Algebraic Equations over Finite Fields: Advances in Resolution Techniques and Practical Impacts

Sihem Mesnager

Department of Mathematics, University of Paris VIII
and University Sorbonne Paris Cité, LAGA, CNRS, France

Conference Women in mathematics
February 7, 2025
Palermo, Italy

Outline

- Motivations, specifications and main framework for applications
- On the famous equation $x^{p^k+1} + x + a = 0$ over $\mathbb{F}_{p^n}$
  - Motivation in the case of $\mathbb{F}_{2^n}$
  - Ingredients for the resolution in $\mathbb{F}_{2^n}$, when $\gcd(n, k) = 1$
  - The two related problems for solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$ and their solutions
  - The solution of $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $gcd(n, k) = 1$
- Three impacts (results obtained in 2021, 2022 and 2023)

Our interest and Specifications

In this talk, we are interested in solving algebraic equations over fields K.
Specifically :

- The algebraic equations are polynomial equations over K.
- These polynomial equations can be classified based on the degree of the polynomial involved (e.g., linear polynomial, quadratic polynomial, etc.).
- The field K is a finite field, which is a commutative field that is also finite. Up to isomorphism, a finite field is entirely determined by its cardinality, which is always the power of a prime number p. This prime number is known for its characteristics. For any prime number p and any non-zero integer n, there exists a field of cardinality p^n, which serves as the unique extension of degree n of the prime field $\mathbb{Z}/p\mathbb{Z}$. Notation : $K := \mathbb{F}_{p^n}$ and $K^\star := K \setminus \{0\}$.

General motivations

The following points highlight the importance of this topic :

- It is a fundamental problem in mathematics.
- Our understanding of this area is still quite limited.
- There is a strong motivation to explore its attractive applications.
- It is vital for many aspects of modern technology and is a key component of information theory and security, particularly in coding theory and cryptography.

Our Key Ingredients and Motivations

Let p be a prime power, and let n and m be two positive integers.

- Our framework focuses on solving polynomial equations related to coding theory and symmetric cryptography.
- In this context, the polynomials considered derive from functions over finite fields : $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^m}$.
- Their components functions (functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$) can be represented in two unique ways : (1) as a *univariate representation* when viewed over $\mathbb{F}_{p^n}$, and (2) as a *multivariate representation* when viewed over $\mathbb{F}_p^n$.
- Notably, if $n = m$, then F has a unique representation given by $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$ where $a_i \in \mathbb{F}_{p^n}$.

Functions over Finite Fields and Symmetric Cryptography

Let p be a prime. Consider a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$:

- *When $p = 2$, these functions are referred to as S-boxes (substitution boxes) when utilized in a block cipher (in symmetric cryptography).*
- *When $p = 2$ and $m = 1$, they are known as Boolean functions when applied in a stream cipher (in symmetric cryptography).*
- *These functions are fundamental components in symmetric cryptography ; the security of the cryptosystem heavily depends on their selection.*

Functions over Finite Fields and Linear Codes

Cryptographic functions are extensively used to design linear codes, and the main generic constructions of linear codes are based on functions. Many families of "good" codes can be derived from cryptographic functions ([SM, "Linear codes from functions", 2021]).

- A linear code $\mathcal{C}$ is denoted as $[n, k, d]_q$ over a field $\mathbb{F}_q$, where it represents a k-dimensional subspace of $\mathbb{F}_q^n$ with a minimum Hamming distance d. This distance is defined as :

$$d := d(\mathcal{C}) = \min_{\bar{a},\bar{b}\in\mathcal{C},\bar{a}\neq\bar{b}} d(\bar{a},\bar{b}),$$

  where $d(\bar{a},\bar{b})$ denotes the number of coordinates in which the vectors $\bar{a}$ and $\bar{b}$ differ.

- The support of a vector $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ is defined as :

$$\text{supp}(a) := \{0 \leq i \leq n-1 : a_i \neq 0\}.$$

  The Hamming weight of a, denoted $wt(a)$, is the cardinality of its support, i.e.,

$$wt(a) := \#\text{supp}(a).$$

- To design linear codes, the trace function $\text{Tr}_{p^n/p^m} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is defined as : $\text{Tr}_{p^n/p^m}(x) := \sum_{i=0}^{n/m-1} x^{p^i}$.

