang Ho Kim[4,5] · Jong Hyok Choe[4] · Dok Nam Lee[4] · Dae Song Go[6]

Received: 20 August 2019 / Accepted: 26 January 2020 / Published online: 11 February 2020

Abstract

This paper presents an explicit representation for the solutions of the equation $\sum_{i=0}^{\frac{k}{l}-1} x^{2^{li}} = a \in \mathbb{F}_{2^n}$ for any given positive integers k, l with $l|k$ and n, in the closed field $\overline{\mathbb{F}_2}$ and in the finite field $\mathbb{F}_{2^n}$. As a by-product of our study, we are able to completely characterize the a's for which this equation has solutions in $\mathbb{F}_{2^n}$.

Keywords Linear equation · Binary finite field · Zeros of polynomials · Linearized polynomial

Mathematics Subject Classification 2010 11D04 · 12E05 · 12E12

1 Introduction

Solving equations over the binary finite field $\mathbb{F}_{2^n}$ is of high importance. In particular, those involving the trace functions are crucial in many contexts in the framework of Boolean and vectorial functions for symmetric cryptography and error-correcting codes [2, 3].

✉ Sihem Mesnager
smesnager@univ-paris8.fr

Kwang Ho Kim
khk.cryptech@gmail.com

[1] Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France

[2] University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cité, 93430, Villetaneuse, France

[3] Telecom ParisTech, Palaiseau 91120, France

[4] Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People's Republic of Korea

[5] PGItech Corp., Pyongyang, Democratic People's Republic of Korea

[6] Master School, University of Natural Science, Pyongyang, Democratic People's Republic of Korea

Let $\overline{\mathbb{F}_2}$ be the algebraic closure of $\mathbb{F}_2$. Let n be any positive integer and k and l be positive integers such that $l|k$. In this paper, we discuss the sets of the solutions of the affine equation:

$$T_l^k(x) := \sum_{i=0}^{\frac{k}{l}-1} x^{2^{li}} = a \in \mathbb{F}_{2^n}, \tag{1}$$

in $\overline{\mathbb{F}_2}$ and in the finite field $\mathbb{F}_{2^n}$. When $l = 1$, we shall simply write T_k instead of T_1^k.

Such an equation has no multiple roots since its derivative is a non-zero constant polynomial. Linearized polynomials T_l^k induce a linear map between fields viewed as vectorspaces over $\mathbb{F}_2$. Therefore, the set of preimages of $a \in \mathbb{F}_{2^n}$ under T_l^k is a coset of the kernel of T_l^k. Despite this fact is well-known, no explicit representations for such preimage sets can be found in the literature except the quadratic equation $x^2 + x = a$ [1, 4]. In this paper, we shall provide an explicit representation for the solutions of (1) in $\overline{\mathbb{F}_2}$ as well as in $\mathbb{F}_{2^n}$ for any $n \geq 1$.

This paper is organized as follows. In Section 2, we state some properties about the linearized polynomials involved in (1). Next, in Section 3, we study the solutions of (1). To this end, we exploit the linearity to divide our study into two steps. Firstly, we identify the zeros of the linearized polynomials T_l^k in the algebraic closure and next in the given finite field (Propositions 2 and 3). Secondly, in Section 3.2, we explicit all the solutions in the algebraic closure $\overline{\mathbb{F}_2}$ (Theorems 2 and 3). At this stage, the key step is to explicit particular solutions of (1) (Lemmas 2 and 3). Finally, We identify in Section 3.3 all the solutions that lies in a given finite field (Theorems 5 and 7). As a by-product of our study, we are able to completely characterize when (1) has solutions in a given finite field (Theorems 4 and 6).

2 Preliminaries

Throughout this paper, we maintain the following notation.

- n is a positive integer.
- a is any element of the finite field $\mathbb{F}_{2^n}$.
- k and l are positive integers such that $l|k$.
- L is any common multiple of n and k.
- We denote the greatest common divisor and the lowest common multiple of two positive integers u and v by (u, v) and $[u, v]$, respectively.
- $d = (n, k)$.
- Given a positive integer m, we denote by μ_{2^m+1} the multiplicative group of $\overline{\mathbb{F}_2}$ of order $2^m + 1 : \mu_{2^m+1} = \{\zeta \in \overline{\mathbb{F}_2} \mid \zeta^{2^m+1} = 1\} \subset \mathbb{F}_{2^{2m}}$.

