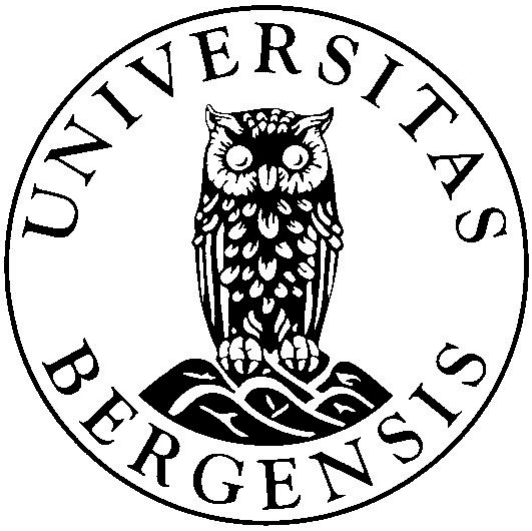
Computational search for isotopic semifields and planar functions in characteristic 3

University of Bergen



Markus Aleksander Bergmann

Supervisor: Lilya Budaghyan

Co-supervisors: Nikolay S. Kaleyski & Enrico Piccione

August 31, 2023

Abstract

In this thesis, we study vectorial functions, i.e. mappings between finite fields. Such functions correspond to objects of interest in other areas of mathematics and computer science, but one of the primary motivations for their study is that they play an important role in modern cryptography. All vectorial functions have properties that measure their resistance to cryptanalytic attacks when used as building blocks of cryptographic primitives. Therefore, it is important to find and study functions having optimal values of these properties.

This is especially true when designing block ciphers which are particularly susceptible to differential cryptanalysis, a powerful attack that was first introduced by Biham and Shamir in 1990. In the case of functions over finite fields of characteristic 2, the notion of differential uniformity was introduced by Nyberg in 1993 as a measurement of the resistance to differential attacks. However, the same notion naturally generalizes to vectorial functions over finite fields of any characteristic. We note that the notion of differential uniformity is a very natural one, and has appeared in essence in many different contexts in mathematics even before its introduction by Nyberg in the context of cryptography.

Therefore, there is a great interest in finding vectorial functions that have the best possible differential uniformity. In the case of characteristic 2, the best possible value of the differential uniformity is 2, and the functions attaining this value are called almost perfect nonlinear (APN). In the case of odd characteristic, the optimal value is 1, and the corresponding functions are called perfect nonlinear (PN) or planar. The latter class of functions is the primary subject of this thesis.

Planar functions have been shown to be connected to multiple areas of mathematical study. One of these is the study of semifields, which are objects that have received a lot of attention since their introduction in the early 20th century. Quadratic planar functions and commutative semifields in odd characteristic are in a one-to-one correspondence, and so finding new commutative semifields equates to finding new planar functions, and vice versa.

Due to the large number of vectorial functions, they are typically only considered up to some appropriate notion of equivalence. In the case of planar functions, this is typically Carlet-Charpin-Zinoviev-equivalence, or CCZ-equivalence, which is the most general known equivalence relation that preserves differential uniformity. Finding planar functions that are CCZ-inequivalent to the known ones is hard in general, and is a challenging and active area of study.

An equivalence relation called isotopism can be defined on the set of all semifields. The planar functions corresponding to two isotopic semifields are not necessarily CCZ-equivalent. This suggests that the isotopism relation can potentially be used to find new planar functions that are

CCZ-inequivalent to the known ones. This was previously exploited by Budaghyan and Helleseth to extend their newly constructed family of planar functions into an even larger one under isotopism. However, the question of whether the isotopism relation can produce new, CCZ-inequivalent functions from other known families and instances has not been systematically studied before.

In this thesis, we investigate the possibility of doing this for the known families and sporadic instances of planar functions. Using the conditions laid out by Coulter and Henderson, we are able to deduce that a number of the known infinite families can never produce CCZ-inequivalent functions via isotopism. For the remaining families, we computationally investigate the isotopism classes of their instances over $\mathbb{F}_{3^n}$ for $n \leq 8$. We find previously unknown isotopisms between the semifields corresponding to some of the known planar functions for $n = 6$ and $n = 8$. This allows us to refine the known classification of planar functions up to isotopism, and to provide an updated, partial classification up to isotopism over $\mathbb{F}_{3^n}$ for $n \leq 8$.

Acknowledgements

I would like to thank my supervisor, Lilya Budaghyan and cosupervisors Nikolay Kaleyski and Enrico Piccione. In particular, I would like to thank Nikolay Kaleyski and Enrico Piccione for always being there to answer my questions, and for helping me with technical issues. Their motivation and passion for their field has been of great inspiration to me. Finally, I would like to thank my family and friends for all the support during my studies.

Contents

Chapter 1

Introduction

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, where p is a prime number and n is a positive integer. Vectorial functions are widely useful mathematical objects mapping elements of the vector space $\mathbb{F}_p^n$ to the vector space $\mathbb{F}_p^m$. Vectorial functions are frequently used as building blocks of cryptographic primitives, particularly in the case of $p = 2$ when they are called vectorial Boolean functions. The security of these primitives then directly depends on the properties of the functions. Their resistance to various kinds of cryptanalytic attacks is measured through various properties that can be computed for a given function. Each property measures the resistance to some particular attack. One of the most powerful attacks against block ciphers is differential cryptanalysis, introduced by Biham and Shamir in 1990 [8]. The property of a vectorial function measuring resistance to this kind of attack is called differential uniformity, and it should be as low as possible in order to provide security. While this notion was originally defined for vectorial Boolean functions, it naturally generalizes to vectorial functions of any characteristic. Furthermore, its definition is very natural, and it has appeared in many contexts even before its introduction in the context of cryptography.

In the case of even characteristic, the functions over $\mathbb{F}_{2^n}$ having the lowest possible differential uniformity, are called almost perfect nonlinear (APN). In the case of odd characteristic, we can go as low as a differential uniformity of 1, and the corresponding functions are called perfect nonlinear (PN) or planar. Both APN and planar functions are of interest not only because of their optimal cryptographic properties, but also because they correspond to optimal objects in many other areas of study, such as combinatorics, coding theory and sequence design. Both of these classes of functions have been the subject of intense study, and the class of planar functions is the primary topic of this thesis.

Perfect nonlinear functions were first formally introduced in the seminal paper [23] by P. Dembowski and T. G Ostrom in 1968. In that paper, they are referred to as planar functions due to their close connection to projective planes. However, a 1965 paper by J. E. H. Elliot and A. T. Butson on relative difference sets [28] led the way to a later proof that relative difference sets and planar functions are in fact equivalent [41], using the notion that planar mappings may be seen as projections of relative difference sets. As such, planar functions have played an important part in

multiple different research areas even before their formal introduction by Dembowski and Ostrom.

One prominent connection is the correspondence between commutative semifields and quadratic planar functions, which has been used successfully to construct the first new infinite family of commutative semifields over $\mathbb{F}_{p^n}$ for any odd characteristic p since the early 50s [14]. Since the study of semifields is an old and challenging topic, having been researched since Dickson's paper in 1905 [24], this breakthrough demonstrates the importance of studying and finding new instances of planar functions.

Finding new planar functions is known to be a hard problem, both mathematically and computationally. One reason for this is that the number of vectorial functions is very large. This makes it necessary to only consider vectorial functions (including planar functions) up to some notion of equivalence. Planar functions are typically considered up to Carlet-Charpin-Zinoviev-equivalence, or CCZ-equivalence, which is the most general currently known relation that preserves differential uniformity [10]. While reducing the number of functions that have to be considered, this also makes it quite difficult to find "new" planar functions, since in order for a function to be "new" it needs to be CCZ-inequivalent to all previously known instances.

In the case of quadratic planar functions, we can define an even broader equivalence relation by means of the commutative semifields corresponding to the functions. An equivalence relation called isotopism can be defined on semifields, and if two commutative semifields are isotopic, we say that their corresponding quadratic planar functions are isotopic, or isotopic equivalent. While any two CCZ-equivalent quadratic planar functions correspond to isotopic commutative semifields, two isotopic planar functions are not necessarily CCZ-equivalent. This suggests that it may be possible to obtain new instances of planar functions up to CCZ-equivalence from the known ones by exploring the isotopism classes of their corresponding semifields. Such an approach has previously been successfully exploited by Budaghyan and Helleseth to extend their infinite family of planar functions to a larger one [14]. However, to the best of our knowledge, no systematic study has been done on the possibility of obtaining new planar functions in this way from the rest of the known families and sporadic instances. The main goal of this thesis is thus to evaluate the possibility of doing precisely this.

Inspired by the notion of isotopic planar functions, the isotopic shift of a planar function was introduced in 2020 [12]. For a given planar function, then an isotopic planar function is CCZ-equivalent to an isotopic shift of the original planar function. However, the reverse is not true in general, and the isotopic shift of a planar function is not necessarily itself a planar function.

There is a special case of isotopism called strong isotopism, which precisely corresponds to CCZ-equivalence between the corresponding planar functions. In other words, two quadratic planar functions are CCZ-equivalent if and only if their corresponding semifields are strongly isotopic [14]. Thus, in order to find new planar functions up to CCZ-equivalence, we want to find semifields that are isotopic but not strongly isotopic to the known ones.

Coulter and Henderson give necessary conditions on when a semifield can be isotopic but not strongly isotopic to another semifield. These conditions are based on the so-called nuclei of the semifields, whose orders are invariant under isotopism. By utilizing these conditions, we are able

to show that for a number of the known families of planar functions, no new ones (up to CCZ-equivalence) can be obtained using isotopism.

For representatives from the remaining families and sporadic instances, we conduct a computational search for isotopic semifields over $\mathbb{F}_{3^n}$ for $n \leq 8$. We use the algorithm from [32] to compare the resulting functions for CCZ-equivalence against the original ones. We do not find any new planar functions up to CCZ-equivalence, but we do find previously unknown isotopisms between some of the known planar functions for $n = 6$ and $n = 8$. We are thus able to refine the classification of the known planar functions up to isotopism for the relevant dimensions. There remain some instances where we could not decide whether functions CCZ-inequivalent to them exist in the isotopism class, and so this is only a partial classification. However, we have demonstrated computationally that isotopism leading to CCZ-inequivalent functions of a certain form do not exist.

This thesis is divided into chapters in the following way. In Chapter 2 we lay out the preliminary theory of planar functions and semifields along with the known families of semifields and planar functions and their corresponding invariants (in particular, the orders of their nuclei that we use when evaluating the Coulter-Henderson conditions). We also present a table of the known CCZ-inequivalent planar function representatives over $\mathbb{F}_{3^n}$ with $n \leq 8$, collected from [30]. In Chapter 3 we investigate a method by which new planar functions can be constructed from existing ones, using the isotopism of their corresponding commutative semifields. We study in which particular cases such endeavours might lead to finding new planar functions up to CCZ-equivalence. We conclude that this is only possible in even dimensions, and then only in doubly even dimensions for the Bierbrauer, Dickson and Cohen-Ganley families. We also report on the results of our computational search for representatives from these families over $\mathbb{F}_{3^n}$ for $n \leq 8$, and show previously unknown isotopisms between some of the known planar functions. We also show instances for which an isotopic planar function is CCZ-equivalent to an isotopic shift of that planar function by a monomial permutation. We summarize this in a partial classification of planar functions for $n \leq 8$ up to isotopism. Finally, we conclude in Chapter 4 with a summary of the work that we did and with potential directions for further studies.

Chapter 2

Preliminaries

2.1 Planar functions

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, for a prime number p and a natural number n. A function F mapping elements in $\mathbb{F}_p^n$ to elements in $\mathbb{F}_p^m$ is called a *vectorial function*, and it is often called (n, m, p)-function. For $p = 2$, $(n, m, 2)$-functions are called (n, m)-functions, and are referred to as *vectorial Boolean* functions, and when $m = 1$ simply *Boolean* functions.

