FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

HABILITATION THESIS

Faruk Göloğlu

Projective polynomials over finite fields and their applications in cryptography and combinatorics

Prague 2023

Projective polynomials over finite fields and their applications in cryptography and combinatorics

Habilitation thesis

Faruk Göloğlu
March 2023

Faruk.Gologlu@mff.cuni.cz

Charles University
Faculty of Mathematics and Physics
Department of Algebra
Sokolovská 49/83
186 75 Prague 8
Czech Republic

Contents

Preface

The aim of this thesis is to provide background for and commentary to some recent results [**A, B, C, D, E, F, G, H, J, K**] on **cryptography, combinatorics and algebra**, covering

- constructions and enumeration of **finite semifields**,
- resolution of several problems regarding **highly nonlinear functions**,
- classification results for **cryptographic permutations** in polynomial and rational function form, and
- development of very efficient algorithms for solving the cryptographically important **discrete logarithm problem** on finite fields providing record computation instances,

all by developing novel techniques for **projective polynomials over finite fields**. These results have appeared in the publications listed below.

Main publications

- F. Göloğlu and L. Kölsch, *An exponential bound on the number of non-isotopic commutative semifields*, Trans. Amer. Math. Soc. **376(3)** (2023), 1683–1716.

  DOI:10.1090/tran/8785
- F. Göloğlu, *Biprojective almost perfect nonlinear functions*, IEEE Trans. Inform. Theory **68** (2022), no. 7, 4750–4760.

  DOI:10.1109/TIT.2022.3157798 MR 4449070
- F. Göloğlu and L. Kölsch, *Equivalences of biprojective almost perfect nonlinear functions*, J. Comb. Th. A (submitted) (2021), 26 pages. arXiv:2111.04197.

  DOI:10.48550/arXiv.2111.04197
- F. Göloğlu, *Classification of fractional projective permutations over finite fields*, Finite Fields Appl. **81** (2022), Paper No. 102027, 50 pages.

  DOI:10.1016/j.ffa.2022.102027 MR 4397755
- F. Göloğlu, *Classification of (q, q)-biprojective APN functions*, IEEE Trans. Inform. Theory **69** (2022), no. 3, 1988–1999.

  DOI:10.1109/TIT.2022.3220724
- F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities: application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$*, Advances in cryptology—CRYPTO 2013. Part II,

Lecture Notes in Comput. Sci., vol. 8043, Springer, Heidelberg, 2013, pp. 109–128.

DOI:10.1007/978-3-642-40084-1_7 MR 3126472

- F. Göloğlu and A. Joux, *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, Math. Comp. **88** (2019), no. 319, 2485–2496.

  DOI:10.1090/mcom/3404 MR 3957902

- F. Göloğlu and Ph. Langevin, *Almost perfect nonlinear families which are not equivalent to permutations*, Finite Fields Appl. **67** (2020), Paper No. 101707, 21 pages.

  DOI:10.1016/j.ffa.2020.101707 MR 4122629

Supplementary publications

- F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *Solving a 6120-bit DLP on a desktop computer*, Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers (Tanja Lange, Kristin E. Lauter, and Petr Lisonek, eds.), Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 136–152.

  DOI:10.1007/978-3-662-43414-7_7

- F. Göloğlu and L. Kölsch, *Counting the number of non-isotopic Taniguchi semifields*, Des. Codes Crypt. (submitted) (2022), 13 pages. arXiv:2207.13497.

  DOI:10.48550/arXiv.2207.13497

A note on publications

The list of publications is divided into two categories. The thesis is mostly based on the main publications but we also use some results and explanations from the supplementary publications. Although large portions of the following is written exclusively for this thesis we also incorporate text from our publications.

Contributions

In this thesis, we provide commentary to publications which have the following contributions to four areas in the conjunction of algebra, combinatorics and cryptography.

(i) **Finite semifields:** [**A, K**] We give a prolific family of semifields which leads to the solution of the major enumeration problem on commutative semifields. Deciding whether the number of non-isotopic commutative semifields of odd order p^n is not bounded by a polynomial in n has been described (by Pott in [**128**], the most recent survey on the topic) as **"the main problem in connection with commutative semifields."** The family introduced in [**A**] solves precisely this problem by giving an exponential number of pairwise non-isotopic semifields.

The even characteristic case (commutative and general) was proved by Kantor and Williams [**85, 89**] two decades ago (where the numbers are super-polynomial in the order) who posed the problem of providing similar results for the odd characteristic. We were able to improve the odd characteristic bound for the general (i.e., not necessarily commutative) case, however the improvement here is not as dramatic as the commutative case. The following table reflects the situation before and after our contributions.

	commutative	general
before	$\approx n^2$	$\approx (p^n)^{1/2}$
after	$\approx (p^n)^{1/4}$	$\approx (p^n)^{2/3}$

TABLE 1. Known number of pairwise non-isotopic semifields of odd order p^n

We have actually developed a method to decide the isotopy problem for a large class of (biprojective) semifields which addresses another remark by Kantor and Williams [**89**].

(ii) **Discrete logarithm problem:** [**F, G, J**] We provide very efficient algorithms that solve the discrete logarithm problem on the multiplicative group of a finite field. These algorithms were then employed to **break two records** [**58, 59**] **for computing discrete logarithms in largest order finite fields**. We also give the rigorous analysis of one of these algorithms [**G**] whose running time is quasi-polynomial in the bitsize of the order. The publication [**F**] has been awarded the prestigious **best paper award** at CRYPTO—2013, one of the leading conferences in cryptography.

(iii) **Highly nonlinear functions:** [**B, C, E, H**] We deliver a rather comprehensive study of biprojective almost perfect nonlinear (APN) functions. This includes introducing biprojectivity [**B**], discovery of three new infinite families of APN functions that are nontrivial hybrids of Gold functions, one of which contains an exponential number of inequivalent members [**B, C**], as well as classifying (q, q)-biprojective APN functions [**E**], giving a method to check equivalences of (biprojective) APN functions theoretically [**C**], and showing that Gold and Kasami functions are not equivalent to permutations on certain extensions [**H**].

All of these are natural problems on nonlinear functions some of which have been explicitly stated as interesting problems in the literature. We completely solve in [**E**], for instance, the open problem listed by Carlet [**29**, Section 3.7] in a recent survey on "open problems on nonlinearity."

(iv) **Cryptographic permutations:** [**D**] We fully classify fractional q-projective and (q, q)-biprojective permutations. This result single-handedly covers/generalizes/proves the open problems of many recent publications [**139, 138, 111, 110, 114, 137, 97, 143, 113**].

Contributions in context

Many combinatorially and/or cryptographically interesting objects over a finite field $\mathbb{F}_{p^n}$ arise from quadratic (in the sense of *algebraic degree*) monomials from $\mathbb{F}_{p^n}[X]$. Most such objects have been identified in the literature. Usually they produce the first example of an interesting definition. Naturally, generalizations of such objects are sought after. When n is composite, subfield structures can be employed to achieve this goal. In this thesis we define **biprojectivity** to identify a natural generalization of quadratic monomials when n is even. A biprojective function is a pair of bivariate functions each of which is a homogeneous function with *polynomial degrees* $p^i + 1, p^j + 1$ and algebraic degrees 2. Although some such generalizations have been identified in the literature, a thorough analysis has not been done. In the literature, exclusively, the cases when one bivariate function is chosen as a simple one such as $(x, y) \mapsto xy^{p^i}$ were considered which allows for techniques dating back to Dickson. In this thesis, general (and complicated) choices for bivariate functions are analyzed and novel techniques are introduced. Our definitions and techniques make rather full use of the underlying structure (e.g., groups $\Gamma\mathrm{L}(2, p^{n/2}), \mathrm{GL}(2, p^{n/2})$ and $\mathrm{PGL}(2, p^{n/2})$) and are natural but non-trivial.

Organization of the thesis

Part 1 of this thesis is organized as follows.

(i) We start in Chapter 1 by introducing projective and biprojective polynomials. Most important for us throughout the thesis is the zeroes of projective polynomials which is the subject of this chapter as well as actions of the general linear and projective general linear groups. The reader is advised to skip most of this chapter (after definitions of projective and biprojective polynomials) in the first reading until it is referred to.

(ii) Chapter 2 through Chapter 7 are devoted to the background on finite semifields. First, the semifields and their properties are introduced in Chapter 2. Chapter 3 is devoted to the connection between cryptographic highly nonlinear functions and finite semifields where biprojective functions are put in the context of vectorial functions using the two notions of degree (polynomial and algebraic) we use throughout the thesis. Chapter 4 is a survey on known constructions of semifields. Chapter 5 lists the known bounds on the number of pairwise non-isotopic semifields. Chapter 6 puts our construction from [**A**] in context and shows how it can be viewed as a natural generalization of Albert's twisted fields. Chapter 7 gives a survey on biprojective representations of known semifields. Finally, Chapter 8 contains detailed commentary to our contribution [**A**].

(iii) Chapters 9 and 10 are devoted to the background for almost perfect nonlinear (APN) functions and permutations. The lengthy introduction for semifields is also helpful for APN functions as they are (in a sense) binary analogues of commutative semifields in odd characteristic. In Problem 10.8 of Chapter 10 we introduce five problems, all of which are solved in five subsequent chapters which provides commentary to [**H, D, E, B, C**].

(iv) Chapter 16 contains its own introduction as it explains the discrete logarithm problem (DLP) which is not directly related to finite semifields or highly nonlinear functions. This chapter relies heavily on projective polynomials as well. A commentary to [**F, G**] is provided.

In Part 2 of the thesis, we simply reprint the papers to which we provide commentary.

Acknowledgments

I would like to thank my co-authors Robert Granger, Antoine Joux, Lukas Kölsch, Philippe Langevin, Gary McGuire, and Jens Zumbrägel.

I also would like to thank Claude Carlet, Pascale Charpin, Aleš Drápal, William Kantor, Gohar Kyureghyan, Petr Lisoněk, Wilfried Meidl, Ferruh Özbudak, Alexander Pott, Yue Zhou and Michael Zieve for mathematical discussions on the topics of the thesis.

I also thank Lukas Kölsch for a careful reading of the draft and many suggestions that improved the thesis.

My research on this thesis was conducted mostly at

- Charles University, Prague,

and partly at

- University College Dublin,
- Sorbonne Université —Campus Pierre et Marie Curie, Paris,
- Katholieke Universiteit Leuven,
- University of Tartu, and
- Université de Toulon.

I am thankful to colleagues and staff from all these institutions for their hospitality.

Most of this work [**A, B, C, D, E, G, H, K**] was supported by the GAČR Grant 17-19087S - 301-13/201843, except [**F, J**] which were supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

Part 1

Commentary

CHAPTER 1

Projective and biprojective polynomials

The overarching topic of this thesis is **projective polynomials over finite fields**. Let $\mathbb{L} = \mathbb{F}_{p^l}$ be a finite field and $q = p^k$ with $0 \leq k < l$. A polynomial of the form

$$\phi_f(x) = ax^{q+1} + bx^q + cx + d \in \mathbb{L}[x] \tag{1}$$

is called a **q-projective polynomial** over $\mathbb{L}$. We will extensively use the following bivariate version. A polynomial of the form

$$f(x, y) = ax^{q+1} + bx^q y + cxy^q + dy^{q+1} \in \mathbb{L}[x, y]$$

is called a **q-biprojective polynomial** over $\mathbb{L}$. Note that

$$\phi_f(x) = f(x, 1).$$

We will use the shorthand notation

$$f = (a, b, c, d)_q$$

to refer to both types of polynomials for simplicity and when the context is clear. Our main interest is in *cryptographic functions* of the following forms:

- **(q, r)-biprojective functions** of the form:

  $$\begin{aligned} F : \mathbb{L} \times \mathbb{L} &\to \mathbb{L} \times \mathbb{L} \\ (x, y) &\mapsto (f(x, y), g(x, y)), \end{aligned}$$

  where f and g are q- and r-biprojective polynomials, and
- **fractional q-projective functions** of the form

  $$\begin{aligned} \Pi : \mathcal{P}^1(\mathbb{L}) &\to \mathcal{P}^1(\mathbb{L}) \\ x &\mapsto \frac{\phi_f(x)}{\phi_g(x)}, \end{aligned}$$

  where ϕ_f and ϕ_g are q-projective polynomials. Note that we assume $\phi_f(x) = 0 = \phi_g(x)$ does not happen for $x \in \mathbb{L}$.

Remark 1.1. We will allow $k = 0$, that is to say, $q = 1$ in our definition. In this case, one of b, c in the notation is superfluous. However, we will set $b = 0$ and continue using it.

1. Origins

To the best of our knowledge, the first reference to the name “projective polynomials” is by Abhyankar [**2**] in 1997. Let $q = p^k$ with $k > 0$ and K be a field containing $\mathbb{F}_q$. Abhyankar showed that the Galois group $\mathrm{Gal}(F, K(x))$ of

$$F(y) = y^{(q^t-1)/(q-1)} + y + x$$

for $t > 1$ is $\mathrm{PGL}(t, q)$, and named such polynomials projective. Abhyankar [**1**, p. 131] ascribes the proof for $t = 2$ to Serre, for which we have $(q^2 - 1)/(q - 1) = q + 1$. Hughes and Kleinfeld [**71**] and Knuth [**101**] had already used these polynomials in 1960s (see Chapter 4 and Remark 7.2) for constructing semifields without using the name "projective polynomial."

Bluher [**18**] studied polynomials of the form

$$x^{q+1} + ex^q + ax + b \in \mathbb{L}[x]$$

where $ea \neq b$ and $a \neq e^q$, and determined the numbers and locations of zeroes of such polynomials over finite fields. We refer to Bluher's results extensively overall the thesis. In this thesis, our applications require to address all such polynomials without exceptions. Thus, we slightly extend the definition as given in this section.

In the following, we will first derive the possible numbers of $\mathbb{L}$-zeroes of projective polynomials over finite fields (which was essentially done by Bluher in [**18**]). In our extended definition, when $a = 0$ in Eq. (1), the projective polynomials reduce to *affine* or even *constant* polynomials. We will first address this case. For the rest of this chapter we will assume $0 < k < l$.

2. Zeroes of some affine polynomials, the trace map and Hilbert's Theorem 90

Let $\mathbb{L}$ be the finite field with p^l elements, $q = p^k$ for $0 < k < l$ and let $\mathbb{D} \subset \mathbb{L}$ be a finite field of order p^δ with $\delta = \gcd(k, l)$. The **trace map** is defined as

$$\mathsf{tr}_{\mathbb{L}/\mathbb{D}}(x) = \sum_{j=0}^{l/\delta - 1} x^{(p^\delta)^j}.$$

When $\mathbb{D} = \mathbb{F}_p$ then we simply write

$$\mathsf{tr}(x) = \mathsf{tr}_{\mathbb{L}/\mathbb{F}_p}(x).$$

The following is the finite fields version of Hilbert's Theorem 90.

Lemma 1.2 (Hilbert's Theorem 90). *Let $\gcd(j, l) = 1$ and $a \in \mathbb{L}$. Then $\mathsf{tr}_{\mathbb{L}/\mathbb{D}}(a) = 0$ if and only if $a = x^{(p^\delta)^j} - x$ for some $x \in \mathbb{L}$.*

The $\mathbb{D}$-linear vector-space endomorphisms of $\mathbb{L}$ can be written as

$$L(x) = \sum_{j=0}^{l/\delta - 1} a_j x^{(p^\delta)^j}, \quad a_j \in \mathbb{L},$$

and are called **$\mathbb{D}$-linearized polynomials**. Determining kernels of such endomorphisms in $\mathbb{L}$, especially of the form $L(x) = ax^q - bx$ and the zeroes of its translates $L(x) + c$, is important for this thesis. This can simply be done by observing

$$L(r) = ar^q - br = 0$$

for some nonzero $r \in \mathbb{L}^\times$ if and only if $r^{q-1} = b/a$. In that case $L(rx)/rb = x^q - x$.

Then one can deduce that the $\mathbb{L}$-zeroes of L are 0 and ϵr for $\epsilon \in \mathbb{D}^\times$ if such r exists. Then the case $L(x) + c$ can be handled using Hilbert's Theorem 90. The following lemma is relevant and will be needed overall the thesis.

Lemma 1.3. *For a prime p,*

(i) $\gcd(p^k - 1, p^l - 1) = p^{\gcd(k,l)} - 1$.

(ii)

$$\gcd(p^k + 1, p^l - 1) = \begin{cases} 1 & \text{if } \frac{l}{\gcd(k,l)} \text{ is odd, and } p = 2, \\ 2 & \text{if } \frac{l}{\gcd(k,l)} \text{ is odd, and } p \text{ is odd,} \\ p^{\gcd(k,l)} + 1 & \text{if } \frac{l}{\gcd(k,l)} \text{ is even.} \end{cases}$$

Before considering the zeroes of projective polynomials, we should first explain the natural actions on projective, biprojective and fractional projective polynomials and functions.

3. Actions of GL(2, $\mathbb{L}$) and PGL(2, $\mathbb{L}$)

In this section we outline the basics of several actions of GL(2, $\mathbb{L}$) and PGL(2, $\mathbb{L}$) on biprojective and projective functions/polynomials. Let

$$\mathcal{V}_{q,\mathbb{L}} = \{(a, b, c, d)_q \ : \ a, b, c, d \in \mathbb{L}\},$$

be the set of all q-biprojective polynomials. Let $f, g \in \mathcal{V}_{q,\mathbb{L}}$ be two q-biprojective polynomials and

$$\begin{aligned} F : \mathbb{L} \times \mathbb{L} &\to \mathbb{L} \times \mathbb{L} \\ (x, y) &\mapsto (f(x, y), g(x, y)) \end{aligned}$$

be the associated (q, q)-biprojective function. Define $\mathcal{F}_{q,\mathbb{L}}$ to be the set of all (q, q)-biprojective functions, i.e.,

$$\mathcal{F}_{q,\mathbb{L}} = \mathcal{V}_{q,\mathbb{L}} \times \mathcal{V}_{q,\mathbb{L}}.$$

Let $\mathfrak{L}(\mathbb{L})$ be the group of all **non-singular $\mathbb{L}$-linear transformations** of $\mathbb{L} \times \mathbb{L}$, i.e.,

$$\mathrm{GL}(2, \mathbb{L}) \cong \mathfrak{L}(\mathbb{L}) = \{(x, y) \mapsto (tx + uy, vx + wy) \ : \ t, u, v, w \in \mathbb{L} \mid tw - uv \neq 0\}.$$

We are mainly interested in the standard action of GL(2, $\mathbb{L}$)×GL(2, $\mathbb{L}$) on (q, q)-biprojective functions $F \in \mathcal{F}_{q,\mathbb{L}}$. That is

$$F_1(x, y) = (L_1 \circ F \circ L_2)(x, y).$$

This action defines an equivalence relation which we denote by $F_1 \approx_{\mathfrak{L}} F$. Define also the action of the group $\mathbb{L}^\times \times \mathrm{GL}(2, \mathbb{L})$ on q-biprojective polynomials $f \in \mathcal{V}_{q,\mathbb{L}}$ where $\mathbb{L}^\times < \mathrm{GL}(2, \mathbb{L})$ acts on f by **scaling**, and the action of GL(2, $\mathbb{L}$) is the usual right action, i.e.,

$$\begin{aligned} f_1(x, y) &= \alpha(f \circ L(x, y)), \\ &= \alpha\left(a(tx + uy)^{q+1} + b(tx + uy)^q(vx + wy) + c(tx + uy)(vx + wy)^q + d(vx + wy)^{q+1}\right), \end{aligned}$$

where $(\alpha, L) \in \mathbb{L}^\times \times \mathrm{GL}(2, \mathbb{L})$. In this case we say that $f \sim_{\mathfrak{L}} f_1$.

Set $\phi_f(x) = f(x, 1)$ so that ϕ_f is the corresponding q-projective polynomial. The projective version of the above action on the bivariate q-projective polynomial f, on the univariate q-projective polynomial ϕ_f can be given using the **fractional linear (Möbius)**

transformations over the finite field $\mathbb{L}$, i.e.,

$$\mathrm{PGL}(2,\mathbb{L}) \cong \mathfrak{M}(\mathbb{L}) = \left\{ x \mapsto \frac{tx+u}{vx+w} \ : \ t,u,v,w \in \mathbb{L} \mid tw - uv \neq 0 \right\}.$$

Now, define the action

$$\phi_{f_1}(x) = \alpha(vx+w)^{q+1}(\phi_f \circ \mu(x)),$$

for $(\alpha,\mu) \in \mathbb{L}^\times \times \mathrm{PGL}(2,\mathbb{L})$ and $\mu : x \mapsto \frac{tx+u}{vx+w}$. One addresses the zero of the denominator $(vx+w)$ by introducing $\infty = \beta/0$ for all $\beta \in \mathbb{L}^\times$. We define $\mathcal{P}^1(\mathbb{L}) = \mathbb{L} \cup \{\infty\}$. By defining $\mu(\infty) = t/v$, we see that all $\mu \in \mathfrak{M}(\mathbb{L})$ permutes $\mathcal{P}^1(\mathbb{L})$. Note that we view the action as

$$\phi_{f_1}(x) = \alpha\left(a(tx+u)^{q+1} + b(tx+u)^q(vx+w) + c(tx+u)(vx+w)^q + d(vx+w)^{q+1}\right),$$

so that ϕ_{f_1} is a (q-projective) polynomial over $\mathbb{L}$ and we do not have to deal with ∞ (but we will do that later, since it is helpful). We write $\phi_f \sim_{\mathfrak{M}} \phi_{f_1}$. The following lemma is straightforward.

Lemma 1.4. *We have $f \sim_{\mathfrak{L}} f_1$ if and only if $\phi_f \sim_{\mathfrak{M}} \phi_{f_1}$.*

We will not use ϕ_f to refer to univariate q-projective version of f and instead use f for both univariate and bivariate functions and polynomials. We will also use $\mathcal{V}_{q,\mathbb{L}}$ as the ambient space of both types of functions/polynomials.

4. Zeroes of projective polynomials

Let

$$f(x) = ax^{q+1} + bx^q + cx + d \in \mathbb{L}[x]$$

be a nonzero q-projective polynomial. If $a = 0$, then f is an affine polynomial and the set of $\mathbb{L}$-zeroes of f, i.e.,

$$Z_f' = \{x \in \mathbb{L} \ : \ f(x) = 0\}$$

satisfies $|Z_f'| \in \{0, 1, p^\delta\}$. To see that, first observe that **scaling**, i.e., $f \mapsto \alpha f$ for $\alpha \in \mathbb{L}^\times$, the **translations** $f(x) \mapsto f(x+\beta)$ for $\beta \in \mathbb{L}$ and the **dilations** $f(x) \mapsto f(\gamma x)$ for $\gamma \in \mathbb{L}^\times$ keep the number of $\mathbb{L}$-zeroes of f invariant. Then we have only a few options to consider:

- $f = 1$

  has no $\mathbb{L}$-zeroes —degenerate case (together with the omitted case $f = 0$).
- $f \in \{x, x^q\}$

  has one $\mathbb{L}$-zero.
- $f = x^q - cx - d$ where $c \neq 0$.

  We have
  - if $c = A^{q-1} \in (\mathbb{L}^\times)^{q-1}$, then f has
    - p^δ $\mathbb{L}$-zeroes if $\mathsf{tr}_{\mathbb{L}/\mathbb{D}}(d/A^q) = 0$, and
    - no $\mathbb{L}$-zeroes if $\mathsf{tr}_{\mathbb{L}/\mathbb{D}}(d/A^q) \neq 0$; or
  - one $\mathbb{L}$-zero if $c \notin (\mathbb{L}^\times)^{q-1}$,

  by Hilbert's Theorem 90.

Now assume $a \neq 0$. We will show that $|Z'_f| \in \{0, 1, 2, p^\delta + 1\}$. Assume f has at least one $\mathbb{L}$-zero $r \in Z'_f$. Now consider

$$f_1(x) = f(x + r) = ax^{q+1} + b'x^q + c'x.$$

The **reciprocal** $f_2(x) = x^{q+1} f_1(1/x)$ is

$$f_2(x) = a + b'x + c'x^q,$$

where $\deg f_2 < q + 1$. Now f_2 has one fewer $\mathbb{L}$-zeroes than f_1 (since we *punctured* the zero of f_1 at 0) and thus we have

$$|Z'_{f_2}| + 1 = |Z'_{f_1}| = |Z'_f| \in \{1, 2, p^\delta + 1\}.$$

When f has no $\mathbb{L}$-zeroes, it can be seen that translations, dilations, reciprocation and scaling cannot make the first and last coefficient zero. Therefore, in general case (including f has no $\mathbb{L}$-zeroes),

$$|Z'_f| \in \{0, 1, 2, p^\delta + 1\}.$$

These observations, together with the fact that $\mathrm{PGL}(2, \mathbb{L})$ is generated by translations, dilations and inversion (for which the corresponding action is reciprocation) [**140**], motivates us to ascribe $f(\infty) = 0$ if and only if $\deg f < q+1$ so that $\sim_{\mathfrak{M}}$ preserves the number of roots in $\mathcal{P}^1(\mathbb{L})$. Now we can define

Definition 1.5. The $\mathbb{P}^1(\mathbb{L})$**-zeroes** of a q-projective polynomial f is defined as

$$Z_f = \{x \in \mathcal{P}^1(\mathbb{L}) \ : \ f(x) = 0\},$$

where we define $f(\infty) = 0$ if and only if $\deg f < q + 1$.

Thus we have

Lemma 1.6. *Let $f \neq 0$ be a q-projective polynomial. Then,*

(i) $|Z_f|$ is invariant under $\sim_{\mathfrak{M}}$, and

(ii) $|Z_f| \in \{0, 1, 2, p^\delta + 1\}$.

Remark 1.7. A more rigorous proof of the lemma can be found in [**E**, Lemma 3.3].

When $q = 1$ (i.e., $k = \delta = 0$); Eq. (1) becomes quadratic, and the above lemma follows almost trivially. The case is therefore omitted in our treatment.

5. Group actions

For (q, r)-biprojective functions (f, g) where $q \neq r$, the left application of $\mathrm{GL}(2, \mathbb{L})$ does not work as a group action, i.e., $af + bg$ is not in general q-biprojective. However, scaling both components is a group action of $(\mathbb{L}^\times \times \mathbb{L}^\times) \leq \mathrm{GL}(2, \mathbb{L})$ on (q, r)-biprojective functions.

Let us summarize the notions of equivalence on projective and biprojective functions where $[\mathbb{F} : \mathbb{L}] = 2$.

Remark 1.8 (The semilinear group). The semi-linear group $\Gamma\mathrm{L}(2, \mathbb{L}) = \mathrm{Gal}(\mathbb{L}/\mathbb{F}_p) \ltimes \mathrm{GL}(2, \mathbb{L})$ comprising semi-linear mappings of type $(x, y) \mapsto (ax^q + by^q, cx^q + dy^q)$ where $q \in \mathrm{Gal}(\mathbb{L}/\mathbb{F}_p)$ and $a, b, c, d \in \mathbb{L}$ satisfying $ad - bc \neq 0$, is important in our treatment ($\Gamma\mathrm{L}(k, \mathbb{F}_{p^{n/k}})$ is defined similarly). We usually separate the actions of $\mathrm{GL}(2, \mathbb{L})$ and the

ϕ_f	q-projective	$\sim_{\mathfrak{M}}$	$\mathbb{L}^\times \times \mathrm{PGL}(2,\mathbb{L})$	scaling $\times$ right application of $\mu \in \mathrm{PGL}(2,\mathbb{L})$
f	q-biprojective	$\sim_{\mathfrak{L}}$	$\mathbb{L}^\times \times \mathrm{GL}(2,\mathbb{L})$	scaling $\times$ right application of $M \in \mathrm{GL}(2,\mathbb{L})$
(f,g)	(q,r)-biprojective		$(\mathbb{L}^\times \times \mathbb{L}^\times) \times \mathrm{GL}(2,\mathbb{L})$	scaling on f and g $\times$ right application of $M \in \mathrm{GL}(2,\mathbb{L})$
(f,g)	(q,q)-biprojective	$\approx_{\mathfrak{L}}$	$\mathrm{GL}(2,\mathbb{L}) \times \mathrm{GL}(2,\mathbb{L})$	left application of $L \in \mathrm{GL}(2,\mathbb{L})$ $\times$ right application of $M \in \mathrm{GL}(2,\mathbb{L})$
F	vectorial	$\approx_{\mathrm{GL}(\mathbb{F})}$	$\mathrm{GL}(\mathbb{F}) \times \mathrm{GL}(\mathbb{F})$	left application of $L \in \mathrm{GL}(\mathbb{F})$ $\times$ right application of $M \in \mathrm{GL}(\mathbb{F})$

TABLE 1. Notions of equivalence regarding projective and biprojective functions

Galois group to simplify the presentation. In principle they can be combined by simple modifications.

6. Bluher's enumeration results

The specific projective polynomial (originally considered by Abhyankar)

$$P_b(x) = x^{q+1} + x + b \in \mathbb{L}[x]$$

is rather important. Bluher counted the number of those $b \in \mathbb{L}$ for which P_b has j $\mathbb{L}$-zeroes, where $j \in \{0, 1, 2, p^\delta + 1\}$. Recall that $q = p^k$, $\delta = \gcd(k, l)$ and $\mathbb{L} = \mathbb{F}_{p^l}$.

THEOREM 1.9 ([**18**, Theorem 5.6.]). *Let $N_j(p,l)$ denote the number of polynomials $P_b(x) = x^{q+1} + x + b$ with $b \in \mathbb{L}$ such that P_b has j $\mathbb{L}$-zeroes. Then*

$$N_0(p,l) = \begin{cases} \frac{p^{l+\delta}-p^\delta}{2(p^\delta+1)} & \textit{if } l/\delta \textit{ is even,} \\ \frac{p^{l+\delta}-1}{2(p^\delta+1)} & \textit{if } p \textit{ is odd and } l/\delta \textit{ is odd,} \\ \frac{p^{l+\delta}+p^\delta}{2(p^\delta+1)} & \textit{if } p \textit{ is even and } l/\delta \textit{ is odd.} \end{cases}$$

$$N_1(p,l) = p^{l-\delta}.$$

$$N_2(p,l) = \begin{cases} \frac{p^{l+\delta}-2p^l-2p^\delta+3}{2(p^\delta-1)} & \textit{if } p \textit{ is odd and } l/\delta \textit{ is odd,} \\ \frac{(p^\delta-2)(p^l-1)}{2(p^\delta-1)} & \textit{otherwise.} \end{cases}$$

$$N_{p^\delta+1}(p,l) = \begin{cases} \frac{p^{l-\delta}-p^\delta}{p^{2\delta}-1} & \textit{if } l/\delta \textit{ is even,} \\ \frac{p^{l-\delta}-1}{p^{2\delta}-1} & \textit{if } l/\delta \textit{ is odd.} \end{cases}$$

7. Some references on projective polynomials

For background on finite fields we refer to [**115**] and the handbook [**121**]. Some papers that are related to the Galois theory of projective polynomials are [**1, 2, 3, 32**]. Bluher's paper [**18**] is a major source on the zeroes of projective polynomials. Many papers of Dillon and Dobbertin (also with other co-authors) are on important combinatorial applications of projective polynomials [**45, 46, 52, 51**]. Irreducible polynomials arising from projective polynomials and/or using the (above) natural action of PGL are addressed in [**35, 56,**

134, 62]. Many recent publications address zeroes of projective polynomials [**19, 119, 141, 94, 95, 96, 68, 69**].

We note that there are many more references on projective polynomials cited throughout the thesis that are in connection with the subject matter such as semifields, APN functions and the discrete logarithm problem.

