Equations over the finite field $\mathbb{F}_{2^n}$

Sihem Mesnager

University of Paris VIII (department of Mathematics),
University of Paris XIII (LAGA), CNRS and Telecom ParisTech

The 4th International Conference on Boolean functions and their Applications (BFA 2019)
June 18, 2019 Florence, Italy

Outline

1. On some equations in $\mathbb{F}_{2^n}$
2. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $(n,k) = 1$ [joint work with Kwang Ho Kim]
   1. Motivation
   2. Preliminaries
   3. The two related problems for solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $(n,k) = 1$
   4. Solving the two problems
   5. The solution of the equation $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$
3. Conclusions

Notation

- $\mathbb{F}_{2^n}$ the finite field of order 2^n.
- The *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ equals $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

A fundamental equation

Let q be a power of 2.

- The equation $x^q - x = 0$ admits $\mathbb{F}_q$ as set of solutions.
- Finding the solutions in $\mathbb{F}_q$ of an equation $P(x) = 0$ over $\mathbb{F}_q$ is equivalent to finding the solutions of the equation $(P(x), x^q - x) = 0$. The number of solutions equals the degree of $(P(x), x^q - x)$.

Equation of degree 1

The equation $ax + b = 0$, $a \neq 0$, admits one solution $-b/a$, in $\mathbb{F}_q$ in any field.

Equations of degree 2

- A necessary condition for the existence of a solution x in $\mathbb{F}_{2^n}$ of the equation $x^2 + x = \beta$ is that $Tr_1^n(\beta) = 0$.

THEOREM

The solutions of the equation $x^2 + x = \beta$ *are* $x = \sum_{j=1}^{n-1} \beta^{2^j} (\sum_{k=0}^{j-1} c^{2^k})$ *and* $x = 1 + \sum_{j=1}^{n-1} \beta^{2^j} (\sum_{k=0}^{j-1} c^{2^k})$, *where* c *is any (fixed) element such that* $Tr_1^n(c) = 1$.

- $ax^2 + bx + c = 0$, $a \neq 0$ is equivalent to $\left(\frac{ax}{b}\right)^2 + \frac{ax}{b} = \frac{ac}{b^2}$.
- The equation $ax^2 + bx + c = 0$ of degree 2 reduces to solving the equation $x^2 + x = \beta$

Equation $x + x^{2^k} = b$ in $\mathbb{F}_{2^{2n}}$

Define $S_{n,k}(x) = \sum_{i=0}^{n-1} x^{2^{ki}}$ and $M = \left\{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\right\}$. Then,

PROPOSITION (K. H. KIM- SM 2019)

Let $(k,n) = 1$ and k odd. Let ζ be an element of $M \setminus \{1\}$. Then, for any $b \in \mathbb{F}_{2^n}^{\star}$, we have

$$\{x \in \mathbb{F}_{2^{2n}} \mid x + x^{2^k} = b\} = S_{n,k}\left(\frac{b}{\zeta + 1}\right) + \mathbb{F}_2$$

Proof :
Set $q = 2^k$. As it was assumed that k is odd and $(n,k) = 1$, it holds $(2n,k) = 1$ and so the linear mapping $x \in \mathbb{F}_{2^{2n}} \longmapsto x + x^q$ has kernel of dimension 1, i.e. the equation $x + x^q = b$ has at most 2 solutions in $\mathbb{F}_{2^{2n}}$. Since $S_{n,k}(x) + (S_{n,k}(x))^q = x + x^{q^n}$, we have

$$\begin{aligned} S_{n,k}\left(\frac{b}{\zeta+1}\right) + \left(S_{n,k}\left(\frac{b}{\zeta+1}\right)\right)^q + b &= \frac{b}{\zeta+1} + \left(\frac{b}{\zeta+1}\right)^{q^n} + b \\ &= \frac{b}{\zeta+1} + \frac{b}{\zeta^{q^n}+1} + b \\ &= \frac{b}{\zeta+1} + \frac{b}{1/\zeta+1} + b \\ &= 0 \end{aligned}$$

and thus really $S_{n,k}\left(\frac{b}{\zeta+1}\right), S_{n,k}\left(\frac{b}{\zeta+1}\right) + 1 \in \mathbb{F}_{2^{2n}}$ are the $\mathbb{F}_{2^{2n}}-$solutions of the equation $x + x^q = b$.