Block ciphers are widely used in modern cryptography, and vectorial functions play an important part in many implementations of them. Block ciphers take a block of plaintext as an input, and transform it into an encrypted output block (ciphertext), of the same length as the original block. One of the most powerful attacks against block ciphers are differential attacks, which use differential cryptanalysis to deduce information about the form of the transformation being used. In a differential attack, the attacker first collects a number of inputs x and corresponding outputs y. By observing the relationships between the differences of inputs and differences of outputs, the attacker can gain valuable insight into the inner workings of the transformation that defines the encryption in the block cipher, and thereby breaking the cipher. A cryptographically strong function therefore needs to be resistant against these types of attacks. That is, for any given difference between inputs $d_x = x_1 - x_2$ we ideally want any value for the difference in outputs $d_y = y_1 - y_2$ to be equally likely, i.e., uniformly distributed. This is the motivation behind the notion of differential uniformity.

Definition 2.1.1. Let F be a vectorial function from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ and let $0 \neq a \in \mathbb{F}_p^n$. Then

$$D_a F(x) = F(x + a) - F(x)$$

is called the *derivative of F with respect to a*.

Then it is easy to see that the problem of determining the distribution of solutions to the derivative of F with respect to some nonzero direction a for each given output $D_a F(x) = b$, is exactly the same problem as determining the distribution of differences in inputs for each possible difference among corresponding outputs in the block cipher. More formally, we use the following definition.

Definition 2.1.2. A vectorial function F from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ is *differentially δ-uniform* if for all $0 \neq a \in \mathbb{F}_p^n$ and $b \in \mathbb{F}_p^m$, the equation $D_aF(x) = b$ has at most δ solutions.

The lower the number δ, the closer the distribution of differences in possible inputs is to being uniform for each given difference in outputs. We say that a vectorial function has differential uniformity δ if it is differentially δ-uniform. Over vector spaces of odd characteristic, that is for p an odd prime, the lowest possible differential uniformity of vectorial function is 1. These vectorial functions are called *perfect nonlinear* (PN) or *planar* functions. That is, a perfect nonlinear vectorial function evenly distributes the possible differences in inputs for each possible difference in outputs. However, these functions over $\mathbb{F}_p^n$ can only exist for odd primes p, since the lowest differential uniformity of a vectorial Boolean function is $\delta = 2$. This is clearly the case, since any solution $x_0 \in \mathbb{F}_p^n$ to $F(x) - F(x+a) = F(x) + F(x+a) = b$ immediately allows a second solution $x_0 + a$. Vectorial functions having differential uniformity of 2 are called *almost perfect nonlinear* (APN).

In this thesis, we are primarily interested in (n, n, p)-functions F, i.e., mappings from $\mathbb{F}_p^n$ to itself, and we consider the univariate representation of the vectorial function F. In fact, any vectorial function from the vector space $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$ can be uniquely represented as a univariate polynomial over the finite field $\mathbb{F}_{p^n}$ of p^n elements of degree less than p^n [34].

Definition 2.1.3. A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called

- *Linear* if $F(x) = \sum_{0 \leq i < n} a_i x^{p^i}$, $a_i \in \mathbb{F}_{p^n}$,
- *Affine* if F is a sum of a linear function and a constant,
- *Dembowski-Ostrom* (DO) polynomial if $F(x) = \sum_{0 \leq k,j < n} a_{k,j} x^{p^k + p^j}$, where $a_{k,j} \in \mathbb{F}_{p^n}$
- *Quadratic* if F is a sum of a DO-polynomial and an affine function.

The number of univariate polynomials that exist over a given finite field $\mathbb{F}_{p^n}$ of degree less than p^n is very. Therefore, it is useful to have a notion of equivalence between functions allowing us to only consider a single polynomial from each equivalence class.

Definition 2.1.4. Two functions F and F' from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ are called

- *Linear equivalent* if $F' = A_1 \circ F \circ A_2$, where A_1 and A_2 are linear permutations of $\mathbb{F}_{p^n}$,
- *Affine equivalent* if $F' = A_1 \circ F \circ A_2$, where A_1 and A_2 are affine permutations of $\mathbb{F}_{p^n}$,
- *Extended affine (EA) equivalent* if $F' = A_1 \circ F \circ A_2 + A$, where the mappings A_1, A_2, A are affine and A_1, A_2 are permutations,
- *Carlet-Charpin-Zinoviev (CCZ) equivalent* if for some affine permutation $\mathcal{L}$ over $\mathbb{F}_{p^n}^2$ the image of the graph of F is equal to the graph of F', i.e.
  $\mathcal{L}(G_F) = G_{F'}$, where $G_F := \{(x, F(x)) \mid x \in \mathbb{F}_{p^n}\}$.

It has been proven that differential uniformity is invariant under CCZ-equivalence [16]. However, checking whether two functions are CCZ-equivalent is hard in general [15], and building

functions that are CCZ-equivalent but not EA-equivalent is also hard. It is easier to check for EA-equivalence between two functions, and constructing EA-equivalent functions is easy as well. [14]. Identifying situations in which CCZ-equivalence reduces to EA-equivalence is therefore useful, as one can save substantial computational effort when checking for equivalence between functions. In particular, CCZ-equivalence is known to reduce to EA-equivalence for all Boolean functions [14].

EA-equivalence is a special case of CCZ-equivalence, and CCZ-equivalence is proven to be more general than EA-equivalence [10]. Additionally, for planar functions (n, n, p)-functions, it is proven that CCZ-equivalence coincides with EA-equivalence (so that two planar (n, n, p)-functions are CCZ-equivalent if and only if they are EA-equivalent. For planar DO polynomials, EA-equivalence reduces to linear equivalence [14]. We shall explore the consequences of this more thoroughly in Chapter 2.3.

The first infinite family of planar functions defined over a finite field $\mathbb{F}_{p^n}$ for any odd prime p were the planar functions corresponding to the commutative semifields of Dickson and Albert in 1905 [24]. This connection between planar functions and commutative semifields will be explored in detail in the next sections of this chapter. Since then, more infinite families defined for any odd prime p have been constructed. One of these families was constructed in [13] by way of extension of a known family of APN functions over $\mathbb{F}_{2^{2k}}$. This showed that known classes of APN functions over fields of even characteristic can serve as sources of further constructions of planar mappings over fields of odd characteristic.

2.2 Semifields

Planar functions are worth studying because, as was previously indicated, they correspond to optimal objects in other branches of mathematics in addition to having strong cryptographic qualities. The algebraic objects known as presemifields and semifields are possibly one of the best illustration of this. After the study of finite fields was finished, scholars began looking into more generic structures that were governed by axioms and relaxation conditions. Finite fields are relaxed into semifields, which satisfy all the axioms except for the requirement that they be associative and commutative. The study of these algebraic objects was started in the early 20th century by Dickson [24], despite the term semifield not being used in the literature until much later. Prior to Knuth's thesis in 1965 [33], they were known as "distributive quasifields" or "nonassociative division rings" for about 60 years. A formal definition of semifields can be given as follows.

Let S be a finite set of elements, let $+$ and $\star$ be two operations defined on the set S such that

- $(S, +)$ is an Abelian group with identity 0_S,
- The left and right distributivity law holds, $a \star (b + c) = a \star b + a \star c$ and $(a + b) \star c = a \star c + b \star c$ for all $a, b, c \in S$,
- There are no zero divisors, meaning if $a \star b = 0_S$ then either a or b is equal to 0_S.

Then $\mathbb{S} = (S, +, \star)$ is called a *presemifield*. If, in addition, a presemifield has a multiplicative identity, then it is called a *semifield*. We here refer to the operation $\star$ as the *presemifield operation* or

presemifield multiplication of $\mathbb{S}$. Furthermore, we say that a semifield is *commutative*, if $x \star y = y \star x$ for all $x, y \in S$.

We can represent any presemifield as $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$, where $\mathbb{F}_{p^n}$ is a finite field with p^n elements. Crucially, there is no condition on whether the semifield operation $\star$ is associative. In fact, if associativity holds for a semifield, then it is a finite field. This is because in the finite case, associativity always implies commutativity for semifields[9]. However, a commutative semifield is not necessarily associative, and therefore not necessarily a field.

If a semifield is not a field, i.e. associativity does not hold, then it is called a *proper* semifield. However, in this thesis, we shall simply use the term semifield when referring to a proper semifield. Commutative semifields are also interesting, as they are in a sense the "closest" structures to fields [9]. Additionally, for a semifield $\mathbb{S}$ with p^n elements, we say that the *characteristic* of $\mathbb{S}$ is the prime number p, and the positive integer n is called the *dimension* of $\mathbb{S}$. The first proper semifields, different from finite fields, were the commutative semifields of Dickson and Albert [14] which have order p^{2k} with p an odd prime and $k > 1$ an integer.

From any commutative presemifield, one can construct its corresponding commutative semifield in the following way. Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$ be a commutative presemifield and choose any nonzero $a \in \mathbb{F}_{p^n}$ and define the operation $\circ$ as

$$(x \star a) \circ (a \star y) = x \star y \qquad \text{for all } x, y \in \mathbb{F}_{p^n}.$$

Then one can easily check that $\mathbb{S}' = (\mathbb{F}_{p^n}, +, \circ)$ is a commutative semifield, with $a \star a$ as its identity element. We say the semifield $\mathbb{S}'$ *corresponds* to the presemifield $\mathbb{S}$ with identity $a \star a$ corresponding to $\mathbb{S}$.

Definition 2.2.1. Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \circ_1)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \circ_2)$ be presemifields. Then they are said to be *isotopic* if there exist linear permutations L, M, N over $\mathbb{F}_{p^n}$ such that

$$L(x \circ_1 y) = M(x) \circ_2 N(y), \qquad \text{for all } x, y \in \mathbb{F}_{p^n}$$

The triple (L, M, N) is called the *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$.

Definition 2.2.2. Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \star)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \circ)$ be isotopic presemifields. Then if there exists an isotopism (L, N, N) between $\mathbb{S}_1'$ and $\mathbb{S}_2$ then we say that $\mathbb{S}_1'$ and $\mathbb{S}_2$ are *strongly isotopic*.

The differences in the properties of strongly isotopic semifields as opposed to non-strongly isotopic semifields have many important implications for planar functions. That is, commutative semifields and quadratic planar functions are in one-to-one correspondence, and strongly isotopic semifields imply that their corresponding planar functions are CCZ-equivalent.

Clearly, a presemifield $\mathbb{S}$ is strongly isotopic to its corresponding semifield $\mathbb{S}'$, through the strong isotopism (id, L_a, L_a), where $L_a = a \star x$.

Definition 2.2.3. Given a semifield $\mathbb{S}' = (\mathbb{F}_{p^n}, +, *)$, we define

$$\begin{aligned} N_l(\mathbb{S}') &:= \{a \in \mathbb{F}_{p^n} \mid (a * x) * y = a * (x * y) \quad \forall\ x, y \in \mathbb{F}_{p^n}\} \\ N_m(\mathbb{S}') &:= \{a \in \mathbb{F}_{p^n} \mid (x * a) * y = x * (a * y) \quad \forall\ x, y \in \mathbb{F}_{p^n}\} \\ N_r(\mathbb{S}') &:= \{a \in \mathbb{F}_{p^n} \mid (x * y) * a = x * (y * a) \quad \forall\ x, y \in \mathbb{F}_{p^n}\} \end{aligned}$$

the *left, middle* and *right nucleus* of $\mathbb{S}'$ respectively, and

$$N(\mathbb{S}') := N_l(\mathbb{S}') \cap N_m(\mathbb{S}') \cap N_r(\mathbb{S}')$$

the *nucleus* of $\mathbb{S}'$.