8. Notation

The following remark is on the Big-O notation.

Remark 1.10. We write (cf. [**63**, Chapter 9]),

$$\begin{aligned}
f(n) = \mathcal{O}(g(n)) &\quad \text{if } \exists\, c > 0 \text{ and } n_0 \geq 1 \text{ such that } f(n) \leq cg(n) \text{ for all } n \geq n_0,\\
f(n) = \Omega(g(n)) &\quad \text{if } \exists\, c > 0 \text{ and } n_0 \geq 1 \text{ such that } f(n) \geq cg(n) \text{ for all } n \geq n_0,\\
f(n) = \Theta(g(n)) &\quad \text{if } f(n) = \mathcal{O}(g(n)) \text{ and } f(n) = \Omega(g(n)),\\
f(n) = o(g(n)) &\quad \text{if } \lim_{n\to\infty} f(n)/g(n) = 0,\\
f(n) = \omega(g(n)) &\quad \text{if } \lim_{n\to\infty} f(n)/g(n) = \infty,\\
f(n) \sim g(n) &\quad \text{if } \lim_{n\to\infty} f(n)/g(n) = 1.
\end{aligned}$$

CHAPTER 2

Finite semifields

A **finite semifield** $\mathbb{S} = (S, +, \circ)$ is a finite set S equipped with two operations $(+, \circ)$ satisfying the following axioms.

(S1) $(S, +)$ is a group.

(S2) For all $x, y, z \in S$,

- $x \circ (y + z) = x \circ y + x \circ z$,
- $(x + y) \circ z = x \circ z + y \circ z$.

(S3) For all $x, y \in S$, $x \circ y = 0$ implies $x = 0$ or $y = 0$.

(S4) There exists $\epsilon \in S$ such that $x \circ \epsilon = x = \epsilon \circ x$.

In this thesis, we are only interested in finite semifields. Henceforth, when we say a semifield we will mean a finite semifield.

1. Preliminaries on semifields

- An algebraic object satisfying the first three of the above axioms is called a **pre-semifield**.
- If $\mathbb{P} = (P, +, \circ)$ is a pre-semifield, then $(P, +)$ is an elementary abelian p-group [**101**, p. 185], and $(P, +)$ can be viewed as an n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. The prime p is called the **characteristic** of the pre-semifield.
- If $\circ$ is associative then $\mathbb{S}$ is the finite field $\mathbb{F}_{p^n}$ by Wedderburn's theorem.
- By a result of Menichetti (known as Kaplansky's conjecture [**120**]) when $n > 2$, there exist *proper* semifields of odd order p^n where $\circ$ is non-associative. There are no proper semifields of order 2^3. For $n > 3$, there exists proper semifields of order 2^n [**101**].
- A pre-semifield $\mathbb{P} = (\mathbb{F}_p^n, +, \circ)$ can be converted to a semifield $\mathbb{S} = (\mathbb{F}_p^n, +, *)$ using *Kaplansky's trick* by defining the new multiplication as

$$(x \circ e) * (e \circ y) = (x \circ y),$$

for any nonzero element $e \in \mathbb{F}_p^n$, making $(e \circ e)$ the multiplicative identity of $\mathbb{S}$.
- A pre-semifield is an $\mathbb{F}_p$-algebra, thus the multiplication is bilinear. Therefore we have $\mathbb{F}_p$-bilinear $B : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$, satisfying

$$B(x, y) = x \circ y,$$

and $\mathbb{F}_p$-linear left and right multiplications $L_x, R_y : \mathbb{F}_p^n \to \mathbb{F}_p^n$, with

$$L_x(y) := B(x, y) =: R_y(x).$$

The mapping L_x (resp. R_y) is a bijection whenever $x \neq 0$ (resp. $y \neq 0$) by (S3). Thus,

$$R_e(x) * L_e(y) = x \circ y.$$

2. Isotopy

Two pre-semifields $\mathbb{P}_1 = (\mathbb{F}_p^n, +, \circ_1)$ and $\mathbb{P}_2 = (\mathbb{F}_p^n, +, \circ_2)$ are said to be **isotopic** if there exist $\mathbb{F}_p$-linear bijections L, M and N of $\mathbb{F}_p^n$ satisfying

$$N(x \circ_1 y) = L(x) \circ_2 M(y).$$

Such a triple $\gamma = (N, L, M)$ is called an **isotopism** between $\mathbb{P}_1$ and $\mathbb{P}_2$. If additionally $L = M$ holds, we call γ a **strong isotopism** and $\mathbb{P}_1$ and $\mathbb{P}_2$ **strongly isotopic**. Isotopisms between a pre-semifield $\mathbb{P}$ and itself are called **autotopisms**. Thus the pre-semifield $\mathbb{P}$ and the corresponding semifield $\mathbb{S}$ constructed by Kaplansky's trick are isotopic and even strongly isotopic if $\mathbb{P}$ is commutative. Isotopy of pre-semifields is an equivalence relation and the isotopism class of a pre-semifield $\mathbb{P}$ is denoted by $[\mathbb{P}]$.

3. Nuclei

Associative substructures of a semifield $\mathbb{S} = (\mathbb{F}_p^n, +, *)$, namely the **left, middle and right nuclei**, are defined as follows:

$$\begin{aligned}
\mathbb{N}_l(\mathbb{S}) &:= \{x \in \mathbb{S} \ : \ (x * y) * z = x * (y * z), \ \forall y, z \in \mathbb{S}\},\\
\mathbb{N}_m(\mathbb{S}) &:= \{y \in \mathbb{S} \ : \ (x * y) * z = x * (y * z), \ \forall x, z \in \mathbb{S}\},\\
\mathbb{N}_r(\mathbb{S}) &:= \{z \in \mathbb{S} \ : \ (x * y) * z = x * (y * z), \ \forall x, y \in \mathbb{S}\}.
\end{aligned}$$

Intersection of the nuclei is denoted by $\mathbb{N}(\mathbb{S})$. Also relevant is the associative-commutative **center** of a semifield:

$$C(\mathbb{S}) = \{x \in \mathbb{N}(\mathbb{S}) \ : \ xy = yx, \ \forall y \in \mathbb{S}\}.$$

- It is easy to check that $\mathbb{N}_l(\mathbb{S}), \mathbb{N}_m(\mathbb{S}), \mathbb{N}_r(\mathbb{S}), \mathbb{N}(\mathbb{S}), C(\mathbb{S}) \subseteq \mathbb{F}_{p^n}$ are finite fields and if $\mathbb{S}$ is commutative then $\mathbb{N}_l(\mathbb{S}) = \mathbb{N}_r(\mathbb{S})$.
- Nuclei are isotopy invariants for semifields.
- The above definitions of nuclei do not apply directly to pre-semifields that are not semifields. However, since every pre-semifield $\mathbb{P} \in [\mathbb{S}]$ for some semifield $\mathbb{S}$, the nuclei can be thought to extend to pre-semifields. Thus, when we speak of the nuclei of a pre-semifield $\mathbb{P}$ we mean the nuclei of an isotopic semifield $\mathbb{S}$.
- A semifield $\mathbb{S}$ is a $C(\mathbb{S})$-algebra as well as a left vector space over $\mathbb{N}_l(\mathbb{S})$, a right vector space over $\mathbb{N}_r(\mathbb{S})$, a left and right vector space over $\mathbb{N}_m(\mathbb{S})$.

4. Connections to geometry and coding theory

Semifields coordinatize projective planes that are called semifield planes and different semifields coordinatize isomorphic planes if and only if they are isotopic ([**6**], see [**101**, Section 3] for a detailed treatment).

Semifields are equivalent to maximum rank distance codes with certain parameters (see e.g. [**133**]) and can be used to construct relative difference sets (see [**129**]).

5. Pre-semifields, bilinear maps and Dembowski-Ostrom polynomials

Let $\mathrm{End}(\mathbb{F}_p^n)$ denote the $\mathbb{F}_p$-linear endomorphisms of the vector space $\mathbb{F}_p^n$. Every $\mathbb{F}_p$-linear mapping $L \in \mathrm{End}(\mathbb{F}_p^n)$ can be written uniquely as an $\mathbb{F}_p$-linearized polynomial

$$L(x) = \sum_{i=0}^{n-1} b_i x^{p^i},$$

in the polynomial ring $\mathbb{F}_{p^n}[x]/(x^{p^n} - x)$. We will not make distinction between mappings and the polynomials. Consider the polynomials of the form

$$F(x) = \sum_{0 \le i \le j < n} a_{ij} x^{p^i + p^j}.$$

These polynomials are called **Dembowski-Ostrom (DO)** polynomials. Note that in characteristic two, some authors prefer $i < j$ on the indices to avoid linear terms. The **polarization** of a DO polynomial F is defined as

$$\Delta_F(x, y) = F(x + y) - F(x) - F(y) + F(0).$$

The mapping $\Delta_F : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is symmetric and $\mathbb{F}_p$-bilinear. Moreover, every symmetric $\mathbb{F}_p$-bilinear mapping is the polarization of a DO polynomial if and only if p is odd.

Dembowski and Ostrom showed that if $\Delta_F(x, y) = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in \mathbb{F}_{p^n}$, then $\Delta_F(x, y)$ describes a commutative pre-semifield multiplication [**41**]. Conversely, by a counting argument, every commutative pre-semifield multiplication can be written as $\Delta_F(x, y)$ for some DO polynomial F when p is odd [**39**]. In that case, we call F a **planar DO polynomial/mapping**.

Remark 2.1. When $p = 2$, the fact that $x \mapsto x^{2^i + 2^i}$ are Galois automorphishms of $\mathbb{F}_{2^n}$ introduces a fundamental problem: The terms $(xy)^{2^i}$ cannot appear in the polarization of a DO polynomial. Moreover, $\Delta_F(x, x) = 0$ for all $x \in \mathbb{F}_{2^n}$ and one cannot describe a pre-semifield multiplication via polarization of a DO polynomial.

Strong isotopy between pre-semifields can be recognized also in the corresponding planar DO polynomials:

Theorem 2.2. [**38**, Theorem 3.5.] *Let $F, G \in \mathbb{F}_{p^n}[x]$ be planar DO polynomials and $\mathbb{P}_1$, $\mathbb{P}_2$ be the corresponding pre-semifields. Then $\mathbb{P}_1$ and $\mathbb{P}_2$ are strongly isotopic via an isotopism $\gamma = (N, L, L)$ if and only if $F = NGL^{-1}$.*

Consequently, we say that two planar DO polynomials F, G are **linearly equivalent** if bijective linear mappings L_1, L_2 exist such that $F = L_1 G L_2$ and write $F \approx_{\mathrm{GL}(\mathbb{F}_{p^n})} G$. Note that this type of equivalence is the most general equivalence known to preserve the planarity of a DO polynomial, see [**105**].

Coulter and Henderson [**38**, Theorem 2.6] showed that the isotopy class of a commutative pre-semifield contains at most two strong isotopy classes.

Remark 2.3. For a DO polynomial F, the value $F(0)$ vanishes, therefore the definition of the polarization seem to have a superfluous term. However, the definition is for more general *quadratic* polynomials where the term $F(0)$ is necessary. The polarization of a DO polynomial F is identical to the polarization of the quadratic polynomial $F + L + c$ where $L \in \mathbb{F}_{p^n}[x]$ is an $\mathbb{F}_p$-linearized polynomial and $c \in \mathbb{F}_{p^n}$ a constant.

We refer the reader to surveys [**108, 86, 37**] for more on finite semifields.

CHAPTER 3

Commutative semifields and cryptography: Perfect nonlinear functions

In cryptography, **vectorial functions** $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ are employed (as *S-Boxes*) to introduce *nonlinearity* to the cipher as explained by Shannon using the notion *confusion* [**132**]. In symmetric cryptography, a well-known method to attack such a cipher is the so-called **differential cryptanalysis**, introduced by Biham and Shamir [**16**].

Let for $a, b \in \mathbb{F}_p^n$, where $a \neq 0$,

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_p^n \ : \ F(x+a) - F(x) = b\}.$$

If for carefully chosen a_i, b_i the value $\delta_F(a_i, b_i)$ are all *high*, one can devise a cryptanalysis of a cipher where the S-Box F is used in several consecutive *rounds*, which is a common practice in symmetric cryptography under the names SPN (substitution/permutation networks) and Feistel structures [**99**]. Therefore, to get a mathematical criterion for suitability of vectorial functions for cryptography (arising from the differential cryptanalysis), one defines **differential uniformity** of F as

$$\delta_F = \max\{\delta_F(a,b) \ : \ a, b \in \mathbb{F}_p^n, \ a \neq 0\}.$$

Now,

- if p is odd, then $\delta_F \geq 1$; and if the equality holds, then the function F is called **perfect nonlinear (PN)**; and
- if $p = 2$, then $\delta_F \geq 2$; and if the equality holds, then the function F is called **almost perfect nonlinear (APN)**.

Remark 3.1. This is yet another crucial difference between even and odd characteristics introduced by the fact that $x + x = 0$ for all $x \in \mathbb{F}_{2^n}$.

1. Representations of vectorial functions

Let $n = mk$. Then one can consider the vector space $\mathbb{F}_p^n$ as a k-dimensional $\mathbb{F}_{p^m}$-vector space. Thus, for all possible factorizations of $n = mk$, we can represent the function F in equivalent but different representations in the polynomial rings

$$\mathbb{F}_{p^m}[x_1, \ldots, x_k]/(x_1^{p^m} - x_1, \ldots, x_k^{p^m} - x_k),$$

written as

$$F(x_1, \ldots, x_k) = \sum_{0 \leq i_1, \ldots, i_k \leq p^m - 1} a_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}, \quad a_{i_1,\ldots,i_k} \in \mathbb{F}_{p^m}^k.$$

It is easy to see by **Lagrange interpolation** that every vectorial function F can uniquely be represented in every such representation. We view $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ to be composed of k parts $F = (f_1, f_2, \ldots, f_k)$, where each $f_i : \mathbb{F}_p^n \to \mathbb{F}_p^m$ are also vectorial functions.

2. Algebraic degree

These representations induce a natural definition of **algebraic degree** (equal for every representation of F for every suitable m and k) as

$$\deg F = \max \left\{ \sum_{j=1}^{k} \mathrm{wt}_p(i_j) \ : \ a_{i_1,\ldots,i_k} \neq (0, 0, \ldots, 0) \right\},$$

where $\mathrm{wt}_p(i_j) = \sum_{l=1}^{m} i_{jl}$. Note that $0 \leq \deg F \leq n(p-1)$. We speak of **univariate** ($k = 1$), **bivariate** ($k = 2$), and **multivariate** ($k > 1$) representations of F.

Remark 3.2.

- The DO polynomials of the previous chapter are quadratic vectorial functions with no linear or constant term in their univariate representations.
- Also, (the geometric naming) planarity of the previous chapter corresponds to (the cryptographic naming) perfect nonlinearity defined in this chapter by simply observing the correspondence between differential uniformity and polarizations of vectorial functions.

3. Polynomial degree

Another natural notion of degree, the so-called **polynomial degree** is defined by

$$\mathrm{pdeg}_k F = \max \left\{ \sum_{j=1}^{k} i_j \ : \ a_{i_1,\ldots,i_k} \neq (0, 0, \ldots, 0) \right\}.$$

For distinct factorizations $n = m_1 k_1$ and $n = m_2 k_2$, the polynomial degrees $\mathrm{pdeg}_{k_1} F$ and $\mathrm{pdeg}_{k_2} F$ are not necessarily the same. Thus, for the applications explored in this thesis, the algebraic degree is regarded more important.

4. Biprojective functions

The (q, r)-biprojective functions $F = (f_1, f_2)$ of Chapter 1 that are central to this thesis are quadratic (in the sense of algebraic degree) vectorial functions in bivariate representation $F(x, y) = (f_1(x, y), f_2(x, y))$ where both f_1 and f_2 are homogeneous (in the sense of polynomial degree) of homogeneity degrees $q + 1$ and $r + 1$ respectively.

5. Uni- and multiprojective functions

It is straightforward to generalize the concept to k-multiprojectivity for every possible factorization $n = km$. A k-**multiprojective** vectorial function F is a quadratic (in the sense of algebraic degree) function in k-variate representation $F = (f_1, \ldots, f_k)$, where all f_i are homogeneous (in the sense of polynomial degree) of homogeneity degrees $q_i + 1$, where $q_i = p^{j_i}$ for some $0 \leq j_i < m$ for $1 \leq i \leq k$.

Thus, the quadratic monomial maps $x \mapsto x^{p^i+1}$ are uniprojective, covering all quadratic monomials under composition of Galois automorphisms. Also, trivially, every quadratic vectorial function that is homogeneous in the n-variate representation can be thought of as an n-multiprojective vectorial function with homogeneity degrees $(2, 2, \ldots, 2)$.

CHAPTER 4

Classical methods for finding new commutative semifields

As we have seen, finding pre-semifields of order p^n is equivalent to finding bilinear mappings $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ satisfying

$$B(X, U) = 0 \iff XU = 0.$$

Since any bilinear mapping can be written as

$$B(X, U) = \sum_{0 \le i,j < n} A_{ij} X^{p^i} U^{p^j}, \quad A_{ij} \in \mathbb{F}_{p^n},$$

it is natural to consider first the *simplest* bilinear mappings that have few terms in this representation.

For commutative pre-semifields of order p^n when p is odd (as explained in previous chapters), one can consider DO polynomials

$$F(X) = \sum_{0 \le i,j < n} B_{ij} X^{p^i + p^j}, \quad B_{ij} \in \mathbb{F}_{p^n},$$

and try to identify planar mappings among them in increasing complexity, i.e., monomials, binomials, and so on.

1. Bilinear maps that correspond to pre-semifield multiplication

Let us try to give a picture on (commutative) pre-semifields with increasing complexity. In the commutative case, these correspond to planar DO polynomials in increasing complexity.

1.1. Monomials (Finite fields). Obviously, the monomial bilinear mappings

$$B(X, U) = AX^q U^r,$$

describe pre-semifields (via $X * U = B(X, U)$) that are isotopic to finite fields where q, r are $\mathbb{F}_{p^n}$-automorphisms and $A \in \mathbb{F}_{p^n}^\times$. The simplest commutative semifield is, of course, the finite field whose multiplication is given by the simplest bilinear mapping $B(X, U) = XU$ and it corresponds to the polarization of the planar DO polynomial

$$F(X) = \frac{1}{2} X^2.$$

1.2. Binomials (Albert's generalized twisted fields). Any binomial can be written up to isotopy

$$B(X, U) = AXU - X^q U^r,$$

and describes a pre-semifield if and only if

$$A \notin (\mathbb{F}_{p^n}^\times)^{q-1} (\mathbb{F}_{p^n}^\times)^{r-1}.$$

These were found by Albert [**7**] and are called **generalized twisted fields**. The original family of Albert, which is named **twisted fields**, requires $q = r$. Albert showed that the generalized twisted fields that are isotopic to a commutative semifield are isotopic to the twisted field

$$B(X, U) = X^q U + XU^q,$$

when $n/\gcd(k, n)$ is odd where $q = p^k$ (cf. [**85**, Proposition 5.3 (i)]). In this case the corresponding planar DO polynomial whose polarization gives a commutative twisted field is

$$F(X) = X^{q+1}.$$

We denote the family of commutative twisted fields of Albert by Family $\mathcal{A}$.

1.3. Tri- and multinomials. The natural approach that is used to classify the above cases does not seem to work for larger number of terms. Indeed, the only known (to the best of our knowledge) instance of trinomial pre-semifields not isotopic to finite fields or generalized twisted fields are isotopic to the pre-semifield described by the bilinear map

$$B(X, U) = X^{81}U^9 + X^9U^{81} - XU$$

over $\mathbb{F}_{3^5} \times \mathbb{F}_{3^5}$.

1.4. More complex planar mappings. Polarizations of monomial DO mappings are either monomial or binomial bilinear mappings. One can next consider binomial DO mappings which always give polarizations that have up to four terms. Zha, Kyureghyan and Wang (Family $\mathcal{ZKW}$) [**146**] and Bierbrauer (Families $\mathcal{B}_3$ and $\mathcal{B}_4$) [**13**] gave new commmutative semifields from binomial DO mappings. Budaghyan and Helleseth (Family $\mathcal{BH}$) [**21**] gave a new family of commutative semifields from multinomial planar functions, which was discovered independently by Zha and Wang [**147**] whose corresponding planar function is a trinomial.

2. The bivariate method of Dickson and others

To construct a semifield of order p^n where p is odd and $n = 2m$ is even, one can consider a quadratic polynomial F in bivariate representation

$$F(x, y) = (f(x, y), g(x, y)).$$

To show that F is planar, one has to show that the polarization of F has only nontrivial zeroes. In the bivariate method, this corresponds to solving

$$\Delta_f((x, y), (u, v)) = f(x + u, y + v) - f(x, y) - f(u, v) + f(0, 0) = 0,$$
$$\Delta_g((x, y), (u, v)) = g(x + u, y + v) - g(x, y) - g(u, v) + f(0, 0) = 0,$$

simultaneously. If one chooses f to be the *simplest* nontrivial function (i.e., that involves both variables) $f(x, y) = xy$, that is to say the finite field multiplication, the first polarization becomes

$$\Delta_f((x, y), (u, v)) = xv + uy = 0,$$

which in turn gives $x = -uy/v$ for nonzero v. Thus, one can plug this into the second polarization to eliminate x and possibly solve the problem for judicious choices of g. In fact, starting with Dickson in 1935, many new semifields have been found using this method and by considering different g, again in increasing *complexity*. The family of Dickson (Family $\mathcal{D}$) [**43**] and the family of Zhou and Pott (Family $\mathcal{ZP}$) [**148**] as well as Bierbrauer's (not necessarily commutative) family [**14**] that includes $\mathcal{BH}/\mathcal{ZW}$ can be seen as examples to this method.

Remark 4.1. Extending the method to the non-commutative case is rather straightforward: Choose again the same left-part multiplication (or a similarly simple one), and then choose some right-part (not necessarily symmetric) bilinear multiplication (that is, not necessarily induced by the polarization of a quadratic polynomial in the bivariate representation). That is to say, define a multiplication by

$$(x, y) * (u, v) = (xv + uy, \mu((x, y), (u, v))),$$

where μ is bilinear on (x, y) and (u, v). There are many such constructions in the literature which includes Hughes and Kleinfeld [**71**], Knuth [**101**], Bierbrauer [**14**] and Taniguchi [**136**].

3. Bivariate method and weak nucleus semifields

Knuth [**101**] explored a generalization of Family $\mathcal{D}$ by introducing the notion of a *weak nucleus*. In fact, Knuth's families mentioned above fall into this setting. A **weak nucleus** $\mathbb{W}$ of a semifield $\mathbb{S} = (\mathbb{W}^n, +, *)$ is a finite field for which $(x * y) * z = x * (y * z)$ whenever any two of $x, y, z \in \mathbb{S}$ are in $\mathbb{W}$. Ganley [**55**] and Cohen and Ganley [**36**] explored (commutative) semifields that are two dimensional over a weak nucleus. In this special case they show that the semifield multiplication $(x, y) * (u, v)$ can be written as

$$(x, y) * (u, v) = (\mu(x, u) + xv + uy, \nu(x, u) + yv),$$

where μ, ν are bilinear. Simple cases lead to Dickson semifields $\mathcal{D}$ and the finite field. Investigating more complicated choices for μ, ν, they discovered two new families of commutative semifields: Family $\mathcal{G}$ and Family $\mathcal{CG}$. This method also leads to non-commutative semifields including the families found by Hughes and Kleinfeld [**71**] and Knuth [**101**] as it is a generalization of these semifields.

4. Squared permutation polynomials

For a vectorial function F in odd characteristic such that $F(0) = 0$, we say that F is **two-to-one**, if for every $x \in \mathbb{F}_{p^n}^{\times}$, $F(x) = F(y)$ for exactly two $y \in \mathbb{F}_{p^n}^{\times}$ and $F(x) \neq 0$ for all $x \in \mathbb{F}_{p^n}^{\times}$. For a DO polynomial F this is equivalent to saying $|\operatorname{Im}(F)| = (p^n + 1)/2$ since $F(x) = F(-x)$ for all $x \in \mathbb{F}_{p^n}^{\times}$.

Weng and Zeng proved [**142**] a strong sufficient condition on planar DO polynomials. Namely, they proved: If a DO polynomial F is two-to-one, then F is planar. The converse is also true as shown by Kyureghyan and Pott [**105**]. Thus, a possible way to produce commutative semifields is to find a permutation polynomial P with $P(0) = 0$ such that $P(x^2)$ is a DO polynomial. Indeed, some Dickson polynomials (cf. [**121**, Section 8.1.8]) satisfy this property:

$$D_5^+(x) = x^5 + x^3 - x \text{ and } D_5^-(x) = x^5 - x^3 - x,$$

over $\mathbb{F}_{3^n}$ where n is odd (i.e., $10 = 3^2 + 1$, $6 = 3 + 3$ and $2 = 1 + 1$, hence $D_5^{\pm}(x^2)$ is a DO polynomial). The corresponding semifields are $\mathcal{CM}$ and $\mathcal{DY}$ and found by Coulter and Matthews [**39**] and Ding and Yuan [**47**] respectively.

5. Methods in characteristic two

To the best of our knowledge there are only two families of commutative semifields in characteristic two. Both are based on trace maps and Kantor's family generalizes the Knuth family.

- Knuth observed [**100**] that the multiplication

  $$X * Y = XY + (\mathsf{tr}_{\mathbb{F}/\mathbb{K}}(X)Y + \mathsf{tr}_{\mathbb{F}/\mathbb{K}}(Y)X)^2$$

  describes a commmutative pre-semifield $\mathbb{P} = (\mathbb{F}, +, *)$ where $\mathbb{F} = \mathbb{F}_{2^{km}}$, $\mathbb{K} = \mathbb{F}_{2^k}$ with odd $m > 1$.
- Kantor [**85**] showed (under the same conditions on m) that

  $$X * Y = XY + \left(X \sum_{i=1}^{n} \mathsf{tr}_{\mathbb{F}/\mathbb{F}^{(i)}}(\zeta_i Y) + Y \sum_{i=1}^{n} \mathsf{tr}_{\mathbb{F}/\mathbb{F}^{(i)}}(\zeta_i X) \right)^2,$$

  where

  $$\mathbb{F} \supset \mathbb{F}^{(1)} \supset \cdots \supset \mathbb{F}^{(n)} \supseteq \mathbb{K},$$

  is a commutative pre-semifield $\mathbb{P} = (\mathbb{F}, +, *)$ where $\zeta_i \in \mathbb{F}^{\times}$ are arbitrary and $n \geq 1$.

Kantor's pre-semifields are commutative versions of the *symplectic* pre-semifields of the Kantor-Williams construction [**89**]. Neither method seems generalizable to the odd characteristic case. The converse observation is also worth noting: no odd characteristic family of (proper) commutative pre-semifields seems to have analogues in the binary case.

CHAPTER 5

Enumeration results for finite semifields

In this chapter, we list the known results on the number of non-isotopic commutative and non-commutative semifields of odd and even orders and show how our results sit in the context of the state of the art.

1. Commutative semifields in the odd characteristic

Two decades ago, Kantor [**85**, Section 5] wrote a survey that listed the exact numbers of non-isotopic commutative semifields of odd order p^n for the known families at the time. The listed families were $\mathcal{A}, \mathcal{CM}, \mathcal{D}, \mathcal{CG}, \mathcal{G}$, along with the sporadic example of Penttila and Williams [**126**]. These numbers as well as the references where the enumeration is done are listed in Tables 1 and 2. The total number of pairwise non-isotopic semifields arise from these families add up to less than n. Since then, several new families have been found. These are $\mathcal{ZKW}, \mathcal{DY}, \mathcal{BH}/\mathcal{ZW}, \mathcal{ZP}, \mathcal{B}_3, \mathcal{B}_4$, excluding our new family $\mathcal{S}$. Apart from $\mathcal{ZP}$, the known number of non-isotopic commutative semifields in these families are (sub)linear in n. The number of non-isotopic commutative semifields Family $\mathcal{ZP}$ provides is quadratic in n. Therefore, before our family, (letting N_{p^n} be the number of pairwise non-isotopic commutative semifields of odd order p^n) the lower bound on the number was as follows:

$$N_{p^n} \geq \frac{n(\sigma(n)-1)}{8} + cn,$$

when $\nu_2(n) \geq 1$ and c a constant where $\nu_2(n)$ denotes the 2-adic valuation of n (i.e., $2^{\nu_2(n)}|n$ and $2^{\nu_2(n)+1} \nmid n$) and $\sigma(n)$ denotes the odd part of an integer n (i.e., $\sigma(n) = n/2^{\nu_2(n)}$).

Improving this number to an exponential level was considered a major open problem. In fact, Pott noted [**128**]:

> Deciding whether the number of nonisotopic (commutative) semifield[s] can be bounded by a polynomial in n [is] the main problem in connection with commutative semifields of [odd] order p^n.

The main enumeration result we give in Chapter 3, after Family $\mathcal{S}$, is exponential in n,

$$N_{p^n} \geq \frac{(\sigma(n)-1)(p^{n/4}-1)}{2n},$$

when $\nu_2(n) \geq 2$; and solves this problem.

2. Commutative semifields in the even characteristic

For a long time until 1965 when Knuth [**100**] provided the first family, there were no known (proper) commutative semifield of even order whereas families of Dickson and Albert providing proper commutative semifields of odd order had been in existence for decades.

The situation took a dramatic turn in 2003 with Kantor's family [**85**] that arose from the *symplectic* semifield family of Kantor and Williams [**89**]. While there were only a linear number (in n) of known non-isotopic commutative semifields in the odd characteristic, the number of known non-isotopic commutative semifields in the even characteristic became super-polynomial (i.e., not bounded by a polynomial) in $q = p^n$.

The number of non-isotopic commutative semifields of even order arising from the family of Kantor [**85**] is:

$$N_{2^{km}} \geq \frac{2^{km(\rho(m)-1)}}{k^2m^4},$$

when $m > 1$ is odd and m is not a power of 3, where we denote by $\rho(m)$ the number of prime factors of m counting multiplicities.

Kantor [**85**, p. 112] noted that the disparity between the numbers in the odd (polynomial in n) and in the even (super-polynomial in q) characteristic cases is a major problem:

> The main problem concerning commutative semifields is that there are too few of them known. [...] However, the results of the present paper now indicate a major problem in the opposite direction, since now there are many different semifield planes known in characteristic 2 but not so many in odd characteristic.

Also, Kantor and Williams [**89**] remarked:

> Finally, we come to the most important problem: *much larger numbers of semifield planes are needed in all characteristics.* The difficulty is the nonisomorphism question for planes, which is harder than that for the semifields themselves. Isotopies are notoriously difficult to deal with. [...] What is needed is a better and more general approach to proving nonisotopy. A simple way is to compare the kernels of two semifields, or to compare various nuclei [**40**, p. 237]. However, these are very weak invariants, and by themselves appear to be unable to produce as many as m nonisomorphic planes of order q^m for prime q and large m.

The isotopy method we establish for biprojective semifields in Chapter 2, which is key to our enumeration results, addresses this important remark of Kantor and Williams.

3. The non-commutative case

In the odd characteristic case, there are several constructions that give similar amount of pairwise non-isotopic semifields that are not necessarily commutative.

3.1. Generalized twisted fields. The number of generalized twisted fields of order p^n is at best $\Theta(p^{n/3})$ and in general $\Theta(p^s)$, where s satisfies $s|n$ and $s < n/2$ as given in [**130**, Corollary 27], which uses results on the automorphishms of generalized twisted fields by Biliotti, Jha and Johnson [**17**].