Equation of degree 3 : $x^3 + ax + b = 0$

THEOREM (BERLEKAMP-RUMSEY-SOLOMON 1967-WILLIAMS 1975)

Let t_1 and t_2 denote the roots of $t^2 + bt + a^3$ in $\mathbb{F}_{2^{2n}}$, where $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^n}^*$. Let $f(x) = x^3 + ax + b$ over $\mathbb{F}_{2^n}$. Then

- *f has three zeros in F_{2^n} if and only if $Tr_1^n\left(\frac{a^3}{b^2} + 1\right) = 0$ and t_1, t_2 are cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd).*
- *f has exactly one zero in $\mathbb{F}_{2^n}$ if and only if $Tr_1^n\left(\frac{a^3}{b^2} + 1\right) = 1$.*
- *f has no zero in $\mathbb{F}_{2^n}$ if and only if $Tr_1^n\left(\frac{a^3}{b^2} + 1\right) = 0$ and t_1, t_2 are not cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd).*

Power equations

Let i be a positive integer. Let U be a multiplicative subgroup of $\mathbb{F}_{2^n}^{\star}$ of order $\frac{2^n-1}{gcd(i,2^n-1)}$. The equation $x^i = a$ has :

- one solution if $a = 0$;
- no solution if $a \in \mathbb{F}_{2^n}^{\star} \setminus U$;
- $gcd(i, 2^n - 1)$ solutions if $a \in U$.

$x^{2^k+1} + x + a = 0$: motivation

Solving $x^{2^k+1} + x + a = 0$ has interests in

- the general theory of finite fields
- the construction of difference sets with Singer parameters [Dillon 2002] ;
- finding cross-correlation between m-sequences [Helleseth-Kholosha-Ness 2007] ;
- constructing error correcting codes [Bracken-Helleseth 2009] ;
- the context of APN functions [Budaghyan-Carlet 2006], [Bracken-Tan-Tan 2014], [Canteaut-Perrin-Tian 2019] ;
- constructions designs [Tang 2019] ;
- etc.

[Dillon 2002], [Dillon-Dobbertin 2004]

DEFINITION

The k-subset D of the group G of order v is a difference set with parameters (v,k,λ) if for all nonidentity elements g of G the equation $g=xy^{-1}$ has exactly λ solutions with x and y in D.

If G is the multiplicative group of $\mathbb{F}_{2^m}$ of order 2^m-1, then the subset D of G is a difference set with the so-called Singer parameters if $(v,k,\lambda)=(2^m-1,2^{m-1},2^{m-2})$ (or the complementary parameters $(2^m-1,2^{m-1}-1,2^{m-2}-1)$).

- ☞ the polynomial $x^{2^k+1}+x+a$ allows to construct difference sets with Singer parameters $(v,k,\lambda)=(2^m-1,2^{m-1},2^{m-2})$ with $m\geq 3$.

THEOREM (BUDAGHYAN-CARLET 2006)

Under some conditions, if $G(x) := x^{2^i+1} + cx^{2^i} + c^{2^k}x + 1$ *has no solution* x *such that* $x^{2^k+1} = 1$ *the* $F(x) = x(x^{2^i} + x^{2^k} + cx^{2^{k+i}}) + x^{2^i}(c^{2^k}x^{2^k} + bx^{2^{k+i}}) + x^{2^{k+i}+2^k}$ *is APN on* $\mathbb{F}_{2^{2k}}$.

[Bracken-Tan-Tan 2014] constructed explicitly the polynomial G (when k even and 3 does not divide k).

☞ The polynomial G relates to the polynomial $x^{2^k+1}+x+a=0$: substituting $sx+c$ to x with $s^{2^i} = c^{2^i} + c^{2^k}$ we get $G(sx+c) = s^{2^i+1}(x^{2^k+1}+x+a)$.

DEFINITION

Let $s(t)$ and $v(t)$ be two binary m-sequences. $s(t)=Tr_1^m(\alpha^t)$ where α is an element of order $n=2^m-1$. Assume $v(t)=u(dt)$ where $u(t)=Tr_1^k(\beta^t)$ where β is an element of order $2^{m/2}-1$. Let d such that $gcd(d,2^{m/2}-1)=1$. The cross-correlation function $C_d(\tau)$ between the two m-sequences $s(t)$ and $v(t)$ is defined (for $\tau=0,1,\cdots,2^k-2$) by $C_d(\tau)=\sum_{t=0}^{n-1}(-1)^{s(t)+v(t+\tau)}$.

[Helleseth-Kholosha-Ness 2007] gave a three-valued cross-correlation function between the pairs of sequences of different lengths.

THEOREM (HELLESETH-KHOLOSHA-NESS 2007)

Let $m=2k$ and $d(2^l+1)\equiv 2^i \pmod{2^k-1}$ for some odd k and integer l with $0<l<k$ and $gcd(l,k)=1$. Then the cross-correlation function $C_d(\tau)$ has the following distribution :
$-1-2^{k+1}$ *occurs* $\frac{2^{k-1}-1}{3}$ *times*; -1 *occurs* $2^{k-1}-1$ *times*; $-1+2^k$ *occurs* $\frac{2^k+1}{3}$ *times*.

