Solutions of $x^{q^k} + \cdots + x^q + x = a$ in $\mathbb{F}_{2^n}$

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

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

[4] LAGA, Department of Mathematics, University of Paris VIII and Paris XIII, CNRS and Telecom ParisTech, France smesnager@univ-paris8.fr

Abstract. Though it is well known that the roots of any affine polynomial over finite field can be computed by a system of linear equations by using a normal base of the field, such solving approach appears to be difficult to apply when the field is fairly large. Thus, it may be of great interest to find explicit representation of the solutions independently of the field base. This was previously done only for quadratic equations over binary finite field. This paper gives explicit representation of solutions for much wider class of affine polynomials over binary prime field.
Keywords: Linear equation · Binary finite field · Base of field · Zeros of polynomials · Irreducible polynomials.

1 Introduction

Define

$$T_l^k(x) := x + x^{2^l} + \cdots + x^{2^{l(k/l-2)}} + x^{2^{l(k/l-1)}}$$

when $l|k$, and in particular

$$T_k(x) := T_1^k(x) = x + x^2 + \cdots + x^{2^{k-2}} + x^{2^{k-1}}.$$

The degree of the polynomial $T_l^k(x)$ is 2^{k-l}.

This paper gives the explicit representations of all $\overline{\mathbb{F}_2}-$ and $\mathbb{F}_{2^n}-$solutions to the affine equation

$$T_l^k(x) = a, a \in \mathbb{F}_{2^n}.$$

Obviously, this equation has no multiple roots since $(T_l^k)' = 1 \neq 0$. Throughout this paper, we set $d = \gcd(n, k)$.

To the best of our knowledge, following is the only previous result in this direction.

Lemma 1. *(Page 26 of [1], 11.1.120 of [2]) The quadratic equation*

$$x^2 + x + a = 0, a \in \mathbb{F}_{2^n}$$

has solutions in $\mathbb{F}_{2^n}$ *if and only if*

$$T_n(a) = 0.$$

Let us assume $T_n(a) = 0$. *Let* δ *be an element in* $\mathbb{F}_{2^n}$ *such that* $T_n(\delta) = 1$ *(if* n *is odd, then one can take* $\delta = 1$*). Then,*

$$x_0 = \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n-1} \delta^{2^j} \right) a^{2^i}$$

is a solution to the equation.

2 Some useful facts

Lemma 2. *For any positive integers* k, k', l, l' *such that* $s|l|k$ *and* $l'|k'$, *followings hold.*

1. *(Commutativity)*
$$T_l^k \circ T_{l'}^{k'} = T_{l'}^{k'} \circ T_l^k.$$
2. *(Transitivity)*
$$T_l^k \circ T_s^l = T_s^k.$$
3. $$T_k \circ T_2(x) = T_k^{2k}(x) = x + x^{2^k}.$$
4. $$T_k \circ T_k \circ T_2 = T_{2k}.$$

Proof. All statements can be easily checked by direct calculation. □

Lemma 3. *For any positive integers* n *and* k, *it holds*

$$T_k(x) \in \mathbb{F}_{2^n} \iff T_n(x) \in \mathbb{F}_{2^k}.$$

In particular, letting $k = 1$, *we have*

$$x \in \mathbb{F}_{2^n} \iff T_n(x) \in \mathbb{F}_2 \iff T_n \circ T_2(x) = 0.$$

Proof. Since $T_k(x) + T_k(x)^{2^n} = T_n(x) + T_n(x)^{2^k}$ which is checked by direct computation, it follows $T_k(x) \in \mathbb{F}_{2^n} \iff T_k(x)^{2^n} = T_k(x) \iff T_k(x) + T_k(x)^{2^n} = 0 \iff T_n(x) + T_n(x)^{2^k} = 0 \iff T_n(x) \in \mathbb{F}_{2^k}$. □

Following fact, though already well-known, can be reformulated.

