Solving some affine equations over finite fields

Sihem Mesnager, Kwang Ho Kim, Jong Hyok Choe, Dok Nam Lee

Version of Record: https://www.sciencedirect.com/science/article/pii/S1071579720301155
Manuscript_2251d18b70639291f86dbdc056b8ab3a

Solving Some Affine Equations over Finite Fields

Sihem Mesnager[1], Kwang Ho Kim[2,3], Jong Hyok Choe[2], and Dok Nam Lee[2]

[1] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France, and Telecom Paris, 91120 Palaiseau, France. Email: smesnager@univ-paris8.fr
[2] Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People's Republic of Korea. Email: khk.cryptech@gmail.com
[3] PGItech Corp., Pyongyang, Democratic People's Republic of Korea.

Abstract. Let l and k be two integers such that $l|k$. Define $T_l^k(X) := X+X^{p^l}+\cdots+X^{p^{k-2l}}+X^{p^{k-l}}$ and $S_l^k(X) := X-X^{p^l}+\cdots+(-1)^{(k/l-1)}X^{p^{k-l}}$, where p is any prime.
This paper gives explicit representations of all solutions in $\mathbb{F}_{p^n}$ to the affine equations $T_l^k(X) = a$ and $S_l^k(X) = a$, $a \in \mathbb{F}_{p^n}$. The case $p = 2$ was solved very recently in [10]. The results of this paper reveal another solution.

Keywords: Affine equation · Finite field · Zeros of a polynomial · Linearized polynomial.

Mathematics Subject Classification. 11D04, 12E05, 12E12.

1 Introduction

Let $\mathbb{F}_{p^n}$ be the finite field of p^n elements where p is a prime and $n \geq 1$ is a positive integer. A polynomial $L(X) \in \mathbb{F}_{p^n}[X]$ of shape

$$L(X) = \sum_{i=0}^{t} a_i X^{p^i}, a_i \in \mathbb{F}_{p^n}$$

is called a linearized polynomial over $\mathbb{F}_{p^n}$ or a $p-$polynomial over $\mathbb{F}_{p^n}$. An affine equation over $\mathbb{F}_{p^n}$ is an equation of type

$$L(X) = a, \tag{1}$$

where L is a linearized polynomial and $a \in \mathbb{F}_{p^n}$.

Affine equations arise in many different problems and contexts (e.g. [4–7, 9–15]). In particular, those involving the trace functions are crucial in many

Version : August 23, 2020

contexts of cryptography and error-correcting codes [1–3]. However, to find explicit solutions is often challenging and it is the ultimate goal to achieve.

Let k and l be positive integers such that $l|k$. Define two $p-$polynomials over $\mathbb{F}_p$:

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

and

$$S_l^k(X) := \sum_{i=0}^{\frac{k}{l}-1} (-1)^i X^{p^{li}}.$$

In this paper, we study the following two affine equations

$$T_l^k(X) = a, a \in \mathbb{F}_{p^n} \tag{2}$$

and

$$S_l^k(X) = a, a \in \mathbb{F}_{p^n}. \tag{3}$$

It is well-known that a linearized polynomial induce a linear transformation of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. In particular, if x_1 and x_2 are two solutions in $\mathbb{F}_{p^n}$ to Equation (1), then their difference $x_1 - x_2$ is a zero of L in $\mathbb{F}_{p^n}$, that is, their difference lies in the set $\{x \in \mathbb{F}_{p^n} \mid L(x) = 0\}$, that we call the kernel of L in $\mathbb{F}_{p^n}$. Determination of the $\mathbb{F}_{p^n}-$ solutions to Equation (1) can therefore be divided into two problems: to determine the kernel of L in $\mathbb{F}_{p^n}$ and to find a solution x_0 in $\mathbb{F}_{p^n}$ of the affine equation. Indeed, if those two problems are solved then the set of all $\mathbb{F}_{p^n}-$solutions to Equation (1) is $x_0 + \{x \in \mathbb{F}_{p^n} \mid L(x) = 0\}$.

In this paper, we solve these two problems for the linearized polynomials T_l^k and S_l^k. We firstly determine the kernels of T_l^k and S_l^k in Section 3. Next, we give explicit representations of particular solutions to Equation (2) and Equation (3) in Section 4. As by-product of those results, we also characterize the elements a in $\mathbb{F}_{p^n}$ for which Equation (2) and Equation (3) has at least one solution in $\mathbb{F}_{p^n}$ in Section 4.

Remark 1. In [10], we considered the particular case of $p = 2$ for which $T_l^k(X) = S_l^k(X)$. Interestingly, Theorem 1 and Theorem 4 in this paper provide another solution for this particular case.

2 Preliminaries

Throughout this paper, we maintain the following notation (otherwise, we will point it out at the appropriate place).

- p is any prime and n is any positive integer.
- a is any element of the finite field $\mathbb{F}_{p^n}$.
- k and l are any positive integers such that $l|k$.
- We denote the greatest common divisor and the smallest common multiple of two positive integers u and v by (u, v) and $[u, v]$, respectively.

- $d := (n,k)$, $e := (n,l)$ and $L := [d,l]$.

We now present a lemma that will be heavily used throughout this paper.

Lemma 1. *For any positive integers k, l and m with $m|l|k$ the following holds:*

1. $T_l^k \circ T_m^l(X) = T_m^k(X)$ *is an identity. Also,* $T_l^k \circ S_m^l(X) = S_m^k(X)$ *if* l/m *is even and* $S_l^k \circ S_m^l(X) = S_m^k(X)$ *if* l/m *is odd.*
2. $S_l^k \circ T_l^{2l}(X) = S_k^{2k}(X) = X - X^{p^k}$ *if* $\frac{k}{l}$ *is even and* $S_l^k \circ T_l^{2l}(X) = T_k^{2k}(X) = X + X^{p^k}$ *if* $\frac{k}{l}$ *is odd.*
3. $T_l^k \circ S_l^{2l}(X) = S_k^{2k}(X)$.
4. $T_k^{[n,k]}(x) = T_{(n,k)}^n(x)$ *for any* $x \in \mathbb{F}_{p^n}$. *Furthermore, if* $\frac{[n,k]}{k}$ *is even, then* $S_k^{[n,k]}(x) = S_{(n,k)}^n(x)$ *for any* $x \in \mathbb{F}_{p^n}$.
5. *If* $\frac{k}{l}$ *is even, then* $S_l^k(x) + S_l^k(x)^{p^l} = 0$ *for any* $x \in \mathbb{F}_{p^k}$.

Proof. The first three assertions are obtained by easy straightforward calculations. Hence, we give proofs only for the last two assertions.