To prove their main result above, they need to compute three exponential sums $S_i(a) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(r^i a y^{2^l+1})+\mathrm{Tr}_1^k(y^{2^k+1})}$ for $i=0,1$
$S_2(a) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(r^{-1} a y^{2^l+1})+\mathrm{Tr}_1^k(y^{2^k+1})}$.
In order to determine $S_0(a)$, they need to consider zeros in $\mathbb{F}_{2^k}$ of the affine polynomial $A_a(v) = a^{2^l}v^{2^{2l}} + v^{2^l} + av + 1$ where $l<k$ and $(l,k)=1$
The distribution of the zeros in $\mathbb{F}_{2^n}$ of $A_a(v) = a^{2^l}v^{2^{2l}} + v^{2^l} + av + 1$ will determine to a large extent the distribution of their cross-correlation function.

THEOREM (HELLESETH-KHOLOSHA-NESS 2007)

Let $M_i = \{a \mid A_a(v)$ has exactly i zeros in $\mathbb{F}_{2^n}\}$ Then $A_a(v)$ has either one, two, or four zeros in $\mathbb{F}_{2^n}$. For $i\in\{1,2,4\}$ we have $a\in M_i$ if and only if $x^{2^k+1}+x+a=0$ has exactly $i-1$ zeros in $\mathbb{F}_{2^n}$.

The binary primitive triple-error-correcting BCH code is a cyclic code of minimum distance $d=7$ with generator polynomial $g(x)$ having zeros α ,α^3 and α^5 where α is a primitive (2^n-1)-root of unit in $\mathbb{F}_{2^n}$. The zero set of the code is said to be the triple $1,3,5$. Let $d_1=1$, d$_2=3$ and $d_3=5$. Then the parity-check matrix

$$\mathbf{H}=\begin{pmatrix} 1 & \alpha^{d_1} & \alpha^{2d_1} & \dots & \alpha^{(2^n-2)d_1} \\ 1 & \alpha^{d_2} & \alpha^{2d_2} & \dots & \alpha^{(2^n-2)d_2} \\ 1 & \alpha^{d_3} & \alpha^{2d_3} & \dots & \alpha^{(2^n-2)d_3} \end{pmatrix}. \qquad (1)$$

$x^{2^k+1} + x + a = 0$: motivation 4

[Bracken-Helleseth 2009] constructed triple-error-correcting BCH-like codes.

Theorem (Bracken-Helleseth 2009)

Let n be odd and $gcd(k,n) = 1$. Then the error-correcting code constructed using the zero set $1, 2^k+1, 2^{3k}+1$ is triple-error-correcting.

Their proof shows an interesting connection to the equation of the form $x^{2k+1} + bx^{2k} + cx = d$ defined on $\mathbb{F}_{2^n}$ which has no more than three solutions when $gcd(k,n) = 1$ for all b,c, and d in $\mathbb{F}_{2^n}$ (as a consequence of a result in [Bluher 2004] on $x^{2^k+1} + x + a = 0$).

DEFINITION

Let $\mathcal{P}$ be a set of v elements and let $\mathcal{B}$ be a set of k-subsets of $\mathcal{P}$. Let t be positive integer with $t \leq k$. The pair $(\mathcal{P}, \mathcal{B})$ is called incident structure. It said to be a $t-(v, k, \lambda)$ design if every t-subset of $\mathcal{P}$ is contained in exactly λ elements of $\mathcal{B}$.

[Tang 2019] constructed 3-designs : let $q=2^n$ and let $B_s := \{(x+1)^s + x^s \mid x \in \mathbb{F}_q\}$.

Proposition (Tang 2019)

Let $n = 3k \pm 1$ and $s = 2^{2k} - 2^k + 1$ where i an even integer. Let $d = 1/s \pmod{2^n - 1}$. Then the incidence structure $(\mathbb{F}_q, \{\pi(B_s) \mid \pi(x) = ax + b\})$ is 3-design if and only if $\#\{x \in \mathbb{F}_{2^n} \mid u^d x + (1+u^d)^{2^k+1} + x^{2^k+1} + 1 = 0\}$ is independent of $u \in \mathbb{F}_q \setminus \mathbb{F}_2$.

The equation $u^d x + (1+u^d)^{2^k+1} + x^{2^k+1} + 1 = 0$ can be reduced to $x^{2^k+1} + x + a = 0$.

Müller-Cohen-Matthews polynomials are defined over $\mathbb{F}_{2^n}$ as follows :

$$f_{k,d}(X) := \frac{T_k(X^c)^d}{X^{2^k}}$$

where

$$T_k(X) := \sum_{i=0}^{k-1} X^{2^i} \quad \text{and} \quad cd = 2^k + 1.$$

A basic property for such polynomials is :

THEOREM (1)

[Müller-Cohen-Matthews 1994, Dillon-Dobbertin 2004]
Let k and n be two positive integers with $(k,n) = 1$.