In the case of a commutative semifield, the left and right nuclei are identical. Additionally, for a commutative semifield the right nucleus is contained in the middle nucleus [9], clearly it then follows for a commutative semifield that

$$N(\mathbb{S}') = N_r(\mathbb{S}') = N_l(\mathbb{S}').$$

In effect, the orders of the nuclei measure how far the semifield $\mathbb{S}$ is from being a field. Although it is widely stated in other literature, these sets are not always subfields of $\mathbb{F}_{p^n}$, that is, subsets that are themselves fields. This depends on whether the multiplicative identity of the semifield $a \star a$ is the same identity 1 as in the finite field $\mathbb{F}_{p^n}$ [30].

The following fact about the orders of the nuclei of semifield is quite important for our investigation. Therefore, we formulate it as a theorem.

Theorem 2.2.1. *[19, page 286] The orders of the left, middle and right nuclei and the nucleus of a semifield are invariant under isotopism.*

When investigating whether two semifields might be isotopic, observing that the orders of their nuclei are different immediately provides a negative answer.

2.3 Connections between CCZ-equivalence and isotopism

Here, we explain the connection between planar functions and commutative semifields over fields of odd characteristic. In particular, how an instance of a quadratic planar function can be used to define a commutative semifield, and vice versa. Additionally, we discuss how their respective properties are connected. This is useful as results in classification of planar functions have important consequences on the classification of commutative semifields [14]. In fact, every commutative presemifield in odd characteristic defines a planar DO polynomial and vice versa.

Let F be a quadratic planar function over $\mathbb{F}_{p^n}$. Then $\mathbb{S} := (\mathbb{F}_{p^n}, +, \star)$ defined by

$$x \star y := F(x + y) - F(x) - F(y) \qquad \forall x, y \in \mathbb{F}_{p^n} \tag{2.1}$$

is a commutative presemifield. We say that $\mathbb{S}$ is the *commutative semifield defined by the quadratic planar function* F.

Conversely, given a commutative presemifield $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$ of odd order, then the function given by

$$F(x) = \frac{1}{2}(x \star x) \tag{2.2}$$

is a quadratic planar function [19].

Due to this connection between quadratic planar functions and commutative semifields, it is possible to identify a presemifield and its corresponding planar function. And for the sake of brevity, when two planar functions correspond to isotopic presemifields and semifields, we here refer to them as isotopic planar functions.

The following theorems and corollaries regarding planar functions and commutative semifields are collected from Coulter and Henderson's paper on semifields and presemifields from 2008, in [19], and from the papers by Budaghyan and Helleseth from 2008 [13] and 2011 [14].

Theorem 2.3.1. *[14, Theorem 3] Let p be any prime, m and n any positive integers. If a function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is such that all its derivatives $D_a(x) = F(x) - F(x+a)$, $a \in \mathbb{F}_{p^n}^*$, are surjective, then any function CCZ-equivalent to F is EA-equivalent to it.*

Clearly, by the definition of a planar function, Theorem 2.3.1 applies to planar functions, as the derivative has a unique solution for any given value $b = F(x+a) - F(x)$ in $\mathbb{F}_{p^n}$ no matter the choice of direction $a \in \mathbb{F}_{p^n}^*$.

Corollary. *[14, Corollary 1] Let F be a planar function and F' be CCZ-equivalent to F. Then F and F' are EA-equivalent.*

Therefore, for planar functions, CCZ-equivalence reduces to EA-equivalence, and checking whether two planar functions are CCZ-equivalent equates to checking whether they are EA-equivalent, which is far easier.

Corollary. *[14, Corollary 2] If a planar function F is CCZ-equivalent to a DO polynomial F' then F is also DO.*

"DO-ness" is invariant for planar functions under CCZ-equivalence (and in particular EA-equivalence).

Corollary. *[14, Corollary 3] Perfect nonlinear DO polynomials F and F' are CCZ-equivalent if and only if they are linear equivalent.*

Consequently, it is sufficient to check for linear equivalence between two planar DO-polynomials to see if they are CCZ-equivalent. Therefore, the time spent checking whether two functions are CCZ-equivalent can be drastically reduced, since linear equivalence is easier to determine.

Theorem 2.3.2. *[13] Let F and F' be two DO polynomials over $\mathbb{F}_{p^n}$, and $\mathbb{S}_F$ and $\mathbb{S}_{F'}$ be their corresponding commutative semifields. Then F and F' are CCZ-equivalent if and only if $\mathbb{S}_F$ and $\mathbb{S}_{F'}$ are strongly isotopic.*

As an immediate consequence, it also follows that two isotopic commutative semifields defined by CCZ-inequivalent quadratic planar functions cannot be strongly isotopic. Additionally, it is

proven in Corollary 2.8 in [19] that two commutative presemifields of order p^n with n odd are isotopic if and only if they are strongly isotopic. There are also some sufficient conditions for n even, where isotopism of semifields implies strong isotopism.

Theorem 2.3.3. *[19, Theorem 2.6] If $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic commutative presemifields of characteristic p with the order of the middle nucleus p^m and order of the nucleus p^k of their corresponding semifields, then one of the following statements must hold:*

(i) $\frac{m}{k}$ is odd and $\mathbb{S}_1$ and $\mathbb{S}_2$ are strongly isotopic,

(ii) $\frac{m}{k}$ is even and either $\mathbb{S}_1$ and $\mathbb{S}_2$ are strongly isotopic or the only isotopism between the corresponding semifields $\mathbb{S}_1'$ and $\mathbb{S}_2'$ are of the form

$$(L, \beta * N, N),$$

where β is a non-square element of $N_m(\mathbb{S}_1')$.

Consequently, by Theorem 2.3.3, in the case n is even, it is possible that isotopic commutative presemifields (that are not strongly isotopic) define CCZ-inequivalent quadratic planar functions. That is, starting with one quadratic planar function F, corresponding to a commutative presemifield $\mathbb{S}_F$, over $\mathbb{F}_{p^n}$ with n even and order of the middle nucleus p^m and nucleus p^k such that $\frac{m}{k}$ is even, then it is potentially possible to construct a quadratic planar function F' that is CCZ-inequivalent to F, by way of finding a semifield isotopic to $\mathbb{S}_F$ of the form $(L, \beta * N, N)$. Theorem 2.3.3 also results in this useful corollary.

Corollary. *[19, Theorem 2.6] [14] Any commutative presemifield can generate at most two CCZ-equivalence classes of planar DO polynomials.*

Therefore, for any isotopism class of semifields, there exist at most two CCZ-inequivalent corresponding quadratic planar functions.

Definition 2.3.1. [12, Definition I.1] Let $F, L \in \mathbb{F}_{p^n}[x]$. Then the *isotopic shift of* F by L, denoted by F_L, is the polynomial given by

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)).$$

This definition is inspired by the notion of isotopic equivalence of planar functions, and as we shall see in Theorem 2.3.4 is a natural relation between quadratic planar functions [12].

Theorem 2.3.4. *[12, Theorem I.1] Let $F, G \in \mathbb{F}_{p^n}[x]$ be quadratic planar functions (null at 0). If F and G are isotopic equivalent, then G is EA-equivalent to some isotopic shift F_L of F by a linear permutation polynomial $L \in \mathbb{F}_{p^n}[x]$.*

However, the converse is not always true [12]. That is, not every isotopic shift of a planar function gives an isotopic planar function. In fact, for an arbitrary linear permutation L, F_L is not always planar either.

In 2008, two infinite families of quadratic perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ with p any odd prime and k a positive integer were constructed [13]. This family was then also extended to

include isotopic planar functions [14], by the same method as the one being investigated in this thesis. It was also proven that this family is CCZ-inequivalent to previously known families, and supplied direct results indicating that these planar functions define new semifields. These were the firstly found infinite families of commutative semifields of order p^n that are defined for any odd prime p since the commutative semifields by Dickson [24] in 1905 and Albert [1] in 1961.

2.4 Known planar functions and commutative presemifields

Here we present the known families of planar functions and their corresponding presemifields as of the time of writing. The following list contains families of presemifields, given by their presemifield operation, and families of planar functions, and supposing they are quadratic, then using the canonical construction of a presemifield multiplication operator one can also define commutative presemifields as shown in Equation 2.1.

It should be noted that many of the instances of planar functions generated by these families are CCZ-equivalent to each other, and in particular over fields of small dimensions. This also happens for many instance of the same family. However, as the size of the finite field on which the families are defined increases, they can produce more distinct CCZ-inequivalent planar functions. In the case that a family has been shown to be contained in another family, we have chosen to not use bold text on its abbreviated name.

FF Finite fields $F(x) = x^2$ over $\mathbb{F}_{p^n}$, for p odd. [Folklore]

CM The Coulter-Matthews planes [22],[31]

$$x^{(3^t+1)/2}$$

on $\mathbb{F}_{3^n}$ is planar if $t \geq 3$ is odd and $gcd(t, n) = 1$. Notably, these functions are not quadratic and do not correspond to any semifield.

A Commutative twisted fields, a.k.a. Albert semifields [22], [23]

$$F(x) = x^{p^e+1}$$

is planar on $\mathbb{F}_{p^n}$ if and only if $gcd(n, e)$ is odd.

Note. There is a larger class of these semifields, the so-called *generalized twisted fields*, but these are the only commutative ones.

D Dickson semifields [26]
Defined by the presemifield multiplication

$$(a, b) \star (c, d) = (ac + \alpha b^q d^q, ad + bc),$$

where $\alpha \in \mathbb{F}_{q^k}$ is a nonsquare. Then $\mathbb{S} = (\mathbb{F}_{q^k}^2, +, \star)$ is a presemifield.

G Ganley semifields [29] Defined by $\mathbb{S} = (\mathbb{F}_{3^{2k}}, +, \star)$ for k odd, where

$$(a, b) \star (c, d) = (ac - b^9 d - bd^9, ad + bc + b^3 d^3)$$

where $a, b, c, d \in \mathbb{F}_{3^k}$. Then $\mathbb{S}$ is a presemifield.

CG Cohen-Ganley semifields [17] Defined by $\mathbb{S} = (\mathbb{F}_{3^{2n}}, +, \star)$ for $n \geq 2$, where

$$(a, b) \star (c, d) = (ac + \beta bd + \beta^3 (bd)^9, ad + bc + \beta (bd)^3)$$

with $\beta \in \mathbb{F}_{3^n}$ a nonsquare and where $a, b, c, d \in \mathbb{F}_{3^n}$. Then $\mathbb{S}$ is a presemifield.

CM/DY Coulter-Matthews-Ding-Yuan semifields [22], [27]

$$x^{10} \pm x^6 - x^2$$

is planar over $\mathbb{F}_{3^n}$ if and only if n is odd or $n = 2$.

ZKW Zha-Kyureghyan-Wang presemifields [5], [42]

$$x^{p^s+1} - \alpha^{p^k+1} x^{p^k+2^{2k+s}}$$

is planar on $\mathbb{F}_{p^{3k}}$ whenever p is odd, s, k are integers such that $gcd(3, k) = 1$, $0 < s < 3k$, $k \equiv s \bmod 3$, $k \neq s$, $\frac{3k}{gcd(s,3k)}$ is odd and $\alpha \in \mathbb{F}_{p^{3k}}$ is primitive. The construction of these planar functions was motivated by the APN binomials from [11].

B Bierbrauer presemifields [6] Defined by $\mathbb{S} = (\mathbb{F}_{p^{4s}}, +, \star)$, p an odd prime, where

$$x \star y = y^{p^t} x + y x^{p^t} - u^{p^s-1} (y^{p^{s+t}} x^{p^{3s}} + y^{p^{3s}} x^{p^{s+t}}),$$

where u is a primitive element of $\mathbb{F}^*_{p^{4s}}$ and $0 < t < 4s$ such that $\frac{2s}{gcd(2s,t)}$ is odd and $p^s \equiv p^t \equiv 1 \bmod 4$. For $s = 1$, the Bierbrauer family was shown to be isotopic to a Dickson presemifield, in [37].