3.2. Cyclic semifields and semifields from skew polynomial rings. Johnson, Marino, Polverino and Trombetti showed [**74**] that the cyclic semifields found by Jha and Johnson [**73**] (generalizing the work of Sandler [**131**]) contains at least

$$\frac{q^d - T}{hd(q-1)}$$

semifields of order q^{2d} where T is the number of elements contained in a proper subfield of $\mathbb{F}_{q^d}$ and $q = p^h$. Lavrauw and Sheekey [**107**] slightly improving the upper bound of Kantor and Liebler [**88**], showed that the upper bound is

$$\frac{q^d - T}{d}.$$

Therefore, the number is at best $\Theta(p^{n/2})$.

3.3. HMO construction. Hiramine, Matsumoto and Oyama [**70**] gave a construction (HMO) of semifields of order q^4 from semifields of order q^2. Kantor [**87**] showed that the number of pairwise non-isotopic HMO semifields of order q^4 is at least $q^2/4pe^2$ where $q = p^e$.

Therefore the known number of pairwise non-isotopic semifields of order p^n arising from HMO construction is $\Omega(p^{n/2})$.

Remark 5.1. Kantor gives an *elementary* upper bound that is quite larger than the lower bound [**87**, Theorem 1.6], while still polynomial in the order. But the aim of Kantor is to show that the number is not super-polynomial in the order $q = p^n$ and therefore the bound is not necessarily tight.

Remark 5.2 (The number of pairwise non-isomorphic translation planes). Recall that semifields coordinatize projective planes that are called **semifield planes**. If we relax exactly one of the distributivity axioms (S2) of the semifield, we get an algebraic object called a **quasifield**. Quasifields coordinatize projective planes that are called **translation planes** ([**67**], see also [**72**] for types of projective planes and algebraic objects coordinatizing them). Therefore, semifield planes are translation planes. It is natural to ask enumeration questions about translation planes. We remark that the HMO construction is actually for translation planes. In fact, Kantor shows [**87**, Theorem 1.5 (ii)], the number of pairwise non-isomorphic HMO (translation) planes of order q^4 is exponential in the order.

3.4. The even characteristic case. In the even characteristic case, the Kantor-Williams family is the main source (enumeration-wise) of pairwise non-isotopic semifields. Therefore the number of commutative and general semifields do not differ substantially.

3.5. Taniguchi semifields. We show in Chapter 5 and [**K**, Theorem 5] that the number of pairwise non-isotopic Taniguchi semifields of order p^n is at least

$$p^{\frac{n}{2}+s},$$

where s is the largest divisor of $n/2$ such that $s < n/4$. Therefore, for $n = 6s$ the number is $\Theta(p^{2n/3})$ which makes the Taniguchi family the largest known family of non-commutative semifields of odd order.

CHAPTER 6

Biprojective method: Generalizing Albert's twisted fields

Let us first recall our setting. Let $n = 2m$, p be odd and $\mathbb{M} = \mathbb{F}_{p^m}$. We define

$$\mathcal{V}_{q,\mathbb{M}} = \{(a, b, c, d)_q \ : \ a, b, c, d \in \mathbb{M}\},$$

for $q = p^k$ for an integer $0 \leq k < m$, recalling that by $(a_0, b_0, c_0, d_0)_q$ we mean the q-biprojective function $f : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$,

$$f : (x, y) \mapsto a_0 x^{q+1} + b_0 x^q y + c_0 x y^q + d_0 y^{q+1}.$$

A (q, r)-biprojective function $F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$, $F : (x, y) \mapsto (f(x, y), g(x, y))$ belongs to

$$F \in \mathcal{V}_{q,\mathbb{M}} \times \mathcal{V}_{r,\mathbb{M}},$$

where $r = p^l$ for an integer $0 \leq l < m$ and

$$g : (x, y) \mapsto a_1 x^{r+1} + b_1 x^r y + c_1 x y^r + d_1 y^{r+1}.$$

As mentioned before, a (q, r)-biprojective function $F = (f, g)$ is a quadratic (in the sense of algebraic degree) vectorial function in bivariate notation, whose components f and g are homogeneous with homogeneity degrees (in the sense of polynomial degree) $q + 1$ and $r + 1$ respectively. In this view, biprojective functions generalize quadratic monomials (*uniprojective* functions) in univariate notation.

We will now try to give the intuition behind pursuing biprojective functions in search for new semifields.

1. The number of required permutations is low

Let us first consider polarizations of quadratic monomials in univariate notation (i.e., Albert's twisted fields) which we generalize. These are $F(X) = X^{q+1}$ (for $q = p^k$) and their polarizations are

$$\Delta_F(X, U) = X^q U + X U^q = 0,$$

for which we try to show that there are no nontrivial zeroes. It is immediate to see

$$X^{q-1} = (-1) U^{q-1}$$

implies, whenever $-1 \notin (\mathbb{F}_{p^n}^\times)^{q-1}$ we have pre-semifields. However, we will show a slightly more difficult proof to make our point. For every $U \in \mathbb{F}_{p^n}^\times$, apply $X \mapsto XU$ to get

$$U^{q+1}(X^q + X) = 0.$$

This means that proving bijectivity of *one* linear mappping is enough. In this case, this mapping is described by $X \mapsto \Delta_F(X, 1) = X^q + X$. Note that, for an arbitrary vectorial function, the number of required bijective linear mappings is $|\mathbb{F}_{p^n}^\times / \mathbb{F}_p^\times| = (p^n - 1)/(p -$

1). Now, for a (q,r)-biprojective function over $\mathbb{M}\times\mathbb{M}$, it is easy to show that checking polarizations for

$$\mathcal{P}^1(\mathbb{M}) = \{(0,1)\} \cup \{(1,v) : v \in \mathbb{M}\}$$

is enough, by applying $\mathbb{M}$-linear transformations on variables. To that end, define

$$\begin{aligned} \mathsf{D}_f^0(x,y) &= b_0x^q + c_0x + d_0y^q + d_0y, & \mathsf{D}_f^\infty(x,y) &= a_0x^q + a_0x + c_0y^q + b_0y,\\ \mathsf{D}_g^0(x,y) &= b_1x^r + c_1x + d_1y^r + d_1y, & \mathsf{D}_g^\infty(x,y) &= a_1x^r + a_1x + c_1y^r + b_1y, \end{aligned}$$

and for $u \in \mathcal{P}^1(\mathbb{M}) \setminus \{0,\infty\}$,

$$\begin{aligned} \mathsf{D}_f^u(x,y) &= (a_0u+b_0)x^q + (a_0u^q+c_0)x + (c_0u+d_0)y^q + (b_0u^q+d_0)y,\\ \mathsf{D}_g^u(x,y) &= (a_1u+b_1)x^r + (a_1u^r+c_1)x + (c_1u+d_1)y^r + (b_1u^r+d_1)y. \end{aligned}$$

The following lemma was proved in [**A**, Lemma 3.1].

Lemma 6.1. *Let $(x,y) \mapsto F(x,y) = (f(x,y), g(x,y))$ be a (q,r)-biprojective mapping of $\mathbb{M}\times\mathbb{M}$. Then F is planar if and only if the pair of equations*

$$\mathsf{D}_f^u(x,y) = 0 = \mathsf{D}_g^u(x,y)$$

has exactly one solution for each $u \in \mathcal{P}^1(\mathbb{M})$.

Proof. We need to show that the polarization $\Delta_F((x,y),(u,v)) = (x,y)*(u,v) = 0$ has a unique zero for each $(u,v) \in \mathbb{M}\times\mathbb{M}\setminus(0,0)$ if and only if $\mathsf{D}_f^w(x,y) = 0 = \mathsf{D}_g^w(x,y)$ has a unique solution for each $w \in \mathcal{P}^1(\mathbb{M})$. Inspecting the equations, one immediately sees that the case $v = 0$ corresponds to $\mathsf{D}_f^\infty(x,y) = 0 = \mathsf{D}_g^\infty(x,y)$ after applying $x \mapsto xu$ and $y \mapsto yu$. For $v \in \mathbb{M}^\times$, apply $x \mapsto xv$, $y \mapsto yv$ and $u \mapsto uv$ to get the remaining cases $\mathsf{D}_f^w(x,y) = 0 = \mathsf{D}_g^w(x,y)$ for $w \in \mathbb{M}$. □

Thus, the number of bijections we need to show becomes $p^{n/2}+1$. Even though this number is larger than 1, it is much smaller than $(p^n-1)/(p-1)$. Technically, these numbers correspond to proving bijectivity of polarizations indexed by

- the **projective point** $\mathcal{P}^0(\mathbb{F}_{p^n})$ for quadratic monomials in univariate notation (uniprojective functions),
- the **projective line** $\mathcal{P}^1(\mathbb{F}_{p^{n/2}})$ for biprojective functions, instead of
- the $(n-1)$-dimensional **projective space** $\mathcal{P}^{n-1}(\mathbb{F}_p)$ for arbitrary vectorial functions.

This idea can easily be generalized to non-commutative case and also to k-multiprojective functions.

2. Covers many of the previous constructions

Letting f be the simplest biprojective function that involves both variables, for instance $f = xy^q$, one easily sees that many of the commutative semifield families that were introduced in the previous chapter are covered by the (q,r)-biprojective idea with suitable biprojective choices of g. This includes Families $\mathcal{D}, \mathcal{BH}/\mathcal{ZW}, \mathcal{ZP}$ as well as the finite field as shown in the next chapter. Also the Family $\mathcal{A}$ falls into our setting with more complicated choices of f and g while resorting to the simplified setting $q = r$ for the automorphisms. These observations hints the possibility of new families within the (q, r)-biprojective setting since the arbitrary (and complicated) choices had not been fully analyzed.

Remark 6.2. The biprojective idea is easily generalized to non-commutative semifields. We say that a pre-semifield multiplication is (q, r)-biprojective if

$$(x, y) * (u, v) = (\mu((x, y), (u, v)), \nu((x, y), (u, v))),$$

where μ, ν are bilinear (in (x, y) and (u, v)) and homogeneous with homogeneity degrees $q+1$ and $r+1$ respectively (i.e., μ contains monomials from $\{x^q u, xu^q, x^q v, xv^q, y^q u, yu^q, y^q v, yv^q\}$ and similarly for ν where q is replaced with r).

Many of the non-commutative families including Hughes-Kleinfeld, Knuth, Bierbrauer and Taniguchi fall into the (q, r)-biprojective setting.

3. Autotopisms/Isotopisms within family are "nice"

Biliotti, Jha and Johnson determined the full autotopisms groups of generalized twisted fields (GTF) in [**17**]. Previous work on autotopisms and isotopisms of GTFs was by Albert who determined solvability of their autotopism groups [**5**] and gave the exact conditions when two GTFs are isotopic [**8**] as well as when a GTF is isotopic to a commutative semifield [**7**]. Purpura determined the exact numbers of pairwise non-isotopic GTFs using these results [**130**]. Recall that rough numbers were already given in Kantor's survey [**85**, Section 5].

3.1. Isotopisms of twisted fields (uniprojective GTFs). Consider the special case of GTFs described by homogeneous bilinear pre-semifield multiplications (i.e., the twisted fields), $B_1(X, Y) = X^q Y + DXY^q$ and $B_2(X, Y) = X^{q'} Y + EXY^{q'}$ over $\mathbb{F}_{p^n}$ where q and q' are $\mathbb{F}_{p^n}$-automorphisms such that $1 \notin \{q^2, q'^2\}$ and $D, E \in \mathbb{F}_{p^n}^\times$. Let B_1, B_2 be the multiplications of two isotopic twisted fields. By [**17**, Theorem 6.1], an isotopism triple $(L, M, N) \in (\mathrm{GL}(n, \mathbb{F}_p))^3$ mapping B_1 to B_2, i.e.,

$$N(B_1(X, Y)) = B_2(L(X), M(Y)),$$

satisfy $(L, M, N) \in \Gamma\mathrm{L}(1, \mathbb{F}_{p^n})^3$ which immediately implies q and q' should *agree*, i.e., $q' \in \{q, \overline{q}\}$. Moreover, (L, M, N) satisfies (setting $q = q'$),

$$L(X) = AX^r, M(Y) = BY^r, \text{ and } N(Z) = A^q BZ^r,$$

where $A, B \in \mathbb{F}_{p^n}^\times$ and r is an $\mathbb{F}_{p^n}$-automorphism satisfying $D^r/E = (B/A)^{q-1}$. When, $\overline{q} = q'$, one has a similar set of requirements.

- This observation immediately gives a method to count pairwise non-isotopic twisted fields that have the specific homogeneous form $B(X, Y) = X^q Y + DXY^q$ for multiplication. For every fixed $E \in \mathbb{F}_{p^n}^\times$ one can easily count such $D \in \mathbb{F}_{p^n}^\times$ with $D^r/E \in (\mathbb{F}_{p^n}^\times)^{q-1}$ which is at most

$$n(p^n - 1)/\gcd(p^k - 1, p^n - 1) = n(p^n - 1)/(p^{\gcd(k,n)} - 1).$$

This gives the immediate lower bound

$$(p^{\gcd(k,n)} - 1)/n$$

on the number of pairwise non-isotopic twisted with homogeneous multiplication $B(X,Y) = X^qY + DXY^q$ for a specific $q = p^k$. Recall that $q = p^{n/2}$ is not allowed. Thus, for the largest number of isotopy classes, we choose $\gcd(k,n) = n/3$ when $n = 3k$.

- Recall that a GTF that is isotopic to a commutative semifield is isotopic to a twisted field with multiplication $B(X,Y) = X^qY+XY^q$ for some $\mathbb{F}_{p^n}$-automorphism $q = p^k$ such that $n/\gcd(k,n)$ is odd, as proved by Albert ([**7**], see also [**17**, Theorem 1.11]). This immediately shows that the number of pairwise non-isotopic commutative twisted fields is precisely $\lfloor(\sigma(n) - 1)/2\rfloor$ where $\sigma(n)$ denotes the odd part of n.

3.2. Autotopism groups of uniprojective GTFs. Let, as above, $B(X,Y) = X^qY + DXY^q$ be the multiplication of a twisted field $\mathbb{P}$. One sees immediately that

$$\mathbb{F}_{p^n}^{\times} \cong \{(N_A, L_A, M_A) \ : \ A \in \mathbb{F}_{p^n}^{\times}\},$$

where

$$L_A : X \mapsto AX, \quad M_A : Y \mapsto AY, \quad N_A : Z \mapsto A^{q+1}Z,$$

is a subgroup of the autotopism group $\mathrm{Aut}(\mathbb{P})$.

Existence of such large autotopism groups simplifies many combinatorial problems. In fact, group theoretic arguments involving large automorphism/autotopism groups have been employed quite often: for instance, by Yoshiara [**145**] and by Dempwolff [**42**] in the context of vectorial functions and also by Biliotti, Jha and Johnson in the very context of GTFs [**17**, Sections 3 and 6]. Our method in Chapter 2 is inspired by the methods of Dempwolff and Yoshiara.

3.3. Biprojective generalizations. Note that the above ideas will be extended to the biprojective case. Let $\mathbb{P}$ be a pre-semifield of order p^n with (q,r)-biprojective multiplication. Then

$$\mathbb{F}_{p^{n/2}}^{\times} \cong \{(N_a, L_a, M_a) \ : \ a \in \mathbb{F}_{p^{n/2}}^{\times}\},$$

where

$$L_a : (x_1, x_2) \mapsto (ax_1, ax_2), \quad M_a : (y_1, y_2) \mapsto (ay_1, ay_2), \quad N_a : (z_1, z_2) \mapsto (a^{q+1}z_1, a^{r+1}z_2),$$

is a subgroup of $\mathrm{Aut}(\mathbb{P})$.

It is natural to expect that the role of $\Gamma\mathrm{L}(1, \mathbb{F}_{p^n})^3$ in the uniprojective setting is played by $\Gamma\mathrm{L}(2, \mathbb{F}_{p^{n/2}})^3$ in the biprojective setting. We will show that a version of this expectation indeed holds under a certain condition. Instead of the result of Albert that shows that every isotopism between uniprojective twisted fields must be of the form $\Gamma\mathrm{L}(1, \mathbb{F}_{p^n})^3$, we will prove that **if there is an isotopism between two biprojective semifields $\mathbb{P}_1, \mathbb{P}_2$, then there is an isotopism of the form $\Gamma\mathrm{L}(2, \mathbb{F}_{p^{n/2}})^3$** under a certain condition (see Chapter 2 for details) which is equivalent in strength when one wants to solve the enumeration problem. Then, the enumeration problem in the biprojective setting is handled via a direct analogy (albeit with considerable complexity) to the uniprojective setting.

REMARK 6.3 (Equivalence of planar functions and isotopy). As explained in Chapter 2, one can consider equivalence of planar functions instead of strong isotopy of commutative presemifields. The group actions of $\mathrm{GL}(2,\mathbb{F}_{p^{n/2}})\times\mathrm{GL}(2,\mathbb{F}_{p^{n/2}})$ on (q,q)-biprojective functions and $(\mathbb{F}^{\times}_{p^{n/2}}\times\mathbb{F}^{\times}_{p^{n/2}})\times\mathrm{GL}(2,\mathbb{F}_{p^{n/2}})$ on (q,r)-biprojective functions are instrumental in the analysis of such functions partly thanks to the above observations. Note also that in most cases GL and ΓL can be used interchangeably with small adjustments. We usually prefer GL for its simplicity and handle the semi-linearity (Galois automorphisms) separately.

4. There are many free spots for field coefficients

Let us go back to the bilinear multiplications of GTFs of order p^n, i.e., $B(X,Y)=X^qY+DXY^r$. Here we have two options for *variation*:

- different choices for the field automorphisms q,r, and
- different choices for the field coefficient D.

Naturally, since there are only a quadratic (n^2) number of field automorphism choices but an exponential (p^n) number of field coefficient choices, the latter is better suited for constructing large families. A simple inspection shows that we have no other choice than $D=1$ and $q=r$ to get a commutative pre-semifield, thus the only variation comes from (up to) n field automorphism choices. For the non-commutative case, there are many possibilities for D (depending on a gcd condition), which indeed gives an exponential count. The disparity between enumeration results for commutative and non-commutative semifields is introduced by this observation.

Biprojective setting supplies many more spots for field coefficients even in the commutative case:

$$F=((a_0,b_0,c_0,d_0)_q,(a_1,b_1,c_1,d_1)_r),\quad a_i,b_i,c_i,d_i\in\mathbb{M},q,r\in\mathrm{Gal}(\mathbb{M}/\mathbb{F}_p).$$

Let us explain intuitively why the known biprojective constructions were not able to exploit these spots.

- All of the families $\mathbb{F},\mathcal{D},\mathcal{ZP},\mathcal{BH}/\mathcal{ZW},\mathcal{A}$ contain only one free coefficient (the non-square a in Table 1). However, simple isotopisms show that the different choices for the free coefficient cannot produce new semifields. Thus the number of pairwise non-isotopic semifields is only due to the use of distinct field automorphisms and therefore polynomial in n.
- For $\mathbb{F},\mathcal{D},\mathcal{ZP},\mathcal{BH}/\mathcal{ZW}$ families, the simplicity of $(0,0,1,0)_q$ allows many isotopisms that stabilize this part, thus limiting the number of pairwise non-isotopic family members. Considering the action of $\mathbb{M}\times\mathrm{GL}(2,\mathbb{M})$ on biprojective functions which gives strong isotopy between the corresponding polarizations, we see that $f(x,y)=xy^q$ is stabilized by $(1/ab^q)f(L(x,y))=f(x,y)$ where $L:(x,y)\mapsto(ax,by)$ with $a,b\in\mathbb{M}^{\times}$. Other more complicated components usually admit smaller stabilizers. The stabilizer for the left part renders many coefficient choices for the right part isotopic to each other.
- Similarly the field automorphisms satisfying $q^2=1$ admit more isotopisms limiting again the number of pairwise non-isotopic family members. This is in

line with the uniprojective twisted field case. The pre-semifields defined by $X^qY + DXY^q$ are isotopic to the finite field if $q^2 = 1$, thus there is, up to isotopy, only one such semifield.

- If the field automorphisms q and r agree, i.e., $r \in \{q, \overline{q}\}$ as in Family $\mathcal{A}$, the left and right action of $\mathrm{GL}(2, \mathbb{M})$ on planar functions supplies many (strong) isotopisms limiting the number of pairwise non-isotopic semifields. If q and r do not agree, the left action is restricted to the scaling of both components (i.e., $\mathbb{M} \times \mathbb{M} \leq \mathrm{GL}(2, \mathbb{M})$).

Example 6.4 (The Zhou-Pott case). Consider the Family $\mathcal{ZP}$ which produces a quadratic number of pairwise non-isotopic commutative semifields:

$$F = ((0,0,1,0)_r, (1,0,0,a)_q), \quad a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2, \text{ for certain } q, r \in \mathrm{Gal}(\mathbb{M}/\mathbb{F}_p).$$

It is obvious that one of the non-zero field coefficients in each component can be assumed to be 1. It is then easy to show that $y \mapsto yb$ and re-scaling left part gives $((0,0,1,0)_r, (1,0,0,b^{q+1}a)_q)$. Since $\gcd(q+1, p^m-1) = 2$ by the parameter choice and Lemma 1.3, different choices of a are strongly isotopic as shown by Zhou and Pott [**148**].

Therefore, in order to get a large family, a rather natural *heuristic* is to try to find biprojective families with

- many nonzero coefficients running freely on large sets,
- field automorphisms that do not agree with each other,
- field automorphisms that are not *simple* (order larger than two),
- *complicated* components that do not admit large stabilizers.

5. Biprojective point-of-view puts known constructions in perspective

Inspecting Families $\mathcal{D}, \mathcal{BH}/\mathcal{ZW}, \mathcal{ZP}$ and the finite field $\mathbb{F}$, one notices the following remarkable similarity. These families are all of the form which we call **finite field type coefficients**,

$$((0,0,1,0)_q, (1,0,0,a)_r),$$

for a non-square $a \in \mathbb{M} \setminus \mathbb{M}^\times$ and

$$(q,r) = \begin{cases} (1,1) & \text{for finite fields,} \\ (q,1) & \text{for Family } \mathcal{D}, \\ (1,r) & \text{for Family } \mathcal{BH}/\mathcal{ZW}_{\text{odd}}, \\ (q,r) & \text{for Family } \mathcal{ZP}, \end{cases}$$

for judicious choices of q and r. For **Albert type coefficients**, i.e.,

$$((0,1,b,0)_q, (1,0,0,a)_r),$$

with select $a, b \in \mathbb{M}^\times$, we have

$$(q,r) = \begin{cases} (1,1) & \text{for finite fields,} \\ (q,q) & \text{for Family } \mathcal{A}, \\ (1,r) & \text{for Families } \mathcal{ZP} \text{ and } \mathcal{BH}/\mathcal{ZW}_{\text{odd}}, \\ (q,1) & \text{for Family } \mathcal{BH}/\mathcal{ZW}_{\text{even}}, \end{cases}$$

again for judicious choices of q and r and recalling that $(t, u, v, w)_1 = (t, 0, u + v, w)_1$. Therefore, within these two coefficient sets, the only case that has not been studied is the arbitrary (q, r) case in the more complicated coefficient set of Albert type.

- Family $\mathcal{S}$ (found in [**A**], explained in Chapter 8) is precisely this parameter combination for judicious choices of a and b, and q and r.
- Family $\mathcal{S}$ explains all pre-semifields with those parameters we were able to observe after a rather extensive computer experiment.
- We note that the field coefficient sets different from the above two cases of the finite field and Albert types, do not seem to give (new) commutative pre-semifields, again relying upon our experiments.

6. Systematic analysis is possible via the $\mathrm{PGL}(2, \mathbb{M})$ action on projective polynomials

Finding the parameter sets that give commutative semifields is rather difficult for biprojective semifields. However, using the orbits of the action $\mathbb{M}^\times \times \mathrm{PGL}(2, \mathbb{M})$ (see Chapter 3), one can simplify the analysis. If one finds the orbits of this action on q-projective polynomials ϕ_f, then for every r-biprojective polynomial g_1 we have an r-biprojective g_2 such that,

$$\phi_{f_1} \sim_{\mathfrak{M}} \phi_{f_2} \iff f_1 \sim_{\mathfrak{L}} f_2 \implies (f_1, g_1) \approx_{\mathfrak{L}} (f_2, g_2).$$

This means that $\mathbb{P}_1$ is strongly isotopic to $\mathbb{P}_2$ where $\mathbb{P}_1, \mathbb{P}_2$ are commutative pre-semifields whose multiplications are polarizations of the (q, r)-biprojective functions (f_1, g_1) and (f_2, g_2) respectively. Therefore, concentrating only on orbit representatives in the component f is enough for complete analysis.

This analysis is helpful in both practical (efficiency of computer experiments) and theoretical (classification and/or determining autotopism groups) aspects. We determine the orbits of this action in [**C**, Lemma 7] for some special cases. In a forthcoming work we do this in full generality. Moreover, using orbit representatives, we provide a classification of (q, q)-biprojective APN functions in [**E**] (see Chapter 13). Classifications of $(1, q)$- and (q, q)-biprojective commutative semifields are addressed in a forthcoming work.

7. New proof methods

When we fix one component to $(0, 0, 1, 0)_q$, we have a simple and well-known method to analyze the (q, r)-biprojective function dating back to Dickson (see Chapter 2). However, for more complicated components that involve more than one non-zero coefficient, there were no known methods available to us. In fact, an important part of the research that constitute this thesis was to find ways to solve this problem. These methods appear in [**A, B, C, D, E**] and are explained throughout the thesis.

CHAPTER 7

A survey on biprojective representations of known commutative semifields

In the following, we will show that many known commutative semifields of odd order fall into the (q, r)-biprojective setting where $\mathbb{M}$ denotes the finite field of order p^m, with p an odd prime, $q = p^k, r = p^l$ are automorphishms of $\mathbb{M}$ and $\overline{q}$ denotes the inverse automorphism, i.e., $x^{q\overline{q}} = x$ for $x \in \mathbb{M}$.

1. Dickson semifields $\mathcal{D}$

Dickson introduced [**43**] the commutative semifields $\mathbb{S} = (\mathbb{M} \times \mathbb{M}, +, \circ)$ with

$$(x, y) \circ (u, v) = (xu + ay^q v^q, xv + yu)$$

where $q = p^k$ with $0 < k < l$ and $a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$. Note that the isotopic multiplication

$$(x, y) * (u, v) = (xu + ayv, xv^{\overline{q}} + y^{\overline{q}}u)$$

is $(1, \overline{q})$-biprojective and isotopic to the polarization of the $(1, q)$-biprojective planar mapping

$$F_{\mathcal{D}} = ((1, 0, 0, a)_1, (0, 1, 0, 0)_q).$$

Different choices of $a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$ produce isotopic semifields and there are a total of $\lfloor \frac{n}{4} \rfloor$ non-isotopic Dickson semifields [**85**, p. 107].

2. Albert's twisted fields $\mathcal{A}$

Albert introduced [**7**] a family of commutative and noncommutative semifields. The commutative ones may be given as $\mathbb{S} = (\mathbb{F}, +, \circ)$ with

$$X \circ U = X^q U + U^q X,$$

where $q = p^k$ with $0 < k < n$ satisfying $n/\gcd(k, n)$ odd. When $\mathbb{F} = \mathbb{M}(\xi)$ with $[\mathbb{F} : \mathbb{M}] = 2$, one can write $X = x\xi + y$ with $x, y \in \mathbb{M}$. One can choose $\xi \in \mathbb{F} \setminus \mathbb{M}$ satisfying $\xi^2 = a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$, leading to the multiplication

$$\begin{aligned}(x\xi + y) \circ (u\xi + v) &= (x\xi + y)^q (u\xi + v) + (u\xi + v)^q (x\xi + y) \\ &= \xi^{q+1}(x^q u + u^q x) + \xi^q (x^q v + u^q y) + \xi(y^q u + v^q x) + (y^q v + v^q y) \\ &= a^{(q+1)/2}(x^q u + u^q x) + a^{(q-1)/2}\xi(x^q v + u^q y) + \xi(y^q u + v^q x) + (y^q v + v^q y).\end{aligned}$$

Identifying $\xi\mathbb{M} + \mathbb{M}$ with $\mathbb{M} \times \mathbb{M}$, we get

$$(x, y) \circ (u, v) = \Big(a^{(q-1)/2}(x^q v + u^q y) + (y^q u + v^q x), \quad a^{(q+1)/2}(x^q u + u^q x) + (y^q v + v^q y)\Big),$$

which is (q,q)-biprojective and isotopic to the polarization of the (q,q)-biprojective planar mapping

$$F_{\mathcal{A}} = ((0, a^{(q-1)/2}, 1, 0)_q, (a^{(q+1)/2}, 0, 0, 1)_q).$$

Different choices of $a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$ produce isotopic semifields and there are a total of $\lfloor \frac{\sigma(n)-1}{2} \rfloor$ non-isotopic commutative twisted fields [**85, 7**].

3. Zhou-Pott semifields $\mathcal{ZP}$

Zhou and Pott [**148**] gave a family of pre-semifields $S = (\mathbb{M} \times \mathbb{M}, +, \circ)$ given by

$$(x,y) \circ (u,v) = (x^q u + u^q x + a(y^q v + y v^q)^r, xv + yu),$$

where $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$, $q = p^k$ and $r = p^j$ with $0 \leq j, k \leq m$ where $m/\gcd(k,m)$ is odd. The isotopic multiplication

$$(x,y) * (u,v) = (x^q u + u^q x + a(y^q v + y v^q), x^r v + y u^r),$$

is (q,r)-biprojective and isotopic to the polarization of the (q,r)-biprojective planar mapping

$$F_{\mathcal{ZP}} = ((1,0,0,a)_q, (0,1,0,0)_r).$$

Different choices of $a \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$ produce isotopic semifields and there are a total of $\lfloor \frac{\sigma(n)}{2} \rfloor \cdot \lceil \frac{n}{4} \rceil$ non-isotopic $\mathcal{ZP}$ semifields [**148**].

4. Budaghyan-Helleseth/Zha-Wang semifields ($\mathcal{BH}, \mathcal{ZW}, \mathcal{LMPTB}$)

These semifields were found in [**21**] and independently in [**147**]. The commutative semifields given later in [**117**] and [**14**] were shown to be isotopic to the previous ones [**118**]. We note that Bierbrauer's construction in [**14**] gives also non-commutative semifields. We will use the definition from [**14**]. Let $S = (\mathbb{M} \times \mathbb{M}, +, \circ)$ be the pre-semifield given by

$$(x,y) \circ (u,v) = \begin{cases} (xv + yu, x^q u + x u^q + a(y^q v + y v^q)) & \text{if } m/\gcd(k,m) \text{ is odd,} \\ (xu + ayv, x^q v + y u^q + a^{(q-1)/2}(x v^q + y^q u)) & \text{if } m/\gcd(k,m) \text{ is even,} \end{cases}$$

where $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$ and $q = p^k$ with $0 < k < m$. The pre-semifield multiplication is $(1,q)$-biprojective. Similarly, the corresponding $(1,q)$-biprojective planar mapping whose polarization is isotopic to $\mathbb{S}$ is given by

$$F_{\mathcal{BH}/\mathcal{ZW}} = \begin{cases} ((0,0,1,0)_1, (1,0,0,a)_q) & \text{if } m/\gcd(k,m) \text{ is odd,} \\ ((1,0,0,a)_1, (0,1,a^{(q-1)/2},0)_q) & \text{if } m/\gcd(k,m) \text{ is even.} \end{cases}$$

The number of non-isotopic semifields in this family is $\lfloor \frac{n}{4} \rfloor$ which is proved in [**53**].