To begin with, we present several results that should help us in our study of the solutions of (1). First of all, note that T_l^k restricted to $\mathbb{F}_{2^k}$ is the trace map Tr_l^k, that is, $T_l^k(x) = Tr_l^k(x)$ when $x \in \mathbb{F}_{2^k}$. We now present some properties about the linearized polynomials T_l^k.

Proposition 1 *Let k, l, k', l', m be positive integers such that $l \mid k$, $l' \mid k'$ and $m \mid l$. Then, the followings hold true:*

1. $T_l^k \circ T_{l'}^{k'} = T_{l'}^{k'} \circ T_l^k$.
2. $T_m^l \circ T_l^k = T_m^k$.

Lemma 1 *The followings hold true:*

1. *For any $x \in \mathbb{F}_{2^k}$, $T_l^k(x) \in \mathbb{F}_{2^l}$. Furthermore, $T_l^k(\mathbb{F}_{2^k}) = \mathbb{F}_{2^l}$.*
2. *$T_k \circ T_2(x) = T_k^{2k}(x) = x + x^{2^k}$ for any $x \in \overline{\mathbb{F}_2}$.*
3. *For any $x \in \mathbb{F}_{2^l}$,*
$$T_l^k(x) = \begin{cases} x & \textit{if } \frac{k}{l} \textit{ is odd,} \\ 0 & \textit{if } \frac{k}{l} \textit{ is even.} \end{cases}$$
4. *For any $x \in \mathbb{F}_{2^n}$, $T^n_{(n,k)}(x) = T_k^{[n,k]}(x)$.*

Proof The first three statements are obtained by straightforward calculations. Hence, we give a proof only for the last statement.

Since $nk = [n,k](n,k)$, we have $\frac{n}{(n,k)} = \frac{[n,k]}{k}$. Furthermore, one has $\{j(n,k) \mod n \mid 0 \leq j \leq \frac{n}{(n,k)} - 1\} = \left\{ik \mod n \mid 0 \leq i \leq \frac{[n,k]}{k} - 1\right\}$ because n divides ik if and only if i is a multiple of $n/(n,k) = [n,k]/k$. □

3 On the solutions of (1)

We shall often view the algebraic closure $\overline{\mathbb{F}_2}$ and any finite field $\mathbb{F}_{2^m}$, $m \geq 1$, as vectorspaces over $\mathbb{F}_2$ and the linearized polynomials involved in (1) as linear maps between the vectorspaces over $\mathbb{F}_2$. Given a finite dimensional subspace E of the linear space $\overline{\mathbb{F}_2}$ over $\mathbb{F}_2$, $\dim(E)$ denotes its dimension over $\mathbb{F}_2$. Let us now recall some well-known facts in linear algebra that we shall use in the sequel. Let f be a linear map of $\overline{\mathbb{F}_2}$ to itself. Then

$$\dim f(E) = \dim(E) - \dim(\ker(f) \cap E)$$

and

$$\dim f^{-1}(E) = \dim(E \cap \operatorname{Im}(f)) + \dim(\ker(f)),$$

where $\operatorname{Im}(f) := \{f(x) \mid x \in \overline{\mathbb{F}_2}\}$ denotes the range of f and $\ker(f) := \{x \in \overline{\mathbb{F}_2} \mid f(x) = 0\}$ denotes the kernel of f.

