Difference Sets From Projective Planes

Dissertation

zu Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von M. Sc. Yue Zhou

geb. am 16.07.1984 in Shanxi

genehmigt durch die Fakultät für Mathematik

der Otto-von-Guericke-Universität Magdeburg.

Gutachter: Prof. Dr. Alexander Pott

Prof. Dr. Michel Lavrauw

eingereicht am: 28.03.2013

Verteidigung am: 28.06.2013

Zusammenfassung

Wir befassen uns in dieser Dissertation mit mehreren Typen verallgemeinerter Differenzmengen in abelschen Gruppen.

Zunächst konzentrieren wir uns auf $(q, q, q, 1)$-relative Differenzmengen mit ungeradem q. Diese sind äquivalent zu planaren Funktionen über $\mathbb{F}_q$. Die meisten bekannten Beispiele führen zu kommutativen Halbkörpern. Eines unserer Hauptresultate ist die Konstruktion einer neuen Familie von Halbkörpern ungerader Charakteristik. Wir bestimmen ihre linken, rechten und mittleren Nuklei. Wir zeigen, dass dieser Halbkörper für bestimmte Parameter auf zwei nicht äquivalente planare Funktionen führen.

Durch Anwendung der Charakter-Methode auf planare Funktionen über $\mathbb{F}_q$ mit q ungerade zeigen wir einige überraschende Beziehungen zwischen planaren Funktionen über $\mathbb{F}_{p^m}$ und planaren Funktionen über $\mathbb{F}_{p^{2m}}$. Wir untersuchen Projektionen und Hochhebungen von planaren Funktionen, wobei wir auch einen Ansatz der Kodierungstheorie ausnutzen. Wir geben einige Resultate computergestützter Rechnungen über die "Switchings" planarer Funktionen von $\mathbb{F}_{3^n}$ für $n = 3, 4, 5, 6$ an.

Danach untersuchen wir $(2^n, 2^n, 2^n, 1)$-relative Differenzmengen in C_4^n relativ zu C_2^n. Dabei werden zwei Darstellungen eingeführt, von denen eine das Analogon klassischer planarer Funktionen ist, welche auf $\mathbb{F}_q$ mit q ungerade definiert sind. Genauer gesagt führt eine Funktion f auf $\mathbb{F}_{2^n}$ genau dann zu einer $(2^n, 2^n, 2^n, 1)$-Differenzmenge, wenn die Abbildung $x \mapsto f(x+a) + f(x) + f(a) + xa$ für beliebige $a \neq 0$ eine Permutation auf $\mathbb{F}_{2^n}$ ist. Solche f nennen wir ebenfalls planare Funktionen. Wir zeigen, dass eine planare Funktion f auf $\mathbb{F}_{2^n}$ genau dann als Dembowski-Ostrom-Polynom geschrieben werden kann, wenn $x * a := f(x+a) + f(x) + f(a) + xa$ die Multiplikation auf einem Halbkörper der Ordnung 2^n definiert. Für den Fall, dass f eine Abbildung auf $\mathbb{F}_{2^n}$ mit den Eigenschaften $f(0) = 0$ und $\mathrm{Im}(f) = \{0, \xi\}$ mit $\xi \neq 0$ ist, beweisen wir, dass f genau dann eine planare Abbildung ist, wenn $f(x+y) = f(x) + f(y)$ für alle $x, y \in \mathbb{F}_{2^n}$ gilt. Wir betrachten auch Projektionen von planaren Funktionen, die wir "shifted-bent" Funktionen nennen. Wir zeigen einen interessante Zusammenhang zu bent Funktionen über $\mathbb{F}_2^n$ auf.

Schließlich untersuchen wir perfekte Sequenzen über $\mathbb{F}_p$. Wir beweisen, dass diese äquivalent zu verallgemeinerten Differenzmengen sind. Es stellt sich heraus, dass die klassischen Beispiele Projektionen verschiedener Typen verallgemeinerter Differenzmengen sind, die von desarguesschen Ebenen abgeleitet werden. Wir präsentieren auch einige Aussagen zur Nichtexistenz.

Abstract

The topic of this dissertation are several types of generalized difference sets in abelian groups.

First, we concentrate on $(q, q, q, 1)$-relative difference sets with q odd, which are equivalent to planar functions over $\mathbb{F}_q$. Most of the known examples lead to commutative semifields. One of our main results is the construction of a new family of semifields of odd characteristic. We determine their left, right and middle nuclei. We show that for certain parameters, some of these semifields lead to two inequivalent planar functions.

By applying the character approach to planar functions over $\mathbb{F}_q$ with q odd, we present some unexpected links between planar functions over $\mathbb{F}_{p^m}$ and planar functions over $\mathbb{F}_{p^{2m}}$. We study the projections and liftings of planar functions, where we also apply a coding theory approach. Some computational results about the switchings of planar functions on $\mathbb{F}_{3^n}$ for $n = 3, 4, 5, 6$ are given.

Then we turn to $(2^n, 2^n, 2^n, 1)$-relative difference sets in C_4^n relative to C_2^n. Two representations are introduced, one of which is the counterpart of the classical planar functions defined on $\mathbb{F}_q$ with q odd. In more detail, a function f on $\mathbb{F}_{2^n}$ leads to a $(2^n, 2^n, 2^n, 1)$-relative difference set if and only if for any nonzero a, the mapping $x \mapsto f(x+a) + f(x) + f(a) + xa$ is a permutation on $\mathbb{F}_{2^n}$. We also call such f planar functions. We show that a planar function f on $\mathbb{F}_{2^n}$ can be written as a Dembowski-Ostrom polynomial if and only if $x * a := f(x+a) + f(x) + f(a) + xa$ defines the multiplication of a semifield of order 2^n. When f is a mapping on $\mathbb{F}_{2^n}$ satisfying $f(0) = 0$ and $\mathrm{Im}(f) = \{0, \xi\}$ with $\xi \neq 0$, we prove that f is a planar mapping if and only if $f(x+y) = f(x) + f(y)$ for any $x, y \in \mathbb{F}_{2^n}$. We also consider projections of planar functions, which we call shifted-bent functions. They are shown to have an interesting relation with bent functions over $\mathbb{F}_2^n$.

Finally, for any prime p, we investigate almost p-ary sequences which are perfect or nearly perfect. They are proved to be equivalent to certain types of generalized difference sets. The classical examples come from the projections of several types of generalized difference sets derived from desarguesian planes. We also present several nonexistence results.

Acknowledgements

First of all, I would like to express my gratitude to my supervisor Prof. Dr. Alexander Pott for the guidance and support. It is always enjoyable for me to discuss mathematics with him. His insight and patience helped me to discover many interesting results and to finish this dissertation.

I am also grateful to Prof. Dr. Jürgen Bierbrauer, Dr. Ayça Çeşmelioğlo, Dr. Anton Malevich, Dr. Gohar Kyureghyan, Prof. Dr. Ferrüh Özbudak, Dr. Kai-Uwe Schmidt, Wei Su, Dr. Yin Tan, Carsten Thiel, Dr. Qi Wang and Prof. Dr. Wolfgang Willems for fruitful discussions, valuable comments and joyful collaborations.

I am further grateful to other people who had indirect influence to my work: To my colleagues for their kindness friendship and support, together with their help on many occasions, to my former Master thesis supervisor Prof. Dr. Chao Li, who taught me finite fields.

My deep gratitude goes to my parents and my brother Kai for all their love and encouragement.

Finally, but not least, I would like to acknowledge the financial, academic and technical support from the Otto-von-Guericke University of Magdeburg and the financial support from CSC (*China scholarship council*).

Contents

List of Tables

List of Figures

Overview

In the present thesis, we are interested in generalized difference sets, the developments of which can be uniquely extended to projective planes.

In Chapter 1, in addition to fundamental definitions and results, I attempt to provide a comprehensive tour, from projective planes to generalized difference sets.

After a brief introduction to the foundations of incidence structures, difference sets and finite fields, in Section 1.5 we start to focus on projective planes, which are quite special incidence structures. A projective plane is an incidence structure with points and lines such that any two distinct points (resp. lines) are incident with a unique line (resp. point), and there exists a quadrangle. The classical examples are the desarguesian planes $\mathrm{PG}(2, \mathbb{K})$.

It is well-known that every line of a projective plane $\mathbf{P}$ is incident with exactly $n+1$ points, and n is called the order of $\mathbf{P}$. The most important and long-standing conjecture on projective planes is the so called prime power conjecture, which states that a projective plane of order n exists if and only if n is a prime power. It seems that there is no promising strategy to prove this elusive conjecture with the present methods of mathematics. One natural compromise is to consider this conjecture under a certain assumption, for example, the existence of a certain collineation group.

Hence, at this point, we introduce collineation groups, and we mainly consider two classifications of projective planes with respect to their collineation groups.

The first classification is based on planar ternary rings derived from projective planes by coordinatization. They can be found in most standard text books. Important cases in this thesis are quasifields and semifields, which are briefly introduced in Sections 1.7 and 1.8.

The second classification is about projective planes with a "large" quasiregular collineation groups. They were completely classified by Dembowski and Piper (1967) into 8 cases. According to the results by Hughes (1955), Ganley and McFarland (1975) and Ganley (1977), the projective planes in 6 of these 8 cases can be obtained by the extensions of the developments of certain types of generalized difference sets. It is widely conjectured that projective planes derived from 5 of these 6 types of generalized difference sets, are desarguesian. The

only exceptional cases are the projective planes derived from $(n, n, n, 1)$-relative difference sets. Due to the results by Ganley (1976) and Blokhuis, Jungnickel, and Schmidt (2002), the prime power conjecture is true for the projective planes derived from abelian $(n, n, n, 1)$-relative difference sets.

All of the above results are covered in Chapter 1, in which we also introduce projections and liftings of generalized difference sets, as well as CCZ and EA-equivalences.

Then, we investigate $(q, q, q, 1)$-relative difference sets and semifields. Shortly speaking, semifields are algebras satisfying all of the axioms for a skew field except (possibly) multiplicative associativity. Finite semifields have a subtle relationship with $(q, q, q, 1)$-relative difference sets. We restrict ourselves to commutative semifields and abelian relative difference sets. On one hand, abelian $(q, q, q, 1)$-relative difference sets can be derived from finite commutative semifields, but the converse is not true in general. On the other hand, it is possible that one commutative semifield gives rise to two inequivalent $(q, q, q, 1)$-relative difference sets.

We arrange the investigation of abelian $(q, q, q, 1)$-relative difference sets into three chapters. In Chapters 2 and 3 we investigate the case q is odd. Let C_m denote the cyclic group of order m. When $q = p^n$ is odd, it is well-known that $(q, q, q, 1)$-relative difference sets in C_p^{2n} are equivalent to planar functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, which satisfy the condition that for each nonzero $a \in \mathbb{F}_{p^n}$, the mapping $x \mapsto f(x + a) - f(x)$ is a permutation on $\mathbb{F}_{p^n}$. Chapter 4 deals with the case $q = 2^n$ is even, where $(q, q, q, 1)$-relative difference sets are subsets of C_4^n. We establish the equivalence between these relative difference sets and a special type of functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, such that for any nonzero $a \in \mathbb{F}_{2^n}$, mapping $x \mapsto f(x + a) + f(x) + xa$ is a permutation on $\mathbb{F}_{2^n}$. We also call such f planar functions.

For odd p, before 2008, every known family of commutative semifields of order p^n has at most one parameter. As Kantor (2003) surveyed, the total number of pairwise non-isotopic commutative semifields of order p^n from these families is less than $n \cdot \log p$. Five years ago, Budaghyan and Helleseth (2008) constructed a new family of semifields of order p^{2n}, which has more than one parameters. Later, Zha, Kyureghyan, and Wang (2009) and Bierbrauer (2010) also introduced two new semifield families with several parameters. However, until now, there is still no evidence to show that for any constant $c > 0$, the number of pairwise non-isotopic semifields in each of these new families is not bounded by $c \cdot n$. In Chapter 2, we construct a new family of (pre)semifields with two parameters:

Theorem 2.4. *Let p be an odd prime, and 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 binary operation $*$ as follows:*

$$(a, b) * (c, d) = (a \circ_k c + \alpha (b \circ_k d)^\sigma, ad + bc),$$

where α is a non-square element in $\mathbb{F}_{p^m}$ and σ is a field automorphism of $\mathbb{F}_{p^m}$. Then, $(\mathbb{F}_{p^{2m}}, +, *)$ is a presemifield, which we denote by $\mathbb{P}_{k,\sigma}$.

To get a semifield $\mathbb{S}_{k,\sigma}$ from one of our presemifields, we define the multiplication $\star$ of $\mathbb{S}_{k,\sigma}$ as:

$$(a,b) \star (c,d) := B^{-1}((a,b) * (c,d)),$$

where $B(a,b) := (a,b) * (1,0) = (a + a^{p^k}, b)$. Then we consider the isotopisms between these semifields, and we can show that the number of non-isotopic semifields of order p^n is not bounded by $c \cdot n$ for any constant $c > 0$, where $n = 2m$.

Corollary 2.15. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ of order p^{2m}, where $m = 2^e\mu$ with $\gcd(\mu, 2) = 1$. Then the families $\mathbb{S}_{k,\sigma}$ contain*

1. $\lfloor \frac{\mu}{2} \rfloor \cdot \lceil \frac{m}{2} \rceil$ *non-isotopic semifields, and*
2. $\lfloor \frac{\mu}{2} \rfloor \cdot (\lceil \frac{m}{2} \rceil + 1)$ *inequivalent planar functions.*

At the end of this chapter, we introduce one family of APN functions (Theorem 2.21) which are analogues of the planar functions derived from Theorem 2.4.

In Chapter 3, we apply two approaches to planar functions. First, by the well-known character approach, we show an unexpected link between planar functions over $\mathbb{F}_{p^m}$ and planar functions over $\mathbb{F}_{p^{2m}}$:

Theorem 3.1. *Let $\psi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be any permutation, and let $\varphi_1, \varphi_2 : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be arbitrary functions. Then the mapping*

$$\begin{array}{rccc} f: & \mathbb{F}_{p^m}^2 & \to & \mathbb{F}_{p^m}^2 \\ & \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & \begin{pmatrix} x^2 + \varphi_1(y) \\ 2x \cdot \psi(y) + \varphi_2(y) \end{pmatrix} \end{array}$$

is planar if and only if

$$\begin{array}{rccc} g: & \mathbb{F}_{p^m} & \to & \mathbb{F}_{p^m} \\ & y & \mapsto & -u^2 \cdot \psi^2(y) + u \cdot w \cdot \psi(y) + \varphi_1(y) + u \cdot \varphi_2(y) \end{array}$$

is planar for all $u, w \in \mathbb{F}_{p^m}$.

We can use this theorem to show that the semifields constructed by Ganley (1981) immediately give rise to the semifields found by Coulter and Matthews (1997) and extended by Ding and Yuan (2006).

Then we focus on "projections" and "liftings" of planar functions. Although planar functions are defined over $\mathbb{F}_{p^n}$, to get the relative difference sets we only need the additive group of $\mathbb{F}_{p^n}$. Hence we can also say a planar function from

$\mathbb{F}_p^n$ to itself (or from C_p^n to itself). Let H be an $(n-m)$-dimensional subspace of $\mathbb{F}_p^n$, and let $\varphi_H : \mathbb{F}_p^n \to \mathbb{F}_p^n/H$ be the canonical projection. We project planar mappings $f, g : \mathbb{F}_p^n \to \mathbb{F}_p^n$ to $\varphi_H \circ f$ and $\varphi_H \circ g$, and investigate the equivalence between them. By MAGMA programs, we list some computational results for $p = 3$ and $n = 3, 4, 5, 6$.

In Chapter 4, we introduce several necessary and sufficient conditions for $(2^n, 2^n, 2^n, 1)$-relative difference sets in C_4^n relative to $2C_4^n$ (Theorem 4.3), one of which allows us to write a relative difference set as a planar function on $\mathbb{F}_{2^n}$. We also prove that the projective plane derived from a $(2^n, 2^n, 2^n, 1)$-relative difference set is a semifield plane if and only the corresponding planar function is a Dembowski-Ostrom polynomial (Theorem 4.14). Then we consider planar functions with exactly two elements in their image sets and we prove the following theorem.

Theorem 4.20. *Let n be a positive integer and f be a mapping on $\mathbb{F}_{2^n}$ where $f(0) = 0$ and $\mathrm{Im}(f) = \{0, \xi\}$ with $\xi \neq 0$. Then f is a planar mapping if and only if f is additive, i.e. $f(x+y) = f(x) + f(y)$ for any $x, y \in \mathbb{F}_{2^n}$.*

In Section 4.4, we consider some projections of planar functions, which we call shifted-bent functions. We show their relation with bent functions over $\mathbb{F}_2^n$ in Theorems 4.26 and 4.28.

In the last chapter, motivated by the results of Ma and Ng (2009) for perfect and nearly perfect p-ary sequences for any prime p, we study almost p-ary sequences which are perfect or nearly perfect. It turns out that almost p-ary perfect sequences of period $n+1$ are equivalent to $(n+1, p, n, (n-1)/p)$-relative difference sets in $C_{n+1} \times C_p$ relative to C_p (Theorem 5.6). Let D be an $(n+1, n-1, n, 1)$-relative difference set in $C_{n+1} \times C_{n-1}$ relative to C_{n-1} where n is a power of an odd prime. The classical example R of $(n+1, p, n, (n-1)/p)$-relative difference sets comes from the projection of D, i.e. $R = \varphi_{C_{n-1}}(D)$, see Result 1.67 (d).

We also investigate almost p-ary nearly perfect sequences. It is shown that periodic almost p-ary nearly perfect sequences correspond to certain direct product difference sets (Theorem 5.20). Our main contributions in Chapter 5 are the nonexistence of almost p-ary perfect sequences and nearly perfect sequences with certain parameters. At the end, we summarize the existence status of almost p-ary perfect and nearly perfect sequences with period less than 100 in Tables 5.2 and 5.3.

Chapter 1

Projective planes and related algebraic structures

The woods are lovely, dark and deep.
But I have promises to keep,
And miles to go before I sleep,
And miles to go before I sleep.

Robert Frost, *Stopping by woods in a snowy evening*

In this chapter, we start with some fundamental ideas about design theory. Then we focus on difference sets in Section 1.2 and Section 1.3. A brief introduction to finite fields is given in Section 1.4. In Section 1.5, we turn to projective planes. After introducing collineation groups of projective planes, we focus on two classifications: The Lenz-Barlotti classification and the Dembowski-Piper classification of planes with a quasiregular collineation group. By coordinatizing projective planes with planar ternary rings (PTR), we list various links between algebraic properties of PTRs and geometric properties of the corresponding projective planes. Several special PTRs such as quasifields, nearfields and semifields are briefly introduced in Section 1.7 and 1.8. The Dembowski-Piper classification leads to (generalized, relative) difference sets in groups, and they are discussed in Section 1.9, the contents of which can be found in the papers by Ganley and McFarland (1975) as well as Ghinelli and Jungnickel (2003). The projections and liftings of (generalized, relative) difference sets are introduced in Section 1.10, which is partially from Pott, Wang, and Zhou (2012). Finally, in Section 1.11, we consider several equivalence relations of a certain type of relative difference sets.

1.1 Incidence structures

We begin briefly recalling some fundamental definitions from design theory. The interested reader may consult the standard books by Beth, Jungnickel, and Lenz (1999) and by Hughes and Piper (1988).

Definition 1.1. An *incidence structure* is a triple $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$, where $\mathcal{P}$ is a set of elements called *points* and $\mathcal{B}$ is a set of elements called *blocks (lines)*, and $I \subseteq (\mathcal{P} \times \mathcal{B})$ is a binary relation, called *incidence relation*. The elements of I are called *flags*.

Usually we use upper case Latin letters to denote points and lower case Latin letters to denote blocks. Distinct blocks may be incident with the same point set, and they are called *repeated blocks*. When distinct blocks of a given incidence structure have distinct point sets, we shall often identify each of its blocks with the point set incident with it for convenience. If a point P is incident with a block l, we can write either $P \ \mathrm{I} \ l$ or $P \in l$ and use such geometric languages as "P lies on l", "l passes through P", "l contains P", etc.

Clearly an incidence structure can be defined on infinite $\mathcal{P}$ or $\mathcal{B}$, but in this thesis we will restrict our study to the finite case, i.e. $\mathcal{P}$ and $\mathcal{B}$ are both finite. A finite incidence structure with equally many points and blocks is called *square*.

Suppose that $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is an incidence structure with v points and b blocks, where $v > 0$ and $b > 0$. The points of $\mathcal{P}$ are indexed $P_1, P_2, \ldots, P_v$, while the blocks are $l_1, l_2, \ldots, l_b$. Then the *incidence matrix* $M = (m_{ij})$ for $\mathbf{D}$ is a $v \times b$ matrix where $m_{ij} = 1$ if P_i is on l_j and $m_{ij} = 0$ otherwise. It is clear that M depends on the labeling used, but up to row and column permutations it is unique. Conversely, every $(0,1)$-matrix (entries are 0 or 1) determines an incidence structure.

Given any two incidence structures $\mathbf{D}_1$ and $\mathbf{D}_2$, we define an *isomorphism* α from $\mathbf{D}_1$ onto $\mathbf{D}_2$ to be a one-to-one mapping from the points of $\mathbf{D}_1$ onto the points of $\mathbf{D}_2$ and from the blocks of $\mathbf{D}_1$ onto the blocks of $\mathbf{D}_2$ such that P is on l if and only if P^α is on l^α. If there is an isomorphism between $\mathbf{D}_1$ and $\mathbf{D}_2$, then we say that they are *isomorphic*. In terms of their incidence matrices M_1 and M_2, $\mathbf{D}_1$ and $\mathbf{D}_2$ are isomorphic if and only if there exist row and column permutations transforming M_1 to M_2, i.e. there are permutation matrices P and Q such that

$$PM_1Q = M_2.$$

An *automorphism* of a given incidence structure $\mathbf{D}$ is an isomorphism of $\mathbf{D}$ onto itself. Obviously, the set of automorphisms of $\mathbf{D}$ forms a group, which is called the full automorphism group of $\mathbf{D}$ and denoted by $\mathrm{Aut}(\mathbf{D})$. Any subgroup of $\mathrm{Aut}(\mathbf{D})$ will be called an *automorphism group* of $\mathbf{D}$.

The following result was proved by Brauer (1941) and Parker (1957).

Lemma 1.2. *Let* $\mathbf{D}$ *be a square incidence structure and* $\alpha \in \mathrm{Aut}(\mathbf{D})$. *If the incidence matrix of* $\mathbf{D}$ *is non-singular, then the number of fixed points of* α *equals the number of fixed blocks.*

Proof. Let M be an incidence matrix of $\mathbf{D}$. The automorphism α gives rise to two permutation matrices P and Q such that $PMQ = M$. The number of fixed points

of α is the trace of P, and the number of fixed blocks of α is the trace of Q. As M is non-singular, we have $P = MQ^{-1}M^{-1}$. Thus $\mathrm{Tr}(P) = \mathrm{Tr}(Q^{-1}) = \mathrm{Tr}(Q)$, because Q is a permutation matrix. □

According to our definition, any binary relation between $\mathcal{P}$ and $\mathcal{B}$ gives an incidence structure. Thus it is too general to be of any interest. Actually, we often consider incidence structures satisfying certain extra properties.

Definition 1.3. Let $\mathbf{D} = (\mathbf{P}, \mathcal{B}, I)$ be an incidence structure with $|\mathbf{P}| = v > 0$ and $|\mathcal{B}| = b > 0$. Let t and λ be two positive integers. Then $\mathbf{D}$ is called *t-balanced* with parameter λ if and only if every subset of t points of $\mathbf{P}$ is incident with exactly λ blocks of $\mathcal{B}$. If every block of $\mathbf{D}$ is also of the same size k, then $\mathbf{D}$ is called a t-(v, k, λ) *design*, or merely *t-design*.

Obviously, t-designs with $k = t$ or $k = v$ always exist, and we call such examples *trivial*. Given a t-design $\mathbf{D}$, it is not difficult to show that $\mathbf{D}$ is also an s-design for any $s < t$. Precisely, the parameter λ_s (the number of blocks containing an s-set) equals $\lambda_t \binom{v-s}{t-s} / \binom{k-s}{t-s}$, where λ_t is the number of blocks contain a t-set, see Theorem 3.2 in the book of Beth, Jungnickel, and Lenz (1999) for a proof. In particular, every point of a t-design $\mathbf{D}$ is on a same number of blocks, i.e. the incidence matrix of $\mathbf{D}$ has a constant row sum which is denoted by r. When $t = 2$, we have

$$r = \lambda(v-1)/(k-1) \tag{1.1}$$

and $r > \lambda$ if $k < v$. A 2-design is called *symmetric* if $v = b$.

When $t = 2$, we can easily prove the following necessary and sufficient condition for $\mathbf{D}$ being a 2-design.

Theorem 1.4. *Let M be an incidence matrix of an incidence structure $\mathbf{D}$. Then $\mathbf{D}$ is a 2-(v, k, λ) design if and only if*

$$MM^T = (r-\lambda)I_v + \lambda J_v, \tag{1.2}$$

where I_v is the $v \times v$-identity matrix and J_v is the all-one $v \times v$-matrix. □

As J_v has the eigenvector $(1, \ldots, 1)^T$ with eigenvalue v and $v-1$ linearly independent eigenvectors

$$(1, -1, 0, \ldots, 0)^T,\ (1, 0, -1, \ldots, 0)^T, \ldots, (1, 0, \ldots, 0, -1)^T$$

with eigenvalue 0, MM^T satisfying (1.2) has one eigenvalue $r - \lambda + \lambda v$ and $v-1$ eigenvalues $r - \lambda$. Therefore, we can get the determinant of MM^T.

Lemma 1.5. *Let M be a $v \times v$-matrix satisfying* (1.2)*. Then*

$$\det MM^T = (r-\lambda)^{v-1}(v\lambda - \lambda + r).$$

If M is an incidence matrix of a 2-(v, k, λ)-design with $v > k$, then by (1.1)

$$\det MM^T = (r-\lambda)^{v-1} rk \neq 0.$$ □

Now we can prove the following fundamental result due to Brauer (1941), which was rediscovered by Dembowski (1958), Hughes (1957) and Parker (1957).

Theorem 1.6 (Orbit Theorem)**.** *Let $D = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a square incidence structure whose incidence matrix M is non-singular over $\mathbb{R}$, for instance a non-trivial symmetric design, and let G be an automorphism group of $\mathbf{D}$. Then the number $o_{\mathbf{P}}(G)$ of G-orbits on $\mathcal{P}$ equals the number $o_{\mathcal{B}}(G)$ of G-orbits on $\mathcal{B}$. In particular, G is transitive (resp. regular) on the set of blocks of $\mathbf{D}$ if and only if G is transitive (resp. regular) on the set of points of $\mathbf{D}$.*

Proof. Given any $\alpha \in G$, by Lemma 1.2, the number $f_{\mathcal{P}}(\alpha)$ of points fixed by α is equal to the number $f_{\mathcal{B}}(\alpha)$ of blocks fixed by α. Hence by the well-known Cauchy-Frobenius Lemma (also called Burnside's Lemma),

$$o_{\mathcal{P}}(G) = \frac{1}{|G|} \sum_{\alpha \in G} f_{\mathcal{P}}(\alpha) = \frac{1}{|G|} \sum_{\alpha \in G} f_{\mathcal{B}}(\alpha) = o_{\mathcal{B}}(G).$$

Indeed the assertion applies for non-trivial symmetric designs, since any such design has a non-singular incidence matrix, by Theorem 1.4. □

1.2 Difference sets and their generalization

Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a square incidence structure, for instance a symmetric 2-(v, k, λ) design, and $G \subseteq \mathrm{Aut}(\mathbf{D})$. For a given point $P \in \mathcal{P}$, we use P^g to denote the image of P under $g \in G$. If G acts regularly on the points as well as on the blocks of $\mathbf{D}$, then $\mathbf{D}$ is called *regular*, and G is called a *Singer group* of $\mathbf{D}$. It should be noted that in the case of symmetric 2-(v, k, λ) designs with $v > k$, the regularity on points implies the regularity on blocks by Theorem 1.6. For any point P, we have $\mathcal{P} = \{ P^g : g \in G \}$, and $x = y$ if and only if $P^x = P^y$. Hence we may identify $\mathcal{P}$ with G, and any block l of $\mathbf{D}$ with a subset $D \subseteq G$. The other blocks are the translates $D + g$ with $g \in G$, where we use "$+$" to denote the binary operator of the group G, which is not necessarily commutative. When $\mathbf{D}$ is a 2-(v, k, λ) design, for any two points $x, y \in G$, and any block $D + g$ with $g \in G$, we have $x, y \in D + g$ if and only if

$$x = d + g \quad \text{and} \quad y = d' + g \quad \text{for some } d, d' \in D.$$

This is equivalent to

$$x - y = d - d' \quad \text{and} \quad x = d + g \text{ for some } d, d' \in D.$$

Hence λ, the number of blocks containing both x and y, equals the number of occurrences of $x - y$ as a difference $d - d'$ with $d, d' \in D$.

Definition 1.7. Let G be an additively written group of order v, and let D be a k-subset of G. Then D is called a (v, k, λ)*-difference set* if the list of differences $d - d'$ with $d, d' \in D$, $d \neq d'$, covers all nonzero elements in G exactly λ times.

Definition 1.8. Let G be an additively written group and D a nonempty subset of G. Then the incidence structure $\mathrm{dev}(D) := (G, \mathcal{B}, \in)$ with $\mathcal{B} := \{D + x : x \in G\}$ is called the *development* of D. It may be possible that $D + g = D + h$ for $g \neq h$, in which case we consider the block $D + g$ twice (or even more).

By the first paragraph of this section, we can show the following theorem.

Theorem 1.9. *Let G be a finite group and D a proper, nonempty subset of G. Then D is a (v, k, λ)-difference set if and only if* $\mathrm{dev}(D)$ *is a symmetric* 2-(v, k, λ) *design which is regular with respect to G. Moreover, every regular symmetric* 2-(v, k, λ) *design can be represented in this way.* □

Let $H(n+1, q) \leq \mathrm{GL}(n+1, q)$ be the subgroup of all linear mappings setwise fixing each 1-dimensional linear subspace, i.e.

$$H(n+1, q) := \{\lambda I_{n+1} : \lambda \in \mathbb{F}_q^*\},$$

where I_{n+1} is the $(n+1) \times (n+1)$ identity matrix. The group

$$\mathrm{PGL}(n+1, q) := \mathrm{GL}(n+1, q)/H(n+1, q)$$

is called the *projective general linear group*. The following classical and seminal construction of (v, k, λ)-difference sets is due to Singer (1938).

Theorem 1.10. *Let q be a prime power and n a positive integer. Then* $\mathrm{PGL}(n+1, q)$ *contains a cyclic subgroup of order $(q^{n+1} - 1)/(q - 1)$ acting regularly on the points and hyperplanes of* $\mathrm{PG}(n, q)$*. Hence, there is a cyclic $\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$-difference set.*

By representing regular designs as difference sets, we can apply several powerful algebraic tools, for instance, group algebras, character theory and algebraic number theory, which may help us to prove or disprove the existences of designs with certain parameter. One way to generalize the concept of difference sets is the following.

Definition 1.11. Let G be an additively written group of order v and let N_1, $\cdots$, N_r be subgroups of order $n_1, \ldots, n_r$. Assume that N_1, $\cdots$, N_r intersect pairwise trivially. A $(v; n_1, \ldots, n_r; k, \lambda; \lambda_1, \ldots, \lambda_r)$-*generalized difference set* (abbreviated to GDS) relative to the subgroups N_i's is a k-subset D of G such that the list of differences $d - d'$ with $d, d' \in D$, $d \neq d'$, covers all the elements in $G \backslash (N_1 \cup N_2 \cup \cdots \cup N_r)$ exactly λ times, and the nonzero elements in N_i exactly λ_i times. The N_i's are called the *exceptional* subgroups. A generalized difference set D is called *cyclic* or *abelian* if G has the respective property.

Furthermore, if $r = 1$, $\lambda_1 = 0$ and $v = mn$ where $n := n_1$, then we call D a *relative difference set* with parameters (m, n, k, λ) (an (m, n, k, λ)-RDS for short), and we call N_1 the *forbidden subgroup*. If N_1 is a direct factor of G, the RDS is called *splitting*.

Example 1.12. Let C_n denote the cyclic group of order n.

1. The set $\{1,2,4\} \subseteq C_7$ is a $(7,3,1)$-difference set.
2. The set $\{0,1\} \subseteq C_4$ is a $(2,2,2,1)$-RDS.
3. The set $\{(1,2),(2,0),(0,3)\}$ is a $(16;4,4,4;3,1;0,0,0)$-GDS in $C_4 \times C_4$ relative to the three subgroups $C_4 \times \{0\}$, $\{0\} \times C_4$ and $\{(x,x) : x \in C_4\}$. □

We will see more examples in Section 1.9.

Remark 1.13. Let D is a splitting $(m,n,m,m/n)$-RDS in $G := H \times N$ relative to $\{0\} \times N$. For any two element $(a,b),(c,d) \in D$, the difference $(a-c,b-d)$ does not belong to $\{0\} \times N$. It implies that $a \neq c$. Since $|D| = m = |H|$, there exists a mapping $f : H \to N$, such that $D = \{(x,f(x)) : x \in H\}$. Furthermore, D is an $(m,n,m,m/n)$-RDS in G if and only if $|\{x : f(x+a) - f(x) = b\}|$ is a constant for all nonzero $a \in H$ and all $b \in N$.

For more details about (relative) difference sets, see the surveys by Jungnickel and Schmidt (1997, 1998), Pott (1995, 1996) and Chapter VI in the book of Beth, Jungnickel, and Lenz (1999).

The incidence structure related to a generalized difference set D has the same number of points as blocks. If the generalized difference set D has parameters $(v;n_1,\ldots,n_r;k,\lambda;\lambda_1,\ldots,\lambda_r)$ relative to subgroups N_i with $i = 1,\ldots,r$, we can define several equivalence relations on points as follows: $g \sim_i h$ if and only if $g - h \in N_i$, namely, the equivalence classes are the right cosets of N_i. Furthermore, the incidence structure has the following properties:

- The structure has v points and v blocks.
- Any block contains exactly k points.
- There are r equivalence relations $\sim_i$ on the point set, where the size of an equivalence class relative to $\sim_i$ is n_i.
- Any two equivalence classes of $\sim_i$ and $\sim_j$ with $i \neq j$ intersect in at most one point.
- Two distinct points which are not contained in one equivalence class are contained in exactly λ blocks, and points p,q with $p \sim_i q$ are contained in exactly λ_i blocks.

Finally, we discuss the equivalences among (relative, generalized) difference sets.

Definition 1.14. Two (generalized, relative) difference sets D_1 and D_2 in G are *equivalent* if there is a group automorphism φ such that

$$\varphi(D_1) := \{\varphi(d) : d \in D_1\} = a + D_2 + b$$

for suitable $a, b \in G$. If we take $D_2 = D_1$, then φ is called a *multiplier* of D_1 which obviously leads to an automorphism of $\mathrm{dev}(D_1)$. If G is abelian and α is an automorphism of the form $\alpha : x \mapsto mx$ for some integer m, then α is called a *numerical multiplier*. By abuse of language, the integer m is then also called a numerical multiplier of D. All of the multipliers together form a group denoted by $\mathcal{M}(D_1)$, which is called the *multiplier group* of D_1.

It is obvious that equivalent generalized difference sets give rise to isomorphic incidence structures, and for any given generalized difference set D, its multiplier group $\mathcal{M}(D)$ is a subgroup of the full automorphism group $\mathrm{Aut}(\mathrm{dev}(D))$ of its development. However isomorphic incidence structures do not necessarily come from equivalent generalized difference sets. For example, Edel and Pott (2009a) noticed a Hadamard design which can be derived from two inequivalent Hadamard difference sets (namely, bent functions) in C_2^6.

In general, it is easier to check whether two generalized difference sets are equivalent or not than to check isomorphisms between their developments. There are several invariants which can be used to distinguish incidence structures, for instance, ranks of incidence matrices, Smith normal forms, automorphism groups, intersection numbers, etc., see the survey by Xiang (2005).

1.3 Group rings and characters

Let $\mathbb{C}[G]$ denote the set of formal sums $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{C}$ and G is any (not necessarily abelian) group which we write here multiplicatively. The set $\mathbb{C}[G]$ is basically just the set of complex vectors whose basis is the set of group elements. We add these vectors componentwise, i.e.

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g,$$

and

$$(\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} b_g g) := \sum_{g\in G} (\sum_{h\in G} a_h b_{gh^{-1}}) \cdot g.$$

Moreover,

$$\lambda \cdot (\sum_{g\in G} a_g g) := \sum_{g\in G} (\lambda a_g) g$$

for $\lambda \in \mathbb{C}$.

If $D = \sum_{g\in G} a_g g$, we define

$$D^{(t)} := \sum_{g\in G} a_g g^t.$$

An important case is $D^{(-1)} = \sum_{g\in G} a_g g^{-1}$. If D is a subset of G, we identify D with the group ring element $\sum_{g\in D} d$. The following result is straightforward.

Lemma 1.15. *The set D is a $(v; n_1, \ldots, n_r; k, \lambda; \lambda_1, \ldots, \lambda_r)$-GDS relative to the subgroups N_i's if and only if*

$$\begin{aligned} D \cdot D^{(-1)} =& k - (\lambda(1-r) + \lambda_1 + \cdots + \lambda_r) + \\ & \lambda(G - N_1 - N_2 - \cdots - N_r) + \lambda_1 N_1 + \cdots + \lambda_r N_r. \quad \square \end{aligned} \tag{1.3}$$

A *character* of a finite abelian group G is a homomorphism χ from G into the multiplicative group of some field $\mathbb{K}$. The characters of G form a group under the multiplication defined as

$$\chi\chi'(g) := \chi(g)\chi'(g) \quad \text{for all } g \in G,$$

and we call it the *character group* $\hat{G}$ of G. We will always assume that $\mathbb{K}$ is a *splitting field* for G, i.e. that the characteristic of K does not divide $|G|$ and that $\mathbb{K}$ contains a primitive e-th root of unity, where e denotes the exponent of G. Under this assumption, we can apply Maschke's Theorem to decompose the representations of G into irreducible pieces. Let the decomposition of G be a direct product of m primary cyclic groups $C_i \cong \langle g_i \rangle$ with $|C_i| = v_i$. Then $\chi(g_i)$ is a v_i-th root of unity for any $\chi \in \hat{G}$. Let ζ_i be a primitive v_i-th root of unity. It is not difficult to verify that

$$\chi_i(g) := \chi_i(g_i^{e_i}) = \zeta_i^{e_i} \quad \text{for } g = g_1^{e_1} \ldots g_m^{e_m}$$

is a character, and all χ_i together generate $\hat{G}$ which is isomorphic to G. We use χ_0 to denote the identity element of $\hat{G}$, i.e. $\chi_0(g) = 1$ for all $g \in G$, and χ_0 is called the *principal* character of G.

Let H be a subgroup of G. Then the set

$$H^{\perp} := \{\, \chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in H \,\}$$

is a subgroup of $\hat{G}$ of order $|G/H|$. The characters in $H^{\perp}$ are basically the characters of G/H: If $\chi' \in \widehat{G/H}$, then the mapping $\chi : G \to \mathbb{K}$, which is defined by $\chi(g) := \chi'(gH)$, is a character in $H^{\perp}$, and conversely, each character in $H^{\perp}$ gives rise to a character of G/H.

Group characters satisfy the well-known *orthogonality relations*

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G|, & \text{for } g = 1; \\ 0, & \text{for } g \neq 1. \end{cases} \tag{1.4}$$

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{for } \chi = \chi_0; \\ 0, & \text{for } \chi \neq \chi_0. \end{cases} \tag{1.5}$$

Group characters may be extended to the group algebra $\mathbb{K}[G]$ by linearity:

$$\chi(A) := \sum_{g \in G} a_g \chi(g) \quad \text{for } A = \sum_{g \in G} a_g g.$$

Usually the characters we consider will be complex characters, i.e. $\mathbb{K} = \mathbb{C}$.

Characters are quite useful for (generalized, relative) difference sets in connection with the next lemma, which can be directly proved by using the orthogonality relations of characters.

Proposition 1.16 (inversion formula)**.** *Let $\mathbb{K}$ be a splitting field for the finite abelian group G, and let $A = \sum_{g\in G} a_g g \in \mathbb{K}[G]$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi\in\hat{G}} \chi(A)\chi(g^{-1}).$$

Hence, if $A, B \in \mathbb{K}[G]$ satisfy $\chi(A) = \chi(B)$ for all characters χ of G, then $A = B$. □

By applying Proposition 1.16 to (1.3), we can get another necessary and sufficient condition for D being a (generalized, relative) difference set. For instance, D is an (m, n, k, λ)-RDS in G relative to N if and only if the following identity holds for every complex character of G:

$$|\chi(D)|^2 = \begin{cases} k, & \text{for } \chi_{|N} \neq \chi_0; \\ k - \lambda n, & \text{for } \chi_{|N} = \chi_0, \chi \neq \chi_0; \\ k^2, & \text{for } \chi = \chi_0. \end{cases} \tag{1.6}$$

For more character theoretic approaches to difference sets, we refer the reader to Chapter VI in the book of Beth, Jungnickel, and Lenz (1999), the monograph by Pott (1995) and the paper by Schmidt (2002).

1.4 Finite fields

We briefly provide some facts about finite fields, for details we refer to the text books by Lidl and Niederreiter (1997) and Jungnickel (1993).

A *finite field* is a field with only a finite number of elements. The *order* of a finite field is the number of elements in it. The *characteristic* of a finite field is the smallest positive integer (and hence a prime) p such that $px = 0$ for all x in it.

Let p be a prime. Let $\mathbb{Z}/p\mathbb{Z}$ denote the residue class ring of integers modulo p. Then $\mathbb{Z}/p\mathbb{Z}$ further forms a finite field of order p, which is also denoted by $\mathbb{F}_p$. A finite field of characteristic p has a subfield isomorphic to $\mathbb{F}_p$ and has p^n elements for some positive integer n.

Let F be an irreducible polynomial of degree n in $\mathbb{F}_p[x]$, and let $q = p^n$. Then we define $\mathbb{F}_q := \mathbb{F}_p[x]/(F)$. Every element a of $\mathbb{F}_q$ satisfies $a^q - a = 0$, and there exists ξ in $\mathbb{F}_q$ such that $\mathbb{F}_q = \{0, 1, \xi, \cdots, \xi^{q-2}\}$. Such an element ξ is called a *primitive element* of $\mathbb{F}_q$. Any field of order q is isomorphic to $\mathbb{F}_q$. In another word, finite field of order q is unique up to isomorphism. Hence, we will always use $\mathbb{F}_q$ to denote it.

The additive group of $\mathbb{F}_q$ is isomorphic to the elementary abelian group C_p^n. The multiplicative group of $\mathbb{F}_q$ is a cyclic group of order $q-1$, and it is generated by a primitive element of $\mathbb{F}_q$.

The field $\mathbb{F}_{p^n}$ contains a subfield isomorphic to $\mathbb{F}_{p^m}$ if and only if m divides n. When we restrict ourselves to the additions of a finite field $\mathbb{F}_{q^m}$, we can consider $\mathbb{F}_{q^m}$ as an m-dimensional vector space over $\mathbb{F}_q$.

An *automorphism* of a field $\mathbb{K}$ is an isomorphism $\sigma : \mathbb{K} \to \mathbb{K}$. If $\mathbb{K} = \mathbb{F}_q$ with $q = p^n$, then every automorphism is of the type

$$\sigma : u \mapsto u^{p^i} \quad 0 \le i \le n-1.$$

The *Galois group* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the group of automorphisms of $\mathbb{F}_{q^m}$ that fixes every element of $\mathbb{F}_q$. Let G denote $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Then the *trace function* $\mathrm{Tr}_{q^m/q}$ on $\mathbb{F}_{q^m}$ is given by

$$\mathrm{Tr}_{q^m/q}(u) = \sum_{\sigma \in G} u^\sigma = u + u^q + \cdots + u^{q^{m-1}}.$$

The *norm function* $\mathrm{N}_{q^m/q}$ on $\mathbb{F}_{q^m}$ is given by

$$\mathrm{N}_{q^m/q}(u) = \prod_{\sigma \in G} u^\sigma = u^{1+q+\cdots+q^{m-1}}.$$

The image of both $\mathrm{Tr}_{q^m/q}$ and $\mathrm{N}_{q^m/q}$ is $\mathbb{F}_q$.

Every polynomial in $\mathbb{F}_q[x]$ defines a function on $\mathbb{F}_q$ by evaluating. The converse is also true, but the polynomials derived from a given function are not unique. For example, both polynomials x and x^q define the identity mapping on $\mathbb{F}_q$. However, for every function $f : \mathbb{F}_q \to \mathbb{F}_q$, there is exactly one polynomial F in $\mathcal{F}(q;x) := \{F \in \mathbb{F}_q[x] : \deg F < q\}$ defining f by evaluating. In fact, for any $u \in \mathbb{F}_q$, we have $f(u) = F(u)$, where

$$F(x) = -\sum_{a \in \mathbb{F}_q} f(a) \cdot \frac{x^q - x}{x - a} \in \mathcal{F}(q;x).$$

This is Lagrange's classical interpolation formula. An element F in $\mathcal{F}(q;x)$, for which the corresponding function is a permutation, is called a *permutation polynomial*. In the following, we introduce several special types of polynomials which will be frequently used later.

Definition 1.17. A polynomial of the form $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ with coefficients in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called a *q-polynomial* over $\mathbb{F}_{q^m}$. If the value of q is clear form the context, then it is also called a *linearized polynomial*.

Let $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^m}$, then

$$\begin{aligned} L(\alpha+\beta) &= L(\alpha) + L(\beta) \quad \text{for all } a, b \in \mathbb{F}_{q^m}, \\ L(c\alpha) &= cL(\alpha) \quad \text{for all } c \in \mathbb{F}_q \text{ and all } \alpha \in \mathbb{F}_{q^m}. \end{aligned}$$

It means that, if $\mathbb{F}_{q^m}$ is regarded as a vector space over $\mathbb{F}_q$, then the q-polynomial $L(x)$ induces a linear mapping on $\mathbb{F}_q^m$. The converse is also true: every linear mapping on $\mathbb{F}_q^m$ can be described by a q-polynomial.

Definition 1.18. A polynomial of the form

$$D(x) = \sum_{0 \le i \le j \le n-1} a_{ij} x^{p^i + p^j}$$

with coefficients in an extension field $\mathbb{F}_q$ of $\mathbb{F}_p$ is called a *Dembowski-Ostrom (DO) polynomial*.

For any Dembowski-Ostrom polynomial $D(x) = \sum_{i \le j} a_{ij} x^{p^i + p^j}$ in $\mathbb{F}_{p^n}[x]$, we can define a commutative multiplication $*$ on $\mathbb{F}_{p^n}$ by

$$x * y := D(x+y) - D(x) - D(y)$$

for any $x, y \in \mathbb{F}_{p^n}$. For any given nonzero y in $\mathbb{F}_{p^n}$, the polynomial

$$\begin{aligned} D(x+y) - D(x) - D(y) &= \sum_{0 \le i \le j \le n-1} a_{ij} (x^{p^i} y^{p^j} + y^{p^i} x^{p^j}) \\ &= \sum_{i=0}^{n-1} 2a_{ii} x^{p^i} y^{p^i} + \sum_{i<j} a_{ij} x^{p^i} y^{p^j} + \sum_{i>j} a_{ji} x^{p^i} y^{p^j} \end{aligned} \tag{1.7}$$

is a linearized polynomial in $\mathbb{F}_{p^n}[x]$. Hence the multiplication $*$ satisfies left and right distributive laws.

When $p > 2$, we have

$$x * x = D(2x) - 2D(x) = 4D(x) - 2D(x) = 2D(x).$$

Hence, $D(x) = (x * x)/2$.

Many (generalized, relative) difference sets in abelian groups are constructed by using functions on finite fields.

Definition 1.19. Let f be a function from $\mathbb{F}_q$ to itself. If for all nonzero a in $\mathbb{F}_q$, the mappings

$$x \mapsto f(x+a) - f(x)$$

are permutations on $\mathbb{F}_q$, then f is called a *planar function* or *a perfect nonlinear function* on $\mathbb{F}_q$. The polynomial defined by f is called a *planar polynomial*.

As the additive group of $\mathbb{F}_q$ with $q = p^n$ is isomorphic to C_p^n, we can identify the elements of C_p^n with those of $\mathbb{F}_q$. Hence, a mapping $f : C_p^n \to C_p^n$ can also be viewed as a function on $\mathbb{F}_q$. From Remark 1.13, we get the following result immediately.

Proposition 1.20. *Let $G = C_p^n \times C_p^n$. Let f be a mapping from C_p^n to itself, which we also regard as a function on $\mathbb{F}_{p^n}$. The subset*

$$D = \{(x, f(x)) : x \in C_p^n\}$$

is a $(q, q, q, 1)$-RDS in G relative to $\{0\} \times C_p^n$, if and only if, f is a planar function on $\mathbb{F}_{p^n}$. □

Remark 1.21. When q is odd, $f(x) = x^2$ is a planar function on $\mathbb{F}_q$, because for each $a \neq 0$, mapping $x \mapsto f(x+a) - f(x) = 2ax + a^2$ is a permutation on $\mathbb{F}_q$.

When q is even, there is no planar function on $\mathbb{F}_q$: Let f be an arbitrary function on $\mathbb{F}_q$. For any $a \neq 0$ and b, if x_0 is a root of the equation $f(x+a) - f(x) = b$, then $x_0 + a$ is another root of it. Hence $f(x+a) - f(x)$ can not be a permutation.

1.5 Projective and affine planes

Next, we focus on a special type of 2-designs, which are called *projective planes*. Most of the contents here can be found in the books by Dembowski (1997) and by Hughes and Piper (1973).

Definition 1.22. A *projective plane* **P** is an incidence structure consisting of a point set $\mathcal{P}$ and a line set $\mathcal{L}$, together with an incidence relation between the points and lines such that

1. any two distinct points are incident with a unique line;
2. any two distinct lines are incident with a unique point;
3. there exists a *quadrangle*, i.e. four points no three of which are incident with one line.

Any set of points incident with a common line are said to be *collinear*. Similarly, any set of lines incident with a common point are called *concurrent*. Conditions 1 and 2 are dual to each other, and together with condition 3 they imply the dual of it: there exist quadrilaterals.

If **P** is a projective plane and l is any line of **P**, then let $\mathbf{P}^l$ be the set of points and lines of **P** obtained by deleting the line l and all the points on it. It is clear that any two points of $\mathbf{P}^l$ are on a unique line. However, it is no longer true that any two lines intersect at a point. Actually, it is not difficult to check $\mathbf{P}^l$ satisfies the following axioms of affine planes.