LMPTB Lunardon-Marion-Polverino-Trombetti-Bierbrauer [7]

$$\mathrm{Tr}(x^2) + G(x^{q^2+1})$$

is planar over $\mathbb{F}_q^{2m}$, where q is a power of a prime p, $m = 2k + 1$, Tr is the trace from $\mathbb{F}_q^{2m}$ to $\mathbb{F}_{q^m}$, and $G(x) = h(x - x^{q^m})$, where $h \in \mathbb{F}_q^{2m}[x]$ is defined as

$$h(x) = \sum_{i=0}^{k} (-1)^i x^{q^{2i}} + \sum_{j=0}^{k-1} (-1)^{k+j} x^{q^{2j+1}}.$$

This family is Bierbrauer's generalization of the semifields discovered by Lunardo, Marion, Polverino and Trombetti over q^6 in [36]. However, it was proven in [37] that the LMPTB family is contained in the BHB family.

BHB Budaghyan-Helleseth-Bierbrauer semifields [7]

$$\mathrm{Tr}(x^{p^m+1}) + \mathrm{Tr}(\beta x^{p^s+1})$$

is planar over $\mathbb{F}_{p^{2m}}$, where p is an odd prime, $q = p^m$, the trace function from $\mathbb{F}_{p^{2m}}$ to $\mathbb{F}_{p^m}$, $\omega, \beta \in \mathbb{F}_{p^{2m}}$, $\mathrm{Tr}(\omega) = 0$ and $\mathbb{S}$ is a positive integer such that the following holds:

- β^{p^m-1} is not contained in the subgroup of order $(p^m+1)/\gcd(p^m+1, p^s+1)$ in $(\mathbb{F}_{p^{2m}}, *)$,

Table 2.1: Sporadic instances of planar functions in characteristic 3

p^n	Defining polynomial	Name	Reference
3^5	$x^{90}+x^2$	ACW	[3]
3^5	$x^{162}+x^{108}+2x^{84}+x^2$	CK[1]	[21]
3^6	$\alpha^{91}x^{30}+x^{10}+x^2$	H[1]	[30]
3^6	$\alpha^{91}x^{486}+x^{10}+x^2$	H[2]	[30]
3^6	$\alpha^{182}x^{82}+2x^{10}+\alpha^{91}x^6+x^2$	H[3]	[30]
3^6	$\alpha^{182}x^{82}+2x^{10}+\alpha^{273}x^6+x^2$	H[4]	[30]
3^6	$\alpha^{91}x^{486}+\alpha^{182}x^{90}+2x^{10}+x^2$	H[5]	[30]
3^6	$\alpha^{273}x^{486}+\alpha^{182}x^{90}+2x^{10}+x^2$	H[6]	[30]
3^6	$\alpha^{273}x^{246}+\alpha^{182}x^{82}+\alpha^{91}x^6+x^2$	H[7]	[30]

Note that α is an arbitrary primitive element of $\mathbb{F}_{p^n}^*$, and so generates all nonzero elements under multiplication by itself. All coefficients are given in the form of some power of α, except the nonzero elements inherited from the prime field, here; 1 and 2.

– there is no $0 \neq a \in \mathbb{F}_{p^{2m}}$ such that $\mathrm{Tr}(a)=0$ and $a^{p^s}=-a$.

This family is the generalized form of the Budaghyan-Helleseth family [14] by Bierbrauer. However, it is not known whether this family is more general than the Budaghyan-Helleseth family.

ZP Zhou-Pott semifields [44] Let m,k be positive integers, such that $\frac{m}{gcd(m,k)}$ is odd. Define $x \circ_k y = x^{p^k}y + y^{p^k}x$. For elements $(a,b),(c,d) \in \mathbb{F}_{p^m}^2$, define a presemifield operation $\star$ as follows, $(a,b)\star(c,d) = (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad+bc)$, where $\alpha \in \mathbb{F}_{p^m}$ a nonsquare and $\sigma \in Aut(\mathbb{F}_{p^m})$. Then $\mathbb{S} = (\mathbb{F}_{p^{2m}}, +, \star)$ is a presemifield. It has been proven that the ZP family is isotopic to the BHB family for trivial σ in [44].

The known sporadic instances of planar functions in characteristic 3 are listed in Table 2.1, with the exception of the planar function corresponding to the Pentilla-Williams presemifield and the two sporadic planar functions CK[2] by Coulter and Kosick in $\mathbb{F}_{5^5}$.

The Pentilla-Williams (**PW/BLP**) commutative semifield is a sporadic instance of a commutative semifield in dimension 10. This semifield is defined by the presemifield operation defined as

$$(a,b)\star(c,d) = ((ac+bd)^9, ad+bc+(bd)^{27})$$

on $\mathbb{F}_{3^5}\times\mathbb{F}_{3^5}$, i.e., in $\mathbb{F}_{3^{10}}$. It is the only sporadic instance we know of in this dimension [40].

All the currently known sporadic instances of planar functions in dimension 6 were found in the thesis by Haukenes in 2022, and they are listed in Table 2.1 with the name H[1] to H[7]. The orders of their middle nucleus and nucleus have been calculated computationally and are shown in Table 2.4.

The sporadic planar functions CK[2] in characteristic 5 are the only known sporadic planar functions in characteristic 5 as of the time of this writing. It is defined as

$$F(x) := L(t^2(x)) + D(t(x)) + \frac{1}{2}x^2,$$

where $L(x) = x^{5^3} + x^{5^2} + 2x^5 + 3x$ and $D(x) = 0$ or $L(x) = 2x^{5^2} + x^5$ and $D(x) = 2x^{5^3+5} + 2x^{5^2+1}$, and where $t(x) = x^5 - x$ [21].

As regards the nuclei, meaning the right, left, middle nucleus and nucleus, of the semifields defined by the known families and sporadic instances of planar functions and presemifields, some have been found analytically and are displayed in Table 2.2.

It is important to note that many of the infinite families, although they might be different in general, do produce some CCZ-equivalent instances. This is particularly the case for small dimensions. Additionally, many of the instances of a single family in the same dimension generated by choosing different parameters are also often CCZ-equivalent. Therefore, it is necessary to identify the CCZ-inequivalent representatives from all families and from all sporadic cases.

In the thesis by Haukenes in [30] she performs this classification in characteristic 3, and the representatives of the CCZ-inequivalent planar functions show in Table 2.3 and the orders of their nuclei as shown for dimensions 6 to 8 in Table 2.4 are collected from her thesis, with some minor adjustments with respect to the orders of the middle nucleus for representatives 6.4, 6.5 and 8.6. Whilst performing this classification, she also found new sporadic instances of planar functions in dimension 6, which were CCZ-inequivalent to the previously known ones. They are named in Table 2.3 as H[1] up to H[7]. In that same thesis, it was also shown that another sporadic instance in dimension 8, namely the Coulter-Henderson-Kosick semifield (CHK), listed as representative 8.8 in Table 2.3, is in fact EA-equivalent to an instance of Zhou-Pott, a problem which had remained open for a long time. These CCZ-inequivalent representatives of planar functions over fields of order 3^n, for n from 2 to 8, are listed here in Table 2.3

Table 2.2: Order of middle nucleus and nucleus of known families of commutative semifields

TYPE	$\lvert\mathbb{S}\rvert$	$\lvert N(\mathbb{S})\rvert$	$\lvert N_m(\mathbb{S})\rvert$	Existence Results	Reference
D	q^{2k}, $k > 1$ odd	q	q^k	$\exists\ \forall\ q$ odd	[25]
A	q^t, $t > 1$ odd	q	q	$\exists\ \forall\ q$ odd	[1], [2]
ZKW	q^{3k}, $h > 1$ odd	q	q	$\exists\ \forall\ q$ odd, $k + s \equiv 0 \pmod 3$, $\exists \forall q$ odd : $q \equiv 1 \pmod 3$	[37]
B	q^{4s}, $s > 1$ odd	q	q^2	$\exists\ \forall\ q \equiv 1 \pmod 4$	[37]
BH	q^{2m}, $m > 2$	q	q^2	$\exists\ \forall\ q$ odd	[37]
ZP	q^{2l}, $l > 2$	q	q^2 (if $\sigma = 1$), q (if $\sigma \neq 1$)	$\exists\ \forall\ q$ odd	[44]
CG	3^{2s}, $s \geq 3$	3	3^s		[17]
G	3^{2r}, $r \geq 3$ odd	3	3		[29]
CM/DY	3^e, $e \geq 5$ odd	3	3		[27], [19]
PW/BLP	3^{10}	3	3^5		[39], [4]

The orders of the nuclei for the known proper commutative semifields in odd characteristic. Note that the size of the semifield $\lvert\mathbb{S}\rvert$ is the same as the order of the finite field on which the family is defined. Note that q is a power of the prime characteristic p. This table was collected from [37].

Table 2.3: CCZ-inequivalent planar functions in characteristic 3 and dimension 2 to 8

Dim	**N^0**	**Representative**	**Family**
2	2.1	x^2	FF
3	3.1	x^2	FF
	3.1	x^4	A
4	4.1	x^2	FF
	4.2	x^{14}	CM
	4.3	$x^{36}+2x^{10}+2x^4$	BHB
5	5.1	x^2	FF
	5.2	x^4	A
	5.3	x^{10}	A
	5.4	$x^{10}+x^6+2x^2$	CM/DY
	5.5	$x^{10}+2x^6+2x^2$	CM/DY
	5.6	x^{14}	CM
	5.7	$x^{90}+x^2$	ACW
	5.8	$x^{162}+x^{108}+2x^{84}+x^2$	CK[1]
6	6.1	x^2	FF
	6.2	x^{10}	A
	6.3	$x^{162}+x^{82}+\alpha^{58}x^{54}+\alpha^{58}x^{28}+x^6+\alpha^{531}x^2$	D
	6.4	$\alpha^{75}x^{2214}+x^{756}+\alpha^{205}x^{82}+x^{28}$	BHB
	6.5	$2x^{270}+x^{246}+2x^{90}+x^{82}+x^{54}+2x^{30}+x^{10}+x^2$	LMPTB/BHB
	6.6	$x^{270}+2x^{244}+\alpha^{449}x^{162}+\alpha^{449}x^{84}+\alpha^{534}x^{54}+2x^{36}$ $+\alpha^{534}x^{28}+x^{10}+\alpha^{449}x^6+\alpha^{279}x^2$	G
	6.7	$x^{486}+x^{252}+\alpha^{561}x^{162}+\alpha^{561}x^{84}+\alpha^{183}x^{54}+\alpha^{183}x^{28}$ $+x^{18}+\alpha^{561}x^6+\alpha^{209}x^2$	CG
	6.8	x^{122}	CM
	6.9	$\alpha^{438}x^{486}+\alpha^{180}x^{324}+\alpha^{458}x^{270}+\alpha^{672}x^{252}+\alpha^{622}x^{246}$ $+\alpha^{94}x^{244}+\alpha^{650}x^{162}+\alpha^{441}x^{108}+\alpha^{50}x^{90}+x^{84}+\alpha^{77}x^{82}$ $+\alpha^{328}x^{36}+\alpha^{583}x^{30}+\alpha^{407}x^{28}+\alpha^{178}x^{18}+\alpha^{492}x^{12}$ $+\alpha^{692}x^{10}+\alpha^{78}x^6+\alpha^{219}x^4+\alpha^{69}x^2$	ZP
	6.10	$\alpha^{91}x^{30}+x^{10}+x^2$	H[1]
	6.11	$\alpha^{91}x^{486}+x^{10}+x^2$	H[2]
	6.12	$\alpha^{182}x^{82}+2x^{10}+\alpha^{91}x^6+x^2$	H[3]
	6.13	$\alpha^{182}x^{82}+2x^{10}+\alpha^{273}x^6+x^2$	H[4]
	6.14	$\alpha^{91}x^{486}+\alpha^{182}x^{90}+2x^{10}+x^2$	H[5]
	6.15	$\alpha^{273}x^{486}+\alpha^{182}x^{90}+2x^{10}+x^2$	H[6]
	6.16	$\alpha^{273}x^{246}+\alpha^{182}x^{82}+\alpha^{91}x^6+x^2$	H[7]