3.1 On the zeros of T_l^k

The zeros of the linearized polynomials T_l^k are the zeros of the trace map Tr_l^k, that is, T_l^k has no zeros outside $\mathbb{F}_{2^k}$. Indeed, the number of the zeros of the linearized polynomial T_l^k is equal to 2^{k-l} since its degree is 2^{k-l} which is exactly the number of the zeros of Tr_l^k. Therefore,

$$\left\{x \in \overline{\mathbb{F}_2} \mid T_l^k(x) = 0\right\} = \left\{x \in \mathbb{F}_{2^k} \mid Tr_l^k k(x) = 0\right\}. \tag{2}$$

Now, it is well-known that $Tr_l^k k(x) = 0$ with $x \in \mathbb{F}_{2^k}$ is equivalent to $x = y + y^{2^l} = T_l^{2l}(y)$ for some $y \in \mathbb{F}_{2^k}$ (see for instance [4]). Hence, according to Item 2 of Lemma 1, it follows

Proposition 2 $\left\{x \in \overline{\mathbb{F}_2} \mid T_l^k(x) = 0\right\} = T_l \circ T_2(\mathbb{F}_{2^k})$.

Let us now study the zeros of T_l^k lying in the finite field $\mathbb{F}_{2^n}$. We deduce from (2) that

$$\{x \in \mathbb{F}_{2^n} \mid T_l^k(x) = 0\} = \{x \in \mathbb{F}_{2^k} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^d} \mid Tr_l^k k(x) = 0\}. \tag{3}$$

Next, observe that, since $l|[d,l]|k$, for any $x \in \mathbb{F}_{2^d} \subset \mathbb{F}_{2^{[d,l]}}$,

$$Tr_l^k k(x) = T_l^k(x) = T_l^{[d,l]}\left(T_{[d,l]}^k(x)\right) = \begin{cases} T_l^{[d,l]}(x) & \text{if } \frac{k}{[d,l]} \text{ is odd,} \\ 0 & \text{if } \frac{k}{[d,l]} \text{ is even} \end{cases} \tag{4}$$

by Item 2 of Proposition 1 and Item 3 of Lemma 1. On the other hand, by Item 4 of Lemma 1, one has $T_l^{[d,l]}(x) = T_{(d,l)}^d(x)$ for any $x \in \mathbb{F}_{2^d}$ and

$$\{x \in \mathbb{F}_{2^d} \mid T_{(d,l)}^d(x) = 0\} = \left\{y + y^{2^{(d,l)}} \mid y \in \mathbb{F}_{2^d}\right\} = T_{(d,l)}^{2(d,l)}\left(\mathbb{F}_{2^d}\right) = T_2 \circ T_{(d,l)}\left(\mathbb{F}_{2^d}\right).$$

Therefore, one has

Proposition 3

$$\ker(T_l^k) \cap \mathbb{F}_{2^n} = \{x \in \mathbb{F}_{2^n} \mid T_l^k(x) = 0\} = \begin{cases} T_2 \circ T_{(d,l)}\left(\mathbb{F}_{2^d}\right) & \textit{if } \frac{k}{[d,l]} \textit{ is odd,} \\ \mathbb{F}_{2^d} & \textit{if } \frac{k}{[d,l]} \textit{ is even.} \end{cases}$$

Remark 1 When $l = 1$, the above proposition rewrites as

$$\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = \begin{cases} T_2\left(\mathbb{F}_{2^d}\right) & \text{if } \frac{k}{d} \text{ is odd,} \\ \mathbb{F}_{2^d} & \text{if } \frac{k}{d} \text{ is even.} \end{cases}$$

Remark 2 Proposition 3 states that

$$\dim\left(\ker(T_l^k) \cap \mathbb{F}_{2^n}\right) = \begin{cases} d - (d,l) & \text{if } \frac{k}{[d,l]} \text{ is odd,} \\ d & \text{if } \frac{k}{[d,l]} \text{ is even.} \end{cases}$$

Indeed, suppose that $\frac{k}{[d,l]}$ is odd. The dimension of the subspace $T_2 \circ T_{(d,l)}\left(\mathbb{F}_{2^d}\right)$ is equal to $\dim\left(T_{(d,l)}\left(\mathbb{F}_{2^d}\right)\right) - \dim\left(\ker T_2 \cap T_{(d,l)}\left(\mathbb{F}_{2^d}\right)\right) = \dim\left(T_{(d,l)}\left(\mathbb{F}_{2^d}\right)\right) - \dim\left(\mathbb{F}_2 \cap T_{(d,l)}\left(\mathbb{F}_{2^d}\right)\right)$. By Remark 1, $\dim(T_{(d,l)}\left(\mathbb{F}_{2^d}\right)) = \dim(\mathbb{F}_{2^d}) - \dim\left(T_2(\mathbb{F}_{2^{(d,l)}})\right) = d - ((d,l) - 1) = d - (d,l) + 1$. On the other hand, $T_{(d,l)}\left(\mathbb{F}_{2^d}\right)$ contains $\mathbb{F}_2$, yielding the result.