1. *If k is odd, then $f_{k,2^k+1}$ is a permutation on $\mathbb{F}_{2^n}$.*
2. *If k is even, then $f_{k,2^k+1}$ is a 2-to-1 on $\mathbb{F}_{2^n}$.*

The Dickson polynomial of the first kind of degree k in indeterminate x and with parameter $a \in \mathbb{F}_{2^n}^*$ is

$$D_k(x,a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i}\binom{k-i}{i} a^k x^{k-2i},$$

where $\lfloor k/2 \rfloor$ denotes the largest integer less than or equal to $k/2$.
In this talk, we consider only Dickson polynomials $D_k(x,1)$, that we shall denote $D_k(x)$.

Proposition

For any positive integer k and any $x \in \mathbb{F}_{2^n}$, we have

$$D_k\left(x+\frac{1}{x}\right) = x^k + \frac{1}{x^k}. \quad (2)$$

Let N_a be the number of solutions of the equation $P_a(x) := x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$.

- In 2004 : [Bluher 2004] the number of solutions N_a are only 0, 1 and 3 when $(k,n) = 1$.
- In 2008 : [Helleseth-Kholosha 2008] got criteria for $N_a = 1$ and an explicit expression of the unique solution when $(k,n) = 1$.
- In 2014 : [Bracken-Tan-Tan 2014] presented a criterion for $N_a = 0$ when n is even and $(k,n) = 1$.

Notation : $q = 2^k$.

We will exploit a recent polynomial identity involving Dickson polynomials :

THEOREM (2)

[Bluher 2016]

In the polynomial ring $\mathbb{F}_q[X,Y]$, we have the identity

$$X^{q^2-1} + \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1} = \prod_{w\in\mathbb{F}_q^*} \left(D_{q+1}(wX) - Y\right).$$

If k is odd, since $(q-1, 2^n-1) = 1$, the zeros of $P_a(x)$ are the images of the zeros of $P_a(x^{q-1})$ by the map $x \mapsto x^{q-1}$.

Now $f_{k,q+1}$ is a permutation polynomial of $\mathbb{F}_{2^n}$ by Theorem 1. Therefore, for any $a \in \mathbb{F}_{2^n}^*$, there exists a unique Y in $\mathbb{F}_{2^n}^*$ such that $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Hence, we have

$$P_a\left(x^{q-1}\right) = x^{q^2-1} + x^{q-1} + \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}} \tag{3}$$

Substituting tx to X in the above identity with $t^{q^2-q} = Y^q T_k\left(\frac{1}{Y}\right)^2$, we get :

$$\begin{aligned} P_a\left(x^{q-1}\right) &= x^{q^2-1} + x^{q-1} + \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}} \\ &= \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}}\left(X^{q^2-1} + \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1}\right) \end{aligned}$$

By Theorem 2 :

$$X^{q^2-1}+\left(\sum_{i=1}^{k} Y^{q-2^i}\right)X^{q-1}+Y^{q-1}=\prod_{w\in\mathbb{F}_q^*}\left(D_{q+1}\left(wX\right)-Y\right)$$

Therefore

$$P_a\left(x^{q-1}\right) = \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}}\prod_{w\in\mathbb{F}_q^*}\left(D_{q+1}\left(wtx\right)-Y\right)$$

☞ when k is odd, finding the zeros of $P_a(x^{q-1})$ amounts to determine preimages of Y under the Dickson polynomial D_{q+1}.

When k is even, $f_{k,q+1}$ is 2-to-1, Fortunately, we can go back to the odd case by rewriting the equation. Indeed, for $x \in \mathbb{F}_{2^n}$,

$$\begin{aligned} P_a(x) = x^{2^k+1} + x + a &= \left(x^{2^{n-k}+1} + x^{2^{n-k}} + a^{2^{n-k}}\right)^{2^k} \\ &= \left((x+1)^{2^{n-k}+1} + (x+1) + a^{2^{n-k}}\right)^{2^k} \end{aligned}$$

and so

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{x + 1 \mid x^{2^{n-k}+1} + x + a^{2^{n-k}} = 0,\ x \in \mathbb{F}_{2^n}\right\}. \tag{4}$$

☞ If k is even, then $n - k$ is odd and we can reduce to the odd case.

We now summarize all the above discussions in the following theorem.

Theorem (K. H. Kim- SM 2019)

Let k and n be two positive integers such that $(k, n) = 1$.