Definition 1.23. An *affine plane* **A** is an incidence structure of a set of points and a set of lines, together with an incidence relation between the points and lines such that

1. any two distinct points are incident with a unique line;

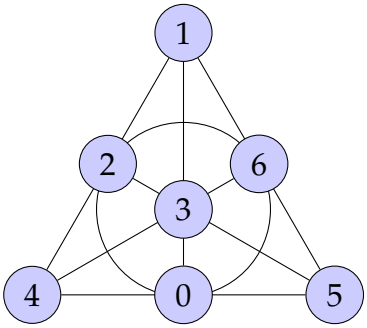

Figure 1.1: Fano plane

2. given any line l and any point P not on l there is a unique line m such that P is on m, and l and m have no common point;

3. there exists a *triangle*, i.e. three non-collinear points.

Let $\mathbf{A}$ be an affine plane. In fact, there is, up to isomorphism, a unique projective plane $\mathbf{P}$ such that $\mathbf{A} = \mathbf{P}^l$ for some line l of $\mathbf{P}$. Its proof can be found in Theorem 3.10 in the book by Hughes and Piper (1973) or Section 3.1 in the book by Dembowski (1997).

Clearly, from the definition, a projective plane must contain at least 4 points and 4 lines. Next we give an example of a projective plane $\mathbf{P}$ which has exactly 7 points and lines.

Example 1.24. Take $\mathcal{P} = \{0, 1, \ldots, 6\}$ as the point set, $\mathcal{L} = \{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,0,5\}, \{5,6,1\}, \{1,3,0\}, \{2,0,6\}\}$ as the line set and take the membership relation as the incidence relation. This plane $\mathbf{P}$ is called *Fano plane*, as shown in Figure 1.1. □

In Example 1.24, we see that the Fano plane has the same number of points and lines. Actually, it is true for any finite projective plane, see Proposition I.2.2 in the book by Beth, Jungnickel, and Lenz (1999) or Theorem 3.5 in the book by Hughes and Piper (1973) for a proof.

Theorem 1.25. *Let* $\mathbf{P}$ *be a finite projective plane. Then there exists a positive integer* $n \geq 2$*, such that*

1. *each line contains exactly* $n + 1$ *points;*

2. *each point is on exactly* $n + 1$ *lines;*

3. $\mathbf{P}$ *contains* $n^2 + n + 1$ *points and* $n^2 + n + 1$ *lines.*

The integer n in Theorem 1.25 is called the *order of the projective plane* $\mathbf{P}$. Since $n \geq 2$, the number of points in a projective plane must be at least $2^2 + 2 + 1 = 7$. Hence the Fano plane is of the smallest order.

From Theorem 1.25, we can derive that for any affine plane $\mathbf{A}$, there exists a positive integer n such that

1. each line contains exactly n points;
2. each point is on exactly $n+1$ lines;
3. **A** contains n^2 points and n^2+n lines.

Proposition 1.26. *For each prime power q, there is a projective plane of order q.*

Proof. We can use a 2-dimensional projective space $\mathrm{PG}(2,\mathbb{K})$ over a field $\mathbb{K}$ to define a projective plane. Let V be a 3-dimensional vector space over $\mathbb{K}$, and (x_0,x_1,x_2) be a nonzero element of V. The point $P(x_0,x_1,x_2)$ on $\mathrm{PG}(2,\mathbb{K})$ is defined as

$$P(x_0,x_1,x_2) := \{\, t(x_0,x_1,x_2) : t \in \mathbb{K}^* \,\},$$

i.e. the 1-dimensional subspace $\langle (x_0,x_1,x_2)\rangle$ of V. One could obtain a unique representation for points by making the first nonzero coordinate from the left equal to 1 via an appropriate scalar multiplication. Thus the points of $\mathrm{PG}(2,\mathbb{K})$ can be uniquely represented by

$$\{\,(0,0,1)\,\} \cup \{\,(0,1,y) : y \in \mathbb{K})\,\} \cup \{\,(1,x,y) : x,y \in \mathbb{K}\,\}.$$

For any nonzero $(a_0,a_1,a_2) \in V$, we can define a line on $\mathrm{PG}(2,\mathbb{K})$ as:

$$l(a_0,a_1,a_2) := \{\, P(x_0,x_1,x_2) \in \mathcal{P} : a_0x_0 + a_1x_1 + a_2x_2 = 0 \,\},$$

which is 2-dimensional subspace of V. Clearly, if $t \neq 0$, then $l(a_0,a_1,a_2)$ and $l(t\cdot a_0, t\cdot a_1, t\cdot a_2)$ define the same line.

By the dimension formula of linear algebra, we can show that the first two axioms in Definition 1.22 are satisfied. For the last axiom, we may choose four points $P(1,0,0)$, $P(0,1,0)$, $P(0,0,1)$ and $P(1,1,1)$.

When $\mathbb{K} = \mathbb{F}_q$, we use $\mathrm{PG}(2,q)$ to denote $\mathrm{PG}(2,\mathbb{F}_q)$. The number of 1-dimensional subspace of V is $(q^3-1)/(q-1) = q^2+q+1$. Hence, the order of $\mathrm{PG}(2,q)$ is q. □

Remark 1.27. It should be noted that when $\mathbb{K}$ is a *skew field* (a ring in which division is possible), similarly as the proof of Proposition 1.26, we can also define a projective plane. This plane is called *desarguesian plane*, because Desargues' theorem is universally valid in it. For a proof, see Hughes and Piper (1973, Chapter II).

Take $l := l(1,0,0)$, then $\mathrm{AG}(2,q) := \mathrm{PG}(2,q)^l$ has q^2 points $P(1,x,y)$ for $x,y \in \mathbb{F}_q$. Denote all these points by (x,y). It is routine to check that there are q^2+q lines on $\mathrm{AG}(2,q)$ which are defined by $\{\,(x,y) : y = ax+b\,\}$ for $a,b \in \mathbb{F}_q$ and $\{\,(x,y) : x = c\,\}$ for $c \in \mathbb{F}_q$.

The order of all the known finite projective planes are prime powers, which motivates the following long-standing conjecture.

Conjecture 1.28 (The prime power conjecture - PPC)**.** *A projective plane of order n exists if and only if n is a prime power.*

The nonexistence of a projective plane of order n is only known for all $n \equiv 1$ or $2 \pmod 4$ which are not the sum of two squares by Bruck and Ryser (1949) and for $n = 10$ by Lam, Thiel, and Swiercz (1989).

A *subplane* of a projective plane $\mathbf{P}$ is a subset of points and lines which is itself a projective plane, relative to the incidence relation given in $\mathbf{P}$. By simple counting, the following theorem is due to Bruck (1955).

Theorem 1.29. *Let $\mathbf{P}$ be a projective plane of order n, and $\mathbf{P}_0$ be a proper subplane of order m. Then $m^2 = n$ or $m^2 + m \leq n$.*

When $m^2 = n$ in Theorem 1.29, the subplane $\mathbf{P}_0$ is called *Baer subplane*. In the latter case, if equality were achieved in the stated inequality, i.e. $m^2 + m = n$, then the ambient plane would necessarily have an order which is not a prime power. However, no such example is known.

1.6 Collineation and coordinatization

It seems that there is no promising strategy to prove the elusive "prime power conjecture" in general. One natural compromise is to consider this conjecture under a certain assumption that the projective plane has a specific algebraic structure, for instance, the existence of a certain collineation group.

Let $\mathbf{P}_1$ and $\mathbf{P}_2$ be two projective planes. We can define an *isomorphism* from $\mathbf{P}_1$ to $\mathbf{P}_2$, because they are both incidence structures. An *automorphism* of a projective plane $\mathbf{P}$ is also called a *collineation* of $\mathbf{P}$. Clearly, all collineations of $\mathbf{P}$ form a group $\mathrm{Aut}(\mathbf{P})$, which is called the *full collineation group of* $\mathbf{P}$.

Let $\mathbf{P}$ be a projective plane and P be a point of it. If a non-identity collineation α fixes a line l pointwise, then it can be shown that there is a point V fixed linewise by α, and α fixes no other point or line, see Theorem 4.9 in the book of Hughes and Piper (1973). We call such α a (V,l)*-perspectivity* or (V,l)*-central collineation*. The point V is called the *center* of α and l is the *axis* of α. Now two possibilities arise: if V is on l we call α an *elation*, and if α is not on l we call it a *homology*. It is straightforward to check that, given a point-line pair (V,l), all the (V,l)-perspectivities form a subgroup $\Gamma_{(V,\,l)}$ of the full collineation group of $\mathbf{P}$. If $\Gamma_{(V,\,l)}$ is transitive on the non-fixed points of any line $\neq l$ through V, then $\Gamma_{(V,\,l)}$ is called (V,l)-transitive. A projective plane $\mathbf{P}$ is called (V,l)*-transitive* if its full collineation group $\mathrm{Aut}(\mathbf{P})$ is (V,l)-transitive. If a projective plane $\mathbf{P}$ is (V,l)-transitive for all points V on a line m, then $\mathbf{P}$ is called (m,l)*-transitive*. Dually, we can define (A,B)*-transitivity* for two given points A and B. If l is any line of $\mathbf{P}$ such that $\mathbf{P}$ is (l,l)-transitive then l is called a *translation line* of $\mathbf{P}$. Dually, a point P is called a *translation point* if $\mathbf{P}$ is (P,P)-transitive. The concept

of (V,l)-transitivity, due to Baer (1942), is a very useful classification principle for projective planes. Define

$$\mathbf{T}(\mathbf{P}) := \{\, (V,l) : \mathbf{P} \text{ is } (V,l) - \text{transitive} \,\}.$$

There are totally 53 possibilities for $\mathbf{T}(\mathbf{P})$, which are called *Lenz-Barlotti types for projective planes* due to Lenz (1954) and Barlotti (1957), see page 124–126 in the book by Dembowski (1997) for a complete list. For a recent update of the existence problem of projective planes of certain Lenz-Barlotti types, see the survey by Ghinelli and Merola (2005).

The main tool for the proofs of many of the existence results for projective planes of certain Lenz-Barlotti types is coordinatizing a projective plane with a *planar ternary ring (PTR)*. We follow the way of Hughes and Piper (1973) to coordinatize projective planes, and we also use the corresponding definition of PTRs.

Definition 1.30. A *planar ternary ring* (R,T) is a nonempty set R containing distinct elements called 0 and 1, together with a ternary mapping $T : R^3 \to R$ satisfying the following axioms:

1. $T(a,0,c) = T(0,b,c) = c$ for all a, b and $c \in R$.
2. $T(a,1,0) = T(1,a,0) = a$ for all $a \in R$.
3. If a, b, c and $d \in R$, $a \neq c$, then there is a unique $x \in R$ such that $T(x,a,b) = T(x,c,d)$.
4. If a, b, $c \in R$, then there is a unique $x \in R$ such that $T(a,b,x) = c$.
5. If a, b, c and $d \in R$, $a \neq c$, then there is a unique ordered pair $x,y \in R$ such that $T(a,x,y) = b$ and $T(c,x,y) = d$.

Theorem 1.31. *Let (R,T) be a PTR, and let ∞ be a symbol not contained in R. An incidence structure* **P** *is defined as follows:*

Points: $|R|^2$ *points* (x,y) *for* $x,y \in R$, $|R|$ *points* (z) *for* $z \in R$ *and one point* (∞).

Lines: $|R|^2$ *lines* $[m,k]$ *for* $m,k \in R$, $|R|$ *lines* (l) *for* $l \in R$ *and one line* $[\infty]$.

The incidence is defined in the following manner:

- (x,y) *is on* $[m,k]$ *if and only if* $T(m,x,y) = k$,
- (x,y) *is on* $[l]$ *if and only if* $x = l$,
- (x) *is on* $[m,k]$ *if and only if* $x = m$,
- (x) *is on* $[\infty]$ *for all* $x \in R$ *and* (∞) *is on* $[l]$ *for all* $l \in R$. *Finally* (∞) *is on* $[\infty]$.

Then **P** *is a projective plane.*

Generally speaking, if a projective plane **P** has a large $\mathbf{T}(\mathbf{P})$, then the PTR derived from **P** is quite close to a field. The next theorem can be found in the text book by Hughes and Piper (1973).

Theorem 1.32. *Let* **P** *be a projective plane,* $\mathrm{Aut}(\mathbf{P})$ *be the full collineation group of it and T be the planar ternary ring coordinatizing it.*

(a) T is a field if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (V,l)*-transitive for all V and l plus the "Configuration of Pappus"(see Theorem 2.6 in Hughes and Piper (1973)). Then* **P** *is called a* Pappian plane.

(b) T is a skew field if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (V,l)*-transitive for all V and l. Then* **P** *is called a* desarguesian plane.

(c) T is an alternative division ring if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (V,l)*-transitive for all incident pairs* (V,l)*. Then* **P** *is called a* Moufang plane.

(d) T is a semifield if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (l,l)*-transitive and* (V,V)*-transitive for one incident pair* (V,l)*. Then* **P** *is called a* semifield plane.

(e) T is a nearfield if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (l,l)*-transitive and* (V,m)*-transitive with V on l but not on m. Then* **P** *is called a* nearfield plane.

(f) T is a right nearfield if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (V,V)*-transitive and* (W,l)*-transitive with V but not W on l. Then* **P** *is called a* dual nearfield plane.

(g) T is a quasifield if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (l,l)*-transitive for one l. Then* **P** *is called a* translation plane.

(h) T is a right quasifield if and only if $\mathrm{Aut}(\mathbf{P})$ *is* (V,V)*-transitive for one V. Then* **P** *is called a* dual translation plane.

Remark 1.33. There is another way to coordinatize projective planes presented by Hall (1943), which has been widely applied in text books, for instance, the books by Casse (2006), Dembowski (1997) and Hall (1959). The corresponding definition of PTR is slightly different, which is often called *Hall ternary ring*.

1.7 Quasifields

When the order of **P** is finite, both skew fields and alternative division rings are finite fields due to Wedderburn (1905) and the Artin-Zorn theorem by Zorn (1931). Thus, (a), (b) and (c) in Theorem 1.32 are the same for finite projective plane. Notice that (h) (resp. (f)) is just the dual of (g) (resp. (e)), hence in the following we only give a brief introduction to quasifields, nearfields and semifields. First, by Theorem 1.32 it is obvious that both semifields and nearfields are quasifields.

Definition 1.34. A *quasifield* Q is a set with two binary operations $+$ and $\cdot$ satisfying:

1. $(Q, +)$ is a group with identity element 0.
2. $(Q^*, \cdot)$ is a loop (that is, a quasigroup with an identity element), where $Q^* := Q \setminus \{0\}$.
3. Left distributivity, i.e. $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in Q$.
4. The additive identity 0 satisfies $0 \cdot x = 0$ for all $x \in Q$.
5. $a \cdot x = b \cdot x + c$ has a unique solution for x, given $a, b, c \in Q$ and $a \neq b$.

If $(Q^*, \cdot)$ further forms a group, then Q is called a *nearfield*; if both the left and the right distributivity are satisfied, then Q is called a *semifield*.

Remark 1.35. A finite quasifield, which is neither a semifield nor a nearfield, coordinatize a plane of Lenz-Barlotti type IV a.1. A non-right-distributive finite nearfield coordinatize a plane of Lenz-Barlotti type IV a.2 or IV a.3. A non-associative finite semifield coordinatize a plane of Lenz-Barlotti type V.1. A finite field leads to a plane of Lenz-Barlotti type VII.1. All these results can be found in the text book by Dembowski (1997).

A *right quasifield* is defined by replacing left distributivity by right distributivity in Definition 1.34. When Q is finite, quasifields can also be defined in the following way.

Definition 1.36. A finite quasifield Q is a finite set with two binary operations $+$ and $\cdot$ satisfying:

1. $(Q, +)$ is an abelian group with identity element 0.
2. $(Q^*, \cdot)$ is a loop.
3. Left distributivity holds, i.e. $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in Q$.
4. The additive identity 0 satisfies $0 \cdot x = 0$ for all $x \in Q$.

When $(Q^*, \cdot)$ is a quasigroup without the identity and all the other axioms are still guaranteed, Q is called a *prequasifield*.

André (1954) showed that the additive group of a quasifield Q is an elementary abelian group, which means that Q can be defined on a vector space over a finite field $\mathbb{K}$. The characteristic of $\mathbb{K}$ is called the *characteristic* of Q. Furthermore, the order of a (dual) translation plane is always a prime power, and the prime power conjecture holds for the planes in Theorem 1.32.

A quasifield, which is neither a semifield nor a nearfield, was given by Hall (1943), which can also be found in the text book of Hall (1959).

Definition 1.37. A *finite Hall quasifield* is a quasifield $H(q^2, f)$ constructed as follows. Let $f(x) = x^2 - rx - s$ be an irreducible quadratic over $\mathbb{F}_q$ and λ be a zero of f in $\mathbb{F}_{q^2}$. Hence every element in $\mathbb{F}_{q^2}$ can be written as $(a, b) := a + b\lambda$ where $a, b \in \mathbb{F}_q$. The addition $+$ in $H(q^2, f)$ is defined by

$$(a, b) + (c, d) = (a + c, b + d).$$

The multiplication $*$ in $H(q^2, f)$ is defined by

$$(a, b) * (c, 0) = (ac, bc),$$

$$(a, b) * (c, d) = (ac - bd^{-1}f(c), ad - bc + br), \quad \text{for } d \neq 0.$$

Definition 1.38. The *kernel* K of a quasifield Q is the set of all elements $k \in Q$ such that

1. $(x + y) \cdot k = x \cdot k + y \cdot k$, and
2. $(x \cdot y) \cdot k = x \cdot (y \cdot k)$

holds for all $x, y \in Q$.

In fact, the kernel K is a field with respect to $\cdot$ and $+$, and Q may be regarded as a right vector space over K, see Theorem 7.2 in Hughes and Piper (1973) for a proof. Assume that $K = \mathbb{F}_q$ and $|Q| = q^m$. We can use the elements of $\mathbb{F}_{q^m}$ to denote those of Q. For each $a \in \mathbb{F}_{q^m}$, the mapping $x \mapsto a \cdot x$ defines a q-polynomial

$$\sum_{i=0}^{m-1} c_i(a) x^{q^i} \in \mathbb{F}_{q^m}[x]. \tag{1.8}$$

Spreads and *spreadsets* are important tools to characterize quasifields or, equivalently, translation planes.

Definition 1.39. Let $(V, +)$ be a vector space over a field $\mathbb{K}$. Then a collection $\mathfrak{S}$ of subspaces of V is called a *spread* if

1. $A, B \in \mathfrak{S}$ and $A \neq B$ then $V = A \oplus B$ and
2. every $x \in V^*$ lies in a unique member of $\mathfrak{S}$.

The members of $\mathfrak{S}$ are called the *components* of the spread and V is called the *ambient space* for the spread.

Definition 1.40. A set $\mathcal{S}$ of $n \times n$ matrices over $\mathbb{F}_q$ is a *spreadset* if

1. $|\mathcal{S}| = q^n$,
2. $M_1 - M_2$ is nonsingular, for any $M_1, M_2 \in \mathcal{S}$, $M_1 \neq M_2$,

3. $\mathcal{S}$ includes the zero matrix.

Actually prequasifields, spreads and spreadsets are equivalent concepts. A proof can be found in Chapter 5 of the handbook by Johnson, Jha, and Biliotti (2007). Here we give a very basic example to illustrate the relation among them.

Result 1.41. Take $\mathrm{AG}(2,q)$ as in Remark 1.27. It is not difficult to check that

$$\{\,(0,x) : x \in \mathbb{F}_q\,\} \text{ and } \{\,(x,y) : y = ax, x \in \mathbb{F}_q\,\} \text{ for all } a \in \mathbb{F}_q$$

form a spread. Actually, they are all the lines passing through $(0,0)$. Furthermore, let $q = p^n$ with p prime, then $\mathbb{F}_q$ can be viewed as an n-dimensional vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$, and there are q linear mappings L_a from $\mathbb{F}_p^n$ to itself defined by $L_a(x) = ax$ with $a \in \mathbb{F}_q$. When $a \neq 0$, L_a can be expressed as nonsingular matrices M_a, and it is obvious that $M_a - M_b$ is always nonsingular if $a \neq b$, since $M_a - M_b = M_{a-b}$. The set $\{\,M_a : a \in \mathbb{F}_q\,\}$ forms the spreadset derived from $\mathrm{AG}(2,q)$. □

Quasifields are an important topic in the research of finite geometry. People are interested in various quasifields, with special collineation groups. On the other hand, it is also interesting to look at some geometric objects, for example ovals and unitals, within the translation planes. There is a more than 800 pages handbook by Johnson, Jha, and Biliotti (2007) about quasifields.

To classify all the quasifields seems a very difficult task, simply because there are too many of them. But some special quasifields have been classified: First, it is well-known that up to isomorphism, finite fields are unique. On the other hand, finite nearfields have also been completely classified by Zassenhaus (1935), see also the text book of Hall (1959). Actually, since $(Q^*, \cdot)$ form a group when Q is a nearfield, the set of all transformations $x \mapsto ax + b$ with $a, b \in Q$ and $a \neq 0$ acts sharply 2-transitive on Q, which is a very strong condition from a group theoretical point of view.

As one of the main contributions of this thesis is about semifield, we discuss semifields in more detail in Section 1.8.

1.8 Semifields

As we mentioned in Section 1.7, a *semifield* $\mathbb{S}$ is a quasifield with the extra property that it satisfies the right distributive law, i.e. an algebraic structure satisfying all the axioms of a skewfield except (possibly) associativity of multiplication. In other words, $\mathbb{S}$ satisfies the following axioms:

- $(\mathbb{S}, +)$ is a group, with identity element 0.
- $(\mathbb{S} \setminus \{\,0\,\}, *)$ is a loop.

- $0 * a = a * 0 = 0$ for all a.
- The left and right distributive laws hold, namely, for any $a, b, c \in \mathbb{S}$,

$$(a + b) * c = a * c + b * c,$$

$$a * (b + c) = a * b + a * c.$$

A finite field is a trivial example of a semifield. If $\mathbb{S}$ does not necessarily have a multiplicative identity, then it is called a *presemifield* denoted by $\mathbb{P}$. A semifield is not necessarily commutative or associative. However, by Wedderburn (1905)'s Theorem, in the finite case, associativity implies commutativity. Therefore, a non-associative finite commutative semifield is the structure closest to a finite field.

In the earlier literature, the term semifield was not used. They were called "nonassociative division rings " or "distributive quasifields" instead. The study of these algebraic structures were initiated by Dickson (1906). The term semifield was introduced by Knuth (1965b). A recent and comprehensive survey was written by Lavrauw and Polverino (2011).

Let $\mathbb{S}$ be a finite semifield of order q. Since $\mathbb{S}$ is a special finite quasifield, the order q is a prime power and the additive group of $\mathbb{S}$ is an elementary abelian group of order q. Thus, we can identify the elements of $\mathbb{S}$ with those of $\mathbb{F}_q$, and the addition on $\mathbb{S}$ is the same as the addition "+"on $\mathbb{F}_q$. Furthermore, we can also identify the elements of $\mathbb{S}$ with the elements of $\mathbb{F}_{\tilde{q}}^n$, where $\tilde{q}^n = q$.

Definition 1.42. The first non-trivial semifields were given by Dickson (1906). Dickson's semifield $(\mathbb{F}_q^2, +, \circ)$ is defined by

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \circ (c, d) = (ac + \alpha(bd)^\sigma, ad + bc),$$

where q is a power of an odd prime p, α is a non-square in $\mathbb{F}_q$ and $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is not the identity.

Let $(\mathbb{F}_{q^m}, +, *)$ be a semifield with kernel $\mathbb{F}_q$. According to (1.8), there exist mappings $c_i(x)$ on $\mathbb{F}_{q^m}$ for $i = 0, \ldots, m-1$ such that

$$x * y = \sum_{i=0}^{m-1} c_i(x) y^{q^i}.$$

Since the right distributive law also holds, it can be further written as

$$x * y = \sum_{i,j=0}^{m-1} c_{ij} x^{q^i} y^{q^j}. \tag{1.9}$$

Definition 1.43. Let $\mathbb{P}_1 = (\mathbb{F}_{p^n}, +, *)$ and $\mathbb{P}_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields. If there exist three bijective linear mappings $L, M, N : \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_{p^n}$, then $\mathbb{P}_1$ and $\mathbb{P}_2$ are called *isotopic*, and the triple (M, N, L) is an *isotopism* between $\mathbb{P}_1$ and $\mathbb{P}_2$. Furthermore, if there exists an isotopism of the form (N, N, L) between $\mathbb{P}_1$ and $\mathbb{P}_2$, then $\mathbb{P}_1$ and $\mathbb{P}_2$ are called *strongly isotopic*. If $\mathbb{P} = \mathbb{P}_1 = \mathbb{P}_2$, then we call (M, N, L) an *autotopism* of $\mathbb{P}$ and (N, N, L) a *strong autotopism* of $\mathbb{P}$. All the autotopisms of $\mathbb{P}$ form a group $\mathrm{Aut}(\mathbb{P})$, which has a subgroup $\mathrm{Aut}_S(\mathbb{P})$ consisting of all the strong autotopisms of $\mathbb{P}$.

In the geometric language, a semifield plane is a translation plane and also a dual translation plane. The importance of the notion of isotopism arises from the result by Albert (1960):

Theorem 1.44. *Two (pre)semifields coordinatize isomorphic projective planes if and only if they are isotopic.*

Let $\mathbb{P} = (\mathbb{F}_{p^n}, +, *)$ be a presemifield. We can obtain a semifield from it in several ways. The following method was recently given by Bierbrauer (2012). If we define a new multiplication $\star$ by the rule

$$x \star y := B^{-1}(B_1(x) * y), \tag{1.10}$$

where $B(x) := 1 * x$ and $B_1(x) * 1 = 1 * x$. We have $x \star 1 = B^{-1}(B_1(x) * 1) = B^{-1}(1 * x) = x$ and $1 \star x = B^{-1}(B_1(1) * x) = B^{-1}(1 * x) = x$, thus $(\mathbb{F}_{p^n}, +, \star)$ is a semifield with unit 1. In particular, when $\mathbb{P}$ is commutative, B_1 is the identity mapping.

Let q be an odd prime power. When the multiplication $*$ of a (pre)semifield $\mathbb{P}$ of order q is commutative, we define $f : \mathbb{F}_q \to \mathbb{F}_q$ by

$$f(x) := x * x \tag{1.11}$$

Then f is a planar function, because for every nonzero a,

$$x \mapsto f(x + a) - f(x) = 2a * x + a * a$$

is a bijection on $\mathbb{F}_q$. Furthermore, by (1.9), $f(x) = x * x$ can also be written as a Dembowski-Ostrom polynomial.

On the other hand, let f be a Dembowski-Ostrom polynomial which defines a planar function on $\mathbb{F}_q$. Define

$$x \circ y := \frac{f(x + y) - f(x) - f(y)}{2}, \tag{1.12}$$

for $x, y \in \mathbb{F}_q$. Then by (1.7), both the left and right distributive laws hold for $(\mathbb{F}_q, +, \circ)$. Since f is planar, $(\mathbb{F}_q, \circ)$ is a quasigroup. Therefore, $(\mathbb{F}_q, +, \circ)$ is a commutative presemifield. We summarize the above results in the following theorem, which was also proved by Coulter and Henderson (2008).

Theorem 1.45. *Let q be an odd prime power. Then commutative presemifields of order q and planar functions described by DO polynomials on $\mathbb{F}_q$ are equivalent in the following sense:*

(a) Let $(\mathbb{F}_q, +, *)$ be a commutative presemifield. Then the mapping $x \mapsto x * x$ is planar, and it defines a DO polynomial in $\mathbb{F}_q[x]$.

(b) Let f be a planar DO polynomial in $\mathbb{F}_q[x]$. Let $x \circ y := \frac{1}{2}(f(x+y) - f(x) - f(y))$ for $x, y \in \mathbb{F}_q$. Then $(\mathbb{F}_q, +, \circ)$ is a commutative presemifield. □

As a special quasifield, a semifield has its characteristic and kernel. It also has some other special invariants under isotopism. Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ be a semifield. The subsets

$$N_l(\mathbb{S}) = \{\, a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S} \,\},$$
$$N_m(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathbb{S} \,\},$$
$$N_r(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * y) * a = x * (y * a) \text{ for all } x, y \in \mathbb{S} \,\},$$

are called the *left, middle* and *right nucleus* of $\mathbb{S}$, respectively. It is not difficult to check that these sets form finite fields and are invariant under isotopism. According to Definition 1.38, $N_r(\mathbb{S})$ is the kernel of $\mathbb{S}$ when $\mathbb{S}$ is viewed as a quasifield. $N_l(\mathbb{S})$, $N_m(\mathbb{S})$, $N_r(\mathbb{S})$ are called the *semi-nuclei* of $\mathbb{S}$. The subset $N(\mathbb{S}) := N_l(\mathbb{S}) \cap N_m(\mathbb{S}) \cap N_r(\mathbb{S})$ is called the *associative center* of $\mathbb{S}$. The subset $\{a \in \mathbb{S} : a * x = x * a \text{ for all } x \in \mathbb{S}\}$ is called the *commutative center* of $\mathbb{S}$ and its intersection with the $N(\mathbb{S})$ is called the *center* of $\mathbb{S}$.

When $\mathbb{S}$ is commutative and $a \in N_l(\mathbb{S})$, then for any x and $y \in \mathbb{S}$

$$(x * a) * y = (a * x) * y = a * (x * y) = (a * y) * x = x * (a * y),$$

thus $a \in \mathbb{N}_m(\mathbb{S})$. Clearly $N_l(\mathbb{S}) = N_r(\mathbb{S})$, therefore $N_l(\mathbb{S}) = N_r(\mathbb{S}) = N(\mathbb{S})$.

For a geometric description of these semi-nuclei, see Theorem 8.2 in the book of Hughes and Piper (1973).

As a quasifield can be always viewed as a right vector space over its kernel, a semifield $\mathbb{S}$ can also be regarded as a left vector space over its left nucleus, as a left or right vector space over its middle nucleus, and as a right vector space over its right nucleus. Define $L_a(x) := a * x$ and $R_a(x) := x * a$. Since $L_a(x) * c = L_a(x * c)$ for any $c \in N_r(\mathbb{S})$, L_a defines a linear mapping from $\mathbb{S}$ as a left vector space over its left nucleus to itself. Similarly R_a is a linear mapping from $\mathbb{S}$ as a right vector space over its right nucleus to itself.

Let $(\mathbb{F}_p^n, +, \circ)$ be a semifield, and let $\{\, e_i : i = 1, \ldots, n \,\}$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_p^n$. Let $x = \sum_{i=1}^n x_i e_i$ and $y = \sum_{i=1}^n y_i e_i$, then

$$x \circ y = \sum_{i,j=1}^{n} x_i y_i (e_i \circ e_j) = \sum_{i,j=1}^{n} x_i y_j (\sum_{k=1}^{n} a_{ijk} e_k)$$

for certain $a_{ijk} \in \mathbb{F}_p$. Then we get a 3-dimensional $n \times n \times n$ array (a_{ijk}), which is also called a *Knuth's cubical array*. Knuth (1965b) noticed that, given a semifield $\mathbb{S}$, another five semifields can be obtained from the action of the symmetric group S_3 on the indices of the Knuth's cubical array of $\mathbb{S}$.

As Hughes and Piper (1973, Lemma 8.4 and Theorem 8.6) showed, the automorphism group of a semifield plane can be decomposed in the following way:

Theorem 1.46. *Let $\mathbf{P}(\mathbb{S})$ be a semifield plane defined by a semifield $\mathbb{S}$. Let l_∞ be the translation line of $\mathbf{P}(\mathbb{S})$ and l_0 be another line meeting l_∞ at point (∞). Let $\Gamma_{(l_\infty,\, l_\infty)}$ be its translation group and $\Gamma_{((\infty),\, l_0)}$ be a group of* shears *(automorphisms fixing (∞) and l_0). Let* Aut$(\mathbb{S})$ *denote the autotopism group of $\mathbb{S}$. Then we have*

- $\Sigma := \Gamma_{(l_\infty,\, l_\infty)} \rtimes \Gamma_{((\infty),\, l_0)}$ *is a subgroup of* Aut$(\mathbf{P}(\mathbb{S}))$*;*
- Aut$(\mathbf{P}(\mathbb{S})) \cong \Sigma \rtimes$ Aut$(\mathbb{S})$.

In contrast to nearfields, semifields have not been completely classified. However, there are several results for semifields, which have small dimension over their centers.

Theorem 1.47. *(i) A semifield of dimension* 2 *over its center is a finite field.*

(ii) A semifield of order q^3 with center containing $\mathbb{F}_q$ is either a field or isotopic to a generalized twisted field.

(iii) Let $\mathbb{S}$ be a semifield of prime dimension over its center $\mathbb{F}_q$. If q is large enough, then $\mathbb{S}$ is a field or isotopic to a generalized twisted field.

Remark 1.48. Result (i) was proved by Dickson (1906). Menichetti (1977, 1996) proved (ii) and (iii).

When the dimension of a semifield over its center is getting larger, there are several recent results. Semifields of order q^4 with left nucleus $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ were classified by Cardinali, Polverino, and Trombetti (2006). Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$, right nucleus $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ were classified by Marino, Polverino, and Trombetti (2011).

Semifields of order 2^4, 2^5, 2^6, 3^4 and 3^5 are also classified by hand or by computer, see the papers by Kleinfeld (1960), Walker (1963), Rúa, Combarro, and Ranilla (2009), Dempwolff (2008) and Rúa and Combarro (2012), respectively.

At present, there are various constructions of semifields, see the list in the survey by Lavrauw and Polverino (2011). About the total number of pairwise non-isotopic semifields, Kantor (2006) has the following conjecture:

Conjecture 1.49. *The number of pairwise non-isomorphic semifield planes of order N is not bounded above by a polynomial in N.*

As Kantor (2006) summarized,

- for N odd, the number of known semifields is less than N^3,
- for N even, then the conjecture is true by the result of Kantor (2003).

For commutative semifields, what we have known is even less, as Kantor (2003) said:

> The study of finite commutative semifields was begun by Dickson almost a century ago ... It is a bit surprising that so few examples are known (up to isotopism).

For N odd, there are several new constructions obtained after Kantor's comments, but the total number of commutative semifields of order N remains still very small. As far as I know, it is even not proved that the number of pairwise non-isotopic commutative semifields of order $N = p^n$ is not bounded above by a polynomial in n.

For N even, there is only one infinite family of semifields constructed by Kantor (2003), as a generalization of the binary semifields constructed by Knuth (1965a). However, the construction by Kantor is so powerful that it provides a number of pairwise non-isotopic semifields of order N, which is not bounded above by a polynomial in N. We note that no non-associative commutative semifield of order 2^{2^t} is known.

We list all the commutative semifields of order p^n that are already known.

- Any odd prime p:
  - (i) The finite fields.
  - (ii) Albert's commutative twisted fields.
  - (iii) Dickson's semifields.
  - (iv) The Budaghyan-Helleseth semifields with n even.
  - (v) The Zha-Kyureghyan-Wang semifields with $n = 3k$.
  - (vi) Bierbrauer's semifields with $n = 4k$.
  - (vii) Our new semifields with n even, see Chapter 2.
- $p = 2$:
  - (viii) Kantor's semifields, where n has an odd divisor.
- $p = 3$:
  - (ix) The Coulter-Matthews-Ding-Yuan semifields with n odd.
  - (x) Ganley's semifields with n even.

(xi) The Cohen-Ganley semifields with n even.

- Sporadic examples:

(xii) The Coulter-Henderson-Kosick semifield with $p = 3$ and $n = 8$.

(xiii) The Penttila-Williams semifield with $p = 3$ and $n = 10$.

(xiv) Semifield defined by $x^{90} + x^2$ on $\mathbb{F}_{3^5}$.

(xv) Semifield defined by $x^{162} + x^{108} - x^{84} + x^2$ on $\mathbb{F}_{3^5}$.

(xvi) Semifield defined by $x^{50} + 3x^6$ on $\mathbb{F}_{5^5}$.

Remark 1.50. Family (ii) is due to Albert (1961a). They belong to a subfamily of generalized twisted fields which are not necessarily commutative, see Definition 2.2. Family (iii) was constructed by Dickson (1906), see Definition 1.42. Budaghyan and Helleseth (2008, 2011), as well as Zha and Wang (2009) independently proved (iv), see Theorem 2.17. Family (v) is due to Zha, Kyureghyan, and Wang (2009), and family (vi) is due to Bierbrauer (2010). Family (vii) is recently introduced by Zhou and Pott (2013), see Theorem 2.4 for a proof.

Kantor (2003) constructed family (viii), which is a generalization of the binary semifields due to Knuth (1965a), see Definition 4.6.

Family (ix) was first constructed by Coulter and Matthews (1997) and later extended by Ding and Yuan (2006).[1] Ganley (1981) showed (xi), and Cohen and Ganley (1982) proved (xi).

Semifield (xii) was discovered by Coulter, Henderson, and Kosick (2007), and semifield (xiii) is due to Penttila and Williams (2004). Weng and Zeng (2012) constructed semifield (xiv). Semifields (xv) and (xvi) are due to Coulter and Kosick (2010) and Weng and Zeng (2012).

1.9 Dembowski-Piper classification

As we mentioned before in the connection with the Lenz-Barlotti classification, one typical hypothesis on the collineation group of a projective plane is the (V, l)-transitivity for some point-line pair (V, l). Another typical hypothesis concerns orbits of points and/or orbits of lines of a projective plane under its collineation group. One celebrated theorem was proved by Ostrom and Wagner (1959):

Theorem 1.51. *Let* **P** *be a projective plane of order n admitting a doubly transitive collineation group G. Then* Π *is desarguesian, and* $\mathrm{PSL}(3, n)$ *is a subgroup of G.*

[1] I was informed that family (ix) was also described in the master thesis by Kristensen (Department of Informatics, University of Bergen, 1997).

We can weaken the hypothesis in Theorem 1.51 and only require the group to be flag-transitive, which is transitive on every incident point-line pair. It is conjectured that the result should be the same as before. Unfortunately, despite many authors' efforts, this case is not yet settled, see the survey by Thas (2003).

Now suppose that the projective plane $\mathbf{P}$ has a *quasiregular* collineation group G, that is, G induces a regular action on each point (or line) orbit $\mathcal{O}$: for any $\gamma \in G$, if γ fixes one element in $\mathcal{O}$, then it fixes all the elements in $\mathcal{O}$. This condition is satisfied in particular when G is abelian or hamiltonian. Indeed it is not difficult to show that all permutation representations of a group are quasiregular if and only if every subgroup of it is normal, see the books by Dembowski (1997) and by Hall (1959).

Dembowski (1965) showed that every finite collineation group of a projective plane acts faithfully on at least one (point or line) orbit, which we call a *faithful orbit*. It implies that, if a quasiregular group G is "large" in the sense that

$$|G| > \frac{1}{2}(n^2 + n + 1),$$

then there is a unique faithful point (or line) orbit under the action of G. Dembowski and Piper (1967) classified these planes into the following eight classes.

Theorem 1.52. *Let G be a collineation group acting quasiregularly on the points and lines of a projective plane of order n, and assume $|G| > \frac{1}{2}(n^2 + n + 1)$. Let t denote the number of point orbits (which agrees with the number of line orbits by Theorem 1.6), and let F denote the incidence structure consisting of the fixed points and fixed lines. Then one of the following holds:*

(a) $|G| = n^2 + n + 1$, $t = 1$ *and F is empty. In this case, G is transitive.*

(b) $|G| = n^2$, $t = 3$ *and F is a flag, i.e. an incident point-line pair (∞, l_∞).*

(c) $|G| = n^2$, $t = n + 2$, *F is either a line and all its points, or dually a point together with all its lines.*

(d) $|G| = n^2 - 1$, $t = 3$, *F is an anti-flag, i.e. a non-incident point-line pair.*

(e) $|G| = n^2 - \sqrt{n}$, $t = 2$ *and F is empty. In this case, one point and one line orbit together form a Baer subplane of order $\sqrt{n}$.*

(f) $|G| = n(n-1)$, $t = 5$, *F consists of two points U, V, the line UV, and another line trough one of U, V.*

(g) $|G| = (n-1)^2$, $t = 7$, *F consists of the vertices and sides of a triangle.*

(h) $|G| = (n - \sqrt{n} + 1)^2$, $t = 2\sqrt{n} + 1$, *F is empty. In this case there are $2\sqrt{n}$ disjoint subplanes of order $\sqrt{n} - 1$ whose point sets constitute $2\sqrt{n}$ orbits, each of length $n - \sqrt{n} + 1$.*

Remark 1.53. Dembowski (1965) proved the types (b) and (c), and Dembowski and Piper (1967) showed the remaining types. For recent updates, see the survey by Ghinelli and Jungnickel (2003) and Chapter 5 of the monograph by Pott (1995).

Planes of type (c) are translation planes or dual translation planes. As we mentioned in Section 1.7, the translation group G is always an elementary p-group and the prime power conjecture for a translation plane always holds.

Planes of type (h) are completely determined by Ganley and McFarland (1975), who proved the following theorem implying that the prime power conjecture also holds in case (h).

Theorem 1.54. *A finite projective plane of order n admits a quasiregular collineation group G of order $(n - \sqrt{n} + 1)^2$ if and only if $n = 4$.*

Next we consider projective planes with the quasiregular collineation groups listed in Theorem 1.52 except for (c) and (h). Let us first look at type (a). We see that all the points of the projective plane are in one orbit on which G acts regularly. By Theorem 1.9, there exists an $(n^2 + n + 1, n + 1, 1)$-difference set $D \subseteq G$ such that the development of D is this projective plane. Actually, we can use (generalized, relative) difference sets to illustrate all the other types of projective planes with the quasiregular collineation groups listed in Theorem 1.52 except for (c) and (h).

Theorem 1.55. *Suppose that we are in one of the cases (a), (b), (d), (e), (f) and (g) of Theorem 1.52. Let P be a point in the point orbit of length $|G|$ and let l be a line in the line orbit of length $|G|$. Define $D := \{ g \in G : P^g \in l \}$, then D is a (generalized, relative) difference set with the following parameters:*

(a) $(n^2 + n + 1, n + 1, 1)$*-difference set. One usually calls D a* planar difference set *of order n.*

(b) $(n, n, n, 1)$*-RDS.*

(d) $(n + 1, n - 1, n, 1)$*-RDS. One usually calls D an* affine difference set *of order n.*

(e) $(n + \sqrt{n} + 1, n^2 - \sqrt{n}, n, 1)$*-RDS.*

(f) $(n(n-1); n, n-1; n-1, 1; 0, 0)$*-GDS relative to subgroups A and B of orders n and $n - 1$, which is originally called an* $(n, n-1, n-1, 0, 0, 1)-$direct product difference set *introduced by Ganley (1977).*

(g) $((n-1)^2; n-1, n-1, n-1; n-2, 1; 0, 0, 0)$*-GDS relative to three subgroups of order $n - 1$ which intersect pairwise trivially.*

Conversely, when a (generalized, relative) difference set D with the above parameters is given, the development of D either is or can be uniquely extended to a projective plane of order n.

Remark 1.56. As we showed, case (a) follows directly from Theorem 1.9. Cases (b), (d) and (e) in Theorem 1.55 are proved by Ganley and McFarland (1975). Case (f) is due to Ganley (1977), and case (g) is due to Hughes (1955).

Type (a): Planar difference sets

Let $n = 2$ in Theorem 1.10. Then we get a $(q^2 + q + 1, q + 1, 1)$-difference set, which defines the desarguesian plane $\mathrm{PG}(2, q)$.

It was shown by Bruck (1955) that any cyclic projective plane of order $n \equiv 1 \pmod 3$ also admits a non-abelian Singer group. That means there is a non-abelian planar difference set of order $n \equiv 1 \pmod 3$ whenever n is a prime power, see also Theorem VI.7.1 in the book by Beth, Jungnickel, and Lenz (1999).

Both the scarcity of known examples and strong nonexistence results led to a couple of famous unsolved conjectures on planar difference sets:

- Any finite projective plane admitting a Singer group is desarguesian.
- Any abelian planar difference set is cyclic.

The prime power conjecture is still open for planes of this type:

- Assume the existence of an abelian planar difference set of order n. Then n is a prime power.

Type (b): $(n, n, n, 1)$-RDSs

Projective planes of type (b) are the main objects in Chapters 2, 3 and 4. Hence, we give more information about them than the other cases.

Result 1.57. Let D be a $(n, n, n, 1)$-RDS in $(G, +)$ relative to N, then the projective plane $\mathbf{P}(D)$ can be obtained in the following way:

affine points: $g \in G$;

lines: $D + g := \{d + g : d \in D\}$, and the distinct cosets of N: $N + g_1, \ldots, N + g_n$ and an extra line l_∞ defined as a set of extra points;

points on l_∞: (g_i) defined by the parallel classes $\{D + g_i + h : h \in N\}$ and (∞) defined by the parallel classes $\{N + g_1, \ldots, N + g_n\}$.

An affine point x is mapped to $x+g$ under the action of $g \in G$. Therefore, all the affine points form a orbit under G. Furthermore, (∞) is fixed under G, and the points on l_∞ except for (∞) form a orbit. The lines of $\mathbf{P}(D)$ also have three orbits: $\{D+g : g \in G\}$, $\{l_\infty\}$, and all the lines incident with (∞) except for l_∞. When G is commutative, $\mathbf{P}(D)$ is called a *shift plane* and G is its *shift group*. □

The next result by Jungnickel (1982) shows that, every semifield of order q leads to a $(q,q,q,1)$-RDS (not necessarily abelian). It implies that semifields can be regarded as a subset of $(q,q,q,1)$-RDSs.

Result 1.58. Let $*$ be the multiplication of a semifield $\mathbb{S}$. We can define a projective plane $\mathbf{P}(\mathbb{S})$ in the following way: We use $(x,y) \in \mathbb{S} \times \mathbb{S}$ to denote the affine points of $\mathbf{P}(\mathbb{S})$, and we label the lines by the point sets

$$[m,k] = \{\,(x,y) : m * x + y = k\,\} \quad \text{with } m,k \in \mathbb{S}$$

and all $[k] = \{\,(k,y) : y \in \mathbb{S}\,\}$ with $k \in \mathbb{S}$. The points on l_∞ are defined by the parallel lines in the affine plane, i.e. all the lines with the same slope m define a point (m) on l_∞ and all lines $[k]$ define the point (∞) on l_∞. Then there are p^{2n} bijections

$$\alpha_{a,b} : (x,y) \mapsto (x+a, y+a*x+b) \quad \text{with } a,b \in \mathbb{S} \times \mathbb{S},$$

which form a collineation group G of $\mathbf{P}(\mathbb{S})$, since

$$\alpha_{a,b}(\alpha_{c,d}(x,y)) = \alpha_{a+c,b+d+a*c}(x,y). \tag{1.13}$$

Under the action of $\alpha_{a,b}$, point (m) is mapped to $(m+a)$ because

$$\alpha_{a,b}(x, m*x+k) = (x+a, (m+a)*x+k+b).$$

Hence, all the points of $\mathbf{P}(\mathbb{S})$ are divided into 3 orbits: all the affine points $\{(x,y) : x,y \in \mathbb{S}\}$, $\{(m) : m \neq \infty\}$ and $\{(\infty)\}$. They are exactly of type (b) of Theorem 1.52.

By (1.13), we see that $\alpha_{0,b}\alpha_{0,d} = \alpha_{0,b+d}$, and

$$\alpha_{a,b}\alpha_{0,d} = \alpha_{a,b+d} = \alpha_{0,d}\alpha_{a,b}.$$

It follows that all $\alpha_{0,b}$ form a normal subgroup of G. Furthermore, it follows from (1.13) that G is abelian if and only if $*$ is commutative. If we choose $(0,0)$ as the "base point" and $[-1,0]$ as the "base line", by Theorem 1.55 we get a $(p^n,p^n,p^n,1)$-RDS

$$D := \{\alpha_{x,x} : x \in \mathbb{S}\} \subseteq G.$$

In particular, since there are many non-commutative semifields, non-abelian $(p^n,p^n,p^n,1)$-RDSs do exist. □

Now, we focus on abelian cases. First, the prime power conjecture on the planes derived from abelian $(n, n, n, 1)$-RDSs is proved.

Theorem 1.59. *Let D be a $(n, n, n, 1)$-RDS in an abelian group G of order n^2.*

(i) If n is even, then n is a power of 2 (say $n = 2^m$), $G \cong C_4^m$ and the forbidden subgroup $N \cong C_2^m$.

(ii) If n is odd, then n is a prime power (say $n = p^m$) and the rank of G, i.e. the smallest cardinality of a generating set for G, is at least $m + 1$.

Remark 1.60. Result (i) was proved by Ganley (1976). A short proof was also given by Jungnickel (1987b). Result (ii) is due to Blokhuis, Jungnickel, and Schmidt (2002).

Let G be an elementary abelian group of order q^2, where q is an odd prime power. The forbidden subgroup N is one of its subgroups of order q. As we mentioned in Proposition 1.20, every $(q, q, q, 1)$-RDS in G can be always written as

$$D := \{ (x, f(x)) : x \in \mathbb{F}_q \},$$

where f is a planar function on $\mathbb{F}_q$.

(i) The classical planar function is $f(x) = x^2$, the corresponding RDS defines the desarguesian plane.

(ii) Most of the known planar functions can be written as DO polynomials, which are equivalent to commutative presemifields with odd characteristic, see Theorem 1.45.

(iii) The only known planar functions, which are not equivalent to DO polynomials, are

$$x^{\frac{3^k+1}{2}} \in \mathbb{F}_{3^n}[x] \tag{1.14}$$

where k is odd and $\gcd(k, n) = 1$. These planar functions were found by Coulter and Matthews (1997) as well as Helleseth and Sandberg (1997), independently. This family of planar functions defines planes of Lenz-Barlotti class II.1, but not semifield planes.

When n is even, by Theorem 1.59 (i), the $(n, n, n, 1)$-RDSs are not splitting. Hence, we can not use planar functions to represent them anymore. We will see constructions in Example 4.5 and Definition 4.6.

Type (d): Affine difference sets

The following result is due to Bose (1942) and Elliott and Butson (1966).

Theorem 1.61. *Let G be the multiplicative group of $\mathbb{F}_{q^n}$. Let*

$$D := \{\, x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}_{q^n/q}(x) = 1 \,\},$$

where $\mathrm{Tr}_{q^n/q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is the trace mapping. Then D is a $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$-RDS relative to $N = \mathbb{F}_q^*$. In particular, when $n = 2$, D is a $(q+1, q-1, q, 1)$-RDS.

The project planes defined by the RDSs from Theorem 1.61 are always desarguesian.

Some non-abelian affine difference sets describing desarguesian planes of odd order were given by Ganley and McFarland (1975), but no non-abelian examples seem to be known for planes of even order.

The prime power conjecture for this type of planes is far from solved, in spite of many authors' efforts, see the survey by Jungnickel (1992). A stronger version of the PPC conjectures that any plane associated with an affine difference set is necessarily desarguesian.

Type (e): Baer subplanes

The only known abelian example up to equivalence is described by the $(7, 2, 4, 1)$-RDS $\{\, 0, 1, 4, 6 \,\}$ in C_{14}. It corresponds to the desarguesian plane $\mathrm{PG}(2, 4)$.

The unique known non-abelian example comes from the Hughes plane of order 9 associated with an RDS in $C_{13} \times S_3$, see Hughes (1955) for the Hughes planes and see Jungnickel (1987a) for the RDS representation.