Since $n \cdot k = [n,k] \cdot (n,k)$, one has $\frac{n}{(n,k)} = \frac{[n,k]}{k}$ and $\{j \cdot (n,k) \mid 0 \leq j \leq \frac{n}{(n,k)} - 1\} = \{ik \mod n \mid 0 \leq i \leq \frac{[n,k]}{k} - 1\}$ because n divides ik if and only if i is a multiple of $\frac{n}{(n,k)} = \frac{[n,k]}{k}$. Therefore $T_k^{[n,k]}(x) = T_{(n,k)}^n(x)$.

Furthermore, if $\frac{[n,k]}{k} = \frac{n}{(n,k)}$ is even, then $\frac{k}{(n,k)}$ is odd since it is prime to $\frac{n}{(n,k)}$. Thus, when two integers i and j are such that $jd \equiv ik \pmod{n}$, then they have the same parity. This proves $S_k^{[n,k]}(x) = S_{(n,k)}^n(x)$ if $\frac{[n,k]}{k}$ is even.

Finally, the last assertion is proved as follows: by Assertion 1 (with $2l$ at the place of l and with l at the place of m), we have $S_l^k(X) = S_l^{2l} \circ T_{2l}^k(X)$. Let $x \in \mathbb{F}_{p^k}$. Then $y := T_{2l}^k(x) \in \mathbb{F}_{p^{2l}}$. Hence $S_l^k(x) + S_l^k(x)^{p^l} = S_l^{2l}(y) + S_l^{2l}(y)^{p^l} = (y - y^{p^l}) + (y - y^{p^l})^{p^l} = 0$. □

It is well known that the set of $p-$polynomials over $\mathbb{F}_p$ forms an integral domain under the operations of symbolic multiplication (composition of polynomials) and ordinary addition (e.g. see page 115 in [8]). Therefore, under the symbolic multiplication, any two $p-$polynomials over $\mathbb{F}_p$, involving T_l^k and S_l^k, are commutative.This fact will be implicitly used throughout this paper.

3 On the Kernels of T_l^k and S_l^k

To determine the kernels of T_l^k and S_l^k in $\mathbb{F}_{p^n}$, we begin by determining the zeros of T_l^k and S_l^k in the algebraic closure $\overline{\mathbb{F}_p}$.

Lemma 2. *It holds:*

1. $$\{x \in \overline{\mathbb{F}_p} \mid T_l^k(x) = 0\} = S_l^{2l}(\mathbb{F}_{p^k}) = \{x - x^{p^l} \mid x \in \mathbb{F}_{p^k}\}.$$

2. *When* $\frac{k}{l}$ *is even,*

$$\{x \in \overline{\mathbb{F}_p} \,|\, S_l^k(x) = 0\} = T_l^{2l}(\mathbb{F}_{p^k}) = \{x + x^{p^l} \,|\, x \in \mathbb{F}_{p^k}\}.$$

3. *When* $\frac{k}{l}$ *is odd,*

$$\{x \in \overline{\mathbb{F}_p} \,|\, S_l^k(x) = 0\} = S_k^{2k} \circ T_l^{2l}(\mathbb{F}_{p^{2k}}) = \{(x + x^{p^l}) - (x + x^{p^l})^{p^k} \,|\, x \in \mathbb{F}_{p^{2k}}\}.$$

Proof. For $x \in \mathbb{F}_{p^k}$, by Assertion 3 of Lemma 1, $T_l^k \circ S_l^{2l}(x) = x - x^{p^k} = 0$ proving the inclusion of $S_l^{2l}(\mathbb{F}_{p^k})$ in $\{x \in \overline{\mathbb{F}_p} \,|\, T_l^k(x) = 0\}$. We then conclude the equality from the fact that the two sets have the same cardinality p^{k-l}. The second assertion is similarly proved by using Assertion 2 of Lemma 1. The third assertion can be proved similarly by using Assertions 2 and 3 of Lemma 1. □

Corollary 1. *The following holds:*

1. $$\ker(T_l^k) \subset \mathbb{F}_{p^k}.$$

2. $$\ker(S_l^k) \subset \begin{cases} \mathbb{F}_{p^k}, & \text{if } \frac{k}{l} \text{ is even,} \\ \mathbb{F}_{p^{2k}}, & \text{if } \frac{k}{l} \text{ is odd.} \end{cases}$$

Based on the lemma above, we can determine the kernels of T_l^k and S_l^k in $\mathbb{F}_{p^n}$. For the reader's convenience, we present our results as three statements, each of them corresponding to an assertion of Lemma 2.

Theorem 1. *The following holds true:*

$$\{x \in \mathbb{F}_{p^n} \,|\, T_l^k(x) = 0\} = \begin{cases} \mathbb{F}_{p^d}, & \text{if } p|\frac{k}{L} \\ S_e^{2e}(\mathbb{F}_{p^d}), & \text{otherwise.} \end{cases}$$

Consequently,

$$\#\{x \in \mathbb{F}_{p^n} \,|\, T_l^k(x) = 0\} = \begin{cases} p^d, & \text{if } p|\frac{k}{L} \\ p^{d-e}, & \text{otherwise.} \end{cases}$$

Proof. By Assertion 1 of Lemma 2,

$$\{x \in \mathbb{F}_{p^n} \,|\, T_l^k(x) = 0\} = S_l^{2l}(\mathbb{F}_{p^k}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^{(n,k)}} = \mathbb{F}_{p^d}.$$

By Assertion 1 of Lemma 1 we have $T_l^k(X) = T_L^k \circ T_l^L(X)$ and therefore

$$\begin{aligned} \{x \in \mathbb{F}_{p^n} \,|\, T_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \,|\, T_l^k(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \,|\, \frac{k}{L} T_l^L(x) = 0\}. \end{aligned}$$

Thus, if $p|\frac{k}{L}$, then

$$\{x \in \mathbb{F}_{p^n} \,|\, T_l^k(x) = 0\} = \mathbb{F}_{p^d},$$

and if $p \nmid \frac{k}{L}$, then

$$\begin{aligned}\{x \in \mathbb{F}_{p^n} \mid T_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \mid T_l^L(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \mid T_e^d(x) = 0\} \text{ (by Assertion 4 of Lemma 1)} \\ &= S_e^{2e}(\mathbb{F}_{p^d}) \text{ (by Assertion 1 of Lemma 2).}\end{aligned}$$

□

Theorem 2. *Suppose that $\frac{k}{l}$ is even.*

1. *If $\frac{d}{e}$ is even, then*

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \begin{cases} \mathbb{F}_{p^d}, & \text{if } p|\frac{k}{L} \\ T_e^{2e}(\mathbb{F}_{p^d}), & \text{otherwise} \end{cases}$$

and consequently

$$\#\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \begin{cases} p^d, & \text{if } p|\frac{k}{L} \\ p^{d-e}, & \text{otherwise.} \end{cases}$$

2. *If $\frac{d}{e}$ is odd, then*

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \mathbb{F}_{p^d}$$

and consequently

$$\#\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = p^d.$$

Proof. By Assertion 2 of Lemma 2, when $\frac{k}{l}$ is even, we know that $\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = T_l^{2l}(\mathbb{F}_{p^k}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^d}$ and thus