Dim	**N^0**	**Representative**	**Family**
7	7.1	x^2	FF
	7.2	x^4	A
	7.3	x^{10}	A
	7.4	x^{28}	A
	7.5	$x^{10} + x^6 + 2x^2$	CM/DY
	7.6	$x^{10} + 2x^6 + 2x^2$	CM/DY
	7.7	x^{14}	CM
	7.8	x^{122}	CM
8	8.1	x^2	FF
	8.2	x^{14}	CM
	8.3	x^{122}	CM
	8.4	x^{1094}	CM
	8.5	$\alpha^{3994}x^{244} + \alpha^{5354}x^{84} + 2x^{82}$	BHB
	8.6	$\alpha^{264}x^{1458} + x^{82}$	B
	8.7	$\alpha^{3698}x^{2188} + \alpha^{1058}x^{108} + 2x^{82}$	BHB
	8.8	$x^{4374}+x^{2430}+x^{2214}+2x^{2190}+2x^{1458}+2x^{810}+x^{486}+$ $2x^{270} + x^{246} + x^{82} + x^{54} + x^{30} + x^{18} + x^{10} + x^6 + x^2$	CHK/ZP
	8.9	$\alpha^{3608}x^{1458} + \alpha^{3608}x^{738} + \alpha^{3810}x^{486} + \alpha^{3810}x^{246}$ $+\alpha^{3413}x^{162}+\alpha^{3413}x^{82}+\alpha^{3608}x^{18}+\alpha^{3810}x^6+\alpha^{2565}x^2$	CG
	8.10	$\alpha^{164}x^{1458} + \alpha^{164}x^{738} + \alpha^{950}x^{486} + \alpha^{950}x^{246}$ $+\alpha^{616}x^{162} + \alpha^{616}x^{82} + \alpha^{164}x^{18} + \alpha^{950}x^6 + \alpha^{6297}x^2$	CG

The representatives of the CCZ-inequivalent classes were classified in [30], and each representative is expressed with coefficients that are powers of an arbitrary primitive element $\alpha \in \mathbb{F}_{3^n}$ except for the inherited prime field elements 1 and 2.

Table 2.4: Order of the nuclei for the representatives over $\mathbb{F}_{3^n}$ for n from 6 to 8

Dim	$\mathbf{N}^0$	$\lvert N_m(\mathbb{S}')\rvert$	$\lvert K(\mathbb{S}')\rvert$	**Family**
6	6.1	3^6	3^6	FF
	6.2	3^2	3^2	A
	6.2	3^2	3^2	A
	6.3	3^3	3	D
	6.4	3^2	3	BHB
	6.5	3^2	3	LMPTB/BHB
	6.6	3	3	G
	6.7	3	3	CG
	6.8	–	–	CM
	6.9	3	3	ZP
	6.10	3^2	3	H[1]
	6.11	3^2	3	H[2]
	6.12	3^2	3	H[3]
	6.13	3^2	3	H[4]
	6.14	3^2	3	H[5]
	6.15	3^2	3	H[6]
	6.16	3^2	3	H[7]
7	7.1	3^7	3^7	FF
	7.2	3	3	A
	7.3	3	3	A
	7.4	3	3	A
	7.5	3	3	CM/DY
	7.6	3	3	CM/DY
	7.7	–	–	CM
	7.8	–	–	CM
8	8.1	3^8	3^8	FF
	8.2	–	–	CM
	8.3	–	–	CM
	8.4	–	–	CM
	8.5	3^2	3	BHB
	8.6	3^4	3^2	B
	8.7	3^2	3	BHB
	8.8	3^4	3	CHK/ZP
	8.9	3^4	3	CG
	8.10	3^4	3	CG

The orders of the nuclei of the corresponding semifields for the planar function representatives in Table 2.3 in dimensions 6 to 8. Note that for the representatives that are not quadratic, there is no corresponding semifield.

Chapter 3

Search for isotopic semifields in characteristic 3

3.1 Constructing isotopic planar functions

It is possible to extend infinite families of planar functions to include isotopic planar functions that are not CCZ-equivalent to those already in the family. This was done successfully in [14], where a known family, which was constructed from a family of APN quadrinomials redefined for odd prime characteristic, was extended up to isotopy. Not long after, Zhou showed in [43] that an instance of the LMPTB family was contained up to isotopy in the BHB family, which was perhaps a premonition for the results in [37] showing that the LMPTB family is contained in the BHB family up to isotopy. Therefore, the study of isotopic planar functions, that is, planar functions that correspond to isotopic semifields, can have an effect on the infinite family of planar functions that generate it.

By studying Theorem 2.3.3 one observes that any two isotopic commutative semifields $\mathbb{S}'_F = (\mathbb{F}_{p^n}, +, \circ_F)$ and $\mathbb{S}'_G = (\mathbb{F}_{p^n}, +, \circ_G)$ which correspond to two EA-inequivalent quadratic planar functions, F and G, cannot be strongly isotopic. In fact, there has to exist an isotopism between them of a particular form. Namely, there must exist some nonsquare element $\beta \in N_m(\mathbb{S}'_F)$, the middle nucleus of $\mathbb{S}'_F$, and linear permutations N and L such that

$$L(x \circ_G y) = (\beta \circ_F N(x)) \circ_F N(y), \quad \beta \in N_m(\mathbb{S}'_F). \tag{3.1}$$

For a known presemifield $\mathbb{S}_F = (\mathbb{F}_{p^n}, +, \star_F)$ defined by the presemifield operation as in Equation 2.1 using a known quadratic planar function F, one can attempt to construct an isotopic planar function G by first defining an isotopic presemifield, along the lines of Equation 3.1 as

$$L(x \star_G y) = (\beta \star_F N(x)) \star_F N(y). \tag{3.2}$$

Then their corresponding semifields can be constructed in the following way. Let $\mathbb{S}'_G = (\mathbb{F}_{p^n}, +, \circ_G)$ be the semifield corresponding to $\mathbb{S}_G$, with semifield operation $\circ_G$ defined as

$$(x \star_G a) \circ_G (a \star_G y) = x \star_G y,$$

for some fixed element $a \in \mathbb{F}_{p^n}^*$ and let the semifield $\mathbb{S}'_F = (\mathbb{F}_{p^n}, +, \circ_F)$ corresponding to $\mathbb{S}_F$ be defined by

$$(x \star_F b) \circ_F (b \star_F y) = x \star_F y,$$

for some fixed element $b \in \mathbb{F}_{p^n}^*$. Using these definitions for the semifield operations, Equation 3.2 becomes,

$$\begin{aligned} L(x \star_G y) = L((x \star_G a) \circ_G (a \star_G y)) &= (\beta \star_F N(x)) \star_F N(y) \\ &= ((\beta \star_F N(x)) \star_F b) \circ_F (b \star_F N(y)) \\ &= (((\beta \star_F b) \circ_F (b \star_F N(x))) \star_F b) \circ_F (b \star_F N(y)), \end{aligned}$$

which is an isotopism of the desired form between the corresponding semifields.

Therefore, we can proceed using the presemifield $\mathbb{S}_F$ and look for isotopic presemifields $\mathbb{S}_G$ of the form $(L, \beta \star_F N, N)$. Then, one can retrieve the isotopic planar function G from the presemifield operation $\star_G$ using the canonical construction in Equation 2.2. That is,

$$\begin{aligned} G(x) &= \frac{1}{2}(x \star_G x) \\ &= \frac{1}{2} L^{-1}((\beta \star_F N(x)) \star_F N(x)). \end{aligned}$$

And for a known quadratic planar function F, the presemifield operation of its corresponding commutative presemifield can be defined as in Equation 2.1.

$$x \star_F y = F(x + y) - F(x) - F(y).$$

By iterating over the possible linear permutations L and N, and nonsquare elements β in the middle nucleus of the semifield $\mathbb{S}'_F$ corresponding to the presemifield $\mathbb{S}_F$, it is possible one can retrieve an EA-inequivalent planar function G. With this method, we have chosen to limit our search to linear permutations L and N, with L being the identity map ($id : x \to x$) and permutations $N : x \to x^{p^i}$ for $0 \leq i < n$, where n is the dimension of the finite field.

However, if such a search does not yield a CCZ-inequivalent planar function, one can also attempt the same search with a planar function F_2 that is linear equivalent to F. That is, given a quadratic planar function F, one may take linear permutations $B1$ and $B2$ and define a linear equivalent function $F_2(x) = B1(F(B2(x)))$ which, if it is planar, one can then perform a search for isotopic planar functions G to F_2 in the same way. For our purposes, we used linear permutations $B1$ and $B2$ that were constructed in the following way.

Take an arbitrary element $a \in \mathbb{F}_{p^n}^*$, and define a linear permutation B as

$$B(x) = x \star_F a \tag{3.3}$$

By the definition of a planar function, $B(x) = x \star_F a = F(x + a) - F(x) - F(a)$ is a bijection on $\mathbb{F}_{p^n}$ for all $a \in \mathbb{F}_{p^n}^*$, and if B is linear, then it is a linear permutation over $\mathbb{F}_{p^n}$. Then one can compose B with itself repeatedly, that is, define $B^2(x) := B(B(x))$, $B^3(x) := B(B^2(x))$ and so on, until many of these compositions have been collected. By the finiteness of the finite field $\mathbb{F}_{p^n}$,

this process must terminate. Meaning, $B^k(x) = B(x) \bmod x^{p^n} - x$ for some natural number k. Then, since any composition of two linear permutation polynomials is itself a linear permutation polynomial, at every instance $1 \leq i \leq k$, B^k is a linear permutation [34]. Now take any two of these permutations, $B_1(x) = B^i$, and $B_2(x) = B^j$, and attempt to find a CCZ-inequivalent isotopic planar function G using $F_2(x) = B_1(F(B_2(x)))$. It is necessary for the permutation polynomials B^k to be linear, as the structure of the "right orbits" of the planar function F is invariant under linear equivalence [32]. This requirement is needed so that we can check G for CCZ-equivalence with F_2 using the fast algorithm explained in Chapter 3.2. For the choices of a in Equation 3.3, we chose to limit them to elements of the middle nucleus of the semifield corresponding to the planar function F.

3.2 Narrowing down the search

We have chosen in this thesis to perform a search for isotopic planar functions using the method explained in Chapter 3.1 over finite fields in characteristic 3 and dimension $n \leq 8$.

By combining Theorem 2.3.3 and Theorem 2.3.2 in Chapter 2, we deduce the following. Given a quadratic planar function F, then an isotopic planar function G which is CCZ-inequivalent to F can only exist if $\frac{m}{k}$ is even, where p^m, and p^k are the orders of the middle nucleus and nucleus, respectively, of the semifield corresponding to F. Additionally, Coulter and Henderson in [19] showed that in fact, the prime power order of the finite field on which the semifield is defined must also be even. Hence, we can restrict ourselves to only searching for isotopic planar functions in even dimensions n and that correspond to semifields which fulfil the Coulter-Henderson conditions in Theorem 2.3.3 on the nucleus and middle nucleus.

Looking at the analytic results for the orders of the nuclei of the known families of planar functions and semifields in Table 2.2, the following families can be worth investigating in our search in characteristic 3. From the table we can see that the available families are BHB, LMPTB and ZP with trivial automorphism σ, as well as D, B and CG in doubly even dimensions. We know that LMPTB and ZP with trivial σ are contained in BHB, as proven in [37] and [44]. Additionally, many instances from these remaining families are CCZ-equivalent, and therefore we make use of the representatives of CCZ-inequivalent planar functions in Table 2.3. When referring to these representatives in this thesis, we shall call them by their indexes, $d.m$, as listed in the table.

Looking at the CCZ-inequivalent representatives in dimension 4, the only quadratic representative which does not correspond to a finite field in dimension 4 is function 4.3. And since it is from the BHB family, it has already been extended up to isotopy. Therefore, there are no functions for us to investigate in dimension 4. However, in dimension 6 and 8 there are more functions that fulfil the Coulter-Henderson criteria.