Ghinelli and Jungnickel (2003) conjectured that the only projective planes admitting a quasiregular collineation group of type (e) are $\mathrm{PG}(2, 4)$ and the Hughes plane of order 9, and an abelian group of this type exists only in the former case.

Type (f): Direct product difference sets

Theorem 1.62. *Let G be the direct product of the additive group N_1 and the multiplicative group N_2 of $\mathbb{F}_q$. Then the subset*

$$D := \{\, (x, x) \in N_1 \times N_2 : x \in \mathbb{F}_q^* \,\}$$

is an $(q, q-1, q-1, 0, 0, 1)$-direct product difference set. The associated projective plane is desarguesian.

The direct product difference sets from Theorem 1.62 are the only known abelian examples of type (f) in Theorem 1.55 up to equivalence.

In fact, Theorem 1.62 was first noted by Spence, see Ganley (1977). It was shown by Hiramine (1999) that if one replaces the field $\mathbb{F}_q$ in the above construction by a non-right-distributive nearfield and uses its additive and multiplicative groups, then non-abelian GDSs will be obtained.

It is conjectured that any finite projective plane admitting an abelian group of type (f) is desarguesian.

The prime power conjecture was proved for this type of planes.

Theorem 1.63. *Let G be an abelian collineation group of type (f) in Theorem 1.52 for a projective plane of order n. Then n must be a power of a prime p.*

Remark 1.64. The even order case of Theorem 1.63 was established by Ganley (1977), and the whole theorem was proved by Jungnickel and de Resmini (2002).

Type (g): Neofields

The following construction is due to Hughes (1955).

Theorem 1.65. *Let $G := (\mathbb{F}_q^*, \cdot) \times (\mathbb{F}_q^*, \cdot)$. Let subgroups $N_1 := \{1\} \times (\mathbb{F}_q^*, \cdot)$, $N_2 := (\mathbb{F}_q^*, \cdot) \times \{1\}$ and $N_3 := \{ (x, x) : x \in \mathbb{F}_q^* \}$. Then the subset*

$$D := \{ (x, y) : x + y = 1 \}$$

is a $((q-1)^2; q-1, q-1, q-1; q-2, 1; 0, 0, 0)$-GDS relative to N_1, N_2 and N_3. It corresponds to the desarguesian plane $\mathrm{PG}(2, q)$.

GDS from Theorem 1.65 are the only known abelian examples of type (g) in Theorem 1.55 up to equivalence.

Coordinatizing a plane of type (g) yields a planar ternary ring (R, T) with special properties: Let $a \cdot b := T(a, b, 0)$ and $a + b := T(1, a, b)$. Then (R, T) satisfies

- (R, T) is linear, i.e. $T(x, y, z) = x \cdot y + z$ for all $x, y, z \in R$;
- $(R^*, \cdot)$ is a group;
- both distributive laws hold in $(R, +, \cdot)$.

Kantor (1974) called such a planar ternary ring a *neofield*. It should be noted that, in the literature, the term neofield may refer to a slightly different algebraic structure, see Keedwell (2000).

Every neofield coordinatizes a projective plane which is either of Lenz-Barlotti type I.4 (when the neofield is proper, i.e. not a field) or desarguesian. However, no proper neofield is known, and it is widely conjectured that proper neofields do not exist.

The prime power conjecture for this type of planes is still open.

One can also replace $\mathbb{F}_q$ in the above construction by a nearfield to obtain a non-abelian GDS. This is also proved by Hiramine (1999). One may check that the group G is not quasiregular in this case.

Equivalences

Finally, we look at the equivalences among (relative, generalized) difference sets and the isomorphism problem for the corresponding planes. More precisely, when two equivalent (relative, generalized) difference sets are given, it is clear that the projective planes derived from these two difference sets are isomorphic. However, the converse in general is not true. Actually, up to now only few results are known:

(a) When D and D' are two abelian $(n^2+n+1, n+1, 1)$-difference sets, Jungnickel (2008) showed that the planes derived by D and D' are isomorphic if and only if D and D' are equivalent. The proof used a deep theorem due to Ott (1975), see also Müller (1994) and Ho (1998).

(b) Let D and D' be two abelian $(n, n, n, 1)$-RDSs. If n is odd and D is equivalent to D', then the planes derived from D and D' are in general not isomorphic, see Pieper-Seier and Spille (1999) and Theorem 2.9. If n is even and both D and D' are constructed from semifields, then the planes derived from them are isomorphic if and only if D and D' are equivalent, see Theorem 4.14.

1.10 Projections and liftings of difference sets

Let H be a normal subgroup of G, and let φ_H denote the canonical epimorphism (projection) $G \to G/H$ with $\varphi_H(g) = H + g$. We may extend φ_H by linearity to an epimorphism $\mathbb{C}[G] \to \mathbb{C}[G/H]$. Let D be a $(v; n_1, \ldots, n_r; k, \lambda; \lambda_1, \ldots, \lambda_r)$-GDS relative to the subgroups N_i's for $1 \le i \le r$. If $H \le N_i$ for some N_i with $\lambda_i = 0$, then $\varphi_H(D)$ has just 0, 1-coefficients, hence we may interpret $\varphi_H(D)$ as a subset of G/H.

Now we restrict ourselves to the (relative, generalized) difference sets in Theorem 1.55. Group G is quasiregular which means every subgroup is normal. Since (a) in Theorem 1.55 has no non-trivial forbidden subgroup H, we will not consider its projection. First, for relative difference sets, it is not difficult to prove the following lemma.

Lemma 1.66. *Let D be an (m, n, k, λ)-RDS in G relative to N. If $H \subseteq N$ is a subgroup of order t, then $\varphi_H(D)$ is an $(m, n/t, k, t\lambda)$-RDS. In particular, if $t = n$, then $\varphi_H(D)$ is a difference set.* □

Applying Lemma 1.66 on the abelian relative difference sets in Theorem 1.55, we get the following results.

Result 1.67. (b) When $n = p^a$ and p odd, the projections of an $(n, n, n, 1)$-RDS

$$D := \{ (x, f(x)) : x \in \mathbb{F}_{p^a} \}$$

are (p^a, p^b, p^a, p^{a-b})-RDSs. It defines a *vectorial p-ary bent function* when $b > 1$, and a *p-ary bent function* when $b = 1$. Not all (p^a, p^b, p^a, p^{a-b})-RDSs can be obtained from the projections. However, it is generally difficult to show whether a (p^a, p^b, p^a, p^{a-b})-RDS can be embedded in a $(p^a, p^a, p^a, 1)$-RDS.

It is worth noting that p-ary bent functions are studied recently, and various new constructions of them have been given, see for instance the results by Helleseth, Hollmann, Kholosha, Wang, and Xiang (2009), Helleseth and Kholosha (2007, 2010), Çeşmelioğlo, McGuire, and Meidl (2012) and Çeşmelioğlo and Meidl (2012, 2013). For $n = 2^a$, we will give examples of projections in Section 4.4.

(d) Let D be an affine difference set with parameters $(n+1, n-1, n, 1)$ relative to a subgroup N of order $n-1$. We choose a subgroup H of N that has index prime p in N, where $\gcd(n+1, p) = 1$. Then $\varphi_H(D)$ is an $(n+1, p, n, (n-1)/p)$-RDS. Regarding $\varphi_H(D)$ as an element in $\mathbb{C}[G/H]$, we have the group ring equation

$$\varphi_H(D) \cdot \varphi_H(D)^{(-1)} = n + (n-1)/p \cdot (G/H - N/H), \tag{1.15}$$

where N/H is a subgroup of order p. We have $G/H \cong C_{n+1} \times C_p$. Let ξ be a generator of C_p. We apply a homomorphism $C_p \to \mathbb{C}$, which maps ξ to $\zeta_p = e^{\frac{2\pi i}{p}}$, to (1.15). Then the right-hand side of (1.15) becomes n, and the image of $\varphi_H(D)$ is in $\mathbb{C}[C_{n+1}]$, where the coefficient of exactly one element in C_{n+1} is 0, the remaining coefficients are powers of ζ_p. This can be interpreted as an *almost p-ary sequence* $(a_i)_{i=0,1,\ldots,n}$ of period $n+1$ where a_i is a power of ζ_p for all i but one, for which $a_i = 0$. That explains the term "almost". This sequence is perfect in the sense that for all nontrivial autocorrelation coefficients we have $\sum_{i=0}^{n} a_i \bar{a}_{i+t} = 0$ for $t = 1, \ldots, n$. For more details, see the papers by Wolfmann (1992), Pott and Bradley (1995) and Chapter 5. If $p = 2$, we cannot get a sequence out of $\varphi_H(D)$ since G/H does not split as $C_{n+1} \times C_2$.

(e) Note that (e) has only one known example when G is abelian, thus we will skip this type of relative difference sets. □

Similarly for GDSs with two forbidden subgroups, it is also not difficult to prove the following lemma.

Lemma 1.68. *Let D be a $(v;, n_1, n_2; k, \lambda; 0, 0)$ GDS in G relative to N_1 and N_2. If $H \subseteq N_1$ is a subgroup of order m, then $\varphi_H(D)$ is a $(v/m; n_1/m, n_2; k, m\lambda; 0, \lambda(m-1))$ GDS.* □

Applying Lemma 1.66 on (f) in Theorem 1.55, we have the following results.

(f) Let H be a subgroup of the addition group of $\mathbb{F}_q$, where $q = p^a$. We consider the trace function, i.e. $\varphi_H(\mathbb{F}_q) \cong \mathbb{F}_p$. If $f(x) = x$, i.e. if we start with the desarguesian plane, we obtain the set $\{ (x, \mathrm{Tr}(x)) : x \in \mathbb{F}_q^* \}$. This is not a relative difference set, but the sequence $(\mathrm{Tr}(\alpha^t))_t$ is a p-ary m-sequence and has a two-valued autocorrelation spectrum (here α is a primitive element in $\mathbb{F}_q^*$). For background on sequences, we refer the reader to the book by Golomb and Gong (2005). In our language of GDSs, these constructions show that there are several $(p(p^a-1); p, p^a-1; p^a-1, p^{a-1}; 0, p^{a-1}-1)$-GDSs in $C_{p^a-1} \times C_p$, where p is prime. It may be interesting to find vectorial versions, or ask the question which of the known constructions are projections from $(p^b(p^a-1); p^b, p^a-1; p^a-1, p^{a-b}; 0, p^{a-b}-1)$-GDSs. An example is due to Gordon, Mills, and Welch (1962). Let $\mathbb{F}_{q'}$ be a subfield of $\mathbb{F}_q$ where $q = p^a$ and $q' = p^b$. Then the sets

$$D_r := \{ (x, (\mathrm{Tr}_{q/q'}(x))^r) : x \in \mathbb{F}_q^* \} \subseteq (\mathbb{F}_q^*, \cdot) \times (\mathbb{F}_{q'}, +)$$

are $(p^b(p^a-1); p^b, p^a-1; p^a-1, p^{a-b}; 0, p^{a-b}-1)$-GDSs.

Note that D_r describes a vectorial function $f : \mathbb{F}_q^* \to \mathbb{F}_p^b$. Let α be a primitive element of $\mathbb{F}_q^*$. The component functions $\mathrm{Tr}(\beta \cdot f(\alpha^t))_{t=0,\ldots,q-2}$ give rise to p-ary sequences $(\zeta_p^{\mathrm{Tr}(\beta \cdot f(\alpha^t))})_t$, where $\zeta_p = e^{\frac{2\pi i}{p}}$ is a p-th root of unity in $\mathbb{C}$. These sequences are the well known Gordon-Mills-Welch sequences whose nontrivial autocorrelations are all -1. We have stated the Gordon-Mills-Welch construction in a "vectorial" form. The construction actually gives a b-dimensional vector space of functions with autocorrelation -1.

When q is a prime, the additive group of $\mathbb{F}_q$ is also cyclic. Thus we can also project the multiplication group of $\mathbb{F}_q$. See the details in Result 5.22.

When D is a GDS relative to more than 2 subgroups, the situation is more involved since $\varphi_H(N_i)$ and $\varphi_H(N_j)$ with $i > j \geq 2$ may have a nontrivial intersection, when we project D onto G/H with $H \subseteq N_1$. This is the reason why we skip the last type of GDS in Theorem 1.55.

Let us go back to (b). We have seen that we can always get a p-ary bent function from a planar function for odd prime p. But there are many p-ary bent functions which may not be derived from a planar function. The question is: which p-ary bent function can be embedded in a (p^a, p^b, p^a, p^{a-b})-RDS? We may formulate this problem in a general way.

Problem 1.1 (Lifting problem)**.** Assume that R is a subset of a group G' such that $RR^{-1} = \varphi_H(DD^{-1})$ for some $D \subseteq G$, where $G' = \varphi_H(G)$. Is it possible to choose D such that $\varphi_H(D) = R$?

Problem 1.1 is generally difficult to answer. In Section 3.2, we will consider the case that R is a $(q, q, q, 1)$-RDS, where q is an odd prime power.

1.11 CCZ and EA equivalences

It is in general a difficult problem to investigate the isotopism between commutative semifields, or equivalently the isomorphism between commutative semifield planes. A more feasible strategy is to look at the equivalence of the corresponding $(q, q, q, 1)$-RDSs (planar functions) first. Let $q = p^n$, where p is an odd prime. Since every $(q, q, q, 1)$-RDS in C_p^{2n} can always be described by $D = \{ (x, f(x)) : x \in \mathbb{F}_{p^n} \} \subseteq (\mathbb{F}_{p^n}, +) \times (\mathbb{F}_{p^n}, +)$, the automorphism group of D is isomorphic to a subgroup of $\mathrm{GL}(2n, p)$.

A function from a finite field $\mathbb{F}_{p^n}$ to itself is *affine*, if it is defined by the sum of a constant and a linearized polynomial over $\mathbb{F}_{p^n}$. There are several equivalence relations of functions under which the planar property is invariant:

Definition 1.69. Let p be a prime (not necessarily odd). Two functions f and $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are called

- *extended affine equivalent* (EA-equivalent), if $g = l_1 \circ f \circ l_2 + l_3$, where l_1, l_2 and l_3 are affine functions, and where l_1, l_2 are permutations of $\mathbb{F}_{p^n}$. Furthermore, if l_3 is the zero mapping, then f and g are called *affine equivalent*; if l_1 and l_2 are both linearized, and l_3 is the zero mapping, then f and g are called *linearly equivalent*;

- *Carlet-Charpin-Zinoviev equivalent* (abbreviated to CCZ-equivalent or graph equivalent, which was introduced by Carlet, Charpin, and Zinoviev (1998)), if there is a certain affine permutation L of $\mathbb{F}_{p^n}^2$, such that $L(D_f) = D_g$, where $D_f = \{ (x, f(x)) : x \in \mathbb{F}_{p^n}) \}$ and $D_g = \{ (x, g(x)) : x \in \mathbb{F}_{p^n}) \}$.

Generally speaking, EA-equivalence implies CCZ-equivalence, but not vice versa, see counterexamples from APN functions found by Budaghyan, Carlet, and Pott (2006). However, for some special cases, they are the same. For instance, if planar functions f and g are CCZ-equivalent, then they are also EA-equivalent. This result was proved by Budaghyan and Helleseth (2008) as well as Kyureghyan and Pott (2008), independently.

Now let $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be two planar functions. By comparing the definitions of CCZ-equivalence and equivalence of RDSs, we can actually see that f is CCZ-equivalent to g if and only if $D_f := \{ (x, f(x)) : x \in \mathbb{F}_{p^n} \}$ is equivalent to $D_g := \{ (x, g(x)) : x \in \mathbb{F}_{p^n} \}$. Together with the results by Budaghyan and Helleseth (2008) or Kyureghyan and Pott (2008), we have that D_f is equivalent to D_g if and only if f is EA-equivalent to g. Moreover, those affine terms and l_3 in EA-equivalence can be removed when some conditions are provided (see also Budaghyan and Helleseth (2008, Corollary 3)):

Theorem 1.70. *Let f and g be both planar DO polynomials in $\mathbb{F}_{p^n}[x]$, where p is an odd prime. Let $\mathbb{P}_f$ (resp. $\mathbb{P}_g$) denote the (pre)semifield $(\mathbb{F}_{p^n}, +, *_f)$ (resp. $(\mathbb{F}_{p^n}, +, *_g)$), where the multiplication is defined by* (1.12)*, i.e. $x *_f y := (f(x+y) - f(x) - f(y))/2$*

(resp. $x *_g y := (g(x+y) - g(x) - g(y))/2$*). Then the following statements are equivalent:*

(a) f *and* g *are CCZ-equivalent;*

(b) f *and* g *are EA-equivalent;*

(c) f *and* g *are linearly equivalent;*

(d) $\mathbb{P}_f$ *and* $\mathbb{P}_g$ *are strongly isotopic.*

Proof. The equivalence of the first two statements was proved by Budaghyan and Helleseth (2008) and Kyureghyan and Pott (2008).

Since linear equivalence is a special case of EA-equivalence, we only need to prove the contrary statement (b) $\Rightarrow$ (c). Now assume that f and g are EA-equivalent, i.e. there is affine functions l_1, l_2 and l_3 such that

$$g = l_1 \circ f \circ l_2 + l_3, \tag{1.16}$$

where l_1 and l_2 are both permutations. Let $l_i(x) = \bar{l}_i(x) + a_i$, where $\bar{l}_i(0) = 0$ for $i = 1, 2$. Note that $f(x) = x *_f x$, hence we can write the right-hand side of (1.16) as:

$$\begin{aligned} & l_1 \circ f(\bar{l}_2(x) + a_2) + l_3 \\ =& l_1\left(\bar{l}_2(x) *_f \bar{l}_2(x) + 2\bar{l}_2(x) *_f a_2 + a_2 *_f a_2\right) + l_3 \\ =& \bar{l}_1\left(\bar{l}_2(x) *_f \bar{l}_2(x)\right) + 2\bar{l}_1\left(\bar{l}_2(x) *_f a_2\right) + \bar{l}_1(a_2 *_f a_2) + a_1 + l_3. \end{aligned}$$

Since every term in $\bar{l}_2(x) *_f \bar{l}_2(x)$ is of the form $x^{p^i+p^j}$, $\bar{l}_1(\bar{l}_2(x) *_f \bar{l}_2(x))$ is also a DO polynomial, and the rest part of the equation above is affine. However, as the left-hand side of (1.16) is a DO polynomial, we have

$$g(x) = \bar{l}_1\left(\bar{l}_2(x) *_f \bar{l}_2(x)\right) = \bar{l}_1 \circ f \circ \bar{l}_2(x),$$

which means that f and g are linearly equivalent.

Finally, we prove the equivalence between the last two statements (c) and (d). By definition, when $\mathbb{P}_f$ and $\mathbb{P}_g$ are strongly isotopic, there are linear bijections N and $L : \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that $N(x) *_f N(y) = L(x *_g y)$. Hence $N(x) *_f N(x) = L(x *_g x)$, i.e.

$$L^{-1}(f(N(x))) = g(x),$$

where N and L^{-1} can be both viewed as linearized polynomials. It follows that f and g are linearly equivalent.

When f and g are linearly equivalent, i.e. there are linearized permutation polynomials l_1 and l_2 such that $g(x) = l_1 \circ f \circ l_2(x)$, then

$$l_1^{-1}(x *_g x) = l_2(x) *_f l_2(x).$$

It follows that

$$\begin{aligned} l_1^{-1}(x *_g y) &= l_1^{-1}\left(\frac{1}{2}((x+y) *_g (x+y) - x *_g x - y *_g y)\right) \\ &= \frac{1}{2}\left(l_1^{-1}((x+y) *_g (x+y)) - l_1^{-1}(x *_g x) - l_1^{-1}(y *_g y)\right) \\ &= \frac{1}{2}(l_2(x+y) *_f l_2(x+y) - l_2(x) *_f l_2(x) - l_2(y) *_f l_2(y)) \\ &= l_2(x) *_f l_2(y), \end{aligned}$$

which means that $\mathbb{P}_f$ and $\mathbb{P}_g$ are strongly isotopic. □

As all these three type of equivalences of planar DO polynomials are essentially the same, we will just call them directly the *equivalence* of planar DO polynomials. Theorem 1.70 will be used in Chapter 2 to determine the isomorphism of some new commutative semifields.

Chapter 2

A new family of semifields with two parameters

Ich pflanzt es wieder
Am kühlen Ort;
Nun zweigt und blüht es
Mir immer fort.

J.W. von Goethe, *Gefunden*

In this chapter, we focus on $(q, q, q, 1)$-RDS in C_p^{2n} relative to C_p^n where $q = p^n$ and p is an odd prime. They can be expressed as a planar function $f : \mathbb{F}_q \to \mathbb{F}_q$, as we explained in Proposition 1.20. Most planar functions come from commutative semifields, and these planar functions can also be written as a Dembowski-Ostrom (abbreviated to DO) polynomials. The unique known exception is the Coulter-Matthews planar function defined by (1.14). For the list of known commutative semifields we refer to Section 1.8.

In Section 2.1, we introduce a family of commutative semifields with two parameters. Then we determine their left, middle and right nuclei in Section 2.2. The isotopisms between different members of this family are discussed in Section 2.3. After that, in Section 2.4 we show that this family of commutative semifields is new, i.e. it contains some members which do not belong to other known semifield families. At the end, we consider APN functions of a similar form.

This chapter is based on the paper by Zhou and Pott (2013).

2.1 A family of commutative semifields

We need the following lemma which can be proved by using elementary number theory.

Lemma 2.1. *Let $v(b)$ denote the maximal power of 2 dividing integer b. For an odd prime p,*

- $\gcd(p^j-1, p^i-1) = p^{\gcd(j,i)}-1$ *and*
- $\gcd(p^j+1, p^i-1) = \begin{cases} p^{\gcd(j,i)}+1, & \text{if } \nu(j) < \nu(i); \\ 2, & \text{otherwise.} \end{cases}$

Proof. Let $d := \gcd(i,j)$. As $(p^d-1) \mid (p^j-1)$ and $(p^d-1) \mid (p^i-1)$, we have $(p^d-1) \mid \gcd(p^j-1, p^i-1)$.

On the other hand, for any positive integers u, v satisfying $ui - vj \geq 0$, there are $(p^i-1) \mid (p^{ui}-1)$, $(p^j-1) \mid (p^{vj}-1)$ and

$$(p^{ui}-1) - (p^{vj}-1) = (p^{ui-vj}-1)p^{vj},$$

which mean that $\gcd(p^j-1, p^i-1) \mid (p^{ui-vj}-1)$. Hence $\gcd(p^j-1, p^i-1) \mid p^d-1$ and the first claim follows.

Now we know that $\gcd(p^{2j}-1, p^i-1) = p^{\gcd(2j,i)}-1$. It follows that

$$\begin{aligned} \gcd(p^{2j}-1, p^i-1) =& \gcd(p^j-1, p^i-1)\gcd\left(p^j+1, \frac{p^i-1}{\gcd(p^j-1, p^i-1)}\right) \\ =& (p^d-1)\gcd\left(p^j+1, \frac{p^i-1}{p^d-1}\right) \\ =& (p^d-1)\frac{\gcd\left(p^j+1, p^i-1\right)\gcd\left(p^j+1, p^d-1, \frac{p^i-1}{p^d-1}\right)}{\gcd(p^j+1, p^d-1)}. \end{aligned}$$

Noting that $2 \mid \gcd(p^j+1, p^d-1)$ and $\gcd(p^j+1, p^d-1) \mid \gcd(p^j+1, p^j-1) = 2$, we have $\gcd(p^j+1, p^d-1) = 2$. Together with

$$(p^i-1)/(p^d-1) = p^{(i/d-1)d} + \cdots + p^d + 1 \equiv \begin{cases} 0 \pmod 2, & \text{if } \nu(j) < \nu(i); \\ 1 \pmod 2, & \text{otherwise.} \end{cases}$$

we have

$$\gcd(p^{2j}-1, p^i-1) = \begin{cases} (p^d-1)\gcd(p^j+1, p^i-1), & \text{if } \nu(j) < \nu(i); \\ \frac{p^d-1}{2}\gcd(p^j+1, p^i-1), & \text{otherwise.} \end{cases}$$

On the other hand, it is readily verified that

$$\gcd(2j, i) = \begin{cases} 2d, & \text{if } \nu(j) < \nu(i); \\ d, & \text{if otherwise.} \end{cases}$$

Therefore, the second claim in the lemma follows. □

Before introducing our new construction of semifields, let us look at a type of (pre)semifields which were discovered by Albert (1961a).

Definition 2.2. Let $q = p^m$ and let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$, $a \in \mathbb{F}_q$ be such that the equation $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Then

$$x * y := xy - ax^{\sigma}y^{\tau}$$

defines a presemifield $(\mathbb{F}_q, +, *)$. A corresponding semifield is called a *generalized twisted field* or *Albert's twisted field* if $\sigma \neq \tau$, $\sigma \neq 1$ and $\tau \neq 1$.

Remark 2.3. Generally speaking, Albert's twisted fields are not isotopic to commutative semifields. Note that when $a = -1$ and $x^{\sigma} = x^{\tau^{-1}} = x^{p^k}$ for all $x \in \mathbb{F}_q$, then $-1 = x^{p^k-1}y^{1-p^k}$ has no solution if and only if there is no integer u satisfying $(p^m-1)/2 = u \cdot \gcd(p^k-1, p^m-1)$, which is equivalent to $(p^m-1)/\gcd(p^k-1, p^m-1)$ being odd. By Lemma 2.1, this condition can also be written as $m/\gcd(m,k)$ is odd. Now we have that

$$x * y = xy + x^{p^k}y^{-p^k},$$

in which replacing y by y^{p^k}, we get

$$x \circ_k y := x^{p^k}y + xy^{p^k}. \tag{2.1}$$

It follows that $(\mathbb{F}_q, +, *)$ is isotopic to a commutative presemifield $(\mathbb{F}_q, +, \circ_k)$.

Cohen and Ganley (1982) made significant progress in the investigation of commutative semifields of rank 2 over their middle nucleus. Here "rank 2" means that if the size of semifield is p^{2m}, then its middle nucleus is of size p^m. Let $a, b, c, d \in \mathbb{F}_{p^m}$, $n = 2m$. Cohen and Ganley defined a binary mapping $*$ from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ as follows:

$$(a,b) * (c,d) = (ac + \varphi_1(bd), ad + bc + \varphi_2(bd)), \tag{2.2}$$

where φ_1 and φ_2 are linearized polynomials. They considered under which condition $*$ defines the multiplication of a semifield. Some necessary and sufficient conditions were derived, see the papers by Cohen and Ganley (1982) and Ball and Lavrauw (2002) for details. Finite fields, Dickson's semifields, the Cohen-Ganley semifields and the Penttila-Williams semifield are all of this form.

Observe that the multiplication of $\mathbb{F}_{p^m}$ is used in the multiplication $*$ defined by (2.2), which is basically a linear combination of ac, ad, bc and $(bd)^{p^i}$ for $i = 0, \ldots, m-1$. Hence, one natural question arises: Is it possible to construct some semifields or presemifields, if we replace some of these finite field multiplications by semifield or presemifield multiplications? As the multiplication of Albert's commutative twisted fields, which is defined in Remark 2.3, is of a comparatively simple form, we take it as our first candidate.

Theorem 2.4. *Let p be an odd prime, and 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 binary operation $*$ as follows:*

$$(a,b) * (c,d) = (a \circ_k c + \alpha (b \circ_k d)^\sigma, ad + bc), \tag{2.3}$$

where α is a non-square element in $\mathbb{F}_{p^m}$ and σ is a field automorphism of $\mathbb{F}_{p^m}$. Then, $(\mathbb{F}_{p^{2m}}, +, *)$ is a presemifield, which we denote by $\mathbb{P}_{k,\sigma}$.

Proof. It is routine to check the distributive law in $\mathbb{P}_{k,\sigma}$. Hence, to prove $\mathbb{P}_{k,\sigma}$ is a presemifield, we only need to prove that

$$(a,b) * (c,d) = 0 \text{ if and only if } a = b = 0 \text{ or } c = d = 0.$$

Assume that $(a,b) * (c,d) = 0$, then we have

$$\begin{aligned} a \circ_k c + \alpha (b \circ_k d)^\sigma &= 0\,, \\ ad + bc &= 0\,. \end{aligned} \tag{2.4}$$

When $d = 0$, we have $a \circ_k c = 0$ and $bc = 0$, which means $c = 0$ or $a = b = 0$ since $\circ_k$ is Albert's presemifield multiplication on $\mathbb{F}_{p^m}$.

When $d \neq 0$, we have $a = -\frac{bc}{d}$. If $b = 0$, then $a = 0$. If $b \neq 0$, then eliminating a in (2.4), we have

$$\alpha (b^{p^k} d + d^{p^k} b)^\sigma = c^{p^k+1} \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right),$$

which means that

$$\alpha \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right)^\sigma (d^{p^k+1})^\sigma = c^{p^k+1} \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right).$$

Thus,

$$\alpha = (c^{p^k+1} (d^{-\sigma})^{p^k+1}) \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right)^{1-\sigma}.$$

However, the equation cannot hold, since α is a non-square in $\mathbb{F}_{p^m}$. Therefore, we get $a = b = 0$. □

2.2 Left and middle nuclei

To analyze the properties of $\mathbb{P}_{k,\sigma}$, we need the following results, which follows from Lemma 2.1.

Lemma 2.5. *Let p be an odd prime, and let m, k be positive integers, such that $\frac{m}{\gcd(m,k)}$ is odd. Then*

(a) $\gcd(p^m-1, p^k+1) = 2$, *which means that* x^{p^k+1} *is a 2-1 mapping on* $\mathbb{F}_{p^m}^*$;

(b) mapping $x \mapsto x^{p^k} + x$ *is a permutation on* $\mathbb{F}_{p^m}$. □

It is not difficult to see that different non-square α's generate isotopic semifields, because for any nonzero β,

$$\begin{aligned}(a, \beta b) * (c, \beta d) =& (a \circ_k c + \alpha(\beta b \circ_k \beta d)^\sigma, a(\beta d) + c(\beta b)) \\ =& (a \circ_k c + \alpha\beta^{(p^k+1)\sigma}(b \circ_k d)^\sigma, \beta(ad + bc)),\end{aligned}$$

the set $\{\alpha\beta^{(p^k+1)\sigma} : \beta \in \mathbb{F}_{p^m}^*\}$ are all the non-squares in $\mathbb{F}_{p^m}$ by Lemma 2.5 and $(x, \beta y) \mapsto (x, y)$ is a linear bijection on $(\mathbb{F}_{p^m}, +) \times (\mathbb{F}_{p^m}, +)$. Hence, in the remaining part we may assume that the non-square α is an element of $\mathbb{F}_{p^k} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^l}$, where $l = \gcd(k, m)$. Furthermore, by (1.11) a planar function that corresponds to $\mathbb{P}_{k,\sigma}$ is

$$(x, y) \mapsto (2x^{p^k+1} + 2\alpha(y^{p^k+1})^\sigma, 2xy).$$

Dividing by 2, we have

$$(x, y) \mapsto (x^{p^k+1} + \alpha(y^{p^k+1})^\sigma, xy).$$

If there exists some u such that $p^k + 1 \equiv p^u(p^s + 1) \pmod{p^m - 1}$, then $\mathbb{P}_{k,\sigma}$ is isotopic to $\mathbb{P}_{s,\sigma}$, since

$$(x, y) \mapsto (x^{p^k+1} + \alpha(y^{p^k+1})^\sigma, xy)$$

is equivalent to

$$(x, y) \mapsto ((x^{p^u})^{p^s+1} + \alpha((y^{p^u})^{p^s+1})^\sigma, (x^{p^u} y^{p^u})^{p^{-u}}),$$

which is also equivalent to

$$(x, y) \mapsto (x^{p^s+1} + \alpha(y^{p^s+1})^\sigma, xy).$$

Similarly, $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{k,\sigma^{-1}}$ are also isotopic, because

$$(x, y) \mapsto (x^{p^k+1} + \alpha(y^{p^k+1})^{\sigma^{-1}}, xy)$$

is equivalent to

$$(x, y) \mapsto (y^{p^k+1} + (\alpha^{-1}x^{p^k+1})^\sigma, xy),$$

i.e.

$$(x, y) \mapsto (y^{p^k+1} + \alpha^{-\sigma}(x^{p^k+1})^\sigma, yx).$$

Hence, in the rest of this chapter, we always concentrate on the cases with $0 \le k, r \le \lfloor \frac{m}{2} \rfloor$, where $\sigma(x) = x^{p^r}$.

To get a semifield $\mathbb{S}_{k,\sigma}$ from our presemifield, we use (1.10) to define the multiplication $\star$ of $\mathbb{S}_{k,\sigma}$:

$$(a,b)\star(c,d) := B^{-1}((a,b)*(c,d)), \tag{2.5}$$

where

$$B(a,b) := (a,b)*(1,0) = (a+a^{p^k},b), \tag{2.6}$$

which is a linearized mapping and a permutation on $\mathbb{F}_{p^{2m}}$ by Lemma 2.5. For convenience, when σ is the identity mapping on $\mathbb{F}_{p^m}$, we use $\mathbb{P}_k$ and $\mathbb{S}_k$ to denote our presemifield and semifield, respectively.

Let y be an element in the middle nucleus of $\mathbb{S}_{k,\sigma}$. Then for any $x,z\in\mathbb{F}_{p^{2m}}$ we have

$$(x\star y)\star z = x\star(y\star z),$$

which can be written as

$$B^{-1}(B^{-1}(x*y)*z) = B^{-1}(x*B^{-1}(y*z)).$$

Hence $y\in N_m(\mathbb{S}_{k,\sigma})$ if and only if

$$B^{-1}(x*y)*z = x*B^{-1}(y*z). \tag{2.7}$$

Now we can precisely determine the middle nucleus of $\mathbb{S}_{k,\sigma}$:

Theorem 2.6. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined on $\mathbb{F}_{p^{2m}}$ as in* (2.5) *with $\alpha\in\mathbb{F}_{p^l}^*$, where $l=\gcd(m,k)$.*

(a) If $\sigma=\mathrm{id}$, then the middle nucleus $N_m(\mathbb{S}_k)$ is isomorphic to $\mathbb{F}_{p^{2l}}$.

(b) If $\sigma\neq\mathrm{id}$, then the middle nucleus $N_m(\mathbb{S}_{k,\sigma})$ is isomorphic to $\mathbb{F}_{p^l}$.

Proof. Let $c,d\in\mathbb{F}_{p^m}$, such that $(c,d)\in N_m(\mathbb{S}_{k,\sigma})$. Then (2.7) becomes

$$B^{-1}((a,b)*(c,d))*(e,f) = (a,b)*B^{-1}((c,d)*(e,f)), \tag{2.8}$$

for any $(a,b),(e,f)\in\mathbb{F}_{p^m}^2$. For given $a,b\in\mathbb{F}_{p^m}$, there is a unique $u\in\mathbb{F}_{p^m}$ such that

$$u+u^{p^k} = a\circ_k c+\alpha(b\circ_k d)^\sigma, \tag{2.9}$$

since $x^{p^k}+x$ is a permutation on $\mathbb{F}_{p^m}$. We obtain

$$\begin{aligned}
&B^{-1}((a,b)*(c,d))*(e,f)\\
=&B^{-1}(a\circ_k c+\alpha(b\circ_k d)^\sigma, ad+bc)*(e,f)\\
=&B^{-1}(u+u^{p^k},ad+bc)*(e,f)\\
=&(u,ad+bc)*(e,f)\qquad\text{(using the definition of } B)\\
=&(u\circ_k e+\alpha(f\circ_k(ad+bc))^\sigma, uf+(ad+bc)e).
\end{aligned}\tag{2.10}$$

Similarly, for given $e, f \in \mathbb{F}_{p^m}$ we define v by

$$v + v^{p^k} = c \circ_k e + \alpha(d \circ_k f)^\sigma, \tag{2.11}$$

and the right-hand side of (2.8) is

$$\begin{aligned}&(a,b) * B^{-1}((c,d) * (e,f))\\ =&(a \circ_k v + \alpha(b \circ_k (cf + de))^\sigma, vb + a(cf + de)).\end{aligned} \tag{2.12}$$

By comparing the second component of the two sides of (2.8), we have

$$uf + bce = vb + acf.$$

For $f = 0$ but $b \neq 0$, we have $ceb = vb$, which means that $v = ce$. Eliminating v in (2.11), we have

$$ce + (ce)^{p^k} = c^{p^k} e + ce^{p^k},$$

for any $e \in \mathbb{F}_{p^m}$. That means $c = c^{p^k}$, hence,

$$c \in \mathbb{F}_{p^l}. \tag{2.13}$$

Furthermore, for $f \neq 0$, we have

$$u + \frac{bce}{f} = \frac{bv}{f} + ac.$$

It follows that

$$u + u^{p^k} + \frac{bce}{f} + \left(\frac{bce}{f}\right)^{p^k} = \frac{bv}{f} + \left(\frac{bv}{f}\right)^{p^k} + ac + (ac)^{p^k}. \tag{2.14}$$

By eliminating u using (2.9), the left-hand side of (2.14) becomes

$$(a^{p^k} + a)c + \alpha(b^{p^k} d + bd^{p^k})^\sigma + c\left(\frac{be}{f} + \left(\frac{be}{f}\right)^{p^k}\right).$$

Similarly, by (2.11), the right-hand side of (2.14) becomes

$$\begin{aligned}&\frac{bv}{f} + \left(\frac{b}{f}\right)^{p^k} (c \circ_k e + \alpha(d \circ_k f)^\sigma - v) + ac + (ac)^{p^k}\\ =&\frac{bv}{f} + \left(\frac{b}{f}\right)^{p^k} (c(e + e^{p^k}) + \alpha(d \circ_k f)^\sigma - v) + c(a + a^{p^k}).\end{aligned}$$

By canceling the same terms on both sides of (2.14), we have

$$\alpha\left((b \circ_k d)^\sigma - (d \circ_k f)^\sigma \left(\frac{b}{f}\right)^{p^k}\right) + \left(\frac{b}{f} - \left(\frac{b}{f}\right)^{p^k}\right)(ce - v) = 0. \tag{2.15}$$

If σ is the identity mapping, then (2.15) becomes

$$\alpha\left(b^{p^k}d+bd^{p^k}-(d^{p^k}f+df^{p^k})\left(\frac{b}{f}\right)^{p^k}\right)+\left(\frac{b}{f}-\left(\frac{b}{f}\right)^{p^k}\right)(ce-v)=0,$$

which can be simplified as

$$\left(\frac{b}{f}-\left(\frac{b}{f}\right)^{p^k}\right)(\alpha fd^{p^k}+ce-v)=0.$$

Since the equation above holds for any b and $f\neq 0$, we have $v=\alpha fd^{p^k}+ce$ which means that

$$v+v^{p^k}=(e^{p^k}+e)c+\alpha(f^{p^k}d^{p^{2k}}+fd^{p^k}),$$

since $\alpha\in\mathbb{F}_{p^l}=\mathbb{F}_{p^k}\cap\mathbb{F}_{p^m}$. Together with (2.11), we have

$$df^{p^k}+fd^{p^k}=f^{p^k}d^{p^{2k}}+fd^{p^k},$$

for any $f\neq 0$, which means that $d=d^{p^k}$. Therefore, if $(c,d)\in N_m(\mathbb{S}_k)$, then $c,d\in\mathbb{F}_{p^k}\cap\mathbb{F}_{p^m}(=\mathbb{F}_{p^l})$. Since the middle nucleus of a finite semifield is isomorphic to a finite field, $N_m(\mathbb{S}_k)$ is isomorphic to a subfield of $\mathbb{F}_{p^{2l}}$. Conversely, for $c,d\in\mathbb{F}_{p^l}$

$$\begin{aligned}
&B^{-1}((a,b)*(c,d))*(e,f)\\
=&B^{-1}\left((a^{p^k}+a)c+\alpha(b^{p^k}+b)d,ad+bc\right)*(e,f)\\
=&(ac+\alpha bd,ad+bc)*(e,f)\\
=&((ac)\circ_k e+(\alpha bd)\circ_k e+\alpha(ad+bc)\circ_k f,(ac+\alpha bd)f+(ad+bc)e)\\
=&(ca\circ_k e+\alpha d(b\circ_k e)+\alpha d(a\circ_k f)+\alpha c(b\circ_k f),acf+\alpha bdf+ade+bce),
\end{aligned}$$

which equals $(a,b)*B^{-1}((c,d)*(e,f))$ by symmetry. Therefore we proved the first claim.

If σ is not trivial, then it follow that $(c,0)\in N_m(\mathbb{S}_{k,\sigma})$, for $c\in\mathbb{F}_{p^l}$, because

$$\begin{aligned}
&B^{-1}((a,b)*(c,0))*(e,f)\\
=&B^{-1}\left((a^{p^k}+a)c,bc\right)*(e,f)\\
=&(ac,bc)*(e,f)\\
=&((ac)\circ_k e+\alpha((bc)\circ_k f)^{\sigma},acf+bce)\\
=&(c(a\circ_k e)+\alpha c^{\sigma}(b\circ_k f)^{\sigma},acf+bce)\\
=&(a,b)*B^{-1}((c,0)*(e,f)).
\end{aligned}$$

Thus $\mathbb{F}_{p^l}$ is a subfield of $N_m(\mathbb{S}_{k,\sigma})$.

Next, we prove that $d = 0$ if $(c, d) \in N_m(\mathbb{S}_{k,\sigma})$. We separate this proof into two steps, first let us prove that $d \in \mathbb{F}_{p^l}$. Let $(c, d) \in N_m(\mathbb{S}_{k,\sigma})$, which means that $c \in \mathbb{F}_{p^l}$, because (2.13) holds without any assumption on σ. It follows that

$$(c, d) \star (c, d) = B^{-1}((c, d) * (c, d)) = B^{-1}(2c^2 + 2\alpha d^{\sigma(p^k+1)}, 2cd).$$

Notice that the middle nucleus is a finite field in the semifield, hence the first component of $B^{-1}(2c^2 + 2\alpha d^{\sigma(p^k+1)}, 2cd)$ is in $\mathbb{F}_{p^l}$. As $x + x^{p^k} = 2x$ for any $x \in \mathbb{F}_{p^l}$, we have

$$B^{-1}(2c^2 + 2\alpha d^{\sigma(p^k+1)}, 2cd) = (c^2 + \alpha d^{\sigma(p^k+1)}, 2cd).$$

Thus $c^2 + \alpha d^{\sigma(p^k+1)} \in \mathbb{F}_{p^l}$, which means that $d^{p^k+1} \in \mathbb{F}_{p^l}$. Since $l = \gcd(m, k)$, we have $d^{p^k+1} = d^{p^{2k}+p^k}$, hence $d \in \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^l}$. This shows that $N_m(\mathbb{S}_{k,\sigma})$ is isomorphic to a subfield of $\mathbb{F}_{p^{2l}}$.

Now we are going to show that d must be 0. As α, c and $d \in \mathbb{F}_{p^l}$, we have

$$\begin{aligned}
&B^{-1}((a, b) * (c, d)) * (e, f)\\
=&B^{-1}\left((a^{p^k} + a)c + \alpha((b^{p^k} + b)d)^\sigma, ad + bc\right) * (e, f)\\
=&(ac + \alpha(bd)^\sigma, ad + bc) * (e, f)\\
=&((ac) \circ_k e + (\alpha(bd)^\sigma) \circ_k e + \alpha((ad + bc) \circ_k f)^\sigma, (ac + \alpha(bd)^\sigma)f + (ad + bc)e)\\
=&(ca \circ_k e + \alpha d^\sigma(b^\sigma \circ_k e) + \alpha d^\sigma(a \circ_k f)^\sigma + \alpha c^\sigma(b \circ_k f)^\sigma, acf + \alpha(bd)^\sigma f + ade + bce).
\end{aligned}$$

By symmetry, the second component of $(a, b) * B^{-1}((c, d) * (e, f))$ is

$$acf + \alpha(fd)^\sigma b + ade + bce,$$

which equals to $acf + \alpha(bd)^\sigma f + ade + bce$ if $(c, d) \in N_m(\mathbb{S}_{k,\sigma})$. That means $d^\sigma(b^\sigma f - bf^\sigma) = 0$ for any b and $f \in \mathbb{F}_{p^m}$, which holds if and only if $d = 0$. Therefore, we proved the second claim. □

Noticing that $N_l(\mathbb{S}_{k,\sigma}) = N_r(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma})$, since $\mathbb{S}_{k,\sigma}$ is commutative, the center $N(\mathbb{S}_{k,\sigma})$ of $\mathbb{S}_{k,\sigma}$ can also be derived:

Theorem 2.7. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined as in* (2.5) *on $\mathbb{F}_{p^{2m}}$ with $\alpha \in \mathbb{F}_{p^l}^*$, where $l = \gcd(m, k)$. Then its (left, right) nucleus $N(\mathbb{S}_{k,\sigma})$ is isomorphic to $\mathbb{F}_{p^h}$, where $x^\sigma = x^{p^s}$ and $h = \gcd(m, k, s)$.*

Proof. By using the same notations as in the proof of Theorem 2.6, assume that (a, b) is an element in $N(\mathbb{S}_{k,\sigma})$. Since $N(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma})$, by Theorem 2.6, we have $a \in \mathbb{F}_{p^l} = \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m}$ and $b = 0$ when $\sigma \neq \mathrm{id}$. Moreover, by (2.10) and (2.12), we have

$$B^{-1}((a, b) * (c, d)) * (e, f) = (u \circ_k e + \alpha(f \circ_k (ad))^\sigma, uf + ade),$$

and

$$(a,b) * B^{-1}((c,d) * (e,f)) = (a \circ_k v, a(cf + de)).$$

Since $u + u^{p^k} = a \circ_k c + \alpha(0 \circ_k d)^\sigma = a(c + c^{p^k})$, we have $u = ac$,

$$B^{-1}((a,b) * (c,d)) * (e,f) = (a(c \circ_k e) + \alpha a^\sigma (f \circ_k d)^\sigma, acf + ade),$$

and

$$(a,b) * B^{-1}((c,d) * (e,f)) = (a(v + v^{p^k}), a(cf + de)).$$

By the definition of v in (2.11), it follows that:

$$B^{-1}((a,b) * (c,d)) * (e,f) = (a,b) * B^{-1}((c,d) * (e,f)) \text{ if and only if } a^\sigma = a.$$

Since $N(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma})$, when σ is non-trivial, from Theorem 2.6 (b), we know that $N_m(\mathbb{S}_{k,\sigma}) = \{ (a,0) : a \in \mathbb{F}_{p^l}, l = \gcd(m,k) \}$. Therefore, we have $N(\mathbb{S}_{k,\sigma}) \cong \mathbb{F}_{p^h}$.

When σ is the identity mapping, let $(a,b) \in N(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma}) \cong \mathbb{F}_{p^{2l}}$. We want to show that b must be 0. Now assume that $b \neq 0$ and $d = f = 0$. By comparing the second components of (2.10) and (2.12), we have $vb = ceb$, which means that

$$v + v^{p^k} = ce + c^{p^k} e^{p^k}.$$

However, by (2.11), we have

$$v + v^{p^k} = c \circ_k e.$$

Hence,

$$(c - c^{p^k})(e - e^{p^k}) = 0,$$

which cannot hold for $c, e \in \mathbb{F}_{p^m} \setminus \mathbb{F}_{p^k}$. Therefore, $b = 0$.

Finally it is routine to show that $(a,0) \in N(\mathbb{S}_{k,\sigma})$ for any $a \in \mathbb{F}_{p^l}$. Therefore we have $N(\mathbb{S}_{k,\sigma}) \cong \mathbb{F}_{p^l}$ and $l = h = \gcd(m,k,0)$. □

Remark 2.8. If we let $k = 0$, then $\mathbb{S}_{k,\sigma}$ is a Dickson's semifield. In other words, Theorem 2.6 and Theorem 2.7 also hold for Dickson's semifields.

2.3 The isotopism between $\mathbb{S}_{k,\sigma}$

It is natural to ask, whether (2.3) defines isotopic presemifields for the same m but different k and σ. As we mentioned after Lemma 2.1, if there exists some u such that $p^k + 1 \equiv p^u(p^s + 1) \pmod{p^m}$, then $\mathbb{P}_{k,\sigma}$ is isotopic to $\mathbb{P}_{s,\sigma}$; similarly, $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{k,\sigma^{-1}}$ are also isotopic. Our main result in this section is as follows:

Theorem 2.9. *Let $0 < k, s \leq \lfloor \frac{m}{2} \rfloor$ and $0 \leq r, t \leq \lfloor \frac{m}{2} \rfloor$, and let $\sigma(x) := x^{p^r}$ and $\tau(x) := x^{p^t}$. Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined as in (2.5) on $\mathbb{F}_{p^{2m}}$ with $\alpha \in \mathbb{F}_{p^l}^*$, where $l = \gcd(m,k)$. If $(k,\sigma) \neq (s,\tau)$, then $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$ are not isotopic.*

Furthermore, if $\sigma = \mathrm{id}$, then for every k, the semifield $\mathbb{S}_k$ defines two inequivalent planar functions over $\mathbb{F}_{p^{2m}}$.

Before proving Theorem 2.9, first we would like to look at the isotopism between Albert's twisted fields, because their multiplications are used in the construction of the presemifield $\mathbb{P}_{k,\sigma}$ in Theorem 2.4. In fact, the isotopisms between Albert's twisted fields have been completely determined by Albert (1961b). Similar results with a different proof were also given by Biliotti, Jha, and Johnson (1999). Here we just need a partial result for the commutative cases.

Lemma 2.10. *Let m, k and s be positive integers such that $0 \leq k \leq s \leq \lfloor \frac{m}{2} \rfloor$ and both $m/\gcd(m,k)$ and $m/\gcd(m,s)$ are odd. Then the presemifield $(\mathbb{F}_{p^m}, +, \circ_k)$ is strongly isotopic to $(\mathbb{F}_{p^m}, +, \circ_s)$ if and only if $k = s$. Furthermore, the strong autotopism group of $(\mathbb{F}_{p^m}, +, \circ_k)$ is isomorphic to the semi-linear group $\Gamma\mathrm{L}(1, p^m)$.*

Remark 2.11. It is worth noting that when $k = 0$, Lemma 2.10 shows that the proper commutative Albert's twisted fields are not strongly isotopic to finite fields, and the strong autotopism group of finite field $\mathbb{F}_{p^m}$ is isomorphic to $\Gamma\mathrm{L}(1, p^m)$.

Proof. By Theorem 1.70, we only need to consider the equivalence between two planar functions $x \circ_k x$ and $x \circ_s x$. Notice that $x \circ_k x = 2x^{p^k+1}$ is clearly equivalent to x^{p^k+1}, so we can look at the equivalence between $f(x) := x^{p^k+1}$ and $g(x) := x^{p^s+1}$ instead.