Remark 7.1 (Explanations and tables). The known infinite families of biprojective semifields and their planar representations are summarized in Tables 1. Families $\mathcal{A}, \mathcal{D}, \mathcal{BH}/\mathcal{ZW}$ reduce to $\mathbb{F}$ when $k \in \{0, m\}$. Family $\mathcal{ZP}$ reduces to $\mathcal{D}$ when $k = 0$, to $\mathcal{BH}/\mathcal{ZW}$ when $j = 0$, and to $\mathbb{F}$ when $j = k = 0$. Family $\mathcal{S}$ reduces to $\mathcal{ZP}$ when $a = 0$, and to $\mathcal{D}$ when $k \in \{0, l\}$. We excluded those cases in the Notes and also in the Counts columns of Table 1. Table 2 lists known commutative semifields that are not biprojective. We should say here that these commutative semifields are not *obviously* represented as biprojective semifields.

Family	**Planar Mapping**	**#$\mathbb{S}$**	**Notes**	$(\#\mathbb{N}_l, \#\mathbb{N}_m)$	**Count**	**Proved in**
$\mathbb{F}$	X^2	p^n		(p^n, p^n)	1	
	$[(0,1,0,0)_1, (1,0,0,a)_1]$		$a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2, n = 2m$			
$\mathcal{A}$	X^{q+1}	p^n	$q = p^k$, $0 < k < m$, $\gcd(k, n) = d$, n/d odd.	(p^d, p^d)	$\left\lfloor \frac{\sigma(n)-1}{2} \right\rfloor$	[**7**]
	$[(0, a^{s_1}, 1, 0)_q, (a^{s_2}, 0, 0, 1)_q]$		$a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2, n = 2m$ $s_1 = \frac{q-1}{2}, s_2 = \frac{q+1}{2}$			
$\mathcal{D}$	$[(1,0,0,a)_1, (0,1,0,0)_q]$	p^{2m}	$q = p^k$, $0 < k < m$, $\gcd(k, m) = d$, $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$.	(p^d, p^m)	$\lfloor \frac{n}{4} \rfloor$	[**43**]
$\mathcal{ZP}$	$[(1,0,0,a)_q, (0,1,0,0)_r]$	p^{2m}	$q = p^k, r = p^j$, $0 < j, k < m$, $\gcd(k, m) = d$, $\gcd(j, k, m) = d'$, m/d odd, $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$.	$(p^{d'}, p^d)$	$\left\lfloor \frac{\sigma(n)-1}{2} \right\rfloor \lfloor \frac{n}{4} \rfloor$	[**148**]
$\mathcal{BH}/\mathcal{ZW}$	$[(0,1,0,0)_1, (1,0,0,a)_q]$	p^{2m}	$q = p^k$, $0 < k < m$, $\gcd(k, m) = d$, m/d odd, $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$.	(p^d, p^{2d})	$\lfloor \frac{n}{4} \rfloor$	[**21, 147, 53**]
	$[(1,0,0,a)_1, (0,1,a^{s_1},0)_q]$		$q = p^k$, $0 < k < m$, $\gcd(k, m) = d$, m/d even, $a \in \mathbb{M} \setminus (\mathbb{M}^\times)^2, s_1 = \frac{q-1}{2}$.			
$\mathcal{S}$	$[(1,0,0,B)_q, (0,1,\frac{a}{B},0)_r]$	p^{4l}	$q = p^k, \quad r = p^{k+l}$, $0 < k < l, m = 2l$, $\gcd(k, m) = e, m/e$ odd, $a \in \mathbb{L}^\times, \quad B \in \mathbb{M} \setminus (\mathbb{M}^\times)^2$.	$(p^{e/2}, p^e)$	$\geq \left\lfloor \frac{\sigma(n)-1}{2} \right\rfloor \left\lceil \frac{p^l-1}{n} \right\rceil$	Theorem 8.2

TABLE 1. Known infinite families of biprojective commutative semifields of odd order p^n

Family	**Planar Mapping**	**#$\mathbb{S}$**	**Notes**	$(\#\mathbb{N}_l, \#\mathbb{N}_m)$	**Count**	**Proved in**
$\mathcal{ZKW}$	$X^{q+1} - a^{Q-1}X^{qQ+Q^2}$	p^{3s}	$Q = p^s, \quad q = p^t$, $d = \gcd(s,t), \quad s' = s/d, \quad t' = t/d$, s' odd, $\quad s' + t' \equiv 0 \pmod 3$, $\langle a \rangle = \mathbb{F}_{p^{3s}}^\times$.	(p^d, p^d) [**118**]	≥ 1	[**146**]
$\mathcal{B}_3$	$X^{q+1} - a^{Q-1}X^{qQ+Q^2}$	p^{3s}	$Q = p^s, q = p^t$, $d = \gcd(s,t), \quad s/d$ odd, $q \equiv Q \equiv 1 \pmod 3$, $\langle a \rangle = \mathbb{F}_{p^{3s}}^\times$.	(p^d, p^d) [**118**]	$\leq 9\sigma(s)$	[**13**]
$\mathcal{B}_4$	$X^{q+1} - a^{Q-1}X^{qQ+Q^3}$	p^{4s}	$Q = p^s, q = p^t$, $d = \gcd(2s,t), \quad 2s/d$ odd, $q \equiv Q \equiv 1 \pmod 4$, $\langle a \rangle = \mathbb{F}_{p^{4s}}^\times$.	$(p^{d/2}, p^d)$ [**118**]	$\leq 8\sigma(s)$	[**13**]
$\mathcal{CG}$	$(x^2 + ay^2 + a^3y^{18}, xy - ay^6)$	3^{2m}	$m \geq 3$, $a \in \mathbb{F}_{3^m}^\times \setminus (\mathbb{F}_{3^m}^\times)^2$	$(3, 3^m)$	1	[**36**]
$\mathcal{G}$	$(x^2 + y^{10}, xy - y^6)$	3^{2m}	$m \geq 3$ odd	$(3, 3)$	1	[**55**]
$\mathcal{CM}/\mathcal{DY}$	$X^{10} \pm X^6 - X$	3^m	$m \geq 5$ odd	$(3, 3)$	2	[**39, 47**]

TABLE 2. Known infinite families of (non-biprojective) commutative semifields of odd order p^n

When the order is square, there might be isotopic semifields that can be biprojective, but we are not aware of such isotopisms.

Remark 7.2 (Non-commutative biprojective semifields). Let us shortly explain non-commutative biprojective constructions.

- Let $q = p^k$ be an automorphism of $\mathbb{M}$ and $c, d \in \mathbb{M}$ such that
$$x^{q+1} + cx - d = 0$$
has no solutions $x \in \mathbb{M}$. The pre-semifields defined by
$$(x, y) * (u, v) = \begin{cases} (x^{q^2} v + yu^{q^2}, & y^q v + dx^q u + cyu^q), \\ (x^q v + yu^q, & y^q v + dxu^q + cyu^q), \\ (x^q v + yu^q, & yv^q + dx^q u + cyu^q), \\ (xv + yu, & y^q v + d^q x^q u + cy^q u), \end{cases}$$
are called Knuth semifields of Type II.i–iv [**101**, Eq. (7.16), p. 215]. We note that Knuth formulated these multiplications in a non-biprojective way which is then repeated in surveys in the same way (see for instance [**86, 37**]). We give here $(q^2, q), (q, q), (q, q)$ and $(1, q)$-biprojective representations of these non-commutative semifields. Knuth also gives a non-biprojective and non-commutative generalization of Dickson semifields that are called Knuth Type I which we do not cover here [**101**, Eq. (7.15), p. 215].
- Bierbrauer extended Knuth Type II.iv semifields [**14**] in odd characteristic (and in univariate notation). Later the $(1, q)$-biprojective representations were given in [**11, 15**] in even and odd characteristics. The construction requires a q-projective polynomial
$$x^{q+1} - bx^q + cx - d \in \mathbb{M}[x],$$
which has no $\mathbb{M}$-zeroes. Then the Bierbrauer pre-semifields are defined as
$$\begin{aligned}(x, y) * (u, v) = (xv + yu, \quad & (xu^q - \alpha x^q u) + b(yu^q + \alpha x^q v) \\ & c(xv^q + \alpha y^q u) + d(yv^q - \alpha y^q v)),\end{aligned}$$
where $\alpha \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^{q-1}$. This family includes commutative semifields that are isotopic to the $\mathcal{BH}/\mathcal{ZW}$ family.
- Taniguchi [**136**] extended Knuth Type II.i pre-semifields in the manner Bierbrauer extended Knuth Type II.iv family. We again give the (q, q^2)-biprojective version that is used in [**K**]. As in Knuth's construction, let $q = p^k$ be an automorphism of $\mathbb{M}$ and $c, d \in \mathbb{M}$ such that
$$x^{q+1} + cx - d = 0$$
has no solutions $x \in \mathbb{M}$ and $\alpha \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^{q-1}$. The Taniguchi pre-semifields are defined by
$$(x, y) * (u, v) = (xv^{q^2} + y^{q^2} u, \quad x^q u - \alpha^{q^2} xu^q - c(xv^q + \alpha^q y^q u) + d(y^q v - \alpha yv^q)).$$

CHAPTER 8

The number of non-isotopic commutative semifields is exponential [**A**]

Recall that Albert's commutative twisted fields over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ admit the planar functions

$$F_{\mathcal{A}} = ((1,0,0,\alpha)_q, (0,1,\beta,0)_q),$$

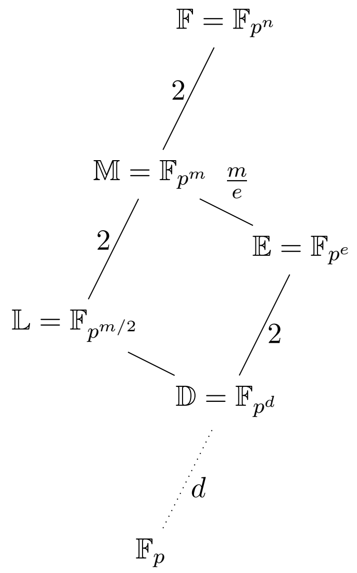
for $\alpha = a^{(q+1)/2}, \beta = a^{(q-1)/2}$ with suitable $a \in \mathbb{F}_{p^m}$ and $q = p^k$. Since our aim is, as explained in previous chapters, to generalize Albert's twisted fields in the sense that families $\mathcal{D}, \mathcal{ZP}, \mathcal{BH}/\mathcal{ZW}/\mathcal{LMPTB}$ generalize the finite field, we look for possible planar functions of the form

$$F = ((1,0,0,\gamma)_q, (0,1,\delta,0)_r),$$

for suitable γ, δ, q, r. The first main result of [**A**] is to give such a planar function family. For the above parameters, the family we present covers all the planar functions we encountered during an extensive search.

1. The family

The following diagram and its annotations describe our setting.


$\mathbb{F} = \mathbb{F}_{p^n}$
2
$\mathbb{M} = \mathbb{F}_{p^m}$
$\frac{m}{e}$
2
$\mathbb{E} = \mathbb{F}_{p^e}$
$\mathbb{L} = \mathbb{F}_{p^{m/2}}$
2
$\mathbb{D} = \mathbb{F}_{p^d}$
d
$\mathbb{F}_p$

Notation 8.1.

- p is an odd prime.
- $n = 2m$, m is even.
- $Q = p^{m/2}, \quad Q^2 = p^m$.
- $q = p^k, \quad r = p^{k+m/2} = Qq$ with $1 \le k \le m-1$.
- $e = \gcd(k, m)$ with m/e odd.
- $d = \gcd(k + m/2, m)$.
- $e = 2d$.
- $(\mathbb{M}^\times)^2$ — the subgroup of non-zero squares in $\mathbb{M}^\times$.
- $\mathbb{L}^\times = (\mathbb{M}^\times)^{Q+1} \le (\mathbb{M}^\times)^2 \le \mathbb{M}^\times$.
- $(\mathbb{M}^\times)^{Q-1} \le (\mathbb{M}^\times)^2 \le \mathbb{M}^\times$ — the subgroup of $(Q+1)^{\text{st}}$ roots of unity in $\mathbb{M}^\times$.
- $\mathbb{E} = \mathbb{F}_q \cap \mathbb{M} = \mathbb{F}_{q^2} \cap \mathbb{M} = \mathbb{F}_{r^2} \cap \mathbb{M}$.
- $\mathbb{D} = \mathbb{F}_r \cap \mathbb{M}$.

Now we present the family of planar mappings [**A**, Theorem 4.4].

Theorem 8.2. *Let $a \in \mathbb{L}^\times$ and $B \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$ and let*

$$F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$$

be defined as

$$F : (x, y) \mapsto F(x, y) = ((1, 0, 0, B)_q, (0, 1, a/B, 0)_r).$$

Then F is planar.

The proof of this theorem is rather involved. Note that both parts of the biprojective function F are complicated as we explained in Chapter 4. The method of Dickson which works when one part is $(0, 0, 1, 0)_q$ is not available here. The proof eventually works by building up contradictions involving non-squares (see [**A**, Section 4] for details).

2. A method to determine isotopy of biprojective pre-semifields

We denote the set of all autotopisms of a pre-semifield $\mathbb{P}$ by $\mathrm{Aut}(\mathbb{P})$. It is easy to check that $\mathrm{Aut}(\mathbb{P})$ is a group under component-wise composition, i.e.,

$$(N_1, L_1, M_1)(N_2, L_2, M_2) = (N_1N_2, L_1L_2, M_1M_2).$$

We view $\mathrm{Aut}(\mathbb{P})$ as a subgroup of $\mathrm{GL}(\mathbb{F})^3 \cong \mathrm{GL}(\mathbb{M} \times \mathbb{M})^3 \cong \mathrm{GL}(n, \mathbb{F}_p)^3$. Our approach is based on the following simple and well-known result.

Lemma 8.3. *Let $\mathbb{P}_1 = (\mathbb{F}_p^n, +, *_1)$ and $\mathbb{P}_2 = (\mathbb{F}_p^n, +, *_2)$ be two isotopic pre-semifields via the isotopism $\delta \in \mathrm{GL}(\mathbb{F})^3$. Then $\delta^{-1} \mathrm{Aut}(\mathbb{P}_2)\delta = \mathrm{Aut}(\mathbb{P}_1)$.*

We start by identifying a subgroup of the autotopism group of any (q, r)-biprojective pre-semifield. See [**A**, Theorems 5.2 and 5.3] for Sylow's and Zsigmondy's theorems.

- Define the cyclic group

  $$Z^{(q,r)} = \{\gamma_a : a \in \mathbb{M}^\times\},$$

  of order $p^m - 1$, where

  $$\gamma_a = (\mathrm{diag}(m_{a^{q+1}}, m_{a^{r+1}}), \mathrm{diag}(m_a, m_a), \mathrm{diag}(m_a, m_a)),$$

  where m_a denotes multiplication with the finite field element $a \in \mathbb{M}^\times$.
- Let p' be a p-primitive divisor of $p^m - 1$. Such a prime p' always exists if $m > 2$ and $(p, m) \neq (2, 6)$ by Zsigmondy's theorem. In our case, we have $p > 2$. We will also stipulate $m > 2$. Note that $p' \neq 2$ since $p' \nmid p - 1$ by the definition of p-primitivity.
- Let R be the unique Sylow p'-subgroup of $\mathbb{M}^\times$. Define

  $$Z_R^{(q,r)} = \{\gamma_a \colon a \in R\},$$

  which is the unique Sylow p'-subgroup of $Z^{(q,r)}$ with $|R|$ elements.
- Define

  $$S = \{\mathrm{diag}(m_a, m_a) \colon a \in \mathbb{M}^\times\},$$

  and

  $$S_R = \{\mathrm{diag}(m_a, m_a) \colon a \in R\}.$$

Note that S_R (resp. S) corresponds to the second and third components of $Z_R^{(q,r)}$ (resp. $Z^{(q,r)}$) and is independent of q and r.

The following lemma is straightforward, but very important.

LEMMA 8.4. *Let $\mathbb{P}$ be any (q,r)-biprojective pre-semifield. Then*

$$Z_R^{(q,r)} \leq Z^{(q,r)} \leq \mathrm{Aut}(\mathbb{P}).$$

The central idea of the technique we develop is to identify large abelian Sylow subgroups in the autotopism group of biprojective semifields. We then use tools from group theory to obtain strong constraints on when the autotopism groups of two pre-semifields are conjugate. This approach is inspired by a similar technique for inequivalences of power functions on finite fields developed by Dempwolff [**42**] and Yoshiara [**145**].

METHOD 8.5. The following is a high-level explanation of our method explaining [**A**, Theorem 5.10].

(i) Let $\mathbb{P}_1 = (\mathbb{M}\times\mathbb{M},+,*_1)$ and $\mathbb{P}_2 = (\mathbb{M}\times\mathbb{M},+,*_2)$ be (q_1,r_1)- and (q_2,r_2)-biprojective pre-semifields, respectively, such that $q_1 \notin \{r_1,\overline{r_1}\}$, $1 \notin \{q_1,r_1\}$ and $Q \notin \{q_1,r_1\}$, where $q_i = p^{k_i}$ and $r_i = p^{l_i}$ for $i \in \{1,2\}$.

(ii) Let G_1, G_2 be defined as

$$\begin{aligned} G_1 &= Z_R^{(q_1,r_1)} \leq \mathrm{Aut}(\mathbb{P}_1), \text{ and}\\ G_2 &= Z_R^{(q_2,r_2)} \leq \mathrm{Aut}(\mathbb{P}_2). \end{aligned}$$

We first prove that G_1 is a Sylow p'-subgroup of $\mathrm{Aut}(\mathbb{P}_1)$ under Condition (C).

(iii) Let $\delta = (N_\delta, L_\delta, M_\delta) \in \mathrm{GL}(\mathbb{F})^3$ be an isotopism between $\mathbb{P}_1$ and $\mathbb{P}_2$, i.e.,

$$N_\delta(x *_1 y) = L_\delta(x) *_2 M_\delta(y).$$

Then $\delta^{-1}\,\mathrm{Aut}(\mathbb{P}_2)\delta = \mathrm{Aut}(\mathbb{P}_1)$ and, in particular, $\delta^{-1}G_2\delta \leq \mathrm{Aut}(\mathbb{P}_1)$.

(iv) Then, $\delta^{-1}G_2\delta$ is a Sylow-p' subgroup of $\mathrm{Aut}(\mathbb{P}_1)$ by Sylow Theorem (i) and for some $\lambda \in \mathrm{Aut}(\mathbb{P}_1)$, we have

$$(\delta\lambda)^{-1}G_2(\delta\lambda) = G_1$$

by Sylow Theorem (iii).

(v) Set $\gamma = (N,L,M) \in \mathrm{GL}(\mathbb{F})^3$ as $\gamma = \delta\lambda$. Since $\lambda : \mathbb{P}_1 \mapsto \mathbb{P}_1$ and $\delta : \mathbb{P}_1 \mapsto \mathbb{P}_2$, we have $\gamma : \mathbb{P}_1 \mapsto \mathbb{P}_2$ is an isotopism between $\mathbb{P}_1$ and $\mathbb{P}_2$.

(vi) The conjugacy $\gamma^{-1}G_2\gamma = G_1$ implies $L, M \in \Gamma\mathrm{L}(2,\mathbb{M})$ using [**A**, Lemma 5.7] which states that $N_{\mathrm{GL}(\mathbb{F})}(S_R) = \Gamma\mathrm{L}(2,\mathbb{M})$ where $N_{\mathrm{GL}(\mathbb{F})}(S_R)$ is the normalizer of S_R in $\mathrm{GL}(\mathbb{F})$.

(vii) Now an analysis on the degrees appearing in the isotopy equation induced by γ implies that

(a) the defining Galois automorphisms of $\mathbb{P}_1$ and $\mathbb{P}_2$ should agree. That is to say,

(i) $k_1 \equiv \pm k_2 \pmod m$ and $l_1 \equiv \pm l_2 \pmod m$, or,

(ii) $k_1 \equiv \pm l_2 \pmod m$ and $l_1 \equiv \pm k_2 \pmod m$; and,

(b) we have $\gamma = (N, L, M) \in \Gamma\mathrm{L}(2, \mathbb{M})^3$ with further restrictions on N, L, M listed in the statement of [**A**, Theorem 5.10]. That is to say, for every isotopism δ between $\mathbb{P}_1$ and $\mathbb{P}_2$, there is an isotopism $\gamma \in \Gamma\mathrm{L}(2, \mathbb{M})^3$ between $\mathbb{P}_1$ and $\mathbb{P}_2$.

We explain the steps in a series of remarks.

Remark 8.6 (Condition (C)). For a (q, r)-biprojective pre-semifield $\mathbb{P}$, denote by

$$C_{\mathbb{P}} = C_{\mathrm{Aut}(\mathbb{P})}(Z_R^{(q,r)}),$$

the centralizer of $Z_R^{(q,r)}$ in $\mathrm{Aut}(\mathbb{P})$.

- By Condition (C) we mean that "$C_{\mathbb{P}}$ **contains** $Z^{(q,r)}$ **as an index** I **subgroup such that** p' **does not divide** I".
- We prove in [**A**, Lemma 5.8], under Condition (C), $Z_R^{(q,r)}$ is a Sylow p'-subgroup of $\mathrm{Aut}(\mathbb{P})$, handling Part (ii).
- In [**A**, Lemma 5.7], we prove

$$N_{\mathrm{GL}(\mathbb{F})}(Z_R^{(q,r)}) = \Gamma\mathrm{L}(2, \mathbb{M}),$$
$$C_{\mathrm{GL}(\mathbb{F})}(Z_R^{(q,r)}) = \mathrm{GL}(2, \mathbb{M}),$$

which is instrumental in proving that Condition (C) holds for specific biprojective semifields as well as in Method 8.5 (vii) (b). Observe that the conjugacy condition $\gamma^{-1} G_2 \gamma = G_1$ on the second and third components of $Z_R^{(q,r)}$ is the same as the normalizer condition on S_R by definition which is essential for Part (vi).

Remark 8.7. The crux of the method is that the problem of determining conjugacy (in $\mathrm{GL}(\mathbb{F})$) of two groups ($\mathrm{Aut}(\mathbb{P}_1)$ and $\mathrm{Aut}(\mathbb{P}_2)$ that we do not know) is converted to the problem of determining conjugacy (in $\mathrm{Aut}(\mathbb{P}_1)$) of two *nice* subgroups (G_1, G_2 that we do know) whose centralizers and normalizers (in $\mathrm{GL}(\mathbb{F})$) are also known.

Remark 8.8. Part (vii) is the analogue of the theorem of Albert that states (under certain conditions) that every isotopism δ between two twisted fields (i.e., uniprojective case) with defining field automorphisms q and q' respectively, has to satisfy:

- $\delta \in \Gamma\mathrm{L}(1, \mathbb{F})^3$,
- q and q' should agree, and
- L, M, N, the component linear maps of δ, satisfy further restrictions.

We promised a generalization for the biprojective case. The method above establishes that under certain conditions. We prove that if there is an isotopism δ between two biprojective semifields with defining field automorphisms (q, r) and (q', r') respectively, then there is an isotopism γ between these semifields with

- $\gamma \in \Gamma\mathrm{L}(2, \mathbb{M})^3$,
- (q, r) and (q', r') should *agree*, and
- L, M, N, the component linear maps of γ, satisfy further restrictions.

Remark 8.9. In Part (i), we assume certain conditions on (q_i, r_i), for instance, their order should be larger than 2. This assumption is, again, similar to the uniprojective Albert case. Recall that the twisted fields $X^qY + DXY^q$ are isotopic to finite fields when $q^2 = 1$ and allow isotopisms outside $\Gamma\mathrm{L}(1, \mathbb{F})^3$. This is very similar to our case (see [**A**, Remark 5.11 (i)]) where the excluded cases allow different types of isotopisms. If required, one can prove a similar result for the excluded cases, however, for our purpose, this was not necessary and left out for the sake of simplicity. We also show [**A**, Remark 8.3] that these simpler cases for (q, r) leads to isotopisms between Family $\mathcal{S}$ and other biprojective families.

Next, we specialize to Family $\mathcal{S}$.

3. Isotopisms within the Family $\mathcal{S}$

Recall that, to prove G_1 is Sylow-p' subgroup of $\mathrm{Aut}(\mathbb{P}_1)$, it is enough to prove Condition (C) for $\mathbb{P}_1$.

Method 8.10. The following is a high-level explanation of our method showing that the number of non-isotopic semifields within the Family $\mathcal{S}$ is exponential in n.

(i) First we prove [**A**, Lemma 6.1] that if $\mathbb{P}$ is a (q, r)-biprojective pre-semifield in the Family $\mathcal{S}$, then,

$$|C_{\mathbb{P}}| = (p^m - 1)(p^{\gcd(k,m)} - 1), \text{ or}$$
$$|C_{\mathbb{P}}| = 2(p^m - 1)(p^{\gcd(k,m)} - 1).$$

In particular, Condition (C) is always satisfied.

(ii) Now, using Method 8.5 (vii) we show strong isotopy conditions within the Family $\mathcal{S}$ ([**A**, Theorem 6.2]). The notation $\mathbb{P}_{q,B,a}$ denotes a pre-semifield in Family $\mathcal{S}$ with the subscripted variables employed in the statement Theorem 8.2.

(a) $\mathbb{P}_{q,B,a}$ and $\mathbb{P}_{q',B',a'}$ are isotopic if and only if they are strongly isotopic.

(b) $\mathbb{P}_{q,B,a}$ is isotopic to $\mathbb{P}_{\overline{q},B,a'}$ for $a' = B^{Q+1}/a$ and arbitrary q.

(c) $\mathbb{P}_{q,B,a}$ is isotopic to $\mathbb{P}_{q,B',a'}$ for arbitrary q, B, B', a and a suitable choice for a'.

(d) If $\mathbb{P}_{q,B,a}$ is isotopic to $\mathbb{P}_{q,B,a'}$, then it is also isotopic to $\mathbb{P}_{q,B,-a'}$.

(e) There are at most $2m = n$ different a' such that $\mathbb{P}_{q,B,a}$ is isotopic to $\mathbb{P}_{q,B,a'}$.

(f) No other isotopisms exist.

(iii) Finally, this immediately gives the following bounds. Let $N_{\mathcal{S}}(p, n)$ be the number of pairwise non-isotopic pre-semifields in Family $\mathcal{S}$ on $\mathbb{F}_p^n$. Then

$$\frac{\sigma(n) - 1}{2} \cdot \frac{p^{n/4} - 1}{n} \le N_{\mathcal{S}}(p, n) \le \frac{\sigma(n) - 1}{2}\left(p^{n/4} - 1\right).$$

Several remarks on the details of the method follow.

Remark 8.11 (Part (i)). By [**A**, Lemma 5.7], the second and third component L, M of an isotopism $\delta = (N, L, M) \in C_{\mathbb{P}}$ has to be in $\mathrm{GL}(2, \mathbb{M})$. Now, the isotopy equation imposes, after rather lengthy calculations, a certain form on N and in turn on δ. Then the cardinality of the centralizer can easily be counted.

Remark 8.12 (Part (ii)). The proof of this part is similar to that of Part (i). The conditions listed in [**A**, Theorem 5.10] imposes strict restrictions on the shape of the isotopism $\gamma = (N, L, M)$ between two pre-semifields in the Family $\mathcal{S}$. These restrictions lead, again after lengthy calculations, to the isotopy conditions listed above.

Remark 8.13 (Part(iii)). The proof is straightforward after Part (ii) and resembles the simple method for Albert's twisted fields we explained in Chapter 3. There are $\sigma(n) - 1$ admissible values for q, and only $q, \overline{q}$ yield isotopic pre-semifields. Then there are $p^{n/4} - 1$ admissible values for a, with at most n of them yielding isotopic pre-semifields.

In particular, $\mathcal{S}$ is the first known family of commutative (pre-)semifields that yields exponentially many non-isotopic (pre-)semifields. Since non-isotopic pre-semifields lead to inequivalent planar mappings (see Theorem 2.2), this also shows that the number of inequivalent planar mappings grows exponentially in n.

Corollary 8.14. *The number of non-isotopic commutative semifields of order p^n and the number of inequivalent planar DO mappings of $\mathbb{F}_{p^n}$ are exponential in n for a fixed odd prime p and n divisible by 4.*

4. Nuclei and comparison to other semifields

The nuclear parameters of the family can be computed using similar methods.

Theorem 8.15. *The left, middle and right nuclei $\mathbb{N}_l(\mathbb{S}), \mathbb{N}_m(\mathbb{S}), \mathbb{N}_r(\mathbb{S})$ satisfy $\mathbb{N}_l(\mathbb{S}) = \mathbb{N}_r(\mathbb{S}) \cong \mathbb{D}$ and $\mathbb{N}_m(\mathbb{S}) \cong \mathbb{E}$.*

Using the nuclei and the biprojective method we can show that Family $\mathcal{S}$ is new.

Theorem 8.16. *Let $\mathbb{P}_{q,B,a} = (\mathbb{M} \times \mathbb{M}, +, *)$ be a pre-semifield in the Family $\mathcal{S}$. $\mathbb{P}_{q,B,a}$ is not isotopic to any other known commutative semifield, except possibly semifields from Family $\mathcal{B}_4$. Family $\mathcal{S}$ yields new examples of commutative semifields.*

Although the parameters p, m, q for the pre-semifields from Family $\mathcal{S}$ are more general than that of Family $\mathcal{B}_4$, for suitable choices of p, m, q the parameters may coincide. The next proposition shows that even in that case Family $\mathcal{S}$ contains new semifields thanks to its exponential count. More precisely, we show that the number of non-isotopic semifields from Families $\mathcal{B}_3$ and $\mathcal{B}_4$ of order p^{3s} and p^{4s}, respectively, is linear in s.

Proposition 8.17. *The number of non-isotopic pre-semifields in Family $\mathcal{B}_3$ (and $\mathcal{B}_4$ resp.) of order p^{3s} (and p^{4s} resp.) is at most $9\sigma(s)$ (and $8\sigma(s)$ resp.).*

Remark 8.18. For the Family $\mathcal{ZKW}$ we are not aware of any result on the exact value or a bound on the number of non-isotopic pre-semifields.

5. Counting the number of pairwise non-isotopic Taniguchi semifields

We apply the method explained in this chapter to Taniguchi family (see Remark 7.2). Although it has some peculiarities which we address throughout the paper [**K**], the overall scheme is almost identical. We prove (recalling that $q = p^k$):

THEOREM 8.19. *Let $N_T(p,k,m,a)$ be the number of non-isotopic Taniguchi semifields $T(q,\alpha,a,b)$ over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with $k \neq m/2$. Set $d = \gcd(k,m)$ and $l = m/d$. Then*

$$(p^d - 2) \cdot N_0(p,m)/m \leq N_T(p,k,m,1) \leq (p^d - 2) \cdot N_0(p,m),$$

where $N_0(p,m)$ is determined in Theorem 1.9. Further,

$$(p^d - 2) \cdot p^d/m \leq N_T(p,k,m,0) \leq (p^d - 2) \cdot p^d$$

if l is even,

$$N_T(p,k,m,0) = p^d - 2$$

if p, l are odd and $N_T(p,k,m,0) = 0$ if p is even and l is odd. The total number of non-isotopic Taniguchi semifields with $k \neq m/2$ is

$$N_T(p,m) = \sum_{k=1}^{\lfloor \frac{m}{2} \rfloor} \left(N_T(p,k,m,0) + N_T(p,k,m,1)\right).$$

For $m = 3k$ we get the best number.