Example 1 When $k = 2l$, we can recover from Remark 2 the well-known result $\dim\left(\ker(T_l^{2l}) \cap \mathbb{F}_{2^n}\right) = (n,l)$. Indeed, one has

$$\dim\left(\ker(T_l^{2l}) \cap \mathbb{F}_{2^n}\right) = \begin{cases} (n,2l) - ((n,2l),l) = (n,2l) - (n,l) & \text{if } \frac{2l}{[(n,2l),l]} \text{ is odd,} \\ (n,2l) & \text{if } \frac{2l}{[(n,2l),l]} \text{ is even.} \end{cases}$$

Now, $[(n,2l),l] = \frac{(n,2l)l}{((n,2l),l)} = \frac{(n,2l)l}{(n,l)}$. Thus, if $(n,2l) = (n,l)$, then $\frac{2l}{[(n,2l),l]} = 2$ (i.e. even) and otherwise (i.e. $(n,2l) = 2(n,l)$) $\frac{2l}{[(n,2l),l]} = 1$.

Example 2 When $k = n$, that is, $d = n$, $(d,l) = l$ and $\frac{k}{[d,l]} = 1$, Remark 2 states that $\dim(\ker(T_l^n) \cap \mathbb{F}_{2^n}) = n - l$.

A direct consequence of Proposition 3 is:

Corollary 1 *T_l^k is a permutation of $\mathbb{F}_{2^n}$ if and only if $d|l$ and $\frac{k}{l}$ is odd. Hence, when $\frac{k}{l}$ is odd, $T_l^k(x)$ is an exceptional polynomial over $\mathbb{F}_2$.*

We can deduce the number of $\mathbb{F}_{2^n}$-solutions of (1) from Remark 2.

Theorem 1 *The number of the $\mathbb{F}_{2^n}$-solutions to* (1) *is* 2^d *if* $\frac{k}{[d,l]}$ *is even and* $2^{d-(d,l)}$ *if* $\frac{k}{[d,l]}$ *is odd.*

3.2 Solutions in the algebraic closure

In Section 3.1, we presented an explicit representation of the kernel of the linear map T_l^k on $\overline{\mathbb{F}_2}$. Therefore, in order to describe all the solutions of (1) in $\overline{\mathbb{F}_2}$, it suffices to find an explicit representation of a particular solution to (1). We begin with the case where $l = 1$ which contains the main idea.

Lemma 2 *Let* $\zeta \in \mu_{2^L+1} \setminus \{1\}$. *Set* $x_0 = T_k^L \circ T_2\left(\frac{a}{\zeta+1}\right)$. *Then* $T_k(x_0) = a$.

Proof By Item 2 of Proposition 1 and Item 2 of Lemma 1, one has

$$\begin{aligned} T_k(x_0) &= T_k\left(T_k^L\left(T_2\left(\frac{a}{\zeta+1}\right)\right)\right) \\ &= T_L\left(T_2\left(\frac{a}{\zeta+1}\right)\right) \\ &= \frac{a}{\zeta+1} + \left(\frac{a}{\zeta+1}\right)^{2^L} \\ &= \frac{a}{\zeta+1} + \frac{a}{1/\zeta+1} = a. \end{aligned}$$

In the last line, we have used the fact that $\zeta^{2^L} = 1/\zeta$. □

If x_1 are x_2 are two solutions of (1), then $x_1 + x_2$ is a zero of T_l^k. Hence, we deduce from Lemma 2 and Proposition 2 the following representation of the solutions to (1) when $l = 1$.