Assume that f and g are (linear) equivalent, which means there are linearized polynomials $N(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$ and $L(x) = \sum_{i=0}^{m-1} b_i x^{p^i} \in \mathbb{F}_{p^m}[x]$ which are both invertible, such that

$$(N(x))^{p^k+1} = L(x^{p^s+1}).$$

Expanding both sides of it, we have

$$\sum_{i,j=0}^{m-1} a_i^{p^k} a_j x^{p^{k+i}+p^j} = \sum_{i=0}^{m-1} b_i x^{p^{s+i}+p^i}, \tag{2.16}$$

the left-hand side of which can be written as

$$\sum_{i=0}^{m-1} a_{i-k}^{p^k} a_i x^{2p^i} + \sum_{0 \leq i < j \leq m-1} (a_{i-k}^{p^k} a_j + a_{j-k}^{p^k} a_i) x^{p^j+p^i}, \tag{2.17}$$

where the subscripts of a_i are calculated modulo m.

First we assume $s > 0$, which means that for each i the coefficient $a_{i-k}^{p^k} a_i$ of x^{2p^i} in (2.17) must be 0, i.e. at least one of a_{i-k} and a_i is 0. Notice that $N(x)$ is invertible, we assume that there is a i_0 satisfying $a_{i_0-k} \neq 0$. Hence a_{i_0} is 0.

On the other hand, by comparing both sides of (2.16), for every $j \not\equiv i_0 \pm s \pmod{m}$, the coefficient of $x^{p^j+p^{i_0}}$ in (2.17) must be 0, i.e.

$$a_{i_0-k}^{p^k} a_j + a_{j-k}^{p^k} a_{i_0} = a_{i_0-k}^{p^k} a_j = 0,$$

which means $a_j = 0$.

If $k \neq s > 0$, then $i_0 - k \not\equiv i_0 \pm s \pmod{m}$ (here we need that $0 \leq k \leq s \leq \lfloor \frac{m}{2} \rfloor$), which means that $a_{i_0-k} = 0$. This is a contradiction. Therefore, f and g are not equivalent.

If $k = s > 0$, we see that there are only two a_i which can be nonzero: a_{i_0-k} and a_{i_0+k}. However, as the coefficient of $x^{p^{i_0+2k}+p^{i_0-k}}$ should also be 0, we know that

$$a_{i_0+k}^{p^k} a_{i_0-k} = a_{i_0+k}^{p^k} a_{i_0-k} + a_{i_0-2k}^{p^k} a_{i_0+2k} = 0.$$

It means that there is exactly one nonzero a_i in $\{a_{i_0-k}, a_{i_0+k}\}$, and $N(x)$ and $L(x)$ are both monomials. As $L(x)$ is uniquely determined when the monomial $N(x) = ax^{p^i}$ is given, we see that the strong autotopism group of $(\mathbb{F}_{p^m}, +, \circ_k)$ is isomorphic to the semi-linear group $\Gamma\mathrm{L}(1, p^m)$.

Finally we consider the case $s = 0$. As $0 \leq k \leq s$, k also equals 0 and $\circ_s = \circ_k$ is exactly the multiplication of the finite field $\mathbb{F}_{p^m}$. Now (2.16) becomes

$$\sum_{i=0}^{m-1} a_i^2 x^{2p^i} + \sum_{0 \leq i < j \leq m-1} 2a_i a_j x^{p^j+p^i} = \sum_{i=0}^{m-1} b_i x^{2p^i}.$$

By comparing the terms on both sides of it, we see that there is exactly one $a_i \neq 0$. Therefore, the strong autotopism group of $(\mathbb{F}_{p^m}, +, \cdot)$ is also isomorphic to the semi-linear group $\Gamma\mathrm{L}(1, p^m)$. □

Now we look at strong isomorphisms among $\mathbb{P}_{k,\sigma}$'s.

Theorem 2.12. *Let $0 < k, s \leq \lfloor \frac{m}{2} \rfloor$ and $0 \leq r, t \leq \lfloor \frac{m}{2} \rfloor$. Let $\mathbb{P}_{k,\sigma}$ be the presemifield with multiplication $*$ defined as in* (2.3) *on $\mathbb{F}_{p^{2m}}$ with $\alpha \in \mathbb{F}_{p^l}^*$, where $l = \gcd(m, k)$. Define automorphisms $\sigma(x) = x^{p^r}$ $\tau(x) = x^{p^t}$. If $(k, \sigma) \neq (s, \tau)$, then $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$ are not strongly isotopic. Furthermore, the strong autotopism group $\mathrm{Aut}_S(\mathbb{P}_{k,\sigma})$ of $\mathbb{P}_{k,\sigma}$, is isomorphic to a subgroup of the general semi-linear group $\Gamma\mathrm{L}(2, p^m)$, and*

$$|\mathrm{Aut}_S(\mathbb{P}_{k,\sigma})| = \begin{cases} 4m(p^m - 1), & \sigma^2 = \mathrm{id}; \\ 2m(p^m - 1), & \textit{otherwise.} \end{cases}$$

Proof. Let l be a linearized polynomial over $\mathbb{F}_{p^{2m}}$. Since every element $z \in \mathbb{F}_{p^{2m}}$ can be viewed as a vector $(x, y) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by choosing a basis of $\mathbb{F}_{p^{2m}}$ over

$\mathbb{F}_{p^m}$, $l(z)$ can be written as a polynomial $L(x,y) \in \mathbb{F}_{p^{2m}}[x,y]$ whose terms are x^{p^i} and y^{p^i} with $i = 0, \ldots, m-1$.

Let f and g denote the planar functions corresponding $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$, respectively. Since strong isotopism between $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$ is equivalent to the linear equivalence between f and g (Theorem 1.70), we assume that there exist linearized polynomials $l_1, l_2 : \mathbb{F}_{p^{2m}} \to \mathbb{F}_{p^m}$ which can be written as $L_1(x,y), L_2(x,y)$, respectively, and a linearized polynomial $l(z) = L(x,y)$ where both $L(x,y)$ and $(L_1(x,y), L_2(x,y))$ are invertible, such that

$$L\left(L_1(x,y)^{p^k+1} + a(L_2(x,y)^{p^k+1})^\sigma, L_1(x,y)L_2(x,y)\right) = (x^{p^s+1} + a(y^{p^s+1})^\tau, xy). \tag{2.18}$$

For convenience, we denote $L_i(x,0)$ and $L_i(0,y)$ by $L_i(x)$ and $L_i'(y)$, respectively. We first prove:

Claim: If (2.18) holds, then $s = k$ and $L_i(x)$ and $L_i'(y)$ are monomials or zero, for $i = 1, 2$.

Here we only prove the result for $L_i(x)$. By symmetry, a similar proof can be derived for $L_i'(y)$. Let $y = 0$, then we have

$$\begin{aligned}&\left(L_1(x)^{p^k+1} + a(L_2(x)^{p^k+1})^\sigma, L_1(x)L_2(x)\right)\\ =&L^{-1}(x^{p^s+1}, 0)\\ =&(\varphi_1(x^{p^s+1}), \varphi_2(x^{p^s+1})),\end{aligned}$$

where $L_1(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$, $L_2(x) = \sum_{i=0}^{m-1} b_i x^{p^i}$, $\varphi_1(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$ and $\varphi_2(x) = \sum_{i=0}^{m-1} d_i x^{p^i}$ are linearized polynomials. We divide the following proof into two cases:

I. Neither $L_1(x)$ nor $L_2(x)$ equals 0;

II. $L_1(x)$ or $L_2(x)$ equals 0.

Case I: Since $L_1(x)L_2(x) = \varphi_2(x^{p^s+1})$ and $s > 0$, we have

$$\begin{cases} (a_i b_{i+s} + a_{i+s} b_i) = d_i, & \text{for any } i;\\ a_i b_j + a_j b_i = 0, & \text{for } j \neq i \pm s. \end{cases}$$

Assume that $d_u \neq 0$, then, noticing that $a_i b_i = 0$ for any $0 \leq i \leq m-1$, we have $d_u = a_u b_{u+s}$ or $a_{u+s} b_u$.

(a) If $a_u \neq 0$, then $b_u = 0$ and for any $j \neq u \pm s$, we have

$$a_u b_j + a_j b_u = 0,$$

which means that $b_j = 0$, and $L_2(x) = b_{u-s} x^{p^{u-s}} + b_{u+s} x^{p^{u+s}}$.

If b_{u+s} and b_{u-s} are both not 0, then there is

$$\begin{cases} a_{u+s} b_j + a_j b_{u+s} = a_j b_{u+s} = 0, & \text{for } j \neq u+s \pm s, u-s;\\ a_{u-s} b_j + a_j b_{u-s} = a_j b_{u-s} = 0, & \text{for } j \neq u-s \pm s, u+s. \end{cases}$$

which means that $a_j = 0$ for $j \neq u$. Hence $L_1(x) = a_u x^{p^u}$. It follows that

$$\varphi_1(x^{p^s+1}) = a_u^{p^k+1}(x^{p^k+1})^{p^u} + \alpha(b_{u-s}x^{p^{u-s}} + b_{u+s}x^{p^{u+s}})^{(p^k+1)\sigma}. \tag{2.19}$$

The right-hand side of (2.19) is

$$\begin{aligned}&\left(a_u^{p^k+1}x^{(p^k+1)p^u} + \alpha b_{u-s}^{(p^k+1)\sigma}x^{(p^k+1)\sigma p^{u-s}} + \alpha b_{u+s}^{(p^k+1)\sigma}x^{(p^k+1)\sigma p^{u+s}}\right)\\ &+\alpha\left(b_{u-s}^{p^k}b_{u+s}x^{(p^{k-s}+p^s)p^u} + b_{u-s}b_{u+s}^{p^k}x^{(p^{-s}+p^{s+k})p^u}\right)^{\sigma},\end{aligned}$$

which shows that (2.19) cannot hold, since $x^{(p^{k-s}+p^s)}$ and $x^{(p^{-s}+p^{s+k})}$ cannot be simultaneously written in the form $x^{(p^s+1)p^i}$ for some i, respectively. Therefore, one of b_{u-s} and b_{u+s} must be 0.

If $b_{u-s} = 0$, then we can derive that $L_1(x) = a_u x^{p^u} + a_{u+2s}x^{p^{u+2s}}$. By symmetry of $L_1(x)$ and $L_2(x)$, it can also be proved that $a_{u+2s} = 0$. These arguments show that $L_1(x)$ and $L_2(x)$ are both monomials, and we have that

$$\varphi_1(x^{p^s+1}) = a_u^{p^k+1}(x^{p^k+1})^{p^u} + \alpha(b_{u+s}x^{p^{u+s}})^{(p^k+1)\sigma}. \tag{2.20}$$

When $s \neq k$, then (2.20) also cannot hold, otherwise the Albert's twisted semifields defined by x^{p^s+1} and x^{p^k+1} are strongly isotopic, which contradicts Lemma 2.10.

If $b_{u+s} \neq 0$, then by symmetry we can also get $L_1(x) = a_{u+s}x^{p^{u+s}}$ and $L_2(x) = b_u x^{p^u}$ and $s = k$.

(b) Similarly as in **(a)**, if $b_u \neq 0$, by the symmetry of L_1 and L_2 in $L_1(x)L_2(x) = \varphi_2(x^{p^s+1})$, we can prove that $s = k$ and both $L_1(x)$ and $L_2(x)$ are monomials.

Case II: Without loss of generality, we assume that $L_1(x) \neq 0$ and $L_2(x) = 0$. It follows that $L_1(x)^{p^k+1} = \varphi_1(x^{p^s+1})$, which cannot hold for $s \neq k$, since two different Albert's twisted fields are not strongly isotopic, according to Lemma 2.10. When $s = k$, it follows from Lemma 2.10 that $L_1(x)$ and $\varphi_1(x)$ are both linearized monomials.

Therefore, we have proved our **Claim**.

Now, for $k = s$ we know that $L_1(x, y)$ and $L_2(x, y)$ are both linearized binomials or monomials. Assume that the possible degrees of x in L_1 and L_2 are p^u and p^{u+k}, those of y are p^v and p^{v+k}, then there are four possible combinations:

(a) $L_1(x, y) = a_u x^{p^u} + a'_v y^{p^v}$ and $L_2(x, y) = b_{u+k}x^{p^{u+k}} + b'_{v+k}y^{p^{v+k}}$;

(b) $L_1(x, y) = a_u x^{p^u} + a'_{v+k} y^{p^{v+k}}$ and $L_2(x, y) = b_{u+k}x^{p^{u+k}} + b'_v y^{p^v}$;

(c) $L_1(x, y) = a_{u+k} x^{p^{u+k}} + a'_v y^{p^v}$ and $L_2(x, y) = b_u x^{p^u} + b'_{v+k}y^{p^{v+k}}$;

(d) $L_1(x, y) = a_{u+k} x^{p^{u+k}} + a'_{v+k} y^{p^{v+k}}$ and $L_2(x, y) = b_u x^{p^u} + b'_v y^{p^v}$.

Next, we are going to show that $L_1(x,y)$ and $L_2(x,y)$ are both monomials. We write

$$L^{-1} = \begin{pmatrix} \varphi_1 & \varphi_3 \\ \varphi_2 & \varphi_4 \end{pmatrix},$$

more precisely

$$L_1(x,y)^{p^k+1} + \alpha(L_2(x,y)^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy), \quad (2.21)$$

$$L_1(x,y)L_2(x,y) = \varphi_2(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_4(xy), \quad (2.22)$$

where $\varphi_3(x)$ and $\varphi_4(x)$ are both linearized polynomials in $\mathbb{F}_{p^m}[x]$ as well as φ_1 and φ_2 which are already defined.

First, by comparing both sides of (2.22), we know that it is impossible to have one of L_1 and L_2 to be monomial and the other not.

Second, we assume that none of L_1 and L_2 is monomial. We notice that for any given $i \not\equiv j \pmod m$, $x^{p^i}y^{p^j}$ cannot appear on the right-hand side of (2.22). Hence both (a) and (d) are not feasible, and we must have $u = v$ for (b) and (c).

We look at case (b) first. The terms $a_u x^{p^u} a'^{p^k}_{u+k} y^{p^{u+2k}}$ and $(b^{p^k}_{u+k} x^{p^{u+2k}} b'_u y^{p^u})^\sigma$ occur on the left-hand side of (2.21), but they cannot appear on its right-hand side. That means $L_1(x,y)$ and $L_2(x,y)$ are both monomials with the same degree.

The same argument also shows that $L_1(x,y)$ and $L_2(x,y)$ are monomials for case (c).

Now we know that $L_1(x,y)$ and $L_2(x,y)$ are both monomials. There are two possibilities: $L_1(x,y)$ (resp. $L_2(x,y)$) depends on x (resp. y) or $L_1(x,y)$ (resp. $L_2(x,y)$) depends on y (resp. x). By (2.22), we see that L_1 and L_2 are of the same degree.

For the first case, let $L_1(x,y) = a_u x^{p^u}$ and $L_2(x,y) = b'_u y^{p^u}$. Now (2.21) becomes

$$(a_u x^{p^u})^{p^k+1} + \alpha((b'_u y^{p^u})^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy).$$

It follows that $\varphi_1(x)$ has to be a monomial, $\varphi_3(x) = 0$ and $\sigma = \tau$. Furthermore, assume that $\varphi_1(x) = cx^{p^u}$ for some $c \in \mathbb{F}^*_{p^m}$, then $a_u^{p^k+1} = (b'^{p^k+1}_u)^\sigma = c$, which means that $a_u = \pm b'^{\sigma}_u$. Since there are m different u that can be chosen, there are exactly $2m(p^m-1)$ pairs (a_u, b'_u) which can be used to form a strong autotopism of $\mathbb{P}_{k,\sigma}$. Clearly these strong autotopisms can be viewed as elements in the general semi-linear group $\Gamma\mathrm{L}(2, p^m)$.

For the second case, let $L_1(x,y) = a'_v y^{p^v}$ and $L_2(x,y) = b_v x^{p^v}$. Now (2.21) becomes

$$(a'_w y^{p^w})^{p^k+1} + \alpha((b_w x^{p^w})^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy).$$

It follows that $\varphi_1(x)$ is a monomial and $\varphi_3(x) = 0$. Moreover, we have $\sigma = \tau$ and σ^2 is the identity. As the first case, we have another $2m(p^m-1)$ elements in $\mathrm{Aut}_S(\mathbb{P}_{k,\sigma})$. □

To investigate the isotopism between $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$ further, we need the following result by Coulter and Henderson (2008):

Theorem 2.13. *Let $\mathbb{S}_1 = (\mathbb{F}_q, +, \star)$ and $\mathbb{S}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then every isotopism (M, N, K) between $\mathbb{S}_1$ and $\mathbb{S}_2$ satisfies either*

(a) $M = N$, or

(b) $M(x) \equiv \gamma \star N(x)$ $(x^q - x)$, where $\gamma \in N_m(\mathbb{S}_1)$, $\gamma \neq 0$.

The next results follow from Theorem 2.13:

Corollary 2.14. *Let $\mathbb{S} = (\mathbb{F}_q, +, \star)$ be a commutative semifield. Define*

$$U_{\mathbb{S}} := \{\, \mathbb{S}' : \mathbb{S}' \text{ is a semifield isotopic to } \mathbb{S} \,\},$$

and its subset

$$V_{\mathbb{S}} := \{\, \mathbb{S}' : \mathbb{S}' \text{ is a semifield strongly isotopic to } \mathbb{S} \,\}.$$

(a) When q is even, $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$ is empty, see also Coulter and Henderson (2008, Corollary 2.7).

(b) When q is odd, if $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$ is not empty, then for any two semifields $\mathbb{S}_1 = (\mathbb{F}_q, +, *_1)$, $\mathbb{S}_2 = (\mathbb{F}_q, +, *_2) \in U_{\mathbb{S}} \setminus V_{\mathbb{S}}$, $\mathbb{S}_1$ is strongly isotopic to $\mathbb{S}_2$. Furthermore, $\mathbb{S}$ defines at most two inequivalent planar function.

Proof. Assume that $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$ is not empty, i.e. there is a semifield $\mathbb{S}' = (\mathbb{F}_q, +, *)$ which is isotopic but not strongly isotopic to $\mathbb{S}$. By Theorem 2.13, there is an isotopism (M, N, K) between $\mathbb{S}$ and $\mathbb{S}'$ such that $M(x) \equiv \gamma \star N(x)$ $(x^q - x)$, where $\gamma \in N_m(\mathbb{S})$. We can prove that γ is not a square in $N_m(\mathbb{S})$; otherwise assume that $\gamma = \beta^2$, as $\star$ restricted on $N_m(\mathbb{S})$ is the same as the finite field multiplication, we have

$$K(x * y) = (\beta^2 \star N(x)) \star N(y) = (\beta \star N(x)) \star (\beta \star N(x)),$$

which contradicts the assumption that $\mathbb{S}'$ is not strongly isotopic to $\mathbb{S}$. When q is even, every element in $\mathbb{S}$ is a square, which means that $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$ is empty.

Now suppose that q is odd. Let $\mathbb{S}_1$, $\mathbb{S}_2$ be different elements of $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$, namely, they are isotopic but not strongly isotopic to $\mathbb{S}$. By Theorem 2.13 there are two isotopisms $(\gamma_i * N_i, N_i, K_i)$ for $i = 1, 2$ such that

$$K_i(N_i^{-1}(x) *_i N_i^{-1}(y)) = (\gamma_i \star x) \star y,$$

and both γ_1 and γ_2 are non-squares. Hence $\gamma_2 = \gamma_1 \beta^2$ for some $\beta \in N_m(\mathbb{S})$, and

$$K_2(N_2^{-1}(x) *_2 N_2^{-1}(y)) = ((\gamma_1 \beta^2) \star x) \star y = (\gamma_1 \star (\beta \star x)) \star (\beta \star y),$$

which means that

$$K_2(N_2^{-1}(B(x)) *_2 N_2^{-1}(B(y))) = (\gamma_1 \star x) \star y,$$

where $B(x)$ is the inverse of $\beta \star x$. It follows that

$$K_2(N_2^{-1}(B(x)) *_2 N_2^{-1}(B(y))) = K_1(N_1^{-1}(x) *_1 N_1^{-1}(y)).$$

Therefore, $\mathbb{S}_1$ is strongly isotopic to $\mathbb{S}_2$.

By Theorem 1.70, $V_{\mathbb{S}}$ (resp. $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$) defines one planar function up to equivalence. Hence, if $U_{\mathbb{S}} \setminus V_{\mathbb{S}}$ is empty, then $\mathbb{S}$ defines one inequivalent planar function; otherwise $\mathbb{S}$ defines two inequivalent planar functions. □

Next, we are going to show the non-isotopism between $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$.

Proof of Theorem 2.9. Let $\star$ and $\diamond$ be the multiplication of $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$, respectively defined by (2.5), where $(k,\sigma) \neq (s,\tau)$. To show that these semifields are not isotopic, by Theorem 2.13 we need to show that it is impossible to find linearized polynomials N, K and $\gamma \in N_m(\mathbb{S}_{k,\sigma})$ such that

$$(\gamma \star N(x)) \star N(y) = K(x \diamond y),$$

which is

$$(\gamma \star x') \star y' = K(N^{-1}(x') \diamond N^{-1}(y')),$$

by replacing $N(x)$ with x' and $N(y)$ with y'. Define $x \star_\gamma y := (\gamma \star x) \star y$, and let $*$ be the multiplication of $\mathbb{P}_{k,\sigma}$. By (2.5), we have

$$\begin{aligned} x \star_\gamma y &= (\gamma \star x) \star y \\ &= B^{-1}(B^{-1}(\gamma * x) * y), \end{aligned}$$

which is strongly isotopic to

$$x \otimes_\gamma y := B^{-1}(\gamma * x) * y. \tag{2.23}$$

Hence we only need to prove that for any nonzero γ the semifield defined by $\otimes_\gamma$ is not strongly isotopic to $\mathbb{S}_{s,\tau}$. We divide the proof into two cases: $\sigma \neq \mathrm{id}$ and $\sigma = \mathrm{id}$.

When σ is non-trivial, we know that $N_m(\mathbb{S}_{k,\sigma}) = \mathbb{F}_{p^m} \cap \mathbb{F}_{p^k}$, which can be viewed as $\{ (c,0) \mid c \in \mathbb{F}_{p^l} \}$ with $l = \gcd(k,m)$ by Theorem 2.6. Write γ as $(c,0)$ where $c \neq 0$, and write x as (a,b), then

$$B^{-1}(\gamma * x) = B^{-1}\left((c,0) * (a,b)\right) = B^{-1}\left(a \circ_k c, bc\right) = (ac, bc).$$

Take $y = (e,f)$, then (2.23) becomes

$$\begin{aligned} &(a,b) \otimes_\gamma (e,f) \\ =&B^{-1}\left((c,0) * (a,b)\right) * (e,f) \\ =&\left((a \circ_k e)c + \alpha c^\sigma (b \circ_k f)^\sigma, c(af + be)\right). \end{aligned}$$

The corresponding planar function of $\otimes_\gamma$ can be written as

$$(x, y) \mapsto 2 \cdot (cx^{p^k+1} + \alpha c^\sigma (y^{p^k+1})^\sigma, cxy),$$

which is equivalent to the one defined by $\mathbb{S}_{k,\sigma}$. That means, if the presemifield defined by $\otimes_\gamma$ is strongly isotopic to $\mathbb{S}_{s,\tau}$, then $\mathbb{S}_{k,\sigma}$ is also strongly isotopic to $\mathbb{S}_{s,\tau}$, which contradicts Theorem 2.12. Hence $\mathbb{S}_{k,\sigma}$ is not isotopic to $\mathbb{S}_{s,\tau}$.

For the case that σ is trivial, as proved in Theorem 2.6, $N_m(\mathbb{S}_{k,\sigma}) = \mathbb{F}_{p^{2l}}$ which can be written as $\{ (c, d) \mid c, d \in \mathbb{F}_{p^l} \}$ with $l = \gcd(k, m)$. We write γ as (c, d), where $cd \neq 0$, and write x as (a, b), then

$$\begin{aligned} & B^{-1}(\gamma * x) \\ =& B^{-1}((c, d) * (a, b)) \\ =& B^{-1}\left(c(a + a^{p^k}) + \alpha d(b + b^{p^k}), ad + bc\right) \\ =& (ac + \alpha bd, ad + bc). \end{aligned}$$

Take $y = (e, f)$, then (2.23) becomes

$$\begin{aligned} & (a, b) \otimes_\gamma (e, f) \\ =& ((ac + \alpha bd) \circ_k e + \alpha((ad + bc) \circ_k f), (ad + bc)e + (ac + \alpha bd)f) \\ =& (c(a \circ_k e + \alpha(b \circ_k f)) + \alpha d(b \circ_k e + a \circ_k f), c(af + be) + d(ae + bf\alpha)). \end{aligned}$$

If $c \neq 0$, but $d = 0$, then it becomes

$$(a, b) \otimes_\gamma (e, f) = (c(a \circ_k e + \alpha(b \circ_k f)), c(af + be)),$$

which is strongly isotopic to $\mathbb{S}_k$. By Theorem 2.12, $\mathbb{S}_k$ is not strongly isotopic to $\mathbb{S}_s$, therefore the semifield defined by $\otimes_\gamma$ is also not strongly isotopic to $\mathbb{S}_s$.

If $d \neq 0$, then without loss of generality, we assume that $d = 1$ (otherwise, we divide the two components of $(a, b) \otimes_\gamma (e, f)$ by d). Now $(a, b) \otimes_\gamma (e, f)$ becomes

$$(c(a \circ_k e + b \circ_k f\alpha) + \alpha(b \circ_k e + a \circ_k f), c(af + be) + (ae + bf\alpha)), \tag{2.24}$$

and the corresponding planar function is

$$(x, y) \mapsto (2c(x^{p^k+1} + \alpha y^{p^k+1}) + 2\alpha x \circ_k y, 2cxy + x^2 + \alpha y^2),$$

which is equivalent to

$$(x, y) \mapsto (2cxy + x^2 + \alpha y^2, c(x^{p^k+1} + \alpha y^{p^k+1}) + \alpha x \circ_k y). \tag{2.25}$$

Now we need a claim:
Claim: If $c^2 - \alpha$ is a non-square in $\mathbb{F}_{p^l}$, where $l = \gcd(m, k)$, then the presemifield defined by $\otimes_\gamma$ in (2.24) is not strongly isotopic to $\mathbb{S}_s$, for any $s > 0$.

Let us first assume that this claim holds. It is well-known (for example, see Lemma 6.24 in the text book by Lidl and Niederreiter (1997)) that there always exist some $c \in \mathbb{F}_{p^l}$ such that $c^2 - \alpha$ is a non-square in $\mathbb{F}_{p^l}$, where $l = \gcd(m,k)$ and $\alpha \in \mathbb{F}_{p^l}$ is also a non-square. Therefore, for any γ, the presemifield defined by $\otimes_\gamma$ and $\mathbb{S}_s$ are not strongly isotopic. Hence $\mathbb{S}_k$ and $\mathbb{S}_s$ are also not isotopic. Furthermore, as the presemifield $(\mathbb{F}_{p^{2m}}, +, \otimes_\gamma)$ and $\mathbb{S}_k$ are also not strongly isotopic, we see that the semifield $\mathbb{S}_k$ defines exactly two inequivalent planar functions $x \star x$ and $x \otimes_\gamma x$ over $\mathbb{F}_{p^{2m}}$ by Corollary 2.14 (b).

Finally, we are going to prove the claim. Assume that the presemifield defined by $\otimes_\gamma$ in (2.24) is strongly isotopic with $\mathbb{S}_s$, then, similarly as in the proof of Theorem 2.12, we have linearized polynomials $L_1(x,y), L_2(x,y)$ and $L(x,y)$, where $L(x,y)$ is a permutation such that

$$\begin{aligned} & L \circ \begin{pmatrix} 2cL_1(x,y)L_2(x,y) + L_1(x,y)^2 + \alpha L_2(x,y)^2 \\ c(L_1(x,y)^{p^k+1} + \alpha L_2(x,y)^{p^k+1}) + \alpha L_1(x,y) \circ_k L_2(x,y) \end{pmatrix}^T \\ =& (x^{p^s+1} + \alpha y^{p^s+1}, xy). \end{aligned}$$

Let $y = 0$, and we use $L_i(x)$ to denote $L_i(x,0)$ as before. We get

$$\begin{aligned} & \begin{pmatrix} 2cL_1(x)L_2(x) + L_1(x)^2 + \alpha L_2(x)^2 \\ c(L_1(x)^{p^k+1} + \alpha L_2(x)^{p^k+1}) + \alpha L_1(x) \circ_k L_2(x) \end{pmatrix}^T \\ =& L^{-1}(x^{p^s+1}, 0) = (\varphi_1(x^{p^s+1}), \varphi_2(x^{p^s+1})), \end{aligned}$$

where $\varphi_1(x), \varphi_2(x)$ are linearized polynomials. Let $L_1(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$, $L_2(x) = \sum_{i=0}^{m-1} b_i x^{p^i}$ and $\varphi_1(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$, then

$$\begin{aligned} & L_1(x)^2 + \alpha L_2(x)^2 + 2cL_1(x)L_2(x) \\ =& \sum_{i>j} 2(a_i a_j + \alpha b_i b_j + c a_i b_j + c a_j b_i) x^{p^i+p^j} + \sum_{i=0}^{m-1} (a_i^2 + \alpha b_i^2 + 2c a_i b_i) x^{2p^i}. \end{aligned}$$

Since $s \neq 0$, by comparing the equation above with $\varphi_1(x^{p^s+1})$, we have that

$$a_i^2 + \alpha b_i^2 + 2c a_i b_i = 0, \text{ for any } 0 \leq i \leq m-1,$$

which can also be written as,

$$(a_i + c b_i)^2 + (\alpha - c^2) b_i^2 = 0, \text{ for any } 0 \leq i \leq m-1.$$

If $c^2 - \alpha$ is a non-square in $\mathbb{F}_{p^l}$, then it is also a non-square in $\mathbb{F}_{p^m}$, since $\frac{m}{l}$ is odd. Hence the equation above has no solution. Therefore, the claim is proved, and we also finish the proof of this theorem. □

The total number of non-isotopic semifields and inequivalent planar functions defined by $\mathbb{S}_{k,\sigma}$ can also be counted:

Corollary 2.15. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined as in* (2.5) *on $\mathbb{F}_{p^{2m}}$, where $m = 2^e\mu$ with $\gcd(\mu, 2) = 1$. Then the families $\mathbb{S}_{k,\sigma}$ contain*

1. $\lfloor \frac{\mu}{2} \rfloor \cdot \lceil \frac{m}{2} \rceil$ *non-isotopic semifields, and*
2. $\lfloor \frac{\mu}{2} \rfloor \cdot (\lceil \frac{m}{2} \rceil + 1)$ *inequivalent planar functions.* □

Together with Theorem 2.12 and Theorem 2.13, we can determine the autotopism group of $\mathbb{S}_{k,\sigma}$ completely.

Corollary 2.16. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined as in* (2.5) *on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Let $\mathrm{Aut}(\mathbb{S}_{k,\sigma})$ be the autotopism group of $\mathbb{S}_{k,\sigma}$. Then*

$$|\mathrm{Aut}(\mathbb{S}_{k,\sigma})| = \begin{cases} 2m(p^m-1)(p^{2l}-1), & \sigma = \mathrm{id}; \\ 4m(p^m-1)(p^l-1), & \sigma^2 = \mathrm{id} \text{ and } \sigma \neq \mathrm{id}; \\ 2m(p^m-1)(p^l-1), & \text{otherwise}, \end{cases}$$

where $l = \gcd(m, k)$. □

2.4 $\mathbb{S}_{k,\sigma}$ is a new family

In previous sections, we showed that our new family looks like a combination of Dickson's semifields and generalized twisted fields, and $\mathbb{S}_k$ behaves quite different from $\mathbb{S}_{k,\sigma}$ with nontrivial σ. Therefore, we divide this family into two subfamilies, according to whether σ is trivial.

Next, we will consider the following question:

Do $\mathbb{S}_k$ and $\mathbb{S}_{k,\sigma}$ contain new semifields compared with the other known families?

In fact, for some cases, we can prove that $\mathbb{S}_k$ is contained in the family discovered by Budaghyan and Helleseth (2008, 2011), which can be rewritten in the following form:

Theorem 2.17 (Bierbrauer and Kyureghyan (2010))**.** *Let p be an odd prime number. Let $q = p^m$, $n = 2m$ and let integers i, j be such that $s = i - j$. Then the mapping $M_s : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by*

$$M_s(x) = x^{p^m+1} + \omega \mathrm{Tr}_{q^2/q}(\beta x^{p^i+p^j}), \qquad i \geq j \geq 0,$$

is planar if and only if all the following conditions are fulfilled:

1. *s=0 or $\nu(s) \neq \nu(m)$,*
2. *$\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,*
3. *β is a non-square in $\mathbb{F}_{q^2}$,*

where $\nu(s)$ is defined by $s = 2^{\nu(s)}s_1$ with s_1 an odd integer.

As $u^{p^m+1} \in \mathbb{F}_{p^m}$ for any $u \in \mathbb{F}_{p^{2m}}$, $M_s(x)$ can be viewed as an element $(x^{p^m+1}, \mathrm{Tr}_{q^2/q}(\beta x^{p^i+p^j})) \in \mathbb{F}_q \times \mathbb{F}_q$. Thus different choices of ω give equivalent planar functions. Moreover, by applying the field automorphism $x \mapsto x^{p^{n-j}}$ to $\mathrm{Tr}_{q^2/q}(\beta x^{p^i+p^j})$, we have $\mathrm{Tr}_{q^2/q}(\beta x^{p^s+1})$. It follows that different (i,j) with the same $s = i - j$ also lead to equivalent M_s, so we redefine $M_s(x)$ as follows:

$$M_s(x) = x^{p^m+1} + \omega \mathrm{Tr}_{q^2/q}(\beta x^{p^s+1}), \tag{2.26}$$

where $s = 0$ or $\nu(s) \neq \nu(m)$, and β and ω are the same as in Theorem 2.17.

Now we concentrate on the case $2 \nmid m$. It follows that there exists $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ such that

$$\omega + \omega^{p^m} = \omega + \omega^p = 0.$$

As ω is also in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$, we can use this ω in (2.26).

Furthermore, as m is odd and $\nu(s) \neq \nu(m)$, by Lemma 2.1 we have that $\gcd(p^s+1, p^{2m}-1) = 2$. Hence every non-square β' can be written as $\beta' = \beta\theta^{p^s+1}$ for some $\theta \in \mathbb{F}_{q^2}$, and

$$M'_s(x) := x^{p^m+1} + \omega \mathrm{Tr}_{q^2/q}(\beta' x^{p^s+1}) = \frac{1}{\theta^{p^m+1}}(\theta x)^{p^m+1} + \omega \mathrm{Tr}_{q^2/q}(\beta(\theta x)^{p^s+1}),$$

which can be viewed as an element $(\frac{1}{\theta^{p^m+1}}(\theta x)^{p^m+1}, \mathrm{Tr}_{q^2/q}(\beta(\theta x)^{p^s+1}))$ in $\mathbb{F}_q \times \mathbb{F}_q$. Multiplying its first component by θ^{p^m+1} and replacing θx by x we have

$$(x^{p^m+1}, \mathrm{Tr}_{q^2/q}(\beta x^{p^s+1})),$$

which means that $M'_s(x)$ is equivalent to $M_s(x)$, defined in (2.26). Therefore different non-square β lead to equivalent $M_s(x)$, and we may assume that $\beta = \omega^{-1}$. We use $\odot$ to denote the multiplication derived from the planar function defined by (2.26). Use $a + b\omega$ and $c + d\omega$ to denote $u, v \in \mathbb{F}_{p^{2m}}$, respectively, then we have

$$\begin{aligned}
u \odot v =& (a + b\omega) \odot (c + d\omega) \\
=& (a + b\omega^{p^m})(c + d\omega) + (a + b\omega)(c + d\omega^{p^m}) + \omega \mathrm{Tr}_{q^2/q}(\omega^{-1} x \circ_s y) \\
=& 2ac - 2bd\omega^2 + ((a + b\omega) \circ_s (c + d\omega) - (a - b\omega) \circ_s (c - d\omega)) \\
=& 2(ac - bd\omega^2) + 2(a \circ_s (d\omega) + (b\omega) \circ_s c) \\
=& 2(ac - bd\omega^2) + 2(a \circ_s d + b \circ_s c)\omega.
\end{aligned}$$

The last equality holds, because $\omega^{p^s-1} = 1$, since s must be even. Moreover, the corresponding planar function is equivalent to

$$M_s(x, y) = (x^{p^s} y + x y^{p^s}, x^2 - \omega^2 y^2),$$

which is equivalent to (2.25) with $c = 0$, when -1 is a square in $\mathbb{F}_{p^m}$.

On the other hand, since we showed above that when m is odd and -1 is a square, the Budaghyan-Helleseth semifield is isotopic to $\mathbb{S}_k$, it can not be isotopic to $\mathbb{S}_{k,\sigma}$ with non-trivial σ by Theorem 2.9. Furthermore, by the middle and left nucleus of $\mathbb{S}_{k,\sigma}$, we know that it is not isotopic with Albert's or Dickson's semifields. Moreover, as $\mathbb{S}_{k,\sigma}$ is defined over p^{2m} for any odd p, it contains elements which are neither Zha-Kyureghyan-Wang semifields (defined over $\mathbb{F}_{p^{3m}}$) nor Bierbrauer's semifields (defined over $\mathbb{F}_{p^{4m}}$).

Theorem 2.18. *When $m \geq 5$ is odd and -1 is a square, $\mathbb{S}_{k,\sigma}$ with non-trivial σ contains semifields which are not isotopic to any previously known ones.* □

2.5 APN functions of a similar form

From Theorem 1.59 (i), we know that there is no $(2^n, 2^n, 2^n, 1)$-RDS in $C_2^n \times C_2^n$ relative to C_2^n. We can also show this result in another way: subset D is a $(2^n, 2^n, 2^n, 1)$-RDS in $C_2^n \times C_2^n$, if and only if, there is a planar function f on $\mathbb{F}_{2^n}$, i.e. $f(x+a) - f(x)$ is a permutation for any nonzero a. However, as we mentioned in Remark 1.21, if $x_0 \in \mathbb{F}_{2^n}$ is a root of $f(x+a) - f(x) = b$, then $x_0 + a$ is also a root of it. It follows that $f(x+a) - f(x)$ can not be a permutation. Hence there is no planar function on $\mathbb{F}_{2^n}$, and $|\{x : f(x+a) - f(x) = b\}| \geq 2$ for any $a \neq 0$ and b.

Definition 2.19. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear (APN)*, if for each $a, b \in \mathbb{F}_{p^n}$, $a \neq 0$, $f(x+a) - f(x) = b$ has exactly 2 solutions.

The following family of APN functions is due to Gold (1968) and Nyberg (1994), and they are often called *Gold's APN functions*.

Proposition 2.20. *Let k, n be positive integers satisfying $\gcd(n,k) = 1$. Mapping f defined by $x \mapsto x^{2^k+1}$ on $\mathbb{F}_{2^n}$ is an APN mapping. If n is odd, then f is a permutation. If n is even, then f is a 3-1 mapping on $\mathbb{F}_{2^n}^*$.*

Proof. For any nonzero $a \in \mathbb{F}_{2^n}$,

$$f(x+a) - f(x) = x^{2^k} a - a^{2^k} x + a^{2^k+1}.$$

As it is an affine polynomial, we have

$$|\{x : f(x+a) - f(x) = b\}| = |\{x : x^{2^k} a = a^{2^k} x\}| = |\{0\} \cup \{x : (x/a)^{2^k-1} = 1\}|.$$

An argument similar to that of Lemma 2.1, can show that:

- $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1$,
- $\gcd(2^m + 1, 2^n - 1) = (2^{\gcd(2m,n)} - 1)/(2^{\gcd(m,n)} - 1)$,

for any integers m, n. It follows that $\gcd(2^k-1, 2^n-1) = 1$. Therefore,

$$|\{x : (x/a)^{2^k-1} = 1\}| = 1,$$

i.e. f is an APN mapping. On the other hand, since

$$\gcd(2^k+1, 2^n-1) = \begin{cases} 1, & n \text{ is odd;} \\ 3, & n \text{ is even.} \end{cases}$$

we see that f is a permutation if n is odd, and f is 3-1 on $\mathbb{F}_{2^n}^*$ if n is even. □

Gold's APN functions are analogues of $x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ which define Albert's commutative twisted fields. It is also shown by Budaghyan and Helleseth (2008) and Zha, Kyureghyan, and Wang (2009) that more planar functions can be derived from quadratic APN functions. Similar constructions for planar function are further investigated by Bierbrauer (2009, 2010), Zha and Wang (2009). One natural question is the following: Is it possible to get some new APN functions from known planar ones?

In fact, from our new presemifields family, we can derive a similar family of APN functions on $\mathbb{F}_{2^{2m}}$:

Theorem 2.21. *Let $m \geq 2$ be an even integer, and let k be an integer, such that $\gcd(k, m) = 1$. Define a function f on $\mathbb{F}_{2^{2m}}$ by*

$$f(x, y) = (x^{2^k+1} + \alpha y^{(2^k+1)\sigma}, xy),$$

where $\alpha \in \mathbb{F}_{2^m}$, $\alpha \neq 0$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^m})$. Then f is an APN function, if and only if, α cannot be written as $a^{2^k+1}(t^{2^k}+t)^{1-\sigma}$, where $a, t \in \mathbb{F}_{2^m}$.

Proof. Since f is quadratic, we only have to prove that for each $(a, b) \neq 0$, the equations

$$\begin{aligned} x \circ_k a + \alpha(y \circ_k b)^\sigma &= 0 \\ ay + bx &= 0 \end{aligned} \tag{2.27}$$

have at most two roots, where $x \circ_k y = x^{2^k} y + y^{2^k} x$.

If $b = 0$, then we have $x \circ_k a = 0$ and $ay = 0$, which means $y = 0$, $x = a$ or 0, since x^{2^k+1} is an APN function on $\mathbb{F}_{2^m}$ and $a \neq 0$.

If $b \neq 0$, then $x = \frac{ay}{b} = t \cdot a$, where $t := \frac{y}{b}$. Plugging them into (2.27), we obtain

$$(at) \circ_k a + \alpha((bt) \circ_k b)^\sigma = 0,$$

i.e.

$$(t^{2^k}+t)a^{2^k+1} + \alpha(t^{2^k}+t)^\sigma b^{(2^k+1)\sigma} = 0.$$

If $t^{2^k} + t = 0$, then $x = y = 0$ or $y = b$, $x = a$. If $t^{2^k} + t \neq 0$, then we have

$$\alpha = \left(\frac{a}{b^\sigma}\right)^{2^k+1} (t^{2^k}+t)^{1-\sigma},$$

which finishes the proof. □

Let us further consider the condition of Theorem 2.21. As $\gcd(k,m)=1$ and $2 \mid m$, we have $\gcd(2^k+1, 2^m-1)=3$ and $\gcd(2^i-1, 2^m-1)=2^{\gcd(i,m)}-1$. Hence, if i is even and $\sigma(x)=x^{2^i}$, then $a^{2^k+1}(t^{2^k}+t)^{1-\sigma}$ is a cube. Therefore, if α is not a cube, then the condition in Theorem 2.21 holds.

Corollary 2.22. *Let $m \geq 2$ be an even integer, and let k be an integer, such that $\gcd(k,m)=1$. Define a function f on $\mathbb{F}_{2^{2m}}$ as follows:*

$$f(x,y)=(x^{2^k+1}+\alpha y^{(2^k+1)2^i}, xy),$$

where the nonzero $\alpha \in \mathbb{F}_{2^m}$ is a non-cubic and i is even. Then f is an APN function. □

Let $m=4$, $k=1$ and α be a primitive element of $\mathbb{F}_{2^4}$. By Corollary 2.22, we can choose $i=0$ or 2 to get two APN functions. Using MAGMA, it can be computed that, when $i=0$, this APN function is equivalent to the function No. 2.1 in Table 10 by Edel and Pott (2009b). However, when $i=2$, the Γ-rank of this APN function is 13642, which does not occur in the list of known APN functions by Edel and Pott (2009b). More precisely, the function

$$f(x,y)=(x^3+\alpha y^{12}, xy)$$

is a new APN function on $\mathbb{F}_{2^8}$.

Remark 2.23. Carlet (2011) presents some constructions of APN functions, which include a similar result to Theorem 2.21 with $\sigma = \mathrm{id}$.

Chapter 3

Two approaches to planar functions

The one will be like the reflection of the moon in water;
the other like a flower reflected in a mirror.

Xueqin Cao, *Dream of the Red Chamber*

In this chapter, we concentrate on planar functions on $\mathbb{F}_q$ where q is odd. Two approaches are applied to them. In Section 3.1, we use the well known character approach to prove some unexpected links between planar functions over $\mathbb{F}_{p^m}$ and planar functions over $\mathbb{F}_{p^{2m}}$. In Section 3.2, we study the projections and liftings of planar functions. We applied coding theoretical approaches, and we give computational results about the switchings of planar functions on $\mathbb{F}_{3^n}$ with $n = 3, 4, 5, 6$.

This chapter is based on the papers by Pott and Zhou (2010, 2011).

3.1 A character approach to planar functions

Let D be a $(q, q, q, 1)$-relative difference set in $G = (\mathbb{F}_q^2, +)$ relative to $N = (\mathbb{F}_q, +)$ where $q = p^n$ and p is an odd prime. As we mentioned in Proposition 1.20, D can be written as

$$D := \{ (x, f(x)) : x \in \mathbb{F}_q \},$$

where $f(x) : \mathbb{F}_q \to \mathbb{F}_q$ is a planar function. By (1.6), D is a $(q, q, q, 1)$-RDS if and only if for each $\chi \in \hat{G}$

$$|\chi(D)|^2 = \begin{cases} q, & \text{for } \chi_{|N} \neq \chi_0; \\ 0, & \text{for } \chi_{|N} = \chi_0, \chi \neq \chi_0; \\ q^2, & \text{for } \chi = \chi_0. \end{cases}$$

A character of abelian group G is a homomorphism $\chi : G \to \mathbb{C}^*$, and all characters together form the character group $\hat{G}$ of G. Actually every character $\chi \in \hat{G}$ can be written as

$$\chi_a(g) = \zeta^{\mathrm{Tr}(a \cdot g)},$$

for some $a \in G$, where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace mapping and $a \cdot g$ denotes the inner product of a and g, which are viewed as elements in $\mathbb{F}_q^2$. Assume that $n = 2m$, then we may identify $g \in G$ as $g = (g_1, g_2, g_3, g_4)$ where $g_i \in \mathbb{F}_{p^m}$, and

$$\chi_a(g) = \chi_{a_1,a_2,a_3,a_4}(g_1, g_2, g_3, g_4) = \prod_{i=1}^{4} \zeta_p^{\mathrm{Tr}(a_i g_i)} = \zeta_p^{\sum_{i=1}^{4} \mathrm{Tr}(a_i g_i)}.$$

Now we can use the well known character approach to prove the following unexpected result.

Theorem 3.1. *Let $\psi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be any permutation, and let $\varphi_1, \varphi_2 : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be arbitrary functions. Then the mapping*

$$\begin{array}{rccc} f: & \mathbb{F}_{p^m}^2 & \to & \mathbb{F}_{p^m}^2 \\ & \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & \begin{pmatrix} x^2 + \varphi_1(y) \\ 2x \cdot \psi(y) + \varphi_2(y) \end{pmatrix} \end{array}$$

is planar if and only if

$$\begin{array}{rccc} g: & \mathbb{F}_{p^m} & \to & \mathbb{F}_{p^m} \\ & y & \mapsto & -u^2 \cdot \psi^2(y) + u \cdot w \cdot \psi(y) + \varphi_1(y) + u \cdot \varphi_2(y) \end{array} \tag{3.1}$$

is planar for all $u, w \in \mathbb{F}_{p^m}$.

Proof. Let $\chi(x) = \zeta_p^{\mathrm{Tr}(x)}$ for $x \in \mathbb{F}_{p^m}$, and let D be the set

$$D := \{ (x, y, x^2 + \varphi_1(y), 2x \cdot \psi(y) + \varphi_2(y)) \ : \ x, y \in \mathbb{F}_{p^m} \}.$$

We compute the character values of $D \subseteq \mathbb{F}_{p^m}^4$. The characters are indexed by four parameters $a_1, a_2, b_1, b_2 \in \mathbb{F}_{p^m}$, corresponding to the four components in $\mathbb{F}_{p^m}^4$.

If $(b_1, b_2) = (0, 0)$ and $(a_1, a_2) \neq (0, 0)$, then $\chi_{a_1,a_2,0,0}(D) = 0$. Next, we compute $\chi_{a_1,a_2,b_1,b_2}(D)$ for $(b_1, b_2) \neq (0, 0)$. We have

$$\begin{aligned} \chi_{a_1,a_2,b_1,b_2}(D) &= \sum_{x,y} \chi(b_1 x^2 + b_1 \varphi_1(y)) \chi(2b_2 x \psi(y) + b_2 \varphi_2(y)) \chi(a_1 x) \chi(a_2 y) \\ &= \sum_{x,y} \chi(b_1 x^2 + (2b_2 \psi(y) + a_1) x) \chi(b_1 \varphi_1(y) + b_2 \varphi_2(y) + a_2 y). \end{aligned}$$

If $b_1 = 0$ and $b_2 \neq 0$, this reduces to

$$\begin{aligned} \chi_{a_1,a_2,0,b_2}(D) &= \sum_{x,y} \chi((2b_2 \psi(y) + a_1) x) \chi(b_2 \varphi_2(y) + a_2 y) \\ &= p^m \chi(b_2 \varphi_2(y_o) + a_2 y_o), \end{aligned}$$

where $y_0 = \psi^{-1}(-\frac{a_1}{2b_2})$ (using (1.5)). This shows $|\chi_{a_1,a_2,0,b_2}(D)| = p^m$ if $b_2 \neq 0$. If $b_1 \neq 0$, then we need to compute the character sum

$$\sum_{x \in \mathbb{F}_{p^m}} \chi(b_1 x^2 + (2b_2 \psi(y) + a_1) x),$$

which is basically a Gaussian sum. The absolute value of this sum is known to be $p^{m/2}$, however we need the exact value of it, which was given by Helleseth and Kholosha (2007, Corollary 2). Using that corollary, we obtain

$$\begin{aligned}
&\chi_{a_1,a_2,b_1,b_2}(D)\\
=&C\sum_y \chi\left(-\frac{(2b_2\psi(y)+a_1)^2}{4b_1}\right)\chi\left(b_1\varphi_1(y)+b_2\varphi_2(y)+a_2y\right)\\
=&C\sum_y \chi\left(-\frac{(2b_2\psi(y)+a_1)^2}{4b_1}+b_1\varphi_1(y)+b_2\varphi_2(y)+a_2y\right)\\
=&C\sum_y \chi\left(-\frac{b_2^2}{b_1}\psi^2(y)-\frac{b_2a_1}{b_1}\psi(y)-\frac{a_1^2}{4b_1}+b_1\varphi_1(y)+b_2\varphi_2(y)+a_2y\right),
\end{aligned}$$

where $C=\pm p^{m/2}$ and the sign depends on m and b_1. If $b_2=0$, we have

$$\chi_{a_1,a_2,b_1,0}(D)=C\cdot\chi\left(-\frac{a_1^2}{4b_1}\right)\sum_y\chi(a_2y)\cdot\chi(b_1\varphi_1(y)).$$

The summation over y in this expression is

$$\sum_y\chi(a_2y)\cdot\chi(b_1\varphi_1(y))=\sum_y\chi(a_2y+b_1\varphi_1(y)).$$

If f is planar, then $|\sum_y\chi(a_2y+b_1\varphi_1(y))|=p^{m/2}$ for all $b_1\neq 0$, in particular $\varphi_1(y)$ has to be planar.