COROLLARY 8.20. *The number of pairwise non-isotopic Taniguchi semifields of order p^{2m} is $\Theta(p^{4m/3})$.*

CHAPTER 9

Even characteristic: Almost perfect nonlinear functions

In this chapter we address specifics of APN functions and mostly assume that the characteristic is two (see Chapter 3).

Family	**Monomial**	**Conditions**	**Proved in**
Gold	X^{2^i+1}	$\gcd(i, n) = 1$	[**57**]
Kasami	$X^{2^{2i}-2^i+1}$	$\gcd(i, n) = 1$	[**90**]
Welch	X^{2^t+3}	$n = 2t + 1$	[**50**]
Niho	$X^{2^t+2^{\frac{t}{2}}-1}$, t even $X^{2^t+2^{\frac{3t+1}{2}}-1}$, t odd	$n = 2t + 1$	[**49**]
Inverse	$X^{2^{2t+1}-2}$	$n = 2t + 1$	[**122**]
Dobbertin	$X^{2^{4t}+2^{3t}+2^{2t}+2^t-1}$	$n = 5t$	[**48**]

Table 1. Known infinite families (up to Galois automorphisms and inversion) of APN monomials on $\mathbb{F}_{2^n}$

Known monomial APN families are listed in Table 1 (in the univariate notation). The reader is referred to [**128**, Section 5.3] for a list of known families of APN functions that are not necessarily monomials. A few remarks follow.

- The only quadratic functions in Table 1 are the Gold functions. Note that these functions are the binary analogues of the (odd characteristic) Albert planar functions on $\mathbb{F}_{p^n}$ mapping $X \mapsto X^{p^k+1}$ with $n/\gcd(k, n)$ odd. The requirement $\gcd(i, n) = 1$ is necessary for the Gold functions to be APN. It can be shown that the derivatives of Gold functions in general are $2^{\gcd(i,n)}$-to-1 [**57**].
- In contrast, all known infinite APN families that are not monomials are quadratic.

An important difference between odd and even characteristic concerns the notion of equivalence. We let $\mathbb{F} = \mathbb{F}_{p^n}$ in the following section.

1. Equivalences of vectorial functions

Let $F, G : \mathbb{F} \to \mathbb{F}$ be vectorial functions. The widest known notion of equivalence that keeps the PN/APN property invariant is called the **CCZ-equivalence** [**31**]. Define the **graph** of the function F by

$$\Gamma_F = \{(x, F(x)) \ : \ x \in \mathbb{F}\}.$$

Then F is said to be CCZ-equivalent to G if there exist $\mathbb{F}_p$-linear endomorphisms A, B, C, D of $\mathbb{F}$ such that $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is full rank, $u, v \in \mathbb{F}$ and a permutation $\pi : \mathbb{F} \to \mathbb{F}$ such that

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x \\ F(x) \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \pi(x) \\ G(\pi(x)) \end{pmatrix}, \tag{2}$$

for all $x \in \mathbb{F}$. In that case we write $F \approx_{\mathsf{CCZ}} G$. A narrower notion of equivalence that also keeps the algebraic degree of F invariant is called the **extended affine (EA) equivalence**. We write $F \approx_{\mathsf{EA}} G$ if for all $x \in \mathbb{F}$, we have

$$A_1 \circ F \circ A_2(x) + A_3(x) = G(x),$$

for affine maps $A_1, A_2, A_3 : \mathbb{F} \to \mathbb{F}$ with A_1, A_2 bijective. It can be shown that EA-equivalence is a special case of CCZ-equivalence where one sets $B = 0$. If A_1, A_2, A_3 are linear then we talk about **extended linear (EL) equivalence** (denoted by $F \approx_{\mathsf{EL}} G$). We can restrict the equivalence even more if, for instance, we want to keep the property of being a permutation invariant. The functions F and G are said to be **linearly equivalent** if

$$L_1 \circ F \circ L_2 = G,$$

for $L_1, L_2 \in \mathrm{GL}(\mathbb{F})$. Note that this is equivalent to setting $B = C = 0$ and $u = v = 0$ in (2) (if L_1, L_2 are affine, then they are called **affinely equivalent**). We denote this equivalence by $F \approx_{\mathrm{GL}(\mathbb{F})} G$.

REMARK 9.1. (i) An important theorem for quadratic APN functions is that for two quadratic APN functions F, G, we have, by a result of Yoshiara [**144**],

$$F \approx_{\mathsf{EA}} G \iff F \approx_{\mathsf{CCZ}} G.$$

For quadratic APN functions one can be more specific (see for instance [**92**, Proposition 2.2]):

$$F \approx_{\mathsf{EL}} G \iff F \approx_{\mathsf{CCZ}} G.$$

(ii) The CCZ-equivalence is interesting for APN functions but not for PN functions. As shown in [**105, 21**], for two PN functions F, G, we have,

$$F \approx_{\mathsf{EA}} G \iff F \approx_{\mathsf{CCZ}} G.$$

(iii) The CCZ-equivalence does not necessarily keep the degree invariant. For an invertible map F we have $F \approx_{\mathsf{CCZ}} F^{-1}$ via an *anti-diagonal* matrix in (2).

(iv) The CCZ-equivalence is induced by the natural left action of $\mathrm{AGL}(\mathbb{F} \times \mathbb{F})$ on the graph of F. All the others we describe here are equivalences induced by subgroup actions of $\mathrm{AGL}(\mathbb{F} \times \mathbb{F})$.

(v) We use even narrower types of equivalences (see Chapter 3) when addressing biprojective functions.

2. Biprojective APN functions

Note that the explanations we gave in previous chapters for biprojective planar functions and commutative semifields analogously hold for biprojective APN functions after some suitable and minor modifications. We will, however, give a brief state of the art on biprojective APN functions before the constructions of the current thesis appeared. For the APN functions, the initial work on bivariate functions was by Carlet [**27**] who found the first biprojective APN family, and then Zhou and Pott [**148**] introduced another family of biprojective APN functions (an analogue of their commutative semifields family) that contains a quadratic number of inequivalent members. Carlet then introduced [**28**] a method to find bivariate (but not necessarily biprojective) APN functions from his previous biprojective family (revisited in [**23**]). Further work on biprojective APN functions includes the family of Taniguchi [**136**]. Further work that does not involve constructions of bivariate functions but studies their important properties include [**9, 93, 92, 102, 91**].

We now give a survey on the known biprojective APN functions.

3. A survey on biprojective representations of known APN functions

We will now show that many known infinite families of APN functions

$$F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$$

where $\mathbb{M} = \mathbb{F}_{2^m}$ are (q, r)-biprojective. To the best of our knowledge these are the only known APN families that can be represented as biprojective functions.

- It is clear that the Gold functions $X \mapsto X^{2^i+1}$ can be written as (q, q)-biprojective functions, as

  $$(x + \beta y)^{2^i+1} = x^{2^i+1} + \beta(x^{2^i} y) + \beta^{2^i}(xy^{2^i}) + \beta^{2^i+1} y^{2^i+1}$$

  shows. When m is odd, we can use $\beta = \omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$. In that case

  $$(\mathcal{G}) \quad F(x, y) = ((1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^i}).$$

- When $i = 0$ (or $j = 0$), i.e., $q = 2^0 = 1$ and $r = 2^j$ with $j > 0$, then the resulting biprojective function can be written up to equivalence

  $$(\mathcal{C}) \quad F(x, y) = (xy, (a, b, c, d)_r),$$

  which is the family $\mathcal{C}$ introduced by Carlet [**27**]. Indeed, Carlet showed that F is APN if and only if $a \neq 0$ and $g(x, 1) \neq 0$ for any $x \in \mathbb{M}$.

- Zhou and Pott found the following APN family [**148**] which also falls into the scheme of (q, r)-biprojective functions. The functions

  $$(\mathcal{ZP}) \quad F(x, y) = ((1, 0, 0, d)_{2^i}, (0, 0, 1, 0)_{2^j}), \quad d \in \mathbb{M}^\times,$$

  are APN if and only if $\gcd(i, m) = 1$, m is even and $d \neq a^{2^i+1}(b^{2^i} + b)^{1-2^j}$ for any $a, b \in \mathbb{M}$.

- In [**136**], Taniguchi found the following APN family

  $$(\mathcal{T}) \quad F(x, y) = ((1, 0, c, d)_{2^i}, (0, 0, 1, 0)_{2^{2i}}), \quad c, d \in \mathbb{M}^\times,$$

  where $\gcd(i, m) = 1$, $f(x, 1) \neq 0$ for any $x \in \mathbb{M}$. If $c = 0$ and m is even, then the corresponding function belongs to the Zhou-Pott family [**136**].

Remark 9.2. Although not an infinite family, the κ_1-function (which is CCZ-equivalent to the κ-function whose representation is slightly more complicated) can be represented as a $(2,2)$-biprojective function:

$$\kappa_1(x,y) = ((b,1,0,b+1)_2, (0,b,b,b+1)_2),$$

where b is a root of x^3+x+1. We will see in the next chapter why this function is important.

Remark 9.3. Observe that (apart from the uniprojective Gold functions) all known biprojective APN functions have one part equivalent to $(0,0,1,0)_q$ (see Chapter 4 for the analogy to the commutative semifields case). This is also true for the κ-function (see [**E**, Remark V.3]). Recall that one aim of our thesis is to present techniques for functions with generic components (which we will do in the forthcoming chapters).

Family	**Function**	**Notes**	**Count**	**Proved in**
$\mathcal{G}$	X^{q+1}	$q=2^k$, $\gcd(k,m)=1$	$\frac{\varphi(2m)}{2}$	[**57**]
	$((0,1,1,0)_q,(1,0,1,1)_q)$	m odd.		
	$[(1,0,b,a)_q,(0,1,1,b+1)_q)$	m even, $\mathrm{tr}_{\mathbb{M}/\mathbb{F}_2}(a)=1$, $b=\sum_{i=0}^{k-1} a^{2^i}$.		
$\mathcal{C}$	$(xy,(1,b,c,d)_q)$	$q=2^k$, $0<k<m$, $\gcd(k,m)=1$, $x^{q+1}+bx^q+cx+d\neq 0$ for $x\in\mathbb{M}$.	$\frac{\varphi(m)}{2}$ [**C**, Thm. 4, 5]	[**27**]
$\mathcal{T}$	$((1,0,1,d)_q,(0,0,1,0)_{q^2})$	$q=2^k$, $0<k<m$, $\gcd(k,m)=1$, $x^{q+1}+x+d\neq 0$ for $x\in\mathbb{M}$.	$\geq \frac{\varphi(m)}{2}\lceil\frac{2^m+1}{3m}\rceil$ [**92**]	[**136**]
$\mathcal{ZP}$	$((1,0,0,d)_q,(0,0,1,0)_r)$	$q=2^k, r=2^j$, $0<j,k<m$, m even $\gcd(k,m)=1$, $d\neq a^{q+1}(b^q+b)^{1-r}$ for $a,b\in\mathbb{M}$.	$\frac{\varphi(m)}{2}\lfloor\frac{m}{4}+1\rfloor$ [**93**]	[**148**]
$\mathcal{F}_1$	$((1,0,1,1)_q,(1,1,0,1)_{q^2})$	$q=2^k$, $\quad 0<k<m$, $\gcd(3k,m)=1$.	$\frac{\varphi(m)}{2}$ [**C**, Thm. 5]	[**B**]
$\mathcal{F}_2$	$((1,0,1,1)_q,(0,1,1,0)_{q^3})$	$q=2^k$, $\quad 0<k<m$, $\gcd(3k,m)=1$, m odd.	$\frac{\varphi(m)}{2}$ [**C**, Thm. 5]	[**B**]
$\mathcal{F}_4$	$((1,0,0,B)_q,(0,1,\frac{a}{B},0)_r)$	$q=2^k$, $\quad r=2^{k+m/2}$, $\quad 0<k<m$, $m\equiv 2 \pmod 4$, $\quad \gcd(k,m)=1$, $a\in\mathbb{K}^\times$, $\quad B\in\mathbb{M}^\times\setminus(\mathbb{M}^\times)^3$, $\quad B^{q+r}\neq a^{q+1}$.	$\geq \frac{\varphi(m)}{2m}(2^{\frac{m}{2}}-2)$ [**C**, Cor. 1]	[**C**, Thm. 1]

Table 2. Known infinite families of biprojective APN functions on $\mathbb{M}\times\mathbb{M}$

Remark 9.4. Table 2 lists all known biprojective APN families. We denote the families of Gold, Carlet, Taniguchi and Zhou-Pott functions by $\mathcal{G}$, $\mathcal{C}$, $\mathcal{T}$ and $\mathcal{ZP}$. We want to note that the first component of the Taniguchi functions is often also written (in our notation) as $(1,0,c,d)_q$. However, it is easy to verify that all values $c\neq 0$ are equivalent to the $c=1$ case and the $c=0$ case is a Zhou-Pott function.

CHAPTER 10

APN permutations

Permutations $P : \mathbb{F}_p^n \to \mathbb{F}_p^n$ find natural applications in cryptography, for instance as S-Boxes in the SPN construction of block ciphers which includes the cryptography standard AES. Particularly interesting are permutations that are *simple* in natural (polynomial) representations since simply represented functions *usually* satisfy some interesting properties in an extremal way. We have already seen some examples: Gold APN and Albert planar functions, both of which have the simplest monomial form in the most natural univariate notation, deliver the optimal differential behaviour.

Now, we explain how the classical constructions of PN/APN functions behave in terms of bijectivity.

- Gold functions $X \mapsto X^{2^k+1}$ (which are APN if and only if $\gcd(k, n) = 1$) permute $\mathbb{F}_{2^n}$ if and only if $\gcd(2^k + 1, 2^n - 1) = 1$. This means that a Gold APN function is bijective if and only if n is odd by Lemma 1.3. When n is even, Gold APN functions are three-to-one on $\mathbb{F}_{2^n}^\times$. Finding APN permutations seem to be a difficult problem on even dimensions. An observation of Dobbertin [**30**] states that a monomial APN function $X \mapsto X^d$ is necessarily three-to-one (on $\mathbb{F}_{2^n}^\times$) when n is even and bijective when n is odd. The cryptographically interesting inverse function $X \mapsto X^{2^n-2}$ is always a permutation but not APN when n is even (however, it is quite *close* to being APN).
- Planar functions cannot be bijective since for all nonzero $A \in \mathbb{F}_p^n$ one can always find an $X \in \mathbb{F}_p^n$ such that $F(X+A)-F(X) = 0$ since the maps $X \mapsto F(X+A)-F(X)$ are necessarily bijective for a planar function F. Actually, Albert's planar maps $X \mapsto X^{p^k+1}$ are always two-to-one on $\mathbb{F}_{p^n}^\times$ noting again the requirement that $n/\gcd(k, n)$ is odd. Recall the result of Weng and Zeng that states that two-to-one DO mappings (on $\mathbb{F}_{p^n}^\times$) are planar and the converse result of Kyureghyan and Pott: planar DO mappings are two-to-one (see Chapter 4).

These observations entail a natural question which is usually named **"the big APN problem"**.

PROBLEM 10.1. Do there exist APN permutations when n is even?

To continue further, we need to explain another important cryptanalytic attack and the corresponding mathematical ideas behind it.

1. Fourier transform and linear attacks

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function and define for $(u, v) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ and $u \neq 0$,

$$\lambda_F(u, v) = \#\{x \in \mathbb{F}_2^n : \langle u, F(x)\rangle = \langle v, x\rangle\} - 2^{n-1}.$$

Note that λ_F measures how much information linear combinations of input and output bits leak. Similar to differential attacks, if for carefully chosen u_i, v_i the value $|\lambda_F(u_i, v_i)|$ are all *high*, one can devise a cryptanalysis of a cipher where the S-Box F is used in several consecutive rounds, called **linear cryptanalysis**. The **nonlinearity** of a vectorial Boolean function is then defined as

$$\mathsf{NL}_F = 2^{n-1} - \max\{|\lambda_F(u, v)| \ : \ (u, v) \in \mathbb{F}_2^m \times \mathbb{F}_2^n, \ u \neq 0\}.$$

Relevant to the concept is the **Walsh transform** of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, defined as

$$\widehat{f}(v) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}(-1)^{\langle v,x\rangle},$$

which is the **Fourier transform** of $\tilde{f} : \mathbb{F}_2^n \to \{-1, 1\}$, where $\tilde{f} = (-1)^f$. We naturally extend the definition to cover vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ as (for $u \in \mathbb{F}_2^m, v \in \mathbb{F}_2^n$),

$$\widehat{F}(u, v) = \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle u,F(x)\rangle+\langle v,x\rangle},$$

which can be seen as the collection of the Walsh transforms of the **component Boolean functions** $F_u = \langle u, F\rangle$. The **linearity** of F is defined by

$$\mathsf{L}_F = \max\{|\widehat{F}(u, v)| \ : \ (u, v) \in \mathbb{F}_2^m \times \mathbb{F}_2^n, \ u \neq 0\}.$$

Observe that $\widehat{F}(u, v) = 2\lambda_F(u, v)$.

To deduce the optimal (minimal) absolute value of λ_F for a (vectorial) Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ one uses the following fundamental identity for Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

$$\sum_{v\in\mathbb{F}_2^n} (\widehat{f}(u))^2 = 2^{2n},$$

known as **Parseval's identity**, which immediately gives

$$\mathsf{L}_F \geq 2^{n/2}.$$

When n is even, the bound is sharp for every $m \leq n/2$ (that is to say, there are functions F satisfying the bound with equality). The functions satisfying the bound are called **bent functions** which then necessarily satisfy

$$\widehat{F}(u, v) = \pm 2^{n/2}, \text{ for all } u \in \mathbb{F}_2^m, v \in \mathbb{F}_2^n \text{ with } u \neq 0.$$

The following extended definition of differential uniformity of Chapter 3 is only natural (we only require the Boolean case — odd characteristic or even arbitrary abelian group generalizations are straightforward). A vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called **perfect nonlinear** if

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n \ : \ F(x + a) + F(x) = b\}| = 2^{n-m},$$

for all $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ with $a \neq 0$. When n is even and $m \leq n/2$, a (vectorial) Boolean function F is bent if and only if F is perfect nonlinear.

We will restrict our attention to the vectorial Boolean case $n = m$. Recall that the optimal differential uniformity in this case is two and is satisfied by APN functions. When n is odd, the bound (which also holds for n even)

$$\mathsf{L}_F \geq 2^{(n+1)/2}$$

is sharp and attained by **almost bent (AB) functions**. In that case

$$\widehat{F}(u,v) \in \{0, \pm 2^{(n+1)/2}\}, \text{ for all } u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^n \text{ with } u \neq 0.$$

REMARK 10.2. The Walsh spectra of affine and quadratic (recall that these always refer to the algebraic degree) Boolean functions are well-known. For an affine function it is $\{0, \pm 2^n\}$ and for a quadratic function $\{0, \pm 2^{k_f}\}$ for some $k_f \geq n/2$ which is fixed by the quadratic function f. The determination of k_f for a given function can be done via the theory of **quadratic forms** (i.e., a quadratic function with no affine part), which shows that every possible k_f is attained by some quadratic function. In the bent case (i.e., $k_f = n/2$), the value 0 does not appear in the spectrum and when $k_f > n/2$ it always does which can easily be seen by Parseval's identity. A Boolean function that has the spectrum of a quadratic or an affine function is called **plateaued**, and the vectorial Boolean functions all of whose components are plateaued are called **component-wise plateaued**. See [**121**, Section 7.2] for quadratic forms over finite fields and [**121**, Section 9.1], [**30**] for Boolean functions.

When n is odd, every AB function is APN and every plateaued APN function is AB (See [**121**, Section 9.2], [**104, 128**] for more on AB/APN/PN functions). However, there are APN functions that are not AB (e.g., the inverse and Dobbertin power functions).

When n is even, the optimal value for L_F is unknown. The best known value is attained for instance by the Gold and the Kasami power functions and is $\mathsf{L}_F = 2^{(n+2)/2}$.

When n is even, define the set of non-bent components of F by

$$\mathsf{NB}_F = \{u \in \mathbb{F}_2^n \ : \ F_u \text{ is not bent } \}.$$

Berger et al. [**12**, Corollary 3] showed that for a component-wise plateaued APN function F (the proof of the quadratic sub-case is due to Nyberg [**123**, Theorem 10]), we have

$$|\mathsf{NB}_F| \leq 1 + \frac{2^n - 1}{3}. \tag{3}$$

The importance of these results for us is related to the following character theoretic characterization [**115**, Theorem 7.7] of bijectivity of $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

THEOREM 10.3. *A vectorial Boolean function F is bijective if and only if*

$$\widehat{F_u}(0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, F(x) \rangle} = 0,$$

for all $0 \neq u \in \mathbb{F}_2^n$.

Thus, a component-wise plateaued APN function F cannot be bijective by (3).

Remark 10.4 (Hermite's criterion). Another characterization of the bijectivity of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is known as **Hermite's criterion** [**115**, Lemma 7.3 and Theorem 7.4] and states that F is bijective if and only if

$$\sum_{x\in\mathbb{F}_{p^n}} F(x)^d = \begin{cases} 0 & \text{if } 0 \leq d \leq p^n - 2, \\ -1 & \text{if } d = p^n - 1. \end{cases}$$

2. Dillon's idea

Let $n = 2m$ be even. A non-bijective APN function F might be equivalent to a bijective APN function G, if the notion of equivalence

- preserves being APN, and
- does not necessarily preserve being bijective.

The EA- and CCZ-equivalences both satisfy these two properties. A component-wise plateaued APN function cannot be bijective, thus if we want to select F to be component-wise plateaued, we have to avoid EA-equivalence since it preserves being component-wise plateaued as well. However, CCZ-equivalence does not necessarily preserve this property. Noting that many known APN families are quadratic (and that it covers the EA-equivalence), the choice of CCZ-equivalence for this purpose is quite logical.

This is the crux of Dillon's idea:

(i) find a sufficient condition to decide whether a function F is CCZ-equivalent to a bijection G, and then,

(ii) on small dimensions $m \geq 3$, try every known APN family/sporadic function.

Denote by

$$Z_{\widehat{F}} = \{(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ : \ \widehat{F}(u, v) = 0\} \cup \{(0, 0)\}$$

the set of **zeroes of the Walsh transform**. In fact, Browning et al. [**20**] found a *necessary and sufficient* condition which then gives a method to check whether an APN function f is CCZ-equivalent to a permutation.

Theorem 10.5. [**20**] *A vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation if and only if there exist two n-dimensional subspaces*

$$U, V \subseteq Z_{\widehat{F}} \subseteq \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$$

such that $U \cap V = \{(0, 0)\}$.

Browning et al. [**20**] tried every known APN function at that time for $3 \leq m \leq 5$ and found an APN permutation when $m = 3$.

Theorem 10.6. *The κ-function defined by*

$$\kappa : X \mapsto X^3 + X^{10} + UX^{24},$$

is CCZ-equivalent to an APN permutation with $U \in \mathbb{F}_{2^6}$ satisfying $U^6 + U^4 + U^3 + U = 1$.

The function κ is the only known APN function (up to CCZ-equivalence) on an even dimension over $\mathbb{F}_2$ that is equivalent to a permutation. Thus "the big APN problem" is defined on even dimensions larger than six.

Remark 10.7. For a bijection $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the vector spaces U, V of Theorem 10.5 are

$$U = \{0\} \times \mathbb{F}_{2^n} \text{ and } V = \mathbb{F}_{2^n} \times \{0\}.$$

For κ, these are

$$U = u_1\mathbb{F}_{2^3} \times u_2\mathbb{F}_{2^3} \text{ and } V = v_1\mathbb{F}_{2^3} \times v_2\mathbb{F}_{2^3},$$

for some $u_1, u_2, v_1, v_2 \in \mathbb{F}_{2^m}^\times$ with $u_1 \neq v_1$ and $u_2 \neq v_2$. That is to say, instead of the direct products of the $\mathbb{F}_{2^n}$-vector space with the trivial vector space, direct products of $\mathbb{F}_{2^{n/2}}$-vector spaces are employed. This nice structure is partly a consequence of the fact that κ is a (q, r)-biprojective function. Note that for a q-biprojective $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, we have

$$\widehat{f}(u, (v, w)) = \widehat{f}(a^{q+1}u, (av, aw))$$

for all $a \in \mathbb{F}_{2^m}$.

3. Results on bijectivity of uni- and biprojective functions

In the following we will solve the following fundamental problems on bijectivity of uniprojective (Gold) and biprojective functions.

Problem 10.8. The following problems are natural problems we solve in this thesis on uni- and biprojective functions.

(i) **Decide whether Gold APN functions are CCZ-equivalent to permutations.**

Dillon's idea leads to APN permutations when used with the (q, q)-biprojective function κ. The question whether the most natural infinite family of APN functions (i.e., the uniprojective Gold functions) are equivalent to permutations on even dimensions is a very natural one, since they are equivalent to permutations on odd dimensions and they are (q, q)-biprojective (recall that biprojectivity is a natural generalization of uniprojectivity). We will give a negative answer to this question in Chapter 11.

(ii) **Classify (q, q)-biprojective permutations.**

We showed that (q, r)-biprojective functions in bivariate representation are natural generalizations of uniprojective functions in univariate representation. Inspecting their bijective behaviour is also a natural direction. We will classify (q, q)-biprojective permutations and fractional q-projective permutations in Chapter 12. This result covers and generalizes main results from numerous recent papers solving many problems listed in them.

(iii) **Classify (q, q)-biprojective APN functions.**

This will decide whether Dillon's APN permutation arising from κ-function on $\mathbb{F}_2^6$ is generalizable. As we will see, it turns out that the κ-function is an anomaly and every (q, q)-biprojective APN function (when $n > 6$) is CCZ-equivalent to a Gold APN function. Together with the solution of the relevant problem that shows that Gold APN functions are not CCZ-equivalent to permutations, we will deduce that if a (q, q)-biprojective APN function is CCZ-equivalent to a permutation then it must be the κ-function. This will be done in Chapter 13.

(iv) **Find more (q, r)-biprojective APN functions.**

Finding new APN functions is already a difficult problem. Here, we further restrict ourselves to the more difficult problem of finding biprojective APN functions. Given that the only known APN permutation is equivalent to a biprojective one, this problem is also interesting regarding the "big APN problem". We will find new (q, q^2)- and (q, q^3)-biprojective APN families in Chapter 14. However, we will also show that they are not equivalent to permutations on small extensions.

(v) **Determine equivalences between (q, r)-biprojective APN functions.**

Checking inequivalences of APN functions are usually done by checking invariants with the help of a computer. Finding a generic theoretical method for checking inequivalences of APN functions is an important problem. We give a method for the large superclass of (q, r)-biprojective functions in Chapter 15.

Remark 10.9. Similar classification problems on (q, r)-biprojective functions seem to be very difficult. Nevertheless, we will give some positive and negative results in forthcoming chapters.

CHAPTER 11

Gold APN maps are not CCZ-equivalent to permutations on even extensions [**H**]

The main result of this chapter is the following theorem which solves Problem 10.8 (i). See Table 1 for the definitions of Gold and Kasami APN functions.

THEOREM 11.1. *The following monomial APN functions are not CCZ-equivalent to permutations.*

(i) Gold functions on $\mathbb{F}_{2^n}$ when n even,

(ii) Kasami functions on $\mathbb{F}_{2^n}$ when n divisible by 4.

First, let us explain the method.

1. APN families/functions that are not CCZ-equivalent to bijections

We only need the *sufficiency* part of the condition in Theorem 10.5 to find APN permutations using Dillon's idea. On the contrary, in order to rule out families, it is enough to have a *necessary* condition. A simpler condition would be helpful for both theoretical and practical purposes. Now, the following is a simpler necessary (but not sufficient) condition which follows from the proof of Theorem 10.5, implicit in [**H**, Section 3] and proved in full in [**61**, Condition 2].

THEOREM 11.2. *If a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation then there exist $\mathbb{F}_2$-vector spaces $S, T \subseteq \mathsf{NB}_F \subseteq \mathbb{F}_{2^n}$ such that $S + T = \mathbb{F}_{2^n}$.*

We define the vector

$$\mathsf{N}_F = \big[\eta_d(\mathsf{NB}_F) \; : \; 0 \leq d \leq n\big],$$

where $\eta_d(S)$ is the number of $\mathbb{F}_2$-vector spaces of dimension d in S. This vector is shown to be an EA-invariant for vectorial functions in [**61**].

Theorem 11.2 has the following bound as corollary.

COROLLARY 11.3. *If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is equivalent to a permutation then*

$$\eta_{n/2}(\mathsf{NB}_F) \geq 2.$$

2. Summary

The analysis is naturally divided into two cases.

(i) If $4|n$, we will show that the non-bent components of Gold and Kasami APN functions cannot contain an $\mathbb{F}_2$-vector space of dimension $n/2$, which by Corollary 11.3 implies that they cannot be equivalent to a permutations.

Gold and Kasami APN functions are component-wise plateaued and thus have large bent sets. These sets are highly structured. The following table lists bent components of Gold and Kasami functions which state that if F is a Gold or Kasami APN function then $\mathsf{NB}_F = (\mathbb{F}_{2^n})^3$.

Family	**Monomial**	**Conditions**	**Proved in**
Gold	$\mathsf{tr}(\alpha X^{2^i+1})$	$\gcd(i,n)=1, \alpha \in \mathbb{F}_{2^n}^\times \setminus (\mathbb{F}_{2^n}^\times)^3$	folklore
Kasami	$\mathsf{tr}(\alpha X^{2^{2i}-2^i+1})$	$\gcd(i,n)=1, \alpha \in \mathbb{F}_{2^n}^\times \setminus (\mathbb{F}_{2^n}^\times)^3$	[**46, 144**]

Table 1. Bent components of APN monomials on $\mathbb{F}_{2^n}$

(ii) If $4 \nmid n$, the analysis is more difficult.

3. Doubly even dimension

(i) The following lemma, which gives a bound on the maximum dimension of an $\mathbb{F}_2$-vector space in $(\mathbb{F}_{2^n})^3$, is key to proving our main result in this chapter. Let $n = 2m$ and $\mathbb{F} = \mathbb{F}_{2^n}$. The odd m case of the following lemma is easy.

Lemma 11.4. *Let $[\mathbb{F} : \mathbb{F}_2] = 2m$ and $U \subseteq (\mathbb{F})^3$ be an $\mathbb{F}_2$-subspace of $\mathbb{F}$. Then*

$$\dim U \leq \begin{cases} m, & \text{if } m \text{ is odd,} \\ m-1, & \text{if } m \text{ is even.} \end{cases}$$

The proof employs a double summation argument and the following classical result of Carlitz. In [**H**], we denote by $\chi(e) = (-1)^{\mathrm{Tr}(e)}$.

Theorem 11.5 (Carlitz). [**33**, Theorem 1] *Let $[\mathbb{F} : \mathbb{F}_2] = 2m$. Define*

$$\mathsf{Cz}(a) := \sum_{x \in \mathbb{F}} \chi(ax^3).$$

We have

$$\mathsf{Cz}(a) = \begin{cases} 2^{2m}, & a = 0, \\ (-1)^{m+1}2^{m+1}, & a \in (\mathbb{F}^\times)^3, \\ (-1)^m 2^m, & a \in \mathbb{F}^\times \setminus (\mathbb{F}^\times)^3. \end{cases}$$

The theorem of Carlitz can be seen as the Walsh transforms $\widehat{F_\beta}(0)$ of components F_β of Gold and Kasami APN functions.