1. *Let k be odd and $q = 2^k$. Let $Y \in \mathbb{F}_{2^n}^*$ be (uniquely) defined by $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Then,*

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{ \frac{z^{q-1}}{YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}} \mid D_{q+1}(z) = Y,\ z \in \mathbb{F}_{2^n} \right\}.$$

2. *Let k be even and $q' = 2^{n-k}$. Let $Y' \in \mathbb{F}_{2^n}^*$ be (uniquely) defined by $a^{q'} = \frac{1}{f_{n-k,q'+1}\left(\frac{1}{Y'}\right)^{\frac{2}{q'}}}$. Then,*

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{ 1 + \frac{z^{q'-1}}{Y'T_{n-k}\left(\frac{1}{Y'}\right)^{\frac{2}{q'}}} \mid D_{q'+1}(z) = Y',\ z \in \mathbb{F}_{2^n} \right\}.$$

Solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$

☞ we can split the problem of finding the zeros in $\mathbb{F}_{2^n}$ of P_a into two independent problems with odd k.

PROBLEM (1)

For $a \in \mathbb{F}_{2^n}^*$, find the unique element Y in $\mathbb{F}_{2^n}^*$ such that

$$a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}. \tag{5}$$

PROBLEM (2)

For $Y \in \mathbb{F}_{2^n}^*$, find the preimages in $\mathbb{F}_{2^n}$ of Y under the Dickson polynomial D_{q+1}, that is, find the elements of the set

$$D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^\star \mid D_{q+1}(z) = Y\}. \tag{6}$$

Recall :

PROPOSITION

Let n be a positive integer. Then, every element z of $\mathbb{F}_{2^n}^\star$ can be written (twice) $z = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star \cup M$ with $c \neq 1$ and where $M = \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\}$

On Problem 1 : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

One has $Y = T + \frac{1}{T}$ where $T \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ or $T \in M \setminus \{1\}$ where $M = \left\{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\right\}$ (observe that $M \setminus \{1\} \subset \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$). Now,

$$\frac{1}{Y} = \left(\frac{1}{T+1}\right)^2 + \frac{1}{T+1}.$$

The next step is to use an approach used in [Dillon-Dobbertin 2004] by introducing $\Delta_k(X) = (X+1)^{2^{2k}-2^k+1} + X^{2^{2k}-2^k+1} + 1$ and a permutation on $\mathbb{F}_{2^n}$ defined as

$$Q_{k,k'}(X) = \begin{cases} \frac{\sum_{i=1}^{k'} X^{2^{ik}}}{X^{2^k+1}} & \text{if } k' \text{ is odd} \\ \frac{\sum_{i=1}^{k'} X^{2^{ik}}+1}{X^{2^k+1}} & \text{if } k' \text{ is even} \end{cases} \tag{7}$$

where k' is the inverse of k modulo n, that is, $kk' = 1 \mod n$. We then recall two properties of these polynomials [Dillon 1999] :

$$\Delta_k(X) = \left(Q_{k,k'}\left(X + X^{2^k}\right)\right)^{-1} = f_{k,q+1}(X + X^2). \tag{8}$$

On Problem 1 : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

Recall : $\Delta_k(X) = \left(Q_{k,k'}\left(X + X^{2^k}\right)\right)^{-1} = f_{k,q+1}(X + X^2)$ and $\frac{1}{Y} = \left(\frac{1}{T+1}\right)^2 + \frac{1}{T+1}$.
Collecting together all the above discussion, we get

$$\begin{aligned} a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{-1} &\iff a^{-\frac{q}{2}} = \Delta_k\left(\frac{1}{T+1}\right) \\ &\iff a^{-\frac{q}{2}} = \frac{1}{Q_{k,k'}\left(\left(\frac{1}{T+1}\right)^q + \left(\frac{1}{T+1}\right)\right)} \end{aligned} \tag{9}$$

On Problem 1 : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

PROPOSITION (K. H. KIM- SM 2019)

Let $a \in \mathbb{F}_{2^n}^{\star}$. *Let* $T \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \cup M \setminus \{1\}$ *be a solution of*

$$R_{k,k'}\left(a^{-\frac{q}{2}}\right) = \left(\frac{1}{T+1}\right)^q + \left(\frac{1}{T+1}\right)$$

where $R_{k,k'}$ *is the compositional inverse of* $1/Q_{k,k'}$. *Then,* $Y = T + \frac{1}{T}$ *is the unique solution of* $a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{-1}$.

the proposition above shows that solving Problem 1 amounts to find the solutions of a linear equation of the form $x^q + x = b$. The polynomial expression of the solutions of such a linear equation has been given.