The case $b_2\neq 0$ is similar. Now we obtain

$$\begin{aligned}
&\chi_{a_1,a_2,b_1,b_2}(D)\\
=&C\cdot\chi\left(-\frac{a_1^2}{4b_1}\right)\sum_y\chi(a_2y)\cdot\chi\left(b_2(-\frac{b_2}{b_1}\psi^2(y)-\frac{a_1}{b_1}\psi(y)+\frac{b_1}{b_2}\varphi_1(y)+\varphi_2(y))\right).
\end{aligned}$$

We put $u=\frac{b_2}{b_1}$, $v=b_1$ and $w=-\frac{a_1}{b_1}$ and obtain

$$\begin{aligned}
&b_2\left(-\frac{b_2}{b_1}\psi^2(y)-\frac{a_1}{b_1}\psi(y)+\frac{b_1}{b_2}\varphi_1(y)+\varphi_2(y)\right)\\
=&v(-u^2\psi^2(y)+uw\psi(y)+\varphi_1(y)+u\varphi_2(y)).
\end{aligned}$$

Therefore, if f is planar then $-u^2\psi^2(y)+uw\psi(y)+\varphi_1(y)+u\varphi_2(y)$ must be planar for all $u\in\mathbb{F}_{p^m}$, $u\neq 0$.

Note that the converse (the "only if" statement) follows in the same way: If $-u^2\psi^2(y)+uw\psi(y)+\varphi_1(y)+u\varphi_2(y)$ is planar, then the character values of D have the correct size. □

If we take $\psi(y)$ in Theorem 3.1 to be a linearized polynomial, then we may assume without loss of generality that $\psi(y)=y$ (note that ψ is a permutation).

We found many quadratic functions φ_1 and φ_2 which satisfy the necessary and sufficient conditions of our main theorem, but unfortunately we could not find a new one so far.

In the special case that $\varphi_1(y) = L_1(y^2)$ and $\varphi_2(y) = L_2(y^2)$ for linear functions L_1 and L_2, our construction uses basically the same approach as Cohen and Ganley (1982) used to construct commutative semifields. However, since we can derive a necessary and sufficient condition, we can actually say more: The so called Ganley's semifields constructed in 1981 immediately give rise to the Coulter-Matthews-Ding-Yuan semifields, constructed only in 1997 and 2006. This shows the power of Theorem 3.1.

To be more specific, we can rephrase our necessary and sufficient condition (3.1) as follows: We assume $\varphi_1(y) = L_1(y^2)$, $\varphi_2(y) = L_2(y^2)$ and $\psi(y) = y$ for linearized polynomials L_1 and L_2. In this case, the planar function

$$-u^2y^2 + uwy + L_1(y^2) + uL_2(y^2)$$

must be equivalent to the classical quadratic function y^2, which is the case if and only if

$$-u^2x + L_1(x) + uL_2(x)$$

is a permutation polynomial for all u.

- If we take $L_1(x) = kx^\sigma$, where σ is a field automorphism and k is a non-square, and $L_2 = 0$, then we obtain Dickson's semifields (and if σ is the identity, then we obtain the finite field).
- The Cohen-Ganley semifields occur for $L_1(x) = kx + k^3x^9$ and $L_2(x) = kx^3$, where k is a non-square, again.
- The sporadic example due to Penttila and Williams (2004) is $L_1(x) = x^9$, $L_2(x) = x^{27}$.

By setting $\varphi_1(x) = x^{10}$ and $\varphi_2(x) = x^6 \in \mathbb{F}_{3^m}[x]$, we obtain the semifields found by Ganley (1981). Then Theorem 3.1 shows that

$$x^{10} + ux^6 - u^2x^2$$

is planar for all u, which is also proved by Coulter and Matthews (1997) and Ding and Yuan (2006). Note that this gives a surprising connection between Ganley's semifields and the Coulter-Matthews-Ding-Yuan semifields.

3.2 Switchings of planar functions

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a planar function with $q = p^n$. Although f is defined over $\mathbb{F}_q$, to get the relative difference set we only need the additive group of

$\mathbb{F}_q$, which means that we can also say that f is a planar function from $\mathbb{F}_p^n$ to itself (or from C_p^n to itself). We use $D_f := \{ (x, f(x)) : x \in \mathbb{F}_p^n \}$ to denote the corresponding element in the group ring $\mathbb{K}[\mathbb{F}_p^{2n}]$. (Strictly speaking, $\mathbb{F}_p^{2n}$ is a vector space. However, as we only use its additive group here, we view it as a group.)

Now we recall the projections of elements $D \in \mathbb{K}[G]$, which is defined in Section 1.10. Let H be a subgroup of G. Then the canonical homomorphism $\varphi_H : G \to G/H$ defined by $\varphi_H(g) := g + H$ (denoted by $\bar{g}$) can be extended to a homomorphism $\varphi_H : \mathbb{K}[G] \to \mathbb{K}[G/H]$. To be precise, let $D = \sum a_g g \in \mathbb{K}[G]$, then $\varphi_H(D) = \sum_{\bar{g} \in G/H} (\sum_{h \in g+H} a_h) \cdot \bar{g}$. If D corresponds to a set in G, i.e. D has only coefficients 0 and 1, then the coefficient of $\bar{g}$ is $|D \cap (g + H)|$.

Definition 3.2. Let $f, g : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be two functions, and let H be a subgroup of $\{0\} \times (\mathbb{F}_p^n, +)$. Then H can be naturally viewed as a subspace of $\mathbb{F}_p^n$. We call f and g *switching neighbors with respect to* H if $\varphi_H(D_f)$ is equivalent to $\varphi_H(D_g)$ and $1 \leqslant \dim(H) < n$, where $D_f := \sum_{x \in \mathbb{F}_p^n} (x, f(x))$, $D_g := \sum_{x \in \mathbb{F}_p^n} (x, g(x)) \in \mathbb{K}[\mathbb{F}_p^{2n}]$. If $\dim(H) = 1$, f and g are called *switching neighbors in the narrow sense*.

If f, g are switching neighbors with respect to H, then g can be obtained from f by first projecting D_f onto $\varphi_H(D_f)$, and then "lifting" this element to D_g. In fact, this project and lift method turns out to be very powerful for the construction of new APN functions. Edel and Pott (2009b) showed that many APN functions can be constructed by switching, and they found a new non-quadratic APN function over $\mathbb{F}_{2^6}$. So, it is natural to consider the following research problems related to Problem 1.1.

Problem 3.1. Is it possible that two planar functions are switching neighbors?

Problem 3.2. Can we use the switching idea for the construction of new planar functions?

One of the difficulties to generalize the idea of Edel and Pott (2009b) to odd characteristic is that the linear restrictions for the switching in the even characteristic case become nonlinear conditions in the odd characteristic case. Due to the limitation of computer capacity, we only consider the switching for the case $p = 3$ in the next theorem. For convenience, for any mapping f defined on groups (or fields) we define $\Delta_f(x, a) := f(x + a) - f(x)$.

Theorem 3.3. *Assume that $f : \mathbb{F}_3^n \to \mathbb{F}_3^n$ is a planar function. Let $u \in \mathbb{F}_3^n \setminus \{0\}$, and let $\delta : \mathbb{F}_3^n \to \mathbb{F}_3$. Then $f(x) + \delta(x) \cdot u$ is a planar function if and only if*

$$\sum_{i=0}^{2} \Delta_\delta(x_i, a) = 0, \quad \text{and} \quad \Delta_\delta(x_1, a) - \Delta_\delta(x_2, a) \neq 1, \tag{3.2}$$

for all $0 \neq a, x_i \in \mathbb{F}_3^n$ with

$$\Delta_f(x_i, a) = b + i \cdot u, \tag{3.3}$$

for $i = 0, 1, 2$ and $b \in \mathbb{F}_3^n$.

Proof. Since f is a planar function, the three equations

$$\Delta_f(x,a) = b + i \cdot u, \quad i = 0,1,2$$

have precisely one solution for each i, denoted by x_i, $i = 0,1,2$. Now we consider the value of $\Delta_\delta(x_i,a)$. Function $f + \delta \cdot u$ is planar if and only if

$$\{\, \Delta_f(x_i,a) + \Delta_\delta(x_i,a) \cdot u : i = 0,1,2 \,\} = \{\, b, b+u, b+2u \,\}$$

That means the vector $(\Delta_\delta(x_0,a), \Delta_\delta(x_1,a), \Delta_\delta(x_2,a))$ belongs to

$$\{\ (i,i,i) : i = 0,1,2 \,\} \cup \{\, (i,i+1,i+2) : i = 0,1,2 \,\},$$

which is equivalent to (3.2). □

Theorem 3.3 suggests a strategy to find the p-ary function δ such that $f + \delta \cdot u$ is a planar function: Determine all the x_i and $x_i + a$ such that (3.3) holds. Then they give rise to linear constraints $\sum_{i=0}^{2} \Delta_\delta(x_i,a) = 0$, and nonlinear constraints $\Delta_\delta(x_1,a) - \Delta_\delta(x_2,a) \neq 1$. Finally, find out whether these planar functions obtained from the switching construction above are new.

For the $p > 3$ case, the nonlinear conditions can not be written as some linear equalities and inequalities as in Theorem 3.3, and it seems quite difficult to make an efficient MAGMA program to do the switching construction.

Linear codes from planar functions

Similar to the link between APN functions and linear codes which was investigated by Carlet, Charpin, and Zinoviev (1998), Edel and Pott (2009b) and Browning, Dillon, McQuistan, and Wolfe (2010), we could establish links between linear codes and planar functions to investigate the equivalence of planar functions.

A *linear code* of length n and rank k is a k-dimensional subspace C of a vector space $\mathbb{K}^n$ over an arbitrary field $\mathbb{K}$. Here we are basically interested in the case $\mathbb{K} = \mathbb{F}_q$. As a linear subspace of $\mathbb{K}^n$, the entire code C may be represented as the span of a minimal set of codewords (known as a basis of the subspace C). These basis codewords are often collated in the rows of a matrix known as a *generator matrix* for the code C.

The *dual code* $C^\perp$ of a linear code C over $\mathbb{K}$ is defined to be

$$C^\perp := \{u \in \mathbb{K}^n : u \cdot v = 0 \text{ for all } v \in C\},$$

where $u \cdot v = \sum_{i=1}^{n} u_i v_i$.

Two linear codes in $\mathbb{K}^n$ are *monomially equivalent* if each can be obtained from the other by permuting the coordinate positions in $\mathbb{K}^n$ and multiplying each coordinate by a non-zero field element. The codes are called to be *permutation equivalent* if a permutation of the coordinate positions suffices to take one to the other.

Table 3.1: Weight distribution of C_f for odd n

weight	frequency
0	1
$(p-1)p^{n-1} - p^{\frac{n-1}{2}}$	$\frac{1}{2}(p-1)(p^{2n}-p^n)$
$(p-1)p^{n-1}$	$(p^n+p)(p^n-1)$
$(p-1)p^{n-1} + p^{\frac{n-1}{2}}$	$\frac{1}{2}(p-1)(p^{2n}-p^n)$
p^n	$p-1$

The two equivalences mentioned above can be represented by monomial matrices and permutation matrices, respectively, which we multiply from the right-hand side of the generator matrix of the code. The set of monomial matrices that map the linear code C to itself form the group $\mathrm{MAut}(C)$ called the *monomial automorphism group of* C. Similarly, the set of permutation matrices that map C to itself form another group $\mathrm{PAut}(C)$ named the *permutation automorphism group of* C. The groups $\mathrm{MAut}(C)$ and $\mathrm{PAut}(C)$ are important invariants of linear codes and they are also useful to investigate linear codes.

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be any function. Define a matrix $M_f \in \mathbb{M}_{(m+n+1)\times p^n}(\mathbb{F}_p)$ as follows:

$$M_f = \begin{pmatrix} \cdots & 1 & \cdots \\ \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{pmatrix}_{x\in\mathbb{F}_p^n} \tag{3.4}$$

Then we can construct a code C_f over $\mathbb{F}_p$ using M_f as a generator matrix.

As we mentioned before, all the known planar functions from $\mathbb{F}_{p^n}$ to itself can be written as a DO polynomial except for the Coulter-Matthews planar functions (see (1.14) for its definition). Let f be one of the known planar functions, the weight distribution of C_f is known, see Table 3.1 and Table 3.2. The weight distributions of the codes corresponding to the Coulter-Matthews planar functions were determined by Li, Ling, and Qu (2009). For planar DO polynomials f, the proof of the weight distributions of the code C_f were given by Li, Li, and Zhou (2010) using non-degenerate quadratic forms.

It is worth noting that the codes corresponding to two different APN functions over the same finite field $\mathbb{F}_{2^n}$ do not necessarily have the same weight distribution, see the paper by Edel and Pott (2009b). Furthermore, as Carlet, Charpin, and Zinoviev (1998) showed, when f is defined on $\mathbb{F}_{2^n}$ to itself, the minimum distance of $C_f^\perp$ is 6 if and only if f is APN. However, when f is defined on $\mathbb{F}_{p^n}$ with odd p, there is no such necessary and sufficient condition. We can use these codes to test the equivalence of two functions, due to the following proposition:

Table 3.2: Weight distribution of C_f for even n

weight	frequency
0	1
$(p-1)(p^{n-1}-p^{\frac{n-2}{2}})$	$\frac{1}{2}(p^{2n}-p^n)$
$(p-1)p^{n-1}-p^{\frac{n-2}{2}}$	$\frac{1}{2}(p-1)(p^{2n}-p^n)$
$(p-1)p^{n-1}$	$(p^{n-1}-p)$
$(p-1)p^{n-1}+p^{\frac{n-2}{2}}$	$\frac{1}{2}(p-1)(p^{2n}-p^n)$
$(p-1)(p^{n-1}+p^{\frac{n-2}{2}})$	$\frac{1}{2}(p^{2n}-p^n)$
p^n	$p-1$

Proposition 3.4. *Let p be a prime, and let m, n be integers. Functions $f, g : \mathbb{F}_p^n \to \mathbb{F}_p^m$ are CCZ-equivalent if and only if the corresponding codes C_f and C_g are permutation equivalent.*

Proof. Assume that C_f and C_g are permutation equivalent, then we have a permutation matrix P and an $(n+m+1)\times(n+m+1)$ matrix L of full rank, such that

$$L \cdot M_f \cdot P = M_g.$$

That means there are $u \in \mathbb{F}_p^n$, $v \in \mathbb{F}_p^m$ and a matrix $\tilde{L}$ of full rank such that

$$\tilde{L} \cdot \begin{pmatrix} \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{pmatrix} \cdot P = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & g(x) & \cdots \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}.$$

Therefore, by the definition of CCZ-equivalence, f and g are CCZ-equivalent. The proof of the converse is the same. □

By Proposition 3.4, we see that when f is a planar function defined over $\mathbb{F}_p^n$, its permutation automorphism group $\mathrm{PAut}(C_f)$ is isomorphic to

$$\begin{aligned}\mathrm{PAut}(C_f) \cong& \{\, L \in \mathbb{M}_{(2n+1)\times(2n+1)}(\mathbb{F}_p) : L \cdot M_f = M_f \,\} \\ \cong& \{\, \varphi \in \mathrm{Aut}(C_p^{2n}) : \varphi(D_f) = D_f + (u,v) \text{ for some } u,v \in C_p^n \,\} \\ =& \mathcal{M}(D_f)\end{aligned}$$

and the multiplier group of $D_f := \{\, (x, f(x)) : x \in \mathbb{F}_p^n \,\}$.

Dempwolff and Röder (2006) proved the following result:

Theorem 3.5. *Let $f(x) = x^d \in \mathbb{F}_{p^n}[x]$ be a planar function with p odd. Assume that the plane $\mathbf{P}(f)$ derived from D_f as in Result 1.57 is not a translation plane, then $f(x)$ is not a Dembowski-Ostrom polynomial and the automorphism group of $\mathrm{Aut}(\mathbf{P}(f))$ is isomorphic to $(C_p^n \times C_p^n) \rtimes \Gamma\mathrm{L}(1, p^n)$.*

Now let f be a Coulter-Matthews planar function on $\mathbb{F}_{p^n}$, which defines a non-translation plane. It follows that $\mathrm{Aut}(\mathbf{P}(f)) \cong (C_p^n \times C_p^n) \rtimes \Gamma\mathrm{L}(1, p^n)$ from Theorem 3.5. In fact, every $(x, y) \in (C_p^n \times C_p^n) \lhd \mathrm{Aut}(\mathbf{P}(f))$ defines a mapping

$$(a, b) \mapsto (a + x, b + y),$$

which maps the line $D_f + (a, b)$ of $\mathbf{P}(f)$ to another line $D_f + (a + x, b + y)$, see Result 1.57. This mapping is not in $\mathrm{Aut}(C_p^{2n})$, thus $(C_p^n \times C_p^n) \cap \mathcal{M}(D_f) = \varnothing$. Moreover, every element in $\Gamma\mathrm{L}(1, p^n)$ fixes D_f in the following way

$$\{\, (ax^{p^i}, a^d (x^d)^{p^i}) : x \in \mathbb{F}_{p^n} \,\} = \{\, (x, x^d) : x \in \mathbb{F}_{p^n} \,\}.$$

which means that $\Gamma\mathrm{L}(1, p^n) \leq \mathcal{M}(D_f)$. As $\mathcal{M}(D_f)$ is a subgroup of the automorphism group $\mathrm{Aut}(\mathbf{P}(f))$ and $(C_p^n \times C_p^n) \cap \mathcal{M}(D_f) = \varnothing$, we see that

$$\mathcal{M}(D_f) \cong \mathrm{PAut}(C_f) \cong \Gamma\mathrm{L}(1, p^n).$$

When a planar function f can be written as a DO polynomial, we can also use the strong autotopism group of the semifield $\mathbb{S}_f$ defined by f to determine $\mathcal{M}(D_f)$.

Theorem 3.6. *Let f be a DO polynomial in $\mathbb{F}_{p^n}[x]$ with p odd. If f is a planar function, then*

$$\mathcal{M}(D_f) \cong C_p^n \rtimes \mathrm{Aut}_s(\mathbb{S}_f).$$

Proof. Every element of $\mathcal{M}(D_f)$ can be written as a $2n \times 2n$ invertible matrix

$$\tilde{L} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ acting by left multiplication on } \begin{pmatrix} \cdots & x & \cdots \\ \cdots & g(x) & \cdots \end{pmatrix},$$

where A, B, C and $D \in \mathbb{M}_{n\times n}(\mathbb{F}_p)$. By the result from Kyureghyan and Pott (2008), we have $B = 0$. It follows that A and D are both invertible. If we use linearized polynomials l_1, l_2 and l_3 to represent A, D and C, respectively, then there is some $u, v \in \mathbb{F}_{p^n}$ such that

$$l_2 \circ f(l_1^{-1}(x) + u) + l_3 \circ l_1^{-1}(x) + v = f(x).$$

Since $f(x)$ is a DO polynomial, for fixed l_1, l_2, we see by expanding $f(l_1^{-1}(x) + u)$ that $l_3 \circ l_1^{-1}$ is completely determined by u. Actually, if we take $l_1 = l_2 = \mathrm{id}$, then for any $u \in \mathbb{F}_{p^n}$ there is $l_3(x) = -2u * x$ and $v = -u * u$, where $*$ is the multiplication defined by $f(x)$, i.e. $x * y = \frac{1}{2}(f(x + y) - f(x) - f(y))$. Therefore, all such l_3 form a group which is isomorphic to C_p^n. This group is a normal subgroup of $\mathcal{M}(D_f)$, because for any invertible A, D, we have

$$\begin{pmatrix} A & 0 \\ C & D \end{pmatrix}^{-1} \begin{pmatrix} I & 0 \\ N & I \end{pmatrix} \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} = \begin{pmatrix} I & 0 \\ D^{-1}NA & I \end{pmatrix}.$$

Every element in $\mathcal{M}(D_f)/C_p^n$ can be written as a $2n \times 2n$ matrix

$$\begin{pmatrix} N & 0 \\ 0 & L \end{pmatrix},$$

where N and L are both invertible $n \times n$ matrices. This is exactly the matrix representation of a strong autotopism of $\mathbb{S}_f$. Hence $\mathcal{M}(D_f) \cong C_p^n \rtimes \mathrm{Aut}_s(\mathbb{S}_f)$ □

Let f be a planar function which can be written as a DO polynomial. Theorem 3.6 and Theorem 1.46 together tell us that the permutation automorphism group $\mathrm{PAut}(C_f) \cong \mathcal{M}(D_f)$ can be derived from $\mathrm{Aut}_s(\mathbb{S}) \leq \mathrm{Aut}(\mathbb{S}) \leq \mathrm{Aut}(\mathbf{P}(\mathbb{S}))$. For instance, when $f(x) = x^2$ or x^{p^k+1} over $\mathbb{F}_{p^n}$ where $k > 0$ and $\frac{n}{\gcd(n,k)}$ is odd, it follows from Lemma 2.10 that $\mathrm{PAut}(C_f) \cong C_p^n \rtimes \Gamma\mathrm{L}(1, p^n) = \mathrm{A}\Gamma\mathrm{L}(1, p^n)$. It can also be determined by methods from coding theory, which is due to Berger and Charpin (1996).

When we project the code C_f to some of its subcodes, we can not completely determine its permutation automorphisms group here, but we know two of its subgroups.

Theorem 3.7. *Let $f \in \mathbb{F}_{p^n}[x]$ be a DO polynomial, and let l be a linear mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. The linear code $C_{l\circ f}$ is defined by the generator matrix $M_{l\circ f}$. Then the elementary abelian group C_p^n and* $\mathrm{Gal}(\mathbb{F}_{p^n})$ *are subgroups of* $\mathrm{PAut}(C_{l\circ f})$.

Proof. It is trivial to prove that $\mathrm{Gal}(\mathbb{F}_{p^n}) \subseteq \mathrm{PAut}(C_{l\circ f})$. Here we only prove $(\mathbb{F}_{p^n}, +) \subseteq \mathrm{PAut}(C_{l\circ f})$. For any $a \in \mathbb{F}_{p^n}$, define the matrix $M_{l\circ f}^{(a)}$ as follows

$$M_{l\circ f}^{(a)} = \begin{pmatrix} \cdots & 1 & \cdots \\ \cdots & x+a & \cdots \\ \cdots & l \circ f(x+a) & \cdots \end{pmatrix}_{x \in \mathbb{F}_p^n}.$$

It is obvious that $M_{l\circ f}^{(a)}$ can be obtained by permuting the columns of $M_{l\circ f}$. Let $C_{l\circ f}^{(a)}$ be the code generated by $M_{l\circ f}^{(a)}$. If we show that $C_{l\circ f}^{(a)} = C_{l\circ f}$, then we prove the theorem.

Let $l_1 : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $l_2 : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be two linear mappings, and $c \in \mathbb{F}_p$, then any codeword in C_f can be written as

$$(l_1(x) + l_2 \circ l \circ f(x) + c)_{x \in \mathbb{F}_p^n}.$$

Since f is a DO polynomial, $u(x) = l_2 \circ l(f(x+a) - f(x) - f(a))$ is a linear mapping. Define a linear mapping $l_3 : \mathbb{F}_{p^n} \to \mathbb{F}_p$ by

$$l_3(x) = l_1(x) - u(x).$$

It follows that

$$l_1(x) + l_2 \circ l \circ f(x) = l_3(x+a) + l_2 \circ l \circ f(x+a) + d \ ,$$

where $d = l_2 \circ l \circ f(a) - l_3(a)$, for any $x, a \in \mathbb{F}_{p^n}$. Therefore, $C_{l\circ f} = C_{l\circ f}^{(a)}$. □

Remark 3.8. MAGMA only provides us a command to tell whether two codes are monomially equivalent. However for the codes C_f and C_g obtained from the planar functions f, g, monomial and permutation equivalences are identical. The reason is as follows: From Table 3.1 and Table 3.2, we see that there are only $p-1$ code words $(i, i, \ldots, i)$ of weight p^n $(0 < i < p)$ in C_f (resp. C_g). It follows that if C_f is monomially equivalent to C_g, a codeword $(i, i, \ldots, i)$ in C_f is mapped to a codeword $(j, j, \ldots, j)$ in C_g for some j. It means that the nonzero entries of the corresponding monomial matrix multiplied on the right-hand side of M_f are identical, i.e. there is a nonzero $c \in \mathbb{F}_p$ such that

$$L \cdot M_f \cdot (cP) = M_g,$$

where L is invertible and P is a permutation matrix. Hence

$$(cL) \cdot M_f \cdot P = M_g,$$

which means that C_f and C_g are permutation equivalent.

Computational Results

Now we describe the switching construction of planar functions on $\mathbb{F}_{3^n}$. First, we "project" all known functions to $(n-1)$-dimensional subspaces, and calculate how many inequivalent classes there are. Then, we do the "lift" for all the inequivalent projections, and construct $f'(x) = f(x) + \delta(x) \cdot u$. Finally, we test whether f' is inequivalent to the known planar functions.

Due to the nonlinear conditions in Theorem 3.3, we can only do the exhaustive search for the switching of all known planar functions on $\mathbb{F}_{3^n}$ with $n \leq 6$. All the planar functions obtained this way are equivalent to known ones.

Next, we investigate the number of equivalent m-dimensional projections of two known inequivalent planar functions, for every $0 < m < n$. If l is a projection from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, then l can be expressed as an $m \times n$ matrix, and there are $\frac{\prod_{i=n-m+1}^{n}(p^i-1)}{\prod_{i=1}^{m}(p^i-1)}$ such projections.

When $m = 1$, the function $l \circ f(x)$ can always be expressed by $\mathrm{Tr}(a \cdot f(x))$, where $a \in \mathbb{F}_{p^n}^*$ and $\mathrm{Tr}(\cdot)$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. If f is a planar DO polynomial, then $\mathrm{Tr}(a \cdot f(x))$ is a non-degenerate quadratic form on $\mathbb{F}_p$. Furthermore, up to equivalence, there are two non-degenerate quadratic forms for even n, and only one non-degenerate quadratic form for odd n, see Theorem 5.8 in the text book by Hirschfeld (1998). Moreover, it is obvious that $\mathrm{Tr}(a \cdot g(x))$ is not quadratic, when g can be written as a non-DO monomial, for example Coulter-Matthews functions $x^{\frac{3^k+1}{2}}$ with odd $k > 1$ and $\gcd(n, k) = 1$. Therefore we have the following result:

Proposition 3.9. *Assume that g is defined by a non-DO monomial in $\mathbb{F}_{p^n}[x]$, then g is not a switching neighbor of any planar DO polynomial functions on $\mathbb{F}_{p^n}$ with respect to any $m-$dimensional subspace $U \in \mathbb{F}_p^n$ with $0 < m < n$.* □

Table 3.3: Switching neighbors with respect to all $l : \mathbb{F}_3^3 \to \mathbb{F}_3^2, \mathbb{F}_3$

	x^2	x^4
x^2	1	1
x^4	1	1

(a) $\mathbb{F}_3^3 \to \mathbb{F}_3^2$

	x^2	x^4
x^2	1	1
x^4	1	1

(b) $\mathbb{F}_3^3 \to \mathbb{F}_3$

In the following, we do the calculations for the known planar functions on $\mathbb{F}_{3^n}$ with $n \geqslant 3$, since x^2 is the unique planar function on $\mathbb{F}_3$ and on $\mathbb{F}_{3^2}$. For the list of known planar functions from commutative semifields, see Section 1.8.

The $\mathbb{F}_{3^3}$ case

There are only two inequivalent planar DO polynomials x^2 and x^{p+1} over $\mathbb{F}_{p^3}$. Obviously, the Coulter-Matthews planar function family does not provide any other functions here, so we have only 2 known inequivalent planar functions over $\mathbb{F}_{3^3}$. By Theorem 3.7, the permutation automorphism groups of the corresponding codes are both $A\Gamma L_1(p^n)$. For $m = 1, 2$, let R_f^m denote the set of all the inequivalent functions $l \circ f : \mathbb{F}_3^3 \to \mathbb{F}_3^m$, where l goes through all projections from $\mathbb{F}_3^3$ to $\mathbb{F}_3^m$. In Table 3.3, the numbers on the diagonals denote $|R_f^m|$, and the numbers off the diagonals denote $|\{h \in R_f^m : \exists h' \in R_g^m, \text{ s.t. } h \text{ is equivalent to h'}\}|$.

The $\mathbb{F}_{3^4}$ case

All the known planar functions on $\mathbb{F}_{3^4}$ are the Coulter-Matthews function and those from the following commutative semifields of order 3^4: finite field, Dickson's semifields, the Budaghyan-Helleseth semifields and the Cohen-Ganley semifields. However, by MAGMA program, we know that all the planar functions from Dickson's, the Budaghyan-Helleseth and the Cohen-Ganley semifields are EA-equivalent. Hence, we list the only 3 known inequivalent planar functions on $\mathbb{F}_{3^4}$ in Table 3.4, with the order of the permutation automorphism groups of corresponding codes. Furthermore, as Table 3.3, we list the switching neighbors among all these planar functions in Table 3.5. It is worth noting that two inequivalent examples (x^2, Dickson's semifield abbreviated to D in Table 3.5) are switching neighbors in the narrow sense.

The $\mathbb{F}_{3^5}$ case

From the lists in Section 1, Table 3.6 contains all the known inequivalent planar functions on $\mathbb{F}_{3^5}$. $CMDY_1$ and $CMDY_2$ are two inequivalent semifields from the Coulter-Matthews-Ding-Yuan semifield family. No two functions are switching

Table 3.4: All known inequivalent planar functions over $\mathbb{F}_{3^4}$

No.	Name	Function	$\lvert\mathrm{PAut}(C_f)\rvert / \lvert\mathrm{Gal}(\mathbb{F}_{3^4})\rvert$
1	$\mathbb{F}_{3^4}$	x^2	$\lvert\mathrm{AGL}(1,3^4)\rvert$
2	Dickson's	$x^4+x^{10}-x^{36}$	$16\cdot\lvert\mathbb{F}_{3^4}\rvert$
3	Coulter-Matthews	x^{14}	$\lvert\mathbb{F}_{3^4}^*\rvert$

Table 3.5: Switching Neighbors with respect to all $l:\mathbb{F}_3^4\to\mathbb{F}_3^3,\mathbb{F}_3^2,\mathbb{F}_3$

	x^2	D	x^{14}
x^2	2	1	0
D	1	4	0
x^{14}	0	0	2

(a) $\mathbb{F}_3^4\to\mathbb{F}_3^3$

	x^2	D	x^{14}
x^2	5	5	0
D	5	7	0
x^{14}	0	0	6

(b) $\mathbb{F}_3^4\to\mathbb{F}_3^2$

	x^2	D	x^{14}
x^2	2	2	0
D	2	2	0
x^{14}	0	0	2

(c) $\mathbb{F}_3^4\to\mathbb{F}_3$

neighbors with respect to 1-dimensional linear spaces. Therefore, we do not write down the entire matrix of the number of switching neighbors since all off-diagonal elements are 0 (Table 3.7). Furthermore, Tables 3.8 and 3.9 show their switching neighbors with respect to all the projections from $\mathbb{F}_3^5$ to $\mathbb{F}_3^3$ and $\mathbb{F}_3^2$, respectively. As we mentioned at the beginning of this section, with respect to all the projections from $\mathbb{F}_3^5$ to $\mathbb{F}_3$, all the planar functions share only one quadratic form on $\mathbb{F}_p$, except for the Coulter-Matthews function, which is a nonquadratic function on $\mathbb{F}_p$ under these projections. Hence, we do not give another table to describe the $\mathbb{F}_3^5\to\mathbb{F}_3$ case.

Table 3.6: All known inequivalent planar functions over $\mathbb{F}_{3^5}$

No.	Name	Function	$\lvert\mathrm{PAut}(C_f)\rvert / \lvert\mathrm{Gal}(\mathbb{F}_{3^5})\rvert$
1	$\mathbb{F}_{3^5}$	x^2	$\lvert\mathrm{AGL}(1,3^5)\rvert$
2	Albert	x^4	$\lvert\mathrm{AGL}(1,3^5)\rvert$
3	Albert	x^{10}	$\lvert\mathrm{AGL}(1,3^5)\rvert$
4	CMDY_1	$x^{10}+x^6-x^2$	$2\cdot\lvert\mathbb{F}_{3^5}\rvert$
5	CMDY_2	$x^{10}-x^6-x^2$	$2\cdot\lvert\mathbb{F}_{3^5}\rvert$
6	Sporadic	x^2+x^{90}	$22\cdot\lvert\mathbb{F}_{3^5}\rvert$
7	Coulter-Matthews	x^{14}	$\lvert\mathbb{F}_{3^5}^*\rvert$

Table 3.7: Number of inequivalent $l \circ f$ for all $l : \mathbb{F}_3^5 \to \mathbb{F}_3^4$

f	x^2	x^4	x^{10}	CMDY_1	CMDY_2	$x^2 + x^{90}$	x^{14}
Number	1	1	1	25	25	3	1

Table 3.8: Switching neighbors with respect to all $l : \mathbb{F}_3^5 \to \mathbb{F}_3^3$

	x^2	x^4	x^{10}	CMDY_1	CMDY_2	$x^2 + x^{90}$	x^{14}
x^2	2	0	0	0	0	0	0
x^4	0	2	0	0	2	0	0
x^{10}	0	0	2	0	0	0	0
CMDY_1	0	0	0	239	14	3	0
CMDY_2	0	2	0	14	230	1	0
$x^2 + x^{90}$	0	0	0	3	1	22	0
x^{14}	0	0	0	0	0	0	2

Table 3.9: Switching neighbors with respect to all $l : \mathbb{F}_3^5 \to \mathbb{F}_3^2$

	x^2	x^4	x^{10}	CMDY_1	CMDY_2	$x^2 + x^{90}$	x^{14}
x^2	2	2	2	2	2	2	0
x^4	2	2	2	2	2	2	0
x^{10}	2	2	2	2	2	2	0
CMDY_1	2	2	2	4	4	4	0
CMDY_2	2	2	2	4	4	4	0
$x^2 + x^{90}$	2	2	2	4	4	4	0
x^{14}	0	0	0	0	0	0	2

Table 3.10: All known inequivalent planar functions over $\mathbb{F}_{3^6}$

No.	Name	Function	$\frac{\lvert \mathrm{PAut}(C_f)\rvert}{\lvert \mathrm{Gal}(\mathbb{F}_{3^6})\rvert}$
1	$\mathbb{F}_{3^6}$	x^2	$\lvert \mathrm{AGL}(1,3^6)\rvert$
2	Albert	x^{10}	$\lvert \mathrm{AGL}(1,3^6)\rvert$
3	Dickson	$x^{162}+x^{84}+\alpha^{58}x^{54}+\alpha^{58}x^{28}+x^6+\alpha^{531}x^2$	$26\cdot\lvert\mathbb{F}_{3^6}\rvert$
4	BH	$\alpha^{75}x^{2214}+x^{756}+\alpha^{205}x^{82}+x^{28}$	$52\cdot\lvert\mathbb{F}_{3^6}\rvert$
5	BHγ	$x^{270}-x^{246}+x^{90}-x^{82}-x^{54}+x^{30}-x^{10}-x^2$	$52\cdot\lvert\mathbb{F}_{3^6}\rvert$
6	N	$x^{324}+2x^{246}+\alpha^{144}x^{108}-x^{90}+\alpha^{534}x^{82}+\alpha^2x^{54}$ $+\alpha^{586}x^{30}+\alpha^{449}x^{28}+x^{12}+\alpha^{248}x^4+\alpha^{28}x^2$	$26\cdot\lvert\mathbb{F}_{3^6}\rvert$
7	Ganley	$x^{270}-x^{244}+\alpha^{449}x^{162}+\alpha^{449}x^{84}+\alpha^{534}x^{54}$ $-x^{36}+\alpha^{534}x^{28}+x^{10}+\alpha^{449}x^6+\alpha^{279}x^2$	$13\cdot\lvert\mathbb{F}_{3^6}\rvert$
8	CG	$x^{486}+x^{252}+\alpha^{561}x^{162}+\alpha^{561}x^{84}+\alpha^{183}x^{54}$ $+\alpha^{183}x^{28}+x^{18}+\alpha^{561}x^6+\alpha^{209}x^2$	$4\cdot\lvert\mathbb{F}_{3^6}\rvert$
9	CM	x^{122}	$\lvert\mathbb{F}_{3^6}^*\rvert$

Table 3.11: Number of inequivalent $l\circ f$ for all $l:\mathbb{F}_3^6\to\mathbb{F}_3^5$

f	x^2	x^{10}	BH	BHγ	N	Dickson	Ganley	CG	x^{122}
Number	2	2	7	7	7	7	12	43	2

The $\mathbb{F}_{3^6}$ case

Table 3.10 contains all the known inequivalent planar functions on $\mathbb{F}_{3^6}$, where α is a primitive element of $\mathbb{F}_{3^6}$ and a root of $x^6-x^4+x^2-x-1$. We abbreviate Cohen-Ganley to CG and Coulter-Matthews to CM. It should be noted that, there are two semifields from Theorem 2.4 which define three inequivalent planar functions, see Corollary 2.15. They also cover the Budaghyan-Helleseth semifield of order 3^6. Let "BH" and "BHγ" denote the two inequivalent planar functions from the same semifield obtained by setting $\sigma=\mathrm{id}$ in Theorem 2.4 (or, equivalently, in the Budaghyan-Helleseth semifields). We use "N" to denote the third planar function obtained by setting $\sigma(x)=x^3$ in Theorem 2.4.

For all the projections $l:\mathbb{F}_3^6\to\mathbb{F}_3^5$, the numbers of inequivalent $l\circ f$ are listed in Table 3.11. We have shown that there is only one equivalent pair which comes from the projections of Dickson's and Cohen-Ganley planar function, respectively, i.e. there is again one case where two inequivalent functions are switching neighbors in the narrow sense. Since there are 11011 projections from $\mathbb{F}_3^6$ to $\mathbb{F}_3^4$ or $\mathbb{F}_3^2$, it is beyond our computation capacity to compute all the projections up to equivalence. Hence, we can not give the classification of projections in other dimensions here.

Chapter 4

$(q, q, q, 1)$-relative difference sets with q even

It's time for the odd to get even!

Revenge of the Nerds (1984)

In Chapter 2, we have considered $(p^n, p^n, p^n, 1)$-RDSs in C_p^{2n} relative to C_p^n with odd prime p. They can be expressed also as a polynomial in $\mathbb{F}_{p^n}[x]$ defining a planar function. This expression offers us a convenient way to construct and analyze these RDSs, because we can use the theory of polynomials over finite fields. When $p = 2$, by Theorem 1.59, we see that every abelian $(2^n, 2^n, 2^n, 1)$-relative difference set D is in C_4^n relative to $2C_4^n \cong C_2^n$. At first glance, it seems that D has nothing to do with polynomials over $\mathbb{F}_{2^n}$.

However, given a semifield $\mathbb{S}$ with multiplication $*$, the product $x * y$ can always be written as a polynomial in $\mathbb{F}_{p^n}[x, y]$. This gives us a hint that even when $p = 2$, there should also be some necessary and sufficient condition in a polynomial form for getting a $(2^n, 2^n, 2^n, 1)$-RDS, because every semifield $\mathbb{S}$ defines a projective plane $\mathbf{P}(\mathbb{S})$ of type (b) of Theorem 1.52, see Result 1.58.

In Section 4.1, we introduce several necessary and sufficient conditions for $(2^n, 2^n, 2^n, 1)$-RDSs in C_4^n relative to $2C_4^n$, one of which allows us to write the RDSs as a special type of polynomials in $\mathbb{F}_{2^n}[x]$. We call the functions defined by this type of polynomials "planar over $\mathbb{F}_{2^n}$", see Section 4.1. Then we investigate the plane $\mathbf{P}(D)$ defined by a relative difference set D of this type, and we show that $\mathbf{P}(D)$ is a semifield plane if and only the corresponding planar function is a Dembowski-Ostrom polynomial.

In Section 4.3, we consider planar functions with exactly two elements in their image sets. We prove that $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfying $|\mathrm{Im}(f)| = 2$ and $f(0) = 0$ is planar, if and only if, f is *additive*, i.e. $f(x + y) = f(x) + f(y)$ for any $x, y \in \mathbb{F}_{2^n}$.

In Section 4.4, we consider some projections of planar functions, which we call shifted-bent functions. We show their subtle relation with bent functions over $\mathbb{F}_2^n$.

For convenience, we will always say "C_4^n relative to C_2^n" instead of "C_4^n relative to $2C_4^n$" in the rest of this chapter.

4.1 Planar functions over $\mathbb{F}_{2^n}$

Before considering these relative difference sets, we introduce some notation for the elements in C_4^n. We define an embedding $\psi : C_2 \to C_4 = \{0,1,2,3\}$ by $0^\psi = 0$ and $1^\psi = 1$, and define $\Psi : C_2^n \to C_4^n$ by

$$(x_0, x_1, \ldots, x_{n-1})^\Psi = (x_0^\psi, x_1^\psi, \ldots, x_{n-1}^\psi).$$

As $0^\psi + 0^\psi = 0$, $0^\psi + 1^\psi = 1$ and $1^\psi + 1^\psi = 0 + 2 \cdot 1^\psi$, we have

$$x^\psi + y^\psi = (x+y)^\psi + 2(xy)^\psi \tag{4.1}$$

for $x, y \in C_2$. Every $\xi \in C_4^n$ can be uniquely expressed as a 2-tuple

$$\xi = \lfloor a, b \rfloor := a^\Psi + 2b^\Psi,$$

where $a, b \in C_2^n$. For instance, $3 \in C_4$ is $\lfloor 1, 1 \rfloor$ and the normal subgroup C_2^n can be written as $\{\lfloor 0, b \rfloor : b \in C_2^n\}$. Let $\lfloor a, b \rfloor, \lfloor c, d \rfloor \in C_4^n$, it follows from (4.1) that

$$\lfloor a, b \rfloor + \lfloor c, d \rfloor = \lfloor a + c, b + d + (a \odot c) \rfloor,$$

where $a \odot c := (a_0 c_0, \ldots, a_{n-1} c_{n-1})$ for $a = (a_0, \ldots, a_{n-1})$ and $c = (c_0, \ldots, c_{n-1})$. It will always be clear from the context whether the symbol "$+$" refers to the addition of C_4^n or the addition of C_2^n.

Remark 4.1. In the language of group theory, C_4^n can be viewed as an extension of C_2^n by C_2^n. The set $\{\lfloor a, 0 \rfloor : a \in \mathbb{F}_2^n\}$ forms a transversal for the subgroup C_2^n in C_4^n and $\odot : C_2^n \times C_2^n \to C_2^n$ is the corresponding *factor set* (or *cocycle*). Factor sets form an important tool for many combinatorial objects, see the book by Horadam (2007) for the applications to Hadamard matrices and RDSs.

Let D be a transversal for the normal subgroup C_2^n in C_4^n, then we can write every element in D as

$$\lfloor d, h(d) \rfloor = d^\Psi + 2h(d)^\Psi, \tag{4.2}$$

where h is a mapping from C_4^n / C_2^n to C_2^n. When D is a $(2^n, 2^n, 2^n, 1)$-RDS, D is also a transversal, otherwise the list of differences of D will contain some element of the forbidden subgroup C_2^n. Let $\lfloor a, b \rfloor \in C_4^n$ and $a \neq 0$. As there is exactly one element in $(D + \lfloor a, b \rfloor) \cap D$, the equation

$$\lfloor d + a, h(d) + b + (d \odot a) \rfloor = \lfloor d', h(d') \rfloor,$$

holds for exactly one pair (d, d'), which means that the mapping

$$\Delta_{h,a} : d \mapsto h(d + a) + h(d) + (d \odot a) \tag{4.3}$$

is bijective for each $a \neq 0$. Conversely, if h is such that $\Delta_{h,a}$ is a permutation for all nonzero a, then D is a $(2^n, 2^n, 2^n, 1)$-RDS.

Remark 4.2. In fact, $\Delta_{h,a}$ has been already investigated by Hiramine (1991) in the form of factor sets. However, our main idea here is to use it to derive special types of functions over finite fields.

The mapping $h : C_4^n/C_2^n \to C_2^n$ defined by D by (4.2) can be considered as a mapping from $\mathbb{F}_2^n$ to itself, hence we call h the $\mathbb{F}_2^n$*-representation* of the transversal D. We will use it to introduce the polynomial representation over a finite field.

Let $B = \{\xi_i : i = 0, 1, \ldots, n-1\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. We can view both h and $\Delta_{h,a}$ as mappings from $\mathbb{F}_{2^n}$ to itself using this basis B, and express them as polynomials $h_B, \Delta_{h_B,a} \in \mathbb{F}_{2^n}[x]$. Furthermore, for $x = \sum_{i=0}^{n-1} x_i\xi_i$ and $y = \sum_{i=0}^{n-1} y_i\xi_i \in \mathbb{F}_{2^n}$, $\mu_B(x)$ is the polynomial defined by the mapping $x \mapsto \sum_{i<j} x_i x_j \xi_i \xi_j$,

$$x \odot_B y := \sum_{i=0}^{n-1} x_i y_i \xi_i,$$

and

$$f_B(x) := h_B(x)^2 + \mu_B(x). \tag{4.4}$$

Then

$$\begin{aligned}
\nabla_{f_B,a}(x) :&= f_B(x+a) + f_B(x) + f_B(a) + xa \\
&= (h_B(x+a) + h_B(x) + h_B(a))^2 + (\mu_B(x+a) + \mu_B(x) + \mu_B(a)) + xa \\
&= (h_B(x+a) + h_B(x) + h_B(a))^2 + (x \odot_B a)^2 \\
&= (\Delta_{h_B,a}(x) + h_B(a))^2.
\end{aligned}$$

It follows that for each $a \neq 0$, (4.3) is a bijection if and only if $\nabla_{f_B,a}(x)$ is a permutation polynomial. We call $f_B(x) \in \mathbb{F}_{2^n}[x]$ the $\mathbb{F}_{2^n}$*-representation* of D with respect to the basis B. We summarize the above results in the following theorem:

Theorem 4.3. *Let $D \subseteq C_4^n$ be a transversal for C_2^n in C_4^n, let B be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and let h be the $\mathbb{F}_2^n$-representation of D and f_B be its $\mathbb{F}_{2^n}$-representation with respect to B. Then the followings are equivalent:*

1. *D is an RDS in C_4^n relative to C_2^n;*
2. *$\Delta_{h,a}$ is bijective for each $a \neq 0$;*
3. *$\nabla_{f_B,a}(x)$ is a permutation polynomial for each $a \neq 0$.* □

Remark 4.4. Let $u, v \in \mathbb{F}_{2^n}$, let $(c_0, c_1, \ldots, c_{n-1})$ be a nonzero vector in $\mathbb{F}_2^n$ and let $d_0 \in \mathbb{F}_2$. If $g_B(x) = f_B(x) + ux^{2^i} + v$ for some i, then

$$\begin{aligned}
\nabla_{g_B,a}(x) &= g_B(x+a) + g_B(x) + g_B(a) + xa \\
&= f_B(x+a) + f_B(x) + f_B(a) + v + xa \\
&= \nabla_{f_B,a}(x) + v
\end{aligned}$$

which means that adding affine terms $ux^{2^i}+v$ to $f_B(x)$ does not change the permutation properties of $\nabla_{f_B,a}$. A similar argument shows that adding $\sum_i c_i x_i + d_0$ to any coordinate functions h_i of h does not change the permutation properties of $\Delta_{h,a}$ either. If there is no ux^{2^i} or constant term in $f_B(x)$ (resp. no linear or constant term in every coordinate function of h), we call f_B a *normalized* $\mathbb{F}_{2^n}$-representation (resp. h a *normalized* $\mathbb{F}_2^n$-representation) of D. They are similar to DO polynomials in $\mathbb{F}_{p^n}[x]$ with odd p, because both of them have no linear or constant term.

Since we can always use an RDS in C_4^n relative to C_2^n to construct a plane of order 2^n, we call $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ a *planar function* if for each $a\neq 0$,

$$f(x+a)+f(x)+xa \tag{4.5}$$

is a permutation on $\mathbb{F}_{2^n}$. This definition does not conflict with Definition 1.19, because, as we mentioned in Remark 1.21, planar functions from Definition 1.19 can not exist on $\mathbb{F}_q$ when q is even. As every mapping from $\mathbb{F}_{2^n}$ to itself can be written as a polynomial in $\mathbb{F}_{2^n}[x]$, the corresponding polynomial of a planar function is called a *planar polynomial*.

The advantage of the above representations of $(2^n,2^n,2^n,1)$-RDSs in C_4^n is that we can apply finite fields theory to construct and analyze these RDSs. Here are some examples:

Example 4.5. For each positive integer n, every affine mapping on $\mathbb{F}_{2^n}$, especially $f(x)=0$, is a planar function. They define the desarguesian planes.

The $\mathbb{F}_2^n$-representations of the corresponding RDSs are more complicated. Let us look at the case $n=4$. Let ξ be a root of the irreducible polynomial

$$x^4+x^3+x^2+x+1\in\mathbb{F}_2[x].$$

It follows that $\mathbb{F}_2[\xi]\cong\mathbb{F}_{2^4}$. Let ξ_i denote ξ^{2^i} for $i=0,\ldots,3$. We can show by hand or by computer that $B:=\{\xi_0,\xi_1,\xi_2,\xi_3\}$ is a basis of $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, and

$$\begin{array}{lcl}
\xi_0\xi_1 &=& \xi_3\\
\xi_0\xi_2 &=& \xi_0+\xi_1+\xi_2+\xi_3\\
\xi_0\xi_3 &=& \xi_2\\
\xi_1\xi_2 &=& \xi_0\\
\xi_1\xi_3 &=& \xi_0+\xi_1+\xi_2+\xi_3\\
\xi_2\xi_3 &=& \xi_1
\end{array}$$

As the planar function $f(x)=0$, from (4.4) we have $h_B(x)=\sqrt{\mu_B(x)}$, where $\mu_B: x\mapsto\sum_{i<j}x_ix_j\xi_i\xi_j$. It follows that the coordinate functions $h_i(x)$'s of the $\mathbb{F}_2^n$-representation $h(x)$ are:

$$\begin{array}{lcl}
h_0(x) &=& x_0x_2+x_1x_3+x_2x_3\\
h_1(x) &=& x_0x_2+x_0x_3+x_1x_3\\
h_2(x) &=& x_0x_1+x_0x_2+x_1x_3\\
h_3(x) &=& x_0x_2+x_1x_2+x_1x_3
\end{array}$$

□

Kantor (2003) derived the following commutative presemifields of characteristic 2 from the symplectic semifields constructed by Kantor and Williams (2004):

Definition 4.6. Assume that we have a chain of fields $\mathbb{F} = \mathbb{F}_0 \supset \mathbb{F}_1 \supset \cdots \supset \mathbb{F}_n$ of characteristic 2 with $[\mathbb{F} : \mathbb{F}_n]$ odd and corresponding trace mappings $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$. Define commutative presemifield $\mathbf{B}((\mathbb{F}_i)_0^n, (\zeta_i)_1^n) := (\mathbb{F}, +, *)$ by:

$$x * y = xy + (x \sum_{i=1}^{n} \mathrm{Tr}_i(\zeta_i y) + y \sum_{i=1}^{n} \mathrm{Tr}_i(\zeta_i x))^2, \tag{4.6}$$

where $\zeta_i \in \mathbb{F}^*$, $1 \leq i \leq n$.