The Symmetric Cryptography framework

Consider the specific case where $p = 2$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$.

- ☞ When attacking a cryptographic system, we need to analyze the cryptographic parameters of F and assess them against cryptographic criteria.
- ☞ Primary Goal : Design "optimal" cryptographic resistance against attacks !

Symmetric Cryptography and a Key Example

A key example in symmetric cryptography is using vectorial functions, which effectively resist differential cryptanalysis.

- ☞ Differential Attack [Biham and Shamir, 1991] $\Rightarrow$ Differential Uniformity $\Rightarrow$ Almost Perfectly Nonlinear (APN).

- Difference Distribution Table (DDT)

$$\mathrm{DDT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}. \tag{1}$$

- Differential Uniformity [Nyberg (1992-1993)]

$$\delta_F = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} \mathrm{DDT}_F(a,b). \tag{2}$$

- ✯ The smaller the value of δ_F, the better the resistance to differential cryptanalysis.
- ✯ For any function F, it holds that $\delta_F \geq 2$ if $p = 2$.
- ✯ If $\delta_F = 2$, the function F (when $p = 2$) is considered Almost Perfectly Nonlinear (APN).

An Important Example : Solving the Equation $P_a(x) := x^{2^k+1} + x + a = 0$ over $\mathbb{F}_{2^n}$

- ☞ The polynomial $P_a(x)$ (where $a \in \mathbb{F}_{2^n}^\star$) is relevant in the context of cryptography, particularly for APN functions, as noted in works by Budaghyan and Carlet (2006), Bracken, Tan, and Tan (2014), and Canteaut, Perrin, and Tian (2019).

However, its significance extends beyond this area of study, as it is also of interest in various other contexts :

- The general theory of finite fields
- The inverse Galois problem (Abhyankar, Cohen, Zieve, 2000)
- 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)
- Construction of designs (Tang, 2019)
- Among others.

Main Ingredients for the Resolution of $P_a(x) := x^{2^k+1} + x + a = 0$ Over $\mathbb{F}_{2^n}$

Ingredient 1 : Dickson Polynomials

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

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

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

- **Properties** For all $x \in \mathbb{F}_{2^n}$ and for any integers $h, k > 0$, the following properties hold :
  - $\deg D_k = k$;
  - $D_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}$;
  - D_k is a permutation over $\mathbb{F}_{2^n}$ if and only if $\gcd(k, 2^{2n} - 1) = 1$;
  - $D_{hk}(x) = D_h(D_k(x))$;
  - ...

Main Ingredients for the Resolution of $P_a(x) := x^{2^k+1} + x + a = 0$ Over $\mathbb{F}_{2^n}$

Let k and n be two positive integers.
Ingredient 2 : Müller-Cohen-Matthews Polynomials The polynomials $f_{k,d}$ 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 $f_{k,2^k+1}$ (when $\gcd(k,n) = 1$) :

1. If k is odd, then $f_{k,2^k+1}$ is a permutation polynomial over $\mathbb{F}_{2^n}$ ([Müller, Cohen, Matthews 1994]).
2. If k is even, then $f_{k,2^k+1}$ is two-to-one on $\mathbb{F}_{2^n}$ ([Dillon, Dobbertin 2004]).

The Two Related Problems for Solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

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

Now $f_{k,q+1}$ is a permutation polynomial over $\mathbb{F}_{2^n}$ by **Ingredient 2**. Therefore, for any $a \in \mathbb{F}_{2^n}^*$, there exists a unique Y in $\mathbb{F}_{2^n}^*$ such that

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

Thus, we have

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

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

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

The Two Related Problems for Solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n, k) = 1$

Key Polynomial Identity Involving Dickson Polynomials A crucial result, due to [Bluher, 2016], states that in the polynomial ring $\mathbb{F}_q[X, Y]$ (where $q := 2^k$), we have the identity :

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

Thus, we rewrite

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

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

The Two Related Problems for Solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

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

$$P_a(x) = x^{2^k+1} + x + a = \left(x^{2^{n-k}+1} + x^{2^{n-k}} + a^{2^{n-k}}\right)^{2^k}$$
$$= \left((x+1)^{2^{n-k}+1} + (x+1) + a^{2^{n-k}}\right)^{2^k}.$$

Thus,

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

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

Two Related Problems for Solving $P_a(x) := x^{q+1} + x + a = 0$; with $q = 2^k$, $\gcd(n,k) = 1$

To summarize the discussions above : Let k and n be two positive integers such that $\gcd(k,n) = 1$.