(ii) When m is even, the non-bent components of Gold and Kasami functions cannot contain $\mathbb{F}_2$-vector spaces of dimension $m = n/2$ by Lemma 11.4 and by Table 1. By Corollary 11.3, we prove the following.

Corollary 11.6. *Gold and Kasami APN functions on a doubly-even-degree extension of $\mathbb{F}_2$ are not equivalent to permutations.*

4. Oddly even dimension

Let $[\mathbb{F} : \mathbb{F}_2] = n = 2m$ with m odd (i.e., n is oddly even) and $\mathbb{K} = \mathbb{F}_{2^m}$.

(i) Theorem 10.5 and Theorem 10.3 together implies the following necessary condition for an APN function to be CCZ-equivalent to a permutation.

PROPOSITION 11.7. *If $F : \mathbb{F} \to \mathbb{F}$ is CCZ-equivalent to a permutation of $\mathbb{F}$, then there exist two $\mathbb{F}_2$-linear maps S, T of $\mathbb{F}$ such that for all $\alpha \in \mathbb{F}^\times$,*

$$\sum_{x \in \mathbb{F}} \chi(T(\alpha)F(x) + S(\alpha)x) = 0,$$

with $\operatorname{rank} T \geq m$.

(ii) It is easy to see that $c\mathbb{K}$ where $c \in (\mathbb{F}^\times)^3$ are maximal $\mathbb{F}_2$-vector spaces in cubes. The following theorem (proved by Sziklai) shows that the $\mathbb{F}_2$-vector spaces in cubes with maximal dimension m are precisely the vector spaces $c\mathbb{K}$ above.

THEOREM 11.8. [**135**, Theorem 1.1] *If $d|(q+1)$, then in $\mathbb{F}_{q^2}$ (any characteristic) the only q-subsets with the property that the difference of any two elements is always a d-th power are $\alpha^d \mathbb{F}_q$ for some $\alpha \in \mathbb{F}_{q^2}^\times$.*

Recall that in our case m is odd, $q = 2^m$ and $3|(q+1)$.

(iii) Now restricting the linear map T of Proposition 11.7 to have $\operatorname{Im} T = c\mathbb{K}$ for some $c \in (\mathbb{F}^\times)^3$, and an intricate analysis, we prove the main result of the paper.

THEOREM 11.9. *Gold APN functions on an oddly-even-degree extension of $\mathbb{F}_2$ are not equivalent to permutations.*

We refer to the original paper [**H**, pp. 15–19] for the lengthy proof using triple exponential sums.

CHAPTER 12

Classification of (q,q)-biprojective and fractional q-projective permutations [D]

Classification of bijections of $\mathbb{F}_{p^n}$ induced by the monomials $X^d \in \mathbb{F}_{p^n}[X]$ is well-known.

The mapping $X \mapsto X^d$ permutes $\mathbb{F}_{p^n}$ if and only if $\gcd(d, p^n - 1) = 1$.

Thus, the standard gcd arguments of Lemma 1.3 immediately provides the classification of bijective uniprojective (Gold) mappings $G_k : X \mapsto X^{p^k+1}$.

The mapping G_k permutes $\mathbb{F}_{p^n}$ if and only if $p = 2$ and $n/\gcd(k, n)$ is odd.

In this chapter, we are going to produce full classification results on bijections induced by

- (q,q)-biprojective functions of the form:
$$\begin{aligned} F : \mathbb{L}\times\mathbb{L} &\to \mathbb{L}\times\mathbb{L} \\ (x,y) &\mapsto (f(x,y), g(x,y)), \end{aligned}$$
where f and g are q-biprojective polynomials, and
- fractional q-projective functions of the form
$$\begin{aligned} \pi : \mathcal{P}^1(\mathbb{L}) &\to \mathcal{P}^1(\mathbb{L}) \\ x &\mapsto \frac{\phi_f(x)}{\phi_g(x)}, \end{aligned}$$
where ϕ_f and ϕ_g are q-projective polynomials.

For fractional q-projective functions, we require that

(i) ϕ_f and ϕ_g do not have a common zero in $\mathbb{L}$, and

(ii) $q + 1 \in \{\deg \phi_f, \deg \phi_g\}$.

These two conditions can succinctly be described as (see Lemma 1.6 in Chapter 1)

"ϕ_f and ϕ_g do not have a common zero in $\mathcal{P}^1(\mathbb{L})$."

In this chapter, we classify

- (q,q)-biprojective permutations under the natural action of $\mathrm{GL}(2,\mathbb{L}) \times \mathrm{GL}(2,\mathbb{L})$ where $(L, M) \in \mathrm{GL}(2,\mathbb{L})^2$ acts on F as $L^{-1} \circ F \circ M$, and
- fractional q-projective permutations under the natural action of $\mathrm{PGL}(2,\mathbb{L}) \times \mathrm{PGL}(2,\mathbb{L})$ where $(\mu, \nu) \in \mathrm{PGL}(2,\mathbb{L})^2$ acts on π as $\mu^{-1} \circ \pi \circ \nu$,

as described in Chapter 3 (see also [**D**, Sections 1 and 2] and [**E**, Section III]). The corresponding notions of equivalence are denoted by $\approx$ and $\sim$ respectively (in the notation of the thesis, these are $\sim_{\mathfrak{L}}$ and $\sim_{\mathfrak{M}}$ respectively).

Remark 12.1. If we consider the division ϕ_f/ϕ_g to be *formal* (i.e., cancellations carried out only for units in $\mathbb{L}$), then the notions of equivalence coincide (as in Lemma 1.4), that is to say $F_{f_1,g_1} \approx F_{f_2,g_2}$ if and only if $\pi_{f_1,g_1} \sim \pi_{f_2,g_2}$. Since we do not assume $\gcd(\phi_f, \phi_g) = 1$, the actual division may collapse two $\sim$-equivalence classes to one. However, we show that this does not happen for the cases that are important to our classification (see [**D**, Section 6.4]).

The next section derives the result that the two types of permutations are closely related.

1. The projective-affine correspondence between π and F

The two types F and π of permutations are related to each other, akin to the correspondence between the affine plane and the projective line.

- Suppose that $F_{f,g} = (f, g)$ is a (q,q)-biprojective permutation of $\mathbb{L} \times \mathbb{L}$ where
$$f = (a_{q+1}, a_q, a_1, a_0)_q \text{ and } g = (b_{q+1}, b_q, b_1, b_0)_q.$$
Then fixing $y = 0$ (similar for $x = 0$) we immediately see that we must have
$$(a_{q+1}, b_{q+1}) \neq (0,0),$$
and
$$\gcd(q+1, r-1) = 1,$$
since the map $x \mapsto x^{q+1}$ permutes $\mathbb{L}$ if and only if $\gcd(q+1, r-1) = 1$.
- Now (w.l.o.g.) assume (exactly) one of $a_{q+1} = 0$ and $b_{q+1} = 0$ holds, and consider
$$G(x,y) = F_{f,g}(xy, y) = (y^{q+1} f(x,1), y^{q+1} g(x,1)), \tag{4}$$
for $y \neq 0$. If $0 \notin \{a_{q+1}, b_{q+1}\}$, one can then consider $(f, b_{q+1} f - a_{q+1} g) \approx (f,g)$.
- Assume (w.l.o.g.) that $b_{q+1} = 0$ (otherwise use $(g,f) \approx (f,g)$). Then, we must have
  - (i) $g(x,1) \neq 0$ for all $x \in \mathbb{L}$, and
  - (ii) $\pi_{f,g}(x) = \frac{f(x,1)}{g(x,1)}$ is a permutation of $\mathbb{L}$, which implies $f(x_0, 1) = 0$ for unique $x_0 \in \mathbb{L}$,

  by (4).
- These mean that $\pi_{f,g}(x)$ permutes $\mathcal{P}^1(\mathbb{L})$. Note that since we also assume that $y \mapsto y^{q+1}$ permutes $\mathbb{L}^\times$, these conditions are sufficient for $F_{f,g}$ to be a permutation.

Therefore, for q-biprojective polynomials $f, g \in \mathbb{L}[x,y]$, we have

Proposition 12.2. *The function $F_{f,g} : (x,y) \mapsto (f(x,y), g(x,y))$ is a permutation of $\mathbb{L} \times \mathbb{L}$ if and only if the following hold*

(i) $\gcd(q+1, r-1) = 1$,

(ii) $q + 1 \in \{\deg_x(f), \deg_x(g)\}$,

(iii) $f(x,1) = 0 = g(x,1)$ *is not satisfied for* $x \in \mathbb{L}$*, and*

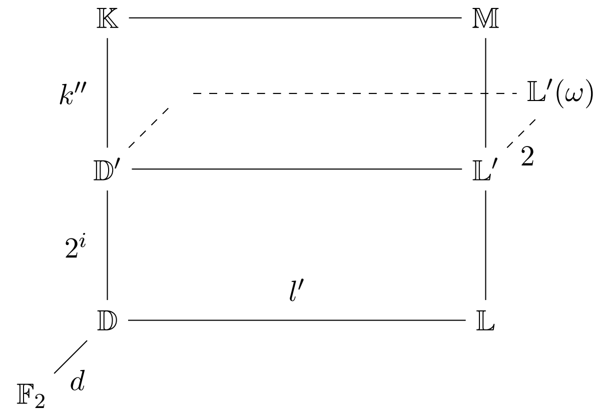
(iv) $\pi_{f,g}(x) = \frac{f(x,1)}{g(x,1)}$ *permutes* $\mathcal{P}^1(\mathbb{L})$.

2. The classification theorem

We show that fractional q-projective (and therefore (q,q)-biprojective) permutations exist if and only if the characteristic is two and in that case there are two classes of such permutations. The following diagram and its annotations describe our setting in characteristic two in order to carefully define the permutations.

Notation 12.3. Let

$$\begin{aligned} \mathbb{L} &= \mathbb{F}_r, & r &= 2^l, \quad l \in \mathbb{N},\\ \mathbb{K} &= \mathbb{F}_q, & q &= 2^k, \quad l > k \in \mathbb{N},\\ \mathbb{D} &= \mathbb{F}_s = \mathbb{K} \cap \mathbb{L}, & s &= 2^d, \quad d = \gcd(l,k),\\ \mathbb{M} &= \mathbb{F}_t = \mathbb{K} \cdot \mathbb{L}, & t &= 2^m, \quad m = \operatorname{lcm}(l,k). \end{aligned}$$



- $\omega^2 + \omega = \epsilon_2 \in \mathbb{L}'$,
- $\omega^q + \omega = \epsilon_q \in \mathbb{L}$,
- $k' = 2^i k''$, with k'' odd,
- $k = dk'$, $l = dl'$,
- $\gcd(k', l') = 1$,
- $\delta \in \mathbb{K}$ with $\delta + \epsilon_2 \in \mathbb{L}$,
- $q = 2^k, r = 2^l, s = 2^d$.

Let $\epsilon_q \in \mathbb{L}$ be an element satisfying $\mathsf{tr}_{\mathbb{L}/\mathbb{D}}(\epsilon_q) = 1$. Then there exists $\omega \in \overline{\mathbb{L}'}$ satisfying $\omega + \omega^q = \epsilon_q$ and $\omega + \omega^2 = \epsilon_2 \in \mathbb{L}'$ (as shown in [**D**, Lemma 4.1]). Let $\delta \in \mathbb{K}$ be defined as

$$\delta = \begin{cases} 0 & \text{if } [\mathbb{K} : \mathbb{D}] = k' \text{ is odd,} \\ \epsilon_2 + z & \text{if } [\mathbb{K} : \mathbb{D}] = k' \text{ is even,} \end{cases}$$

where $z \in \mathbb{L}$ satisfies $z^q + z = \epsilon_q^2 + \epsilon_q$ with $\mathsf{tr}_{\mathbb{L}/\mathbb{F}_2}(z) = 1$. Such δ exists and is easy to determine by [**D**, Theorem 5.11] and same for all ϵ_q.

Theorem 12.4. *Let $\pi(x)$ be a fractional q-projective permutation of $\mathcal{P}^1(\mathbb{L})$ over a finite field $\mathbb{L}$ of arbitrary characteristic. Then,* $\operatorname{char}(\mathbb{L}) = 2$ *and $\pi(x)$ is projectively equivalent to, either*

(i)

$$\pi(x) \sim \frac{x^{q+1} + (\epsilon_q + 1)x + \epsilon_2 + \delta + \epsilon_1}{x^q + x + \epsilon_q},$$

with $\mathsf{tr}_{\mathbb{D}/\mathbb{F}_2}(\epsilon_1) = 1$, *or*

(ii)

$$\pi(x) \sim \frac{x^{q+1} + (\epsilon_q + 1)x + \epsilon_2 + \delta}{x^q + x + \epsilon_q}.$$

Remark 12.5. Another (and possibly simpler) way of phrasing this classification is as follows.

- Every fractional projective bijection of $\mathcal{P}^1(\mathbb{L})$ is equivalent to
$$\pi_\alpha : x \mapsto \frac{x^{q+1} + (\epsilon_q + 1)x + \alpha}{x^q + x + \epsilon_q}$$
for some $\alpha \in \mathbb{L}$ such that $\alpha^q + \alpha = \epsilon_q^2 + \epsilon_q$, and all such α gives bijections.
- $\pi_\alpha \sim \pi_\beta$ if and only if $\mathsf{tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha) = \mathsf{tr}_{\mathbb{L}/\mathbb{F}_2}(\beta)$. and there exist such $\alpha_0, \alpha_1 \in \mathbb{L}$ satisfying $\mathsf{tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha_0) = 0$ and $\mathsf{tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha_1) = 1$.

Remark 12.6. When $[\mathbb{L} : \mathbb{D}] = l'$ is odd, the classification becomes simpler. In that case, $\pi(x)$ is projectively equivalent to, either

(i)
$$\pi(x) \sim x^{q+1} \sim \frac{x^{q+1}}{x^q + x + 1}, \text{ or,}$$

(ii)
$$\pi(x) \sim \frac{x^{q+1} + \epsilon_1}{x^q + x + 1},$$
with $\mathsf{tr}_{\mathbb{D}/\mathbb{F}_2}(\epsilon_1) = 1$.

3. The method

We first note that the class of (q, q)-biprojective functions of $\mathbb{L} \times \mathbb{L}$ is in one-to-one correspondence with the following subclass of Dembowski-Ostrom polynomials over $\mathbb{L}(\xi)$ where $[\mathbb{L}(\xi) : \mathbb{L}] = 2$. Recall that $|\mathbb{L}| = r$ and let
$$D_q = \{q + 1, r(q + 1), q + r, qr + 1\}.$$
The subclass of Dembowski-Ostrom polynomials we mentioned above is defined by
$$R(X) = \sum_{d \in D_q} A_d X^d, \quad A_d \in \mathbb{L}(\xi). \tag{5}$$
It is straightforward to see by $\mathbb{L}(\xi) = \mathbb{L} + \xi\mathbb{L}$ (i.e., writing $X \in \mathbb{L}(\xi)$ as $X = x + \xi y$ for $x, y \in \mathbb{L}$) that all R (when $\mathbb{L}(\xi) = \mathbb{L} + \xi\mathbb{L}$ is viewed as $\mathbb{L} \times \mathbb{L}$) describe (q, q)-biprojective functions and simple counting shows that the two families are in one-to-one correspondence. Let $R(x + \xi y) = f(x, y) + \xi g(x, y)$ where f, g are q-biprojective. One can define the fractional q-projective function
$$\pi_R : x \mapsto \frac{f(x, 1)}{g(x, 1)},$$
whenever f, g do not have common $\mathcal{P}^1(\mathbb{L})$-zeroes. We call this process **projectivization**. Note that different choices for the basis $\{1, \xi\}$ lead to equivalent (q, q)-biprojective and fractional q-projective functions under $\approx$ and $\sim$ respectively.

Method 12.7. Let $\mathrm{char}(\mathbb{L}) = 2$ and π_1, π_2 be the two fractional q-projective permutations of Theorem 12.4. Let F_1, F_2 be the two corresponding (q, q)-biprojective functions.

(i) First we identify π_1, π_2 in a different way.
   - (The case $[\mathbb{L} : \mathbb{D}]$ is odd.) Then,
     (a) π_1 is the projectivization of X^j for some $j \in \{q + 1, q + r\}$ depending on whether $[\mathbb{K} : \mathbb{D}]$ is odd or even; and

(b) $\pi_2 \sim x^{q+1}$.

- (The case $[\mathbb{L} : \mathbb{D}]$ is even.) Then, π_1, π_2 are projectivizations of X^j where $j \in \{q+1, q+r\}$.

These are proved in [**D**, Sections 7.2 and 7.3].

(ii) In the odd $[\mathbb{L} : \mathbb{D}]$ case: the corresponding (q,q)-biprojective function F_1 is bijective by a simple gcd consideration on X^j. One proves the bijectivity of π_1 immediately by Proposition 12.2. Bijectivity of π_2 is clear, again by a simple use of gcd.

In the even $[\mathbb{L} : \mathbb{D}]$ case: F_1, F_2 are not bijective, again by gcd conditions. The bijectivity of π_1, π_2 is proved by representing π_1 and π_2 in a univariate way (see [**D**, Proposition 7.4]).

(iii) The converse (i.e., every fractional q-projective bijection is equivalent to one of π_1, π_2) is proved using the **discrete Fourier transform (DFT)**. For a function $F : \mathbb{L} \to \mathbb{L}$, define

$$\mathfrak{f}_j = \begin{cases} F(0) & \text{if } j = 0, \\ -\sum_{y \in \mathbb{L}} F(y) y^{-j} & \text{if } 1 \le j \le |\mathbb{L} - 1|, \end{cases}$$

where $-j = |\mathbb{L}| - 1 - j$. The following fact is well-known.

LEMMA 12.8. *The function F satisfies $F(x) = \sum_{j=0}^{|\mathbb{L}|-1} \mathfrak{f}_j x^j$.*

Now, using the (fractional) polynomial forms of π and an effective use of DFT, we deduce several contradictions via the Hermite's criterion (see Remark 10.4). We prove that every fractional q-projective bijection π is equivalent to π_1 or π_2. The details are in [**D**, Sections 6.1, 6.2, and 6.3].

(iv) The final step concerns the full classification. We show that π_1 and π_2 are inequivalent using the definition of equivalence $\sim$ directly (see [**D**, Section 6.5]). That is to say, there are no $\mu_1, \mu_2 \in \mathrm{PGL}(2, \mathbb{L})$ such that $\pi_1 = \mu_1 \circ \pi_2 \circ \mu_2$.

4. Results on the roots of q-projective polynomials

A large portion of [**D**, Sections 4 and 5] is devoted to the roots of q-projective polynomials with one zero in $\mathcal{P}^1(\mathbb{L})$.

Let

$$I_1(q, \mathbb{L}) = \{b \in \mathbb{L} \ : \ x^{q+1} + x + b \ \text{ has one } \mathbb{L}\text{-zero}\}.$$

These sets are quite important (see Chapter 13).

- We provide ([**D**, Theorem 5.13]) (2^d+1)-to-one mappings $f_{\delta+\epsilon} : \mathbb{L} \to I_1(q, \mathbb{L})$ generalizing [**45**, Theorem 6.1] (which is also the main result of [**68**, Theorem 1]) which requires $d = \gcd(k,l) = 1$ to the arbitrary d case.
- We provide a method (see [**D**, Remark 5.14]) to explicitly (i.e., depending only on y and a parameter $c \in \mathbb{K}$) determine all $q+1$ roots of $x^{q+1} + x + f_{\delta+\epsilon}(y)$. These methods are extendable to $I_j(q, \mathbb{L})$ for any number of $\mathbb{L}$-roots j a q-projective

polynomial allows. These results are essential in our study of q-projective polynomials and used quite often in the thesis. A less explicit description was given by Bluher [**18**, Theorem 2.5] which we heavily use.

- We give an alternative proof to Theorem 12.4. The proof is more direct but quite complicated. Our aim is, again, to provide a method which is essential for the study of combinatorial objects that arise from q-projective polynomials as exemplified for instance by the results in the next chapter.

5. Related results

Motivated by the cryptographic applications, quite a few papers have been published recently [**139, 138, 111, 110, 114, 137**] on permutations of type (5) for special cases of parameters (p, k, l). Recall that $p^k = q$ and $p^l = r$. By Lemma 1.3 and Proposition 12.2, $\gcd(q+1, r-1) = 1$ is required for the permutations of the form (5), the condition $p = 2$ is necessary for these polynomials to be permutations.

- In [**139**], some permutations of type (5) were given when $(p, k, l) = (2, 1, \mathrm{odd})$.
- In [**138**], more permutations of type (5) were given when $(p, k, l) = (2, 1, \mathrm{odd})$, and it was conjectured that these are all such permutations.
- In [**111**], it was proved that the permutations given in [**139, 138**] covers all such permutations when $(p, k, l) = (2, 1, \mathrm{odd})$.
- In [**110, 114**], some permutations of type (5) were given when $(p, k, l) = (2, k, \mathrm{odd})$, with the additional restriction $\gcd(k, l) = 1$, and it was conjectured that these are all such permutations. The authors raised equivalence questions on the found classes.

In [**D**], we solve all these problems not just for the specific parameters but for all (p, k, l) using the setting $\mathbb{L} \times \mathbb{L}$, instead of the univariate setting $\mathbb{L}(\xi)$ of the form (5). Namely, we give all q-biprojective permutations of $\mathbb{L} \times \mathbb{L}$ for all (p, k, l) without any restriction on the parity of l or $\gcd(k, l)$. This is equivalent to determining all permutations of the form (5) as we have shown above. Further, we give a complete classification under $\mathbb{L}$-linear equivalence solving the equivalence problems raised by the authors, again in our setting and for all (p, k, l).

Moreover, recall that our classification of q-biprojective permutations of $\mathbb{L} \times \mathbb{L}$ arose from the classification of the fractional q-projective permutations of $\mathcal{P}^1(\mathbb{L})$. Proposition 12.2 states that the classification of the fractional q-projective permutations is stronger, since one does not need the requirement $\gcd(q+1, r-1) = 1$ or $p = 2$. Note that the fractional q-projective permutations has not been studied before to the best of our knowledge.

In the papers [**110, 114, 137**], the authors analyzed the cryptographic *boomerang uniformity* property of the permutations given in [**111, 110, 114**]. In [**D**, Section 7], we proved that all of the permutations in the cited papers are equivalent to Gold permutations (and the degenerate doubly-Gold permutation in one case), hence they are not new.

Remark 12.9. Since the publication of [**D**], three more papers [**97, 143, 113**] have appeared that are mostly covered by [**D**].

CHAPTER 13

Classification of (q, q)-biprojective APN functions [E]

Our aim in this this chapter is to classify (q, q)-biprojective functions $\mathcal{V}_{q,\mathbb{L}} \times \mathcal{V}_{q,\mathbb{L}}$, under the equivalence relation $\approx_{\mathfrak{L}}$ induced by the action of $\mathrm{GL}(2, \mathbb{L}) \times \mathrm{GL}(2, \mathbb{L})$ (the left and right application). As observed in Chapter 6, it is enough to consider representatives from the orbits of q-projective polynomials $\mathcal{V}_{q,\mathbb{L}}$ under the equivalence relation $\sim_{\mathfrak{M}}$ induced by the action of $\mathbb{L}^{\times} \times \mathrm{PGL}(2, \mathbb{L})$ (scaling and right application).

We say that $\mathcal{S}_{q,\mathbb{L}} \subseteq \mathcal{V}_{q,\mathbb{L}}$ is a **representative set** of $\mathcal{V}_{q,\mathbb{L}}$ if (denoting by $[f]_{\sim}$ the equivalence class of f under $\sim$)

$$[\mathcal{S}_{q,\mathbb{L}}]_{\sim_{\mathfrak{M}}} = \bigcup_{f \in \mathcal{S}_{q,\mathbb{L}}} [f]_{\sim_{\mathfrak{M}}} = \mathcal{V}_{q,\mathbb{L}}.$$

Define the sets (recalling that Z_f is the number of $\mathcal{P}^1(\mathbb{L})$-zeroes of f)

$$\begin{aligned} D_0 &= \{(0,0,0,0)_q\}, \\ D_1 &= [(0,0,0,1)_q]_{\sim_{\mathfrak{M}}}, \\ D &= D_0 \cup D_1, \\ \Pi_j &= \{f \in \mathcal{V}_{q,\mathbb{L}} \setminus D \ : \ |Z_f| = j\}, \end{aligned}$$

for $j \in \{0, 1, 2, p^{\delta} + 1\}$ where $\delta = \gcd(k, l)$.

In [**E**, Section 3], we determine the orbits of q-projective polynomials when $p = 2$ and $\delta = \gcd(k, l) = 1$. The fact that Π_0 has one orbit was established in [**C**, Lemma 7].

We then deduce [**E**, Lemma 3.6] a representative set of $\mathcal{V}_{q,\mathbb{L}}$.

Lemma 13.1. *Let $p = 2, q = 2^k$, $\delta = \gcd(k, l) = 1$, and*

$$S = \{(0,0,0,0)_q, (0,0,0,1)_q, (0,0,1,0)_q\} \cup \{(1,0,0,a)_q \ : \ a \in \mathbb{L}^{\times}\}.$$

(i) If l is odd then

$$\mathcal{S}_{q,\mathbb{L}} = S \cup \{(0,1,1,0)_q\} \cup \Pi_0.$$

(ii) If l is even then

$$\mathcal{S}_{q,\mathbb{L}} = S \cup \Pi_1.$$

Then $\mathcal{S}_{q,\mathbb{L}}$ is a representative set for $\mathcal{V}_{q,\mathbb{L}}$.

1. The method

In this chapter we prove the following theorem.

Theorem 13.2. *Let $q = 2^k$, $r = 2^l$, $\mathbb{L} = \mathbb{F}_{2^l}$ with $0 < k < l$ and $F : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \times \mathbb{L}$ be a (q, q)-biprojective function. Then F is APN if and only if $\gcd(k, l) = 1$, and*

(i) l is even and $F \approx_{\mathfrak{L}} G_{q+1}$ or $F \approx_{\mathfrak{L}} G_{q+r}$, or

(ii) l *is odd,* k *is odd, and* $F \approx_{\mathfrak{L}} G_{q+1}$*, or*

(iii) l *is odd,* k *is even, and* $F \approx_{\mathfrak{L}} G_{q+r}$*, or*

(iv) $l = 3$ *and* $F \approx_{\mathfrak{L}} \kappa$*.*

The biprojective maps $G_s : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \times \mathbb{L}$ with $s \in \{q+1, q+r\}$ are the so-called Gold maps $X \mapsto X^s$ in the univariate notation with a suitable identification of the vector spaces (see Chapter 3).

Method 13.3. (i) Deduce [**E**, Proposition 5.1] that $\gcd(k, l) = 1$ is necessary.

(ii) Use $\mathcal{S}_{q,\mathbb{L}}$ of Lemma 13.1 and analyse case by case:

(a) The case $f \in \{(0,0,0,0)_q, (0,0,0,1)_q\}$ is trivial.

(b) The case $f \in \{(0,0,1,0)_q\}$ is handled by [**E**, Lemmas 4.2 and 4.3].

The only allowed case is when $\mathbb{L} = \mathbb{F}_{2^3}$ and the corresponding function is κ. In this part, we use a method using properties of Dillon-Dobbertin difference sets.

(c) The case $f \in \{(1,0,0,a)_q\}$ reduces to (b).

(iii) Now we analyze the last case: $(f, g) \in \Pi_1 \times \Pi_1$ when l is even.

We must have $rf(x,1) + sg(x,1) \in \Pi_1$ for every $(r,s) \in \mathbb{L} \times \mathbb{L} \setminus \{(0,0)\}$ otherwise it falls into one of the above cases (some details require care [**E**, Proposition 5.5]). That is to say

$$\pi(x) = \frac{f(x,1)}{g(x,1)} = \frac{s}{r}$$

has a unique solution $x \in \mathbb{P}^1(\mathbb{L})$ for every $s/r \in \mathbb{P}^1(\mathbb{L})$, i.e., $x \mapsto \pi(x)$ is bijective. That is to say

$$F \approx_{\mathfrak{L}} G_{q+1} \text{ or } F \approx_{\mathfrak{L}} G_{q+r},$$

by Method 12.7. Thus the problem of classifying biprojective APN function has reduced to the classification of fractional projective permutations.

The case when l is odd is much more involved but similarly natural. We use the $\mathrm{PGL}(2, \mathbb{L})$ action and exploit transitivity of the action on Π_1. The proof [**E**, Proposition 5.6] again boils down to the classification of fractional q-projective permutations of the last chapter.

Remark 13.4. (i) Combining with the previous results we deduce that a (q, q)-biprojective APN function F over $\mathbb{L} \times \mathbb{L}$ is CCZ-equivalent to a permutation if and only if $l = 3$ and $F \approx_{\mathfrak{L}} \kappa$.

(ii) The problem we solved is one of the open problems listed by Carlet in [**29**, Section 3.7] where important problems on cryptographic functions was surveyed.

(iii) The special case $k = 1$ was solved in [**34**] using results from [**109, 103, 60**]. Thus, our theorem generalizes the main results of [**34, 109, 103, 60**].

(iv) Another idea to attack the problem is to identify a class of functions that includes κ when $l = 3$ and also are CCZ-equivalent to permutations for larger l. This is the case of the so-called butterfly construction [**127**] which requires l to be odd. We show in [**E**, Remark V.4] that a subcase of [**E**, Proposition V.2] (which is a subcase of the main theorem) strictly generalizes the butterfly construction. Thus, our theorem also generalizes the main results of [**26, 25**].

(v) The proof is based on three concepts:

- zeroes of projective polynomials [**18**],
- properties of Dillon-Dobbertin difference sets [**46**], and
- recent classification of fractional projective permutations over finite fields [**D**].

(vi) The proof avoids the use of Weil bound (which usually allows only small degree cases) and is purely combinatorial.

CHAPTER 14

Hybrid Gold functions [B]

The main aim of [**B**] was

- to introduce (q, r)-biprojectivity,
- to introduce a method to find (q, r)-biprojective APN functions, and
- to introduce two infinite families of such functions.

As we have seen in Chapter 10, the κ-function, which is $(2, 2)$-biprojective, is CCZ-equivalent to an APN permutation of $\mathbb{F}_{2^3} \times \mathbb{F}_{2^3}$. This was our motivation to investigate (q, q)-biprojective functions. However, we have seen in the last chapter that (q, q)-biprojective APN functions are not CCZ-equivalent to permutations on larger dimensions. One of the main motivation of studying (q, r)-biprojective functions was finding new APN functions that might be equivalent to permutations. The main theorem is [**B**, Theorem III.1].

Theorem 14.1. *The following (q, r)-biprojective functions*

$$F : (x, y) \mapsto (f(x, y), g(x, y))$$

are APN on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

$$F = \begin{cases} ((1, 0, 1, 1)_{2^i}, (1, 1, 0, 1)_{2^{2i}}) & \gcd(i, m) = 1, \gcd(3, m) = 1 \quad (\mathcal{F}_1), \\ ((1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^{3i}}) & \gcd(i, m) = 1, \gcd(6, m) = 1 \quad (\mathcal{F}_2), \\ ((0, 1, 1, 0)_2, (1, u, u^3, u^{13})_{2^3}) & m = 5 \text{ and } u^5 + u^2 = 1 \quad (\mathcal{F}_3). \end{cases}$$

Remark 14.2. Note that left and right parts of functions from Families $\mathcal{F}_1$ and $\mathcal{F}_2$ are left or right parts of some Gold functions. This idea of construction used later in the pre-semifield Family S of [**A**] by using left and right parts of Albert's twisted fields.