On Problem 1 : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

Define $S_{n,k}(x) = \sum_{i=0}^{n-1} x^{2^{ki}}$. Then,

Proposition

Let ζ be an element of $M \setminus \{1\}$. Then, for any $b \in \mathbb{F}_{2^n}^{\star}$, we have

$$\{x \in \mathbb{F}_{2^{2n}} \mid x + x^q = b\} = S_{n,k}\left(\frac{b}{\zeta+1}\right) + \mathbb{F}_2$$

We can now explicit the solutions of Problem 1.

THEOREM (K. H. KIM- SM 2019)

Let $a \in \mathbb{F}_{2^n}^\star$. Let k' be the inverse of k modulo n. Then, the unique solution of Problem 1 in $\mathbb{F}_{2^n}^\star$ is $Y = T + \frac{1}{T}$ where

$$T = \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)} + 1$$

where ζ denotes any element of $\mathbb{F}_{2^{2n}}$ such that $\zeta^{2^n+1} = 1$, $S_{n,k}(x) = \sum_{i=0}^{n-1} x^{2^{ki}}$ and $R_{k,k'}$ stands for the compositional inverse of $1/Q_{k,k'}$ defined by (7). Furthermore, we have

$$Y = \frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right) + \left(S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)\right)^2}$$

Remark

One can derive the polynomial representation of the inverse $R_{k,k'}$ of the mapping induced by $1/Q_{k,k'}$ on $\mathbb{F}_{2^n}$. This question has been studied in [Dillon-Dobbertin 2004] where it is introduced the following sequences of polynomials :

$$A_1(x) = x,\ A_2(x) = x^{q+1},\ A_{i+2}(x) = x^{q^{i+1}} A_{i+1}(x) + x^{q^{i+1}-q^i} A_i(x), \quad i \geq 1,$$

$$B_1(x) = 0,\ B_2(x) = x^{q-1},\ B_{i+2}(x) = x^{q^{i+1}} B_{i+1}(x) + x^{q^{i+1}-q^i} B_i(x), \quad i \geq 1.$$

The polynomial expression of $R_{k,k'}$ is then $R_{k,k'}(x) = \sum_{i=1}^{k'} A_i(x) + B_{k'}(x)$.

Write $z = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star$ or $c \in M \setminus \{1\}$. One gets

$$Y = D_{q+1}(z) = c^{q+1} + \frac{1}{c^{q+1}} = T + \frac{1}{T} \tag{10}$$

with $T = c^{q+1}$

The equation $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n}^\star \cup M$ for any $Y \in \mathbb{F}_{2^n}^\star$ because it is equivalent to the quadratic equation $\left(\frac{T}{Y}\right)^2 + \frac{T}{Y} = \frac{1}{Y^2}$ and that $Tr_1^{2n}\left(\frac{1}{Y}\right) = 0$ since $Y \in \mathbb{F}_{2^n}$. In fact, we have two situations that occur depending on the value of $Tr_1^n\left(\frac{1}{Y}\right)$:

- If $Tr_1^n\left(\frac{1}{Y}\right) = 0$, $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$;
- If $Tr_1^n\left(\frac{1}{Y}\right) = 1$, $T + \frac{1}{T} = Y$ has two solutions in $M \setminus \{1\}$.

We shall now study separately those two cases.

Suppose that $Tr_1^n\left(\frac{1}{Y}\right) = 0$. Denote T and $\frac{1}{T}$ the two distinct elements of $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $T + \frac{1}{T} = Y$. Let us now turn our attention to the equation $c^{q+1} = T$ with $c \in \mathbb{F}_{2^n}^\star \cup M$, $c \neq 1$. Necessarily, $c \in \mathbb{F}_{2^n}^\star$ Recall that

$$(q+1, 2^n - 1) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 3 & \text{if } n \text{ is even} \end{cases}$$

Therefore, there are 0 or 3 elements c in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $c^{q+1} = T$ when n is even while there is a unique c when n is odd.

On Problem 2 : find $D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^\star \mid D_{q+1}(z) = Y\}$

We can then conclude from the above discussion and calculation the following result.

THEOREM (K. H. KIM- SM 2019)

Let $Y \in \mathbb{F}_{2^n}^\star$ such that $Tr_1^n\left(\frac{1}{Y}\right) = 0$. We have

1. *If n is even, let T be any element of $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $T + \frac{1}{T} = Y$. Then*

$$D_{q+1}^{-1}(Y) = \left\{cw + \frac{1}{cw} \mid c^{q+1} = T,\, c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\, w \in \mathbb{F}_4^\star\right\}$$

Notably, $D_{q+1}^{-1}(Y) = \emptyset$ if there is no c in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $c^{q+1} = T$.