Theorem 2 *Let* $\zeta \in \mu_{2^L+1} \setminus \{1\}$. *Then, for any* $a \in \mathbb{F}_{2^n}$,

$$\{x \in \overline{\mathbb{F}_2} \mid T_k(x) = a\} = T_k^L \circ T_2\left(\frac{a}{\zeta+1}\right) + T_2(\mathbb{F}_{2^k}).$$

Using the fact $T_k = T_l \circ T_l^k$, the preceding result can be easily extended to find a particular solution to the equation $T_l^k(x) = a$.

Lemma 3 *Let* $\zeta \in \mu_{2^L+1} \setminus \{1\}$. *Set* $x_1 = T_l \circ T_k^L \circ T_2\left(\frac{a}{\zeta+1}\right)$. *Then* $T_l^k(x_1) = a$.

Proof By Lemma 2, $x_0 = T_k^L \circ T_2\left(\frac{a}{\zeta+1}\right)$ is a particular solution to $T_k(x) = a$. Then $x_1 = T_l(x_0)$ is a particular solution of $T_l^k(x) = a$ since $T_l^k(x_1) = T_l^k(T_l(x_0)) = T_l(T_l^k(x_0)) = T_k(x_0) = a$. □

We then deduce from Proposition 2 that

Theorem 3 *Let* $\zeta \in \mu_{2^L+1} \setminus \{1\}$. *Then, for any* $a \in \mathbb{F}_{2^n}$,

$$\{x \in \overline{\mathbb{F}_2} \mid T_l^k(x) = a\} = T_l \circ T_k^L \circ T_2\left(\frac{a}{\zeta+1}\right) + T_l \circ T_2(\mathbb{F}_{2^k}).$$

3.3 Solutions in a finite field

In this section, we study the solutions of (1) lying in $\mathbb{F}_{2^n}$. As in Section 3.2, we begin with the case $l = 1$ because it contains some ingredients of the general case and is more simple to study in the first stage. To this end, we have firstly to characterize the a's for which (1) has solutions in $\mathbb{F}_{2^n}$.

Theorem 4 *The equation $T_k(x) = a$ has a solution in $\mathbb{F}_{2^n}$ if and only if $T_2 \circ T_d^n(a) = 0$ when $\frac{k}{d}$ is odd and if and only if $T_d^n(a) = 0$ when $\frac{k}{d}$ is even.*

Proof Let $a \in T_k(\mathbb{F}_{2^n})$, that is, there exists $x \in \mathbb{F}_{2^n}$ such that $a = T_k(x)$. Then,

$$\begin{aligned} T_d^n(a) &= T_d^n(T_k(x)) = T_k(T_d^n(x)) = T_d(T_d^k(T_d^n(x))) \\ &= \begin{cases} T_d(T_d^n(x)) = T_n(x) & \text{if } \frac{k}{d} \text{ is odd,} \\ 0 & \text{if } \frac{k}{d} \text{ is even} \end{cases} \end{aligned}$$

by Lemma 1 and Proposition 1. Now, $T_2(T_n(x)) = T_n(T_2(x)) = 0$ for any $x \in \mathbb{F}_{2^n}$ according to Proposition 1 and Item 2 of Lemma 1. This proves that $T_k(\mathbb{F}_{2^n}) \subset \ker(T_2 \circ T_d^n) \cap \mathbb{F}_{2^n}$ if $\frac{k}{d}$ is odd and $T_k(\mathbb{F}_{2^n}) \subset \ker(T_d^n)$ if $\frac{k}{d}$ is even.

Suppose that $\frac{k}{d}$ is odd. Then T_k is a linear map from $\mathbb{F}_{2^n}$ to itself whose kernel is of dimension $d - 1$ according to Remark 2. Therefore, $T_k(\mathbb{F}_{2^n})$ is of dimension $n - (d - 1) = n - d + 1$ over $\mathbb{F}_2$. On the other hand,

$$\begin{aligned} \dim\left(\ker(T_2 \circ T_d^n) \cap \mathbb{F}_{2^n}\right) &= n - \dim(T_2 \circ T_d^n(\mathbb{F}_{2^n})) \\ &= n - \dim\left(T_d^n(\mathbb{F}_{2^n})\right) + \dim\left(\ker(T_2) \cap T_d^n(\mathbb{F}_{2^n})\right) \\ &= \dim\left(\ker(T_d^n) \cap \mathbb{F}_{2^n}\right) + 1 \\ &= (n - d) + 1. \end{aligned}$$