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \{x \in \mathbb{F}_{p^d} \mid S_l^k(x) = 0\}.$$

Now, suppose that $\frac{d}{e} = \frac{d}{(d,l)} = \frac{L}{l}$ is even. Then, by Assertion 1 of Lemma 1

$$\begin{aligned}\{x \in \mathbb{F}_{p^d} \mid S_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \mid T_L^k \circ S_l^L(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \mid \frac{k}{L} S_l^L(x) = 0\}.\end{aligned}$$

Therefore, if $p|\frac{k}{L}$, then

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \mathbb{F}_{p^d},$$

and if $p \nmid \frac{k}{L}$, then

$$\begin{aligned}\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \mid S_l^L(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \mid S_e^d(x) = 0\} \text{ (by Assertion 4 of Lemma 1)} \\ &= T_e^{2e}(\mathbb{F}_{p^d}) \text{ (by Assertion 2 of Lemma 2).}\end{aligned}$$

Suppose now that $\frac{d}{e} = \frac{L}{l}$ is odd. In this case, $\frac{k}{L}$ is even as $\frac{k}{l} = \frac{k}{L} \cdot \frac{L}{l}$ is even by the assumption. Thus, we have

$$\begin{aligned}\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \mid S_l^k(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \mid S_L^k \circ S_l^L(x) = 0\} \text{ (by Assertion 1 of Lemma 1)} \\ &= \mathbb{F}_{p^d}\end{aligned}$$

because $S_l^L(x) \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^L}$ for $x \in \mathbb{F}_{p^d}$. □

Theorem 3. *Suppose that $\frac{k}{l}$ is odd.*

1. *When $\frac{n}{d}$ is odd,*
$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \{0\}$$
and consequently
$$\#\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = 1.$$
2. *When $\frac{n}{d}$ is even,*
$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \begin{cases} S_d^{2d}(\mathbb{F}_{p^{2d}}), & \text{if } p|\frac{k}{L} \\ S_d^{2d} \circ T_e^{2e}(\mathbb{F}_{p^{2d}}), & \text{otherwise} \end{cases}$$
and consequently
$$\#\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \begin{cases} p^d, & \text{if } p|\frac{k}{L} \\ p^{d-e}, & \text{otherwise.} \end{cases}$$

Proof. First of all, note that $\frac{L}{l}$ and $\frac{k}{L}$ are odd since both of them are divisors of $\frac{k}{l}$ which is odd. Then by Assertion 3 of Lemma 2 one has

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = S_k^{2k} \circ T_l^{2l}(\mathbb{F}_{p^{2k}}) \cap \mathbb{F}_{p^n} = \{x \in \mathbb{F}_{p^{(n,2k)}} \mid S_l^k(x) = 0\}.$$

Suppose that $\frac{n}{d}$ is odd. Then, $(n, 2k) = d$ and we have

$$\begin{aligned}\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} &= \{x \in \mathbb{F}_{p^d} \mid S_l^k(x) = 0\} \\ &= \{x \in \mathbb{F}_{p^d} \mid S_L^k \circ S_l^L(x) = 0\} \text{ (by Assertion 1 of Lemma 1)} \\ &= \{x \in \mathbb{F}_{p^d} \mid S_l^L(x) = 0\} \\ &= \{S_L^{2L} \circ T_l^{2l}(\beta) \in \mathbb{F}_{p^d} \mid \beta \in \mathbb{F}_{p^{2L}}\} \text{ (by Assertion 3 of Lemma 2).}\end{aligned}$$

Now, if $S_L^{2L} \circ T_l^{2l}(\beta) \in \mathbb{F}_{p^d}$ for $\beta \in \mathbb{F}_{p^{2L}}$, then we have

$$\begin{aligned}(S_L^{2L} \circ T_l^{2l}(\beta))^{p^L} = S_L^{2L} \circ T_l^{2l}(\beta) &\iff -S_L^{2L} \circ T_l^{2l}(\beta) = S_L^{2L} \circ T_l^{2l}(\beta) \\ &\iff S_L^{2L} \circ T_l^{2l}(\beta) = 0.\end{aligned}$$

Thus, in that case

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \{0\}.$$

Now, suppose that $\frac{n}{d}$ is even. Then, $(n, 2k) = 2d$ and

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = \{x \in \mathbb{F}_{p^{2d}} \mid S_l^k(x) = 0\}.$$

Since $\frac{L}{l}$ is odd, from by Assertion 5 of Lemma 1 it follows

$$S_l^{2L}(x) + S_l^{2L}(x)^{p^L} = 0 \tag{4}$$

for every $x \in \mathbb{F}_{p^{2d}}$.

Also, $\frac{k}{d}$ is odd since $\frac{n}{d}$ is even and $(\frac{n}{d}, \frac{k}{d}) = 1$. This implies $\frac{L}{d}$ odd as well since it is divisor of $\frac{k}{d}$. Therefore, for every $x \in \mathbb{F}_{p^{2d}}$, it holds

$$x^{p^L} = (x^{p^{\frac{L-d}{d} \cdot d}})^{p^d} = x^{p^d},$$

$$x^{p^k} = (x^{p^{\frac{k-d}{d} \cdot d}})^{p^d} = x^{p^d}$$

and hence

$$S_L^{2L}(x) = S_d^{2d}(x) \text{ and } T_k^{2k}(x) = T_d^{2d}(x). \tag{5}$$

Moreover, since $\frac{L}{d} = \frac{[d,l]}{d}$ is odd, one has $(2d, l) = (d, l) = e$ and $[2d, l] = \frac{2dl}{(2d,l)} = 2\frac{dl}{(d,l)} = 2[d, l] = 2L$. Therefore, by Assertion 4 of Lemma 1, for every $x \in \mathbb{F}_{p^{2d}}$ we have $S_l^{2L}(x) = S_l^{[2d,l]}(x) = S_{(2d,l)}^{2d}(x) = S_{(d,l)}^{2d}(x) = S_e^{2d}(x)$, that is,

$$S_l^{2L}(x) = S_e^{2d}(x). \tag{6}$$

Then, for every $x \in \mathbb{F}_{p^{2d}}$ one has

$$\begin{aligned}
S_d^{2d} \circ S_l^k(x) &= S_L^{2L} \circ S_l^k(x) \text{ (by (5))} \\
&= S_L^{2L} \circ S_L^k \circ S_l^L(x) \text{ (by Assertion 1 of Lemma 1)} \\
&= S_L^k \circ S_L^{2L} \circ S_l^L(x) \\
&= S_L^k \circ S_l^{2L}(x) \text{ (again by Assertion 1 of Lemma 1)} \\
&= \frac{k}{L} S_l^{2L}(x) \text{ (by (4))} \\
&= \frac{k}{L} S_e^{2d}(x) \text{ (by (6)),}
\end{aligned}$$

that is,

$$S_l^k(S_d^{2d}(x)) = \begin{cases} 0, & \text{if } p|\frac{k}{L} \\ S_e^{2d}(x), & \text{otherwise.} \end{cases} \tag{7}$$