2. *If n is odd, let T be any element of $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $T + \frac{1}{T} = Y$. Then*

$$D_{q+1}^{-1}(Y) = \left\{T^{\frac{1}{q+1}} + \frac{1}{T^{\frac{1}{q+1}}}\right\}.$$

On Problem 2 : find $D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^{\star} \mid D_{q+1}(z) = Y\}$

Next, suppose $Tr_1^n\left(\frac{1}{Y}\right) = 1$. In that case, the two elements T and $\frac{1}{T}$ such that $T + \frac{1}{T} = Y$ are both in $M \setminus \{1\}$. Now,

$$(q+1, 2^n+1) = \begin{cases} 1 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases}$$

Theorem (K. H. Kim- SM 2019)

Let $Y \in \mathbb{F}_{2^n}^{\star}$ such that $Tr_1^n\left(\frac{1}{Y}\right) = 1$. We have

1. *If n is odd, let T be any element of $M \setminus \{1\}$ such that $T + \frac{1}{T} = Y$. Then*

$$D_{q+1}^{-1}(Y) = \left\{cw + \frac{1}{cw} \mid c^{q+1} = T,\ c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\ w \in \mathbb{F}_4^{\star}\right\}$$

   Notably, $D_{q+1}^{-1}(Y) = \emptyset$ if there is no c in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $c^{q+1} = T$.

2. *If n is even, let T be any element of $M \setminus \{1\}$ such that $T + \frac{1}{T} = Y$. Then*

$$D_{q+1}^{-1}(Y) = \left\{T^{\frac{1}{q+1}} + \frac{1}{T^{\frac{1}{q+1}}}\right\}.$$

Solution of the equation (*) $x^{2^k+1}+x+a=0$ in $\mathbb{F}_{2^n}$ with $(n,k)=1$

Let k' be the inverse of k modulo n. Let $\zeta \in \mathbb{F}_{2^{2n}}$ such that $\zeta \neq 1$ and $\zeta^{2^n+1}=1$. Define

$$T=\frac{1}{S_{n,k}\left(\frac{R_{k,k'}\left(a^{-\frac{q}{2}}\right)}{\zeta+1}\right)}+1.$$

Theorem (n is even (then k is necessarily odd)-K. H. Kim- SM 2019)

1. *If T is in $\mathbb{F}_{2^n}$ but is not a cube of an element of $\mathbb{F}_{2^n}$, Equation (*) has no solutions in $\mathbb{F}_{2^n}$.*
2. *If T is in $\mathbb{F}_{2^n}$ and is a cube of an element of $\mathbb{F}_{2^n}$, Equation (*) has three distinct solutions in $\mathbb{F}_{2^n}$ that can be written as $\frac{\left(cw+\frac{1}{cw}\right)^{q-1}}{YT_k^{\frac{2}{q}}\left(\frac{1}{Y}\right)}$ where $c^{q+1}=T$, $w\in\mathbb{F}_4^\star$ and $Y=T+\frac{1}{T}$.*
3. *If T is in $\mathbb{F}_{2^{2n}}\setminus\mathbb{F}_{2^n}$; Equation (*) has a unique solution in $\mathbb{F}_{2^n}$ that can be written as $\frac{\left(T^{\frac{1}{q+1}}+\frac{1}{T^{\frac{1}{q+1}}}\right)^{q-1}}{YT_k^{\frac{2}{q}}\left(\frac{1}{Y}\right)}$ where $Y=T+\frac{1}{T}$.*

Solution of the equation (*) $x^{2^k+1}+x+a=0$ in $\mathbb{F}_{2^n}$ with $(n,k)=1$

THEOREM (n IS ODD AND k ODD-K. H. KIM- SM 2019)

Let M be the multiplicative subgroup of $\mathbb{F}_{2^{2n}}$ of order 2^n+1. Then, we have :

1. *If T is in M but is not a cube of an element of M, the equation has no solutions in $\mathbb{F}_{2^n}$.*
2. *If T is in M and is a cube of an element of M, the equation has three distinct solutions in $\mathbb{F}_{2^n}$ that can be written as $\frac{\left(cw+\frac{1}{cw}\right)^{q-1}}{YT_k^{\frac{2}{q}}\left(\frac{1}{Y}\right)}$ where $c^{q+1}=T$, $w\in\mathbb{F}_4^\star$ and $Y=T+\frac{1}{T}$.*
3. *If T is in $\mathbb{F}_{2^n}$; the equation has a unique solution in $\mathbb{F}_{2^n}$ that can be written as $1+\frac{\left(T^{\frac{1}{q+1}}+\frac{1}{T^{\frac{1}{q+1}}}\right)^{q-1}}{YT_k^{\frac{2}{q}}\left(\frac{1}{Y}\right)}$ where $Y=T+\frac{1}{T}$.*

Solution of the equation (*) $x^{2^k+1}+x+a=0$ in $\mathbb{F}_{2^n}$ with $(n,k)=1$