The third line follows from the fact that $\mathbb{F}_2 \subset T_d^n(\mathbb{F}_{2^n}) = \mathbb{F}_{2^d}$ and the last line follows from Remark 2. We therefore conclude that $T_k(\mathbb{F}_{2^n}) = \ker(T_2 \circ T_d^n) \cap \mathbb{F}_{2^n}$ if $\frac{k}{d}$ is odd (because they have the same dimension).

Suppose that $\frac{k}{d}$ is even. Then T_k is a linear map from $\mathbb{F}_{2^n}$ to itself whose kernel is of dimension d according to Remark 2. Therefore, $T_k(\mathbb{F}_{2^n})$ is of dimension $n - d$ which is exactly the dimension of the kernel of the restriction of T_d^n to $\mathbb{F}_{2^n}$. By the same arguments as in the odd case, we conclude that $T_k(\mathbb{F}_{2^n}) = \ker(T_d^n)$. □

We are now in position to state an explicit representation of the solutions to (1) in $\mathbb{F}_{2^n}$ when $l = 1$.

Theorem 5 *Let $\zeta \in \mu_{2^n+1} \setminus \{1\}$.*

1. *Let $\frac{k}{d}$ be odd. Suppose that $T_2 \circ T_d^n(a) = 0$. Then,*

$$\{x \in \mathbb{F}_{2^n} \mid T_k(x) = a\} = T_2 \circ T_k^{[n,k]}\left(\frac{a}{\zeta + 1}\right) + T_2\left(\mathbb{F}_{2^d}\right). \tag{5}$$

2. *Let $\frac{k}{d}$ be even. Suppose that $T_d^n(a) = 0$. Then,*

$$\{x \in \mathbb{F}_{2^n} \mid T_k(x) = a\} = T_2 \circ T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta + 1}\right) + \mathbb{F}_{2^d}. \tag{6}$$

Proof Firstly, suppose that $\frac{k}{d} = \frac{[n,k]}{n}$ is odd. Then, according to Lemma 2, $x_0 = T_2 \circ T_k^{[n,k]}\left(\frac{a}{\zeta+1}\right)$ is a solution to $T_k(x) = a$ since $\mu_{2^n+1} \subset \mu_{2^{[n,k]}+1}$. Let us now show that x_0 lies in $\mathbb{F}_{2^n}$:

$$\begin{aligned} x_0 + x_0^{2^n} &= T_n \circ T_2\left(T_2 \circ T_k^{[n,k]}\left(\frac{a}{\zeta+1}\right)\right) \\ &= T_2 \circ T_k^{[n,k]}\left(T_n \circ T_2\left(\frac{a}{\zeta+1}\right)\right) \\ &= T_2 \circ T_k^{[n,k]}\left(\frac{a}{\zeta+1} + \left(\frac{a}{\zeta+1}\right)^{2^n}\right) \\ &= T_2 \circ T_k^{[n,k]}\left(\frac{a}{\zeta+1} + \frac{a}{1/\zeta+1}\right) \\ &= T_2 \circ T_k^{[n,k]}(a) = T_2 \circ T_d^n(a) = 0. \end{aligned}$$

Since $\frac{k}{d}$ is odd, (5) follows then from Proposition 3 (because the set of solutions to $T_k(x) = a$ is the affine subspace $x_0 + \ker(T_k) \cap \mathbb{F}_{2^n}$).

Suppose that $\frac{k}{d}$ is even. Observe that in this case $\frac{n-k}{d} = \frac{n}{d} - \frac{k}{d}$ is odd since $(\frac{n}{d}, \frac{k}{d}) = 1$. Furthermore, the equation $x^{2^{n-k}} + x = a^{2^{n-k}}$ has the same $\mathbb{F}_{2^n}$-solutions as the equation $x^{2^k} + x = a$. Therefore, it can be shown that $y_0 = T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta+1}\right)$ is a particular $\mathbb{F}_{2^n}$-solution to $T_k^{2k}(x) = a$. Thus, $x_0 = T_2(y_0) = T_2 \circ T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta+1}\right)$ is a particular $\mathbb{F}_{2^n}$-solution to $T_k(x) = a$ since $T_k(x_0) = T_k \circ T_2(y_0) = T_k^{2k}(y_0) = a$. Equation (6) follows then from Proposition 3. □

Now, we will consider the general case. Following the case when $l = 1$, we begin with characterizing all the a's for which (1) has solutions in $\mathbb{F}_{2^n}$.