Thus, when $p|\frac{k}{L}$, it holds

$$\{x \in \mathbb{F}_{p^{2d}} \mid S_l^k(x) = 0\} \supset S_d^{2d}(\mathbb{F}_{p^{2d}}) = \ker(T_d^{2d}),$$

where the equality is from Assertion 1 of Lemma 2. On the other hand, by (5) and Assertion 2 of Lemma 1, $T_d^{2d}(x) = T_k^{2k}(x) = T_l^{2l} \circ S_l^k(x)$ for every $x \in \mathbb{F}_{p^{2d}}$ and therefore $\{x \in \mathbb{F}_{p^{2d}} \mid S_l^k(x) = 0\} \subset \ker(T_d^{2d})$. Hence, when $p|\frac{k}{L}$, we get

$$\{x \in \mathbb{F}_{p^n} \mid S_l^k(x) = 0\} = S_d^{2d}(\mathbb{F}_{p^{2d}}).$$

On the other hand, if $p \nmid \frac{k}{L}$, then by (7)

$$\begin{aligned}\{x \in \mathbb{F}_{p^{2d}} \mid S_l^k(x) = 0\} &\supset \{S_d^{2d}(x) \mid S_e^{2d}(x) = 0, x \in \mathbb{F}_{p^{2d}}\} \\ &= \{S_d^{2d} \circ T_e^{2e}(\beta) \mid \beta \in \mathbb{F}_{p^{2d}}\} \text{ (by Assertion 2 of Lemma 2)} \\ &= \ker(S_e^d) \text{ (by Assertion 3 of Lemma 2 since } \frac{d}{e} = \frac{L}{l} \text{ is odd).}\end{aligned}$$

Also, when $x \in \mathbb{F}_{p^{2d}}$, we can write

$$S_l^k(x) = \frac{k-L}{2L} S_l^{2L}(x) + S_l^L(x)$$

because $\frac{k}{L}$ is odd. By (6) and (7), $S_l^k(x) = 0$ implies $S_l^{2L}(x) = 0$ and therefore if $S_l^k(x) = 0$, then $S_l^L(x) = 0$ for $x \in \mathbb{F}_{p^{2d}}$. Then one has

$$\{x \in \mathbb{F}_{p^{2d}} \mid S_l^k(x) = 0\} \subset \ker(S_l^L) \cap \mathbb{F}_{p^{2d}}.$$

Thus, to conclude the theorem, thanks to Assertion 3 of Lemma 2 it is sufficient to prove:

$$\ker(S_e^d) = \ker(S_l^L) \cap \mathbb{F}_{p^{2d}}. \tag{8}$$

To begin with, let us show

$$\ker(S_e^d) \subset \ker(S_l^L) \cap \mathbb{F}_{p^{2d}}.$$

In fact, if $y \in \ker(S_e^d)$ or equivalently $y = S_d^{2d} \circ T_e^{2e}(\beta)$ for some $\beta \in \mathbb{F}_{p^{2d}}$, then

$$\begin{aligned}S_l^L(y) &= S_l^L \circ S_d^{2d} \circ T_e^{2e}(\beta) \\ &= S_l^L \circ S_L^{2L} \circ T_e^{2e}(\beta) \text{ (by (5))} \\ &= S_l^{2L} \circ T_e^{2e}(\beta) \text{ (by Assertion 1 of Lemma 1)} \\ &= S_e^{2d} \circ T_e^{2e}(\beta) \text{ (by (6))} \\ &= S_{2d}^{4d}(\beta) \text{ (by Assertion 2 of Lemma 1)} \\ &= 0 \text{ (since } \beta \in \mathbb{F}_{p^{2d}}).\end{aligned}$$

Next, we prove

$$\#\ker(S_e^d) = \#\{\ker(S_l^L) \cap \mathbb{F}_{p^{2d}}\}$$

which will conclude (8). Let $A := \ker(S_e^{2d}) = T_e^{2e}(\mathbb{F}_{p^{2d}})$. Then, by (6), $A = \ker(S_l^{2L}) \cap \mathbb{F}_{p^{2d}}$, and since $S_l^{2L} = S_L^{2L} \circ S_l^L$ by Assertion 1 of Lemma 1,

$$\ker(S_l^L) \cap \mathbb{F}_{p^{2d}} \subset A.$$

Hence, now we determine $S_l^L(A)$ which will make it possible to compute $\#\{\ker(S_l^L) \cap \mathbb{F}_{p^{2d}}\}$. Since $S_d^{2d}(S_l^L(A)) \overset{(5)}{=} S_L^{2L}(S_l^L(A)) = S_l^{2L}(A) = \{0\}$, it holds

$$S_l^L(A) \subset \mathbb{F}_{p^d}. \tag{9}$$

Then, since $\frac{d}{e} = \frac{L}{l}$ is odd, by Assertion 2 of Lemma 1, $S_e^d(A) = S_e^d \circ T_e^{2e}(\mathbb{F}_{p^{2d}}) = T_d^{2d}(\mathbb{F}_{p^{2d}}) = \mathbb{F}_{p^d}$. The obvious fact $S_e^d(A) \subset A$ yields

$$\mathbb{F}_{p^d} \subset A. \tag{10}$$

Now, let us prove that S_l^L is a permutation on $\mathbb{F}_{p^d}$. In fact, if $y \in \mathbb{F}_{p^L}$ is an element in $\ker(S_l^L)$, then by Assertion 3 of Lemma 2 we can write $y = S_L^{2L} \circ T_l^{2l}(\beta)$ for some $\beta \in \mathbb{F}_{p^{2L}}$ and one has $y = y^{p^L} = (S_L^{2L} \circ T_l^{2l}(\beta))^{p^L} = -S_L^{2L} \circ T_l^{2l}(\beta) = -y$, i.e. $y = 0$. Therefore, $\ker(S_l^L) \cap \mathbb{F}_{p^L} = \{0\}$ and S_l^L is a permutation on $\mathbb{F}_{p^L}$ and subsequently on $\mathbb{F}_{p^d}$. Applying S_l^L on both sides of (10) we get

$$\mathbb{F}_{p^d} \subset S_l^L(A). \tag{11}$$

Combining (9) and (11) proves

$$S_l^L(A) = \mathbb{F}_{p^d}.$$

From this equality, considering $x \mapsto S_l^L(x)$ as an $\mathbb{F}_p-$linear transformation of the $\mathbb{F}_p-$subspace A, it follows that

$$\#\{\ker(S_l^L) \cap \mathbb{F}_{p^{2d}}\} = \#A/p^d = p^{(2d-e)-d} = p^{d-e} = \#\ker(S_e^d).$$

□

4 On particular solutions of $T_l^k(X) = a$ and $S_l^k(X) = a$

In this section, we give particular solutions for each of the two equations (2) and (3) as well as characterizations of the a's in $\mathbb{F}_{p^n}$ for which the equations (2) and (3) have at least one solution in $\mathbb{F}_{p^n}$. As in Section 3, we present these results in three statements. Each of them corresponds to one of the three cases of Lemma 2.