Remark 4.7. The corresponding planar function of $\mathbf{B}((\mathbb{F}_i)_0^n, (\zeta_i)_1^n)$ is

$$(x \sum_{i=1}^{n} \mathrm{Tr}_i(\zeta_i x))^2.$$

This family of presemifields is related to a subfamily of the symplectic spreads constructed by Calderbank, Cameron, Kantor, and Seidel (1997). It is worth noting that this family of presemifield is a generalization of the presemifields constructed by Knuth (1965a), on which the multiplication is defined as:

$$x * y = xy + (x\mathrm{Tr}(y) + y\mathrm{Tr}(x))^2, \tag{4.7}$$

corresponding to the presemifields $\mathbf{B}((\mathbb{F}_i)_0^1, (1))$. The planar function derived from Knuth's presemifield is $(x\mathrm{Tr}(x))^2$.

Next, we consider the equivalence between $(2^n, 2^n, 2^n, 1)$-RDSs and how an equivalence transformation affects the $\mathbb{F}_2^n$-representation h of a $(2^n, 2^n, 2^n, 1)$-RDS.

Let D_1 and $D_2 \subseteq G$ be two $(2^n, 2^n, 2^n, 1)$-RDSs. By definition, they are equivalent if there exists some $\alpha \in \mathrm{Aut}(G)$ and $a \in G$ such that $\alpha(D_1) = D_2 + a$, see Definition 1.14. When G is abelian, every element in $\mathrm{Aut}(G)$ can be expressed by a matrix, for a proof see Ranum (1907) or Hillar and Rhea (2006). In the case that G is C_4^n, the corresponding result is the following lemma, in which we use the same notations to denote the elements in $\mathbb{Z}/4\mathbb{Z}$ and those in C_4:

Lemma 4.8. *Let mapping* $\rho : \mathbb{M}_{n\times n}(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{Hom}(C_4^n, C_4^n)$ *be defined as:*

$$\rho(L)(a_0, \ldots, a_{n-1}) = L(a_0, \ldots, a_{n-1})^T.$$

Then ρ *is surjective. Furthermore,* $\rho(L)$ *is an automorphism of* C_4^n *if and only if* $(L \bmod 2)$ *is invertible.*

For instance, let β be an element of $\mathrm{Hom}(C_4^2, C_4^2)$ defined by $\beta(1,0) = (1,2)$ and $\beta(0,1) = (1,1)$. Then we take matrix

$$L = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},$$

and it follows that $\rho(L) = \beta$. As $(L \bmod 2)$ is invertible, β is an automorphism.

Define $*_h : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ by:

$$x *_h y := h(x+y) + h(x) + h(y) + x \odot y, \quad x, y \in \mathbb{F}_2^n, \tag{4.8}$$

where $x \odot y = (x_0y_0, x_1y_1, \ldots, x_{n-1}y_{n-1})$. The next result is an analogue to Theorem 1.70.

Theorem 4.9. *Let D_1 and D_2 be two $(2^n, 2^n, 2^n, 1)$-RDSs in C_4^n relative to C_2^n, and let $h_1, h_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be their normalized $\mathbb{F}_2^n$-representations, respectively. Then, there exists a matrix $L \in \mathbb{M}_{n\times n}(\mathbb{Z}/4\mathbb{Z})$ such that $D_2 = \rho(L)(D_1)$ if and only if*

$$M(x) *_{h_2} M(y) = M(x *_{h_1} y), \tag{4.9}$$

where M is defined by $(L \bmod 2)$ acting as an element of $\mathbb{M}_{n\times n}(\mathbb{F}_2)$.

Proof. By abuse of notation, we also use Ψ to denote a mapping from $\mathbb{M}_{n\times n}(\mathbb{F}_2)$ to $\mathbb{M}_{n\times n}(\mathbb{Z}/4\mathbb{Z})$, which acts on every entry of the matrix as the embedding $\psi : \mathbb{F}_2 \to \mathbb{Z}/4\mathbb{Z}$ with $\psi(0) = 0$ and $\psi(1) = 1$.

Let $L \in \mathbb{M}_{n\times n}(\mathbb{Z}/4\mathbb{Z})$ be such that $\alpha := \rho(L)$ is an automorphism. By Lemma 4.8, $U := (L \bmod 2)$ as an element of $\mathbb{M}_{n\times n}(\mathbb{F}_2)$ is invertible. Clearly there is $V \in \mathbb{M}_{n\times n}(\mathbb{F}_2)$ such that $L = U^\Psi + 2V^\Psi$. Then we have

$$\begin{aligned}
\alpha(\lfloor a, b \rfloor) &= \alpha(a^\Psi + 2b^\Psi) \\
&= (U^\Psi + 2V^\Psi)(a^\Psi + 2b^\Psi)^T \\
&= U^\Psi a^{\Psi T} + 2(U^\Psi b^{\Psi T} + V^\Psi a^{\Psi T}).
\end{aligned} \tag{4.10}$$

Let u_{ij} denote the (i,j) entry of U. Then by (4.1), the k-th entry of $U^\Psi a^{\Psi T}$ is

$$\begin{aligned}
\sum_{i=0}^{n-1} u_{ki}^\psi a_i^\psi &= u_{k0}^\psi a_0^\psi + u_{k1}^\psi a_1^\psi + \sum_{i=2}^{n-1} u_{ki}^\psi a_i^\psi \\
&= (u_{k0}a_0 + u_{k1}a_1)^\psi + 2(u_{k0}u_{k1}a_0a_1)^\psi + \sum_{i=2}^{n-1} u_{ki}^\psi a_i^\psi \\
&= (u_{k0}a_0 + u_{k1}a_1 + u_{k2}a_2)^\psi + \\
&\quad + 2(u_{k0}u_{k1}a_0a_1 + u_{k0}u_{k2}a_0a_2 + u_{k1}u_{k2}a_1a_2)^\psi + \sum_{i=3}^{n-1} u_{ki}^\psi a_i^\psi \\
&= (u_{k0}a_0 + \cdots + u_{k(n-1)}a_{n-1})^\psi + 2(\sum_{i<j} u_{ki}u_{kj}a_ia_j)^\psi.
\end{aligned}$$

It follows that

$$U^\Psi a^{\Psi T} = (Ua^T)^\Psi + 2(Q(U,a))^\Psi,$$

where the k-th coordinate of $Q(U,a)$ is $Q_k(U,a) = \sum_{i<j} u_{ki}u_{kj}a_ia_j$. Now (4.10) becomes

$$\begin{aligned}\alpha(\lfloor a,b\rfloor) =&(Ua^T)^\Psi + 2(Q(U,a))^\Psi + \\ &+2\left((Ub^T)^\Psi + 2(Q(U,b))^\Psi + (Va^T)^\Psi + 2(Q(V,a))^\Psi\right)\\ =&(Ua^T)^\Psi + 2((Ub^T)^\Psi + (Va^T)^\Psi + (Q(U,a))^\Psi)\\ =&(Ua^T)^\Psi + 2(Ub^T + Va^T + Q(U,a))^\Psi\\ =&\lfloor Ua^T, Ub^T + Va^T + Q(U,a)\rfloor \end{aligned} \tag{4.11}$$

Let M and N be linear mappings from $\mathbb{F}_2^n$ to itself, which are defined by $M(x) := Ux^T$ and $N(x) := Vx^T$, respectively. It follows from (4.11) that

$$\alpha(\lfloor x, h_1(x)\rfloor) = \lfloor M(x), M(h_1(x)) + N(x) + Q(M,x)\rfloor, \tag{4.12}$$

for any $x \in \mathbb{F}_2^n$.

"$\Rightarrow$" Now we assume $D_2 = \alpha(D_1)$, which means that for a given $y \in \mathbb{F}_2^n$ there is a unique $x \in \mathbb{F}_2^n$ such that

$$\lfloor y, h_2(y)\rfloor = \alpha(\lfloor x, h_1(x)\rfloor).$$

Together with (4.12), it becomes

$$\lfloor y, h_2(y)\rfloor = \lfloor M(x), M(h_1(x)) + N(x) + Q(M,x)\rfloor.$$

It follows that

$$h_2(M(x)) = M(h_1(x)) + N(x) + Q(M,x). \tag{4.13}$$

Let $M_k(x \odot y)$ be the k-th coordinate of $M(x \odot y)$. Noticing that

$$\begin{aligned}&Q_k(M, x+y) + Q_k(M,x) + Q_k(M,y) + M_k(x \odot y)\\ =&\sum_{i<j} a_{ki}a_{kj}((x_i+y_i)(x_j+y_j) + x_ix_j + y_iy_j) + \sum_i a_{ki}x_iy_i\\ =&\sum_i a_{ki}x_i \sum_j a_{kj}y_j\\ =&(M(x) \odot M(y))_k,\end{aligned}$$

together with (4.8) and (4.13), we have

$$\begin{aligned}&M(x) *_{h_2} M(y)\\ =&h_2(M(x+y)) + h_2(M(x)) + h_2(M(y)) + (M(x) \odot M(y))\\ =&M(h_1(x+y)) + N(x+y) + Q(M, x+y) +\\ &+ M(h_1(x)) + N(x) + Q(M,x) +\\ &+ M(h_1(y)) + N(y) + Q(M,y) + (M(x) \odot M(y))\\ =&M(h_1(x+y) + h_1(x) + h_1(y)) +\\ &+ (Q(M,x+y) + Q(M,x) + Q(M,y) + (M(x) \odot M(y)))\\ =&M(h_1(x+y) + h_1(x) + h_1(y)) + M(x \odot y)\\ =&M(x *_{h_1} y).\end{aligned}$$

"$\Leftarrow$" Assume that there is linear mapping $M : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that (4.9) holds. Let $U \in \mathbb{M}_{n\times n}(\mathbb{F}_2)$ be such that $Ux^T = M(x)$ for any $x \in \mathbb{F}_2^n$. Let $D_2' := \alpha'(D_1)$ with $\alpha' := \rho(U)$, and let h_2' be the $\mathbb{F}_2^n$-representation of D_2'. Similarly to the proof of "$\Rightarrow$" part, we have

$$h_2'(M(x)) = M(h_1(x)) + Q(M,x), \tag{4.14}$$

and

$$M(x) *_{h_2'} M(y) = M(x *_{h_1} y).$$

Furthermore as (4.9) also holds, we get $x *_{h_2'} y = x *_{h_2} y$, i.e.

$$h_2'(x+y) + h_2'(x) + h_2'(y) = h_2(x+y) + h_2(x) + h_2(y),$$

which implies that

$$(h_2 + h_2')(x+y) + (h_2 + h_2')(x) + (h_2 + h_2')(y) = 0,$$

for all x, y. Hence $N'(x) := h_2'(x) + h_2(x)$ is an additive function on $\mathbb{F}_2^n$. Letting $y := M(x)$, by (4.14) we have

$$\begin{aligned}\lfloor y, h_2(y)\rfloor &= \lfloor y, h_2'(y) + N'(y)\rfloor \\ &= \lfloor M(x), M(h_1(x)) + Q(M,x) + N'(M(x))\rfloor.\end{aligned}$$

Let $N := N'M$, and let $V \in \mathbb{M}_{n\times n}(\mathbb{F}_2)$ be such that $Vx^T = N(x)$ for any $x \in \mathbb{F}_2^n$. By taking $L := U^{\Psi} + 2V^{\Psi}$ and $\alpha := \rho(L)$, we see that (4.12) holds, which means

$$\lfloor y, h_2(y)\rfloor = \alpha(\lfloor x, h_1(x)\rfloor)$$

for any $x \in \mathbb{F}_2^n$ and $y = M(x)$. Therefore we have $D_2 = \alpha(D_1)$. □

Theorem 4.10. *Let D be a $(2^n, 2^n, 2^n, 1)$-RDS in C_4^n relative to C_2^n, $\lfloor a, b\rfloor \in C_4^n$, and let $h, \tilde{h} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the $\mathbb{F}_2^n$-representations of D and $D + \lfloor a, b\rfloor$, respectively. Then we have*

$$x *_{\tilde{h}} y = h(x+y+a) + h(x+a) + h(y+a) + b + x \odot y, \ \text{for } x, y \in \mathbb{F}_2^n.$$

Proof. As $\tilde{h}$ is the $\mathbb{F}_2^n$-representation of $D + \lfloor a, b\rfloor$, for any $x \in \mathbb{F}_2^n$ there is a unique $y \in \mathbb{F}_2^n$ such that

$$\lfloor x + a, h(x) + b\rfloor = \lfloor y, \tilde{h}(y)\rfloor.$$

Hence, $\tilde{h}(x) = h(x+a) + b$ for any $x \in \mathbb{F}_2^n$. It follows that

$$\begin{aligned}x *_{\tilde{h}} y =& \tilde{h}(x+y) + \tilde{h}(x) + \tilde{h}(y) + x \odot y \\ =& h(x+y+a) + h(x+a) + h(y+a) + b + x \odot y,\end{aligned}$$

for any $x, y \in \mathbb{F}_2^n$. □

4.2 Coordinatization

Let D be a $(2^n, 2^n, 2^n, 1)$-RDS in C_4^n relative to $N = C_2^n$, and let h be an $\mathbb{F}_2^n$-representation of D with $h(0) = 0$ (if $h(0) \neq 0$, then take $D - \lfloor 0, h(0) \rfloor$ instead of D). Let $\mathbf{P}(D)$ be the plane defined by D as in Result 1.57. By using the method of Hughes and Piper (1973, Chapter V), we label the points of $\mathbf{P}(D)$ by the elements in $\mathbb{F}_2^n \times \mathbb{F}_2^n$, $\mathbb{F}_2^n$ and by the symbol ∞.

(i) Take three lines $l_x := D$, $l_y := N$ and l_∞ to form a triangle, and label three points: $(0,0) := l_x \cap l_y$, $(\infty) := l_y \cap l_\infty$ and $(0) := l_x \cap l_\infty$.

(ii) Assign (1) to the intersection point J of l_∞ and the affine parallel class $\{D + \lfloor 1, k \rfloor : k \in \mathbb{F}_2^n\}$ (here $1 \in \mathbb{F}_2^n$ is the vector $(0, 0, \ldots, 1)$ for short).

(iii) Label the point $\lfloor 0, y \rfloor$ on l_y with $(0, \tau(y))$, where $\tau : 1 * x \mapsto x$ and $* := *_h$ is defined by (4.8).

(iv) Let $Y = (0, y)$ be a point on l_y, and label $JY \cap l_x$ by $(x, 0)$. Let us consider what is the label for a given point $\lfloor y, h(y) \rfloor$ on l_x. Line JY is the set $D + \lfloor 1, k \rfloor$ for some $k \in \mathbb{F}_2^n$, which satisfies

$$(D + \lfloor 1, k \rfloor) \cap N = \{\lfloor 0, 1 * y \rfloor\}.$$

Solving equation

$$\lfloor u, h(u) \rfloor + \lfloor 1, k \rfloor = \lfloor 0, 1 * y \rfloor,$$

i.e.

$$\lfloor u + 1, h(u) + k + u \odot 1 \rfloor = \lfloor 0, 1 * y \rfloor,$$

we have $u = 1$ and

$$k = h(1) + 1 \odot 1 + 1 * y. \tag{4.15}$$

Similarly, $(D + \lfloor 1, k \rfloor) \cap D$ leads to an equation

$$\lfloor a + 1, h(a) + k + a \odot 1 \rfloor = \lfloor b, h(b) \rfloor,$$

and we have

$$k = h(b + 1) + (b + 1) \odot 1 + h(b).$$

Together with (4.15), we have

$$h(b + 1) + b \odot 1 + h(b) = h(1) + 1 * y.$$

Hence, $1 * b = 1 * y$, i.e. $b = y$. That means the point $\lfloor y, h(y) \rfloor$ on l_x is labeled with $(0, y)$.

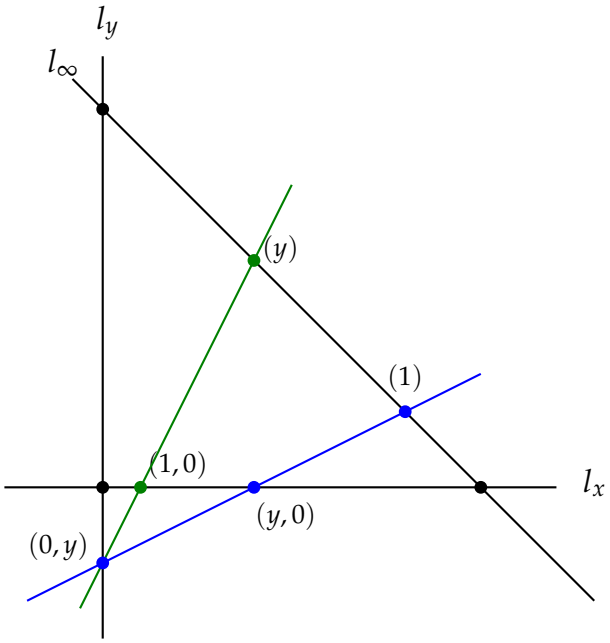

Figure 4.1: Steps (iv) and (v)

(v) For each line through $(1,0)$, which intersects l_y at $(0,m)$, assign (m) to its intersection with l_∞. Let $D+\lfloor v,k\rfloor$ be the set corresponds to this line. Then $\lfloor 1,h(1)\rfloor$ and $\lfloor 0,1*m\rfloor$ are both in $D+\lfloor v,k\rfloor$. It follows that

$$\begin{aligned} h(1) &= h(v+1)+k+(v+1)\odot v, \\ 1*m &= h(v)+k+v\odot v, \end{aligned}$$

which means $1*m = h(v+1)+h(v)+1\odot v+h(1) = 1*v$, i.e. $v=m$.

(vi) For each point E not on l_x, l_y or l_∞, if $XE\cap l_y$ is $(0,y)$ and $YE\cap l_x$ is $(x,0)$, then E is given the coordinate (x,y).

Let T be a planar ternary operation on $\mathbb{F}_2^n$ defined as follows: For $m,a,b\in\mathbb{F}_2^n$, $T(m,a,b)=k$ if and only if (a,b) is on a line, which contains (m) and $(0,k)$.

Mappings $\theta_c : (a,b)\mapsto(a,b+c)$ for $c\in\mathbb{F}_2^n$ form a collineation group on $\mathbf{P}(D)$, and this group is isomorphic to N. It follows that $\mathbf{P}(D)$ is $((\infty),l_\infty)$-transitive. As Hughes and Piper (1973, Theorem 6.2) showed, $(\mathbb{F}_2^n,T)$ is linear with associative addition. That means addition $a+b:=T(1,a,b)$ is the same as addition on the vector space $\mathbb{F}_2^n$. We define multiplication

$$m\star a := T(m,a,0).$$

Now we assume that $D+\lfloor v,w\rfloor$ is a line l through $(a,0)$ and (m) for some $v,w\in\mathbb{F}_2^n$. By Step (v) above, we see that $v=m$. As $(a,0)$ corresponds to $\lfloor a,h(a)\rfloor$, we have $\lfloor a,h(a)\rfloor\in D+\lfloor m,w\rfloor$, i.e. there is $y\in\mathbb{F}_2^n$ such that

$$\lfloor a,h(a)\rfloor = \lfloor y+m,h(y)+w+m\odot y\rfloor,$$

from which we can deduce that $y = m + a$ and

$$w = h(m + a) + h(a) + m + m \odot a = m * a + h(m) + m.$$

Hence the unique element in $(D + \lfloor m, w \rfloor) \cap N$ is

$$\lfloor 0, h(m) + w + m \odot m \rfloor = \lfloor 0, m * a \rfloor.$$

It follows that the intersection point of l and l_y is labeled with $(0, \tau(m * a))$. Hence,

$$m \star a = \tau(m * a). \tag{4.16}$$

Next we consider the conditions, under which Π is a semifield plane.

Theorem 4.11. *Let D be a $(2^n, 2^n, 2^n, 1)$-RDS in C_4^n relative to C_2^n. Let $h : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the normalized $\mathbb{F}_2^n$-representation of D, and let $* := *_h$ and $\star$ be defined by* (4.8) *and* (4.16). *Let $f_B(x)$ be the normalized $\mathbb{F}_{2^n}$-representation of D with respect to a basis B. Then the followings are equivalent:*

(a) $(\mathbb{F}_2^n, \star, +)$ *is a commutative semifield;*

(b) $(\mathbb{F}_2^n, *, +)$ *is a commutative presemifield;*

(c) $h(x + y + z) + h(x + y) + h(x + z) + h(y + z) + h(x) + h(y) + h(z) = 0$, *for all* $x, y, z \in \mathbb{F}_2^n$;

(d) Every component function of $h(x)$ is of degree at most two;

(e) $f_B(x)$ is a Dembowski-Ostrom polynomial;

(f) $\mathbb{P}(D)$ is a commutative semifield plane.

Remark 4.12. It is not trivial to show the equivalence between (a) and (f): Assume that we know (f) holds, i.e. $\mathbb{P}(D)$ can be coordinatized by isotopic semifields. However, there seems to be no apparent reason why the planar ternary ring $(\mathbb{F}_2^n, \star, +)$ has to be one of these semifields.

Proof. We only need to prove the distributivity of $*$ and $\star$ for one side since they are both commutative.

Assume that $*$ defines the multiplication of a presemifield. Then $x \mapsto 1 * x$ is an additive mapping by the distributivity of $*$, so is its inverse $\tau : 1 * x \mapsto x$. Therefore we have

$$\begin{aligned}
&(x + y) \star z - x \star z - y \star z \\
=&\tau((x + y) * z) - \tau(x * z) - \tau(y * z) \\
=&\tau(x * z + y * z - x * z - y * z) \\
=&0,
\end{aligned}$$

for all $x,y,z \in \mathbb{F}_2^n$, from which we deduce the distributivity of $\star$, i.e. we have (b)⇒(a).

Next, we assume that $\star$ defines the multiplication of a commutative semifield. Let $g(x) := x \star x$. As $x * x = x$, we get

$$g(x) = \tau(x * x) = \tau(x),$$

and

$$\begin{aligned} g(x+y) =& (x+y) \star (x+y) \\ =& x \star x + x \star y + y \star x + y \star y \\ =& x \star x + y \star y \\ =& g(x) + g(y) \end{aligned}$$

by the distributivity and commutativity of $\star$. Hence τ is also an additive mapping, so is its inverse. Therefore, $(x+y) * z = \tau^{-1}((x+y) \star z) = \tau^{-1}(x \star z + y \star z)$ $= x * z + y * z$, i.e. (a)⇒(b).

(b)⇔(c): It follows directly from the expansion of $(x+y) * z = x * z + y * z$.

(d)⇒(b): If (d) holds, then we see that for fixed $y \neq 0$ every component function of $x \mapsto x * y$ is an additive mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. It implies the distributive property of the multiplication $*$.

(b)⇒(d): Consider a component function of $x * y$, which defines a bilinear form $B(x,y) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$. By the relationship between quadratic forms and bilinear forms, wee see that the corresponding component functions of h must be of degree at most 2.

(d)⇔(e): As $f_B(x)$ and $h(x)$ are both normalized, $f_B(x)$ is a Dembowski-Ostrom polynomial if and only if all components of $h(x)$ are of degree ≤ 2 (here 0 is also considered as a Dembowski-Ostrom polynomial).

(a)⇒(f): It is directly from the definition.

(f)⇒(a): Assume that $\mathbf{P}(D)$ is a commutative semifield plane, i.e. by coordinatizing $\mathbf{P}(D)$ in an appropriate way, a commutative semifield $(\mathbb{F}_2^n, \diamond, +)$ can be obtained. Now we label the points and lines of $\mathbf{P}(D)$ in another way which is different from the coordinatization at the beginning of this section. Let $(x,y)_\diamond$ denote the affine points of $\mathbf{P}(D)$ with $x,y \in \mathbb{F}_2^n$, and the affine lines are point sets

$$[m,k]_\diamond := \{(x,y)_\diamond : m \diamond x + y = k\} \text{ with } m,k \in \mathbb{F}_2^n,$$

and

$$[k]_\diamond := \{(k,y)_\diamond : y \in \mathbb{F}_2^n\} \text{ with } k \in \mathbb{F}_2^n.$$

Every parallel class of affine lines corresponds to a point, and all such points form the line $\tilde{l}_\infty$ of $\mathbf{P}(D)$. There are 4^n bijections

$$\alpha_{ab} : (x,y)_\diamond \mapsto (x+a, y+a \diamond x+b)_\diamond \text{ with } a,b \in \mathbb{F}_2^n,$$

which are collineations of $\mathbf{P}(D)$ and together form a shift group $\tilde{G}$. Furthermore, as Knarr and Stroppel (2009, Theorem 9.4) showed, every shift group of $\mathbf{P}(D)$ is of the form

$$\tilde{G}_s := \{(x,y)_\diamond \mapsto (x+a, y+(a\diamond s)\diamond x+b)_\diamond : a,b \in \mathbb{F}_2^n\},$$

where s belongs to the middle nucleus of $(\mathbb{F}_2^n, \diamond, +)$. It follows that there exists s_0, such that $\tilde{G}_{s_0}$ and G act on $\mathbf{P}(D)$ in the same way. Let $[m,k]_\diamond$ be an arbitrary affine line, $[m,k]_\diamond$ is mapped to $[m+a\diamond s, k+(m+a\diamond s)\diamond a+b]_\diamond$ under an element of $\tilde{G}_s$ for some a,b, which means that all affine lines form an orbit under $\tilde{G}_s$. Hence $\tilde{l}_\infty$ is the unique line fixed by $\tilde{G}_{s_0}$. Since l_∞ is also fixed by G, we see that $\tilde{l}_\infty$ and l_∞ are the same line. On the other hand, by the distributive law of $(\mathbb{F}_2^n, \diamond, +)$, we have the collineations

$$\beta_{ab} : (x,y)_\diamond \mapsto (x+a, y+b)_\diamond \quad \text{with } a,b \in \mathbb{F}_2^n,$$

which act regularly on the affine points of $\mathbf{P}(D)$ and fix the line $\tilde{l}_\infty$ pointwise. It means that $\tilde{l}_\infty = l_\infty$ is a translation line. Therefore, as Hughes and Piper (1973, corollary of Theorem 6.3) showed, $(\mathbb{F}_2^n, \star, +)$ satisfies the left distributive law. Together with the commutativity of $\star$, we see that $(\mathbb{F}_2^n, \star, +)$ is a commutative semifield. □

Corollary 4.13. *Let D_1 and D_2 be two $(2^n, 2^n, 2^n, 1)$-RDSs in C_4^n relative to C_2^n, which define commutative semifields and 0 is in both D_1 and D_2. If there exists $\alpha \in \mathrm{Aut}(C_4^n)$ and $g \in C_4^n$ such that $\alpha(D_1) = D_2 + g$, then there is also some $\beta \in \mathrm{Aut}(C_4^n)$ such that $\beta(D_1) = D_2$.*

Proof. Let h_i be the $\mathbb{F}_2^n$-representation of D_i for $i = 1, 2$, and let $\lfloor a, b \rfloor = g$. Since $0 = \lfloor 0, 0 \rfloor \in D_1, D_2$ we have $b = h_2(a)$. Let $\tilde{h}_2$ be the $\mathbb{F}_2^n$-representation of $D_2 + g$. Then by Theorem 4.10 and Theorem 4.11(c), we have

$$\begin{aligned} x *_{\tilde{h}_2} y &= h_2(x+y+a) + h_2(x+a) + h_2(y+a) + h_2(a) + x \odot y \\ &= h_2(x+y) + h_2(x) + h_2(y) + x \odot y \\ &= x *_{h_2} y. \end{aligned}$$

Let $\alpha := \rho(L)$, and let M be the linear mapping defined by $(L \bmod 2)$ (see Theorem 4.9). Then

$$M(x *_{h_1} y) = M(x) *_{\tilde{h}_2} M(y) = M(x) *_{h_2} M(y).$$

Thus by Theorem 4.9, there is some $\beta \in \mathrm{Aut}(C_4^n)$ such that $\beta(D_1) = D_2$. □

By Theorem 4.11, we can obtain a non-translation plane by a non-Dembowski-Ostrom polynomial $f(x)$ which acts as a planar function on $\mathbb{F}_{2^n}$. Hence we propose the following open problem:

Problem 4.1. Find a non-Dembowski-Ostrom planar polynomial $f(x) \in \mathbb{F}_{2^n}[x]$, or prove the nonexistence of it.

Finally, we show the relationship between the equivalence of RDSs and the isotopism of the corresponding semifields:

Theorem 4.14. *Let D_1 and D_2 be two $(2^n, 2^n, 2^n, 1)$-RDSs in C_4^n relative to C_2^n, such that 0 is an element of both D_1 and D_2. Let h_1 and h_2 be their $\mathbb{F}_2^n$-representations, respectively, and let $*_{h_1}$ and $*_{h_2}$ be defined by* (4.8)*. For $i = 1, 2$, assume that $(\mathbb{F}_{2^n}, +, \star_{h_i})$ is a commutative semifield (see* (4.16) *for its definition). Then $(\mathbb{F}_{2^n}, +, \star_{h_1})$ is isotopic to $(\mathbb{F}_{2^n}, +, \star_{h_2})$ if and only if D_1 is equivalent to D_2.*

Proof. Since $0 \in D_1$ and D_2, we have $h_1(0) = h_2(0) = 0$. If D_1 and D_2 are equivalent, then by Corollary 4.13 there exists $\alpha \in \mathrm{Aut}(C_4^n)$ such that $\alpha(D_1) = D_2$. By Theorem 4.9, there is $M(x) *_{h_2} M(y) = M(x *_{h_1} y)$ for some linear permutation $M : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Together with $x \star_{h_i} y = \tau_{h_i}(x *_{h_i} y)$ where $\tau_{h_i} : 1 *_{h_i} x \mapsto x$, we obtain

$$\tau_{h_2}^{-1}(M(x) \star_{h_2} M(y)) = M(\tau_{h_1}^{-1}(x \star_{h_1} y)).$$

It implies that $(\mathbb{F}_{2^n}, +, \star_{h_1})$ and $(\mathbb{F}_{2^n}, +, \star_{h_2})$ are isotopic.

On the contrary, if $(\mathbb{F}_{2^n}, +, \star_{h_1})$ is isotopic to $(\mathbb{F}_{2^n}, +, \star_{h_2})$, then by Corollary 2.14 (a) they are strongly isotopic. It follows that the presemifields $(\mathbb{F}_{2^n}, +, *_{h_1})$ and $(\mathbb{F}_{2^n}, +, *_{h_2})$ are also strongly isotopic, i.e. there exist $M, L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$M(x) *_{h_1} M(y) = L(x *_{h_2} y),$$

which is

$$\begin{aligned} &h_1 \circ M(x+y) + h_1 \circ M(x) + h_1 \circ M(y) + M(x) \odot M(y) \\ =&L(h_2(x+y) + h_2(x) + h_2(y) + x \odot y). \end{aligned}$$

Notice that for each quadratic function $h : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $i = 0, 1, \ldots, n-1$, the term $x_i y_i$ can never appear in the components of $h(x+y) + h(x) + h(y)$, hence we have

$$M(x) \odot M(y) = L(x \odot y).$$

Let $x = y = e_i$, which denotes the vector with a 1 in the i-th coordinate and 0's elsewhere. We have

$$M(e_i) = M(e_i) \odot M(e_i) = L(e_i \odot e_i) = L(e_i)$$

for each $i = 0, 1, \ldots, n-1$, which means that $M = L$. Thus

$$\big(M(x) *_{h_1} M(y)\big) = M(x *_{h_2} y).$$

By Theorem 4.9, we see that D_1 and D_2 are equivalent. □

Remark 4.15. Theorem 4.14 is the counterpart of Theorem 1.70, from which we know that when p is odd, the equivalence between RDSs from commutative semifields is equivalent to the strong isotopism between the commutative semifields.

4.3 Nonexistence results for Boolean planar functions

Definition 4.6 shows us that there are many planar functions on $\mathbb{F}_2^m$, where m has at least one odd divisor larger than 1. Actually Kantor (2003) proved that the number of non-isotopic (pre)semifields defined in Definition 4.6 is not bounded by a polynomial in $N = 2^m$, see Conjecture 1.49 and the comments after it. As the chain of fields in Definition 4.6 is of odd length, another quite natural research problem arises as follows:

Problem 4.2. Construct "many" semifields with cardinality 2^{2^n}.

In order to find more planar functions, especially non-Dembowski-Ostrom planar functions, one strategy is to do some "small modifications" to known planar functions, which preserve the planar property. In this section, we consider the Boolean planar functions, or more generally, planar functions f with $\mathrm{Im}(f) = \{0, \xi\}$. They can be considered as a "small modification" of the planar function $g = 0$.

Lemma 4.16. *Let f be a mapping on $\mathbb{F}_{2^n}$, let $\xi \in \mathbb{F}_{2^n}^*$ and suppose that $\mathrm{Im}(f) = \{0, \xi\}$. Then f is a planar mapping, if and only if, for all $a \neq 0$ and x,*

$$f(x+a) + f(x) + f(x + a + \frac{\xi}{a}) + f(x + \frac{\xi}{a}) = 0. \tag{4.17}$$

Proof. If f is planar, then for all $a \neq 0$,

$$f(x+a) + f(x) + ax \neq f(x + a + \frac{\xi}{a}) + f(x + \frac{\xi}{a}) + ax + \xi,$$

which is equivalent to

$$f(x+a) + f(x) + f(x + a + \frac{\xi}{a}) + f(x + \frac{\xi}{a}) \neq \xi.$$

As $\mathrm{Im}(f) \in \{0, \xi\}$, we obtain (4.17).

Next we suppose that f is not a planar function. By definition, there exist $a, x, y \in \mathbb{F}_{2^n}$ satisfying $x \neq y$ and $a \neq 0$ such that

$$f(x+a) + f(x) + xa = f(y+a) + f(y) + ya.$$

Since $\mathrm{Im}(f) = \{0, \xi\}$ and $xa \neq ya$, we have $xa + \xi = ya$, which means that $y = x + \xi/a$ and

$$f(x+a) + f(x) + f(x + a + \frac{\xi}{a}) + f(x + \frac{\xi}{a}) = \xi. \qquad \square$$

Given $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we define

$$\mathcal{A}_f := \{(a, b) : f(x+a) + f(x) + f(x+b+a) + f(x+b) = 0\}. \tag{4.18}$$

The sets $\{0\} \times \mathbb{F}_{2^n}$, $\mathbb{F}_{2^n} \times \{0\}$ and $\{(a, a) : a \in \mathbb{F}_{2^n}\}$ are all contained in $\mathcal{A}_f$. It follows from Lemma 4.16 that $\{(a, \xi/a) : a \in \mathbb{F}_{2^n}^*\} \subseteq \mathcal{A}_f$, if f is a planar function satisfying $\mathrm{Im}(f) = \{0, \xi\}$. We can also prove the following relations between the elements of $\mathcal{A}_f$.

Lemma 4.17. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. There are binary operations $\wedge, \vee : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that*

(a) If $(a,b),(a+b,c) \in \mathcal{A}_f$, then $(a,b) \wedge (a+b,c) = (a+b,b+c) \in \mathcal{A}_f$.

(b) If $(a,b),(a,c) \in \mathcal{A}_f$, then $(a,b) \vee (a,c) = (a,b+c) \in \mathcal{A}_f$.

Proof. We just prove the first case. Since $(a,b),(a+b,c) \in \mathcal{A}_f$, we have

$$\begin{aligned} f(x+a)+f(x)+f(x+b+a)+f(x+b) &= 0 \\ f(x+a+b)+f(x)+f(x+c+a+b)+f(x+c) &= 0. \end{aligned}$$

Summing these equations, we get

$$\begin{aligned} f(x+c+a+b)+f(x+c)+ \\ +f((x+c)+(b+c)+(a+b))+f((x+c)+(b+c))=0, \end{aligned}$$

which means that $(a+b,b+c) \in \mathcal{A}_f$. □

If f is a planar function satisfying $\mathrm{Im}(f) = \{0,\xi\}$, then we have

$$\{(a,\xi/a) : a \in \mathbb{F}_{2^n}^*\} \subseteq \mathcal{A}_f$$

by Lemma 4.16. Thus, for $(a_0,\xi/a_0) \in \mathcal{A}_f$ with $a_0 \neq 0$, if $a_0 + \xi/a_0 \neq 0$, i.e. $a_0 \neq \sqrt{\xi}$, then we also have $(a_0+\xi/a_0, \xi/(a_0+\xi/a_0)) \in \mathcal{A}_f$. Hence we can define $b_0 := \xi/a_0$ and

$$(a_{i+1},b_{i+1}) := (a_i,b_i) \wedge \left(a_i+b_i, \frac{\xi}{a_i+b_i}\right) = \left(a_i+b_i, b_i+\frac{\xi}{a_{i+1}}\right),$$

and all these (a_i,b_i) are contained in $\mathcal{A}_f$ by Lemma 4.17 (a). Furthermore, from the definition of (a_i,b_i), we have

$$a_{i+1} = a_i + b_i = a_{i-1} + \frac{\xi}{a_i}, \tag{4.19}$$

from which we deduce that $(a_i : i = 0,1,\dots)$ is cyclic, if $a_i \neq 0$ for any $i \geq 0$.

Now we show that there is no i such that $a_i = 0$. Let us assume the opposite and see what happens. Suppose that i is the smallest integer such that $a_{i+1} = 0$. As $a_0 \neq 0, \sqrt{\xi}$, we see that $i \geq 2$. By (4.19) we have $a_{i-1} = \xi/a_i$ and

$$a_i = a_{i-2} + \frac{\xi}{a_{i-1}} = a_{i-2} + \frac{\xi}{\xi/a_i},$$

which means $a_{i-2} = 0$. This is a contradiction to the assumption about i.

As $b_i = b_{i+1} + \xi/a_{i+1}$ and $a_i = a_{i+1} + b_i = a_{i+1} + \xi/a_{i+1} + b_{i+1}$, the sequence $((a_i,b_i) : i = 0,1,\dots)$ is also cyclic. Furthermore, from (4.19) and

$$b_i = a_i + a_{i+1} = a_{i-1} + a_i + \frac{\xi}{a_i},$$

we can deduce that a_{i-1} and a_i determine b_i. Hence the period of $((a_i,b_i) : i = 0,1,\dots)$ is the same as the period of $(a_i : i = 0,1,\dots)$.

Lemma 4.18. *Let $a \in \mathbb{F}_{2^n}$ and $a \neq 0, \sqrt{\xi}$. Let $a_0 := a$, $a_1 := a + \xi/a$ and define sequence $S_a = (a_i : i = 0, 1, \dots)$ by*

$$a_{i+1} := a_{i-1} + \frac{\xi}{a_i}. \tag{4.20}$$

Then

$$a_{2i} = a\left(\frac{a^2}{a^2+\xi}\right)^i, \quad a_{2i+1} = a\left(\frac{a^2+\xi}{a^2}\right)^{i+1}, \tag{4.21}$$

and the period N of S_a is $2 \cdot \mathrm{ord}(1 + \xi/a^2)$.

Proof. Since every $a_i \neq 0$, by (4.20) we have that

$$a_{i+1}a_i = a_i a_{i-1} + \xi,$$

together with $a_0 a_1 = a^2 + \xi$ and $a_1 a_2 = a^2$ we can prove that

$$\frac{a_0}{a_{2i}} = \frac{a_0 a_1}{a_1 a_2}\frac{a_2 a_3}{a_3 a_4} \cdots \frac{a_{2i-2}a_{2i-1}}{a_{2i-1}a_{2i}} = \left(\frac{a^2+\xi}{a^2}\right)^i,$$

and

$$\frac{a_1}{a_{2i+1}} = \left(\frac{a^2}{a^2+\xi}\right)^i.$$

Therefore we get (4.21) and $\mathrm{ord}(1 + \xi/a^2) \mid N$. To prove $N = 2 \cdot \mathrm{ord}(1 + \xi/a^2)$, we only have to show that $2 \cdot \mathrm{ord}(1 + \xi/a^2)$ is the smallest positive integer N such that $a_N = a_0$ and $a_{N+1} = a_1$. If N is even, then by (4.21) and $2 \nmid \mathrm{ord}(1 + \xi/a^2)$, we have $N = 2 \cdot \mathrm{ord}(1 + \xi/a^2)$; If N is odd, let $N = 2k + 1$. As $a_{2k+1} = a_0 = a$, we have $k + 1 = \mathrm{ord}(1 + \xi/a^2)$, which means that

$$a_{N+1} = a_{2k+2} = a\left(\frac{1}{1+\xi/a^2}\right)^{k+1} = a \neq a_1.$$

Therefore N can not be odd, and $N = 2 \cdot \mathrm{ord}(1 + \xi/a^2)$. □

Lemma 4.19. *Let f be a mapping from $\mathbb{F}_{2^n}$ to itself satisfying $f(0) = 0$. Then f is an additive mapping if and only if $\mathcal{A}_f = \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.*

Proof. If f is additive, then for each $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ we have

$$f(x + a) + f(x) + f(x + b + a) + f(x + b) = f(a) + f(a) = 0.$$

Hence $\mathcal{A}_f = \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

If $\mathcal{A}_f = \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, then for each given a,

$$f(x + a) + f(x) + f(y + a) + f(y) = 0,$$

which means the mapping $x \mapsto f(x + a) + f(x)$ is constant. Pluging $x = 0$ in it, we see that the constant is $f(a) + f(0) = f(a)$. Hence $f(x + a) = f(x) + f(a)$ for any $x \in \mathbb{F}_{2^n}$. □

Now we can prove the following theorem.

Theorem 4.20. *Let f be a mapping from $\mathbb{F}_{2^n}$ to itself with $f(0)=0$. Let ξ be a nonzero element in $\mathbb{F}_{2^n}$. Write*

$$\mathcal{P}_n := \{1/(1+\alpha) : \alpha \text{ is a primitive element of } \mathbb{F}_{2^n}\} \cup \{1\}.$$

If $\mathcal{P}_n$ spans $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ (as a vector space), then the following statements are equivalent:

(a) $\{(a, \xi/a) : a \in \mathbb{F}_{2^n}\} \subseteq \mathcal{A}_f$;

(b) f *is an additive mapping.*

Proof. By Lemma 4.19, we only need to show that, if $\{(a,\xi/a) : a \in \mathbb{F}_{2^n}^*\} \subseteq \mathcal{A}_f$ then $\mathcal{A}_f = \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

If $\alpha = 1 + \xi/a^2$ is a primitive element, then by Lemma 4.18 the period of sequence $(a_i : i = 0, 1, \dots)$ is $2(2^n-1)$. It follows that every $c \in \mathbb{F}_{2^n}^*$ appears exactly twice in S_a, and one of the corresponding indices of $a_i = c$ is odd, the other is even. Fix c and assume that $a_k = c$. By (4.21), we have

$$a_k a_{k+1} = \begin{cases} a^2, & k \text{ is odd;} \\ a^2 + \xi, & k \text{ is even.} \end{cases}$$

Note that $a^2 = \xi/(1+\alpha)$, it follows that

$$(a_k, a_{k+1}) = \begin{cases} \left(c, \frac{\xi}{c}\frac{1}{1+\alpha}\right), & k \text{ is odd;} \\ \left(c, \frac{\xi}{c}\frac{\alpha}{1+\alpha}\right), & k \text{ is even.} \end{cases}$$

Since $(a_k, a_k + a_{k+1}) = (a_k, b_k) \in \mathcal{A}_f$ and $(a_k, a_k) \in \mathcal{A}_f$, by Lemma 4.17 (b), we have $(a_k, a_k + a_{k+1}) \vee (a_k, a_k) = (a_k, a_{k+1}) \in \mathcal{A}_f$. Therefore,

$$\left\{ \left(c, \frac{\xi}{c}\frac{1}{1+\alpha}\right) : \alpha \text{ is a primitive element of } \mathbb{F}_{2^n} \right\} \subseteq \mathcal{A}_f,$$

and

$$\left\{ \left(c, \frac{\xi}{c}\frac{\alpha}{1+\alpha}\right) : \alpha \text{ is a primitive element of } \mathbb{F}_{2^n} \right\} \subseteq \mathcal{A}_f.$$

It follows from Lemma 4.17 (b) that $(c, d\xi/c) \in \mathcal{A}_f$, where d is a linear combination of elements in $\mathcal{P}_n$. Therefore if $\mathcal{P}_n$ span $\mathbb{F}_{2^n}$, we have $\mathcal{A}_f \supseteq \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, i.e. f is additive by Lemma 4.19. □

Let $\mathrm{Tr}_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be the trace mapping. Notice that $\mathcal{P}_n$ spans $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if and only if the points of $\mathcal{P}_n$ are not contained in any hyperplane of $\mathrm{AG}(n,2)$. It holds if and only if for every $\beta \in \mathbb{F}_{2^n}^*$, there exists some $a \in \mathcal{P}_n$ such that $\mathrm{Tr}_n(\beta a) = 1$. This actually holds for $n \geq 18$ by setting $q = 2$, $r = m = l = 1$, $f_1(x) = \frac{\beta}{x+1}$ and $t_1 = 1$ in the following theorem due to Cohen (2005).

Theorem 4.21. *Let $f_1(x), \ldots, f_r(x) \in \mathbb{F}_{q^n}(x)$ form a strongly linearly independent set over $\mathbb{F}_q$ with $\deg f_i \leq m$, $i = 1, \ldots, r$ and let $t_1, \ldots, t_r \in \mathbb{F}_q$ be given. Also let l be any divisor of $q^n - 1$. Suppose that*

$$n > 4(r + \log_q(9.8l^{3/4}rm)).$$

Then there exists an element $\gamma \in \mathbb{F}_{q^m}$ of order $(q^n - 1)/l$ such that

$$\mathrm{Tr}_n(f_{\gamma_i}(\gamma)) = t_i, \qquad i = 1, \ldots, r.$$

To be *strongly linearly independent* over $\mathbb{F}_q$ means that only the all-zero $\mathbb{F}_q$-linear combination of $f_1, \ldots, f_r$ can be written in the form $h(x)^p - h(x) + \theta$ for some $h(x) \in \mathbb{F}_{q^n}(x)$ and $\theta \in \mathbb{F}_{q^n}$, where p is the characteristic of $\mathbb{F}_q$. When $q = 2$, $r = 1$ and $f_1(x) = \frac{\beta}{x+1}$, we assume that $\{f_1(x)\}$ is not strongly linearly independent. It follows that there are relatively prime polynomials $u(x), v(x) \in \mathbb{F}_{2^n}[x]$ and $\theta \in \mathbb{F}_{2^n}$ such that

$$f_1(x) = \left(\frac{u(x)}{v(x)}\right)^2 + \frac{u(x)}{v(x)} + \theta.$$

Then we have

$$u(x)(u(x) + v(x))(x + 1) = v^2(x)(\beta + \theta(x + 1)). \tag{4.22}$$

As $u(x)$ and $v(x)$ are coprime, from (4.22) we get $u(x) \mid (\beta + \theta(x + 1))$. Let $u(x) = a(\beta + \theta(x + 1))$ for some $a \in \mathbb{F}_{2^n}^*$. Then by canceling $(\beta + \theta(x + 1))$ on both sides of (4.22), we have

$$a(u(x) + v(x))(x + 1) = v^2(x). \tag{4.23}$$

Let $v(x) = b(x + 1)$ for some $b \in \mathbb{F}_{2^n}^*$. Plugging $u(x)$ and $v(x)$ into (4.23), we have

$$a(a(\beta + \theta) + a\theta x + bx + b)(x + 1) = b^2(x + 1)^2.$$

It follows that $(x + 1) \mid ((a\theta + b)x + a(\beta + \theta) + b)$, which means $a\beta = 0$. It contradicts $\beta \neq 0$ and $a \neq 0$. Hence $\{f_1(x)\}$ is strongly linearly independent.

Using a MAGMA program, we showed that $\mathcal{P}_n$ also spans $\mathbb{F}_{2^n}$ for $n < 18$. Hence, we can remove the condition on $\mathcal{P}_n$ in Theorem 4.20.

Theorem 4.20.* Let n be a positive integer and f be a mapping on $\mathbb{F}_{2^n}$ satisfying $f(0) = 0$ and $\mathrm{Im}(f) = \{0, \xi\}$ with $\xi \neq 0$. Then f is a planar mapping if and only if f is additive.

4.4 Shifted-bent functions

We define $f : \mathbb{F}_2^n \to \mathbb{F}_2$ to be a *shifted-bent* (or *bent$_4$*) *function* with respect to $\Lambda \subseteq \{0, 1, \ldots, n - 1\}$, if the function

$$f(x + a) + f(x) + \sum_{i \in \Lambda} x_i a_i \tag{4.24}$$

is balanced (the image set contains 0 and 1 equally often) for all $a \neq (0,\ldots,0)$, where $x = (x_0,\ldots,x_{n-1})$ and $a = (a_0,\ldots,a_{n-1})$. We call Λ the *shift index set* of f. When Λ is empty, shifted-bent functions are called *bent* functions. When $\Lambda = \{0,1,\ldots,n-1\}$, the shifted-bent function is also called *nega-bent*.

Remark 4.22. In fact, bent$_4$ and nega-bent functions are defined by Riera and Parker (2006) through a generalization of the Walsh transform.