Theorem 6 *The equation $T_l^k(x) = a$ has a solution in $\mathbb{F}_{2^n}$ if and only if $T_{(d,l)} \circ T_2 \circ T_d^n(a) = 0$ when $\frac{k}{[d,l]}$ is odd and if and only if $T_d^n(a) = 0$ when $\frac{k}{[d,l]}$ is even.*

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

$$\begin{aligned} T_d^n \circ T_l^k(x) &= T_l^k \circ T_d^n(x) \\ &= T_l^{[d,l]}\left(T_{[d,l]}^k\left(T_d^n(x)\right)\right) \\ &= \begin{cases} T_l^{[d,l]}\left(T_d^n(x)\right) = T_{(d,l)}^d(T_d^n(x)) = T_{(d,l)}^n(x) & \text{if } \frac{k}{[d,l]} \text{ is odd,} \\ 0 & \text{if } \frac{k}{[d,l]} \text{ is even} \end{cases} \end{aligned}$$

and $T_{(d,l)} \circ T_2 \circ T_{(d,l)}^n(x)) = T_2 \circ T_n(x) = 0$. Therefore, it follows that $T_l^k(\mathbb{F}_{2^n}) \subset \ker(T_{(d,l)} \circ T_2 \circ T_d^n) \cap \mathbb{F}_{2^n}$ when $\frac{k}{[d,l]}$ is odd and that $T_l^k(\mathbb{F}_{2^n}) \subset \ker(T_d^n) \cap \mathbb{F}_{2^n}$ when $\frac{k}{[d,l]}$ is even. Now, we will show that the dimensions of the subspaces involved in these inclusion relations are equal.

According to Remark 2, $T_l^k(\mathbb{F}_{2^n})$ is of dimension $n - d + (d,l)$ if $\frac{k}{[d,l]}$ is odd and of dimension $n - d$ if $\frac{k}{[d,l]}$ is even.

Suppose $\frac{k}{[d,l]}$ odd. One has

$$\dim\left(\ker(T_{(d,l)}\circ T_2\circ T_d^n)\cap\mathbb{F}_{2^n}\right)=n-\dim\left(T_{(d,l)}\circ T_2\circ T_d^n(\mathbb{F}_{2^n})\right).$$

First, $T_{(d,l)}\circ T_2\circ T_d^n(\mathbb{F}_{2^n})=T_{(d,l)}\circ T_2(\mathbb{F}_{2^d})=T_{(d,l)}^{2(d,l)}(\mathbb{F}_{2^d})$. Furthermore, Example 1 let us know

$$\dim\left(T_{(d,l)}^{2(d,l)}(\mathbb{F}_{2^d})\right)=d-(d,l).$$

We therefore conclude that

$$\dim\left(\ker(T_{(d,l)}\circ T_2\circ T_d^n)\cap\mathbb{F}_{2^n}\right)=n-d+(d,l),$$

proving that $T_l^k(\mathbb{F}_{2^n})=\ker(T_{(d,l)}\circ T_2\circ T_d^n)\cap\mathbb{F}_{2^n}$.

The case when $\frac{k}{[d,l]}$ is even follows directly from Remark 2 which states $\dim(\ker(T_d^n)\cap\mathbb{F}_{2^n})=n-d$ in this case (see Example 2). □

We now states the main result of this paper.