Let $l=n-k$, $q'=2^l$ and l' the inverse of l modulo n.

$$T' = \frac{1}{S_{n,l}\left(\frac{R_{l,l'}\left(a^{-\frac{(q')^2}{2}}\right)}{\zeta+1}\right)} + 1.$$

Theorem (n odd, k even-K. H. Kim- SM 2019)

Let M be the multiplicative subgroup of $\mathbb{F}_{2^{2n}}$ of order 2^n+1. Then, we have :

1. *If T' is in M but is not a cube of M, equation (*) has no solutions in $\mathbb{F}_{2^n}$.*
2. *If T' is in M and is a cube of M, equation (*) has three distinct solutions in $\mathbb{F}_{2^n}$: $\frac{\left(dw+\frac{1}{dw}\right)^{q-1}}{Y'T_k^{\frac{2}{q}}\left(\frac{1}{Y'}\right)}$ where $d^{q'+1}=T'$, $w\in\mathbb{F}_4^\star$ and $Y'=T'+\frac{1}{T'}$.*
3. *If T' is in $\mathbb{F}_{2^n}$; equation (*) has one solution : $1+\frac{\left(T'^{\frac{1}{q'+1}}+\frac{1}{T'^{\frac{1}{q'+1}}}\right)^{q'-1}}{Y'T_k^{\frac{2}{q}}\left(\frac{1}{Y'}\right)}$ where $Y'=T'+\frac{1}{T'}$.*

Solution of the equation (*) $x^3+x+a=0$ in $\mathbb{F}_{2^n}$, n even

Let $\zeta \in \mathbb{F}_{2^{2n}}$ such that $\zeta \neq 1$ and $\zeta^{2^n+1} = 1$. Define

$$T = \frac{1}{S_{n,1}\left(\frac{a^{-1}}{\zeta+1}\right)} + 1.$$

where $S_{n,1}(x) = \sum_{i=0}^{n-1} x^{2^i}$.

1. If T is in $\mathbb{F}_{2^n}$ but is not a cube of an element of $\mathbb{F}_{2^n}$, Equation (*) has no solutions in $\mathbb{F}_{2^n}$.
2. If T is in $\mathbb{F}_{2^n}$ and is a cube of an element of $\mathbb{F}_{2^n}$, Equation (*) has three distinct solutions in $\mathbb{F}_{2^n}$ that can be written as $cw + \frac{1}{cw}$ where $c^3 = T$, $w \in \mathbb{F}_4^\star$ and $Y = T + \frac{1}{T}$.
3. If T is in $\mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$; Equation (*) has a unique solution in $\mathbb{F}_{2^n}$ that can be written as $T^{\frac{1}{3}} + \frac{1}{T^{\frac{1}{3}}}$ where $Y = T + \frac{1}{T}$.

Solution of the equation (*) $x^3+x+a=0$ in $\mathbb{F}_{2^n}$, n odd

Let $\zeta \in \mathbb{F}_{2^{2n}}$ such that $\zeta \neq 1$ and $\zeta^{2^n+1}=1$. Define

$$T = \frac{1}{S_{n,1}\left(\frac{a^{-1}}{\zeta+1}\right)} + 1.$$

where $S_{n,1}(x) = \sum_{i=0}^{n-1} x^{2^i}$.
Let M be the multiplicative subgroup of $\mathbb{F}_{2^{2n}}$ of order 2^n+1. Then, we have :

1. If T is in M but is not a cube of an element of M, the equation has no solutions in $\mathbb{F}_{2^n}$.
2. If T is in M and is a cube of an element of M, the equation has three distinct solutions in $\mathbb{F}_{2^n}$ that can be written as $cw + \frac{1}{cw}$ where $c^3 = T$, $w \in \mathbb{F}_4^\star$ and $Y = T + \frac{1}{T}$.
3. If T is in $\mathbb{F}_{2^n}$; the equation has a unique solution in $\mathbb{F}_{2^n}$ that can be written as $1 + T^{\frac{1}{3}} + \frac{1}{T^{\frac{1}{3}}}$ where $Y = T + \frac{1}{T}$.

Conclusions

Partial results about the zeros of $P_a(x) = x^{2^k+1} + x + a$ in $\mathbb{F}_{2^n}$ have been obtained in [Bluher 2004], [Helleseth-Kholosha 2008],[Helleseth-Kholosha 2010] and [Bracken-Tan-Tan 2014].

- We provided explicit expression of all possible roots in $\mathbb{F}_{2^n}$ of $P_a(x)$ in terms of a when $(n,k) = 1$.
- We 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 Müller-Cohen-Matthews (MCM) polynomial and to find preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial.

  We completely solved these two independent problems.