We were not able to find a function CCZ-equivalent to a permutation. However, we found the only example (apart from the Gold and κ functions) of a quadratic APN function that has at least two m-dimensional $\mathbb{F}_2$-vector spaces in their non-bent components (i.e., that satisfies Corollary 11.3) which is a necessary condition for being equivalent to a permutation. Also there are only three quadratic APN families that have at least one m-dimensional $\mathbb{F}_2$-vector space in their non-bent components one of which is a family found in this section. The following proposition lists known APN functions and families that have at least one m dimensional $\mathbb{F}_2$-vector spaces in its non-bent components.

Proposition 14.3. *We have the following bounds for the following APN functions $F : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$, when m is odd.*

(i) If $F(X) = X^{2^k+1}$ with $\gcd(k, n) = 1$, then $\eta_m(\mathsf{NB}_F) = (2^m + 1)/3$.

(ii) if $F = \kappa$, *then* $\eta_m(\mathsf{NB}_F) = 2$.

(iii) if $F \in \mathcal{F}_3$, *then* $\eta_m(\mathsf{NB}_F) = 2$.

(iv) If $F(X) = X^3 + \mathsf{tr}(X^9)$, *then* $\eta_m(\mathsf{NB}_F) \geq 1$.

(v) If $F \in \mathcal{F}_2$, *then* $\eta_m(\mathsf{NB}_F) \geq 1$.

1. The method

METHOD 14.4. (i) First we prove

LEMMA 14.5. *Let* $(x, y) \mapsto F(x, y) = (f(x, y), g(x, y))$ *be a* (q, r)*-biprojective mapping of* $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. *Then* F *is APN if and only if the pair of equations*

$$\mathsf{D}_f^u(x, y) = 0 = \mathsf{D}_g^u(x, y)$$

has exactly two solutions for each $u \in \mathcal{P}^1(\mathbb{F}_{2^m})$.

This is the analogue of the PN function case of Lemma 6.1. A slight variation of D with the notation E is used for the method (see [**B**, Lemma 4.1]). In fact, this version is chronologically the first instance of the approach of this thesis.

(ii) We write the (E variant of) polarizations for all $u \in \mathcal{P}^1(\mathbb{F}_{p^m})$ (other than a few exceptions which should be handled separately)

$$x + x^q = M_f^u(y), \tag{6}$$

$$x + x^{q^k} = M_g^u(y), \tag{7}$$

where $M_\cdot^u$ are $\mathbb{F}_2$-linear maps determined by E. Note that $(\mathbb{F}_q \cap \mathbb{F}_{2^m}) \times \{0\}$ are common solutions and $\mathbb{F}_q \cap \mathbb{F}_{2^m} = \mathbb{F}_2$ should be satisfied, for F to be APN, i.e., $\gcd(k, m) = 1$. Consider the $\mathbb{F}_2$-linear operator

$$\mathcal{L}(\alpha, \beta) = \sum_{l=0}^{k-1} \alpha^{q^l} + \beta.$$

It is easy to see

$$\mathcal{L}(x + x^q, x + x^{q^k}) = 0.$$

Define

$$L_F^u(y) = \mathcal{L}(M_f^u(y), M_g^u(y)).$$

We deduce that $\ker L_F^u$ contains all $y \in \mathbb{F}_{p^m}$ such that (x, y) is a common solution of (6) and (7) for some $x \in \mathbb{F}_{p^m}$. Now (6) and (7) have no common solutions other than $\mathbb{F}_2 \times \{0\}$ if and only if

(a) $\ker L_F^u = \{0\}$; or,

(b) $\ker L_F^u \supsetneq \{0\}$ and for all nonzero $y_u \in \ker L_F^u \setminus \{0\}$, we have $\mathsf{tr}(M_f^u(y_u)) = 1$ by Hilbert's Theorem 90,

for all $u \in \mathcal{P}^1(\mathbb{F}_{p^m})$ (other than some simple exceptions mentioned above). See [**B**, Section IV] for details.

(iii) When $k = 2$, the linear maps satisfy $L_F^u(y) = a(u)y^{q^2} + b(u)y^q + c(u)y$ for some maps a, b, c. These maps, via $L_F^u(y) = y\phi_u(y^{q-1})$, are related to a q-projective polynomial ϕ_u. Since we require $\mathbb{F}_q \cap \mathbb{F}_{2^m} = \mathbb{F}_2$, or equivalently,

$\gcd(q-1, p^m-1) = 1$, we have $\ker L_F^u = \{0\}$ if and only if ϕ_u has no $\mathbb{F}_{p^m}$-zeroes. We proceed to show that all ϕ_u are equivalent under the $\mathrm{PGL}(2, \mathbb{F}_{p^m})$ action to the *canonical* projective polynomial $\phi(y) = y^{q+1}+y+1$ which has no $\mathbb{F}_{p^m}$-zeroes if $3 \nmid m$. This proves that $\mathcal{F}_1$ is APN.

When $k = 3$, the proof is substantially more difficult. We show that $L_F'^u = L_F^u + \alpha(u)(L_F^u)^q$ where L_F^u is as in $\mathcal{F}_1$. Then determine $\ker L_F'^u = \{0, y_u\}$ and show that $\mathsf{tr}(M_f'^u(y_u)) = 1$. This proves that $\mathcal{F}_2$ is APN.

(iv) The proof for $\mathcal{F}_3$ is computerized.

2. Related results

Two papers have appeared recently that extend Family $\mathcal{F}_1$.

- Li et al. [**112**] had the interesting idea to add bilinear terms to both components f and g of Family $\mathcal{F}_1$ to get new APN functions.
- Calderini et al. [**24**] noticed that in the Family $\mathcal{F}_1$, the condition $3 \nmid m$ can be removed by modifying Method 14.4 to allow the use of $\phi_a(y) = y^{q+1} + y + a$ instead of $\phi_1 = y^{q+1} + y + 1$ for Family $\mathcal{F}_1$.

3. Equivalence results

The rest of the paper is devoted to showing that the families $\mathcal{F}_1, \mathcal{F}_2$ contain new APN functions that are not contained in previously known families. This is done in [**B**, Section VI]. For every dimension m, two (but not all) of the APN functions of Family $\mathcal{F}_1$ belong to an APN family given by Budaghyan et al. in [**22**]. We give [**B**, Proposition VI.2] a detailed study on the equivalences of the family of Budaghyan et al. and show that they are equivalent to either Gold $\mathcal{G}$, Carlet $\mathcal{C}$ or $\mathcal{F}_1$. The inequivalence results use the invariant $\eta_d(\mathsf{NB}_F)$ we introduced before [**B**, Tables I,II and III] and are computerized which is a common practice in the field. In the next chapter (explaining the results of [**C**]), we give a method to determine inequivalences of biprojective APN functions theoretically.

CHAPTER 15

Equivalences of (q, r)-biprojective APN functions [**C**]

First, let us explain the main contributions of [**C**].

1. Contributions

Let $\mathbb{M} = \mathbb{F}_{2^m}$ and $\mathbb{L} = \mathbb{F}_{2^{m/2}}$.

- We introduce a method to determine equivalences between biprojective functions [**C**, Section 4] and provide a full classification for the known (q, r)-biprojective APN functions [**C**, Theorem 6].

  THEOREM 15.1. *Let $m > 2$, $m \neq 6$ and the (q_1, r_1)- and (q_2, r_2)-biprojective functions*

  $$F, G : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$$

  be in distinct families from the following list (see Table 2):

  (i) The Gold functions $\mathcal{G}$,

  (ii) The Zhou-Pott functions $\mathcal{ZP}$,

  (iii) The Taniguchi functions $\mathcal{T}$,with $(q, m) \neq (2, 4)$,

  (iv) $\mathcal{F}_1$ with $(q, m) \neq (2, 4)$,

  (v) $\mathcal{F}_2$,

  (vi) $\mathcal{F}_4$,

  (vii) The Carlet functions $\mathcal{C}$ for m odd.

  Then F, G are CCZ-inequivalent.

  This is a comprehensive list settling the equivalence question for the large superclass of (q, r)-biprojective APN functions. We establish a method to check whether a putative new (q, r)-birojective APN family is equivalent to a function belonging to the large corpus of known biprojective APN families.

- The Family $\mathcal{F}_4$ is introduced in [**C**, Theorem 1]. In the statement of the following theorem, we have $Q = |\mathbb{L}| = 2^{m/2}$.

  THEOREM 15.2. *Let $B \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^3$ and $a \in \mathbb{L}^\times$ be such that $B^{q+r} \neq a^{q+1}$. let*

  $$F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$$

  be defined as

  $$F : (x, y) \mapsto F(x, y) = ((1, 0, 0, B)_q, (0, 1, a/B, 0)_r),$$

  where $q = 2^k$ with $m \equiv 2 \pmod 4$, $\gcd(k, m) = 1$ and $r = qQ$. Then F is APN.

Note that this family is analogous to our semifield family $\mathcal{S}$ of [**A**].

- Equivalences between functions F, G that belong to the same biprojective family are determined (see [**C**, Theorem 5]). In particular, we determine the equivalences of Carlet's family $\mathcal{C}$ for all dimensions, settling the open problem of Kaspers and Zhou [**93**, Section 6]. Arguably, the Family $\mathcal{C}$ provides the *most natural* biprojective functions due to the simplicity of its definition. However, the techniques for analyzing this family is harder than the other biprojective families.
- We show that the family $\mathcal{F}_4$ produces an exponential number of pairwise inequivalent APN functions. This is only the second such family in the literature. Quite recently, the Taniguchi family $\mathcal{T}$ was shown to produce an exponential number of pairwise inequivalent APN functions in [**92**] by Kaspers and Zhou. Moreover, our work simplifies this and similar proofs of such results by introducing a natural group theoretic method which works not just for the family $\mathcal{T}$, but for all (q,r)-biprojective families.

2. The method

The method is based on Method 8.5. However there are key differences. As explained in Chapter 9, equivalences of vectorial functions in even and odd characteristic differs considerably. While in the commutative semifield case (see [**A**, Remark 6.3]) addressing linear equivalence of planar functions is enough, in the quadratic APN function case one requires extended linear equivalence. In [**C**, Section 4] we address this issue and give a method for the EL-equivalence case.

As explained in [**C**, Theorem 3], the family $\mathcal{C}$ requires special treatment (since it is $(1,q)$-projective). We address these problems in [**C**, Section 5]. An example of such considerations is interesting on its own. In [**C**, Lemma 7], where we determine the orbits of q-projective polynomials under the action of $\mathbb{M}^\times \times \mathrm{PGL}(2,\mathbb{M})$ when $q = 2^k$ and $\gcd(k,m) = 1$.

The remaining parts [**C**, Sections 6 and 7] are intricate analyses required to prove our main theorem.

CHAPTER 16

The discrete logarithm problem (DLP) and projective polynomials [F, G]

Modern cryptography is based on two paradigms: **public key (asymmetric) cryptography** and **secret key (symmetric) cryptography**. The goal in public key cryptography is to establish a secret key required by symmetric cryptographic algorithms which is then employed to establish a fast and secure transmission. Perfect (or highly) nonlinear functions are usually employed as building blocks of symmetric key algorithms. We have studied these functions in previous chapters with the help of projective polynomials.

A major (and the first) key establishment algorithm is the **Diffie-Hellman (DH) key agreement protocol** [**44**] which is closely related to the **Discrete Logarithm Problem (DLP)**. In this chapter, we will show that projective polynomials are useful in attacking the discrete logarithm problem on finite fields. In the case of perfect and almost perfect nonlinear functions over $\mathbb{L}$, we have seen that projective polynomials with no (or few) solutions in $\mathbb{L}$ are critical. In this chapter, we explore the other extreme: we use q-projective polynomials from $\mathbb{L}[X]$ that splits in $\mathbb{L}$ (i.e., that have as many solutions in $\mathbb{L}$ as their polynomial degree $q+1$).

1. DLP and Diffie-Hellman key agreement algorithm

Let $G = \langle g \rangle$ be a cyclic group. Suppose that A and B want to establish a secret key. Both parties generate random integers a, b and compute g^a, g^b respectively and transmit these to each other. Both can now compute g^{ab} which is then established as the secret key.

Given $h \in G$, the **discrete logarithm problem** is to find an integer $0 \leq i < |G|$ such that $g^i = h$ (denoted by $\log_g(h) = i$). It is clear that an attacker intercepting the communication of A and B, and that can solve the DLP on G efficiently, can compute g^{ab} as well. Therefore the security of the DH key agreement protocol depends on the tractability of the DLP.

2. Algorithms for the DLP

The **Pohlig-Hellman algorithm** reduces the DLP on an arbitrary group G with $|G| = \prod p_i^{e_i}$ to DLPs in cyclic groups of prime order p_i. The two other important generic algorithms for the DLP are the **baby step-giant step algorithm** and **Pollard's rho algorithm**, which require time polynomial in $\sqrt{|G|}$.

In this thesis, we are interested in the multiplicative group $\mathbb{F}_{p^n}^{\times}$ of a finite field, especially when p is *small* compared to the order p^n. The **index calculus method** leads to a faster algorithm in this case (see [**82**, Section 4.1] for a history and extensive references).

METHOD 16.1 (Index calculus). Let $\mathcal{F} = \{x_i : i \in I\}$ be a subset of $G = \langle g \rangle$ (containing g) called the **factor base**.

(i) Relation generation: Collect enough multiplicative relations of the form

$$\prod_{i \in I} x_i^{d_i} = \prod_{j \in I} x_j^{e_j},$$

so that the linear relations

$$\sum_{i \in I} d_i \log_g x_i \equiv \sum_{j \in I} e_j \log_g x_j \pmod{|G|}$$

in indeterminates x_i generate a (uniquely) solvable system.

(ii) Linear algebra: Solve the system to find the non-zero solution which gives the logarithms of the factor base elements.

(iii) Individual logarithm: Let $h \in G$ be the element whose logarithm is required. Write h in terms of factor base elements

$$h = \prod_{i \in I} x_i^{d_i},$$

which then allows one to compute the discrete logarithm of h.

Other than Part (ii) which can be simply done by well-known algorithms such as Structured Gaussian Elimination, Lanczos, and Wiedemann algorithms [**106**], how to solve Parts (i) and (iii) is not immediate. Actually, the specific way one solves these tasks determines the complexity of the whole algorithm. When one specializes in the DLP on the multiplicative group of a finite field $\mathbb{F}_{p^n}$, which is viewed as the quotient ring $\mathbb{F}_p[X]/(F)$ where F is a degree n irreducible polynomial, the notion of the Euclidean norm function *degree* on $\mathbb{F}_p[X]$ becomes important in the index calculus method. (In this chapter, by the degree we will mean the polynomial degree.) First of all, the factor base is usually selected in such a way that it contains all polynomials that have degrees smaller than or equal to a bound m. Secondly, in Part (iii) of the index calculus method, an element h (with arbitrary degree) is usually written progressively as a product of lower degree elements in an iterative manner until the expression contains only the elements of degrees smaller than or equal to m, that is to say, the elements that are in the factor base.

DEFINITION 16.2. A polynomial $f \in \mathbb{F}_p[X]$ is said to be **m-smooth** if it factors into irreducible polynomials of degree less than or equal to m.

The following result gives an estimate for the probability that a degree n polynomial to be m-smooth which is essential for the complexity analysis of classical index calculus methods.

THEOREM 16.3. [**54, 124**] *The probability that an arbitrary degree n polynomial $f \in \mathbb{F}_p[X]$ is m-smooth is $u^{-u+o(1)}$ where $u = n/m$.*

In this thesis, we are going to concentrate on the original contributions of [**F, J, G**] that improve Part (i) and Part (iii) of the index calculus method. These contributions arise from the properties of the central objects of this thesis — projective polynomials. Our approach in this chapter reflects the general theme and is based on projective polynomials. We refer to the comprehensive surveys [**124, 125, 82, 64, 84**] and the textbook [**75**, Chapters 2, 3, 4, 6, 15] for the details that are omitted here.

3. Function field sieve

The following is a brief explanation of the variant introduced by Joux and Lercier [**81**], where the function field sieve is explained in an elementary way. Let $\mathbb{F}_{q^n}$ be the finite field in which discrete logarithms are to be solved where q is a prime power. In order to represent $\mathbb{F}_{q^n}$, choose two univariate polynomials $g_1, g_2 \in \mathbb{F}_q[X]$ of degrees d_1 and d_2 respectively. Then whenever $X - g_1(g_2(X))$ possesses a degree n irreducible factor $F \in \mathbb{F}_q[X]$, one can represent $\mathbb{F}_{q^n}$ in two related ways. In particular, let $x \in \mathbb{F}_{q^n}$ be a solution of $F(X) = 0$, and let $y = g_2(x)$, so that by construction $x = g_1(y)$ as well. These relations give an explicit isomorphism between $\mathbb{F}_q(x)$ and $\mathbb{F}_q(y)$, both of which represent $\mathbb{F}_{q^n}$.

In the most basic version of the algorithm (which also leads to the best complexity) one chooses $d_1 \approx d_2 \approx \sqrt{n}$, and considers elements of $\mathbb{F}_{q^n}$ represented by:

$$xy + ay + bx + c\,, \quad \text{with} \quad a, b, c \in \mathbb{F}_q\,.$$

Substituting x by $g_1(y)$, and y by $g_2(x)$, we obtain the following equality in $\mathbb{F}_{q^n}$:

$$xg_2(x) + ag_2(x) + bx + c = yg_1(y) + ay + bg_1(y) + c\,. \tag{8}$$

The factor base consists simply of the degree one elements of $\mathbb{F}_q(x)$ and $\mathbb{F}_q(y)$ (i.e., evaluations of all degree one polynomials in $\mathbb{F}_q[X]$ at x and y, that is to say, $x + u$ and $y + u$ for all $u \in \mathbb{F}_q$). Then for every triple (a, b, c) for which both sides of (8) split over $\mathbb{F}_q$ (i.e., when all of its roots are in $\mathbb{F}_q$) in the factor base, one obtains a relation. Once more than $2q$ such relations have been collected, one performs a linear algebra elimination to recover the individual logarithms of the factor base elements.

4. Impact of projective polynomials on the DLP ([**F**] and [**J**])

Let $q = p^l$. In [**F**] and [**J**] we showcase algorithms when $p = 2$ since it is the fastest case. Here, we also set $p = 2$, but remark that the odd characteristic case can be handled after some minor changes.

Note that the probability of an arbitrary degree d_2 polynomial g_2 over $\mathbb{F}_q[X]$ splits over $\mathbb{F}_q$ is $1/(d_2+1)!$. If we choose $g_2(X) = X^{p^k}$, the left hand side of Eq (8) becomes

$$X^{p^k+1} + aX^{p^k} + bX + c,$$

(that is to say, a p^k-projective polynomial) evaluated at x. Recall that $X \mapsto X + a$ converts the above polynomial to

$$X^{p^k+1} + b'X + c',$$

which can be then converted to the form $X^{p^k+1} + \epsilon X + B$ where $\epsilon \in \{0, 1\}$. Theorem 1.9 shows that the probability that

$$P_B(X) = X^{p^{k+1}} + X + B \in \mathbb{F}_q[X]$$

splits over $\mathbb{F}_q$ is approximately $1/p^{3k}$ when $k|l$. When $l \geq 3k$ such B exists and this probability is much higher than $1/(p^k + 1)!$.

REMARK 16.4. Recall that when $k|l$, a p^k-projective polynomial $f \in \mathbb{F}_{p^l}[X]$ has $0, 1, 2$ or $p^k + 1$ $\mathbb{F}_{p^l}$-roots by Lemma 1.6 of Chapter 1. The projective polynomial f has $p^k + 1$ $\mathbb{F}_{p^l}$-roots if and only if $f \sim_{\mathfrak{M}} X^{p^k} - X$ (cf. [**E**, Lemma III.4]).

Assume for now $n = p^k \pm 1$. If we choose $g_1(X) = \gamma X^{\mp 1}$ then as $g_2(X) = X^{p^k}$, we obtain the polynomials $F(X) = X^{p^k \pm 1} + \gamma$. Furthermore, if $k \mid l$ then $X^{p^k \pm 1} + \gamma$ is irreducible whenever γ has no roots of prime order dividing $(p^k \pm 1)$. In both cases, the right hand side of Eq. (8) has degree two and splits with probability 1/2.

REMARK 16.5. The assumption $n = p^k \pm 1$ is quite restrictive. In the original papers, we employ a *heuristic* method which *empirically* works for arbitrary extension degrees $n \le p^k$. We choose k as large as possible such that $k|l$ and $l \ge 3k$ (by possibly embedding the original finite field $\mathbb{F}_{p^{ln}}$ where we seek discrete logarithms in a slightly larger extension field); and set d_1 as small as possible with g_1 satisfying the condition that $X - g_1(X^{p^k})$ contains a degree n irreducible factor. Experimentally, when $p = 2$, setting $d_1 = 3$ (or $d_1 = 4$) seems to be sufficient to produce an irreducible polynomial of any chosen degree $n \le 2^k$ which potentially can be as high as $n \approx 2^k \cdot d_1$. Although one prefers a heuristic-free algorithm, having such an assumption is standard in index calculus methods throughout its history [**84, 82**]. We explain here the most natural choice $n = p^k \pm 1$ which are called **Kummer extensions** and produce optimal (and rigorous, i.e., heuristic-free) results. The generic results in our original papers will be remarked and cited whenever necessary.

4.1. Relation generation via projective polynomials. Now we explain the polynomial time relation generation algorithm for the even characteristic case $p = 2$, $q = 2^l$, $n = 2^k - 1$, $l \ge 3k$ and $k|l$. This is the setting of [**J**]. We have $g_2(X) = X^{2^k}$ and $g_1(X) = \gamma X$ as above.

Let $B \in \mathbb{F}_q^\times$ be an element such that $P_B(X)$ splits (such B can easily be generated, see [**F**, Section 3.1]) and denote its roots by μ_i for $1 \le i \le 2^k + 1$. For arbitrary $a, b \in \mathbb{F}_q$ (with $a^{2^k} \neq b$) there exists $c \in \mathbb{F}_q$ with $(a^{2^k} + b)^{2^k+1} = B\,(ab + c)^{2^k}$ and we then find that

$$f(X) = P_B\Big(\frac{ab + c}{a^{2^k} + b}\,X + a\Big) = X^{2^k+1} + aX^{2^k} + bX + c$$

and that $f(X)$ also splits over $\mathbb{F}_q$, with roots $\nu_i = \frac{ab+c}{a^{2^k}+b}\,\mu_i + a$.

Now by the definition of $\mathbb{F}_{q^n}$ we have $x^n = \gamma$ and thus $x^{2^k} = \gamma x$, with $\gamma \in \mathbb{F}_q$. Hence in $\mathbb{F}_{q^n}$ we have

$$f(x) = \gamma x^2 + a\gamma x + bx + c = \gamma(x^2 + (a + \tfrac{b}{\gamma})x + \tfrac{c}{\gamma}) = \gamma g(x)\,,$$

where $g(X) = X^2 + (a + \frac{b}{\gamma})X + \frac{c}{\gamma}$. Hence, if the polynomial $g(X)$ splits, i.e., if $g(X) = (X + \xi_1)(X + \xi_2)$, which heuristically occurs with probability 1/2, then we find a relation of factor base elements, namely

$$\prod_{i=1}^{2^k+1} (x + \nu_i) = \gamma(x + \xi_1)(x + \xi_2)\,.$$

Such a relation corresponds to a linear relation between the logarithms of the factor base elements. Once we have found more relations than the cardinality of the factor base we can solve the discrete logarithms of the factor base elements by means of linear algebra.

Remark 16.6. We show in [**F**, Section 3.3] that this approach using a generic g_1 (as explained in Remark 16.5) gives a heuristic polynomial time relation generation algorithm for the index calculus method (see [**F**, Heuristic Result 1] for details).

4.2. Degree two elimination via projective polynomials. Recall that Part (iii) of Method 16.1 progressively writes a high degree element of $\mathbb{F}_{q^n}$ as products of lower degree elements iteratively until it is written completely as degree one (i.e., factor base) elements. In [**F, J**], given an element $h \in \mathbb{F}_{q^n}$ considered as a degree n' polynomial in $\mathbb{F}_q[X]$ evaluated at x, we use classical *descent* techniques to write h as a product of lower degree elements down to degree two elements (see [**F**, Section 4] and [**J**, Section 2.4]). Our original contribution of [**F**] regarding descent is the degree two elimination technique based on projective polynomials explained below.

Given a polynomial $Q(X) = X^2 + q_1X + q_0 \in \mathbb{F}_{q^k}[X]$ we aim at expressing the corresponding finite field element $Q(x) \in \mathbb{F}_{q^n}$ as a product of factor base elements. In essence, what we do is just the reverse of the degree one relation generation, with the polynomial $g(X)$ set to be $Q(X)$.

In particular, we compute (when possible) $a, b, c \in \mathbb{F}_q$ such that, up to a multiplicative constant in $\mathbb{F}_q^\times$, $Q(x) = x^2 + q_1x + q_0$ equals $x^{2^k+1} + ax^{2^k} + bx + c$ where the polynomial $X^{2^k+1} + aX^{2^k} + bX + c$ splits into linear factors.

As $x^n = \gamma$ holds, we have $x^{2^k+1} + ax^{2^k} + bx + c = \gamma(x^2 + (a + \frac{b}{\gamma})x + \frac{c}{\gamma})$ and comparing coefficients we find $\gamma q_0 = c$ and $\gamma q_1 = \gamma a + b$. Now letting $B \in \mathbb{F}_q^\times$ be an element satisfying the splitting property and combining the previous equations with $(a^{2^k} + b)^{2^k+1} = B\,(ab + c)^{2^k}$ we arrive at the condition

$$(a^{2^k} + \gamma a + \gamma q_1)^{2^k+1} + B(\gamma a^2 + \gamma q_1 a + \gamma q_0)^{2^k} = 0\,.$$

Considering $\mathbb{F}_q$ as a degree l/k extension over $\mathbb{F}_{2^k}$ this equation gives a quadratic system (in the sense of algebraic degree) in the l/k $\mathbb{F}_{2^k}$-components of a, which can be solved efficiently by a Gröbner basis method (cf. [**75**, Chapter 11]).

Heuristically, for each of the above B's the probability of success of this method, i.e., when an $a \in \mathbb{F}_{q^k}$ as above exists, is 1/2. Choosing different B's until a successful descent is possible heuristically with an overwhelming probability whenever $l/k > 3$.

Remark 16.7. In [**J**, Section 2.2] we explain how the choice of g_1, g_2 as above leads to a dramatic reduction on the size of the factor base via Galois automorphisms. Note that the complexity of the "Linear algebra" step of the index calculus method depends primarily on the size of the factor base. Moreover, our selection of g_1, g_2 also leads to computationally efficient data structures and algorithms. These are explained in [**J**, Section 3.3] and [**F**, Section 3].

Remark 16.8. In [**F**, Heuristic Result 2 (i) and (ii)] we prove that these arguments lead to an $L_{q^n}(1/3, (2/3)^{2/3})$ algorithm where q^n satisfies [**F**, Eq. (5), p. 117] which means q is "small" compared to q^n. Similarly, in [**J**, Section 5] we prove that the algorithm can be modified to give an $L_{q^n}(1/4)$ algorithm where

$$L_Q(a,c) = \exp\left((c+o(1))\,(\log Q)^a(\log\log Q)^{1-a}\right)$$

is used to measure running times of sub-exponential algorithms for $0 < \alpha < 1$. Note that $\alpha = 0$ is polynomial and $\alpha = 1$ is exponential. Note also that the parameter α is more significant than the parameter c which is sometimes even omitted.

The "smallness" of the prime p is also described by the L-notation. Let $p = L_{p^n}(\alpha)$. Then p is said to be (i) small if $\alpha \leq 1/3$, (ii) medium if $1/3 \leq \alpha \leq 2/3$, and (iii) large (high-characteristic) if $\alpha \geq 2/3$ (see [**82**, Section 4.1] for details such as the explanation for the overlap in the boundary cases).

Remark 16.9 (Record breaking DLP computations). We broke two records for discrete logarithm computations on characteristic two fields of order 2^{1971} and 2^{6120} [**58, 59**]. The first article [**F**] that broke the first record received the prestigious "Best Paper Award" at the conference CRYPTO (August 2013).

Similar algorithms were given by Joux [**76, 77**] independently, also breaking DLP records [**78, 79, 80**] during the same four-month period February—May 2013.

In [**10**], the first heuristic quasi-polynomial algorithm ($n^{\mathcal{O}(\log n)}$) was given by Barbulescu et al., substantially improving upon the $L(1/4)$ algorithms. In [**66**], the degree two elimination method of [**F**] is generalized by Granger et al. to the so-called "ZigZag descent," to give another quasi-polynomial algorithm with fewer heuristic assumptions.

5. A rigorous degree two elimination analysis for quasi-polynomial DLP ([G])

In [**G**] we give a quasi-polynomial algorithm using a new degree two elimination step and a slightly modified ZigZag strategy of [**66**]. This algorithm accounts for a simpler and tighter analysis of quasi-polynomial DLP computations in small characteristic fields $\mathbb{F}_{q^{k_0 k}}$ where k is close to q and k_0 is a small integer.

5.1. The setting. Let q be a prime power, $Q_0 = q^{k_0}$ a (small) power of q; h_0 and h_1 two polynomials of degree at most 2 with coefficients in $\mathbb{F}_{Q_0}$. Assume that the polynomial $h_1(X)X^q - h_0(X)$ has an irreducible factor I_k of degree k. (Computational evidence suggests that degree 2 should be enough to construct all finite fields with k up to $q+2$, however this remains heuristic.) Then, this irreducible polynomial can be used to represent $\mathbb{F}_{Q_0^k}$ as $\mathbb{F}_{Q_0}[X]/(I_k)$. Moreover, if θ denotes a root of I_k in the algebraic closure of $\mathbb{F}_q$ we see that:

$$\theta^q = \frac{h_0(\theta)}{h_1(\theta)}.$$

Since, θ^q is the image of θ by the Frobenius map, this representation is named **Frobenius representation** [**83**]. Let θ be a fixed root of I_k.

We want to find the discrete logarithm $\log_g h$ where $h \in \mathbb{F}^{\times}_{Q_0^k} = \langle g \rangle$. The following method is the main algorithmic contribution of [**G**, Theorem 3] which has quasi-polynomial complexity.

Method 16.10. Let l be such that $2^l \geq k > 2^{l-1}$.

(i) Let $h^r g^s = R(\theta)$ for an irreducible $R \in \mathbb{F}_{Q_0}[X]$ where $\operatorname{pdeg} R = 2^l$, and for r, s chosen uniformly at random. Such R can be found using linear algebra [**G**, p. 2487].

(ii) We have for some $\alpha \in \mathbb{F}_{Q_0^{2^l}}$,

$$\begin{aligned} R(X) &= \prod_{i=0}^{2^l-1} (X - \alpha^{Q_0^i}) \\ &= \prod_{i=0}^{2^{l-1}-1} (X - \alpha^{Q_0^i})(X - \alpha^{QQ_0^i}) \\ &= \prod_{i=0}^{2^{l-1}-1} (X^2 - \operatorname{Tr}(\alpha^{Q_0^i})X + \operatorname{Nm}(\alpha^{Q_0^i})) \end{aligned}$$

where $Q = Q_0^{2^{l-1}}$ and Tr and Nm denote the trace and norm from $\mathbb{F}_{Q_0^{2^l}}$ to $\mathbb{F}_{Q_0^{2^{l-1}}}$.