1. If k is odd and $q = 2^k$, let $Y \in \mathbb{F}_{2^n}^*$ be defined as follows :

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

Then, the set of solutions to $P_a(x) = 0$ is given by :

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

2. If k is even and $q' = 2^{n-k}$, let $Y' \in \mathbb{F}_{2^n}^*$ be defined by :

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

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

Two Related Problems for Solving $P_a(x) := x^{q+1} + x + a = 0$ ($q = 2^k$, $\gcd(n, k) = 1$)

☞ We can split the problem of finding the zeros in $\mathbb{F}_{2^n}$ of P_a into two independent subproblems when k is odd.

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

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

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

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

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

To solve Problem A :

- We utilize two key components : the Müller-Cohen-Matthews polynomials and the machinery for computing the computational inverse of a family of polynomials.
- Problem A amounts to finding the solutions to a linear equation of the form $x^q + x = b$.

An approach to compute the computational inverse of an element of a family of polynomials

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

$$Q'_{k,k'}(x) = \frac{x^{q+1}}{\sum_{i=1}^{k'} x^{q^i}} \tag{7}$$

where $q := 2^k$, $k' < n$ is the inverse of k modulo n.
We have

- if $\gcd(n,k) = 1$ and k' is odd, then $Q'_{k,k'}$ is a permutation on $\mathbb{F}_{2^n}$ ([Dillon, Dobbertin, 1999]) ;
- a relation ([Dillon, 1999]) :

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

where $\Delta_k(X) = (X+1)^{2^{2k}-2^k+1} + X^{2^{2k}-2^k+1} + 1$;

An approach to compute the computational inverse of an element of a family of polynomials [continued]

- the polynomial representation of the inverse $R_{k,k'}$ of $Q'_{k,k'}$ on $\mathbb{F}_{2^n}$ has been studied in [Dillon, Dobbertin, 2004] by introducing 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
$R_{k,k'}(x) = \sum_{i=1}^{k'} A_i(x) + B_{k'}(x)$.

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

Solve Problem A :

- we use the fact : $\Delta_k(X) = Q'_{k,k'}\left(X + X^{2^k}\right) = f_{k,q+1}(X + X^2)$;
- we use a well-known key decomposition : every element z of $\mathbb{F}^{\star}_{2^{2n}}$ can be written (twice) $z = c + \frac{1}{c}$ where $c \in \mathbb{F}^{\star}_{2^n} \cup M$ with $c \neq 1$ and where $M = \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\}$
- 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 $M \setminus \{1\} \subset \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$). Consequently :

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

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

Solve Problem A : We get

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

Next, Problem A amounts to finding the solutions to a linear equation of the form $x^q + x = b$, that we solved.

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

Solve Problem B :

1. Let us express z as $z = c + \frac{1}{c}$, where $c \in \mathbb{F}_{2^n}^\star$ or $c \in M \setminus \{1\}$, with $M = \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\}$.
   Using the properties of Dickson polynomials, we find that
   $$Y = D_{q+1}(z) = c^{q+1} + \frac{1}{c^{q+1}} = T + \frac{1}{T}$$
   where $T = c^{q+1}$.
   The equation $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n}^\star \cup M$ for any $Y \in \mathbb{F}_{2^n}^\star$. This is because it is equivalent to the quadratic equation
   $$\left(\frac{T}{Y}\right)^2 + \frac{T}{Y} = \frac{1}{Y^2}$$
   and we have $\mathrm{Tr}_{2^n/2}\left(\frac{1}{Y}\right) = 0$.
2. We consider two cases depending on the value of $\mathrm{Tr}_{2^n/2}\left(\frac{1}{Y}\right)$:
   - If $\mathrm{Tr}_{2^n/2}\left(\frac{1}{Y}\right) = 0$, then $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$;
   - If $\mathrm{Tr}_{2^n/2}\left(\frac{1}{Y}\right) = 1$, then $T + \frac{1}{T} = Y$ has two solutions in $M \setminus \{1\}$.