Corollary 4. *Let* l *be a divisor of* k. *Then,*

$$T_l^k(\mathbb{F}_{2^k}) = \mathbb{F}_{2^l}.$$

Proof. This follows from the fact that $T_l(T_l^k(\mathbb{F}_{2^k})) = T_k(\mathbb{F}_{2^k}) = \mathbb{F}_2$. □

Theorem 5. *Let us assume* $\gcd(n,k)=1$. *Then it holds*

$$T_k(x)\in\mathbb{F}_{2^n}\iff x\in\mathbb{F}_{2^n}+\mathbb{F}_{2^k},$$

where $\mathbb{F}_{2^n}+\mathbb{F}_{2^k}=\{a+b\,|\,a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^k}\}$.

Proof. ($\Longleftarrow$)
Let $x=a+b$ for $a\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_{2^k}$. Then $a^{2^n}=a$, and $T_k(b)\in\mathbb{F}_2$ by above proposition, thus

$$\begin{aligned}T_k(a+b)^{2^n}&=(T_k(a)+T_k(b))^{2^n}\\&=T_k(a)^{2^n}+T_k(b)^{2^n}\\&=T_k(a^{2^n})+T_k(b)\\&=T_k(a)+T_k(b)=T_k(a+b),\end{aligned}$$

where the linearity of T_k was exploited. That is $T_k(x)=T_k(a+b)\in\mathbb{F}_{2^n}$.

($\Longrightarrow$)
Since the necessity in the statement has been proved, in order to prove the sufficiency in the statement, it is enough to show

$$\#\{x\in\overline{\mathbb{F}_2}\,|\,T_k(x)\in\mathbb{F}_{2^n}\}=\#\{\mathbb{F}_{2^n}+\mathbb{F}_{2^k}\},$$

where $\overline{\mathbb{F}_2}$ is the algebraic closure of $\mathbb{F}_2$. To begin with, we have $\#\{x\in\overline{\mathbb{F}_2}\,|\,T_k(x)\in\mathbb{F}_{2^n}\}=2^{n+k-1}$ because for every $a\in\mathbb{F}_{2^n}$ the equation $T_k(x)=a$ has 2^{k-1} different solutions.

On the other hand, it also holds $\#\{\mathbb{F}_{2^n}+\mathbb{F}_{2^k}\}=2^{n+k-1}$. In fact, for $a,a'\in\mathbb{F}_{2^n}$ and $b,b'\in\mathbb{F}_{2^k}$, it holds $a+b=a'+b'\iff a+a'=b+b'\in\mathbb{F}_{2^n}\cap\mathbb{F}_{2^k}=\mathbb{F}_2$, i.e., ($a=a'$ and $b=b'$) or ($a=a'+1$ and $b=b'+1$). Therefore $\#\{\mathbb{F}_{2^n}+\mathbb{F}_{2^k}\}=\#\{a+b\,|\,a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^k}\}=(2^n\cdot 2^k)/2=2^{n+k-1}$. □

Without the condition $\gcd(n,k)=1$, we give:

Theorem 6. *It holds*

$$\{x\in\overline{\mathbb{F}_2}\,|\,T_k(x)\in\mathbb{F}_{2^n}\}=\{T_n^{[n,k]}\circ T_k^{[n,k]}\circ T_2(x)\,|\,x\in\mathbb{F}_{2^{2[n,k]}}\}(\subset\mathbb{F}_{2^{2[n,k]}}),$$

where $[n,k]$ *is the least common multiple of two integers* n *and* k.

Proof. Let $L=[n,k]$. Let us set $y=T_n^L\circ T_k^L\circ T_2(x)$ for $x\in\mathbb{F}_{2^{2L}}$. To begin with, we will show $T_n\circ T_k(y)\in\mathbb{F}_2$ which is equivalent to $T_k(y)\in\mathbb{F}_{2^n}$ by Lemma 3. In fact,

$$T_n\circ T_k(y)=T_n^L\circ T_n\circ T_k^L\circ T_k\circ T_2(x)=T_L\circ T_L\circ T_2(x)=T_{2L}(x)\in\mathbb{F}_2,$$

where the equalities are from Lemma 3, except for the last equality which is from Lemma 2.