Theorem 4. *Let $\delta \in \mathbb{F}_{p^n}^*$ and $\delta_1 \in \mathbb{F}_{p^d}^*$ be any elements such that $T_d^n(\delta) = 1$ and $T_e^d(\delta_1) = 1$.*

1. *When $p|\frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $T_l^k(X) = a, a \in \mathbb{F}_{p^n}$, if and only if $T_d^n(a) = 0$. In that case,*

$$x_0 = S_l^{2l}\left(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}}\right)$$

   is a particular $\mathbb{F}_{p^n}-$solution to the equation $T_l^k(X) = a$.
2. *When $p \nmid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $T_l^k(X) = a, a \in \mathbb{F}_{p^n}$, if and only if $S_e^{2e} \circ T_d^n(a) = 0$. In that case,*

$$x_0 = y_0 + \frac{L}{k}(a - T_l^k(y_0))\delta_1,$$

where

$$y_0 = \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} S_l^{2l}(a)^{p^{ki}},$$

is a particular $\mathbb{F}_{p^n}-$*solution to the equation* $T_l^k(X) = a$.

Proof. Let $a = T_l^k(x_0)$ for some $x_0 \in \mathbb{F}_{p^n}$. Then

$$\begin{aligned} T_d^n(a) &= T_d^n \circ T_l^k(x_0) \\ &= T_d^n \circ T_L^k \circ T_l^L(x_0) \text{ (by Assertion 1 of Lemma 1)} \\ &= T_L^k \circ T_l^L \circ T_d^n(x_0) \\ &= T_L^k \circ T_e^d \circ T_d^n(x_0) \text{ (by Assertion 4 of Lemma 1)} \\ &= T_L^k \circ T_e^n(x_0) \text{ (by Assertion 1 of Lemma 1)} \\ &= \frac{k}{L} T_e^n(x_0) \text{ (since } T_e^n(x_0) \in \mathbb{F}_{p^e} \subset \mathbb{F}_{p^L}). \end{aligned}$$

Thus, if $p|\frac{k}{L}$, then $T_d^n(a) = 0$, and if $p \nmid \frac{k}{L}$, then $S_e^{2e} \circ T_d^n(a) = \frac{k}{L} S_e^{2e} \circ T_e^n(x_0) = \frac{k}{L} S_n^{2n}(x_0) = 0$ where we applied Assertion 3 of Lemma 1. In other words, if $p|\frac{k}{L}$, then

$$T_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \mid T_d^n(a) = 0\}, \tag{12}$$

and if $p \nmid \frac{k}{L}$, then

$$T_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \mid S_e^{2e} \circ T_d^n(a) = 0\}. \tag{13}$$

By Theorem 1 we have:

$$\#T_l^k(\mathbb{F}_{p^n}) = p^n / \#\{\ker(T_l^k) \cap \mathbb{F}_{p^n}\} = \begin{cases} p^{n-d}, & \text{if } p|\frac{k}{L} \\ p^{n-(d-e)}, & \text{otherwise.} \end{cases}$$

On the other hand, by the well-known nature of the trace mapping one knows

$$\#\{a \in \mathbb{F}_{p^n} \mid T_d^n(a) = 0\} = p^{n-d}$$

and

$$\#\{a \in \mathbb{F}_{p^n} \mid S_e^{2e} \circ T_d^n(a) = 0\} = \#\{a \in \mathbb{F}_{p^n} \mid T_d^n(a) \in \mathbb{F}_{p^e}\} = p^{n-(d-e)}.$$

Thus, we conclude that the inclusions (12) and (13) are actually equalities. That is, the if and only if conditions for $T_l^k(X) = a \in \mathbb{F}_{p^n}$ to have a solution in $\mathbb{F}_{p^n}$ are proved.

Let us check the validity of the given particular solutions. If $T_d^n(a) = 0$, we have

$$\begin{aligned}
&T_l^k \circ S_l^{2l}\left(\sum_{i=0}^{\frac{n}{d}-2}\sum_{j=i+1}^{\frac{n}{d}-1}\delta^{p^{kj}}a^{p^{ki}}\right)\\
&= S_k^{2k}\left(\sum_{i=0}^{\frac{n}{d}-2}\sum_{j=i+1}^{\frac{n}{d}-1}\delta^{p^{kj}}a^{p^{ki}}\right) \text{ (by Assertion 3 of Lemma 1)}\\
&= \sum_{i=0}^{\frac{n}{d}-2}\sum_{j=i+1}^{\frac{n}{d}-1}\delta^{p^{kj}}a^{p^{ki}} - \sum_{i=1}^{\frac{n}{d}-1}\sum_{j=i+1}^{\frac{n}{d}}\delta^{p^{kj}}a^{p^{ki}}\\
&= \sum_{j=1}^{\frac{n}{d}-1}\delta^{p^{kj}}a - \sum_{i=1}^{\frac{n}{d}-1}\delta^{p^{\frac{k}{d}n}}a^{p^{ki}}\\
&= \sum_{j=1}^{\frac{n}{d}-1}\delta^{p^{kj}}a - \sum_{i=1}^{\frac{n}{d}-1}\delta a^{p^{ki}}\\
&= \sum_{j=0}^{\frac{n}{d}-1}\delta^{p^{kj}}a - \sum_{i=0}^{\frac{n}{d}-1}\delta a^{p^{ki}}\\
&= T_k^{[n,k]}(\delta)a - \delta T_k^{[n,k]}(a)\\
&= T_d^n(\delta)a - \delta T_d^n(a) \text{ (by Assertion 4 of Lemma 1)}\\
&= a \text{ (since } T_d^n(\delta) = 1 \text{ and } T_d^n(a) = 0).
\end{aligned}$$

This proves case 1.