By inspection of Table 2.3, the remaining representatives for which a search using the method laid out in Chapter 3.1 might result in CCZ-inequivalent planar functions are the following CCZ-inequivalent representatives in dimension 6 and 8.

3^6 6.10 : $F(x) = \alpha^{91}x^{30} + x^{10} + x^2$

6.11 : $F(x) = \alpha^{91}x^{486} + x^{10} + x^2$

6.12 : $F(x) = \alpha^{182}x^{82} + 2x^{10} + \alpha^{91}x^6 + x^2$

6.13 : $F(x) = \alpha^{182}x^{82} + 2x^{10} + \alpha^{273}x^6 + x^2$

6.14 : $F(x) = \alpha^{91}x^{486} + \alpha^{182}x^{90} + 2x^{10} + x^2$

6.15 : $F(x) = \alpha^{273}x^{486} + \alpha^{182}x^{90} + 2x^{10} + x^2$

6.16 : $F(x) = \alpha^{273}x^{246} + \alpha^{182}x^{82} + \alpha^{91}x^6 + x^2$

3^8 8.5 : $F(x) = \alpha^{3994}x^{244} + \alpha^{5354}x^{84} + 2x^{82}$

8.6 : $F(x) = \alpha^{264}x^{1458} + x^{82}$

8.7 : $F(x) = \alpha^{3698}x^{2188} + \alpha^{1058}x^{108} + 2x^{82}$

8.8 : $F(x) = x^{4374} + x^{2430} + x^{2214} + 2x^{2190} + 2x^{1458} + 2x^{810} + x^{486} + 2x^{270} + x^{246} + x^{82} + x^{54} + x^{30} + x^{18} + x^{10} + x^6 + x^2$

8.9 : $F(x) = \alpha^{3608}x^{1458} + \alpha^{3608}x^{738} + \alpha^{3810}x^{486} + \alpha^{3810}x^{246} + \alpha^{3413}x^{162} + \alpha^{3413}x^{82} + \alpha^{3608}x^{18} + \alpha^{3810}x^6 + \alpha^{2565}x^2$

8.10 : $F(x) = \alpha^{164}x^{1458} + \alpha^{164}x^{738} + \alpha^{950}x^{486} + \alpha^{950}x^{246} + \alpha^{616}x^{162} + \alpha^{616}x^{82} + \alpha^{164}x^{18} + \alpha^{950}x^6 + \alpha^{6297}x^2$

In the thesis by Haukenes, she also listed the invariants corresponding to the known CCZ-inequivalent planar functions in dimensions 2 to 8, including the orders of the nuclei of their corresponding semifields. In that thesis, she also made use of the algorithm checking CCZ-equivalence between planar functions first presented in [32]. It makes use of the pre-calculated "right orbit" representatives, here referred to simply as "orbits" representatives, in order to check for linear equivalence between planar functions. That is, taking a planar function F for which the orbits are known, and constructing another planar function G with the method in 3.2, then the time spent checking whether F and G are linear equivalent can be significantly reduced, especially in the negative case [32]. This owes to the fact that the structure of the orbits of a planar function is invariant under linear equivalence [32].

The orbits for the planar functions in dimension 3 to 6 (except for the sporadic Haukenes functions) are listed in [32]. The remaining orbits for the planar function representatives in dimensions 7 and 8, and the sporadic Haukenes functions in dimension 6 are found in [30]. However, one of the orbit representatives in dimension 8 is missing in [30, Table 3.5]. In particular, for the function listed as 8.10, the orbits were not listed due to time constraints in the project and the time required to compute them. The representatives of the orbits have been found here to be the 410 elements, given as powers of an arbitrary primitive element α in the finite field $\mathbb{F}_{3^8}$.

$\{\alpha^i : i$ in [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 50, 51, 53, 54, 56, 57, 58, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 84, 85, 86, 87, 88, 89, 90, 92, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 111, 112,

113, 114, 115, 116, 117, 118, 120, 121, 122, 124, 125, 126, 128, 129, 132, 133, 134, 136, 138, 139, 140, 141, 143, 144, 145, 146, 147, 149, 150, 151, 152, 153, 154, 155, 156, 157, 159, 161, 162, 163, 164, 166, 167, 168, 169, 170, 171, 172, 173, 174, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 188, 189, 190, 195, 196, 197, 198, 199, 200, 204, 206, 207, 211, 212, 213, 214, 215, 216, 217, 218, 220, 221, 222, 223, 225, 226, 227, 228, 229, 232, 233, 235, 236, 237, 238, 240, 241, 242, 243, 244, 246, 249, 251, 252, 253, 254, 256, 258, 259, 260, 267, 269, 272, 275, 276, 277, 278, 281, 282, 284, 286, 288, 289, 292, 293, 294, 295, 296, 298, 300, 302, 305, 307, 311, 313, 314, 316, 318, 323, 326, 327, 328, 330, 331, 337, 338, 340, 342, 343, 346, 347, 348, 351, 353, 360, 361, 366, 368, 371, 372, 374, 376, 377, 378, 379, 380, 382, 384, 386, 395, 397, 401, 402, 404, 405, 407, 414, 415, 416, 419, 420, 422, 426, 430, 431, 436, 440, 441, 444, 446, 456, 458, 468, 469, 475, 478, 480, 491, 494, 508, 510, 511, 512, 517, 522, 524, 530, 532, 535, 536, 542, 546, 548, 550, 561, 565, 566, 567, 569, 571, 572, 573, 578, 579, 581, 582, 583, 586, 589, 590, 595, 596, 599, 600, 606, 607, 608, 610, 633, 639, 642, 643, 646, 647, 661, 669, 682, 686, 687, 688, 696, 699, 706, 710, 712, 717, 728, 736, 737, 738, 740, 741, 747, 750, 752, 753, 756, 757, 763, 770, 787, 811, 812, 825, 830, 841, 846, 850, 851, 856, 866, 890, 901, 904, 920, 921, 927, 934, 942, 975, 976, 981, 989, 996, 1005, 1020, 1043, 1049, 1052, 1106, 1109, 1116, 1160, 1260, 1337, 1385] }.

In the CCZ-classification of the known planar functions in [30], the method used for finding the order of the middle nucleus and nucleus hinged upon the assumption that the middle nucleus and nucleus were subfields (i.e a subset and a field) of the finite field on which the semifield is defined. However, as mentioned in Chapter 2.2, this is not always the case, and therefore the method used in [30] does not always find the correct orders for the nuclei. Therefore, we have in this thesis performed a direct search for the elements of the middle nucleus and nucleus of the quadratic planar function representatives in dimensions 6 to 8, presented in Table 2.4, and found that these corrections are in correspondence with the analytic results in Table 2.2. In particular, we have found the order of the middle nuclei of representatives 6.4 and 6.5 to both be 3^2, and for the representative 8.6, the order of the nucleus is 3^2, corresponding to $q = 3^2$ in Table 2.2.

We do not perform any search beyond dimension 8. Our calculations are performed in MAGMA V2.24-3 on a server designed for large memory intensive computations, with 56 cores at 2.6 GHz and around 500 GBs of RAM. However, already in dimension 8, the computational time required to check for equivalence can take a long time. Additionally, in order to use the fast algorithm, that is, checking for equivalence using the corresponding orbits of the representatives, it requires the calculation of said orbits. Calculating the orbits of a planar function in dimension 8 can take multiple days, and in the case of the representative 8.10, which had 410 orbits, it took almost four months to complete. Furthermore, there is to our knowledge no classification up to CCZ-equivalence of the planar functions in characteristic 3 and dimension 10 at the time of this writing.

In our computational search we are able to find isotopic planar functions which are not CCZ-equivalent for the representatives 6.4, 6.10, 6.12, 6.14 and 8.9. In essence, six of the sporadic Haukenes functions in dimension 6 form three isotopic equivalence classes, and the two CCZ-inequivalent Cohen-Ganley representatives 8.9 and 8.10 are also isotopic equivalent. Additionally,

we were able to reaffirm that representatives 6.4 and 6.5 are isotopic, as was first shown by Zhou in 2010 [43].

3.3 Refined classification of isotopic semifields

Here we present the results from our search for isotopic commutative semifields using the method described in Section 3.1. The isotopisms found in dimension 6 and 8 are given explicitly, in the form of linear permutations $(L, \beta \star N, N)$. Note that each chosen representative of a CCZ-equivalence class in Figures 3.1 and 3.2 is listed with a given family which generates it, but as previously mentioned, it is possible for another family to generate them as well.

In Figure 3.1 and 3.2, we show how some of the CCZ-inequivalent planar function classes in dimensions 6 and 8 are isotopic to one another. It should also be remarked that Figure 3.1 and 3.2 are not necessarily complete. That is, it is still possible, if not probable, that there exist more EA-inequivalent planar functions, representing classes of strongly isotopic semifields, that have not yet been found. For instance, we expected some BHB and LMPTB instances to be isotopic, since the BHB family has already been extended up to isotopism and contains LMPTB. However, we were unable to find such an isotopism for the given representatives of the CCZ-equivalence classes with the method used here. Additionally, for representatives 8.6 and 8.8 we were unable to find isotopic functions.

For the planar functions in dimension 4, we do not discover any new isotopic planar functions. However, in dimension 6, we discover three new isotopisms between the known CCZ-inequivalent classes, shown in Figure 3.1 along with a previously known isotopism between representatives 6.4 and 6.5 found in [43]. In dimension 8 we are also able to show that the planar functions 8.9 and 8.10 are isotopic as shown in Figure 3.2.

3.3.1 Dimension 6

For the two DO planar functions by Haukenes 6.10 and 6.11, the isotopism can be found in the following way. Let function 6.10 be represented as

$$F(x) = \alpha^{91}x^{30} + x^{10} + x^2,$$

and take the linear permutations $B_1(x) = 2x^9 + 2x$ and $B_2(x) = \alpha^{637}x^{27} + \alpha^{182}x^9 + \alpha^{637}x^3$ and define a linear equivalent planar function F_2 as

$$\begin{aligned} F_2(x) &= B_1(F(B_2(x))) \\ &= \alpha^{546}x^{486} + x^{324} + \alpha^{273}x^{270} + \alpha^{546}x^{252} + 2x^{246} + \alpha^{273}x^{244} + \alpha^{91}x^{162} \\ &+ x^{108} + \alpha^{546}x^{90} + \alpha^{182}x^{84} + \alpha^{546}x^{82} + \alpha^{182}x^{30} + \alpha^{273}x^{28} + x^{18} \\ &+ \alpha^{91}x^{12} + \alpha^{273}x^{10} + \alpha^{182}x^6 + x^4 + \alpha^{637}x^2. \end{aligned}$$

Then let $\beta = \alpha^{91} \in N_m(\mathbb{S}'_{F_2})$ a nonsquare, and define a planar function G isotopic to F_2 through the isotopism $(id, \beta \star_{F_2} id, id)$ accordingly

$$\begin{aligned} G(x) &= \frac{1}{2}((\beta \star_{F_2} x) \star_{F_2} x) \\ &= \alpha^{91}x^{486} + \alpha^{637}x^{324} + \alpha^{273}x^{270} + \alpha^{91}x^{252} + \alpha^{91}x^{246} + 2x^{244} \\ &+ \alpha^{182}x^{162} + 2x^{108} + \alpha^{273}x^{90} + 2x^{84} + \alpha^{546}x^{82} + \alpha^{182}x^{54} + \alpha^{273}x^{36} \\ &+ \alpha^{455}x^{30} + \alpha^{91}x^{28} + \alpha^{637}x^{12} + \alpha^{182}x^{10} + \alpha^{637}x^6 + \alpha^{91}x^4 + \alpha^{182}x^2. \end{aligned}$$