Obviously, the cardinality of the left side set is 2^{n+k-1}. On the other hand, the cardinality of the right side set is also 2^{n+k-1} as it equals $2^{2L-(L-n)-(L-k)-1}=2^{n+k-1}$ and so the two sets coincide. □

Example 7. By Theorem 5, we know that $\{x \in \overline{\mathbb{F}_2} \mid T_k(x) \in \mathbb{F}_{2^n}\} \subset \mathbb{F}_{2^{nk}} = \mathbb{F}_{2^{[n,k]}}$ when $\gcd(n,k) = 1$. However, it is not always the case. Let us consider the case $n = k = 2$.

$$\begin{aligned}
&\{x \in \overline{\mathbb{F}_2} \mid T_2(x) \in \mathbb{F}_{2^2}\} = \{x \in \overline{\mathbb{F}_2} \mid x + x^2 + x^4 + x^8 = 0\} \\
&= \{x \in \overline{\mathbb{F}_2} \mid (x + x^2)(1 + x + x^2)(1 + x + x^4) = 0\}.
\end{aligned}$$

The least field that contains this set is $\mathbb{F}_{2^4} = \mathbb{F}_{2^{2[2,2]}}$.

That is, generally, $\mathbb{F}_{2^{2[n,k]}}$ is the smallest field including

$$\{x \in \overline{\mathbb{F}_2} \mid T_k(x) \in \mathbb{F}_{2^n}\}.$$

Proposition 8. *When $a \in \mathbb{F}_{2^n}$,*

$$T_k^{[n,k]}(a) = T_d^n(a) = T_{n-k}^{[n,n-k]}(a).$$

Proof. By definition $T_k^{[n,k]}(a) = \sum_{i=0}^{\frac{[n,k]}{k}-1} a^{2^{ik}}$, $T_d^n(a) = \sum_{j=0}^{\frac{n}{d}-1} a^{2^{jd}}$ and $T_{n-k}^{[n,n-k]}(a) = \sum_{i=0}^{\frac{[n,n-k]}{n-k}-1} a^{2^{i(n-k)}}$. Note that the upper bounds of indices in three summations are identical: $\frac{[n,k]}{k} = \frac{n}{d} = \frac{[n,n-k]}{n-k}$. It is easy to check $\{ik \mod n \mid 0 \leq i \leq \frac{[n,k]}{k} - 1\} = \{jd \mid 0 \leq j \leq \frac{n}{d} - 1\} = \{i(n-k) \mod n \mid 0 \leq i \leq \frac{[n,n-k]}{n-k} - 1\}$. Since $a^{2^n} = a$, all three summations are identical. □

3 Zeros of T_l^k

Lemma 9. *Followings are facts.*

1. $$\{x \in \overline{\mathbb{F}_2} \mid T_k(x) = 0\} = T_2(\mathbb{F}_{2^k}) = \{x + x^2 \mid x \in \mathbb{F}_{2^k}\}.$$

2. $$\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = T_2(\mathbb{F}_{2^k}) \cap \mathbb{F}_{2^n} = \{x + x^2 \in \mathbb{F}_{2^n} \mid x \in \mathbb{F}_{2^k}\}.$$

In particular,

– *If $\frac{k}{d}$ is odd, then*

$$\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = \{x \in \mathbb{F}_{2^d} \mid T_d(x) = 0\}.$$

– *If $\frac{k}{d}$ is even, then*

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

Proof. For $x \in \mathbb{F}_{2^k}$, by Lemma 2, $T_k(T_2(x)) = x + x^{2^k} = 0$, and the two sets $\{x \in \overline{\mathbb{F}_2} \mid T_k(x) = 0\}$ and $T_2(\mathbb{F}_{2^k})$ have the same cardinality 2^{k-1} and so they coincide. As a immediate consequence, we have $\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = T_2(\mathbb{F}_{2^k}) \cap \mathbb{F}_{2^n}$.