Now, suppose that $p \nmid \frac{k}{L}$ and $S_e^{2e} \circ T_d^n(a) = 0$, i.e., $T_d^n(a) \in \mathbb{F}_{p^e}$. Then, $S_l^{2l}(T_d^n(a)) = T_d^n(a) - T_d^n(a)^{p^l} = 0$, and for $y_0 = \sum_{i=0}^{\frac{n}{d}-2}\sum_{j=i+1}^{\frac{n}{d}-1}\delta^{p^{kj}}S_l^{2l}(a)^{p^{ki}}$, it holds

$$\begin{aligned}
S_k^{2k}(y_0) &= \sum_{i=0}^{\frac{n}{d}-2}\sum_{j=i+1}^{\frac{n}{d}-1}\delta^{p^{kj}}S_l^{2l}(a)^{p^{ki}} - \sum_{i=1}^{\frac{n}{d}-1}\sum_{j=i+1}^{\frac{n}{d}}\delta^{p^{kj}}S_l^{2l}(a)^{p^{ki}}\\
&= S_l^{2l}(a) - \delta T_d^n(S_l^{2l}(a)) = S_l^{2l}(a) - \delta S_l^{2l}(T_d^n(a))\\
&= S_l^{2l}(a).
\end{aligned}$$

Since $S_k^{2k}(y_0) = S_l^{2l}(T_l^k(y_0))$ (by Assertion 3 of Lemma 1), we get

$$\beta := a - T_l^k(y_0) \in \ker(S_l^{2l}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^l} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^e}.$$

Now, $\beta\delta_1 \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^L}$ and therefore

$$\begin{aligned} T_l^k(\beta\delta_1) &= T_L^k \circ T_l^L(\beta\delta_1) \text{ (by Assertion 1 of Lemma 1)} \\ &= \frac{k}{L} T_l^L(\beta\delta_1) \text{ (since } T_l^L(\beta\delta_1) \in \mathbb{F}_{p^L}) \\ &= \frac{k}{L} T_e^d(\beta\delta_1) \text{ (by Assertion 4 of Lemma 1)} \\ &= \frac{k}{L} \beta T_e^d(\delta_1) \text{ (since } \beta \in \mathbb{F}_{p^e}) \\ &= \frac{k}{L}\beta. \end{aligned}$$

That is, we get $T_l^k(\frac{L}{k}(a - T_l^k(y_0))\delta_1) = a - T_l^k(y_0)$, or equivalently,

$$T_l^k(y_0 + \frac{L}{k}(a - T_l^k(y_0))\delta_1) = a.$$

□

Theorem 5. *Let $p \neq 2$, $\frac{k}{l}$ even, $\delta \in \mathbb{F}_{p^n}^*$ be any element such that $T_d^n(\delta) = 1$. When $\frac{d}{e}$ is even, let $\delta_1 \in \mathbb{F}_{p^d}^*$ be any element such that $T_{2e}^d(\delta_1) = 1$.*

1. *When $\frac{d}{e}$ is odd, or, when $\frac{d}{e}$ is even and $p|\frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_l^k(X) = a$ if and only if $T_d^n(a) = 0$. In that case,*

$$x_0 = T_l^{2l}\left(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}}\right) \tag{14}$$

   is a particular $\mathbb{F}_{p^n}-$solution to the equation $S_l^k(X) = a$.
2. *When $\frac{d}{e}$ is even and $p \nmid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_l^k(X) = a$ if and only if $T_e^{2e} \circ T_d^n(a) = 0$. In that case,*

$$x_0 = y_0 + \frac{L}{2k}(a - S_l^k(y_0))\delta_1,$$

   where

$$y_0 = \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}},$$

   is a particular $\mathbb{F}_{p^n}-$solution to the equation $S_l^k(X) = a$.

Proof. Suppose that $S_l^k(x_0) = a$ for some $x_0 \in \mathbb{F}_{p^n}$. When $\frac{d}{e} = \frac{L}{l}$ is odd, $\frac{k}{L}$ is even since $\frac{k}{l} = \frac{L}{l} \cdot \frac{k}{L}$ was assumed to be even. Then, we have

$$\begin{aligned} T_d^n(a) &= T_d^n \circ S_l^k(x_0) \\ &= T_d^n \circ S_L^k \circ S_l^L(x_0) \text{ (by Assertion 1 of Lemma 1)} \\ &= S_L^k(S_l^L \circ T_d^n(x_0)) \\ &= 0 \text{ (since } S_l^L \circ T_d^n(x_0) \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^L} \text{ and } \frac{k}{L} \text{ is even)} \end{aligned}$$

and thus

$$S_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \,|\, T_d^n(a) = 0\}. \tag{15}$$

On the other hand, when $\frac{d}{e} = \frac{L}{l}$ is even, one has

$$\begin{aligned} T_d^n(a) &= T_d^n \circ S_l^k(x_0) \\ &= T_d^n \circ T_L^k \circ S_l^L(x_0) \text{ (by Assertion 1 of Lemma 1)} \\ &= T_L^k \circ S_l^L \circ T_d^n(x_0) \\ &= T_L^k \circ S_e^d \circ T_d^n(x_0) \text{ (by Assertion 4 of Lemma 1)} \\ &= \frac{k}{L} S_e^d \circ T_d^n(x_0) \text{ (since } S_e^d \circ T_d^n(x_0) \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^L}). \end{aligned}$$

Therefore, if $p|\frac{k}{L}$, then (15) still holds true, and if $p \nmid \frac{k}{L}$, then it holds

$$\begin{aligned} T_e^{2e} \circ T_d^n(a) &= \frac{k}{L} T_e^{2e} \circ S_e^d \circ T_d^n(x_0) \\ &= \frac{k}{L} S_d^{2d} \circ T_d^n(x_0) \text{ (by Assertion 2 of Lemma 1)} \\ &= 0 \text{ (since } T_d^n(x_0) \in \mathbb{F}_{p^d}) \end{aligned}$$

and thus

$$S_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \,|\, T_e^{2e} \circ T_d^n(a) = 0\}. \tag{16}$$

By Theorem 2 we have:

$$\#S_l^k(\mathbb{F}_{p^n}) = p^n / \#\{\ker(S_l^k) \cap \mathbb{F}_{p^n}\} = \begin{cases} p^{n-d}, & \text{if } \frac{d}{e} \text{ is odd, or, } \frac{d}{e} \text{ is even and } p|\frac{k}{L} \\ p^{n-(d-e)}, & \text{otherwise.} \end{cases}$$

On the other hand, by the well-known nature of the trace mapping one knows

$$\#\{a \in \mathbb{F}_{p^n} \,|\, T_d^n(a) = 0\} = p^{n-d}$$

and if d/e is even then

$$\#\{a \in \mathbb{F}_{p^n} \,|\, T_e^{2e} \circ T_d^n(a) = 0\} = p^{n-(d-e)}.$$

Therefore the inclusions (15) and (16) are indeed equalities. That is, the if and only if conditions for $S_l^k(X) = a$ to have an $\mathbb{F}_{p^n}-$solution are justified.

Since $S_l^k \circ T_l^{2l} = S_k^{2k}$ (Assertion 2 of Lemma 1), it can be checked by the same computation as in the proof of the first assertion of Theorem 4 that under the condition $T_d^n(a) = 0$,

$$x_0 = T_l^{2l}\Big(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}}\Big)$$

is a particular $\mathbb{F}_{p^n}-$solution to the equation $S_l^k(X) = a$. This proves case 1.