Proposition 4.23. *Let D be a subset of C_4^n which forms a transversal for C_2^n in C_4^n. Let $h = (h_0,\ldots,h_{n-1})$ be its $\mathbb{F}_2^n$-representation, where $h_i : \mathbb{F}_2^n \to \mathbb{F}_2$ (for $i = 0,\ldots,n-1$) are the coordinate functions of h. Then D is a $(2^n,2^n,2^n,1)$-RDS in C_4^n relative to C_2^n if and only if for each nonempty subset $\Lambda \subseteq \{0,\ldots,n-1\}$, $\sum_{i\in\Lambda} h_i$ is a shifted-bent function with respect to Λ.*

Proof. Subset $D \subseteq C_4^n$ is an RDS in C_4^n relative to C_2^n if and only if the mapping $\Delta_{h,a}(x)$ (see (4.3)) is bijective. It holds if and only if each component function of $\Delta_{h,a}(x)$, which is defined by

$$x \mapsto \sum_{i\in\Lambda} (h_i(x+a) + h_i(x) + a_i x_i)$$

for nonempty subset $\Lambda \subseteq \{0,1,\ldots,n-1\}$, is balanced. It is equivalent to that for any $\Lambda \neq \varnothing$, $\sum_{i\in\Lambda} h_i$ is a shifted-bent function with respect to Λ. □

Example 4.24. Proposition 4.23 shows us that shifted-bent functions are the ingredients to build $(2^n,2^n,2^n,1)$-RDSs. Let us take a look at those $h_i : \mathbb{F}_2^4 \to \mathbb{F}_2$ defined in Example 4.5. For instance, $h_2(x) = x_0x_1 + x_0x_2 + x_1x_3$ is a shifted-bent function with respect to $\Lambda = \{2\}$ by Proposition 4.23. We can also get it by showing that the function

$$h_2(x+a) + h_2(x) + a_2x_2 = x_0(a_1+a_2) + x_1(a_0+a_3) + x_2(a_0+a_2) + x_3a_1$$

is balanced if and only if $(a_0,a_1,a_2,a_3) \neq (0,0,0,0)$. It follows from Proposition 4.23 that

$$\sum_{i=0}^{3} h_i(x) = x_0x_1 + x_0x_3 + x_1x_2 + x_2x_3$$

is a nega-bent function from $\mathbb{F}_2^4$ to $\mathbb{F}_2$. □

According to Lemma 1.66, the projection of a $(2^n,2^n,2^n,1)$-RDS into the subgroup $C_4 \times C_2^{n-1}$ of C_4^n is a $(2^n,2,2^n,2^{n-1})$-RDS in $C_4 \times C_2^{n-1}$ relative to $2C_4 \times \{0\}^{n-1}$. For convenience, we will say "$C_4 \times C_2^{n-1}$ relative to $2C_4$" instead of "$C_4 \times C_2^{n-1}$ relative to $2C_4 \times \{0\}^n$".

Theorem 4.25. *Let g be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let Λ be a nonempty subset of $\{i_j : j = 0,1,\ldots,n-1\} = \{0,1,\ldots,n-1\}$ such that $i_0 \in \Lambda$. Let φ be the embedding of C_2 in C_4 (see the beginning of Section 4.1). Then*

$$D_g := \left\{ \left((\sum_{i\in\Lambda} x_i)^\varphi + 2(g(x))^\varphi, x_{i_1},\ldots,x_{i_{n-1}} \right) : (x_{i_0},\ldots,x_{i_{n-1}}) \in \mathbb{F}_2^n \right\}$$

forms a $(2^n, 2, 2^n, 2^{n-1})$*-RDS in* $C_4 \times C_2^{n-1}$ *relative to* $2C_4$ *if and only if* g *is a shifted-bent function with respect to* Λ.

Proof. Without loss of generality, we assume that $i_j = j$ for $j = 0, \ldots, n-1$. Hence $0 = i_0 \in \Lambda$. By definition, D_g is a $(2^n, 2, 2^n, 2^{n-1})$-RDS if and only if for each $a \neq (0, \ldots, 0)$, the image set of mapping

$$x \mapsto \left((\sum_{i\in\Lambda}(x_i + a_i))^\varphi + 2(g(x+a))^\varphi - \left((\sum_{i\in\Lambda} x_i)^\varphi + 2(g(x))^\varphi \right), a_1, \ldots, a_{n-1} \right)$$

covers all the elements in $\{(z, a_1, \ldots, a_{n-1}) : z \in \{1, 3\} \subseteq C_4\}$ exactly 2^{n-1} times. It is equivalent to that

$$(\sum_{i\in\Lambda} a_i)^\varphi + 2(g(x+a) + g(x) + \sum_{i\in\Lambda} a_i x_i)^\varphi$$

covers all the elements in $\{1, 3\} \subseteq C_4$ exactly 2^{n-1} times for any given $a \neq 0$. It holds if and only if g is a shifted-bent function with respect to Λ. □

Let D be a $(2^n, 2, 2^n, 2^{n-1})$-RDS in $C_4 \times C_2^{n-1}$ relative to $2C_4$. It follows that D must be a transversal for $2C_4 \times C_2^{n-1}$ in $C_4 \times C_2^{n-1}$. Hence, there always exists $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$D = \{ (x_0^\varphi + 2(f(x))^\varphi, x_1, x_2, \ldots, x_{n-1}) : x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n \}.$$

By Theorem 4.25, f is a shifted-bent function with respect to $\Lambda_f := \{0\}$. Therefore, there is no essentially difference between shifted-bent functions with different nonempty shift index set Λ. In another word, given a nonempty subset $\Lambda_g \subseteq \{0, \ldots, n-1\}$. We can always derive a shifted-bent function g with respect to Λ_g from a shifted-bent function f with respect to $\{0\}$, and vice versa.

Without loss of generality, we assume that $\Lambda_g = \{0, 1, \ldots, m-1\}$, otherwise, we permutate $\{x_0, x_1, \ldots, x_{n-1}\}$. Now we assume that f is given. Let $\bar{x}_0 := x_0 + x_1 + \cdots + x_{m-1}$. We define $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ as

$$g(x_0, x_1, \ldots, x_{n-1}) := f(\bar{x}_0, x_1, \ldots, x_{n-1}) + \sum_{0<i<j<m} x_i x_j. \tag{4.25}$$

Then g is a shifted-bent function with respect to Λ_g, because

$$\begin{aligned}
&g(x_0 + a_0, x_1 + a_1, \ldots, x_{n-1} + a_{n-1}) + g(x_0, x_1, \ldots, x_{n-1}) + \sum_{i=0}^{m-1} a_i x_i \\
=&f(\bar{x}_0 + \bar{a}_0, x_1 + a_1, \ldots, x_{n-1} + a_{n-1}) + \\
&+ f(\bar{x}_0, x_1, \ldots, x_{n-1}) + \sum_{0<i<j<m} (x_i a_j + a_i x_j + a_i a_j) + \sum_{i=0}^{m-1} a_i x_i \\
=&f(\bar{x}_0 + \bar{a}_0, x_1 + a_1, \ldots, x_{n-1} + a_{n-1}) + \\
&+ f(\bar{x}_0, x_1, \ldots, x_{n-1}) + \sum_{0<i<j<m} a_i a_j + \bar{a}_0 \bar{x}_0
\end{aligned}$$

which is balanced for any nonzero $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^n$. Conversely, given g and Λ_g, we can also get f by (4.25).

Given a subset $D \subseteq C_4 \times C_2^{n-1}$, from (1.6) we can get another necessary and sufficient condition for D being a $(2^n, 2, 2^n, 2^{n-1})$-relative difference set:

$$|\chi(D)|^2 = \begin{cases} 2^n, & \text{for } \chi_{|2C_4 \times \{0\}^{n-1}} \neq \chi_0; \\ 0, & \text{for } \chi_{|2C_4 \times \{0\}^{n-1}} = \chi_0 \text{ and } \chi \neq \chi_0; \\ 2^{2n}, & \text{for } \chi = \chi_0. \end{cases} \tag{4.26}$$

Let $R := \{(x, f(x)) : x \in \mathbb{F}_2^n\}$, where f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. By definition, f is a bent function, if and only if, R is a $(2^n, 2, 2^n, 2^{n-1})$-relative difference set in C_2^{n+1} relative to $\{0\}^n \times C_2$. By (1.6), it is equivalent to

$$|\chi(R)|^2 = \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax)+bf(x)} \right| = \begin{cases} 2^n, & \text{for } b = 1; \\ 0, & \text{for } a \neq 0 \text{ and } b = 0; \\ 2^{2n}, & \text{for } a = 0 \text{ and } b = 0. \end{cases}$$

where $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$. Since this condition always holds when $b = 0$, we only need to focus on

$$\left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax)+f(x)} \right|^2 = 2^n. \tag{4.27}$$

Next, we look at the relation between bent functions and shift-bent functions.

Theorem 4.26. *Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ where n is even. Let Λ be a nonempty subset of $\{0, 1, \ldots, n-1\}$. Then the following statements are equivalent:*

(a) f is a shifted-bent function with respect to Λ.

(b) $f + \sum_{i<j, i,j \in \Lambda} x_i x_j$ is a bent function.

Particularly, when $|\Lambda| = 1$, f is shifted-bent with respect to Λ if and only if f is bent.

Proof. Without loss of generality, we consider $\Lambda = \{0\}$. Other cases can be derived by using (4.25). Let D be a subset of $C_4 \times C_2^{n-1}$, which is defined by

$$D = \{ (x_0^\varphi + 2(f(x))^\varphi, x_1, x_2, \ldots, x_{n-1}) : x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n \}. \tag{4.28}$$

By Theorem 4.25, f is a shifted-bent function with respect to $\{0\}$ if and only if D is a $(2^n, 2, 2^n, 2^{n-1})$-RDS in $C_4 \times C_2^{n-1}$ relative to $2C_4$.

Given a character χ of $C_4 \times C_2^{n-1}$, if $\chi_{|2C_4 \times C_2^{n-1}} = \chi_0$ or $\chi = \chi_0$, then (4.26) holds. It χ satisfies $\chi_{|2C_4 \times C_2^{n-1}} \neq \chi_0$, then we can always find $\xi = \pm 1$ and $u = (u_0, \ldots, u_{n-1}) \in \mathbb{F}_2^n$ such that $\chi = \chi_{u,\xi}$, which is defined as

$$\chi_{u,\xi}\left(x_0^\varphi + 2b^\varphi, x_1, \ldots, x_{n-1}\right) := (-1)^{b+u \cdot x}\, i^{(\xi x_0^\varphi)},$$

where $x = (x_0, \ldots, x_{n-1})$, $u = (u_0, \ldots, u_{n-1})$ and $u \cdot x := u_0x_0 + \cdots + u_{n-1}x_{n-1}$. Hence

$$\begin{aligned}\chi_{u,\xi}(D) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+u\cdot x} i^{(\xi x_0^{\varphi})} \\ &= \sum_{x_0=0} (-1)^{f(x)+u\cdot x} + i^{\xi} \sum_{x_0=1} (-1)^{f(x)+u\cdot x} \\ &= v_0 + v_1 i^{\xi},\end{aligned}$$

where $v_i := \sum_{x_0=i}(-1)^{f(x)+u\cdot x}$.

(a) $\Rightarrow$ (b): When f is a shifted-bent function with respect to $\{0\}$. By (4.26), we know that

$$v_0^2 + v_1^2 = 2^n. \tag{4.29}$$

As both v_0 and v_1 are integers, we can assume that m is the largest integer such that $2^m \mid v_0$ and $2^m \mid v_1$. It follows that

$$\bar{v}_0^2 + \bar{v}_1^2 = 2^{n-2m},$$

where $\bar{v}_i := v_i/2^m$. If $n - 2m \geq 2$, then $\bar{v}_0^2 + \bar{v}_1^2 \equiv 0 \pmod 4$. This means 2 divides v_0 and v_1, which contradicts our assumption about m. As n is even, we have $n = 2m$. Therefore, one of v_0^2 and v_1^2 is 0, the other one is 2^n, and

$$\left| \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+u\cdot x} \right|^2 = |v_0 + v_1|^2 = 2^n,$$

which means that f is a bent function.

(b) $\Rightarrow$ (a): For given $u = (u_0, u_1, \ldots, u_{n-1})$, we have

$$(v_0 + v_1)^2 = 2^n, \tag{4.30}$$

because f is a bent function. Now we take $u' = (u_0 + 1, u_1, \ldots, u_{n-1})$, then

$$v_0' := \sum_{x_0=0} (-1)^{f(x)+u'\cdot x} = \sum_{x_0=0} (-1)^{f(x)+(u_0+1)x_0+\sum_{i=1}^{n-1} u_i x_i} = v_0.$$

Similarly we have $v_1' = -v_1$. It follows that

$$(v_0 - v_1)^2 = (v_0' + v_1')^2 = 2^n.$$

Together with (4.30), we have (4.29). It implies (4.26). Hence, f is a shifted-bent function with respect to $\{0\}$. □

Remark 4.27. From Theorem 4.26, we see the link between $(2^n, 2, 2^n, 2^{n-1})$-RDSs in $C_4 \times C_2^{n-1}$ relative to $2C_4$ and those in C_2^{n+1} relative to C_2. The proof of Theorem 4.26 for the nega-bent cases is due to Parker and Pott (2007, Theorem 12).

When n is odd, we can prove the following result which was shown by Su, Pott, and Tang (2012, Theorem 2) for the nega-bent case.

Theorem 4.28. *Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ where n is odd. For nonempty $\Lambda \subseteq \{0,1,\ldots,n-1\}$, we define $h(x) := f(x) + \sum_{i<j,i,j\in\Lambda} x_i x_j$ and*

$$R_h := \{\, (x, h(x)) : x \in \mathbb{F}_2^n \,\}$$

which can be seen as a subset of C_2^{n+1}. Define $\chi_u(R_h) := \sum_{x\in\mathbb{F}_2^n} (-1)^{h(x)+u\cdot x}$. Then the following statements are equivalent:

(a) f is shifted-bent with respect to Λ.

(b) $\chi_u(R_h) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ and $|\chi_u(R_h)| \neq |\chi_{\tilde{u}}(R_h)|$ where $\tilde{u} = (\tilde{u}_0, \ldots, \tilde{u}_{n-1})$ and

$$\tilde{u}_i := \begin{cases} u_i + 1, & \text{if } i \in \Lambda; \\ u_i, & \text{otherwise.} \end{cases}$$

(c) $g(x,y) := f(x) + \sum_{i<j,i,j\in\Lambda} x_i x_j + y \sum_{i\in\Lambda} x_i$ is a bent function from $\mathbb{F}_2^{n+1}$ to $\mathbb{F}_2$, where $y \in \mathbb{F}_2$.

Proof. We only prove the theorem for $\Lambda = \{0\}$. The proofs of other cases can be derived by using (4.25).

Since $\Lambda = \{0\}$, by definition $h(x) = f(x)$, $R_h = R_f$, $g(x,y) = f(x) + yx_0$ and $\tilde{u} = (u_0 + 1, u_1, \ldots, u_{n-1})$. As the proof of Theorem 4.26, D is defined by

$$D = \{\, (x_0^\varphi + 2(f(x))^\varphi, x_1, x_2, \ldots, x_{n-1}) : x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n \,\}.$$

By Theorem 4.25, f is a shifted-bent function with respect to $\{0\}$ if and only if D is a $(2^n, 2, 2^n, 2^{n-1})$-RDS in $C_4 \times C_2^{n-1}$ relative to $2C_4$. It holds if and only if $v_0^2 + v_1^2 = 2^n$ holds.

(a) $\Rightarrow$ (b): Now we have

$$v_0^2 + v_1^2 = 2^n.$$

As both v_0 and v_1 are integers, we can assume that m is the largest integer such that $2^m \mid v_0$ and $2^m \mid v_1$. It follows that

$$\bar{v}_0^2 + \bar{v}_1^2 = 2^{n-2m},$$

where $\bar{v}_i := v_i/2^m$. If $n - 2m \geq 2$, then $\bar{v}_0^2 + \bar{v}_1^2 \equiv 0 \pmod 4$. That means 2 divides v_0 and v_1, which contradicts our assumption about m. As n is odd, we have $n = 2m + 1$ and $v_0^2 = v_1^2 = 2^{n-1}$, i.e. $v_0, v_1 \in \{-2^{\frac{n-1}{2}}, 2^{\frac{n-1}{2}}\}$.

It follows that

$$\chi_u(R_h) = \chi_u(R_f) = \sum_{x_0=0} (-1)^{f(x)+u\cdot x} + \sum_{x_0=1} (-1)^{f(x)+u\cdot x} = v_0 + v_1 \in \{0, \pm 2^{\frac{n+1}{2}}\},$$

and

$$\chi_{\tilde{u}}(R_h) = \chi_{\tilde{u}}(R_f) = v_0 + \sum_{x_0=1} (-1)^{f(x)+u\cdot x+x_0} = v_0 - v_1.$$

Suppose that $|\chi_u(R_h)| = |\chi_{\tilde{u}}(R_h)|$, i.e. $|v_0 + v_1| = |v_0 - v_1|$. It follows that $v_0 = 0$ or $v_1 = 0$, and it is a contradiction.

(b) $\Rightarrow$ (a): Now $\chi_u(R_h) = v_0 + v_1$ and $\chi_{\tilde{u}}(R_h) = v_0 - v_1$ equals 0 or $\pm 2^{\frac{n+1}{2}}$. As $|\chi_u(R_h)| \neq |\chi_{\tilde{u}}(R_h)|$, we have

$$\begin{cases} v_0 + v_1 = 0, \\ v_0 - v_1 = \pm 2^{\frac{n+1}{2}}. \end{cases} \quad \text{or} \quad \begin{cases} v_0 + v_1 = \pm 2^{\frac{n+1}{2}}, \\ v_0 - v_1 = 0. \end{cases}$$

and all of them lead to $v_0^2 = v_1^2 = 2^{n-1}$. Therefore $v_0^2 + v_1^2 = 2^n$.

(b) $\Leftrightarrow$ (c): We looks at the character values of the set

$$\{\, (x, y, g(x, y)) : x \in \mathbb{F}_2^n, y \in \mathbb{F}_2 \,\} \subseteq \mathbb{F}_2^{n+2},$$

which is

$$\begin{aligned} \sum_{x,y} (-1)^{f(x)+yx_0+u\cdot x+vy} &= \sum_{x} (-1)^{f(x)+u\cdot x} + (-1)^{f(x)+u\cdot x+x_0+v} \\ &= \chi_u(R_f) + (-1)^v \chi_{\tilde{u}}(R_f), \end{aligned}$$

where $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2$. Function g is bent if and only if

$$|\chi_u(R_f) + (-1)^v \chi_{\tilde{u}}(R_f)| = 2^{\frac{n+1}{2}},$$

which is equivalent to (b). □

Theorem 4.26 and Theorem 4.28 show that we can always use bent functions to construct shifted-bent functions. Furthermore, the *algebraic degree* of a shifted-bent function f over $\mathbb{F}_2^n$ (the degree of the polynomial defined by f in $\mathbb{F}_2[x_0, \ldots, x_{n-1}]/(x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1})$) is bounded by $\lceil \frac{n}{2} \rceil$, because the algebraic degree of bent functions is bounded by $\lceil \frac{n}{2} \rceil$ due to Rothaus (1976). There are many constructions and results about bent functions, see the surveys by Dillon (1974), Colbourn and Dinitz (2007, Chapter VI.4) and Carlet (2010).

The following construction of shifted-bent function can be derived from the Maiorana-McFarland bent functions:

Theorem 4.29. *Let g be an arbitrary Boolean function on $\mathbb{F}_2^m$. We use $x \cdot y$ to denote the inner product of x and $y \in \mathbb{F}_2^m$. The mapping*

$$f : (x, y) \mapsto x \cdot \Pi(y) + g(y)$$

is shifted-bent with respect to any subset Λ of the indices of $\{y_i : i = 0, 1, \ldots, m-1\}$ if and only if Π is a permutation on $\mathbb{F}_2^m$.

Proof. Let Π_i be the i-th coordinate function of Π, for $(a,b) \neq (0,0)$ we have

$$f(x+a,y+b)+f(x,y)+\sum_{i\in\Lambda} y_i b_i \tag{4.31}$$
$$=\sum_{i=0}^{m-1} x_i(\Pi_i(y+b)+\Pi_i(y))+\sum_{i=0}^{m-1} a_i\Pi_i(y+b)+g(y+b)+g(y)+\sum_{i\in\Lambda} y_i b_i.$$

When $b=0$, this equals

$$\sum_{i=0}^{m-1} a_i\Pi(y),$$

which is balanced for all $a \neq 0$ if and only if Π is a permutation.

When $b \neq 0$, we only have to show that, if Π is a permutation, then (4.31) is balanced. For each given y, (4.31) defines a balanced Boolean function on $x \in \mathbb{F}_2^m$, since $\Pi(y+b)+\Pi(y) \neq 0$. Hence we prove the theorem. □

By Theorem 4.29, we can get "multi-dimension" shifted-bent functions:

Corollary 4.30. *Let g be an arbitrary mapping from $\mathbb{F}_{2^m}$ to itself. Let f be a mapping from $\mathbb{F}_{2^m}^2$ to $\mathbb{F}_{2^m}$ defined by*

$$f:(x,y)\mapsto x\Pi(y)+g(y).$$

Then every component function of f is shifted-bent with respect to an arbitrary subset of the indices of $\{y_i : i=0,1,\ldots,m-1\}$ if and only if Π is a permutation on $\mathbb{F}_{2^m}$.

We have already seen that the algebraic degree of shifted-bent functions can be larger than 2. Corollary 4.30 shows us that it is possible to combine them together to a "vectorial" one, i.e. a $(2^{2m},2^m,2^{2m},2^m)$-RDS in $C_4^m \times C_2^m$ relative to $2C_4^m \times \{0\}^m$. Actually, the function f in Corollary 4.30 is constructed by Chabaud and Vaudenay (1995). It is often called Maiorana-McFarland vectorial bent function, and it gives rise to a $(2^{2m},2^m,2^{2m},2^m)$-RDS in C_2^{3m} relative to C_2^m. However, we can not use vectorial bent functions to go further, because there is no abelian $(2^{2a},2^b,2^{2a},2^{2a-b})$-RDS in $G \times N$ relative to N if $b > a$, see a proof for the elementary abelian case by Nyberg (1994), and a proof for the general case by Schmidt (1997, Theorem 5.2).

Problem 4.1 is about the existence of a mapping $h : \mathbb{F}_2^n \to \mathbb{F}_2^n$ (the $\mathbb{F}_2^n$-representation), which is an n-dimensional combination of shifted-bent functions h_i with respect to shift index sets $\Lambda_i = \{i\}$ for $i = 0,1,\ldots,n-1$ and at least one of h_i is of degree larger than 2. We extend Problem 4.1 as follows:

Problem 4.3. For each n, what is the maximal m, such that Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 0,1,\ldots,m-1$ satisfy the following two conditions:

1. For each nonempty set $\Lambda \subseteq \{0,\ldots,m-1\}$, $\sum_{i\in\Lambda} f_i$ is a shifted-bent function with respect to Λ;

2. At least one of f_i's is non-quadratic?

Problem 4.1 is the case $m = n$. When n is even, by Theorem 4.26, Problem 4.3 can be rephrased as follows:

Problem 4.4. Let n be a positive even integer. What is the maximal m, such that bent functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 0, 1, \ldots, m-1$ satisfy the following two conditions:

1. For each nonempty set $\Lambda \subseteq \{0, \ldots, m-1\}$, $\sum_{i\in\Lambda} f_i + \sum_{i<j, i,j\in\Lambda} x_i x_j$ is a bent function;

2. At least one of f_i's is non-quadratic?

4.5 Notes

As the following contents involve ideas from Galois rings, error-correcting codes over rings and methods from algebraic geometry, we give a summary here.

First, by using Galois rings, we can also get the definition of planar functions from $\mathbb{F}_{2^n}$ to itself. First, we list several basic facts about Galois rings, which can be found in the text book by Wan (2003). Let $\mathrm{GR}(p^m, n)$ be a Galois ring, which is isomorphic to the ring $(\mathbb{Z}/p^m\mathbb{Z})[x]/(f(x))$ for any monic basic irreducible polynomial $f(x)$ of degree n over $\mathbb{Z}/p^m\mathbb{Z}$. (A monic polynomial $f(x) \in \mathbb{Z}/p^m\mathbb{Z}[x]$ is *basic irreducible* if $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$.) The multiplicative group of the units of $\mathrm{GR}(p^m, n)$ contains a unique cyclic subgroup $\mathcal{T}^*$ of order $p^n - 1$, called the *group of Teichmüller units*. We set $\mathcal{T} := \mathcal{T}^* \cup \{0\}$. Every element a of $\mathrm{GR}(p^m, n)$ can be written uniquely as

$$a = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1},$$

where $a_0, a_1, \ldots, a_{s-1} \in \mathcal{T}$. Moreover, c is a unit if and only if $a_0 \neq 0$.

Actually, $\mathrm{GR}(p^m, n)$ is also isomorphic to the ring $W_m(\mathbb{F}_{p^n})$ of *Witt vectors of lenght m over* $\mathbb{F}_{p^n}$, which is defined as the algebraic structure with underlying set $\mathbb{F}_{p^n}^m$ and two operations "$+$" and "$\cdot$", see Jacobson (1975) or Shanbhag, Kumar, and Helleseth (1998) for details. The isomorphism $\Gamma : \mathrm{GR}(p^m, n) \mapsto W_m(\mathbb{F}_{p^n})$ is given by $\Gamma(a) = (\bar{a}_0, \bar{a}_1^p, \ldots, \bar{a}_{m-1}^{p^{m-1}})$ where $a = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$, $a_i \in \mathcal{T}$ and $\bar{a}_i := a_i + (p) \in \mathrm{GR}(p^m, n)/(p) \cong \mathbb{F}_{p^n}$.

Now let us focus on $\mathrm{GR}(4, n)$, which is isomorphic to $W_2(\mathbb{F}_{2^n})$ with two operations

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1 + a_0 b_0),$$
$$(a_0, a_1) \times (b_0, b_1) = (a_0 b_0, a_0^2 b_1 + a_1 b_0^2).$$

The zero divisors of $W_2(\mathbb{F}_{2^n})$ are $\{\, (0, a_1) : a_1 \in \mathbb{F}_{2^n} \,\}$, which forms a group isomorphic to C_2^n under the addition. The Teichmüller set of $\mathrm{GR}(4, n)$, is mapped

to $\{\,(a_0,0) : a_0 \in \mathbb{F}_{2^n}\,\} \in W_2(\mathbb{F}_{2^n})$. Since the additive group of $\mathrm{GR}(4,n)$ is isomorphic to C_4^n and $\mathcal{T}$ forms a transversal for C_2^n in C_4^n, for any $(2^n,2^n,2^n,1)$-RDS D in C_4^n relative to C_2^n, we can write it as

$$D = \{\, x + 2\cdot g(x) : x \in \mathcal{T}\,\} \subseteq \mathrm{GR}(4,n),$$

where $g : \mathcal{T} \mapsto \mathcal{T}$. Furthermore, by Γ, it can also be viewed as

$$\overline{D} := \{\,(x, f(x)) : x \in \mathbb{F}_{2^n}\,\} \subseteq W_2(\mathbb{F}_{2^n}),$$

where $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is defined by $f(\bar{x}) = \overline{(g(x))}^{\,2^{n-1}}$ for $x \in \mathcal{T}$. It follows that D is a $(2^n,2^n,2^n,1)$-RDS if and only if the list of differences of $\overline{D} \subseteq W_2(\mathbb{F}_{2^n})$

$$\{\,(x+a, f(x+a)) - (x, f(x)) : x, a \in \mathbb{F}_{2^n} \text{ and } a \neq 0\,\}$$

i.e.

$$\{\,(a, f(x+a) + f(x) + ax) : x, a \in \mathbb{F}_{2^n} \text{ and } a \neq 0\,\}$$

covers all the element in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ except for $\{0\} \times \mathbb{F}_{2^n}$ once, which is equivalent to (4.5). When we take $f(x) = 0$, then D is exactly the Teichmüller set of $\mathrm{GR}(4,n)$.

Planar functions or $(2^n,2^n,2^n,1)$-RDSs have also been considered in the context of $\mathbb{Z}_4$-linear generalized Kerdock codes. Generalized means these codes have the same parameter but are not equivalent to the (nonlinear binary) classical Kerdock code presented by MacWilliams and Sloane (1977), which can be obtained from a $\mathbb{Z}_4$-linear code under the Gray mapping, for a proof see the seminal paper by Hammons, Kumar, Calderbank, Sloane, and Sole (1994). The Lee weight distribution of a given $\mathbb{Z}_4$-linear generalized Kerdock codes is actually equivalent to the character values $\{\,\chi(D) : \chi \in \widehat{C_4^n}\,\}$ of a subset $D \subseteq C_4^n$ derived from this code, for a proof see the recent result by Schmidt and Zhou (2013) which is a generalization of the proof for the classical Kerdock code case by Hammons, Kumar, Calderbank, Sloane, and Sole (1994, Theorem 13). The Techmüller set of $\mathrm{GR}(4,n)$ is showed to be a $(2^n,2^n,2^n,1)$-RDS in C_4^n relative to C_2^n by Hammons, Kumar, Calderbank, Sloane, and Sole (1994, Section 3.3) and Bonnecaze and Duursma (1997, Theorem 1), which is used to construct the classical $\mathbb{Z}_4$-linear Kerdock codes.

Generalized Kerdock codes can also be not $\mathbb{Z}_4$-linear, but with the same parameter. Calderbank, Cameron, Kantor, and Seidel (1997) have a construction which leads to many inequivalent $\mathbb{Z}_4$-nonlinear generalized Kerdock codes by using symplectic spreads.

Problem 4.1 was also presented in the context of $\mathbb{Z}_4$-linear Kerdock codes. Precisely speaking, one tries to find some nonlinear binary code which is not embedded in the Reed-Müller Code of order 2 but with the same parameters of $\mathbb{Z}_4$-linear Kerdock codes, see for instance the monograph by Carlet (2010).

Planar monomial functions, namely, functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ that can be written as $f(x) = cx^t$ for some $c \in \mathbb{F}_{2^n}^*$ and some integer t, are considered recently by Schmidt and Zhou (2013). An integer t satisfying $1 \leq t \leq 2^n - 2$ is a *planar exponent* of $\mathbb{F}_{2^n}$ if the function $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$. It is proved that $t = 2^k + 1$ is a planar exponent when $n = 2k$, and $t = 4^k(4^k + 1)$ is also a planar exponent when $n = 6k$, for proofs see the preprints by Schmidt and Zhou (2013) as well as Scherr and Zieve (2013). As the classification of the numbers that are planar exponents of $\mathbb{F}_2^n$ seems to be a challenging problem. This motivates us to study the related problem of classifying those numbers that are planar exponents of $\mathbb{F}_{2^n}$ for infinitely many n. This problem parallels the classifying monomial functions $x \mapsto x^t$ on $\mathbb{F}_{2^n}$ that are almost perfect nonlinear for infinitely many n. To attack this problem, Janwa, Mcguire, and Wilson (1995) proposed to use ideas from algebraic geometry. These ideas were further developed by Jedlicka (2007) and Hernando and McGuire (2011), leading to a complete solution. Schmidt and Zhou (2013) used a similar approach to prove the following result.

Theorem 4.31. *If t is an odd planar exponents of $\mathbb{F}_{2^n}$ for infinitely many n, then $t = 1$.*

Chapter 5

Sequences derived from projective planes

Clearly, if we'd had the kind of computer graphics capability then that we have now, the Star Gate sequence would be much more complex than flat planes of light and color.

Douglas Trumbull

Let $\mathbf{a} = (a_0, a_1, a_2, \ldots, a_n)$ be a complex sequence of period $n+1$. We call $\mathbf{a}$ an *m-ary sequence* if $a_i = \zeta_m^{b_i}$, where ζ_m is a primitive complex m-th root of unity and $b_i \in \{0, 1, \ldots, m-1\}$ for $0 \leq i \leq n$. The sequence $\mathbf{a}$ is called an *almost m-ary sequence* if we allow $a_0 = 0$. We can also allow another entry a_{i_0} of $\mathbf{a}$ to be 0, but it is equivalent to taking $a_0 = 0$ by left-shifting the sequence i_0 times.

For an (almost) m-ary sequence $\mathbf{a}$ with period $n+1$, the *autocorrelation coefficients* of $\mathbf{a}$ are

$$C_t(\mathbf{a}) := \sum_{i=0}^{n} a_i \overline{a_{i+t}} \quad \text{for } 0 \leq t \leq n,$$

where $\bar{\cdot}$ is the complex conjugate and all subscripts are computed modulo $n+1$. For all $t \not\equiv 0 \pmod{n+1}$, the $C_t(\mathbf{a})'$s are called *out-of-phase* autocorrelation coefficients, otherwise *in-phase* autocorrelation coefficients.

Motivated by applications in engineering, sequences with small out-of-phase coefficients are of particular interests. For many applications, one needs sequences $\mathbf{a}$ with a *two-level autocorrelation functions*, i.e. all out-of-phase autocorrelation coefficients are a constant γ. For an almost m-ary sequence $\mathbf{a}$, we call $\mathbf{a}$ *perfect* if it has a two-level autocorrelation function and $\gamma = 0$. Moreover, we call $\mathbf{a}$ *nearly perfect* if the out-of-phase autocorrelation coefficients γ all satisfy $\gamma = 1$, or they all satisfy $\gamma = -1$. We refer to the well-rounded survey on perfect binary sequences by Jungnickel and Pott (1999), to the paper by Ma and Ng (2009) for results on perfect and nearly perfect p-ary sequences, where p is an odd prime.

A square matrix H with entries ± 1 and order v is called a *Hadamard matrix* if $HH^T = vI$. A square matrix C with entries $0, \pm 1$ and order v is called a *conference*

matrix if $CC^T = (v-1)I$, where I is the identity matrix. It is well known that perfect binary (with entries ± 1) sequences of period v are equivalent to cyclic difference sets (see Jungnickel and Pott (1999, Section 2)). In particular, when $v \equiv 0 \pmod 4$, perfect binary sequences are equivalent to circulant Hadamard matrices, or cyclic Hadamard difference sets (see Schmidt (2002, Section 1.1)). More precisely, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be a binary sequence of period v. Let $H = (h_{i,j})_{i,j=0}^{v-1}$ be a circulant matrix (H is called *circulant* if $h_{i+1,j+1} = h_{i,j}$ for all i, j, where the indices of $h_{i,j}$ are calculated modulo v.) defined by $h_{0,j} = a_j$ for $j \in C_v$. Then H is a circulant Hadamard matrix of order v, if and only if, the sequence $\mathbf{a}$ is perfect. Similarly, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be an almost binary sequence, i.e. $a_0 = 0$ and $a_i = \pm 1$ for $1 \le i \le v-1$. Then the circulant matrix $C = (h_{i,j})_{i,j=0}^{v-1}$ defined by $h_{0,j} = a_j$ for $j \in C_v$ is a circulant conference matrix, if and only if, the sequence $\mathbf{a}$ is perfect. . The famous circulant Hadamard matrices conjecture is that there do not exist circulant Hadamard matrices if $v > 4$. In contract to this still open problem, an elegant and elementary proof by Stanton and Mullin (1976) shows that there do not exist circulant conference matrices: It seems that the mathematical behavior of binary perfect sequences and almost binary perfect sequences are quite different, which is one motivation of this chapter.

As shown by Ma and Ng (2009), a perfect p-ary sequence of period n is equivalent to a $(n, p, n, n/p)$-RDS in $C_n \times C_p$ relative to $\{0\} \times C_p$. Hence the classical examples come from the $(p, p, p, 1)$-RDSs for odd prime p. Inspired by this result, we study almost p-ary perfect sequences, where p is a prime. It turns out that almost p-ary perfect sequences of period $n+1$ are equivalent to $(n+1, p, n, (n-1)/p)$-RDSs in $C_{n+1} \times C_p$ relative to C_p (Theorem 5.6). Let D be an $(n+1, n-1, n, 1)$-RDS in $C_{n+1} \times C_{n-1}$ relative to C_{n-1} where n is a power of odd prime. The classical example R of $(n+1, p, n, (n-1)/p)$-RDS comes from the projection of D, i.e. $R = \varphi_{C_{n-1}}(D)$, see Result 1.67 (d).

The lack of examples of almost p-ary perfect sequences motivates our research in almost p-ary nearly perfect sequences. It is shown that periodic almost p-ary nearly perfect sequences correspond to certain direct product difference sets (Theorem 5.20).

This chapter is organized as follows. In Section 5.1, we introduce some tools and lemmas from algebraic number theory and algebraic combinatorics. The discussions about almost p-ary perfect and nearly perfect sequences are given in Section 5.2 and 5.3, respectively. In Appendix, we give two tables of the existence status of almost p-ary perfect and nearly perfect sequences with period less than 100. Our results extend those about perfect and nearly perfect p-ary sequences which have been done by Ma and Ng (2009), to the almost p-ary case. This chapter is based on the paper by Chee, Tan, and Zhou (2010).

5.1 Algebraic-combinatorial tools

In this section, we list some results from algebraic number theory and combinatorics.

A prime p is said to be *self-conjugate* modulo w if $p^j \equiv -1 \pmod{w'}$ for some j, where w' is the maximal p-free part of w, i.e. the maximal factor of w which is relatively prime to p. A composite integer m is said to be self-conjugate modulo w if every prime divisor of m is self-conjugate modulo w. The self-conjugate condition is quite useful in determining the existence of RDSs.

Result 5.1. Let p be a prime and ζ_w be a primitive w-th root of unity in $\mathbb{C}$, and let ϕ denote the Euler's phi function.

(a) If $w = p^e$, then the decomposition of the ideal (p) in $\mathbb{Z}(\zeta_w)$ into prime ideals is $(p) = (1-\zeta_w)^{\phi(w)}$.

(b) If $(w,p) = 1$, then the prime ideal decomposition of the ideal (p) in $\mathbb{Z}(\zeta_w)$ is $(p) = \pi_1 \cdots \pi_g$, where π_i's are distinct prime ideals. Furthermore, $g = \phi(w)/f$ where f is the order of p modulo w. The field automorphism induced by $\zeta_w \mapsto \zeta_w^p$ fixes the ideals π_i.

(c) If $w = p^e w'$ with $(w',p) = 1$, then the prime ideal (p) decomposes as $(p) = (\pi_1 \cdots \pi_g)^{\phi(p^e)}$ in $\mathbb{Z}(\zeta_w)$, where π_i's are distinct prime ideals and $g = \phi(w')/f$. If t is an integer not divisible by p and $t \equiv p^s \pmod{w'}$ for a suitable integer s, then the field automorphism $\zeta_w \to \zeta_w^t$ fixes the ideals π_i.

The following two lemmas are crucial in the proofs of our results in Section 5.2 and 5.3.

Lemma 5.2. *Let q be a prime and a be a positive integer. Let K be an abelian group such that either q does not divide $|K|$ or the Sylow q-subgroup of K is cyclic. Let L be any subgroup of K and $Y \in \mathbb{Z}[K]$ where the coefficients of Y lie between a and b where $a < b$. Suppose*

1. *q is self-conjugate modulo* $\exp(K)$*;*
2. *$q^r | \chi(Y)\overline{\chi(Y)}$ for all $\chi \notin L^\perp$ and $q^{r+1} \nmid \chi(Y)\overline{\chi(Y)}$ for some $\chi \notin L^\perp$;*
3. *$\chi(Y) \neq 0$ for some $\chi \notin L^\perp \cup Q^\perp$ where $Q = K$ if $q \nmid |K|$ and Q is the subgroup of K of order q otherwise. Here $L^\perp$ denotes the subset of the character group which is non-principal on L.*

Then the following statements hold:

(a) If $q \nmid |K|$, then r is even and $q^{\frac{r}{2}} \leq b - a$.

(b) If Sylow q-subgroup of K is cyclic, then $q^{\lfloor \frac{r}{2} \rfloor} \leq 2(b-a)$ *when L is a proper subgroup of* $|K|$ *and* $q^{\lfloor \frac{r}{2} \rfloor} \leq b-a$ *when* $L = K$.

Lemma 5.3. *Let* $G = \langle \alpha \rangle \times H$ *be an abelian group of exponent* $v = uw$, *where* $\mathrm{ord}(\alpha) = u, \exp(H) = w$ *and* $(u, w) = 1$. *Suppose* $y \in \mathbb{Z}[G]$ *and* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ *such that*

1. $\chi(y)\overline{\chi(y)} = n$ *for all characters* χ *of G such that* $\chi(\alpha) = \zeta_u$, *where n is an integer relatively prime to w; and*
2. σ *fixes every prime ideal divisor of* (n) *in* $\mathbb{Z}[\zeta_v]$.

If $\sigma(\zeta_v) = \zeta_v^t$, *then*

$$y^{(t)} = \pm \beta y + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i,$$

where $\beta \in G, x_1, \ldots, x_r \in \mathbb{Z}[G]$ *and* $p_1, \ldots, p_r$ *are all prime divisors of u.*

Furthermore, if u is even, then the sign $\pm$ *can be chosen arbitrarily by choosing appropriate* β.

Remark 5.4. Result 5.1 can be found in the monograph by Pott (1995, Result 1.2.7). Lemma 5.2 was proved by Ma and Ng (2009), and Lemma 5.3 is due to Arasu and Ma (1998).

5.2 Almost p-ary perfect sequences

In this section we construct almost p-ary perfect sequences, and we also prove that they cannot exist with certain periods. First we fix some notations which will be frequently used. Let p be a prime and let $G = H \times P$, where $H = \langle h \rangle$, $P = \langle g \rangle$, $\mathrm{ord}(h) = n+1$ and $\mathrm{ord}(g) = p$. For convenience, we say that H (resp. P), instead of $H \times \{1\}$ (resp. $\{1\} \times P$), is a subgroup of G. Let ζ_p be a primitive p-th root of unity. Let $\mathbf{a} = \{a_0, a_1, \ldots, a_n\}$ be an almost p-ary sequence of period $n+1$, where $a_0 = 0$ and $a_i = \zeta_p^{b_i}$ with $b_i \in \{0, 1, \ldots, p-1\}$ for $i = 1, 2, \ldots, n$.

Now we consider the following n-subset R of G

$$R = \{g^{b_i} h^i | i = 1, 2, \ldots, n\}, \tag{5.1}$$

from which we can deduce that

$$RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{j=1 \\ (\mathrm{mod}\ n+1)}}^{n} g^{b_{j+t} - b_j} h^t. \tag{5.2}$$

Lemma 5.5. *Let* χ *be a character of P and extend* $\chi : \mathbb{Z}[G] \longrightarrow \mathbb{Q}(\zeta_p)[H]$ *to be a ring epimorphism such that* $\chi(x) = x$ *for all* $x \in H$. *Then*

$$\chi(R)\chi(R^{(-1)}) = \begin{cases} \sum_{t=0}^{n} C_t(\mathbf{a})^{\sigma} h^t & \text{if } \chi \text{ is non-principal on } P, \\ 1 + (n-1)H & \text{if } \chi \text{ is principal on } P, \end{cases} \tag{5.3}$$

where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ *and* $\sigma(\zeta_p) = \chi(g)$.

Proof. If χ is principal on P, then $\chi(R)\chi(R^{(-1)}) = (H-1)^2 = 1+(n-1)H$. Otherwise, suppose $\chi(g) = \sigma(\zeta_p)$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, then the results follow from (5.2). □

Theorem 5.6. *Let $G := H \times P$, where $H \cong C_{n+1}$ and $P \cong C_p$. Let* **a** *be an almost p-ary sequence of period $n+1$, and let R be a subset of G defined by* (5.1). *Then* **a** *is perfect if and only if R is an $(n+1, p, n, (n-1)/p)$-RDS in G relative to P, i.e.*

$$RR^{(-1)} = n + \frac{n-1}{p}(G-P). \tag{5.4}$$

Proof. By Lemma 5.5, for all characters χ of G,

$$\chi(RR^{(-1)}) = \begin{cases} n, & \text{for } \chi_{|P} \neq \chi_0; \\ 1+(n-1)H, & \text{for } \chi_{|P} = \chi_0. \end{cases}$$

Now the result follows from (1.6). □

By Theorem 5.6, we get a necessary condition for the existence of almost p-ary perfect sequences with period $n+1$.

Corollary 5.7. *If there exists an almost p-ary perfect sequence of period $n+1$, then $p \mid n-1$.* □

We can get almost p-ary perfect sequences by applying Lemma 1.66 to the classical affine difference sets, see Result 1.67 (d).

Next we give several nonexistence results to show that almost p-ary perfect sequences do not exist with certain periods.

Result 5.8. Abelian splitting $(n+1, 2, n, (n-1)/2)$-relative difference sets do not exist.

By Theorem 5.6, we have the following result.

Corollary 5.9. *Almost binary perfect sequences of period $n+1$ do not exist.* □

Result 5.10. Let R be an abelian $(n+1, n-1, n, 1)$-RDS in G relative to N, then n should be a prime power for $n \leq 10,000$.

It follows from Result 5.10 that when $n-1$ is a prime, then there is no almost $(n-1)$-ary perfect sequence of period $n+1$.

Remark 5.11. Result 5.8 is due to Jungnickel (1990), and Result 5.10 was proved by Jungnickel and Pott (1989).

Using the technique of Ma and Ng (2009), we have the following result.

Theorem 5.12. *Let $G := H \times P$, where $H \cong C_{n+1}$ and $P \cong C_p$. Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to P. Assume that there exists a prime divisor $q \neq p$ of n, such that $q^r \parallel n$ for some r and q is self-conjugate modulo $p \cdot u$, where $u \mid (n+1)$. Then r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$.*

Proof. Let $\rho : G \to K := G/\langle h^u \rangle$ be the canonical epimorphism. Hence, $|K| = p \cdot u$. By (5.4), we have

$$\rho(R)\rho(R^{(-1)}) = n + \frac{n-1}{p}(\frac{n+1}{u}K - \rho(P)).$$

The coefficients of $\rho(R)$ lie between 0 and $\frac{n+1}{u}$ since $|\ker\rho| \leq \frac{n+1}{u}$. If χ is a non-principal character of K, then

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n, & \text{for } \chi_{|\rho(P)} \neq \chi_0; \\ 1, & \text{for } \chi_{|\rho(P)} = \chi_0. \end{cases} \tag{5.5}$$

Now we set $L := \rho(P)$ and $Y := \rho(R)$, and we verify the three conditions in Lemma 5.2:

1. q is self-conjugate modulo $p \cdot u$ by assumption.
2. It follows from (5.5) that $q^r \mid \chi(Y)\overline{\chi(Y)} = n$ for $\chi \notin L^\perp$.
3. By (5.5), we have $\chi(Y) \neq 0$ for some $\chi \notin L^\perp \cup K^\perp$.

As $q \mid n$ and $|K|$ divides $p \cdot (n+1)$, it follows that $q \nmid |K|$. By Lemma 5.2 (a), the theorem is proved. □

By taking $u = n+1$ and $u = 1$ in Theorem 5.12, respectively, the following two results can be directly derived.

Corollary 5.13. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo $p(n+1)$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.* □

Corollary 5.14. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo p. If $q^{2s+1} \parallel n$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.* □

The above results depend on the self-conjugate condition. Usually it is difficult to determine the existence status of almost p-ary perfect sequences if this condition is not satisfied. However, in some cases we can determine whether the almost p-ary perfect sequences exist or not when n is small. We briefly introduce the main idea of this method here. An (m, n, k, λ)-RDS is called *regular* if $k^2 \neq \lambda mn$. Let R be an RDS in G and let t be an integer with $\gcd(t, |G|) = 1$. Let t be a *(numerical) multiplier* of R if $R^{(t)} = Rg$ for some $g \in G$. Then Rg is also an RDS for any $g \in G$. By following result due to Pott (1995, Theorem 1.3.8), we may assume that R satisfies $R^{(t)} = R$ if R is regular.

Result 5.15. Let R be a regular (m, n, k, λ)-RDS and let t be a multiplier of R. Then there exists at least one translate Rg such that $(Rg)^{(t)} = Rg$.

Let Ω be the set of orbits of G under the group automorphism $x \mapsto x^t$. Since $R^{(t)} = R$, we see that R is the union of elements in Ω, namely

$$R = \bigcup_{\omega \in \Phi} \omega,$$

where $\Phi \subseteq \Omega$. A natural way to construct R is to combine the elements in Ω. On the one hand, if there does not exist a subset Φ of Ω such that $|\bigcup_{\omega\in\Phi} \omega| = |R|$, then clearly R does not exist. On the other hand, to construct R, we may find suitable Φ with $|\bigcup_{\omega\in\Phi} \omega| = |R|$ and verify whether $\bigcup_{\omega\in\Phi} \omega$ is an RDS. The next result gives a way to find multipliers of RDSs.

Theorem 5.16. *Let $G := H \times P$, where $H \cong C_{n+1}$ and $P \cong C_p$. Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to P, where p is an odd prime. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$ be the prime decomposition of n. For $1 \le i \le l$, let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ defined by $\sigma_i(\zeta) = \zeta^{p_i}$, where ζ is a primitive $(n+1)p$-th root of unity. Let $\varphi \in \bigcap_{i=1}^{l} \langle\sigma_i\rangle$. If $\varphi(\zeta) = \zeta^t$, then t is a multiplier of R.*

Proof. By (5.4), we have $RR^{(-1)} = n + \frac{n-1}{p}(G - P)$. Let χ be a character of G such that $\chi(g) = \zeta_p$, then $\chi(R)\overline{\chi(R)} = n$. By Result 5.1, the prime ideal factorization of (n) in $\mathbb{Z}[\zeta_{(n+1)p}]$ is

$$(n) = (p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}) = \prod_{i=1}^{l} (P_{1,i} \cdots P_{s_i,i})^{r_i},$$

where $s_i = \phi((n+1)p)/f_i$ and $f_i = \mathrm{ord}_{(n+1)p}(p_i)$. By $\gcd(n, (n+1)p) = 1$ and Result 5.1 (b), we know that σ_i fixes the prime ideals $P_{j,i}$ for $1 \le j \le s_i$. Therefore, φ fixes all prime ideals $P_{j,i}$ for $1 \le j \le s_i$ and $1 \le i \le l$. By Lemma 5.3,

$$R^{(t)} = \pm\beta R + Px,$$

where $\beta \in G$ and $x \in \mathbb{Z}[G]$. Let χ_0 be the principal character of G, then

$$n = \chi_0(R^{(t)}) = \chi_0(\pm\beta R + Px) = \pm n + p\chi_0(x).$$

It follows that $\chi_0(x) = 0$ as $\gcd(p, n) = 1$. Next we show that x must be 0. As $|R| = |G/P| - 1$, we can assume that

$$R = \sum_{i=1}^{n} g^{\beta_i} h^i,$$

Table 5.1: Orbits of G under $x \mapsto x^2$

Length of orbit	number
1	1
3	2
11	2
33	4

where $0 \leq \beta_i \leq p-1$. Therefore we have $RP = G - P$. Now

$$\begin{aligned} R^{(t)}R^{(-t)} &= (\beta R + Px)(\beta R + Px)^{(-1)} \\ &= RR^{(-1)} + \beta x^{(-1)}RP^{(-1)} + \beta^{-1}xR^{(-1)}P + p\ xx^{(-1)}P \\ &= \left(n + \frac{n-1}{p}(G-P)\right) + \beta x^{(-1)}(G-P) + \beta^{-1}x(G-P) + pxx^{(-1)}P \\ &= n + \left(\frac{n-1}{p} + \beta x^{(-1)} + \beta^{-1}x\right)G - \\ &\quad - \left(\frac{n-1}{p} + \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1}\right)P. \end{aligned}$$

On the other hand, noticing that $\gcd(t, |G|) = 1$, we have

$$R^{(t)}R^{(-t)} = (RR^{(-1)})^{(t)} = (n + \frac{n-1}{p}(G-P))^{(t)} = n + \frac{n-1}{p}(G-P).$$

Therefore,

$$\begin{cases} \beta x^{(-1)} + \beta^{-1}x &= 0, \\ \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1} &= 0. \end{cases}$$

From above we have $xx^{(-1)} = 0$, which implies that $x = 0$. It follows that $R^{(t)} = \beta \cdot R$ for some $\beta \in G$, and the proof is completed. □

Next we give an example to disprove the existence of an almost p-ary perfect sequence by applying Theorem 5.16.

Example 5.17. There do not exist almost 7-ary perfect sequence with period 23.