Thus, $\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = T_2(\mathbb{F}_{2^k}) \cap \mathbb{F}_{2^n} \subset \mathbb{F}_{2^d}$, and so $\{x \in \mathbb{F}_{2^n} \mid T_k(x) = 0\} = \{x \in \mathbb{F}_{2^d} \mid T_k(x) = 0\} = \{x \in \mathbb{F}_{2^d} \mid \frac{k}{d} T_d(x) = 0\}$, which completes the proof. □

Lemma 10. *Let l be a divisor of k. Followings are facts.*

1.
$$\{x \in \overline{\mathbb{F}_2} \,|\, T_l^k(x) = 0\} = T_l \circ T_2(\mathbb{F}_{2^k}) = \{x + x^{2^l} \,|\, x \in \mathbb{F}_{2^k}\}.$$

2.
$$\{x \in \mathbb{F}_{2^n} \,|\, T_l^k(x) = 0\} = T_l \circ T_2(\mathbb{F}_{2^k}) \cap \mathbb{F}_{2^n} = \{x + x^{2^l} \in \mathbb{F}_{2^n} \,|\, x \in \mathbb{F}_{2^k}\}.$$

In particular,

– *If $\frac{k}{[d,l]}$ is odd, then*
$$\{x \in \mathbb{F}_{2^n} \,|\, T_l^k(x) = 0\} = \{x \in \mathbb{F}_{2^d} \,|\, T_{(d,l)}^d(x) = 0\} = T_{(d,l)} \circ T_2(\mathbb{F}_{2^d}).$$

– *If $\frac{k}{[d,l]}$ is even, then*
$$\{x \in \mathbb{F}_{2^n} \,|\, T_l^k(x) = 0\} = \mathbb{F}_{2^d}.$$

Proof. Since $T_l^k(T_l \circ T_2(\mathbb{F}_{2^k})) = T_k \circ T_2(\mathbb{F}_{2^k}) = 0$, the set $T_l \circ T_2(\mathbb{F}_{2^k})$ with cardinality 2^{k-l} is a subset of $\{x \in \overline{\mathbb{F}_2} \,|\, T_l^k(x) = 0\}$ with the same cardinality 2^{k-l}, i.e., the two sets coincide. Thus, $\{x \in \mathbb{F}_{2^n} \,|\, T_l^k(x) = 0\} = T_l \circ T_2(\mathbb{F}_{2^k}) \cap \mathbb{F}_{2^n} \subset \mathbb{F}_{2^d}$, and we have

$$\begin{aligned}
&\{x \in \mathbb{F}_{2^n} \,|\, T_l^k(x) = 0\} = \{x \in \mathbb{F}_{2^d} \,|\, T_l^k(x) = 0\} \\
&= \{x \in \mathbb{F}_{2^d} \,|\, \frac{k}{[d,l]} T_l^{[d,l]}(x) = 0\} \\
&= \begin{cases} \mathbb{F}_{2^d}, & \text{if } \frac{k}{[d,l]} \text{ is even,} \\ \{x \in \mathbb{F}_{2^d} \,|\, T_{(d,l)}^d(x) = 0\} = T_{(d,l)} \circ T_2(\mathbb{F}_{2^d}), & \text{if } \frac{k}{[d,l]} \text{ is odd,} \end{cases}
\end{aligned}$$

where Proposition 8 was used for the last equality. □

4 Expression of solutions in closed field

Proposition 11. *Let L be any positive integer. For any $a \in \mathbb{F}_{2^L}^*$ and $\xi \in \mu_{2^L+1} \setminus \{1\}$,*

$$\frac{a}{\xi + 1} + \mathbb{F}_{2^L} = \{\frac{a}{\xi' + 1} \,|\, \xi' \in \mu_{2^L+1} \setminus \{1\}\}.$$

Proof. Let $\eta \in \mathbb{F}_{2^L}$. Then we will show

$$\frac{a}{\xi + 1} + \eta = \frac{a}{\xi' + 1}$$

for some $\xi' \in \mu_{2^L+1} \setminus \{1\}$. Since $\frac{a}{\xi+1} + \eta = \frac{a}{\frac{a\xi+\eta\xi+\eta}{a+\eta\xi+\eta}+1}$, it is enough to show

$$\xi' = \frac{a\xi + \eta\xi + \eta}{a + \eta\xi + \eta} \in \mu_{2^L+1} \setminus \{1\}.$$

In fact, obviously $\xi' \neq 1$ and

$$\xi'^{2^L} = \frac{a\xi^{2^L} + \eta\xi^{2^L} + \eta}{a + \eta\xi^{2^L} + \eta} = \frac{a/\xi + \eta/\xi + \eta}{a + \eta/\xi + \eta} = 1/\xi'.$$