Now, assuming that $\frac{d}{e} = \frac{L}{l}$ is even, let us suppose that $p \nmid \frac{k}{L}$ and $T_e^{2e} \circ T_d^n(a) = 0$, i.e., $T_d^n(a)^{p^e} = -T_d^n(a)$. Then, $\frac{l}{e}$ is odd since it is prime to $\frac{n}{e} = \frac{d}{e} \cdot \frac{n}{d}$ which is even. Hence, $T_l^{2l}(T_d^n(a)) = T_d^n(a) + T_d^n(a)^{p^l} = 0$, and for $y_0 = \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}}$, it holds

$$\begin{aligned} S_k^{2k}(y_0) &= \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} - \sum_{i=1}^{\frac{n}{d}-1} \sum_{j=i+1}^{\frac{n}{d}} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} \\ &= T_l^{2l}(a) - \delta T_d^n(T_l^{2l}(a)) = T_l^{2l}(a) - \delta T_l^{2l}(T_d^n(a)) \\ &= T_l^{2l}(a). \end{aligned}$$

Since $S_k^{2k}(y_0) = T_l^{2l}(S_l^k(y_0))$ (Assertion 2 of Lemma 1), letting $\beta := a - S_l^k(y_0)$, we have

$$\beta \in \ker(T_l^{2l}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^{2l}} \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^{2e}} \subset \mathbb{F}_{p^d}$$

and

$$\begin{aligned} S_l^k(\beta\delta_1) &= \frac{k}{L} S_l^L(\beta\delta_1) \text{ (since } \frac{L}{l} \text{ is even)} \\ &= \frac{k}{L} S_e^d(\beta\delta_1) \text{ (by Assertion 4 of Lemma 1)} \\ &= \frac{k}{L} S_e^{2e}(T_{2e}^d(\beta\delta_1)) \text{ (by Assertion 1 of Lemma 1)} \\ &= \frac{k}{L} S_e^{2e}(\beta T_{2e}^d(\delta_1)) \text{ (since } \beta \in \mathbb{F}_{p^{2e}}) \\ &= \frac{k}{L} S_e^{2e}(\beta) = \frac{k}{L}(\beta - \beta^{p^e}). \end{aligned}$$

On the other hand, since $\ker(T_l^{2l}) \cap \mathbb{F}_{p^{2e}} = S_e^{2e}(\mathbb{F}_{p^{2e}})$ (see Theorem 1), $\beta \in \ker(T_l^{2l}) \cap \mathbb{F}_{p^n}$ means that $\beta = \alpha - \alpha^{p^e}$ for some $\alpha \in \mathbb{F}_{p^{2e}}$, and therefore we get $\beta + \beta^{p^e} = (\alpha - \alpha^{p^e}) + (\alpha - \alpha^{p^e})^{p^e} = 0$ and hence

$$S_l^k(\beta\delta_1) = \frac{2k}{L}\beta,$$

or equivalently,

$$S_l^k\left(y_0 + \frac{L}{2k}(a - S_l^k(y_0))\delta_1\right) = a.$$

□

Theorem 6. *Let $p \neq 2$, $\frac{k}{l}$ odd, $\delta \in \mathbb{F}_{p^n}^*$ and $\delta_1 \in \mathbb{F}_{p^{2d}}^*$ be any elements such that $T_d^n(\delta) = 1$ and $T_{2e}^{2d}(\delta_1) = 1$.*

1. *When $\frac{n}{d}$ is even and $p|\frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_l^k(X) = a$ if and only if $S_d^n(a) = 0$. In that case,*

$$x_0 = T_l^{2l}\left(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}} (-1)^i\right)$$

is a particular $\mathbb{F}_{p^n}-$solution to the equation $S_l^k(X) = a$.

2. *When $\frac{n}{d}$ is even and $p \nmid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_l^k(X) = a$ if and only if $T_e^{2e} \circ S_d^n(a) = 0$. In that case,*

$$x_0 = y_0 + \frac{L}{2k} S_d^{2d}((a - S_l^k(y_0))\delta_1),$$

where

$$y_0 = \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} (-1)^i,$$

is a particular $\mathbb{F}_{p^n}-$solution to the equation $S_l^k(X) = a$.

3. *When $\frac{n}{d}$ is odd, the equation $S_l^k(X) = a$ has a unique $\mathbb{F}_{p^n}-$solution:*

$$x_0 = \frac{T_l^{2l} \circ S_k^{[n,k]}(a)}{2}.$$

Proof. Suppose $a \in S_l^k(\mathbb{F}_{p^n})$, i.e., $a = S_l^k(x_0)$ for some $x_0 \in \mathbb{F}_{p^n}$.

Let us assume that $\frac{n}{d}$ is even. In this case, $\frac{k}{d}$ and its divisor $\frac{L}{d}$ are odd since $(\frac{n}{d}, \frac{k}{d}) = 1$. One has

$$\begin{aligned}
S_d^n(a) &= S_d^n \circ S_l^k(x_0) \\
&= S_d^n \circ S_L^k \circ S_l^L(x_0) \text{ (by Assertion 1 of Lemma 1)} \\
&= S_d^{2d} \circ T_{2d}^n \circ S_L^k \circ S_l^L(x_0) \text{ (again by Assertion 1 of Lemma 1)} \\
&= S_L^{2L} \circ T_{2d}^n \circ S_L^k \circ S_l^L(x_0) \text{ (by (5) since } T_{2d}^n \circ S_L^k \circ S_l^L(x_0) \in \mathbb{F}_{p^{2d}}) \\
&= S_L^k \circ S_L^{2L} \circ S_l^L \circ T_{2d}^n(x_0) \\
&= S_L^k \circ S_l^{2L} \circ T_{2d}^n(x_0) \text{ (by Assertion 1 of Lemma 1)} \\
&= \frac{k}{L} S_l^{2L} \circ T_{2d}^n(x_0) \text{ (by (4))} \\
&= \frac{k}{L} S_e^{2d} \circ T_{2d}^n(x_0) \text{ (by (6) since } T_{2d}^n(x_0) \in \mathbb{F}_{p^{2d}}) \\
&= \frac{k}{L} S_e^n(x_0) = \frac{k}{L} S_e^{2e} \circ T_{2e}^n(x_0) \text{ (once again by Assertion 1 of Lemma 1).}
\end{aligned}$$

Therefore, if $p|\frac{k}{L}$, then it holds

$$S_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \mid S_d^n(a) = 0\}, \tag{17}$$

and if $p \nmid \frac{k}{L}$, then it holds

$$S_l^k(\mathbb{F}_{p^n}) \subset \{a \in \mathbb{F}_{p^n} \mid T_e^{2e} \circ S_d^n(a) = 0\} \tag{18}$$

since $T_e^{2e} \circ S_d^n(S_l^k(x_0)) = T_e^{2e} \circ S_e^{2e} \circ T_{2e}^n(x_0) = 0$. By the second assertion of Theorem 3, if $p|\frac{k}{L}$ then the size of $S_l^k(\mathbb{F}_{p^n})$ equals the degree of S_d^n and when $p \nmid \frac{k}{L}$ then it equals the degree of $T_e^{2e} \circ S_d^n$. It follows that the inclusions (17) and

(18) are actually equalities. That is, the if and only if conditions for $S_l^k(X) = a$ to have an $\mathbb{F}_{p^n}-$solution are justified.