(iii) Now we have 2^l quadratic polynomials $S_i \in \mathbb{F}_{Q_0^{2^{l-1}}}[X]$ where

$$S_i(X) = X^2 - \operatorname{Tr}(\alpha^{Q_0^i})X + \operatorname{Nm}(\alpha^{Q_0^i})$$

for $0 \le i \le 2^l - 1$. We eliminate S_0 using the descent method explained in [**G**, Section 4] (see Remark 16.11 below) which writes S_0 as a product of $q+3$ linear polynomials $X - \beta_j \in \mathbb{F}_{Q_0^{2^{l-1}}}[X]$ and some additional polynomials denoted by $\mathcal{E}$ (see [**G**, p. 2487]). For $1 \le i \le 2^l - 1$, elimination of S_i is now implicitly done since all S_i are related via Galois automorphisms as shown in [**G**, Section 3, p. 2488]. In particular, for all $X - \beta_j$ that appears in the product, we have $X - \beta_j^{\sqrt{Q}}$ appearing in the product as well. Thus $R(X)$ is now written as a product of $q+3$ quadratic polynomials from $\mathbb{F}_{Q_0^{2^{l-2}}}[X]$ and their Galois conjugates.

(iv) Now eliminate those $q+3$ quadratic polynomials over $\mathbb{F}_{Q_0^{2^{l-2}}}[X]$ to get $(q+3)^2$ quadratic polynomials over $\mathbb{F}_{Q_0^{2^{l-3}}}[X]$ and their Galois conjugates whose elimination data is just copied from the original similarly as in Part (iii), and some additional polynomials from $\mathcal{E}$.

(v) Continue this process until we reduce all to the factor base elements which correspond to $X - \gamma$ where $\gamma \in \mathbb{F}_{Q_0}$ and some additional polynomials denoted by $\mathcal{E}$. In total we would have eliminated $(q+3)^{\lceil \log_2 k \rceil}$ quadratic polynomials.

(vi) We show in [**G**, Lemma 6], that the above degree two elimination can be done for one quadratic polynomial in $\mathcal{O}(q^4)$ arithmetic operations in the relevant field.

(vii) Repeating the process of writing $h^r g^s$ as a product of factor base elements for randomly selected r, s more than $Q_0 + q^2 + q + 7$ (the cardinality of the factor base) times, we can find the logarithm of h using the linear algebra technique from [4] which requires Q_0^3 arithmetic operations (see [**G**, p. 2489].

(viii) Thus the total complexity of the algorithm is

$$\mathcal{O}((q+3)^{\lceil \log_2 k \rceil} q^{4+k_0} + q^{3k_0})$$

finite field operations (see [**G**, Theorem 3]).

Remark 16.11 (Descent as the solution of a finite field equation). The main mathematical contribution of [**G**] is as follows.

(i) We prove that degree two descent for a quadratic polynomial $f \in \mathbb{F}_Q[X]$ can be done if f divides

$$F = (a_0 + a_1X)\,(b_0^q\,h_1(X) + b_1^q\,h_0(X)) - (b_0 + b_1X)\,(a_0^q\,h_1(X) + a_1^q\,h_0(X))\,,$$

for some (nontrivial choices of) $a_0, a_1, b_0, b_1 \in \mathbb{F}_Q$.

(ii) We convert this condition to a finite field equality [**G**, Theorem 5 and Lemma 6], and show that it is possible for every choice of f that this equality holds. We prove the following assertion: For any $a \in \mathbb{F}_Q^\times$, the equation

$$\left(\frac{X^q - X^Q}{X^q - X}\right)^{Q+1} = a$$

has a solution $X \in \mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$ (see [**G**, Lemma 6] for details on Q and q).

(iii) We explain in [**G**, Sections 4 and 5] how the existence of such X for a given a is in correspondence with the degree two descent of some f (other than some exceptions).

(iv) In [**G**, p. 2495] we show that the degree two elimination can be done in $\mathcal{O}(q^4)$ arithmetic operations.

(v) The proof of [**G**, Theorem 5 and Lemma 6, pp. 2491–2496] is rather involved. See the original paper for details.

Remark 16.12. Quite recently, in [**98, 116**] rigorous (heuristic-free) quasi-polynomial time algorithms for solving discrete logarithms on fixed prime finite fields were given using the so-called elliptic representation of finite fields. The current record DLP computation is in the binary finite field of order 2^{30750} by Granger et al. [**65**] at the time of writing.

CHAPTER 17

Conclusion

We list here the three most important open problems that cover every subject matter of the thesis.

(i) **Finite semifields:**

Problem 17.1 (Kantor's conjecture). Show that the number of pairwise non-isotopic semifields of odd order Q is super-polynomial (i.e., not bounded by a polynomial) in Q.

A stronger version of the conjecture states that the number is exponential in Q. This should be solved for the even characteristic case as well since the current number there is super-polynomial (but not exponential) in Q.

(ii) **Highly nonlinear functions/cryptographic permutations:**

Problem 17.2 (The big APN problem). Find (a family of) APN permutations on even degree extensions $\mathbb{F}_2^n$ where $n > 6$.

(iii) **Discrete logarithm problem:**

Problem 17.3. Give a polynomial time DLP-algorithm for small characteristic finite fields and quasi-polynomial time algorithms for medium and high characteristic finite fields.

Bibliography

[A] F. Göloğlu and L. Kölsch, *An exponential bound on the number of non-isotopic commutative semifields*, Trans. Amer. Math. Soc. **376(3)** (2023), 1683–1716. DOI:10.1090/tran/8785

[B] F. Göloğlu, *Biprojective almost perfect nonlinear functions*, IEEE Trans. Inform. Theory **68** (2022), no. 7, 4750–4760. DOI:10.1109/TIT.2022.3157798 MR 4449070

[C] F. Göloğlu and L. Kölsch, *Equivalences of biprojective almost perfect nonlinear functions*, J. Comb. Th. A (submitted) (2021), 26 pages. arXiv:2111.04197. DOI:10.48550/arXiv.2111.04197

[D] F. Göloğlu, *Classification of fractional projective permutations over finite fields*, Finite Fields Appl. **81** (2022), Paper No. 102027, 50 pages. DOI:10.1016/j.ffa.2022.102027 MR 4397755

[E] F. Göloğlu, *Classification of (q, q)-biprojective APN functions*, IEEE Trans. Inform. Theory **69** (2022), no. 3, 1988–1999. DOI:10.1109/TIT.2022.3220724

[F] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities: application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$*, Advances in cryptology—CRYPTO 2013. Part II, Lecture Notes in Comput. Sci., vol. 8043, Springer, Heidelberg, 2013, pp. 109–128. DOI:10.1007/978-3-642-40084-1_7 MR 3126472

[G] F. Göloğlu and A. Joux, *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, Math. Comp. **88** (2019), no. 319, 2485–2496. DOI:10.1090/mcom/3404 MR 3957902

[H] F. Göloğlu and Ph. Langevin, *Almost perfect nonlinear families which are not equivalent to permutations*, Finite Fields Appl. **67** (2020), Paper No. 101707, 21 pages. DOI:10.1016/j.ffa.2020.101707 MR 4122629

[J] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *Solving a 6120-bit DLP on a desktop computer*, Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers (Tanja Lange, Kristin E. Lauter, and Petr Lisonek, eds.), Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 136–152. DOI:10.1007/978-3-662-43414-7_7

[K] F. Göloğlu and L. Kölsch, *Counting the number of non-isotopic Taniguchi semifields*, Des. Codes Crypt. (submitted) (2022), 13 pages. arXiv:2207.13497. DOI:10.48550/arXiv.2207.13497

---

[1] Shreeram S. Abhyankar. Galois theory on the line in nonzero characteristic. *Bull. Amer. Math. Soc. (N.S.)*, 27(1):68–133, 1992.

[2] Shreeram S. Abhyankar. Projective polynomials. *Proc. Amer. Math. Soc.*, 125(6):1643–1650, 1997.

[3] Shreeram S. Abhyankar. Galois theory of special trinomials. In *Proceedings of the International Conference on Algebraic Geometry and Singularities (Spanish) (Sevilla, 2001)*, volume 19, pages 265–286, 2003.

[4] Leonard M. Adleman and Jonathan DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Math. Comp.*, 61(203):1–15, 1993.

[5] A. A. Albert. On the collineation groups associated with twisted fields. In *Calcutta Math. Soc. Golden Jubilee Commemoration Vol. (1958/59), Part II*, pages 485–497. Calcutta Math. Soc., Calcutta, 1958/1959.

[6] A. A. Albert. Finite division algebras and finite planes. In *Proc. Sympos. Appl. Math., Vol. 10*, pages 53–70. American Mathematical Society, Providence, R.I., 1960.

[7] A. A. Albert. Generalized twisted fields. *Pacific J. Math.*, 11:1–8, 1961.

[8] A. A. Albert. Isotopy for generalized twisted fields. *An. Acad. Brasil. Ci.*, 33:265–275, 1961.

[9] Nurdagül Anbar, Tekgül Kalaycı, and Wilfried Meidl. Determining the Walsh spectra of Taniguchi's and related APN-functions. *Finite Fields Appl.*, 60:101577, 20, 2019.

[10] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in cryptology—EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Comput. Sci.*, pages 1–16. Springer, Heidelberg, 2014.

[11] Daniele Bartoli, Jürgen Bierbrauer, Gohar Kyureghyan, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. A family of semifields in characteristic 2. *Journal of Algebraic Combinatorics*, 45(2):455–473, Mar 2017.

[12] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions over. *IEEE Trans. Inf. Theor.*, 52(9):4160–4170, September 2006.

[13] Jürgen Bierbrauer. New semifields, PN and APN functions. *Des. Codes Cryptogr.*, 54(3):189–200, 2010.

[14] Jürgen Bierbrauer. Projective polynomials, a projection construction and a family of semifields. *Des. Codes Cryptogr.*, 79(1):183–200, 2016.

[15] Jürgen Bierbrauer, Daniele Bartoli, Giorgio Faina, Stefano Marcugini, and Fernanda Pambianco. A family of semifields in odd characteristic. *Designs, Codes and Cryptography*, 86(3):611–621, Mar 2018.

[16] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[17] Mauro Biliotti, Vikram Jha, and Norman L. Johnson. The collineation groups of generalized twisted field planes. *Geom. Dedicata*, 76(1):97–126, 1999.

[18] Antonia W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields Appl.*, 10(3):285–305, 2004.

[19] Carl Bracken, Chik How Tan, and Yin Tan. On a class of quadratic polynomials with no zeros and its application to APN functions. *Finite Fields Appl.*, 25:26–36, 2014.

[20] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN permutation in dimension six. *Postproceedings of the 9th International Conference on Finite Fields and Their Applications*, 518:33–42, 2010.

[21] Lilya Budaghyan and Tor Helleseth. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. In *Sequences and their applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 403–414. Springer, Berlin, 2008.

[22] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Trans. Inform. Theory*, 66(11):7081–7087, 2020.

[23] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *IACR Cryptol. ePrint Arch.*, 2020.

[24] Marco Calderini, Kangquan Li, and Irene Villa. Two new families of bivariate APN functions. *CoRR*, abs/2204.07462, 2022.

[25] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Trans. Inform. Theory*, 63(11):7575–7591, 2017.

[26] Anne Canteaut, Léo Perrin, and Shizhu Tian. If a generalised butterfly is APN then it operates on 6 bits. *Cryptogr. Commun.*, 11(6):1147–1164, 2019.

[27] Claude Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Des. Codes Cryptogr.*, 59(1-3):89–109, 2011.

[28] Claude Carlet. More constructions of APN and differentially 4-uniform functions by concatenation. *Sci. China Math.*, 56:1373—1384, 2013.

[29] Claude Carlet. Open questions on nonlinearity and on APN functions. In *Arithmetic of finite fields*, volume 9061 of *Lecture Notes in Comput. Sci.*, pages 83–107. Springer, Cham, 2015.

[30] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 2021.

[31] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[32] L. Carlitz. Resolvents of certain linear groups in a finite field. *Canadian J. Math.*, 8:568–579, 1956.

[33] L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44(1):5–16, 1979.

[34] Benjamin Chase and Petr Lisoněk. Kim-type APN functions are affine equivalent to Gold functions. *Cryptogr. Commun.*, 13(6):981–993, 2021.

[35] Stephen D. Cohen. On irreducible polynomials of certain types in finite fields. *Proc. Cambridge Philos. Soc.*, 66:335–344, 1969.

[36] Stephen D. Cohen and Michael J. Ganley. Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra*, 75(2):373–385, 1982.

[37] M. Cordero and G. P. Wene. A survey of finite semifields. volume 208/209, pages 125–137. 1999. Combinatorics (Assisi, 1996).

[38] Robert S. Coulter and Marie Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008.

[39] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

[40] Peter Dembowski. *Finite geometries.* Classics in Mathematics. Springer-Verlag, Berlin, 1997. Reprint of the 1968 original.

[41] Peter Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.

[42] Ulrich Dempwolff. CCZ equivalence of power functions. *Des. Codes Cryptogr.*, 86(3):665–692, 2018.

[43] L. E. Dickson. Linear algebras with associativity not assumed. *Duke Math. J.*, 1(2):113–125, 1935.

[44] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6):644–654, 1976.

[45] J. F. Dillon. Geometry, codes and difference sets: exceptional connections. In *Codes and designs (Columbus, OH, 2000)*, volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 73–85. de Gruyter, Berlin, 2002.

[46] J. F. Dillon and Hans Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields Appl.*, 10(3):342–389, 2004.

[47] Cunsheng Ding and Jin Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[48] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5. In D. Jungnickel and H. Niederreiter, editors, *Proceedings of the conference on Finite Fields and Applications, Augsburg, 1999*, pages 113–121. Springer-Verlag, Berlin, 2001, 1999.

[49] Hans Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Niho case. *Inform. and Comput.*, 151(1-2):57–72, 1999.

[50] Hans Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45(4):1271–1275, 1999.

[51] Hans Dobbertin. Kasami power functions, permutation polynomials and cyclic difference sets. In *Difference sets, sequences and their correlation properties (Bad Windsheim, 1998)*, volume 542 of *NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci.*, pages 133–158. Kluwer Acad. Publ., Dordrecht, 1999.

[52] Hans Dobbertin, Patrick Felke, Tor Helleseth, and Petri Rosendahl. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Trans. Inform. Theory*, 52(2):613–627, 2006.

[53] Tao Feng and Weicong Li. On the isotopism classes of the Budaghyan-Helleseth commutative semifields. *Finite Fields Appl.*, 53:175–188, 2018.

[54] P. Flajolet, X. Gourdon, and D. Panario. The complete analysis of a polynomial factorization algorithm over finite fields. *J. Algorithms*, 40(1):37–81, 2001.

[55] Michael J. Ganley. Central weak nucleus semifields. *European J. Combin.*, 2(4):339–347, 1981.

[56] Theodoulos Garefalakis. On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$. *J. Pure Appl. Algebra*, 215(8):1835–1843, 2011.

[57] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Inf. Th.*, 14:377–385, 1968.

[58] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Discrete Logarithms in $GF(2^{1971})$. NMBRTHRY list, 19 Feb 2013.

[59] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Discrete Logarithms in $GF(2^{6120})$. NMBRTHRY list, 11 Apr 2013.

[60] Faruk Göloğlu, Dasa Krasnayova, and Petr Lisonek. Generalized Kim APN functions are not equivalent to permutations, 2020. preprint.

[61] Faruk Göloğlu and Jiří Pavlů. On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations. *Cryptogr. Commun.*, 13(3):377–391, 2021.

[62] Rod Gow and Gary McGuire. Invariant rational functions, linear fractional transformations and irreducible polynomials over finite fields. *Finite Fields Appl.*, 79:Paper No. 101991, 25, 2022.

[63] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[64] Robert Granger and Antoine Joux. Computing discrete logarithms. In *Computational cryptography—algorithmic aspects of cryptology*, volume 469 of *London Math. Soc. Lecture Note Ser.*, pages 106–139. Cambridge Univ. Press, Cambridge, 2021.

[65] Robert Granger, Thorsten Kleinjung, Arjen Lenstra, Benjamin Wesolowski, and Jens Zumbrägel. Discrete Logarithms in $GF(2^{30750})$. NMBRTHRY list, 10 Jul 2019.

[66] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. *Trans. Amer. Math. Soc.*, 370(5):3129–3145, 2018.

[67] Marshall Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[68] Tor Helleseth and Alexander Kholosha. On the equation $x^{2^l+1}+x+a=0$ over $\mathrm{GF}(2^k)$. *Finite Fields Appl.*, 14(1):159–176, 2008.

[69] Tor Helleseth and Alexander Kholosha. $x^{2^l+1}+x+a$ and related affine polynomials over $\mathrm{GF}(2^k)$. *Cryptogr. Commun.*, 2(1):85–109, 2010.

[70] Yutaka Hiramine, Makoto Matsumoto, and Tuyosi Oyama. On some extension of 1-spread sets. *Osaka J. Math.*, 24(1):123–137, 1987.

[71] Daniel R. Hughes and Erwin Kleinfeld. Seminuclear extensions of Galois fields. *Amer. J. Math.*, 82:389–392, 1960.

[72] Daniel R. Hughes and Fred C. Piper. *Projective planes*. Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

[73] Vikram Jha and Norman L. Johnson. An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem. *Algebras Groups Geom.*, 6(1):1–35, 1989.

[74] Norman L. Johnson, Giuseppe Marino, Olga Polverino, and Rocco Trombetti. On a generalization of cyclic semifields. *J. Algebraic Combin.*, 29(1):1–34, 2009.

[75] Antoine Joux. *Algorithmic cryptanalysis*. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, 2009.

[76] Antoine Joux. Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In *Advances in cryptology—EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Comput. Sci.*, pages 177–193. Springer, Heidelberg, 2013.

[77] Antoine Joux. A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic. In *Selected areas in cryptography—SAC 2013*, volume 8282 of *Lecture Notes in Comput. Sci.*, pages 355–379. Springer, Heidelberg, 2014.

[78] Antoine Joux. Discrete Logarithms in $GF(2^{1778})$. NMBRTHRY list, 11 Feb 2013.

[79] Antoine Joux. Discrete Logarithms in $GF(2^{4080})$. NMBRTHRY list, 22 Mar 2013.

[80] Antoine Joux. Discrete Logarithms in $GF(2^{6168})$. NMBRTHRY list, 21 May 2013.

[81] Antoine Joux and Reynald Lercier. The function field sieve in the medium prime case. In *Advances in cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, pages 254–270. Springer, Berlin, 2006.

[82] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot. The past, evolving present, and future of the discrete logarithm. In *Open problems in mathematics and computational science*, pages 5–36. Springer, Cham, 2014.

[83] Antoine Joux and Cécile Pierrot. Improving the polynomial time precomputation of Frobenius representation discrete logarithm algorithms: simplified setting for small characteristic finite fields. In

Advances in cryptology—ASIACRYPT 2014. Part I, volume 8873 of *Lecture Notes in Comput. Sci.*, pages 378–397. Springer, Heidelberg, 2014.

[84] Antoine Joux and Cécile Pierrot. Technical history of discrete logarithms in small characteristic finite fields: the road from subexponential to quasi-polynomial complexity. *Des. Codes Cryptogr.*, 78(1):73–85, 2016.

[85] William M. Kantor. Commutative semifields and symplectic spreads. *J. Algebra*, 270(1):96–114, 2003.

[86] William M. Kantor. Finite semifields. In *Finite geometries, groups, and computation*, pages 103–114. Walter de Gruyter, Berlin, 2006.

[87] William M. Kantor. HMO-planes. *Adv. Geom.*, 9(1):31–43, 2009.

[88] William M. Kantor and Robert A. Liebler. Semifields arising from irreducible semilinear transformations. *J. Aust. Math. Soc.*, 85(3):333–339, 2008.

[89] William M. Kantor and Michael E. Williams. Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Trans. Amer. Math. Soc.*, 356(3):895–938, 2004.

[90] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[91] Christian Kaspers. *Equivalence problems of almost perfect nonlinear functions and disjoint difference families.* PhD thesis, Otto-von-Guericke-Universität Magdeburg, Fakultät für Mathematik, 2021.

[92] Christian Kaspers and Yue Zhou. The number of almost perfect nonlinear functions grows exponentially. *Journal of Cryptology*, 34(1):4, Jan 2021.

[93] Christian Kaspers and Yue Zhou. A lower bound on the number of inequivalent APN functions. *Journal of Combinatorial Theory, Series A*, 186:105554, 2022.

[94] Kwang Ho Kim, Jong Hyok Choe, and Sihem Mesnager. Complete solution over $\mathbb{F}_{p^n}$ of the equation $X^{p^k+1} + X + a = 0$. *Finite Fields Appl.*, 76:Paper No. 101902, 13, 2021.

[95] Kwang Ho Kim, Junyop Choe, and Sihem Mesnager. Solving $X^{q+1} + X + a = 0$ over finite fields. *Finite Fields Appl.*, 70:Paper No. 101797, 16, 2021.

[96] Kwang Ho Kim and Sihem Mesnager. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$. *Finite Fields Appl.*, 63:101630, 15, 2020.

[97] Kwang Ho Kim, Sihem Mesnager, Jong Hyok Choe, Dok Nam Lee, Sengsan Lee, and Myong Chol Jo. On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. *Des. Codes Cryptogr.*, 90(6):1437–1461, 2022.

[98] Thorsten Kleinjung and Benjamin Wesolowski. Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic. *J. Amer. Math. Soc.*, 35(2):581–624, 2022.

[99] Lars R. Knudsen and Matthew Robshaw. *The Block Cipher Companion.* Information Security and Cryptography. Springer, 2011.

[100] Donald E. Knuth. A class of projective planes. *Trans. Amer. Math. Soc.*, 115:541–549, 1965.

[101] Donald E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2:182–217, 1965.

[102] Lukas Kölsch, Björn Kriepke, and Gohar M. Kyureghyan. Image sets of perfectly nonlinear maps. arXiv 2012.00870, 2021.

[103] Dasa Krasnayova. Constructions of APN permutations. Master's thesis, Charles University, Prague, 2016.

[104] Gohar M. Kyureghyan. Special mappings of finite fields. In *Finite fields and their applications*, volume 11 of *Radon Ser. Comput. Appl. Math.*, pages 117–144. De Gruyter, Berlin, 2013.

[105] Gohar M. Kyureghyan and Alexander Pott. Some theorems on planar mappings. In *Arithmetic of finite fields*, volume 5130 of *Lecture Notes in Comput. Sci.*, pages 117–122. Springer, Berlin, 2008.

[106] Brian A. LaMacchia and Andrew M. Odlyzko. Solving large sparse linear systems over finite fields. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 109–133. Springer, 1990.

[107] Michel Lavrauw and John Sheekey. Semifields from skew polynomial rings. *Adv. Geom.*, 13(4):583–604, 2013.

[108] Lavrauw, Michel and Polverino, Olga. Finite semifields. In Storme, Leo and De Beule, Jan, editor, *Current research topics in Galois geometry*, Mathematics Research Developments, pages 127–155. Nova Science, 2011.

[109] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. A complete characterization of the APN property of a class of quadrinomials. *IEEE Trans. Inform. Theory*, 67(11):7535–7549, 2021.

[110] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. Cryptographically strong permutations from the butterfly structure. *Des. Codes Cryptogr.*, 89(4):737–761, 2021.

[111] Kangquan Li, Longjiang Qu, Chao Li, and Hao Chen. On a conjecture about a class of permutation quadrinomials. *Finite Fields Appl.*, 66:101690, 20, 2020.

[112] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic APN functions. *IEEE Transactions on Information Theory*, pages 1–1, 2022.

[113] Nian Li, Zhao Hu, Maosheng Xiong, and Xiangyong Zeng. A note on “Cryptographically strong permutations from the butterfly structure”. *Des. Codes Cryptogr.*, 90(2):265–276, 2022.

[114] Nian Li, Maosheng Xiong, and Xiangyong Zeng. On permutation quadrinomials and 4-uniform BCT. *IEEE Trans. Inform. Theory*, 67(7):4845–4855, 2021.

[115] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1997.

[116] Guido Lido. A provably quasi-polynomial algorithm for the discrete logarithm problem in finite fields of small characteristic, 2022.

[117] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. Symplectic semifield spreads of PG$(5, q)$ and the Veronese surface. *Ric. Mat.*, 60(1):125–142, 2011.

[118] Giuseppe Marino and Olga Polverino. On the nuclei of a finite semifield. In *Theory and applications of finite fields*, volume 579 of *Contemp. Math.*, pages 123–141. Amer. Math. Soc., Providence, RI, 2012.

[119] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields Appl.*, 57:68–91, 2019.

[120] Giampaolo Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[121] Gary L. Mullen, editor. *Handbook of finite fields*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2013.

[122] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT ’93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 55–64. Springer, Berlin, 1994.

[123] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 111–130. Springer, 1994.

[124] Andrew Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Advances in cryptology (Paris, 1984)*, volume 209 of *Lecture Notes in Comput. Sci.*, pages 224–314. Springer, Berlin, 1985.

[125] Andrew Odlyzko. Discrete logarithms: the past and the future. *Des. Codes Cryptogr.*, 19(2-3):129–145, 2000. Towards a quarter-century of public key cryptography.

[126] Tim Penttila and Blair Williams. Ovoids of parabolic spaces. *Geom. Dedicata*, 82(1-3):1–19, 2000.

[127] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem. In *Advances in cryptology—CRYPTO 2016. Part II*, volume 9815 of *Lecture Notes in Comput. Sci.*, pages 93–122. Springer, Berlin, 2016.

[128] Alexander Pott. Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1):141–195, 2016.

[129] Alexander Pott, Kai-Uwe Schmidt, and Yue Zhou. Semifields, relative difference sets, and bent functions. In *Algebraic curves and finite fields*, pages 161–178. De Gruyter, 2014.

[130] William Purpura. Counting the generalized twisted fields. *Note Mat.*, 27(1):53–59, 2007.

[131] Reuben Sandler. Autotopism groups of some finite non-associative algebras. *Amer. J. Math.*, 84:239–264, 1962.

[132] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[133] John Sheekey. MRD codes: Constructions and connections. In *Combinatorics and Finite Fields*, pages 255–286. de Gruyter, 2019.

[134] Henning Stichtenoth and Alev Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18(1):108–122, 2012.

[135] P. Sziklai. On subsets of $\mathrm{GF}(q^2)$ with dth power differences. *Discrete Math.*, 208/209:547–555, 1999. Combinatorics (Assisi, 1996).

[136] Hiroaki Taniguchi. On some quadratic APN functions. *Des. Codes Cryptogr.*, 87(9):1973–1983, 2019.

[137] Ziran Tu, Nian Li, Xiangyong Zeng, and Junchao Zhou. A class of quadrinomial permutations with boomerang uniformity four. *IEEE Trans. Inform. Theory*, 66(6):3753–3765, 2020.

[138] Ziran Tu, Xianping Liu, and Xiangyong Zeng. A revisit to a class of permutation quadrinomials. *Finite Fields Appl.*, 59:57–85, 2019.

[139] Ziran Tu, Xiangyong Zeng, and Tor Helleseth. New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$. *Finite Fields Appl.*, 50:304–318, 2018.

[140] Oswald Veblen and John Wesley Young. *Projective geometry. Vol. 1.* Blaisdell Publishing Co. [Ginn and Co.], New York-Toronto-London, 1965.

[141] Joachim von zur Gathen, Mark Giesbrecht, and Konstantin Ziegler. Composition collisions and projective polynomials. In *ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 123–130. ACM, New York, 2010.

[142] Guobiao Weng and Xiangyong Zeng. Further results on planar DO functions and commutative semifields. *Des. Codes Cryptogr.*, 63(3):413–423, 2012.

[143] Yanan Wu, Lisha Wang, Nian Li, Xiangyong Zeng, and Xiaohu Tang. On the boomerang uniformity of a class of permutation quadrinomials over finite fields. *Discrete Math.*, 345(10):Paper No. 113000, 14, 2022.

[144] Satoshi Yoshiara. Equivalences of quadratic APN functions. *J. Algebraic Comb.*, 35(3):461–475, May 2012.

[145] Satoshi Yoshiara. Equivalences of power APN functions with power or quadratic APN functions. *J. Algebraic Combin.*, 44(3):561–585, 2016.

[146] Zhengbang Zha, Gohar M. Kyureghyan, and Xueli Wang. Perfect nonlinear binomials and their semifields. *Finite Fields Appl.*, 15(2):125–133, 2009.

[147] Zhengbang Zha and Xueli Wang. New families of perfect nonlinear polynomial functions. *J. Algebra*, 322(11):3912–3918, 2009.

[148] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Adv. Math.*, 234:43–60, 2013.

Part 2

Publications

CHAPTER 18

An exponential bound on the number of non-isotopic commutative semifields

F. Göloğlu and L. Kölsch, *An exponential bound on the number of non-isotopic commutative semifields*, Trans. Amer. Math. Soc. **376(3)** (2023), 1683–1716.

DOI:10.1090/tran/8785

CHAPTER 19

Biprojective almost perfect nonlinear functions

F. Göloğlu, *Biprojective almost perfect nonlinear functions*, IEEE Trans. Inform. Theory **68** (2022), no. 7, 4750–4760.

DOI:10.1109/TIT.2022.3157798 MR 4449070

CHAPTER 20

Equivalences of biprojective almost perfect nonlinear functions

F. Göloğlu and L. Kölsch, *Equivalences of biprojective almost perfect nonlinear functions*, J. Comb. Th. A (submitted) (2021), 26 pages. arXiv:2111.04197.

DOI:10.48550/arXiv.2111.04197

CHAPTER 21

Classification of fractional projective permutations over finite fields

F. Göloğlu, *Classification of fractional projective permutations over finite fields*, Finite Fields Appl. **81** (2022), Paper No. 102027, 50 pages.

DOI:10.1016/j.ffa.2022.102027 MR 4397755

CHAPTER 22

Classification of (q, q)-biprojective APN functions

F. Göloğlu, *Classification of* (q, q)*-biprojective APN functions*, IEEE Trans. Inform. Theory **69** (2022), no. 3, 1988–1999.

DOI:10.1109/TIT.2022.3220724

CHAPTER 23

On the function field sieve and the impact of higher splitting probabilities: application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$

F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities: application to discrete logarithms in* $\mathbb{F}_{2^{1971}}$ *and* $\mathbb{F}_{2^{3164}}$, Advances in cryptology—CRYPTO 2013. Part II, Lecture Notes in Comput. Sci., vol. 8043, Springer, Heidelberg, 2013, pp. 109–128.

DOI:10.1007/978-3-642-40084-1_7 MR 3126472

CHAPTER 24

A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms

F. Göloğlu and A. Joux, *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, Math. Comp. **88** (2019), no. 319, 2485–2496.

DOI:10.1090/mcom/3404 MR 3957902

CHAPTER 25

Almost perfect nonlinear families which are not equivalent to permutations

F. Göloğlu and Ph. Langevin, *Almost perfect nonlinear families which are not equivalent to permutations*, Finite Fields Appl. **67** (2020), Paper No. 101707, 21 pages.

DOI:10.1016/j.ffa.2020.101707 MR 4122629

CHAPTER 26

Solving a 6120-bit DLP on a desktop computer

F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *Solving a 6120-bit DLP on a desktop computer*, Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers (Tanja Lange, Kristin E. Lauter, and Petr Lisonek, eds.), Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 136–152.

DOI:10.1007/978-3-662-43414-7_7

CHAPTER 27

Counting the number of non-isotopic Taniguchi semifields

F. Göloğlu and L. Kölsch, *Counting the number of non-isotopic Taniguchi semifields*, Des. Codes Crypt. (submitted) (2022), 13 pages. arXiv:2207.13497.

DOI:10.48550/arXiv.2207.13497