Resolution of $P_a(X) := X^{q+1} + X + a$, where $a \in \mathbb{F}_Q \setminus \{0\}$, $Q = p^n$, and $q = p^k$, with p being a prime

- (1) In 2004, [Bluher, 2004] proved that the number of roots N_a is either 0, 1, 2, or $p^d + 1$, where $d = \gcd(k, n)$.
- (2) Let M_i represent the number of $a \in \mathbb{F}_Q^*$ for which the polynomial $P_a(X)$ has exactly i zeros in $\mathbb{F}_Q$, for each non-negative integer i. The values of M_i were computed by [Bluher, 2004].
- (3) Some criteria for determining the number of $\mathbb{F}_Q$-zeros of the polynomial $P_a(X)$ were established by [Bluher, 2004].
- (4) A new criterion, showing that $P_a(X)$ can have 0, 1, 2, or $p^d + 1$ roots, was demonstrated by [McGuire and Sheekey, 2019] for any characteristic, based on the number of roots of any projective polynomial of the form $\sum_{i=0}^{t} a_i X^{\frac{q^i-1}{q-1}}$, where $a_i \in \mathbb{F}_{q^m}$.
- Additionally, in [H-Kim, J. Choe, SM, 2021], the discussion extends beyond the existing literature.
- The resolution of $P_a(x) = 0$ have been established of any prime p through new techniques

Impacts of the Resolution of Our Main Equation in Characteristic 2

- (1) A direct, short proof of the APN-ness property of Kasami functions (Carlet, Kim, SM, 2023).
- (2) The complete proof of the bijectivity property of an "exceptional" family of quadrinomials discovered in 2019, based on work by [Perrin, Udovenko, Biryukov, Crypto' 2016] (Kim, SM, Choe, N. Lee, S. Lee, Jo, 2022).
- (3) Solving the equation

$$X^{2^{3n}+2^{2n}+2^n-1} + (X+1)^{2^{3n}+2^{2n}+2^n-1} = b$$

in $\mathbb{F}_{2^{4n}}$ and providing an alternative proof of a conjecture regarding the differential spectrum of the related monomial functions (Kim, SM, 2023).

(1) A direct proof of the APN-ness property of Kasami functions

Kasami (APN) function : $F(X) = X^{q^2-q+1}$, $q = 2^k$, $\gcd(k, n) = 1$

Recall that F is said to be *almost perfect nonlinear* (APN) if for every $a \in \mathbb{F}_{2^n}{}^*$ and every $b \in \mathbb{F}_{2^n}$, the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions.

A power function $F(X) = X^d$ is APN if and only if, for every $b \in \mathbb{F}_{2^n}$ the system

$$\begin{cases} X + Y & = 1 \\ X^d + Y^d & = b \end{cases} \tag{10}$$

has at most one pair $\{X, Y\}$ of solutions in $\mathbb{F}_{2^n}$

(1) A direct proof of the APN-ness property of Kasami functions

Let n odd, $F = G_2 \circ G_1^{-1}$ where $G_1(X) = X^{q+1}$ and $G_2(x) = X^{q^3+1}$.

Equation (10) is equivalent to

$$\begin{cases} x^{q+1} + y^{q+1} & = 1 \\ x^{q^3+1} + y^{q^3+1} & = b \end{cases} \tag{11}$$

Theorem : System (11) has at most one pair $\{x, y\}$ of solutions proving that F is APN ([Carlet, Kim, SM, 2021])

Sketch of the proof : Letting $y = x + z$, $v = z^{q^2-1}$ and $c = b + 1$,

- Proving Equation (11) has at most one pair $\{x, y\}$ of solutions is equivalent to proving that $(\star\star)$ has at most one solution v when $(\star)$ has solutions :

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) & = \frac{1}{v^{\frac{1}{q-1}}} + 1 \quad (\star) \\ (v+1)^{q+1} + cv & = 0 \quad (\star\star) \end{cases}$$

  for every $c \in \mathbb{F}_{2^n}$.

- For every $c \in \mathbb{F}_{2^n}$, the cubic equation $(v+1)^{q+1} + cv = 0$ has at most one solution v in $\mathbb{F}_{2^n}$ such that $Tr_{2^n/2}\left(\frac{1}{v^{\frac{1}{q-1}}} + 1\right) = 0$.