□

Theorem 12. *Let $a \in \mathbb{F}_{2^n}^*$. Let L be any multiple of the least common multiple $[n, k]$ of two integers n and k. Then, for any $\xi \in \mu_{2^L+1} \setminus \{1\}$,*

$$x_0 = T_k^L \circ T_2(\frac{a}{\xi + 1})$$

is a solution to the equation $T_k(x) = a$. In fact, for any $\xi \in \mu_{2^L+1} \setminus \{1\}$,

$$\begin{aligned}\{x \in \overline{\mathbb{F}_2} \,|\, T_k(x) = a\} &= \{T_k^L \circ T_2(\frac{a}{\zeta + 1}) \,|\, \zeta \in \mu_{2^L+1} \setminus \{1\}\} \\ &= T_k^L \circ T_2(\frac{a}{\xi + 1} + \mathbb{F}_{2^L}) \\ &= T_k^L \circ T_2(\frac{a}{\xi + 1}) + T_2(\mathbb{F}_{2^k}).\end{aligned}$$

Proof. Let us set $x = T_k^L \circ T_2(\frac{a}{\xi+1})$ for $\xi \in \mu_{2^L+1}$. Then, by Lemma 2, one has

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

On the other hand, $\#\{x \in \overline{\mathbb{F}_2} \,|\, T_k(x) = a\} = 2^{k-1}$, and $\#T_k^L \circ T_2(\frac{a}{\xi+1} + \mathbb{F}_{2^L}) = \#T_k^L \circ T_2(\mathbb{F}_{2^L}) = T_2(\mathbb{F}_{2^k}) = 2^{k-1}$. This completes the proof. □

Corollary 13. *Let $a \in \mathbb{F}_{2^n}$ and l be a divisor of k. Let L be any multiple of the least common multiple $[n, k]$ of two integers n and k. Then, for any $\xi \in \mu_{2^L+1} \setminus \{1\}$,*

$$x_0 = T_l \circ T_k^L \circ T_2(\frac{a}{\xi + 1})$$

is a solution to the equation $T_l^k(x) = a$. In fact, for any $\xi \in \mu_{2^L+1} \setminus \{1\}$,

$$\begin{aligned}\{x \in \overline{\mathbb{F}_2} \,|\, T_l^k(x) = a\} &= \{T_l \circ T_k^L \circ T_2(\frac{a}{\zeta + 1}) \,|\, \zeta \in \mu_{2^L+1} \setminus \{1\}\} \\ &= T_l \circ T_k^L \circ T_2(\frac{a}{\xi + 1} + \mathbb{F}_{2^L}) \\ &= T_l \circ T_k^L \circ T_2(\frac{a}{\xi + 1}) + T_l \circ T_2(\mathbb{F}_{2^k}).\end{aligned}$$

Note that it is easy to take $\xi \in \mu_{2^L+1} \setminus \{1\}$: Choose any $s \in \mathbb{F}_{2^{2L}} \setminus \mathbb{F}_{2^L}$, then calculate $\xi = s^{2^L-1}$.

5 Solutions in $\mathbb{F}_{2^n}$

Theorem 14. *For $a \in \mathbb{F}_{2^n}$, the linear equation*

$$T_k^{2k}(x) = a \text{ (i.e. } x^{2^k} + x = a) \tag{1}$$

has solution in $\mathbb{F}_{2^n}$ if and only if

$$T_d^n(a) = 0. \tag{2}$$

When $T_d^n(a) = 0$, this equation $T_k^{2k}(x) = a$ has exactly 2^d solutions in $\mathbb{F}_{2^n}$:

– *If $\frac{k}{d}$ is odd, then for any $\xi \in \mu_{2^n+1} \setminus \{1\}$*

$$\{x \in \mathbb{F}_{2^n} \mid x^{2^k} + x = a\} = T_k^{[n,k]}(\frac{a}{\xi+1}) + \mathbb{F}_{2^d}. \tag{3}$$

– *If $\frac{k}{d}$ is even, then for any $\xi \in \mu_{2^n+1} \setminus \{1\}$*

$$\{x \in \mathbb{F}_{2^n} \mid x^{2^k} + x = a\} = T_{n-k}^{[n,n-k]}(\frac{a^{2^{n-k}}}{\xi+1}) + \mathbb{F}_{2^d}. \tag{4}$$