Then F is linear equivalent to 6.11 given as

$$F'(x) = \alpha^{91}x^{486} + x^{10} + x^2,$$

through the linear permutations

$$A_1(x) = \alpha^{273}x^{243} + \alpha^{322}x^{81} + \alpha^{273}x^{27} + \alpha^{714}x^9 + \alpha^{273}x^3 + \alpha^{602}x$$

and

$$A_2(x) = \alpha^{602}x^{243} + \alpha^{399}x^{81} + \alpha^{322}x^{27} + \alpha^{679}x^9 + \alpha^{714}x^3 + \alpha^{287}x.$$

That is,

$$F'(x) = A_1(G(A_2(x))).$$

The planar functions 6.12 and 6.13 are also isotopic. More precisely, looking at the planar function 6.12,

$$F(x) = \alpha^{182}x^{82} + 2x^{10} + \alpha^{91}x^6 + x^2$$

and taking the linear permutations

$$B_1(x) = \alpha^{637}x^{243} + \alpha^{455}x^{81} + \alpha^{455}x^9 + \alpha^{273}x^3 + \alpha^{273}x$$

and

$$B_2(x) = \alpha^{637}x^{243} + \alpha^{182}x^{81} + \alpha^{273}x^{27} + \alpha^{546}x^9 + \alpha^{637}x^3 + x,$$

then let a linear equivalent planar function F_2 be defined as

$$\begin{aligned} F_2(x) &= B_1(F(B_2(x))) \\ &= \alpha^{637}x^{486} + x^{324} + \alpha^{273}x^{270} + \alpha^{273}x^{252} + \alpha^{182}x^{246} + \alpha^{455}x^{244} \\ &+ \alpha^{182}x^{162} + \alpha^{182}x^{108} + \alpha^{455}x^{90} + x^{82} + \alpha^{182}x^{54} + \alpha^{637}x^{36} + x^{30} \\ &+ \alpha^{637}x^{28} + \alpha^{637}x^{18} + \alpha^{637}x^{12} + 2x^{10} + \alpha^{273}x^6 + \alpha^{182}x^4 + \alpha^{546}x^2. \end{aligned}$$

Then construct an isotopic planar function G from F_2 with isotopism $(id, \beta \star_{F_2} id, id)$, and let $\beta = \alpha^{91} \in N_m(\mathbb{S}_{F_2})$ such that

$$\begin{aligned} G(x) &= \frac{1}{2}(\beta \star_{F_2} x) \star_{F_2} x \\ &= \alpha^{91}x^{486} + \alpha^{182}x^{270} + \alpha^{91}x^{252} + \alpha^{273}x^{246} + x^{244} + 2x^{162} \\ &+ \alpha^{273}x^{108} + \alpha^{637}x^{90} + \alpha^{91}x^{84} + \alpha^{546}x^{82} + \alpha^{637}x^{54} + \alpha^{637}x^{36} \\ &+ \alpha^{546}x^{30} + \alpha^{637}x^{28} + \alpha^{637}x^{12} + \alpha^{455}x^{10} + \alpha^{182}x^6 + \alpha^{637}x^4. \end{aligned}$$

Then G is linear equivalent to 6.13

$$F'(x) = \alpha^{182}x^{82} + 2x^{10} + \alpha^{273}x^6 + x^2$$

through the linear permutations

$$A_1(x) = \alpha^{182}x^{243} + x^{81} + \alpha^{546}x^{27} + \alpha^{182}x^9 + \alpha^{182}x$$

and

$$A_2(x) = \alpha^{273}x^{243} + \alpha^{546}x^{81} + \alpha^{637}x^{27} + x^9 + \alpha^{637}x^3 + \alpha^{182}x.$$

For the planar function 6.14 defined as

$$F(x) = \alpha^{91}x^{486} + \alpha^{182}x^{90} + 2x^{10} + x^2,$$

one can take the linear permutations

$$B_1(x) = \alpha^{455}x^{81} + \alpha^{273}x^{27} + \alpha^{273}x^9 + \alpha^{637}x^3 + \alpha^{455}x$$

and

$$B_2(x) = \alpha^{637}x^{243} + \alpha^{546}x^{81} + \alpha^{273}x^{27} + \alpha^{637}x^3 + \alpha^{637}x,$$

and define a linear equivalent planar function F_2 as

$$\begin{aligned}
F_2(x) &= B_1(F(B_2(x))) \\
&= x^{486} + \alpha^{91}x^{324} + \alpha^{182}x^{270} + \alpha^{455}x^{252} + \alpha^{637}x^{246} \\
&+ x^{244} + \alpha^{546}x^{162} + \alpha^{182}x^{108} + \alpha^{182}x^{90} + \alpha^{273}x^{84} \\
&+ \alpha^{273}x^{82} + \alpha^{455}x^{54} + \alpha^{182}x^{36} + \alpha^{546}x^{30} \\
&+ 2x^{28} + \alpha^{273}x^{18} + \alpha^{182}x^{12} + \alpha^{455}x^{10} + \alpha^{182}x^6 + \alpha^{91}x^4.
\end{aligned}$$

Then there is an isotopic planar function G to F_2 through isotopism $(id, \beta \star_{F_2} id, id)$, where $\beta = \alpha^{91} \in N_m(\mathbb{S}_{F_2})$ a nonsquare, given as

$$\begin{aligned}
F(x) &= \frac{1}{2}(\beta \star_{F_2} x) \star_{F_2} x \\
&= \alpha^{273}x^{324} + \alpha^{637}x^{270} + \alpha^{637}x^{252} + \alpha^{273}x^{244} \\
&+ 2x^{162} + \alpha^{91}x^{108} + \alpha^{546}x^{90} + \alpha^{637}x^{82} + 2x^{54} + \alpha^{182}x^{36} \\
&+ x^{30} + x^{28} + \alpha^{455}x^{18} + \alpha^{182}x^{12} + \alpha^{637}x^6,
\end{aligned}$$

which is linear equivalent to 6.15

$$F'(x) = \alpha^{273}x^{486} + \alpha^{182}x^{90} + 2x^{10} + x^2$$

by the linear permutations

$$A_1(x) = \alpha^{182}x^{81} + \alpha^{182}x^{27} + x^9 + \alpha^{546}x^3 + \alpha^{182}x$$

and

$$A_2(x) = \alpha^{637}x^{243} + \alpha^{546}x^{81} + \alpha^{273}x^{27} + \alpha^{637}x^3 + \alpha^{637}x.$$

As mentioned in Chapter 2.1, it is not always true that an isotopic shift F_L of a planar function F is isotopic to F. However, if two planar functions F and G are isotopic, then by Theorem 2.3.4 there must exist some isotopic shift F_L that is EA-equivalent to G. In the case of the planar function representatives, 6.12, 6.13 and 6.14 and 6.15, their isotopic shifts take on a particularly satisfying form. Taking the linear permutation $T(x) = \alpha^{91}x$, then the isotopic shift $\frac{1}{2}F_T$ for both 6.12 and 6.14, result in planar functions that are linear equivalent to 6.13 and 6.15, respectively, through the linear permutations $A_1(x) = \alpha^{91}x$ and $A_2(x) = x$.

We are also able to reaffirm that the planar function representatives 6.5 and 6.4 in [30] are isotopic equivalent, as was first shown in [43]. Let the planar function 6.5 be represented as

$$F(x) = 2x^{270} + x^{246} + 2x^{90} + x^{82} + x^{54} + 2x^{30} + x^{10} + x^2 \tag{3.4}$$

and taking the isotopism $(L, M, N) = (id, \alpha^{91} \star_F id, id)$, then we get

$$\begin{aligned} G(x) &= \frac{1}{2}(\alpha^{91} \star_F x) \star_F x \\ &= \alpha^{637}x^{270} + \alpha^{273}x^{246} + \alpha^{455}x^{90} + \alpha^{91}x^{82} + \alpha^{273}x^{54} \\ &+ \alpha^{637}x^{30} + \alpha^{91}x^{10} + \alpha^{91}x^2, \end{aligned}$$

which is EA-equivalent to 6.4 represented as

$$F'(x) = \alpha^{75}x^{2214} + x^{756} + \alpha^{205}x^{82} + x^{28},$$

through the linear permutations $A_1(x) = \alpha^{140}x^{243} + \alpha^{672}x^{27} + \alpha^{56}x^9 + \alpha^{308}x$ and $A_2(x) = \alpha^{381}x^{81} + \alpha^{368}x^3$.

Looking at the orders of the nuclei of the functions for which an isotopism has not been found in Table 2.4, one sees that the classification into isotopic equivalence classes for the known planar functions in $\mathbb{F}_{3^6}$ is nearly complete, with the possible exception of representative 6.16.

3.3.2 Dimension 8

We found that the two CCZ-inequivalent representatives in dimension 8 of Cohen-Ganley, namely functions 8.9 and 8.10, are also isotopic through isotopism $(L, M, N) = (id, \alpha^{3526} \star_F id, id)$, where $\beta = \alpha^{3526} \in N_m(\mathbb{S}'_F)$ a nonsquare. However, we did not need to perform any linear permutations to these planar functions in order to find the isotopism. That is, function 8.9

$$\begin{aligned} F(x) = &\alpha^{3608}x^{1458} + \alpha^{3608}x^{738} + \alpha^{3810}x^{486} + \alpha^{3810}x^{246} \\ &+ \alpha^{3413}x^{162} + \alpha^{3413}x^{82} + \alpha^{3608}x^{18} + \alpha^{3810}x^6 + \alpha^{2565}x^2 \end{aligned}$$

is isotopic to the planar function,

$$\begin{aligned} G(x) &= \frac{1}{2}(\beta \star_F x) \star_F x \\ &= \alpha^{5822}x^{1458} + \alpha^{5822}x^{738} + \alpha^{4548}x^{486} + \alpha^{4548}x^{246} \\ &+ \alpha^{3659}x^{162} + \alpha^{3659}x^{82} + \alpha^{5822}x^{18} + \alpha^{4548}x^{6} + \alpha^{2811}x^{2} \end{aligned}$$

which is again linear equivalent to 8.10

$$\begin{aligned} F'(x) &= \alpha^{164}x^{1458} + \alpha^{164}x^{738} + \alpha^{950}x^{486} + \alpha^{950}x^{246} \\ &+ \alpha^{616}x^{162} + \alpha^{616}x^{82} + \alpha^{164}x^{18} + \alpha^{950}x^{6} + \alpha^{6297}x^{2} \end{aligned}$$

through the linear permutations $A_1(x) = \alpha^{2563}x^{729} + \alpha^{3937}x^9$ and $A_2(x) = \alpha^{4027}x^{729} + \alpha^{3501}x^9$.

The remaining functions in dimension 8 did not yield linear inequivalent planar functions using this method. That is, they were isotopic, but also strongly isotopic. However, it is still possible to find more isotopic planar functions in dimension 8 as there are more representatives fulfilling the Coulter-Henderson conditions from Theorem 2.3.3.

All our searches were performed using MAGMA and the algorithm from [32] as well as the pre-calculated orbits found in [30] and [32] for checking for EA and linear equivalence. The time spent checking for equivalence was thereby reduced significantly, and in total the time spent on the search took about one month. Most of the time spent on this project was dedicated to writing the necessary MAGMA code to find the elements belonging to the middle nucleus of the semifield and for constructing the isotopic planar functions.