If $S_d^n(a) = 0$, then for $x_0 = T_l^{2l}(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}} (-1)^i)$,

$$\begin{aligned} S_l^k(x_0) &= T_k^{2k}(\sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}} (-1)^i) \text{ (by Assertion 2 of Lemma 1)} \\ &= \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} a^{p^{ki}} (-1)^i + \sum_{i=1}^{\frac{n}{d}-1} \sum_{j=i+1}^{\frac{n}{d}} \delta^{p^{kj}} a^{p^{ki}} (-1)^{i-1} \\ &= a - \delta S_d^n(a) = a. \end{aligned}$$

This finishes the proof of case 1.

Now, suppose that $T_e^{2e} \circ S_d^n(a) = 0$, i.e., $S_d^n(a)^{p^e} = -S_d^n(a)$. Then, $\frac{l}{e}$ is odd since it is prime to $\frac{n}{e} = \frac{d}{e} \cdot \frac{n}{d}$ which is even, and hence $T_l^{2l}(S_d^n(a)) = S_d^n(a) + S_d^n(a)^{p^l} = 0$. Thus, for $y_0 = \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} (-1)^i$ one has

$$\begin{aligned} T_k^{2k}(y_0) &= \sum_{i=0}^{\frac{n}{d}-2} \sum_{j=i+1}^{\frac{n}{d}-1} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} (-1)^i + \sum_{i=1}^{\frac{n}{d}-1} \sum_{j=i+1}^{\frac{n}{d}} \delta^{p^{kj}} T_l^{2l}(a)^{p^{ki}} (-1)^{i-1} \\ &= T_l^{2l}(a) - \delta S_d^n(T_l^{2l}(a)) = T_l^{2l}(a). \end{aligned}$$

Since $T_k^{2k}(y_0) = T_l^{2l} \circ S_l^k(y_0)$ (by Assertion 2 of Lemma 1), we have

$$\beta := a - S_l^k(y_0) \in \ker(T_l^{2l}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^{2e}} \subset \mathbb{F}_{p^{2d}}.$$

Now,

$$\begin{aligned} S_l^k\left(S_d^{2d}(\beta\delta_1)\right) &= S_l^k\left(S_L^{2L}(\beta\delta_1)\right) \text{ (by (5))} \\ &= S_L^k \circ S_l^L\left(S_L^{2L}(\beta\delta_1)\right) \text{ (by Assertion 1 of Lemma 1)} \\ &= S_L^k \circ \left(S_l^{2L}(\beta\delta_1)\right) \text{ (by Assertion 1 of Lemma 1)} \\ &= \frac{k}{L} S_l^{2L}(\beta\delta_1) \text{ (by (4))} \\ &= \frac{k}{L} S_e^{2d}(\beta\delta_1) \text{ (by (6))} \\ &= \frac{k}{L} S_e^{2e} \circ T_{2e}^{2d}(\beta\delta_1) \text{ (by Assertion 1 of Lemma 1)} \\ &= \frac{k}{L} S_e^{2e}(\beta T_{2e}^{2d}(\delta_1)) = \frac{k}{L} S_e^{2e}(\beta) = \frac{k}{L}(\beta - \beta^{p^e}). \end{aligned}$$

Since $\beta \in \ker(T_l^{2l}) \cap \mathbb{F}_{p^{2e}} = S_e^{2e}(\mathbb{F}_{p^{2e}})$ (Theorem 1), it holds $\beta + \beta^{p^e} = 0$ and thus we get

$$S_l^k\left(S_d^{2d}(\beta\delta_1)\right) = \frac{2k}{L}\beta.$$

That is,

$$S_l^k(y_0 + \frac{L}{2k} S_d^{2d}((a - S_l^k(y_0))\delta_1)) = a.$$

This finishes the proof of case 2.

If $\frac{n}{d} = \frac{[n,k]}{k}$ is odd, then by Theorem 3, S_l^k is a permutation on $\mathbb{F}_{p^n}$ and the equation $S_l^k(X) = a$ has a unique $\mathbb{F}_{p^n}-$solution. In fact, applying Assertion 2 of Lemma 1 twice yields

$$S_l^k(T_l^{2l} \circ S_k^{[n,k]}(a/2)) = T_k^{2k} \circ S_k^{[n,k]}(a/2) = T_{[n,k]}^{2[n,k]}(a/2) = a.$$

□

5 Conclusion

We explicitly determined the sets of preimages of linearized polynomials

$$T_l^k(X) := \sum_{i=0}^{\frac{k}{l}-1} X^{p^{li}},$$
$$S_l^k(X) := \sum_{i=0}^{\frac{k}{l}-1} (-1)^i X^{p^{li}},$$

over the finite field $\mathbb{F}_{p^n}$ for any characteristic p and any integer $n \geq 1$. In particular, another solution for the case $p = 2$, which was solved very recently in [10], was obtained in Theorem 1 and Theorem 4.

Acknowledgement

The authors are grateful to the Associate Editor and the anonymous reviewers for their valuable comments and precious suggestions which have highly improved the manuscript.

References

1. I. Blake, G. Seroussi and N. Smart. Elliptic Curves in Cryptography. Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
2. C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397, 2010.
3. C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469, 2010.
4. B. Csajbók. Scalar $q-$subresultants and Dickson matrices. *Journal of Algebra*, 547, pp. 116 -128, 2020.

5. B. Csajbók, G. Marino, O. Polverino and F. Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56, pp. 109-130, 2019.
6. K.H. Kim, J. Choe and S. Mesnager. Solving $X^{q+1} + X + a = 0$ over Finite Fields. https://arxiv.org/abs/1912.12648, 2019.
7. K.H. Kim and 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*, Vol. 63, 101630, 2020. https://doi.org/10.1016/j.ffa.2019.101630
8. R. Lidl and H. Niederreiter, Finite Fields, volume 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second edition, 1997.
9. 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, pp. 68-91, 2019.
10. 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 $\mathbb{F}_{2^n}$. *Cryptography and Communications*, 2020. https://doi.org/10.1007/s12095-020-00425-3
11. S. Mesnager, K.H. Kim, J. Choe and C. Tang. On the Menezes-Teske-Weng's conjecture. *Cryptography and Communications*, 12(1), pp. 19-27, 2020.
12. S. Mesnager, K.H. Kim and M.S. Jo. On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic Boolean functions. *Cryptography and Communications*, 2019. https://doi.org/10.1007/s12095-019-00410-5
13. O. Polverino and F. Zullo On the number of roots of some linearized polynomials. arXiv:1909.00802, 2019.
14. B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22, pp. 79-100, 2013.
15. C. Zanella. A condition for scattered linearized polynomials involving Dickson matrices. *Journal of Geometry*, 110.3:50, 2019.