Proof. This easily follows from the fact that the linear operator $T_k^{2k}(x) = x^{2^k} + x$ on $\mathbb{F}_{2^n}$ has the kernel of dimension d and, thus, the number of elements in the image of T_k^{2k} is 2^{n-d}. For any $x \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} T_d^n(x^{2^k} + x) &= T_d^n(x^{2^k}) + T_d^n(x) \\ &= T_d^n(x)^{2^k} + T_d^n(x) \\ &= T_d^n(x) + T_d^n(x) \text{ (since } T_d^n(x) \subset \mathbb{F}_{2^d} \subset \mathbb{F}_{2^k}) \\ &= 0 \end{aligned}$$

leading to the conclusion that the image of T_k^{2k} contains such all elements in $\mathbb{F}_{2^n}$ since the total number of such elements in $\mathbb{F}_{2^n}$ is exactly 2^{n-d}.

Let us prove the second part of the theorem. First, let us assume $\frac{k}{d}$ is odd. Then, $x_0 = T_k^{[n,k]}(\frac{a}{\xi+1})$ is a solution to the equation since $T_k \circ T_2(T_k^{[n,k]}(\frac{a}{\xi+1})) = T_{[n,k]} \circ T_2(\frac{a}{\xi+1}) = \frac{a}{\xi+1} + (\frac{a}{\xi+1})^{2^{[n,k]}} = a$. On the other hand, under the condition $T_d^n(a) = 0$, this solution really belongs to $\mathbb{F}_{2^n}$. In fact, $x_0 + x_0^{2^n} = T_k^{[n,k]}(\frac{a}{\xi+1} + (\frac{a}{\xi+1})^{2^n}) = T_k^{[n,k]}(a) = T_d^n(a) = 0$.

If $\frac{k}{d}$ is even, then we will consider a new equation $x^{2^{n-k}} + x = a^{2^{n-k}}$ instead of the original equation $x^{2^k} + x = a$. As obvious, this new equation shares the same $\mathbb{F}_{2^n}$-solution set with the original equation. Since $\frac{n-k}{d}$ is odd as $\frac{k}{d}$ is even, we can apply the solution formula (3) for odd case to this new equation. □

Corollary 15. *For any $\xi \in \mu_{2^n+1} \setminus \{1\}$, $x_0 = T_n(\frac{a}{\xi+1})$ and $x_0 + 1$ are solutions of $x^2 + x + a = 0$. These solutions are in $\mathbb{F}_{2^n}$ if and only if*

$$T_n(a) = 0.$$

Theorem 16. *Let $a \in \mathbb{F}_{2^n}$. Consider the linear equation*

$$T_k(x) = a \text{ (i.e. } x + x^2 + \cdots + x^{2^{k-1}} = a) \tag{5}$$

1. *Let $\frac{k}{d}$ be odd. Then, equation (5) has a solution in $\mathbb{F}_{2^n}$ if and only if*

$$T_d^n(a) \in \mathbb{F}_2. \tag{6}$$

When $T_d^n(a) \in \mathbb{F}_2$, the equation $T_k(x) = a$ has exactly 2^{d-1} solutions in $\mathbb{F}_{2^n}$: for any $\xi \in \mu_{2^n+1} \setminus \{1\}$

$$\{x \in \mathbb{F}_{2^n} \,|\, T_k(x) = a\} = T_2 \circ T_k^{[n,k]}(\frac{a}{\xi + 1}) + T_2(\mathbb{F}_{2^d}). \tag{7}$$

2. *Let $\frac{k}{d}$ be even. Then, equation (5) has a solution in $\mathbb{F}_{2^n}$ if and only if*

$$T_d^n(a) = 0. \tag{8}$$

When $T_d^n(a) = 0$, the equation $T_k(x) = a$ has exactly 2^d solutions in $\mathbb{F}_{2^n}$: for any $\xi \in \mu_{2^n+1} \setminus \{1\}$

$$\{x \in \mathbb{F}_{2^n} \,|\, T_k(x) = a\} = T_2 \circ T_{n-k}^{[n,n-k]}(\frac{a^{2^{n-k}}}{\xi + 1}) + \mathbb{F}_{2^d}. \tag{9}$$