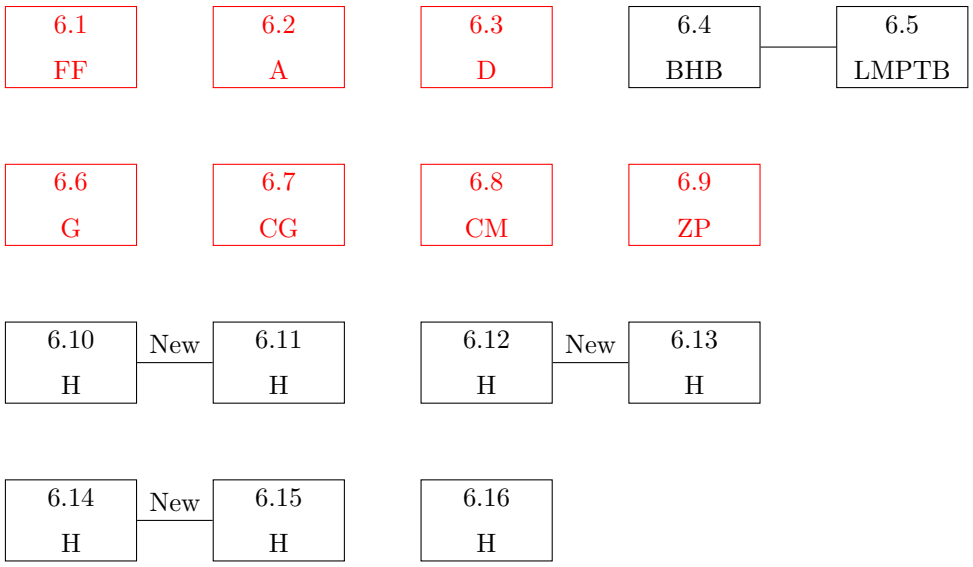


Figure 3.1: The isotopic semifield classes of characteristic 3 and dimension 6, given by representatives of the CCZ-inequivalent classes of planar functions from the paper in [30], where edges connect isotopic planar function representatives. Red colour is used for the representatives that do not fulfil the Coulter-Henderson conditions from Theorem 2.3.3. The isotopism between 6.4 and 6.5 was first discovered by Zhou in [43]. The classification of the known planar functions in $\mathbb{F}_{3^6}$ into isotopic equivalence classes is almost complete, with the possible exception of representative 6.16.

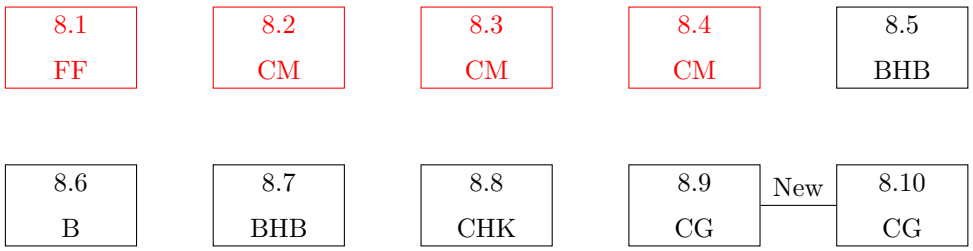


Figure 3.2: The isotopic semifield classes of characteristic 3 and dimension 8, given by representatives of the CCZ-inequivalent classes of planar functions, where edges connect isotopic planar function representatives. Red colour is used for the representatives that do not fulfil the Coulter-Henderson conditions from Theorem 2.3.3. The representative listed as 8.8 was recently discovered to be CCZ-equivalent to an instance of the ZP family in [30].

Chapter 4

Conclusion

The construction of new planar functions up to CCZ-equivalence is an important and difficult problem. One potential way of obtaining new quadratic planar functions is by exploring the isotopism classes of their corresponding commutative semifields. This has been used in [14] but to the best of our knowledge, there has been no systematic study of the possibility of obtaining new planar functions from the rest of the known planar instances.

In this thesis, we have applied the Coulter-Henderson conditions from [19] to eliminate a number of the known families of planar functions by showing that their isotopism classes only contain a single CCZ-equivalence class. In particular, we have concluded that no new planar functions up to CCZ-equivalence can be obtained in this way for odd values of n, and that the only families whose instances can lead to CCZ-inequivalent functions via isotopism are Budaghyan-Helleseth, Bierbrauer, Dickson and Cohen-Ganley families. Furthermore, amongst these families, the only ones that can lead to new CCZ-inequivalent planar functions to the known ones are the Bierbrauer, Dickson and Cohen-Ganley families, all in doubly even dimensions.

For instances from the remaining families and sporadic instances, we have run computational experiments over $\mathbb{F}_{3^n}$ in order to search for functions isotopic to them. We have found isotopisms between some of the known CCZ-inequivalent representatives for $n = 6$ and $n = 8$. For others, we have not been able to determine whether their isotopism class can contain another CCZ-class, however we have computationally shown that this isotopism can not be of a particular form. Based on these results, we have given a partial classification of the known planar functions over $\mathbb{F}_{3^n}$ for $n \leq 8$ up to isotopism.

There are of course several directions for further studies. One would be to run more computational experiments in order to resolve the structure of the isotopism classes of those instances that we were not able to fully determine. Another avenue would be to attempt a similar classification for dimensions n greater than 8. We note that the lowest such dimension would be $n = 10$ (since for odd dimensions, we have discussed that we can never obtain CCZ-inequivalent instances), and such a study is conditioned on the existence of a classification of planar functions over $\mathbb{F}_{3^{10}}$ up to CCZ-equivalence, which is not available at the moment and which would require a significant amount of computation.

Another natural generalization would be to extend the study to odd characteristics other than 3. Going to higher characteristics (as well as higher dimensions) is a challenging task because the available algorithms require significant time and computational resources that were outside the capacity of this project.

Bibliography

[1] Albert, A. A. (1961). Generalized twisted fields. *Pacific J. Math*, 11(1), 1-8.

[2] Albert, A. A. (1961). Isotopy for generalized twisted fields. *An. Acad. Brasil. Ci*, 33(265-275), 227-229.

[3] At, N., & Cohen, S. D. (2008). A new tool for assurance of perfect nonlinearity. *In Sequences and Their Applications-SETA 2008: 5th International Conference Lexington, KY, USA, September 14-18, 2008 Proceedings 5* (pp. 415-419). Springer Berlin Heidelberg.

[4] Bader, L., Lunardon, G., & Pinneri, I. (1999). A new semifield flock. *Journal of Combinatorial Theory*, Series A, 86(1), 49-62.

[5] Bierbrauer, J. (2009). New commutative semifields and their nuclei. *In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 18th International Symposium, AAECC-18 2009, Tarragona, Spain, June 8-12, 2009. Proceedings 18* (pp. 179-185). Springer Berlin Heidelberg.

[6] Bierbrauer, J. (2010). New semifields, PN and APN functions. *Designs, Codes and Cryptography*, 54(3), 189-200.

[7] Bierbrauer, J. (2011). Commutative semifields from projection mappings. *Designs, Codes and Cryptography*, 61, 187-196.

[8] Biham, E., & Shamir, A. (1991) Differential cryptanalysis of DES-like cryptosystems. *In Advances in Cryptology – CRYPTO 1990, Lecture Notes in Computer Science, vol. 537*, Springer Berlin Heidelberg, pp. 2–21. 1, 2.1.3

[9] Budaghyan, L. (2015). *Construction and analysis of cryptographic functions*. Springer.

[10] Budaghyan, L., Carlet, C., & Pott, A. (2006). New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3), 1141-1152.

[11] Budaghyan, L., Carlet, C., & Leander, G. (2008). Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9), 4218-4229.

[12] Budaghyan, L., Calderini, M., Carlet, C., Coulter, R. S., & Villa, I. (2020). Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8), 5299-5309.

[13] Budaghyan, L., & Helleseth, T. (2008, September). New perfect nonlinear multinomials over F for any odd prime p. *In International Conference on Sequences and Their Applications* (pp. 403-414). Berlin, Heidelberg: Springer Berlin Heidelberg.

[14] Budaghyan, L., & Helleseth, T. (2011). New commutative semifields defined by new PN multinomials. *Cryptography and communications*, 3, 1-16.

[15] Budaghyan, L., Helleseth, T., & Kaleyski, N. (2020). A New Family of APN Quadrinomials. *IEEE Transactions on Information Theory*, 66(11), 7081-7087. https://doi.org/10.1109/TIT.2020.3007513

[16] Carlet, C., Charpin, P., & Zinoviev, V. (1998). Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15, 125-156.

[17] Cohen, S. D., & Ganley, M. J. (1982). Commutative semifields, two dimensional over their middle nuclei. *Journal of Algebra*, 75(2), 373-385.

[18] Coulter, R. S. (1999). Planar functions and related topics in finite fields. *Bulletin of the Australian Mathematical Society*, 59(1), 173-174.

[19] Coulter, R. S., & Henderson, M. (2008). Commutative presemifields and semifields. *Advances in Mathematics*, 217(1), 282-304.

[20] Coulter, R. S., Henderson, M., & Kosick, P. (2007). Planar polynomials for commutative semifields with specified nuclei. *Designs, Codes and Cryptography*, 44, 275-286.

[21] Coulter, R. S., & Kosick, P. (2010). Commutative semifields of order 243 and 3125. *Finite fields: theory and applications*, 518, 129-136.

[22] Coulter, R. S., & Matthews, R. W. (1997). Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2), 167-184.

[23] Dembowski, P., & Ostrom, T. G. (1968). Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3), 239–258. https://doi.org/10.1007/BF01111042

[24] Dickson, L. E. (1905). On finite algebras. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1905, 358-393.

[25] Dickson, L. E. (1906). Linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(3), 370-390.

[26] Dickson, L. E. (1906). On commutative linear algebras in which division is always uniquely possible, *Transactions of the American Mathematical Society*, 7 (1906), 514-522.

[27] Ding, C., Wang, Z., & Xiang, Q. (2007). Skew Hadamard difference sets from the Ree–Tits slice symplectic spreads in PG $(3, 3^{2h+1})$. *Journal of Combinatorial Theory, Series A*, 114(5), 867-887.

[28] Elliott, J. E. H. (1965). Relative difference sets (Doctoral dissertation, University of Miami).

[29] Ganley, M. J. (1981). Central weak nucleus semifields. *European Journal of Combinatorics*, 2(4), 339-347.

[30] Haukenes. (2022). Classification and computational search for planar functions in characteristic 3. *The University of Bergen*. https://hdl.handle.net/11250/3001135

[31] Helleseth, T., & Sandberg, D. (1997). Some power mappings with low differential uniformity. *Applicable Algebra in Engineering, Communication and Computing*, 8, 363-370.

[32] Ivkovic, I., & Kaleyski, N. (2022). Deciding and reconstructing linear equivalence of uniformly distributed functions. *Cryptology ePrint Archive*.

[33] Knuth, D. E. (1963). Finite semifields and projective planes (Doctoral dissertation, California Institute of Technology).

[34] Lidl, R., Niederreiter, H., & Cohn, P. M. (1997). *Finite fields: Vol. volume 20 (Second edition.)*. Cambridge University Press. Chapter 7. p.351

[35] Lunardon, G., Marino, G., Polverino, O., & Trombetti, R. (2011). Symplectic semifield spreads of PG (5, q) and the Veronese surface. *Ricerche di matematica*, 60(1), 125-142.

[36] Lunardon, G., Marino, G., Polverino, O., & Trombetti, R. (2009). Symplectic spreads and quadric Veroneseans. *Preprint*.

[37] Marino, G., & Polverino, O. (2012). On the nuclei of a finite semifield. *Theory and applications of finite fields*, 579, 123-141.

[38] Marino, G., & Polverino, O. (2012). On isotopisms and strong isotopisms of commutative presemifields. *Journal of Algebraic Combinatorics*, 36, 247-261.

[39] Penttila, T., & Williams, B. (2000). Ovoids of parabolic spaces. *Geometriae Dedicata*, 82, 1-19.

[40] Pott, A. (2016). Almost perfect and planar functions. *Designs, Codes, and Cryptography*, 78(1), 141–195. https://doi.org/10.1007/s10623-015-0151-x

[41] Pott, A., Schmidt, K. U., & Zhou, Y. (2014). Semifields, relative difference sets, and bent functions. *Algebraic curves and finite fields*, 16, 161-178.

[42] Zha, Z., Kyureghyan, G. M., & Wang, X. (2009). Perfect nonlinear binomials and their semifields. *Finite Fields and Their Applications*, 15(2), 125-133.

[43] Zhou, Y. (2010). A note on the isotopism of commutative semifields. arXiv preprint arXiv:1006.1529.

[44] Zhou, Y., & Pott, A. (2013). A new family of semifields with 2 parameters. *Advances in Mathematics*, 234, 43-60.