Theorem 7 *Let $a\in\mathbb{F}_{2^n}$ and $d=(n,k)$.*

1. *Let $\frac{k}{[d,l]}$ and $\frac{k}{d}$ be odd. Suppose that $T_{(d,l)}\circ T_2\circ T_d^n(a)=0$. Then, one has*

$$\{x\in\mathbb{F}_{2^n}\mid T_l^k(x)=a\}=T_l\circ T_2\circ T_k^{[n,k]}\left(\frac{a}{\zeta+1}\right)+T_{(d,l)}\circ T_2\left(\mathbb{F}_{2^d}\right),\qquad(7)$$

where ζ is any element of $\mu_{2^n+1}\setminus\{1\}$.

2. *Let $\frac{k}{[d,l]}$ be odd and $\frac{k}{d}$ be even. Suppose that $T_{(d,l)}\circ T_2\circ T_d^n(a)=0$. Then, one has*

$$\{x\in\mathbb{F}_{2^n}\mid T_l^k(x)=a\}=T_l\circ T_2\circ T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta+1}\right)+T_{(d,l)}\circ T_2\left(\frac{T_d^n(a)}{\zeta+1}\right)+T_{(d,l)}\circ T_2\left(\mathbb{F}_{2^d}\right),\qquad(8)$$

where ζ is any element of $\mu_{2^d+1}\setminus\{1\}$.

3. *Let $\frac{k}{[d,l]}$ be even. Suppose that $T_d^n(a)=0$. Then, one has*

$$\{x\in\mathbb{F}_{2^n}\mid T_l^k(x)=a\}=T_l\circ T_2\circ T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta+1}\right)+\mathbb{F}_{2^d},\qquad(9)$$

where ζ is any element of $\mu_{2^d+1}\setminus\{1\}$.

Proof When $\frac{k}{[d,l]}$ be odd and $\frac{k}{d}$ is even, the solution formula can be checked as follows: Consider $T_d^n(a)\in\mathbb{F}_{2^d}$. Let $y_0=T_l\circ T_2\circ T_{n-k}^{[n,n-k]}\left(\frac{a^{2^{n-k}}}{\zeta+1}\right)$ and $z_0=T_{(d,l)}\circ T_2\left(\frac{T_d^n(a)}{\zeta+1}\right)$. First, the facts that $y_0\in\mathbb{F}_{2^n}$ and that $z_0\in\mathbb{F}_{2^d}$ can be checked by using Theorem 5 and the condition $T_{(d,l)}\circ T_2\circ T_d^n(a)=0$. Then, it can be easily checked that $T_l^k(z_0)=T_d^n(a)$ i.e. $T_l^{[d,l]}(z_0)=T_d^n(a)$ i.e. $T_{(d,l)}^d(z_0)=T_d^n(a)$. It is also an easy exercise to check by direct calculation $T_l^k(y_0)=T_d^n(a)+a$. So $x_0=y_0+z_0$ is a $\mathbb{F}_{2^n}$-solution to $T_l^k(x)=a$ and Proposition 3 completes the proof.

In remaining cases, the solution formulas are deduced from Theorem 5 and Proposition 3, regarding the fact that $T_l(x_0)$ is a solution in $\mathbb{F}_{2^n}$ to $T_l^k(x)=a$ if $x_0\in\mathbb{F}_{2^n}$ is a solution to $T_k(x)=a$. □

4 Conclusion

In this paper, we discussed the sets of preimages of linearized polynomials

$$T_l^k(x) := \sum_{i=0}^{\frac{k}{l}-1} x^{2^{li}}$$

over $\overline{\mathbb{F}_2}$ and over the finite field $\mathbb{F}_{2^n}$ for any $n \geq 1$ and provided an explicit representation for such preimages. It would be interesting to consider such a problem in odd characteristic.

References

1. Blake, I., Seroussi, G., Smart, N.: Elliptic curves in cryptography. Number 265 in London mathematical society lecture note series. Cambridge University Press, Cambridge (1999)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. Chapter of the monography. In: Crama, Y., Hammer, P. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Carlet, C.: Vectorial Boolean functions for cryptography. Chapter of the monography. In: Crama, Y., Hammer, P. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp. 398–469. Cambridge University Press, Cambridge (2010)
4. Mullen, G.L., Panario, D.: Handbook of finite fields. Discrete mathematics and its applications. CRC Press, Boca Raton (2013)