Proof. Since $T_d^n(\mathbb{F}_{2^n}) = \mathbb{F}_{2^d}$ by Corollary 4, one has

$$T_d^n(T_k(\mathbb{F}_{2^n})) = T_k(T_d^n(\mathbb{F}_{2^n})) = T_k(\mathbb{F}_{2^d}) = \begin{cases} \mathbb{F}_2, & \text{if } \frac{k}{d} \text{ is odd} \\ 0, & \text{if } \frac{k}{d} \text{ is even.} \end{cases} \tag{10}$$

Let us assume $\frac{k}{d}$ is odd. By Corollary 9, we have $\#T_k(\mathbb{F}_{2^n}) = 2^{n-d+1}$. Since $\#\{x \in \overline{\mathbb{F}_2} \,|\, T_d^n(x) \in \mathbb{F}_2\} = 2^{n-d+1}$ as obvious, by (10) we have $\{x \in \overline{\mathbb{F}_2} \,|\, T_d^n(x) \in \mathbb{F}_2\} = T_k(\mathbb{F}_{2^n})$, i.e. $T_k(x) = a$ has a solution in $\mathbb{F}_{2^n}$ if and only if $T_d^n(a) \in \mathbb{F}_2$.

At this time, let us assume $\frac{k}{d}$ is even. Then, by Corollary 9, $\#T_k(\mathbb{F}_{2^n}) = 2^{n-d}$. Since $\#\{x \in \overline{\mathbb{F}_2} \,|\, T_d^n(x) = 0\} = 2^{n-d}$, from (10) it follows $\{x \in \overline{\mathbb{F}_2} \,|\, T_d^n(x) = 0\} = T_k(\mathbb{F}_{2^n})$, i.e., $T_k(x) = a$ has a solution in $\mathbb{F}_{2^n}$ if and only if $T_d^n(a) = 0$.

The assertions about the solution number are consequences of Corollary 9. The solution formulas were deduced from (3), (4) and the fact that if $T_k \circ T_2(x) = a$, then $y = T_2(x)$ is solution to $T_k(y) = 0$. ∎

Theorem 17. *Let $a \in \mathbb{F}_{2^n}$. Consider the linear equation*

$$T_l^k(x) = a \text{ (i.e. } x + x^{2^l} + \cdots + x^{2^{l(\frac{k}{l}-1)}} = a) \tag{11}$$

1. Let $\frac{k}{[d,l]}$ be odd. Then, the equation (11) *has a solution in $\mathbb{F}_{2^n}$ if and only if*

$$T_d^n(a) \in \mathbb{F}_{2^{(d,l)}}. \tag{12}$$

When $T_d^n(a) \in \mathbb{F}_{2^{(d,l)}}$, the equation (11) *has exactly $2^{d-(d,l)}$ solutions in $\mathbb{F}_{2^n}$:*

– *If $\frac{k}{d}$ is odd, then for any $\xi \in \mu_{2^n+1} \setminus \{1\}$*

$$\{x \in \mathbb{F}_{2^n} \mid T_l^k(x) = a\} = T_l \circ T_2 \circ T_k^{[n,k]}(\frac{a}{\xi+1}) + T_{(d,l)} \circ T_2(\mathbb{F}_{2^d}). \tag{13}$$

– *If $\frac{k}{d}$ is even, then for any $\xi \in \mu_{2^d+1} \setminus \{1\}$*

$$\{x \in \mathbb{F}_{2^n} \mid T_l^k(x) = a\} = T_l \circ T_2 \circ T_{n-k}^{[n,n-k]}(\frac{a^{2^{n-k}}}{\xi+1}) + T_{(d,l)} \circ T_2(\frac{T_d^n(a)}{\xi+1}) + T_{(d,l)} \circ T_2(\mathbb{F}_{2^d}). \tag{14}$$