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

In Crypto'2016, [Perrin, Udovenko, Biryukov, 2016] discovered the butterfly structure (that contains the Dillon APN permutation of six variables), later generalized [Canteaut, Perrin, Tian, 2019], which turns out to be a powerful approach that generates infinite families of cryptographic functions with best-known nonlinearity and differential properties.

Let m odd, k odd, $\gcd(m,k)=1$, $Q=2^m$, $q=2^k$

$$f_{\underline{\epsilon}}(X) := \epsilon_1 \overline{X}^{q+1} + \epsilon_2 \overline{X}^q X + \epsilon_3 \overline{X} X^q + \epsilon_4 X^{q+1}, \quad \overline{X} = X^Q \tag{12}$$

where

$$\underline{\epsilon} = (\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4) = \begin{cases} (\varepsilon_3,\varepsilon_4,\varepsilon_1,\varepsilon_2), & \text{if } k \text{ is odd} \\ (\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4), & \text{if } k \text{ is even,} \end{cases} \in \mathbb{F}_Q^4 \tag{13}$$

and ($\alpha,\beta \in \mathbb{F}_Q$.)

$$\begin{cases} \varepsilon_1 = \alpha^q + \alpha + 1 \\ \varepsilon_2 = \alpha^{q+1} + \alpha + \beta + 1 \\ \varepsilon_3 = \alpha^{q+1} + \alpha^q + \beta + 1 \\ \varepsilon_4 = \alpha^{q+1} + \alpha^q + \alpha + \beta \end{cases} \tag{14}$$

Conclusion (1/3)

There is still much work to be done regarding the resolution of equations over finite fields !
Equations of the form $F(x) + F(x+1) = b$, where $F(x) = x^d$ is a power function over finite fields in characteristic 2, have been solved in the following cases :

- In [Kim, S.M., 2023], the equation was resolved in $\mathbb{F}_{2^{4n}}$ for $d = q^3 + q^2 + q - 1$, where $q = 2^k$. This work also explicitly determined the set of b values for which the equation has i solutions for any positive integer i.
- The same equation was later resolved by [Qian, Minjia, Lu, 2023] using two important decompositions (a) and (b) used in ([Kim, S.M., 2020-2022]) :

Decompositions of the underlying fields are important :

1. Decomposition (a) in $\mathbb{F}^*_{2^{2m}}$ ([Kim, S.M., 2020]) : Let m be a positive integer. Every element z of $\mathbb{F}^*_{2^{2m}}$ can be expressed in two ways :
   - If $\mathrm{Tr}_{2^m/2}\left(\frac{1}{z}\right) = 0$, then $z = c + \frac{1}{c}$ for some $c \in \mathbb{F}^\star_{2^m}$.
   - If $\mathrm{Tr}_{2^m/2}\left(\frac{1}{z}\right) = 1$, then c belongs to $\mu^\star_{2^m+1} := \{\zeta \in \mathbb{F}_{2^m} \mid \zeta^{2^m+1} = 1\} \setminus \{1\}$.
2. Decomposition (b) of $\mathbb{F}_{q^4}$ ([Kim, S.M., 2022]) : $\mathbb{F}^*_{q^4} = \mu_{q-1} \cdot \mu_{q+1} \cdot \mu_{q^2+1}$, which arises from the fact that $q-1$, $q+1$, and q^2+1 are pairwise coprime. It can be shown that $\gcd(q^3+q^2+q-1, q^4-1) = \gcd(q^3+q^2+q-1, (q-1)(q+1)(q^2+1)) = 1$.

Conclusion (2/3)

Equations of the form $F(x) + F(x+1) = b$, where $F(x) = x^d$ is a power function over finite fields in characteristic 2, have also been solved in the following case :

- When $d = q^2 + q + 1$ (where $q = 2^k$), [Ho Kim, S.M., Hyok Kim, 2023] provided a direct and complete method to solve such equations. While the number of solutions was known to be $\{0, 2, 4\}$ in $\mathbb{F}_{2^{4k}}$, their work further elucidates this aspect.

Conclusion (3/3)

Here are some open problems (among many others) :

- Solve additional equations of the form $F(x) + F(x + a) = b$. This would enhance our understanding of the differential spectrum of S-boxes F (the most significant cases are those for which $\delta(F) \in \{2, 4\}$).
- Solve more equations of the form $F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a$. This would provide deeper insights into the boomerang spectrum of S-boxes F .
- Handle the big open problem of Dillon.