Proof. First it can be verified that almost 7-ary perfect sequences with period 23 do not satisfy the conditions of Theorem 5.12. By Theorem 5.6, to prove nonexistence is equivalent to prove that there do not exist a $(23, 7, 22, 3)$-RDS, say R, in $G = C_{23} \times C_7$ relative to C_7. It can be checked that 2 is a multiplier of R by Theorem 5.16. Using MAGMA, we compute the orbits of G under the group automorphism $x \mapsto x^2$. The results are in Table 5.2.

We see that there is only one possible combination of orbits such that its cardinality is 22. However, this is not an RDS. □

Using similar arguments, we get the following result.

Theorem 5.18. *There do not exist almost p-ary perfect sequences of period $n+1$, where $p \mid (n-1)$ and $n \in \{22, 28, 45, 52, 77\}$.* □

It will become more difficult to determine the existence of RDSs using this method if the number of orbits gets larger. For $n = 50, 76, 94, 99$ and 100, we cannot use the above methods to show the nonexistence of almost p-ary perfect sequences of period $n+1$.

Recently, Özbudak, Yayla, and Yıldırım (2012) extended our method and proved the nonexistence of these cases.

Result 5.19. Almost p-ary perfect sequences of period $n+1$ do not exist for $n = 50, 76, 94, 99, 100$, where $p \mid (n-1)$.

Table 5.2 in Appendix lists the existence status of p-ary perfect sequences of period $n+1$ for $3 \leq n \leq 100$ and p is a prime divisor of $n-1$.

5.3 Almost p-ary nearly perfect sequences

An $(mn; m, n; k, \lambda; \lambda_1, \lambda_2)$-generalized difference set in a group G relative to H and N is also called an $(m, n, k, \lambda_1, \lambda_2, \lambda)$-direct product difference set relative to H and N, where $G = H \times N$, $|H| = m$ and $|N| = n$.

Now, let $G, H, P, \mathbf{a}$ have the same meaning as in Section 5.2. The sequence $\mathbf{a}$ is called an *almost p-ary nearly perfect sequence* (*NPS*) *of type I* (resp. II) if the out-of-phase autocorrelation coefficients are all -1 (resp. 1). Similar to Theorem 5.6, we have the following result.

Theorem 5.20. *Let $\mathbf{a} = (0, a_1, a_2, \ldots, a_n)$ be an almost p-ary sequence of period $n+1$, where $a_i = \zeta_p^{b_i}$ and $0 \leq b_i \leq p-1$ for $1 \leq i \leq n$. Let $G := H \times P$, where $H \cong C_{n+1}$ and $P \cong C_p$. Let $R = \sum_{i=1}^{n} g^{b_i} h^i$.*

(a) Sequence $\mathbf{a}$ is an almost p-ary NPS of type I if and only if R is an $(n+1, p, n, \frac{n}{p} - 1, 0, \frac{n}{p})$-direct product difference set in G relative to H and P.

(b) Sequence $\mathbf{a}$ is an almost p-ary NPS type II if and only if R is an $(n+1, p, n, \frac{n-2}{p} + 1, 0, \frac{n-2}{p})$-direct product difference set in G relative to H and P. □

From Theorem 5.20 we have the following necessary condition for the existence of almost p-ary NPSs.

Corollary 5.21. *(a) If there exists an almost p-ary NPS of period $n+1$ of type I, then $p \mid n$.*

(b) If there exists an almost p-ary NPS of period $n+1$ of type II, then $p \mid (n-2)$. □

Next we construct a family of almost p-ary NPSs of type I.

Result 5.22. Let q be a prime and let p be a prime divisor of $q-1$. Let H be the additive group of the finite field $\mathbb{F}_q$ and let N be the multiplicative group of $\mathbb{F}_q$. Let $G = H \times N \cong C_q \times C_{q-1}$. Define

$$D = \{ (x, x) | x = 0, 1, \ldots, q-2 \}.$$

By Theorem 1.62, R is a $(q, q-1, q-1, 0, 0, 1)$-direct product difference set in G relative to H and N (namely a $(q(q-1); q-1, q; q-1, 1; 0, 0)$-GDS, see Theorem 1.55). By (1.3),

$$DD^{(-1)} = q + (G - H - N). \tag{5.6}$$

Let $\rho : G \to G/M$ be the natural epimorphism and $R = \rho(D)$, where $M \leqslant N$ and $M \cong C_{\frac{q-1}{p}}$. Then by (5.6), we have $RR^{(-1)} = q - N/M + \frac{q-1}{p}(G/M - N/M)$, from which it follows that R is a $(q, p, q-1, \frac{q-1}{p} - 1, 0, \frac{q-1}{p})$-direct product difference set in $G/M \cong C_q \times C_p$ relative to $H/M \cong C_q$ and $N/M \cong C_p$. By Theorem 5.20 (a), there exists an almost p-ary NPS of type I with period q.

In the following we present results to show that almost p-ary NPSs of type I do not exist with certain periods.

Lemma 5.23. *Let n be an odd integer and $b_i \in \{0, 1, \ldots, n-1\}$ for $1 \leq i \leq n$. Assume that $b_i \neq b_j$ when $i \neq j$, then $|\{b_{i+1} - b_i | i = 1, 2, \ldots, n-1\}| < n-1$ ($b_i - b_j$ is computed modulo n).*

Proof. Let $S = \{b_{i+1} - b_i | i = 1, 2, \ldots, n-1\}$. Clearly $|S| \leq n-1$. Now assume that $|S| = n-1$, then $S = \{1, \ldots, n-1\}$ as $b_i \neq b_j$ for $i \neq j$. Therefore, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = \sum_{i=1}^{n-1} i \equiv \frac{n(n-1)}{2} \equiv 0 \pmod{n}$ as n is odd. On the other hand, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = b_n - b_1$. The contradiction arises as $b_i \not\equiv b_j \pmod{n}$. □

Theorem 5.24. *Let $G := H \times P$, where $H = \langle h \rangle \cong C_{n+1}$ and $P = \langle g \rangle \cong C_n$. If n is an odd integer, then there does not exist an $(n+1, n, n, 0, 0, 1)$-direct product difference set in G relative to H and P. Therefore, for any odd prime p, there do not exist almost p-ary NPSs of type I with period $p+1$.*

Proof. Assume that there is an $(n+1, n, n, 0, 0, 1)$-direct product difference set $R \subseteq G$ relative to H and P. Since $|R| = |G/P| - 1$ and no elements in P can be represented as the differences of elements in R, we can assume that $R = \sum_{i=1}^{n} g^{b_i} h^i$ and $b_i \in \{0, \ldots, n-1\}$. Similarly, as no elements in H can be represented as the differences of elements in R and $|P| = |R| = n$, we have $\{b_i | i = 1, \ldots, n\} = \{0, 1, \ldots, n-1\}$. Now

$$n + 1 + (G - H - P) = RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{i=1 \\ i \not\equiv -t \pmod{n+1}}}^{n} g^{b_{i+t} - b_i} h^t.$$

It follows that for each $t \neq 0$,

$$\{b_{i+t} - b_i : 1 \leq i \leq n | i \not\equiv -t \pmod{n+1}\} = \{1, \ldots, n-1\}.$$

However, by letting $t = 1$ and we see the above equation cannot hold by Lemma 5.23. □

By Lemma 5.2, we have the following result.

Theorem 5.25. *Let p be a prime, and let q be a prime divisor of $n+1$ such that $q^r \parallel (n+1), q \neq p$. Assume that q is self-conjugate modulo $p \cdot u$ for a divisor u of $n+1$. If there exists an almost p-ary NPS of type I with period $n+1$, then the followings hold*

(a) If $q \nmid p \cdot u$, then r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$.

(b) If $q \mid p \cdot u$, then $q^{\lfloor \frac{r}{2} \rfloor} \leq 2\frac{n+1}{u}$.

Proof. By Theorem 5.20, we can assume that there is an $(n+1, p, n, \frac{n}{p} - 1, 0, \frac{n}{p})$-direct product difference set R in $G = H \times P = \langle h \rangle \times \langle g \rangle \cong C_{n+1} \times C_p$ relative to H and P. Then

$$RR^{(-1)} = (n+1) - H + \frac{n}{p}(G - P). \tag{5.7}$$

Let $K := G/\langle h^u \rangle$, and it follows that $|K| = p \cdot u$. Let $\rho : G \to K$ be the natural epimorphism. It follows that $K = \rho(H) \times \rho(P)$, and the coefficients of $\rho(R) \in \mathbb{Z}[K]$ lie between 0 and $\frac{n+1}{u}$. From (5.7) we have

$$\rho(R)\rho(R)^{(-1)} = (n+1) - \rho(H) + \frac{n}{p}\left(\frac{n+1}{u}K - \rho(P)\right). \tag{5.8}$$

For any non-principal character χ of K, from (5.8) we have

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n+1, & \text{if } \chi_{|\rho(P)} \neq \chi_0 \text{ and } \chi_{|\rho(H)} \neq \chi_0; \\ 1, & \text{if } \chi_{|\rho(P)} = \chi_0 \text{ and } \chi_{|\rho(H)} \neq \chi_0; \\ 0, & \text{if } \chi_{|\rho(P)} \neq \chi_0 \text{ and } \chi_{|\rho(H)} = \chi_0. \end{cases} \tag{5.9}$$

Now, we take $L := \rho(P)$ and $Y := \rho(R)$, and we will show that the three conditions in Lemma 5.2 holds.

1. By assumption, we have that q is self-conjugate modulo $\exp(K) = p \cdot u$.
2. From (5.9), we have that $q^r | \chi(Y)(\overline{\chi(Y)})$ for all $\chi \notin L^\perp$, and $q^{r+1} \nmid \chi(Y)(\overline{\chi(Y)})$ for $\chi \notin \rho(H)^\perp \cup L^\perp$.
3. For $\chi \notin \rho(H)^\perp \cup Y^\perp$, we have $\chi(Y)\overline{\chi(Y)} = n+1$ from (5.9). It follows that if $q \nmid |K|$, then $\chi(Y) \neq 0$ for $\chi \notin \rho(H)^\perp \cup L^\perp \subseteq L^\perp \cup K^\perp$; If $q \mid |K|$, then $\chi(Y) \neq 0$ for $\chi \notin \rho(Q)^\perp \cup L^\perp$, where Q is the subgroup of K of order q.

Hence the result follows from Lemma 5.2. □

Corollary 5.26. *Let p be a prime. If there exists a prime divisor q of $n+1$ with $q^{2s+1} \parallel n+1$ and q is self-conjugate modulo p, then there do not exist almost p-ary NPSs of type I with period $n+1$.*

Proof. Now $u = 1$ in Theorem 5.25. It follows that $|K| = p$. By Theorem 5.25 (a), we finish the proof. □

Corollary 5.27. *Let p be a prime. Let q be a prime divisor of $n+1$ such that q is self-conjugate modulo $(n+1)p$. Assume that $q^r \mid n+1$ for $r \geq 4$ if $q = 2$. Then there do not exist almost p-ary NPSs of type I with period $n+1$.*

Proof. Now $u = n+1$ in Theorem 5.25. It follows from Theorem 5.25 (b) that $2^{\lfloor \frac{r}{2} \rfloor} \leq 2$. Hence r can not be larger than 3. □

For almost p-ary NPSs of type II with period $n+1$, we only find the example with $p = 2$ and $n = 2$, namely $\mathbf{a} = (0, 1, 1)$. We have done a computer search for $p = 3$ and $n \in \{2, 5, 8, 11, 14, 17\}$, and however, no example is found. We leave it as the following open problem.

Problem 5.1. Do almost p-ary NPSs of type II with period $n+1$ exist?

In Appendix, Table 5.3 lists the existence status of the almost p-ary NPSs of type I with period $n+1$ for $2 \leq n \leq 100$, where p is a prime divisor of n. The question mark "?" in the table is used to denote an undecided case.

5.4 Appendix

Table 5.2: Existence Status of Perfect Sequences

n	p	Existence Status	n	p	Existence Status
3	2	not exist by Corollary 5.9	4	3	exist by Result 1.67 (d)
5	2	not exist by Corollary 5.9	6	5	not exist by Corollary 5.14 with q=2
7	2	not exist by Corollary 5.9	7	3	exist by Result 1.67 (d)
8	7	exist by Result 1.67 (d)	9	2	not exist by Corollary 5.9
10	3	not exist by Corollary 5.14 with q=2	11	2	not exist by Corollary 5.9
11	5	exist by Result 1.67 (d)	12	11	not exist by Result 5.10
13	2	not exist by Corollary 5.9	13	3	exist by Result 1.67 (d)
14	13	not exist by Corollary 5.14 with q=2	15	2	not exist by Corollary 5.9
15	7	not exist by Corollary 5.14 with q=3	16	3	exist by Result 1.67 (d)
16	5	exist by Result 1.67 (d)	17	2	not exist by Corollary 5.9
18	17	not exist by Corollary 5.14 with q=2	19	2	not exist by Corollary 5.9

19	3	exist by Result 1.67 (d)	20	19	not exist by Result 5.10
21	2	not exist by Corollary 5.9	21	5	not exist by Corollary 5.14 with q=3
22	3	not exist by Corollary 5.14 with q=2	22	7	not exist by Theorem 5.18
23	2	not exist by Corollary 5.9	23	11	exist by Result 1.67 (d)
24	23	not exist by Result 5.10	25	2	not exist by Corollary 5.9
25	3	exist by Result 1.67 (d)	26	5	not exist by Corollary 5.14 with q=2
27	2	not exist by Corollary 5.9	27	13	exist by Result 1.67 (d)
28	3	not exist by Theorem 5.18	29	2	not exist by Corollary 5.9
29	7	exist by Result 1.67 (d)	30	29	not exist by Result 5.10
31	2	not exist by Corollary 5.9	31	3	exist by Result 1.67 (d)
31	5	exist by Result 1.67 (d)	32	31	exist by Result 1.67 (d)
33	2	not exist by Corollary 5.9	34	3	not exist by Corollary 5.14 with q=2
34	11	not exist by Corollary 5.14 with q=2	35	2	not exist by Corollary 5.9
35	17	not exist by Corollary 5.14 with q=5	36	5	not exist by Corollary 5.13 with q=2
36	7	not exist by Corollary 5.13 with q=3	37	2	not exist by Corollary 5.9
37	3	exist by Result 1.67 (d)	38	37	not exist by Result 5.10
39	2	not exist by Corollary 5.9	39	19	not exist by Corollary 5.14 with q=3
40	3	not exist by Corollary 5.14 with q=2	40	13	not exist by Corollary 5.14 with q=2
41	2	not exist by Corollary 5.9	41	5	exist by Result 1.67 (d)
42	41	not exist by Result 5.10	43	2	not exist by Corollary 5.9
43	3	exist by Result 1.67 (d)	43	7	exist by Result 1.67 (d)
44	43	not exist by Result 5.10	45	2	not exist by Corollary 5.9
45	11	not exist by Theorem 5.18	46	3	not exist by Corollary 5.14 with q=2
46	5	not exist by Corollary 5.14 with q=2	47	2	not exist by Corollary 5.9
47	23	exist by Result 1.67 (d)			
48	47	not exist by Result 5.10	49	2	not exist by Corollary 5.9
49	3	exist by Result 1.67 (d)	50	7	not exist by Result 5.19
51	2	not exist by Corollary 5.9	51	5	not exist by Corollary 5.14 with q=3
52	3	not exist by Theorem 5.18	52	17	not exist by Corollary 5.14 with q=13
53	2	not exist by Corollary 5.9	53	13	exist by Result 1.67 (d)
54	53	not exist by Result 5.10	55	2	not exist by Corollary 5.9
55	3	not exist by Corollary 5.14 with q=5	56	5	not exist by Corollary 5.14 with q=2
56	11	not exist by Corollary 5.14 with q=2	57	2	not exist by Corollary 5.9
57	7	not exist by Corollary 5.14 with q=3	58	3	not exist by Corollary 5.14 with q=2
58	19	not exist by Corollary 5.14 with q=2	59	2	not exist by Corollary 5.9
59	29	exist by Result 1.67 (d)	60	59	not exist by Result 5.10
61	2	not exist by Corollary 5.9	61	3	exist by Result 1.67 (d)
61	5	exist by Result 1.67 (d)	62	61	not exist by Result 5.10
63	2	not exist by Corollary 5.9	63	31	not exist by Corollary 5.14 with q=3
64	3	exist by Result 1.67 (d)	64	7	exist by Result 1.67 (d)

65	2	not exist by Corollary 5.9	66	5	not exist by Corollary 5.14 with q=2
66	13	not exist by Corollary 5.14 with q=2	67	2	not exist by Corollary 5.9
67	3	exist by Result 1.67 (d)	67	11	exist by Result 1.67 (d)
68	67	not exist by Result 5.10	69	2	not exist by Corollary 5.9
69	17	not exist by Corollary 5.14 with q=3	70	3	not exist by Corollary 5.14 with q=2
70	23	not exist by Corollary 5.14 with q=5	71	2	not exist by Corollary 5.9
71	5	exist by Result 1.67 (d)	71	7	exist by Result 1.67 (d)
72	71	not exist by Result 5.10	73	2	not exist by Corollary 5.9
73	3	exist by Result 1.67 (d)	74	73	not exist by Result 5.10
75	2	not exist by Corollary 5.9	75	37	not exist by Corollary 5.14 with q=3
76	3	not exist by Result 5.19	77	2	not exist by Corollary 5.9
77	2	not exist by Corollary 5.9	78	7	not exist by Corollary 5.14 with q=3
78	11	not exist by Corollary 5.14 with q=2	79	2	not exist by Corollary 5.9
79	39	exist by Result 1.67 (d)	80	79	not exist by Result 5.10
81	2	not exist by Corollary 5.9	81	5	exist by Result 1.67 (d)
82	3	not exist by Corollary 5.14 with q=2	83	2	not exist by Corollary 5.9
83	41	exist by Result 1.67 (d)	84	83	not exist by Result 5.10
85	2	not exist by Corollary 5.9	85	3	not exist by Corollary 5.14 with q=5
85	7	not exist by Corollary 5.14 with q=5	86	5	not exist by Corollary 5.14 with q=2
85	17	not exist by Corollary 5.14 with q=2	87	2	not exist by Corollary 5.9
87	43	not exist by Corollary 5.14 with q=3	88	3	not exist by Corollary 5.14 with q=2
88	29	not exist by Corollary 5.14 with q=2	89	2	not exist by Corollary 5.9
89	11	exist by Result 1.67 (d)	90	89	not exist by Result 5.10
91	2	not exist by Corollary 5.9	91	3	exist by Result 1.67 (d)
91	5	exist by Result 1.67 (d)	92	91	not exist by Result 5.10
93	2	not exist by Corollary 5.9	93	23	not exist by Corollary 5.14 with q=7
94	3	not exist by Corollary 5.14 with q=2	94	31	not exist by Result 5.19
95	2	not exist by Corollary 5.9	95	47	not exist by Corollary 5.14 with q=5
96	5	not exist by Corollary 5.14 with q=2	96	19	not exist by Corollary 5.14 with q=2
97	2	not exist by Corollary 5.9	97	3	exist by Result 1.67 (d)
98	97	not exist by Result 5.10	99	2	not exist by Corollary 5.9
99	7	not exist by Result 5.19	100	3	not exist by Result 5.19
100	11	not exist by Result 5.19			

Table 5.3: Existence Status of Nearly Perfect Sequences

n	p	Existence Status	n	p	Existence Status
2	2	exist by Result 5.22	3	3	not exist by Theorem 5.24 with q=3
4	2	exist by Result 5.22	5	5	not exist by Corollary 5.26 with q=2
6	2	exist by Result 5.22	6	3	exist by Result 5.22

7	7	not exist by Theorem 5.24 with q=7	8	2	not exist by Corollary 5.27 with q=3
9	3	not exist by Corollary 5.26 with q=2	10	2	exist by Result 5.22
10	5	exist by Result 5.22	11	11	not exist by Theorem 5.24 with q=11
12	2	exist by Result 5.22	12	3	exist by Result 5.22
13	13	not exist by Corollary 5.26 with q=2	14	2	not exist by Corollary 5.26 with q=3
14	7	not exist by Corollary 5.26 with q=3	15	3	not exist by Corollary 5.27 with q=2
15	5	not exist by Corollary 5.27 with q=2	16	2	exist by Result 5.22
17	17	not exist by Corollary 5.26 with q=2	18	2	exist by Result 5.22
18	3	exist by Result 5.22	19	19	not exist by Theorem 5.24 with q=19
20	2	not exist by Corollary 5.26 with q=3	20	5	not exist by Corollary 5.26 with q=3
21	3	not exist by Corollary 5.26 with q=2	21	7	?
22	2	exist by Result 5.22	22	11	exist by Result 5.22
23	23	not exist by Theorem 5.24 with q=23	24	2	not exist by Corollary 5.27 with q=5
24	3	not exist by Corollary 5.27 with q=5	25	5	not exist by Corollary 5.26 with q=2
26	2	not exist by Corollary 5.26 with q=3	26	13	?
27	3	?	28	2	exist by Result 5.22
28	7	exist by Result 5.22	29	29	not exist by Corollary 5.26 with q=2
30	2	exist by Result 5.22	30	3	exist by Result 5.22
30	5	exist by Result 5.22	31	31	not exist by Theorem 5.24 with q=31
32	2	not exist by Corollary 5.26 with q=3	33	3	not exist by Corollary 5.26 with q=2
33	11	not exist by Corollary 5.26 with q=2	34	2	not exist by Corollary 5.26 with q=5
	17	not exist by Corollary 5.26 with q=5	35	5	?
35	7	not exist by Corollary 5.27 with q=3	36	2	exist by Result 5.22
36	3	exist by Result 5.22	37	37	not exist by Theorem 5.24 with q=37
38	2	not exist by Corollary 5.26 with q=3	38	19	not exist by Corollary 5.26 with q=3
39	3	not exist by Corollary 5.26 with q=2	39	13	not exist by Corollary 5.26 with q=2
40	2	exist by Result 5.22	40	5	exist by Result 5.22
41	41	not exist by Corollary 5.26 with q=2	42	2	exist by Result 5.22
42	3	exist by Result 5.22	42	7	exist by Result 5.22
43	43	not exist by Theorem 5.24 with q=43	44	2	not exist by Corollary 5.26 with q=5
44	11	?	45	3	not exist by Corollary 5.26 with q=2
45	5	not exist by Corollary 5.26 with q=2	46	2	exist by Result 5.22
46	23	exist by Result 5.22	47	47	not exist by Theorem 5.24 with q=47
48	2	not exist by Corollary 5.27 with q=7	48	3	not exist by Corollary 5.27 with q=7
49	7	not exist by Corollary 5.27 with q=5	50	2	not exist by Corollary 5.26 with q=3
50	5	not exist by Corollary 5.26 with q=3	51	3	?
51	17	not exist by Corollary 5.26 with q=13	52	2	exist by Result 5.22
52	13	exist by Result 5.22	53	53	not exist by Corollary 5.26 with q=2
54	2	not exist by Corollary 5.26 with q=5	54	3	not exist by Corollary 5.26 with q=5
55	5	not exist by Corollary 5.26 with q=2	55	11	not exist by Corollary 5.26 with q=2

56	2	not exist by Corollary 5.26 with q=3	56	7	not exist by Corollary 5.26 with q=3
57	3	not exist by Corollary 5.26 with q=2	57	19	not exist by Corollary 5.26 with q=2
58	2	exist by Result 5.22	58	29	exist by Result 5.22
59	59	not exist by Theorem 5.24 with q=59	60	2	exist by Result 5.22
60	3	exist by Result 5.22	60	5	exist by Result 5.22
61	61	not exist by Corollary 5.26 with q=2	62	2	not exist by Corollary 5.26 with q=7
62	31	not exist by Corollary 5.27 with q=3	63	3	not exist by Corollary 5.27 with q=2
63	7	?	64	2	not exist by Corollary 5.26 with q=5
65	5	not exist by Corollary 5.26 with q=2	65	13	not exist by Corollary 5.26 with q=2
66	2	exist by Result 5.22	66	2	exist by Result 5.22
66	11	exist by Result 5.22	67	67	not exist by Theorem 5.24 with q=67
68	2	not exist by Corollary 5.26 with q=3	68	17	not exist by Corollary 5.26 with q=3
69	3	not exist by Corollary 5.26 with q=2	69	23	not exist by Corollary 5.26 with q=5
70	2	exist by Result 5.22	70	5	exist by Result 5.22
70	7	exist by Result 5.22	71	71	not exist by Theorem 5.24 with q=71
72	2	exist by Result 5.22	72	3	exist by Result 5.22
73	73	not exist by Theorem 5.24 with q=73	74	2	not exist by Corollary 5.26 with q=3
74	37	not exist by Corollary 5.26 with q=3	75	3	?
75	5	not exist by Corollary 5.26 with q=15	76	2	not exist by Corollary 5.26 with q=7
76	19	?	77	7	?
77	11	not exist by Corollary 5.26 with q=2	78	2	exist by Result 5.22
78	39	exist by Result 5.22	79	79	not exist by Theorem 5.24 with q=79
80	2	not exist by Corollary 5.27 with q=3	80	5	not exist by Corollary 5.27 with q=3
81	3	not exist by Corollary 5.27 with q=2	82	2	exist by Result 5.22
82	41	exist by Result 5.22	83	83	not exist by Theorem 5.24 with q=83
84	2	not exist by Corollary 5.26 with q=5	84	3	not exist by Corollary 5.26 with q=5
84	7	not exist by Corollary 5.26 with q=5	85	5	not exist by Corollary 5.26 with q=2
85	17	not exist by Corollary 5.26 with q=2	86	2	not exist by Corollary 5.26 with q=3
86	43	not exist by Corollary 5.26 with q=3	87	3	not exist by Corollary 5.26 with q=11
87	29	not exist by Corollary 5.26 with q=11	88	2	exist by Result 5.22
88	11	exist by Result 5.22	89	89	not exist by Corollary 5.26 with q=5
90	2	exist by Result 5.22	90	3	exist by Result 5.22
90	5	exist by Result 5.22	91	91	not exist by Theorem 5.24 with q=91
92	2	not exist by Corollary 5.26 with q=3	92	23	?
93	3	not exist by Corollary 5.26 with q=2	93	31	?
94	2	not exist by Corollary 5.26 with q=5	94	47	not exist by Corollary 5.26 with q=5
95	5	not exist by Corollary 5.26 with q=2	95	19	not exist by Corollary 5.26 with q=2
96	2	exist by Result 5.22	96	3	exist by Result 5.22
97	97	not exist by Corollary 5.26 with q=2	98	2	not exist by Corollary 5.26 with q=11
98	7	?	99	3	not exist by Corollary 5.27 with q=5

99	11	?	100	2	exist by Result 5.22

Bibliography

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.

A. A. Albert. Generalized twisted fields. *Pacific Journal of Mathematics*, 11:1–8, 1961a.

A. A. Albert. Isotopy for generalized twisted fields. *Anais da Academia Brasileira de Ciências*, 33:265–275, 1961b.

J. André. Über nicht-Desarguessche ebenen mit transitiver translationsgruppe. *Mathematische Zeitschrift*, 60:156–186, 1954.

K. T. Arasu and S. L. Ma. Abelian difference sets without self-conjugacy. *Designs, Codes and Cryptography. An International Journal*, 15(3):223–230, 1998.

R. Baer. Homogeneity of projective planes. *American Journal of Mathematics*, 64: 137–152, 1942.

S. Ball and M. Lavrauw. Commutative semifields of rank 2 over their middle nucleus. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, page 1–21. Springer, Berlin, 2002.

A. Barlotti. Le possibili configurazioni del sistema delle coppie punto-retta (A, a) per cui un piano grafico risulta (A, a)-transitivo. *Boll. Un. Mat. Ital. (3)*, 12: 212–226, 1957.

T. P. Berger and P. Charpin. The permutation group of affine-invariant extended cyclic codes. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 42(6):2194–2209, 1996.

T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

J. Bierbrauer. New commutative semifields and their nuclei. In M. Bras-Amorós and T. Hoholdt, editors, *Applied Algebra, Algebraic Algorithms and*

Error-Correcting Codes, volume 5527 of *Lecture Notes in Computer Science*, pages 179–185, Tarragona, Spain, June 2009. Springer Berlin / Heidelberg.

J. Bierbrauer. New semifields, PN and APN functions. *Des. Codes Cryptography*, 54(3):189–200, 2010.

J. Bierbrauer. Semifields,theory and elementary constructions. invited talk presented in Combinatorics 2012, Perugia, September 2012.

J. Bierbrauer and G. M. Kyureghyan. On the projection construction of planar and APN mappings. manuscript, appeared at YACC 2010, Porquerolles Island, France, 2010.

M. Biliotti, V. Jha, and N. L. Johnson. The collineation groups of generalized twisted field planes. *Geometriae Dedicata*, 76:97–126, 1999.

A. Blokhuis, D. Jungnickel, and B. Schmidt. Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2. *Proceedings of the American Mathematical Society*, 130(5):1473–1476, 2002.

A. Bonnecaze and I. M. Duursma. Translates of linear codes over $\mathbb{Z}_4$. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 43(4): 1218–1230, 1997.

R. C. Bose. An affine analogue of singer's theorem. *J. Indian Math. Soc. (N.S.)*, 6: 1–15, 1942.

R. Brauer. On the connection between the ordinary and the modular characters of groups of finite order. *Annals of Mathematics. Second Series*, 42:926–935, 1941.

K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN permutation in dimension six. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, page 33–42. Amer. Math. Soc., Providence, RI, 2010.

R. H. Bruck. Difference sets in a finite group. *Transactions of the American Mathematical Society*, 78:464–481, 1955.

R. H. Bruck and H. J. Ryser. The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics. Journal Canadien de Mathématiques*, 1:88–93, 1949.

L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p. In *SETA '08: Proceedings of the 5th international conference on Sequences and Their Applications*, page 403–414, Berlin, Heidelberg, 2008. Springer-Verlag.

L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. *Cryptography and Communications*, 3:1–16, 2011.

L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 52(3):1141–1152, 2006.

A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean Line-Sets. *Proceedings of the London Mathematical Society. Third Series*, 75(2):436–480, 1997.

I. Cardinali, O. Polverino, and R. Trombetti. Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$. *European Journal of Combinatorics*, 27(6):940–961, Aug. 2006.

C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 134 of *Encyclopedia of Mathematics and its Applications*, chapter 8, page 257–297. Cambridge University Press, 2010.

C. Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography*, 59(1):89–109, 2011.

C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography. An International Journal*, 15(2):125–156, 1998.

R. Casse. *Projective geometry: an introduction*. Oxford University Press, Oxford, 2006.

A. Çeşmelioğlo and W. Meidl. Bent functions of maximal degree. *IEEE Transactions on Information Theory*, 58(2):1186–1190, Feb. 2012.

A. Çeşmelioğlo and W. Meidl. A construction of bent functions from plateaued functions. *Designs, Codes and Cryptography*, 66(1-3):231–242, Jan. 2013.

A. Çeşmelioğlo, G. McGuire, and W. Meidl. A construction of weakly and non-weakly regular bent functions. *Journal of Combinatorial Theory, Series A*, 119(2): 420–429, Feb. 2012.

F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in cryptology—EUROCRYPT '94 (Perugia)*, volume 950 of *Lecture Notes in Comput. Sci.*, page 356–365. Springer, Berlin, 1995.

Y. M. Chee, Y. Tan, and Y. Zhou. Almost p-ary perfect sequences. In *Sequences and their applications—SETA 2010*, volume 6338 of *Lecture Notes in Comput. Sci.*, page 399–415. Springer, Berlin, 2010.

S. Cohen and M. Ganley. Commutative semifields, two-dimensional over their middle nuclei. *Journal of Algebra*, 75:373–385, 1982.

S. D. Cohen. Finite field elements with specified order and traces. *Designs, Codes and Cryptography*, 36(3):331–340, 2005.

C. J. Colbourn and J. H. Dinitz, editors. *Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Advances in Mathematics*, 217(1), 2008.

R. S. Coulter and P. Kosick. Commutative semifields of order 243 and 3125. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, page 129–136. Amer. Math. Soc., Providence, RI, 2010.

R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptography*, 10(2):167–184, 1997.

R. S. Coulter, M. Henderson, and P. Kosick. Planar polynomials for commutative semifields with specified nuclei. *Des. Codes Cryptography*, 44(1-3):275–286, 2007.

P. Dembowski. Verallgemeinerungen von transitivitätsklassen endlicher projektiver ebenen. *Mathematische Zeitschrift*, 69:59–89, 1958.

P. Dembowski. Gruppentheoretische kennzeichnungen der endlichen desarguesschen ebenen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 29:92–106, 1965.

P. Dembowski. *Finite Geometries*. Springer, 1997.

P. Dembowski and F. Piper. Quasiregular collineation groups of finite projective planes. *Mathematische Zeitschrift*, 99:53–75, 1967.

U. Dempwolff. Semifield planes of order 81. *Journal of Geometry*, 89(1-2):1–16, 2008.

U. Dempwolff and M. Röder. On finite projective planes defined by planar monomials. *Innovations in Incidence Geometry*, 4:103–108, 2006.

L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(4): 514–522, 1906.

J. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.

C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Comb. Theory Ser. A*, 113(7):1526–1535, 2006.

Y. Edel and A. Pott. On designs and multiplier groups constructed from almost perfect nonlinear functions. In *Cryptography and coding*, volume 5921 of *Lecture Notes in Comput. Sci.*, page 383–401. Springer, Berlin, 2009a.

Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009b.

J. E. H. Elliott and A. T. Butson. Relative difference sets. *Illinois Journal of Mathematics*, 10:517–531, 1966.

M. Ganley. Central weak nucleus semifields. *European Journal of Combinatorics*, 2: 339–347, 1981.

M. J. Ganley. On a paper of P. Dembowski and T. G. Ostrom. *Archiv der Mathematik*, 27(1):93–98, 1976.

M. J. Ganley. Direct product difference sets. *Journal of Combinatorial Theory. Series A*, 23(3):321–332, 1977.

M. J. Ganley and R. L. McFarland. On quasiregular collineation groups. *Archiv der Mathematik*, 26:327–331, 1975.

D. Ghinelli and D. Jungnickel. Finite projective planes with a large abelian group. In *Surveys in combinatorics, 2003 (Bangor)*, volume 307 of *London Math. Soc. Lecture Note Ser.*, page 175–237. Cambridge Univ. Press, Cambridge, 2003.

D. Ghinelli and F. Merola. Lenz-barlotti classification and related open problems: an update. *Quaderni Elettronici del Seminario di Geometria Combinatoria*, 20E, Ottobre 2005.

R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154 – 156, Jan. 1968.

S. W. Golomb and G. Gong. *Signal design for good correlation*. Cambridge University Press, Cambridge, 2005.

B. Gordon, W. H. Mills, and L. R. Welch. Some new difference sets. *Canadian Journal of Mathematics*, 14(0):614–625, Jan. 1962.

M. Hall, Jr. Projective planes. *Transactions of the American Mathematical Society*, 54:229–277, 1943.

M. Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

A. Hammons, P. Kumar, A. Calderbank, N. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *Information Theory, IEEE Transactions on*, 40(2):301–319, 1994.

T. Helleseth and A. Kholosha. On the dual of monomial quadratic p-ary bent functions. In *Sequences, subsequences, and consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, page 50–61. Springer, Berlin, 2007.

T. Helleseth and A. Kholosha. New binomial bent functions over the finite fields of odd characteristic. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 56(9):4646–4652, 2010.

T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applicable Algebra in Engineering, Communication and Computing*, 8(5): 363–370, July 1997.

T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang. Proofs of two conjectures on ternary weakly regular bent functions. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 55(11):5272–5283, 2009.

F. Hernando and G. McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *Journal of Algebra*, 343(1):78–92, Oct. 2011.

C. J. Hillar and D. Rhea. Automorphisms of finite abelian groups. http://arxiv.org/abs/math.GR/0605185, 2006.

Y. Hiramine. Factor sets associated with regular collineation groups. *Journal of Algebra*, 142(2):414–423, Oct. 1991.

Y. Hiramine. Difference sets relative to disjoint subgroups. *Journal of Combinatorial Theory, Series A*, 88(2):205–216, Nov. 1999.

J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

C. Y. Ho. Finite projective planes with abelian transitive collineation groups. *Journal of Algebra*, 208(2):533–550, 1998.

K. J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, 2007.

D. R. Hughes. Planar division neo-rings. *Transactions of the American Mathematical Society*, 80:502–527, 1955.

D. R. Hughes. Collineations and generalized incidence matrices. *Transactions of the American Mathematical Society*, 86:284–296, 1957.

D. R. Hughes and F. C. Piper. *Projective planes*. Springer-Verlag, New York, 1973.

D. R. Hughes and F. C. Piper. *Design theory*. Cambridge University Press, Cambridge, second edition, 1988.

N. Jacobson. *Lectures in abstract algebra. III*. Springer-Verlag, New York, 1975.

H. Janwa, G. Mcguire, and R. Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$. *Journal of Algebra*, 178 (2):665–676, Dec. 1995.

D. Jedlicka. APN monomials over $GF(2^n)$ for infinitely many n. *Finite Fields and Their Applications*, 13(4):1006–1028, Nov. 2007.

N. L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2007.

D. Jungnickel. On automorphism groups of divisible designs. *Canadian Journal of Mathematics. Journal Canadien de Mathématiques*, 34(2):257–297, 1982.

D. Jungnickel. Divisible semiplanes, arcs, and relative difference sets. *Canadian Journal of Mathematics*, 39(4):1001–1024, 1987a.

D. Jungnickel. On a theorem of Ganley. *Graphs Combin.*, 3(2):141–143, 1987b.

D. Jungnickel. On automorphism groups of divisible designs. II. group invariant generalised conference matrices. *Archiv der Mathematik*, 54(2):200–208, 1990.

D. Jungnickel. On affine difference sets. *Sankhya. The Indian Journal of Statistics. Series A*, 54(Special Issue):219–240, 1992.

D. Jungnickel. *Finite fields*. Bibliographisches Institut, Mannheim, 1993.

D. Jungnickel. The isomorphism problem for abelian projective planes. *Applicable Algebra in Engineering, Communication and Computing*, 19(3):195–200, 2008.

D. Jungnickel and M. J. de Resmini. Another case of the prime power conjecture for finite projective planes. *Advances in Geometry*, 2(3):215–218, 2002.

D. Jungnickel and A. Pott. Computational nonexistence results for abelian affine difference sets. *Congressus Numerantium. A Conference Journal on Numerical Themes*, 68:91–98, 1989.

D. Jungnickel and A. Pott. Perfect and almost perfect sequences. In *Discrete Applied Mathematics. The Journal of Combinatorial Algorithms, Informatics and Computational Sciences*, volume 95, page 331–359, 1999.

D. Jungnickel and B. Schmidt. Difference sets: an update. In *Geometry, combinatorial designs and related structures (Spetses, 1996)*, volume 245 of *London Math. Soc. Lecture Note Ser.*, page 89–112. Cambridge Univ. Press, Cambridge, 1997.

D. Jungnickel and B. Schmidt. Difference sets: a second update. *Rendiconti del Circolo Matematico di Palermo. Serie II. Supplemento*, (53):89–118, 1998.

W. M. Kantor. Projective planes of type I-4. *Geometriae Dedicata*, 3:335–346, 1974.

W. M. Kantor. Commutative semifields and symplectic spreads. *Journal of Algebra*, 270(1):96–114, 2003.

W. M. Kantor. Finite semifields. In *Finite geometries, groups, and computation*, page 103–114. Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

W. M. Kantor and M. E. Williams. Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Transactions of the American Mathematical Society*, 356(3):895–938, 2004.

A. D. Keedwell. Construction, properties and applications of finite neofields. *Commentationes Mathematicae Universitatis Carolinae*, 41(2):283–297, 2000.

E. Kleinfeld. Techniques for enumerating Veblen-Wedderburn systems. *Journal of the Association for Computing Machinery*, 7:330–337, 1960.

N. Knarr and M. Stroppel. Polarities of shift planes. *Advances in Geometry*, 9(4): 577–603, Aug. 2009.

D. E. Knuth. A class of projective planes. *Transactions of the American Mathematical Society*, 115:541–549, Mar. 1965a.

D. E. Knuth. Finite semifields and projective planes. *Journal of Algebra*, 2:182–217, 1965b.

G. M. Kyureghyan and A. Pott. Some theorems on planar mappings. In *Arithmetic of finite fields*, volume 5130 of *Lecture Notes in Comput. Sci.*, page 117–122. Springer, Berlin, 2008.

C. W. H. Lam, L. Thiel, and S. Swiercz. The nonexistence of finite projective planes of order 10. *Canadian Journal of Mathematics. Journal Canadien de Mathématiques*, 41(6):1117–1123, 1989.

M. Lavrauw and O. Polverino. Finite semifields. In L. Storme and J. De Beule, editors, *Current research topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, 2011.

H. Lenz. Kleiner desarguesscher satz und dualität in projektiven ebenen. *Jberr. Deutsch. Math. Verein.*, 57(Abt. 1):20–31, 1954.

C. Li, S. Ling, and L. Qu. On the covering structures of two classes of linear codes from perfect nonlinear functions. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 55(1):70–82, 2009.

P. Li, C. Li, and Y. Zhou. Weight distributions of linear codes from perfect nonlinear functions of Dembowski-Ostrom type. *Journal of applied sciences*, 28 (5):441–446, September 2010.

R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

S. L. Ma and W. S. Ng. On non-existence of perfect and nearly perfect sequences. *International Journal of Information and Coding Theory. IJICOT*, 1(1):15–38, 2009.

F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing Co., Amsterdam, 1977.

G. Marino, O. Polverino, and R. Trombetti. Towards the classification of rank 2 semifields 6-dimensional over their center. *Designs, Codes and Cryptography. An International Journal*, 61(1):11–29, 2011.

G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *Journal of Algebra*, 47(2):400–410, 1977.

G. Menichetti. n-dimensional algebras over a field with a cyclic extension of degree n. *Geometriae Dedicata*, 63(1):69–94, 1996.

P. Müller. On the collineation group of cyclic planes. *Journal of Combinatorial Theory. Series A*, 65(1):60–66, 1994.

K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, page 55–64. Springer, Berlin, 1994.

T. G. Ostrom and A. Wagner. On projective and affine planes with transitive collineation groups. *Mathematische Zeitschrift*, 71:186–199, 1959.

U. Ott. Endliche zyklische ebenen. *Mathematische Zeitschrift*, 144(3):195–215, 1975.

F. Özbudak, O. Yayla, and C. C. Yıldırım. Nonexistence of certain almost p-ary perfect sequences. In T. Helleseth and J. Jedwab, editors, *Sequences and Their Applications – SETA 2012*, number 7280 in Lecture Notes in Computer Science, page 13–24. Springer Berlin Heidelberg, Jan. 2012.

E. T. Parker. On collineations of symmetric designs. *Proceedings of the American Mathematical Society*, 8:350–351, 1957.

M. G. Parker and A. Pott. On boolean functions which are bent and negabent. In *Sequences, subsequences, and consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, page 9–23. Springer, Berlin, 2007.

T. Penttila and B. Williams. Ovoids of parabolic spaces. *Geometriae Dedicata*, 82 (1-3):1–19, November 2004.

I. Pieper-Seier and B. Spille. Remarks on the paper: "on strong isotopy of dickson semifields and geometric implications". *Results in Mathematics. Resultate der Mathematik*, 35(3-4):310–313, 1999.

A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

A. Pott. A survey on relative difference sets. In *Groups, difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State Univ. Math. Res. Inst. Publ.*, page 195–232. de Gruyter, Berlin, 1996.

A. Pott and S. P. Bradley. Existence and nonexistence of almost-perfect autocorrelation sequences. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 41(1):301–304, 1995.

A. Pott and Y. Zhou. Switching construction of planar functions on finite fields. In *Proceedings of the Third international conference on Arithmetic of finite fields*, WAIFI'10, page 135–150, Berlin, Heidelberg, 2010. Springer-Verlag.

A. Pott and Y. Zhou. A character theoretic approach to planar functions. *Cryptography and Communications*, 3(4):293–300, Dec. 2011.

A. Pott, Q. Wang, and Y. Zhou. Sequences and functions derived from projective planes and their difference sets. In F. Özbudak and F. Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields*, volume 7369 of *Lecture Notes in Computer Science*, page 64–80. Springer Berlin / Heidelberg, 2012.

I. F. Rúa and E. F. Combarro. Commutative semifields of order 3^5. *Communications in Algebra*, 40(3):988–996, 2012.

I. F. Rúa, E. F. Combarro, and J. Ranilla. Classification of semifields of order 64. *Journal of Algebra*, 322(11):4011–4029, 2009.

A. Ranum. The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. *Transactions of the American Mathematical Society*, 8(1):71–91, 1907.

C. Riera and M. Parker. Generalized bent criteria for boolean functions (I). *Information Theory, IEEE Transactions on*, 52(9):4142–4159, Sept. 2006.

O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory. Series A*, 20 (3):300–305, 1976.

Z. Scherr and M. E. Zieve. Planar monomials in characteristic 2. *arXiv:1302.1244*, Feb. 2013.

B. Schmidt. On (p^a, p^b, p^a, p^{a-b})-relative difference sets. *Journal of Algebraic Combinatorics*, 6(3):279–297, 1997.

B. Schmidt. *Characters and cyclotomic fields in finite geometry*, volume 1797 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.

K.-U. Schmidt and Y. Zhou. Planar functions over fields of characteristic two. *arXiv:1301.6999*, Jan. 2013.

A. G. Shanbhag, P. V. Kumar, and T. Helleseth. An upper bound for the extended kloosterman sums over galois rings. *Finite Fields and their Applications*, 4(3): 218–238, 1998.

J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

R. G. Stanton and R. C. Mullin. On the nonexistence of a class of circulant balanced weighing matrices. *SIAM Journal on Applied Mathematics*, 30(1):98–102, 1976.

W. Su, A. Pott, and X. Tang. Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. *arXiv:1205.6568*, May 2012.

K. Thas. Finite flag-transitive projective planes: a survey and some remarks. *Discrete Mathematics*, 266(1-3):417–429, 2003.

R. J. Walker. Determination of division algebras with 32 elements. In *Proc. Sympos. Appl. Math., Vol. XV*, pages 83–85. Amer. Math. Soc., Providence, R.I., 1963.

Z.-X. Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co. Inc., River Edge, NJ, 2003.

J. H. M. Wedderburn. A theorem on finite algebras. *Transaction of the American Mathematical Society*, 6(3):349–352, 1905.

G. Weng and X. Zeng. Further results on planar DO functions and commutative semifields. *Designs, Codes and Cryptography*, 63(3):413–423, 2012.

J. Wolfmann. Almost perfect autocorrelation sequences. *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, 38(4):1412–1418, 1992.

Q. Xiang. Recent progress in algebraic design theory. *Finite Fields and their Applications*, 11(3):622–653, 2005.

H. Zassenhaus. Über endliche fastkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 11(1):187–220, 1935.

Z. Zha and X. Wang. New families of perfect nonlinear polynomial functions. *Journal of Algebra*, 322(11):3912–3918, 2009.

Z. Zha, G. M. Kyureghyan, and X. Wang. Perfect nonlinear binomials and their semifields. *Finite Fields and Their Applications*, 15(2):125–133, 2009.

Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, Feb. 2013.

M. Zorn. Theorie der alternativen ringe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 8(1):123–147, Dec. 1931.

Index

Notation

$\mathrm{AG}(n,q)$	n-dimensional affine (or vector) space over $\mathbb{F}_q$
$\mathrm{A\Gamma L}(n,q)$	the semi-affine group of degree n over $\mathbb{F}_q$
$\mathrm{AGL}(n,q)$	the affine group of degree n over $\mathbb{F}_q$
$\mathrm{Aut}(\mathbb{P})$	the autotopism group of a presemifield $\mathbb{P}$
$\mathrm{Aut}(\mathbf{P})$	the automorphism group of a plane $\mathbf{P}$
$\mathrm{Aut}_S(\mathbb{P})$	the strong autotopism group of a presemifield $\mathbb{P}$
$\mathbf{A}$	an arbitrary affine plane
$\mathbb{M}_{m\times n}(R)$	the set of $m \times n$ matrices with entries in a ring R
$\mathbb{P}$	an arbitrary presemifield
S	an arbitrary semifield
$\mathbf{P}$	an arbitrary projective plane
$\mathbb{C}$	the complex numbers
χ	character of some abelian group
χ_0	the principal character of some abelian group
$\mathcal{L}$	the lines set of some plane
$\mathcal{M}(D)$	the multiplier group of (generalized, relative) difference set D
$\mathcal{P}$	the points set of some plane
C_n	the cyclic group of order n
$\mathbb{F}_q$	the finite field with q elements
$\mathrm{Gal}(\mathbb{F}_{p^n})$	the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$
$\mathrm{Gal}(\mathbb{K}_2/\mathbb{K}_1)$	the Galois group of the extension of $\mathbb{K}_2$ over $\mathbb{K}_1$

$\Gamma\mathrm{L}(n,q)$	the semi-linear group of degree n over $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	the general linear group of degree n over $\mathbb{F}_q$
$\mathbb{K}$	an arbitrary field
$\langle g_1, g_2, \ldots, g_n \rangle$	the group generated by $g_1, \ldots, g_n$
$\exp(G)$	the exponent of group G, i.e. the smallest positive integer m such that, for every $g \in G$, $g^m = 1$
$\mathrm{MAut}(C)$	the monomial automorphism group of a linear code C
$\mathrm{PAut}(C)$	the permutation automorphism group of a linear code C
$\mathrm{PG}(2,\mathbb{K})$	2-dimensional projective space over $\mathbb{K}$
$\mathrm{PG}(n,q)$	n-dimensional projective space over $\mathbb{F}_q$
$\mathrm{PGL}(n,q)$	the projective general linear group of degree n over $\mathbb{F}_q$
$\mathbb{R}$	the real numbers
$\mathbb{Z}/n\mathbb{Z}$	the residue class ring of integers modulo n
Tr	the absolute trace function defined with respect to a finite field extension $\mathbb{F}_q/\mathbb{F}_p$, where $\mathbb{F}_p$ is the prime subfield of $\mathbb{F}_q$.
$\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}$	the trace function defined with respect to a finite field extension $\mathbb{F}/\mathbb{K}$
Tr_{q_1/q_0}	the trace function defined with respect to a finite field extension $\mathbb{F}_{q_1}/\mathbb{F}_{q_0}$
$\varnothing$	the empty set
$\lvert S \rvert$	number of elements in the set S
$\mathbb{Z}$	the integers
ζ_n	an n-th root of unity in $\mathbb{C}$
$D^{(t)}$	given $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, $D^{(t)} := \sum_{g \in G} a_g g^t$
$G \times H$	the direct product of G and H
$H \leq G$	H is a subgroup of G
$H \lhd G$	H is a normal subgroup of G
$H^\perp$	G is abelian, $H \leq G$ and $H^\perp := \{ \chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in H \}$

$N \rtimes H$	the semidirect product of N and H with $N \lhd N \rtimes H$
$p^r \parallel n$	p^r strictly divide n, namely, $p^r \mid n$ but $p^{r+1} \nmid n$
S^*	$S^* := S \setminus \{0\}$, where S is a set with addition and its additive identity is 0