2. Let $\frac{k}{[d,l]}$ be even. Then, the equation (11) *has a solution in $\mathbb{F}_{2^n}$ if and only if*

$$T_d^n(a) = 0. \tag{15}$$

When $T_d^n(a) = 0$, the equation (11) *has exactly 2^d solutions in $\mathbb{F}_{2^n}$: for any $\xi \in \mu_{2^d+1} \setminus \{1\}$*

$$\{x \in \mathbb{F}_{2^n} \mid T_l^k(x) = a\} = T_l \circ T_2 \circ T_{n-k}^{[n,n-k]}(\frac{a^{2^{n-k}}}{\xi+1}) + \mathbb{F}_{2^d}. \tag{16}$$

Proof. It holds

$$\begin{aligned} T_d^n(T_l^k(\mathbb{F}_{2^n})) &= T_l^k(T_d^n(\mathbb{F}_{2^n})) \\ &= T_l^k(\mathbb{F}_{2^d}) = \frac{k}{[d,l]} T_l^{[d,l]}(\mathbb{F}_{2^d}) \\ &= \frac{k}{[d,l]} T_{(d,l)}^d(\mathbb{F}_{2^d}) \text{ by Proposition 8} \\ &= \begin{cases} 0, & \text{if } \frac{k}{[d,l]} \text{ is even,} \\ \mathbb{F}_{2^{(d,l)}}, & \text{if } \frac{k}{[d,l]} \text{ is odd,} \end{cases} \end{aligned}$$

and on the other hand, Corollary 10 let us know

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

Since $T_d^n(x) = a$ has 2^{n-d} solutions in the closed field (indeed in $\mathbb{F}_{2^n}$), thus we conclude

$$T_l^k(\mathbb{F}_{2^n}) = \begin{cases} \{a \in \mathbb{F}_{2^n} \mid T_d^n(a) = 0\}, & \text{if } \frac{k}{[d,l]} \text{ is even,} \\ \{a \in \mathbb{F}_{2^n} \mid T_d^n(a) \in \mathbb{F}_{2^{(d,l)}}\}, & \text{if } \frac{k}{[d,l]} \text{ is odd,} \end{cases}$$

which is just the sufficient and necessary condition for existence of solution in $\mathbb{F}_{2^n}$.

When $\frac{k}{[d,l]}$ be odd and $\frac{k}{d}$ is even, the solution formula can be checked as follows: Consider $T_d^n(a) \in \mathbb{F}_{2^d}$. First, it can be checked that $z_0 = T_{(d,l)} \circ T_2(\frac{T_d^n(a)}{\xi+1})$ is a solution in $\mathbb{F}_{2^d}$ of $T_l^k(z) = T_d^n(a)$, i.e. $T_{[d,l]}^l(z) = T_d^n(a)$ i.e. $T_{(d,l)}^d(z) = T_d^n(a)$. For $y_0 = T_l \circ T_2 \circ T_{n-k}^{[n,n-k]}(\frac{a^{2^{n-k}}}{\xi+1}) \in \mathbb{F}_{2^n}$, it is 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 solution in $\mathbb{F}_{2^n}$.

In remained cases, the solution formulas are deduced from theorem 16, regarding the fact that $T_l(x_0)$ is solution in $\mathbb{F}_{2^n}$ of $T_l^k(x) = a$ if $x_0 \in \mathbb{F}_{2^n}$ is solution of $T_k(x) = a$. □

As an immediate consequence of these facts, one has (confirms):

Corollary 18. *Followings are true.*

- $T_l^k(x)$ *is a 2-to-1 mapping on* $\mathbb{F}_{2^n}$ *if and only if* $d = 1$ *and* $\frac{k}{l}$ *is even, or,* $d = 2$ *and both* l *and* $\frac{k}{2l}$ *are odd.*
- $T_l^k(x)$ *is a permutation on* $\mathbb{F}_{2^n}$ *if and only if* $\frac{k}{l}$ *is odd and* $d|l$.
  Hence, when $\frac{k}{l}$ *is odd,* $T_l^k(x)$ *is an exceptional polynomial over* $\mathbb{F}_2$.

References

1. I. Blake, G. Seroussi, N. Smart. Elliptic Curves in Cryptography. Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
2. G.L. Mullen and D. Panario. Handbook of Finite Fields. Discrete Mathematics and Its Applications, CRC Press, 2013.